



STO TECHNICAL REPORT

TR-IST-124-Part-I

Heterogeneous Tactical Networks – Improving Connectivity and Network Efficiency

(Réseaux tactiques hétérogènes : amélioration
de la connectivité et de l'efficacité du réseau)

Final Report of NATO IST-124.



Published September 2019





STO TECHNICAL REPORT

TR-IST-124-Part-I

Heterogeneous Tactical Networks – Improving Connectivity and Network Efficiency

(Réseaux tactiques hétérogènes : amélioration
de la connectivité et de l'efficacité du réseau)

Final Report of NATO IST-124.

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published September 2019

Copyright © STO/NATO 2019
All Rights Reserved

ISBN 978-92-837-2201-4

Single copies of this publication or of a part of it may be made for individual use only by those organisations or individuals in NATO Nations defined by the limitation notice printed on the front cover. The approval of the STO Information Management Systems Branch is required for more than one copy to be made or an extract included in another publication. Requests to do so should be sent to the address on the back cover.

Table of Contents

	Page
List of Figures	xv
List of Tables	xxii
List of Acronyms and Abbreviations	xxiv
Glossary	xxx
IST-124 Membership List	xxxii
 Executive Summary and Synthèse	 ES-1
 Heterogeneous Tactical Networks – Improving Connectivity and Network Efficiency	 1
1.0 Introduction	1
1.1 Scope of the Work	1
1.2 The IST-124 Group	2
1.3 Structure of the Report	3
2.0 Work Methods	3
3.0 Scenario and Emulation Environment	5
3.1 Operational Context for IST-124	5
3.2 Anglova Scenario	7
3.3 Experimentation Environment and Tools	7
3.4 Dynamically Allocated Virtual Clustering (DAVC)	8
4.0 Requirements	9
4.1 Requirements to the Routing Function and Management of Routing	9
4.1.1 Heterogeneous Network Routing	9
4.1.2 Robustness	9
4.1.3 Scalability	9
4.1.4 Resource Efficiency and QoS	10
4.1.5 Configuration and Management	10
4.1.6 Other Requirements	10
4.2 Requirements of the Quality of Service (QoS) and Resource Management (RM) Functions	10
4.2.1 General Requirements	10
4.2.2 Robustness	11
4.2.3 Scalability	11
4.2.4 Resource Efficiency and QoS	11
4.2.5 Flexibility	12
5.0 Connectivity and Routing	12
5.1 Routing Architecture Considerations	12
5.1.1 Routing Architecture Approaches at a Glance	13

5.1.2	Architecture Comparison	16
5.1.3	Conclusion	17
5.2	Security Architecture and Its Implication for Routing	17
5.3	Experiments and Analysis	19
5.3.1	The Density of Interconnection Platforms	20
5.3.2	Scalability of the Flat Architecture with the OLSR Protocol	21
5.3.3	OSPF Analysis	23
5.3.4	Naval Routing Experiment	24
5.3.5	Depth First Search Protocol for the Interconnect-Overlay Architecture	26
6.0	Quality of Service in Heterogeneous Networks	27
6.1	Discussion on QoS	29
6.1.1	QoS Mechanisms	29
6.1.2	Network States	29
6.1.3	Quality of Information (QoI), Value of Information (VoI)	30
6.2	Standardization of QoS	31
7.0	Achievements and Recommendations	31
7.1	Routing, Security, Quality of Service and Resource Management	31
7.2	Emulation Environment and Scenario	33
7.3	Summary	34
8.0	Activities	35
8.1	Activities at Conferences/Journals	35
8.1.1	Publications	35
8.1.2	Panel Debates	35
8.1.3	Demonstrations and Experiments	36
8.2	Work Meetings	37
8.2.1	Physical Meetings	37
8.2.2	Web Meetings	37
8.3	Liaison with Other Activities	37
9.0	References	38

Annex A – Operational Perspective for IST-124		A-1
A.1	Operational Context	A-1
A.2	Operational Concepts	A-2
A.2.1	Vignette 1: Intelligence Preparation of the Battlefield	A-4
A.2.2	Vignette 2: Deployment of Coalition Forces and Surveillance	A-5
A.2.2.1	Deployment of the Battalion	A-5
A.2.2.2	Maritime Deployment and Surveillance	A-6
A.2.3	Vignette 3: Insurgent Defeat, MEDEVAC, and EOD	A-6
A.2.3.1	Neutralization of Insurgents	A-7
A.2.3.2	Medical Evacuation	A-7
A.2.3.3	IED Neutralization	A-8
A.3	Actors and Roles	A-8
A.3.1	Equipment for the Operation	A-8
A.3.2	The Radio Characteristics	A-10

A.3.3	Traffic Flow	A-12
A.3.4	Services Implementation – General Network Requirements	A-14

Annex B – Emulation-Based Experiment and the Anglova Scenario **B-1**

B.1	Background	B-2
B.2	Elements of Emulation-Based Experimentation	B-3
B.2.1	Network Emulation Framework	B-3
B.2.2	Radio Models	B-5
B.2.3	Resources and Hosting/Management Tools	B-6
B.2.4	Scenarios	B-7
B.2.5	Candidate Algorithms/Protocols/Software	B-7
B.2.6	Network Load Generators	B-7
B.2.7	Metrics and Measurements	B-8
B.2.8	Visualization	B-8
B.3	Overview of the Anglova Scenario	B-8
B.4	Mobility Patterns in the Scenario	B-10
B.5	Radio Models and Communications Architecture	B-13
B.5.1	25 KHz Narrowband Radio Model	B-14
B.5.2	250 KHz Medium Band Radio Model	B-14
B.5.3	1.25 MHz Wideband Radio Model	B-15
B.5.4	Other Radio Models	B-15
B.5.5	Node Architecture	B-15
B.6	Scenario Characterization	B-17
B.6.1	Connectivity Internal to the Battalion in Vignette 2	B-17
B.6.2	Link Dynamics in Vignette 2	B-20
B.6.2.1	Preliminaries	B-21
B.6.2.2	Results	B-22
B.7	References	B-25

Annex C – Experimentation Environment and Tools **C-1**

C.1	EMANE Overview	C-1
C.2	Dynamically Allocated Virtual Clustering (DAVC) Deployment	C-2
C.3	VMware ESXi Deployment	C-3
C.4	Visualization Tools	C-10
C.4.1	Scripted Display Tools 3D (SDT-3D)	C-10
C.4.2	Mirage	C-12
C.4.3	OpenStreetMap Dataset	C-13
C.5	Scenario Playback Tools	C-14
C.5.1	EMANE Event Service Tool	C-14
C.5.1.1	Event Service XML	C-14
C.5.1.2	EEL Generator XML	C-15
C.5.1.3	EEL Source File	C-15
C.5.2	Anglova Scenario Player	C-15
C.6	Customized Pathloss Generation Tools	C-18
C.7	Open Issues	C-22

C.8	Conclusions	C-22
C.9	References	C-23

Annex D – IST-124 Experimentation Execution **D-1**

D.1	Experimentation Execution	D-1
D.1.1	Introduction	D-1
D.1.2	Anglova Scenario	D-2
D.1.3	Experimentation Environment	D-3
D.1.3.1	Dynamically Allocated Virtual Clustering Management System (DAVC)	D-3
D.1.3.2	Experimentation Virtual Machine	D-4
D.1.4	DAVC Cluster Configuration	D-4
D.1.4.1	Access and Logging into DAVC	D-4
D.1.4.2	Create the DAVC Cluster	D-5
D.1.4.3	Create the DAVC Cluster Networks	D-6
D.1.4.4	Create the DAVC Cluster Nodes	D-8
D.1.4.5	Launching the DAVC Cluster	D-11
D.1.4.6	Logging into the Experimentation Controller	D-13
D.1.5	Experimentation Virtual Machine File System	D-13
D.1.5.1	Experimentation Configuration Files	D-14
D.1.5.2	Experimentation Environment Network Plan	D-15
D.1.5.3	EMANE Configuration Files	D-18
D.1.5.4	EMANE Event Service Configuration Files	D-22
D.1.5.5	Experimentation Scripts	D-24
D.1.6	Launching an Anglova Vignette	D-26
D.1.7	Launching a CUSTOM Anglova Vignette	D-29
D.1.8	Conclusion	D-34
D.2	Dynamically Allocated Virtual Cluster (Dvc) Management System V2.0 Setup Guide	D-34
D.2.1	System Layout	D-34
D.2.2	Assumptions	D-35
D.2.2.1	Number of Systems	D-35
D.2.2.2	Operating System	D-35
D.2.2.3	Network	D-35
D.2.3	Network Layout	D-36
D.2.3.1	DAVC Controller (DAVC)	D-36
D.2.3.2	Virtual Host Servers	D-36
D.2.4	Network Switches Configuration	D-36
D.2.4.1	Management Network Switch	D-36
D.2.4.2	Private (Experiment) Network Switch	D-37
D.2.4.3	Cisco 3750-E Configuration Instructions	D-37
D.2.5	DAVC Controller Base Configuration	D-37
D.2.5.1	Install Operating System	D-37
D.2.5.2	Install Required Packages	D-37
D.2.5.3	Create DAVC Group	D-37
D.2.5.4	Configure DAVC Group Permissions	D-38

D.2.5.5	Create DAVC Directories	D-38
D.2.5.6	Install Django 1.7 and Dependencies	D-38
D.2.5.7	Extract DAVC Package	D-38
D.2.6	Network Configuration	D-38
D.2.6.1	Configure Public and Management Interfaces	D-38
D.2.7	Name Servers	D-39
D.2.8	Configure Host File	D-39
D.2.8.1	Network Time Protocol (NTP)	D-39
D.2.8.2	TFTP/PXE (Syslinux)	D-39
D.2.8.3	Configure Base TFTP/PXE	D-39
D.2.8.4	Create Localboot PXE Configuration	D-39
D.2.9	Network File System (NFS)	D-40
D.2.9.1	Create Directories and Exports	D-40
D.2.9.2	Increase NFS Processes (Count Depends on Number of Active NFS Clients)	D-40
D.2.9.3	Restart NFS Server	D-40
D.2.9.4	Verify NFS	D-40
D.2.10	DNSMASQ	D-40
D.2.10.1	Configure DNSMASQ	D-40
D.2.11	IPTABLES	D-41
D.2.11.1	Enable UFW	D-41
D.2.11.2	Add Rules	D-42
D.2.11.3	Enable NAT Routing (if Desired)	D-42
D.2.11.4	Allow BootPS, DNS, DNSMASQ, DAVC (Port 8001), and Gridengine (Ports 6444 and 6445)	D-43
D.2.11.5	Restart UFW	D-43
D.2.12	Secure Shell (SSH) Client Configuration	D-43
D.2.12.1	Turn Off StrictHostKeyChecking for SSH Client	D-43
D.2.12.2	Passwordless SSH for Root	D-43
D.2.13	Install Mosquitto MQTT (Message Queuing Telemetry Transport)	D-43
D.2.13.1	Install Python Dependencies for Mosquitto	D-43
D.2.13.2	Add Mosquitto Repository	D-44
D.2.13.3	Install Mosquitto	D-44
D.2.14	Virtual Host Servers Base Configuration	D-44
D.2.14.1	Install Operating System	D-44
D.2.14.2	Create DAVC Group	D-44
D.2.14.3	Configure DAVC Group Permissions	D-44
D.2.14.4	Create DAVC Directories	D-44
D.2.14.5	Extract DAVC Package	D-45
D.2.14.6	Install Required Packages	D-45
D.2.14.7	Compile Libvirt 0.10.0+ from Source	D-45
D.2.14.8	Freeze/Hold Libvirt System Packages	D-45
D.2.14.9	Update the System	D-45
D.2.14.10	Configure KVM link	D-45
D.2.15	Network Configuration	D-45
D.2.15.1	Configure Host File	D-45

D.2.15.2	Host Server Network Interface/Bridge Allocation	D-46
D.2.15.3	Create Management and Experiment Bridges	D-47
D.2.16	Disable Multicast Snooping on Private (Experiment) Bridges	D-48
D.2.16.1	Create Script to Run at Start Up	D-48
D.2.16.2	Set Script Permissions	D-49
D.2.16.3	Restart Networking	D-49
D.2.17	SSH Client Configuration	D-49
D.2.17.1	Turn Off StrictHostKeyChecking for SSH Client	D-49
D.2.17.2	Passwordless SSH for Root	D-49
D.2.18	Mount DAVC Controller NFS	D-49
D.2.18.1	Create /Home Entry in /etc/fstab	D-49
D.2.18.2	Mount/Home	D-50
D.2.19	NTP	D-50
D.2.19.1	Configure Services	D-50
D.2.19.2	Libvirt	D-50
D.2.20	Mosquitto MQTT	D-50
D.2.20.1	Install Python Dependencies for Mosquitto	D-50
D.2.20.2	Add Mosquitto Repository	D-50
D.2.20.3	Install Mosquitto	D-50
D.2.21	DAVC ControllerGrid Engine (ge_master) Configuration	D-50
D.2.21.1	Install Grid Engine	D-50
D.2.21.2	Postfix Configuration	D-51
D.2.21.3	Configure Grid Engine Software	D-51
D.2.21.4	Configure Grid Engine Multi-Core Processor Bindings Support	D-52
D.2.22	Virtual Host Servers Grid Engine (execd) Configuration	D-52
D.2.22.1	Install Grid Engine	D-52
D.2.22.2	Postfix Configuration	D-52
D.2.22.3	Configure Grid Engine Software	D-52
D.2.22.4	Configure Grid Engine Multi-Core Processor Bindings Support	D-53
D.2.23	Install libdrmaa.so.1.0	D-53
D.2.24	Configure Grid Engine Queue	D-53
D.2.24.1	Add Administrative Hosts	D-53
D.2.24.2	Add Submit Host	D-53
D.2.24.3	Start Exec Hosts	D-54
D.2.24.4	Execution Hosts	D-54
D.2.24.5	Create Queue for All Exec Hosts	D-54
D.2.24.6	Create Host Group List for all.q	D-54
D.2.25	Modify Queue (all.q)	D-55
D.2.25.1	Add Host Group to Queue (all.q)	D-55
D.2.25.2	Change Load_Thresholds and Slots	D-56
D.2.25.3	Verify Queue	D-56
D.2.25.4	Create Queue for KVM Exec Hosts	D-57
D.2.26	Create Host Group List for kvm.q	D-57
D.2.26.1	Show Host Group Lists	D-57
D.2.26.2	Add (Modify) Host Group	D-57

D.2.26.3	Show Host Group Lists	D-57
D.2.26.4	Verify Hosts in Host Group	D-57
D.2.27	Modify Queue (kvm.q)	D-57
D.2.27.1	Add Host Group to Queue (kvm.q)	D-57
D.2.27.2	Change load_thresholds and Slots	D-58
D.2.27.3	Verify All Queues	D-59
D.2.28	Modify Custom Complex Attributes	D-59
D.2.28.1	Create Custom Complex Attributes	D-59
D.2.28.2	Configure execd for Each Virtual Host Machine	D-59
D.2.28.3	Configure Virtual Host d1	D-60
D.2.28.4	Configure Virtual Host d2	D-60
D.2.29	Create Custom Load Sensor	D-60
D.2.29.1	Create custom_disk_free.sh load sensor	D-60
D.2.29.2	Set Ownership and Permissions	D-61
D.2.29.3	Copy to All Other Virtual Host Servers	D-61
D.2.29.4	Add Custom Load Sensor into Global System	D-61
D.2.29.5	Verify Custom Load Sensors	D-61
D.2.30	Test Grid Engine System	D-61
D.2.30.1	Create Simple Job Script	D-61
D.2.30.2	Submit Simple Job Script	D-62
D.2.30.3	Verify Simple Job Script is Running	D-62
D.2.31	DAVC Controller Configuration	D-62
D.2.31.1	Configure DAVC Software on DAVC Controller	D-62
D.2.32	Configure DAVC Software On Host Servers	D-66
D.2.32.1	Configure Apache2 User	D-66
D.2.32.2	Configure Virtual Hard Drive Service (VHD) On Host Servers	D-67
D.2.33	Create A DAVC System Configuration	D-67
D.2.33.1	Access DAVC Web Application Login Page	D-67
D.2.33.2	Create A New System Configuration	D-67
D.2.33.3	Active the System Configuration	D-69
D.2.34	Deploy VHD Template Images for DAVC	D-70
D.2.34.1	Registering A Virtual Hard Drive In DAVC	D-70
D.2.34.2	Update the Node Provisioning Startup Client Script to Include Correct Controller Hostname	D-70
D.2.34.3	Installing the DAVC Node Provisioning Client Startup Script in a Virtual Hard Drive Images	D-71
D.2.34.4	Configure Node Provisioning Client Startup Script to Run at Boot	D-71
D.2.34.5	Configure Virtual Hard Drives for Hotplug Support	D-71
D.2.34.6	Configure Network Interfaces on Virtual Hard Drives	D-71
D.2.34.7	Clear Hostname File on Virtual Hard Drive	D-72
D.2.34.8	Clear DHCP Leases on Virtual Hard Drive	D-72
D.3	Dynamically Allocated Virtual Clustering Management System User's Guide	D-72
D.3.1	Accessing and Logging into DAVC	D-73
D.3.2	DAVC Cluster Configuration	D-74
D.3.3	DAVC CLUSTER Instantiation	D-79
D.3.4	DAVC Virtual Hard Disk Management	D-85

D.3.5	DAVC Block Disk/Persistent Storage Management	D-89
D.3.6	Creating a New Virtual Hard Disk from a Cluster Node	D-94
D.3.7	Conclusion	D-97
D.4	References	D-97

Annex E – Routing Architecture Considerations for Heterogeneous Tactical Networks **E-1**

E.1	Introduction	E-1
E.1.1	Background	E-1
E.1.2	Routing Architecture Goals and Considerations	E-2
E.1.3	Network Model	E-4
E.1.4	Cognitive Radio and Topology Control	E-5
E.1.5	Other Network Paradigms	E-5
E.1.6	Definitions	E-5
E.2	Requirements	E-7
E.2.1	Heterogeneous Network Routing	E-8
E.2.2	Robustness	E-8
E.2.3	Scalability	E-8
E.2.4	Resource Efficiency and QoS	E-9
E.2.5	Configuration and Management	E-9
E.2.6	Other Requirements	E-9
E.3	Operational Network Topology Considerations	E-9
E.3.1	Stub Topology	E-10
E.3.1.1	Description	E-10
E.3.1.2	Advantages	E-11
E.3.1.3	Challenges	E-11
E.3.2	Tree Topology Stub	E-12
E.3.2.1	Description	E-12
E.3.2.2	Advantages	E-12
E.3.2.3	Challenges	E-13
E.3.3	Mesh Topology	E-13
E.3.3.1	Description	E-13
E.3.3.2	Advantages	E-13
E.3.3.3	Challenges	E-14
E.3.4	Conclusion	E-14
E.4	Routing Architectures for Mobile Heterogeneous Networks	E-14
E.4.1	Symbols	E-15
E.4.2	Routing Architecture Approaches at a Glance	E-16
E.4.2.1	Flat Architecture	E-16
E.4.2.2	Interconnect – Flat Architecture	E-17
E.4.2.3	Interconnect – Overlay Architecture	E-17
E.4.3	Implementation Issues	E-18
E.4.3.1	Layer for Routing Functionality	E-18
E.4.3.2	Network Functionality in One or Many Boxes	E-19
E.4.3.3	Low Data-Rate Radios in the IP Routing Architecture	E-20

E.4.4	Information Exchange	E-20
E.4.4.1	IEI-M Interface	E-22
E.4.4.2	Interconnect-Flat IEI-R and Interconnect-Overlay IEI-RO	E-24
E.4.4.3	Interconnect-Overlay IEI-RO	E-27
E.4.4.4	Design Considerations for Information Exchange	E-28
E.4.5	Addressing Considerations for the Routing Architectures	E-28
E.4.6	Network Policies for Governance of the Routing Architecture	E-29
E.5	Routing Architectures – Detailed Description and Discussion	E-30
E.5.1	Symbols and Performance Parameters	E-30
E.5.1.1	Performance Parameters	E-30
E.5.2	Flat Architecture	E-31
E.5.2.1	Heterogeneous Network Routing	E-32
E.5.2.2	Robustness	E-33
E.5.2.3	Scalability	E-33
E.5.2.4	Resource Efficiency and QoS	E-34
E.5.2.5	Configuration and Management	E-35
E.5.2.6	Ease of Deployment	E-35
E.5.2.7	Conclusion	E-36
E.5.3	Interconnect-Flat	E-36
E.5.3.1	Heterogeneous Network Routing	E-37
E.5.3.2	Robustness	E-38
E.5.3.3	Scalability	E-39
E.5.3.4	Resource Efficiency and QoS	E-39
E.5.3.5	Configuration and Management	E-40
E.5.3.6	Ease of Deployment	E-40
E.5.3.7	Conclusion	E-41
E.5.4	Interconnect-Overlay	E-41
E.5.4.1	Heterogeneous Network Routing	E-43
E.5.4.2	Robustness	E-44
E.5.4.3	Scalability	E-44
E.5.4.4	Resource Efficiency and QoS	E-45
E.5.4.5	Configuration and Management	E-46
E.5.4.6	Ease of Deployment	E-46
E.5.4.7	Conclusion	E-47
E.6	Architecture Comparison	E-47
E.6.1	Heterogeneous Network Routing	E-47
E.6.1.1	Conclusion	E-48
E.6.2	Robustness	E-48
E.6.2.1	Conclusion	E-49
E.6.3	Scalability	E-49
E.6.3.1	Conclusion	E-49
E.6.4	Resource Efficiency and QoS	E-49
E.6.4.1	Conclusion	E-50
E.6.5	Configuration and Management	E-50
E.6.5.1	Conclusion	E-50

E.6.6	Ease of Deployment	E-51
E.6.6.1	Conclusion	E-51
E.6.7	Impact on Coalition Interoperability	E-51
E.6.7.1	Conclusion	E-52
E.6.8	Conclusions	E-52
E.7	Implication of Security Design	E-53
E.7.1	Security Implications of the Flat Routing Architecture	E-54
E.7.2	Security Implications of the Interconnect-Flat Routing Architecture	E-56
E.7.3	Security Implications of the Interconnect-Overlay Routing Architecture	E-58
E.7.4	Additional IEI: Realizing a Flat Routing Architecture in Case of a Hybrid Black and Red Router Configuration	E-58
E.7.5	Conclusive Remarks on Security	E-60
E.8	Proposed Heterogeneous Network Design	E-61
E.9	Conclusions and Next Steps	E-63
E.10	State-of-the-Art, Related Work	E-65
E.11	References	E-67

Annex F – Interconnection Platforms in Vignette 2 **F-1**

F.1	Introduction	F-1
F.2	Interconnection Platform Selection	F-1
F.3	Waveforms	F-1
F.4	Results	F-2
F.5	References	F-4

Annex G – OSPF Scalability **G-1**

G.1	Introduction	G-1
G.2	Tactical Waveforms	G-1
G.3	Different Routing Architectures	G-1
G.3.1	Flat Architecture	G-2
G.3.2	Interconnect-Overlay	G-2
G.4	Some Central Terms of OSPF	G-3
G.4.1	OSPF Areas	G-3
G.4.2	Link State Advertisements	G-3
G.4.3	Adjacencies and Interfaces	G-3
G.5	OSPF Overhead Analysis in a Flat Architecture	G-4
G.6	OSPF Overhead Analysis in an Overlay Network	G-4
G.6.1	Background Assumptions	G-4
G.6.2	Hello	G-5
G.6.3	Database Description Messages	G-6
G.6.4	Router LSA	G-6
G.6.5	LSA Acknowledgement	G-6
G.6.6	Discussion and Conclusions on an OSPF Overlay Network	G-7
G.7	Using Another Routing Protocol in Most Radios	G-7

G.8	Conclusions	G-7
G.9	References	G-8

Annex H – Naval Task Group and Routing Experiment **H-1**

H.1	Operational Context for the Naval Scenario	H-1
H.1.1	Precondition	H-1
H.2	Tools and Utilities Generated to Conduct Experiments	H-4
H.3	Experimentation	H-4
H.3.1	Operational Concept and Scenario Overview	H-4
H.3.2	Experiment Conducted for Tactical Track Dissemination	H-5
H.3.3	Measured Metrics	H-7
H.3.3.1	Broadcast Delivery Analysis at Intermediate Node (@ node-15) for Full Period	H-7
H.3.3.2	Broadcast Delivery Analysis at Intermediate Node (@ Node-15) for Range Helo Airborne	H-8
H.3.3.3	Broadcast Delivery Analysis at Edge Node (@ node-1) for Full Period	H-8
H.3.3.4	Broadcast Delivery Analysis at Edge Node (@ node-1) for Range Helo Airborne	H-9
H.3.3.5	Headquarter Delivery Analysis @ Node-23	H-10
H.4	Results	H-11
H.5	References	H-12

Annex I – QoS Framework **I-1**

I.1	Providing Quality of Service in Civilian Networks	I-1
I.1.1	Network Level QoS	I-2
I.1.2	Non-Network Approaches for Quality of Services	I-3
I.2	Requirements	I-4
I.2.1	General Requirements	I-4
I.2.2	Robustness Requirements	I-4
I.2.3	Scalability Requirements	I-5
I.2.4	Resource Efficiency Requirements	I-5
I.2.5	Flexibility Requirements	I-5
I.3	Network States	I-5
I.4	Quality of Information, Value of Information, and Relationship to Quality of Service	I-6
I.4.1	Introduction	I-6
I.4.2	Overview of Approaches to VoI	I-7
I.4.3	VoI-Based Dissemination Model	I-8
I.4.4	VoI-Based Dissemination Deployment Patterns	I-9
I.5	QoS Mechanisms Implementation and Guidelines	I-10
I.5.1	Characteristics of QoS in Tactical Networks	I-12
I.5.2	Visibility of Traffic Control Mechanisms	I-13
I.6	Service View on Heterogeneous Networks	I-14
I.6.1	Network Control	I-16
I.6.2	Voice and Video	I-16
I.6.3	Situational Awareness	I-17

I.6.4	Sensor	I-17
I.6.5	Real Time Formal Messages	I-17
I.6.6	Informal Messaging	I-17
I.6.7	Non-Real Time Mass Data	I-17
I.6.8	Internet and Remote Access	I-18
I.6.9	Database Queries and Synchronized Messages	I-18
I.7	Summary	I-18
I.8	References	I-19

Annex J – QoS Standards

J-1

J.1	Background	J-1
J.2	Overview of Military Standards Related to QoS	J-6
J.2.1	TACOMS STANAGS	J-6
J.2.2	STANAG 4711 (Under Ratification)	J-9
J.3	Applicability of QoS Standards to Mobile Scenario	J-12
J.3.1	QoS for Mobile Networks with an Infrastructure	J-12
J.3.2	QoS for MANETs	J-13
J.4	QoS Vocabulary	J-14
J.5	References	J-15

List of Figures

Figure		Page
Figure 1	Network Model	2
Figure 2	Operational Scenario for IST-124 RTG-061	6
Figure 3	Emulation Environment for IST-124, Available as a Cloud Service to All IST-124 Members	8
Figure 4	This Network Topology Represents a Situation Where the Different Network Segments are Connected as a Mesh	13
Figure 5	Flat Routing Architecture: There is Only a Single Routing Protocol Domain Built on Top of Multiple Transmission Technologies, Utilizing an Information Exchange Interface (IEI-M) Between the Routing Function and the Modem	14
Figure 6	Interconnect – Flat Architecture: Multiple (Flat) Routing Protocol Domains are Residing Next to Each Other with IEI-Rs Between Each Other	15
Figure 7	Interconnect – Overlay Architecture: Some Platforms in the (Flat) Routing Protocol Domains are also Part of an Overlay Routing Domain (Blue) which Connects all the Separate Routing Protocol Domains	15
Figure 8	Tactical Communication Node with Two Radios – One Layer Two and One Layer Three Radio	18
Figure 9	Tactical Communication Node with Four Radios and No Security Boundary Violations	19
Figure 10	Figure Showing Connectivity with Different Number of Interconnection Platforms per Company for Different Transmission Technologies	21
Figure 11	Illustration of the Movements in Four Companies (24 Nodes Each) of Vignette II of the Anglova Scenario	22
Figure 12	Overhead Analysis Regarding Incoming Protocol Traffic per Node Regarding the Different Protocols	23
Figure 13	Operational Concept of MARLIN Implementation	25
Figure 14	A Routing Function in Selected Interconnection Platforms Builds a Virtual Overlay Routing Protocol Domain to Provide Routes Across Several Local Routing Protocol Domains	27
Figure 15	Deployment Patterns for VoI-Based Dissemination	31
Figure A-1	Operational Scenario for RTG-061	A-2
Figure A-2	High Level Operational View of the IST-124 Scenario	A-3
Figure A-3	Detailed Example View of the Coalition Naval Task Group and its Shore Based Commands	A-4
Figure A-4	The Final Part of the Battalion Deployment into Operational Zone	A-5

Figure B-1	High Level Operational View of the IST-124 Scenario	B-9
Figure B-2	Tracks in the Troop Deployment Vignette – Movement is from Top to Bottom	B-11
Figure B-3	Overview of Mobility Patterns in Vignette 3	B-13
Figure B-4	Visualization of the Range and Density of Narrowband, Medium band, and Wideband Radios	B-15
Figure B-5	System Architecture View of the Coalition Tactical Operations Center Node	B-16
Figure B-6	TACOMS+ Auto Configuration Over IPSec	B-17
Figure B-7	Illustration of the Movements of the Battalion	B-18
Figure B-8	The 25 KHz Transmission Technology at the 50 MHz Frequency Band	B-19
Figure B-9	The 250 KHz Transmission Technology at the 300 MHz Frequency Band	B-19
Figure B-10	The 1.25 MHz Transmission Technology at the 300 MHz Frequency Band	B-20
Figure B-11	The Fraction of Nodes at Different Hop Distances Averaged Over Vignette 2	B-21
Figure B-12	Total Average Number of Links Per Node for Different Values on P_{min}	B-23
Figure B-13	Average Number of Lost Links Per Node and Second for Different Values on P_{min}	B-23
Figure B-14	Average Number of Hops Between all Node Pair in the Network for Different Values on P_{min}	B-24
Figure B-15	Average Number of Not Reachable Nodes for Different Values on P_{min}	B-24
Figure B-16	Average Number of Lost Links Per Node Over the Two-Hour Long Vignette 2	B-25
Figure C-1	The 283 Node DAVC Cluster and Networks	C-3
Figure C-2	Anglova Deployment Over ESXi	C-4
Figure C-3	VSphere Client View After Installation of ESXi Server	C-5
Figure C-4	Creating a vSphere Standard Switch Within ESXi	C-6
Figure C-5	Configuring the VLAN for the EMANETrunk Virtual Switch	C-6
Figure C-6	Configuring Security Properties for EMANETrunk	C-7
Figure C-7	Status of ESXi Server After Installation of EMANEServer VM and 12 Nodes.	C-8
Figure C-8	Creating Another vSphere Switch and Network for the EMANE Over The Air (OTA) Traffic	C-8
Figure C-9	Assigning Appropriate Networks to the Test VM Interfaces	C-9
Figure C-10	Configuration of Networks for the EMANEServer VM	C-10
Figure C-11	Scripted Display Tools (SDT-3D)	C-11
Figure C-12	EMANE SDT-3D Visualization Client/Server Framework	C-11
Figure C-13	Anglova Scenario Emulation Visualization in SDT-3D	C-12
Figure C-14	Mirage Visualizer	C-13
Figure C-15	Example Event Service Configuration File	C-15
Figure C-16	Example EEL Generator Configuration File	C-15
Figure C-17	Example EEL File	C-15
Figure C-18	Anglova Scenario Player	C-16
Figure C-19	ScenGenFromFile Utility Program Initial Directory Structure	C-21

Figure D-1	Operational Scenario for IST-124 RTG-061	D-2
Figure D-2	Emulation Environment for IST-124, Available as a Cloud Service to all IST-124 Members	D-4
Figure D-3	DAVC Web Application Login	D-5
Figure D-4	DAVC User Dashboard	D-5
Figure D-5	Cluster Info Tab	D-6
Figure D-6	Cluster Networks Tab	D-6
Figure D-7	Add the Network 172.15.0.0/23	D-7
Figure D-8	Add the Second Network to the Cluster	D-7
Figure D-9	Add the Network 172.16.0.0/23	D-7
Figure D-10	The Two Experimentation Cluster Networks	D-8
Figure D-11	Cluster Nodes Tab	D-8
Figure D-12	Configure VM Nodes 1-269	D-9
Figure D-13	Add VM Node 270	D-9
Figure D-14	Configure VM Node 270, the Experimentation Controller	D-10
Figure D-15	Complete the Cluster Creation Process	D-10
Figure D-16	Experimentation Cluster Created	D-11
Figure D-17	Cluster Nodes Initializing	D-12
Figure D-18	The Cluster is Active Once All Nodes' Status is Set to 'ACTIVE'	D-12
Figure D-19	Log into VM Node 270's VNC Console	D-13
Figure D-20	VM Node 270's VNC Console	D-13
Figure D-21	Emulation Environment File System	D-14
Figure D-22	Snippet of the Anglova Scenario Network Plan	D-15
Figure D-23	Company1-1 and Company1-2 Network Mappings	D-16
Figure D-24	Network Plan IP Address Mappings	D-16
Figure D-25	Network Plan Host Names	D-17
Figure D-26	Vignette Group Mappings	D-17
Figure D-27	EMANE Configuration Directories	D-18
Figure D-28	Company1 EMANE Configuration Files	D-19
Figure D-29	Company1-1 Platform XML File	D-20
Figure D-30	Company1 Transvirtual XML File	D-20
Figure D-31	Event Service Daemon XML File	D-20
Figure D-32	GPSD Location Agent XML File	D-21
Figure D-33	Wideband1 Radio Model NEM XML File	D-21
Figure D-34	Wideband1 Radio Model PHY Parameters	D-22
Figure D-35	Wideband1 Radio Model MAC Parameters	D-22
Figure D-36	EMANE Event Service Configuration File System	D-23
Figure D-37	Example Event Service Configuration File	D-23

Figure D-38	Example EEL Generator Configuration File	D-23
Figure D-39	Example EEL File	D-24
Figure D-40	start_anglova_experiment.sh Script Usage	D-24
Figure D-41	SDT-3D Visualization Tool	D-26
Figure D-42	EMANE SDT-3D Visualization Client/Server Framework	D-27
Figure D-43	Configure SDT-3D to Listen on TCP Port 55002	D-27
Figure D-44	Configure SDT-3D to Load and Replay an SDT-3D Log File	D-28
Figure D-45	Log into VM Node 270's VNC Console	D-28
Figure D-46	Navigate to the Experimentation Scripts Home Directory on Node Exp-270	D-28
Figure D-47	Vignette 2 Execution Output	D-29
Figure D-48	Vignette 2 Execution Output	D-30
Figure D-49	Vignette 2 Emulation Visualization	D-30
Figure D-50	Example Custom Vignette DAVC Configuration (Platform Nodes)	D-31
Figure D-51	Example Custom Vignette DAVC Configuration (Controller Node)	D-32
Figure D-52	Edit the start_anglova_experiment.sh Script for Custom Vignettes	D-33
Figure D-53	Example Custom Vignette Execution	D-33
Figure D-54	DAVC System Layout	D-34
Figure D-55	Host Server Network Interface Bridge Allocation Layout	D-46
Figure D-56	DAVC Home Page and Login	D-68
Figure D-57	DAVC System Administration Page	D-68
Figure D-58	System Configuration Form	D-69
Figure D-59	Activate System Configuration	D-70
Figure D-60	Accessing and Logging into DAVC	D-73
Figure D-61	DAVC User Dashboard	D-73
Figure D-62	DAVC Cluster Configuration	D-74
Figure D-63	DAVC Cluster Configuration: Cluster Info Tab	D-74
Figure D-64	DAVC Cluster Configuration: Networks Tab	D-75
Figure D-65	DAVC Cluster Configuration: Networks Tab	D-75
Figure D-66	DAVC Cluster Configuration: Nodes Tab	D-76
Figure D-67	DAVC Cluster Configuration: Add Cluster Nodes	D-76
Figure D-68	DAVC Cluster Configuration: Add Cluster Nodes	D-77
Figure D-69	DAVC Cluster Configuration: Add Cluster Nodes	D-77
Figure D-70	DAVC Cluster Configuration: Nodes Tab	D-78
Figure D-71	DAVC Cluster Configuration	D-78
Figure D-72	DAVC Cluster Instantiation: Cluster Details Page	D-79
Figure D-73	DAVC Cluster Instantiation: Cluster Details Page	D-79
Figure D-74	DAVC Cluster Instantiation: Node Options (Inactive Cluster)	D-80
Figure D-75	DAVC Cluster Instantiation: From Cluster Configuration List	D-80

Figure D-76	DAVC Cluster Instantiation	D-81
Figure D-77	DAVC Cluster Instantiation: Cluster Details Page	D-81
Figure D-78	DAVC Cluster Instantiation: Cluster Details Page	D-82
Figure D-79	DAVC Cluster Instantiation: Active Cluster	D-82
Figure D-80	DAVC Cluster Details: (Active Cluster)	D-83
Figure D-81	DAVC Cluster Details	D-83
Figure D-82	DAVC Cluster Details: (Active Cluster)	D-84
Figure D-83	DAVC Cluster Details: (Active Cluster)	D-84
Figure D-84	DAVC Cluster Instantiation: Node Options (Active)	D-85
Figure D-85	DAVC VHD Management	D-85
Figure D-86	DAVC VHD Management: Prepping Your VHD for Upload	D-86
Figure D-87	DAVC VHD Management: Prepping Your VHD for Upload	D-86
Figure D-88	DAVC VHD Management: Prepping Your VHD for Upload	D-87
Figure D-89	DAVC VHD Management: Prepping Your VHD for Upload	D-87
Figure D-90	DAVC VHD Management: Uploading a VHD	D-88
Figure D-91	DAVC VHD Management	D-88
Figure D-92	DAVC VHD Management	D-89
Figure D-93	DAVC Block Disk Management	D-89
Figure D-94	DAVC Block Disk Management	D-90
Figure D-95	DAVC Block Disk Management: Creating a Block Disk	D-90
Figure D-96	DAVC Block Disk Management: Creating a Block Disk	D-91
Figure D-97	DAVC Block Disk Management: Attaching a Block Disk to a Node	D-91
Figure D-98	DAVC Block Disk Management: Attaching a Block Disk to a Node	D-92
Figure D-99	DAVC Block Disk Management: Attaching a Block Disk to a Node	D-92
Figure D-100	DAVC Block Disk Management: Attaching a Block Disk to a Node	D-93
Figure D-101	DAVC Block Disk Management: Detaching a Block Disk from a Node	D-93
Figure D-102	DAVC Block Disk Management: Detaching a Block Disk from a Node	D-94
Figure D-103	Creating a New Virtual Hard Disk	D-94
Figure D-104	Creating a New Virtual Hard Disk	D-95
Figure D-105	Creating a New Virtual Hard Disk	D-95
Figure D-106	Creating a New Virtual Hard Disk	D-96
Figure D-107	Creating a New Virtual Hard Disk	D-96
Figure D-108	Creating a New Virtual Hard Disk	D-97
Figure E-1	Network Model	E-4
Figure E-2	High-Level Overview of the IST-124 Anglova Scenario	E-10
Figure E-3	A Network Topology Where the Different Networks Segments are Connected to a Deployed Network as Stubs	E-11

Figure E-4	A Network Topology Where the Different Networks Segments (Technology Domains) are Connected to a Deployed Network as Stubs in a Tree Structure	E-12
Figure E-5	This Network Topology Represents a Situation Where the Different Network Segments are Connected as a Mesh.	E-13
Figure E-6	Flat Routing Architecture: There is Only a Single Routing Protocol Domain Built on Top of Multiple Transmission Technologies, With IEI-Ms Between the Routing Function and the Modem (Transmission Technology)	E-17
Figure E-7	Interconnect – Flat Architecture: Multiple (Flat) Routing Protocol Domains are Residing Next to Each Other with IEI-Rs Between Each Other	E-17
Figure E-8	Interconnect – Overlay Architecture: Some Military Platforms in the (Flat) Routing Protocol Domains are Also Part of an Overlay Routing Domain (Blue) which Connects all the Separate Routing Protocol Domains	E-18
Figure E-9	An Interconnection Platform that Uses an Internal IEI-M	E-24
Figure E-10	An Interconnection Platform that Uses Some Point-to-Point Protocol to Carry the IEI-M Information Between a Routing Function Residing in One Device and the Transmission Technology Modem Residing in Another Device	E-24
Figure E-11	An Interconnection Platform that Uses an Internal IEI-R.	E-26
Figure E-12	An Interconnection Platform that Uses Some Point-to-Point Protocol to Carry the IEI-R Information Between the Routing Protocol Domains on Two Different Transmission Technology Domains on Two Different Devices	E-26
Figure E-13	An Interconnection Platform that Uses Some Point-to-Point Protocol to Carry the IEI-RO Information Between the Overlay Routing Protocol Domain and Routing Protocol Domains of Two Different Transmission Technology Domains on Separate Devices	E-27
Figure E-14	Assumed Military Platform Architecture	E-30
Figure E-15	Flat Routing Architecture: A Situation Where Flat Routing is Used Internally in a Network Composed of Two Companies	E-32
Figure E-16	A Situation with an Interconnect Architecture with Flat Protocol Interaction for the Two Companies	E-37
Figure E-17	An Example of the Chain of Different Routing Protocols that Might be Needed to Connect Two Different Military IP Radios with the Interconnect-Flat Architecture	E-41
Figure E-18	A Heterogeneous Network Utilizing an Overlay Routing Protocol Domain to Provide Routes Across Several Local Routing Protocol Domains	E-42
Figure E-19	Application-Level with Link Encryption in the Flat Routing Architecture	E-55
Figure E-20	Network-Level Encryption in the Flat Routing Architecture, Where the Crypto is Between Hosts and the Router	E-55
Figure E-21	Network-Level Encryption in the Flat Routing Architecture, Where the Crypto is Between the Router and the Radios	E-55
Figure E-22	Network-Level Encryption Used as Generic Link Encryption in the Flat Routing	E-56
Figure E-23	Application-Level with Link Encryption in the Interconnect-Flat Routing Architecture	E-57
Figure E-24	Network-Level Link Encryption in the Interconnect-Flat Routing Architecture, Where Both Routers are in Different National Domains, Preferably of Comparable Security Level	E-57

Figure E-25	Application-Level Encryption with Link Encryption in the Interconnect- Overlay Routing Architecture	E-58
Figure E-26	Network-Level Encryption Between the Overlay and Local Routing Domains in the Interconnect-Overlay Routing Architecture	E-59
Figure E-27	Hybrid Approach in Which Some Radio Devices are Only Visible to the Red Router and Others Only to the Black Router	E-59
Figure E-28	Information Exchange Interfaces that are Needed to Achieve a Flat Routing Architecture in Case of a Hybrid Platform Configuration in Which Some Radio Devices are Only Visible to the Red Router and Others Only to the Black Router and Where Radios B and D Have the Routing Protocol Used by R1 and R2 Embedded	E-60
Figure E-29	A Hybrid Architecture with the Flat Architecture and the Interconnect-Overlay Architecture Combined	E-63
Figure F-1	Connectivity with Two ICPs Per Company for the Different Cases with Inter-Company Network (IN) and Company Network (CN) Based on the Three Waveforms, NB, MB and WB	F-2
Figure F-2	Connectivity with Four ICPs Per Company for the Different Cases with Inter-Company Network (IN) and Company Network (CN) Based on the Waveforms, NB, MB and WB	F-3
Figure F-3	Average Connectivity for Different Number of ICPs Over the Whole 1000 Second Test Period, for the Different Cases of Inter-Company Network (IN) and Company Network (CN) Based on the Waveforms, NB, MB and WB	F-3
Figure G-1	Single Layer-Three Routing Protocol	G-2
Figure G-2	Single Layer-Three Routing and MANET Routing on Layer Two	G-3
Figure H-1	Operational Concept of MARLIN Implementation	H-4
Figure H-2	Naval Component Vignette 2 Scenario Overview	H-6
Figure I-1	Traditional Information Dissemination Model	I-8
Figure I-2	Value-of-Information-Based Dissemination Model	I-9
Figure I-3	Deployment Patterns for VoI-Based Dissemination	I-10
Figure I-4	Example of Short Paths without Bottleneck	I-13
Figure J-1	UNI (User Network Interface)-to-UNI Reference Path for Network QoS Objectives	J-2
Figure J-2	QoS Building Blocks	J-6
Figure J-3	Communication Between Two Mobile Users	J-13

List of Tables

Table		Page
Table 1	Relative Performance of the Different Architecture Approaches on the Requirements	16
Table A-1	Example Equipment of the Operational Scenario Key Players	A-9
Table A-2	Basic Parameters of Vehicular and Man-Pack VHF Radios	A-10
Table A-3	Basic Parameters of UHF Radios	A-10
Table A-4	Basic Parameters of SATCOM on the Move Terminal	A-11
Table A-5	Basic Parameters of LEO Satellite Terminal	A-11
Table A-6	Basic Parameters of HF Radios	A-11
Table A-7	Basic Parameters of Naval VUHF Radios	A-11
Table A-8	Basic Parameters of Naval HF Radios	A-12
Table A-9	Basic Parameters of Tactical LTE	A-12
Table A-10	List of Proposed Services	A-14
Table B-1	Results of EMANE 802.11 MAC Implementation	B-6
Table B-2	SNR Threshold Values	B-14
Table C-1	Sample Network Plan File	C-18
Table C-2	Sample Program Configuration Initialization File	C-19
Table D-1	A Brief Description of the Files Located in the /opt/nato-experiment Folder of the Controller Node	D-14
Table D-2	The Radio Networks of Company 1	D-17
Table D-3	The Set of Xml Files that are Used to Instantiate a Node's Emulated Radio	D-18
Table D-4	The Different Version of the Script that Starts EMANE	D-25
Table E-1	Overview of Possible Information that Could be Exchanged via Information Exchange Interfaces	E-21
Table E-2	Requirements to Heterogeneous Tactical Networks	E-31
Table E-3	Relative Performance of the Different Architecture Approaches on the Requirements	E-52
Table H-1	Broadcast Delivery Analysis at Intermediate Node (@ Node-15) for Full Period	H-8
Table H-2	Broadcast Delivery Analysis at Intermediate Node (@ Node-15) for Range Helo Airborne	H-9
Table H-3	Broadcast Delivery Analysis at Edge Node (@ Node-1) for Full Period	H-10
Table H-4	Broadcast Delivery Analysis at Edge Node (@ node-1) for Range Helo Airborne	H-11
Table H-5	Headquarter Delivery Analysis @ Node-23	H-12

Table I-1	Network Characteristics Requirements for the Chosen Set of Applications in Order to Achieve Acceptable Fidelity in Heterogeneous Networks	I-15
Table J-1	Examples of IP-Based Services with their Guaranteed Performance Attributes	J-3
Table J-2	IP Network QoS Class Definitions and Network Performance Objectives	J-4
Table J-3	Provisional IP Network QoS Class Definitions and Network Performance Objectives	J-4
Table J-4	Guidance for Network QoS Classes	J-5
Table J-5	TACOMS CO CoS	J-7
Table J-6	DSCP Assignment for C6/7, EF, AF, BE, and PHBs	J-7
Table J-7	DSCP Assignment for Class Selector (CS) Codepoints	J-8
Table J-8	DSCP Field Specification	J-9
Table J-9	Service Classes and their Quality Constraints	J-10
Table J-10	SC Values	J-10
Table J-11	Treatment Aggregates and their Quality Constraints	J-11
Table J-12	Association of SCs to TAs	J-11
Table J-13	Mapping between Military Precedence Level and DSCP-Coding	J-11
Table J-14	Performance Targets Applicable for Tactical Core Networks and Tactical Networks	J-12

List of Acronyms and Abbreviations

2G	Second Generation
4G	Fourth Generation
5G	Fifth Generation
AF	Assured Forwarding
AFCEA	Armed Forces Communications and Electronics Association
AI	Artificial Intelligence
AIS	Advanced Identification System
AMN	Afghan Mission Network
APC	Armoured Personnel Carrier
API	Application Programming Interface
ARL	US Army Research Laboratory
ARQ	Automatic Repeat Request
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BE	Best Effort
BER	Bit Error Rate
BER	Block Error Rate
BFT	Blue Force Tracking
BGP	Border Gateway Protocol
BLOS	Beyond Line of Sight
BMDR	Backup MDR
C2	Command and Control
C4IS	Command, Control, Communications, and Computers Information System
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CBR	Constant Bit Rate
CDN	Content Distribution Network
CDS	Connected Dominating Set
CF	Coalition Forces
CHQ	Coalition Headquarters
CIDR	Classless Inter-Domain Routing
CIMIC	Civil-military Cooperation
CIS	Communications and Information System
CITR	Channel Idle Time Ratio
CL	Connectionless THC
CN	Company Network
CNR	Combat Net Radio
CO	Connection-Oriented THC
COI	Contact Of Interest
COMSEC	Communications Security
CoNSIS	Coalition Network for Secure Information Sharing
CORE	Common Open Research Emulator
CoS	Class of Service
CPU	Central Processing Unit
CS	Class Selector
CS	Combat Support

CSS	Combat Service Support
CTP	Common Tactical Picture
CWIX	Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise
DAT	Directional Airtime
DAVC	Dynamically Allocated Virtual Clustering
DAVCMS	Dynamically Allocated Virtual Clustering Management System
dB	Decibels
dBm	Decibel-milliwatts
DBW	Dedicated Bandwidth
DDS	Data Distribution Services
DHCP	Dynamic Host Configuration Protocol
DLEP	Dynamic Link Exchange Protocol
DNS	Domain Name System
DRM	Distributed Resource Management System
DSCP	Differentiated Services Code Point
DSCP	Differentiated Services Code Point
DTN	Disruption Tolerant Networking
ECN	Explicit Congestion Notification
EEL	Emulation Event Log
EF	Expedited Forwarding
EMANE	Extended Mobile Ad Hoc Network Emulator
EOD	Explosive Ordinance Disposal
ESM	Electronic Support Measures
ETSI	European Telecommunications Standards Institute
EW	Electronic Warfare
FIB	Forwarding Information Base
FMN	Federated Mission Network
GIS	Geospatial Information System
GPS	Global Positioning System
GPSD	GPS Daemon
GRE	Generic Routing Encapsulation
HF	High Frequency
HQ	Headquarters
HUR	High Update Rate
HW	Hardware
Hz	Hertz
ICMP	Internet Control Message Protocol
ICN	Information-Centric Networking
ICP	Interconnection Platform
ICT	Information and Communication Technology
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronics Engineers
IEI	Information Exchange Interface
IEI-M	Information Exchange Interface – Modem
IEI-R	Information Exchange Interface – Router
IEI-RH	Information Exchange Interface – Router Hybrid
IEI-RO	Information Exchange Interface – Router Overlay
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IN	Inter-company Network

IO	Information Object
IOP	Interoperability Point
IP	Internet Protocol
IPDV	IP Delay Variation
IPER	IP packet Error Ratio
IPLR	IP Loss Ratio
IPMPL	IP Military Precedence Level
IPSec	Internet Protocol Security
IPTD	IP Transfer Delay
IR	Infrared
IST	Information Systems Technology
ITM	Irregular Terrain Model
ITU	International Telecommunications Union
JOSM	Java Open Street Map
Kbps	Kilobits per Second
KHz	Kilohertz
KML	Keyhole Markup Language
KVM	Kernel-based Virtual Machines
L2	Layer 2
L3	Layer 3
LAN	Local Area Network
LLC	Logical Link Control
LOS	Line of Sight
LRP	Longley-Rice model Parameter files
LSA	Link State Advertisements
LTE	Long Term Evolution
LXC	Linux Containers
MAC	Medium Access Control
MANET	Mobile Ad Hoc Network
MARLIN	Mobile Ad Hoc Relay Line of Sight Networking
MB	Medium band
MC	Military Contingent
MDR	MANET Designated Routers
MEDEVAC	Medical Evacuation
METOC	Meteorology and Oceanography
MGEN	Multi-Generator
MHz	Megahertz
MIF	Maritime Interdiction Force
MILCOM	Military Communications Conference
MIL-STD	Military Standard
MLPP	Multilevel Precedence and Preemption
MOS	Mean Opinion Score
MPA	Maritime Patrol Aircraft
MPL	Military Precedence Level
MPLS	Multiprotocol Label Switching
MPR	Multipoint Relay
MQTT	Message Queuing Telemetry Transport

NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NB	Narrowband
NBWF	Narrowband Waveform
NCB	NATO Codification Bureaux
NDN	Named Data Networking
NE	Network Equipment
NEM	Network Emulation Module
NetIP	Networking Framework for All-IP Transport Services
NFS	Network File System
NFV	Network Function Virtualization
NIC	Network Interface Controller
NIP	Network Interconnection Point
NMCD	Network Management and Cyber Defence
NMEA	National Marine Electronics Association
NRL	US Naval Research Laboratory
NTP	Network Time Protocol
OGC	Open Geospatial Consortium
OLSR	Optimized Link State Routing
ONAP	Open Network Automation Platform
OpenGL	Open Graphics Language
OSC	On Scene Commander
OSD	Office of the Secretary of Defense
OSI	Open Systems Interconnection
OSM	Open Street Map
OSPF	Open Shortest Path First
OTA	Over The Air
OTC	Officer on Tactical Command
PCN	Protected Core Network
PDR	Packet Delivery Ratio
PHB	Per Hop Behaviour
PHY	Physical Layer
PNR	Personal Networking Radio
PPPoE	Point-to-Point Protocol over Ethernet
PROTEAN	NRL's PROTOcol Engineering Advanced Networking group
PTT	Push-To-Talk
QEMU	Quick Emulator
QoI	Quality of Information
QoS	Quality of Service
RAM	Random Access Memory
RECCE	Reconnaissance
RF	Radio Frequency
RIP	Routing Information Protocol
RM	Resource Management
ROHC	Robust Header Compression
RSVP	Resource Reservation Protocol
RTG	Research Task Group
RTT	Round Trip Time

SATCOM	Satellite Communication
SBW	Statistical Bandwidth
SDK	Software Development Kit
SDN	Software-Defined Networking
SDR	Software-Defined Radio
SDT	Scripted Display Tools
SDT-3D	Scripted Display Tools 3D
SGE	Sun Grid Engine
SINR	Signal to Interference plus Noise Ratio
SLA	Service Level Agreement
SME	Subject Matter Expert
SNR	Signal to Noise Ratio
SOTM	Satcom On The Move
SPLAT!	Signal Propagation, Loss, And Terrain Analysis Tool
SRTM	Shuttle Radar Topography Mission
SSH	Secure Shell
SW	Software
TA	Treatment Aggregates
TACOMS	Tactical Interoperable Communications Standards
TC	Topology Control
TCP	Transport Control Protocol
TDMA	Time Division Multiple Access
TFC	Traffic Flow Confidentiality
THC	Traffic Handling Classes
TN	Test Node
TOC	Tactical Operations Center
TRL	Technology Readiness Level
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UGS	Unattended Ground Sensor
UHF	Ultra-High Frequency
UMTS	Universal Mobile Telecommunications System
UNI	User Network Interface
URL	Uniform Resource Locator
USGS	United States Geological Survey
UTAMS	Unattended Transient Acoustic MASINT sensors
UTD	Uniform Theory of Diffraction
VHD	Virtual Hard Disk
VHF	Very High Frequency
VLAN	Virtual LAN
VM	Virtual Machine
VNC	Virtual Network Computing
VoI	Value of Information
VoIP	Voice over IP
VTC	Video Teleconferencing
WAN	Wide Area Network
WB	Wideband
WBWF	Wideband Waveform
WLAN	Wireless Local Area Network

WMS	Web Map Service
WSN	Wireless Sensor Network
XML	Extensible Markup Language

Glossary

The following terminologies are used in this document:

<i>Network Segment</i>	We use the term network segment to refer to a bounded portion of the heterogeneous network. This can be any portion, smaller than a transmission technology domain and multiple protocol domains, but often the segment will be the same as the transmission technology domain or the routing protocol domain. A network segment has to be bounded and topologically (not necessarily physically) connected.
<i>Network Segment</i>	We use the term network segment to refer to a bounded portion of the heterogeneous network. This can be any portion, smaller than a transmission technology domain and multiple protocol domains, but often the segment will be the same as the transmission technology domain or the routing protocol domain. A network segment has to be bounded and topologically (not necessarily physically) connected.
<i>Transmission Technology Domain</i>	We use the term transmission technology domain to refer to a network segment that uses one unique transmission technology. The transmission technology encompasses both physical (PHY) layer design, medium access (MAC) layer design and logical link control (LLC) layer design. When the same PHY, MAC and LLC are used, but separate frequency bands are allocated, we also consider the network to represent two different transmission technology domains.
<i>Modem</i>	We use modem to refer to a device or function that implements a transmission technology and that does not have an accompanying routing layer.
<i>Routing Protocol Domain</i>	We use the term routing protocol domain to refer to a network segment that uses one routing protocol. The routing protocol domain can consist of one or more transmission technology domains if the routing protocol can support different transmission technologies with the same protocol. In military radio systems the routing protocol domains and transmission technology domains can often coincide, e.g., in case of a radio specific routing protocol. In classical combat net radio (CNR) systems, there is no notion of a routing protocol domain at all, but only radio broadcast is used.
<i>Interconnection Platform</i>	An interconnection platform represents platforms where different routing protocol domains and/or transmission technology domains meet physically. The platform can have a tactical router where more than one routing protocol domain and/or more than one transmission technology domain is connected, or it can have several routers that are connected with wires and implements information exchange interfaces for the routing layer.
<i>Information Exchange Interface Modem (IEI-M)</i>	For the discussion in the report, this is a term used to define an open interface between the lower layers of a radio and a routing function. The routing function can be located in an external router or installed on the same hardware platform.

*Information Exchange
Interface – Router
(IEI-R)*

The IEI-R represents the interface between the routing protocol domains of different network segments. This interface can be used both internal to a nation's network and external in order to establish a coalition network. We include also exchange of routing information with radios that include sub-layer 3 routing in the definition of the IEI-R.

*Information Exchange
Interface – Router
Overlay (IEI-RO)*

The IEI-RO represents the interface between the routing protocol domain of a network segment and the overlay routing domain. This interface can be used both internal to a nation's network and external in order to establish a coalition network. Similar to the IEI-R we include also exchange of routing information with layer-two radios in the definition of the IEI-RO.

Network Control

This term represents signaling messages with the purpose of realizing (reliable) communications. In radio networks, these are usually transmitted in-band. Network control usually aims to learn or react to changes that occur in a network that cannot be predicted upfront, but depend on e.g. the traffic load on the network or changes in the topology because of node mobility or changes in the link quality. Examples of network control messages are routing protocol messages, QoS related messaging (e.g., for the Resource Reservation Protocol (RSVP)), acknowledgements on the MAC layer and congestion control mechanisms for TCP. Some technologies (e.g., SDN) might also send this signaling out-of-band.

Tactical Router

A device or (software) instance with a common routing function for either the flat or overlay architecture. A tactical router acts as the connecting element in a heterogeneous tactical network that requires a common protocol (i.e., the flat architecture and the interconnect-overlay architecture). The tactical router runs the routing protocol of choice for the common routing protocol domain. The device must be able to do routing over both embedded and external modems (transmission technologies).

IST-124 Membership List

CHAIR

Dr. Mariann HAUGE
Norwegian Defence Research Establishment (FFI)
NORWAY
Email: Mariann.Hauge@ffi.no

MEMBERS

Mr. Christoph BARZ*
Fraunhofer-FKIE
GERMANY
Email: christoph.barz@fkie.fraunhofer.de

Ing. Maurizio BISIO*
Leonardo – Società per azioni
ITALY
Email: maurizio.bisio@selex-es.com

Dr. Andreas Boyd BUCHIN*
Rohde & Schwarz GmbH & Co. KG
GERMANY
Email: boyd.buchin@rohde-schwarz.com

Dr. Daniela GHEZZI*
Leonardo – Società per azioni
ITALY
Email: daniela.ghezzi@selex-es.com

Dr. Jimmi GRÖNKVIST*
Swedish Defence Research Agency (FOI)
SWEDEN
Email: jimmi.gronkvist@foi.se

Mr. Anders Ingemar HANSSON*
Swedish Defence Research Agency (FOI)
SWEDEN
Email: anders.hansson@foi.se

Dr. Anne-Marie HEGLAND*
Kongsberg Defence and Aerospace
NORWAY
Email: anne.m.hegland@kongsberg.com

Mr. Arjen HOLTZER*
Netherlands Organisation for Applied
Scientific Research (TNO)
NETHERLANDS
Email: arjen.holtzer@tno.nl

Mr. Ronald IN'T VELT*
Netherlands Organisation for Applied
Scientific Research (TNO)
NETHERLANDS
Email: ronald.intvelt@tno.nl

Mr. Taner KURTULUŞ*
MilSOFT Yazılım Teknolojileri A.Ş
TURKEY
Email: tkurtulus@milsoft.com.tr

Dr. Lars LANDMARK
Norwegian Defence Research Establishment (FFI)
NORWAY
Email: Lars.landmark@ffi.no

Dr. King LEE*
US Army Research Laboratory
UNITED STATES
Email: king.f.lee.civ@mail.mil

Dr. Piotr ŁUBKOWSKI*
Military University of Technology
POLAND
Email: piotr.lubkowski@wat.edu.pl

Mr. Kelvin M. MARCUS*
US Army Research Laboratory
UNITED STATES
Email: kelvin.m.marcus.civ@mail.mil

* Chapter contributor.

LCDR (Rtd) Dr. Mari-Anne MEISTER
Tallinn University of Technology
ESTONIA
Email: mari-anne.meister@ttu.ee

Mr. Levent MİSİRLİOĞLU*
MilSOFT Yazılım Teknolojileri A.Ş
TURKEY
Email: lmisirlioglu@milsoft.com.tr

Tekn.Dr. Jan NILSSON*
Swedish Defence Research Agency (FOI)
SWEDEN
Email: jan.nilsson@foi.se

Mr. Raido PAHTMA
Tallinn University of Technology
ESTONIA
Email: raido.pahtma@ttu.ee

Mr. Sami PELTOTALO*
Finnish Defence Forces Technical
Research Centre
FINLAND
Email: sami.peltotalo@mil.fi

Mr. Markus PEUHKURI*
Aalto University
FINLAND
Email: markus.peuhkuri@aalto.fi

Dipl. Peter SEVENICH
Fraunhofer-FKIE
GERMANY
Email: peter.sevenich@fkie.fraunhofer.de

Mr. Ulf STERNER*
Swedish Defence Research Agency (FOI)
SWEDEN
Email: ulf.sterner@foi.se

Dr. Niranjani SURI*
US Army Research Laboratory
UNITED STATES
Email: niranjani.suri.civ@mail.mil

ADDITIONAL CONTRIBUTORS

Ms. Maggie R. BREEDY
Institute for Human and Machine Cognition
UNITED STATES
Email: mbreedy@ihmc.us

* Chapter contributor.



Heterogeneous Tactical Networks – Improving Connectivity and Network Efficiency

(STO-TR-IST-124-PART-I)

Executive Summary

Collection and sharing of information as well as command and control are essential parts of all military operations. Establishing a flexible communication network that can adapt to the specific requirements for each operation is one of the key requirements to provide the necessary information flow in current and future military operations. There are ongoing activities to provide flexible coalition networks for fixed network infrastructures and to some extent for semi-mobile deployed networks e.g., the Federated Mission Networking (FMN). However no clear guidelines currently exist on how to deploy efficient well-connected heterogeneous tactical radio networks. This greatly hinders information sharing at the lower tactical level. This report presents studies that have been done by IST-124 in order to increase the understanding and provide some recommendations of how to build interoperable heterogeneous mobile radio networks at the tactical edge. The purpose is to find methods to best utilize the mobile networks that are brought to an operation by different coalition partners. The report covers three broad topics:

- 1) Description of a scenario and implementation of a cloud-like testbed environment to evaluate different technological solutions related to the scenario. The testbed is a show case for improving the efficiency of international research collaboration on Information and communication technology. The scenario and the testbed serves a similar purpose as a Collaborative Demonstration of Technology (CDT) to do collaborative scenario based analysis of different technologies, but with a much lower cost than CDT. Exploitation of emulation technologies can speed-up the time from early research results until solutions are ready to be tested for standardization. Tools and scripts to build the testbed environment are made publicly available.
- 2) Description and analysis of architectures and mechanisms to provide end to end connections across different mobile networks. The report compares different routing architectures and proposes a hybrid architecture. A central observation is that there is a need for different mechanisms that the network planner can choose from in order to get the necessary performance for different type of operations. Necessary information exchange interfaces in order to ensure interoperability between the mechanisms has been identified, and the scalability of different protocols has been studied. We provide an overview of different security architectures and discuss the consequence of the choice of security architecture on the efficiency of the routing architecture and propose a target security architecture.
- 3) Guidelines and mechanisms to best prioritize and utilize scarce network resources. Monitoring of three states of network health (normal, reduced, last effort) is proposed to Improve Resource Management (RM) and Quality of Service (QoS) in the network. The different network states will need its own set or subset of mechanisms. We also recommend choosing a single network layer to implement a QoS or RM mechanism as this reduces the risk for no-cooperating mechanisms at different layers that might degrade performance. For RM and QoS to perform well, a notion of the Value of Information (VoI) must be available. The VoI can change over time, and RM/QoS needs to adapt to these changes.

Our effort to better understand the challenges involved when establishing mobile heterogeneous coalition networks at the tactical edge will help NATO nations to evolve/procure network equipment that can be

interoperable. The results from IST-124 are timely. It is expected that FMN will start including different aspects of mobile tactical networks from Spiral 4 and onwards. The results of IST-124 can be important input to the relevant FMN syndicates.

Réseaux tactiques hétérogènes : amélioration de la connectivité et de l'efficacité du réseau

(STO-TR-IST-124-PART-I)

Synthèse

La collecte et le partage d'informations ainsi que le commandement et le contrôle sont des éléments essentiels de toutes les opérations militaires. L'établissement d'un réseau de communication flexible, capable de s'adapter aux exigences spécifiques de chaque opération, est l'une des conditions essentielles pour assurer la circulation de l'information nécessaire aux opérations militaires actuelles et futures. Des activités sont en cours pour fournir des réseaux de coalition flexibles pour des infrastructures de réseaux fixes et, dans une certaine mesure, pour les réseaux déployés semi-mobiles, par exemple le réseau de mission fédéré (*Federated Mission Networking – FMN*). Cependant, il n'existe actuellement aucune directive claire sur la manière de déployer des réseaux radio tactiques hétérogènes efficaces et bien connectés. Cela entrave considérablement le partage d'informations au niveau tactique inférieur. Ce rapport présente les études conduites par IST-124 dans le but d'améliorer la compréhension et de formuler des recommandations sur la manière de construire des réseaux de radio mobile hétérogènes interopérables au niveau tactique. La finalité est de trouver des méthodes pour utiliser au mieux les réseaux de téléphonie mobile mis à contribution par différents partenaires d'une coalition. Le rapport couvre trois grands thèmes :

- 1) Description d'un scénario et mise en œuvre d'un environnement de banc d'essai de type cloud pour évaluer différentes solutions technologiques liées au scénario. Le banc d'essai est un exemple concret d'amélioration de l'efficacité de la collaboration internationale en matière de recherche sur les technologies de l'information et de la communication. Le scénario et le banc d'essai remplissent un objectif similaire à la démonstration collaborative de technologie (*Collaborative Demonstration of Technology – CDT*) pour effectuer une analyse collaborative basée sur des scénarios de différentes technologies, mais à un coût bien inférieur à celui de la CDT. L'exploitation des technologies d'émulation peut accélérer le temps écoulé depuis les premiers résultats de la recherche jusqu'à ce que les solutions soient prêtes à être testées en vue de leur normalisation. Les outils et les scripts qui permettent de construire l'environnement de test sont mis à la disposition du public.
- 2) Description et analyse des architectures et des mécanismes permettant de fournir des connexions de bout en bout sur différents réseaux de téléphonie mobile. Le rapport compare différentes architectures de routage et propose une architecture hybride. Une observation centrale est qu'il existe un besoin pour différents mécanismes parmi lesquels le planificateur de réseau peut choisir afin d'obtenir les performances nécessaires pour différents types d'opérations. Les interfaces nécessaires à l'échange d'informations afin de garantir l'interopérabilité entre les mécanismes ont été identifiées et l'évolutivité de différents protocoles a été étudiée. Nous fournissons une vue d'ensemble des différentes architectures de sécurité et discutons des conséquences du choix de l'architecture de sécurité sur l'efficacité de l'architecture de routage et proposons une architecture de sécurité cible.
- 3) Lignes directrices et mécanismes pour prioriser et exploiter au mieux les ressources en réseau rares. Il est proposé de surveiller trois états de l'état du réseau (normal, réduit, dernier effort) afin d'améliorer la gestion des ressources (*Resource Management – RM*) et la qualité de service du réseau (*Quality of Service – QoS*). Les différents états du réseau auront besoin de leur propre ensemble ou sous-ensemble de mécanismes. Nous recommandons également de choisir une seule

couche réseau pour mettre en œuvre un mécanisme de QoS et de RM, car cela réduit le risque de non-coopération de plusieurs couches susceptible de dégrader les performances. Pour que la RM et la QoS soient performants, une notion de la valeur de l'information (VoI) doit être disponible. La VoI peut changer au fil du temps et la RM et la QoS doivent s'adapter à ces changements.

Nos efforts pour mieux comprendre les défis posés par la mise en place de réseaux de coalition hétérogènes mobiles au niveau tactique aideront les pays de l'OTAN à développer/à se procurer des équipements de réseau pouvant être interopérables. Les résultats de IST-124 arrivent en temps opportun. La FMN devrait commencer à inclure différents aspects des réseaux tactiques mobiles à partir de Spiral 4. Les résultats de IST-124 peuvent constituer un apport important pour les syndicats de FMN concernés.

HETEROGENEOUS TACTICAL NETWORKS – IMPROVING CONNECTIVITY AND NETWORK EFFICIENCY

1.0 INTRODUCTION

This is a report of the activities and findings of the IST-124/RTG-061 “Heterogeneous Tactical Networks – Improving Connectivity and Network Efficiency”. The group is also publishing a separate report “Heterogeneous Networks, Security Architecture”, NATO IST-124-Part-II (NATO UNCLASSIFIED), which documents the details of the group’s work regarding the security architecture.

In short, IST-124 has contributed to a better understanding (through analysis, simulation, emulation and expert opinions) on how to build interoperable heterogeneous networks at the tactical edge. A toolbox of design choices is proposed to help the network planner to orchestrate the best design for a given operation. Necessary information exchange interfaces to enable heterogeneous coalition networking have been identified. Challenges imposed by different security architectures are identified. Monitoring of three states of network health (normal, reduced, last effort) is proposed to improve resource management and service quality in the network. The group has demonstrated the benefit of having a cloud based shared emulated network platform for doing joint experiments.

1.1 Scope of the Work

Communication networks over which to collect and share information as well as to command and control forces and weapons are a central part of all military operations. Without a well-functioning network, the efficiency of most of today’s military operations will be severely degraded. On the other hand, the availability of an efficient and well-connected network is a crucial capability that (in conjunction with other capabilities) can give information superiority and the ability to make improved tactical decisions compared with the military adversary.

Establishing a flexible networking solution that can adapt to the specific requirements for each operation is one of the key requirements to provide the necessary information flow in current and future military operations. Several activities are ongoing to provide flexible coalition networks for fixed network infrastructures and to some extent for semi-mobile deployed networks e.g., the Federated Mission Networking (FMN) [1] and the work done to design a federated Protected Core Network (PCN¹) [2] in the IST-069 and IST-103 RTGs. There is a need to extend the ideas of a federated network to also include mobile tactical edge networks. The trend is that nations deploy smaller and smaller units to coalition operations at the same time as increased data capacity is required and deployed at low echelons. Both of these trends lead to a scenario with an increasing number of different radio systems being present in an operation. These networks should be connected to form a common heterogeneous network that is available for all to improve the overall network robustness and availability. Until now most research on mobile military networks has been focused on optimizing the performance for internal communication in a homogeneous network and very little attention has been paid to solutions for heterogeneous networks. This gap has been the concern of this RTG where the focus has been on end-to-end network performance in a network constructed from many wireless networks (different transmission technology domains).

Network heterogeneity can cover a wide range of differences. e.g., IP versus non-IP networks, commercial versus military networks, and ad hoc versus infrastructure-based networks. The type of heterogeneity that has been in scope for the work of IST-124 has been difference in transmission technologies and difference in

¹ There is also ongoing work to write PCN STANAGS. The head STANAG 5637 is under ratification and the core STANAG 5638 is work in progress.

routing mechanisms. The following definition of heterogeneous networks has been used for the work that is reported here. Heterogeneous networks are networks that encompass elements of diverse:

- Type (radios, routers, etc.), vendor, age (state-of-the-art, legacy); and/or
- Software (communication protocols, implementation, configuration, etc.); and/or
- Channel characteristics (operating frequency, range, bit rate, etc.); and/or
- Security (enforced at different layers, different security domains, etc.).

The heterogeneous network may include both wired and wireless components. In most (all) coalition operations, the war fighter has to deal with one or more of the challenges imposed by this type of network heterogeneity. Some of the challenges that should be solved are described by the group in Ref. [3].

We've restricted our work to consider network elements that are IP-capable or can easily be connected to IP-capable routers, i.e., we assume a traditional TCP/IP network model as shown in Figure 1.

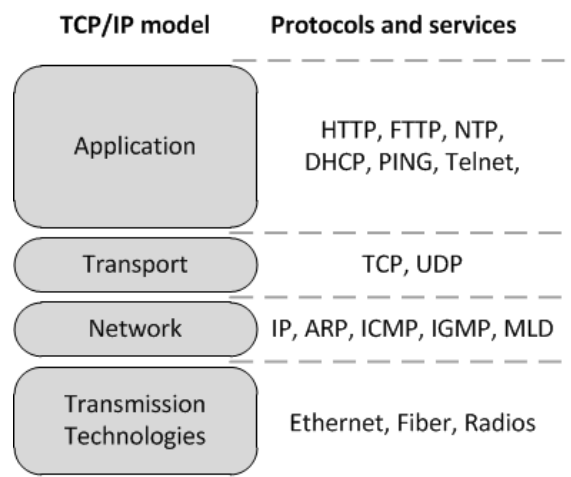


Figure 1: Network Model.

No clear guidelines currently exist on how to deploy efficient well-connected heterogeneous tactical edge networks. This greatly hinders information sharing in these coalition networks. The work of IST-124 contributes to a better understanding of the challenges and trade-offs encountered when deploying these networks. The purpose has not been to write standards; however, the results can be used as input to the standardization of tactical edge networks; e.g., in FMN. With the current roadmap of FMN, mobile networks are planned to be included from Spiral 4 and onwards.

1.2 The IST-124 Group

The IST-124 Task Group brought together the knowledge and experience of participants from ten different nations to better understand the challenges and problems associated with the formation of heterogeneous coalition network at the tactical edge. It was an active group with participants both from academia, research institutes and industry. The group included experts with competence on different transmission technologies, mobile networking protocols, security, QoS, middleware, sensor networks as well as technologies for network virtualization and emulation.

The task group has changed over time with some leaving the activity due to, e.g., retirement, lack of funding, and new members joining midways. IST-124 has had more than 20 appointed participants with an active core of 10 – 15 people that have participated at most meetings and activities.

1.3 Structure of the Report

The main body of this report provides a summary of the work that has been done by the group as well as conclusions and recommendations. Detailed information about the different activities is given in associated annexes to this report, in published papers and in a separate STO technical report. Most of the annexes are standalone documents that can be read separately.

- Section 2 explains how the group has worked, which methods we have used, and how the activities have been supported.
- Section 3 describes the scenario that the group developed. The network emulation environment that the group has orchestrated is also described. This environment implements one instantiation of the scenario. The scenario and the emulation environment are documented in Annex A – D.
- Section 4 gives the overall network requirements that the activities of the group have aimed to support. The requirements are further detailed in Annex E and Annex I.
- Section 5 covers the group's activities related to network connectivity in the heterogeneous environment. Several possible routing architectures as well as experiments and analysis to better understand the trade-offs involved with the different architectures, are described. Possible security architectures that can exist in the heterogeneous network and their implications for the routing architecture are also explained. These activities are further described in Annex E – Annex H.
- Section 6 comprises recommendations for how to provide QoS in the heterogeneous environment as well as an overview over existing relevant QoS standards. Annex I and Annex J gives the details of this activity.
- Section 7 concludes the overview with a list of recommendations as well as suggestions for future work.
- Section 8 gives a list of activities that comprises the group's work.

2.0 WORK METHODS

We've used many different methods for the comprised work. One contribution from the group that has been valued by the group's participants has been the sharing of information and knowledge among the different group members. For this purpose we have reserved time at all group meetings for presentations of relevant ongoing research activities at the different participants' departments. Tours of labs and presentations from colleagues of the participants have also been arranged at some meetings. Group members that also participate in other relevant NATO teams or other research activities have acted as liaisons for information sharing between the activities.

Some activities have been driven by collaboration of experts where a team has provided insight to a problem based on their expert opinion. Other activities have been theoretical analysis, simulation and emulation experiments.

The problem at hand was very complex, involving heterogeneous mobile ad hoc networks where a long history of research has shown that the performance results are often very dependent on the chosen scenario (level of mobility, traffic pattern, network size and the similar). Therefore, we spent quite some time identifying a military relevant scenario that would limit the parameter choice and at the same time include the most important challenges with heterogeneous networking at the mobile tactical edge. Challenges with networking in this scenario led to a list of requirements for the performance of these networks, that the group would seek to solve.

Early on we identified a need for a common test environment where different methods could be combined or compared. The different partners in the group collectively used a range of different experimentation and simulation environments. Comparing results from different simulation and emulation environments can be difficult and lead to very inaccurate overall results [4]. Comparing and combining the mechanisms in a field experiment was considered not possible for the group due to limited funding and available resources. A common virtualized network emulation environment was brought up as an alternative that seemed like an inviting solution to our problem.

The following methods; analysis, simulation, emulation, testbed and field test are all common methods used to evaluate the performance of mobile networks. The different methods have different advantages and disadvantages and suit different phases of research and development of network mechanisms. Network emulation provides many of the advantages of simulation while using implementations that are prepared for field testing. Emulation allows for testing on a larger scale than what is possible in field tests.

In IST-124 we were fortunate to have the necessary expertise to build a virtualized emulated network environment. We also had a partner with the necessary computing resources that was willing to host the emulated testbed for the group. Therefore we decided to put quite some effort into building an emulation environment that the group could use for common experiments. The scenario that the group identified has been emulated in the testbed. More information about the testbed is given in Section 3 and Annex A – Annex D.

The following are some benefits that a common emulation testbed can provide for international/national research collaboration:

- A common testbed environment, accessible by different partners, allows that results from different mechanisms implemented by different partners can be compared with credible results.
- A common emulation testbed environment simplifies testing of a system put together of several different mechanisms provided by different research partners. This is possible since the actual real-life implementation code can be used (e.g., in Linux) in the emulation environment, instead of having to implement all mechanisms for a specific simulator, which would be required in a simulation environment.
- Emulation of a realistic scenario that is used for many different experiments improves the usefulness of test results.
- Gives many of the same research benefits as common field tests, but to a much lower cost.
- Can be used in early stages of research, with mechanisms on a lower Technology Readiness Level (TRL) than what is usually needed for field tests.
- Motivates to move from simulation to emulation at early stages of research. This can speed up the time from the start of the research until the code is ready to be tested for standardization (e.g., STANAG, FMN, experiments at CWIX).
- Use of a common emulation environment among different research collaborations (different IST groups, across STO panels and the similar) can improve cooperation between organizations and different areas of expertise. It also can speed up research efforts by enabling the reuse of results from other groups.

We spent much effort to automate many of the features of the emulation testbed and to put together knowledge from different partners on, amongst others, channel propagation, mobility patterns for different operations, radio models, and virtualization techniques. For this reason, the emulation environment was ready for use quite late in IST-124's timeline. We have finished two experiments using the emulation environment and have started two others which did not finish in time to be reported on in this report. The use of the emulation environment for experimentation is planned to continue in the IST-161 RTG "Efficient

Group and Information Centric Communications in Mobile Military Heterogeneous Networks”, which started in March 2018.

The work method for the common experiments was weekly WebEx meetings to discuss results and distribute tasks between the collaborating nations.

The group also staged two panel debates at IEEE/AFCEA Military Communications Conference (MILCOM) in 2017 and 2018. At these events we exposed the group’s work to a larger audience of researchers and received suggestions for other ideas as well as praise and criticism of our work.

3.0 SCENARIO AND EMULATION ENVIRONMENT

One of the challenges with research on mobile military networks is that it is very difficult to identify general solutions that work well for different scenario parameter values (e.g., network size, level of mobility, maximum data capacity, data load and requirements, etc.). It is also envisioned that the optimal network design will vary depending on the operational scenario. In order to limit the scope of the work and at the same time work with realistic operational conditions, a scenario of a coalition operation with a set of vignettes was defined by the group. The set of vignettes is a “general” description of typical operations that are often encountered in coalition operations. The group studied the challenges associated with end-to-end communication in the vignettes.

Early on we identified a need for a common test environment where different methods could be combined or compared. A common virtualized network emulation environment seemed like an inviting solution to our problem. Fortunately we also had the proper expertise on this in our group. Therefore we decided to put quite some effort into building an emulation environment that the group could use for common experiments. The scenario that the group identified was emulated in the testbed. Most of the emulation environment is available for public release and can be reused by other research collaborations. Several other research groups (both national and international) are already using the emulation environment. The current distribution of scripts and templates is located at two different web sites: <https://www.ihmc.us/nomads/scenarios/anglova/>, and <https://anglova.net/>. These web sites will be kept updated with new developments and enhancements related to the Anglova scenario. At the time of writing the IHMC site has most up-to-date information, but this will most likely change over time, thus we recommend the reader to search both sites for the most recent information.

The following sections give a brief description of the operational perspective for the scenario and the concrete realization of the operational context, the “Anglova scenario”. Also, an overview is provided of the experimentation environment, including the tools that are used to build much of the emulation testbed and the environment that is used to deploy the virtualized emulation environment. Some of this has been published in Refs. [5] and [6] and details are available in:

- Annex A “Operational Perspective for IST-124”;
- Annex B “Emulation-Based Experimentation and the Anglova scenario”;
- Annex C “Experimentation Environment and Tools”; and
- Annex D “IST-124 Experimentation Execution”.

3.1 Operational Context for IST-124

The IST-124 RTG focused on heterogeneous networks in the deployable and mobile tactical domains. An overview of a military scenario that is dependent of these networks is illustrated Figure 2. The scenario was created to show the information needs during the operation and exemplify the challenges related to establishing the necessary services in the heterogeneous network.

The scenario depicts an operation conducted by the company task forces of a mechanized battalion and a naval task group. They are part of the Military Contingent (MC) coordinated by the Coalition HQ. The company Communications and Information System (CIS) is connected to the National Operational WAN and has access to the Coalition systems. The MC HQ plays the reach-back role during the operation and provides Combat Support (CS) and Combat Service Support (CSS) if requested. According to the operational context it is assumed that enemy forces are preparing a complex attack on the coalition base from the village located in the operational zone in the lower right corner of Figure 2. The enemies are well armed and operate in an area which can be mined, so there is a chance of IED (Improvised Explosive Device) hazard. The task of the own forces is to move into the operational zone, to neutralize the insurgents and to destroy the armaments they collected. It is very important to avoid village inhabitants' casualties and to make the insurgents' escape impossible. The most important elements in this mission are CIS, logistics and medical support which are provided by the Coalition Forces. A well-functioning communication capability to help organizing the armed forces is therefore required.



Figure 2: Operational Scenario for IST-124 RTG-061.

The completion of the task requires access to a wide range of systems and communication networks such as radio communications system (HF, VHF, UHF, Satcom), sensor networks and UAV systems. Navy management systems are also in place for supporting reconnaissance and surveillance of the mission and to provide services such as data, voice and video.

Three vignettes were defined in order to implement the actions included in the scenario. The roles and actors are the same for each vignette. The first vignette covers the intelligence preparation of the battlefield. The second vignette consists of the movement of coalition forces into the operational zone, including maritime interdiction operations in the surrounding coastal areas. The third vignette consists of an urban operation resulting in the neutralization of insurgents. The third vignette also includes a medical evacuation to a naval ship following the neutralization of IEDs. Each vignette suggests data that are expected to be exchanged between the actors and C4IS (Command, Control, Communications, and Computers Information System) equipment used in a way that emphasize the problems of connectivity and network efficiency of military heterogeneous networks.

Detailed information about the operational perspective is provided in Annex A.

3.2 Anglova Scenario

The Anglova scenario is a concrete realization of the operational context described in Section 3.1 and depicts an operation conducted by a coalition task force consisting of land forces and a maritime component. The tactical domain is located in the fictitious area of Fieldmont in Anglova, where the Coalition HQ (CHQ) of the Military Contingent (MC) is based. The scenario contains three vignettes as outlined in the operational context. Due to time and resource constraints, different parts of the scenario are modelled with varying detail. We prioritized the modelling of the naval task group and the deployment of the land-based coalition forces since these two elements were good for scalability tests of different routing designs. We've prepared the foundation for all vignettes and the ones that are not fully modelled can be improved by the new IST-161 RTG or other groups that want to utilize the testbed design.

The first vignette involving the Intelligence Preparation of the Battlefield is the Vignette that currently has the least detailed description.

The second vignette is modelled with much detail. It covers the deployment of the land-based coalition forces, a battalion consisting of six companies, into the operational zone as well as a surveillance operation by the naval task force. The forces that are moving into the operational zone use a combination of narrowband VHF and wideband UHF radios for connectivity amongst each other and for connecting to MC forces. The scenario includes detailed mobility patterns of the battalion north of Wellport in Anglova.

The battalion consists of six companies:

- Four mechanized companies with 24 vehicles each;
- One command and artillery company with 22 vehicles; and
- One support and supply company with 39 vehicles.

Together, there are 157 vehicles, each of them being a network node. The maritime component includes 21 ships and one multi-purpose helicopter that can be used to relay communication. In addition, a Coalition Headquarters node and an airborne node were also added to this vignette – a strategic UAV asset that can act as a communications relay and provide persistent surveillance capabilities.

The third vignette covers the urban counter-insurgency operation within the town of Wellport and involves three platoons (72 nodes), 10 unattended ground sensors, one aerial sensor (Aerostat), two UAVs (tactical and data harvest), three satellites, the 21 navy ships that are continuing the maritime mission, and the multi-purpose helicopter that is re-tasked for MEDEVAC. The vignette includes neutralization of the insurgents and the IED, a MEDEVAC from the urban environment to a naval ship, and the platoons returning to base. The mobility and path loss data for this vignette has been modelled. Some radio types are not yet modelled.

The mobility and path loss data for the Anglova scenario have been released into the public domain and are available to be downloaded and utilized by other researchers. Detailed information about the scenario is provided in Annex B.

3.3 Experimentation Environment and Tools

The Anglova scenario is accompanied by a set of tools that simplifies modification of the scenario and its use in an experimentation environment for collaborative research. IST-124 believes that the emulation-based approach to experimentation adopted by the group provides a good compromise and stepping stone between simulations and using actual hardware. In a typical emulation-based experiment, the software components that are deployed in the experiment are ideally the same components that would be utilized on actual hardware and in the field. Therefore, there is no need to maintain multiple implementations. When changes need to be introduced, it is easier to evaluate them in an emulation environment with the actual software components prior to pushing those components out into the field.

The framework selected for the IST-124 experimentation was EMANE (Extendable Mobile Ad hoc Network Emulator) [7]. EMANE was selected for multiple reasons – scalability and flexibility being the two primary technical reasons, and easy access and prior experience by some of the authors being other deciding factors. EMANE is released as open source and is available for download on GitHub [8], making it very easy to be obtained and deployed.

The group has developed a deployable Virtual Machine (VM) that contains all of the tools necessary to instantiate and run the Anglova scenario. The VM is preconfigured with EMANE and includes scripts to configure the network interfaces and radio models, tools to play back the scenario including the mobility and path loss data, tools to generate network load, and tools to capture traffic for analysis. In addition, supplementary tools have been included to generate path loss data and to visualize the scenario during execution.

More information about the tools and how IST-124 has used them can be found in Annex C.

3.4 Dynamically Allocated Virtual Clustering (DAVC)

IST-124 used the US Army Research Laboratory’s Dynamically Allocated Virtual Clustering Management System (DAVC) to deploy the Anglova scenario (Figure 3) using the distributed EMANE emulation model. In this emulation model the EMANE software is installed within VMs that execute the applications that are the subject of the experimentation and whose performance is being evaluated.

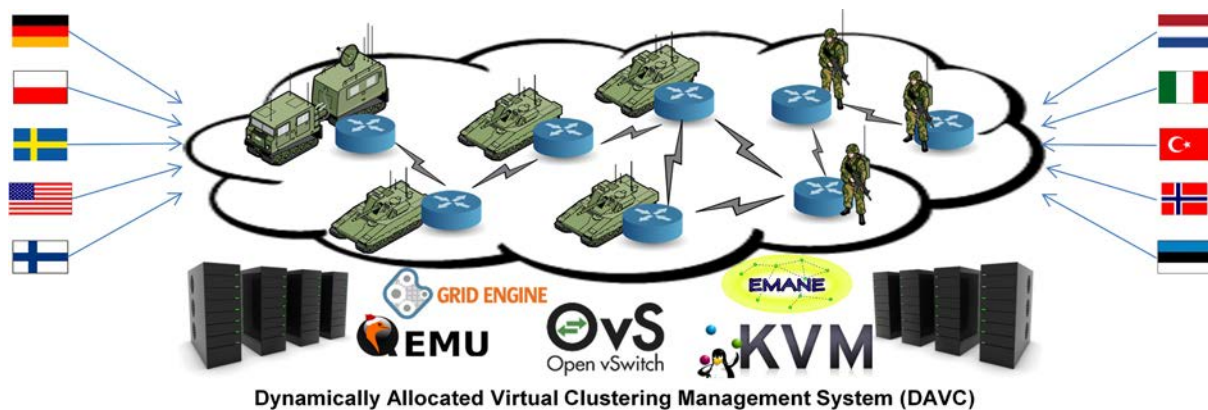


**Figure 3: Emulation Environment for IST-124, Available
as a Cloud Service to All IST-124 Members.**

DAVC is a web based virtualization service and cloud-operating environment that creates complex virtual experimentation clusters that can be used for simulation-based, emulation-based, and hybrid field / emulation experimentation [9]. DAVC deploys networked clusters composed of VMs tailored to user specifications. The DAVC management system abstracts away testbed infrastructure configuration through automated provisioning processes that configure the virtual networking for each VM. Clusters created by DAVC are heterogeneous in the sense that each VM can have a different OS, a different applications set and hardware attributes such as RAM, CPU cores, hard disk and network interfaces. DAVC users can register custom VMs as templates that can be used within their experimentation clusters.

Using DAVC, the Anglova scenario is distributed with a 1-to-1 mapping with each Anglova node running within a single DAVC virtual cluster node. The entire 269 node scenario can run within a 270 node DAVC cluster. When deployed in this manner node 270 acts as the experimentation orchestration node and is responsible for executing the bootstrap scripting that launches the various applications and EMANE on the remaining 269 nodes.

Further step-by-step directions to use DAVC to execute the Anglova scenario are provided in Annex D.

4.0 REQUIREMENTS

In the group we have identified a set of requirements to mobile heterogeneous networks. The requirements are grouped according to the functionality they provide. The requirements are not prioritized. Some of them are essential in order to provide basic end-to-end networking. Others focus on improving the network to increase for instance robustness and throughput. We envision that different operations will assign different priority to the various requirements – some will have a high need for robustness, others will require flexibility in how the networks resources are used, and so on. In the future these priorities will make up parts of the network policy for how to build the operation’s network.

4.1 Requirements to the Routing Function and Management of Routing

4.1.1 Heterogeneous Network Routing

The goal of the heterogeneous network routing requirements is to ensure that connectivity between nodes is arranged between all users that want to exchange information.

- The network must provide end-to-end connectivity supporting both unicast and multicast services if a physical connection of any kind exists, and the network policy allows the connection.
- The heterogeneous network must be “radio silence” aware to cope with radios or network segments in radio silence.
- Multicast is an important traffic type in tactical networks. Efficient means for both intra-domain and inter-domain multicast should be supported. Interaction between traditional multicast and other network segment specific multicast protocols should also be supported.

4.1.2 Robustness

The goal of the robustness requirements is to ensure that the availability of the network for the users is as high as possible, and that disruptions in communications streams and data exchange between users are prevented.

- A network segment should support the possibility to connect to other network segments at more than one connection point simultaneously.
- Multiple paths between the source and destination should be maintained. If possible different sets of transmission technologies should be chosen for the different paths to improve robustness.
- A routing protocol should prioritize “stable” links to improve the robustness of the path.
- There should be security measures that prevent unauthorized entities from disrupting the network service or gaining illegitimate access to the signalling and user payload.
- The heterogeneous network should be able to mitigate Electronic Warfare (EW) threats.

4.1.3 Scalability

The goal of the scalability requirements is to make sure that large numbers of military platforms can successfully exchange information via the heterogeneous network.

- The trade-off between network performance, reliability and overhead must be taken into consideration. Overhead includes signalling, redundant traffic and extra number of transmissions due to longer routing paths or retransmissions on unreliable links.

- The routing protocols should be aware of the available communication resources (e.g., in terms of link data rates) and the routing architecture must support differentiated routing overhead in order to reduce the signalling to a minimum for the low capacity network segments while maintaining a high signalling rate for highly mobile, higher capacity network segments.

4.1.4 Resource Efficiency and QoS

The goal of the resource efficiency requirements is to maximize the user data that can be exchanged between users via the heterogeneous network given a certain time span, and to provide QoS.

- At least one resource efficient path (e.g., in terms of channel usage and spatial reuse) through the heterogeneous network must be found between the source and destination.
- Several paths should be made available for different traffic types (QoS classes) to choose the most suited path for each class. These paths might be calculated using different routing metrics and based on different link/path parameters.
- Policies that govern how control information can be spread in different network segments are needed.
- The network should provide standardized information on the status of the network to applications and/or middleware that want to make use of this.
- The network must be able to implement detailed network policies for providing different QoS to different communication flows / data exchanges.

4.1.5 Configuration and Management

The goal of the configuration and deployment requirements is to minimize the effort needed to configure and maintain the network and reduce the need for human intervention in the network to ensure correct operations in different and changing circumstances.

- The network should be self-configuring as far as possible to reduce the need for complex manual adjustments to the scenario.
- The connection of new network segments (e.g., from coalition partners) to the heterogeneous network should be fully automated.
- It should be easy to include new radio types and tactical routers in the coalition network (zero-config).
- The architecture should be able to implement a change in defined network policies in real time.

4.1.6 Other Requirements

- Protocols and interfaces between routers, transmission technologies and network segments should be based on open standards, or on NATO standards (which can be based on open standards).

4.2 Requirements of the Quality of Service (QoS) and Resource Management (RM) Functions

4.2.1 General Requirements

The goal of the heterogeneous network Quality of Service is to ensure that resources in the network are assigned to traffic according to its importance – resulting in better utilization of the network.

- Different operations will assign different priorities and forwarding treatment for different traffic classes. Also network capacity, number of users, and the operational environment are different for each operation. The network must support the ability to deploy the best working set of QoS mechanisms and policies for each operation.

- The network must implement an admission control to reject some of the traffic if the network does not have enough capacity to forward the traffic while maintaining the priorities.
- If a mobile network is degraded and carries less traffic than planned, it must be possible to adapt the prioritization and admission control to match the present situation.
- The network must be able to pre-empt traffic if it has no more capacity to transfer high-priority traffic flows.
- A traffic class should not be forwarded to a path whose properties cannot provide the service that the class needs. If there is no alternative path, the traffic should be denied.
- Applications, middleware and the users should have knowledge of the network state. If possible they should take advantage of the state information to modify their behavior (traffic generation) to better suit the current network state.
- Users should be made aware if they are using applications the network cannot support at the time.
- The terminals should indicate the network state if the information does not overload the user capability.

4.2.2 Robustness

- The network should seek to choose a traffic path that is sufficiently robust in characteristics so resource allocation and required forwarding characteristics for a flow can be maintained for a reasonable lifetime of a session.
- Each network segment must be able to control the traffic volume and traffic classes and adapt to the available capacity and mission situation independently.
- The network should adapt its network control traffic volume to suit the present network capacity.
- A network device must be able to make the right decisions also when the network is partitioned (i.e., make distributed decisions when there is no connection to a central authority / broker).
- The QoS mechanisms should be as straightforward as possible, because any unnecessary complexity threatens the operational efficiency and the reliability of the services.

4.2.3 Scalability

- Nodes sharing a common channel should share a common view of available network resources and implement appropriate admission control for the situation.
- There must be an efficient method to limit the visibility of network state information in order to not cause too much signaling information.

4.2.4 Resource Efficiency and QoS

- The priority of different traffic should be adapted based on the ratio of the Value of the Information (VoI) for the mission to consumed resources, i.e., if a video clip does not have much added value compared with a short message, the latter should be prioritized.
- There should be an estimate on present network load and available capacity (network state estimation).
- Traffic that cannot be forwarded to the destination should be rejected/dropped as close to the source as possible.
- Traffic that has no value for the recipient because it is too old, or has been replaced with new information, should not be forwarded.

- If radio silence or Traffic Flow Confidentially (TFC) are applied, the impact of those on QoS decisions must be taken into account.

4.2.5 Flexibility

- A common QoS control framework must be easy to implement based on the mission plan.
- It should be easy to reconfigure the QoS control to meet changing requirements if the environment changes. In the ideal case this should require little or no manual operation.
- The network must adapt to the available capacity. It should be possible to modify the network QoS control and policy in real time if the situation requires so – for example in case of an unforeseen Medical Evacuation (MEDEVAC) operation.

5.0 CONNECTIVITY AND ROUTING

One of the main tasks of IST-124 was to study solutions for how to provide end-to-end connectivity in the heterogeneous mobile military network. We have discussed different routing architectures and considerations for this environment and have done analysis, simulation and some emulation experiments to gain more insight. We also describe different network security architectures that can be present in the heterogeneous networks at the tactical edge and we study how they might influence the routing architecture.

5.1 Routing Architecture Considerations

Several routing architectures with different advantages and disadvantages can be used to provide end-to-end connectivity in the heterogeneous network. In Annex E: “Routing Architecture Considerations for Heterogeneous Tactical Networks” we describe and compare three different architectures and identify three routing-related Information Exchange Interfaces (IEI) for coalition and system interoperability. The annex also gives an overview of the state-of-the-art and related work. A summary of the routing architecture discussion is given below.

We believe that there is no single architecture that fits all relevant scenarios. Thus, it is important to understand the characteristics of the different architectures and choose the one (or combination of several) that fits the operation best. The three architectures that we have described all aim to support a meshed network structure where traffic can flow between units or nations directly at low echelons (Figure 4), as opposed to a tree or stub network structure. This meshed structure is the most complex topology, but also the most flexible and robust one.

In order for any of the architectures to provide end-to-end connectivity, it must be possible to establish a connection between different nations. Possible approaches for the inter-nation connections, are (we envision that a combination of these will be in use in operational practice):

- Use a standardized NATO transmission technology common to some or all of the partners, e.g., STANAG 5630 “Narrowband Waveform for VHF/UHF Radios” (NBWF); and/or
- Use a proprietary transmission technology common to some or all of the partners (e.g., Harris 117G radio); and/or
- Interchange a few national radios (transmission technology) with partners; and
- Route via the deployed backbone.

The latter connection alternative does not require support for mesh topology at the tactical edge and is therefore out of scope for this discussion. The purple and grey networks in Figure 4 represent the

inter-nation connections and the dotted ovals shows interconnection platforms where the inter-nation transmission technology must be connected to other inter-nation and/or national transmission technologies. The interconnection platforms are also used to provide connectivity internal to a nation. If only a few interconnection platforms exist, these are likely to be single point of failures for the routing architecture and the connectivity cannot be made very robust. None of the described architectures are more robust than what the heterogeneous network can actually provide of connectivity. In Section 1.3.1 we summarize an analysis that we have done to show how many interconnection platforms we need in order to get good connectivity among the land-based forces in Vignette II of the Anglova scenario.

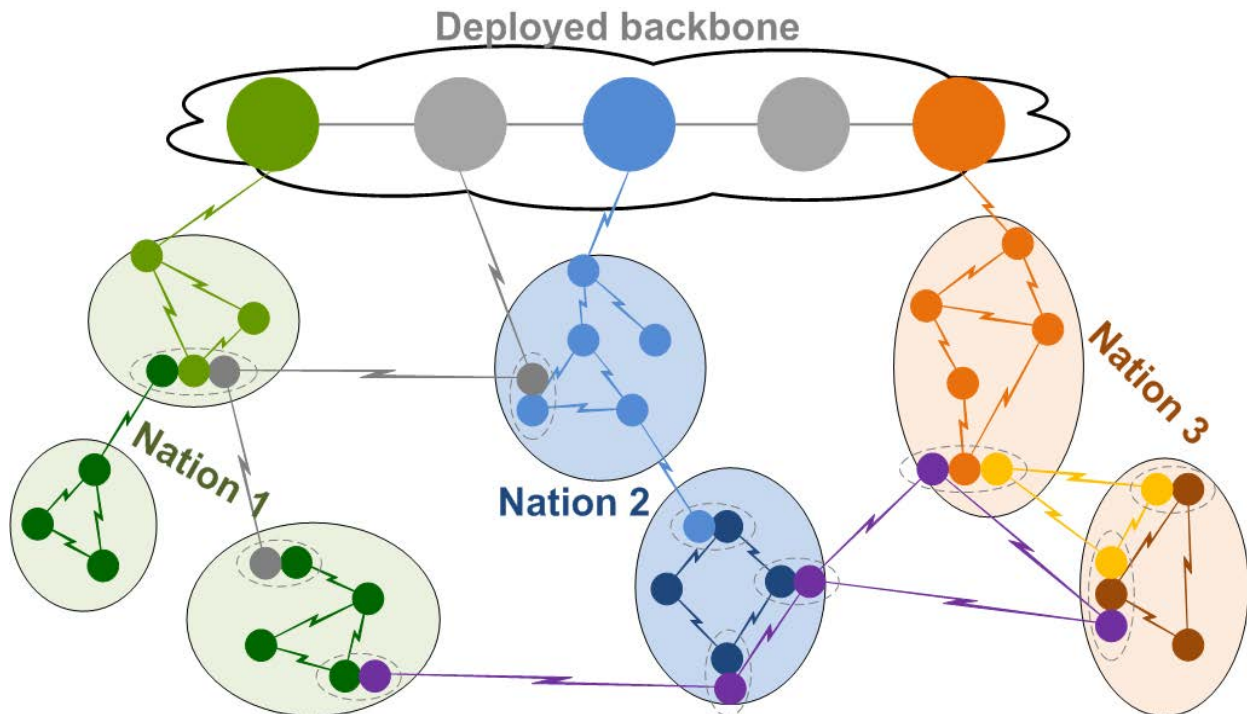


Figure 4: This Network Topology Represents a Situation Where the Different Network Segments are Connected as a Mesh. The network segments can belong to either different national units and/or different nations. The figure shows network connections (which might be different from the information flow).

5.1.1 Routing Architecture Approaches at a Glance

The three routing architectures that we discuss are:

- Flat, single routing protocol domain routing architecture (flat architecture);
- Interconnect routing architecture (multiple routing protocol domains), of which we describe two flavors:
 - Flat, interconnect routing architecture (interconnect-flat architecture); and
 - Interconnect routing architecture using an overlay (interconnect-overlay architecture).

5.1.1.1 Flat Architecture

For this architecture approach, one common routing protocol is installed and used by all network segments. Different transmission technology domains adhere to using a common routing protocol and don't use routing

protocols tailored for the specific transmission technology. The common protocol can also to some extent be tailored for different transmission technologies by utilizing dissimilar configurations of available parameters for the various transmission technologies (e.g., altered hello rates over links with different speed). This approach is visualized in Figure 5. This architecture is typically deployed with transmission technologies that are connected to a tactical router that runs the common routing protocol but could also be deployed with radios that have the common routing protocol embedded and runs this on both the wireless and wired interfaces. No information exchange interface on the routing layer is necessary, but an information exchange interface (IEI-M) between the routing function and the modem (transmission technology) is needed. This interface can also be a coalition interface in situations when a nation lends a radio (transmission technology) to the coalition partner's interconnection platform(s) in order to improve the connectivity in the network. The scalability and flexibility of this architecture is influenced by:

- 1) The required signaling by the routing protocol.
- 2) The information made available over the IEI-M interface.

The group has done a scalability study of this architecture on the Anglova scenario [10]. The experiment is summarized in Section 5.3.2.

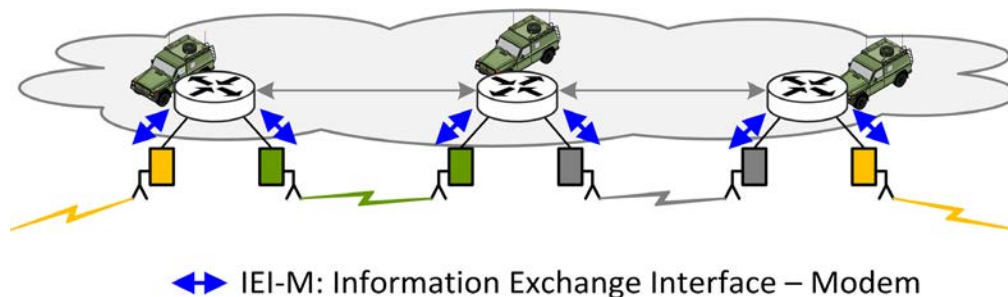
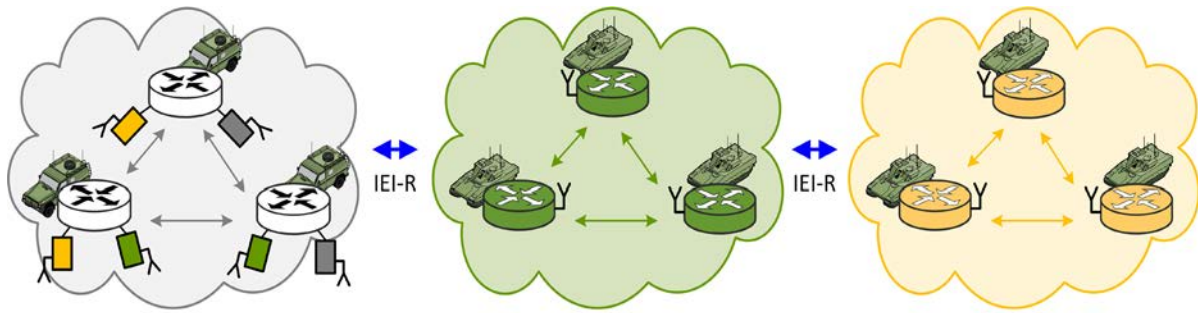


Figure 5: Flat Routing Architecture: There is Only a Single Routing Protocol Domain Built on Top of Multiple Transmission Technologies, Utilizing an Information Exchange Interface (IEI-M) Between the Routing Function and the Modem.

5.1.1.2 Interconnect – Flat Architecture

For this architecture type we are concerned with connecting network segments that are separate routing protocol domains. The network segments can use standardized routing protocols or proprietary protocols. Some segments might also use identical routing protocols on separate frequency bands or under different administrative domains. In this architecture, the routing domains are connected to each other using an Information Exchange Interface (IEI-R). Each location that is part of multiple routing domains (interconnection platforms where routing protocols from multiple routing domains are running) has an IEI-R between each two routing domains. This IEI-R can be both a national interface and a coalition interface. This approach is visualized in Figure 6. Via the IEI-R, the routing protocols of the respective domains inform each other about relevant reachability information for destinations that can be reached via the routing domain. The scalability, flexibility and robustness of this architecture are influenced by:

- 1) The level of detail of topology and link information made available via the IEI-R between adjacent network segments.
- 2) The functionality and overhead of the routing protocols in different routing protocol domains.



IEI-R: Information Exchange Interface – Routing

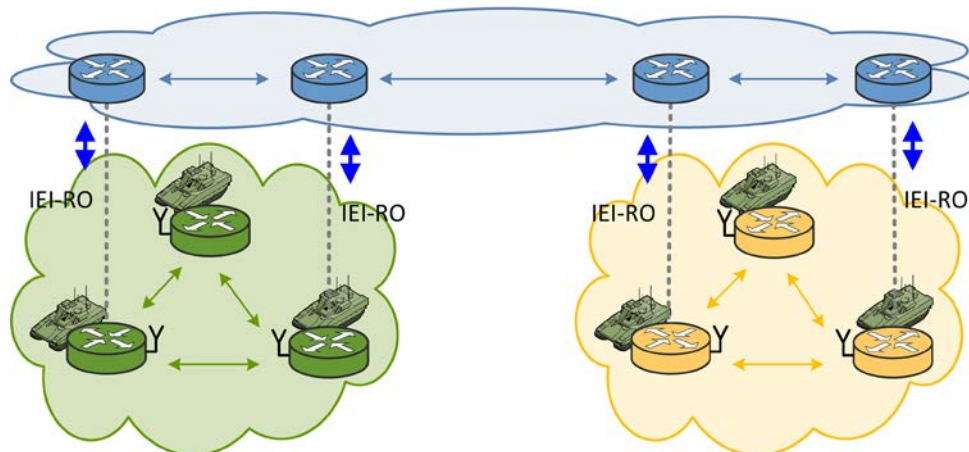
Figure 6: Interconnect – Flat Architecture: Multiple (Flat) Routing Protocol Domains. are Residing Next to Each Other with IEI-Rs Between Each Other.

5.1.1.3 Interconnect – Overlay Architecture

For this architecture we have the same situation as for the interconnect-flat case, with many network segments that are separate routing protocol domains. In this architecture an extra layer of routing is introduced as an overlay that spans the whole heterogeneous network and connects the separate routing protocol domains. Only a subset of the routers in the heterogeneous network participates in the overlay network. These routers are located on the interconnection platforms. This scheme is similar to the architecture the Border Gateway Protocol (BGP) uses to connect different domains. A routing protocol information exchange interface for the overlay (IEI-RO) is needed between the routing protocol in the overlay network and the routing protocol domains in the different network segments. Such an IEI-RO is located on the routers in the interconnection platforms. In this scheme there are no IEI-Rs between the different routing protocol domains. This approach is visualized in Figure 7. The scalability and flexibility of this architecture is influenced by:

- 1) The level of detail of topology and link information made available via the IEI-RO between the routing protocols in the different network segments and the routing protocol in the overlay network.
- 2) The functionality and overhead of the routing protocol in the overlay.

Simulation results of one possible design of this architecture is summarized in Section 1.3.5.



IEI-RO: Information Exchange Interface – Routing Overlay

Figure 7: Interconnect – Overlay Architecture: Some Platforms in the (Flat) Routing Protocol Domains are also Part of an Overlay Routing Domain (Blue) which Connects all the Separate Routing Protocol Domains.

5.1.2 Architecture Comparison

Table 1 shows the relative score of each of the architectures for a set of performance parameters. The parameters are described in Annex E, and the performance is discussed in detail in the annex. Note that the table presents expert opinions by the authors. Some experiments back up some of the scores, but more experiments are needed to proof the correctness of most of the scores. Note also that there are many parameters that control the performance of the architectures. One architecture might be best for one requirement in one scenario whereas another architecture is best for the same requirement in another scenario. For some of the requirements, there are no mature protocols with the necessary support. For those cases the rating represents a probability that a stable and scalable protocol can be designed.

Overall, it can be seen from the table that no single architecture scores the best overall, and combinations of architectural approaches may be necessary in practice. Generically speaking the flat architectures perform well in terms of heterogeneous connectivity, robustness and simplicity while the interconnect architecture may be more scalable, more cyber resilient and, especially the flat-interconnect, and more compatible with existing equipment.

Table 1: Relative Performance¹ of the Different Architecture Approaches on the Requirements.
Note that we assess the importance of some sub-categories to be higher the others, thus the overall character for the category is not necessarily an average of the sub-categories.
See Section E.5 in Annex E for the argumentation that lead to the rating.

Requirement	Flat	Interconnect-Flat	Interconnect-Overlay
Heterogeneous networking routing	***	*	**
• Connectivity	***	*	**
• Radio silence	**	**	***
Robustness	**	*	***
• Detect link break and find new route	***	*	**
• Multiple paths	***	*	**
• Network stability and vulnerability	*	**	***
• Cyber resiliency	**	*	**
Scalability	*	*	**
• Overhead from network control traffic	*	*	***
• Tailoring of the network control traffic	*	**	**
• Overhead from suboptimal paths and tunnels	***	**	*
Resource efficiency and QoS	***	*	**
• Optimized routes and QoS routing	***	*	**
• Providing multiple paths	***	*	**
• Network policies	**	**	***

Requirement	Flat	Interconnect-Flat	Interconnect-Overlay
Configuration and management	***	**	**
• Protocol and configuration complexity	**	**	**
• Remote management	***	*	**
Ease of deployment	*	***	**

¹ Three stars (***) indicates best score on the subject, one star (*) indicates lowest score on the subject. Three stars (***) indicates best performance compared to the other architectures. The stars do not attempt to describe how well the requirement is fulfilled.

5.1.3 Conclusion

Given the fact that the flat architecture does not scale to a large network size and that in practice it is likely that there will be multiple routing domains (e.g., different national tactical routers, separated administrative domains), we propose a target network design that has a hybrid routing architecture in which an interconnect-overlay protocol connects smaller network segments that use the flat architecture as well as some network segments that use an embedded routing protocol that is tailored for the transmission technology. We don't recommend to plan for extended use of the interconnect-flat architecture since it is very difficult to control the end-to-end performance, stability and overhead with this architecture, however we think it is useful to standardized the IEI-R interface for those situations where quick interoperability using interconnect-flat can provide an intermediate solution.

The suggested hybrid architecture is not well studied, and simulation or emulation experiments are needed to better understand the performance and to be able to suggest the best size of the local routing protocol domains and the size of the resulting overlay network. In addition, a well-studied standardized protocol that can act as the overlay routing protocol and that meets all requirements is currently not available. In all routing architecture discussions, we have aimed for a fully meshed architecture where topology information is shared between the different transmission technologies. These routing architectures for the mobile domain should be viewed in conjunction with the deployed networks that will be present in an operation. Some information will be shared via the mobile mesh links, while other information will be shared via the deployed coalition network. Especially for very large networks, the role of the deployed network is expected to be significant. If the deployed backbone is available to lower tactical levels, then the mobile networks can be smaller and the fully meshed routing architectures that we have studied in IST-124 are adequate. If the deployed backbone does not reach this far, then the mobile networks must be larger and aspects such as route aggregation and hierarchical routing approaches are expected to be necessary for scalability reasons. These aspects are left for future work.

5.2 Security Architecture and Its Implication for Routing

The goal of the security architecture work in IST-124 has been to outline the security challenges, possible solutions and provide architecture and design guidance to secure tactical heterogeneous networks. An overview of ongoing NATO standardization and other work relevant for security in tactical heterogeneous networks is also included in the report.

Assets to be protected in tactical heterogeneous networks include user data, user metadata, network management / control data and network, and the report adopts a trust model that discriminates between trusted internal entities, co-operative entities and non-trusted entities. Possible attack vectors are also discussed. Emphasis is put on the consequences of cryptographic protection located at different *levels*. Level here refers to

how close to the data source the cryptographic function is placed. The report distinguishes between *application level* protection located at the originating source host, *network level* protection located at the edge of a network and *link level* protection giving hop-by-hop protection, and discusses their pros and cons and possible combinations. The focal points are the security achieved, the impact on the network service, bandwidth efficiency, key management, and requirements for trusted platforms. Note that application level protection includes both end-device-to-end-device encryption as well application-to-application encryption.

As explained in the previous sections, a communication node in a heterogeneous tactical network may be equipped with transmission technologies (radios) with a routing protocol or with transmission technology (modems) connected to a tactical router that runs the routing protocol. For simplicity reasons, this section uses the term “Layer Three (L3) radios” for transmission technologies (radios) with embedded routing protocol, and “Layer Two (L2) radios” for transmission technology (modems) connected to a tactical router that runs the routing protocol. The layer two radio does not perform any routing. Figure 8 shows a tactical communication node with one layer two and one layer three radio. The radios may come with an embedded crypto that protects data transmitted over the radio network, or no security included at all.

Depending on the required classification level, there is generally a requirement for cryptographic protection of the user data exchanged over the network. User metadata such as traffic patterns and who talks to whom should also be hidden. Network control traffic is sometimes regarded as classified information that must be encrypted. However, for network availability, integrity protection that enables the receiving router to decide whether a routing message has been modified in transit or not can be more important than concealing the content from potential eavesdroppers. In any case, the protection is achieved by introducing cryptographic security boundaries.

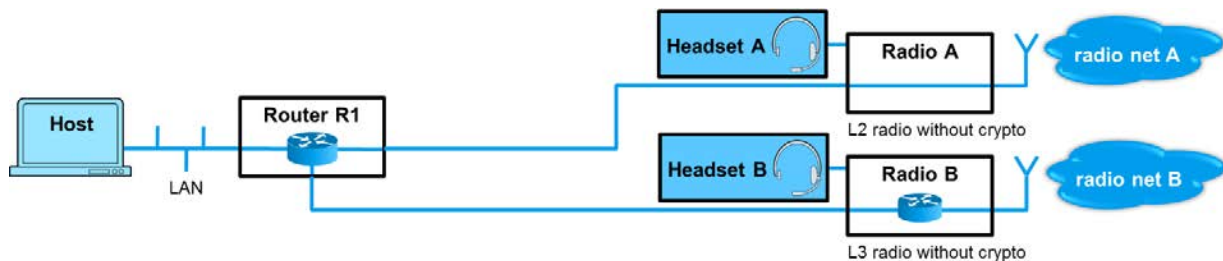


**Figure 8: Tactical Communication Node with Two Radios –
One Layer Two and One Layer Three Radio.**

The cryptographic security boundaries can be embedded with the radio or be external to the radio. This is described in more detail in IST-124’s Security Architecture report [11].

Figure 9 shows an example of a tactical communication node (e.g., a vehicle) that is equipped with four radios – i.e., layer two and layer three radios with and without embedded crypto (Z). The Z is used as a generic symbol for a cryptographic function. Radio A and Radio B have no crypto included. Radio C has link level encryption embedded, and Radio D network level encryption. The Z between Router R1 and R2 is a network level encryption device. Network level protection tends to introduce more routing domains. Routing information from R1 cannot be exchanged with R2 across the cryptographic barrier. If it could, there would be a security violation. This has implications when trying to create a flat routing architecture where R1 and R2 should be part of the same routing domain and/or synchronize their states. Annex E discusses this setup in more detail.

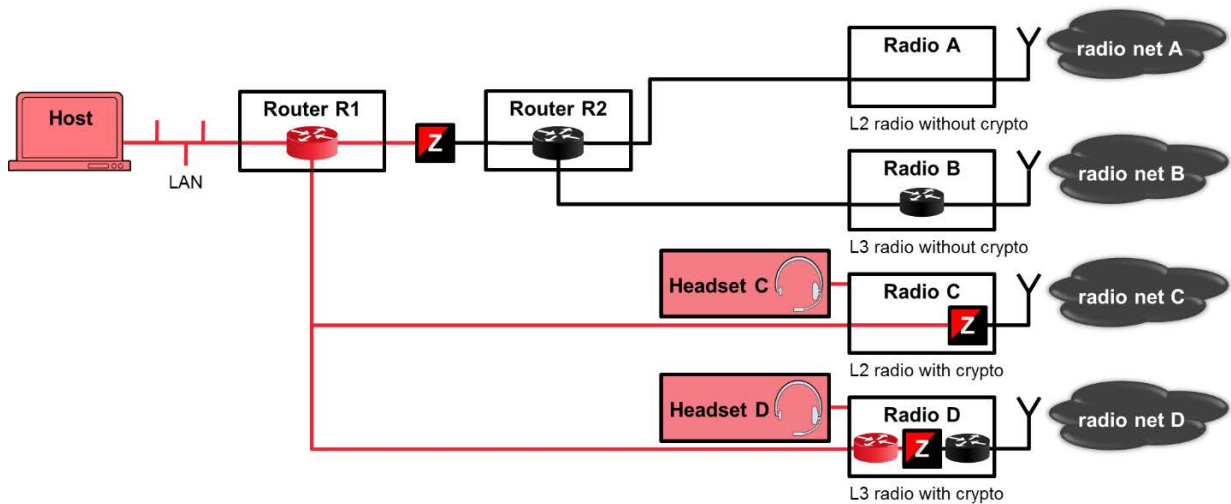


Figure 9: Tactical Communication Node with Four Radios and No Security Boundary Violations (Z Here Used as a Generic Symbol for Cryptographic Security Function).

The routing architecture described in Annex E shows how link level encryption-based solutions have less impact on the routing architecture than network level encryption, in the sense that the Routing Information Exchange Interface (IEI-R and IEI-RO) are less likely to cross a security boundary. Such a hop-by-hop link level protection scheme could be used in conjunction with an application level protection scheme that encrypts data from end-host to end-host for proper protection of user data, as well as user and network metadata and signaling. However, application level protection schemes require a dedicated encryption module in every end-host. This may not always be possible.

The use of network level protection (as illustrated between Router R1 and R2 in Figure 9) protects user data LAN to LAN and simplifies the logistics in the sense that a single encryption device can protect multiple hosts and applications. This reduces the number of cryptographic devices and cryptographic keys required compared to application level protection schemes. Depending on key distribution scheme, it may also reduce the key management overhead. On the flip side, network level protection schemes may lead to separate routing domains on each side of the cryptographic function and complicates the transport of multiple security domains over the black transport network. Both the Security Architecture report [11] and the routing architecture discussed in Annex E show that there is no single solution that fits all situations; all have their advantages and disadvantages. Depending on the radios to be used, different measures may be needed in order to obtain a solution that provides the proper protection. In any case, if an IEI crosses a security boundary, an assessment will have to be made to what extent the functional and performance gains in terms of heterogeneous networking and network centrality outweighs the increased security risk of creating a potential covert channel, or leaking information via the IEI bypass from the plaintext (protected/red) side of the cryptographic boundary to the encrypted (unprotected/black) side. Note that this trade-off also holds when adding QoS functionality where applications have some level of network awareness and rely on information such as available capacity that is obtained from the network.

5.3 Experiments and Analysis

In this section we briefly describe the analysis, simulation and emulation experiments IST-124 has done to gain more insight in the different routing architectures and protocols to realize the different architectures. We have studied:

- How the end-to-end connectivity in a heterogeneous network is dependent on the number of interconnection platforms (circled platforms in Figure 4) in the network.

- The scalability of the Optimized Link State Routing Protocol (OLSR) v1 and v2 utilizing the flat routing architecture in a battalion sized network (land based forces in the Anglova scenario).
- The scalability of Open Shortest Path First (OSPF) with mobility extension utilizing both the flat routing architecture and the interconnect-overlay routing architecture in a battalion sized network (land based forces in the Anglova scenario).
- The performance of OLSRv2 in conjunction with Mobile Ad Hoc Relay Line of Sight Networking (MARLIN, STANAG 4691) using an interconnect overlay architecture in the naval task force in the Anglova scenario.
- The advantages and disadvantages with a depth first search protocol as the protocol in the interconnect-overlay routing architecture.

5.3.1 The Density of Interconnection Platforms

For all heterogeneous networks where different transmission technologies are present (these technologies are not compatible over the air) there must be a number of interconnection platforms where such different transmission technologies can be physically connected (e.g., via a wire) in order to allow traffic to flow from one transmission technology to another. First and foremost, there must be a sufficient number of interconnection platforms to provide full connectivity in the network, secondary it is beneficial to have even more interconnection platforms to allow for alternative paths and prevent single-points-of-failure in the network. With full connectivity in a network, we here mean that any given node can reach (directly or via multi-hop) all other nodes in the network. The number of interconnection platforms impacts both the performance and complexity of the network design. The interconnection platforms are the platforms where topology information is exchanged between transmission technologies and/or routing domains (the grey stippled ovals in Figure 4 represent interconnection platforms). Having multiple interconnect platforms is needed to improve the network robustness, but can also complicate the network design, e.g., the risk of routing loops in the network increases when topology information is exchanged between dissimilar transmission technologies. Moreover, the number of interconnection platforms that is needed to provide the required connectivity and network robustness largely depends on the used transmission technologies, frequency bands and the mobility pattern for a given scenario. As such it is an important parameter when designing/deploying a tactical network that is based on the principles of the routing architectures discussed in Annex E.

For our analysis we consider a heterogeneous network based on Vignette 2 of the Anglova scenario (see Annex A and Annex B), where each company forms a Company Network (CN) with a unique transmission technology. To connect the companies, we select a number of nodes in each company to be interconnection platforms. On these platforms we install a second transmission technology that is used to create an inter-company radio network. We consider a heterogeneous network consisting of four companies (with a total of 96 nodes) in the vignette. To investigate the number of required interconnection platforms needed in order to get sufficient connectivity we have made connectivity calculations. We show how the average connectivity varies with the number of interconnection platforms per company, for different combinations of transmission technologies both in the company network and intra-company network (see Annex F: “Interconnection Platforms in Vignette 2” for details). The connectivity values in the figure represent the average fraction of nodes in the heterogeneous network that can be reached (directly or via multi-hop) from a source node. The average is taken over nodes and time.

For example (Figure 10), almost full connectivity is reached during most of the time by using four interconnection platforms for each company and a medium band transmission technology at a UHF frequency of 300 MHz for the inter-company transmission technology. For the company network, a wideband transmission technology is preferred as it has the highest data rate and the distance between the units is limited. The connectivity is only marginally improved if a medium band transmission technology is

used instead in the companies. If a narrowband transmission technology is used for the inter-company network, good and sufficient connectivity is obtained with only one interconnection platform per company. Unfortunately, the low data rate limits the amount of data traffic that can be sent between the companies considerably. Using a medium band transmission technology in the 50 MHz VHF band is an option but it is questionable if enough spectrum is available in that frequency band for an operational scenario of considerable size. The main option is therefore to use the medium band transmission technology at the 300 MHz band for the inter-company network. Nevertheless, in that case around 4 to 6 interconnection platforms per company are needed as well as an efficient routing architecture to form routes across the company transmission technologies and the inter-company transmission technologies. If the added robustness of multiple paths is required, more interconnection platforms are needed.

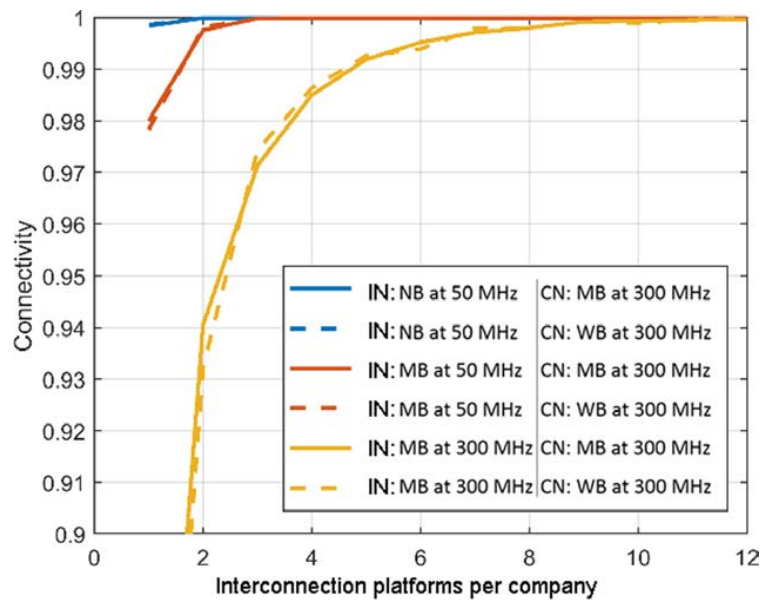


Figure 10: Figure Showing Connectivity with Different Number of Interconnection Platforms per Company for Different Transmission Technologies. IN = Inter-Company Network, CN = Company Network, NB = Narrowband, MB = Mediumband, WB = Wideband.

5.3.2 Scalability of the Flat Architecture with the OLSR Protocol

The increasing demand for information exchange in a tactical operations environment is accompanied by increasing expectations towards reliability of data transmissions. A way of addressing this trade-off in design goals is to combine heterogeneous radio technologies, each designed to match a specific subset of the requirements, in a single routing domain, following the flat routing architecture (described in Annex E). For example, mission-critical information should be transmitted using a robust anti-jam transmission technology, while a less robust transmission technology offering a higher throughput is more appropriate for supplementary data. On the other hand, interconnected and hierarchical routing mechanisms are needed, e.g., to provide additional scalability. In all cases, standardized routing mechanisms provide an ideal basis for interoperability, especially when combined with a standardized IEI-M interface.

Much standardization work has been done recently at the IETF that allows for standardized technical solutions as the basis for many of the interoperability issues that come with current tactical communication solutions. One of these solutions is a flexible modular and extendable ad hoc routing protocol. Due to its already advanced feature set and the progress in standardization, OLSRv2 (The Optimized Link State Routing Protocol Version 2 – RFC 7181) [12] has been deemed the most suitable candidate by the IETF for Mobile Ad Hoc Network (MANET) routing. The protocol currently seems the only viable successor to the widely used ad hoc routing protocol OLSR (Optimized Link State Routing – RFC 3626). Furthermore,

additional standards, such as multi-topology routing, that allows for policy based utilization of the different communication links and routing metrics, as well as heterogeneous communication links (Directional Airtime Metric Based on Packet Sequence Numbers for Optimized Link State Routing Version 2 (OLSRv2) – RFC 7779), are already being defined for OLSRv2 and prototype implementations exist. In contrast to OSPF, OLSRv2 was designed for mobile environments and no mobility extensions are needed that might be incompatible with other extensions like multi-topology routing.

In order to test the suitability of OLSRv2 in comparison to its predecessor OLSRv1 in a mobile tactical scenario and to assess the scalability of the different protocol versions, a comparison of OLSRv1 and OLSRv2 in different configurations has been performed as part of the IST-124 work. A subset of the Anglova scenario (Annex A and Annex B) was used as the basis for emulation-based experimentation with up to 96 nodes. The movement pattern of this part of Anglova Vignette 2 is depicted in Figure 11. Real implementations of OLSRv1 and OLSRv2 [13] were connected via the EMANE [7] network emulation framework. To obtain a wideband transmission technology with a passable range, the model of the narrowband transmission technology was scaled to a 250 kHz medium band transmission technology with a nominal link data rate of 175 kbps. The data rate was only enforced in the emulation for the egress links and no medium access mechanism for a common channel was used.

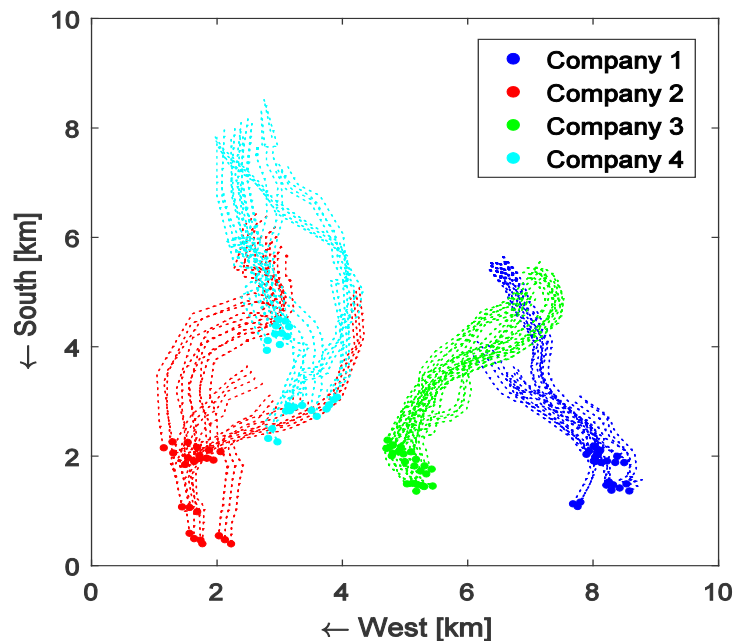


Figure 11: Illustration of the Movements in Four Companies (24 Nodes Each) of Vignette II of the Anglova Scenario. The picture shows about 15 minutes of the more than two hour long Vignette.

Figure 12 provides an overview of the scalability results regarding OLSRv1, OLSRv2, and OLSRv2 with a Multipoint Relay (MPR) mechanism to further reduce the protocol overhead in dense topologies. In general, the overhead is comprised of Hello and Topology Control (TC) messages. We measured the traffic in terms of kilobits per second (kbps) as well as packets per second. The values represent the total amount of incoming traffic as seen by the nodes in the network. Under the emulation presumptions, this reflects best the overall load imposed on the network. In the paper we also show routing traffic as well as packet delivery ratio for the different companies and for different path lengths. Of course, the results are strongly influenced by the parameters used for the protocol. For this reason, we used a single configuration for all protocols. The Hello interval was set to 2s (with a validity interval of 20s), and the TC interval was set to 8 seconds (with a validity interval of 80s).

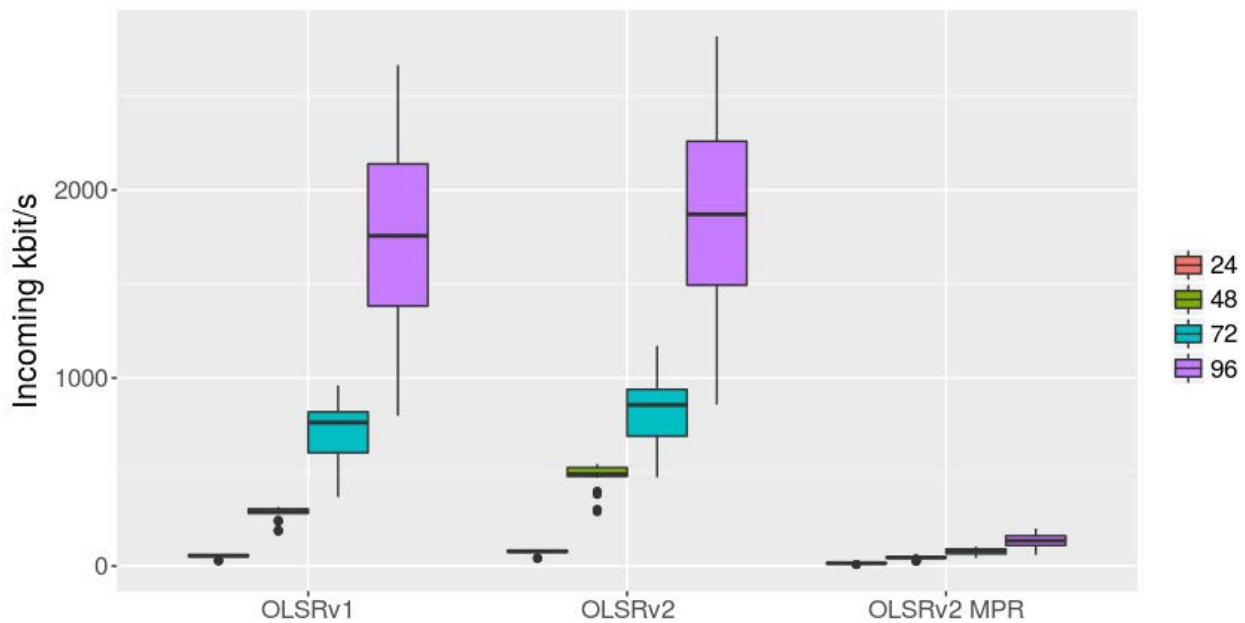


Figure 12: Overhead Analysis Regarding Incoming Protocol Traffic per Node Regarding the Different Protocols.

With these parameters only the overhead of OLSRv2 with MPR is below the link capacity of 175 kbps assumed for the transmission technology. Further reduction in overhead can be achieved by increasing the Hello and TC intervals. However, there is a trade-off with respect to reaction time to topology changes. The overhead of OLSRv1 and OLSRv2 without MPR was very similar.

Additional details can be found in Ref. [10]. As a summary, OLSRv1 and OLSRv2 without MPR could be used only for the 24 node network. OLSRv2 with MPR scales well in terms of generated data overhead. It consumes only a fraction of the link data rate in scenarios up to several tens of nodes. In addition, the variation of produced traffic is also very low. The improvements to the MPR mechanism that were performed as a preparation for the IST-124 experiments were introduced into the open source implementation of OLSRv2. One of the purposes of the experiment presented here was to get a better understanding of the scalability of the most popular proactive routing protocols when used in a military scenario characterized by high node density, long range, and low data rates. OLSRv2 is a promising candidate and scales well even to larger networks. Several mechanisms can be used to further reduce the overhead and improve the scalability as briefly discussed. However, to scale it even further (e.g., battalion size and larger), some hierarchical routing architecture must be in place. For future work, we will look into methods to reduce the overhead, use alternative system configurations such as more efficient parameter settings, explore hierarchical network structures with two level routing, investigate region/fisheye mechanisms with TC filtering and aggregation, and finally use link quality metrics that use information from lower layers. One of the next steps will however be the combination of different transmission technologies in a single flat network. Combining short range high data rate transmission technologies with longer range transmission technologies at certain nodes increases the data rates that can be used with closer neighbours and thus allow for new forms of tactical applications, it also allows for higher spatial reuse and thus relaxes the requirements on the MAC layer of the transmission technology in terms of the number of neighbours it has to cope with.

5.3.3 OSPF Analysis

Open Shortest Path First (OSPF) [14] is one of the most widely used routing protocols on the Internet. OSPF has been developed for fixed networks, with infrequent topology changes. Therefore, additional extensions

to OSPF, OSPF MANET extensions (see Refs. [15], [16], [17]), have been proposed in order to better cope with frequent topology changes in an efficient manner (low signaling overhead). The benefit of using OSPF both in mobile and fixed domains is the need for expertise of only one well known routing protocol. However tactical mobile networks have relatively low capacity and therefore it is uncertain if they can handle the signaling overhead of OSPF. In Annex G: “OSPF Scalability”, we evaluate OSPF MANET extensions used with a broadband transmission technology for a scenario similar to Vignette 2 (up to 156 nodes, see Annex A and Annex B for more information). Similar to the OLSRv2 experiment described above, this work investigates whether OSPF MANET extensions are suitable for use in tactical mobile networks, by studying the signaling overhead caused by the often rapid rate of topology change in the mobile network and comparing it to the available capacity. In this analysis two of the different routing architectures described in Annex E are studied. We assume that the network capacity is between 0.5 and 1 Mbit/s, shared among the nodes. The network has a high rate of topology change: in the order of 100 link changes per second.

The flat architecture (Annex E) can be seen as the typical Internet Engineering Task Force (IETF) architecture for OSPF used in a MANET. For the first set of evaluations with OSPF MANET extensions, the flat routing architecture was used. Because there are no further routing protocols in use, OSPF must handle all link changes, resulting in a constantly high overhead. Other studies (see Annex G) provide simulation results that show an average of over 0.5 Mbit/s in overhead traffic for a flat architecture used in a fairly large network. These results show that using OSPF with MANET extensions in a flat architecture containing all the nodes in Vignette 2 in one network, is not a viable solution.

The OSPF MANET extension OSPF MDR [16], was also investigated in the interconnect-overlay routing architecture described in Annex E. We here assume that OSPF-MDR is used to form an overlay network across all subnetworks, much like BGP (Border Gateway Protocol) and that the radios manage local ad hoc network routing internally. The radio may have an internal IP router (layer three radio) or no internal IP router (layer two radio). In the latter case, for this study we assume that local routing occurs in the ad hoc network below layer three. In our evaluation we assume that the external overlay routers run OSPF-MDR and that the radios are layer two radios that perform local routing below layer three. The interconnect-overlay architecture used in this manner hides much of the topology changes from the overlay routing protocol, in this case of OSPF-MDR. Only changes in the network size, e.g., because of network partitioning, is seen by OSPF-MDR and considered in the overhead evaluation. The results from the analysis show that even if network partitioning occurs sporadically, OSPF-MDR still generates an inconveniently large overhead when network partitioning occurs.

None of the analyzed routing architectures for heterogeneous networks with OSPF with MANET extensions as the network layer routing protocol, are deemed to be suitable for network sizes as seen in Vignette 2. However, it should be noted that the majority of the nodes in a battalion probably only have one radio with sufficient data capacity to be part of the heterogeneous network. Therefore, one option is to use a simpler routing protocol that interacts with OSPF MANET extensions in these nodes (Interconnection platforms). Further investigations are required, both in terms of requirements and how the routing problems should be solved in heterogeneous networks.

5.3.4 Naval Routing Experiment

The Naval Task Group in Vignette 2 of the Anglova scenario is used for this experiment (see Annex A and Annex B). An IP Based Ad Hoc Network Controller product based on STANAG 4691 Multi-hop IP Networking with Legacy UHF Radios: Mobile Ad Hoc Relay Line of Sight Networking (MARLIN) [18] was tested. This product is planned to be used on V/UHF and HF networks and the use of standard routing protocols for naval platforms employing V/UHF and HF frequencies for IP based communication is foreseen. The typical operational concept which is defined is depicted in Figure 13.

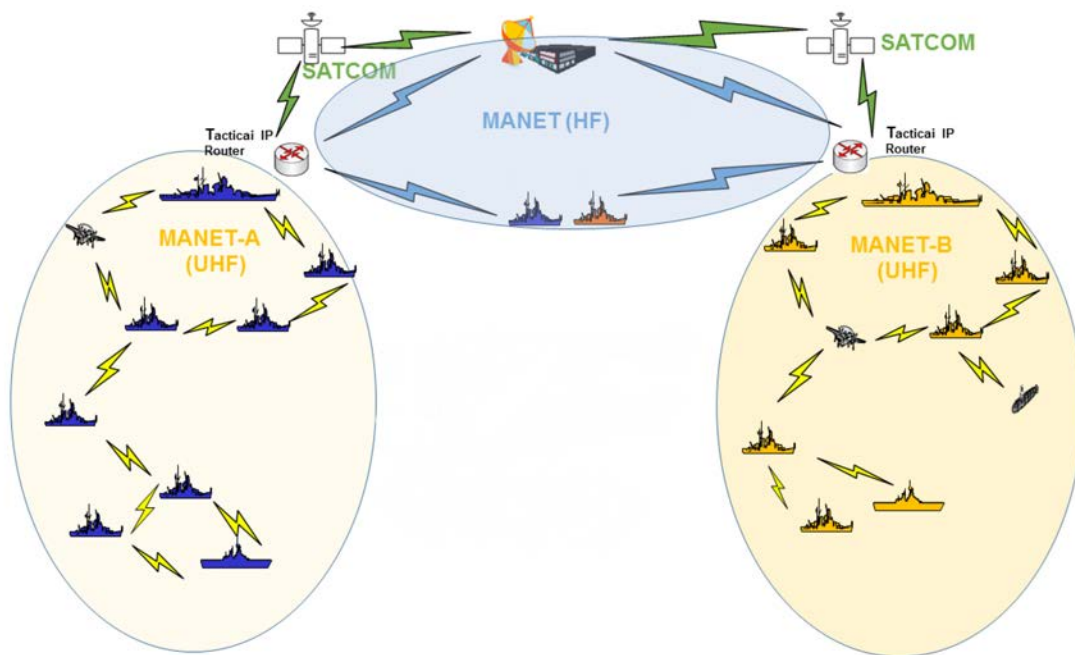


Figure 13: Operational Concept of MARLIN Implementation.

The main objectives of the experiment were:

- Measure the effectiveness of Tactical Track Exchange functionality with the selected routing architecture and protocols.
- Measure the average track delivery time and packet delivery ratio at the target under the following constraints:
 - The typical track stale time for such a Tactical Information Exchange System is assumed to be:
 - Air Track stale time: 20 seconds; and
 - Surface Track stale time: 2 minutes.
 - Achieving a Packet Delivery Ratio (PDR) of 70% for more than two hops is considered as a success.
- Measure the benefits of an airborne relay.
- Test if any improved performance can be seen from using Robust Header Compression (RoHC) [19] (version 1.7.0) on the IP headers.

The following transmission technologies were used in the experiment:

- Transmission technology for V/UHF: @25 kHz, 64 kbit/s; and
- Transmission technology for HF: @3 kHz, 4 kbit/s.

We tested the tactical track exchange capabilities of the system, excluding the Satcom interface. The specifics of the experimentation are listed below:

- The naval part of the Anglova scenario Vignette 2 is used. This is a two-hour scenario with 23 units (21 ships, 1 MEDEVAC helicopter, 1 Shore Based Headquarter).
- 8 ships, the MEDEVAC helicopter and the HQ are deployed with both transmission technologies (UHF and HF). The remaining platforms are only deployed with the UHF transmission technology.

- The scenario starts with full multi-hop UHF connectivity among the units (except HQ). During the experiment topology changes occur in the UHF network. The HF network is always connected. After some time two task groups depart from each other. 40 minutes into the scenario, the MEDEVAC helicopter is airborne to help to improve the network connectivity between the task groups.
- OLSRv2 with MPR [12] is selected as the routing protocol to tie the V/UHF and HF networks together. Both the UHF network and the HF network use internal routing at layer-2 and as such this experiment uses the interconnect-overlay routing architecture with OLSRv2 as the overlay protocol and MARLIN (STANAG 4691) and the underlying protocol (see Section 1.1.1 and Annex E). Since broadcast traffic is not supported by the OLSRv2 routing protocol, broadcast traffic is distributed by the underlying MARLIN implementation.
- Since the HQ is far away, the overlay IP-level routing must always be consulted to deliver the information to the HQ by way of the HF transmission technology.

The Multi-Generator (MGEN) tool was used to generate traffic with the following characteristics:

- Each node sends 200 bytes every 12 seconds in broadcast mode through UHF transmission technology to simulate track exchange by using compact Link 22 track messages. Assuming basic track information via Link 22 can be expressed in 18 bytes, this corresponds to approximately 11 tracks each 12 seconds per ship.
- Each node sends 1000 bytes every 96 seconds /2 minutes through UHF to HQ to simulate track information summary.

We observed that (for the given scenario) the tested design can be effectively used for exchange of surface tracks, with some improvements to the router. With an airborne relay it is even possible to exchange air tactical pictures with distant groups. It is necessary to study closer possible improvements from using header compression and utilizing Information Exchange Interfaces (IEI) between routers and between a modem and the router (e.g., DLEP). We also see that QoS mechanisms for perishability² must be in place.

For more details of this experiment and the results see Annex J: “Naval Component and Routing Experiment”.

5.3.5 Depth First Search Protocol for the Interconnect-Overlay Architecture

In this study we take a closer look at the interconnect-overlay routing architecture (Annex E). One example design of this architecture that has been studied by one partner of the group is the use of a depth first search protocol in the overlay. The target scenario for that study was a heterogeneous network similar to the network present in the Anglova scenario (Annex A and Annex B), where both low data rate and high data rate transmission technologies exist in the network. For such a network, it is important to be able to steer both network control traffic and the user traffic to make sure that the low data-rate networks are not congested. An important design criteria for the protocol was to support dissimilar network management traffic over different transmission technologies and let the network policy decide when and how to utilize the different transmission technologies (e.g., allow only high-priority traffic to ask for routes over low data-rate networks). The protocol should be a tool that could help network planners to enforce the operation’s preferred network policy (e.g., network utilization and QoS support) in the entire heterogeneous network.

Another input parameter to the work was the assumption that most traffic in the network would be local to one transmission technology. Thus, we wanted to support the use of routing protocol domains optimized for a specific transmission technology (radios with tailored routing) and provide an additional means to find routes that cross several transmission technologies, when needed. Using an interconnect-overlay architecture

² Dropping packets that have aged longer than a certain threshold to avoid using network resources to send outdated packets.

seemed to be a wise choice. Using two companies of the Anglova scenario as an example (Figure 14), transmission technologies with tailored embedded routing would then run on the different radio networks in the companies and build local routers, and a lightweight policy enabled protocol would run on the tunnels in the blue overlay of the figure to provide connectivity across different transmission technologies.

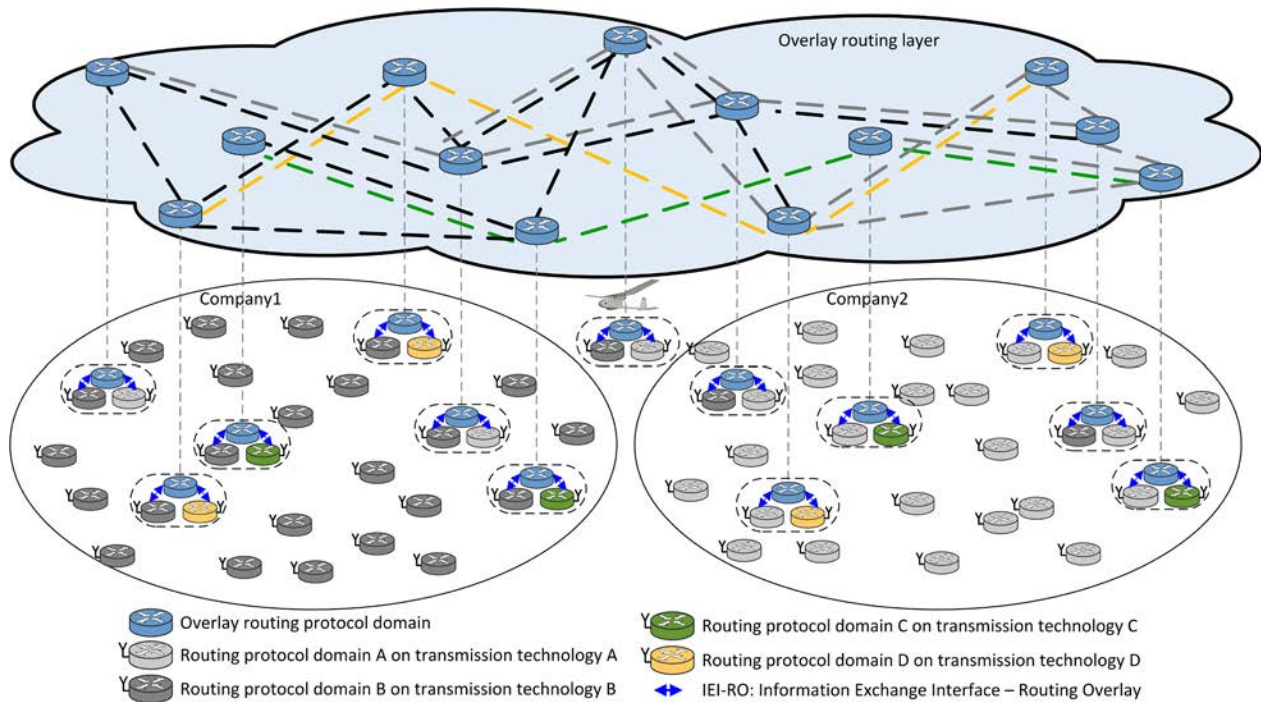


**Figure 14: A Routing Function in Selected Interconnection Platforms Builds
a Virtual Overlay Routing Protocol Domain to Provide Routes
Across Several Local Routing Protocol Domains.**

To limit the signaling overhead we chose a reactive protocol design. Normally reactive protocols use breadth first search, however, that implies that all searches also run over low capacity transmission technologies. Instead we chose depth first search, to avoid traversing low capacity transmission technologies unless the network policy dictates that we should, or all other route possibilities are exhausted. Reactive approach is always a trade-off between delay and overhead. The depth first search will often have increased delay, since there is a risk that unsuitable branches will be searched first. With depth first search there is also a disadvantage of finding suboptimal paths. In Ref. [20] we show how hints can be used to mitigate the disadvantages.

A depth first search strategy allows both the network control traffic and user traffic to be controlled using different policies and QoS methods. The protocol is designed to discover multiple paths with different QoS properties between a source and destination, if needed. This design supports, e.g., the possibility to set access to a virtual link to 0 to block this link (transmission technology) for all transit traffic. See Ref. [20] for more details and early simulation results. We believe that this type of protocol and architecture is a good design for the specified scenario and should be one of several designs available for a network planner to choose from when planning the network for an operation.

6.0 QUALITY OF SERVICE IN HETEROGENEOUS NETWORKS

The other main task of IST-124 was to study solutions for how to provide end-to-end Quality of Service (QoS) in heterogeneous tactical networks. It is commonly agreed that some Quality of Service (QoS) is

needed in networks and especially in military networks. However, QoS is understood differently by different parties and it is good to review these different viewpoints. Implementing QoS brings additional costs to implementing and operating a network, mainly in form of increased complexity. Benefits from QoS mechanisms deployment must be well evaluated and not only based on a subjective feeling from a network manager of having additional network control.

From a network engineer's viewpoint, QoS is a set of mechanisms that can be implemented in network devices to provide a set of different traffic treatments that allow the network to comply with requirements set by an application.

A network user expects the applications to work with sufficient fidelity. How this is accomplished is irrelevant for the user unless additional actions such as payment, physical relocation or change of communication method are needed by her.

One of the overarching goals of the QoS framework of a mobile heterogeneous network is to make sure that the information that best serves the mission's objectives, should be available where and when it is needed. Identifying manually or automatically the information that best serves the mission's objective is a difficult task. Recent research in the area of information management and information dissemination to military operators has resulted in exploiting two notions – that of Quality of Information (or QoI) and Value of Information (or VoI). This research can help identifying the important information, whereas the QoS mechanisms must make sure to bring the information to the right destination, in time.

Tactical networks can be considered as challenged networks. These are often deployed with mobile and semi-mobile networks. The total available capacity of mobile networks is typically only a fraction of what civilian mobile networks can provide. In the latter, traffic demand is controlled by different subscription plans, throttling traffic and subscription quotas. Customers do not expect other than best-effort traffic although providers may prioritize some traffic over another.³ Comparing military mobile networks to civilian mobile networks, we can identify the following key differences regarding treatment of traffic:

- Network users with different roles or different traffic types should get unequal treatment from the network. The information that has most value for the mission should be given a priority. This may result in starvation for some network or rejection of specific traffic types.
- Which traffic to prioritize (the information with most value for the operation) can change over the course of time. Especially, if the type of operation changes suddenly, for example from an offensive operation to a rescue operation.
- Different traffic classes should be marked and the correct marking should be enforced. The marking can be trusted.
- The networks may consist of multiple radio transmission technologies (LOS, BLOS, Satcom) on different frequency ranges (HF, VHF, UHF), with different characteristics. These typically have relatively low capacity compared with civilian networks.
- The network topology can be complex and a path between nodes may have multiple links with different characteristics (see previous).
- Centralized network control cannot rely on real time access to network nodes. In tactical military networks, network access is typically not based on a fixed infrastructure (stationary base stations with wired backbone), on the contrary many networks establish ad hoc connections that change rapidly as network nodes move.
- The offered traffic load to the network will often be higher than the network capacity.

³ Depends on local legislation and concepts such as Network Neutrality.

- Traffic includes real time traffic that does not have any value if it is delayed more than a certain threshold time, expired data should be discarded.

6.1 Discussion on QoS

6.1.1 QoS Mechanisms

Two resource management paradigms have been defined for the Internet: Integrated Services [21] and Differentiated Services [22]. The first one uses reservations based on traffic selectors. It has not gained popularity in part because of missing business cases and is mostly forgotten. The latter one is in use within corporate networks and network providers but is not often used in customer-facing Internet services. This is because it is challenging to make a business case to sell better quality services via other approaches than just increasing the bandwidth for a subscription, e.g., via traffic differentiation or prioritization. For example, Ref. [23] includes a discussion on such challenges.

In civilian networks there is a multitude of actors. In order for QoS mechanisms to work many actors must agree on (and apply) common policies for how different traffic is classified and how different classes are marked and treated. Additionally, since users tend to want the best service for themselves, they would have an incentive to mark all of their traffic to highest priority when they compete for limited resources. Some regulation must be in place to control this. Within a military operation all coalition partners utilizing the same network share a common goal, thus it is easier to enforce common rules for traffic priority and some regulation to ensure that users play fair. For example, email traffic is marked correctly as email and not as low-latency network control.

Each coalition partner has at least two domains where traffic classification and handling are applied: internal to the national networks and on interoperability points to other coalition partners. The latter must be standardized and common principles and mechanisms for the coalition must be defined. If this is not the case, end-to-end QoS treatment cannot be assumed. For example, nations A and B assign voice traffic to a traffic class providing low delay and low packet loss. A call from A to B must transit through a network segment provided by nation C. Nation C does not identify the traffic as voice traffic but treats it as best-effort traffic. The result is that the priority handling of the packet by A and B was a waste of resources since the packet experiences long delay and high packet loss in the nation C's network segment.

In wired networks, link capacities are well known. Unless there is equipment malfunction, a point-to-point gigabit Ethernet connection allows one gigabit of traffic minus framing overhead to pass through. Different traffic (types, different sources, etc.) can be allocated their own fraction of the network capacity expressed in megabits per second. In radio networks where several links share a common channel, and especially in tactical mobile radio networks under the effect of the enemy's Electronic Warfare (EW), the link capacity is uncertain and very variable. Some traffic requires a certain minimum fixed capacity in order to provide a useful service. Other traffic can adapt to use its varying relative share of the network capacity. From this it is given that it is a challenge to build a network that makes near-optimal traffic prioritization and treatment. A realistic solution must be something that provides good enough handling for high-priority traffic and allows any excess capacity to be used by low-priority traffic.

6.1.2 Network States

In order to provide best possible QoS and resource management for heterogeneous mobile military networks, we believe it is necessary to identify the current operating state of the network. We propose to define the three following network operation states that the network can be in:

- 1) **Normal operation** is the state the network is built for. QoS mechanisms can (and should) be enforced to provide good user experience and to cater for application specific needs like low delay

delivery. The network capacity may vary within an order of magnitude of the normal operation capacity because of external factors like troop movement, loss of links, jamming, physical damage to points of presence, and other external factors.

- 2) In **reduced capacity** state there is a significant loss of service. Throughput may be much lower than designed and network-wide end-to-end connectivity is not consistent. QoS mechanisms that aim for fairness and good overall user experience should no longer be used. The roles of the QoS mechanisms in this state are to make sure that the most *important* services – for *the mission* – can still have the fidelity they require. Resource-hungry applications must be blocked.
- 3) In **last effort** state the network has capacity measured as low as tens of bits per second. End-to-end traffic flows can no longer be supported but communication is reduced to bare essentials in individual message mode (e.g., redundant transmissions, use of caching and delay tolerant network modes). A node must identify this situation based on only local information: directly connected peers, links and individual datagrams it observes. QoS mechanisms must work without any signaling or access to any central service.

As indicated in the description of the states, the resource management and traffic management mechanisms and policies must be different in the different states. For example fairness, is important in the “normal operation”, whereas in “reduced state” fairness is not a goal, on the contrary it is important to prioritize the most important services and users. The selected method(s) for traffic control and QoS must be able to automatically adapt or disable itself for the different states.

6.1.3 Quality of Information (QoI), Value of Information (VoI)

In order to best utilize the scarce network resources, the most *important* services – for *the mission* should ideally be identified and conveyed to the admission control and forwarding elements of the network. We believe that network mechanisms (both manual and automatic) must be in place to help identify both QoI and VoI. Particularly VoI which attempts to identify the importance of an information element for the user given the current task and situation is very valuable.

Calculating the actual VoI of an Information Object (IO) for a particular consumer is challenging, as it requires the system to model each consumer in terms of their existing knowledge, their objectives, their information needs, and their decision-making strategy. The literature describes several different approaches (see Annex I for more details). Irrespective of the approach taken to determine the VoI of an IO, the concept of using VoI changes the system design for disseminating information. There must be an added intelligence in the data dissemination model that constantly evaluates if an IO is important for a specific destination (contextual information). The specific nature of the contextual information depends on the algorithm for determining VoI, but it could include elements such as identity, role, mission, and for mobile nodes, current position and planned routes. It could also include logistics-related information such as food, water, fuel, and ammunition levels, as well as physiological and health measures, if the client represents an individual user.

Prior experimentation by some of the group’s members has revealed three different deployment patterns for exploiting information value-based dissemination, which are shown in Figure 15. The first deployment pattern applies to information from a command/operations centre flowing to dismounted soldiers using a tactical network. The second deployment pattern applies to information from the tactical network, including dismounted soldiers and sensor networks, being transmitted back to an operations centre, where the consumer may be an analyst, or other tactical network users that are also connected to the operations centre. The third deployment pattern applies to information sharing directly at the tactical edge – for example from one soldier to another or from a sensor network to a soldier. Unlike the first two cases, these peer-to-peer exchanges occur on an ad hoc basis based on potentially opportunistic contacts between the edge users.

More discussion on the QoS framework can be found in Annex I: “QoS Framework”.

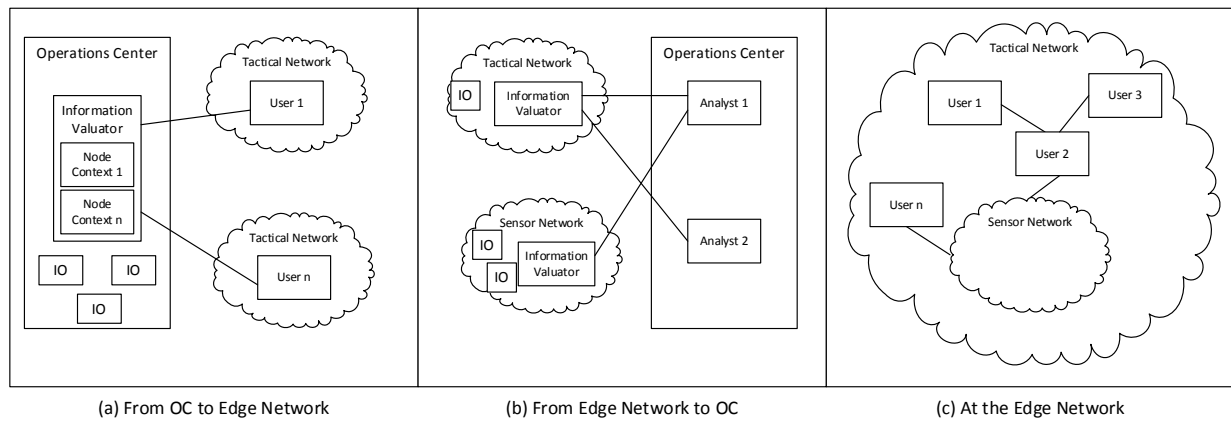


Figure 15: Deployment Patterns for Vol-Based Dissemination.

6.2 Standardization of QoS

Civilian QoS standardization by ITU, ETSI, and IETF for IP networks shares common elements. For example, ITU-T Recommendation Y.1221 defines three IP transfer capabilities:

- Dedicated Bandwidth (DBW) IP transfers capability allowing specified packet loss and delay commitments.
- Statistical Bandwidth (SBW) IP transfers capability allowing packet loss commitments.
- Best-Effort (BE) IP transfer capability providing no QoS commitments of any kind.

Military QoS standardization is based on work done in TACOMS and N&S CaT (Network and Security Capability Team) working groups. As a result, there are STANAG 4711 (IP QoS) and STANAG 4731 Ed2 “Networking Framework for All-IP Transport Services” (NETIP) that are under ratification.

Military standards provide framework for military communication and has more detailed description of quality targets considering tolerance of applications to loss, delay and jitter.

Discussion on QoS standards can be found in Annex J: “QoS Standards”.

7.0 ACHIEVEMENTS AND RECOMMENDATIONS

7.1 Routing, Security, Quality of Service and Resource Management

The objective of IST-124’s work was to provide architecture and design guidance for tactical heterogeneous networks at the mobile tactical edge in order to support coalition interoperability and get more reliable and predictable network performance.

IST-124 has through analysis, simulation, emulation and expert opinions gained a better understanding of how to build interoperable heterogeneous networks at the tactical edge. A main contribution is a toolbox of design choices and recommendations proposed to help the network planner to orchestrate a good design for a given operation.

The toolbox includes considerations and suggestions in the following areas:

- Connectivity, routing and security; and
- Quality of service and resource management.

For “connectivity, routing and security” we conclude:

- The future will bring a tactical edge battlefield that includes many different networks from different nations. In order to provide network connectivity to the coalition as well as improving the robustness of the network service, it is essential to extend the ideas of federated networks to the tactical edge.
- A central observation is that there is no one-size-fits-all solution for the best routing architecture for the target network (heterogeneous mobile networks at the tactical edge). The network planner should be given several designs to choose between in order to select the best for the operation in question.
- We have identified several necessary Information Exchange Interfaces (IEI) to enable heterogeneous coalition networking, IEI-R and IEI-RO to connect routing domains and IEI-M for information flow between the router and a modem (see Annex E). We recommend that these interfaces are standardized as soon as possible to allow nations to require the presence of these interfaces in new procurements of network equipment.
- We have described the advantages and disadvantages and important trade-offs for three different routing architectures that we believe should be part of the future toolbox for the network planner. The routing design should be chosen in order to support the desired network policy for the operation (see Annex E).
 - We recommend aiming for a first target network design that has a hybrid routing architecture in which an interconnect-overlay protocol connects smaller network segments that use the flat architecture as well as some network segments that use an embedded routing protocol that is tailored for the transmission technology.
 - There is a need for a certain density of interconnection platforms in order to get connectivity across different transmission technologies, no matter which routing architecture that is chosen. The network planner must plan with enough interconnection platforms in order to achieve the necessary connectivity and robustness. Annex F gives an estimation of the necessary density in a typical mobile scenario. More experiments are needed.
 - Scalability of the routing mechanism is a major concern. In IST-124 it was a requirement to study solutions that could also include low data rate transmission technologies as part of the heterogeneous network. We observe that it is much more difficult to support a scalable and stable heterogeneous network when the different transmission technologies that make up the network have very different characteristics (e.g., data-rate, range, delay, etc.).
 - Standard MANET routing protocols such as OSPF with MANET extension and OLSR are not designed for large heterogeneous networks with high mobility. In (see Annex G) we conclude that OSPF is not feasible to use in a mobile scenario with over 100 nodes. The same holds for OLSR as shown in Ref. [10].
- We expect the network planning to become more and more automated (eventually using Artificial Intelligence (AI)), thus it is important to provide different solutions that are well characterized in order to support machine decisions.
- A set of different security architectures that might be present in the target network has been identified. Our evaluation shows how the various security concepts have different implications for the routing architectures. Not all routing architectures are compatible with all security architectures. When security is enforced at the network layer by the radio or between the router and radio, all routing architectures will have reduced performance or there might be security violations (see the Security Architecture report [11] and Annex E).
- We have done some experiments to study the performance of the different routing architectures (see Refs. [10], [20], Annex G and Annex H). We conclude that this is a complex research topic and

we need more experiments in order to better understand the performance of the different architectures for different scenarios.

- IST-124's focus has been on unicast solutions for communication sessions between two users or systems. Solutions for efficient group communications in heterogeneous mobile tactical networks should also be studied closer.

For the Quality of Service (QoS) and Resource Management (RM) we conclude:

- All IP traffic must be marked with proper DSCP values per service class and precedence. Use of standard marking, e.g., STANAG 4711 is recommended. DSCP values can be used to disallow traffic on some links or topologies if multi-topology routing is used.
- Admission control is necessary at network edges and within the network. Each service class should have its own allowed capacity.
- A QoS requirement (like delay or reliability) shall be managed only by one network layer. Choose the layer that can best implement the requirement in the mission's network. This reduces the risk for no-cooperating mechanism at different layers that might degrade the performance rather than improve the performance.
- Control loops on different layer should work on different time scales. Synchronization effects across layers can lead to unpredictable performance.
- Three states of network health (normal, reduced, last effort) are to be considered in the network design. Network device must be able to alter their configuration to match the current state autonomously by observing the network, via network control, or by the operator.
- The information that best serves the mission's objectives, should be available where it is needed and in time. For this to happen, the network must establish a notion of the QoI and VoI and convey this information to the QoS and RM mechanisms.
- Core network or LAN traffic may need to be adapted into a more suitable form for narrowband channels. Middleboxes and gateways may be used for this purpose. With the latter solutions, implications for the security architecture must be taken into account.
- Routers must be aware of link statuses. Regarding QoS, it is important to know what the actual available capacity of a link is, and what the occupation levels of data packet queues are.
- Even if one part of the network does not need or is not able to enforce QoS treatment, it must preserve the QoS information associated with the traffic including classification, priority, and precedence. This applies to transit networks.
- Situation-aware, automatic network configuration should be implemented. This calls for more intelligent node and radio configuration. Cognitive, Software Defined Networking and Radio (SDN, SDR) may provide tools to implement this in an interoperable manner.
- Recognize that much of the existing RM and QoS mechanisms are meant for point-to-point links. More research is needed for networks with shared radio channels.

7.2 Emulation Environment and Scenario

A by-product of IST-124's research was a quite realistic test environment using network emulation. Early on we identified a need for a common test environment where different methods could be combined or compared. The group was fortunate to have the necessary expertise to build a virtualized emulated network environment. And we had a partner with the necessary resources that was willing to host the emulated testbed for the group. Therefore, we decided to put quite some effort into building an emulation environment

that the group could use for common experiments. This effort came at the cost of reduced time spent on the two main activities of the group. The scenario that the group identified has been emulated in the testbed. Scripts and tools necessary to build the testbed are deliverables from the group and are publicly available. The scenario and the emulation environment are described in Annex A – Annex D.

For the effort to design and build an emulated network environment we conclude:

- We have demonstrated the benefit of having a cloud based shared emulated network platform for doing joint experiments.
- When a common testbed environment is used to perform different tests, the data from tests of different mechanisms implemented by different partners can be compared with credible results as opposed to comparison of results from different simulators and local testbeds [4].
- A common testbed environment allows different mechanisms to be put together to a complete solution. This is also difficult to do in simulation environment since it requires that all mechanisms are implemented for the same simulator.
- Emulation of a realistic scenario improves test results. In IST-124 we put much effort into realizing a realistic model of the network dynamics. Radio parameters are representing typical systems and the physical layer is adequately modelled.
 - In the second vignette of the scenario all of the nodes are moving, and the dynamics in terms of topology changes per second is high. The emulations are based on a realistic model of the radio propagation in the given terrain.
 - There are currently a limited number of radio models openly available for the emulation environment. Particularly for low data rate transmission technologies (i.e., Narrow Band Waveforms), it would be good to have a better model. This can be easily plugged into the environment as soon as it is ready.
- The emulation testbed can be used in early stages of research, with mechanisms on a lower TRL than what is usually needed for field tests, but still using the software code that can eventually be used in the field, removing the need for implementing a specific simulation model. This motivates researchers to move from simulation to emulation at early stages of research. This can shorten the time from the start of the research until the solution is ready for interoperability testing and standardization (e.g., STANAG, FMN, experiments at CWIX).
- Reuse of a common emulation environment among different NATO (and other) research groups (different IST groups, across STO panels, etc.) can improve cooperation and sharing/reuse of results from different groups.
- A common emulation testbed provided as a cloud service can give many of the same research benefits as common field tests, but to a much lower cost. Decision makers can see the results from tests on the emulation environment and can see the operational capacity of the system without fielding the system.

The emulation environment will be used and further improved in the new IST-161 “Efficient Group and Information Centric Communications in Mobile Military Heterogeneous Networks”.

7.3 Summary

The group had participants from industry, academia and military research institutes. It was very good mix of experts with different backgrounds from 10 different nations. We have had high focus on sharing of knowledge and experience between the experts of the group and have established a common understanding of the problem area and possible solutions to the identified challenges. This is important to pave the way for future standardization of solutions.

Other contributions are 5 peer-reviewed publications, a security architecture report, the final report including 10 annexes, one demonstration and one experiment at CWIX. We've also arranged 2 panel debates at conferences. The panel debates arranged at MILCOM'16 and MILCOM'17 attracted a large audience and was a good experience in order to both present ongoing work from the group and receive suggestions and comments from a large research community.

Our effort to better understand the challenges involved when establishing mobile heterogeneous coalition networks at the tactical edge and identification of necessary information exchange interfaces, will help NATO nations to evolve/procure network equipment that can be interoperable. A well-connected, resource efficient network improves Training, Materiel and Interoperability during operations.

8.0 ACTIVITIES

Regular group meetings and WebEx meetings have been IST-124's main meeting arena, but we have also been present at conferences to present papers, in panel debates and for a demonstration and an experiment. We've also had some information exchange with other STO groups.

8.1 Activities at Conferences/Journals

8.1.1 Publications

Suri, N., Nilsson, J., Hansson, A., Sterner, U., Marcus, K., Mısırhoğlu, L., Hauge, M., Peuhkuri M., M., Buchin, B., in't Velt, R., and Breedy, M., "The Angloval Tactical Military Scenario and Experimentation Environment". Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, Poland 2018.

Marcus, K., Nilsson, J., in't Velt, R., Suri, N., Hansson, A., Sterner, U., Hauge, M., Lee, K., Barz, C., Kirchhoff, J., Rogge, H., Holtzer, A., Buchin, B., Peuhkuri, M., and Misirlioglu, L., "Evaluation of the Scalability of OLSRv2 in an Emulated Realistic Military Scenario". Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, May 2017.

Suri, N., Hansson, A., Nilsson, J., Lubkowski, P., Marcus, K., Hauge, M., Lee, K., Buchin, B., Misirlioglu, L., Peuhkuri, M., "A Realistic Military Scenario and Emulation Environment for Experimenting with Tactical Communications and Heterogeneous Networks". Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium, May 2016.

Lubkowski, P., Hauge, M., Landmark, L., Barz, C., Sevenich, P., "On Improving Connectivity and Network Efficiency in a Heterogeneous Military Environment". Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS), Cracow, Poland, May 2015.

Hauge, M., Landmark, L., Lubkowski, P., Amanowicz, M., "Selected Issues of QoS Provision in Heterogenous Military Networks". International Journal of Electronics and Telecommunications, Vol. 60, No. 1, pp. 7-13, 2014.

8.1.2 Panel Debates

We arranged two technical panel debates at MILCOM.

Panel Debate:

"Challenges and Approaches to Improving Connectivity and Network Efficiency for Heterogeneous Tactical Networks" at MILCOM 2017.

Panel Moderator:

Dr. Niranjani Suri, Associate for Research – Information Sciences Division U.S. Army Research Laboratory (ARL).

Panel Participants:

Dr. Anne Marie Hegland, Principal Engineer, Kongsberg Defence and Aerospace (KDA).

Dr. Mariann Hauge, Principal Scientist, Norwegian Defence Research Establishment (FFI).

Dr. Stephen M. Russell, Chief – Battlefield Information Processing Branch, US Army Research Laboratory (ARL).

Dr. Aaron E Cohen, Senior Electronic Engineer, US Naval Research Laboratory (NRL).

This debate attracted a large audience of more than 70 people. We received many interesting questions and suggestions.

Panel Debate:

“Challenges and Approaches to Improving Connectivity and Network Efficiency for Heterogeneous Tactical Networks” at MILCOM 2016.

Panel Moderator:

Dr. Niranjani Suri, Associate for Research – Information Sciences Division U.S. Army Research Laboratory (ARL).

Panel Participants:

Dr. Jan Nilsson, Deputy Research Director, Swedish Defence Research Agency (FOI).

Dr. Stephan Lopic, Chief Scientist, Networks, Space and Naval Warfare Systems Center, U.S. Navy.

Dr. Andreas Boyd Buchin, Development Principal Predevelopment, Rohde & Schwarz.

Dr. Mariann Hauge, Principal Scientist, Norwegian Defence Research Establishment (FFI).

Mr. Ron Tobin, Electronics Engineer, U.S. Army Research Laboratory (ARL).

This debate was a good experience for the group; we got many interesting questions and suggestions. Due to much interest from the audience, the debate lasted for longer than the scheduled 90 minutes.

8.1.3 Demonstrations and Experiments

IST-124 has spent much time implementing a military scenario in an emulation testbed. Early stages of this virtual testbed were demonstrated by the group at ICMCIS 2016. The demonstration received much positive attention.

At Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) 2017 an implementation of some of the group’s work regarding routing architectures for heterogeneous mobile networks (Annex E) was tested. The experiment was performed in the COMMS focus area. The objective was “to test the coalition routing interoperability in a mobile tactical environment (tactical router)”.

8.2 Work Meetings

8.2.1 Physical Meetings

IST-124 has had regular work meetings 3 times each year. We've also streamed most of the meetings via WebEx to allow group members that could not travel to the meeting for financial reasons or due to meeting conflicts, to participate in all or parts of the meeting via Web. We've had US participants getting up at 2 o'clock in the morning to join the meetings, which is quite impressive. All the members of the group have taken turns offering to host the meetings and we have covered almost all countries and organizations. This has been a good experience, allowing the participants to show the group some of the activities or their organization via presentations and/or technical tours at the meetings and it has been valuable for the group to learn more about the different organizations. We've had the following meetings:

- 1) Kick-off meeting 3rd to 5th of June 2014, hosted by FFI at Kjeller, Norway.
- 2) Group meeting 21st to 23rd of October 2014, hosted by MUT at Warsaw, Poland.
- 3) Group meeting 24th to 26th of February 2015, hosted by Aalto University at Espoo, Finland.
- 4) Group meeting 9th to 11th of June 2015, hosted by LCDR at Tallinn, Estonia.
- 5) Group meeting 3rd to 5th of November 2015, hosted by Fraunhofer, FKIE at Bonn, Germany.
- 6) Group meeting 8th to 10th of March 2016, hosted by Leonardo SpA at Genova, Italy.
- 7) Group meeting 31st of May to 2nd of June 2016, hosted by FOI at Kista, Sweden.
- 8) Group meeting the week after MILCOM 7th to 9th of November 2016, hosted by ARL at Adelphi, MD, USA.
- 9) Group meeting 14th to 16th of February 2017, hosted by TNO at The Hague, The Netherlands.
- 10) Group meeting the week before ICMCIS 10th to 12th of May 2017, hosted by Aalto University at Espoo, Finland.
- 11) The final group meeting the week after MILCOM at 30th of October to 2nd of November 2017, hosted by IHMC/ARL at Pensacola, FL, USA.

8.2.2 Web Meetings

IST-124 has also used Web meetings extensively since the start of the meeting. We've had 2 – 3 Midterm WebEx meetings between the physical meetings for the first 2 and a half year of the group period. For the last year we've had weekly WebEx meetings. In addition, as mentioned above, we've also streamed most of our physical meetings via WebEx. Web meetings has worked very well for us, it has been a great tool to coordinate experiments on the emulation testbed as well as for other specific discussions.

8.3 Liaison with Other Activities

We've also had some liaison with other STO activities. We've given presentations of our activities to other groups:

- Presentation of IST-124 to the SET-218 RTG "Interoperability and Networking of Disparate Sensors and Platforms for ISR Applications" by King LEE, U.S. Army Research Laboratory (ARL)(former), USA.
- Presentation of IST-124 to the SAS-104 RTG "C2 Agility: Next Steps" by King LEE, U.S. Army Research Laboratory (ARL)(former), USA.

We had joint discussion with SET-218 and SAS-104 at our Adelphi meeting to see if we could identify a joint activity. We concluded that it was too late for IST-124 to join in a common experiment with SET-218 or SAS-104, but these groups might use the emulation testbed environment that IST-124 has built.

We've also received information from other groups at IST-124 meetings:

- Information from the SET-218 RTG “Interoperability and Networking of Disparate Sensors and Platforms for ISR Applications” by Michael MERTENS, Fraunhofer FKIE, DEU at our Bonn meeting.
- Information from the IST-142 RTG “Software Defined Network Architectures for the Federated Mission Networks” by Marko LUOMA, Alto university, FIN at our 2017 Espoo meeting.
- Daniela GHEZZI, Leonardo, ITA has kept the group updated on relevant ongoing activities in N&S CaT.

Members of IST-124 also participate in the RTG's IST-140 “Cognitive Radio Networks – Efficient Solutions for Routing, Topology Control, Data Transport, and Network Management” and IST-147 “Military Applications of Internet of Things”.

The experience and results from IST-124 are timely. There are now preparations to establish a new Syndicate for Mobile Tactical Networks in Spiral 4 of FMN. We gave a presentation at the spring 2018 TIDE Sprint to inform the FMN community of IST-124's work. The results of IST-124 are very relevant for the work of this syndicate.

9.0 REFERENCES

- [1] ACT, Federated Mission Networking (FMN) Portal. Available: [https://tide.act.nato.int/tidepedia/index.php/Federated_Mission_Networking_\(FMN\)_Portal](https://tide.act.nato.int/tidepedia/index.php/Federated_Mission_Networking_(FMN)_Portal).
- [2] Hallingstad, G. and Oudkerk, S., “Protected Core Networking: An Architectural Approach to Secure and Flexible Communications,” IEEE Communications Magazine, vol. 46, no. 11, pp. 35-41, 2008.
- [3] Łubkowski, P., Hauge, M., Landmark, L., Barz, C., and Sevenich, P., “On Improving Connectivity and Network Efficiency in a Heterogeneous Military Environment”. Proceedings ICMCIS, Cracow, Poland, pp. 1-9, 2015.
- [4] Kurkowski, S., Camp, T., and Colagrosso, M., MANET Simulation Studies: The Incredibles, in ACM SIGMOBILE Mobile Computing and Communications Review, vol. 9, no. 4, pp 50-61, 2005.
- [5] Suri, N., Hansson, A., Nilsson, J., Lubkowski, P., Marcus, K., Hauge, M., Lee, K., Buchin, B., Mısırhoğlu, L., and Peuhkuri, M., “A Realistic Military Scenario and Emulation Environment for Experimenting with Tactical Communications and Heterogeneous Networks”. Proceedings ICMCIS, Brussels, Belgium, pp. 1-8, 2016.
- [6] Suri, N., Nilsson, J., Hansson, A., Sterner, U., Marcus, K., Mısırhoğlu, L., Hauge, M., Peuhkuri, M., Buchin, B., in't Velt, R., and Breedy, M., “The Angloval Tactical Military Scenario and Experimentation Environment”. Proceedings ICMCIS, Warsaw, Poland 2018.
- [7] Extendable Mobile Ad-hoc Network Emulator (EMANE) – <https://www.nrl.navy.mil/itd/ncs/products/emane> (last visit: Jan. 5th 2018).
- [8] Adjacent Link EMANE – Distributed Wireless Network Emulation Framework – <https://github.com/adjacentlink/emane> (last visit: Jan. 5th 2018).
- [9] Marcus, K., Cannata, J., “Dynamically Allocated Virtual Clustering Management System”, Proc. SPIE 8742, Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR IV, 87420X (22 May 2013).

- [10] Marcus, K., Barz, C., Kirchhoff, J., Rogge, H., Nilsson, J., i. t. Velt, R., Suri, N., Hansson, A., Sterner, U., Hauge, M., Lee, K., Holtzer, A., Buchin, B., Peuhkuri, M., and Misirlioglu, L., “Evaluation of the Scalability of OLSRv2 in an Emulated Realistic Military Scenario”. Proceedings ICMCIS, Oulu, Finland (May 2017).
- [11] Hegland, A.M., Buchin, B., Holtzer, A., Hauge, M., and Peuhkuri, M., “NATO IST-124 Heterogeneous Networks, Security Architecture”, STO-TR-IST-124-Part-II, 2019, NATO UNCLASSIFIED.
- [12] Clausen, T., Dearlove, C., Jacquet, P., and Herberg, U., “The Optimized Link State Routing Protocol Version 2”, IETF, RFC7181. Apr. 2014. Available: <http://www.ietf.org>.
- [13] OLSRv2 implementation maintained by Fraunhofer FKIE – http://www.olsr.org/mediawiki/index.php/OONF_Plugins (last visit: Jan. 5th 2018).
- [14] Moy, J. (Ed.). “OSPF Version 2”, IETF, RFC2328. Apr. 1998. Available: <http://www.ietf.org>.
- [15] Baccelli, E., Jaquet, P., Nguyen, D., and Clausen, T., “OSPF Multipoint Relay (MPR) Extension for Ad Hoc Networks”, RFC5449, IETF, 2009. Available: <http://www.ietf.org>.
- [16] Ogier, R. and Spagnolo, P., “Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding”, RFC5614, IETF, Aug. 2009. Available: <http://www.ietf.org>.
- [17] Roy, A. and Chandra, M., “Extensions to OSPF to Support Mobile Ad Hoc Networking”, RFC5820, IETF, 2010. Available: <http://www.ietf.org>.
- [18] STANAG 4691 – Multi-Hop IP Networking with Legacy UHF Radios: Mobile Ad Hoc Relay Line of Sight Networking (MARLIN), Edition 2, June 2016, (NATO UNCLASSIFIED).
- [19] Sandlund, K., Pelletier, G., and Jonsson, L.-E., “The Robust Header Compression (ROHC) Framework”, IETF, RFC5795. March 2010. Available: <http://www.ietf.org>.
- [20] Landmark, L., Larsen, E., Hauge, M., and Kure, O., “Resilient Internetwork Routing Over Heterogeneous Mobile Military Networks”. Proceedings IEEE MILCOM, Tampa, FL, USA, pp. 388-394, Oct. 2015.
- [21] Braden, R., Clark, D., and Shenker, S., “Integrated Services in the Internet Architecture: An Overview”. IETF RFC 1633. 1994.
- [22] Kalevi, K. Differentiated services for the Internet. Macmillan Publishing Co., Inc., 1999.
- [23] Xiao, X., Technical, Commercial and Regulatory Challenges of QoS. The Morgan Kaufmann, 2008.



Annex A – OPERATIONAL PERSPECTIVE FOR IST-124

Piotr Łubkowski

Military University of Technology (MUT)
POLAND

Levent Mısırlıoğlu

MilSOFT Yazılım Teknolojileri A.Ş
TURKEY

Niranjan Suri and King Lee

U.S. Army Research Laboratory (ARL)
UNITED STATES

Jan Nilsson

Swedish Defence Research Agency (FOI)
SWEDEN

Mariann Hauge

Norwegian Defence Research Establishment (FFI)
NORWAY

Sami Peltotalo

Finnish Defence Research Agency (FDRA)
FINLAND

This annex provides the operational perspective and the scenario for the NATO STO Research Task Group (RTG) on “Heterogeneous Tactical Networks – Improving Connectivity and Network Efficiency” (IST-124-RTG-061). The scenario was also used as the basis for the experimentation activities of the RTG. It covers mission threads related to an attack with mechanized battalions against insurgent forces and is associated with the task of cordon and search of insurgents that threaten security of civilians and peace in the area of operation. The mission is supported by a naval task group that performs reconnaissance and surveillance requirements of the mission.

The mission-scenario was created to show the information needs and thus the challenges that appear when this information needs to flow in the heterogeneous network of the mission. The purpose of IST-124-RTG-061 is to improve connectivity and network efficiency in heterogeneous tactical networks, which are composed of a wide range of radio communications systems (HF, VHF, UHF and SATCOM), sensor networks, UAV systems, and deployed 4G or 5G cellular systems.

The operational perspective describes the task to be fulfilled, Command and Control (C2) system, collaboration among organizational units, information management, and example communications systems used for this purpose.

A.1 OPERATIONAL CONTEXT

The scenario depicts an operation conducted by the company task forces of a mechanized battalion and a naval task group off the shore of the operational zone. They are part of the Military Contingent (MC) coordinated by the Coalition HQ (CHQ). The coalition unit’s Communications and Information System (CIS) is equipped with modern CIS assets and is connected to National Operational WANs as well as the Coalition WAN (e.g., a Federated Mission Network (FMN)). The CHQ plays the reach-back role during the operation and provides Combat Support (CS) and Combat Service Support (CSS) as requested.

Analysis of the intelligence and reconnaissance information indicates that enemy forces are preparing a complex attack against the coalition base from the village located in the operational zone (Figure A-1). The enemy is well armoured and operates in an area that can be mined, so there is a chance of IED (Improvised Explosive Device) hazard. The enemy uses camouflage rules and cannot be distinguished from civilian village inhabitants in their behaviour, clothing, or activity. The enemy potential has been assessed to be approximately 20 people, including 2 people prepared for a suicide mission.

The task of the company forces is to move into the operational zone, neutralize the insurgents, and destroy the armaments they collect. It is very important to avoid civilian casualties and to prevent the insurgents from escaping.

The most important elements in this mission are communications and information system, logistics, and medical support, which are provided by the Coalition Forces.

The completion of the specified mission requires access to a wide range of systems and communication networks, i.e., radio communications systems (HF, VHF, UHF, SATCOM), sensor networks, and Unmanned Aerial Vehicle (UAV) systems. Elevated communications relays can be present at different altitudes and on platforms with varying endurance to improve connectivity in the mission network. Deployed 4G or 5G cellular systems can also be present in the field.

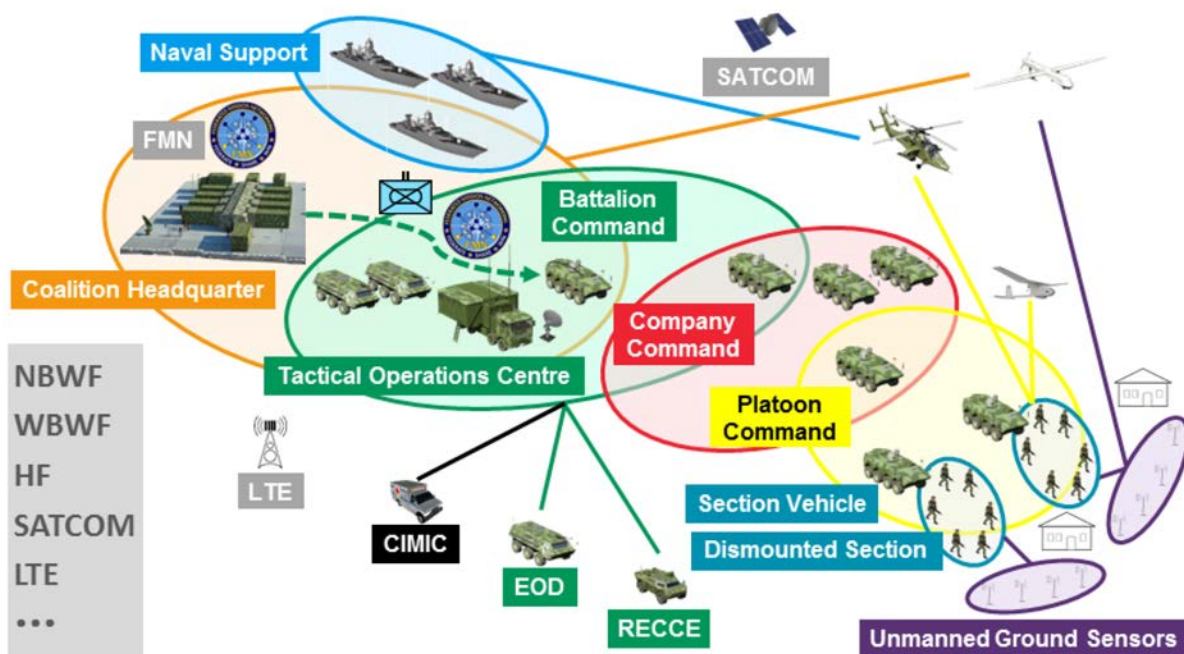


Figure A-1: Operational Scenario for RTG-061 (General Picture). A range of possible networks and transmission technologies that might be present in the operation is listed.

A.2 OPERATIONAL CONCEPTS

The scenario depicts an operation conducted by the company's task forces of a mechanized battalion and a naval task group off the shore of the operational zone (Figure A-2). It shows the tactical domain located in the fictitious area of Fieldmont in Anglova, where the Coalition HQ (CHQ) of the Military Contingent (MC) is based. As part of the scenario, units, systems, and several sensor networks are deployed to the town of Wellport (also in Anglova). The operational context of the three envisaged vignettes with some example communication means is highlighted in Figure A-2. The vignettes use the installed Communications and Information System (CIS) and suitable services in order to exchange information necessary for the realization of the mission tasks.

The mechanized battalion is a part of the MC, which plays the reach-back role during the operation and provides Combat Support (CS) and Combat Service Support (CSS) as requested. According to the operational context, it is assumed that insurgent forces have taken up positions in the town of Wellport and are preparing a complex attack against the coalition forces located in the operational zone. The most important elements in this

mission are CIS, logistics, and medical support, which are provided by Coalition Forces (CF). A functional and reliable communications infrastructure is essential to help organize the armed forces. The battalion CIS is connected to the National Operational WAN and has access to the Coalition WAN (FMN).



Figure A-2: High Level Operational View of the IST-124 Scenario.

The Naval component is present to support reconnaissance and surveillance activities, as well as provide Maritime interception and interdiction operations to control the flow of arms and goods into and out of Anglova. The individual ships have basic radar, AIS (Advanced Identification System), and ESM (Electronic Warfare Support Measure) systems connected to their C2 (Command and Control) systems. Each of the task groups performs operations within Line of Sight (LOS) of at least one other ship in order to utilize LOS connectivity with the group. But there are occasional inevitable positional displacements and, as the operational situation dictates, temporary detachment of small groups for missions like patrols, search and rescue, and reconnaissance missions. These situations require connectivity with the use of BLOS connections. Example communication means for the naval task force is shown in Figure A-3.

Three main vignettes are defined in order to implement the actions included in the scenario. The roles and actors are the same for each vignette. The first vignette covers intelligence preparation of the battlefield by deploying sensor networks and gathering surveillance information. The sensor network gateways have a Beyond Line Of Sight (BLOS) channel for notification of events but the bulk of the data from the sensor networks is exfiltrated via a UAV that harvests the data and provides it to CHQ.

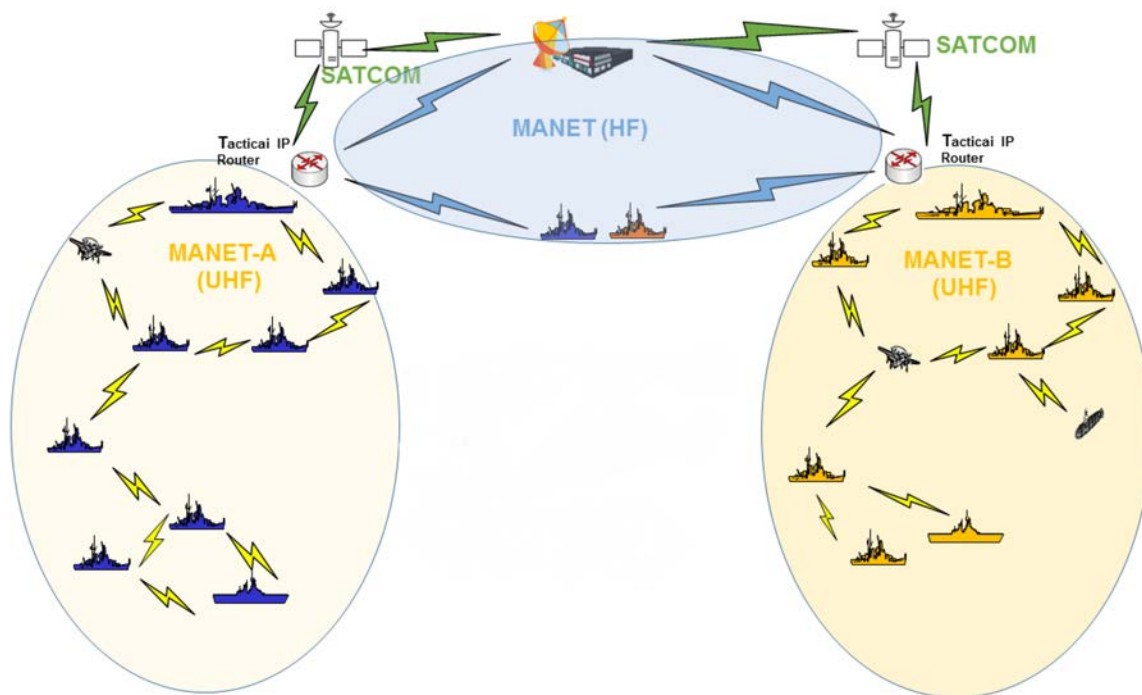


Figure A-3: Detailed Example View of the Coalition Naval Task Group and its Shore Based Commands.

The second vignette covers deployment of the coalition forces into the operational zone. The forces that are moving into the operational zone need local communications and connections with MC forces. It is assumed that as the forces move away from the CHQ, they need to change from local communications to some BLOS communication to reach the CHQ. Another option is to use an organic tactical UAV as a communications relay, or use deployed UAV's at higher altitudes, for the connection to the CHQ. These assets can also be used to improve communications within the deploying force. The naval component arrives and performs surveillance and reconnaissance of the Anglova port and see.

Finally, the third vignette describes neutralization of insurgents and IEDs and medical evacuation of wounded soldiers. This vignette includes an attack of the enemy positions as well as the use of Medical Evacuation (MEDEVAC) helicopter. There is also suspicion of explosives being detonated by the enemy, which requires the support of an EOD (Explosive Ordnance Disposal) team to minimize casualties and damage. The Naval component, which is deployed near the area of operations, supports the MEDEVAC tasks of the mission. Communications with the Navy can be supported with BLOS as well as long range LOS communication. A strategic (high altitude) UAV asset provides an intermittent communications relay as well.

Each vignette describes data that are expected to be exchanged between the actors and C4ISR equipment and emphasizes the challenges of connectivity and network efficiency of heterogeneous military networks.

A.2.1 Vignette 1: Intelligence Preparation of the Battlefield

Given the threat of IEDs, persistent surveillance is deployed fourteen days prior to the operation, where the ingress and egress routes to the operational zone are monitored. This surveillance is achieved by a combination of an Aerostat with long range sensors as well as Unattended Ground Sensors (UGS) being emplaced along the routes. The Aerostat is tethered to a ground station (which is in friendly territory near Fieldmont) and equipped with visual and IR (Infrared) camera sensors. The Unattended Ground Sensors

consist of a variety of tripwire sensors, seismic sensors, and UTAMS (Unattended Transient Acoustic MASINT sensors). The deployed sensors interconnect via a sensor network. The sensor network has two gateways nodes, one of which connects to the Aerostat while the other to the BLOS connection as well as to the tactical UAV (when it is put into operation). Data gathered by these sensors is archived locally, with notifications being generated and transmitted on demand to the Coalition HQ, Tactical Operations Centre (TOC) HQ, as well as dismounted sections.

Three days prior to operation execution, the sensor network is queried for any anomalies that have been detected. The query results indicate that some anomalous behaviour may have been captured and archived by the sensors, and it is determined that the data should be harvested for further analysis.

Two days prior to operation execution, a Harvest UAV is deployed by CHQ to harvest and send data that has been gathered by the Aerostat and the UGS sensors. This data is then delivered to Intelligence Analysts at CHQ to prepare for the upcoming operation.

A.2.2 Vignette 2: Deployment of Coalition Forces and Surveillance

A.2.2.1 Deployment of the Battalion

The example battalion consists of six companies: four tank companies each with 24 vehicles, one command and artillery company with 22 vehicles, and one support and supply company with 39 vehicles. Altogether, there are 157 vehicles, with each one being a network node. The task for the battalion is to stage an attack against a hostile force that is advancing into the area of the battalion. The area selected for the troop deployment consists of hilly terrain covered by forests. The deployment is characterized by movements mainly on large and small roads over a rather large area, a 13 km by 29 km rectangle. The battalion starts out by moving in a single column on one main road from the CHQ. After about 10 km, the battalion splits up over two main roads and after about 25 km splits up further onto many roads grouped in companies. Towards the end, the battalion finally splits up to the level of platoons (Figure A-4). Altogether, the battalion deploys for two hours.

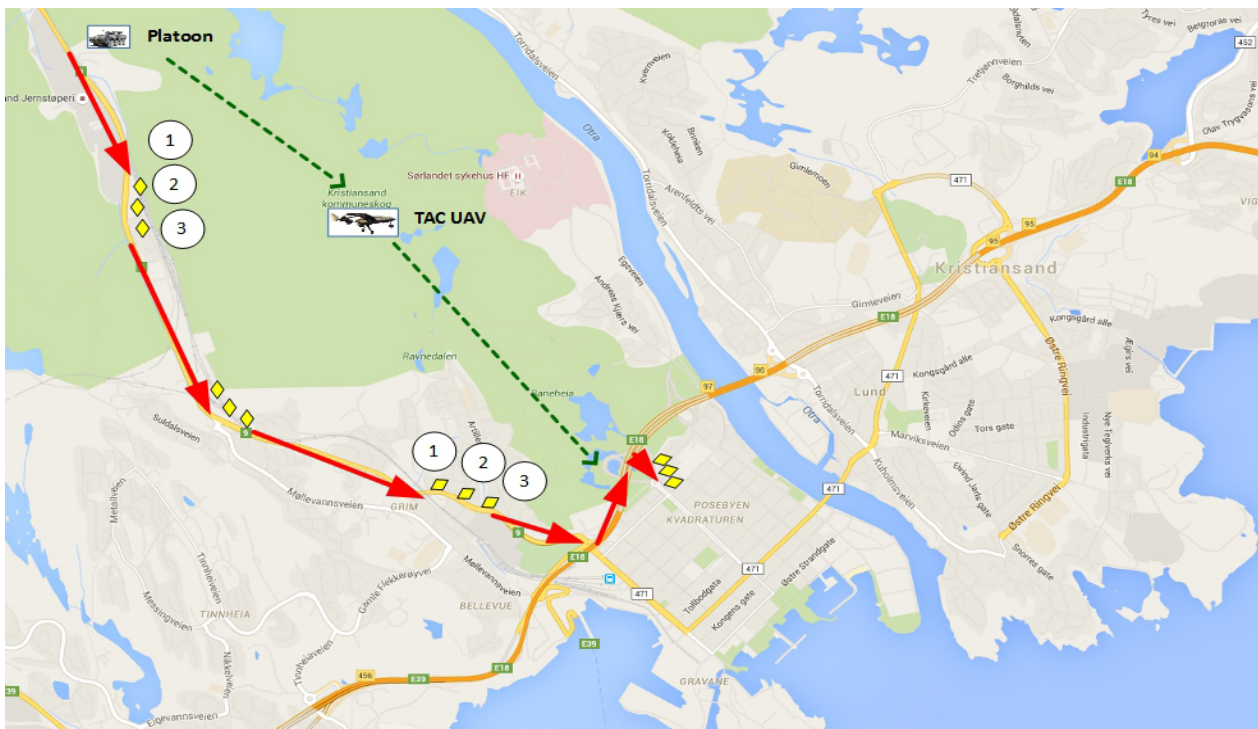


Figure A-4: The Final Part of the Battalion Deployment into Operational Zone.

Deployment of the mechanized battalion is achieved with the simultaneous transfer of voice and data shared between all participants of communication, BFT and intelligence from sensors in Wellport, as well as data gathered by UAV.

A.2.2.2 Maritime Deployment and Surveillance

The Task Group sailed away under the command of OTC (Officer in Tactical Command) from the shore to conduct a Surveillance and Reconnaissance mission. This operation lasts for the duration of both Vignette 2 and Vignette 3. A LOS network among each unit in the Task Group and a BLOS network with the capable units are automatically established.

A blue picture is formed automatically since the unit reports their position frequently through the network. Units exchange their tracks and inform the Navy HQ with summary reports. Units also use text chat / free text messages for coordination purposes. The following activities are carried out by the maritime component during the operation:

- Units in the force detect targets with its primary radar. With the help of AIS and ESM information, the targets are classified, and contact information is reported to the other units.
- One eastbound unit locates a group of targets far away from the friendly task group, moving together as a convoy with suspicious appearance, course, speed, and AIS information. The observation is reported to the OTC. The contacts are initially reported with suspect vessel identity.
- OTC orders a small task group consisting of one command ship with helicopter capability and four fast patrol boats to form a MIF (Maritime Interdiction Force) group to investigate and if required, board and search targets.
- The commander on the departing command ship, now called On Scene Commander (OSC), departs eastwards with his MIF group from the rest of the task force to investigate, while keeping in contact with the OTC and the remaining ships through the BLOS network.
- The OTC also tasks the MEDEVAC helicopter to take off from one of the westbound ships and sail to the MIF Command Ship to be prepared for any emergency call from the land forces and improve communication connectivity between the two separate groups.
- The task group arrives near suspect targets and positively identifies the tracks as Contact Of Interest (COI) tracks and reports this message to headquarters, OTC, and the rest of the fleet with a priority message. The OSC also takes a photograph of the convoy using a daylight camera and e-mails this photo to the OTC in order to give a positive indication to their identification. The e-mail goes through the network with a lower priority.
- The OTC/headquarters then takes necessary actions against the COI tracks and sends their orders with a guaranteed delivery to OSC. The Coalition HQ is informed of the incident and the result.
- The MEDEVAC helicopter lands on deck of the MIF Command ship, and the MIF group enters the harbour of Anglova, while the rest of the task group continues on the Surveillance Task.
- The MEDEVAC helicopter takes off again to answer an emergency call from the Land Forces and lands in the designated landing zone in Wellport.

A.2.3 Vignette 3: Insurgent Defeat, MEDEVAC, and EOD

The start of the operation is scheduled for one hour after Sunrise due to lack of helicopter crews that has training with the use of night vision goggles. The ground troops achieved their position at 5 AM. The route march was secured after a check by the local police and due to the IED hazard, the route was subsequently

monitored by the CHQ. Moreover, continuous intelligence and surveillance are ongoing with the Naval components, UGS sensors and tactical UAVs.

At 5 AM, two platoons cordoned the operation zone creating the fire system to contain the enemy in a few buildings. The third Platoon is ready to support the other two (but is in reserve). Possible support is foreseen in the case of strong resistance. The first Platoon of the Second Company is prepared for action.

The following activities take place as part of this vignette.

A.2.3.1 Neutralization of Insurgents

- Intelligence reports are provided to the platoon commander, which, based on information gathered from UGS sensors and Navy AIS and ESM, indicate an increase in enemy radio traffic. The insurgents have likely become aware of the coalition operation.
- Using RF triangulation between multiple UGS sensors, the base stations providing cell phone coverage to the area are identified. This information is reported to the TOC HQ. The base stations are temporarily disabled to prevent the insurgents from calling for reinforcements or notifying other insurgents about the operation.
- The local Police proceed to remove all residents from the buildings located next to Insurgents' positions and report their progress to the TOC HQ. The Insurgents are called upon to surrender to the Police. Two suicide bombers attempt to attack the blue troops but are neutralized by the sniper. At the same time a few insurgents try to capture a few kids and women as hostages. This action is blocked by the APC's gun fire. The enemies are forced to return to the occupied buildings.
- A tactical UAV is deployed to provide overhead video surveillance of the buildings occupied by the insurgents. The video feed from the UAV is downlinked to the operator on the ground, who monitors any movement around the buildings of interest. He reports the actual situation to dismounted soldiers.
- The UGS that were previously deployed are re-tasked to provide perimeter monitoring for force protection. They will notify the platoons about any detected movement through the ingress and egress routes (i.e., the sensor network must now directly communicate with dismounted troops).
- The rebels indicate that they will fight and are ready to die. The blue troops receive SAF and mortar fire. The company commander – to avoid losses – orders to keep the positions and respond with fire.
- The commander of the Navy support informs Coalition HQ using available radio equipment that the naval task group has prevented unwanted goods to be transferred to the enemy harbour.
- The company commander orders attack on enemy positions by the first Platoon. At the same time the second Platoon covers the first one, and blocks enemy on their positions. Both voice and data must be supported.
- The first Platoon starts the attack. The soldiers take two buildings and neutralize the enemy. Two soldiers are wounded – cat. A and B. The condition of the first one is serious. They must be evacuated. The Platoon Commander reports the situation to the TOC HQ. A MEDEVAC helicopter is needed.

A.2.3.2 Medical Evacuation

- The two wounded soldiers are instrumented with telemetry, which allows the MEDEVAC crew and the Navy hospital to monitor their condition in real-time. This allows the hospital to direct administration of emergency care to the soldier who is seriously wounded to stabilize his/her vital signs.

- The MEDEVAC helicopter is ready for operation.
- The Commanding Officer orders that a field helipad must be secured and prepared. The reserve Platoon is ordered to prepare the landing place and secure it as well as to establish communication directly with the helicopter. The CHQ Duty officer orders the helicopter crew to take off.
- The Navy hospital is informed about the wounded soldiers' condition. The wounded soldiers are evacuated.

A.2.3.3 IED Neutralization

The area surrounding the enemy's buildings is mined by anti-personnel and anti-tanks mines. There is a possibility of unmanned detonation of the mine field:

- The insurgents had constructed a bomb as part of their terror. It can be defused. The commanding officer asks for EOD (Explosive Ordnance Disposal) support to neutralize the mine field.
- The commander ordered to secure and mark the site.
- EOD (from 2 mechanized battalion) arrives. There is suspicion that one or more of the insurgents will try to detonate all enemy explosives to cause as much damage as possible. To prevent this, the EOD deploys wide-area RF jamming.
- The RF jamming interferes with blue force communications as well, causing them to switch to non-affected networks or Electronic Warfare (EW)-resistant transmission technologies.
- After reconnaissance the mine field is cleaned, at the same time the sniper neutralizes the insurgent who was trying to detonate all enemy explosives.
- The operation is completed.
- The detachment returns to the Base.

A.3 ACTORS AND ROLES

A.3.1 Equipment for the Operation

The vignettes describe activities related to three defined mission threads; thus the roles and actors are the same for each vignette.

Each battalion consists of six companies as it was mentioned in Section A.2.2.1. Each vehicle carries one or more radios primarily using VHF and UHF bands.

All endpoint devices are equipped with GPS.

Table A-1 lists examples of network equipment for the operational scenario key players.

It is assumed that the terminal is not a capacity bottleneck for any of the services that are needed in the mission.

Table A-1: Example Equipment of the Operational Scenario Key Players.
NB = Narrow Band, MB = Medium Band, WB = Wide Band.

Military Platform	Radio(s)
Section Command Vehicle	• Soldier radio (MB, WB) • Company radio (NB, MB, WB) • Sensor network gateway radio (WB)
Platoon Command Vehicle	• Soldier radio (MB, WB) • Company radio (NB, MB, WB) • Interoperable Coalition radio (NB, MB, WB)
Company Command Vehicle	• Soldier radio (MB, WB) • Company radio (NB, MB, WB) • Interoperable Coalition radio (NB, MB, WB) • Military BLOS radio (NB, MB, WB) • Cellular network
Tactical UAV	• Company radio (NB, MB, WB)
Tactical Operations Centre HQ	• Soldier radio (MB, WB) • Company radio (NB, MB, WB) • Interoperable Coalition radio (NB, MB, WB) • Sensor network gateway radio (WB) • Military BLOS radio (NB, MB, WB) • Civilian BLOS radio (NB, MB, WB) • Cellular network • Connection to deployed backbone (FMN)
Coalition HQ	• Company radio (NB, MB, WB) • Interoperable Coalition radio (NB, MB, WB) • Military BLOS radio (NB, MB, WB) • Civilian BLOS radio (NB, MB, WB) • Cellular network • Connection to deployed backbone (FMN)
EOD Command Vehicle	• Company radio (BN, MB) • Interoperable Coalition radio (NB, MB, WB) • BLOS radio (NB, MB, WB)

Military Platform	Radio(s)
RECCE Platoon Radio	- Company radio (BN, MB) - Interoperable Coalition radio (NB, MB, WB) - BLOS radio (NB, MB, WB)
MEDEVAC Helicopter	- Interoperable Coalition radio (NB, MB, WB) - Naval task group radio (NB, MB, WB)
Navy Ship	- Naval task group radio (NB, MB, WB) - BLOS Naval radio (NB, MB, WB)
Aerostat Platform	- Sensor network gateway radio (WB) - Military BLOS radio (WB)
Harvest UAV	Sensor network gateway radio (WB)
UGS	Sensor network gateway radio (WB)
Local Police / CIMIC	- Cellular network - Civilian BLOS radio (NB, MB, WB)

A.3.2 The Radio Characteristics

During the operation different communication terminals are used. Example characteristics of some of them are given in Table A-2, Table A-3, Table A-4, Table A-5, Table A-6, Table A-7, Table A-8 and Table A-9.

Table A-2: Basic Parameters of Vehicular and Man-Pack VHF Radios.

Bandwidth	25 kHz
Transmit Power	Max. 50 W (man-pack 5 W, 10 W with booster)
Type of Transmission	Half-duplex
Range	Up to 30 km
Data Transmission Speed	Up to 64 kbs in dedicated packet data network. Substantially less in combined voice and data modes.
Additional Equipment	GPS receiver

Table A-3: Basic Parameters of UHF Radios.

Bandwidth	1 MHz or 5 MHz
Transmit Power	Max. 50 W
Range	Up to 5 km
Data Transmission Speed	Up to several Mbs but typically several hundred kbs.
Additional Equipment	GPS receiver

Table A-4: Basic Parameters of SATCOM on the Move Terminal.

Satellite Orbit	Geostationary
Frequency Band	X-band or Ka-band
Transmit Power (EIRP)	Approx. 40 dBW
Transmit Delay	Star 500 ms, mesh 250 ms
Data Transmission Speed	Up to several Mbs when much of the capacity in the satellite is dedicated to this channel but typically a few tenths to several hundred kbs.

Table A-5: Basic Parameters of LEO Satellite Terminal.

Iridium Satellite Orbit	LEO
Orbit Altitude	780 km
Iridium Applications	Voice (2.4 kbps) and data (128 – 512 kbps)
Satellites in Constellation	66
User Satellite Link Band	1616 – 1626.5 MHz L band
Gateway -> Satellite Up-Link	29.1 – 29.3 GHz
Satellite -> Gateway Downlink	19.1 – 19.6 GHz
Inter-Satellite Link	22.55 – 23.55 GHz
Satellite Relative Velocity	26 804 km/hr
Access Scheme	FDMA / TDMA

Table A-6: Basic Parameters of HF Radios.

Bandwidth	3 kHz (or 8 bands combined to 24 kHz)
Transmit Power	Max. 400 W
Type of Transmission	Half-duplex
Range	Up to 400 km in ground wave propagation over the ocean, unlimited range (depending on the channel quality) in sky wave channel
Data Transmission Speed	75 bps (3 kHz) up 120 kbs (in ground wave on 24 kHz band)

Table A-7: Basic Parameters of Naval VUHF Radios.

Bandwidth	25 kHz, 12.5 kHz, 8.33 kHz
Operational Frequency Range	30 – 512 MHz

Maximum Transmit Power	100 W FM, 30 W AM
Transmission Mode	Fixed Frequency, Frequency Hopping (FH) (have Quick-I/II, SATURN)
Range	20 km
Data Transmission Speed	Up to 96000 bps
Type of Security	TRANSEC and COMSEC key
Additional Equipment	GPS receiver

Table A-8: Basic Parameters of Naval HF Radios.

Bandwidth	3 kHz (USB), 6 kHz (ISB)
Operational Frequency Range	2 – 30 MHz
Maximum Transmit Power	100 W, 400 W, 1 KW
Transmission Mode	SSB, ISB
Range	1000 km
Data Transmission Speed	Up to 9600 bps (can be as low as a few hundred bps, but typically 2.4 kbps)
Type of Security	COMSEC key
Additional Equipment	GPS receiver

Table A-9: Basic Parameters of Tactical LTE.

Bandwidth	1.4 MHz, 3 MHz, 5 MHz, 10 MHz, 20 MHz, (assumed 10 MHz)
Operational Frequency Range	450 MHz – 6 GHz (assumed 700 MHz)
Maximum Transmit Power	UL: 200 mW, DL: 2 x 10 W
Transmission Mode	DL: OFDM, UP: SC-FDMA
Range	For mobile base stations with assumed parameters (0.5 km – 10 km (LOS))
Data Transmission Speed	UL: 50 kbps – 20 Mbps, DL: 1 Mbps – 30 Mbps
Type of Security	COMSEC and NETSEC
Additional Equipment	GPS receiver both for base station and mobile node

A.3.3 Traffic Flow

Example traffic flows in different parts of the network are described below.

The communication between battalion units is handled as voice/data communications. According to these the following data properties should be reflected:

- VHF radio 2400 bps (throughput is shared among all members of the network).
- UHF radio 500 kbps (throughput is shared among all members of the network).
- All vehicles within the TOC HQ are connected via a common LAN and each vehicle will have a VHF radio.
- The satellite capability has a duplex capacity of 512 kbps, which is shared by all users due to the use of a hub located at TOC HQ with a delay of 250 ms.
- The interoperability radio on the company level can be either VHF, e.g., NATO Narrowband Waveform (NBWF), or satellite link (SATCOM on the move).

The units have access to an UAV in the UHF band and can steer UAV's sensors to suitable positions. Moreover, some units use UAV to transmit video from the area of operation.

The sensor network and different types of UAVs provide added situational awareness for the platoon. They are used to exchange the following types of information:

- **Sensor Network:** Network configuration commands, sensor event notifications, seismic signatures, acoustic signatures, low and medium resolution still images (triggered and on command).
- **Aerostat:** Control commands, on command high resolution visual and IR still images (dedicated communication channel to ground control unit), sensor data processing and relaying, communications relay.
- **Harvesting UAV:** Control commands, on command high resolution visual and IR full motion video images (dedicated communication channel to ground control unit), sensor data harvesting and relaying, communications relay.
- **Tactical UAV:** Control commands, on command medium resolution visual and IR full motion video images (dedicated communication channel to ground control unit), real-time sensor data relaying, communications relay.

Information available to units is given in form of data packets described by the following properties:

- **Size of Data Packet:**
 - **Sensor Event Notifications:** 512 bytes every 10~15 seconds max. per sensor (frequency of event trigger varies greatly but should be upper bounded to some number of seconds apart to avoid multiple notifications from the same event).
 - **Non-image Data:** 2 kB per event.
 - **Image Data:** QVGA (15 kB) to VGA (60 kB) images per event.
- **Data Stale Time:**
 - 30 seconds (event notifications).
 - 180 seconds (non-image data).
 - 180 seconds (image data).

The communication between elements of the Navy task group is handled as voice/data communications. The following data properties should be reflected:

- **Number of Tracks within the Surveillance Area:** 250.
- **Number of Tracks Per Network:** 50 (to be updated every 60 seconds).
- **Size of Track Data:** 18 bytes every 12 seconds, 27 bytes over each 96 seconds.

- **Size of Drop Track:** 9 bytes (expected roughly 5 drop tracks per minute).
- **Size of Free Text:** 250 characters long (10 messages per minute per network can be considered).
- **Track Stale Time:** 60 seconds.

On all networks, track with COI statuses and initial report of suspect vessels are first priority. Periodic reports of suspect vessels, blue force information and OTC/Fleet Commander orders are second priority.

COIs and initial report of suspect vessels and command orders along their acknowledgements are serviced with guaranteed delivery. Also, operators may specify the delivery method for e-mails while preparing them. The rest of the information is best effort.

Tactical track data for real-time tracks has a life span of 60 seconds.

A.3.4 Services Implementation – General Network Requirements

The list of proposed services is given Table A-10, with some general requirements.

Table A-10: List of Proposed Services.

Service	General Network Requirements, QoS target	Precedence / Conn. Type
Management of events and occurrences (e.g., the intelligence reports about increase of the enemy radio traffic).	• Med-low availability • Low-med throughput • Elastic	Routine – priority / CL
Planning and Decision Support Tools (e.g., the Navy support inform that prevent unwanted goods to be transferred to enemy forces).	• Med-low availability • Low-med throughput Elastic	Routine – priority / CL
Allocate resources and know their status at all times (e.g., the MEDEVAC helicopter, which is waiting next to the operation spot, due to technical problems is not ready to take off, amphibious crew is ready for taking wounded soldiers).	• High-availability • Med-high throughput (depending on the number of assets) Assured Elastic	Priority – immediate / CL
Up-to-date maps – ability to present information on a map over time (e.g., the first Platoon starts attack, the soldiers take two buildings and neutralize the enemy).	• High throughput Elastic	Routine – priority / CL

Service	General Network Requirements, QoS target	Precedence / Conn. Type
Bi-directional links between operational people: Voice communications (Radio).	- HF/UHF radio - Real-Time (1 – 2)	Routine – flash / CO
Bi-directional links between operational people: Short messages (Data).	- Low throughput - Near-real-time – Elastic	Routine – flash / CL
Bi-directional links between operational people: Reports (Data).	- Med throughput (non-real-time) [Assured] Elastic	Routine – priority / CL
Bi-directional links between operational people: Images and video (Data).	- High throughput - Near-real-time, Elastic	Routine – priority / CO+CL
Information sharing with local authorities / forces (e.g., local Police removed all local residents from the buildings located next to Insurgences positions).	- High throughput - Interface with public(local) networks - Real-time (2) – Elastic	Routine / CO+CL

Precedence indicates military precedence level applicable for the communication (routine, priority, immediate, flash). Connection type is either Connection Oriented (CO) or Connectionless (CL). For the first one, resources are allocated by call (or equivalent) and call admission control should be enforced. For connectionless traffic DiffServ type priority and rate enforcement are applied.

QoS target indicates the required quality that the application needs from the network in terms of delay, jitter, loss and Mean Opinion Score (MOS) for voice communications.

For the Navy task group, the following services should be taken into account:

- Blue force tracking picture;
- Local Tracks / (Contacts of merchant vessels, or aircrafts);
- Common Tactical Picture / Recognized Maritime Picture (with suspect vessels, Contacts of Interest (COIs);
- Text chat for coordination issues;
- E-mail and file transfer to exchange pictures, plans etc.; and
- Limited Web Browsing access to reach out command portals to view mainly text based OPGENs, OPTASKs, orders etc.

From that the following network requirements can be derived:

- Each OTC Task Group shall work on his/her own MANET preferably with UHF frequency in order to utilize UHF frequencies advantages.
- There shall be at least one HF MANET in order to perform data exchange amongst navy headquarter and OTCs. Also, individuals that has no connection otherwise may use this MANET to communicate.

ANNEX A – OPERATIONAL PERSPECTIVE FOR IST-124

- Since the topology changes frequently, a layer 2 routing/relay capability inside the MANETs is required.
- Tactical Information routing between HF and UHF MANETs and/or SATCOM requires a layer 3 Intelligent Tactical IP routing capability.
- These MANETs should be automatically organize themselves to adhere frequent topology changes.
- End-to-end IP connectivity shall be an effective way of communications even when the detachment group switch over HF MANET, still paths exists with the same addressing schema to send their information to their destinations independent of network or frequency band they are in.

Annex B – EMULATION-BASED EXPERIMENTATION AND THE ANGLOVA SCENARIO

**Niranjan Suri, Kelvin Marcus
and King Lee**
U.S. Army Research Laboratory (ARL)
UNITED STATES

**Jan Nilsson, Ulf Sterner
and Anders Hansson**
Swedish Defence Research Agency (FOI)
SWEDEN

Piotr Łubkowski
Military University of Technology (MUT)
POLAND

Mariann Hauge
Norwegian Defence Research Laboratory (FFI)
NORWAY

Boyd Buchin
Rohde & Schwarz
GERMANY

Levent Mısırlıoğlu
MilSOFT Yazılım Teknolojileri A.Ş.
TURKEY

Markus Peuhkuri
Aalto University
FINLAND

This annex provides an overview to emulation-based experimentation and an overview of the emulation of the Anglova Scenario, which is described in Annex A: “Operational perspective for IST-124”. The IST-24 group created the Anglova scenario to perform experimentation, evaluation, and comparison of alternative strategies for connectivity, routing, and QoS in heterogeneous networks. However, the group also identified the value in sharing this scenario with other members of the research community, both within NATO as well as the larger military and academic research community. Therefore, the scenario as well as associated tools to use the scenario are being released in the public domain. Annex C: “Experimentation environment and tools” contains detailed instructions on how to deploy and use the scenario, as well as descriptions of available tools to assist those using the scenario for experimentation.

We wish to highlight that the Anglova scenario as well as a number of accompanying tools to help those wishing to experiment with the scenario have been made available to the research community to use freely. The current distribution is located at several different web sites: <http://www.ihmc.us/nomads/scenarios/anglova>, <http://www.arl.army.mil/nsrl> as well as <https://anglova.net/>. These web sites will be kept updated with any new developments / enhancements related to the Anglova scenario. At the time of writing the IHMC site has most up-to-date information, but this will most likely change over time, thus we recommend the reader to search all sites for the most recent information.

This Annex is organized as follows:

- Section B.1 provides some background and motivations behind the development of the Anglova scenario as well as a discussion of different methods for experimentation with tactical networks;
- Section B.2 goes into further detail on the various elements that must come together for conducting experimentation in an emulation environment;
- Section B.3 presents an overview of the Anglova scenario;
- Section B.4 follows with a more detailed characterization of the mobility patterns in the scenario;
- Section B.5 discusses the radio models and provides an overview of the architecture of a communications node; and

- Section B.6 provides an in-depth analysis of the link dynamics within the scenario, which is an important baseline for conducting experiments using the scenario.

B.1 BACKGROUND

Experimentation and analysis are important steps in the overall research and development process for networks, middleware, and services for military networks. Such experiments need to be conducted using realistic communications hardware, topologies, and military operations to obtain valid results. Typical alternatives include simulation-based experiments, emulation-based experiments, laboratory evaluation with actual hardware, limited field experimentation, and finally live military exercises. Each of these alternatives provides respective advantages and disadvantages and have a role to play in the overall cycle from conceiving an algorithm to developing and deploying components on actual military hardware and systems.

Simulation-based experiments require the least investment in terms of hardware and are quite scalable because the system does not have to run in real time. Hence, a single computer node can simulate very large numbers of entities and accurately model their behavior (and in particular, their communications links). Simulations are also perfectly controlled environments, which makes it easy to repeat tests with the same (or controlled variations of) parameters, collect results, and perform analysis. The drawback, however, is that the components being analyzed must be integrated into the simulation framework. This typically requires that specific programming models be adopted, which are more often than not different from the way these components would be developed for actual use. Hence there is an added cost in designing and building potentially two implementations, one for the simulation environment and one for the actual environment. Moreover, there is the added challenge of ensuring that the parallel implementations do not introduce any differences that invalidate the results obtained by the simulations when deploying the actual components. This is particularly important during continued development and maintenance of the components. For these reasons, simulation-based experiments are ideally suited to the algorithm design phase.

Another challenge is that often the other layers (besides the layer being evaluated) tend to be simplified compared to reality, both due to implementation time/complexity and scalability reasons. Thus, there is a risk that important characteristics have been abstracted away from the simulation environment.

On the other hand, experimentation with actual hardware has its own challenges, mainly in terms of cost and scalability. When using actual hardware in a laboratory setting, the connectivity between radio components still has to be controlled at the RF level to recreate the conditions that the equipment would experience in an outdoor environment. Finally, field experimentation and live exercises provide the best form of validation, but with significantly added cost (especially in the case of live exercises) and are best reserved for final validation of components. The other challenge with field experimentation and live exercises is that they are not repeatable and do not allow control over all the parameters, which makes collecting results and drawing the correct conclusions very difficult.

For these reasons, experimentation with emulation environments provides a good compromise and stepping stone between simulations and using actual hardware. In a typical emulation-based experiment, the software components that are deployed in the experiment are ideally the same components that would be utilized on actual hardware and in the field. Therefore, there is no need to maintain multiple implementations. When changes need to be introduced, it is easier to evaluate them in an emulation environment with the actual software components prior to pushing those components out into the field.

Emulation-based experimentation does introduce its own set of challenges. Scalability could be an issue given that sufficient hardware is necessary to run the actual software components in desired numbers for the experiment to be valid and useful. The recent trends in virtualization have helped to reduce the hardware requirements. Another challenge is the fidelity of the emulation to the real environment. This is particularly a challenge for complex radio models whose behavior depends significantly on aspects such as interference,

terrain, multipath, and other RF propagation challenges. Emulation environments also have a validation and maintenance problem – the software that emulates actual radio hardware must be created, validated, and maintained as the actual radios evolve (or new radios are implemented). However, this does not have to be done as often as with simulation environments, which requires that all components be re-implemented.

Finally, both simulations and emulations require scenarios to drive the experimentation. These scenarios must detail the number and composition of nodes and their hierarchy, the nature and behavior of communications links that are available between these nodes, their mobility as the scenario progresses, and the requirements for communications and information exchange between these nodes.

This annex describes a joint effort by the NATO Science and Technology Organization’s IST-124 task group (RTG) on “Heterogeneous Tactical Networks – Improving Connectivity and Network Efficiency” to develop and distribute an emulation environment and scenario. While this effort was undertaken by the group in order to facilitate experimentation within the group, we also recognize the benefits of making such a scenario and environment available to others in the research and development community. Given the focus on heterogeneous networks by the IST-124 group, we have chosen to include elements of surveillance, reconnaissance, C2, and tactical mission execution. The scenario involves a land-based force and a naval task group. We have also included a variety of communications links and both tactical and strategic UAV assets and a transient helicopter. The scenario also includes elements of coalition operations with realistic organization and communications. Coalition operations will have their communication interoperability based on the Federated Mission Networking (FMN) concept [1]. In future FMN spirals, the mobile networks at the tactical edge will be included. In the Anglova scenario, we intended to model connection points to a deployed FMN network in the coalition headquarter node and the tactical operations center node, but these have not been completed as of this writing.

Note that the scenario and environment that have been developed, are primarily modeling the communications aspects of a military operation. We have not attempted to model human activity (friendly or enemy) except for modeling the movement of friendly nodes and high-level information exchange requirements between those nodes. Finally, we have not included any aspects of cyber operations.

B.2 ELEMENTS OF EMULATION-BASED EXPERIMENTATION

Many elements must be combined in order to setup and conduct experiments using an emulation-based approach. This section describes some of the important elements as well as some of the choices we have made for each of these elements. Where possible, we also identify some alternate choices for completeness.

B.2.1 Network Emulation Framework

The network emulation framework handles the actual emulation of the underlying network elements, which typically includes the Physical Layer (PHY – Layer 1), the Media Access Layer (MAC – Layer 2), and sometimes the Internetworking or Routing Layer (Layer 3).

The framework selected for the IST-124 experimentation was EMANE (Extendable Mobile Ad-hoc Network Emulator) [2]. EMANE was selected for multiple reasons – scalability and flexibility being the two primary technical reasons, and easy access and prior experience by some of the IST-124 group members being other deciding factors. EMANE is released as open source and is available for download on GitHub [3], making it very easy to be obtained and deployed. Annex C further describes the deployments that have been utilized by the IST-124 group, which include a distributed deployment over a managed clustering framework called DAVC (Dynamically Allocated Virtual Clustering) as well as a hybrid distributed/centralized deployment over VMware ESXi virtualization environment.

The architecture of EMANE is sufficiently flexible to support different PHY and MAC implementations. Some standard implementations are provided to make it simple to use. These include a generic RF (Radio

Frequency) propagation model that supports multiple antenna types, antenna gain configuration, transmit power, and bit error rates. An 802.11 model is also provided to emulate common Wi-Fi-style networks, along with a prototype implementation of a Time Division Multiple Access (TDMA) MAC. During the course of experimentation, multiple issues were encountered with the standard implementations provided with EMANE. These are further described in Section B.2.2.

EMANE is an emulator and not a simulator, which, as described earlier, has the primary advantage of being able to run actual, deployable code. It also has some disadvantages in terms of scalability, resource requirements, and execution time (i.e., it runs in real time, not faster or slower).

Within EMANE, each network interface that is part of the test environment is handled by an instance of a Network Emulation Module (or NEM), which is responsible for realizing the communications characteristics of that interface. Each NEM is assigned a unique ID within the deployment.

EMANE also supports multiple deployment models – using LXC (Linux Containers) within a single host, in a distributed manner, where components of EMANE are installed in VMs that execute the code to be evaluated, and in a hybrid manner, where the Network Emulation Modules can be consolidated into a fewer number of hosts (controllers). Therefore, if a deployment requires 24 nodes with one network interface each, the 24 NEMs associated with each of those interfaces could run inside 24 LXC containers, within 24 VMs on one physical node, or with the 24 VMs deployed on multiple physical nodes. Finally, one orthogonal variation is the use of an option called the “raw transport”, which allows actual physical hosts or Virtual Machines (VMs) to be used without EMANE running directly on the host or within the VM. The latter is sometimes preferred because it can be used to connect to network devices (e.g., access points, routers) and also because it does not require the installation of any third party (i.e., EMANE) code into the test systems / VMs. Combinations of the above deployment models are also possible.

Another important aspect of EMANE is that it typically only emulates Layers 1 and 2. Layer 3 (routing) is not handled directly by EMANE but would have to be handled by either VMs running routing software or by connecting to physical routers. EMANE can also operate without introducing any routing, which would typically be useful to emulate a one-hop broadcast domain (or one segment – such as a Wireless Local Area Network (LAN) or a Wireless Sensor Network (WSN)).

A related choice in terms of network emulators is CORE (Common Open Research Emulator) [4]. Note that CORE can work in conjunction with EMANE, by relying on EMANE for the PHY and MAC layer emulation. CORE provides a graphical tool that allows users to generate the configuration files that drive deployment of network topologies, including multiple network segments with routing between them. CORE was initially designed to use LXC for the individual nodes but has since evolved to incorporate multiple physical nodes as well as the ability to integrate physical network devices such as routers. CORE is able to deploy standard Linux routing daemons (e.g., quagga).

While primarily a network simulator, NS3 does offer some options for integrating it into an emulation environment [5]. The primary challenge here is to be able to synchronize the virtual clock utilized by NS3 with the physical clocks of the nodes in the emulated environment. Another challenge is exchanging traffic between the emulated nodes and the NS3 simulator components. Initial work on a Real-Time Scheduler and on using the PCAP library supports some deployment of NS3 for emulation or in mixed simulation/emulation environments [6]. OMNET++ [7] is another network simulator that also supports the same ability as NS3 to simulate the lower layers of a communication network in real time for connected nodes.

Another emulation environment is NETEM [8], which is a follow-on to NIST Net [9], one of the first ever network emulation environments. However, NETEM only provides basic control over parameters such as delay, packet loss, duplication, and re-ordering. It does not provide a framework for implementing sophisticated radio models.

Finally, for completeness, we also refer the reader to Emulab [10], which is more than a network emulation framework. Emulab provides distributed and remote access to emulation testbeds and is very popular among researchers. One disadvantage of Emulab is that it was designed to mostly support remote access to an experimentation facility (although it is available to be deployed locally). Another disadvantage is that Emulab primarily models commercial radios, such as 802.11.

B.2.2 Radio Models

EMANE is really a framework that allows different radio models to be incorporated into the EMANE environment. As mentioned before, EMANE comes with a few pre-defined radio models – in particular, the RFPipe and 802.11. The RFPipe model can either accept externally computed path loss metrics or compute them on the fly based on the antenna model, radio characteristics (frequency, transmit power, receiver sensitivity), and node positions. Note that when path loss calculations are done internally (and in real time) by EMANE, it does not take into account terrain effects (e.g., elevation). There is also an initial implementation of a TDMA radio model.

It is worth noting that there are proprietary implementations of various tactical radios, including fairly high-fidelity implementations of currently deployed radios by the US and other militaries. Should the experimenters have access to these high-fidelity models, they would be able to set up high fidelity experiments. However, our goal is to create an open, easy to share emulation environment. Therefore, for this first stage, we modeled all of the radios described in the scenario in this report using only the open source radio models that are easily available and included with the EMANE distribution. In particular, the RFPipe, 802.11, and TDMA models were used to emulate the HF, VHF, and UHF links needed for the scenario we have developed to date. Note that the EMANE configuration files for the radios are also included as part of the Anglova distribution and are further described in Annexes C and D: “IST-124 Experimentation Execution”. More detailed radio models for some radios such as the NATO Narrow Band Waveform [11] under development, might be included in future work.

However, we also encountered implementation issues with the current implementation of the radio models. For example, we tried to use the RFPipe model to emulate the UHF medium band network for intra-company communication within the Anglova scenario. While it is possible to limit the transmission rate of a radio using RFPipe, there is no implementation of a Media Access Control (MAC) protocol and consequently no modeling of collisions that might occur with overlapping transmissions. Therefore, EMANE will allow two transmitters within interference range of each other to transmit without detecting and processing collisions. It is also possible for multiple transmitters to simultaneously send data to one receiver and the receiver’s data rate will simply be the sum of all the data rates of the transmitters, which may far exceed a realistic behavior of a real radio. The primary reason for this behavior within EMANE is that the RFPipe model is typically used to emulate a point-to-point connection between two radio nodes, and not a multi-node network over a shared medium.

Another problem exhibited by the TDMA model is a strong dependence on a synchronized clock across all the EMANE instances that are part of the same TDMA network. While this would work if all the EMANE instances are deployed on a single node (e.g., using Linux LXC), it does not work with the distributed deployment scenario where EMANE nodes are running in VMs and/or servers on multiple physical systems. Even using the Network Time Protocol (NTP) to synchronize the clock across these nodes does not provide sufficient accuracy to use the TDMA model.

Finally, even the 802.11 model exhibited some limitations in its implementation of the MAC. While not as bad as RFPipe, the 802.11 implementation within EMANE still did not correctly handle collisions at the RF level. For example, consider one receiver (node A) and two senders, B and C, that are simultaneously transmitting to A, with all three nodes within RF range of each other. If both B and C are transmitting simultaneously to A, the resulting data rate should be slightly less than the maximum possible data rate,

assuming some inefficiency in the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. However, the observed behavior is a slight increment in the resulting data rate received at A, which is impossible in reality. Table B-1 shows the results of the overall network traffic received at node A, with the 802.11 radio configured with a maximum data rate of 2 Megabits per second (Mbps). As it can be clearly seen, the data rate creeps up as the number of transmitters increase (which is the opposite of what would be expected). Moreover, the data rate at node A exceeds 2 Mbps with three senders or more, which is impossible if the radio was limited to 2 Mbps.

Table B-1: Results of EMANE 802.11 MAC Implementation.

Number of Senders	Received Data Rate (Kbps)
1	1593
2	1970
3	2664
4	2555
5	3260

It is hoped that future implementations of radio models within EMANE will provide more realistic behavior than what is exhibited currently. There are ongoing efforts within the research community to develop radio models that provide better accuracy and fidelity, as well as to model other types of radios such as LTE. Furthermore, the Anglova scenario and experimentation environment will continue to evolve under the new NATO IST-161 Research Task Group on Efficient Group and Network Centric Communications in Mobile Military Heterogeneous Networks. The radio models that are emulated for the Anglova scenario are described in Section B.5.

B.2.3 Resources and Hosting/Management Tools

The next requirement for experimentation is to be able to deploy the emulation environment and radio models on hardware. For EMANE, VMs are typically used to run the components of the emulation framework as well as the components being subject to experimentation. Resources are also necessary for running any hosting and management tools. Virtualization helps to reduce the number of physical nodes that are necessary, especially with scenarios that involve large numbers of nodes like the one for IST-124. The degree of virtualization can vary quite a bit on the software that needs to be run on the nodes, which can be something very simple, such as routing or transport protocols, to full-fledged C2 tools and services. Resource allocation also depends on the capabilities of the servers (in terms of number of cores, number of CPUs, and RAM available). As a rule of thumb, we try to run one virtualized node per CPU core. EMANE also requires processing resources to handle the network emulation, which, in turn, depends on the complexity of the radio models and on the EMANE deployment model.

Management tools are an equally important concern as the size and complexity of the experiment and scenario grow. Management challenges include deploying and updating large numbers of VMs, starting and stopping the VMs and the experiment code, and isolating one experiment from another. To this end, the US Army Research Laboratory (ARL) has developed DAVC (Dynamically Allocated Virtual Clustering), a set of tools that simplify the lifecycle management of experiments. In IST-124 we have used DAVC to instantiate one or more copy of the emulated network for the Anglova scenario and have also deployed the scenario manually in virtual machines under VMware's ESXi virtualization environment. DAVC is further described in Annex C and Annex D.

B.2.4 Scenarios

The next element required for experimentation is one or more scenarios that can drive the emulation environment (in this case, EMANE). Driving EMANE consists of, at the very least, specifying the positions of each of the nodes as they move through time. Node positions may be updated at any desired rate, depending on the desired level of fidelity and the rate of movement of the nodes. For example, updates could be sent every second, once every five seconds, or once every ten seconds. There is no requirement that this interval be uniform, or that every node's position be updated every update cycle.

Position information for nodes is provided to EMANE through events, which are basically messages sent over a UDP multicast control channel to EMANE. The messages themselves are encoded using Google's Protocol Buffers [12], making it relatively simple to generate and send these messages. In addition to position events, other events that change antenna profiles and radio characteristics are also available. If path loss is computed externally to EMANE, this information can also be sent via EMANE events.

There are multiple ways to generate and send events to EMANE. Example C++ code to generate and send events is provided with the distribution, and we have also developed Java code to do the same. EMANE also provides a command-line tool called EEL (Emulation Event Log) that reads an input file and generates events.

When position data is already available for each node (as in the case of the Anglova scenario), it is simply a matter of playing back the scenario by sending the pre-recorded positions to EMANE. However, if such data is not available, it is also possible to programmatically generate movement behavior for entities such as ground vehicles that are moving over pre-defined routes and UAVs that follow various geometrical paths (e.g., circular as in Figure B-7 and vertical/horizontal scan). Another option is to generate routes for nodes using a set of JavaScript tools that allow a user to click on points in Google Maps to specify waypoints and times. This information is saved off into a route file and then played back by Java code, which interpolates the positions between the waypoints and generates EMANE position update events. Note that these JavaScript tools are available as part of the Anglova distribution.

B.2.5 Candidate Algorithms/Protocols/Software

The next element for experimentation is the set of algorithms, protocols, and/or software that is to be subject to evaluation. IST-124, for example, is using the scenario described in this Annex to experiment with different routing protocols to improve connectivity, Quality of Service (QoS) mechanisms that can work across different network types, data dissemination in sensor networks, and so on. Each of these protocols or middleware components also need drivers or test software to utilize them in a repeatable manner, so that multiple experiment runs will be consistent and the results comparable. The end objective is to duplicate the types of workloads that a live operation might generate, so that we can measure and compare performance of different algorithms, approaches, configurations, and components.

B.2.6 Network Load Generators

An operational network will have a variety of traffic that is generated by a variety of applications. Examples include position updates for friendly and enemy forces, sensor reports, full motion video, Voice over IP (VoIP) traffic, documents and reports, and so on. A controlled experiment that is measuring the performance of one aspect of the network is not likely to be running all of the abovementioned applications. Therefore, recreating the conditions of the operational environment often requires network load generators that recreate the traffic of applications, components, and systems that are not actually present in the scenario. One potential tool that can address this requirement is the ARL Traffic Generation Tool [13], an extension of MGEN (Multi-Generator) [14].

It is worth noting that there are two philosophies when it comes to experimentation. One approach is to have traffic on the network that resembles a realistic environment, and measure how well a protocol performs (for example, how long did a file transfer take given all the other traffic that was also on the network). The other approach is to run the test case in isolation and measure its performance (for example, how much overhead did a discovery protocol generate on the network, or how much bandwidth did dissemination protocol A use compared to dissemination protocol B). The former approach requires network load generators whereas the latter does not. It is also possible to include actual military applications to provide the traffic load in the network, but if these applications depend on user input then either SW must be available to mimic the user's behavior or users must be present (but this is neither scalable nor easy to replicate for repeated tests).

B.2.7 Metrics and Measurements

Arguably the most important part of any experimentation is defining the metrics and collecting the desired results. Some standard metrics are bandwidth utilized, protocol overhead, message loss, latency, jitter, and information availability. Many of these metrics relate to important concerns in military operations (for example, latency relates to staleness of information such as tracks and information availability maps to situation awareness) and can provide important operational feedback. Other protocols and components might have other specific metrics such as convergence time, stabilization time, update time, and reachability. The metrics should be defined ahead of time, as it determines the test software that will need to be written.

The only metric that could be measured somewhat automatically by the emulation testbed is the bandwidth utilized. Sometimes, this is actually non-trivial with EMANE, as the control traffic and EMANE messaging overhead needs to be factored out. One interesting issue is whether the measure includes all traffic generated by any node, or only traffic received by a node. For example, if a node is out of range, the test could choose the measurement to include its transmissions or not. Likewise, if there is packet loss, the measurement could include just the bits received or all the bits that were sent.

B.2.8 Visualization

The last element of an emulation-based experiment is visualization, which is useful for observation as well as demonstration purposes. Visualizations could show real-time (i.e., as the experiment is running) views of the positions and movement of nodes, connectivity between nodes, as well as any metrics being measured, such as bandwidth, latency, failures, etc. These visualizations could also be captured into full-motion video clips for future display or presentation. Finally, individual screen shots are useful to include within publications.

One visualization tool that is already integrated with EMANE is SDT/SDT3D (Scripted Display Tools) [15], built on top of the NASA WorldWind toolkit [16]. Mirage is another NASA WorldWind-based visualization tool that is described further in Annex C.

B.3 OVERVIEW OF THE ANGLOVA SCENARIO

Annex A provides a detailed description of the military operational perspective for the Anglova scenario. This section presents a brief overview followed by more details on the mobility and communication patterns within the Anglova scenario.

The scenario depicts an operation conducted by the company task forces of a mechanized battalion and a naval task group (Figure B-1). It shows the tactical domain located in the fictitious area of Fieldmont in Anglova, where the Coalition HQ (CHQ) of the Military Contingent (MC) is based. As part of the scenario, units, systems and several sensor networks are deployed to the town of Wellport (also in Anglova) and outside the port of Wellport. The operational context of the three envisaged vignettes is highlighted in Figure B-1. The vignettes use the installed Communications and Information System (CIS) and suitable services in order to

exchange information necessary for the realization of the mission tasks. The completion of the tasks requires access to a wide range of systems and communication networks, i.e., radio communications system (HF, VHF, UHF and SATCOM), sensor networks, and UAV systems. Elevated communications relays can be present at different altitudes and on platforms with different levels of endurance to improve connectivity in the mission network. Deployed 4G or 5G cellular systems can also be present in the field.



Figure B-1: High Level Operational View of the IST-124 Scenario.

The mechanized battalion is a part of the MC, which plays the reach-back role during the operation and provides Combat Support (CS) and Combat Service Support (CSS) as requested. According to the operational context, it is assumed that insurgent forces have taken up positions in the town of Wellport and are preparing a complex attack against the coalition forces located in the operational zone. The enemies are well armed and operate in an area that can be mined, so there is a chance of IED (Improvised Explosive Device) hazard. The task of the coalition forces is to move into the operational zone, neutralize the insurgents, and to destroy the armaments they have collected. It is very important to avoid civilian casualties and to reduce the probability of the insurgents escaping. The most important elements in this mission are CIS, logistics, and medical support, which are provided by Coalition Forces. A functional and reliable communications infrastructure is essential to help organize the armed forces. The battalion CIS is connected to the Coalition network (FMN).

The Naval Task Group is present to support reconnaissance and surveillance activities, as well as provide Maritime interception and interdiction operations to control the flow of arms and goods into and out of Anglova. The individual ships have basic radar, Automatic Identification System (AIS) and Electronic Support Measures (ESM) systems connected to their C2 systems. Each of the task groups perform operations within Line of Sight (LOS) of at least one other ship in order to utilize LOS connectivity with the group. But there are occasional inevitable positional displacements and, as the operational situation dictates, temporary detachment of small groups for missions like patrols, search and rescue, and reconnaissance missions. These situations require connectivity with the use of BLOS networks.

Three main vignettes are defined in order to implement the actions included in the scenario. The roles and actors are the same for each vignette. The first vignette covers intelligence preparation of the battlefield by deploying sensor networks and gathering surveillance information. The sensor network gateways have a SATCOM-based channel for notification of events but the bulk of the data from the sensor networks is exfiltrated via a UAV that harvests the data and provides it to CHQ (using a Disruption Tolerant Networking (DTN) style communication pattern). The sensor network is mostly static, except for the harvesting UAV. The naval component is also involved in this vignette, supporting the surveillance and reconnaissance efforts. While some details of this first vignette have been defined, it has not been fully developed as of the writing of this report and will likely be completed in the future. Instead, the IST-124 group primarily focused on Vignette 2 and 3, which have significantly more mobile nodes and hence present more interesting scenarios from a mobility and network dynamics perspective.

The second vignette covers deployment of the coalition forces into the operational zone. The forces that are moving into operational zone use VHF connections for their own interoperability and operability with MC forces. However, it is assumed that as the forces move away from the CHQ, they can lose this connection due to range and may require the use of a SATCOM link for communications to the CHQ. Another option is to use an organic tactical UAV as a communication link or use deployed UAV's at higher altitudes for the connection to the CHQ. These assets can also be used to improve the communication within the deploying force. The second vignette is the most developed of the three and consists of 157 mobile ground vehicles, the coalition headquarters node, a UAV (with three different configurations for its altitude), and 21 ships that are part of the naval contingent. This vignette runs for 130 minutes in total. Note that the second vignette is primarily set in a rural environment, with the ground movement primarily consisting of vehicles that make up the six companies within the mechanized battalion.

Finally, the third vignette describes neutralization of insurgents and IEDs and medical evacuation of wounded soldiers. This vignette includes an attack of the enemy positions as well the use of a Medevac helicopter. It is also assumed that there is suspicion of explosives being detonated by the enemy, which requires the support of an EOD (Explosive Ordnance Disposal) team to minimize casualties and damage. Also, the Naval Task Group, which is deployed near the area of operation, supports the medical evacuation tasks of the mission. Communications with the Navy uses HF and VHF links although a strategic (high altitude) UAV asset provides an intermittent communications relay as well. The third vignette is set in an urban environment and drills down to operations at the squad level.

Each vignette describes data that are expected to be exchanged between the actors and C4ISR equipment used in a way that emphasizes the challenges of connectivity and network efficiency of heterogeneous military networks. The data exchange requirements are outlined in Annex A.

B.4 MOBILITY PATTERNS IN THE SCENARIO

One of the significant contributions of the scenario is detailed mobility patterns of a complete battalion over the course of two hours, as it moves from the starting point towards the objective. This is the troop deployment vignette (Vignette 2) within the scenario and is particularly significant because the positions of

each vehicle (and consequently the movement over the course of time) has been developed by military experts in planning and performing real exercises.

The modeled battalion consists of six companies: four tank companies each with 24 vehicles, one command and artillery company with 22 vehicles, and one support and supply company with 39 vehicles. Altogether, there are 157 vehicles, with each one being a network node. The CHQ and an airborne node has also been added to this vignette – a strategic UAV asset that can act as a communications relay and provide persistent surveillance capabilities.

The mobility pattern of the battalion models action north of Wellport in Anglova. The task for the battalion during Vignette 2 is to deploy the forces close to the town of Wellport in order to setup for counter-insurgency operations within the town (Vignette 3). The area selected for the troop deployment vignette primarily consists of hilly terrain covered by forests. The mobility pattern is characterized by movements mainly on large and small roads over a rather large area, a 14 km by 33 km rectangle. The speed of the vehicles varies, with speeds up to 60 km/h on the main roads. The battalion starts out by moving in a single column on one main road from the CHQ. After about 10 km, the battalion splits up over two main roads and after about 25 km splits up further onto many roads grouped in companies. Towards the end, the battalion finally splits up to the level of platoons. Altogether, the original mobility pattern is roughly two hours long [17] and is shown in Figure B-2.

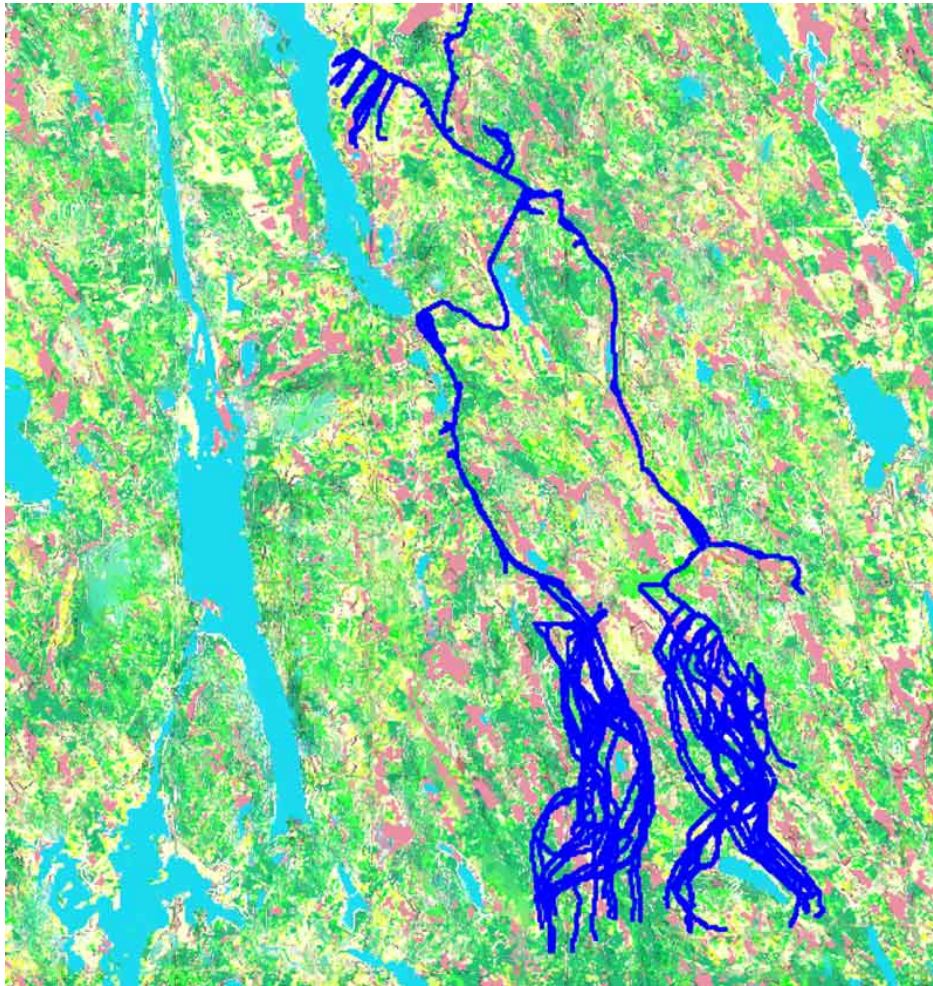


Figure B-2: Tracks in the Troop Deployment Vignette – Movement is from Top to Bottom.

To estimate the network performance, assumptions about the communication networks and the propagation environment are required. The basic path loss is calculated for an antenna height of 3 m for the moving vehicles. The antenna height at the CHQ is 20 meters. Furthermore, the pathloss was calculated for both a 50 MHz frequency and a 300 MHz frequency. This allows the experimenter to choose different radio characteristics for the vehicles as part of the configuration and setup of the experiment. For example, one possibility is to select the 300 MHz frequency for the vehicles within the same company (i.e., the intra-company network) and the 50 MHz frequency for communications between the companies and the Coalition HQ. Alternatively, the 50 MHz frequency could be selected for all the nodes.

The path loss values were also calculated between a UAV and the other 158 nodes in the scenario. Three configurations were chosen for the UAV altitude: 50 meters, 100 meters, and 500 meters. The calculations were also made for two frequencies: 50 MHz and 300 MHz.

Within each company, two vehicles are capable of acting as gateways, as they have two radios onboard each vehicle. Different frequencies could be chosen for each of these two radios. One could be part of the intra-company network and the other could be part of the inter-company (and UAV) network. All of these options provide many choices in terms of realizing a specific, desired configuration for the nodes within the emulation environment.

These path loss values are subsequently used in estimating achievable data rates. We use a Uniform Theory of Diffraction (UTD) propagation model by Holm [18] [19] to estimate the path loss between each node pair. We use a digitized terrain database, which adds significant realism to the communications model than a simple free space propagation model based on distance.

Finally, Vignette 3 provides the mobility models for the urban operation within the town of Wellport. Figure B-3 shows an overview of the mobility within the third vignette and is divided into three phases. The top part of the figure shows the ingress into the town of Wellport. The second part in the bottom left shows the mobility pattern leading up to the insurgents being neutralized. Finally, the third part in the bottom right shows the medevac activity, which is the last part of Vignette 3.

It is important to note that all of the detailed position data, along with the pairwise path loss data, updated every second over the two hour period, is included in the scenario. Mobility patterns and path loss for the Naval Task Group as well as UAV nodes and all actors in the third vignette has also been modeled.

The naval Task Group of the Anglova scenario is part of both Vignette 2 (troop deployment) and Vignette 3 (urban operation). One Task group is formed along the coast of Anglova. The Task Group is under the operational control of Fleet Commander / Maritime Interdiction Force (MIF) Commander located in Coalition Head Quarters. The task group consists of one command ship holding the flag officer and 20 other surface vessels. There is also one multipurpose helicopter, which provides MEDEVAC duties within the task group. Each of the task units perform operations within LOS of at least one other ship in order to utilize Line of Sight (LOS) connectivity with the group, so that they can take advantage of V/UHF frequency band for communications. However, in some situations, HF communications is utilized when LOS is not possible.

Pathloss generation for the naval platforms in Vignette 2 and for all platforms in Vignette 3 was accomplished by using the open source SPLAT! (Signal Propagation, Loss, And Terrain analysis tool) program [20] using Longley-Rice model. Topographical information was imported from the 3-arc second Shuttle Radar Topography Mission (SRTM) data, which is publicly available. These calculated pathloss values for the ships is also available as part of the Anglova distribution (see Annex H: “Naval Task Group and Routing Experiments” for more details about the modeling of the Naval Task Group).

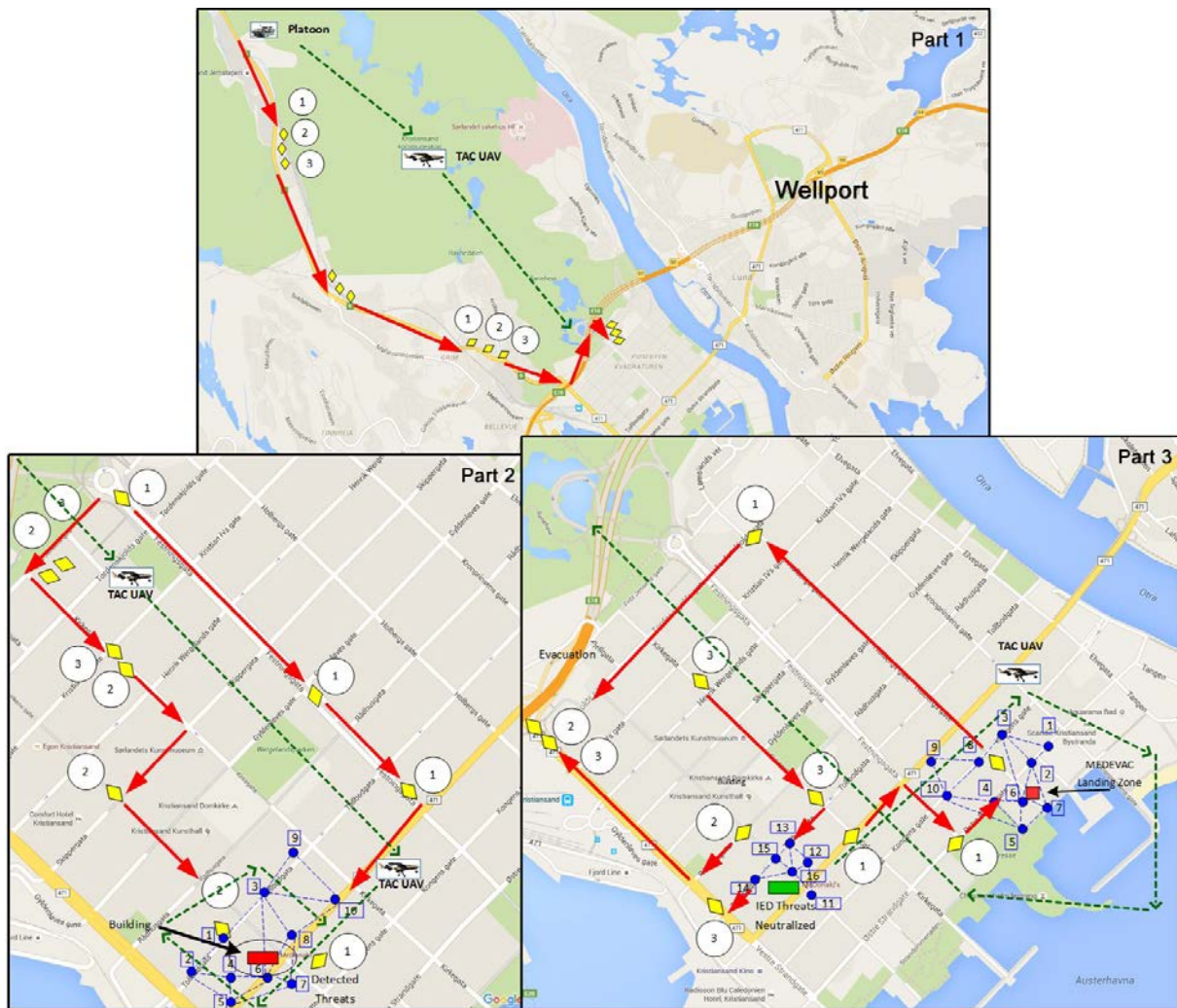


Figure B-3: Overview of Mobility Patterns in Vignette 3.

B.5 RADIO MODELS AND COMMUNICATIONS ARCHITECTURE

The emulation contains radio models for naval, ground vehicular, manpack, handheld, soldier, sensor network, and UAV radios. A Long Term Evolution (LTE) network was planned but not completed as of the writing of this report and will likely be included in the future. The models contain the typical characteristics of these types of radios such as transmit power, antenna type, and height.

The radios can run different waveforms (transmission technologies). As a typical representative for a Narrowband Waveform (NBWF), we have used NATO NBWF as the basis for our model. The original intent was to use publicly available information on the Soldier Radio Waveform (SRW) as typical representative for a Wideband Waveform (WBWF). However, due to time limitations, the currently distributed model for the WBWF was derived from the NBWF. The models contain the typical characteristics of the Physical (PHY) layer of these waveforms like data rate, transmission delay, and Signal-to-Noise Ratio (SNR). The Medium Access layer (MAC) on the other hand is (due to lack of time) currently based on either 802.11 MAC or no MAC.

Radio model configurations were generated for narrowband, medium band, and wideband radios. The actual EMANE files are available for download as part of the Anglova scenario. This section describes the characteristics of the radio models.

B.5.1 25 KHz Narrowband Radio Model

We have based the radio models on the following assumptions: Vehicle mounted narrowband tactical radios typically have an output power of 50 watts (i.e., 47 dBm) with a typical noise figure of 12 dB or better. Antenna gain, cable loss, and connector losses typically sum up to 0 dB. When two radios are on the same vehicle and operating in the same frequency band (i.e., co-site operation), they have a desensitization of 6 dB or better. However, this aspect is not currently included in the emulation models.

Fading has to be taken into account. Fading consists of two components, slow and fast fading. A typical fading margin is 8 dB. As parts of the emulation is based UTD propagation calculations with digitized terrain, the precomputed propagation model includes slow fading. Fast fading is not currently modeled and not taken into account in the emulation. The thermal noise figure is -144 dBm/KHz, which is included in EMANE.

To represent a typical narrowband radio, characteristics similar to the N2 mode of the physical layer of the NATO Narrowband Waveform (NATO NBWF [11]) was chosen as it provides a good compromise between data rate and range. This mode has a bandwidth of 25 KHz. Thus, the thermal noise power is -130 dBm ($10 * \log_{10}(25) = 14$ dB). Adding the noise figure provides the receiver sensitivity, which is -118 dBm. As typical frequencies in the military VHF band (30 to 88 MHz) the frequencies 50 MHz, 51 MHz and 52 MHz were chosen.

Simulation results of an approximated model of the NATO NBWF mode N2 require the following signal to noise ratio (SNR) threshold values to get the given Block Error Rates (BER) (Table B-2; see Ref. [21] for more information):

Table B-2: SNR Threshold Values.

BER	100%	90%	60%	30%	10%	0%
SNR	< 8.7 dB	9.0 dB	9.3 dB	9.7 dB	10.1 dB	≥ 10.9 dB

The average block size was estimated as follows. An average transmission requires two slots. The NATO NBWF PHY for mode N1 uses the interleaver best suited to the packet size. For a large packet this is 284 user bits for the first slot and 432 user bits for the second slot. The NATO NBWF mode N1 has a PHY data rate of 20.0 kbps and mode N2 has a PHY data rate of 31.5 kbps. The number of user bits per mode scales linear to the NATO NBWF PHY data rate. For mode N2, the factor is 31.5 kbps / 20.0 kbps. The average block size thus is 564 bits = (284 bits + 432 bits) / 2 * (31.5 kbps / 20.0 kbps).

Mode N2 has a MAC data rate of 17.5 kbps and uses a dynamic MAC., which was emulated within EMANE using the TDMA MAC model, a generic TDMA scheme that supports schedule distribution and updates in real-time using events. However, as noted earlier, using the currently implemented TDMA model within EMANE is not dynamic and requires a shared clock (or clocks synchronized to a high degree of precision) and as a result was not usable by the IST-124 group.

B.5.2 250 KHz Medium Band Radio Model

The medium band radio model is deduced from the narrowband radio model by increasing the bandwidth and the data rate by a factor of 10 to 250 kHz and 175 kbps. Thus, the thermal noise power is -113 dBm ($10 * \log_{10}(1250) = 31$ dB). Adding the noise figure provides the receiver sensitivity, which is -101 dBm. As typical frequencies in the military UHF band (225 to 400 MHz), the frequencies 300 MHz, 301 MHz, 302 MHz and 303 MHz were chosen for the different wideband networks within the scenario.

B.5.3 1.25 MHz Wideband Radio Model

As an alternative to the 250 KHz medium band radio model, a 1.25 MHz wideband radio model was also developed by increasing the bandwidth and the data rate by a factor of 50 to 1.25 MHz and 875 kbps. Thus, the thermal noise power is -120 dBm ($10 * \log_{10}(250) = 24$ dB). Adding the noise figure provides the receiver sensitivity, which is -108 dBm. As typical frequencies in the military UHF band (225 to 400 MHz), the frequencies 300 MHz, 302 MHz, 304 MHz and 306 MHz were chosen for the different wideband networks within the scenario.

Figure B-4 shows a graphical comparison of the three radio models that have been implemented and distributed with the Anglova scenario. With the narrowband radio model, the coverage for a single radio is typically 20 km. To cover the same area with medium band, at least four radios would be required. Finally, when using the wideband radio model, many more radios would be needed (typically 24-32) to provide the same coverage. Of course, in the narrowband case, the bandwidth is limited and shared between all the nodes in that range. However, with the wideband radio model, radios in non-overlapping ranges can communicate in parallel with no interference.

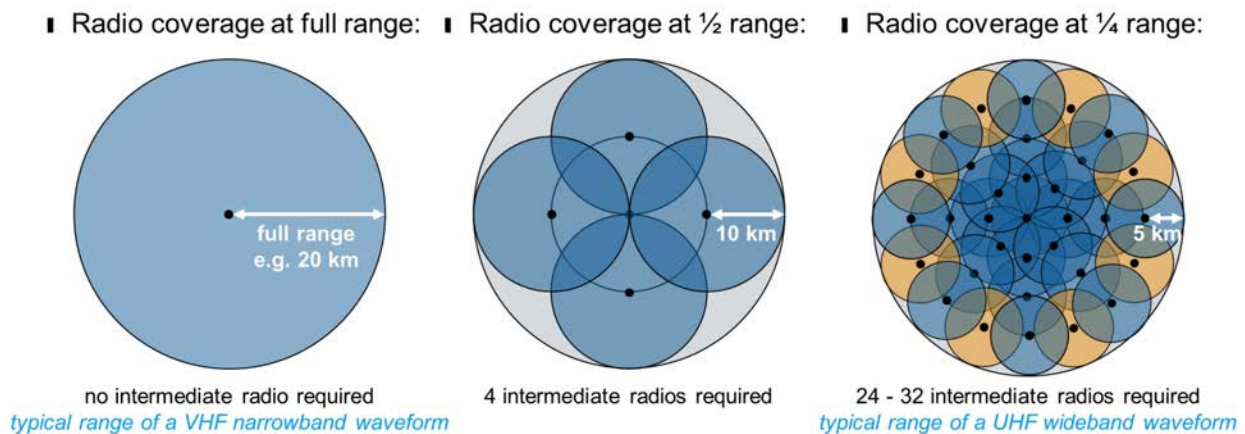


**Figure B-4: Visualization of the Range and Density of
Narrowband, Medium band, and Wideband Radios.**

B.5.4 Other Radio Models

The Anglova scenario also incorporates a few other radio models – including an HF and VHF model for the naval contingent, which is described in Annex H. Other models include a communications link for SATCOM, the Aerostat sensor platform that is part of vignette 1, and an LTE model. The modeling of the last three were not yet completed at the time of this writing.

The EMANE configuration files for these radios are available as part of the overall Anglova scenario distribution. The distribution will be updated as the other radio models are further developed.

B.5.5 Node Architecture

As part of the scenario development, some initial development was also completed on the system architecture for each node in the emulated environment. These architectural models are not complete and hence have not been released as part of the Anglova distribution. As an example, the Coalition Tactical Operations Center (TOC) node is depicted in Figure B-5. Security aspects have been removed from the excerpt shown. In reality, the TOC will require access to information from different security domains (multiple levels of security) and be employing equipment that realizes COMSEC on different layers

(application layer, network layer, and/or link layer). A separate IST-124 Security Architecture report is being published with a discussion regarding possible security architectures for this environment. We note that the COMSEC security aspects are not included in the emulation developed so far, partly to simplify distribution.

On the left side of Figure B-5, the different information sources and sinks are depicted. These are connected to the outside world via one or more routers. Potential connections to the outside world are a gateway to FMN and a multitude of different radio types. On the right side of the diagram the nodes that are potentially reachable over these links are listed. Within the current emulation environment setup, each platform is modeled as one node with multiple emulated links, one for each type of radio.

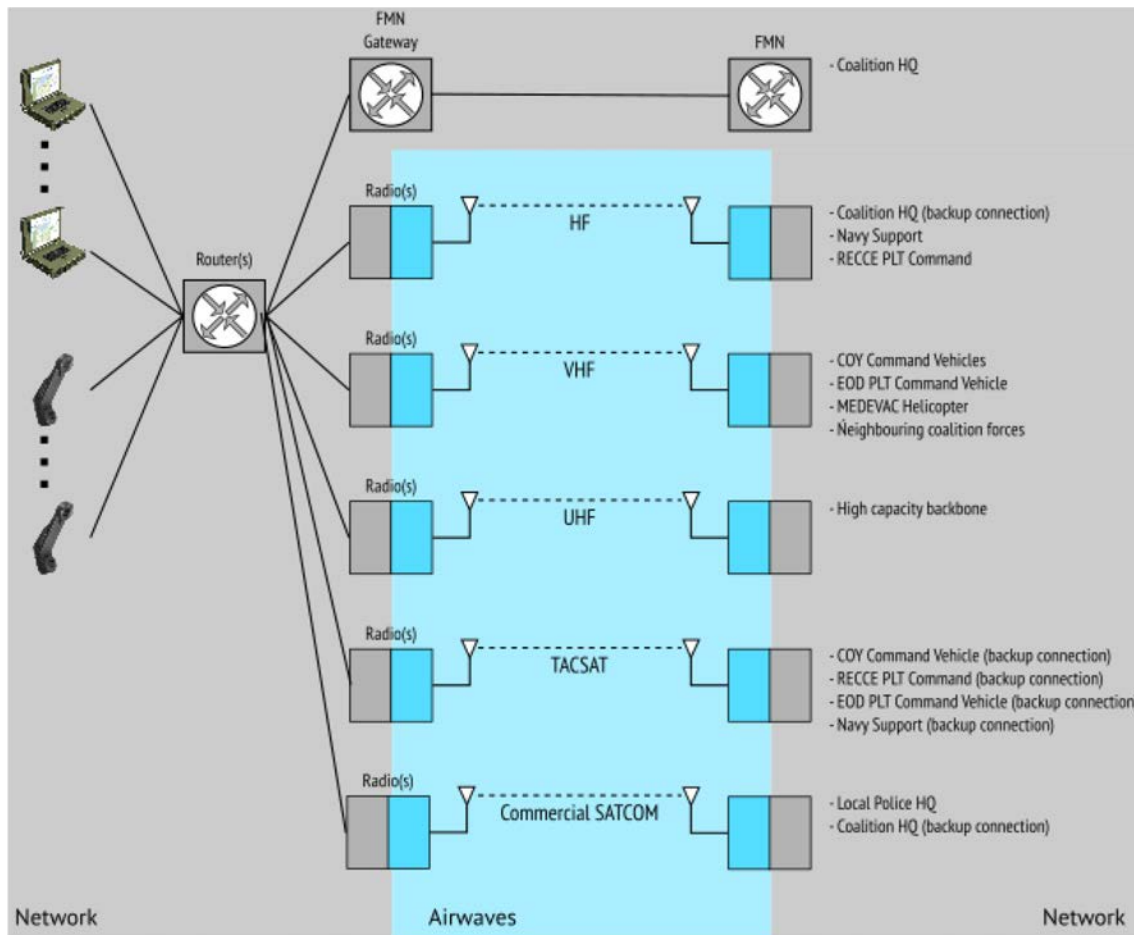


**Figure B-5: System Architecture View of the Coalition
Tactical Operations Center (TOC) Node.**

Figure B-5 also shows a link between the Coalition TOC and the Coalition HQ via an FMN gateway. The original intent for the scenario was to include the Finnish TACOMS+ implementation of NIP (Network Interconnection Point) auto configuration node to represent an (early spiral version of) an FMN network connection. It includes features planned for FMN Spiral 3 and onwards towards full Protected Core Network (PCN) capabilities [22]. The node contains four auto configuration interfaces. Local client and server networks and connection towards tactical networks use static configurations. When two nodes are connected, they identify each other using specific RIPv2 messages and establish a Generic Routing Encapsulation (GRE) over IPSec connection to secure traffic. Nodes authenticate each other using certificates or pre-shared secrets. All traffic between nodes is protected and authenticated. After a connection is established, a BGP session shares routing information and allows interdomain routing

(Figure B-6). It is also likely that in an actual deployment, the headquarters of the different nations that are part of the coalition would also be connected to each other and to the Coalition HQ node using the FMN approach. At the time of writing this report, the FMN gateway has not yet been included and released as part of the Anglova scenario. This might happen as part of the IST-161 RTG's activities.



Figure B-6: TACOMS+ Auto Configuration Over IPsec.

B.6 SCENARIO CHARACTERIZATION

Characterizing the Anglova scenario is important in order for experimenters to understand and anticipate expected behavior at the RF level. As of the writing of this report, the focus has been on the second vignette, which has the most complicated dynamics due to the motion and terrain, and on the naval task group of the scenario.

B.6.1 Connectivity Internal to the Battalion in Vignette 2

As described earlier, the second vignette covers the deployment of the coalition forces, a battalion consisting of six companies, into the operational zone. The battalion starts out by moving in a single column on one of the main roads (see Figure B-7); the Coalition Head Quarters (CHQ) is indicated with a cyan-colored star. After about 10 km, the battalion splits up over two main roads and after about 25 km splits up further into many paths grouped in companies. Towards the end, the battalion finally splits up to the level of platoons. Altogether, the Vignette 2 mobility pattern is 7800 seconds (130 minutes) long.

The battalion consists of six companies. Altogether there are 157 vehicles, each of them being a network node. In addition, an Unmanned Aerial Vehicle (UAV) node was also added to this vignette (with a trajectory in the shape of two connected green circles in Figure B-7) – it can act as a communications relay and provide persistent surveillance capabilities.

To estimate the path loss between the nodes, a UTD propagation model by Holm is used [19]. In Figure B-8, Figure B-9, and Figure B-10, the path loss is used to calculate the connectivity in the 157-node network for the whole deployment phase. Note, the UAV and the CHQ were not included in this calculation, which was completed prior to the UAV and CHQ were introduced into the scenario. The calculations show the connectivity that is possible in the scenario and serves as a benchmark that the performance of the routing protocols can be compared with. Three different transmission technologies to connect the nodes are investigated. The connectivity is illustrated by showing how the fraction of nodes at h hops distance from each other varies over time. The average of h is taken over all nodes in the network. The hop distance is theoretically calculated, with the assumption that there is a communication link between two nodes if the path loss value is less than a system gain G_{sys} that varies for the transmission technologies. The three investigated transmission technologies are: 25 kHz, 17.5 kbit/s with $G_{sys}=156$ dB; 250 kHz, 175 kbit/s with $G_{sys}=146$ dB; and 1.25 MHz, 875 kbit/s with $G_{sys}=139$ dB.

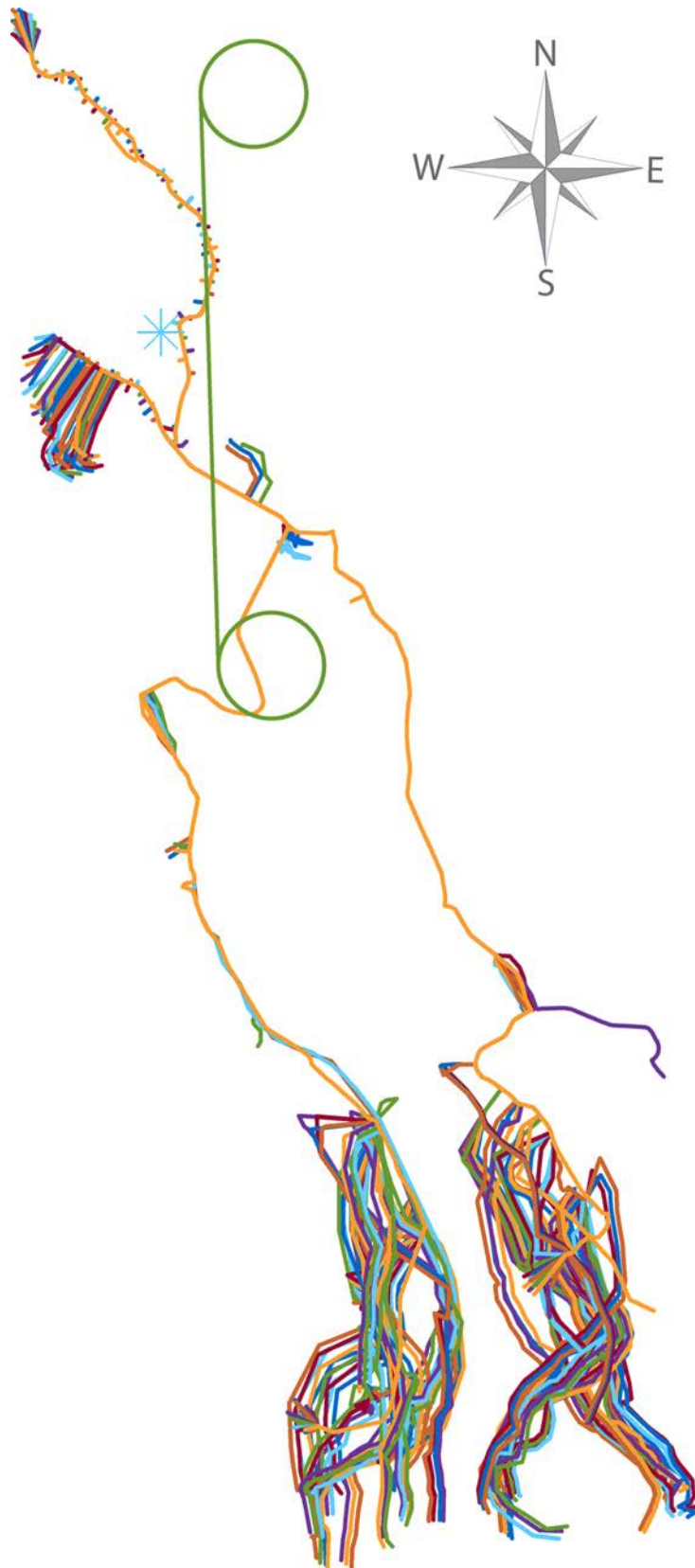


Figure B-7: Illustration of the Movements (Directed from the North to the South) of the Battalion.

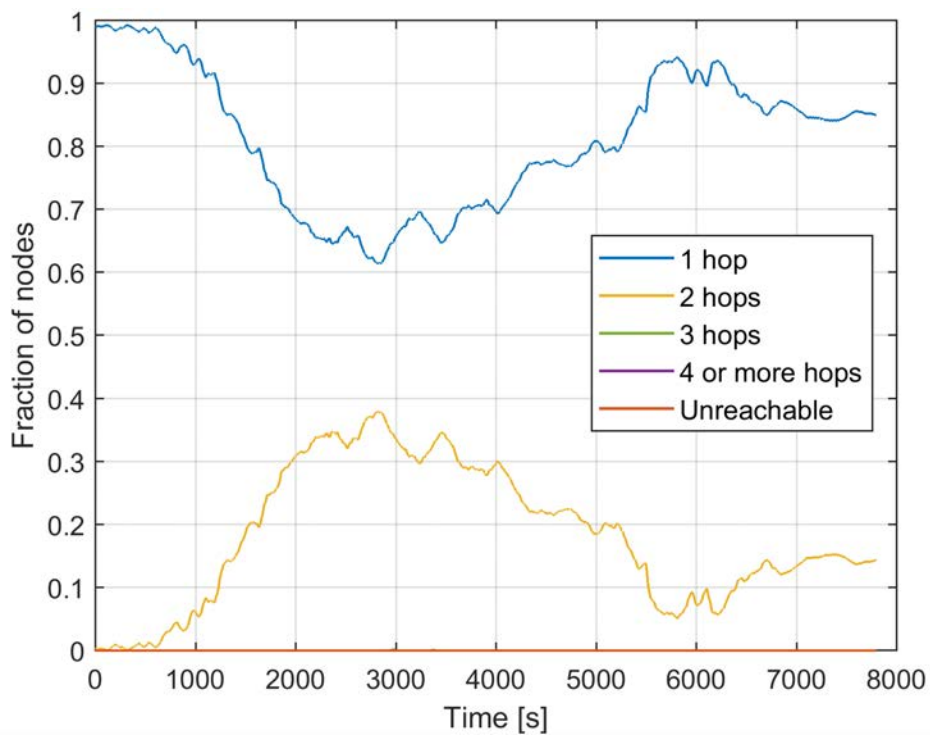


**Figure B-8: The 25 KHz Transmission Technology
at the 50 MHz Frequency Band.**

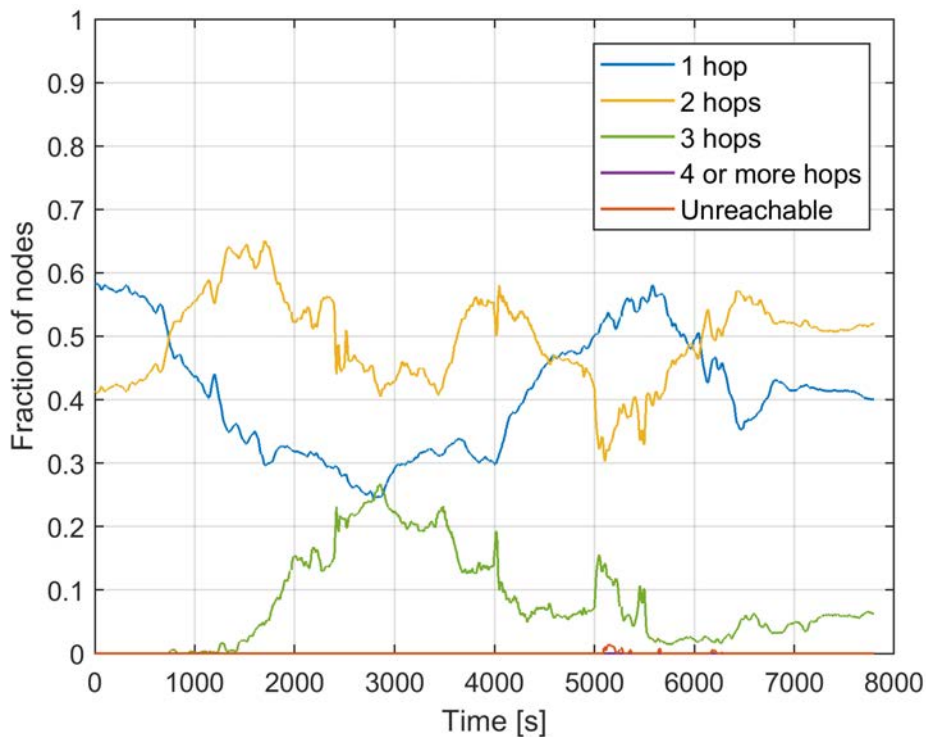


**Figure B-9: The 250 KHz Transmission Technology
at the 300 MHz Frequency Band.**

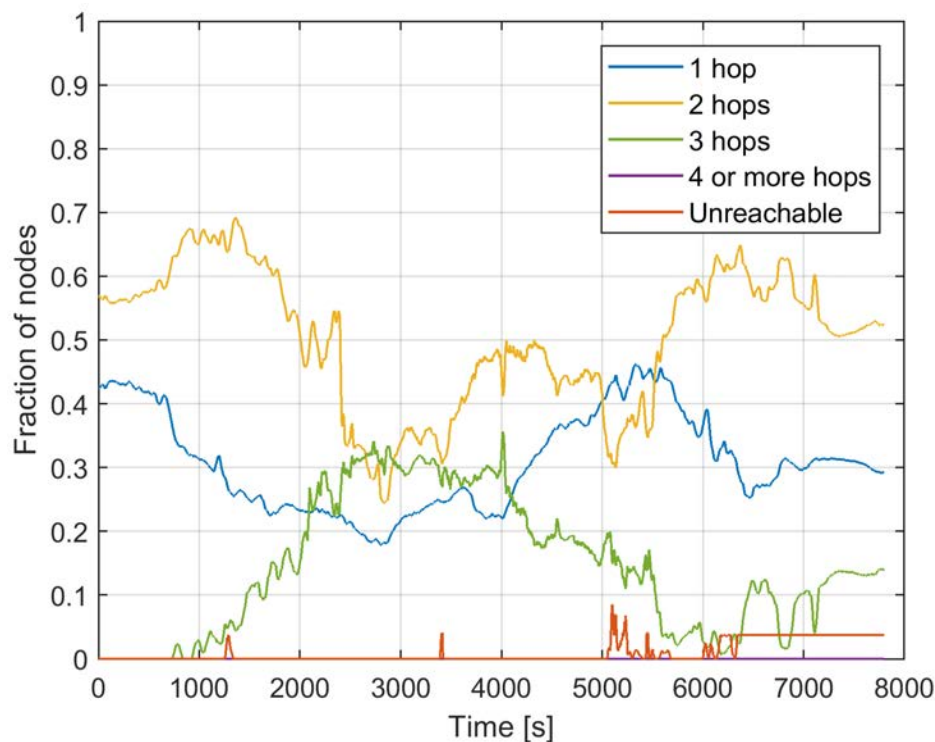


**Figure B-10: The 1.25 MHz Transmission Technology
at the 300 MHz Frequency Band.**

As can be seen the 25 kHz transmission technology at 50 MHz keeps the network connected for the whole deployment phase and no more than two hops are required. For the other two transmission technologies, the network is not always fully connected as there are a number of unreachable nodes at various times. After about 2000 seconds into the scenario, the network start to be stretched out and the number of hops increases. Towards the end of the vignette, the network is fragmented with a few nodes behind the main part of the battalion that cannot be reached using the WB transmission technology. However, within the main part of the battalion, almost all nodes can be reached with a maximum of three hops. This is the reason why four or more hops seldom occurs. In Figure B-11 the bar graph shows the fraction of nodes at different hop distances averaged over the vignette. In the figure it is shown that at least a few paths need 4 or more hops. Furthermore, it can be seen that the number of hops is larger for the 1.25 MHz than for the 250 kHz transmission technology.

Vignette 2 and a 1000 second long segment in the latter phase of the vignette has been used to investigate the scalability and performance of the Optimized Link State Routing protocol (OLSR) in Ref. [23]. Also, by using this segment, the effects of small-scale fading on the stability of the links is analyzed in Ref. [24].

B.6.2 Link Dynamics in Vignette 2

One important configuration of proactive routing protocol relates to how fast, or cautious the protocol should be in including tentative links in its routing tables. Maintaining the routes in a dynamic mobile scenario can be more or less difficult dependent on how frequent the link changes, which in turn requires that the routes are updated. In particular, it is problematic if links are lost without the routing protocol being aware. To investigate this topic further, we consider Vignette 2 of the Anglova scenario, see Refs. [23] and [25]. A network based on the 157 vehicles, and over the whole around two hours, of Vignette 2 is researched. Note that the Coalition Headquarters, and the UAV nodes are excluded. The reason is that the links connecting these two nodes have different link characteristics and therefore need separate treatment. The CHQ is a static node having a high mast and the UAV an airborne node with a longer communication range.

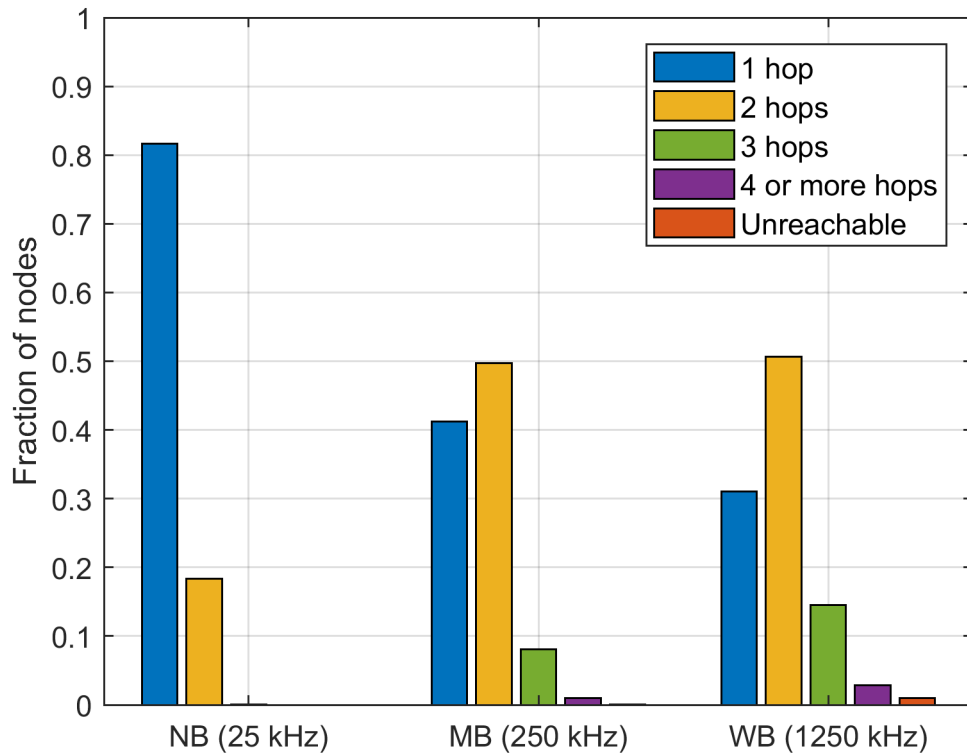


Figure B-11: The Fraction of Nodes at Different Hop Distances Averaged Over Vignette 2.

B.6.2.1 Preliminaries

Whether a link exists and can be lost is a rather diffuse concept. Several definitions can be used. In Ref. [26] a time hysteresis criterion is used to calculate how often a link changes. Another related option that we use here is the way OLSR establishes and remove links by utilizing HELLO messages. A HELLO message is transmitted from each node with a given retransmission interval, with the default value in OLSR being two seconds.

To decide whether a link exists, we use the basic link metric included in the OLSRv1 RFC [27]. This method estimates the reliability of a link based solely on OLSR HELLO packets. The method assigns weight 1 to all received hello packets and weight 0 to all lost hello packets over a link. To obtain a measure of the link quality, denoted Q , the weight sequence is exponentially filtered according to Ref. [27], resulting in values in the range between zero and one. With standard OLSR parameter settings, a link is classified as reliable if Q is larger than an upper threshold set to 0.8. When a link is classified as reliable, it will remain reliable until Q becomes lower than a lower threshold set to 0.3.

We denote the minimum required number of consecutive correctly received HELLO packets to establish a link by P_{min} . For the OLSR standard setting, the algorithm will consider a new link reliable if three consecutive hello packets are received, i.e., $P_{min} = 3$. If two consecutive packets are lost on a reliable link, the link will be considered unreliable. To obtain other values on P_{min} the upper threshold of Q is adjusted.

We define the radio system gain G to be equal to the maximum possible path loss from transmitter to receiver for connections that satisfy a given error requirement. That is, radio systems with good transceiver performance have a larger system gain than transceivers with low performance. We consider the three defined transmission technologies NB (Narrowband), MB (Mediumband) and WB (Wideband) with

different settings of bandwidth W , data rate R and radio system gain G_{sys} :

- Transmission technology NB: $W = 25$ kHz, $R = 17.5$ kbit/s, $G_{sys} = 156$ dB,
- Transmission technology MB: $W = 250$ kHz, $R = 175$ kbit/s, $G_{sys} = 146$ dB; and
- Transmission technology WB: $W = 1.25$ MHz, $R = 875$ kbit/s, $G_{sys} = 139$ db.

The transmission technology NB uses the 50 MHz band, and the other two the 300 MHz band. These choices correspond to the NB, MB, and WB radios that were modeled within EMANE for the emulation environment.

B.6.2.2 Results

The value on P_{min} determines how cautiously a link is established. With a large value for P_{min} it takes longer to establish a link, fewer links exist in the network and the connectivity is lower than with a small value for P_{min} . A lower degree of connectivity means that more nodes are missing. A node is missing when a given node cannot reach that node. Furthermore, the number of lost links per node and per second is lower with a large value than with a small value on P_{min} .

These effects are illustrated in Figure B-12, through Figure B-16. Using the NB transmission technology results in significantly better connectivity than with the other two transmission technologies. On average, about 120 – 130 of the possible 156 links from a node are available and about 1.2 hops are required to reach a given node. The network is almost connected, i.e., very few nodes are unreachable, as compared to when the wideband transmission technology WB is used, in which case between 2 to 6 nodes cannot be reached on average. The value used for P_{min} is important for the longevity and stability of a link exists as it determines how many consecutive HELLO messages need to be received correctly. When $P_{min}=3$, on average around 0.3 links per node is lost for all the transmission technologies. However, at certain times in Vignette 2, the difference between the NB and WB can be large. For example, around 6000 seconds into the vignette, only 0.15 links per node are lost with the NB transmission technology but as many as 0.6 links per node are lost with the WB transmission technology (see Figure B-16). The number of lost links per second decreases with a larger value for P_{min} . In a well-connected network with many links, many links can also be lost per second as compared to a sparser network with fewer links. The investigation shows this tradeoff in particular between prioritizing good connectivity or fewer lost links per second. Note, however, that to have a well-connected network and also fewer lost links per second requires using the narrowband transmission technology NB at the 50 MHz band and choosing a large value on P_{min} as this transmission technology has considerably better range than the other two transmission technologies. The drawback, however, is the low data rate of the NB transmission technology that limits what can be transmitted between the companies. Many lost links per second reduce the packet delivery ratio. As the HELLO retransmission is 2 seconds, it may take up to 4 seconds to detect that a link is lost. Therefore, even if a link in reality is lost during this time period a node may still try to use it to send a packet. We can conclude that the dynamics is rather high and varies depending on the transmission technology used and elapsed time of Vignette 2.

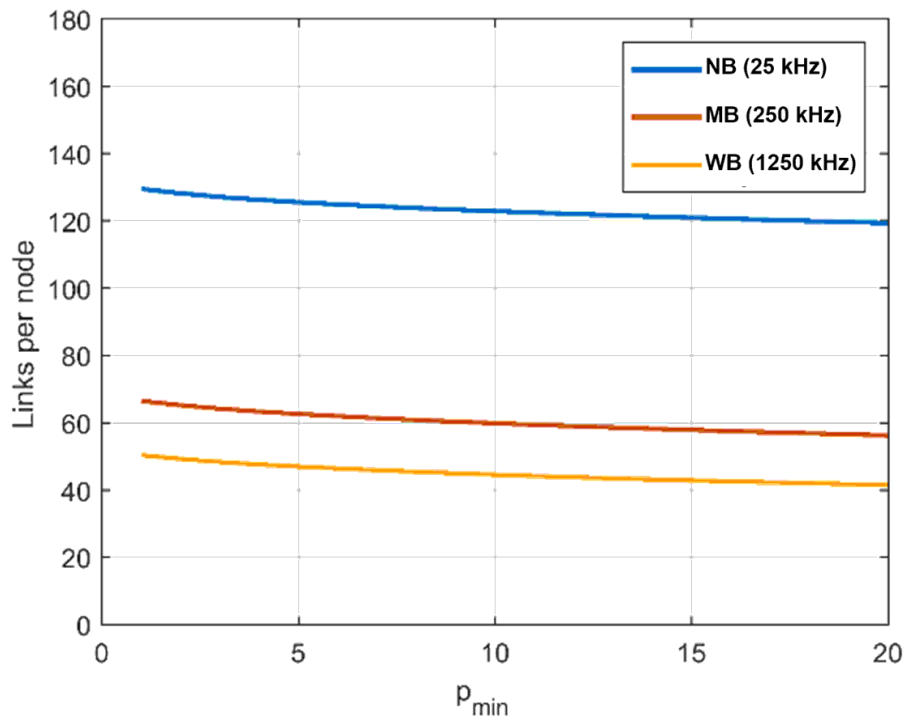


Figure B-12: Total Average Number of Links
Per Node for Different Values on P_{min} .

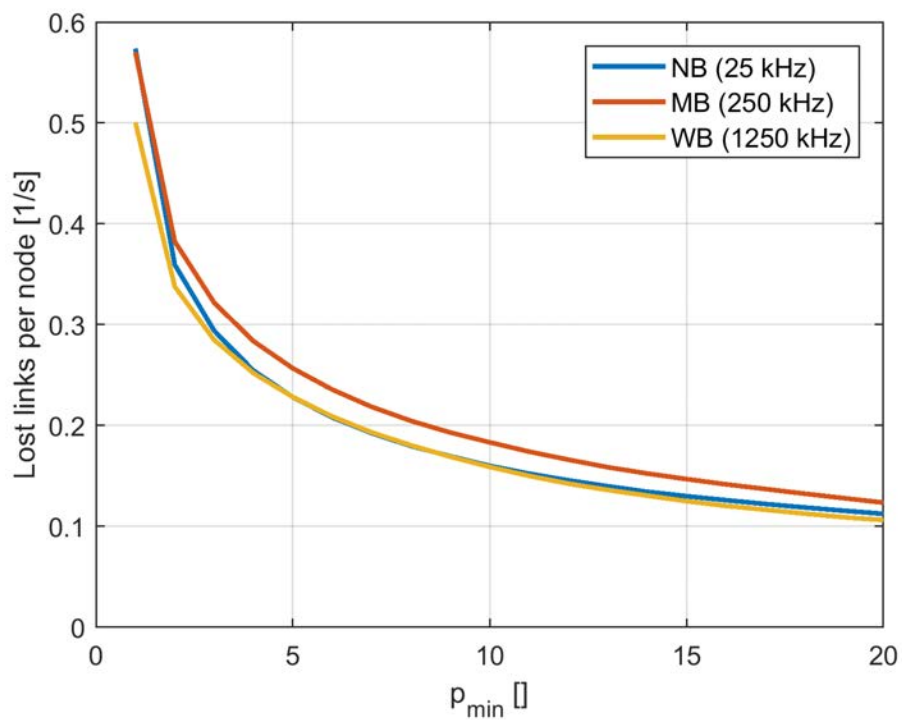


Figure B-13: Average Number of Lost Links Per Node
and Second for Different Values on P_{min} .

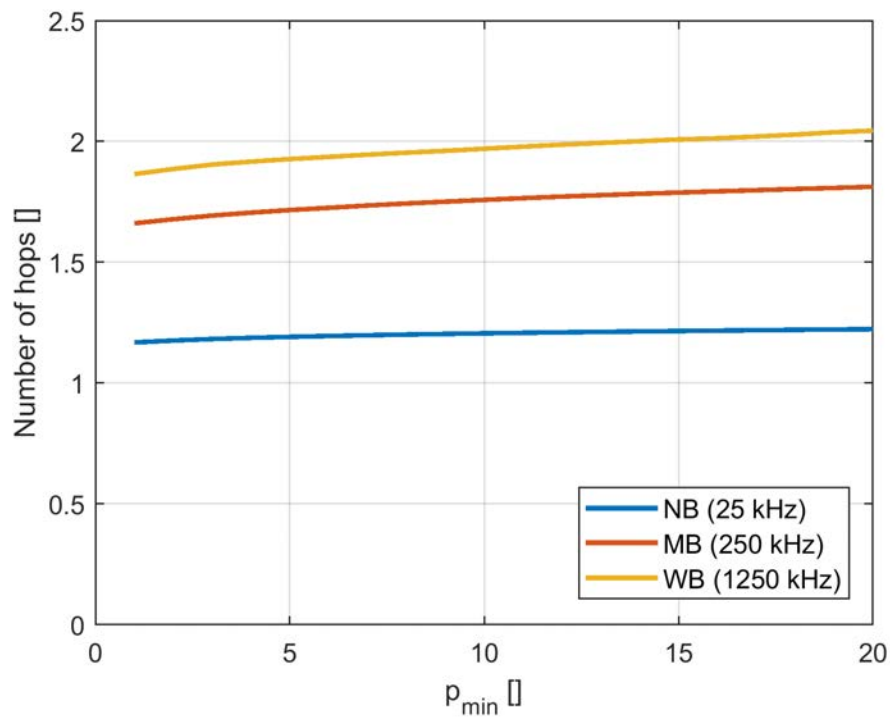


Figure B-14: Average Number of Hops Between all Node Pair in the Network for Different Values on P_{min} .

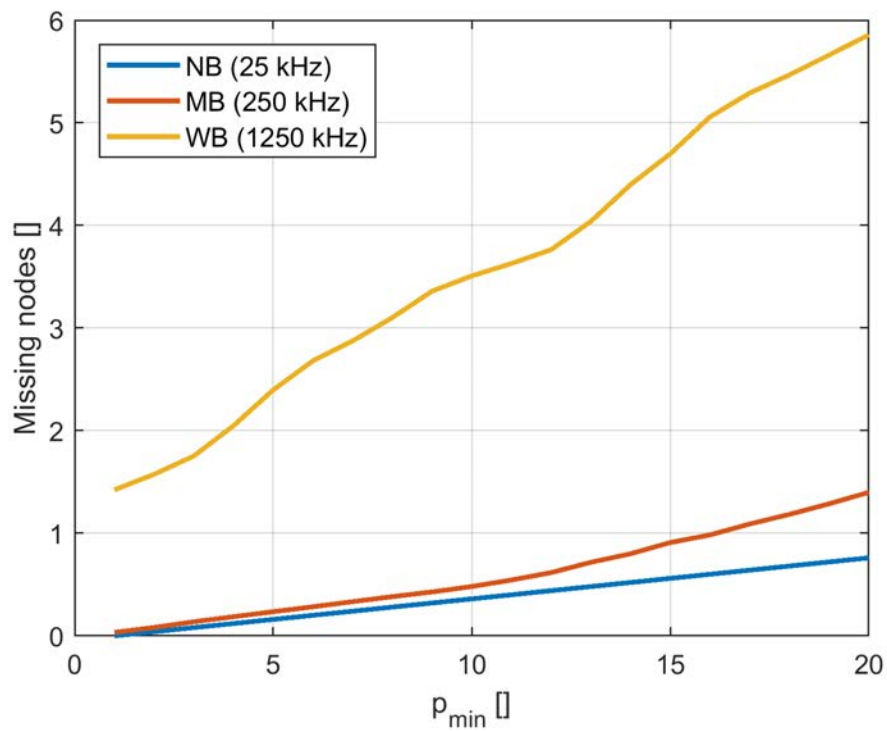


Figure B-15: Average Number of Not Reachable Nodes for Different Values on P_{min} .

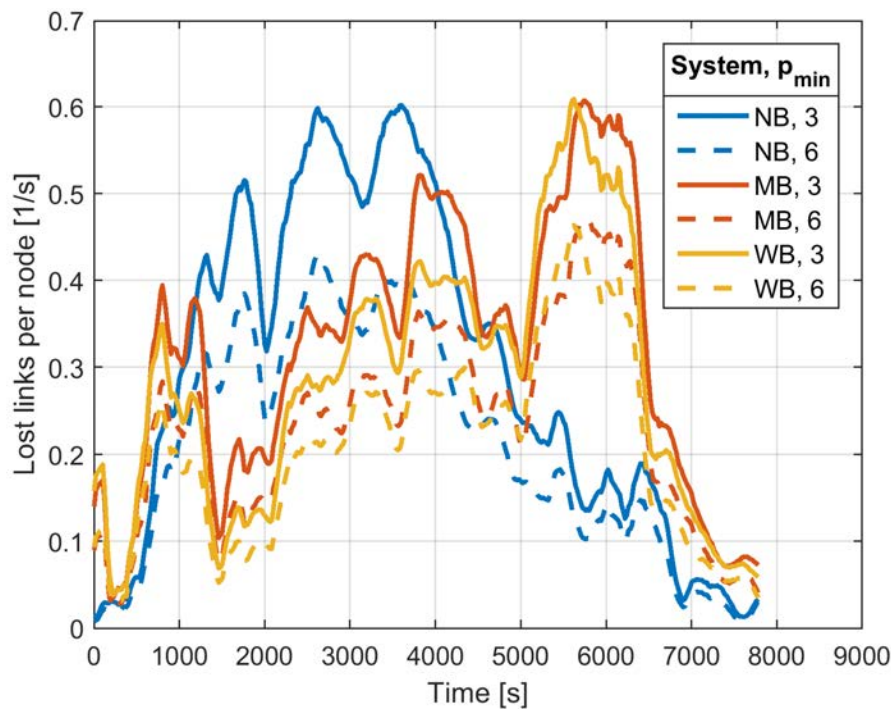


**Figure B-16: Average Number of Lost Links Per Node
Over the Two-Hour Long Vignette 2.**

B.7 REFERENCES

- [1] North Atlantic Treaty Organization (NATO), Federated Mission Networking (FMN). Internet: <http://www.act.nato.int/fmn>, January 2, 2016.
- [2] AdjacentLink, LLC, Extendable Mobile Ad-hoc Network Emulator (EMANE) Wiki. Internet: <https://github.com/adjacentlink/emane/wiki>, January 2, 2016.
- [3] AdjacentLink, LLC, Extendable Mobile Ad-hoc Network Emulator (EMANE). Internet: <https://github.com/adjacentlink/emane>, January 2, 2016.
- [4] Ahrenholz, J., Comparison of CORE Network Emulation Platforms, in IEEE Military Communications Conference (MilCom 2010), pp. 166-171, October 31 – November 3, 2010.
- [5] NS3 Consortium. NS3 Project Homepage. Internet: <https://www.nsnam.org/>, January 2, 2016.
- [6] University of Southern California Information Sciences Institute, Network Emulation with the NS Simulator. Internet: <http://www.isi.edu/nsnam/ns/ns-emulation.html>, January 2, 2016.
- [7] OMNeT++ Discrete Event Simulator. Internet: <https://www.omnetpp.org/>, April 6, 2018.
- [8] Linux Foundation, Network Emulation (NETEM) Project Homepage. Internet: <http://www.linuxfoundation.org/collaborate/workgroups/networking/netem>, January 2, 2016.
- [9] Carson, M., and Santay, D., NIST Net – A Linux-based Network Emulation Tool, on ACM SIGCOMM Computer Communications Review, vol. 33, no. 3, pp. 111-126, July, 2003.
- [10] Emulab, Emulab Project Home Page. Internet: <http://www.emulab.net/>, January 2, 2016.

- [11] North Atlantic Treaty Organization (NATO), STANAG 5630/AComP-5630: Narrowband Waveform for VHF/UHF Radios – Head STANAG, STANAG 5630/AComP-5630, Edition A, Version 1. To be published.
- [12] Google, Inc., Protocol Buffers. Internet: <https://developers.google.com/protocol-buffers/>, January 2, 2016.
- [13] US Army Research Laboratory. Traffic Generation Tool. Internet: <http://www.arl.army.mil/www/default.cfm?page=2490>, January 2, 2016.
- [14] US Naval Research Laboratory. Multi-Generator (MGEN). Internet: <http://www.nrl.navy.mil/itd/ncs/products/mgen>, January 2, 2016.
- [15] US Naval Research Laboratory. Scripted Display Tools (std/std3d). Internet: <http://www.nrl.navy.mil/itd/ncs/products/sdt>, January 2, 2016.
- [16] National Aeronautics and Space Administration. NASA World Wind. Internet: <http://worldwind.arc.nasa.gov/>, January 2, 2016.
- [17] Eklöf, F., and Johansson, B., On Situation Awareness for a Mechanized Battalion in Two Tactical Scenarios, in Swedish, Defence Research Est., Div. of Command and Control Warfare Tech., FOA-R-00-01734-504-SE, Linköping, Sweden, December 2000.
- [18] Asp, B., Eriksson, G., and Holm, P., Detvag-90 – Final Report, Defence Research Est., Div. of Command and Control Warfare Tech., FOA-R-97-00566-504-SE, Linköping, Sweden, September 1997.
- [19] Holm, P., UTD-Diffraction Coefficients for Higher Order Wedge Diffracted Fields. IEEE Trans. Antennas Propagat., vol. AP-44, pp. 879-888, June 1996.
- [20] Magliacane, J., SPLAT! Internet: <http://www.qsl.net/kd2bd/splat.html>, May 8, 2017.
- [21] Libæk B., and Solberg, B., A simulator model of the NATO Narrowband Waveform Physical Layer, FFI Notat 2011/00533, 2011.
- [22] Hallingstad, G., and Oudkerk, S., Protected Core Networking: An Architectural Approach to Secure and Flexible Communications, in IEEE Communications Magazine, vol. 46, no. 11, pp. 35-41, November, 2008.
- [23] Marcus, K., Barz, C., Kirchhoff, J., Roge, H., Nilsson, J., in't Velt, R., Suri, N., Hansson, A., Sterner, U., Hauge, M., Lee, K., Holtzer, A., Buchin, B., Peuhkuri, M., and Mısırlıoğlu, L., Evaluation of the Scalability of OLSRv2 in an Emulated Realistic Military Scenario, in Proceedings of the 2017 International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, 2017.
- [24] Sterner, S., and Uppman, U., On the Robustness of OLSR in a Mobile Tactical Scenario in Rural Terrain, in Proceedings of the 2017 International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, 2017.
- [25] Suri, N., Hansson, A., Nilsson, J., Lubkowski, P., Marcus, K., Hauge, M., Lee, K., Buchin, B., Mısırlıoğlu, L., and Peuhkuri, M., A Realistic Military Scenario and Emulation Environment for Experimenting with Tactical Communications and Heterogeneous Networks, in Proceedings of the 2016 International Conference on Military Communications and Information Systems (ICMCIS), Brussels, 2016, doi: 10.1109/ICMCIS.2016.7496568.

- [26] Örn Tengstrand, S., Hansson, A., and Grönkvist, J., Routing Architectures for Heterogeneous Networks, Swedish Defence Research Agency (FOI), FOI-R-4133—SE, Linköping, Sweden, September 2015.
- [27] Clausen, T., and Jacquet, P., Optimized Link State Routing Protocol (OLSR), IETF Network Working Group, RFC 3626, October 2003.



Annex C – EXPERIMENTATION ENVIRONMENT AND TOOLS

Niranjan Suri and Kelvin Marcus
U.S. Army Research Laboratory (ARL)
UNITED STATES

Levent Mısırlıoğlu
MilSOFT Yazılım Teknolojileri A.Ş
TURKEY

Markus Peuhkuri
Aalto University
FINLAND

Maggie Breedy
Florida Institute for Human & Machine Cognition
(IHMC)
UNITED STATES

This annex provides an overview of the Anglova experimentation environment and surrounding tools that were created or co-opted for the activities of the NATO IST-124 RTG. The Anglova military scenario itself is described in Annex A: “Operational Perspective for IST-124” and details about the mobility patterns and experimentation methodologies for the Anglova scenario are described in Annex B: “Emulation-based Experimentation and the Anglova Scenario”. The IST-124 RTG instantiated the Anglova scenario using the Extendable Mobile Ad-hoc Networking Environment (EMANE). This annex provides some detail on EMANE and discusses alternate deployment models for the experimentation environment. In particular, two deployment models are discussed – the US Army Research Laboratory’s (ARL’s) Dynamically Allocated Virtual Clustering (DAVC) and VMware ESXi. Additional details about using DAVC to conduct experiments are covered in Annex D: “IST-124 Experimentation Execution”.

This annex is organized as follows:

- Section C.1 provides some background on EMANE.
- Section C.2 provides an overview of deploying Anglova over the DAVC environment.
- Section C.3 provides an overview of deploying Anglova over the VMware ESXi environment, including step-by-step directions to configuring the networks and Virtual Machines (VMs) within ESXi.
- Section C.4 discusses two different visualization tools – SDT3D and Mirage, along with the OpenStreetMap dataset that has been created to support the Anglova scenario.
- Section C.5 discusses tools for playing the Anglova scenario and driving the emulation.
- Section C.6 discusses tools for generation of custom pathloss data.
- Section C.7 discusses lessons learned.
- Section C.8 describes some open issues that are yet to be resolved.

C.1 EMANE OVERVIEW

The Extendable Mobile Ad-hoc Networking Emulator (EMANE) [1] was developed by CenGen (now AdjacentLink) under sponsorship by the US Naval Research Laboratory (NRL), the Office of the Secretary of Defense (OSD), and the US Army Research Laboratory (ARL). It is freely available on GitHub and provides a flexible framework for emulating multiple types of radios. EMANE primarily addresses the Physical (PHY) and Media Access (MAC) layers of the network stack and includes three different radio models – a generic RF Pipe model, an 802.11abg model, and a TDMA model. Each of these models offers various customizations of the radio parameters, antennas, and error models. While models of some specific tactical radios exist, they are not available in the public domain and hence will not be discussed in this document.

EMANE supports a flexible deployment model – centralized, fully distributed, or a hybrid of the two. Each radio interface of a network node in the emulated network is represented within EMANE by an instance of a Network Emulation Module (NEM). The NEMs instantiate the PHY and MAC layers of the radio being emulated and each EMANE instance can contain one or more NEMs. In the centralized model, all the NEMs are instantiated with a single instance of EMANE. In the fully distributed model, each EMANE instance contains only one NEM. In the hybrid model, there are multiple instances of EMANE each with multiple NEMs. In the hybrid and distributed deployment models, the NEMs communicate with each other using an Over The Air (OTA) channel, which uses UDP multicast over a control network (which is independent of the emulated network interfaces). The NEMs also react to control events that are sent to them over the EMANE event channel, typically also via UDP multicast. For example, when playing the Anglova scenario, the position and pathloss updates are sent to EMANE via this control channel. See the EMANE documentation for more details [1].

C.2 DYNAMICALLY ALLOCATED VIRTUAL CLUSTERING (DAVC) DEPLOYMENT

The NATO IST-124 RTG uses the US Army Research Laboratory’s Dynamically Allocated Virtual Clustering (DAVC) Management System to deploy the Anglova scenario using the distributed EMANE emulation model. In this emulation model the EMANE software is installed within VMs that also execute the applications that are the subject of the experimentation (routing protocols, data dissemination protocols, etc.) and whose performance is being evaluated.

DAVC is a web-based virtualization service and cloud-operating environment that creates complex virtual experimentation clusters that can be used for simulation-based, emulation-based, and hybrid field/emulation experimentation [2]. DAVC deploys networked clusters composed of VMs tailored to user specifications. The DAVC management system abstracts away test-bed infrastructure configuration through automated provisioning processes that configures the virtual networking for each VM [2]. Clusters created by DAVC are heterogeneous, so each VM can have different OSs, application sets, and hardware attributes such as RAM, CPU cores, hard disk, and network interfaces. DAVC users can register custom VMs as templates that can be used within their experimentation clusters.

The NATO working group created a custom Linux Ubuntu 16.04 VM to represent a single Anglova scenario node. This template VM was preinstalled with the applications necessary for running the Anglova scenario including EMANE, the Multi Generator (MGEN) traffic generator [3], and the OLSRv1 and OLSRv2 routing protocols [4]. The VM was preinstalled with the various EMANE radio models, mobility and pathloss configuration files specific to the Anglova scenario. Custom scripting to bootstrap the Anglova scenario and emulation environment was also preinstalled within the VM. Once registered with DAVC, the VM is then used as a template within a DAVC experimentation cluster to run the Anglova scenario.

Using DAVC, the Anglova scenario is distributed with a 1-to-1 mapping with each Anglova node running within a single DAVC virtual cluster node. The entire 283 node scenario can run within a 284 node DAVC cluster as shown in Figure C-1. When deployed in this manner node 284 acts as the experimentation orchestration node and is responsible for executing the bootstrap scripting that launches the various applications and EMANE on the remaining 283 nodes. Also shown in Figure C-1 are the two networks DAVC auto-configures for the 284 node cluster. The first network is an out-of-band control/debug network that allows node 284 to communicate with and execute experimentation instructions on the other 283 nodes. The second network is the experimentation network that EMANE uses to overlay the emulated Anglova network channel upon – the OTA channel.

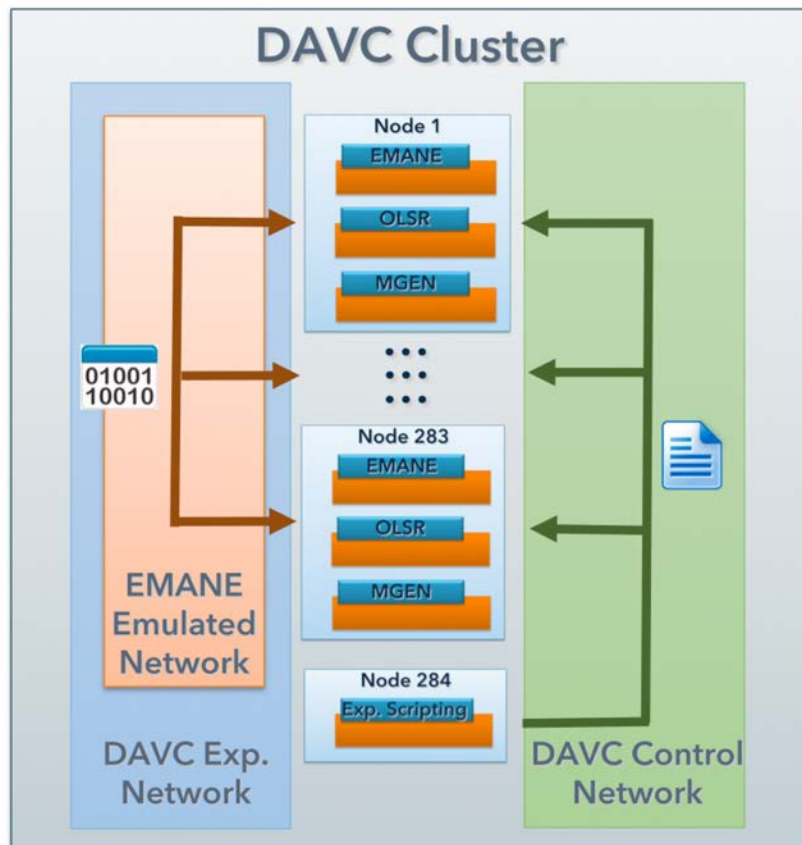


Figure C-1: The 283 Node DAVC Cluster and Networks. The emulated EMANE network is overlaid on the DAVC experimentation network while experimentation commands flow across the DAVC control network.

The emulation environment provides the flexibility to deploy subsections of the entire 283 node scenario within a DAVC cluster. If a researcher is only interested in experimenting with the 159 mobile nodes contained in Vignette 2, the bootstrap scripting can map only those nodes contained within that portion of the Anglova scenario to 159 DAVC cluster nodes, where the corresponding EMANE configuration files will be run. This type of deployment model that uses only a subset of the Anglova scenario was used in the experiment performed in Ref. [5]. The authors were interested in evaluating the scalability of the OLSRv2 routing protocol on company and multi-company sized topologies ranging from 24 nodes to 96 nodes, and hence deployed several 96 node DAVC clusters and configured the experimentation scripting to only run a portion of the scenario that contained four 24 node companies.

The DAVC model also supports experimentation concurrency, which allows multiple experiments to be executed in parallel. The experiments performed in Ref. [5] are an example of this model. Multiple DAVC clusters were deployed where each hosted a different experimental test case. Some experiments were run in parallel where each executed a different version of the OLSR routing protocol and different parameters were provided to the experimentation scripting that varied the MGEN background traffic generation model, network traffic shaping, and the number of Anglova nodes involved in the experiment. This feature of the DAVC model has the effect of reducing overall experimentation runtime.

C.3 VMWARE ESXI DEPLOYMENT

In addition to the DAVC environment, the Anglova scenario was also deployed using a second, alternate configuration using the VMware ESXi virtualization platform. This deployment uses the hybrid model for

EMANE configuration, where n virtual machines have one EMANE Server VM that runs all of the emulation components for those n VMs. An example configuration is shown in Figure C-2. Note that the test VMs are designated Test Node- n (TN- n) and there could be multiple TNs per physical server, with a recommendation of one VM per CPU core. Each test VM is also configured with at least two network interfaces, one for the application data and one for control traffic (similar to the DAVC configuration). Each physical server also contains an EMANE Server VM, which runs all of the EMANE components. One advantage of this deployment model is that the test VMs do not have to run any of the EMANE components. In fact, the network link to the test VM could also be connected to other computing and network devices (e.g., an embedded device, proprietary hardware, radio, a WiFi access point), which allows hybrid experimentation with VMs and other physical hardware in the loop.

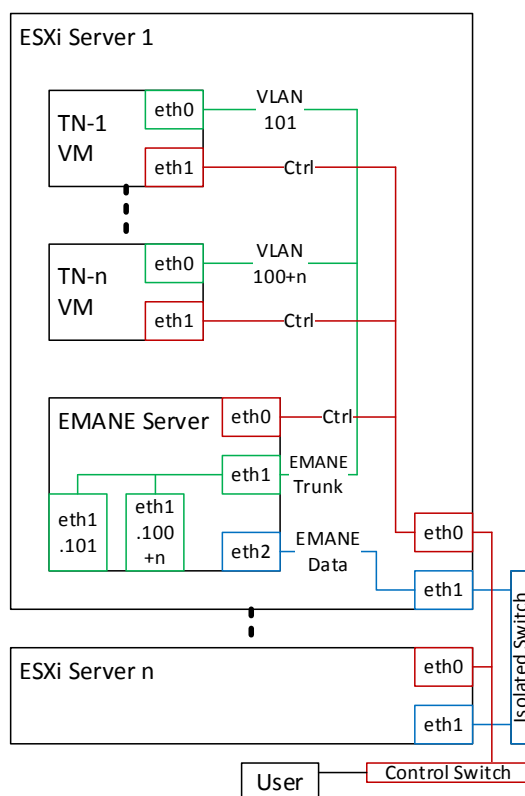


Figure C-2: Anglova Deployment Over ESXi.

The network shown in green is configured as a virtual switch within ESXi, with each test VM connecting one or more interfaces to this virtual switch. Each connection is assigned a different VLAN ID. The EMANE Server VM connects to this switch using a VLAN trunk, which uses the 802.1q protocol. Within the EMANE Server VM, multiple virtual interfaces are created, one per VLAN, which are then managed by EMANE. This configuration results in any traffic generated in the data interfaces of the TNs to be transferred to the corresponding virtual Ethernet interfaces inside the EMANE Server, where each interface is mapped to one NEM. At runtime, EMANE reads from each interface, applies the necessary communications effects, and writes the data out to the interfaces that should receive the data. The network shown in blue is for EMANE data (OTA and events) exchanged between the different physical servers. Finally, the network shown in red is the control network used by a user to log into the VMs, start/stop the experiments, and collect data.

The basic principle of this deployment model is to ensure that any data generated by one TN VM is isolated within a VLAN and is not directly seen by any other TN VM directly. Instead, the data is sent to the EMANE

Server VM, where the data will be consumed by EMANE. Once EMANE decides upon which other TN VMs that should receive that data, it is retransmitted on the appropriate VLAN(s) back to the TN VMs.

The following steps detail the process of configuring one or more ESXi servers to support this deployment model for Anglova. This document assumes that Version 6.5 of the ESXi server is utilized. The management screens shown are using the VSphere Client, and not the web-based interface (although it should be possible to use the web-based interface as well).

After a fresh install of ESXi, the VSphere Client should show something along the lines of Figure C-3. This particular server has 32 logical processors, so it could host up to 32 nodes in the Anglova scenario. Additional nodes could be deployed on additional servers (details later).

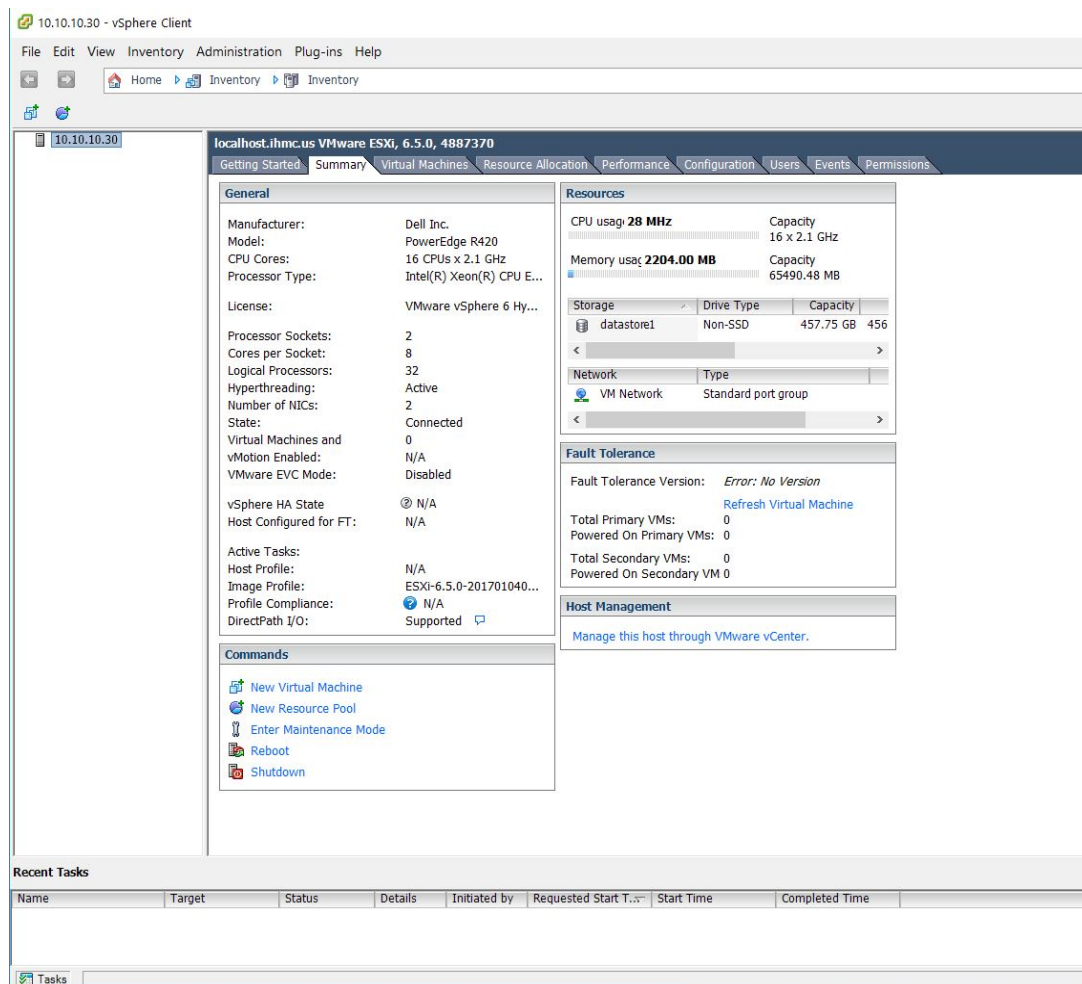


Figure C-3: VSphere Client View After Installation of ESXi Server.

An important part of configuring the ESXi server is setting up the virtual switches and VLANs within the server in order to replicate a topology like the one shown in Figure C-2. Within the VSphere Client, this is accomplished by first selecting the server (10.10.10.30 in this case), clicking on the Configuration tab, and then selecting the Networking option. The Add Networking option is then used to create a new Virtual Switch, of type vSphere Standard Switch, as shown in Figure C-4.

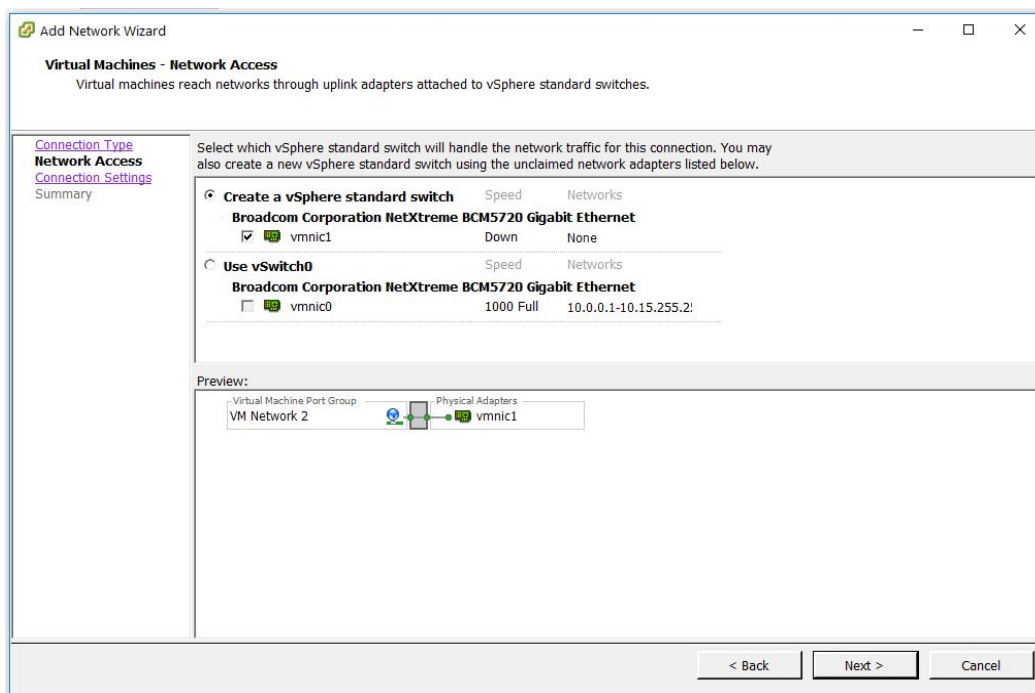


Figure C-4: Creating a vSphere Standard Switch Within ESXi.

Two virtual switches need to be created; the first one for all the VLANs for each VM and the VLAN trunk – called EMANETrunk, and the second one for EMANEData, which allows a multi-server EMANE installation. The EMANETrunk is a trunk for all of the VLANs used by the different TN VMs to transfer data to/from the EMANEServer VM. As shown in Figure C-5, the VLAN ID for this virtual switch should be set to ALL. Note that this particular virtual switch does not need to be connected to a physical Ethernet network, as it only needs to be connected to VMs internal to the server.

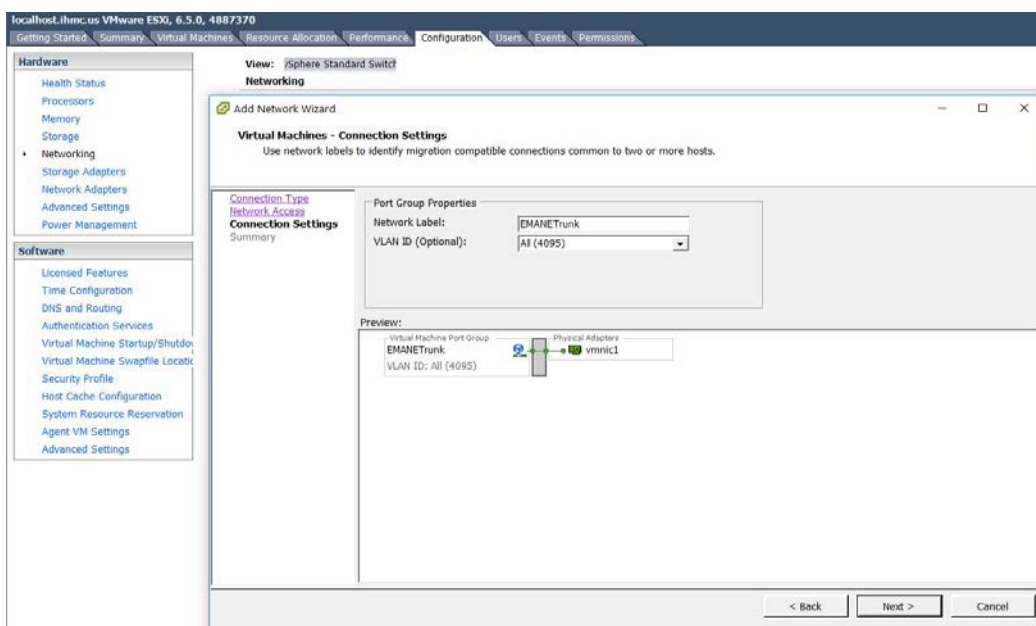


Figure C-5: Configuring the VLAN for the EMANETrunk Virtual Switch.

It is important that the security properties of the EMANETrunk switch are configured to allow Promiscuous Mode. This configuration is set in the Security tab of the EMANETrunk Properties dialog and is shown in Figure C-6.

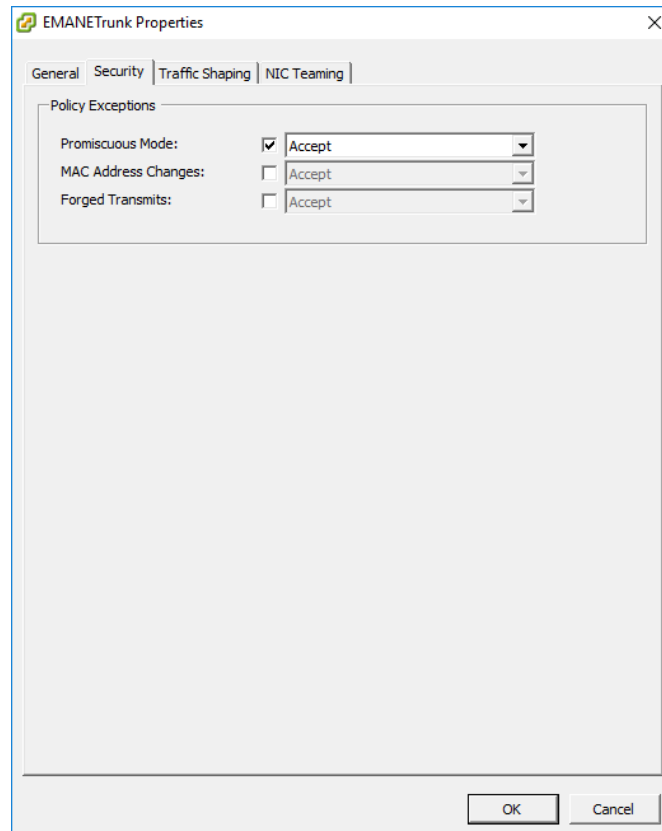


Figure C-6: Configuring Security Properties for EMANETrunk.

The next step is to add VLANs for each TN VM to the same virtual switch. In this example, the VLANs are numbered starting at 100 and in increments of 10 for each test VM. This provides room to add additional VLANs later in case a VM needs multiple interfaces (as some do within the Anglova scenario). Figure C-7 shows the configuration screen for ESXi after deploying EMANE within a VM named EMANEServer and twelve VMs that represent the first twelve nodes of Company 1 within the Anglova scenario. Note that all the VLANs show up as interfaces that can be assigned to specific VMs being deployed on the server.

Another vSphere virtual switch needs to be created for EMANEDData. This is only required if the test VMs will span multiple physical servers, and there will be multiple EMANEServer VMs to handle all of the VMs. The EMANEDData network needs to be connected to a physical network (as shown in Figure C-2), so that EMANE can pass the Over The Air (OTA) traffic between the multiple EMANE VMs on each physical server. Creation of this virtual switch is shown in Figure C-8.

Each of the deployed test VMs need to have two network interfaces. The first interface must be connected to a unique VLAN, which will guarantee that its network traffic will only be sent to the corresponding NEM in the EMANEServer. The second, control interface, is connected to the VM Network, which is typically used to be able to log into the VM and otherwise communicate with it. Applications that are being evaluated need to be configured to transmit their traffic on the test VLAN interfaces and not on the control interface. An example of this configuration for the first node in the first company in the Anglova scenario is shown in Figure C-9.

ANNEX C – EXPERIMENTATION ENVIRONMENT AND TOOLS

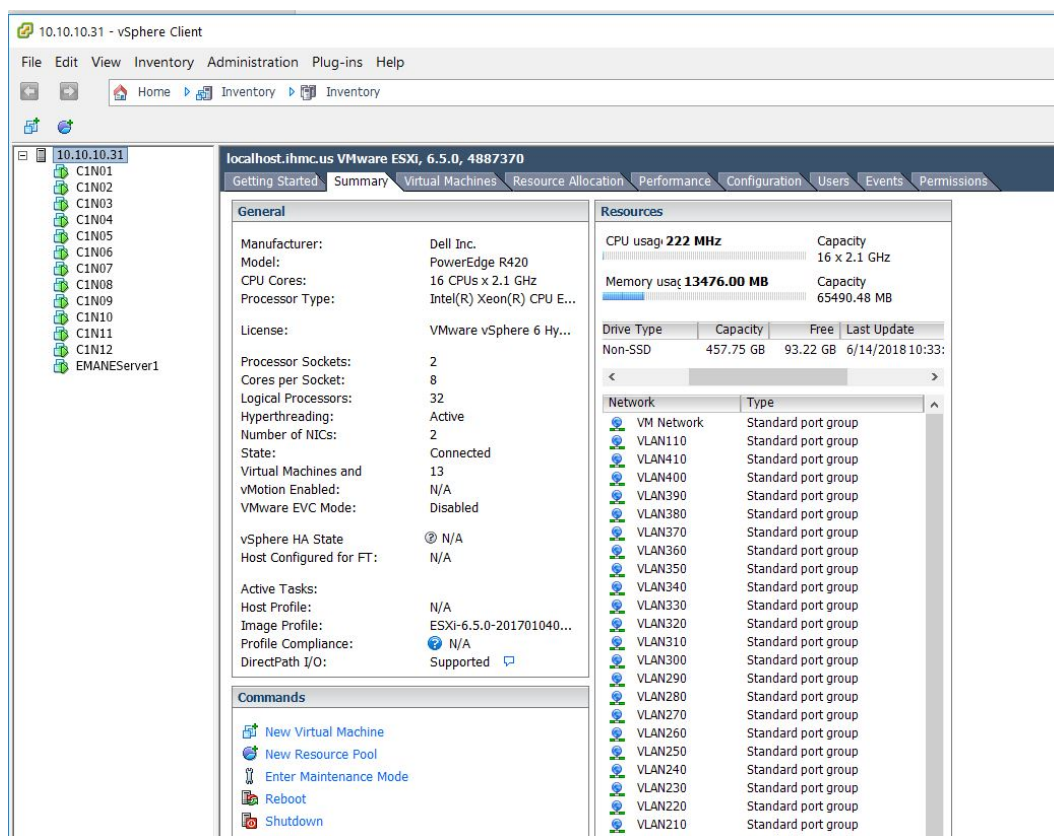


Figure C-7: Status of ESXi Server After Installation of EMANEServer VM and 12 Nodes.

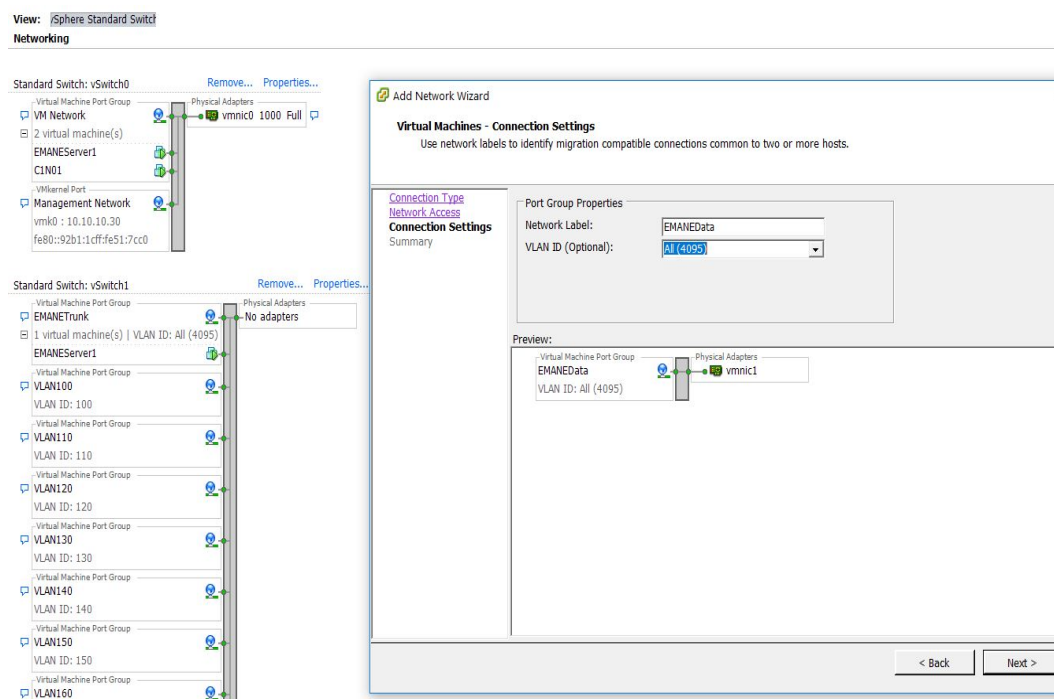


Figure C-8: Creating Another vSphere Switch and Network for the EMANE Over The Air (OTA) Traffic.

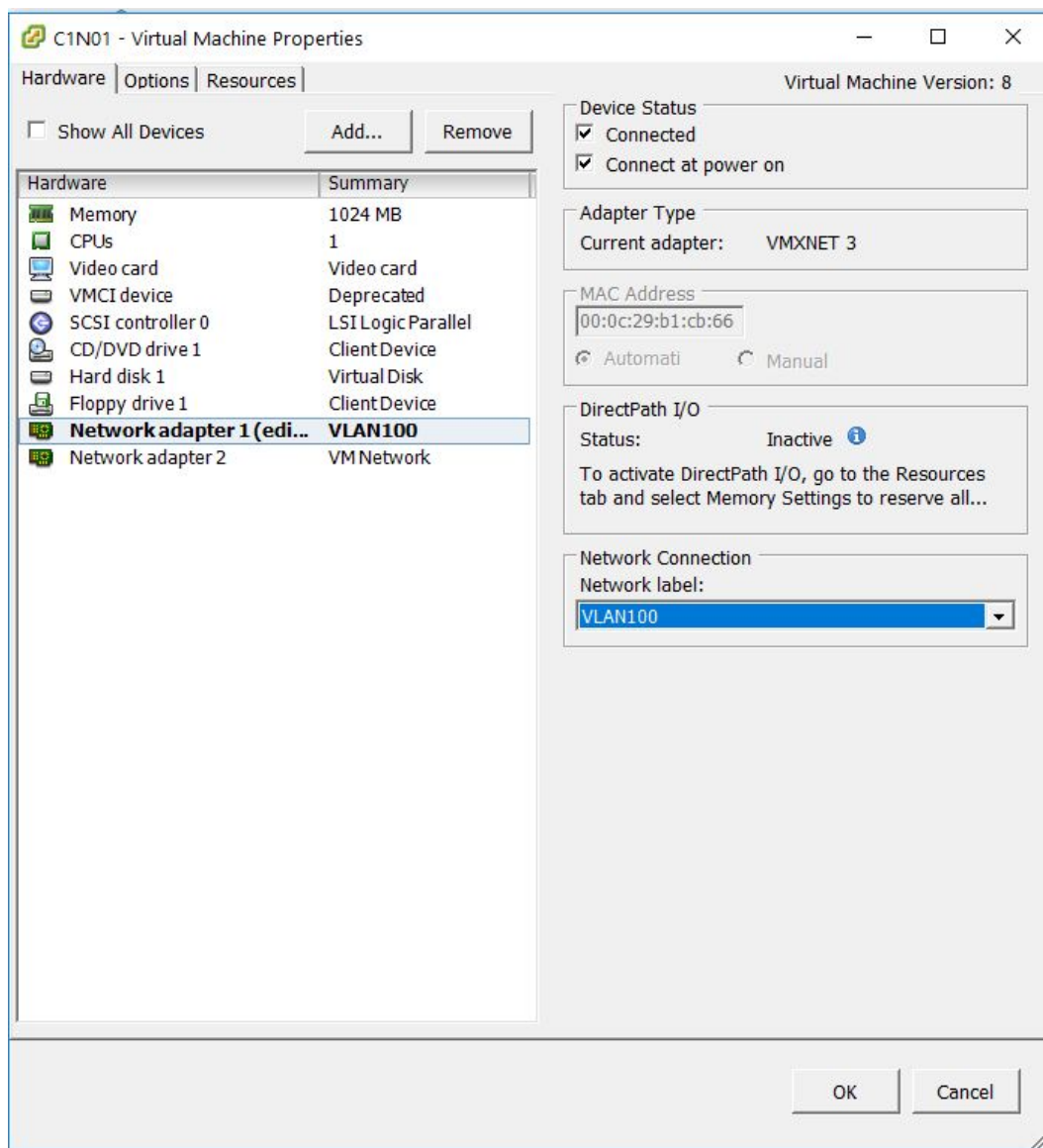


Figure C-9: Assigning Appropriate Networks to the Test VM Interfaces.

Finally, the EMANEServer needs to be assigned three interfaces:

- The VM Network (for control);
- The EMANetrunk (for all of the TN VM traffic); and
- The EMANEdat (to communicate with other EMANEServers running on other physical machines).

This is shown in Figure C-10.

Lastly, an IP address scheme must be developed and assigned to each of these interfaces. As an example, the control interfaces for each VM could be assigned an IP such as 10.0.12.x, where x is unique for each VM. Each of the data interfaces could be assigned an IP in the 192.168.x.y range, where x represents a company within the Anglova scenario and the y represents a node within the company. The protocols/service to be tested must be configured to use the 192.168.x.y networks for data exchange.

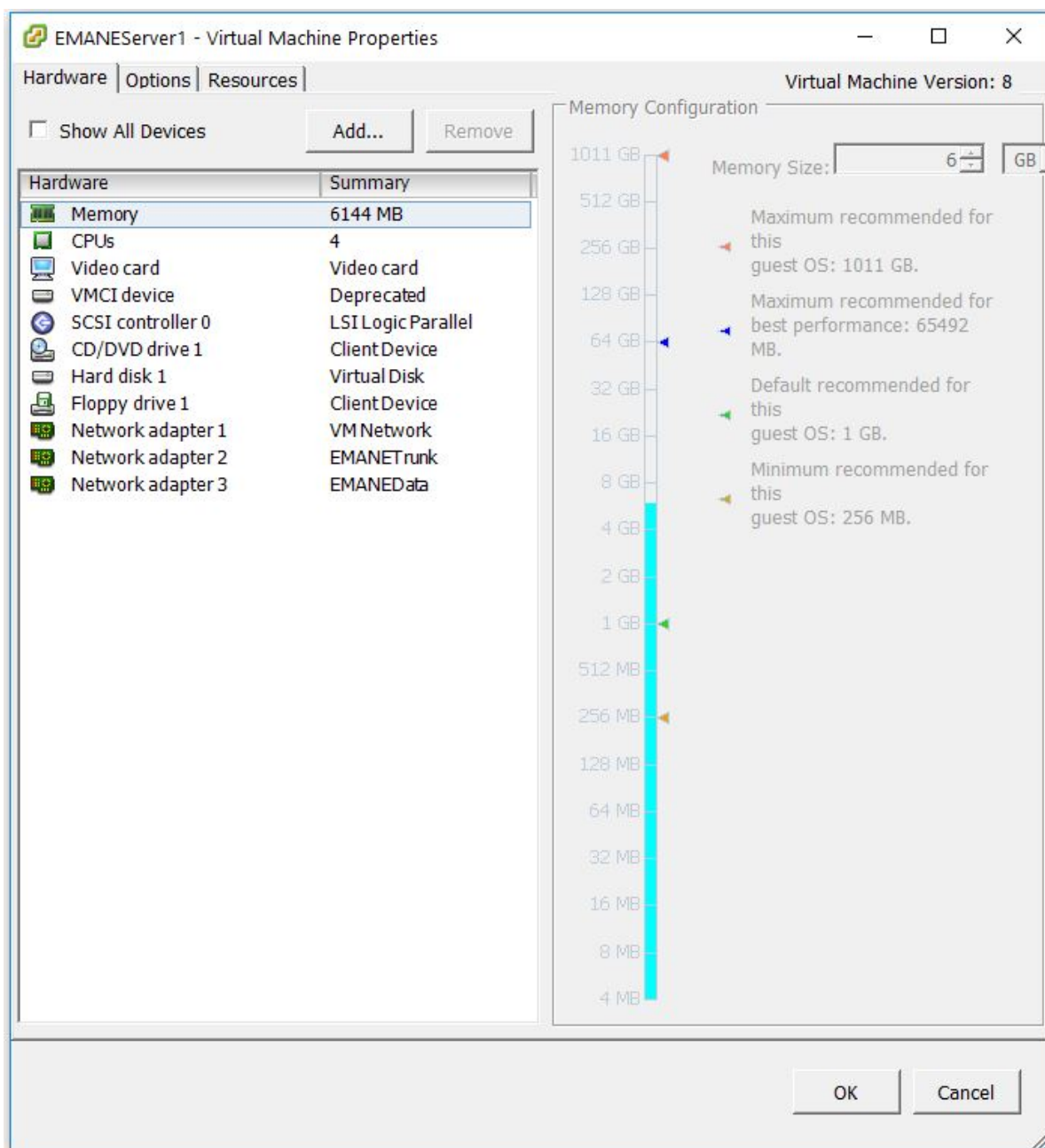


Figure C-10: Configuration of Networks for the EMANEServer VM.

C.4 VISUALIZATION TOOLS

C.4.1 Scripted Display Tools 3D (SDT-3D)

One method to visualize the Anglova scenario is by using the Scripted Display Tools (SDT-3D) and the EMANE SDT-3D client/server framework. The Scripted Display Tools (Figure C-11) are open source software developed by the Naval Research Laboratory (NRL) Protocol Engineering Advanced Networking (PROTEAN) group. SDT-3D provides real-time visualization of dynamic mobile data communication networks [6].



Figure C-11: Scripted Display Tools (SDT-3D).

The EMANE SDT-3D client/server framework (Figure C-12) enables the sending of visualization scripting commands to a running instance of SDT-3D to visualize a running EMANE emulation in real-time. The EMANE SDT-3D client reads location and network connectivity from the EMANE software and sends that information to the EMANE SDT-3D server. The EMANE SDT-3D server uses this information to generate and send SDT-3D scripting commands to visualize the running emulation.

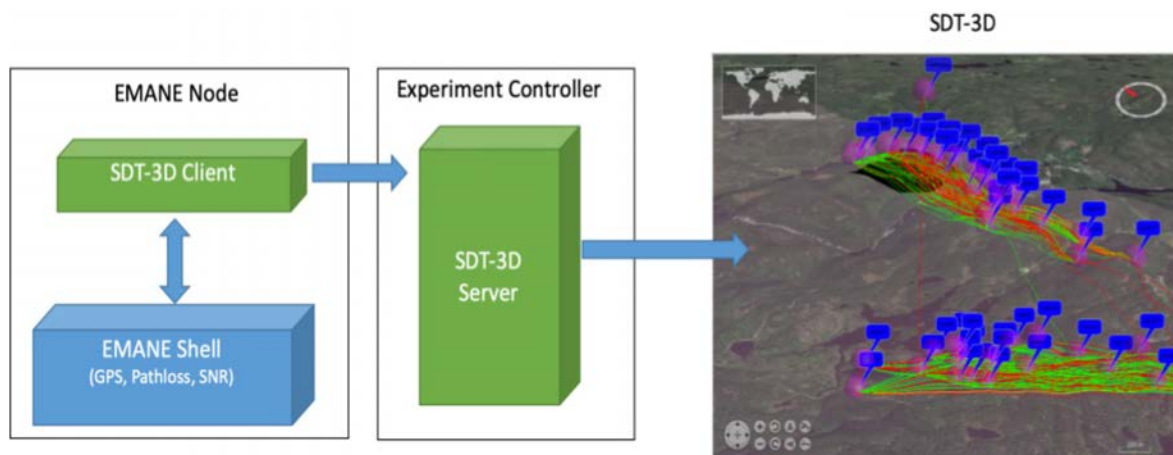


Figure C-12: EMANE SDT-3D Visualization Client/Server Framework.

Using SDT-3D and the EMANE SDT-3D client/server framework, the Anglova scenario's emulated nodes and their mobility, links and connectivity are drawn and updated dynamically on a NASA Whirlwind geographic background (Figure C-13).

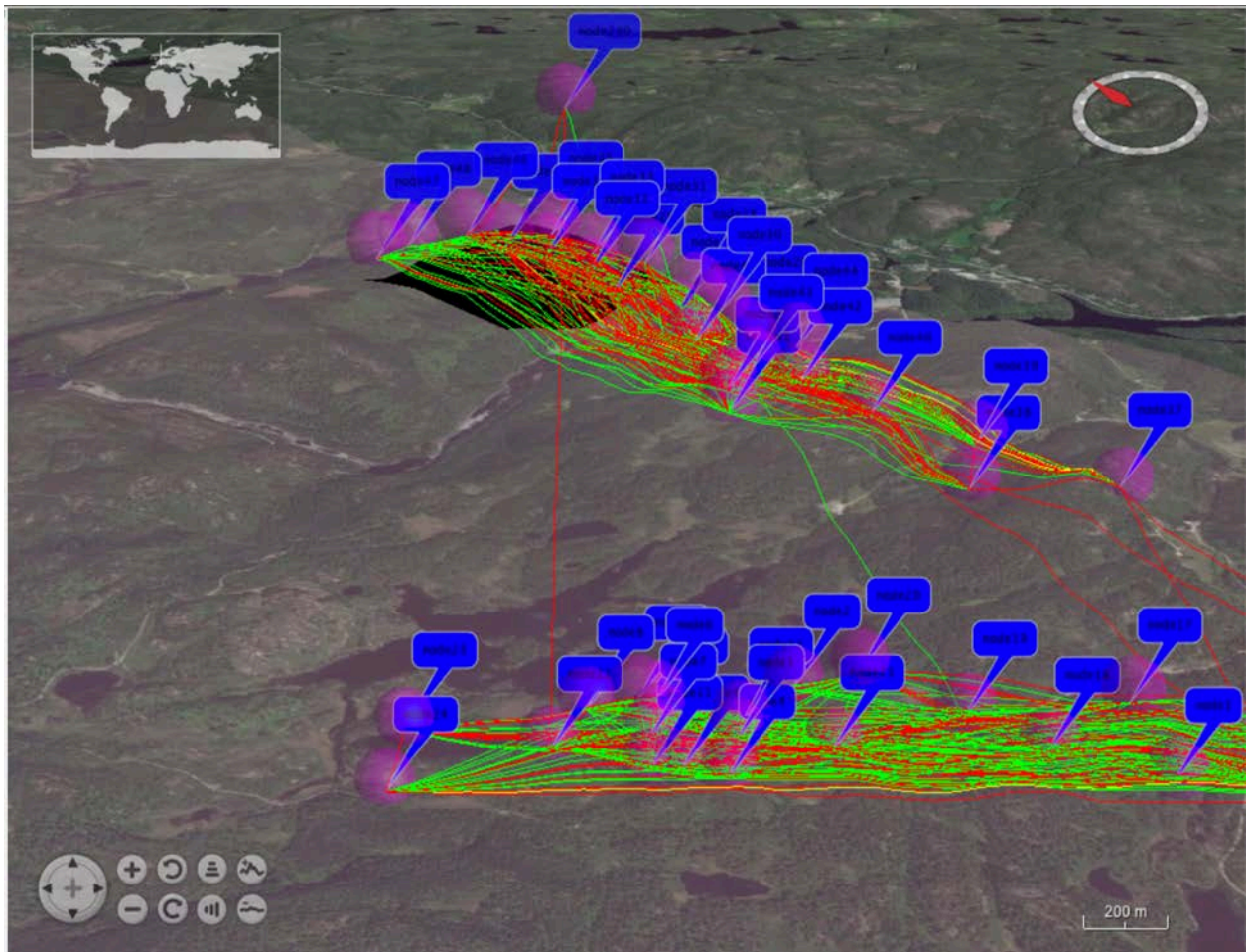


Figure C-13: Anglova Scenario Emulation Visualization in SDT-3D.

C.4.2 Mirage

Mirage is a tactical 3D visualizer based on the NASA World Wind library for Java. World Wind Java is a Software Development Kit (SDK) that adopts a set of OpenGL libraries for rendering. Mirage supports custom maps and tiles while being able to overlay NASA and United States Geological Survey (USGS) satellite imagery, topographic maps, aerial photography, Keyhole Markup Language (KML), and Collada files.

Users can interact with the 3D representation of the earth by rotating it, tilting the view, and zooming in and out. Mirage is able to display different kinds of data, from MIL-STD-2525 standard objects (Tracks, Graphical Shapes, etc.) to place names, political boundaries, latitude/longitude lines, and so forth. Mirage is able to receive real-time updates and notifications from a variety of data sources.

As part of developing the Anglova scenario, the task group also integrated the OpenStreetMap dataset and the EMANE events so that Mirage can be used to display the scenario as it is played during the course of an experiment.

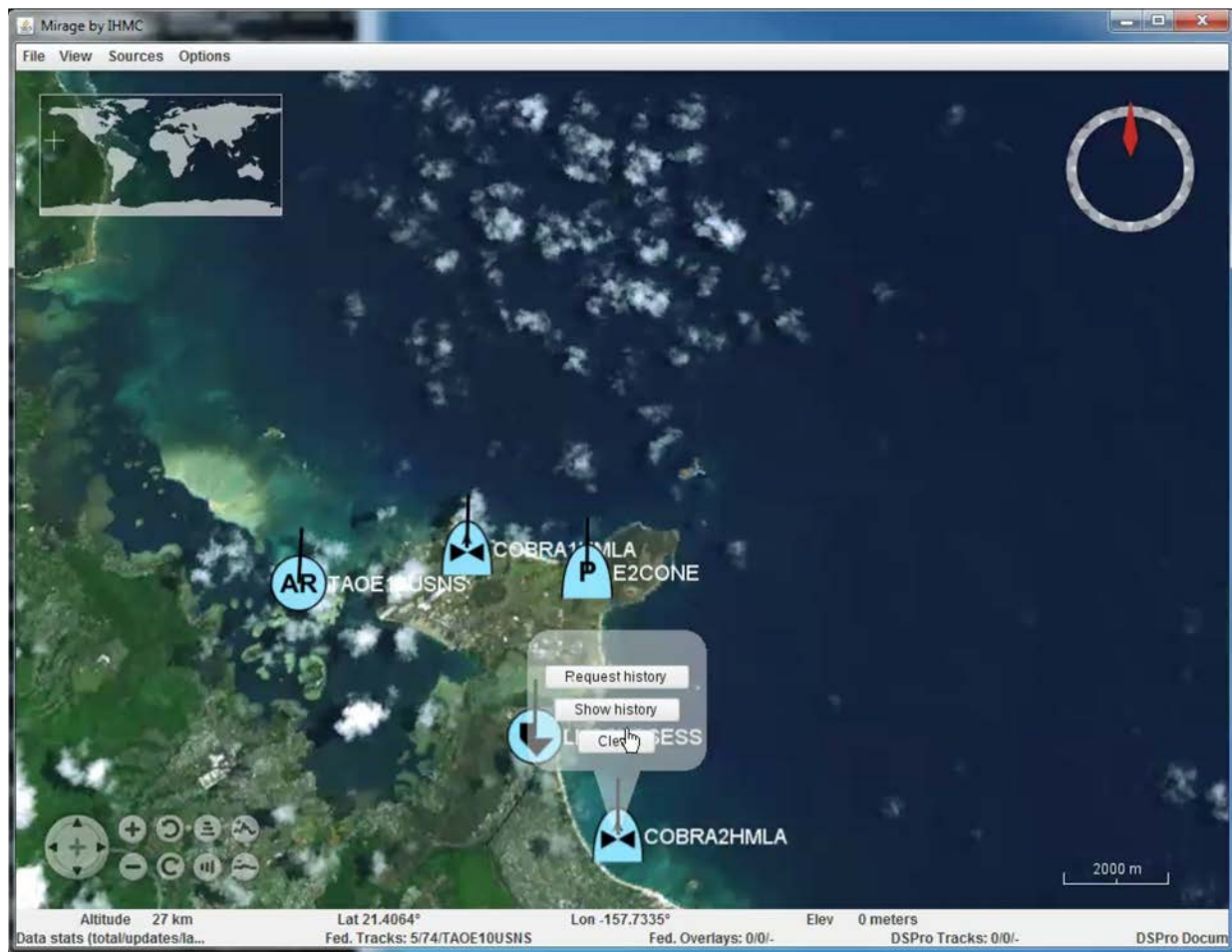


Figure C-14: Mirage Visualizer.

C.4.3 OpenStreetMap Dataset

The original location from where parts of the Anglova scenario traces were obtained was considered sensitive, resulting in the location data being anonymized and relocated to an area near Kristiansand in Norway. The coordinates were recalculated by taking Earth curvature into account so that distances were maintained within the scenario area. Actual destination location was decided based on matching topographical features. However, a drawback with relocation or movement patterns was that visualization tools could not realistically depict the movement of the vehicles over a map, as the movement would not match roadways and other elements of the terrain. As a result, the IST-124 RTG decided to generate new map data that could be used by a visualization tool while showing the movement of nodes within the Anglova scenario.

The relocated area is under web tile map tile $x = 133$, $y = 76$ on zoom level 8, coordinates (58.1298N, 7.60E) – (58.502N, 8.095E). Using the Overpass API, a slightly larger area from OpenStreetMap database was downloaded. Because of some large features this area was actually (57.74N, 6.66E) – (58.88N, 9.35E). The original area where the scenario takes place was downloaded from OpenStreetMap (OSM). Coordinates from the original area were transformed. Also all names within that dataset were transformed to Scandinavian-sounding names to hide the origin. All these modifications were simple to perform as OpenStreetMap data is XML-based and well documented, such that text-based tools could be utilized.

The two datasets were loaded into JOSM editor [7]. The section of the original terrain north of Kristiansand was removed. The terrain of the relocated scenario replaced the original terrain and then some map features, most notably the road network and waterways within scenario, were connected to surrounding areas with some artistic freedom.

After the OSM data was completed, new map tiles covering the modified area were generated. The data was imported to Postgres database with GIS extension. Map tiles were generated using litesrv renderer with OpenStreetMap Carto style as in April 2016.

The tiles are hosted at a server operated by Aalto University. Preview of the map can be seen by visiting <https://www.anglova.net/>. To view the modified tiles that represents the Anglova terrain within an application, the URL of <https://tile.anglova.net/{z}/{x}/{y}.png> can be used. The {x}, etc. placeholders should be replaced with application-specific ones. The format is identical to the one OpenStreetMap uses for its tile servers. All generated tiles (size 1.7 GiB) can be downloaded from <https://tile.anglova.net/ist124.tiles.tar.gz> for local hosting. As both the map style and map data are evolving documents there may be discontinuity at the border areas of the modified tiles.

However, many GIS and visualization applications, including the Worldwind component of SDT3D, do not support tile maps but only Open Geospatial Consortium (OGC) Web Map Service (WMS). For this reason, a WMS service is available at <https://wms.anglova.net/wms> supporting WMS versions 1.0.0, 1.1.1, and 1.3.0. The Anglova scenario imagery is available on the “ist124” layer. The site <https://www.anglova.net> contains instructions of how to configure the service into various GIS software, including SDT3D.

The modified tiles provides the correct map data to be used with tools to render the Anglova scenario environment. However, as yet, there is no areal imagery to match the modified map area. This is under study and possible options are being explored.

C.5 SCENARIO PLAYBACK TOOLS

C.5.1 EMANE Event Service Tool

In order for the Anglova scenario to progress, each node must receive the location and path loss events for each time step in the scenario. The EMANE event service is responsible for generating mobility and pathloss events for each node running within the Anglova scenario emulation. The EMANE event service takes as its input several XML configuration files as well as event files in Emulation Event Log (EEL) format and multicasts these events over a shared network channel accessible by each emulated node. Each node runs the EMANE event daemon which listens to and receives events from the event multicast channel. The event daemon’s remaining role is to make events available to ‘application space’ by means of its ‘agent’ plug-ins such as the GPSd location agent. This agent is responsible for making location events available as National Marine Electronics Association (NMEA) sentences, which can serve as input to user applications (e.g., GPSd, the GPS daemon) running on the node. The EMANE event service tool’s XML files are discussed below.

C.5.1.1 Event Service XML

The event service XML configuration file (Figure C-15) defines the multicast channel and interface where events will be published. It also defines the EEL generator configuration file, which contains the event parser and multicast channel configurations.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE eventservice SYSTEM "file:///usr/share/eman/dtd/eventservice.dtd">
<eventservice>
  <param name="eventservicegroup" value="224.1.2.8:45703"/>
  <param name="eventservicedevice" value="eth1"/>
  <generator definition="eelgenerator_vignette3_part1.xml"/>
</eventservice>
```

Figure C-15: Example Event Service Configuration File.

C.5.1.2 EEL Generator XML

The EEL generator configuration file (Figure C-16) defines the source EEL event file and the various parser plug-ins that will be used to parse sentences from the EEL event file.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE eventgenerator SYSTEM "file:///usr/share/eman/dtd/eventgenerator.dtd">
<eventgenerator library="eelgenerator">
  <param name="inputfile" value="vignette3_part1.eel" />
  <paramlist name="loader">
    <item value="commeffect:eelloadercommeffect:delta"/>
    <item value="location,velocity,orientation:eelloaderlocation:delta"/>
    <item value="pathloss:eelloaderpathloss:delta"/>
    <item value="antennaprofile:eelloaderantennaprofile:delta"/>
  </paramlist>
</eventgenerator>
```

Figure C-16: Example EEL Generator Configuration File.

C.5.1.3 EEL Source File

Mobility and pathloss events are stored in and parsed from EEL source files (Figure C-17). These files consist of time stamped entries for each node's GPS location (latitude, longitude, altitude) as well as time stamped entries for the pathloss values between the nodes. Mobility and pathloss events may be combined into a single file or separated into individual files.

```
0.0 nem:12350 location gps 58.170309,7.944924,2.0
0.0 nem:12350 pathloss nem:12550,0.0 nem:12650,0.0 nem:12700,0.0 nem:12750,0.0 nem:12800,0.0 nem:12850,0.0 nem:12900,0.0 nem:12950,0.0 nem:13000,0.0 nem:13050,0.0
0.0 nem:13100,26.2 nem:13150,26.2 nem:13250,26.2 nem:13300,26.2 nem:13350,26.2 nem:13400,26.2 nem:13450,26.2 nem:13500,26.2 nem:13550,26.2 nem:13600,26.2 nem:13650,26.2 nem:13700,0.0 nem:13760,26.2
0.0 nem:12400 location gps 58.170309,7.944924,2.0
0.0 nem:12400 pathloss nem:12600,0.0 nem:13200,10.7 nem:13850,17.3 nem:14100,17.3 nem:14700,17.3 nem:15350,19.5 nem:15550,19.5 nem:16150,10.7
0.0 nem:12450 location gps 58.170309,7.944924,2.0
0.0 nem:12450 pathloss nem:13900,32.9 nem:15400,35.0
0.0 nem:12500 location gps 58.170309,7.944924,2.0
0.0 nem:12500 pathloss nem:13740,0.0 nem:13775,10.7 nem:14000,17.3 nem:15180,17.3 nem:15250,17.3 nem:15450,19.5 nem:16680,19.5 nem:16750,10.7 nem:16800,55.9
0.0 nem:12550 location gps 58.170309,7.944924,2.0
0.0 nem:12550 pathloss nem:12350,0.0 nem:12650,0.0 nem:12700,0.0 nem:12750,0.0 nem:12800,0.0 nem:12850,0.0 nem:12900,0.0 nem:12950,0.0 nem:13000,0.0 nem:13050,0.0 nem:13100,26.2 nem:13150,26.2 nem:13250,26.2 nem:13300,26.2 nem:13350,26.2 nem:13400,26.2 nem:13450,26.2 nem:13500,26.2 nem:13550,26.2 nem:13600,26.2 nem:13650,26.2 nem:13700,0.0 nem:13760,26.2
```

Figure C-17: Example EEL File.

C.5.2 Anglova Scenario Player

As an alternative to playing back the scenario via EEL files and the EMANE Event Service Tool, we developed the Anglova scenario player, a Java-based graphical user interface, to load the scenario data files and generate the necessary EMANE events to drive the emulation. This player is showed in Figure C-18.

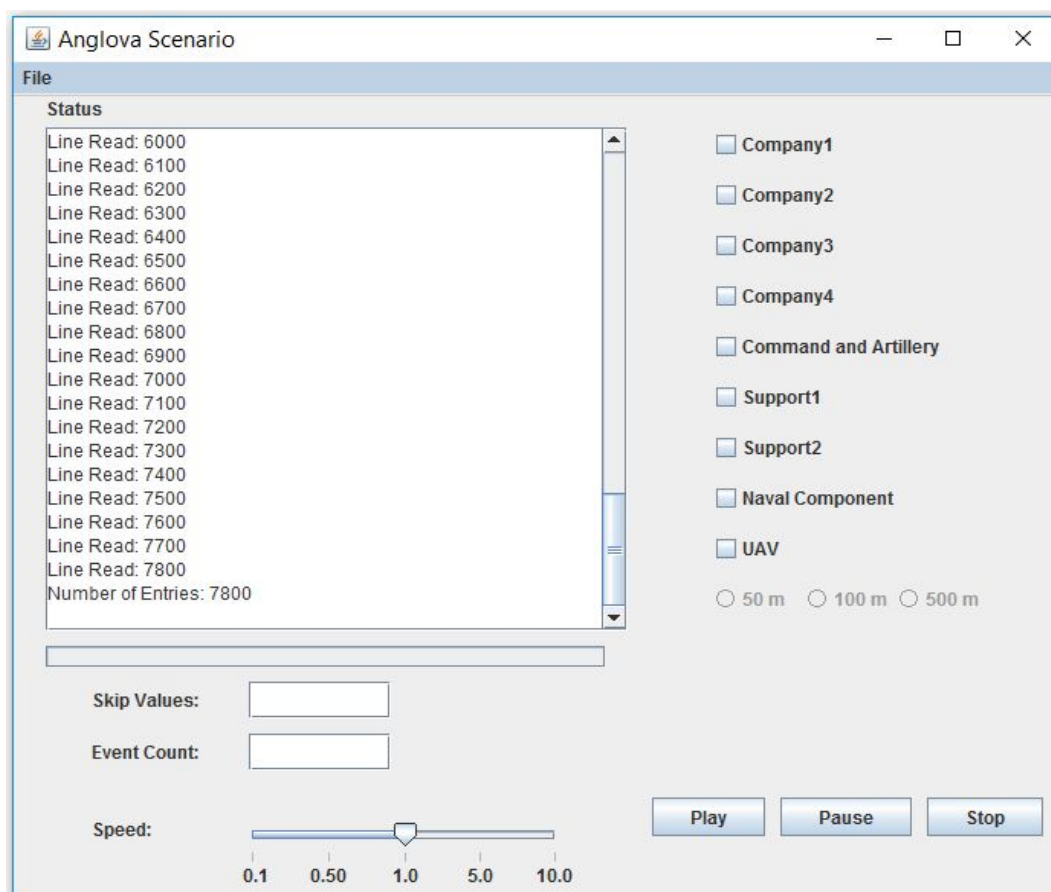


Figure C-18: Anglova Scenario Player.

The File menu item allows to load the pathloss and position files from the file system and shows the progress on the status window. Then, the events are generated by pressing the Play button. This process can be paused or stopped by using the other 2 buttons. The player also allows skipping values and counts the events that have been generated as well as regulate the speed at which the events are generated. The user can also select a subset of the companies, the naval component, and the Unmanned Aerial Vehicle (UAV), that are part of the scenario playback. For the UAV, it is also possible to select from three different altitudes. The status window provides updates about the progress of loading the event files and the playback of the scenario.

We developed some utility code in order to facilitate the generation of EMANE events to drive the emulation. EMANE receives the position and pathloss events for each node via messages that are encoded using Google ProtoBuf. This code leverages the ability to process .proto files to generate Java classes, where each class represents one event. The utility code and the underlying classes were packaged into a single .jar file so that it can provide an API for anyone wishing to generate and send EMANE events.

The following Java API describes all the steps for generating a pathloss event using the parameters target NEM id, a float array of the pathloss values, an integer array of NEM mapping, a sequence number and the uuid of the node.

The first step is generating the pathloss event builder and add the target NEM id:

```
Pathlossevent.PathlossEvent.Builder pathlossEventBuilder =
Pathlossevent.PathlossEvent.newBuilder();
```


The second step is adding the pathloss values between the target NEM and all the other NEMS, adding the pathloss values and then create a new builder:

```
Pathlossevent.PathlossEvent.Pathloss.Builder pathlossBuilder =  
Pathlossevent.PathlossEvent.Pathloss.newBuilder();  
pathlossBuilder.setNemId (nemMapping[i]);  
pathlossBuilder.setForwardPathlossdB (pathlossValues[i]);  
pathlossBuilder.setReversePathlossdB (pathlossValues[i]);  
pathlossEventBuilder.addPathlosses (pathlossBuilder);
```

Create a byte array:

```
ByteString pathlossEventBA =  
pathlossEventBuilder.build().toByteString();
```

Then we need to serialize the event by constructing a serial builder and setting the event id to 101 which is the identification for pathloss events that has to be manually set into a BasicEvent instance:

```
EMANEMessage.BasicEvent.Event.Data.Serialization.Builder  
serialBuilder = BasicEvent.Event.Data.Serialization.newBuilder();  
serialBuilder.setNemId (targetNEMId);  
serialBuilder.setEventId (101);  
serialBuilder.setData (pathlossEventBA);  
serialBuilder.build();
```

Create a Basic event builder:

```
EMANEMessage.BasicEvent.Event.Builder evtBuilder =  
EMANEMessage.BasicEvent.Event.newBuilder();  
evtBuilder.setUuid (uuid);  
evtBuilder.setSequenceNumber (seqNo);  
BasicEvent.Event.Data.Builder dataBuilder =  
BasicEvent.Event.Data.newBuilder();  
dataBuilder.addSerializations (serialBuilder);  
BasicEvent.Event.Data data = dataBuilder.build();
```

Convert it to a byte array, compute the length of the event and prepends the network packet with 2 bytes:

```
byte[] fullDataByteArray = evtBuilder.setData  
(data).build().toByteArray();  
int arrayLen = fullDataByteArray.length;  
byte[] newbuf = new byte [fullDataByteArray.length + 2];  
ByteBuffer bb = ByteBuffer.wrap (newbuf);  
bb.putShort ((short) arrayLen);  
bb.put (fullDataByteArray);
```

The last step is to create a datagram packet and send it over the EMANE event channel via UDP multicast:

```
MulticastSocket multicastSock = new MulticastSocket (45703);
DatagramPacket dp = new DatagramPacket (newbuf, newbuf.length,
_group, 45703);
multicastSock.send (dp);
```

These network packets are picked up by the EMANE Network Emulation Modules (NEMs), which then interpret the pathloss information to enforce the communications characteristics.

C.6 CUSTOMIZED PATHLOSS GENERATION TOOLS

We have also produced utility programs to generate pathloss data for some of the nodes within the Anglova scenario. Pathloss generation for the Naval Platforms in Vignette 2 and for all platforms in Vignette 3 is accomplished by using open source SPLAT! (an RF Signal Propagation, Loss, And Terrain analysis tool) [8] program using the Longley-Rice model. Location information can be generated from a motion plan template or from the locations previously entered into an EMANE Emulation (EEL) file. Antenna heights can be retrieved from the altitude information from the EEL file, or can be used as fixed antenna heights from a configuration file. Longley-Rice parameter data files are required for SPLAT! to determine RF path loss in either point-to-point or area prediction mode. Several parameter files can be specified to serve with each different network (frequency settings, relative permittivity, earth conductivity, etc.) to cope with over the sea or land communication conditions. Topographic data can be imported from various sources. Significantly better resolution and accuracy can be obtained through the use of Shuttle Radar Topography Mission-3 (SRTM-3) Version 2 digital elevation models. We have used 3-arc second SRTM data which is publicly available for over the land calculations. Ground clutter can be specified as an input parameter to pathloss generation process, we have used 30 feet average ground clutter to better simulate the effects of ground structure for over the land pathloss calculations.

While the pathloss calculations give pretty realistic results for the naval platforms and sensor network, problems occurred when calculating pathloss generation of very close units such as trucks moving in a convoy or infantry. Because the Longley-Rice (ITM) model did not give us results for objects closer than 176 meters, we have assumed 0 dB pathloss for those platforms. Also lack of exact terrain models prevented us from calculating realistic pathloss values which take into account obscuration due to buildings, plants, etc.

In particular, we developed a utility program called “ScenGenFromFile” and used it to provide recalculated path loss (as described above) as part of the Anglova scenario. The utility program is being made available with the distribution package of the IST-124 emulation environment. It can use a network plan (network_plan.csv – excel file saved as csv format) file as an input as maintained by IST-124 group to show the platforms, networks and connectivity requirements among those networks by assigning a radio (nem id is shown in green background) for the required networks as shown in Table C-1.

Table C-1: Sample Network Plan File.

id	Group	wideband1	wideband2	wideband3	wideband4	narrowband1
network	Subnets	192.168.1.0	192.168.2.0	192.168.3.0	192.168.4.0	192.168.5.0
1	company1	1	0	0	0	50
2	company1	100	0	0	0	150
3	company1	200	0	0	0	0
4	company1	250	0	0	0	0
5	company1	300	0	0	0	0
6	company1	350	0	0	0	0

id	Group	wideband1	wideband2	wideband3	wideband4	narrowband1
7	company1	400	0	0	0	0
8	company1	450	0	0	0	0
9	company1	500	0	0	0	0
10	company1	550	0	0	0	0
11	company1	600	0	0	0	0
12	company1	650	0	0	0	0
13	company1	700	0	0	0	0
14	company1	800	0	0	0	0
15	company1	850	0	0	0	0
16	company1	900	0	0	0	0
17	company1	1000	0	0	0	0
18	company1	1050	0	0	0	0
19	company1	1100	0	0	0	0
20	company1	1200	0	0	0	0
21	company1	1250	0	0	0	0
22	company1	1300	0	0	0	0
23	company1	1400	0	0	0	0
24	company1	1450	0	0	0	0
25	company2	0	1500	0	0	1550
26	company2	0	2000	0	0	2050
27	company2	0	2100	0	0	0

In this plan the leftmost “id” column corresponds to the platform depicted by that id and the green cells represents the nem id for each specific network that is deployed on the platform.

In order to generate the pathloss information the antenna heights are to be specified. The antenna heights can be fixed or variable length as some platforms may hover up and down during the scenario. The antenna height information is handled as follows. The altitude information is the mobility file location event can be used an antenna height and a platform_conf.xls file can depict default platform heights if the former information does not exist.

In this setup, the default minimum antenna heights are taken from the platform_conf.csv (excel file saved as csv format) configuration file and if a location event with higher antenna height is seen at the mobility file it is accepted as the current antenna height (see Table C-2).

Table C-2: Sample Program Configuration Initialization File.

#ID	TYPE	IMAGE	NAME	NETWORK	ANTENNA HEIGHT (meters)
1	Truck	truck	company1	0	3
2	Truck	truck	company1	0	3
3	Truck	truck	company1	0	3
4	Truck	truck	company1	0	3
5	Truck	truck	company1	0	3
6	Truck	truck	company1	0	3

#ID	TYPE	IMAGE	NAME	NETWORK	ANTENNA HEIGHT (meters)
7	Truck	truck	company1	0	3
8	Truck	truck	company1	0	3
9	Truck	truck	company1	0	3
10	Truck	truck	company1	0	3
11	Truck	truck	company1	0	3
12	Truck	truck	company1	0	3
13	Truck	truck	company1	0	3
14	Truck	truck	company1	0	3
15	Truck	truck	company1	0	3

The #ID column must match the platform ids at the network plan and the other columns are used for SDT3D visualization.

SPLAT! requires Longley-Rice model Parameter files (LRP files) for each network in order to calculate pathloss information according to the model. These files should be prepared and named as “splat_<n>.lrp” file where n is the network number in the network plan where 1 is the leftmost network column (n = 1 is wideband1, n = 2 is wideband2, ... n = 14 navy uhf, etc.) in the network plan. The contents of these files are depicted in the SPLAT! Documentation [8].

A sample LRP file is shown below:

```

5.000      ; Earth Dielectric Constant (Relative permittivity)
0.001      ; Earth Conductivity (Siemens per meter)
301.000    ; Atmospheric Bending Constant (N-Units)
300.000    ; Frequency in MHz (20 MHz to 20 GHz)
6          ; Radio Climate
0          ; Polarization (0 = Horizontal, 1 = Vertical)
0.50       ; Fraction of Situations
0.50       ; Fraction of Time
0.00       ; Transmitter Effective Radiated Power in Watts or dBm (optional)

```

Please consult SPLAT! documentation for the meaning and use of this data.

Another input to the process is the topographic data .sdf files. The SPLAT! manual describes how to obtain these files, but some of the links are old or obsolete. In the current project we downloaded and used 3 arc seconds (90 m) Shuttle Radar Topography Mission (SRTM) data for the region of interest from the Web, by searching SRTM-3 via the internet. For example, webGIS internet site [9] can be used to obtain this kind of data.

The SRTM data can be changed to the format which the SPLAT! program understands by using srtm2sdf utility which comes with the SPLAT! Package [8].

Figure C-19 shows the outline of the directory structure of the provided utility program.

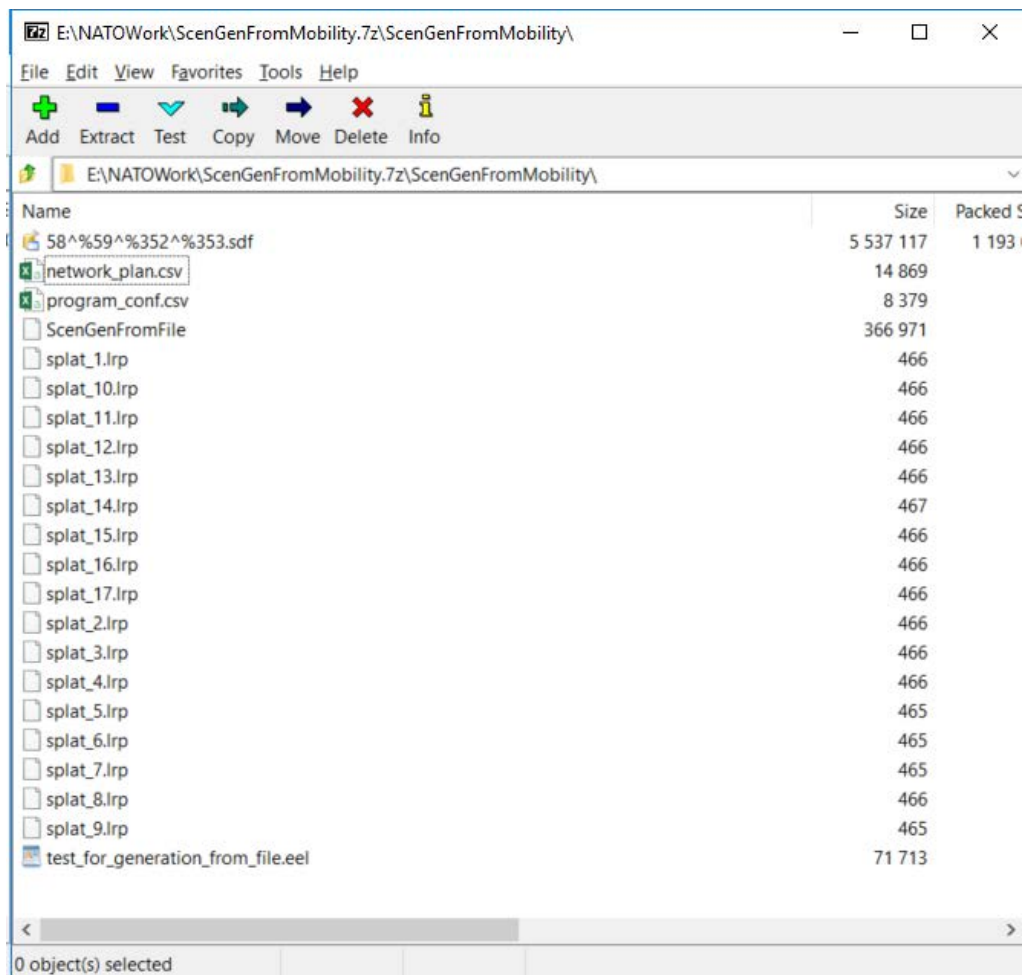


Figure C-19: ScenGenFromFile Utility Program Initial Directory Structure.

The program “ScenGenFromFile” is a Linux executable and tested to work with Centos 7 or Ubuntu 14. The file “test_for_generation_from_file.eel” is a sample input mobility file which contains mobility information of the platforms.

To use the utility program, type in the command shell:

```
./ScenGenFromFile <mobility_filename.eel>
```

The program outputs progress and when the execution finishes, the target EEL file is generated with the default name “generated_file.eel” in the same directory. The generated EEL file has the location events with altitude information as antenna height as explained before and pathloss events for all the nem ids depicted in the network plan. Sample output is shown below:

```
0.0 nem:17250 pathloss nem:17050,96.7 nem:17350,0.0 nem:17450,0.0 nem:17550,84.7
nem:17700,84.7 nem:17800,80.2 nem:17900,80.2 nem:18000,88.0 nem:18100,88.0 nem:18200,78.4
nem:18250,78.4 nem:18300,86.3 nem:18350,86.3 nem:18400,90.2 nem:18450,90.2 nem:18500,76.0
nem:18550,76.0 nem:18600,83.1 nem:18650,83.1 nem:18700,78.3 nem:18850,78.3 nem:20750,94.2

0.0 nem:17300 location gps 58.124413,8.035026,20.0
```

```
0.0 nem:17300 pathloss nem:17100,95.9 nem:17400,0.0 nem:17500,0.0 nem:17650,73.0
nem:17750,73.0 nem:17850,64.2 nem:17950,64.2 nem:18050,79.3 nem:18150,79.3 nem:18900,60.5
nem:20800,88.2
```

```
0.0 nem:17350 location gps 58.124413,8.035026,20.0
```

```
0.0 nem:17350 pathloss nem:17250,0.0 nem:17050,96.7 nem:17450,0.0 nem:17550,84.7
nem:17700,84.7 nem:17800,80.2 nem:17900,80.2 nem:18000,88.0 nem:18100,88.0 nem:18200,78.4
nem:18250,78.4 nem:18300,86.3 nem:18350,86.3 nem:18400,90.2 nem:18450,90.2 nem:18500,76.0
nem:18550,76.0 nem:18600,83.1 nem:18650,83.1 nem:18700,78.3 nem:18850,78.3 nem:20750,94.2
```

C.7 OPEN ISSUES

During the course of experimentation, four open issues were encountered with how we used EMANE in the Anglova scenario. This should be resolved with further work on the Anglova scenario. The first issue was with the RFPipe implementation of EMANE. In particular, the radio models for Anglova were first developed to use RFPipe. However, the RFPipe model, as configured and used in the Anglova scenario, does not implement any MAC algorithm and does not realize any interference effects. While the radio model allows the definition of a capacity limit as well as realize latency and reliability effects, multiple nodes are allowed to transmit at their individual rate limits and the receivers could receive, in aggregate, data rates higher than the capacity of the radio. Furthermore, RFPipe does not realize typical wireless communications effects such as hidden neighbors. RFPipe is good for point-to-point links, but cannot be used as-is for a radio network sharing a common channel.

Another issue with the radio models was discovered when using the TDMA model to emulate the narrowband links within the scenario. Unlike the RFPipe, the TDMA model includes a MAC and limits the data rates correctly. However, the TDMA implementation requires that all the NEMs using the TDMA model have synchronized clocks with an accuracy that is a function of the TDMA time slice. For the Anglova scenario, the accuracy of the Network Time Protocol (NTP) was insufficient for the TDMA model to work in a distributed deployment. The hybrid deployment works if the NEMs for all of the nodes that are part of a TDMA network are deployed within the same EMANE instance.

We observed the following issue with our reduced data rate modification of the 802.11abg model within EMANE: when multiple senders are transmitting at the maximum data rate to a single receiver, the incoming data rate at the receiver exceeds the maximum channel rate by a small fraction (as a function of the number of transmitters).

Finally, the last issue was with the EMANE event generation model, which allows a control application to generate events that control the emulation environment. These events are sent to the NEMs via UDP multicast. As mentioned earlier, the Anglova scenario has a playback component that generates the position and pathloss events to send to EMANE. Given the size of the Anglova scenario and the update rate of 1 Hz, the EMANE receiver seemed to be too slow to receive and process the events without losing some of the packets due to the UDP receive buffer being too small. This problem was solved by splitting the scenario into smaller subsets that were played back independently but still synchronized so that EMANE could support all the nodes simultaneously.

C.8 CONCLUSIONS

The Anglova scenario and all of the related files for setting up and running experiments using EMANE are available for download at <http://www.ihmc.us/nomads/scenarios> and also at <http://anglova.net>. For IST-124, having this common scenario has worked very well for efficient collaboration across multiple countries and

organizations, especially when hosted in a cloud environment with tools such as DAVC to setup experiments and provide access. We hope that the details provided in this annex are useful to other researchers that are interested in using the Anglova scenario for their own experimentation.

C.9 REFERENCES

- [1] AdjacentLink, LLC. Extendable Mobile Ad-hoc Network Emulator (EMANE). Internet: <https://github.com/adjacentlink/emane/wiki>, [May 8, 2017].
- [2] Marcus, K. and Cannata, J. Dynamically Allocated Virtual Clustering Management System. Proceedings of SPIE 8742, Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR IV, May 2013.
- [3] US Naval Research Laboratory. Multi-Generator (MGEN). Internet: <http://www.nrl.navy.mil/itd/ncs/products/mgen>, [May 5, 2017].
- [4] Optimized Link State Routing (OLSR). Internet: <http://www.olsr.org>, [May 5, 2017].
- [5] Marcus, K., Barz, C., Kirchhoff, J., Rogge, H., Nilsson, J., in't Velt, R., Suri, N., Hansson, A., Sterner, U., Hauge, M., Lee, K., Holtzer, A., Buchin, B. Peuhkuri, M., and Mısırlıoğlu, L., "Evaluation of the Scalability of OLSRv2 in an Emulated Realistic Military Scenario", Proceedings of the 2017 International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, 2017.
- [6] The Scripted Display Tools www.nrl.navy.mil/itd/ncs/products/sdt, [May 8, 2017].
- [7] JOSM extensible editor for OpenStreetMap (OSM). Internet: <http://josm.openstreetmap.de>, [May 8, 2017].
- [8] Magliacane, J., SPLAT! an RF Signal Propagation, Loss, And Terrain Analysis Tool. <http://www.qsl.net/kd2bd/splat.html>, [May 8, 2017].
- [9] WebGIS <http://www.webgis.com/srtm3.html>, [May 8, 2017].



Annex D – IST-124 EXPERIMENTATION EXECUTION

Kelvin Marcus

U.S. Army Research Laboratory (ARL)
UNITED STATES

NATO IST-124 RTG uses the US Army Research Laboratory's Dynamically Allocated Virtual Clustering Management System (DAVC) to deploy the Anglova scenario using the distributed EMANE emulation model [1]. In this emulation model the EMANE software is installed within VMs that execute the applications that are the subject of the experimentation and whose performance is being evaluated.

This annex is divided into 3 sections:

- Section D.1 details the steps required to launch the EMANE emulation of the IST-124-061 Anglova experimentation scenario within the DAVC environment.
- Section D.2 is a guide for DAVC system setup and configuration.
- Section D.3 is the DAVC user guide with step-by-step instructions to perform common DAVC operations to access and manage DAVC clusters, nodes, virtual hard disks, and persistent block storage.

D.1 EXPERIMENTATION EXECUTION

This portion of the annex provides guidance and instructions for executing the IST-124-RTG-061 experimentation environment. Specifically, it contains the instructions for executing the EMANE emulation for the 2nd and 3rd Anglova scenario vignettes. The first vignette has had the lowest priority in the group and is not fully modelled yet. For more information about the Anglova scenario and tools see:

- Annex A: "Operational Perspective for IST-124";
- Annex B "Emulation Based Experimentation and the Anglova Scenario"; and
- Annex C "Experimentation Environment and Tools".

D.1.1 Introduction

The IST-124-RTG-061 activity was focused on heterogeneous networks in the deployable and mobile tactical levels. A typical network can be illustrated with the scenario given in Figure D-1. This scenario was created to show the information needs and exemplify the challenges related to the heterogeneity of the network. The operational needs have been defined; tasks to be fulfilled, collaboration among organizational units, information management as well as communications, command and control systems used.

The scenario depicts an operation conducted by the company task forces of the mechanized battalion. They are part of the Military Contingent (MC) coordinated by the Coalition Head Quarter (HQ). The company Communications and Information System (CIS) is connected to the National Operational WAN and has access to the Coalition systems. The MC HQ plays the reach-back role during the operation and provides Combat Support (CS) and Combat Service Support (CSS) if requested. According to the operational context it is assumed that enemy's forces are preparing a complex attack against the coalition base from the village located in the operational zone. The enemies are well armoured and operate in an area which can be mined, so there is a chance of IED (Improvised Explosive Device) hazard. The task of the own forces is to move into the operational zone and neutralize the

insurgents and to destroy the armaments they collected. It is very important to avoid village inhabitants' casualties and to make the insurgents' escape impossible. The most important elements in this mission are CIS, logistics and medical support, which are provided by Coalition Forces. A well-functioning communication platform to help organizing the armed forces is therefore required.

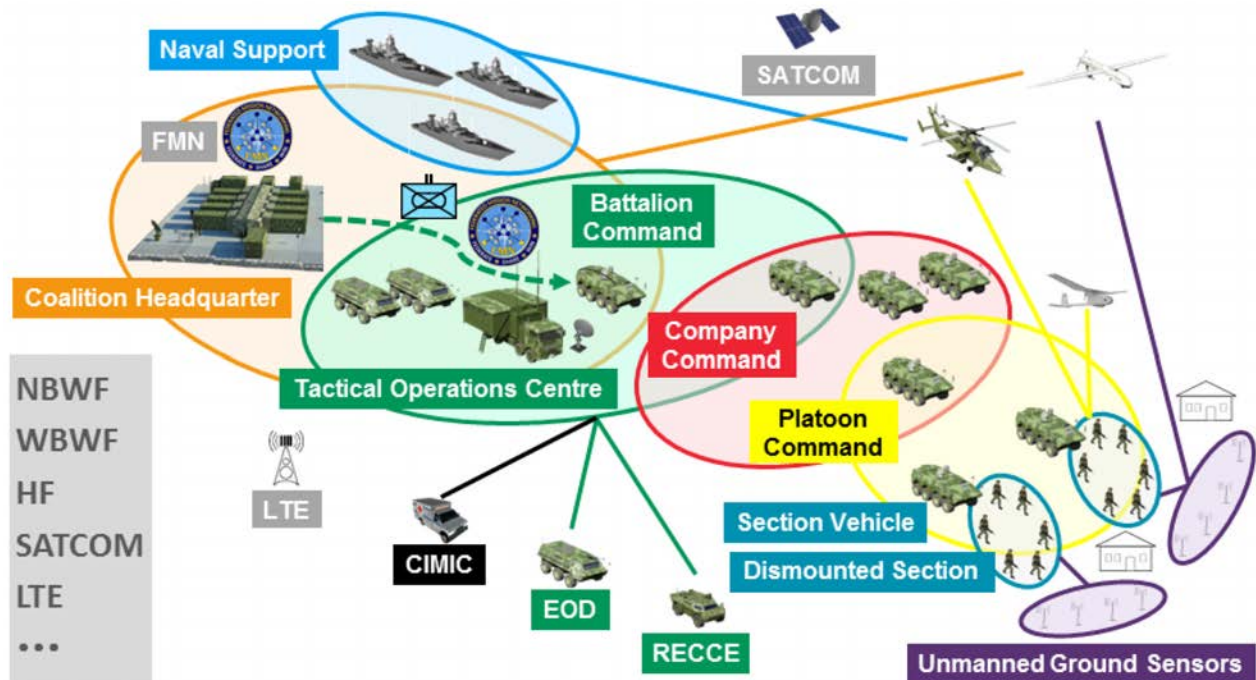


Figure D-1: Operational Scenario for IST-124 RTG-061.

The completion of the task mentioned requires access to a wide range of systems and communication networks, i.e., radio communications system (HF, VHF, UHF, SATCOM), sensor networks and Unmanned Aerial Vehicle (UAV) systems, NAVY management systems in terms of supporting reconnaissance and surveillance of the mission and services such as data, voice and video.

Three vignettes were defined in order to implement the actions included in the scenario. The roles and actors are the same for each vignette. The first vignette covers the intelligence preparation of the battlefield. The second vignette consists of the movement of coalition forces into the operational zone, including maritime interdiction operations in the surrounding coastal areas. The third vignette consists of an urban operation resulting in the neutralization of insurgents. The third vignette also includes a medical evacuation to a naval ship following the neutralization of IEDs. Each vignette describes data that are expected to be exchanged between the actors and C4ISR (Command, Control, Communications, and Computers Information System) equipment used in a way that emphasize the problems of connectivity and network efficiency of military heterogeneous networks.

D.1.2 Anglova Scenario

The Anglova scenario is a concrete realization of the operational context described above and depicts an operation conducted by a coalition task force including a maritime component. The tactical domain is located in the fictitious area of Fieldmont in Anglova, where the Coalition HQ (CHQ) of the Military Contingent (MC) is based. The scenario contains three vignettes as outlined in the operational context. However, the first vignette involving the Intelligence Preparation of the Battlefield has not yet been fully modelled.

The second vignette covers the deployment of the coalition forces, a battalion consisting of six companies, into the operational zone. The forces that are moving into the operational zone use a combination of narrowband VHF and wideband UHF connections for their own interoperability and operability with MC forces. The scenario includes detailed mobility patterns of the battalion north of Wellport in Anglova.

The battalion consists of six companies:

- Four mechanized companies with 24 vehicles each;
- One command and artillery company with 22 vehicles; and
- One support and supply company with 39 vehicles.

Together, there are 157 vehicles, each of them being a network node. The maritime component includes 21 ships and one multi-purpose helicopter that provides communications relays. In addition, a Coalition Headquarters node and an airborne node are also included in this vignette – a strategic UAV asset that can act as a communications relay and provide persistent surveillance capabilities.

The third vignette covers the urban counter-insurgency operation within the town of Wellport and involves three platoons (72 nodes), 10 unattended ground sensors, one aerial sensor (Aerostat), two UAVs (tactical and data harvest), three satellites, the 21 navy ships that are continuing the maritime mission, and the multi-purpose helicopter that is re-tasked for Medevac. The vignette is split into 3 parts which include neutralization of the insurgents and the IED, a Medevac from the urban environment to a naval ship, and the platoons returning to base.

The experimentation environment provides a common platform to explore research issues relevant to heterogeneous tactical networks including routing architectures and their impact on delivery rates, overheads, and scalability; data dissemination protocols; quality of service and resource management; and leveraging and integration of sensor networks. The instructions provided in this annex can be used as a guide to launch various subsets of the 269-node Anglova emulation scenario for a wide range of experimentation backdrops.

D.1.3 Experimentation Environment

The experimentation environment consists of the Dynamically Allocated Virtual Clustering (DAVC) management system, a customized Virtual Machine (VM) template preconfigured with the EMANE network emulator software, and scripting to launch vignettes 2 and 3 of the Anglova scenario.

D.1.3.1 Dynamically Allocated Virtual Clustering Management System (DAVC)

DAVC (Figure D-2) is a web based virtualization service and cloud-operating environment that creates complex virtual experimentation clusters that can be used for simulation-based, emulation-based, and hybrid field/emulation experimentation. DAVC deploys networked clusters composed of VMs tailored to user specifications. The DAVC management system abstracts away test-bed infrastructure configuration through automated provisioning processes that configure the virtual networking for each VM. Clusters created by DAVC are heterogeneous, so each VM can have different OSs, application sets, and hardware attributes such as RAM, CPU cores, hard disk, and network interfaces. DAVC users can register custom VMs as templates that can be used within their experimentation clusters.

Using DAVC, the Anglova scenario is distributed with a 1-to-1 mapping with each Anglova node running within a single DAVC virtual cluster node. The entire 269 node scenario can run within a 270 node DAVC cluster. When deployed in this manner node 270 acts as the experimentation orchestration node and is responsible for executing the bootstrap scripting that launches the various applications and EMANE on the remaining 269 nodes.

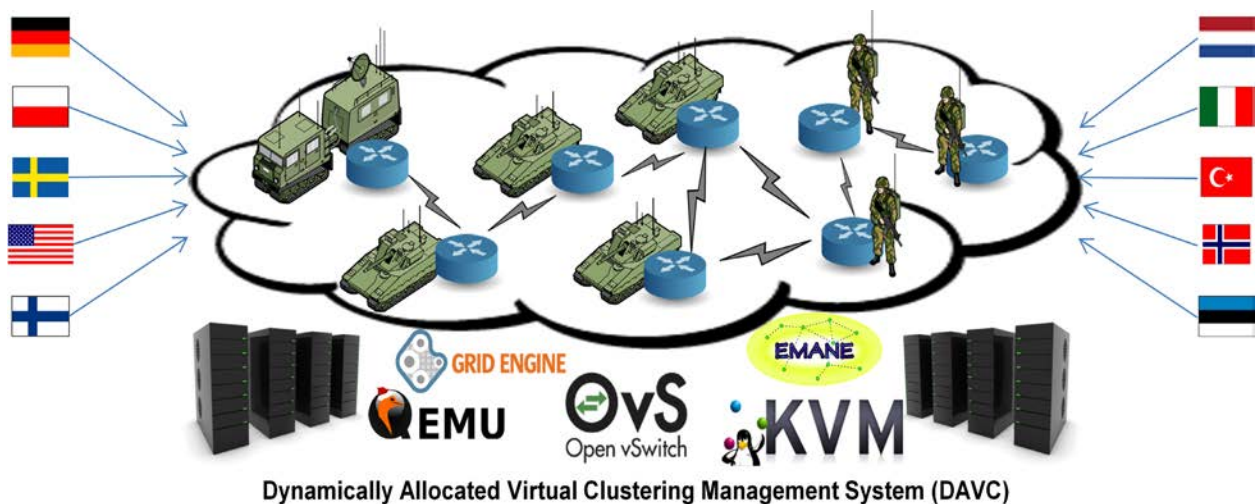


Figure D-2: Emulation Environment for IST-124, Available as a Cloud Service to all IST-124 Members.

D.1.3.2 Experimentation Virtual Machine

A custom Ubuntu 16.04 VM is used to represent a single Anglova scenario node. The template VM is preinstalled with the applications necessary for running the Anglova scenario including EMANE, the Multi Generator (MGEN) [2], and the Optimized Link State Routing Protocol (OLSR)v1 [3] and OLSRv2 [4] routing protocols. The VM is also preinstalled with the various EMANE radio models, mobility and path-loss configuration files specific to the Anglova scenario vignettes. Custom scripting to bootstrap the Anglova scenario and emulation environment is also preinstalled within the VM. This VM is registered with DAVC and used as a template within a DAVC experimentation cluster to run the Anglova scenario.

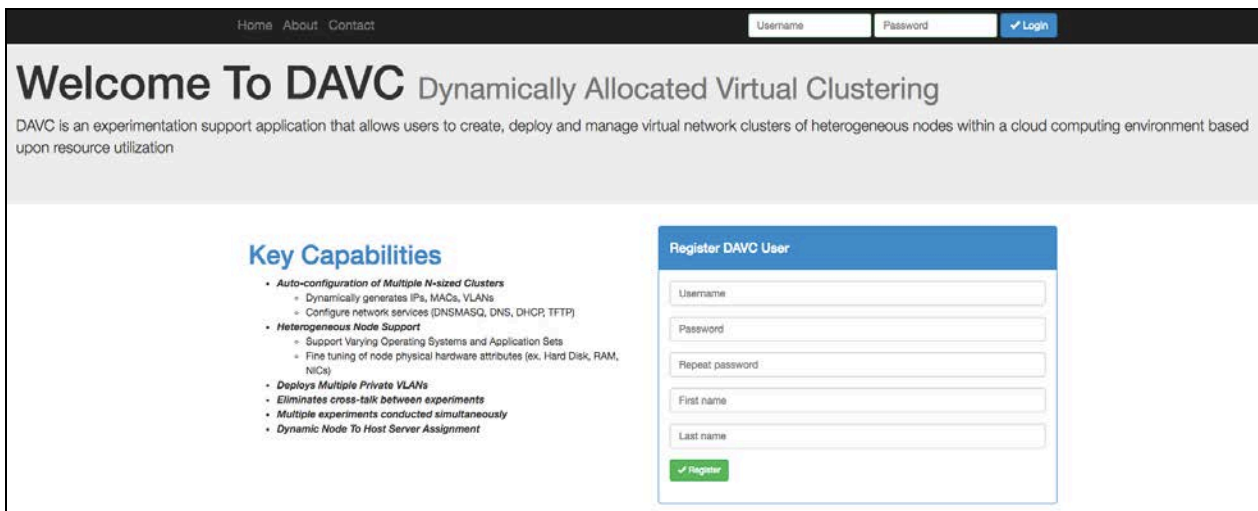
The specifics of the VM's file system including the EMANE configuration files and the experimentation scripting files will be covered in Section D.1.5. Section D.1.4 details the process to create a DAVC cluster that will host the VMs where the experimentation environment will be run.

D.1.4 DAVC Cluster Configuration

The first step in executing the experimentation environment is creating and launching a DAVC Cluster to host the VM nodes where the experimentation environment components will be run. This step will automatically provision multiple instances of the custom VM discussed in the previous section with the base settings necessary to run the EMANE emulation and the experimentation environment scripting. Specifically, this step will create a DAVC cluster consisting of 270 instances of the experimentation VM node connected to the following networks 172.15.0.0/23 and 172.16.0.0/23. The provisioned cluster will provide enough resources to run Anglova scenario Vignette 2 or all portions of Vignette 3.

D.1.4.1 Access and Logging into DAVC

Access the DAVC web application URL with a browser. On the DAVC home page, login using the username/password form at the top right of the application shown in Figure D-3.



Home About Contact

Username Password Login

Welcome To DAVC

Dynamically Allocated Virtual Clustering

DAVC is an experimentation support application that allows users to create, deploy and manage virtual network clusters of heterogeneous nodes within a cloud computing environment based upon resource utilization

Key Capabilities

- **Auto-configuration of Multiple N-sized Clusters**
 - Dynamically generates IPs, MACs, VLANs
 - Configure network services (DNSMASQ, DNS, DHCP, TFTP)
- **Heterogeneous Node Support**
 - Support Varying Operating Systems and Application Sets
 - Fine tuning of node physical hardware attributes (ex. Hard Disk, RAM, NICs)
- **Deploys Multiple Private VLANs**
 - Eliminates cross-talk between experiments
- **Multiple experiments conducted simultaneously**
- **Dynamic Node To Host Server Assignment**

Register DAVC User

Username

Password

Repeat password

First name

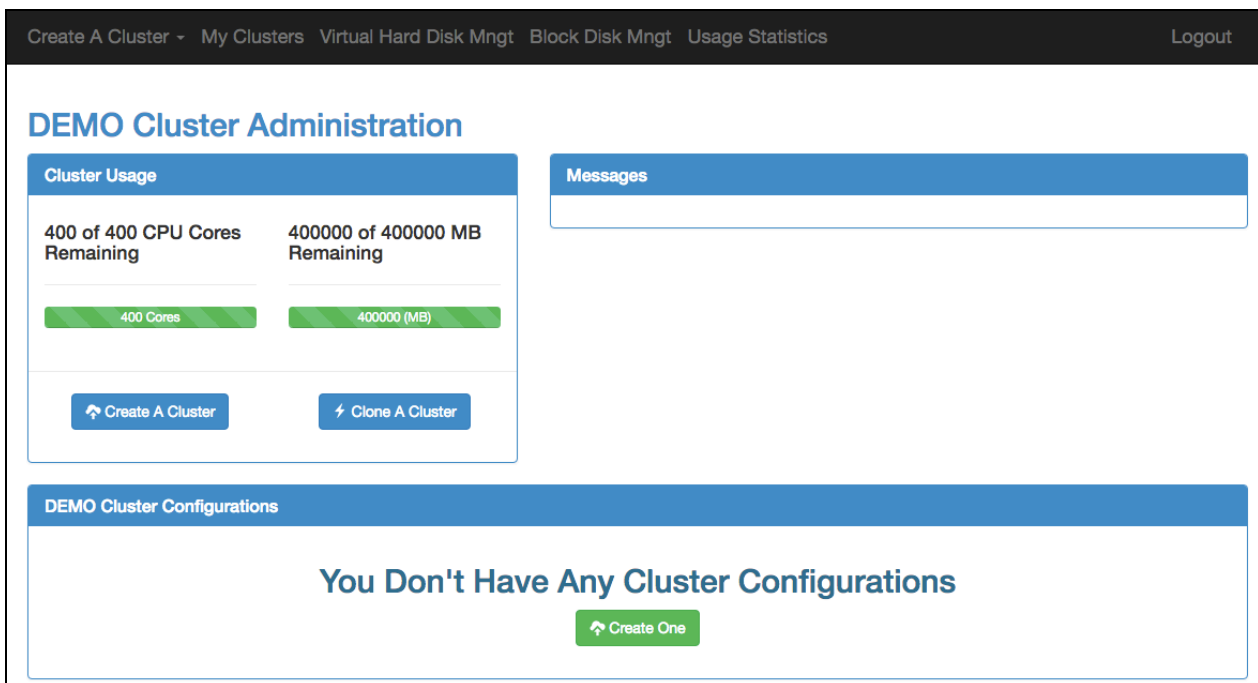
Last name

Register

Figure D-3: DAVC Web Application Login.

D.1.4.2 Create the DAVC Cluster

On the user dashboard screen, shown in Figure D-4, press the “Create A Cluster” button to begin creating the 270 node DAVC cluster.



Create A Cluster - My Clusters Virtual Hard Disk Mngt Block Disk Mngt Usage Statistics Logout

DEMO Cluster Administration

Cluster Usage

400 of 400 CPU Cores Remaining

400000 of 400000 MB Remaining

400 Cores 400000 (MB)

Create A Cluster Clone A Cluster

Messages

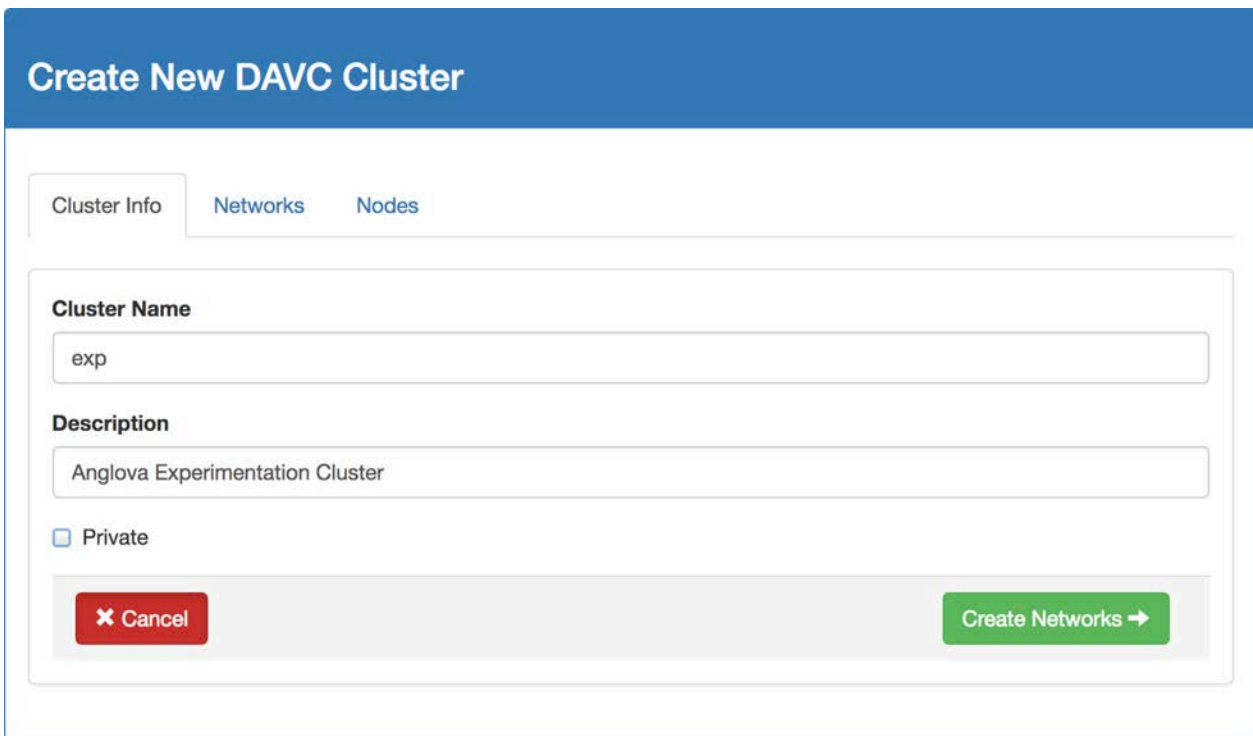
DEMO Cluster Configurations

You Don't Have Any Cluster Configurations

Create One

Figure D-4: DAVC User Dashboard.

Next, on the ‘Create New DAVC Cluster’ dialog’s ‘Cluster Info’ tab (Figure D-5), set the cluster’s name and description. Press the ‘Create Networks’ button when complete.



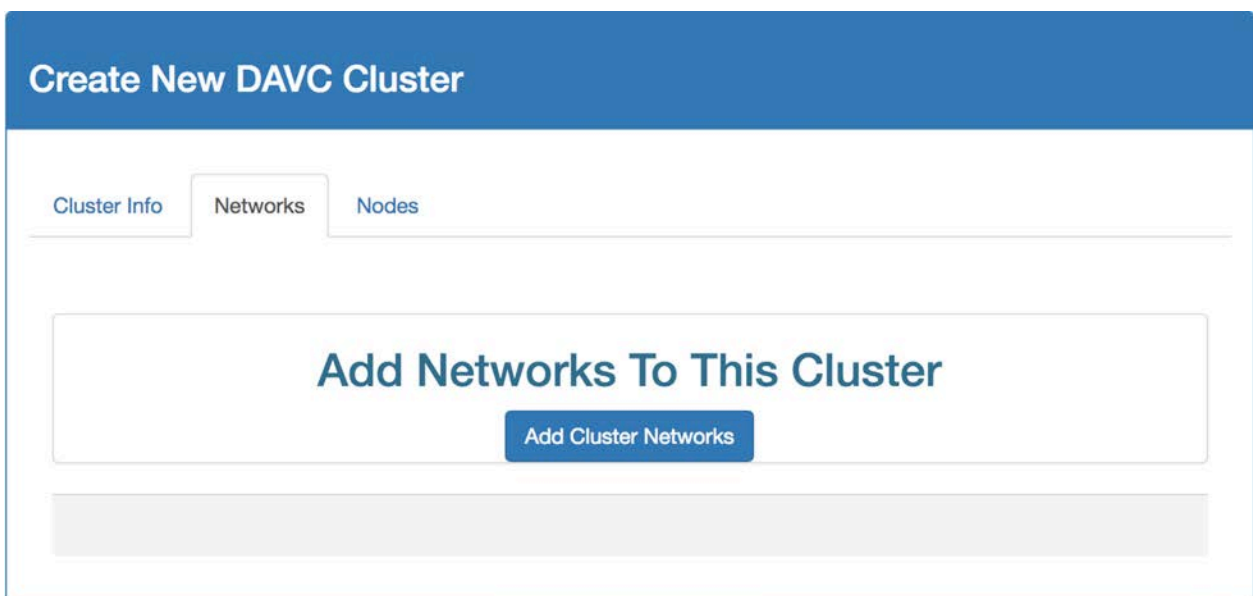
The screenshot shows the 'Create New DAVC Cluster' interface with the 'Cluster Info' tab selected. The form contains the following elements:

- Cluster Name:** A text input field containing the value 'exp'.
- Description:** A text input field containing the value 'Anglova Experimentation Cluster'.
- Private:** A checkbox labeled 'Private' which is currently unchecked.
- Buttons:** A red 'Cancel' button with a close icon and a green 'Create Networks' button with a right-pointing arrow.

Figure D-5: Cluster Info Tab.

D.1.4.3 Create the DAVC Cluster Networks

On the 'Networks' tab (Figure D-6), press the "Add Cluster Networks" button to begin adding the two networks required (172.15.0.0/23 and 172.16.0.0/23) for the experimentation environment. These networks will be associated with the emulated EMANE 'Over-The-Air' radio network.

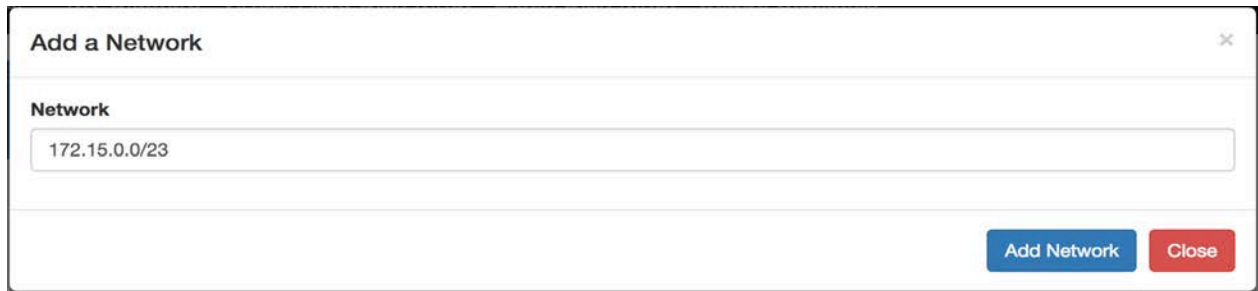


The screenshot shows the 'Create New DAVC Cluster' interface with the 'Networks' tab selected. The form contains the following elements:

- Buttons:** A blue 'Add Cluster Networks' button.
- Text:** The text 'Add Networks To This Cluster' is displayed in a large, bold font.

Figure D-6: Cluster Networks Tab.

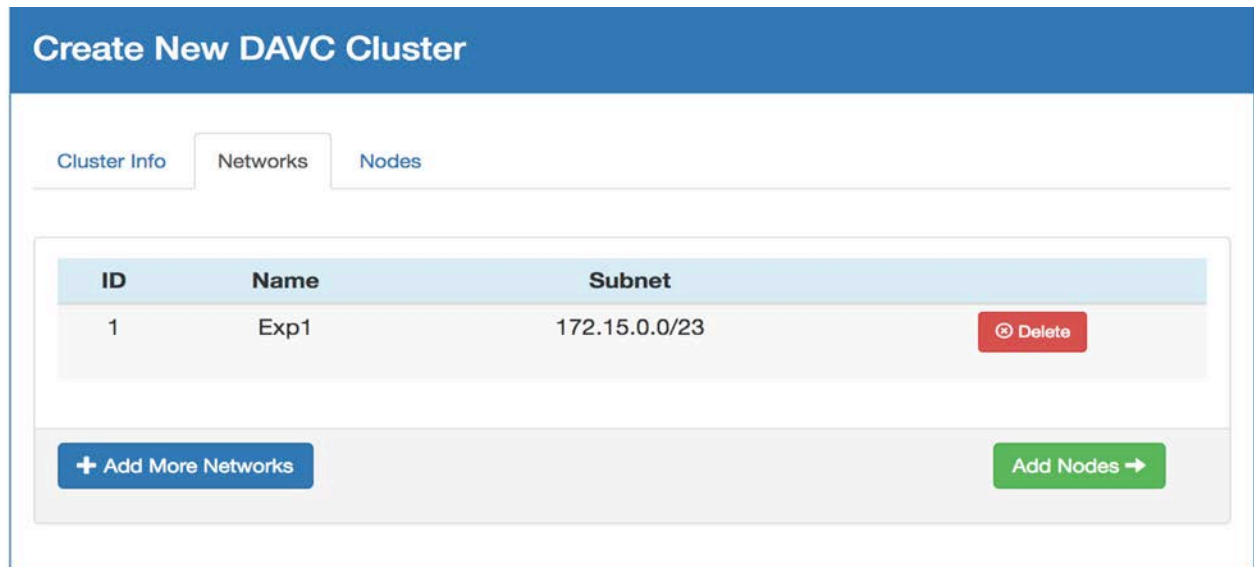
Enter the network 172.15.0.0/23 into the ‘Add a Network’ dialog (Figure D-7) and press ‘Add Network’ when complete.



The dialog box titled "Add a Network" has a close button (X) in the top right corner. Below the title bar, there is a label "Network" followed by a text input field containing "172.15.0.0/23". At the bottom right, there are two buttons: "Add Network" (blue) and "Close" (red).

Figure D-7: Add the Network 172.15.0.0/23.

After adding the first network, press the “Add More Networks” button (Figure D-8) to add the second required network.



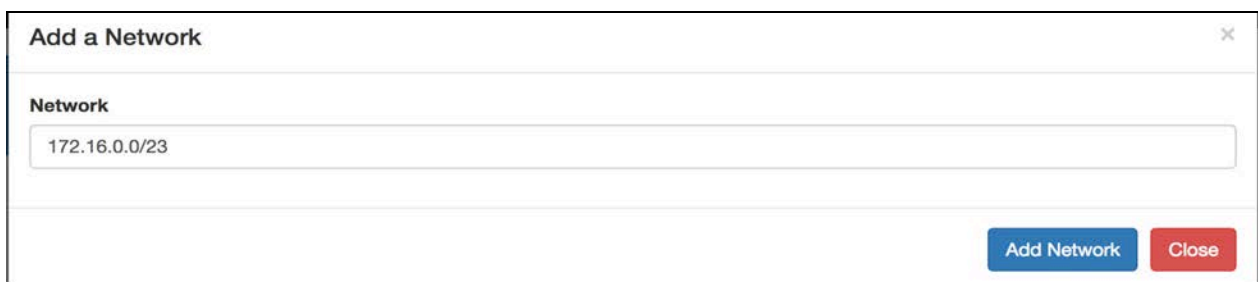
The interface is titled "Create New DAVC Cluster". It has three tabs: "Cluster Info", "Networks", and "Nodes". The "Networks" tab is active. Below the tabs, there is a table with the following data:

ID	Name	Subnet
1	Exp1	172.15.0.0/23

Below the table, there is a red "Delete" button. At the bottom, there are two buttons: "+ Add More Networks" (blue) and "Add Nodes →" (green).

Figure D-8: Add the Second Network to the Cluster.

Enter the second required network 172.16.0.0/23 into the ‘Add a Network’ dialog (Figure D-9) and press ‘Add Network’ when complete.



The dialog box titled "Add a Network" has a close button (X) in the top right corner. Below the title bar, there is a label "Network" followed by a text input field containing "172.16.0.0/23". At the bottom right, there are two buttons: "Add Network" (blue) and "Close" (red).

Figure D-9: Add the Network 172.16.0.0/23.

After the two required networks have been set, press the ‘Add Nodes’ button (Figure D-10) to begin configuring the 270 VM nodes required for the experimentation environment.



ID	Name	Subnet	
1	Exp1	172.15.0.0/23	Delete
2	Exp2	172.16.0.0/23	Delete

[+ Add More Networks](#) [Add Nodes ->](#)

Figure D-10: The Two Experimentation Cluster Networks.

D.1.4.4 Create the DAVC Cluster Nodes

The experimentation environment DAVC cluster consists of a total of 270 VM nodes. VM nodes 1-269 are mapped to the various Anglova scenario nodes and VM node 270 is the experimentation controller node responsible for starting and stopping the experiment. On the ‘Nodes’ tab (Figure D-11), press the ‘Add More Nodes’ to begin configuring VM nodes 1-269.



ID	Controller	OS/Image	Non-Persistent Block Space (GB)	RAM (MB)	Cores	VNIC	Networks
1							

[Add More Nodes](#) [Create Cluster](#)

Figure D-11: Cluster Nodes Tab.

Configure VM nodes 1-269 as shown in Figure D-12. Each node uses the ‘Anglova_node_v3’ VM template and is configured with 1 CPU Core, 5GBs of non-persistent storage for logging, 2GBs of RAM, the virtio virtual network driver, and the 2 networks configured in Section D.1.4.3. Press the ‘Add Nodes’ button to add the 269 VM nodes.

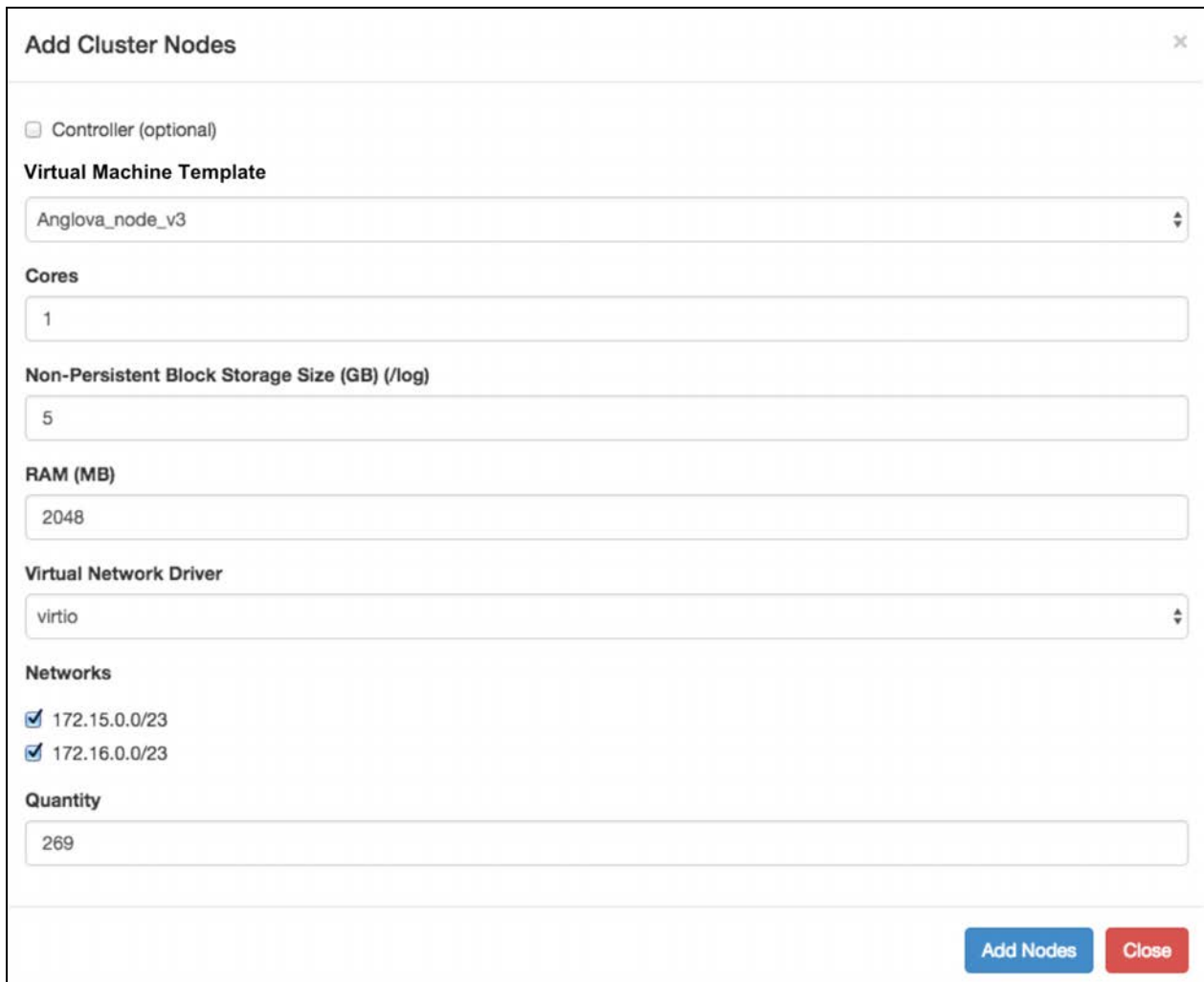


Figure D-12: Configure VM Nodes 1-269.

After adding VM nodes 1-269, press the ‘Add More Nodes’ button at the bottom of the cluster nodes dialog (Figure D-13) to configure and add the final DAVC cluster VM node.

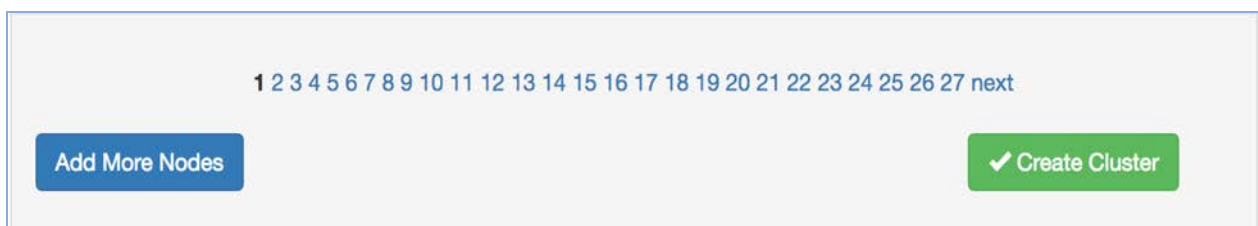


Figure D-13: Add VM Node 270.

ANNEX D – IST-124 EXPERIMENTATION EXECUTION

Configure VM node 270 as shown in Figure D-14. This node also uses the ‘Anglova_node_v3’ VM template but it is configured with 6 CPU Core, 5GBs of non-persistent storage for logging, and 10GBs of RAM. It is also configured with the virtio virtual network driver, and the 2 networks configured in Section D.1.4.3. Press the ‘Add Nodes’ button to add this VM node to the cluster.

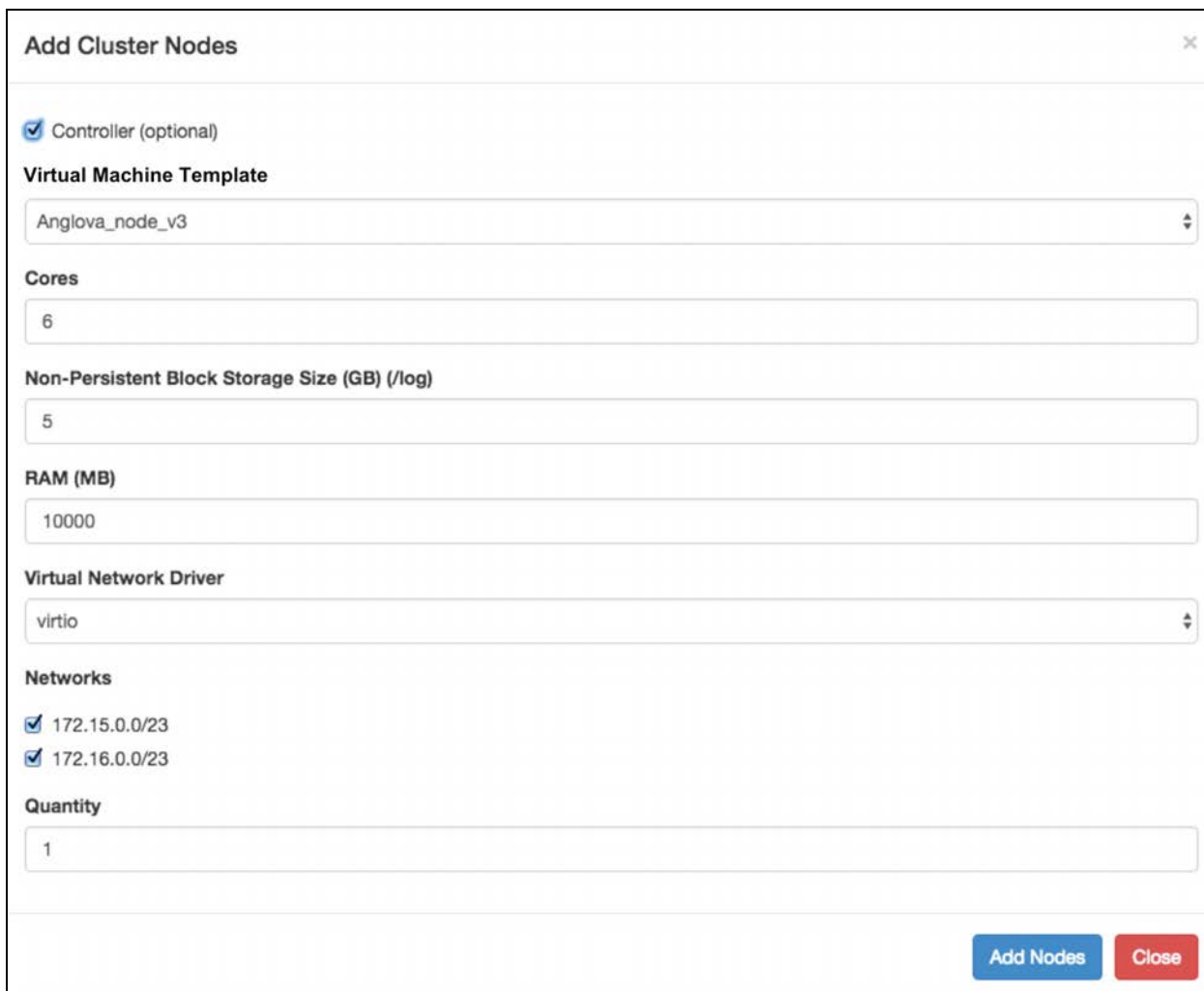


Figure D-14: Configure VM Node 270, the Experimentation Controller.

After all 270 VM nodes have been configured, press the ‘Create Cluster’ at the bottom of the cluster nodes dialog (Figure D-15) to complete the cluster creation process.

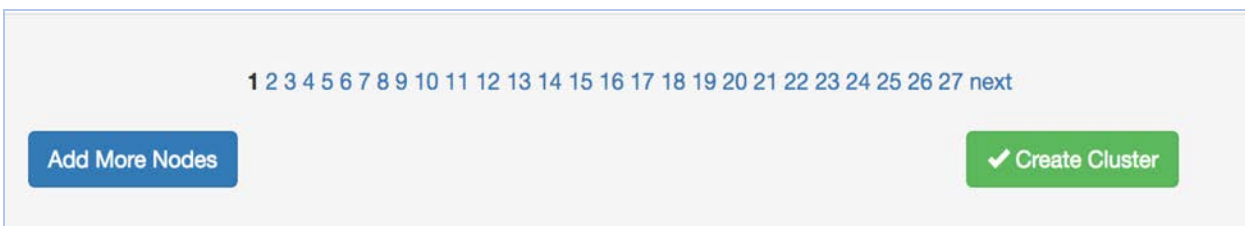


Figure D-15: Complete the Cluster Creation Process.

After completing the cluster creation process, the user is navigated to the cluster details page (Figure D-16) where the cluster can be launched.

Cluster Details: EXP

Launch exp

Edit

Networks

Name	Net
Exp1	172.15.0.0/23
Exp2	172.16.0.0/23

Messages

Core Allocation Policy: No Core Sharing

Cluster exp created successfully

Cluster Nodes (270)

Add Nodes

Node Name	Status	Host Server	OS/Image	Non-Persistent Block Space (GB)	RAM (MB)	Cores	VNIC	IP Addresses	
exp-1	INACTIVE	None	Anglova_node_v3	1	2048	1	virtio	eth0: 10.2.0.0/15 eth1.627:172.15.0.0/23 eth2.628:172.16.0.0/23	Node Options ▾
exp-2	INACTIVE	None	Anglova_node_v3	1	2048	1	virtio	eth0: 10.2.0.0/15 eth1.627:172.15.0.0/23 eth2.628:172.16.0.0/23	Node Options ▾
exp-3	INACTIVE	None	Anglova_node_v3	1	2048	1	virtio	eth0: 10.2.0.0/15 eth1.627:172.15.0.0/23 eth2.628:172.16.0.0/23	Node Options ▾
exp-4	INACTIVE	None	Anglova_node_v3	1	2048	1	virtio	eth0: 10.2.0.0/15 eth1.627:172.15.0.0/23 eth2.628:172.16.0.0/23	Node Options ▾

Figure D-16: Experimentation Cluster Created.

D.1.4.5 Launching the DAVC Cluster

Launch the cluster by pressing the green ‘Launch’ button in the ‘Cluster Controls’ box (Figure D-17). The status of the nodes will begin updating from ‘INACTIVE’ to ‘INITIALIZING’ and finally to ‘ACTIVE’ once the cluster is fully active. Up until this step the cluster has only been a configuration. Now the virtual machines are created, given resources from the servers and powered on.

The cluster activation process will take a while to fully complete as it involves copying and provisioning 270 VMs across several host servers. The activation process is complete and the cluster is active once all of the node’s status is updated to the green ‘ACTIVE’ label as shown in Figure D-18.

ANNEX D – IST-124 EXPERIMENTATION EXECUTION

Cluster Details: EXP

Launch exp
Edit

Name	Net
Exp1	172.15.0.0/23
Exp2	172.16.0.0/23

Messages

Core Allocation Policy: No Core Sharing

Cluster exp created successfully

Cluster Nodes (270)

Add Nodes

Node Name	Status	Host Server	OS/Image	Non-Persistent Block Space (GB)	RAM (MB)	Cores	VNIC	IP Addresses	
exp-1	INITIALIZING	None	Anglova_node_v3	1	2048	1	virtio	eth0: 10.2.0.0/15 eth1.627:172.15.0.0/23 eth2.628:172.16.0.0/23	Node Options
exp-2	INITIALIZING	None	Anglova_node_v3	1	2048	1	virtio	eth0: 10.2.0.0/15 eth1.627:172.15.0.0/23 eth2.628:172.16.0.0/23	Node Options
exp-3	INITIALIZING	None	Anglova_node_v3	1	2048	1	virtio	eth0: 10.2.0.0/15 eth1.627:172.15.0.0/23 eth2.628:172.16.0.0/23	Node Options
exp-4	INITIALIZING	None	Anglova_node_v3	1	2048	1	virtio	eth0: 10.2.0.0/15 eth1.627:172.15.0.0/23 eth2.628:172.16.0.0/23	Node Options

Figure D-17: Cluster Nodes Initializing.

Node Name	Status	Host Server	OS/Image	Non-Persistent Block Space (GB)	RAM (MB)	Cores	VNIC	IP Addresses	
exp-1	ACTIVE	davc2-d8	Anglova_node_v3	1	2048	1	virtio	eth0: 10.2.1.137 eth1.627: 172.15.0.1 rate: 1000000 (Kbps) Set Rate eth2.628: 172.16.0.1 rate: 1000000 (Kbps) Set Rate	Node Options
exp-2	ACTIVE	davc2-d8	Anglova_node_v3	1	2048	1	virtio	eth0: 10.2.1.138 eth1.627: 172.15.0.2 rate: 1000000 (Kbps) Set Rate eth2.628: 172.16.0.2 rate: 1000000 (Kbps) Set Rate	Node Options
exp-3	ACTIVE	davc2-d2	Anglova_node_v3	1	2048	1	virtio	eth0: 10.2.1.139 eth1.627: 172.15.0.3 rate: 1000000 (Kbps) Set Rate	Node Options

Figure D-18: The Cluster is Active Once All Nodes' Status is Set to 'ACTIVE'.

D.1.4.6 Logging into the Experimentation Controller

When the status of all of the nodes in the experimentation cluster is marked active, log into VM node 270's Virtual Network Computing (VNC) console by clicking on its 'Open VNC' button in the 'Node Options' dropdown menu (Figure D-19).



Figure D-19: Log into VM Node 270's VNC Console.

This will open a browser page with a VNC session hosting VM Node 270's desktop (Figure D-20). This node will run the experimentation scripting, which bootstraps the other cluster nodes to run the appropriate EMANE configurations and scripts for the specified vignette (Vignette 2 or Vignette 3 Part 1, Part 2, or Part 3). VM Node 270 will also run the EMANE event service, which will generate the location and path loss data for the specified vignette.

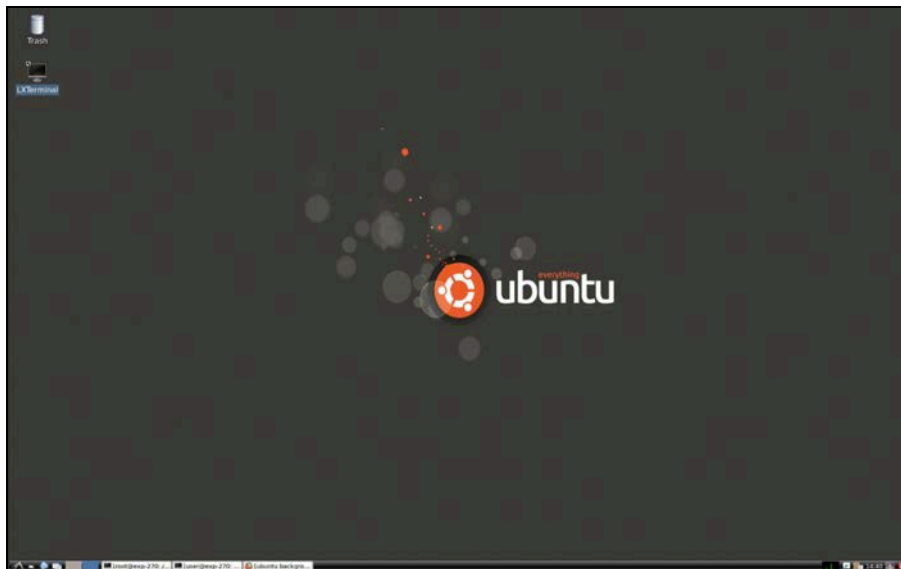


Figure D-20: VM Node 270's VNC Console.

The experimentation environment's DAVC cluster is ready and the Anglova scenario emulation can now be run. But first the experimentation environment's file system including the EMANE configuration files and the experimentation scripting files are described in the next section.

D.1.5 Experimentation Virtual Machine File System

A custom Ubuntu 16.04 VM is used to represent a single Anglova scenario node. The template VM is preinstalled with the applications necessary for running the Anglova scenario including EMANE, the Multi Generator (MGEN), and the OLSRv1 and OLSRv2 routing protocols. The VM is also preinstalled with the various EMANE radio models, mobility and path-loss configuration files specific to the Anglova scenario

vignettes. Custom scripting to bootstrap the Anglova scenario and emulation environment is also preinstalled within the VM. As outlined in the previous section, this VM is used as the template VM to create a 270 node DAVC experimentation cluster to run the Anglova scenario.

The experimentation environment's file system including the EMANE configuration files, and the experimentation scripting files are described in the following sections.

D.1.5.1 Experimentation Configuration Files

All of the experimentation environment's configuration and scripting files are located in the /opt/nato-experiment directory shown in Figure D-21.

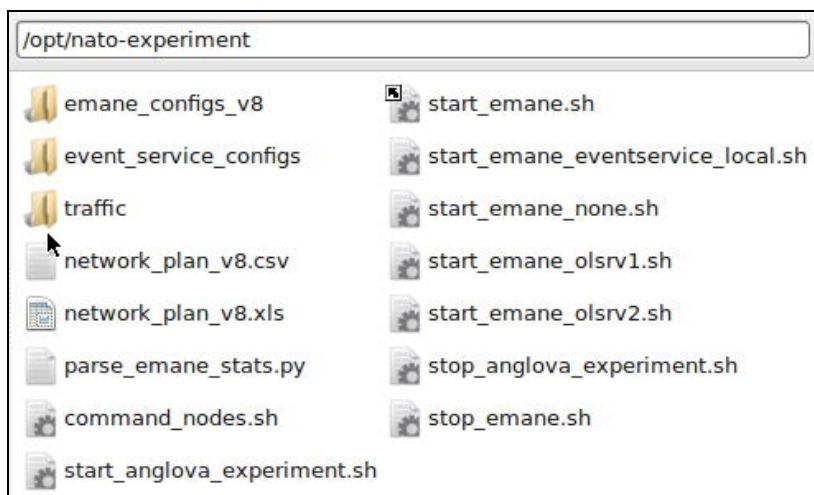


Figure D-21: Emulation Environment File System.

Table D-1 provides a brief description of the files located in this directory. A more detail description of these files will be covered in later sections.

Table D-1: A Brief Description of the Files Located in the /opt/nato-experiment Folder of the Controller Node.

File	Description
start_anglova_experiment.sh	Starts the experiment components on the DAVC cluster nodes.
stop_anglova_experiment.sh	Stops the experiment components on the DAVC cluster nodes.
start_emane.sh	Symbolic link that points to one of the other start_emane_<routing protocol version>.sh scripts.
start_emane_none.sh	Script to start the EMANE emulator without a routing protocol on a DAVC cluster node.
start_emane_olsrv1.sh	Script to start the EMANE emulator with the OLSRv1 routing protocol on a DAVC cluster node.
start_emane_olsrv2.sh	Script to start the EMANE emulator with the OLSRv2 routing protocol on a DAVC cluster node.
stop_emane.sh	Script to stop the EMANE emulator running on the DAVC cluster nodes.

File	Description
start_emane_eventservice.sh	Script to start the EMANE event service, which sends location and path loss events to the event service daemons on the DAVC cluster nodes.
parse_emane_stats.sh	Script to output the statistics and values retrieved from the EMANE shell.
command_nodes.sh	Utility script used to run a command on all of the DAVC cluster nodes
emane_configs_v8	Directory: Contains the EMANE platform and radio configuration files for the nodes in the Anglova emulation.
network_plan_v8.xls	Network plan spreadsheets containing node to network mappings for the Anglova emulation.
network_plan_v8.csv	Comma separated version of the network_plan_v8.xls file.
event_service_configs	Directory: Contains the EMANE mobility and path loss configuration files used to generate location and path loss events.
traffic	Directory: Contains the MGEN configurations and scripting to generate background traffic.

D.1.5.2 Experimentation Environment Network Plan

The experimentation environment’s network plan (*/opt/nato-experiment/network_plan_v8.xls*) is a set of spreadsheets used by the experimentation scripting to configure the correct settings for each node’s EMANE Network Emulation Module (NEM).

A portion of the experimentation environment’s network plan is shown in Figure D-22. The network plan defines how the Anglova scenario nodes are mapped to the 17 emulated EMANE radio networks (See Annex B for more information about the modelling of the radios). Specifically it shows the node groupings (column 2) and their membership within the radio networks (rows 1 and 2, columns 3 to 17). A green entry in a column indicates that node is a member of and has a radio on the corresponding network. The numbers in the green cells are the radio IDs that will be assigned to the emulated EMANE radio. A dark gray ‘0’ entry indicates the node does not have a radio on the corresponding network.

id	group	wideband1	wideband2	wideband3	wideband4	narrowband1	narrowband2	narrowband3	satcom	lwav	indium	cellular	laser-f	laser-hf	laser-net	navy-uhf	navy-hf	acoustic-fiber	acoustic-vf
network	subnets	192.168.1.0	192.168.2.0	192.168.3.0	192.168.4.0	192.168.5.0	192.168.6.0	192.168.7.0	192.168.8.0	192.168.9.0	192.168.10.0	192.168.11.0	192.168.12.0	192.168.13.0	192.168.14.0	192.168.15.0	192.168.16.0	192.168.17.0	
1	company1	1	0	0	0	90	0	0	0	0	0	0	0	0	0	0	0	0	0
2	company1	100	0	0	0	150	0	0	0	0	0	0	0	0	0	0	0	0	0
3	company1	200	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	company1	230	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	company1	300	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	company1	350	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	company1	400	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	company1	450	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	company1	500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	company1	550	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	company1	600	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	company1	650	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	company1	700	0	0	0	0	0	0	750	0	0	0	0	0	0	0	0	0	0
14	company1	800	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	company1	850	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	company1	900	0	0	0	0	0	0	850	0	0	0	0	0	0	0	0	0	0
17	company1	1000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	company1	1050	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	company1	1100	0	0	0	0	0	0	0	1150	0	0	0	0	0	0	0	0	0
20	company1	1200	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	company1	1250	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	company1	1300	0	0	0	0	0	0	0	1350	0	0	0	0	0	0	0	0	0
23	company1	1400	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	company1	1450	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	company2	0	1500	0	0	1550	0	0	0	0	0	0	0	0	0	0	0	0	0
26	company2	0	2000	0	0	2050	0	0	0	0	0	0	0	0	0	0	0	0	0
27	company2	0	2100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	company2	0	2150	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	company2	0	2200	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
30	company2	0	2250	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	company2	0	2300	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32	company2	0	2350	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	company2	0	2400	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	company2	0	2450	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
35	company2	0	2500	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
36	company2	0	2550	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
37	company2	0	2600	0	0	0	0	0	2650	0	0	0	0	0	0	0	0	0	0
38	company2	0	2700	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39	company2	0	2750	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	company2	0	2800	0	0	0	0	0	2850	0	0	0	0	0	0	0	0	0	0
41	company2	0	2850	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
42	company2	0	3000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
43	company2	0	3050	0	0	0	0	0	0	3100	0	0	0	0	0	0	0	0	0
44	company2	0	3150	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
45	company2	0	3200	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
46	company2	0	3250	0	0	0	0	0	0	1300	0	0	0	0	0	0	0	0	0
47	company2	0	3350	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
48	company2	0	3400	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure D-22: Snippet of the Anglova Scenario Network Plan.

ANNEX D – IST-124 EXPERIMENTATION EXECUTION

Taking a closer look at the network plan we can see in Figure D-23 that Anglova scenario nodes 1 and 2 are members of the ‘company1’ group and have radios on the ‘wideband1’ and ‘narrowband1’ networks. In this documentation an Anglova scenario node will be referred by its group name and position within that group. Using this convention we refer to Anglova scenario nodes 1 and 2 as company1-1 and company1-2 respectively. Note that Anglova scenario node 25 is referred to as company2-1 not company2-25. The IDs for the radios on company1-1 are 1 and 50. The IDs for the radios on company1-2 are 100 and 150. The ‘wideband1’ and ‘narrowband1’ network subnets are ‘192.168.1.0/24’ and ‘192.168.5.0/24’ respectively. When the emulation is started, the VM nodes mapped to the Anglova scenario nodes company1-1 and company1-2 will have EMANE radios configured on these subnets. The IP address assignments for the subnets are sequential per radio and across groups as shown in the network plan snippet in Figure D-24. Each radio is also assigned a host name in the format <group>-<group id>-<radio name>. Examples of the host name assignments are shown in the network plan snippet in Figure D-25.

id	group	wideband1	wideband2	wideband3	wideband4	narrowband1	narrowband2	narrowband3	satcom	uav
network	subnets	192.168.1.0	192.168.2.0	192.168.3.0	192.168.4.0	192.168.5.0	192.168.6.0	192.168.7.0	192.168.8.0	192.168.9.0
1	company1	1	0	0	0	50	0	0	0	0
2	company1	100	0	0	0	150	0	0	0	0

Figure D-23: Company1-1 and Company1-2 Network Mappings.

id	group	wideband1	wideband2	wideband3	wideband4	narrowband1	narrowband2	narrowband3	satcom	uav
network	subnets	192.168.1.0	192.168.2.0	192.168.3.0	192.168.4.0	192.168.5.0	192.168.6.0	192.168.7.0	192.168.8.0	192.168.9.0
1	company1	192.168.1.1	0	0	0	192.168.5.1	0	0	0	0
2	company1	192.168.1.2	0	0	0	192.168.5.2	0	0	0	0
3	company1	192.168.1.3	0	0	0	0	0	0	0	0
4	company1	192.168.1.4	0	0	0	0	0	0	0	0
5	company1	192.168.1.5	0	0	0	0	0	0	0	0
6	company1	192.168.1.6	0	0	0	0	0	0	0	0
7	company1	192.168.1.7	0	0	0	0	0	0	0	0
8	company1	192.168.1.8	0	0	0	0	0	0	0	0
9	company1	192.168.1.9	0	0	0	0	0	0	0	0
10	company1	192.168.1.10	0	0	0	0	0	0	0	0
11	company1	192.168.1.11	0	0	0	0	0	0	0	0
12	company1	192.168.1.12	0	0	0	0	0	0	0	0
13	company1	192.168.1.13	0	0	0	0	0	0	0	0
14	company1	192.168.1.14	0	0	0	0	0	0	0	0
15	company1	192.168.1.15	0	0	0	0	0	0	0	0
16	company1	192.168.1.16	0	0	0	0	0	0	0	0
17	company1	192.168.1.17	0	0	0	0	0	0	0	0
18	company1	192.168.1.18	0	0	0	0	0	0	0	0
19	company1	192.168.1.19	0	0	0	0	0	0	0	0
20	company1	192.168.1.20	0	0	0	0	0	0	0	0
21	company1	192.168.1.21	0	0	0	0	0	0	0	0
22	company1	192.168.1.22	0	0	0	0	0	0	0	0
23	company1	192.168.1.23	0	0	0	0	0	0	0	0
24	company1	192.168.1.24	0	0	0	0	0	0	0	0
25	company2	0	192.168.2.1	0	0	192.168.5.3	0	0	0	0
26	company2	0	192.168.2.2	0	0	192.168.5.4	0	0	0	0
27	company2	0	192.168.2.3	0	0	0	0	0	0	0
28	company2	0	192.168.2.4	0	0	0	0	0	0	0
29	company2	0	192.168.2.5	0	0	0	0	0	0	0
30	company2	0	192.168.2.6	0	0	0	0	0	0	0
31	company2	0	192.168.2.7	0	0	0	0	0	0	0
32	company2	0	192.168.2.8	0	0	0	0	0	0	0
33	company2	0	192.168.2.9	0	0	0	0	0	0	0
34	company2	0	192.168.2.10	0	0	0	0	0	0	0
35	company2	0	192.168.2.11	0	0	0	0	0	0	0
36	company2	0	192.168.2.12	0	0	0	0	0	0	0
37	company2	0	192.168.2.13	0	0	0	0	0	0	0
38	company2	0	192.168.2.14	0	0	0	0	0	0	0
39	company2	0	192.168.2.15	0	0	0	0	0	0	0
40	company2	0	192.168.2.16	0	0	0	0	0	0	0
41	company2	0	192.168.2.17	0	0	0	0	0	0	0

Figure D-24: Network Plan IP Address Mappings.

According to the network plan, Anglova scenario nodes company1-1 and company1-2 will be assigned the following radios (Table D-2).

Note that not all nodes are involved in each vignette. The network plan also includes a spreadsheet that specifies which groups are mapped to each vignette. The group vignette mappings are shown in Figure D-26.

Table D-2: The Radio Networks of Company 1.

company1-1	Host name: company1-1-wideband1 IP Address: 192.168.1.1/24	Host name: company1-1-narrowband1 IP Address: 192.168.5.1/24
company1-2	Host name: company1-2-wideband1 IP Address: 192.168.2.2/24	Host name: company1-2-narrowband1 IP Address: 192.168.5.2/24

id	group	wideband1	wideband2	wideband3	wideband4	narrowband1	narrowband2	narrowband3	satcom	uav
network	subnets	192.168.1.0	192.168.2.0	192.168.3.0	192.168.4.0	192.168.5.0	192.168.6.0	192.168.7.0	192.168.8.0	192.168.9.0
1	company1	company1-1-wideband1	0	0	0	company1-1-narrowband1	0	0	0	0
2	company1	company1-2-wideband1	0	0	0	company1-2-narrowband1	0	0	0	0
3	company1	company1-3-wideband1	0	0	0	0	0	0	0	0
4	company1	company1-4-wideband1	0	0	0	0	0	0	0	0
5	company1	company1-5-wideband1	0	0	0	0	0	0	0	0
6	company1	company1-6-wideband1	0	0	0	0	0	0	0	0
7	company1	company1-7-wideband1	0	0	0	0	0	0	0	0
8	company1	company1-8-wideband1	0	0	0	0	0	0	0	0
9	company1	company1-9-wideband1	0	0	0	0	0	0	0	0
10	company1	company1-10-wideband1	0	0	0	0	0	0	0	0
11	company1	company1-11-wideband1	0	0	0	0	0	0	0	0
12	company1	company1-12-wideband1	0	0	0	0	0	0	0	0
13	company1	company1-13-wideband1	0	0	0	0	0	0	company1-13-satcom	0
14	company1	company1-14-wideband1	0	0	0	0	0	0	0	0
15	company1	company1-15-wideband1	0	0	0	0	0	0	0	0
16	company1	company1-16-wideband1	0	0	0	0	0	0	company1-16-satcom	0
17	company1	company1-17-wideband1	0	0	0	0	0	0	0	0
18	company1	company1-18-wideband1	0	0	0	0	0	0	0	0
19	company1	company1-19-wideband1	0	0	0	0	0	0	0	company1-19-uav
20	company1	company1-20-wideband1	0	0	0	0	0	0	0	0
21	company1	company1-21-wideband1	0	0	0	0	0	0	0	0
22	company1	company1-22-wideband1	0	0	0	0	0	0	0	company1-22-uav
23	company1	company1-23-wideband1	0	0	0	0	0	0	0	0
24	company1	company1-24-wideband1	0	0	0	0	0	0	0	0
25	company2	0	company2-1-wideband2	0	0	company2-1-narrowband1	0	0	0	0
26	company2	0	company2-2-wideband2	0	0	company2-2-narrowband1	0	0	0	0
27	company2	0	company2-3-wideband2	0	0	0	0	0	0	0
28	company2	0	company2-4-wideband2	0	0	0	0	0	0	0
29	company2	0	company2-5-wideband2	0	0	0	0	0	0	0
30	company2	0	company2-6-wideband2	0	0	0	0	0	0	0
31	company2	0	company2-7-wideband2	0	0	0	0	0	0	0
32	company2	0	company2-8-wideband2	0	0	0	0	0	0	0
33	company2	0	company2-9-wideband2	0	0	0	0	0	0	0
34	company2	0	company2-10-wideband2	0	0	0	0	0	0	0
35	company2	0	company2-11-wideband2	0	0	0	0	0	0	0
36	company2	0	company2-12-wideband2	0	0	0	0	0	0	0
37	company2	0	company2-13-wideband2	0	0	0	0	0	company2-13-satcom	0
38	company2	0	company2-14-wideband2	0	0	0	0	0	0	0
39	company2	0	company2-15-wideband2	0	0	0	0	0	0	0
40	company2	0	company2-16-wideband2	0	0	0	0	0	company2-16-satcom	0
41	company2	0	company2-17-wideband2	0	0	0	0	0	0	0

Figure D-25: Network Plan Host Names.

group	Vignette 2	Vignette 3-1	Vignette 3-2	Vignette 3-3
company1	*			
company2	*			
company3	*			
company4	*			
command	*			
support1	*			
support2	*			
platoon1		*	*	*
platoon2		*	*	*
platoon3		*	*	*
tac-uav	*	*	*	*
harvest-uav		*	*	*
navy		*	*	*
med-helicopter		*	*	*
aerostat		*	*	*
tac-sat		*	*	*
iridium-sat		*	*	*
geo-sat		*	*	*
ugs		*	*	*
coalition-hq	*	*	*	*
toc-hq	*	*	*	*

Figure D-26: Vignette Group Mappings.

D.1.5.3 EMANE Configuration Files

The EMANE configuration and radio model files for running the experimentation environment are separated by group in the `/opt/nato-experiment/emane_configs_v8` directory shown in Figure D-27.

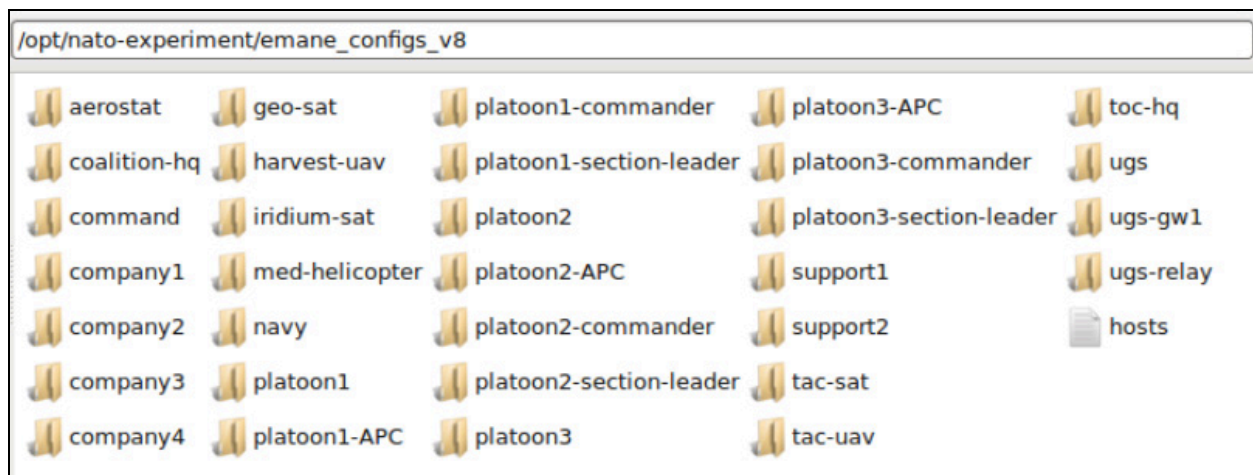


Figure D-27: EMANE Configuration Directories.

Each group directory contains the EMANE configuration files required to instantiate the EMANE radios for each Anglova scenario node within that particular group as defined by the network plan discussed in Section D.1.5.2. EMANE requires several Extensible Markup Language (XML) configuration files to properly instantiate a node's emulated radio. These include files listed in Table D-3.

Table D-3: The Set of Xml Files that are Used to Instantiate a Node's Emulated Radio.

File	Description
platform.xml	Defines radio model instantiations and their multicast group/interface mappings. One file per node.
eventdaemon.xml	Defines the multicast group/interface mappings for the event daemon. One file per emulated radio.
gpsdlocationagent.xml	Defines the configuration parameters for the GPS Daemon (GPSD) location agent. One file per emulated radio.
transvirtual.xml	Defines the transport component responsible for delivering messages between an emulator instance and application space processes. One per node.
radio_nem.xml	Specifies the radio model's Medium Access (MAC) and Physical layer (PHY) configuration files. One per radio network.
radio_mac.xml	Specifies the radio model's MAC layer configurations. One per radio network.
radio_phy.xml	Specifies the radio model's PHY layer configurations. One per radio network.

Figure D-28 shows the EMANE configuration files for the ‘company1’ group. Since the ‘company1’ group consists of 24 nodes there are 24 different ‘platform.xml’ files, one per node. The naming convention for the platform files is ‘platform<platform ID>.xml’, where the platform ID is the ID from column 1 of the network plan file discussed in Section D.1.5.2.

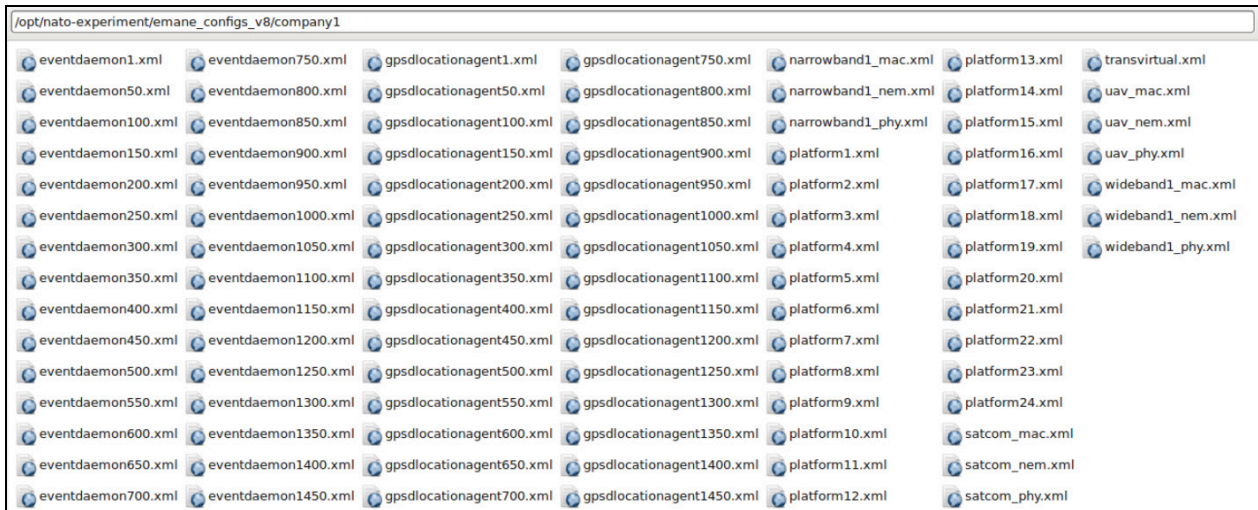


Figure D-28: Company1 EMANE Configuration Files.

D.1.5.3.1 Platform Configuration File

Figure D-29 shows the contents of ‘platform1.xml’, the platform XML file for Anglova scenario node company1-1. The top portion of the file specifies the configurations for the multicast channel EMANE uses to send and receive application traffic (Over-The-Air (OTA) group and device), and the multicast channel EMANE uses to receive location and path loss events (event service group and device). The values of the ‘otamanagerdevice’ and ‘eventservicedevice’ are set to the network interface associated with the DAVC network (172.15.0.0/23 – eth1) configured in Section D.1.4.3. The OTA service and the event service use the same device in this example, but they could be separated by setting either the ‘otamanagerdevice’ or ‘eventservicedevice’ to the second DAVC interface (172.16.0.0/23 - eth2) configured in Section D.1.4.3. The bottom portion contains 2 Network Emulation Module (NEM) entries for each of the radios this particular node is equipped with. A NEM is EMANE’s representation of an emulated radio. Note that the IP addresses defined for these NEMs are the same as what is defined in the network plan discussed in Section D.1.5.2.

D.1.5.3.2 Transport Configuration File

All of the nodes share the same ‘transvirtual.xml’ and radio model configuration files (wideband1, narrowband1, satcom, and uav). However, each radio within the ‘company1’ group has its own ‘eventdaemon.xml’ and ‘gpsdlocationagent.xml’ files. The naming conventions for these files are ‘eventdaemon<radio ID>.xml’ and ‘gpsdlocationagent<radio ID>.xml’, where the radio ID is one of the numbers in the green cells in the network plan file discussed in Section D.1.5.2. In EMANE terminology the radio ID is referred to as a NEM ID.

Figure D-30 shows the contents of the shared ‘transvirtual.xml’ file. This file is the same across all groups and therefore is shared. This file defines the transport library that provides the entry and exit point for the emulator and application space messages. The experimentation environment uses the Virtual Transport library, which uses a TAP interface to create a virtual interface as the application/emulation boundary entry/exit point. The virtual interfaces that will be created on a node are defined in the NEM/transport entries in the platform

XML file. Referring to the NEM/transport entries in Figure D-29, we can see that the DAVC VM node mapped to Anglova scenario node company1-1 node will have 2 virtual interfaces ('emane0' and 'emane4') created on it that will define the boundary between that node's application space and the emulated radio.

```
<?xml version="1.0" ?><!DOCTYPE platform SYSTEM 'file:///usr/share/emane/dtd/platform.dtd'>
<platform>
  <param name="otamanagerchannelenable" value="on"/>
  <param name="otamanagerdevice" value="eth1"/>
  <param name="otamanagergroup" value="224.1.2.8:45702"/>
  <param name="eventservicegroup" value="224.1.2.8:45703"/>
  <param name="eventservicedevice" value="eth1"/>
  <param name="controlportendpoint" value="0.0.0.0:47000"/>

  <nem definition="wideband1 nem.xml" id="1">
    <transport definition="transvirtual.xml">
      <param name="device" value="emane0"/>
      <param name="address" value="192.168.1.1"/>
      <param name="mask" value="255.255.255.0"/>
    </transport>
  </nem>

  <nem definition="narrowband1 nem.xml" id="50">
    <transport definition="transvirtual.xml">
      <param name="device" value="emane4"/>
      <param name="address" value="192.168.5.1"/>
      <param name="mask" value="255.255.255.0"/>
    </transport>
  </nem>
</platform>
```

OTA and Event Service Configurations

NEM 1 Radio Configurations

NEM 50 Radio Configurations

Figure D-29: Company1-1 Platform XML File.

```
<?xml version="1.0" ?>
<!DOCTYPE transport SYSTEM 'file:///usr/share/emane/dtd/transport.dtd'>
<transport library="transvirtual" name="Virtual Transport">
  <param name="devicepath" value="/dev/net/tun"/>
</transport>
```

Figure D-30: Company1 Transvirtual XML File.

D.1.5.3.3 Event Daemon Configuration File

Figure D-31 shows the contents of 'eventdaemon1.xml', the event daemon settings for Anglova scenario node company1-1. In order for the scenario to progress, each NEM or radio must receive the location and path loss events for the each time step in the scenario. The event daemon listens to and receives events from the event channel. The event daemon's (remaining) role is to make events available to 'application space' by means of its 'agent' plug-ins such as the gpsdlocationagent. The event daemon XML file defines the multicast group and interface where it will listen for events. Each NEM, as indicated by the 'nemid' value in this file, must have its own event daemon XML file defining these settings.

```
<?xml version="1.0" ?>
<!DOCTYPE eventdaemon SYSTEM 'file:///usr/share/emane/dtd/eventdaemon.dtd'>
<eventdaemon nemid="1">
  <param name="eventservicegroup" value="224.1.2.8:45703"/>
  <param name="eventservicedevice" value="eth1"/>
  <agent definition="gpsdlocationagent1.xml"/>
</eventdaemon>
```

Figure D-31: Event Service Daemon XML File.

D.1.5.3.4 GPS Daemon Configuration File

This event daemon file also specifies specialized event agents that handle specific types of events. All of the nodes in the experimentation environment specify the GPSD location event agent shown in Figure D-32. This agent is responsible for making location events available as NMEA sentences, which can serve as input to user applications (e.g., GPSd, the GPS daemon) running on the node.

```
<?xml version="1.0" ?>
<!DOCTYPE eventagent SYSTEM 'file:///usr/share/emane/dtd/eventagent.dtd'>
<eventagent library="gpsdlocationagent">
  <param name="pseudoterminalfile" value="/tmp/gps.pty"/>
</eventagent>
```

Figure D-32: GPSD Location Agent XML File.

D.1.5.3.5 Radio Model Configuration Files

The configuration files for the radio models represented within each group are located in the group directory also. Referring to Figure D-22 and Figure D-28, we see that company1 has nodes that will run the ‘wideband1’, ‘narrowband1’, ‘satcom’, and ‘uav’ radio models. Each of these radio model configuration files are located in the ‘/opt/nato-experiment/emane_configs_v8/company1’ directory and are shared amongst the nodes in the company1 group. A radio model is represented by 3 types of configuration files: a radio model NEM, MAC layer, and PHY layer file.

The ‘wideband1’ radio model NEM file is shown in Figure D-33. This file specifies the files that define the radio model’s MAC and PHY layer configurations. It also specifies the transport definition file previously discussed.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nem SYSTEM 'file:///usr/share/emane/dtd/nem.dtd'>
<nem>
  <transport definition="transvirtual.xml"/>
  <mac definition="wideband1_mac.xml"/>
  <phy definition="wideband1_phy.xml"/>
</nem>
```

Figure D-33: Wideband1 Radio Model NEM XML File.

The ‘wideband1’ radio model PHY layer file is shown in Figure D-34. This file specifies the PHY layer library the radio will use (‘universalphy’) and contains the radio model’s physical layer properties such as bandwidth, frequency and transport model. It also sets the radio’s propagation model to precomputed, which means the NEM will be expecting to receive precomputed path loss events via the event service multicast channel previously discussed.

The ‘wideband1’ radio model MAC layer file is shown in Figure D-35. This file defines the MAC layer library (in this example: RFPipe) and contains the radio model’s MAC layer properties such as datarate, jitter and delay. It also defines the radio model’s packet completion rate curve XML file. This curve definition is comprised of a series of SINR (Signal to Interference plus Noise Ratio) values along with their corresponding probability of reception. The radio model uses the packet completion rate curve to determine an incoming packet’s probability of reception.

The experimentation environment consists of 17 different sets of radio model configuration files, all of which are similar in format to the configuration files discussed in this section but define different values for the various parameters.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE phy SYSTEM 'file:///usr/share/emane/dtd/phy.dtd'>
<phy name="universalphy">
  <param name="bandwidth" value="250K"/>
  <param name="frequency" value="3000000000"/>
  <param name="frequencyofinterest" value="3000000000"/>
  <param name="subid" value="1"/>
  <param name="systemnoisefigure" value="12.0"/>
  <param name="txpower" value="47.0"/>
  <param name="fixedantennagain" value="0.0"/>
  <param name="fixedantennagainenable" value="on"/>
  <param name="noisemode" value="none"/>
  <param name="noisebinsize" value="20"/>
  <param name="propagationmodel" value="precomputed"/>
</phy>
```

Figure D-34: Wideband1 Radio Model PHY Parameters.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE mac SYSTEM 'file:///usr/share/emane/dtd/mac.dtd'>
<mac library="rfpipemac" name="RF-PIPE MAC">
  <param name="enablepromiscuousmode" value="off"/>
  <param name="datarate" value="175K"/>
  <param name="flowcontrolenable" value="off"/>
  <param name="flowcontroltokens" value="10"/>
  <param name="pcrcurveuri" value="/usr/share/emane/xml/models/mac/rfpipe/rfpipepcr.xml"/>
  <param name="jitter" value="0.0"/>
  <param name="delay" value="0.0"/>
</mac>
```

Figure D-35: Wideband1 Radio Model MAC Parameters.

D.1.5.4 EMANE Event Service Configuration Files

The EMANE event service is responsible for generating mobility and pathloss events for the NEMs running within the emulation. The EMANE event service takes as its input several XML configuration files as well as event files in Emulation Event Log (EEL) format to function correctly. The EMANE mobility and pathloss event configuration files for the Anglova scenario vignettes are located in the `/opt/nato-experiment/event_service_configs` directory shown in Figure D-36.

D.1.5.4.1 Event Service XML

The event service XML configuration file (Figure D-37) defines the multicast channel and interface where events will be published. It also defines the EEL generator configuration file, which contains event parser and multicast channel configurations.

D.1.5.4.2 EEL Generator XML

The EEL generator configuration file (Figure D-38) defines the source EEL event file and the various parser plugins that will be used to parse sentences from the EEL event file.

D.1.5.4.3 EEL Source File

Mobility and pathloss events are stored in and parsed from emulation event log files (Figure D-39). These files consist of time stamped entries for each NEM's GPS location (latitude, longitude, altitude) as well as time stamped entries for the pathloss values between the nodes. Mobility and pathloss events may be combined into a single file or separated into individual files.

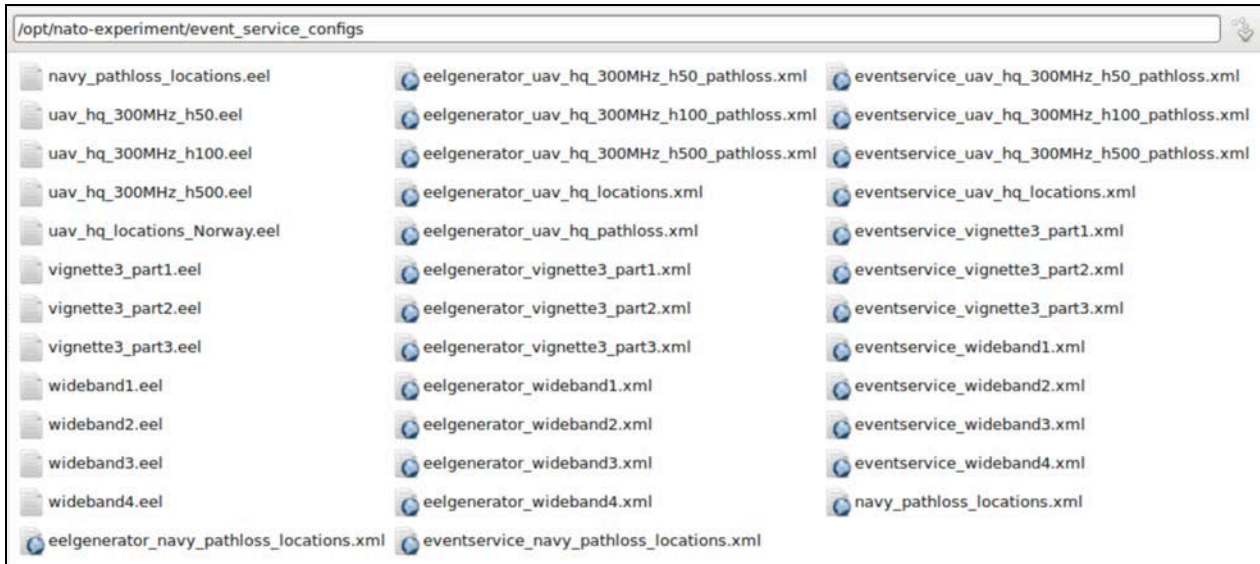


Figure D-36: EMANE Event Service Configuration File System.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE eventservice SYSTEM "file:///usr/share/emane/dtd/eventservice.dtd">
<eventservice>
  <param name="eventservicegroup" value="224.1.2.8:45703"/>
  <param name="eventservicedevice" value="eth1"/>
  <generator definition="eelgenerator_vignette3_part1.xml"/>
</eventservice>
```

Figure D-37: Example Event Service Configuration File.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE eventgenerator SYSTEM "file:///usr/share/emane/dtd/eventgenerator.dtd">
<eventgenerator library="eelgenerator">
  <param name="inputfile" value="vignette3_part1.eel" />
  <paramlist name="loader">
    <item value="commeffect:eelloadercommeffect:delta"/>
    <item value="location,velocity,orientation:eelloaderlocation:delta"/>
    <item value="pathloss:eelloaderpathloss:delta"/>
    <item value="antennaprofile:eelloaderantennaprofile:delta"/>
  </paramlist>
</eventgenerator>
```

Figure D-38: Example EEL Generator Configuration File.

```
0.0 nem:12350 location gps 58.170309,7.944924,2.0
0.0 nem:12350 pathloss nem:12550,0.0 nem:12650,0.0 nem:12700,0.0 nem:12750,0.0 nem:12800,0.0 nem:12850,0.0 nem:12900,0.0 nem:12950,0.0 nem:13000,0.0 nem:13050
0.0 nem:13100,26.2 nem:13150,26.2 nem:13200,26.2 nem:13250,26.2 nem:13300,26.2 nem:13350,26.2 nem:13400,26.2 nem:13450,26.2 nem:13500,26.2 nem:13550,26.2 nem:13600,26.2 nem:13650,26.2 nem:13700,0.0 nem:13750,26.2
0.0 nem:12400 location gps 58.170309,7.944924,2.0
0.0 nem:12400 pathloss nem:12600,0.0 nem:13200,10.7 nem:13850,17.3 nem:14100,17.3 nem:14700,17.3 nem:15350,19.5 nem:15550,19.5 nem:16150,10.7
0.0 nem:12450 location gps 58.170309,7.944924,2.0
0.0 nem:12450 pathloss nem:13900,32.9 nem:15400,35.0
0.0 nem:12500 location gps 58.170309,7.944924,2.0
0.0 nem:12500 pathloss nem:13740,0.0 nem:13775,10.7 nem:14000,17.3 nem:15180,17.3 nem:15250,17.3 nem:15450,19.5 nem:16680,19.5 nem:16750,10.7 nem:16800,55.9
0.0 nem:12550 location gps 58.170309,7.944924,2.0
0.0 nem:12550 pathloss nem:12350,0.0 nem:12650,0.0 nem:12700,0.0 nem:12750,0.0 nem:12800,0.0 nem:12850,0.0 nem:12900,0.0 nem:12950,0.0 nem:13000,0.0 nem:13050
0.0 nem:13100,26.2 nem:13150,26.2 nem:13200,26.2 nem:13250,26.2 nem:13300,26.2 nem:13350,26.2 nem:13400,26.2 nem:13450,26.2 nem:13500,26.2 nem:13550,26.2 nem:13600,26.2 nem:13650,26.2 nem:13700,0.0 nem:13750,26.2
```

Figure D-39: Example EEL File.

D.1.5.5 Experimentation Scripts

There are two scripts that manage the starting and stopping of the experimentation environment, *start_anglova_experiment.sh* and *stop_anglova_experiment.sh*. These two scripts are the only scripts that are explicitly executed by the user on the command line. The other scripts that will be discussed (*start_emane.sh** and *stop_emane.sh*) are not explicitly executed by the user, but are instead executed indirectly by the *start_anglova_experiment.sh* and *stop_anglova_experiment.sh* scripts.

D.1.5.5.1 *start_anglova_experiment.sh*

The *start_anglova_experiment.sh* script is responsible for starting the EMANE emulation of the various Anglova vignettes. The *start_anglova_experiment.sh* input parameters are shown in Figure D-40. This script requires 3 parameters:

- (-c) The name of the DAVC experimentation cluster that was created in Section D.1.4.2.
- (-n) The number of VMs that are available in the cluster to be mapped to Anglova scenario nodes. This number should not include the experimentation controller VM.
- (-v) The Anglova vignette that will be executed. The possible options are:
 - 2: Vignette 2 (Deployment of the Coalition Forces).
 - 3-1: Vignette 3 Part 1 (Insurgent Neutralization).
 - 3-2: Vignette 3 Part 2 (IED Neutralization).
 - 3-3: Vignette 3 Part 3 (Medevac of Wounded).
 - Custom: Custom vignette where the user specifies which groups will be executed.
- (-s) The IP Address of the SDT-3D visualization application (see Section D.1.6.1).

```
start_anglova_experiment.sh [-h] [-c Cluster Name] [-n Available VMs] [-v Vignette] [-s SDT-3D IP]
-- Starts the EMANE Emulation of the specified Anglova Vignette

where:
-h Shows this help text.
-c Experimentation cluster name.
-n Number of available virtual machines excluding the experiment controller.
-v Anglova Vignette to start:
    2 = Vignette 2
    3-1 = Vignette 3 part 1
    3-2 = Vignette 3 part 2
    3-3 = Vignette 3 part 3
    custom = Custom Vignette (requires editing this script)
-s IP Address of the SDT-3D Visualization Application
```

Figure D-40: *start_anglova_experiment.sh* Script Usage.

When executed the script file does the following:

- 1) Determines which groups in the Anglova scenario should be started in the experimentation environment based on the specified vignette parameter.
- 2) Cycles through the DAVC VM nodes sequentially and assigns each to a group node from the scenario. For example, when executing Vignette 2, the first group node from company1, company1-1, will be assigned to and started on the first DAVC VM node exp-1, company1-2 on exp-2 and so on.
- 3) Reads the network plan file to determine which radio models to start on the chosen node.
- 4) Remotely launches the **start_emane.sh** script with the corresponding EMANE radio model configuration files on the chosen node. The **start_emane.sh** will be discussed next but its execution will ultimately result in the creation of the virtual EMANE interfaces on the chosen node as discussed in Section D.1.5.3.
- 5) Creates an updated host file with host names for each Anglova scenario node in the experiment corresponding to the radios they possess. This host file is copied to each of the DAVC VM nodes. The host file is based on the radio host name and IP addresses outlined in the network plan as shown in Section D.1.5.2, Figure D-24 and Figure D-25.
- 6) Starts the EMANE event service to begin sending the specified vignette's location and path loss events to EMANE event service multicast channel.

D.1.5.5.2 start_emane.sh*

The **start_emane.sh*** scripts are not executed directly by the user but are executed indirectly and remotely by the **start_anglova_experiment.sh** script as discussed in the previous section. Shown in Table D-4 are the 3 versions of the **start_emane.sh*** script that starts the EMANE emulator components on the DAVC VM node, however the **start_emane_olsrv1.sh** and the **start_emane_olsrv2.sh** scripts also start the OLSRv1 or OLSRv2 routing protocols respectively. The **start_emane_none.sh** script does not start a routing protocol. Note that **start_emane.sh** is simply a symbolic link that should be set to point to one of the other **start_emane.sh*** scripts depending on if a routing protocol should be run or not.

Table D-4: The Different Version of the Script that Starts EMANE.

File	Description
start_emane.sh	Symbolic link that points to one of the other start_emane.sh_<routing protocol version> scripts.
start_emane_none.sh	Script to start the EMANE emulator without a routing protocol on a DAVC cluster node.
start_emane_olsrv1.sh	Script to start the EMANE emulator with the OLSRv1 routing protocol on a DAVC cluster node.
start_emane_olsrv2.sh	Script to start the EMANE emulator with the OLSRv2 routing protocol on a DAVC cluster node.

When executed, the **start_emane.sh*** script files do the following:

- 1) Starts the EMANE executable with the EMANE platform configuration file (see Figure D-29) for the assigned Anglova scenario node. This results in the creation of the virtual EMANE interfaces specified in that node's *platform.xml* file.

- 2) Starts the EMANE event daemon executable with the EMANE event daemon configuration file (see Figure D-31) for each NEM present on the Anglova scenario node.
- 3) Starts the GPS Daemon executable. The *gpsd* service collects information from a specified GPS source.
- 4) If *start_emane.sh_olsrv1* or *start_emane.sh_olsrv2* is selected, launches the Optimized Link State Routing (OLSR) protocol on the EMANE interfaces on the chosen node (Figure D-19). For example, on node company1-1, OLSRv1 or OLSRv2 will be started on its emane0 and emane4 network interfaces.

D.1.6 Launching an Anglova Vignette

Now that the experimentation environment's DAVC cluster has been configured and the environment's experimentation scripting has been reviewed, an Anglova scenario emulation can be run. In this section the instructions to launch Anglova Vignette 2 using the DAVC experimentation cluster configured in Section D.1.4 will be outlined. Vignette 2 covers the deployment of the coalition forces, a battalion consisting of 157 nodes, into the operational zone as discussed in Section D.1.2. The same instructions can be used to launch Anglova Vignette 3 parts 1, 2, and 3 with the only difference being the input parameters provided to the *start_anglova_experiment.sh* experimentation scripting discussed in the previous section.

D.1.6.1 Configure Scenario Visualization

The IST-124-061 experimentation environment uses the Naval Research Lab's Scripted Display Tools (SDT-3D) [5] to visualize the emulated scenario's nodes, mobility, links and connectivity on a NASA Whirlwind geographic background. See Figure D-41.



Figure D-41: SDT-3D Visualization Tool.

The experimentation environment template VM contains an EMANE SDT-3D client/server framework (Figure D-42) that enables the sending of visualization commands to a running instance of SDT-3D to visualize the running EMANE emulation. When the experimentation environment is started, the EMANE SDT-3D client starts automatically on each scenario node's VM. This client reads location and network connectivity from the EMANE software and sends that information to the EMANE SDT-3D server, which is started on the experimentation controller VM. The EMANE SDT-3D server uses this information to generate and send SDT-3D commands to visualize the running emulation. The receiving SDT-3D application can run on an external machine as long as that machine has network connectivity to the experimentation controller.

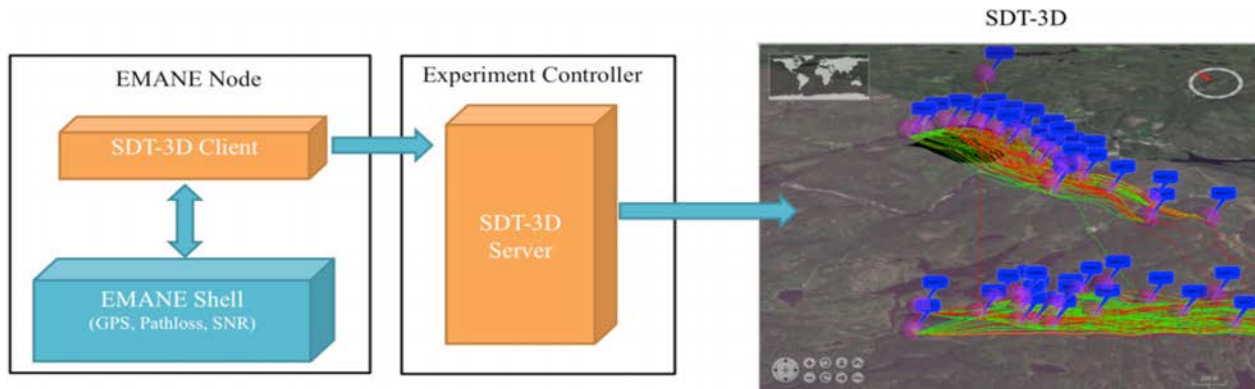


Figure D-42: EMANE SDT-3D Visualization Client/Server Framework.

To configure the SDT-3D application to listen and receive scenario visualization commands from the EMANE SDT-3D server, open the SDT-3D application and in the **'File'** menu select the **'Listen to TCP port...'** option (Figure D-43). Enter port **'55002'** into the input dialog that appears and press **'OK'**. SDT-3D is now configured to listen for visualization commands from the EMANE SDT-3D server. The EMANE SDT-3D server will be configured to send the visualization commands to the SDT-3D application in a later step.

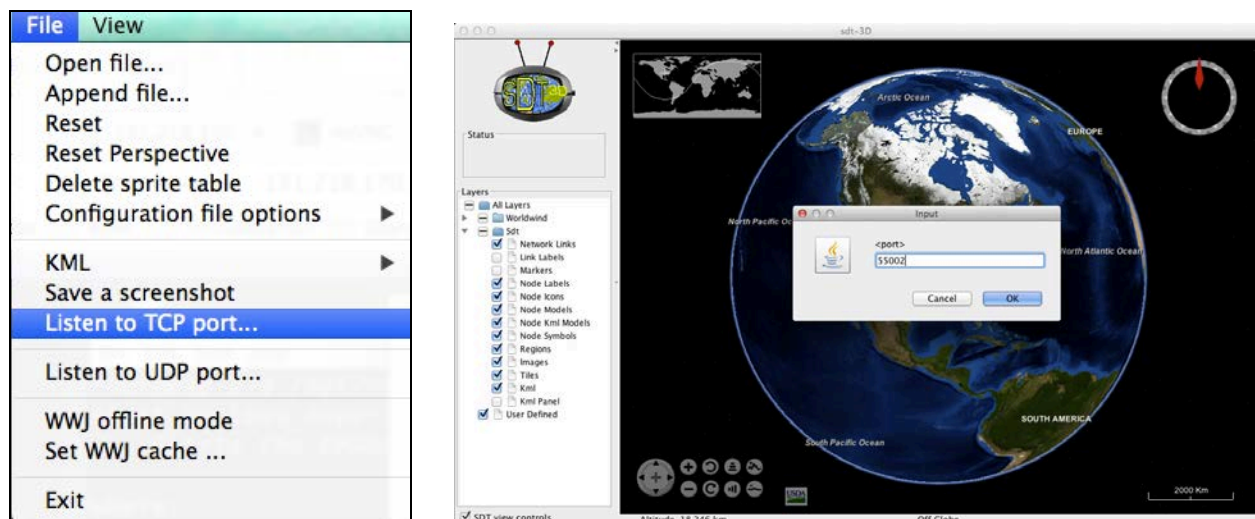


Figure D-43: Configure SDT-3D to Listen on TCP Port 55002.

The EMANE SDT-3D framework will generate an SDT-3D log file containing all of the events processed during the scenario. This file can be loaded into the SDT-3D application to replay the scenario visualization. This feature is useful if an EMANE SDT-3D server is not available. The log file will be located on the

experimentation controller in `/log/<timestamp>.sdt` where `<timestamp>` is the time the experimentation scenario was run. To configure the SDT-3D application to load and replay the scenario visualization, open the SDT-3D application and in the **'File'** menu select the **'Open file...'** option (Figure D-44). Navigate to the SDT-3D log file and press **'OK'**.

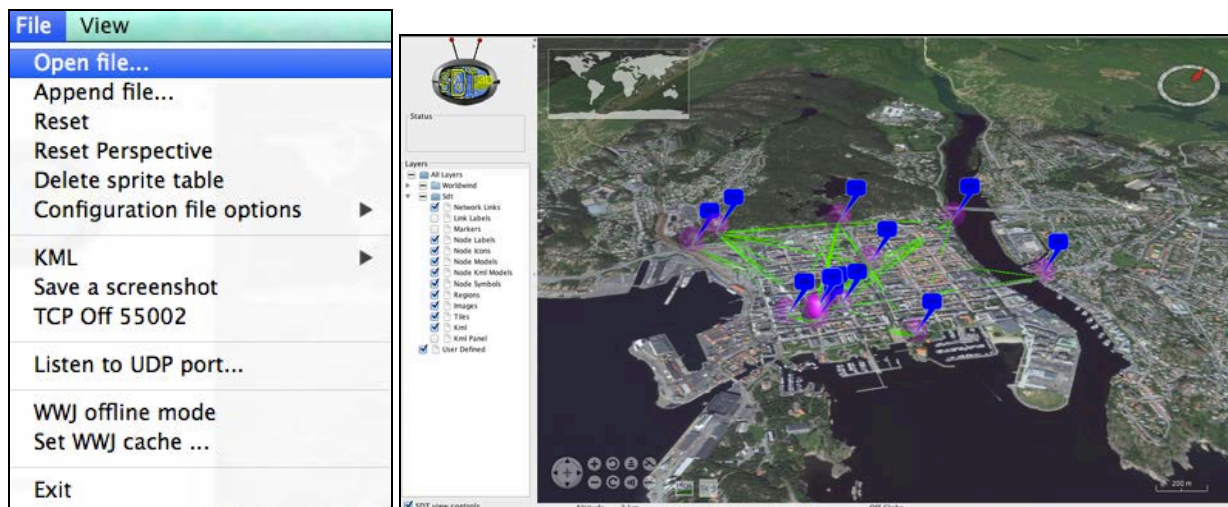


Figure D-44: Configure SDT-3D to Load and Replay an SDT-3D Log File.

D.1.6.2 Log into the Experimentation Controller

The vignette will be executed from the experimentation controller node. From the experiment's DAVC details page, log into VM node 270's Virtual Network Computing (VNC) console by clicking on its **'Open VNC'** button in the **'Node Options'** dropdown menu (Figure D-45).

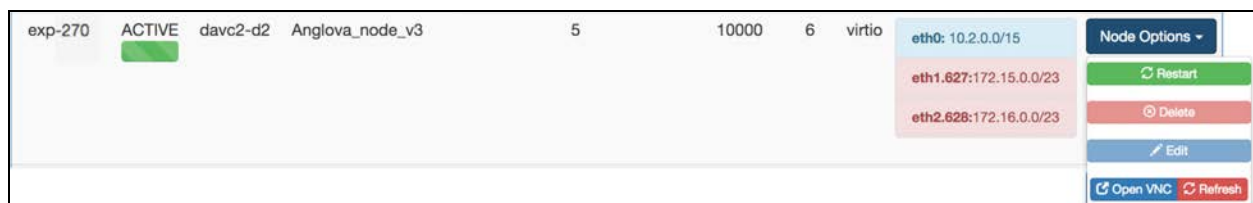


Figure D-45: Log into VM Node 270's VNC Console.

Next, open a console terminal and navigate to the experimentation script's home directory `/opt/nato-experiment` (Figure D-46).

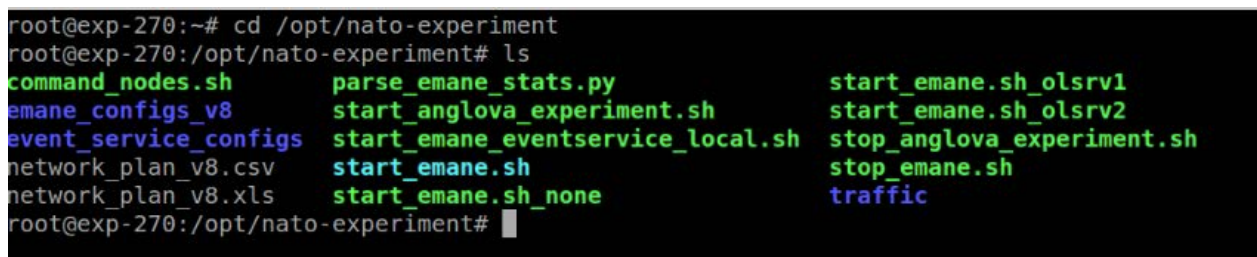


Figure D-46: Navigate to the Experimentation Scripts Home Directory on Node Exp-270.

Next, to start Vignette 2, execute the **start_anglova_experiment.sh** script as shown in Figure D-47, using the following command: **./start_anglova_experiment.sh -c exp -n 269 -v 2 -s 10.2.1.40**. The parameters used in this command specify that Vignette 2 (**-v 2**) will be executed in the ‘exp’ DAVC cluster (**-c exp**), which has 269 available cluster nodes (**-n 269**). The command also specifies the SDT-3D application’s IP Address (**-s 10.2.1.40**) where the EMANE SDT-3D server discussed in Section D.1.6.1 will send visualization commands. The script will launch the experimentation components (EMANE, EMANE event daemon, GPS daemon, etc.) on each scenario node within the DAVC cluster nodes.

```

root@exp-270:/opt/nato-experiment# ./start_anglova_experiment.sh -c exp -n 269 -v 2 -s 10.2.1.40
Adding multicast route, 224.1.2.8, to eth1
Refreshing SDT-3D Visualization Server...
Stopping emanesdtfrmwrk sdt_set_manager_1 ... done
Stopping emanesdtfrmwrk emane_data_queue_1 ... done
Stopping emanesdtfrmwrk redis_server2_1 ... done
Stopping emanesdtfrmwrk redis_server_1 ... done
Removing emanesdtfrmwrk sdt3d_driver_1 ... done
Removing emanesdtfrmwrk sdt_set_manager_1 ... done
Removing emanesdtfrmwrk emane_data_queue_1 ... done
Removing emanesdtfrmwrk redis_server2_1 ... done
Removing emanesdtfrmwrk redis_server_1 ... done
Creating emanesdtfrmwrk redis_server_1
Creating emanesdtfrmwrk redis_server2_1
Creating emanesdtfrmwrk emane_data_queue_1
Creating emanesdtfrmwrk sdt_set_manager_1
Creating emanesdtfrmwrk sdt3d_driver_1

Starting company1 platforms: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Starting scenario node company1-1
Scenario node company1-1 assigned to DAVC cluster node exp-1
NEMS allocated to company1-1: 1 50

Copying script files to exp-1...

start_emane.sh          100% 1548    1.5KB/s   00:00
stop_emane.sh          100% 387    0.4KB/s   00:00
hosts                  100% 23KB   23.0KB/s   00:00

Starting EMANE on node exp-1...

Clearing experiment logs...
rm: cannot remove '/log/*.pcap': No such file or directory
rm: cannot remove '/log/*.tar.gz': No such file or directory
Adding multicast route, 224.1.2.8, on eth1...
STOCADDRT: File exists
Starting EMANE...
emane /opt/nato-experiment//emane_configs_v8/company1/platform1.xml -r -d -l 4 -f /log/emane1.log
Starting EMANE event daemon for NEM 1....

```

Figure D-47: Vignette 2 Execution Output.

The script also performs other actions including launching an EMANE SDT-3D visualization framework client and OLSR routing (Figure D-48) on the cluster nodes as well. The EMANE event service discussed in Section D.1.5.4 is also started on the experimentation controller node with the corresponding mobility and pathloss EEL files for Vignette 2.

After the **start_anglova_experiment.sh** script completes the vignette is now running. The SDT-3D instance will begin to update showing the vignette’s nodes, their mobility and connectivity (Figure D-49). Refer to the network plan discussed in D.1.5.2 to identify the nodes involved in the vignettes. Each node can be accessed via their DAVC VNC console or via ssh using their DAVC node names as host names. The network plan also contains the host names and IP addresses for the emulated EMANE radios.

The instructions outlined in this section can be used to run Vignette 3, just specify the appropriate vignette parameter to the **start_anglova_experiment.sh**.

D.1.7 Launching a CUSTOM Anglova Vignette

The **start_anglova_experiment.sh** script can also be used to launch custom vignettes. When running a custom vignette the user specifies which groups should be activated in the vignette. This allows users to run subsets of the nodes in a particular vignette. The group-to-vignette mapping spreadsheet (Figure D-26) discussed in Section D.1.5.2 is especially useful in determining viable custom vignette group combinations. For example, if a user is only interested in running Vignette 3 part 2 with Platoon1 and the Unattended Ground Sensor (UGS) nodes, the user can achieve this by using the ‘**-v custom**’ command line parameter.

ANNEX D – IST-124 EXPERIMENTATION EXECUTION

In addition, the user would not be required to instantiate a DAVC cluster with all 270 VMs. Instead, a DAVC cluster with 35 VMs would be sufficient to run a custom vignette that includes Platoon1 (24 VMs/nodes) and the UGS (10 VMs/nodes). The last VM would be used as the experimentation controller.

```
Starting OLSR Routing....
*** olsr.org - 0.6.6.2-git 0000000-hash 12fa41b5362519d37bea6715ce291978 ***
Build date: 2014-09-11 13:09:19 on toyol
http://www.olsr.org

Parsing file: "/opt/nato-experiment/emane_configs_v8/routing.conf"
Debug level: 0
IpVersion: 4
Lock file /log/olsrd.lock
Clear screen enabled
Link quality aging factor 0.200000
HNA IPv4 entry: 172.100.19.3/255.255.255.255
setting ifs in curr_cfg = 0
HELLO interval: 2.00
HELLO validity: 20.00
TC interval: 0.00
TC validity: 80.00
IPv4 broadcast/multicast: AUTO
Mode: mesh
IPv6 multicast: ::
HELLO emission/validity: 2.00 (d)/20.00 (d)
TC emission/validity: 0.00 (d)/80.00 (d)
MID emission/validity: 0.00/0.00
HNA emission/validity: 0.00/0.00
Autodetect changes: no
IPv4 broadcast/multicast: AUTO
Mode: mesh
IPv6 multicast: ::
HELLO emission/validity: 2.00 (d)/20.00 (d)
TC emission/validity: 0.00 (d)/80.00 (d)
MID emission/validity: 0.00/0.00
HNA emission/validity: 0.00/0.00
Autodetect changes: no
IPv4 broadcast/multicast: AUTO
Mode: mesh
IPv6 multicast: ::
```

Figure D-48: Vignette 2 Execution Output.

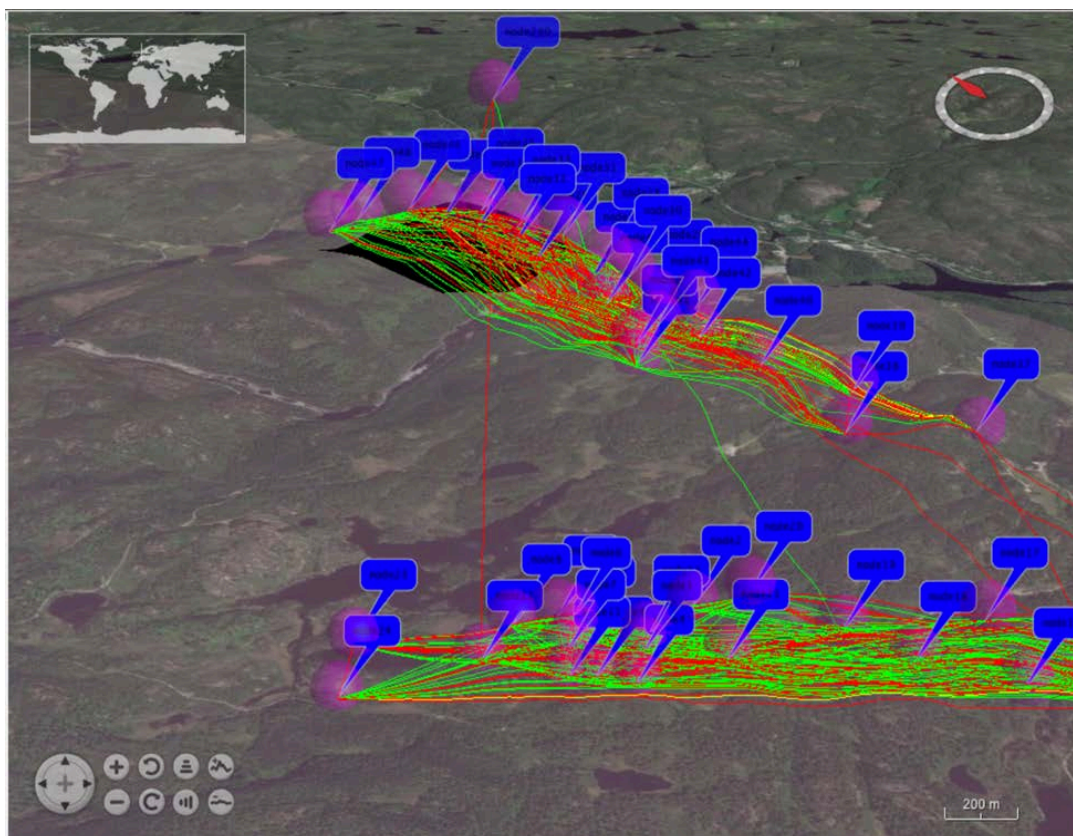
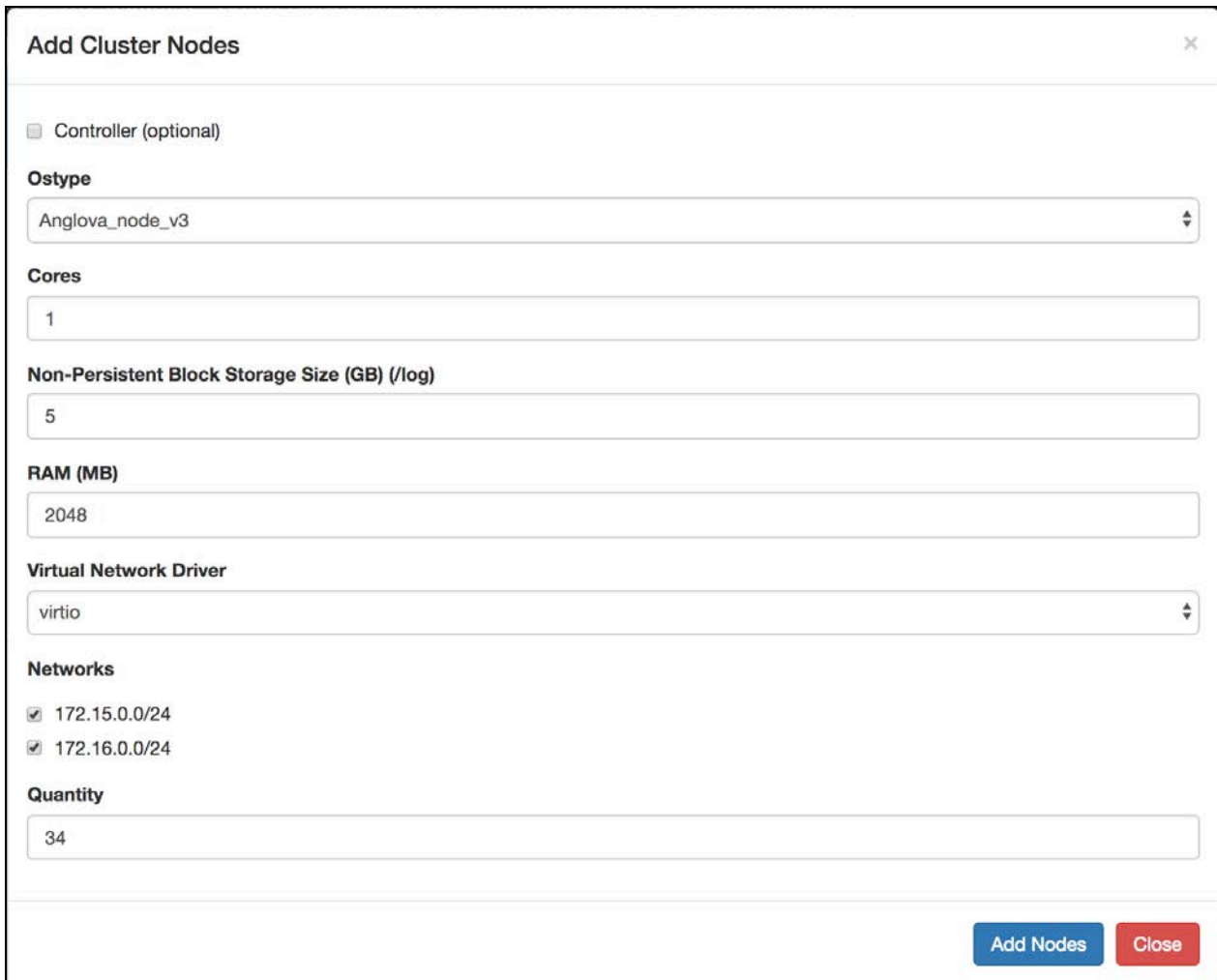


Figure D-49: Vignette 2 Emulation Visualization.

To configure this custom vignette create a DAVC cluster following the steps outlined in Section D.1.4, but instead of configuring 269 VMs, configure 34 VMs as shown in Figure D-50. These VMs will host the 24 Platoon1 and 10 UGS nodes. In general, to calculate the correct number of DAVC VM nodes to configure when preparing a custom vignette, refer to the network plan files discussed Section D.1.5.2. However, it is not a problem to have more VMs in a cluster than are actually assigned to emulated network nodes unless DAVC resources are scarce. In some experimentation setups, having more nodes may be more efficient than creating and deleting DAVC clusters for each individual experiment. Creating a single cluster to accommodate the largest custom vignette would allow different sized vignette experiments to be run in quick succession using the same cluster.



Add Cluster Nodes

☐ Controller (optional)

Ostype
Anglova_node_v3

Cores
1

Non-Persistent Block Storage Size (GB) (/log)
5

RAM (MB)
2048

Virtual Network Driver
virtio

Networks
☒ 172.15.0.0/24
☒ 172.16.0.0/24

Quantity
34

Add Nodes Close

Figure D-50: Example Custom Vignette DAVC Configuration (Platform Nodes).

Configure an additional DAVC VM for the experimentation controller (Figure D-51). The VM should be configured just like the experimentation controller VM outlined in Section D.1.4. The steps to launch and activate the DAVC cluster are the same as in Section D.1.4 with the exception that the experimentation controller is now VM node **exp-35** instead of **exp-270**.

Add Cluster Nodes

☒ Controller (optional)

Virtual Machine Template

Anglova_node_v3

Cores

6

Non-Persistent Block Storage Size (GB) (/log)

5

RAM (MB)

10000

Virtual Network Driver

virtio

Networks
☒ 172.15.0.0/23
☒ 172.16.0.0/23

Quantity

1

Add Nodes

Close

Figure D-51: Example Custom Vignette DAVC Configuration (Controller Node).

The steps to configure the SDT-3D application are the same as outlined in Section D.1.6.1, so no changes are required.

Next, log into the experimentation controller DAVC VNC console where the *start_anglova_experiment.sh* script will be run. However, when running a custom vignette the user must first edit the script to specify the groups that will be included in the vignette.

Navigate to the */opt/nato-experiment* directory and open the *start_anglova_experiment.sh* script file with an editor. Edit the “*ACTIVE_GROUPS*” variable definition starting on line 208 by marking ‘*true*’ for each group that should be included and ‘*false*’ for the groups that should not be included. Save and close the file. Figure D-52 shows the “*ACTIVE_GROUPS*” definition for the custom vignette with Platoon1 and the UGS. The ‘*platoon1**’ and ‘*ugs**’ groups are marked ‘*true*’ while all other groups are marked ‘*false*’.

Next, to start the custom vignette, execute the *start_anglova_experiment.sh* script as shown in Figure D-53, using the following command: *./start_anglova_experiment.sh -c exp -n 34 -v custom -c 10.2.1.40*. The parameters used in this command specify that a custom vignette will be launched (*-v custom*) in the ‘exp’ DAVC cluster (*-c exp*), which has 34 available cluster nodes (*-n 34*). The command also specify the SDT-3D application’s IP Address (*-s 10.2.1.40*) where the EMANE SDT-3D server discussed in Section D.1.6.1 will send visualization commands.

```
"custom")

declare -A ACTIVE_GROUPS=(
[company1]="false"
[company2]="false"
[company3]="false"
[company4]="false"
[command]="false"
[support1]="false"
[support2]="false"
[geo-sat]="false"
[harvest-uav]="false"
[iridium-sat]="false"
[med-helicopter]="false"
[navy]="false"
[platoon1]="true"
[platoon1-APC]="true"
[platoon1-commander]="true"
[platoon1-section-leader]="true"
[platoon2]="false"
[platoon2-APC]="false"
[platoon2-commander]="false"
[platoon2-section-leader]="false"
[platoon3]="false"
[platoon3-APC]="false"
[platoon3-commander]="false"
[platoon3-section-leader]="false"
[tac-sat]="false"
[tac-uav]="false"
[toc-hq]="false"
[ugs]="true"
[ugs-gw]="true"
[ugs-relay]="true"
)
;;
```

Figure D-52: Edit the start_anglova_experiment.sh Script for Custom Vignettes.

```
root@exp-270:/opt/nato-experiment# ./start_anglova_experiment.sh -c exp -n 34 -v custom -s 10.2.1.40
Adding multicast route, 224.1.2.8, to eth1
Refreshing SDT-3D Visualization Server...
Stopping emansdtfrmwrk_sdt3d_driver_1 ... done
Stopping emansdtfrmwrk_emane_data_queue_1 ... done
Stopping emansdtfrmwrk_redis_server_1 ... done
Stopping emansdtfrmwrk_redis_server2_1 ... done
Removing emansdtfrmwrk_sdt3d_driver_1 ... done
Removing emansdtfrmwrk_sdt_set_manager_1 ... done
Removing emansdtfrmwrk_emane_data_queue_1 ... done
Removing emansdtfrmwrk_redis_server_1 ... done
Removing emansdtfrmwrk_redis_server2_1 ... done
Creating emansdtfrmwrk_redis_server2_1
Creating emansdtfrmwrk_redis_server_1
Creating emansdtfrmwrk_emane_data_queue_1
Creating emansdtfrmwrk_sdt_set_manager_1
Creating emansdtfrmwrk_sdt3d_driver_1

Starting platoon1 platforms: 160 161 162 163 164 165 166 167 168 169 171 172 173 174 175 176 177 178 179

Starting scenario node platoon1-1
Scenario node platoon1-1 assigned to DAVC cluster node exp-1
NEMS allocated to platoon1-1: 12650

Copying script files to exp-1...

start_emane.sh          100% 1548    1.5KB/s  00:00
stop_emane.sh           100% 387    0.4KB/s  00:00
hosts                   100% 23KB   23.0KB/s  00:00

Starting EMANE on node exp-1...

Clearing experiment logs...
rm: cannot remove '/log/.pcap': No such file or directory
rm: cannot remove '/log/.tar.gz': No such file or directory
Adding multicast route, 224.1.2.8, on eth1...
SIOCADDRT: File exists
Starting EMANE...
emane /opt/nato-experiment//emane_configs_v8/platoon1/platform160.xml -r -d -l 4 -f /log/emane160.log
Starting EMANE event daemon for NEM 12650...
```

Figure D-53: Example Custom Vignette Execution.

After the script has completed, the custom vignette emulation will be running on the cluster nodes. The SDT-3D instance will begin to update showing the specified vignette nodes, their mobility and connectivity. Each node can be accessed via their DAVC VNC console or via ssh using their DAVC node names as host names. The network plan also contains the host names and IP addresses for the emulated EMANE radios.

D.1.8 Conclusion

The NATO-IST-124 experimentation environment provides a common platform to explore research issues relevant to heterogeneous tactical networks, including routing topology architectures and their impact on delivery rates, overheads, and scalability; data dissemination protocols; quality of service and resource management; and leveraging and integration of sensor networks. This portion of the annex detailed the steps required to launch the EMANE emulation of the IST-124 Anglova experimentation scenario within ARL's DAVC environment. The instructions provided can be used as a guide to launch various subsets of the entire 269-node emulation scenario for a wide range of experimentation backdrops.

D.2 DYNAMICALLY ALLOCATED VIRTUAL CLUSTER (DAVC) MANAGEMENT SYSTEM V2.0 SETUP GUIDE

The Dynamically Allocated Virtual Clustering Management System (DAVC) is an experimentation infrastructure that provides the means to dynamically create, deploy, and manage virtual clusters of heterogeneous nodes within a cloud computing environment. The system allows researchers to create clusters that can be utilized for software development, experimentation, and integration with existing hardware and software. DAVC is built on proven technologies that are open, scalable, and well documented. The system can deploy both stateless nodes via network booting and nodes from Virtual Hard Drives containing a preinstalled operating system. It uses Kernel-based Virtual Machines (KVM) and Quick EMULATOR (QEMU), a full virtualization solution where each virtual machine has private virtual hardware. It also interfaces with Oracle Grid Engine Distributed Resource Management System (DRM) to dynamically assign Virtual Machines (VMs) to hardware resources based on CPU, RAM, hard disk and network traffic. This document is a guide for DAVC system setup and configuration. Please refer to the DAVC User Guide in Section D.3 for specific DAVC usage details.

D.2.1 System Layout

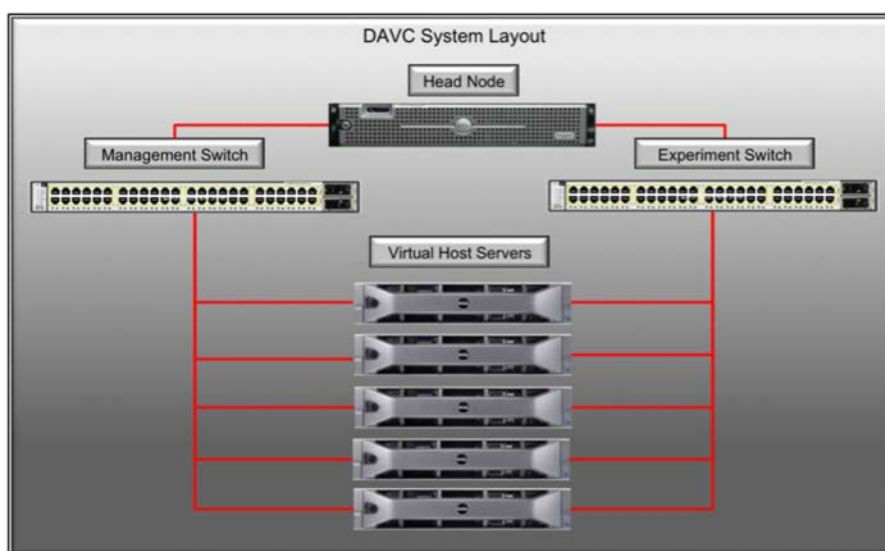


Figure D-54: DAVC System Layout.

Notes:

The characters for single (') and double quotes (") do not always translate correctly if copying from the document to a terminal window. Be prepared to retype quotes if problems arise.

Every command is run as root unless otherwise stated.

D.2.2 Assumptions

This document makes the following assumptions.

D.2.2.1 Number of Systems

The Dynamically Allocated Virtual Cluster (DAVC) Management System will consist of a DAVC Controller (DAVC) and at least two Virtual Host Servers (d1-d2). You may add as many Virtual Host Servers as needed.

D.2.2.2 Operating System

The system will use Ubuntu 14.04 Server 64-bit on both the DAVC Controller and the Virtual Host Servers. Other recent versions of Ubuntu or Debian could be used if one is willing to experiment.

D.2.2.3 Network

The system will consist of two main physical networks: Management and Private (referred to by the name "experiment"). By default, neither of these networks resides on the public Internet. The administrator of the system must have full control over the Management and Private networks. This includes configuring the physical switches and the IP space. In addition, the DAVC Controller contains a link to the Internet, which is called Public. If desired, Network Address Translation (NAT) routing can be configured between the Public and the Management networks. The IP spaces used throughout this installation guide are examples and should be replaced accordingly by the administrator of the system.

D.2.2.3.1 Virtual Host Servers Network Ports**Note:**

The number of ports for the Management and Private bridges can be different across host servers.

- 1 x 1 Gb Ethernet Port for Base Management IP address;
- 4 x 1 Gb Ethernet Port for Management network bridges; and
- 4 x 1 Gb Ethernet Port for Private network bridges.

D.2.2.3.2 Switches

- 1 x Cisco 3750-E Switch (Management); and
 - 1 x Cisco 3750-E Switch (Private).
- or
- 1 x Cisco 2960-S Switch (Management); and
 - 1 x Cisco 2960-S Switch (Private).

D.2.2.3.3 Public (Internet) Network

- Address Space: 126.118.70.0/25.

D.2.2.3.4 Management Network

- Address Space: 10.0.0.0/15; and
- DHCP Range: 10.0.5.0-10.1.255.255.

D.2.3 Network Layout

This section summarizes the network configuration for the DAVC Controller, Virtual Host Servers and the Management and Experiment network switches.

D.2.3.1 DAVC Controller (DAVC)

D.2.3.1.1 Public (Internet) Network

Note:

The IP-Address, Subnet mask, Gateway and DNS name servers will most likely be different in your setup than what is indicated below.

- IP Address 126.118.70.18.
- Subnet mask 255.255.255.128.
- Gateway 126.118.70.1.
- DNS name servers 126.118.70.8.

D.2.3.1.2 Management Network

- IP Address 10.0.0.18.
- Subnet mask 255.254.0.0.

D.2.3.2 Virtual Host Servers

D.2.3.2.1 Management Network

- d1: IP Address 10.0.0.101/15, Gateway 10.0.0.18, DNS name servers 10.0.0.18.
- d2: IP Address 10.0.0.102/15, Gateway 10.0.0.18, DNS name servers 10.0.0.18.

D.2.4 Network Switches Configuration

D.2.4.1 Management Network Switch

Be sure to do the following:

- Remove all VLANs except for default; and
- Set ports to access.

D.2.4.2 Private (Experiment) Network Switch

Be sure to do the following:

- Remove all VLANs except for the default; and
- Set ports to trunk (requires incoming and outgoing traffic to be VLAN tagged).

D.2.4.3 Cisco 3750-E Configuration Instructions

Notes:

Connect to the switch using serial console, telnet, HTTP, or SSH to execute the following commands:

```
Switch> enable
Switch# configure terminal
Switch# vlan 300-999
Switch# end
Switch# show vlan

Switch# configure terminal
Switch# interface range g4/0/1-48
Switch# switchport trunk encapsulation dot1q
Switch# switchport mode trunk
Switch# end
Switch# show interfaces status
Switch# write
```

There is a limit to the number of Spanning Tree Protocol instances that can run at once. The VLANs get created, but it seems that only 128 VLANs can be in use with STP running.

D.2.5 DAVC Controller Base Configuration

This section covers the steps needed to configure the DAVC Controller.

D.2.5.1 Install Operating System

D.2.5.1.1 Install Ubuntu 14.04 Server 64-bit

Do the following:

- Select a minimal install;
- Set the hostname to ‘davic’; and
- Configure Automatic Updates.

D.2.5.1.2 Configure User/Group Accounts

Configure User/Group accounts as normal.

D.2.5.2 Install Required Packages

Execute the following:

```
]# aptitude -P install openssh-client openssh-server build-essential ethtool ntp
dstat sysv-rc-conf dnsmasq syslinux nfs-kernel-server libdrmaa-dev libapache2-
mod-wsgi python-setuptools xfsprogs python-pip ubuntu-virt
```

D.2.5.3 Create DAVC Group

Create a ‘davic’ group:

```
]# groupadd davic -g 1001
```

D.2.5.4 Configure DAVC Group Permissions

Give the 'davic' group the following permissions in /etc/sudoers:

```
#DAVC v2.0
%davc ALL=NOPASSWD: /opt/davc2.0/davc/scripts/vmscripts/dnsmasq.sh, /bin/chown,
/bin/chmod, /sbin/tune2fs, /sbin/mkfs*, /usr/bin/uuidgen, /usr/bin/qemu-img*
```

D.2.5.5 Create DAVC Directories

Create the following directories:

```
]# mkdir -p /opt/davc2.0
]# mkdir -p /home/PIDs/VHDs
]# chown -R root:davc /home/PIDs
]# chmod 775 -R /home/PIDs
```

D.2.5.6 Install Django 1.7 and Dependencies

```
]# pip install Django==1.7.1
]# pip install django_mathfilters
]# pip install django_bootstrap3==6.2.2
]# pip install djangorestframework
]# pip install django-progressbarupload
]# pip install netaddr
]# pip install ipcalc
]# pip install minixsv
]# apt-get install python-libvirt
```

D.2.5.7 Extract DAVC Package

```
]# tar -xvf davc_<version>.tar.gz --directory /opt/davc2.0
]# chown -R root:davc /opt/davc2.0
]# chmod 775 -R /opt/davc2.0
```

D.2.6 Network Configuration

Note:

Make sure the subnet mask is the same for the management network on the interfaces and DNSMASQ.

D.2.6.1 Configure Public and Management Interfaces

Note:

The IP-Address, Subnet mask, Gateway and DNS name servers should be the same as the configurations in Section D.2.3.

```
]# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# auto start
auto lo eth0 eth1

# The loopback network interface
iface lo inet loopback

# Public Network
iface eth0 inet static
address 126.118.70.18
netmask 255.255.255.128
gateway 126.118.70.1
dns-nameservers 126.118.70.8
```

```
# DAVC Management Network
iface eth1 inet static
address 10.0.0.18
netmask 255.254.0.0
```

D.2.7 Name Servers

- 127.0.0.1; and
- 126.118.70.8.

D.2.8 Configure Host File

```
]# cat /etc/hosts
127.0.0.1 localhost

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

## Needed if DNSMASQ goes down

# Management Node
10.0.0.18 davc

# Virtual Host Servers
10.0.0.101 d1
10.0.0.102 d2
```

D.2.8.1 Network Time Protocol (NTP)

Configure NTP as normal.

D.2.8.2 TFTP/PXE (Syslinux)

TFTP/PXE is used to network boot specific Operating System images.

D.2.8.3 Configure Base TFTP/PXE

```
]# mkdir -p /tftpboot/pxelinux.cfg
]# cp -a /usr/lib/syslinux/*pxelinux.0 /tftpboot/

]# ll /tftpboot/ total 120
-rw-r--r-- 1 root root 89501 May 20 2011 gpxelinux.0
-rw-r--r-- 1 root root 26828 May 20 2011 pxelinux.0
drwxr-xr-x 2 root root 4096 Mar 6 16:24 pxelinux.cfg
```

Set permissions and ownership:

```
]# chown -R root:davc /tftpboot
]# chmod -R 775 /tftpboot
```

D.2.8.4 Create Localboot PXE Configuration

```
]# cat /tftpboot/pxelinux.cfg/localboot
DEFAULT local
PROMPT 0
TIMEOUT 0
TOTALTIMEOUT 0
ONTIMEOUT local
LABEL local
LOCALBOOT 0
```

D.2.9 Network File System (NFS)

NFS is used for the root file systems (NFSROOT) for the network boot images.

D.2.9.1 Create Directories and Exports

```
]# mkdir /nodelog
]# chown -R root:davc /nodelog
]# chmod -R 775 /nodelog
]# cat /etc/exports
/tftpboot 10.0.0.0/15(ro,no_root_squash,subtree_check)
/home      10.0.0.0/15(rw,no_root_squash,no_subtree_check)
/nodelog    10.0.0.0/15(rw,no_root_squash,subtree_check)
```

D.2.9.2 Increase NFS Processes (Count Depends on Number of Active NFS Clients)

```
]# cat /etc/default/nfs-kernel-server
RPCNFSDCOUNT=32
```

D.2.9.3 Restart NFS Server

```
]# service nfs-kernel-server restart
```

D.2.9.4 Verify NFS

```
]# showmount -e
Export list for davc:
/nodelog 10.0.0.0/15
/home    10.0.0.0/15
/tftpboot 10.0.0.0/15
```

D.2.10 DNSMASQ

DNSMASQ provides DHCP, DNS, and TFTP service for all DAVC Cluster Nodes.

D.2.10.1 Configure DNSMASQ

D.2.10.1.1 Create the DAVC DNSMASQ Directory

```
]# mkdir /etc/dnsmasq.d/davc
]# chmod 775 /etc/dnsmasq.d/davc/
```

D.2.10.1.2 Set the DNSMASQ Conf-dir Variable In /etc/dnsmasq.conf

```
]# grep ^\[^\#] /etc/dnsmasq.conf
conf-dir=/etc/dnsmasq.d
```

D.2.10.1.3 Update the DNSMASQ base-dnsmasq.conf file

```
]# cat /etc/dnsmasq.d/base-dnsmasq.conf
# /etc/dnsmasq.d/base-dnsmasq.conf
```

****Set 'conf-dir' to the /etc/dnsmasq.d/davc directory previously created.**

```
### Add DAVC Directory
conf-dir=/etc/dnsmasq.d/davc
```

****Set 'interface' to the Management network interface on the DAVC Controller.**

```
### General Settings (depends on site)
## listen only on this interface
```

```
interface=eth1
bogus-priv cache-size=5000
log-queries
log-dhcp
```

****Set 'server' to DNS Server on the public network.**

```
## Hard Code Upstream DNS Server(s)
no-resolv
server=126.118.70.8
```

****Add the following DHCP options, ensure the 'dhcp-option=option:router' option is set to the DAVC Controller's Management network IP address.**

```
### DHCP
dhcp-lease-max=5000
dhcp-option=vend:PXEClient,1,0.0.0.0
dhcp-option-force=208,f1:00:74:7e
dhcp-option=option:router,10.0.0.18
dhcp-boot=pxelinux.0
```

```
## Needed for old gPXE/KVM clients
dhcp-no-override
```

****Set the dhcp range for the dhcp clients on the DAVC Cluster Nodes. Set the network tag to 'management-net'. The DAVC Cluster Nodes dhcp range should begin at an offset to leave space on the Management network for statically addressed DAVC Virtual Host Servers. Here we assume the DAVC Virtual Host Servers will be given static IP addresses prior to 10.0.0.20 and the DAVC Cluster Nodes will receive DHCP configured IP addresses starting at 10.0.0.20 and up to 10.1.255.254.**

```
##DHCP Range
dhcp-range=management-net,10.0.0.20,10.1.255.254,static,255.254.0.0,1h
```

****Enable TFTP.**

```
## TFTP
enable-tftp
tftp-root=/tftpboot
tftp-max=1000
```

D.2.11 IPTABLES

Ubuntu uses UFW (Uncomplicated Firewall) to manage IPTABLES.

D.2.11.1 Enable UFW

```
]# cat /etc/ufw/ufw.conf
# Set to yes to start on boot.
# If setting this remotely, be sure to add a rule
# to allow your remote connection before starting ufw.
# Eg: 'ufw allow 22/tcp'
ENABLED=yes

# Please use the 'ufw' command to set the loglevel.
# Eg: 'ufw logging medium'.
# See 'man ufw' for details.
LOGLEVEL=low

]# ufw enable
```

D.2.11.2 Add Rules

Note:

eth0 is the Public interface and eth1 is the Management interface.

```
]# cat /etc/ufw/after.rules
# Don't delete these required lines, otherwise there will be errors
*filter
:ufw-after-input - [0:0]
:ufw-after-output - [0:0]
:ufw-after-forward - [0:0]

# End required lines
# don't log noisy services by default
-A ufw-after-input -p udp --dport 137 -j ufw-skip-to-policy-input
-A ufw-after-input -p udp --dport 138 -j ufw-skip-to-policy-input
-A ufw-after-input -p tcp --dport 139 -j ufw-skip-to-policy-input
-A ufw-after-input -p tcp --dport 445 -j ufw-skip-to-policy-input
-A ufw-after-input -p udp --dport 67 -j ufw-skip-to-policy-input
-A ufw-after-input -p udp --dport 68 -j ufw-skip-to-policy-input

# don't log noisy broadcast
-A ufw-after-input -m addrtype --dst-type BROADCAST -j ufw-skip-to-policy-input

### DAVC ###
# Added for DAVC
-A ufw-after-input -m state --state NEW -p tcp --dport 22 -j ACCEPT
-A ufw-after-input -i eth1 -j ACCEPT

# For routing, uncomment the next two lines

#-A ufw-after-forward -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
#-A ufw-after-forward -i eth1 -o eth0 -j ACCEPT
### DAVC ###

# don't delete the 'COMMIT' line or these rules won't be processed
COMMIT
```

D.2.11.3 Enable NAT Routing (if Desired)

D.2.11.3.1 Enable Kernel Forwarding

```
]# cat /etc/ufw/sysctl.conf
net/ipv4/ip_forward=1
```

D.2.11.3.2 Uncomment ufw-after-forward Lines in /etc/ufw/after.rules

```
# For routing, uncomment the next two lines
-A ufw-after-forward -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
-A ufw-after-forward -i eth1 -o eth0 -j ACCEPT
```

D.2.11.3.3 Add Routing Rules to End of after.rules

```
]# cat /etc/ufw/after.rules
### DAVC ###
# Added for DAVC NAT
*nat
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -s 10.0.0.0/15 -o eth0 -j MASQUERADE COMMIT
### DAVC ###
```


D.2.11.4 Allow BootPS, DNS, DNSMASQ, DAVC (Port 8001), and Gridengine (Ports 6444 and 6445)

```
]# ufw allow bootps
]# ufw allow 53
]# ufw allow 67
]# ufw allow 8001
]# ufw allow 6445
]# ufw allow 6444
```

D.2.11.5 Restart UFW

```
]# service ufw restart
```

D.2.12 Secure Shell (SSH) Client Configuration

D.2.12.1 Turn Off StrictHostKeyChecking for SSH Client

```
]# cat /etc/ssh/ssh_config
*
*
*
StrictHostKeyChecking no
*
*
*
```

D.2.12.2 Passwordless SSH for Root

D.2.12.2.1 Generate Key

```
]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): Enter passphrase (empty for
no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa. Your public key has been
saved in /root/.ssh/id_rsa.pub.
The key fingerprint is: 19:22:22:22:22:22:22:22:22:22:22:22:3a:fb:c6:51 root@davc The
key's randomart image is:
<randomart image>
```

D.2.12.2.2 Configure Authorized Key

```
]# cd /root/.ssh
]# cat id_rsa.pub >authorized_keys
```

D.2.12.3 Services

Disable unneeded services. Be sure to keep DNSMASQ, UFW, NFS, and SSHD.

D.2.13 Install Mosquitto MQTT (Message Queuing Telemetry Transport)

Mosquitto is the python implementation of the MQTT publish/subscribe framework.

D.2.13.1 Install Python Dependencies for Mosquitto

```
]# apt-get install python-software-properties python-setuptools
```

D.2.13.2 Add Mosquitto Repository

```
]# apt-add-repository ppa:mosquitto-dev/mosquitto-ppa  
]# apt-get update
```

D.2.13.3 Install Mosquitto

```
]# aptitude install mosquitto  
]# pip install paho-mqtt
```

D.2.14 Virtual Host Servers Base Configuration

This section covers the steps needed to configure the DAVC Virtual Host Servers.

D.2.14.1 Install Operating System

D.2.14.1.1 Install Ubuntu 14.04 Server 64-bit

Do the following:

- Select a minimal install;
- Set host name to dn (d1 and d2 in this example); and
- Configure Automatic Updates.

D.2.14.1.2 Configure User/Group Accounts

Configure User/Group accounts as normal.

D.2.14.2 Create DAVC Group

Create a 'davic' group.

```
]# groupadd davc -g 1001
```

D.2.14.3 Configure DAVC Group Permissions

Give the davc group the following permissions in /etc/sudoers.

```
#DAVC 2.0  
%davic ALL=NOPASSWD: /bin/kill, /bin/chown, /bin/chmod, /usr/bin/virt-install*,  
/usr/bin/ovs*,  
/usr/bin/virsh*, /sbin/brctl*, /sbin/ifconfig*, /usr/sbin/tunctl*, /sbin/ifconfig*,  
/etc/init.d/apache2 restart, /etc/init.d/libvirt-bin*, /usr/sbin/service libvirt-bin*
```

D.2.14.4 Create DAVC Directories

Create the DAVC home directory.

```
]# mkdir -p /opt/davic2.0
```

Create the DAVC image directory – it can be a directory or a mount point.

```
]# mkdir -p /davic/{backups,images,blocks,vnc}  
]# mkdir -p /davic/images/repository/VHDs
```

Set the DAVC directory's owner and permission.

```
]# chown -R root:davic /davic  
]# chmod 775 -R /davic
```

D.2.14.5 Extract DAVC Package

```
]# tar -xvf davc_<version>.tar.gz --directory /opt/davc2.0  
]# chown -R root:davc /opt/davc2.0  
]# chmod 775 -R /opt/davc2.0
```

D.2.14.6 Install Required Packages

Execute the following:

```
]# aptitude -P install openssh-client openssh-server build-essential ubuntu-virt  
ethtool ntp dstat sysv-rc-conf nfs-common uml-utilities kvm-ipxe x11-apps vinagre  
openvswitch-switch xfsprogs curl python-pip
```

D.2.14.7 Compile Libvirt 0.10.0+ from Source

Install pre-reqs from source:

```
]# apt-get install build-essential libyajl-dev libyajl2 libxml2 libxml2-dev  
libdevmapper1.02.1 libdevmapper-dev libnl-3-dev libnl-route-3-dev pkg-config  
libgnutls-dev libpciaccess-dev
```

Run the configuration script, compile and install all utilities and libraries using the standard system paths:

```
]# cd /opt/davc2.0/libvirt  
]# ./configure --prefix=/usr --localstatedir=/var --sysconfdir=/etc  
]# make && make install
```

D.2.14.8 Freeze/Hold Libvirt System Packages

Ensure the libvirt system packages don't get overwritten in the future by marking them on hold.

```
]# apt-mark hold libvirt-bin  
]# apt-mark hold libvirt0  
]# apt-mark hold python-libvirt
```

D.2.14.9 Update the System

Note:

You may need to reboot the system after the upgrade has completed.

```
]# aptitude update  
]# aptitude -P upgrade
```

D.2.14.10 Configure KVM link

Make sure that the KVM script points to the correct version of qemu.

```
]# cat /usr/bin/kvm  
#!/bin/sh exec qemu-system-86_64 -enable-kvm "$@"
```

D.2.15 Network Configuration

D.2.15.1 Configure Host File

Note:

Be sure to remove any 127.0.x.x entry that points to the host name.

ANNEX D – IST-124 EXPERIMENTATION EXECUTION

```

]# cat /etc/hosts
127.0.0.1 localhost

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

## Needed if DNSMASQ goes down

# Management Node
10.0.0.18 davg

# Virtual Host Servers
10.0.0.101 d1
10.0.0.102 d2

```

D.2.15.2 Host Server Network Interface/Bridge Allocation

Figure D-55 shows an example network interface bridge allocation layout for a host server with 9 physical network interfaces. Each physical interface will be mapped to either a Management or Experiment network bridge. Interfaces mapped to a management bridge are connected to the management switch. Interfaces mapped to an experiment bridge are connected to the experimentation switch.

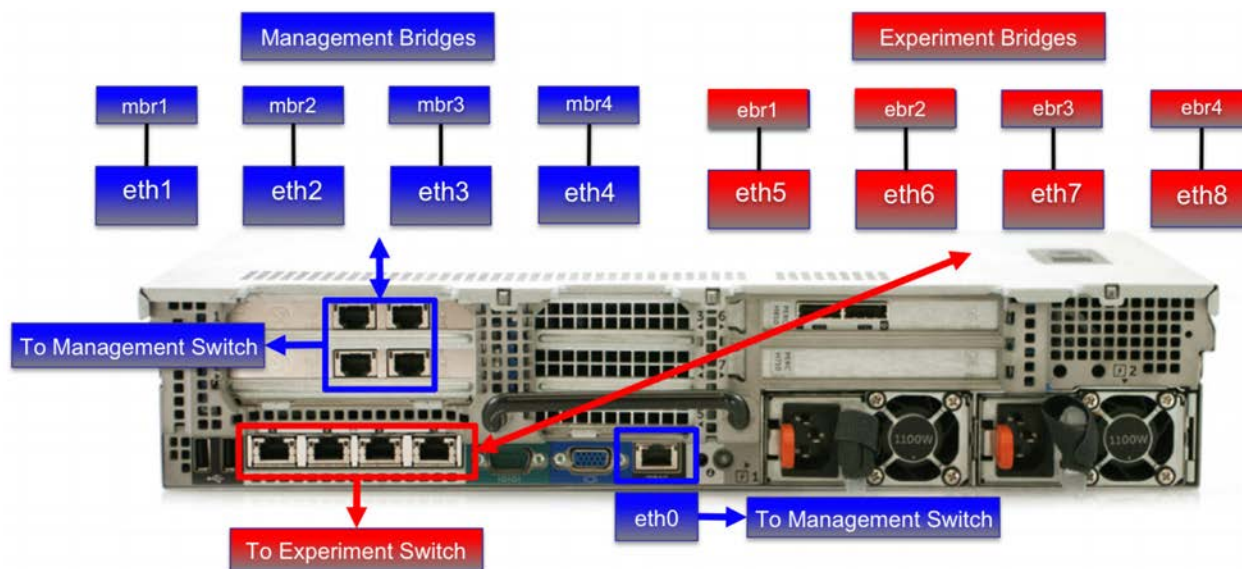


Figure D-55: Host Server Network Interface Bridge Allocation Layout.

D.2.15.2.1 Configure Base Management Interface

```

]# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# auto start
auto lo eth0

# The loopback network interface
iface lo inet loopback

# DAVC Management Network
iface eth0 inet static

```

```
address 10.0.0.101
netmask 255.254.0.0
gateway 10.0.0.18
dns-nameservers 10.0.0.18
```

D.2.15.2.2 Update /opt/davc2.0/server/davc.config

This file sets values for the DAVC Controller server IP (DAVC_SERVER_IP) and port information (DAVC_SERVER_PORT), the names of the Management (MBRIDGE) and Experiment bridges (EBRIDGE) configured for this host, and the VNC proxy server's Public IP Address (DAVC_VNC_PROXY_IP) and Management IP Address (DAVC_VNC_PROXY_CONTROL_IP).

```
DAVC_SERVER_IP=davc
DAVC_SERVER_PORT=8001
DAVC_VNC_PROXY_CONTROL_IP=d1
DAVC_VNC_PROXY_IP=<d1 Public IP Address>
MBRIDGE=mbr0,mbr1,mbr2,mbr3
EBRIDGE=ebr0,ebr1,ebr3,ebr3
```

D.2.15.2.3 Update /opt/davc2.0/server/configure_davc_bridges.sh

Note:

The number of ports for the Management and Private bridges can be different across host servers. Just ensure the appropriate port/bridge mapping is reflected in this script file.

This script configures the bridges for the Management and Experimentation networks. Set MBRIDGE to a comma separated list of the management bridge names on the host server. Set MBRIDGE_PORT to a comma separated list of the corresponding network interfaces associated with each MBRIDGE. Update EBRIDGE and EBRIDGE_PORT in the same manner for the experimentation bridges and network interfaces.

```
MBRIDGE=mbr0,mbr1,mbr2,mbr3
MBRIDGE_PORT=eth1,eth2,eth3,eth4
EBRIDGE=ebr0,ebr1,ebr3,ebr3
EBRIDGE_PORT=eth5,eth6,eth7,eth8
```

If the server does not have a dedicated Management network interface, meaning an interface that is connected to the Management network but not associated with an MBRIDGE, then its Management network IP Address must be associated with one of its MBRIDGES. If this is the case then the last two lines should read as follows:

```
ifconfig eth0 0.0.0.0
ip addr add 10.0.0.101/255.254.0.0 dev mbr0
```

This IP and interface may be adjusted as appropriate for the DAVC Management network. If the server does have a dedicated control network interface then these lines should be removed.

D.2.15.3 Create Management and Experiment Bridges

Note:

Be sure to verify that a bridge gets assigned to the correct physical port (ethn). For example, if ports eth[1-4] are connected to the Management network, then it does not matter if mbr0 gets assigned to eth4 and mbr2 gets assigned to eth1. For convenience and clarity, we assign them in order.

Run the /opt/davc2.0/server/configure_davc_bridges.sh script. The output of ovs-vsctl show should be similar to below.

```

]# /opt/davc2.0/server/configure_davc_bridges.sh
]# ovs-vsctl show
a9136477-3cdf-49b8-b55d-b3b9eff22e26
Bridge "mbr0"
  Port "mbr0"
    Interface "mbr0"
      type: internal
  Port "eth1"
    Interface "eth1"

Bridge "ebr0"
  Port "eth5"
    Interface "eth5"
  Port "ebr0"
    Interface "ebr0"
      type: internal

Bridge "ebr3"
  Port "ebr3"
    Interface "ebr3"
      type: internal
  Port "eth8"
    Interface "eth8"

Bridge "mbr3"
  Port "eth4"
    Interface "eth4"
  Port "mbr3"
    Interface "mbr3"
      type: internal

Bridge "ebr1"
  Port "ebr1"
    Interface "ebr1"
      type: internal
  Port "eth6"
    Interface "eth6"

Bridge "mbr1"
  Port "mbr1"
    Interface "mbr1"
      type: internal
  Port "eth2"
    Interface "eth2"

Bridge "ebr2"
  Port "ebr2"
    Interface "ebr2"
      type: internal
  Port "eth7"
    Interface "eth7"

Bridge "mbr2"
  Port "mbr2"
    Interface "mbr2"
      type: internal
  Port "eth3"
    Interface "eth3"

ovs_version: "1.4.6"

```

D.2.16 Disable Multicast Snooping on Private (Experiment) Bridges

D.2.16.1 Create Script to Run at Start Up

```

]# cat /etc/network/if-up.d/disable_multicast-snooping
#!/bin/sh

# Show multicast_snooping setting
for n in `ls -d /sys/class/net/ebr*`
do

```



```
cat $n/bridge/multicast_snooping
done

# Disable multicast_snooping
for n in `ls -d /sys/class/net/ibr*`
do
    echo 0 >$n/bridge/multicast_snooping
done

# Show multicast_snooping setting
for n in `ls -d /sys/class/net/ibr*`
do
    cat $n/bridge/multicast_snooping
done
```

D.2.16.2 Set Script Permissions

```
]# chmod 755 /etc/network/if-up.d/disable_multicast-snooping
```

D.2.16.3 Restart Networking

```
]# service networking restart
```

D.2.17 SSH Client Configuration

D.2.17.1 Turn Off StrictHostKeyChecking for SSH Client

```
]# cat /etc/ssh/ssh_config
*
*
*
StrictHostKeyChecking no
*
*
*
```

D.2.17.2 Passwordless SSH for Root

Copy /root/.ssh to /root on Virtual Host Server.

Note:

This step is executed on the DAVC Controller (dave).

```
root@davc:~]# ssh-copy-id d1
```

D.2.18 Mount DAVC Controller NFS

This is for DAVC to be able to forcibly stop/delete jobs, if necessary.

D.2.18.1 Create /Home Entry in /etc/fstab

```
]# cat /etc/fstab
# /etc/fstab: static file system information.
#
# Use blkid to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name
# devices that works even if disks are added and removed. See
# fstab(5).
#
```

```
# <file system> <mount point> <type> <options> <dump> <pass> proc /proc proc
nodev,noexec,nosuid 0 0
# / was on /dev/sda1 during installation
UUID=930ef260-1906-4ff9-a79a-56dd3c0ff395 / ext4 errors=remount-ro 0 1

# swap was on /dev/sda5 during installation
UUID=804584c6-b6b6-4d1c-985a-2efaae90cf1d none swap sw 0 0

davc:/home /home nfs defaults 0 0
```

D.2.18.2 Mount/Home

```
]# mount -a
```

D.2.19 NTP

Configure NTP as normal.

D.2.19.1 Configure Services

Disable unneeded services. Be sure to keep SSHD.

D.2.19.2 Libvirt

D.2.19.2.1 Enable Libvirt Service

```
]# service libvirt-bin start
```

D.2.19.2.2 Disable Libvirt Default Network

```
]# virsh net-destroy default
```

D.2.20 Mosquitto MQTT

Mosquitto is the python implementation of the MQTT publish/subscribe framework.

D.2.20.1 Install Python Dependencies for Mosquitto

```
]# apt-get install python-software-properties python-setuptools
```

D.2.20.2 Add Mosquitto Repository

```
]# apt-add-repository ppa:mosquitto-dev/mosquitto-ppa
]# apt-get update
```

D.2.20.3 Install Mosquitto

```
]# aptitude install mosquitto
]# pip install paho-mqtt
```

D.2.21 DAVC ControllerGrid Engine (ge_master) Configuration

This section covers the steps to configure the Grid Engine Job Scheduler on the DAVC Controller.

D.2.21.1 Install Grid Engine

Install the Grid Engine master and client tools.

```
]# aptitude -P install gridengine-master gridengine-client python-drmaa
```

D.2.21.2 Postfix Configuration

dpkg may ask to configure Postfix. Say no.

Postfixno configuration

D.2.21.3 Configure Grid Engine Software

D.2.21.3.1 dpkg Portion

dpkg will then ask to configure Grid Engine. Say yes.

```
Configure SGE automatically? Yes cell: default
master hostname: dave
```

```
Setting up gridengine-master (6.2u5-3ubuntu1) ...
Initializing cluster with the following parameters:
=> SGE_ROOT: /var/lib/gridengine
=> SGE_CELL: default
=> Spool directory: /var/spool/gridengine/spooldb
=> Initial manager user: sgeadmin
Initializing spool (/var/spool/gridengine/spooldb)
Initializing global configuration based on /usr/share/gridengine/default-
configuration
Initializing complexes based on /usr/share/gridengine/centry
Initializing usersets based on /usr/share/gridengine/usersets Adding user
sgeadmin as a manager
Cluster creation complete
```

D.2.21.3.2 Manual Portion

Set the Grid Engine daemons to start on boot up.

```
]# cat /etc/default/gridengine
# Sun Grid Engine configuration
# Boolean options in this file must be set to yes or no

# Start the queue master daemon? (if installed) SGE_START_MASTERD=yes

# Start the execution daemon? (if installed)
SGE_START_EXECD=yes

# SGE_ROOT will default to /var/lib/gridengine SGE_ROOT=/var/lib/gridengine

# SGE_CELL will default to default
SGE_CELL=default
```

Note:

The Ubuntu Grid Engine package places its main configuration files and spooling directories in the following locations:

- /usr/share/gridengine/
- /var/lib/gridengine/

D.2.21.3.3 Export Grid Engine Root

Create file /etc/profile.d/env.sh and add the following line:

```
export SGE_ROOT=/var/lib/gridengine
```

D.2.21.4 Configure Grid Engine Multi-Core Processor Bindings Support

The multi-core processor binding software is located in the DAVC software package tar file in the following directory:

```
/gridengine/sge-hwloc-ssl.tar.gz
```

Unzip the contents of the sge-hwloc-ssl.tar.gz into a temporary folder <tmp>.

```
]# tar -xvf sge-hwloc-ssl.tar.gz
```

Replace the loadcheck file.

```
]# cp <tmp>/utilbin/lx26-amd64/loadcheck /usr/lib/gridengine/
```

D.2.22 Virtual Host Servers Grid Engine (execd) Configuration

This section covers the steps to configure the Grid Engine Job Scheduler on the DAVC Virtual Host Servers.

D.2.22.1 Install Grid Engine

Only install the execd portion of Grid Engine.

```
]# aptitude -P install gridengine-exec
```

D.2.22.2 Postfix Configuration

dpkg may ask to configure Postfix. Say no.

Postfixno configuration

D.2.22.3 Configure Grid Engine Software

D.2.22.3.1 dpkg Portion

dpkg will then ask to configure Grid Engine. Say yes.

```
Configure SGE automatically? Yes cell: default
master hostname: dave
Setting up gridengine-common (6.2u5-3ubuntu1) ...
Creating config file /etc/default/gridengine with new version
```

D.2.22.3.2 Manual Portion

Set the Grid Engine daemons to start on boot up.

```
]# cat /etc/default/gridengine
# Sun Grid Engine configuration
# Boolean options in this file must be set to yes or no

# Start the queue master daemon? (if installed) SGE_START_MASTERD=yes

# Start the execution daemon? (if installed)
SGE_START_EXECD=yes

# SGE_ROOT will default to /var/lib/gridengine SGE_ROOT=/var/lib/gridengine

# SGE_CELL will default to default
SGE_CELL=default
```

Note:

The Ubuntu Grid Engine package places execd files in the following locations:

- /var/spool/gridengine/ (Main Messages)
- /tmp/execd_messages.\$PID (Job Error Messages)

D.2.22.4 Configure Grid Engine Multi-Core Processor Bindings Support

The multi-core processor binding software is located in the DAVC software tar file in the following directory:

/opt/davc2.0/gridengine/sge-hwloc-ssl.tar.gz

Unzip the contents of the sge-hwloc-ssl.tar.gz into a temporary folder <tmp>.

```
]# tar -xvf sge-hwloc-ssl.tar.gz --directory <tmp>
```

Replace the sge_shepherd, sge_execd and loadcheck files.

```
]# service gridengine-exec stop
]# cp <tmp>/bin/lx26-amd64/sge_shepherd /usr/lib/gridengine/
]# cp <tmp>/bin/lx26-amd64/sge_execd /usr/lib/gridengine/
]# cp <tmp>/utilbin/lx26-amd64/loadcheck /usr/lib/gridengine/
```

D.2.23 Install libdrmaa.so.1.0

The library libdrmaa.so.1.0 needs to be installed. Copy the file from the DAVC software installation package to the /usr/lib folder.

```
]# cp /opt/davc2.0/gridengine/libdrmaa.so.1.0 /usr/lib
```

D.2.24 Configure Grid Engine Queue**Note:**

Do this on DAVC Controller davc (the Grid Engine Master). All commands can be done as sgeadmin or root.

D.2.24.1 Add Administrative Hosts

Administrative hosts can add, delete, and modify the Grid Engine system.

```
]# qconf -sh davc
]# qconf -ah d1
d1 added to administrative host list
```

```
]# qconf -ah d2
d2 added to administrative host list
```

```
]# qconf -sh d1
d2 davc
```

D.2.24.2 Add Submit Host

Submission hosts can submit jobs to Grid Engine.

```
]# qconf -as davc
davc added to submit host list
]# qconf -ss davc
```

D.2.24.3 Start Exec Hosts

```
]# ssh d1 -C "service gridengine-exec start"  
]# ssh d2 -C "service gridengine-exec start"
```

D.2.24.4 Execution Hosts

Execution hosts run the submitted jobs. They are synonymous with Virtual Host Servers in the DAVC.

D.2.24.4.1 Verify Execution Hosts

Make sure the Virtual Host Servers were added to the execution host list.

```
]# qconf -sel  
d1  
d2
```

D.2.24.4.2 If Needed, Add Exec Hosts

```
]# qconf -ae d1  
]# qconf -ae d2
```

D.2.24.5 Create Queue for All Exec Hosts

Grid Engine execution hosts are grouped within queues. Different queues can be allocated to process different categories of jobs and allow one to perform administrative operations to all of the execution hosts within a queue by referencing the queue name. This step will configure a queue called 'all.q' that will contain all execution hosts.

```
]# qconf -aq all.q  
root@davc added "all.q" to cluster queue list
```

D.2.24.6 Create Host Group List for all.q

A Host Group List is a way to group all execution hosts. This step configures a host group list with all of the Virtual Host Servers/Execution hosts.

D.2.24.6.1 Show Host Group Lists

```
]# qconf -shgrp1  
no host group list defined
```

D.2.24.6.2 Add (Modify) Host Group

To add a new Host Group use the command 'qconf -ahgrp'. To edit an already existing Host Group use the command 'qconf -mhgrp <host group name>'.

```
]# qconf -ahgrp  
group_name @allhosts  
hostlist d1 d2  
  
root@davc added "@allhosts" to host group list
```

D.2.24.6.3 Show Host Group Lists

```
]# qconf -shgrp1  
@allhosts
```


D.2.24.6.4 Show Hosts in Host Group

```

]# qconf -shgrp
@allhosts group_name
@allhosts hostlist d1 d2

```

D.2.25 Modify Queue (all.q)

This section covers the steps needed to configure the Grid Engine queue ‘all.q’. Note below that entries highlighted in a box are to be updated.

D.2.25.1 Add Host Group to Queue (all.q)

```

]# qconf -mq all.q
qname all.q

```

hostlist	@allhosts
seq_no	0
load_thresholds	np_load_avg=1.75
suspend_thresholds	NONE
nsuspend	1
suspend_interval	00:05:00
priority	0
min_cpu_interval	00:05:00
processors	UNDEFINED
qtype	BATCH INTERACTIVE
ckpt_list	NONE
pe_list	make
rerun	FALSE
slots	8
tmpdir	/tmp
shell	/bin/csh
prolog	NONE
epilog	NONE
shell_start_mode	posix_compliant
starter_method	NONE
suspend_method	NONE
resume_method	NONE
terminate_method	NONE
notify	00:00:60
owner_list	NONE
user_lists	NONE
xuser_lists	NONE
subordinate_list	NONE
complex_values	NONE
projects	NONE
xprojects	NONE
calendar	NONE
initial_state	default
s_rt	INFINITY
h_rt	INFINITY
s_cpu	INFINITY
h_cpu	INFINITY
s_fsize	INFINITY
h_fsize	INFINITY
s_data	INFINITY
h_data	INFINITY
s_stack	INFINITY
h_stack	INFINITY
s_core	INFINITY
h_core	INFINITY
s_rss	INFINITY
h_rss	INFINITY
s_vmem	INFINITY
h_vmem	INFINITY

D.2.25.2 Change Load_Thresholds and Slots

Note:

Each Virtual Host Server (execd) may have a different number of slots. The first number listed in the **slots** section is the default value if no entry exists for a specific execd.

```

]# qconf -mq all.q
qname                all.q
hostlist              @allhosts
seq_no               0
load_thresholds      np_load_avg=1
suspend_thresholds   NONE
nsuspend              1
suspend_interval      00:05:00
priority              0
min_cpu_interval      00:05:00
processors            UNDEFINED
qtype                 BATCH INTERACTIVE
ckpt_list             NONE
pe_list              make
rerun                 FALSE
slots                 8, [d1=16], [d2=24]
tmpdir                /tmp
shell                 /bin/csh
prolog                NONE
epilog                NONE
shell_start_mode      posix_compliant
starter_method         NONE
suspend_method         NONE
resume_method          NONE
terminate_method       NONE
notify                00:00:60
owner_list             NONE
user_lists             NONE
xuser_lists           NONE
subordinate_list       NONE
complex_values         NONE
projects              NONE
xprojects              NONE
calendar              NONE
initial_state          default
s_rt                  INFINITY
h_rt                  INFINITY
s_cpu                 INFINITY
h_cpu                 INFINITY
s_fsize               INFINITY
h_fsize               INFINITY
s_data                INFINITY
h_data                INFINITY
s_stack               INFINITY
h_stack               INFINITY
s_core                INFINITY
h_core                INFINITY
s_rss                 INFINITY
h_rss                 INFINITY
s_vmem                INFINITY
h_vmem                INFINITY

```

D.2.25.3 Verify Queue

```

]# qstat -f
queuename    qtype    resv/used/tot.    load_avg    arch    states
-----
all.q@d1     BIP       0/0/1             0.01        lx26-amd64
all.q@d2     BIP       0/0/1             0.01        lx26-amd64

```

D.2.25.4 Create Queue for KVM Exec Hosts

DAVC maintains queues for each hypervisor within the system. Execution hosts configured to run a particular hypervisor are added to the appropriate queue. This step configures a queue for the KVM hypervisor. In the future, when support is added for other hypervisors, additional queues can be created using these same steps by replacing `kvm.q` with `<hypervisor>.q` and `@kvmhosts` with `@<hypervisor>hosts`.

```
]# qconf -aq kvm.q
root@davc added "kvm.q" to cluster queue list
```

D.2.26 Create Host Group List for `kvm.q`

This step configures a host group list with the Virtual Host Servers/Execution hosts configured to run the KVM hypervisor.

D.2.26.1 Show Host Group Lists

```
]# qconf -shgrp1
@allhosts
```

D.2.26.2 Add (Modify) Host Group

To add a new Host Group use the command `'qconf -ahgrp'`. To edit an already existing Host Group use the command `'qconf -mhgrp <host group name>'`.

```
]# qconf -ahgrp group_name @kvmhosts hostlist d1 d2
root@davc added "@kvmhosts" to host group list
```

D.2.26.3 Show Host Group Lists

```
]# qconf -shgrp1
@allhosts @kvmhosts
```

D.2.26.4 Verify Hosts in Host Group

```
]# qconf -shgrp @kvmhosts group_name
@kvmhosts hostlist d1 d2
```

D.2.27 Modify Queue (`kvm.q`)

This section covers the steps needed to configure the Grid Engine queue `'kvm.q'`. Note below that entries highlighted in a box are to be updated.

D.2.27.1 Add Host Group to Queue (`kvm.q`)

```
]# qconf -mq kvm.q
qname          kvm.q
hostlist      @kvmhosts
seq_no         0
load_thresholds np_load_avg=1.75
suspend_thresholds NONE
nsuspend       1
suspend_interval 00:05:00
priority       0
min_cpu_interval 00:05:00
processors     UNDEFINED
qtype          BATCH INTERACTIVE
ckpt_list      NONE
pe_list        make
rerun          FALSE
```

```

slots                        8
tmpdir                      /tmp
shell                      /bin/csh
prolog                     NONE
epilog                    NONE
shell_start_mode           posix_compliant
starter_method             NONE
suspend_method            NONE
resume_method             NONE
terminate_method          NONE
notify                    00:00:60
owner_list                NONE
user_lists                NONE
xuser_lists               NONE
subordinate_list          NONE
complex_values            NONE
projects                  NONE
xprojects                 NONE
calendar                  NONE
initial_state             default
s_rt                      INFINITY
h_rt                      INFINITY
s_cpu                     INFINITY
h_cpu                     INFINITY
s_fsize                   INFINITY
h_fsize                   INFINITY
s_data                   INFINITY
h_data                   INFINITY
s_stack                   INFINITY
h_stack                   INFINITY
s_core                    INFINITY
h_core                    INFINITY
s_rss                     INFINITY
h_rss                     INFINITY
s_vmem                    INFINITY
h_vmem                    INFINITY

```

D.2.27.2 Change load_thresholds and Slots

Note:

Each Virtual Host Server (execd) may have a different number of slots. The first number listed in the **slots** section is the default value, if no entry exists for a specific execd.

```

]# qconf -mq kvm.q
qname kvm.q
hostlist                  @kvmhosts
seq_no                   0
load_thresholds          np_load_avg=1
suspend_thresholds       NONE
nsuspend                 1
suspend_interval         00:05:00
priority                 0
min_cpu_interval         00:05:00
processors               UNDEFINED
qtype                    BATCH INTERACTIVE
ckpt_list                NONE
pe_list                  make
rerun                    FALSE
slots                    8, [d1=16], [d2=24]
tmpdir                   /tmp
shell                   /bin/csh
prolog                  NONE
epilog                  NONE
shell_start_mode        posix_compliant
starter_method          NONE
suspend_method          NONE
resume_method           NONE
terminate_method        NONE

```

```

notify                00:00:60
owner_list            NONE
user_lists            NONE
xuser_lists           NONE
subordinate_list      NONE
complex_values        NONE
projects              NONE
xprojects             NONE
calendar              NONE
initial_state         default
s_rt                  INFINITY
h_rt                  INFINITY
s_cpu                 INFINITY
h_cpu                 INFINITY
s_fsize               INFINITY
h_fsize               INFINITY
s_data                INFINITY
h_data                INFINITY
s_stack               INFINITY
h_stack               INFINITY
s_core                INFINITY
h_core                INFINITY
s_rss                 INFINITY
h_rss                 INFINITY
s_vmem                INFINITY
h_vmem                INFINITY

```

D.2.27.3 Verify All Queues

```

]# qstat -f
queueName      qtype      resv/used/tot.  load_avg      arch          states
-----
all.q@d1       BIP         0/0/1           0.01          lx26-amd64
all.q@d2       BIP         0/0/1           0.01          lx26-amd64
kvm.q@d1       BIP         0/0/1           0.01          lx26-amd64
kvm.q@d2       BIP         0/0/1           0.01          lx26-amd64

```

D.2.28 Modify Custom Complex Attributes

D.2.28.1 Create Custom Complex Attributes

Note:

The attribute **mem_free** is built into Grid Engine, while attributes **custom_mem_free**, **custom_disk_free**, and **custom_vdisk_free** are custom and have to be defined manually.

```

]# qconf -mc
#name          shortcut  type    relop  requestable consumable default urgency
#-----
custom_disk_free  c_df    MEMORY  <=    YES        NO        0        0
custom_mem_free   c_mf    MEMORY  <=    YES        YES       0        0
custom_vdisk_free c_vdf   MEMORY  <=    YES        YES       0        0
mem_free          mf       MEMORY  <=    YES        NO        0        0

```

D.2.28.2 Configure execd for Each Virtual Host Machine

Note:

Set **custom_mem_free** to Virtual Host Server's RAM minus 2 GB (e.g., 32 GB - 2 GB = 30 GB). Set **custom_vdisk_free** to the size of the hard disk minus at least 20 GB. Each execd may have different values.

D.2.28.3 Configure Virtual Host d1

```
]# qconf -me d1
hostname
```

```
d1
```

```
load_scaling          NONE
complex_values        custom_mem_free=30G,custom_vdisk_free=140G
user_lists            NONE
xuser_lists           NONE
projects              NONE
xprojects             NONE
usage_scaling         NONE
report_variables      NONE
```

D.2.28.4 Configure Virtual Host d2

```
]# qconf -me d2
hostname
```

```
d2
```

```
load_scaling          NONE
complex_values        custom_mem_free=30G,custom_vdisk_free=140G
user_lists            NONE
xuser_lists           NONE
projects              NONE
xprojects             NONE
usage_scaling         NONE
report_variables      NONE
```

D.2.29 Create Custom Load Sensor

Note:

Do this on the Virtual Host Servers. You can create one sensor script and then copy it to the other systems.

D.2.29.1 Create custom_disk_free.sh load sensor

```
]# cat /var/lib/gridengine/bin/custom_disk_free.sh
#!/bin/bash
#
# custom_disk_free.sh
#
## Partition where VM images reside
PARTITION=/davc/

## Specify where SGE is installed (not needed for Ubuntu package)
#SGE_ROOT=/var/lib/gridengine
#ARCH='$SGE_ROOT/util/arch'
#HOST='$SGE_ROOT/utilbin/$ARCH/gethostname -name'

## For Ubuntu Grid Engine Package, use system hostname HOST='hostname'
end=false
while [ $end = false ]; do
# -----
# wait for an input
#
read input result=$?
if [ $result != 0 ]; then
end=true
break
fi

if [ "$input" = "quit" ]; then
end=true break
fi

# -----
```



```
# send mark for begin of load report echo "begin"

DFOUTPUT="'df -k $PARTITION| tail -1 | awk 1{ print $4 }1'"
echo "$HOST:custom_disk_free:${DFOUTPUT}k"

# -----
# send mark for end of load report
echo "end"
done
```

D.2.29.2 Set Ownership and Permissions

```
]# chmod 744 /var/lib/gridengine/bin/custom_disk_free.sh
[# chown sgeadmin:sgeadmin /var/lib/gridengine/bin/custom_disk_free.sh
```

D.2.29.3 Copy to All Other Virtual Host Servers

Note:

Make sure that permissions and ownership are correct.

D.2.29.4 Add Custom Load Sensor into Global System

Note:

Do this on the DAVC Controller. Do not change any other line except for the **load_sensor** line.

```
]# qconf -mconf global
load_sensor /var/lib/gridengine/bin/custom_disk_free.sh
```

D.2.29.5 Verify Custom Load Sensors

```
]# qstat -F custom_mem_free,custom_disk_free,slots,mem_free,custom_vdisk_free
queuename      qtype      resv/used/tot.  load_avg      arch          states
-----
all.q@d1       BIP         0/0/16          0.01          lx26-amd64
hl:mem_free=31.046G
hl:custom_disk_free=154.870G
hc:custom_mem_free=30.000G
hc:custom_vdisk_free=140.000G
qc:slots=16
-----
all.q@d2       BIP         0/0/24          0.01          lx26-amd64
hl:mem_free=31.050G
hl:custom_disk_free=154.805G
hc:custom_mem_free=30.000G
hc:custom_vdisk_free=140.000G
qc:slots=24
```

D.2.30 Test Grid Engine System

D.2.30.1 Create Simple Job Script

```
]$ cat simple.sh
#!/bin/sh
#
# request Bourne shell as shell for job
#$ -S /bin/sh
#
#$ -N SIMPLE
#
# merge stdout and stderr
#$ -j yes
```

```
# print date and time
date
hostname

# Sleep for 20 seconds
sleep 20

# print date and time again
date
```

D.2.30.2 Submit Simple Job Script

```
]$ qsub simple.sh
Your job 1 ("SIMPLE") has been submitted
```

D.2.30.3 Verify Simple Job Script is Running

```
]$ qstat -f
queuename      qtype      resv/used/tot.  load_avg      arch          states
-----
all.q@d1       BIP         0/0/16          0.03          lx26-amd64
1             0.50000    SIMPLE      root          r             12/04/2012 15:28:01 1
```

D.2.31 DAVC Controller Configuration

This section covers the steps needed to configure the Apache2 Web Server that will host the DAVC web application.

D.2.31.1 Configure DAVC Software on DAVC Controller

D.2.31.1.1 Configure Apache2 Web Server

Note:

This installation assumes the default Apache user ‘www-data’ will be used. It may be necessary to update the ‘www-data’ user’s password. An alternate Apache user could be used, if so replace the ‘www-data’ with the appropriate user and substitute the appropriate home directory.

DAVC uses the Django Web Application framework and runs within the Apache2 Web Server.

D.2.31.1.2 Configure Apache2 User

Update the Apache user ‘www-data’ shell.

```
]# usermod www-data -s /bin/bash
```

Add the Apache user ‘www-data’ to the ‘davic’ group.

```
]# usermod -a -G davc www-data
```

Create the Apache user ‘www-data’ home directory and set its permissions.

```
]# mkdir /var/www
]# chown -R www-data:www-data /var/www
]# chmod 775 /var/www
```

Create .ssh folder and generate ssh keys

```
]# su www-data
]# cd /var/www/
]# mkdir -p .ssh
```

```

]# chmod 700 .ssh/
]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/var/www/.ssh/id_rsa):
Created directory 1/var/www/.ssh1.
Enter passphrase (empty for no passphrase): Enter same passphrase again:
Your identification has been saved in /var/www/.ssh/id_rsa.
Your public key has been saved in /var/www/.ssh/id_rsa.pub.

```

D.2.31.1.3 Install Apache2 Mod WSGI

```

]# apt-get install libapache2-mod-wsgi
]# a2enmod wsgi

```

D.2.31.1.4 Update the Apache2 Configuration

Update the /etc/apache2/httpd.conf file as shown below. Note that (\) indicates the continuation of a line.

```

Alias /static/admin /usr/local/lib/python2.7/dist-
packages/django/contrib/admin/static/admin
Alias /static/js/progress_bar.js /usr/local/lib/python2.7/dist- \
packages/progressbarupload/static/js/progress_bar.js
Alias /static/jquery.js /opt/davc2.0/davc/src/davcserver/static/jquery.js
Alias /static/client/client.js
/opt/davc2.0/davc/src/davcserver/static/client/client.js
Alias /static/client/createcluster.js
/opt/davc2.0/davc/src/davcserver/static/client/createcluster.js \
Alias /static/client/clonecluster.js \
/opt/davc2.0/davc/src/davcserver/static/client/clonecluster.js
Alias /static/cluster/details.js
/opt/davc2.0/davc/src/davcserver/static/cluster/details.js
Alias /static/system/system.js
/opt/davc2.0/davc/src/davcserver/static/system/system.js
Alias /static/vhd/vhd.js /opt/davc2.0/davc/src/davcserver/static/vhd/vhd.js
Alias /static/blockdisk/blockdisk.js \
/opt/davc2.0/davc/src/davcserver/static/blockdisk/blockdisk.js
Alias /static/provisioning/rmprovisionclientvhd_v2.py \
/opt/davc2.0/davc/src/davcserver/static/provisioning/rmprovisionclientvhd_v2.p
y

```

```

<VirtualHost *:8001>
    ServerAlias davc.com
    WSGIScriptAlias / /opt/davc2.0/davc/src/davc/wsgi.py

    WSGIDaemonProcess davc.com python-path=/opt/davc2.0/davc/src/davc
    WSGIProcessGroup davc.com
    WSGIPassAuthorization On

    <Directory /opt/davc2.0/davc/src/davc>
        <Files wsgi.py>
            Order deny,allow
            Allow from all
            Require all granted
        </Files>
    </Directory>

    <Directory /static>
        Order deny,allow
        Allow from all
        Require all granted
    </Directory>

    <Directory /usr/local/lib/python2.7/dist-
packages/django/contrib/admin/static/admin>
        Order deny,allow
        Allow from all
        Require all granted
    </Directory>

```

```
<Directory /opt/davc2.0/davc/src/davcserver/static>
    Order deny,allow
    Allow from all
    Require all granted
</Directory>

<Directory /usr/local/lib/python2.7/dist-
packages/progressbarupload/static/js>
    <Files progress_bar.js>
        Order deny,allow
        Allow from all
        Require all granted
    </Files>
</Directory>
</VirtualHost>
```

Update the /etc/apache2/ports.conf file as shown below:

```
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf
Listen 80
Listen 8001

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>
```

Update the /etc/apache2/apache2.conf file as shown below:

```
# Include all the user configurations:
Include httpd.conf
```

D.2.31.1.5 Update Apache2 envvars

Update /etc/apache/envvars with DAVC environment variables.

```
#DAVC 2.0 envs
export DAVC_BACKUP_DIR=/davc/backups
export DAVC_DNSMASQ_DIR=/etc/dnsmasq.d/davc
export DAVC_DNSMASQ_ID=managment-net
export DAVC_HOST_NODE_IMAGES_DIR=/davc/images
export DAVC_HOST_REPOSITORY_DIR=/davc/images/repository/VHDs/
export DAVC_KILL_DIR=/home/PIDs
export DAVC_SCRIPTS_DIR=/opt/davc2.0/davc/scripts/vmscripts
export DAVC_SHARE_DIR=/home/PIDs
export DAVC_TFTP_DIR=/tftpbboot
export DAVC_VHD_DIR=/home/PIDs/VHDs/
export DAVC_BLOCK_DISK_DIR=/davc/blocks
export SGE_ROOT=/var/lib/gridengine
export DAVC_NET_CONTROLLER=ovs
export DRMAA_LIBRARY_PATH=/usr/lib/libdrmaa.so.1.0
export PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
```

D.2.31.1.6 Install and Configure MySQL

```
]# apt-get install mysql-server python-dev libmysqlclient-dev python-mysqldb
]# pip install mysql-python
```

D.2.31.1.7 Create DAVC Database

```
]# mysql -u root -p
]# mysql> CREATE DATABASE davc CHARACTER SET utf8;
```

D.2.31.1.8 Create DAVC User

```
]# mysql -u root -p
]#mysql> GRANT ALL PRIVILEGES ON davc.* TO 'davc'@'localhost' IDENTIFIED BY
'<password>' WITH GRANT OPTION;
]#mysql> GRANT ALL PRIVILEGES ON davc.* TO 'davc'@'%' IDENTIFIED BY ' <password>' WITH
GRANT OPTION;
```

D.2.31.1.9 Update the Django Database Connection Information

Edit /opt/davc2.0/davc/src/davc/settings.py and update the davc user's password to the password set above.

```
DATABASES = {
    'default': {
        'ENGINE': 'django.db.backends.mysql',
        'NAME': 'davc',
        'USER': 'davc',
        'PASSWORD': '<password>',
        'HOST': 'localhost',    # Or an IP Address that your DB is hosted on
        'PORT': '3306',
    }
}
```

D.2.31.1.10 Create Database Superuser and Database Tables

Create super user:

```
]# cd /opt/davc2.0/davc/src
]# python manage.py createsuperuser
```

Output:

```
Username (leave blank to use 'root'):
Email address:
Password:
Password (again):
Superuser created successfully.
```

Create databases.

```
]# cd /opt/davc2.0/davc/src
]# python manage.py migrate
```

Output:

```
Operations to perform:
Synchronize unmigrated apps: rest_framework, bootstrap3
Apply all migrations: admin, contenttypes, davcserver, auth, sessions
Synchronizing apps without migrations:
Creating tables... Installing custom SQL...
Installing indexes...
Running migrations:
Applying contenttypes.0001_initial... OK
Applying auth.0001_initial... OK
Applying admin.0001_initial... OK
Applying davcserver.0001_initial... OK
Applying davcserver.0002_auto_20141120_0750... OK
Applying davcserver.0003_auto_20141219_0811... OK
Applying davcserver.0004_auto_20150508_1359... OK
Applying davcserver.0005_blockdisk_quota... OK
Applying davcserver.0006_auto_20150611_1835... OK
Applying davcserver.0007_auto_20150616_1935... OK
Applying davcserver.0008_cluster_istempcreationcluster... OK
Applying davcserver.0009_auto_20150625_1405... OK
Applying davcserver.0010_auto_20150625_1409... OK
Applying davcserver.0011_auto_20150629_1359... OK
Applying davcserver.0012_cluster_resourcespulled... OK
Applying davcserver.0013_auto_20160125_1700... OK
Applying davcserver.0014_auto_20160208_1425... OK
Applying sessions.0001_initial... OK
```

D.2.31.1.11 Add CRON Job to Refresh DAVC

Update /opt/davc2.0/server/start_davc_server.sh and set the root user's password in the curl command to the super user's password created in the previous section:

```
touch /opt/davc2.0/davc/src/davc/wsgi.py
sleep 5
curl -X POST davc:8001/davc/api/server/start/ -u root:<password> -d '{}' -H \
"Content-Type:application/json"
```

Update /etc/crontab to include the following rule:

```
#refresh davc service
00 22 * * * root /opt/davc2.0/server/start_davc_server.sh
```

D.2.31.1.12 Update ProgressbarUpload Python Library to Account for Different JSON Libraries

Perform the copy commands shown below. This will update the ProgressbarUpload python library to use conditional python import statements.

```
]# cp /opt/davc2.0/progressbarupload/views.py /usr/local/lib/python2.7/dist-
packages/ progressbarupload/.
]# cp /opt/davc2.0/progressbarupload/uploadhandler.py \ /usr/local/lib/python2.7/dist-
packages/ progressbarupload/.
```

D.2.32 Configure DAVC Software On Host Servers

D.2.32.1 Configure Apache2 User

Set the Apache2 user 'www-data' password.

```
]# passwd www-data
```

Update the Apache2 user 'www-data' shell.

```
]# usermod www-data -s /bin/bash
```

Add the Apache 2 user 'www-data' to the 'davc' group and 'libvirtd' group.

```
]# usermod -a -G davc www-data
]# usermod -a -G libvirtd www-data
```

Create the Apache2 user 'www-data' home directory and set its permissions.

```
]# mkdir /var/www
]# chown -R www-data:www-data /var/www
]# chmod 775 /var/www
```

Create .ssh folder.

```
]# su www-data
]# cd /var/www/
]# mkdir -p .ssh
]# chmod 700 .ssh/
```

Note:

Perform this next step on the DAVC Controller davc as the 'www-data' user.

```
]# cd /var/www/.ssh
]# ssh-copy-id www-data@<HOSTSERVER>
```


D.2.32.2 Configure Virtual Hard Drive Service (VHD) On Host Servers

The VHD Service is an automated process that copies uploaded VHDs from the DAVC Controller to a local repository on the DAVC Host Server.

D.2.32.2.1 Add the VHD Service to rc.local So it Will Be Started When The Host Servers Boot

The VHD Service Script is located at /opt/davc2.0/hosts/launch_vhdsyncer.sh. The VHD Service script takes the hostname of the DAVC Controller as its only parameter.

Update /etc/rc.local as below:

```
]# cat /etc/rc.local
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
/opt/davc2.0/server/config_davc_bridges.sh
/opt/davc2.0/hosts/launch_vhdsyncer.sh davc &
exit 0
```

D.2.32.2.2 Start the VHD Service

```
]# /opt/davc2.0/hosts/launch_vhdsyncer.sh davc > /dev/null &
```

D.2.33 Create A DAVC System Configuration

A DAVC System Configuration defines system-wide settings and constraints for DAVC Clusters and Cluster Nodes.

D.2.33.1 Access DAVC Web Application Login Page

At this point DAVC should be installed and accessible via a web browser at the following URLs (replace <DAVC CONTROLLER MANAGEMENT IP ADDRESS> or <DAVC CONTROLLER PUBLIC IP ADDRESS> with the correct DAVC Controller IP address):

http://<DAVC CONTROLLER MANAGEMENT IP ADDRESS>:8001/davc or

http://<DAVC CONTROLLER PUBLIC IP ADDRESS>:8001/davc

Log in using the form in the upper right hand part of the DAVC Home Page (Figure D-56). Use the superuser username and password created in Section D.2.31.1.10.

D.2.33.2 Create A New System Configuration

After logging in, Click the 'Create System Config' button in the DAVC System Administration Page (Figure D-57) to access the System Configuration Form.

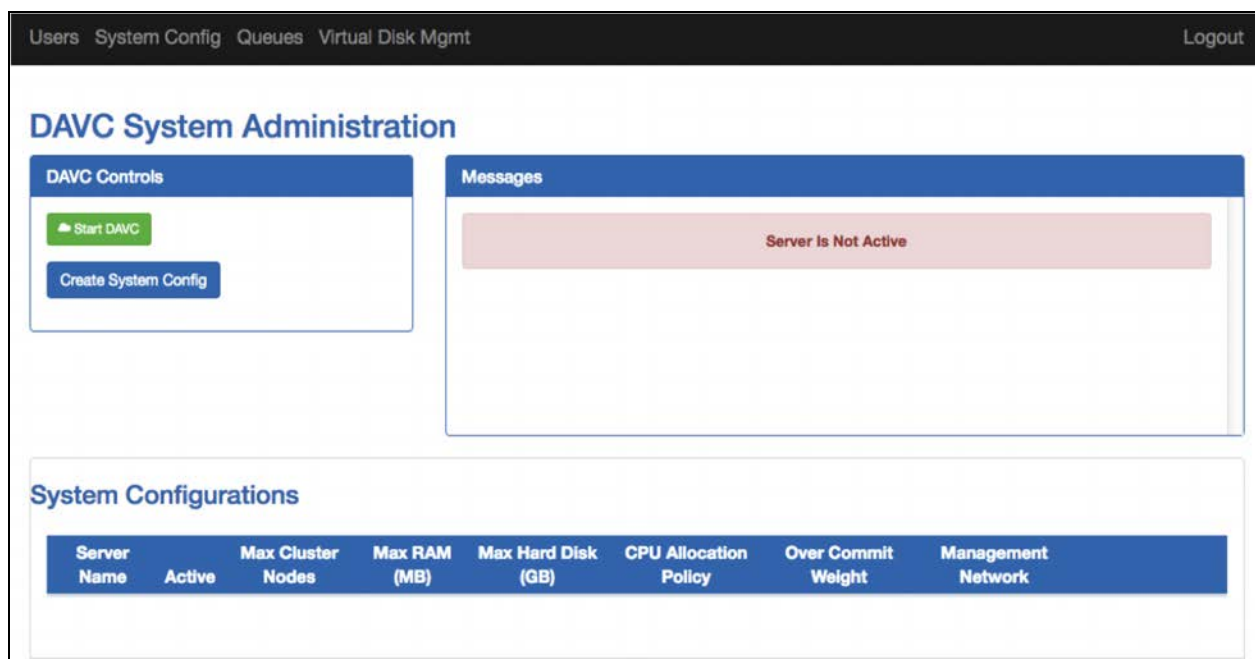


Figure D-56: DAVC Home Page and Login.

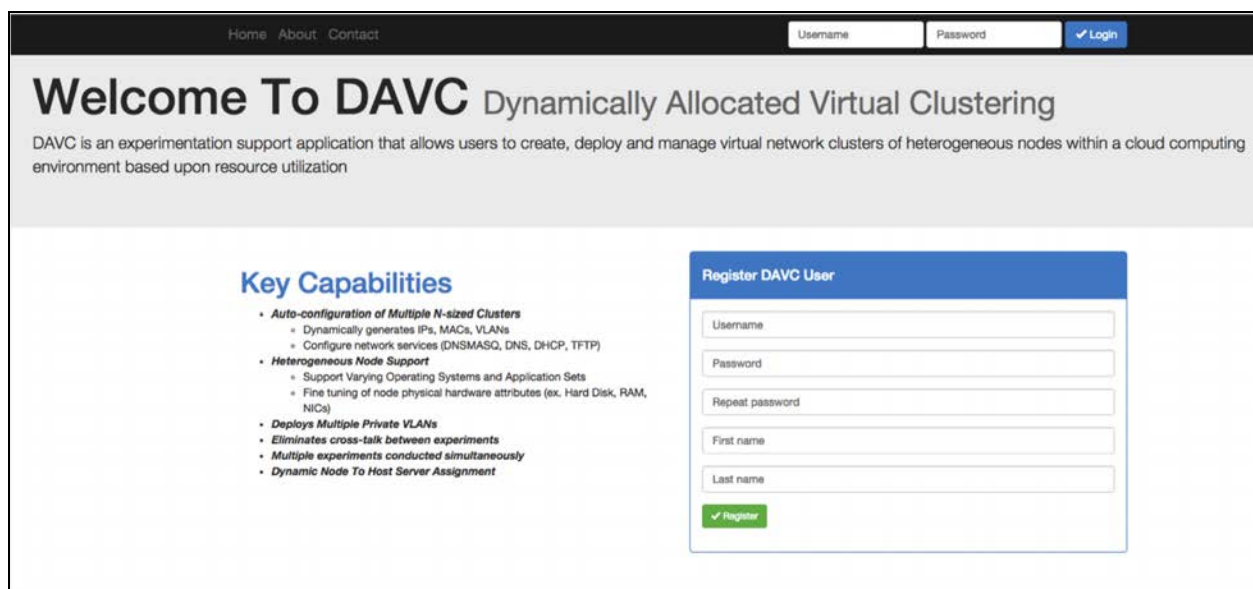


Figure D-57: DAVC System Administration Page.

Edit the System Configuration form (Figure D-58) and fill in the appropriate values for the following:

- DAVC Server Management Network Hostname – This is the DAVC Controller’s Management Network hostname.
- Max Node RAM in MB – This is the maximum amount of RAM a Cluster Node can have in MB.
- Max Nodes Per Cluster – This the maximum number of Nodes that can be included in a single Cluster.

- **Max Node Hard Drive Size in GB** – This is the maximum non-persistent hard disk space a single Cluster Node can be allocated in GB.
- **VLAN Pool Range** – This defines the range of VLAN IDs the system will use when creating Cluster networks. Each Experiment network added to a cluster will be allocated a VLAN from this pool.
- **Node to CPU CORE Allocation Policy** – This determines how the system will allocate CPU CORES to Cluster Nodes. The options include:
 - **Share CPU CORES** – Cluster Nodes share all the CPU CORES on the DAVC Host Server where they are allocated.
 - **Do Not Share CPU CORES** – All Cluster Nodes will be allocated to dedicated CPU CORES as defined by that Cluster’s specific configuration.
 - **1 Node To 1 CPU CORE** – All Cluster Nodes will be allocated to a single dedicated CPU CORE ignoring the Cluster’s specific configuration.
- **Over Commit CPU CORES** – This Policy Is Not Implemented.
- **Over Commit Weighting** – This Value Is Not Used.
- **Management Network In CIDR (Classless Inter-Domain Routing) Format** – This is the Management Network in CIDR Format.

Click the ‘Create Config’ button when complete.

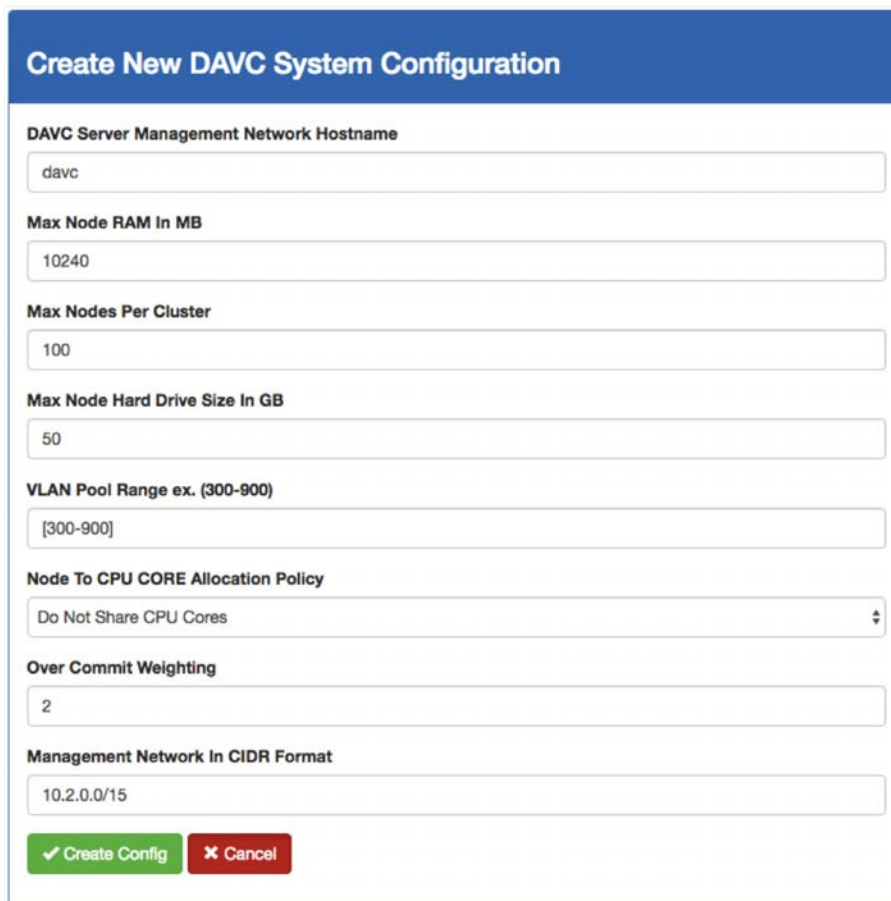


Figure D-58: System Configuration Form.

D.2.33.3 Active the System Configuration

The new System Configuration should now be listed in the DAVC System Administration System Configuration list. Administrator's Console. Click 'Activate' in the 'Config Options' dropdown menu (Figure D-59).

Note:

The DAVC System Configuration activation process may take a few minutes to complete depending upon the size of the Management network defined in the configuration.

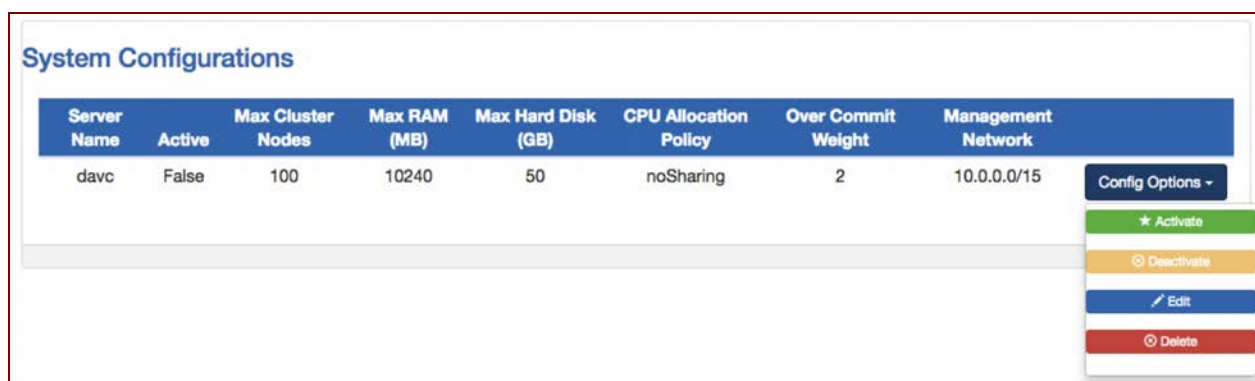


Figure D-59: Activate System Configuration.

D.2.34 Deploy VHD Template Images for DAVC

D.2.34.1 Registering A Virtual Hard Drive In DAVC

DAVC can register/install Virtual Hard Drives (VHDs) that contain preinstalled operating systems. The VHDs can then be used as templates to create cluster nodes.

D.2.34.2 Update the Node Provisioning Startup Client Script to Include Correct Controller Hostname

The DAVC node provisioning startup client script auto configures the VHD on boot-up. The script assumes that the hostname for the controller is 'davic'. This is used as a fallback in the event that the controller hostname cannot be determined automatically. If the hostname for the controller has been changed from the default, the provisioning startup script should be updated accordingly.

```

]# cat /opt/davic2.0/davic/scripts/provisioning/provision_startup.sh

#get the DAVC server address
DAVCSERVER='grep dhcp-server-identifier /var/lib/dhcp/dhclient.eth0.leases |\
uniq | cut echo $DAVCSERVER
if [ "$DAVCSERVER" == "" ];
then
    echo "Couldn't Get DAVC Server Address From DHCP Records." >> \
    /opt/getProvisioning.log
    echo "Using Default DAVC Server Address: davc" >> \
    /opt/getProvisioning.log
    DAVCSERVER="davic"
fi

```

Modify line 13 of this script (DAVCSERVER="davic") with the correct hostname for the DAVC Controller.

D.2.34.3 Installing the DAVC Node Provisioning Client Startup Script in a Virtual Hard Drive Images

A Virtual Hard Drive Image must be preinstalled with the DAVC Node Provisioning Client Startup Script in order to be compatible with DAVC. This client runs after the virtual machine has booted and performs configurations of NFS, VLANs, NICs and several services including SSH and DNS. The DAVC Node Provisioning Startup Client is located in the following directory along with a wrapper start script:

```
/opt/davc2.0/davc/scripts/provisioning/rmprovisionclientvhd_v2.py
/opt/davc2.0/davc/scripts/provisioning/provision_startup.sh
```

D.2.34.4 Configure Node Provisioning Client Startup Script to Run at Boot

Copy the client and the startup script to Virtual Hard Drive's /opt directory and add an entry to /etc/rc.local so the startup script will be launched when the virtual machine boots up.

```
]# cat /etc/rc.local
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
/opt/provision_startup.sh
exit 0
```

D.2.34.5 Configure Virtual Hard Drives for Hotplug Support

Hotplug support is required so DAVC Block Disks can be attached and detached to and from the running Virtual Machine without rebooting.

```
]# echo 'acpiphp' >> /etc/modules
]# echo 'pci_hotplug' >> /etc/modules
```

D.2.34.6 Configure Network Interfaces on Virtual Hard Drives

The DAVC Node Provisioning Client Startup Script expects only the interface 'lo' and 'eth0' to be active and configured for DHCP on boot up for Virtual Hard Drives. This can be achieved by editing the network interfaces configuration file (Debian-based) as below:

```
]# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network
interface auto lo
iface lo inet loopback

# The primary network
interface auto eth0
iface eth0 inet dhcp
Also ensure the persistent network labelling rules file is empty so that interfaces
provisioned by DAVC will be labelled starting with eth0:
]# cat /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
#
# You can modify it, as long as you keep each rule on a single
# line, and change only the value of the NAME= key.
```

D.2.34.7 Clear Hostname File on Virtual Hard Drive

DAVC provides each virtual machine node with its hostname, so ensure the hostname file is also empty:

```
]# cat /etc/hostname
```

D.2.34.8 Clear DHCP Leases on Virtual Hard Drive

The DAVC server provides DHCP services to each node's control interface (eth0), so ensure any existing DHCP leases are removed:

```
]# rm /var/lib/dhcp/dhclient.eth0*
```

D.3 DYNAMICALLY ALLOCATED VIRTUAL CLUSTERING MANAGEMENT SYSTEM USER'S GUIDE

The Dynamically Allocated Virtual Clustering Management System (DAVC) is an experimentation infrastructure that provides the means to dynamically create, deploy, and manage virtual clusters of heterogeneous nodes within a cloud-computing environment. The system allows researchers to create virtual clusters of nodes that can be used for experimentation, software development, and integration with existing hardware and software. This report provides usage instructions for the DAVC version 2.0 web application.

This report is separated into the following sections, which detail, via examples and step-by-step instructions, actions the user will perform when using DAVC version 2.0:

- 1) Accessing and logging into DAVC;
- 2) DAVC cluster configuration;
- 3) DAVC cluster instantiation;
- 4) DAVC cluster and node details;
- 5) DAVC virtual hard disk management;
- 6) DAVC block disk/persistent storage management; and
- 7) Creating a new virtual hard disk from a cluster node.

Each section contains slides from a PowerPoint presentation on using DAVC version 2.0. The slides are presented without change from the original version or additional comment.

D.3.1 Accessing and Logging into DAVC

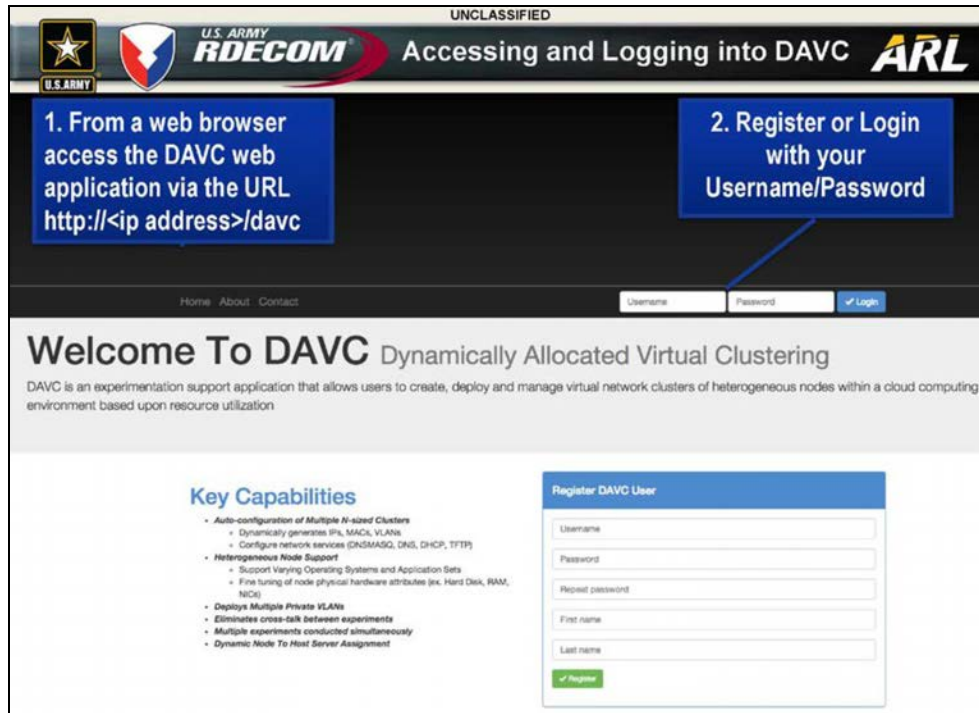


Figure D-60: Accessing and Logging into DAVC.

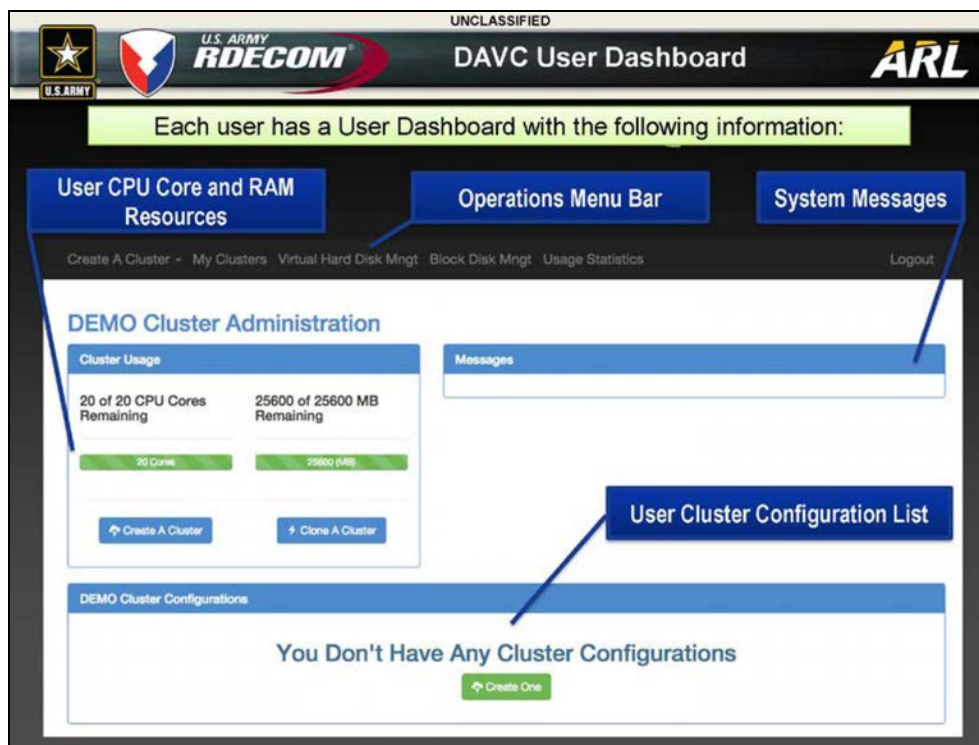


Figure D-61: DAVC User Dashboard.

D.3.2 DAVC Cluster Configuration

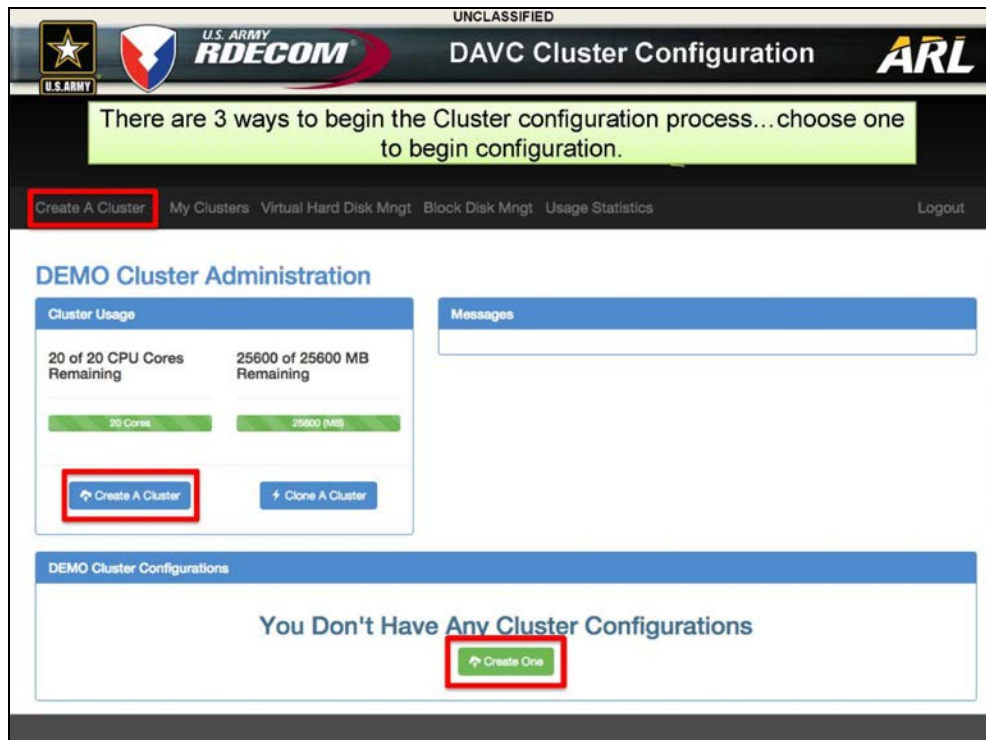


Figure D-62: DAVC Cluster Configuration.

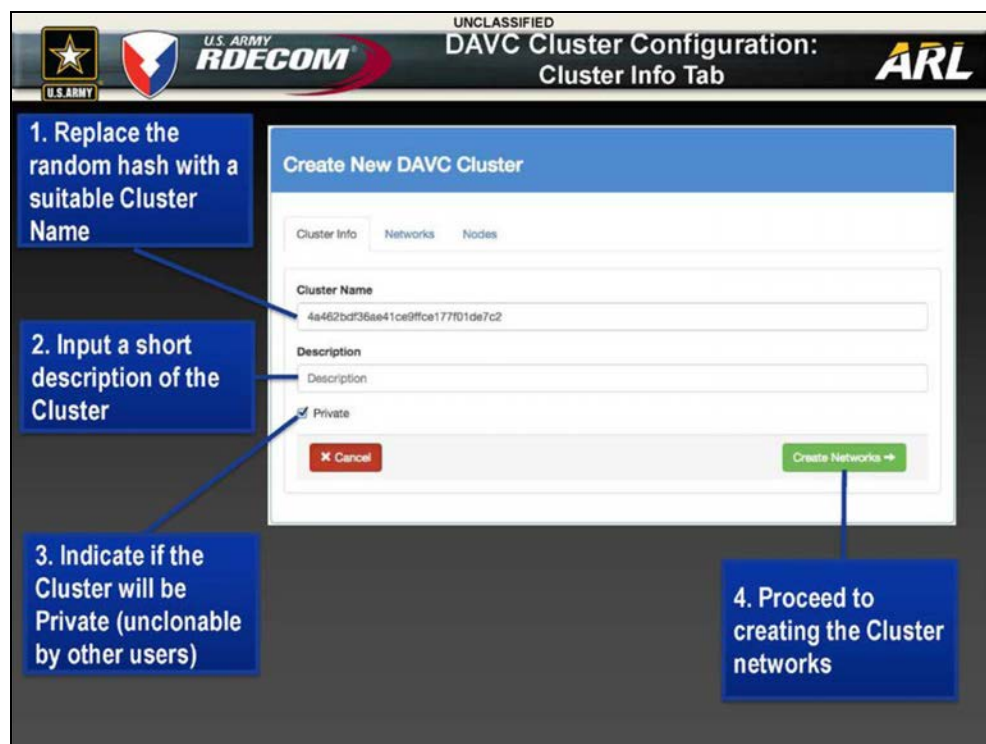


Figure D-63: DAVC Cluster Configuration: Cluster Info Tab.

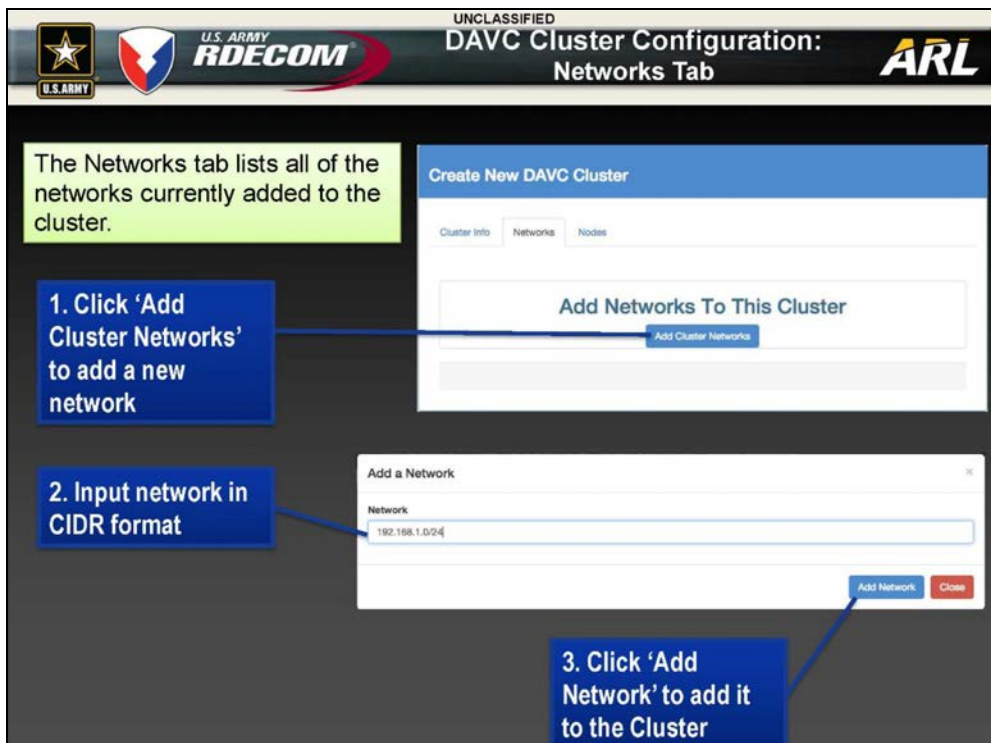


Figure D-64: DAVC Cluster Configuration: Networks Tab.

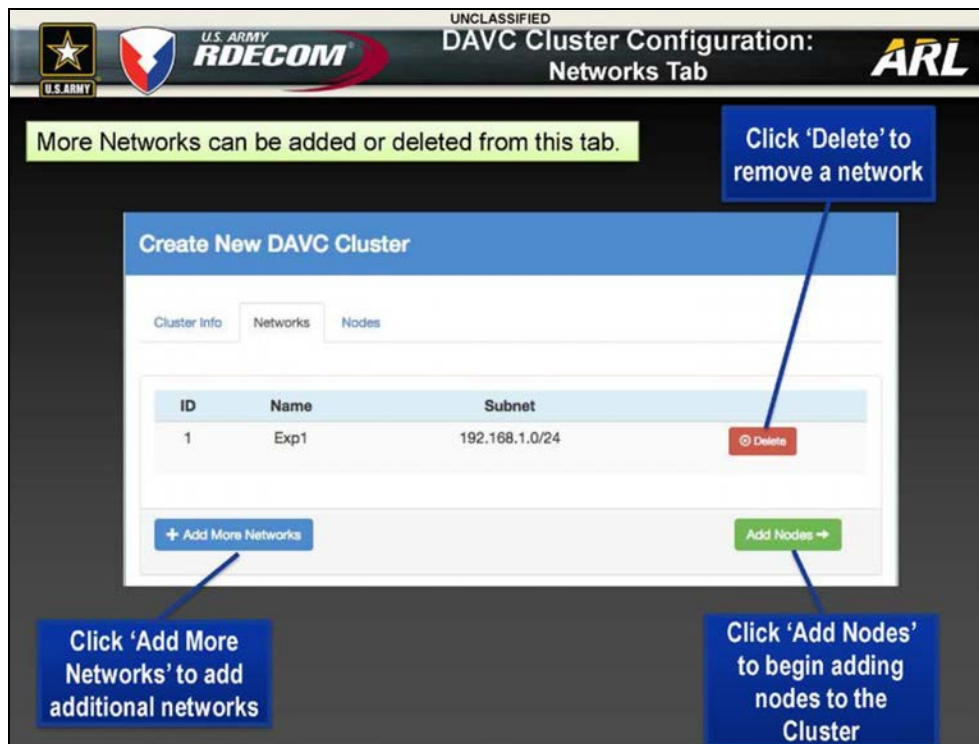


Figure D-65: DAVC Cluster Configuration: Networks Tab.

ANNEX D – IST-124 EXPERIMENTATION EXECUTION

UNCLASSIFIED

U.S. ARMY RDECOM DAVC Cluster Configuration: Nodes Tab ARL

The Nodes tab lists all of the nodes currently associated with the cluster.

Create New DAVC Cluster

Cluster Info Networks Nodes

ID	Controller	OS/Image	Disk Space (GB)	RAM (MB)	Cores	VNIC	Networks
1							

Add More Nodes Create Cluster

Click 'Add More Nodes' to begin adding Nodes

Figure D-66: DAVC Cluster Configuration: Nodes Tab.

UNCLASSIFIED

U.S. ARMY RDECOM DAVC Cluster Configuration: Add Cluster Nodes ARL

The Add Cluster Nodes dialog is used to set the attributes of the nodes that will be added to the cluster.

Add Cluster Nodes

☐ Controller (optional)

Ostype

Cores

Non-Persistent Block Storage Size (GB) (/log)

RAM (MB)

Virtual Network Driver

Networks

Quantity

Add Nodes Close

1. Click the Ostype/Virtual Machine template dropdown box

Figure D-67: DAVC Cluster Configuration: Add Cluster Nodes.

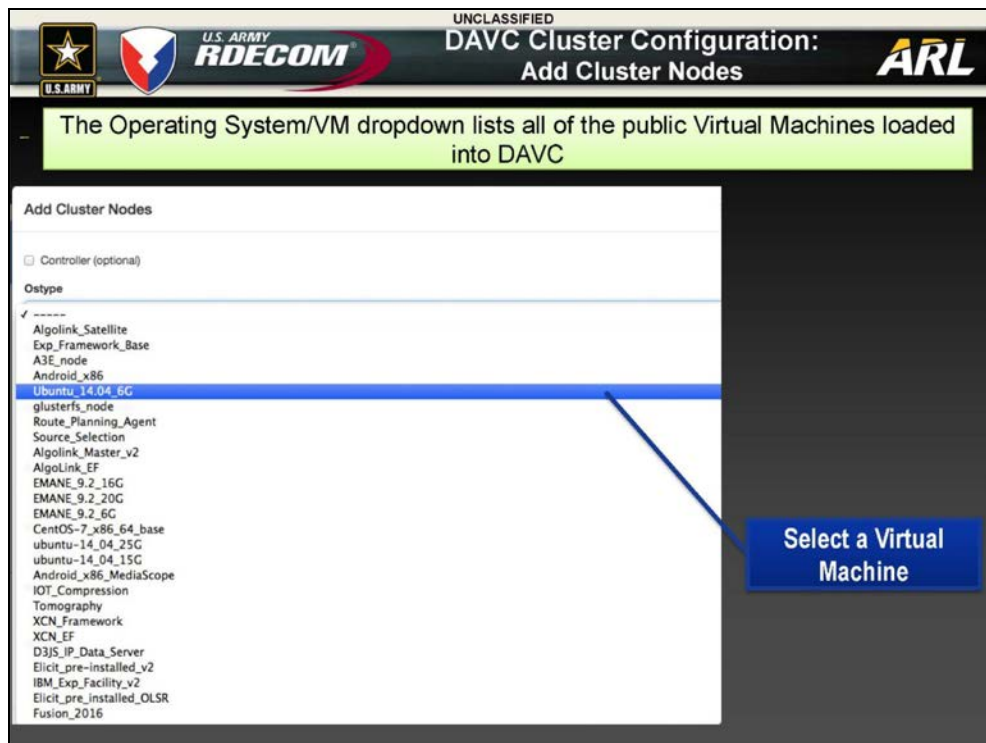


Figure D-68: DAVC Cluster Configuration: Add Cluster Nodes.

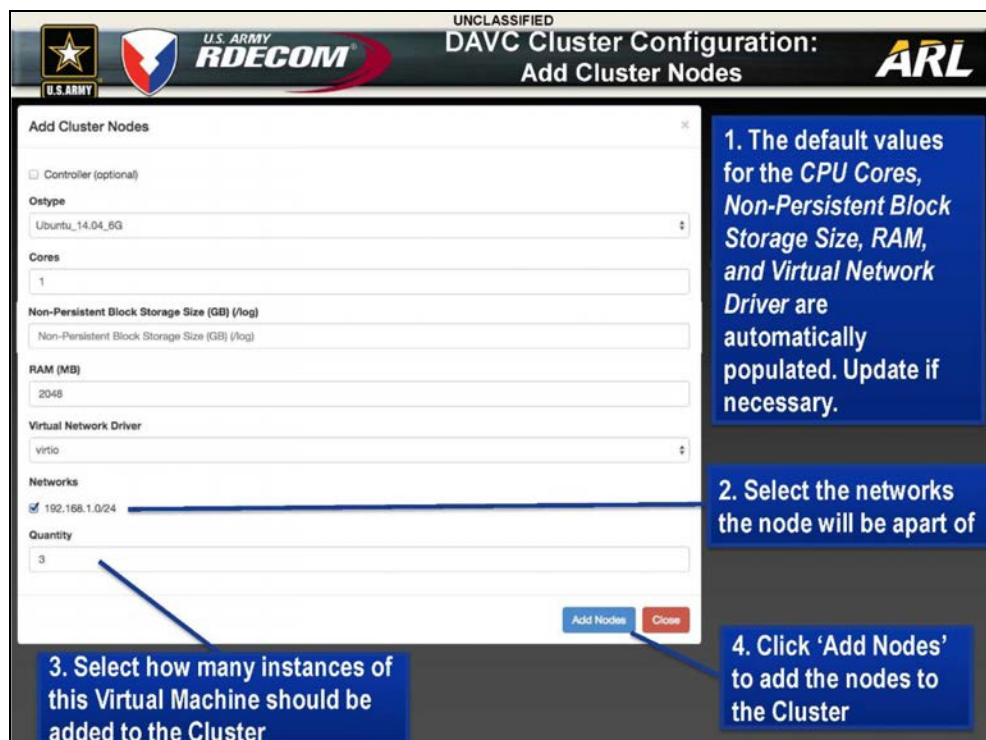


Figure D-69: DAVC Cluster Configuration: Add Cluster Nodes.

ANNEX D – IST-124 EXPERIMENTATION EXECUTION

UNCLASSIFIED

U.S. ARMY RDECOM ARL

DAVC Cluster Configuration: Nodes Tab

Create New DAVC Cluster

Cluster Info Networks Nodes

ID	Controller	OS/Image	Non-Persistent Block Space (GB)	RAM (MB)	Cores	VNIC	Networks	Actions
1	False	Ubuntu_14.04_6G	1	2048	1	virtio	eth0: 10.0.20.0/15 eth1: 172.15.0.0/24	Delete Edit
2	False	Ubuntu_14.04_6G	1	2048	1	virtio	eth0: 10.0.20.0/15 eth1: 172.15.0.0/24	Delete Edit
3	False	Ubuntu_14.04_6G	1	2048	1	virtio	eth0: 10.0.20.0/15 eth1: 172.15.0.0/24	Delete Edit

2. Click 'Add More Nodes' to add more nodes

1. Delete or edit nodes as necessary

3. Click 'Create Cluster' when done.

Add More Nodes Create Cluster

Each node is automatically added to the system's control (blue) network in addition to the networks the user selected.

Figure D-70: DAVC Cluster Configuration: Nodes Tab.

UNCLASSIFIED

U.S. ARMY RDECOM ARL

DAVC Cluster Configuration

The Cluster is now configured and ready to be launched and instantiated.

Cluster Details: DEMO

Cluster Controls

Launch demo Edit

Networks

Name	Net
Exp1	192.168.1.0/24

Messages

Core Allocation Policy: No Core Sharing

Cluster demo created successfully

Cluster Nodes (3)

Add Nodes

Node Name	Status	Host Server	OS/Image	Non-Persistent Block Space (GB)	RAM (MB)	Cores	VNIC	IP Addresses	Actions
demo-1	INACTIVE	None	Ubuntu_14.04_6G	1	2048	1	virtio	eth0: 10.0.20.0/15 eth1: 192.168.1.0/24	Node Options -
demo-2	INACTIVE	None	Ubuntu_14.04_6G	1	2048	1	virtio	eth0: 10.0.20.0/15 eth1: 192.168.1.0/24	Node Options -
demo-3	INACTIVE	None	Ubuntu_14.04_6G	1	2048	1	virtio	eth0: 10.0.20.0/15 eth1: 192.168.1.0/24	Node Options -

Figure D-71: DAVC Cluster Configuration.

D.3.3 DAVC CLUSTER Instantiation

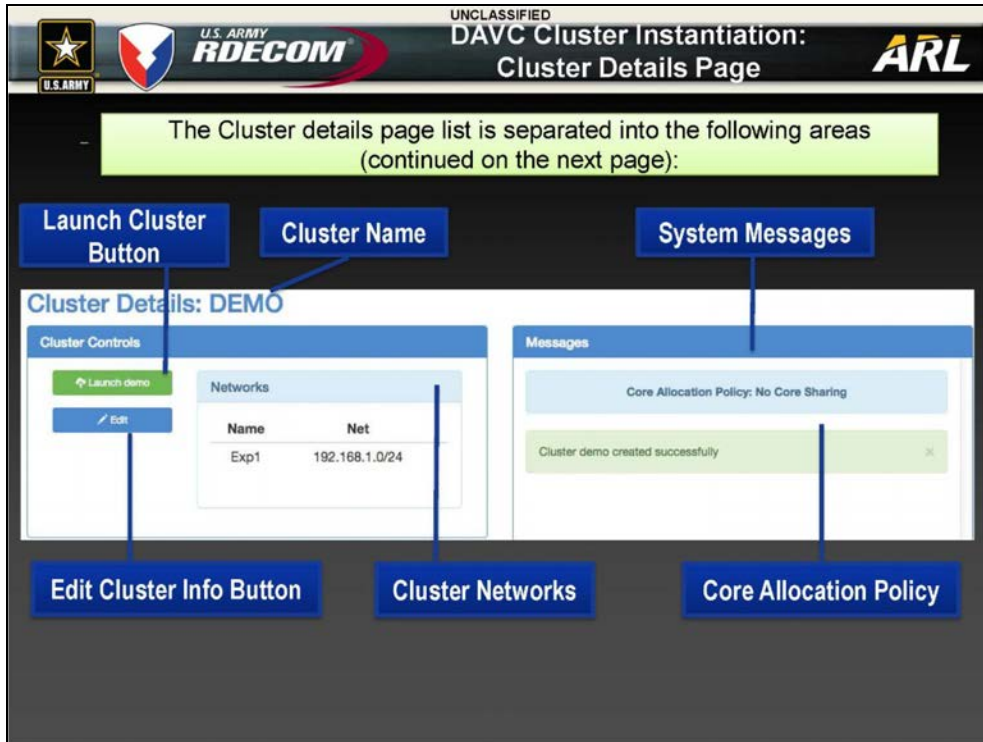


Figure D-72: DAVC Cluster Instantiation: Cluster Details Page.

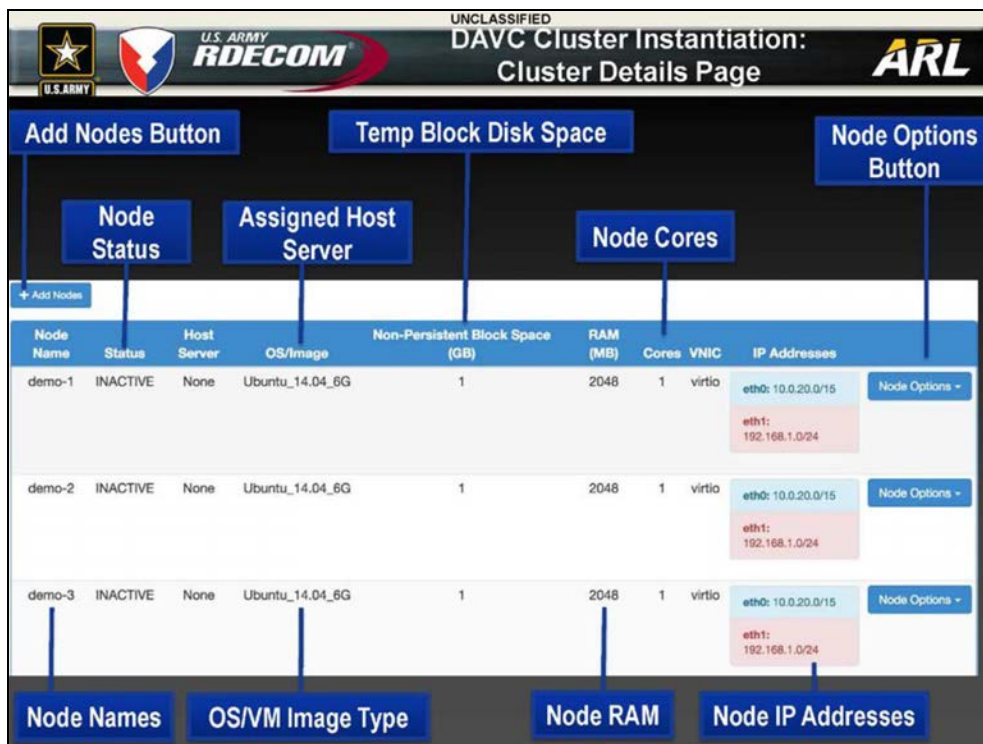


Figure D-73: DAVC Cluster Instantiation: Cluster Details Page.

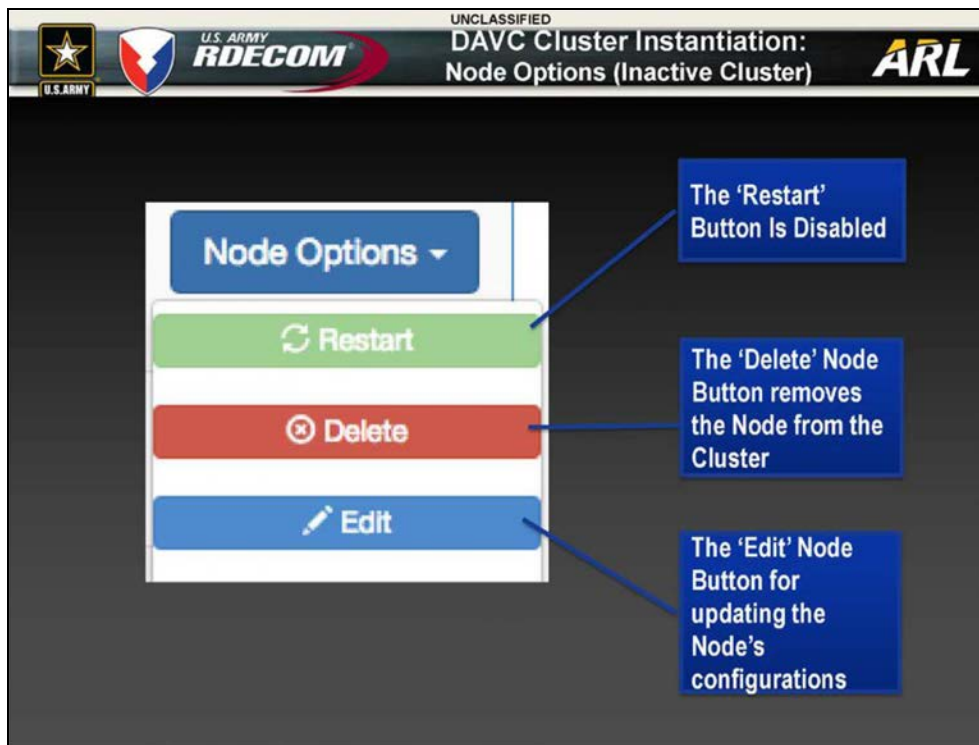


Figure D-74: DAVC Cluster Instantiation: Node Options (Inactive Cluster).

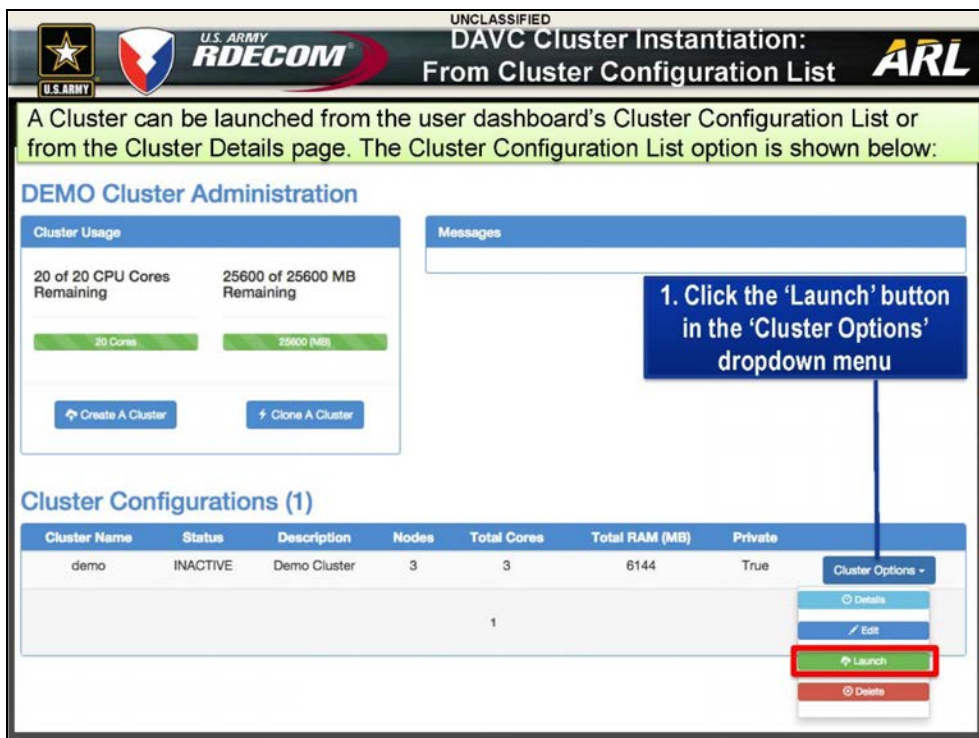


Figure D-75: DAVC Cluster Instantiation: From Cluster Configuration List.

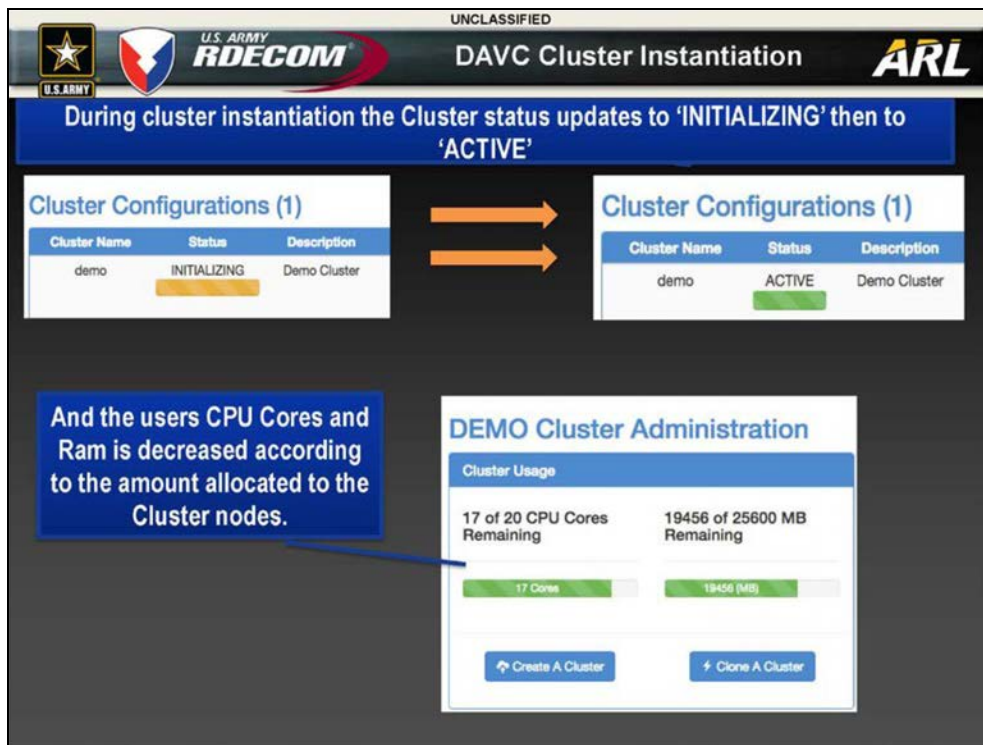


Figure D-76: DAVC Cluster Instantiation.

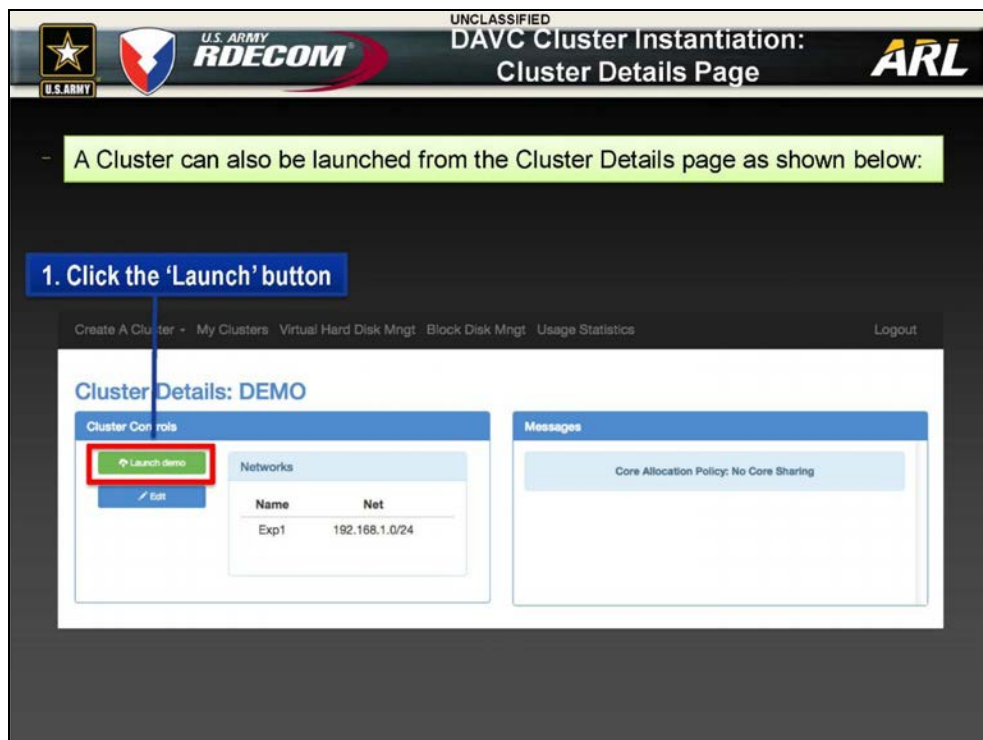


Figure D-77: DAVC Cluster Instantiation: Cluster Details Page.

ANNEX D – IST-124 EXPERIMENTATION EXECUTION

UNCLASSIFIED

U.S. ARMY RDECOM ARL

DAVC Cluster Instantiation: Cluster Details Page

During cluster instantiation each node's status updates to 'INITIALIZING', to 'CHECKING IN', then 'ACTIVE'

Cluster Nodes (3)

Node Name	Status	Host Server	OS/Image
demo-1	INITIALIZING	None	Ubuntu_14.04_6G

Cluster Nodes (3)

Node Name	Status	Host Server	OS/Image
demo-1	CHECKING IN	d10	Ubuntu_14.04_6G

Cluster Nodes (3)

Node Name	Status	Host Server	OS/Image	Non-Persistent Block Space (GB)	RAM (MB)	Cores	VNIC	IP Addresses	Node Options
demo-1	ACTIVE	d10	Ubuntu_14.04_6G	1	2048	1	virtio	eth0: 10.0.0.26 eth1.314: 192.168.1.1 rate: 1000000 (Kbps) Set Rate	

Figure D-78: DAVC Cluster Instantiation: Cluster Details Page.

UNCLASSIFIED

U.S. ARMY RDECOM ARL

DAVC Cluster Instantiation: Active Cluster

The Cluster is active once all of the nodes are in the 'ACTIVE' state.

Cluster Details: DEMO

Cluster Controls

⬆️ KB demo

Networks

Name	Net
Exp1	192.168.1.0/24

Messages

Core Allocation Policy: No Core Sharing

Cluster Nodes (3)

Node Name	Status	Host Server	OS/Image	Non-Persistent Block Space (GB)	RAM (MB)	Cores	VNIC	IP Addresses	Node Options
demo-1	ACTIVE	d10	Ubuntu_14.04_6G	1	2048	1	virtio	eth0: 10.0.20.0/15 eth1.314: 192.168.1.0/24	
demo-2	ACTIVE	d11	Ubuntu_14.04_6G	1	2048	1	virtio	eth0: 10.0.20.0/15 eth1.314: 192.168.1.0/24	
demo-3	ACTIVE	d9	Ubuntu_14.04_6G	1	2048	1	virtio	eth0: 10.0.20.0/15 eth1.314: 192.168.1.0/24	

Figure D-79: DAVC Cluster Instantiation: Active Cluster.

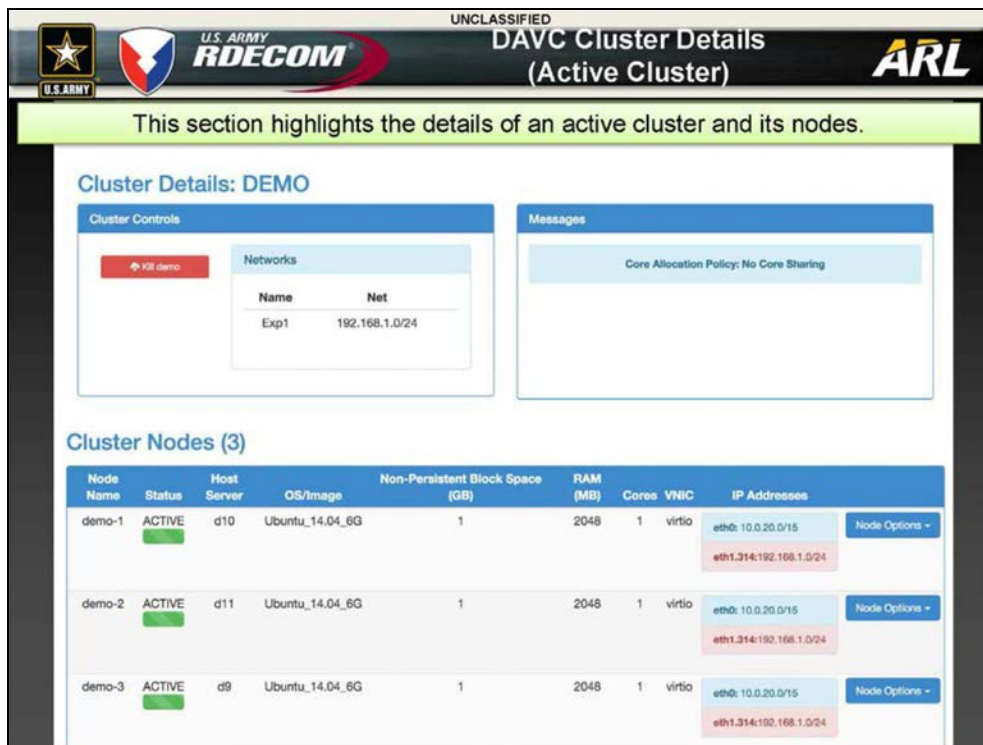


Figure D-80: DAVC Cluster Details: (Active Cluster).

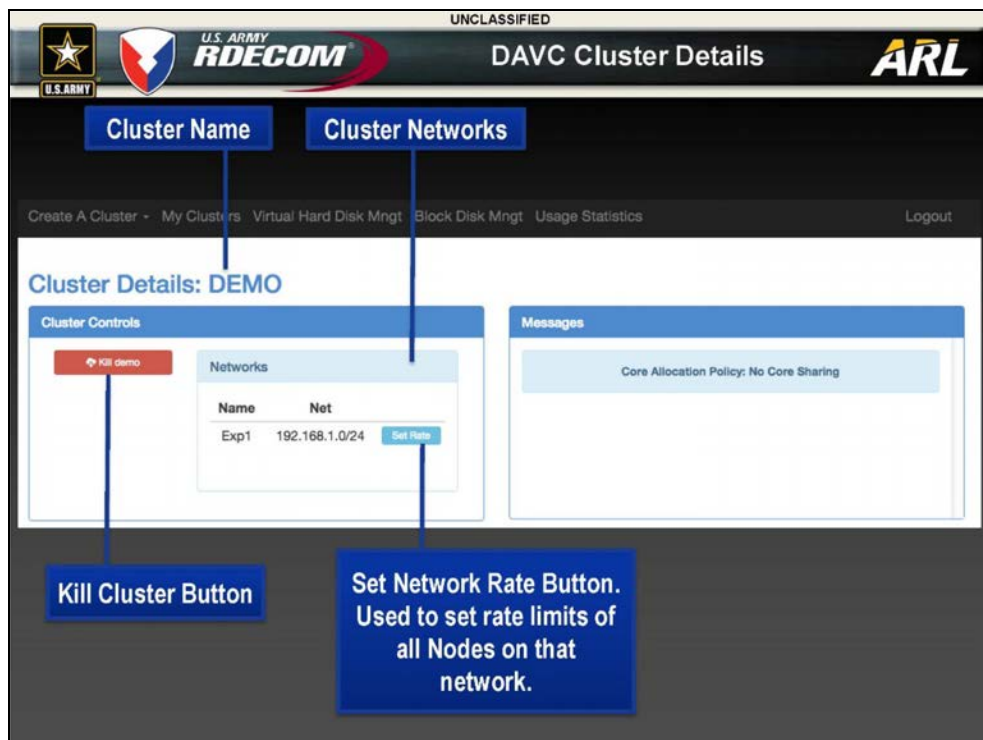


Figure D-81: DAVC Cluster Details.

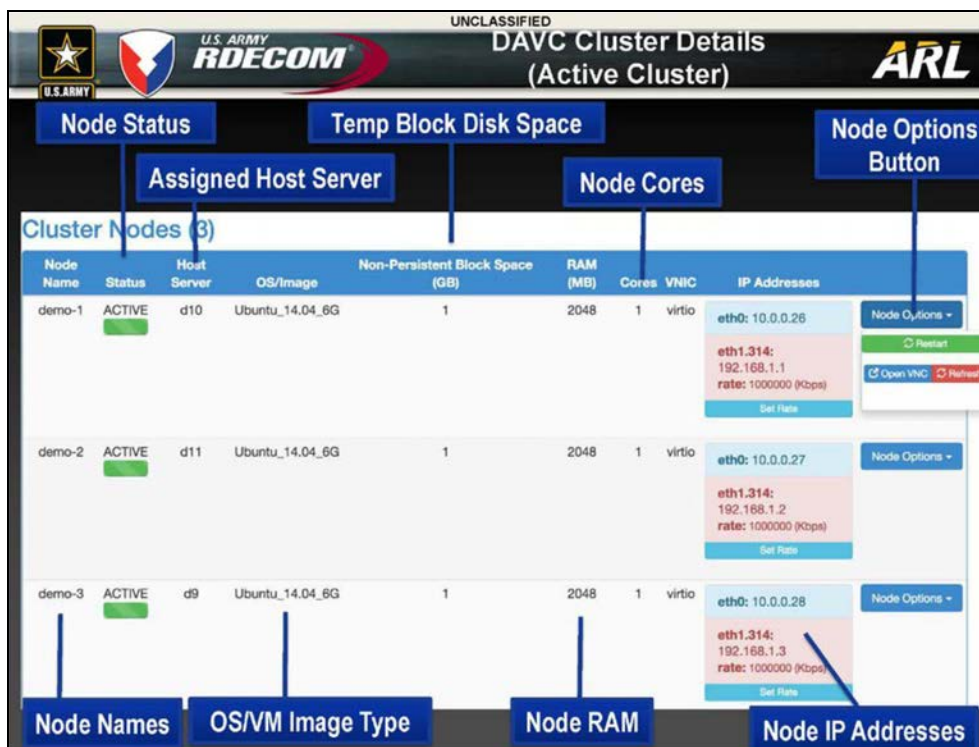


Figure D-82: DAVC Cluster Details: (Active Cluster).

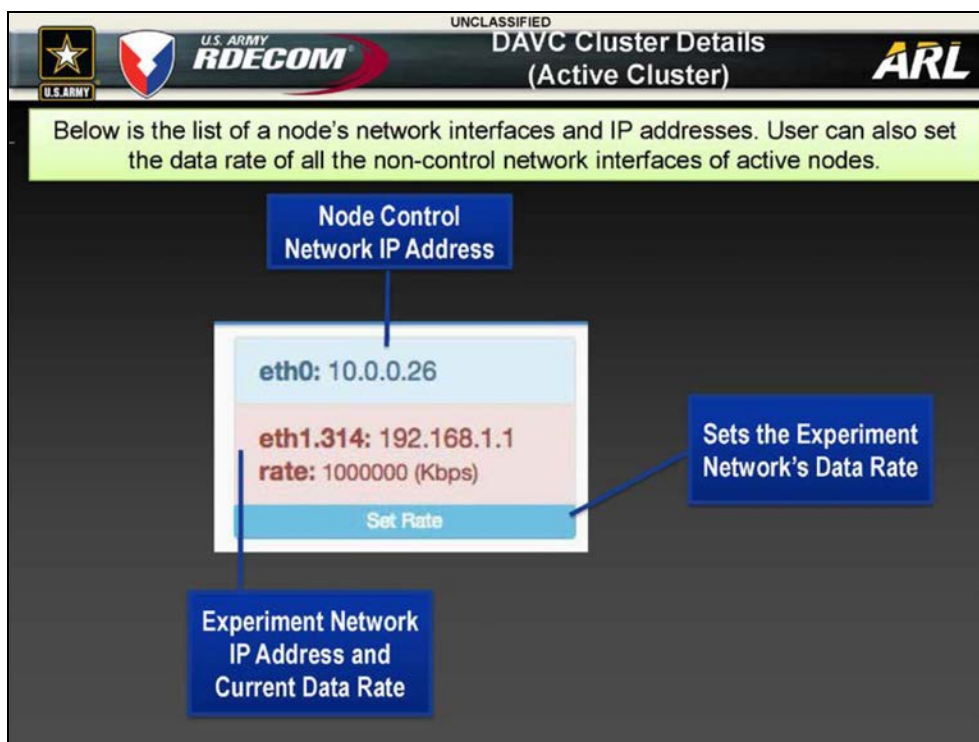


Figure D-83: DAVC Cluster Details: (Active Cluster).

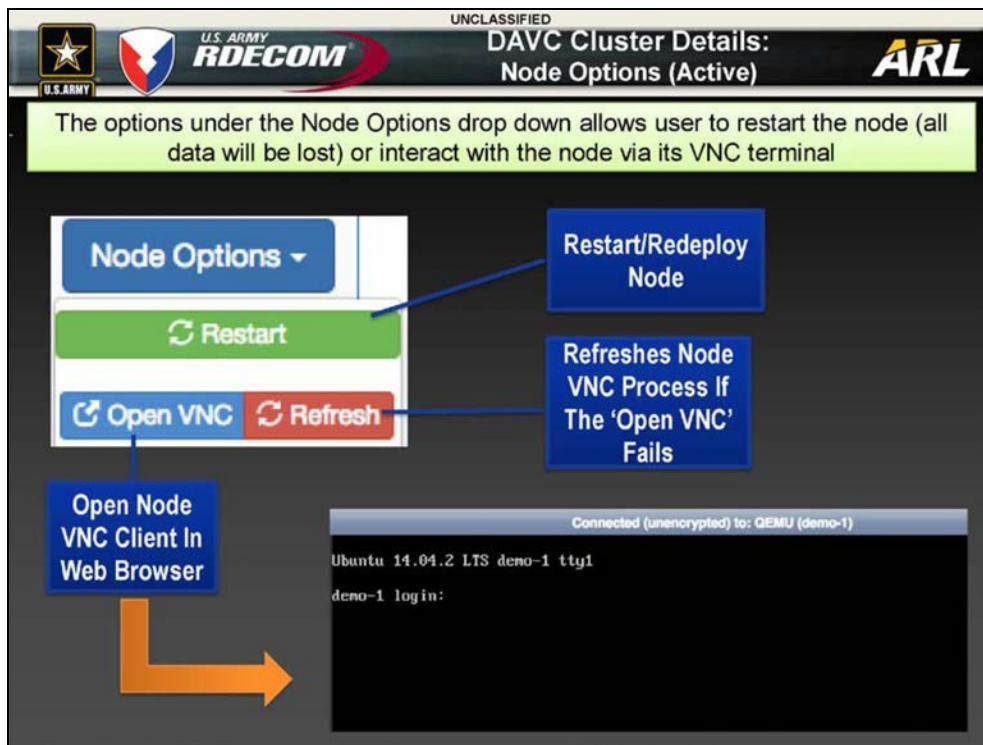


Figure D-84: DAVC Cluster Instantiation: Node Options (Active).

D.3.4 DAVC Virtual Hard Disk Management

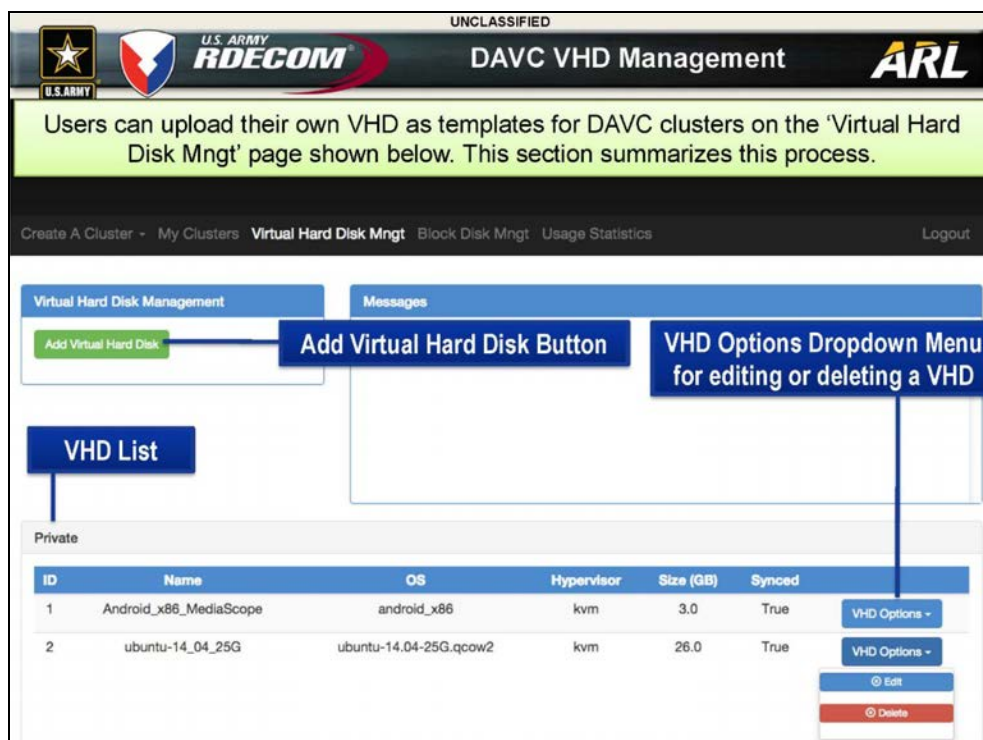


Figure D-85: DAVC VHD Management.

UNCLASSIFIED

U.S. ARMY RDECOM DAVC VHD Management: Prepping Your VHD For Upload ARL

A VHD template must be preinstalled with the DAVC Node Provisioning Client Python script. Thus Python is a prerequisite for the operating system on the VHD.

The DAVC Node Provisioning Client is located in the following location in the DAVC distribution along with a wrapper start script:

- /davic2.0/davic/scripts/provisioning/rmprovisionclientvhd_v2.py
- /davic2.0/davic/scripts/provisioning/provision_startup.sh

1. Copy the client and startup script to the VHD's /opt directory and add an entry to the /etc/rc.local, as shown, so the script will launch at boot time.

```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
/opt/provision_startup.sh
exit 0
```

Figure D-86: DAVC VHD Management: Prepping Your VHD for Upload.

UNCLASSIFIED

U.S. ARMY RDECOM DAVC VHD Management: Prepping Your VHD For Upload ARL

The DAVC Node Provisioning Client expects the interfaces 'lo' and 'eth0' to be active and configured for DHCP on bootstrap. This can be achieved with the edits shown below.

2. Edit the network interfaces configuration file (Debian-based), as shown to the right.

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

#control network interface
auto eth0
iface eth0 inet dhcp
```

3. Ensure the persistent network labeling rules file is empty so that interfaces provisioned by DAVC will be labeled starting with eth0. The file is located at:

- /etc/udev/rules.d/70-persistent-net.rules

Figure D-87: DAVC VHD Management: Prepping Your VHD for Upload.




UNCLASSIFIED

DAVC VHD Management:
Prepping Your VHD For Upload

DAVC provides each node with a hostname and provides DHCP services as well as a Block Disk storage service for nodes. Perform the steps below in your VHD to ensure these services will function correctly.

4. Clear the hostname file on the VHD by editing the file:
 - `/etc/hostname`
5. Remove the DHCP leases file on the VHD by running the command
 - `rm /var/lib/dhcp/dhclient.eth0*`
6. Execute the following commands to add 'Hotplug Support' to the VHD. This is required so that DAVC Block Disks can be attached and detached to and from a running instance of the virtual machine:
 - `echo 'acpiphp' >> /etc/modules`
 - `echo 'pci_hotplug' >> /etc/modules`

The VHD is now ready to be uploaded to DAVC. This process is shown next.

Figure D-88: DAVC VHD Management: Prepping Your VHD for Upload.




UNCLASSIFIED

DAVC VHD Management:
Prepping Your VHD For Upload

A VHD template must be in the qcow2 format with backwards capability before uploading to DAVC.

The qemu-img convert command can be used to convert a VHD to qcow2 format. The syntax of the command is shown below:

- `qemu-img convert -o compat=0.10 -f <current format> <image file> -O qcow2 <new image file>.qcow2`
- `-o compat=0.10` - Ensures the new virtual machine image will be backwards compatible
- `<current format>` - The current format of your virtual machine (raw, vdi, qcow, cow, vmdk)
- `<image file>` - The name of your virtual machine image file
- `-O qcow2` - Specifies qcow2 as the output format
- `<new image file>` - The name of the new converted virtual machine image file.
 - Do not use spaces in the file name
- Example:
 - `qemu-img convert -o compat=0.10 -f vmdk ubuntu14.04.vmdk -O qcow2 ubuntu14.04.qcow2`

Refer to <https://linux.die.net/man/1/qemu-img> for more information on the qemu-img command

Figure D-89: DAVC VHD Management: Prepping Your VHD for Upload.

ANNEX D – IST-124 EXPERIMENTATION EXECUTION

UNCLASSIFIED

U.S. ARMY RDECOM DAVC VHD Management: Uploading a VHD ARL

Virtual Hard Disk Management

Add Virtual Hard Disk

1. Click 'Add Virtual Hard Disk Button'

2. Input a descriptive name

3. Input the VHD OS

4. Input the minimum Core and RAM requirements

5. Indicate if the VHD can be shared with other users

6. Browse for the VHD file (qcow2 format)

7. Click 'Upload VHD' when complete

Boot Type, Hyper Visor Type and VNIC can be left at their defaults.

Virtual Hard Disk Name: EMANE_TEST_NODE

OS: Ubuntu14.04

Boot Type: d

Hyper Visor Type: kvm

Minimum Required Cores: 2

Minimum Required Non-Persistent Block Disk Size (GB): 5

Minimum Required RAM (MB): 2048

Virtual Network Driver: virtio

File: Choose file: EMANE_TEST...tu14.qcow2

Upload VHD Close

Figure D-90: DAVC VHD Management: Uploading a VHD.

UNCLASSIFIED

U.S. ARMY RDECOM DAVC VHD Management ARL

A system message will indicate the success or failure of the VHD upload.

Messages

Virtual Hard Disk EMANE_TEST_NODE uploaded successfully.

The VHD will not be available during cluster configuration until it has 'Synced' (copied) onto all host servers. This can take a while depending on the size of the VHD.

ID	Name	Owner	OS	Hypervisor	Size(GB)	Synced	VHD Options
1	EMANE_TEST_NODE	demo	Ubuntu14.04	kvm	26.0	False	VHD Options -
1	EMANE_TEST_NODE	demo	Ubuntu14.04	kvm	26.0	True	VHD Options -

Figure D-91: DAVC VHD Management.

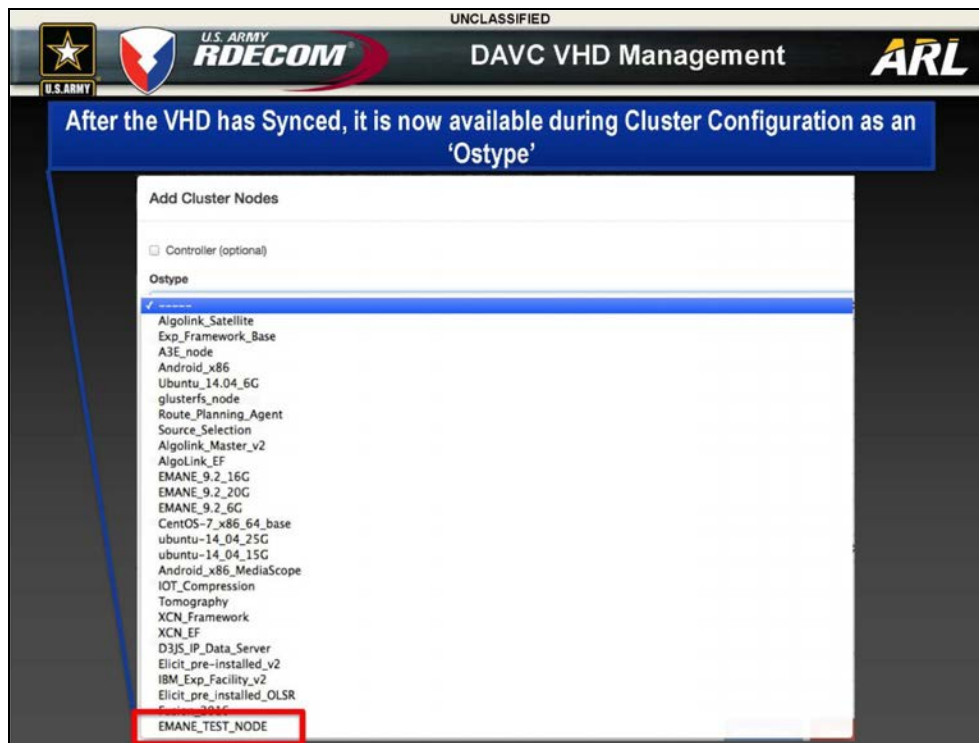


Figure D-92: DAVC VHD Management.

D.3.5 DAVC Block Disk/Persistent Storage Management

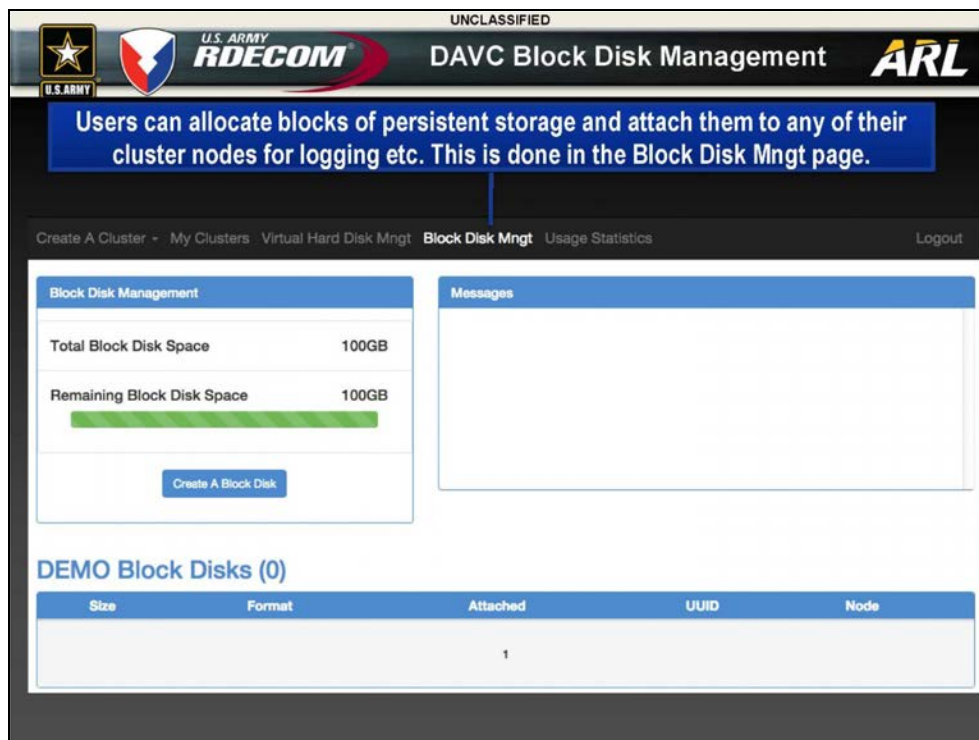


Figure D-93: DAVC Block Disk Management.

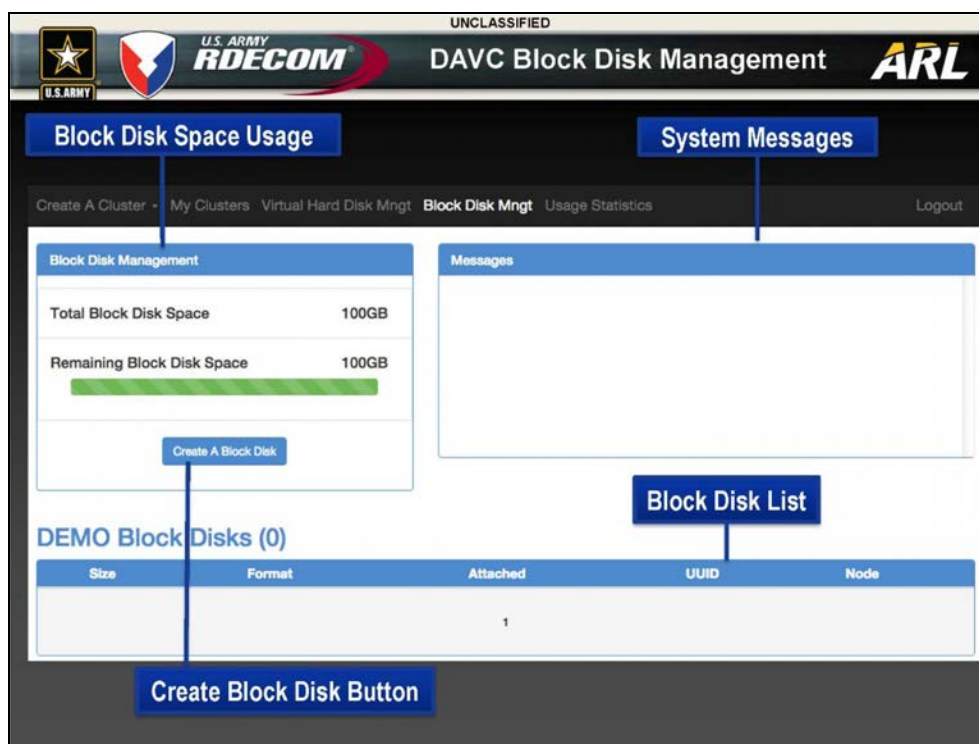


Figure D-94: DAVC Block Disk Management.

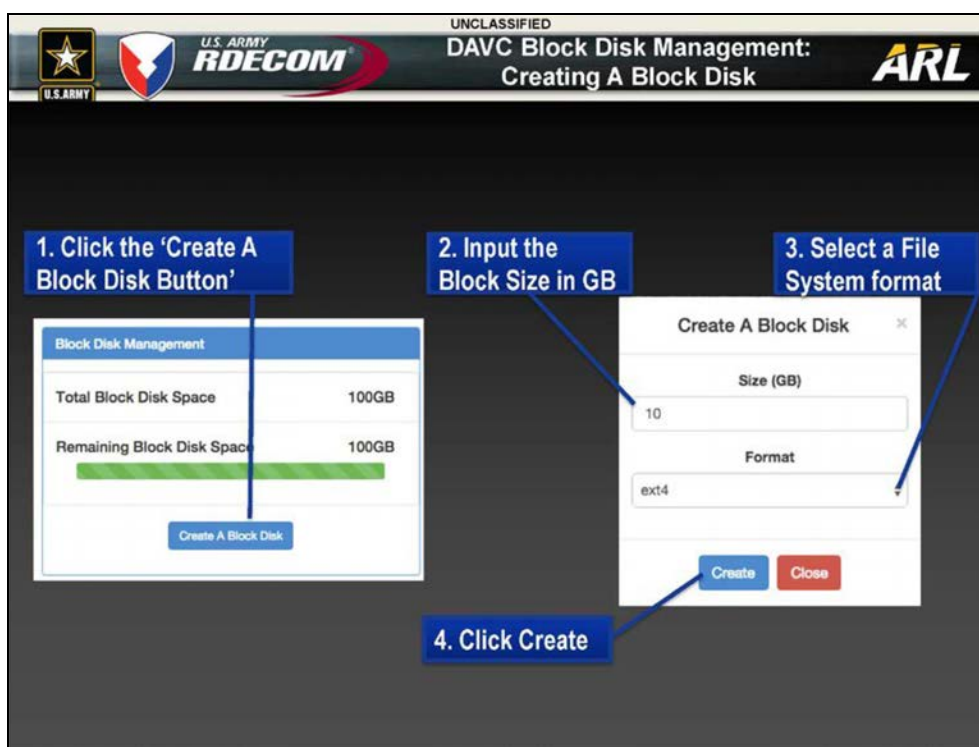


Figure D-95: DAVC Block Disk Management: Creating a Block Disk.

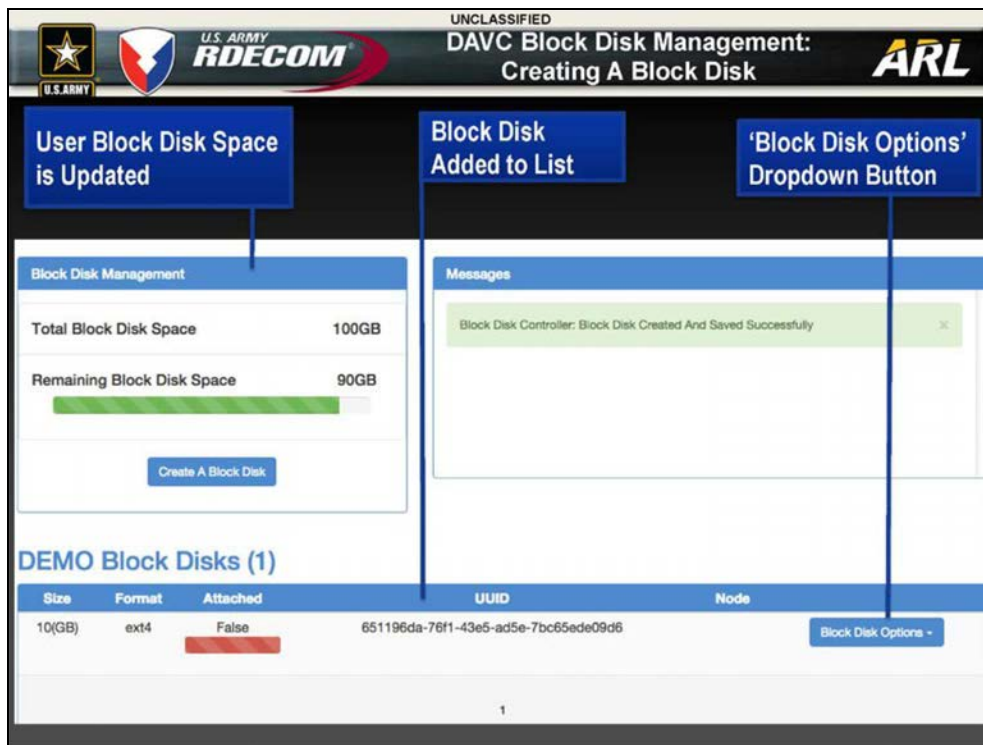


Figure D-96: DAVC Block Disk Management: Creating a Block Disk.

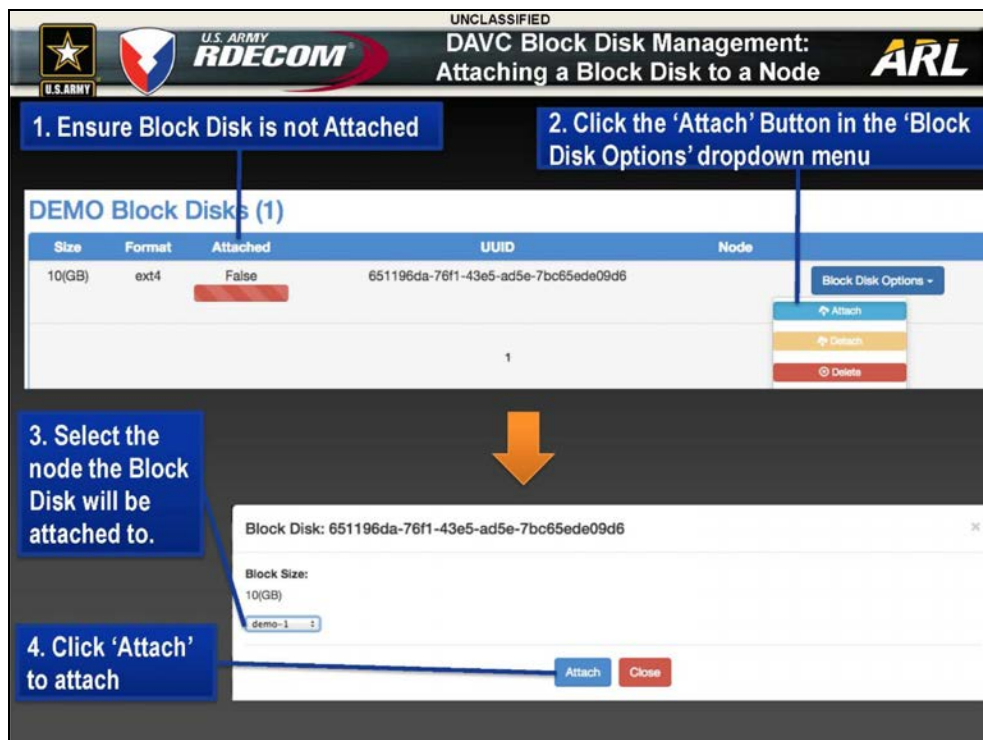


Figure D-97: DAVC Block Disk Management: Attaching a Block Disk to a Node.

UNCLASSIFIED

U.S. ARMY RDECOM ARL

DAVC Block Disk Management: Attaching a Block Disk to a Node

System message will indicate success or failure

Messages

Attaching Block Disk To demo-1...

Block Disk Controller: Block Disk 651196da-76f1-43e5-ad5e-7bc65ede09d6 attached successfully to node demo-1

Block Disk is now attached

Block Disk has associated Node

DEMO Block Disks (1)

Size	Format	Attached	UUID	Node
10(GB)	ext4	True	651196da-76f1-43e5-ad5e-7bc65ede09d6	demo-1

Block Disk Options ~

Figure D-98: DAVC Block Disk Management: Attaching a Block Disk to a Node.

UNCLASSIFIED

U.S. ARMY RDECOM ARL

DAVC Block Disk Management: Attaching a Block Disk to a Node

Although the Block Disk has been attached, the user has to mount it from within the node. This process is shown below:

5. Execute 'blkid' command to list the block attributes

Connected (unencrypted) to: QEMU (demo-1)

```

root@demo-1:~# blkid
/dev/sda1: UUID="28757865-1a3d-45ee-8d6e-f379cbf146e0" TYPE="ext4"
/dev/sda5: UUID="ada9d957-8b6f-4c5d-a09f-4337a428cdd6" TYPE="swap"
/dev/sdb1: UUID="8e979bd4-d101-490c-9692-d64c66127275" TYPE="ext4"
/dev/vda: UUID="651196da-76f1-43e5-ad5e-7bc65ede09d6" TYPE="ext4"
  
```

6. Find the block device (/dev/vda) with the UUID that matches the Block Disk that was just attached

DEMO Block Disks (1)

Size	Format	Attached	UUID	Node
10(GB)	ext4	True	651196da-76f1-43e5-ad5e-7bc65ede09d6	demo-1

Figure D-99: DAVC Block Disk Management: Attaching a Block Disk to a Node.



UNCLASSIFIED

DAVC Block Disk Management:
Attaching a Block Disk to a Node



7. Create a mount point/directory for the block

8. Mount the block device to the mount point/directory

Connected (unencrypted) to: GEMU (demo-1)

```

root@demo-1:~# mkdir /dave_block
root@demo-1:~# mount /dev/vda /dave_block/
root@demo-1:~# df -h

```

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda1	4.8G	1.8G	2.8G	40%	/
none	4.0K	0	4.0K	0%	/sys/fs/cgroup
udev	991M	8.0K	991M	1%	/dev
tmpfs	201M	384K	200M	1%	/run
none	5.0M	0	5.0M	0%	/run/lock
none	1001M	0	1001M	0%	/run/shm
none	100M	0	100M	0%	/run/user
/dev/sdb1	990M	1.3M	922M	1%	/log
/dev/vda	9.8G	23M	9.2G	1%	/dave_block

9. The Block Disk can now be used to store data.

Figure D-100: DAVC Block Disk Management: Attaching a Block Disk to a Node.



UNCLASSIFIED

DAVC Block Disk Management:
Detaching a Block Disk from a Node



The process to Detach a Block Disk from a node is shown below:

1. Execute the 'umount' command on the node

2. Click the 'Detach' Button

Connected (unencrypted) to: GEMU (demo-1)

```

root@demo-1:~# df -h

```

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda1	4.8G	1.8G	2.8G	40%	/
none	4.0K	0	4.0K	0%	/sys/fs/cgroup
udev	991M	8.0K	991M	1%	/dev
tmpfs	201M	384K	200M	1%	/run
none	5.0M	0	5.0M	0%	/run/lock
none	1001M	0	1001M	0%	/run/shm
none	100M	0	100M	0%	/run/user
/dev/sdb1	990M	1.3M	922M	1%	/log
/dev/vda	9.8G	23M	9.2G	1%	/dave_block

```

root@demo-1:~# umount /dev/vda

```

DEMO Block Disks (1)

Size	Format	Attached	UUID	Node	
10(GB)	ext4	True	651196da-76f1-43e5-ad5e-7bc85edeC90a	demo-1	Block Disk Options
					1 Attach Detach Details

Figure D-101: DAVC Block Disk Management: Detaching a Block Disk from a Node.

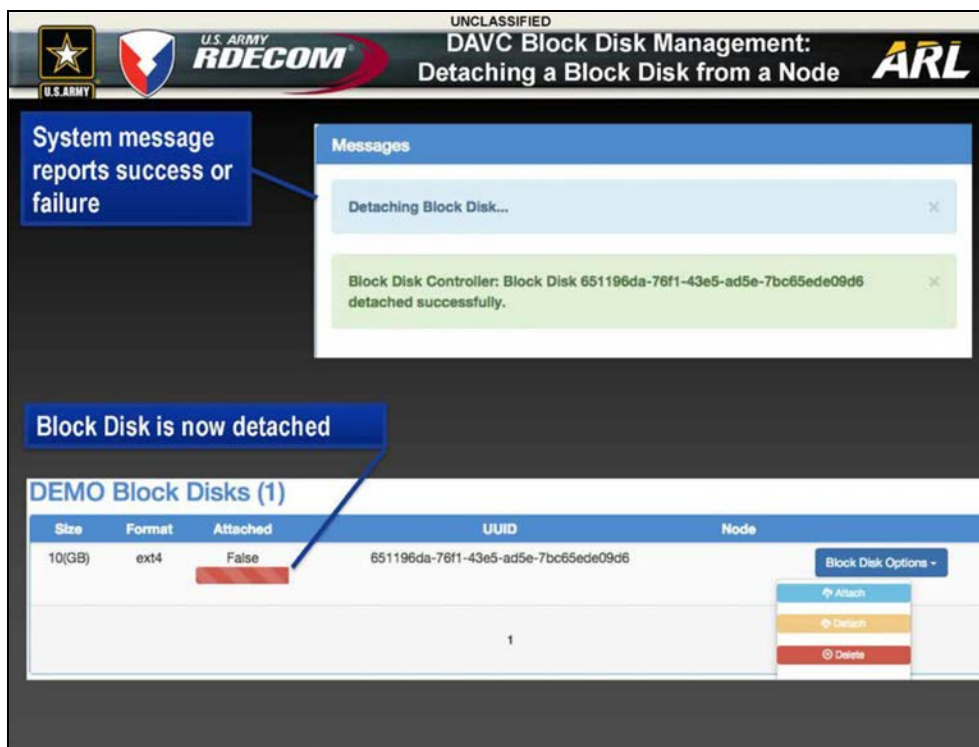


Figure D-102: DAVC Block Disk Management: Detaching a Block Disk from a Node.

D.3.6 Creating a New Virtual Hard Disk from a Cluster Node

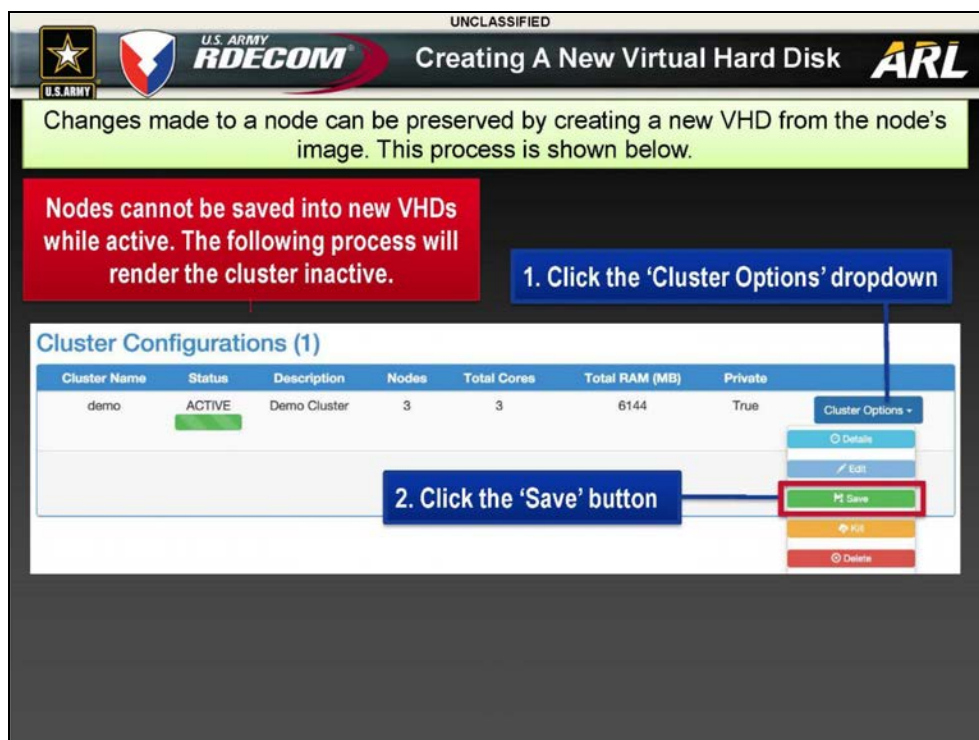


Figure D-103: Creating a New Virtual Hard Disk.

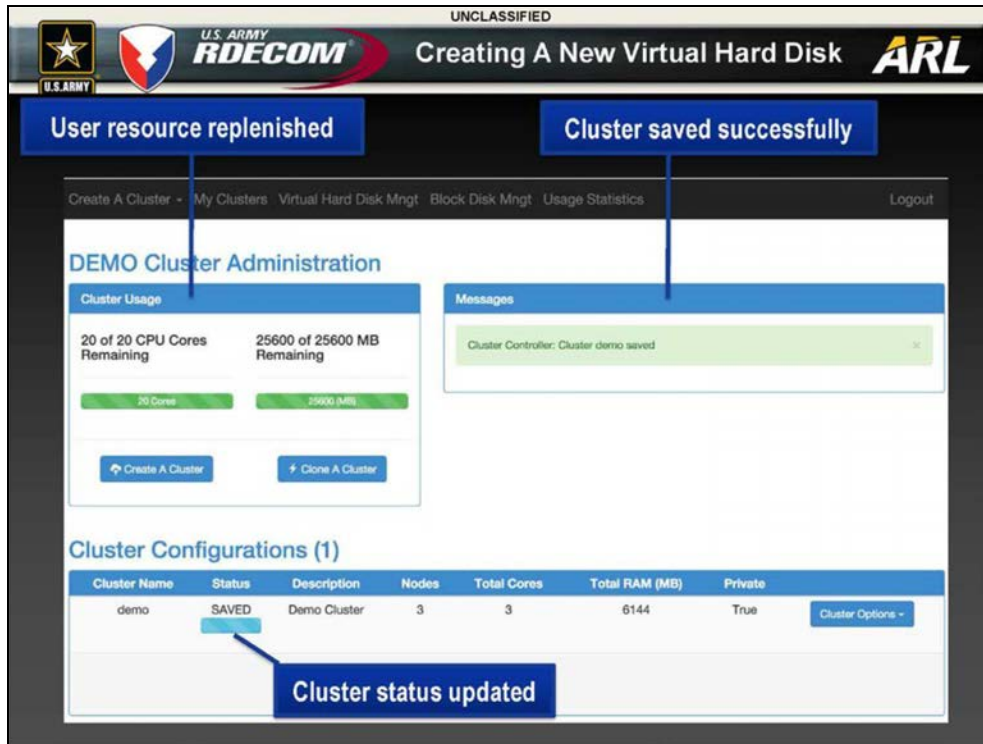


Figure D-104: Creating a New Virtual Hard Disk.

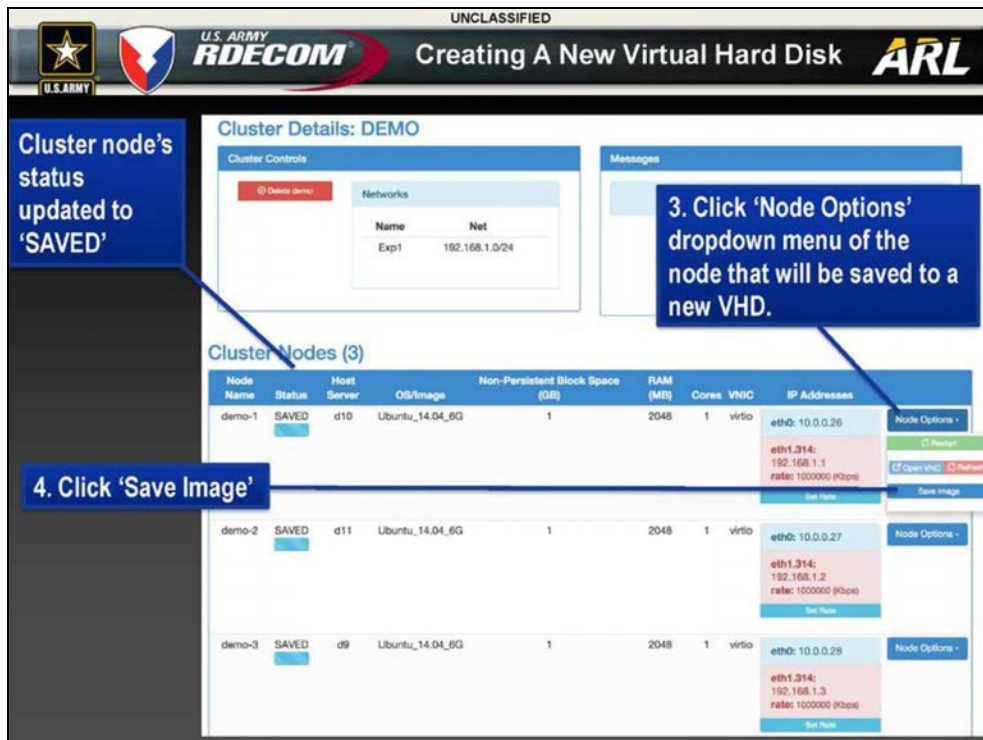


Figure D-105: Creating a New Virtual Hard Disk.

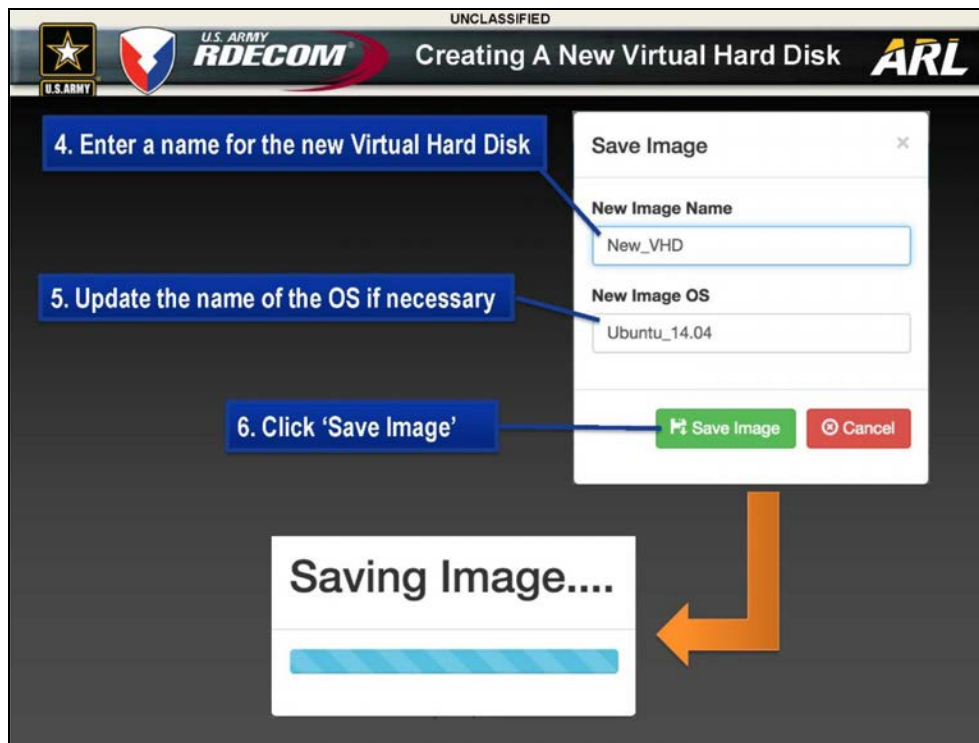


Figure D-106: Creating a New Virtual Hard Disk.

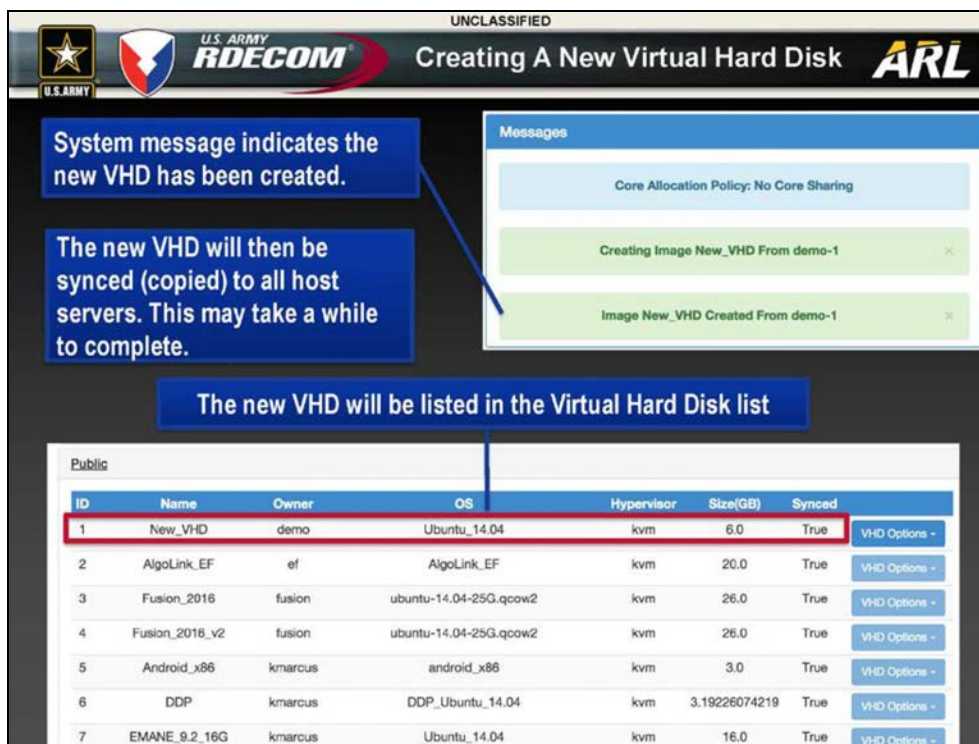


Figure D-107: Creating a New Virtual Hard Disk.

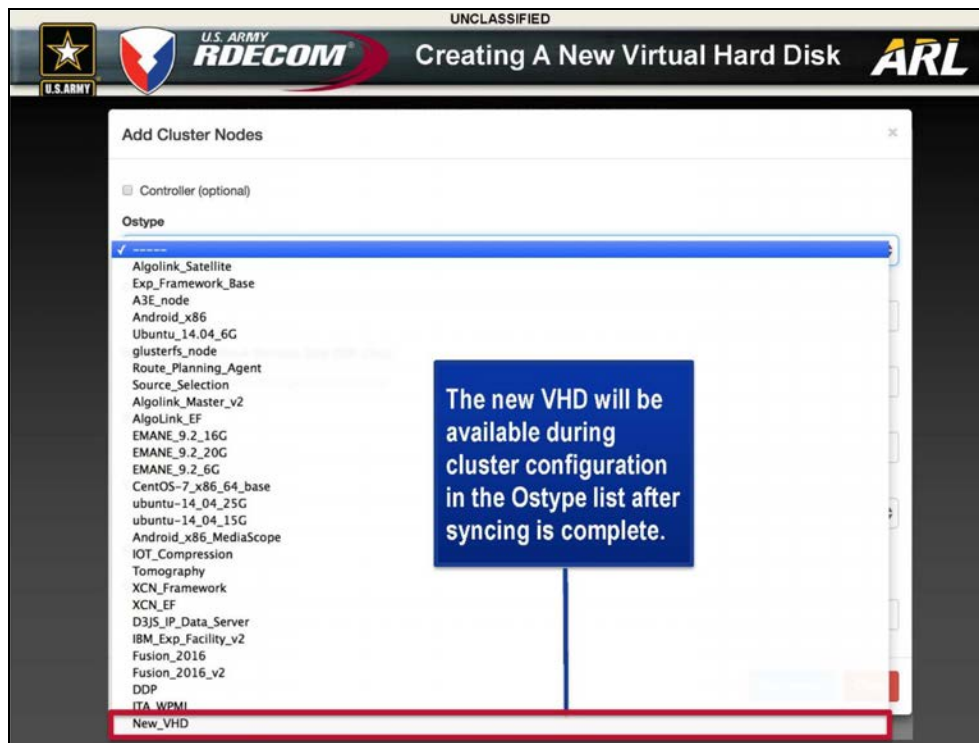


Figure D-108: Creating a New Virtual Hard Disk.

D.3.7 Conclusion

This section displayed the step-by-step instructions to perform common DAVC version 2.0 operations to access DAVC and manage DAVC clusters, nodes, virtual hard disks, and persistent block storage.

D.4 REFERENCES

- [1] AdjacentLink, LLC. Extendable Mobile Ad-hoc Network Emulator (EMANE). Internet: <https://github.com/adjacentlink/emane>, [January 2, 2016].
- [2] US Naval Research Laboratory. Multi-Generator (MGEN). Internet: <http://www.nrl.navy.mil/itd/ncs/products/mgen>, [January 2, 2016].
- [3] Optimized Link State Routing Protocol V1 – OLSRv1. Internet: <http://www.olsr.org/mediawiki/index.php/Projects>, [January 2, 2016].
- [4] Optimized Link State Routing Protocol V2 – OLSRv2. Internet: <http://www.olsr.org/mediawiki/index.php/Projects>, [January 2, 2016].
- [5] US Naval Research Laboratory. Scripted Display Tools (std/std3d). Internet: <http://www.nrl.navy.mil/itd/ncs/products/sdt>, [January 2, 2016].



Annex E – ROUTING ARCHITECTURE CONSIDERATIONS FOR HETEROGENEOUS TACTICAL NETWORKS

Mariann Hauge

Norwegian Defence Research Establishment (FFI)
NORWAY

Arjen Holtzer

Netherlands Organisation for Applied Scientific
Research (TNO)
THE NETHERLANDS

Anders Hansson

Swedish Defence Research Agency (FOI)
SWEDEN

Anne Marie Hegland

Kongsberg Defence & Aerospace (KDA)
NORWAY

Christoph Barz

Fraunhofer FKIE
GERMANY

Ronald In't Velt

Netherlands Organisation for Applied Scientific
Research (TNO)
THE NETHERLANDS

E.1 INTRODUCTION

E.1.1 Background

Successful military operations require seamless cooperation between nations. Such cooperation requires in-mission information sharing and communication between the involved nations. This requirement has led to work within NATO on defining standards for interoperability between mission networks of different nationalities on the deployed level, e.g., Protected Core Network (PCN¹) [1] in the IST-069 and IST-103 RTGs. During the missions in Afghanistan, the Afghan Mission Network (AMN) was an instantiation of a coalition network, which led to the NATO effort to define a more generic Federated Mission Network (FMN) [2] that can be deployed quickly during all kinds of coalition missions in the future. There is an increasing need for cooperation between nations also on lower tactical levels e.g., formation of teams with elements (e.g., platoons or tank battalions) from different nations. Mechanisms and standards for interoperability on the lower tactical level are currently not sufficiently present. The multilateral project “Coalition Network for Secure Information Sharing (CoNSIS)” started to address this [3], [4]. The work in IST-124 “Heterogeneous Networks – improving connectivity and network efficiency” has had its main focus on the tactical edge and technical challenges in realizing a heterogeneous coalition network for the lower echelons. Our purpose has not been to write standards, however the results will be used as input to the standardization of tactical edge networks, for instance in FMN. In the current FMN roadmap, mobile networks are planned to be included in spiral 4 [2].

The networks of the mobile tactical edge are agile, often highly mobile, and inevitably heterogeneous. They incorporate sub-networks with significant diversity in terms of latency, data-rate, robustness, and other factors. The reasons for this are manifold:

- One radio system (transmission technology) cannot support all requirements (e.g., long-range, high data-rate), so multiple radio systems, each with different characteristics, are used, leading to a heterogeneous environment.
- Nations deploy smaller units to coalition operations. A coalition operation can be manned with small expert teams from different nations. Thus in a multi-national (joint) operation there may be

¹ There is also ongoing work in NATO Consultation, Command and Control Board (C3B), Network and Security Capability Team (N&S CaT) to write PCN STANAGS. The head STANAG 5637 is under ratification and the core STANAG 5638 is work in progress.

- different network boundaries and domains and interoperability between them is required on lower tactical levels.
- The systems are in different phases of their lifecycles leading to coexistence of legacy systems and new systems.
 - NATO standards for relevant transmission technologies and network technologies are few. Therefore proprietary technologies are currently often the only ones capable of providing adequate services, resulting in different nations and forces using several diverse proprietary technologies from different vendors.
 - Commercial technologies (such as 4G-LTE and wireless sensor networks) are entering the tactical network domain, adding even more to the diversity of transmission and network technologies in the tactical edge networks.

Traditionally, the radio systems in these networks have been robust waveforms operating in low frequency bands (HF, VHF). In these frequency bands there is no practical way of providing capacity to support high data-rates. In recent years military systems in UHF bands, Satellite Communication On The Move (SOTM), civilian technologies (e.g., WiFi and LTE) have also been, or are on the verge of being introduced to the mobile tactical edge to include enclaves with higher data-rates. The end-to-end data-rates in mobile military networks will nevertheless usually be much lower than what we have come to expect from civilian communication in well planned, infrastructure based cellular networks and satellite communication.

Combining the traditional low data-rate military networks with higher data-rate networks to form one heterogeneous network of networks, leads to a situation where we have some network segments with frequent topology changes due to mobility and communication in difficult terrain for signal propagation (for UHF or higher frequencies) and some network segments with few topology changes but little capacity to sustain much network control overhead. This means that the network control traffic must be carefully designed to work well in this environment. When using the IP-model for data communication, having an up to date picture of the overall topology for the whole network is crucial for realizing high availability and reliability for voice and data services for soldiers in the field. In a fast-changing mobile environment, out-of-date topology information will typically result in service disruptions and disconnections. The fact that we are considering a heterogeneous environment in this activity where there is a high diversity in data-rates and also a high diversity in the rate of topology changes, makes it very hard to design mechanisms to efficiently handle the tradeoff between overhead and the quality of the resulting picture of the topology.

No clear guidelines exist on how to deploy efficient well-connected heterogeneous tactical edge networks. This greatly hinders information sharing in these coalition networks. The work of IST-124 contributes to a better understanding of the challenges and tradeoff encountered when deploying these networks.

E.1.2 Routing Architecture Goals and Considerations

The chosen architecture for routing on the network layer is an important design consideration when building a mobile heterogeneous network. With routing architecture, we mean how one or several routing protocol(s) is/are used to provide end-to-end connectivity in the heterogeneous network and how topology and link information is shared in the whole network. Selecting a certain routing architecture has impact on aspects such as the scalability, robustness and flexibility of the heterogeneous network. In this document we discuss a few different architectures and design choices and highlight the important tradeoffs and the consequences of choosing the different routing architectures.

When designing a routing architecture for tactical coalition edge networks three main aspects have to be considered:

- Architecture: Choosing the architecture that best meets the network requirements and gives an optimized performance for the operation type in question.

- Interconnections: Deciding where and how network elements of different coalition partners should be connected (e.g., information exchange interfaces and interconnection platforms).
- Administration: Deciding what kind of network control and network management information that should be exchanged between connected network elements of coalition partners.

This document focuses on the first two aspects and provides a starting point for the third aspect.

We describe different routing architectures and discuss their advantages and disadvantages for a heterogeneous network that aims to connect all or most networks available in the mission (or in each operation) into one common infrastructure that can be used by all coalition partners. We also consider low data-rate narrow band networks to take part in the common network, whenever possible. All sensors and all services that the warfighter need should be available via this network. Some cases exist where this common infrastructure will be difficult to achieve (e.g., legacy radio systems with no IP support, or radios with very low data-rate such as, e.g., 3kHz HF radios and acoustic underwater networks). How to deal with legacy systems and very low data-rate networks in the context of realizing a common tactical IP infrastructure will have to be investigated, but this is beyond the scope of IST-124. A simple solution is to attach such networks as stub networks that do not allow transit traffic. We also identify information exchange interfaces and interconnection platforms that are necessary for the different architectures to perform well. Our goal is to give insight into the tradeoffs and important choices that have to be made when choosing a routing architecture for a heterogeneous network and the capabilities of the routing function that is required to implement such a routing architecture.

It is given that there is no “one size fits all” for the most efficient routing architecture in this environment. The best choice will depend on factors such as:

- The size of the network;
- The traffic demands;
- The difference in capacity of the different transmission technologies;
- The impacts of the differences of the link layer protocols;
- The level of mobility;
- The required robustness and availability;
- The architectural difference in functionality of the different network segments – for instance layer-two routing versus layer-three routing, proprietary segment routing versus non-proprietary routing, and systems with star topology;
- Whether the network should be optimized for local traffic or transit traffic;
- Whether it is a national network or a coalition network; and
- Whether it should be possible to choose different routes for different content.

The routing architecture can be tailored in different ways to fit different scenarios. However, a network that keeps changing its routing architecture frequently to fit the current operational need may face serious challenges in terms of stability if such changes occur in-mission. If changes can be made prior to a certain mission or action, the challenge lies mainly in enabling easy reconfiguration of network devices between operational actions. Identifying the important triggers for a change in the architecture and how often this should be allowed to happen during and between military actions, is a study that is needed, but this is out of scope for the discussion in this document.

It should be noted that state-of-the-art and legacy put constraints on what can currently be achieved with respect to the routing architectures that are presented here. Some aspects can be achieved in short term, while others represent a longer term target architecture.

E.1.3 Network Model

This document primarily addresses routing at Layer-Three (L3), the network layer in the OSI model. The exception is the discussion in Section E.4.3.1 that discusses some aspects of a combined L3 routing and layer-two (L2) routing scenario. We use the network model as shown in Figure E-1 as one of the basic architecture principles for the discussed heterogeneous network architectures. In this model the IP protocol suite is the means to realize a single network layer in which the network devices of all military platforms in the operation participate, hence making them technically interoperable on this layer. The IP layer provides a common interface for application protocols to access the IP network. The IP network, in its turn, uses all kinds of different layer 1 and 2 technologies (different transmission technologies) to connect individual military platforms to their neighboring platforms. It is expected that the lower layer protocols do not alter any of the IP layer header fields. With this model, the network heterogeneity can be hidden from the application developer, allowing the use of generic applications leading to a higher innovation potential. It should be noted that the use of generic, transmission-layer unaware, applications in a military mobile network may result in inefficient use of bandwidth and low quality of service. Therefore, mechanisms should be in place that enables efficient use of the scarce communication resources. This can for example be done by arranging that the end user application/service (we use both terms interchangeably in the text) and/or a higher layer communication middleware has some awareness of the characteristics of the network it uses to transport its data. Alternatively, a middleware layer may take care of such aspects on behalf of the end user application. Either way this means that for military mobile networks the classical TCP/IP-model must be expanded to allow a well-defined, minimal set of metadata that describe the characteristics of the current status of the network, to be exchanged in a cross-layer way within the TCP/IP protocol stack. In Section E.4.4 a cross-layer information exchange interface that can improve the performance of one of the routing architectures is described. Cross-layer aspects for the purpose of network-awareness of applications and services are out of scope of this study. Please note that there might be additional cross-layer information that can be of interest also to the routing layer, e.g., for auto-configuration of the tactical router.

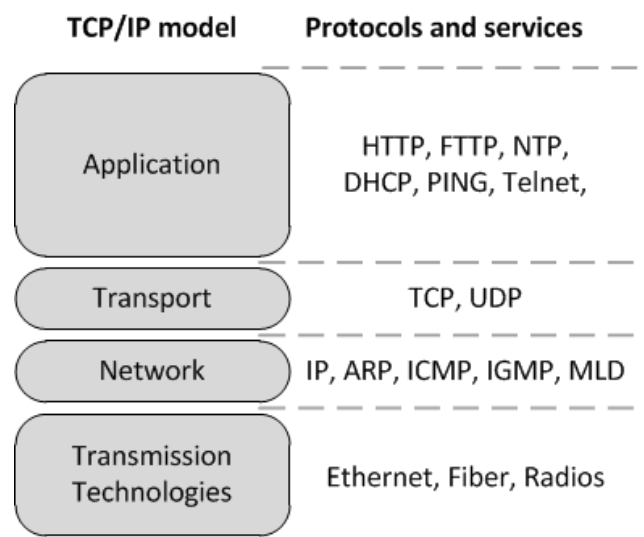


Figure E-1: Network Model.

In order to explain the different routing architectures, we try to use protocols that are standardized or best practices in the IP and MANET communities (most notably the IETF) as far as possible. Whenever these protocols are insufficient to fully explain our architecture(s), we use modifications of them or refer to other protocols that are proposed by the research community. Some protocols may be more open to additions than others. It is of high value to build upon an extensible protocol design while not breaking the standard compliance with the vanilla protocol.

E.1.4 Cognitive Radio and Topology Control

There is much ongoing research on cognitive radio and networks with topology control. In Ref. [5], network controlled topology is described as follows: “*Network-controlled topology describes a network control system that proactively and fluidly controls the network topology through configuring each node’s operating band, waveform, and waveform parameters. This is a radical change from prior network stack designs where the network layer’s job is to optimize performance within a topology given by lower layers.*” We can expect these types of networks to represent one or several network segments of the common heterogeneous tactical mobile network in the future. Many challenges are associated with this topic: Innovative routing techniques are needed to control and utilize such networks in the best manner. Signaling must be done in a different way, new mechanisms are needed for metrics and path calculation. The routing protocol must interact closely with the topology control element. This is still an immature research area, thus we will not consider topology controlled networks to be present in the heterogeneous network discussed in this report, and leave that for future work.

E.1.5 Other Network Paradigms

While the focus of this study is on realizing a common IP layer for tactical networks, we are aware of emerging technologies that may have impact of the role of IP in network technology. We consider Software Defined Networking (SDN), Network Function Virtualization (NFV), Information-Centric Networking (ICN) and Named Data Networking (NDN) as prominent examples of this.

SDN changes the paradigm of IP routing, which is a distributed signaling mechanism where control and data plane are collocated on each single router [6], [7]. SDN in its pure form separates the control plane from the data plane and creates a centralized entity that controls the forwarding nodes (“SDN-switches”) via a configuration interface. For military contexts more decentralized approaches are under investigation for example by IST-142 “Software Defined Network Architectures for the Federated Mission Networks” and in Refs. [8] and [9].

Network Functions Virtualization [10] enables network functions to run on commodity hardware instead of specialized hardware for that specific function. More advanced forms of NFV include flexibility of function placement, allowing functions to be moved to other hardware to improve usage efficiency of the hardware or influence the performance of the end-to-end service. Whereas SDN focuses more on programmable connectivity, NFV covers management and control of connectivity as well as computing and storage resources. SDN and especially NFV have found their applications first in commercial operator and data center networks (e.g., Refs. [7], [11]).

ICN and NDN (e.g., Refs. [12] and [13]) provide an alternative mechanism for distributing content, where instead of addressing nodes by their IP address, content is being addressed directly, using interest messages and caching of content on intermediate nodes. ICN can run on top of an IP network, but could also replace the IP layer. In the latter case, the introduction of ICN can be quite disruptive. A follow-up group IST-161 plans to further investigate ICN.

E.1.6 Definitions

In this section we define terms that are used throughout this document in the context of routing in heterogeneous networks. We provide these definitions to avoid confusion in the interpretation of terms that may have different connotations among different readers.

Network Segment: We use the term network segment to refer to a bounded portion of the heterogeneous network. This can be any portion, smaller than a transmission technology domain and multiple protocol domains, but often the segment will be the same as the transmission technology domain or the routing protocol domain. A network segment has to be bounded and topologically (not necessarily physically) connected.

Transmission Technology Domain: We use the term transmission technology domain to refer to a network segment that uses one unique transmission technology. The transmission technology encompasses Physical (PHY) layer design, Medium Access (MAC) layer design and Logical Link Control (LLC) layer design. When the same PHY, MAC and LLC are used, but separate frequency bands are allocated, we also consider the network to represent two different transmission technology domains.

Modem: We use modem to refer to a device or function that implements a transmission technology and that does not have an accompanying routing layer. We use the layer-two radio and modem interchangeably to visualize that sometimes this is a device implemented in its own casing and other times it is a hardware and software function embedded with a tactical router or a layer-three radio.

Routing Protocol Domain: We use the term routing protocol domain to refer to a network segment that uses one routing protocol. The routing protocol domain can consist of one or more transmission technology domains if the routing protocol can support different transmission technologies with the same protocol. In military radio systems the routing protocol domains and transmission technology domains can often coincide, e.g., in case of a radio-specific routing protocol. In classical Combat Net Radio (CNR) systems, there is no notion of a routing protocol domain at all, but only radio broadcast is used.

Administrative Domain: We also need to take into account connectivity between different administrative domains, which is a set of Information Communication Technology (ICT) systems (hosts, radios, routers, switches) that are managed by the same administrative entity. This domain can be larger, equal or smaller than the transmission technology domains and protocol domains. We can even envision that a technology domain and/or routing protocol domain can be part of two or more different administrative domains (e.g., STANAG 5630 “Narrowband Waveform for VHF/UHF Radios” (NBWF) used for interoperability between different nations in a coalition operation).

Autonomous Systems (AS): An Autonomous System (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the network. Often this domain will be larger than the transmission technology domains and routing protocol domains.

Interconnection Platform: An interconnection platform represents platforms where different routing protocol domains and/or transmission technology domains meet physically. The platform can have a tactical router where more than one routing protocol domain and/or more than one transmission technology domain is connected or it can have several routers that are connected with wires and implements information exchange interfaces for the routing layer.

End-to-end Connectivity: Connectivity for routing paths that crosses several transmission technology domains and/or several routing protocol domains.

Security Domain: A security domain is defined as a (sub) system under the control of a single authority which the entities herein trust. The security policy in place over a domain is defined either implicitly or explicitly by its authority [14].

Information Exchange Interface – Modem (IEI-M): For the discussion in the report, this is a term used to define an open interface between the lower layers of a radio and a routing function. The routing function can be located in an external router or installed on the same hardware platform. This interface is described in more detail in Section E.4.4.

Information Exchange Interface – Router (IEI-R): The IEI-R represents the interface between the routing protocol domains of different network segments that reside on the same hierarchical level. This interface can

be used both internal to a nation's network and external in order to establish a coalition network. As discussed in Section E.4.3.1, sometimes the routing functionality of a radio is placed on layer-two in the network protocol stack. We include also exchange of routing information with radios that include sub-layer 3 routing in the definition of the IEI-R. This interface is described in more detail in section A.4.4.

Information Exchange Interface – Router Overlay (IEI-RO): The IEI-RO represents the interface between the routing protocol domain of a network segment and the overlay routing domain. This interface can be used both internal to a nation's network and external in order to establish a coalition network. Similar to the IEI-R we include also exchange of routing information with layer-two radios in the definition of the IEI-RO. This interface is described in more details in section A.4.4.

Network Control: This term represents signaling messages with the purpose of realizing (reliable) communications. In radio networks, these are usually transmitted in-band. Network control usually aims to learn or react to changes that occur in a network that cannot be predicted upfront, but depend on, e.g., the traffic load on the network or changes in the topology because of node mobility or changes in the link quality. Examples of network control messages are routing protocol messages, QoS related messaging (e.g., for the Resource Reservation Protocol (RSVP)), acknowledgements on the MAC layer and congestion control mechanisms for TCP. Some technologies (e.g., SDN) might also send this signaling out-of-band.

Network Management: The term network management means actions (usually configuration but also performance monitoring) on network elements with the purpose of providing them with the right information such that the network elements can function correctly when the network is running. Traditionally, network management in the tactical domain takes place out-of-band prior to the start of an operation, but it also includes maintenance of the network during an operation in case something has gone wrong. Network management can be seen as an action from outside to configure or fix the network. While network control traffic is caused by autonomic processes such as routing daemons, network management is traditionally executed by humans. With technology advancement, e.g., under the influence of virtualization and SDN technologies, some network management functions become automated, and the separation between the areas of network management and network control becomes less clear.

Tactical Router: A device or (software) instance with a common routing function for either the flat or overlay architecture. A tactical router acts as the connecting element in a heterogeneous tactical network that requires a common protocol (i.e., the flat architecture and the interconnect-overlay architecture (see Section E.4). The tactical router runs the routing protocol of choice for the common routing protocol domain. The device must be able to do routing over both embedded and external modems (transmission technologies).

E.2 REQUIREMENTS

IST-124 has identified a set of requirements to mobile heterogeneous networks. These requirements are all related to the process of establishing a network and to provide and sustain connectivity. In Annex I: "QoS Framework," additional requirements related to resource management and Quality of Service (QoS) can be found. The connectivity requirements are grouped according to the functionality they provide. The requirements are not prioritized. Some of them are essential in order to provide a basic end-to-end connectivity. Others focus on improving the network to increase for instance robustness and throughput. We use the terms "must" and "shall" in those requirements we consider more important, and "should" for the others. However, we envision that dissimilar operations will prioritize the requirement differently. As an example; some will have a high need for robustness while others will require flexibility in how the networks resources are used.

E.2.1 Heterogeneous Network Routing

The goal of the heterogeneous network routing requirements is to ensure that connectivity between nodes is arranged between all users that want to exchange information.

- The network must provide end-to-end connectivity supporting both unicast and multicast services if a physical connection of any kind exists, and the network policy allows the connection.
 - It must be possible to find a route from any source to any destination through a sequence of any of the network segments deployed in the operation.
 - If a mobile network segment becomes partitioned, it must be possible to find a route (if one physically exists) via other mobile networks or the deployed backbone networks, to a destination in the other partition of the network segment.
 - If a mobile network becomes partitioned it should be possible to find routes between all sources and destinations inside each of the partitions.
 - If the deployed backbone becomes partitioned, it should be possible to find a route through a mobile network (if one exists) for high priority traffic.
- The heterogeneous network must be “radio silence” aware to cope with radios or network segments in radio silence.
- Multicast is an important traffic type in tactical networks. Efficient means for both intra domain and inter-domain multicast should be supported. Interaction between traditional multicast and other network segment specific multicast protocols should also be supported.

E.2.2 Robustness

The goal of the robustness requirements is to ensure that the availability of the network for the users is as high as possible, and that disruptions in communications streams and data exchange between users are prevented.

- Within a technology domain, connectivity should be high enough to allow for alternative paths especially in the case of link failure.
- There should be mechanisms to make smart use of available frequency spectrum. Combining different transmission technology domains can increase robustness in the presence of jamming while allowing for high data-rates when jamming is not present.
- A network segment should support the possibility to connect to other network segments at more than one connection point simultaneously.
- A routing protocol should prioritize “stable” links to improve the robustness of the path.
- There should be security measures that prevent unauthorized entities from disrupting the network service or gaining illegitimate access to the signaling and user payload.
- The heterogeneous network should be able to mitigate Electronic Warfare (EW) threats.

E.2.3 Scalability

The goal of the scalability requirements is to make sure that large numbers of military platforms can successfully exchange information via the heterogeneous network.

- The heterogeneous network can in total consist of a large number of nodes. Some network segments can also be large. The tradeoff between network performance, reliability and overhead must be taken into consideration. Overhead includes signaling, redundant traffic and extra number of transmissions due to longer routing paths but also retransmissions because of using less reliable links.

- The routing protocols should be aware of the available communication resources (e.g., in terms of link data-rates) and the routing architecture must support differentiated routing overhead in order to reduce the signaling to a minimum for the low capacity network segments while maintaining a high signaling rate for highly mobile, higher capacity network segments.

E.2.4 Resource Efficiency and QoS

The goal of the resource efficiency requirements is to maximize the user data that can be exchanged between users via the heterogeneous network given a certain time span, and to provide QoS.

- At least one resource efficient path (e.g., in terms of channel usage and spatial reuse) through the heterogeneous network must be found between the source and destination.
- Several paths should be made available for different traffic types (QoS classes) to choose the most suited path for each class. These paths might be calculated using different routing metrics and based on different link/path parameters.
- Policies that govern how control information can be spread in different network segments are needed.
- The network should provide standardized information on the status of the network to applications and/or middleware that want to make use of this.
- The network must be able to implement detailed network policies for providing different QoS to different communication flows/data exchanges.

E.2.5 Configuration and Management

The goal of the configuration and deployment requirements is to minimize the effort needed to configure and maintain the network and reduce the need for human intervention in the network to ensure correct operations in different and changing circumstances.

- The network should be self-configuring as far as possible to reduce the need for complex manual adjustments to the scenario.
- The connection of new network segments (e.g., from coalition partners) to the heterogeneous network should be fully automated.
- It should be easy to include new radio types and tactical routers in the coalition network (zero-config).
- The architecture should be able to implement a change in defined network policies in real time.

E.2.6 Other Requirements

- Protocols and interfaces between routers, radios and network segments should be based on open standards, or on NATO standards (which can be based on open standards).

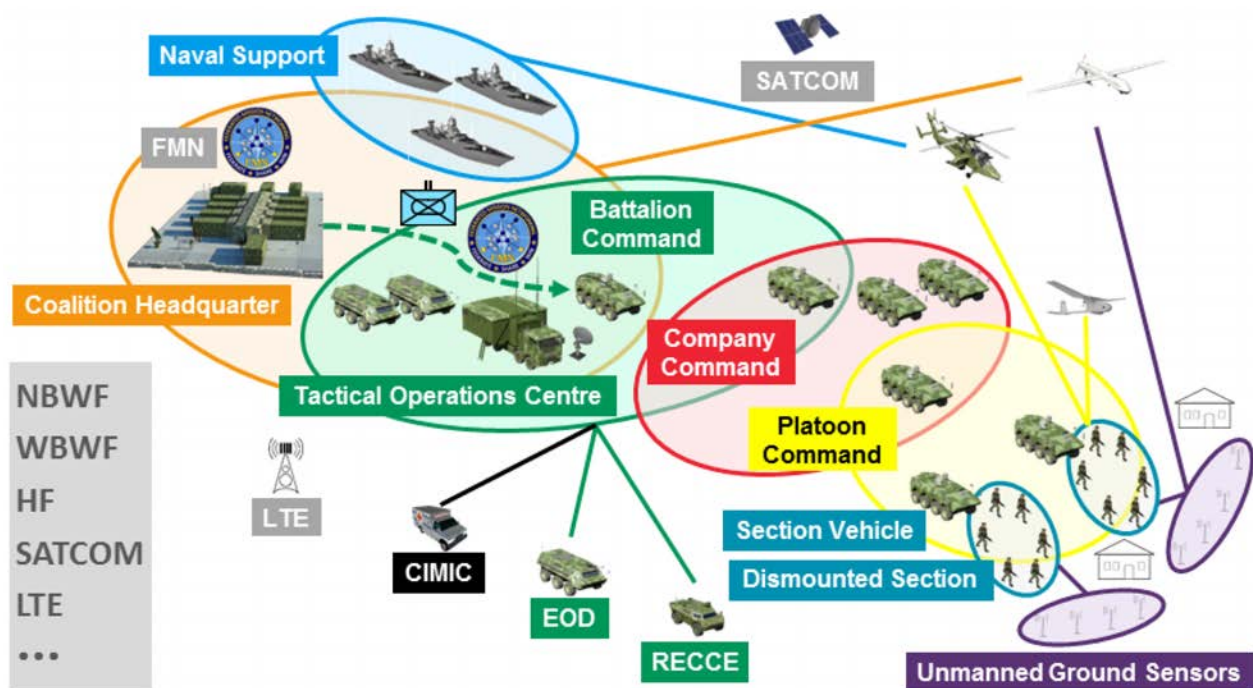
E.3 OPERATIONAL NETWORK TOPOLOGY CONSIDERATIONS

One important aspect when designing a routing architecture is what the networks look like in operational practice, both the way the nodes are positioned relative to each other, how they are connected, and between which users data will be exchanged. Next to executing a clean slate analysis, we should also take into consideration how data is currently (or in near future) exchanged between units at the tactical edge. The latter is determined by aspects such as the availability of interoperability standards (e.g., FMN), national security policies, and the technical capabilities of the systems in terms of range and capacity.

- Annex A: “Operational Perspective for IST-124”;
- Annex B “Emulation-Based Experimentation and the Anglova Scenario”; and
- Annex C “Experimentation Environment and Tools”.

Three types of tactical network attachment can be considered:

- The mobile tactical edge is connected as a stub topology.
- The mobile tactical edge is connected in a tree topology stub.
- The mobile tactical edge networks represent a mesh topology.



E.3.1 Stub Topology

The easiest and least complex constellation is to connect each radio network (transmission technology) to the deployed backbone networks as stubs. Local Area Networks (LANs) directly connected to the stub are assumed to be an integrated part of the stub. In this situation the traffic is either produced or consumed in the stub network. The stub networks cannot be transit networks (Figure E-3). The stub network can have one or more interfaces to the backbone, but transit traffic across the stub network is not allowed. The network segments can belong to either different national units or different nations. The colors in the figure represent different transmission technologies. The figure shows network connections and not information flow.

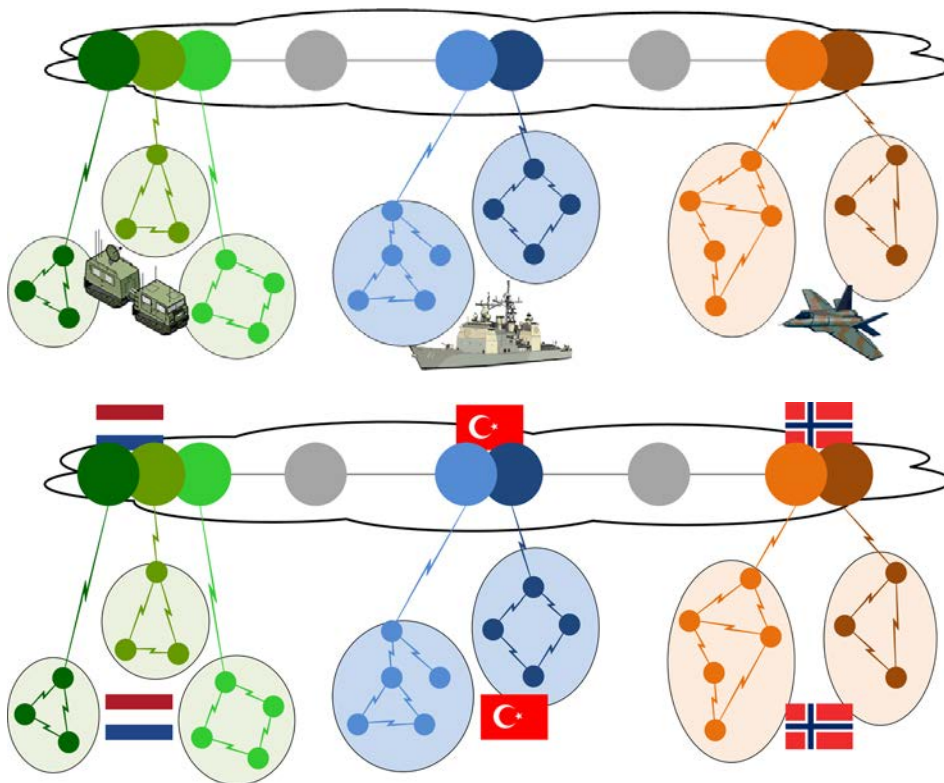


Figure E-3: A Network Topology Where the Different Networks Segments (Technology Domains) are Connected to a Deployed Network as Stubs.

E.3.1.2 Advantages

A stub constellation for edge networks does not require much routing information to flow between networks, thus the signaling overhead can be low. One or several interconnection platform(s) that connects the transmission technology to the backbone is sufficient, and the end-to-end routing decisions are handed over to the backbone. In order for data to flow from a soldier connected to one radio network to a soldier connected to another radio network in this constellation, the data traffic must travel via the backbone networks. In terms of interoperability, the stub network constellation means that interoperability mechanisms on the deployed level can be used to share data between edge networks of different nations, and that no coalition interoperability measures on the network layer are necessary on the mobile tactical level.

E.3.1.3 Challenges

This stub network constellation puts a tough requirement on the range of the backbone network in the theater. This network must be extended to lower tactical levels to provide sufficient connectivity with this topology. Alternatively, the different stub networks must strive to maintain an internal topology with for instance deployed relays providing a connected route to the backbone. If the connection to the backbone becomes unavailable there will be no end-to-end connectivity in the heterogeneous network between soldiers connected to different transmission technologies (including soldiers of other nations that cooperate on team or platoon level). In addition, it is not bandwidth efficient to send data that are only needed on the lower tactical levels, via the backbone. The end-to-end connections may also have long delays. The robustness of this network constellation can be improved, by having multiple connection points between each stub and the backbone.

E.3.2 Tree Topology Stub

E.3.2.1 Description

This is a topology that reflects the chain of command in a military network. In this topology the different transmission technology domains of the heterogeneous edge network are connected in a predefined tree topology. The IP address plan also reflects the tree such that leaf networks have a network mask that is part of the shorter network mask of the parent network. All transit traffic (flowing from leaves to the backbone) can be routed over multiple tactical transmission technology domains, by letting each domain send traffic to an interconnection platform that forwards the traffic to the next level in the tree (Figure E-4). Traffic from the backbone to the leaves will be routed towards the interconnection platform that announces the longest prefix match of the address. Seen from the backbone network, each tree represents a stub. The network segments can belong to either different national units or different nations. The colors in the figure represent different transmission technologies. The figure shows network connections and not information flow.

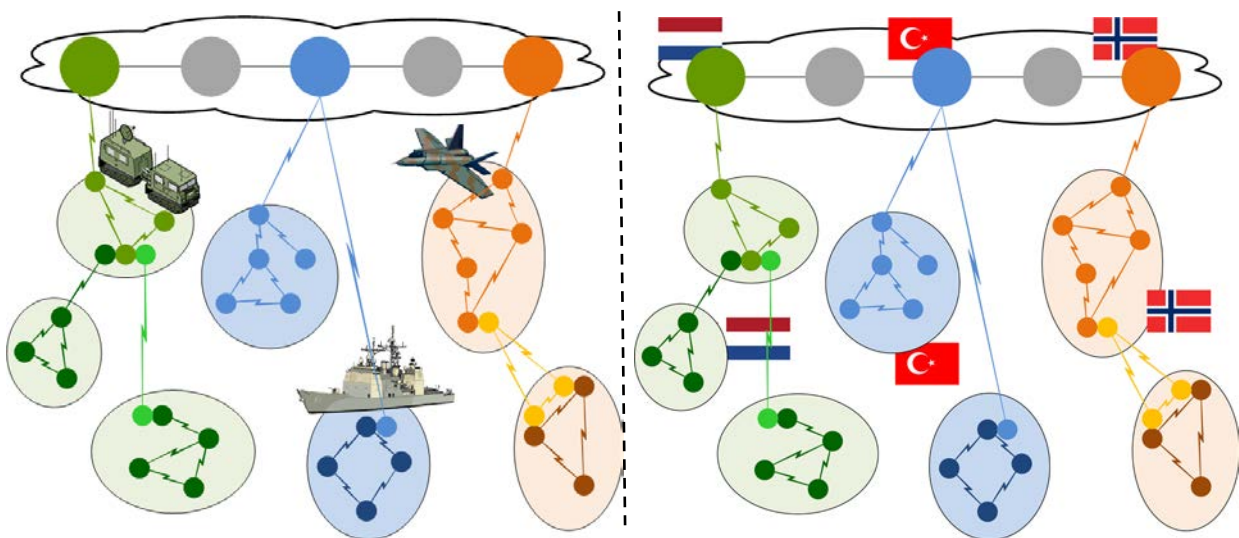


Figure E-4: A Network Topology Where the Different Networks Segments (Technology Domains) are Connected to a Deployed Network as Stubs in a Tree Structure.

E.3.2.2 Advantages

This is also a low complexity network topology where the leaf networks of the tree topology can still work well by having predefined interconnection platform(s) and no other signaling of external routing information is needed. This topology does not require the backbone network to be deployed to lower tactical levels. It also lessens the burden on the different radio networks to maintain a connection to the backbone. In this situation the radio networks must maintain connectivity to the parent node in the tree.

This topology is more flexible than the pure stub topology in the sense that it allows for more routes to be found and used in the tactical network without having to route the traffic via the deployed semi mobile network or the backbone. In a military network (e.g., the Army) the trees would resemble the military structure where command vehicles (or more likely the signaling vehicle in the unit) will be the parent node for the subunits of the larger unit. In this manner traffic only need to flow up to the nearest common command level for traffic to flow end-to-end from one leaf network to another in the heterogeneous network. The figure shows a national tree, but it can also be a coalition tree.

E.3.2.3 Challenges

A main consideration is the preconfigured and static nature of this approach, and the challenge that it poses to achieve robustness. The routers on the interconnection platform(s) that connect the different tree levels have to be configured in advance of the operation. Any change in the organization of the units (e.g., a company joins an adjacent battalion to strengthen a certain position) will require reconfiguration of the network as well. Also, the networks, that are configured to be higher up in the tree, effectively become transit networks for the lower networks. Long end-to-end delays are also likely with this topology. Capacity on reach-back connections can be low (e.g., expensive satellite capacity or other low data-rate Beyond Line-Of-Sight (BLOS) links).

E.3.3 Mesh Topology

E.3.3.1 Description

The mesh network topology is the most flexible topology, and likely also the most robust design. In this constellation all networks can be transit networks (if the policy allows this). The aim is to decide per packet via which nodes and networks the traffic flows, choosing the most optimal path to the destination at that moment in time.

E.3.3.2 Advantages

This is by far the most flexible topology where all possible links in the heterogeneous network of an operation can be used to find the best path for the traffic. In this case there can be many interconnection platforms that connect different transmission technologies and routing domains and the network segment must have sufficient routing information to select the correct interconnection platform(s) for the path (Figure E-5). Because of this, the topology is very robust. It doesn't rely on a set of 'key' nodes in the network topology. And it makes optimal use of network resources. In Figure E-5, the network segments can belong to either different national units or different nations. The colors in the figure represent different transmission technologies. The figure shows network connections and not information flow.

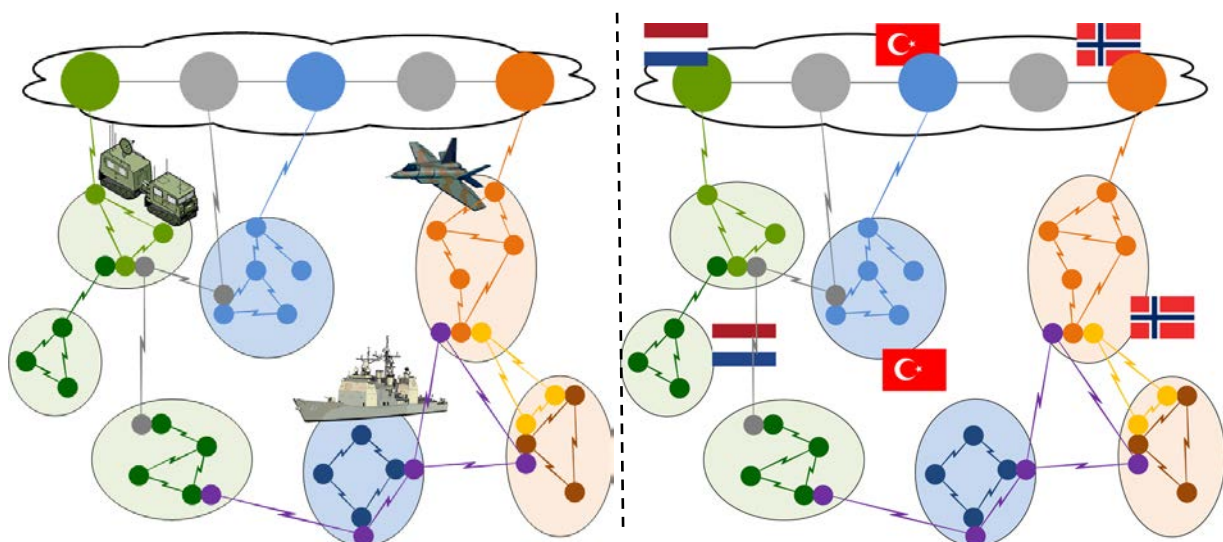


Figure E-5: This Network Topology Represents a Situation Where the Different Network Segments are Connected as a Mesh.

E.3.3.3 Challenges

This network topology is the most complex of the three presented here. To be able to form mesh connections, one or several common² waveforms must be present in the heterogeneous network, or radio(s) of the different transmission technologies must be borrowed between coalition partners to establish the necessary interconnection platforms. There is a lack of standardized common waveforms – tactical radios tend to come with different proprietary waveforms. However, NATO's interoperability waveform, NBWF, is one example of an emerging common waveform. To find the best path, nodes must learn about the network topology of the complete heterogeneous mobile network. This means that lots of information must flow between nodes and protocols leading to a scalability concern, especially narrow band networks can get overloaded just by carrying the signaling traffic. When a narrow band network is used as the common waveform, care must be taken to prevent overloading of those links. In addition, there is also a risk of instability of one network segment to affect nearby segments.

E.3.4 Conclusion

A network topology for a heterogeneous network where few of the network segments allow transit traffic requires relatively little signaling traffic to maintain routes. The stub topology approach is the situation we often see today. The reliance on a deployed backbone that is extended to lower tactical levels or long communication paths in the radio networks provide challenges in terms of robustness, bandwidth efficiency, delay and flexibility. As we envision a growing number of different networks to be present in future operations, and an increasing requirement for multi-national cooperation on the tactical team level and below, we believe that some mesh structure is necessary in the design of the mobile military heterogeneous network. Therefore, the investigation of a mesh network topology is the main focus of the remainder of this document. A mesh topology will increase the signaling in the network and we discuss different methods to mitigate that as well as allowing some networks to alter between being stubs or transit networks controlled by policy. It should be noted that the mesh approaches may also be used to realize a more flexible flavor of the tree topology in conjunction with stub elements. The choice of tree structure versus mesh structure is also discussed in Ref. [15], where the authors discuss several consequences (also non-technical) of choosing the one or the other.

In this section we have not shown how the security architecture of the network is designed, we have focused on the tree different network topologies assuming a security architecture that does not limit the information flow between protocols. See “IST-124 Heterogeneous Networks, Security architecture” for a description of possible security architectures for the heterogeneous network [16]. This architecture will heavily influence the routing design. We will discuss the implications of this in Section E.7.

E.4 ROUTING ARCHITECTURES FOR MOBILE HETEROGENEOUS NETWORKS

In this section, we discuss a few alternative routing architectures that can be applied in realizing a well-connected heterogeneous tactical network. State-of-the-art radios and routers cannot support all functionality that is assumed for the described architectures. Some functionality can be accomplished in short term, whereas other functionality represents a longer term target architecture. The architecture approaches are briefly described in Section E.4.2. We describe implementation issues that have consequences for the architectures such as the deployment of functionality in one or several separate boxes in Section E.4.3. We discuss interfaces for information exchange in the different architectures in Section E.4.4, IP address considerations in Section E.4.5 and in Section E.4.6 we discuss network policies that might govern the choice of architecture or that must be supported by the architectures. The architectures aim to realize the mesh-topology concept that was introduced in Section E.3.

² A common waveform can be either a common standardized waveform or a vendor-specific waveform that are common to several of the coalition partners in an operation.

For any of the architectures to work, it must be possible to establish a transmission connection (wireless or physical) between the nations. Possible approaches for the inter-nation connections are:

- Use a standardized NATO transmission technology common to some or all of the partners (e.g., NATO NBWF); and/or
- Use a proprietary transmission technology common to some or all of the partners (e.g., Harris 117G); and/or
- Interchange a few national radios (transmission technology) with partners.

The purple and grey networks in Figure E-5 represent the inter-nation connections. The connection between the inter-nation networks and national networks happens on the interconnection platforms. The interconnection platforms are also used to provide connectivity internal to a nation. If only a few interconnection platforms exist these are likely to be single point of failures for the routing architecture and the connectivity cannot be made very robust. None of the described architectures are more robust than what the heterogeneous network can actually provide of connectivity. How to select which military platforms that should serve as interconnection platforms is a challenging network planning task. Annex F: “Interconnection platforms in vignette 2” provides some insight in this challenge, by showing the effects of choosing different numbers of interconnection platforms in the Anglova scenario (see Annex A and Annex B). A simple choice that is assumed for the routing architecture discussion is to pick all military platforms that have two or more transmission technologies installed and/or several routing protocol domains, as interconnection platforms.

The three routing architectures that we discuss are:

- **Flat architecture:** Flat, single routing domain routing architecture; and
- Interconnect routing architecture, of which we describe two flavors:
 - **Interconnect-flat:** Flat, interconnect routing architecture; and
 - **Interconnect-overlay:** Interconnect routing architecture using an overlay.

The routing architectures define how one or several routing protocol(s) is/are used to provide end-to-end connectivity in the heterogeneous network. When several protocols are used, information exchange interfaces between the protocols are needed. The architectures also define how topology and link information is shared in the whole network and over which information exchange interface the information flows. It should be noted that a combination of some or all of these architectures can be applied at the same time to form a hybrid architecture; this is in fact the most likely case. But in order to identify their strengths and weaknesses, we describe them separately. The architectures are briefly described next and discussed in detail in Section E.5. A comparison of these approaches is presented in the Section E.6.

First, we describe the symbols that are used in the figures. Not all the symbols are used in the figures in this section but are used in figures in following sections.

E.4.1 Symbols

We use the following symbols in the figures:



Transmission technology devices **without** Layer-Three (L3) IP functionality. Different colors represent different transmission technologies (modems). This modem can be either an interface card with an antenna which represents a modem embedded in a device or a separate handheld or vehicle-mounted device with an additional wireline interface. It is assumed that this transmission technology does not do any routing (no Layer-Two (L2) routing).

	Routers with an antenna represent transmission technologies with embedded L3 IP or sub-IP routing. The routing protocol can be a standardized protocol or a protocol that is particularly designed to work together with the transmission technology for improved performance of the radio. Different colors represent different routing protocol domains, and different transmission technologies or frequency assignment. For the remainder of this section we assume that these routers do L3 routing both for the wireless interface and for their wired interface(s). Implications and consequences for situations when the router does L2 routing are discussed in Section E.4.3.
	Router with two transmission technologies, that participates in two different routing protocol domains.
	The white router is a router fulfilling the flat IP routing function as described in the flat architecture. If the router has antenna(s) it holds one or more transmission technologies, for example a device that runs the routing protocol and has a wireless interface card on board.
	White routers with a colored line are used to indicate routers of the flat routing architecture that form different routing protocol domains (e.g., one for each nation). They may or may not run the same routing protocol.
	The blue router is a router fulfilling the overlay IP routing functionality as described in the interconnect-overlay architecture.
	The LAN represents the local area network to which all services and sensors are connected. We envision that there will be a LAN also on small military platforms such as soldiers and vehicles.
	A dotted oval represents an interconnection platform. Radios and routers and other devices that are together inside a dotted line are collocated on a single military platform.
	The cloud represents a routing protocol domain.
	A closed circle indicates military platforms that are grouped together into an operational unit, e.g., a company.

E.4.2 Routing Architecture Approaches at a Glance

E.4.2.1 Flat Architecture

For this architecture approach, one common routing protocol is used by all network segments. Different transmission technology domains use the same routing protocol. There are no routing protocols tailored for the specific transmission technology included, but the common protocol can to some extent be tailored for different transmission technology with different configuration of available parameters. This approach is visualized in Figure E-6. This architecture is typically deployed with layer-two radios that are connected to a tactical router that runs the common routing protocol, but could also be deployed with layer-three radios that are running the common routing protocol on both the wireless and wired interfaces. See Section E.4.3.1 for more discussion on the placement of different network functionality. No information exchange interface on the routing layer is necessary, but an Information Exchange Interface (IEI-M) between the routing function and the Modem (transmission technology) is needed. This interface can also be a coalition interface in situations when a nation lends a radio to the coalition partner's interconnection platform(s). The scalability and flexibility of this architecture is influenced by:

- 1) The required signaling by the routing protocol; and
- 2) The information made available over the IEI-M interface.

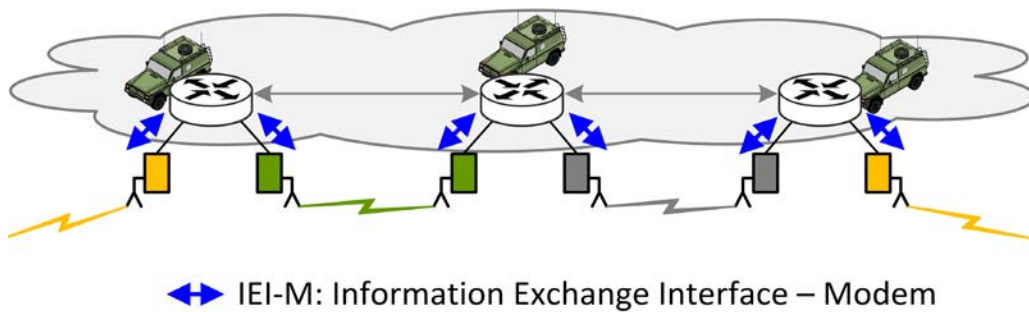
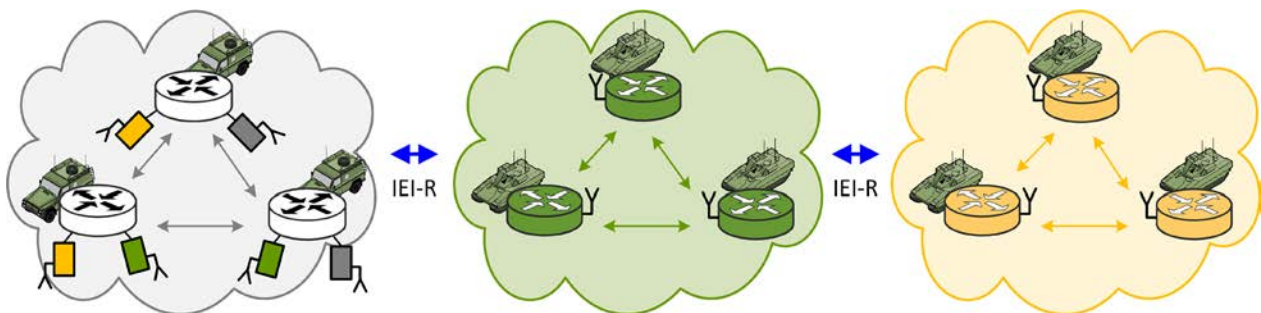


Figure E-6: Flat Routing Architecture: There is Only a Single Routing Protocol Domain Built on Top of Multiple Transmission Technologies, With IEI-Ms Between the Routing Function and the Modem (Transmission Technology).

E.4.2.2 Interconnect – Flat Architecture

This architecture type connects network segments that are separate routing protocol domains. The network segments can use standardized routing protocols or proprietary protocols. Some segments might also use identical routing protocols on separate frequency bands or under different administrative domains. The routing domains interconnect via an Information Exchange Interface (IEI-R). Each location that is part of multiple routing domains (interconnection platforms where routing protocols from multiple routing domains are running) has an IEI-R between each two routing domains. This IEI-R can be both a national interface and a coalition interface. This approach is visualized in Figure E-7. Via the IEI-R, the routing protocols of the respective domains inform each other about relevant reachability information for destinations that can be reached via the routing domain. The scalability, flexibility and robustness of this architecture are influenced by:

- 1) The level of detail of topology and link information made available via the IEI-R between adjacent network segments; and
- 2) The functionality and overhead of the routing protocols in different routing protocol domains.



IEI-R: Information Exchange Interface – Routing

Figure E-7: Interconnect – Flat Architecture: Multiple (Flat) Routing Protocol Domains are Residing Next to Each Other with IEI-Rs Between Each Other.

E.4.2.3 Interconnect – Overlay Architecture

This architecture is similar to the interconnect-flat case in the sense that it includes multiple network segments that are separate routing protocol domains. However, in this architecture an extra layer of routing is introduced in an overlay that spans the whole heterogeneous network and connects the separate routing protocol domains. Only a subset of the routers in the heterogeneous network participates in the overlay network. These routers are located on the interconnection platforms. This scheme is similar to the architecture the Border Gateway Protocol (BGP) uses to connect different domains. A routing protocol

Information Exchange Interface (IEI-RO) is needed between the routing protocol in the overlay network and the routing protocol domains in the different network segments. Such IEI-RO is located on the routers in the interconnection platforms. In this scheme there are no IEI-Rs between the different routing protocol domains. This approach is visualized in Figure E-8. The scalability and flexibility of this architecture is influenced by:

- 1) The level of detail of topology and link information made available via the IEI-RO between the routing protocols in the different network segments and the routing protocol in the overlay network; and
- 2) The functionality and overhead of the routing protocol in the overlay.

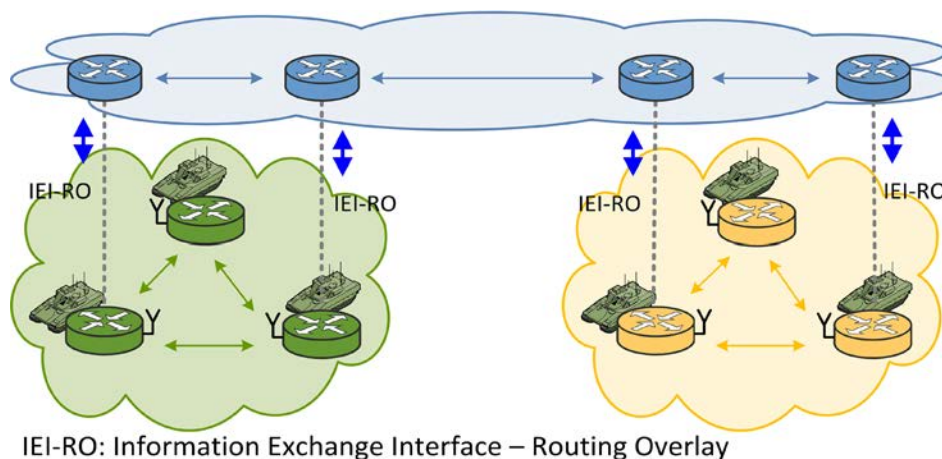


Figure E-8: Interconnect – Overlay Architecture: Some Military Platforms in the (Flat) Routing Protocol Domains are Also Part of an Overlay Routing Domain (Blue) which Connects all the Separate Routing Protocol Domains.

E.4.3 Implementation Issues

In the introduction of the routing architectures, we have followed strictly the TCP/IP-model where we assume that the lower layers (or a layer-two radio) do not alter any of the IP layer header fields. The use of the TCP/IP-model however raises some questions and poses some challenges with respect to practice, where these TCP/IP layered principles for various reasons are not always in place which is the case for many existing military radios. This section briefly discusses the following design issues, and the consequences they may have for the routing architecture:

- The network layer chosen to perform the routing function;
- The deployment of network functionality in one or many separate boxes; and
- VHF radios and IP.

E.4.3.1 Layer for Routing Functionality

In the description of the different architectures we have assumed that routing is performed on the network layer in the protocol stack (Figure E-1). It is likely that some of the radio vendors might instead place the routing functionality on layers below the network layer. If layer-three routing is included in the radio, it depends on the architecture and the availability of an IEI-R or IEI-RO whether routing paths and metrics in the radio's wireless routing protocol domain is visible to adjacent network segments or not. If on the other hand the radio does not have a built-in layer-three router, it is a layer-two device (modem) with or without routing functionality on lower layers. In this case, when a network segment that does routing below the

network layer, is connected to classical routers, then all topology information of this network is hidden and it appears (for the IP layer) as a network with one hop to all destinations in that network segment. The lower layer domain is not able to report any topology details over a routing protocol information exchange interface between routing functions on layer-three (IEI-R/IEI-RO). In order to make the topology information and metrics available for the network layer, a cross-layer function must be made available. For example, in Ref. [17], work is proposed to make lower layer topology information known to the network layer of an external router. If such functionality is in place it does not matter for the architecture discussed here, which layer the routing functionality is implemented on. However, the different solutions may have consequences on how easily the different routing architectures can be deployed. For example, in order to use a radio with layer-three routing in a flat architecture the common protocol must be available in all radios with layer-three routing.

As different nations may use dissimilar approaches, it is appropriate to be able to handle both layer-two and layer-three radio systems within the same architecture. For layer-two radios an external tactical router is used, which probably can be more easily adapted to the architecture of choice compared to a built-in layer-three router. This means that if the rest of the networks use a common routing protocol (flat architecture), a network segment with layer-two radios without routing is easily included in the heterogeneous network via a direct connection to the tactical router. If the layer-two radio does routing, it can still be easily introduced to the heterogeneous network via a tactical router resulting in an interconnect type architecture. In order to exchange topology information between the layer-two routing domain and a connected domain, an IEI must be in place this can be implemented as special case of the IEI-R/IEI-RO. This is not discussed further here. If the layer-two routing does not carry IP address information, the tactical routers must also run some lightweight protocol to share IP addresses over the layer-two radio. This aspect is out of scope for this report.

An interconnect-overlay architecture can also be built on some network segments based on layer-three radios and others based on external routers and layer-two radios. If the layer-two radios do routing, then some of the connected external routers are chosen to be interconnection platforms. These must also run the routing protocol of the overlay. As discussed above, an IEI is needed to share topology information between the layer-two routing and the overlay. Also for this case the tactical routers might need to run a lightweight protocol to share IP addresses over the layer-two radio. An advantage of placing the routing functionality on layer-two, is that tunneling of the overlay routing information through the radio network is not necessary. The overlay routers will all be one hop away from each other at layer-three. For this discussion it is assumed that the routing functionality at layer-two support the same functionality that is typically expected from routing at layer-three such as loop detection and multihop multicast. In Annex G: “OSPF scalability” we shed some light on the scalability and feasibility of using OSPF as an overlay over layer-two radios in a heterogeneous network.

Identifying the layer on which the routing functionality should be implemented for optimized performance is out of scope for this document. The best choice may depend on the properties of the local radio network, for instance mobility and traffic types.

E.4.3.2 Network Functionality in One or Many Boxes

The network functionality on a military platform can be manufactured and deployed in many different ways. In one case, one powerful server can be used for all network functionality on a platform. For this case, the different transmission technologies must be made available and installed as different network cards to the server and routing software (and maybe even lower layer protocols) runs on the common server. Both manufacturer-specific protocols and/or standard protocols can be installed. In the other case there can be a handful of separate boxes all with internal processing power. The boxes can be routers, radios with routing functionality or radios without routing functionality. For the routing architecture discussion, it does not matter how the functionality is manufactured. For the server case the IEI-R, the IEI-RO and the IEI-M

interface between the routing layer and the lower radio layers will be internal to the server, whereas for the case with many boxes, the interface must be implemented with a protocol over a wire between two different devices. In present military networks, the case with multiple boxes is prevalent. Only when different transmission technologies from one vendor are present on a military platform, they might be combined in a box providing multiple radio channels.

One reason for bringing up this discussion is to show that in the future a more flexible solution with one server for all network functionality on a military platform might be available, removing the cost of installing multiple boxes on a platform. Using one server for all network functionality can also reduce “Size, Weight and Power”. Thus, the argument that one architecture leads to a situation with many more boxes than another architecture, is not considered important here.

E.4.3.3 Low Data-Rate Radios in the IP Routing Architecture

Traditional Combat Net Radios (CNR) are VHF transmission technologies characterized by their small bandwidth of traditionally 25 kHz, resulting in limited data capacities. Traditional CNR technologies may have data capacities under 16 kbps, while state-of-the-art transmission technologies such as the NATO NWBF enable shared data-rates from 20 kbps to 82 kbps [18]. STANAG 4691 “Mobile Ad Hoc Relay Line-of-Sight IP Networking (MARLIN)” and HF transmission technologies with STANAG 5066 “Profile for High Frequency (HF) Radio Data Communication” are also examples of networks/links that can have very low data rates. Including such transmission technologies into a mesh IP routing topology as presented in Section E.3.3 is a challenging task, because of the overhead that is introduced by IP-headers, as well as the network control signaling that is required to keep the network connected. While IP header overhead can be dealt with by applying header compression or header replacement, reducing routing overhead is a challenge that is discussed further in Section E.5. Developing a protocol implementation that meets overhead requirements is identified as an important next step. Also, data dissemination mechanisms that can contribute to solving this problem and that may or may not be using a routing layer are in scope of the follow-up IST panel IST-161.

E.4.4 Information Exchange

Independent of the choice of routing architecture, it is necessary to have some network control information flowing in the network. This can be horizontal information exchange internal to a protocol or between protocols. Or it can be vertical information exchange between layers of one node, or between different layers of different nodes. In this report we are concerned with the performance of the routing architecture and interaction between routing protocols, rather than the details of individual routing protocols, thus we don’t consider horizontal information exchange internal to a protocol other than mentioning functionality that should be supported to enable its participation in the routing architecture.

In the introduction of the three routing architectures in Section E.4.2 the following IEIs were identified:

- The IEI-M interface between a routing function and a modem (transmission technology);
- The IEI-R between the routing protocol domains of different network segments; and
- The IEI-RO between the routing protocol domain of a network segment and the overlay routing domain.

Besides these interfaces the flat and overlay architectures require (multi-) national agreement on which flat or overlay protocol to use and parameter choices for these.

The IEI-M interface is used to exchange information between the lower layers of a radio (modem) and a standalone³ routing protocol. This interface is used by the flat architecture and should be available on

³ Stand-alone means that the router comes from another source (manufacturer) than (some of) the radios it connects to now or in the future. It can run on a separate device or can be also be a separate piece of software running on the same device as the modem.

interfaces between all standalone routers and connected transmission technologies. The interface is necessary also for the two other architectures, however when radios with embedded routing is used, the IEI-M interface can be implemented as part of an internal proprietary interface. The IEI-R is used by the interconnect-flat architecture and provides the information exchange between different equal level routing protocol domains. The IEI-RO is used by the interconnect-overlay architecture and provides the information exchange between the routing protocol domain of a network segment and the overlay routing domain. The latter two interfaces are needed only on interconnection platform(s). It is also possible to combine the architecture approaches to a hybrid architecture in a single network. If we have a hybrid architecture of interconnect and flat approaches, then the IEI-M interface will be used in network segments that use the flat architecture.

An IEI consists of two parts:

- 1) The information elements that should be made available via the interface; and
- 2) The protocol or function that carries the information elements from the producer to the consumer.

In Table E-1 we focus on the information elements. The table lists the result of an IST-124 brainstorm on what type of information elements we would like the IEIs to support and serves as a starting point for future determination on what information should be exchanged via the IEIs. The information mentioned in the table serves different purposes, and the importance of the information varies. Some of the listed objects are dynamic and expected to change over time and some are static capabilities of the modem and router. The latter elements can also be conveyed via a management interface.

Currently no satisfactory specifications for all of these IEIs exist. Some discussion on an IEI-M interface is given in Ref. [19] and there is ongoing standardization of the IEI-M interface with the Dynamic Link Exchange Protocol (DLEP) initiative [20]. Table E-1 suggests many more information elements for the IEI-M interface than what the current version of DLEP supports. We expect that future military networks for the tactical edge must be tailored for different operations. That means also choosing proper routing metrics and configuration for the operation. For the flat architecture we will then see a need for more information being made available from the lower layer of the radio to the router. Extensions of DLEP can specify a wider range of information elements for this interface. There are vendor specific implementations of the IEI-R (the route redistribute function). As pointed out in Ref. [21], there are no standards describing this interface.

Table E-1: Overview of Possible Information that Could be Exchanged via Information Exchange Interfaces.

Router-Modem IEI-M Interface	Interconnected-Flat IEI-R	Interconnected-Overlay IEI-RO
Link/channel characteristics: • Signal-to-Noise Ratio (SNR) • Channel Idle Time Ratio (CITR) • Round Trip Time (RTT) • Link capacity b/s (maximum/available) • Tx Power (maximum/current)	Topology information: • Forwarding table • Forwarding table w/metric • Full topology database	Topology information: • Forwarding table • Forwarding table w/metric • Full topology database
Radio capabilities: • Automatic Repeat Request (ARQ) support	Protocol information: • Reactive/Proactive	Topology information: • Reactive/Proactive

Router-Modem IEI-M Interface	Interconnected-Flat IEI-R	Interconnected-Overlay IEI-RO
Radio capabilities (cont'd): - Type of Medium Access Control (MAC) - Half duplex / full duplex - Antenna type (beamforming, omnidirectional) - Capacity for network control signalling - QoS classes	Protocol information: (cont'd): - Metric type: - Additive/concave /multiplicative - Hop count / minimum cost - Directional Airtime Metric (DAT) - Etc.	Topology information: (cont'd): - Metric type: - Additive/concave/ multiplicative - Hop count / minimum cost - Directional Airtime Metric (DAT) - Etc.
Current configuration: - Frequency band - Bandwidth	Policy information Transit traffic yes/no	Policy information to/from overlay - To: - Capacity for external network control signaling - Transit traffic yes/no - From: - Route prioritization
List of layer-two neighbors		
Queue size / occupancy		

In the following sections, the use of different information elements as well as protocols/functions to carry the information is discussed for each IEI.

E.4.4.1 IEI-M Interface

The IEI-M interface allows the router to collect information from the modem or to send configuration commands to the modem. The need to send commands from the router to the modem relates more to cognitive networking and is out of scope for this document. The former provides predominantly real time information for local use by the routing protocol of the network segment and can be used by the router for the following purposes:

- Collect link measurements and statistics as well as traffic load and buffer sizes for the router to turn into routing metrics used in path selection and to control the traffic flow between the router and the modem.
- Properly configuring the routing protocol configuration parameters such that the routing protocol stays aware of all changes in the topology while protecting low capacity links from signaling congestion.
- To inform the router of which topology information is already collected by the modem.

For a), routing decisions, several parameters that give insight in the radio link quality can be relevant (e.g., SNR, link speed, CTR, latency, BER). On the routing layer, only one metric at a time can be used per topology. Different metrics can be used for different topologies and it might therefore be interesting to also change the metric during an operation. In the literature, different proposals for modem-dependent metrics

can be found. An example metric is the Directional Airtime Metric (DAT) [22], which is calculated from the link speed and the expected transmission count of the link. The link speed information is obtained from the transmission technology via an IEI-M interface. The expected transmission count can be obtained by counting signaling messages of the routing protocol. Another solution is to acquire this information from the transmission technology (i.e., modem) that can for instance count the retransmissions on layer-two. Another example is to inform higher layers of the CITR for QoS routing and admission control [23]. Deciding which radio parameters are the most suitable and which routing metrics are most useful for mobile ad hoc networks is a contemporary research topic.

Some flow control or other means should be available for the interface to avoid buffer overflow of the modem's sender queue. It might also be beneficial for the router to know how large the modem's buffer is. If the buffer is large then traffic shaping and priorities made at the routing layer will have little effect, and the radio might transmit many 'garbage' routing packets. This happens in situations when a topology change happens and the routing protocol updates its routes; the modem might have many packets stored in its queue with the old next hop address. These garbage packets will waste channel capacity until the sender queue is flushed of the packets with out-of-date next hop information.

For b), configuring the routing protocol configuration parameters, the router should be aware of the capabilities and characteristics of the radio technology in terms of frequency of topology changes and available capacity. If the capacity is low (e.g., VHF link), the amount of control traffic sent over the link should be minimized (e.g., lower than a threshold link capacity). If the topology is very dynamic, the signaling rate should be frequent enough to keep the topology view up to date. Note that such decisions in state-of-the-art are usually done statically. In future scenarios they may be automated.

For c), sharing radio topology information (destination up/down) collected by the modem with the router layer, serves to reduce the network control overhead. If the transmission technology already collects information on for example its 1-hop neighbors, it is not necessary for the routing protocol to send additional network control traffic to obtain the same information.

In current practices, many of the b) and c) aspects are statically configured before the mission, since such configurations are not automated. In the future, however, this may change. For the shorter term this essentially leaves a) to be supported by the IEI-M interface.

E.4.4.1.1 Protocols/Functions to Carry the Information of the IEI-M

The information elements of the IEI-M must be able to flow from the modem to the routing function and sometime also the other way around. This can happen in two different ways depending on the placement of the producer and the consumer:

- 1) **Box-Internal:** On a device-internal interface for information exchange between a modem function and a routing protocol function on the same physical device.
- 2) **Box-External:** On a point-to-point connection between two separate boxes; a modem and an external tactical router on the same interconnection platform.

For 1) (see Figure E-9), a standardized set of functions and a repository must be made available internal to a device, for the routing protocol and the modem to share relevant IEI-M information elements. Many radio vendors have defined this type of interface for own internal use, but it is usually not made available for an external routing protocol to use.

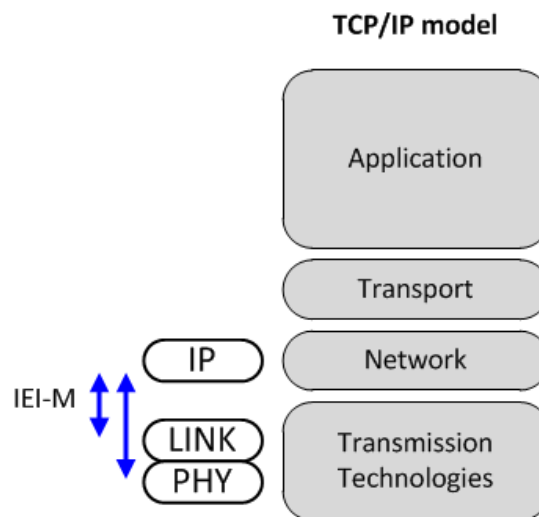


Figure E-9: An Interconnection Platform that Uses an Internal IEI-M.
In this case the IEI-M will be a set of functions that provide the IP layer with information from lower layers.

For 2) (see Figure E-10) a protocol must be specified that can transport the information elements of the IEI-M over a point-to-point connection between the modem and a router. Several protocols exist, the most relevant is the Dynamic Link Exchange protocol (DLEP), another one is PPPoE extensions for Credit Flow and Link Metrics [24]. The latter approach introduces tunnels over the air and is therefore considered to be less suitable for bandwidth constraint wireless environments than DLEP [25]. None of these protocols are currently able to transport all information elements of Table E-1.

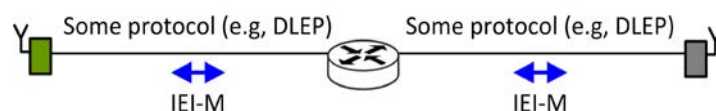


Figure E-10: An Interconnection Platform that Uses Some Point-to-Point Protocol to Carry the IEI-M Information Between a Routing Function Residing in One Device and the Transmission Technology Modem Residing in Another Device.

Note: As for the internal IEI-M, it is information from the lower layer of the radio that is carried by the protocol to be consumed by the routing function on the IP layer.

E.4.4.2 Interconnect-Flat IEI-R and Interconnect-Overlay IEI-RO

The IEI-R and IEI-RO interfaces are quite different in nature from the IEI-M interface. The IEI-R and IEI-RO should mostly provide real time network reachability information that must be redistributed by another routing protocol. The information might propagate a long distance and should be marked with metadata describing how long the information can be expected to be valid. The validity information is more important for sharing of QoS and resource management information elements than for the routing specific information listed above, but also for routing, validity information should be bundled with the topology information in order to share with the whole network the expected accuracy of the routing information. Another information element that should be supplied with the topology information is an identifier of the originator network for the information. This is important in order to avoid routing loops. Both the validity and originator metadata place requirements on the different routing protocols to be able to carry this metadata with the information as it is redistributed in the network. For this section we focus on identifying the important elements to flow over the IEI-R and IEI-RO.

The two IEs are similar in many ways thus in a standardization effort, one option can be to standardize a single IE that supports the characteristics of both interfaces. Some differences between the interfaces are:

- The IE-RO interface should provide a wider range of network policy information – for instance information from a network segment of maximum capacity that can be used for overlay signaling – in order to assure efficient operation of the overlay routing protocol.
- The IE-R must be bidirectional, whereas the IE-RO can be a one-way interface or support asymmetric bidirectional information flow.

We opt to describe the interfaces one by one in the following.

E.4.4.2.1 Interconnect-Flat IE-R

The information exchange interface between two peer routing protocol domains serves the purpose of sharing routing information where network segments from different routing protocol domains interconnect. Such a scenario occurs for example when two nations want to form a coalition tactical IP network at the platoon or team level, but the nations use dissimilar tactical routing protocols. Another example is when the heterogeneous network consists of layer-three radios that belong to separate routing protocol domains. The information that is exchanged between two routers can serve the following purposes:

- a) Exchange routing information to enable end-to-end path selection. Bundled with the routing information may also be additional metadata such as information validity and originator identifier to prevent routing loops.
- b) Exchange protocol information such as the type of routing protocol (e.g., MANET or not, reactive or proactive) and type of metric used.

For a), this includes sharing topology information between two routing protocol domains with different levels of details:

- 1) The most basic element is to share only the network prefix of the whole routing protocol domain. This can also be done with static configuration in adjacent routing protocol domains.
- 2) Periodically sharing plain connectivity information from the forwarding table. This is a more elaborate element type. Sharing this information informs that a network segment can be reached via a certain interface, but does not give any information about the cost of the route.
- 3) If the cost (with metric information) is shared with the forwarding table, then it is possible to make better end-to-end routing decisions (given that similar metrics are used by the different routing protocols).
- 4) If full topology information is shared, then there can be full flexibility in the end-to-end routing decisions, but this is not likely to be implemented as it is not a scalable solution.

For the three latter element types, it will be possible to discover that a routing protocol domain is partitioned and establishes routes via other network segments if available. If, on the other hand, only the network prefix of the whole routing protocol domain is shared and not the individual routes to the different mobile nodes, then adjacent network segments will not be able to discover a network partition of the routing protocol domain and cannot take any actions to avoid, or help mending the partition. Thus the IE-R should be prepared to share full forwarding information and leave it to the routing architecture and the routing protocols to decide how much information to share in order to keep the network control traffic below a given threshold.

For b), type of protocol and other capabilities, the exchanged information provides the other router with an indication of what kind of information it can exchange and what not. For example, if router A runs a distance vector routing protocol and router B a link state protocol, the information they can share will be different. Information about the routing metric can also be shared.

E.4.4.2.2 Protocols/Functions to Carry the Information of the IEI-R

The information elements of the IEI-R must be able to flow between every two adjacent routing protocol domains. As for the IEI-M, this can happen in two different ways depending on the placement of the routing function:

- 1) On a device-internal interface for information exchange between different routing protocol domains on the same physical device (e.g., via the Forwarding Information Base (FIB) in the router with appropriate filtering rules).
- 2) On a point-to-point connection between two separate boxes; two different routers on the same interconnection platform.

For 1) a standardized set of functions and a repository must be made available internal to a device, to access the relevant information elements of the different routing protocol domains. An example of this interface is the vendor specific “route redistribution” function that many router vendors provide. Route redistribution allows one routing protocol to learn routes from another routing protocol running on another interface on the same device. See Ref. [21] for more insight. Figure E-11 shows a situation where the routing protocol domains on two different transmission technology domains share topology information via an internal IEI-R. The Draft STANAG 5634 “Internet protocol interface to half-duplex radio networks” is an ongoing NATO standardization activity that specifies access to IP-based half-duplex radios, and is geared towards communication between a router and layer-three radio. This STANAG currently assumes an internal IEI-R for route redistribution.

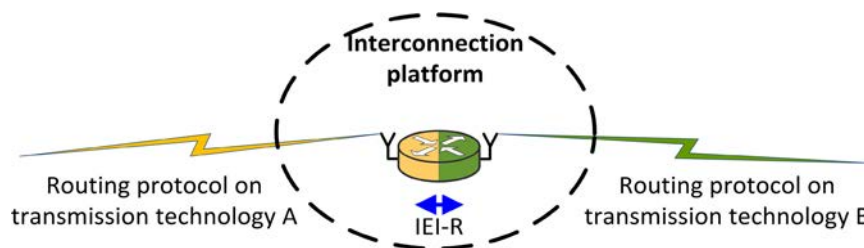


Figure E-11: An Interconnection Platform that Uses an Internal IEI-R.

For 2) (see Figure E-12) a protocol must be specified that can transport the information elements of the IEI-R over a point-to-point connection between two separate boxes running different routing protocol domains. The military jargon “putting radios back to back” describes a similar approach. To our knowledge there is no standard protocol for this interface. Possible options could be to make an extension for the Internet Control Message Protocol (ICMP) or to come up with a new protocol to transport the information of the IEI-R or using a local Data Distribution Service (DDS). If the interconnect-flat architecture becomes prevalent, a protocol to provide this interface should be defined.

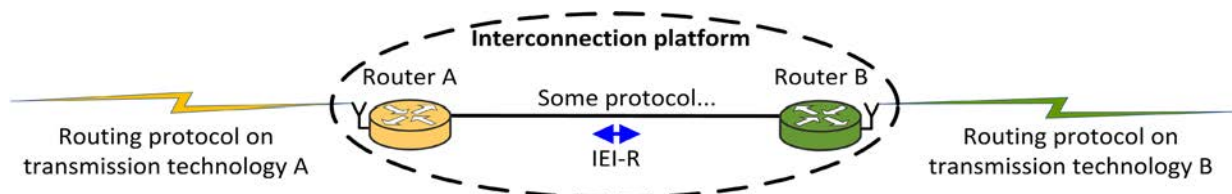


Figure E-12: An Interconnection Platform that Uses Some Point-to-Point Protocol to Carry the IEI-R Information Between the Routing Protocol Domains on Two Different Transmission Technology Domains on Two Different Devices.

E.4.4.3 Interconnect-Overlay IEI-RO

The information exchange interface between a routing protocol domain of a network segment and the overlay routing domain serves much of the same purpose as the IEI-R, but for the interconnect-overlay architecture. The scenario is the same; the need to connect different nation's routing protocol domains, and/or routers from different vendors that form separate routing protocol domains. The information that is exchanged between the network segments and the overlay can serve the following purposes:

- Exchange routing information to enable optimal end-to-end path selection. Bundled with the routing information should also be additional metadata such as information validity and originator identifier to prevent routing loops.
- Exchange protocol information such as type of routing protocol (e.g., MANET or not, reactive or proactive) and type of metric used.
- Exchange network policy related information (e.g., Capacity available for external network control traffic and transit traffic allowed).

For a) the situation is the same as for the IEI-R interface. The difference is that for the IEI-R, routing information must flow both ways, for the IEI-RO it is most important that detailed routing information is made available from the network segments to the overlay, detailed routing information from the overlay to the different network segments is only necessary for advance end-to-end routing such as different types of QoS routing. When the routing information is not shared both ways, the routers on interconnection platforms that implement the IEI-RO interface must be configured as default gateways.

For b) the purpose of the information elements is also the same as for IEI-R.

For c), sharing policy information between the network segments and the overlay helps the routing protocol in the overlay to tailor its behavior to suit the network policy, e.g., include or exclude specific network segments in the route calculation depending on whether transit traffic is allowed or not. Information about capacity available for external network signaling also helps the overlay protocol tailor its behavior. For information from the overlay to the network segments, it can be beneficial to ask the network segments for specific treatment of the overlay paths.

E.4.4.3.1 Protocols/Functions to Carry the Information of the IEI-RO

The information elements of the IEI-RO must be able to flow between every routing protocol domain and the overlay routing protocol domain (Figure E-13).

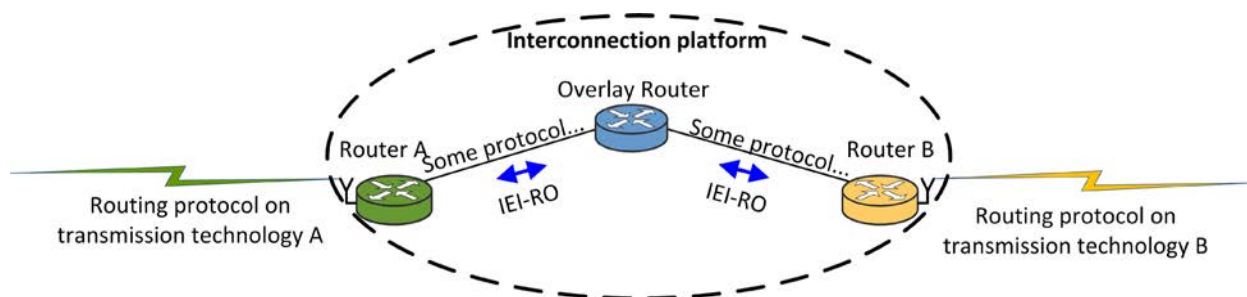


Figure E-13: An Interconnection Platform that Uses Some Point-to-Point Protocol to Carry the IEI-RO Information Between the Overlay Routing Protocol Domain and Routing Protocol Domains of Two Different Transmission Technology Domains on Separate Devices.

As for the IEI-R this can happen in two different ways depending on the placement of the routing functions:

- 1) On a device-internal interface for information exchange between a routing protocol domain of a network segment and the overlay routing protocol domain on the same device.
- 2) On a point-to-point connection between two different boxes; the router running in the overlay routing protocol domain and a router participating in the routing protocol domain of a network segment on the same interconnection platform.

For 1) this can be supported in the same manner as for IEI-R.

For 2) this can be supported in the same manner as for IEI-R.

E.4.4.4 Design Considerations for Information Exchange

The scope of the IEI-M information exchange is very limited, since the information always only flows between two adjacent devices, namely the router and the modem. For the IEI-R and IEI-RO this is different. If tactical IP networks increase in size, the size of some information types may become large, introducing additional signaling traffic in the network. The size of other information types does not depend on the network size. A topology database is good example of information that may greatly increase when networks become larger, since it sends all knowledge of the entire network. A forwarding table increases with the size of the network since more destinations can be reached, but not as much as the topology database, since it only shows active forwarding rules. Information on capabilities very likely does not depend much on the size of the network.

E.4.5 Addressing Considerations for the Routing Architectures

Connecting separate administrative domains and sharing information between national networks over the defined IEIs, has implications for the IP addressing that is used for the routing architectures:

- It must be possible to uniquely identify a host that resides in another routing domain.
- A host must be able to set a destination IP address in its packets to ensure the destination is reached.
- IP address spaces in different routing domains must be deconflicted to ensure proper end-to-end connectivity.

The architecturally best way would be to make a common address plan and prevent the use of overlapping address spaces in different routing domains. This means that the national IP address ranges used by network segments that participate in the common coalition heterogeneous mobile network must be internationally agreed upon. When using IPv6, this can easily be done if nations use the address space that has been formally assigned to them from their provider or Local Internet Registry, or if Unique Local Addresses (ULAs) are used [26]. Other possibilities are to use a common coalition address space for IPv4 or a NATO space for IPv6. For these two cases, structured IP addresses built on the country codes maintained by the NATO Codification Bureaux (NCB) is one example solution [27]. If IPv4 private address space is used in a distributed unsynchronized manner, there is a high likelihood of address collisions between networks.

Another alternative may be to introduce Network Address Translation (NAT) at the IEIs between routing protocols. However, when NAT is used, IP addresses can no longer be used to uniquely identify hosts in the tactical network, which may break the possibility of end-to-end communications within the tactical network. In addition, in a mobile mesh topology, the hierarchy between different network domains may change over time: whether a network segment is behind or in front of the NAT relative to other network segments can be ambivalent and differ based on the actual topology. Introducing a more strict hierarchy in the network would be required, for example following a tree topology, but it limits the dynamics of the network in the sense that generic connectivity will be lower. Especially, when more network segments are added, and routing domains

can be split during mobile operations, handling an addressing space that is tied via NAT is becoming increasingly complex and management-intensive. In general, it holds that a coalition IP addressing plan must be in place in order to build a coalition heterogeneous network at the tactical edge. A common address range without NATs is necessary for the architectures presented here.

In Internetworks, IP addresses are often assigned in a hierarchical manner which enables the use of route aggregation in router advertisements. This saves router memory and reduces the network control overhead since a network prefix can be stored and signaled instead of a list of routes to single destinations in the network. Such an approach works well in stub or tree topologies. When MANETs are included and there are meshed connections between network segments that do not have the same parent network (IP address assignment), this will lead to an increase in routing entries that need to be stored and shared. The increase in routing entries is also driven by node mobility: if nodes attach to other branches of the tree (or mesh) and keep their IP address this also requires additional specific routes. Defining a coalition approach to IP addressing for the tactical edge is out of scope of the IST-124 study but should be taken into account when defining international network interoperability on the mobile tactical edge.

E.4.6 Network Policies for Governance of the Routing Architecture

We envision that network planning will become an increasingly important part of mission planning. A set of network policies that describe the desired behavior of the network, must be defined. The network policies can include many different targets such as frequency planning, choosing network profiles, traffic shaping and prioritization, setting up filters for traffic types, setting security levels, etc. Currently the processes of identifying the desired network behavior, setting the network policies and deducting the rules and management configuration needed are, to a large extent, manual procedures. The field of network management and control is in rapid change with the introduction of SDN, NFV and new management frameworks (e.g., Open Network Automation Platform (ONAP) [28]). It is likely that the future will bring a situation where much of today's manual processes will be taken over by automated processes that configure the network based on the operation plan and collected information about the operation environment.

Independent of the procedure for obtaining the desired network behavior, the network elements must provide mechanisms that allow the management system to implement the chosen desired behavior of the network. As the networks become more flexible it is possible to provide more configuration choices to the network planners. In IST-124 we believe that one approach that can lead to better performance of the future heterogeneous network is to make more architecture choices available to the network planners. It is very difficult to come up with network architecture and routing design that has good performance for all scenarios. There are always compromises in the design. One compromise may suit one scenario whereas a different compromise should be made for a different scenario. As we move towards a situation where much of the network planning will be done by a machine, we should give the network planning algorithm as many configuration choices as possible together with a description of the tradeoff in network performance that must be considered for each choice of configuration. It can also be beneficial to be able to change the network behavior in real time during an operation and to control this with (pre-programmed) network policies.

The choice and configuration of routing architecture for an operation are one element that can help govern how the network resources can be utilized for a specific mission. In Section E.5 we show the many tradeoffs for the various architectures and that varying configurations give different network optimizations. In most cases different design and configuration choices do not completely change the character of the network. It can rather be thought of as a lever that is being dragged towards one or the other of two conflicting optimizations. The tradeoffs are not either/or policies but represent a need to improve the performance of one characteristic or requirement which will often come at the cost of reduced performance of the other. Ideally, we want to build a network that is flexible, robust, stable, secure, with high capacity and low network control overhead, and that is efficient both for local traffic and end-to-end traffic, with low delay and complexity.

It is not possible to optimize for all of these characteristics at the same time. In some situations, flexibility might be more important than capacity whereas in other situations network stability and robustness is most important. With a toolbox of design choices, mechanisms and a set of policies that describe the desired network characteristics for an operation, a network can be tailored to the operation.

We strongly believe that the future will show a need for much more detailed policy control of the mission's tactical edge networks in order to optimize the performance for the specific operation. In this annex we point out some choices for routing architectures and some tradeoffs that can be set differently for different operation with policy decisions.

E.5 ROUTING ARCHITECTURES – DETAILED DESCRIPTION AND DISCUSSION

In this section we will introduce and discuss in more detail the individual routing architectures. The architectures are described using two companies of the Anglova scenario (see Annex B) as an example. We explain the expected characteristics and major tradeoffs for the different architectures in the light of the requirements that were presented in Section E.2. Some of these characteristics are well known and studied in detail whereas others are expert opinions by the group members and need to be studied in more detail with simulation, emulation or field test experiments. The purpose is to provide a better understanding of the important factors to consider when choosing the routing architecture for a heterogeneous tactical network.

E.5.1 Symbols and Performance Parameters

For this section we use the symbols defined in Section E.4.1.

For all military platforms we assume a local network architecture like the one in Figure E-14. All devices and sensors on the platform are connected to the platform LAN⁴. Some routing functionality (in the figure the flat routing architecture is used as an example) decides which network (transmission technology) to forward traffic on. That is, the green transmission technology, the grey transmission technology or the LAN. Security including authentication, integrity, and confidentiality both for end user traffic and for network protection must be in place and can be solved in many different ways. See the IST-124's Security architecture for more information about this [16]. The functional aspects of the routing architectures will be introduced and discussed first. In Section E.7 we discuss the implications of the security architecture on the different routing architectures.

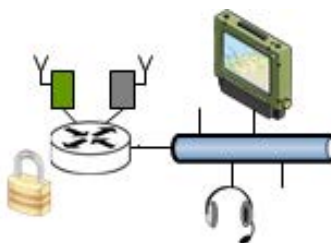


Figure E-14: Assumed Military Platform Architecture.

E.5.1.1 Performance Parameters

For readability the requirement categories of Section E.2 are summarized in Table E-2.

⁴ Note that the platform LAN may include wireless components as well (e.g., WLAN).

Table E-2: Requirements to Heterogeneous Tactical Networks.

Requirement	Goal	Technical Characteristics
Heterogeneous Networking Routing	Ensure that connectivity between nodes is arranged between all users that want to exchange information.	• Connectivity • Radio silence¹
Robustness	Ensure that the availability of the network for the users is as high as possible, and that disruptions in communications streams and data exchange between users are prevented.	• Detect link break and find new route • Multiple paths • Network stability and vulnerability • Cyber resiliency
Scalability	Make sure that large numbers of military platforms can successfully exchange information via the heterogeneous network.	• Overhead from network control traffic • Tailoring of the network control traffic • Overhead from suboptimal paths
Resource Efficiency and QoS	Maximize the user data that can be exchanged between users via the heterogeneous network given a certain time span, and to provide QoS.	• QoS routing² • Providing multiple paths • Network policies
Configuration and Management	Minimize the effort needed to configure and maintain the network and reduce the need for human intervention in the network to ensure correct operations in different and changing circumstances.	• Protocol and configuration complexity • Remote management
Ease of Deployment	Consider deployment challenges in order to assess how easy it is to realize the architecture design with state-of-the-art military communications equipment.	• Ease of deployment, both nationally as well as in coalition settings
1) With this parameter we judge the routing algorithm's performance when some nodes go into radio silence. If the routing algorithm support radio silence we expect that the nodes going into radio silence signal this before stopping transmission and that the rest of the network should continue forwarding traffic to the nodes in radio silence, even though the routes cannot be maintained.		
2) Note that QoS mechanisms other than QoS routing are comparable in their challenges regardless of the chosen architecture. Also, bear in mind that QoS has to be arranged at the transmission level, in addition to the network layer (see Annex I for more on QoS).		

E.5.2 Flat Architecture

Figure E-15 shows a situation where flat routing is used in both companies to form one routing protocol domain. This means that a single routing protocol is running over all three transmission technologies deployed in the example. The routing function can use the IEI-M interface to communicate with the transmission technology in order to learn about link quality, data-rate, and the similar. In Section E.4.4 we suggest a list of information elements to share over IEI-M and discuss some of these. The flat architecture is reported on in

Refs. [29], [30] and [31]. For most of the transmission technologies it is assumed that a common channel is utilized for each radio type, thus providing an efficient broadcast medium (internal to each transmission technology), but satellite connections and other point-to-point connections might also be present. In order for the routing information to be shared over the different transmission technologies, there must be interconnection platform(s) where two or more transmission technologies are physically connected via one or several routers. Four such interconnection platforms are available in each company in Figure E-15. In the figure three different transmission technologies are deployed. All devices participate in the same routing protocol domain. The figure depicts eight interconnected platforms, which carry two transmission technologies.

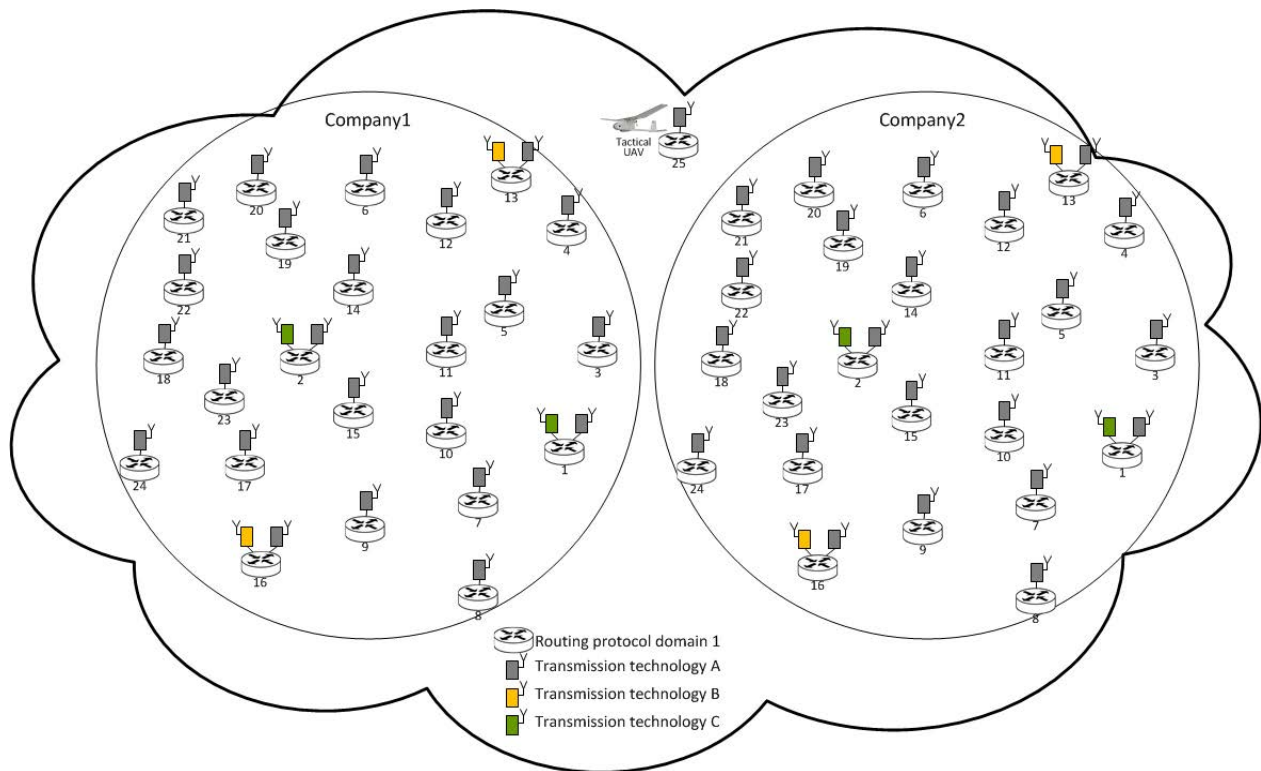


Figure E-15: Flat Routing Architecture: A Situation Where Flat Routing is Used Internally in a Network Composed of Two Companies.

In the following the main characteristics and tradeoffs of this architecture are explained in the context of the requirements given in Section E.2.

E.5.2.1 Heterogeneous Network Routing

E.5.2.1.1 Connectivity

Information about all possible links across all available transmission technologies can be made available for the routing function in this architecture, thus this architecture allows for very good connectivity, since it by nature converges to a full mesh as much as possible. A route should be found if a connection via any order of links from the different transmission technologies exists.

The time required from a route is requested until it is found, depends on the protocol design and protocol timers (short for proactive routing and longer for reactive routing). However, since we here use a single protocol, there is no additional time introduced for translation and redistribution of signaling information over routing protocol information exchange interfaces (IEI-R or IEI-RO).

E.5.2.1.2 Radio Silence

To which effect the network can support radio silence depends on the installed protocol. For the flat architecture to support radio silence for specific transmission technologies, it requires extra complexity in the routing protocol to identify and keep track of the network control traffic over a specific transmission technology. This is advanced routing functionality that increases the complexity of the protocols.

E.5.2.2 Robustness

E.5.2.2.1 Detect Link Break and Find New Route

The connectivity in this architecture is as good as the physical topology allows. Thus, it is able to respond quickly to reroute traffic to bypass a link failure or to avoid transmission technologies that for instance are experiencing jamming attacks. The routing protocol will eventually detect all relevant link breaks and repair the routes if a connection across any transmission technology exists. Since we run one common routing protocol in the whole network, the time needed to detect and repair the route can be quite short.

E.5.2.2.2 Multiple Paths

For added robustness the availability of multiple paths allows for quicker rerouting times after link breaks as well as providing parallel paths over which redundant copies of the information can be sent. For this architecture with a single routing protocol, multiple paths can easily be supported in the entire tactical network by choosing to use a routing protocol that supports this.

E.5.2.2.3 Network Stability and Vulnerability

Network stability for a large flat network can be a concern. When a transmission technology experiences frequent disruptions due to topology changes, or a network segment with configuration error / malicious node produces erroneous network control traffic, this instability will typically be flooded in the whole network and reduce the overall stability for the network.

E.5.2.2.4 Cyber Resiliency

A focused cyber-attack on a vulnerable remote part of the network can succeed in degrading the whole network. A common protocol in the whole network allows the attacker to focus on methods to efficiently attack only one protocol in order to disrupt the enemy's network service. On the other hand, monitoring and detection of cyber threats as well as reacting to cyber threats may be easier with a common flat routing domain.

E.5.2.3 Scalability

E.5.2.3.1 Overhead from Network Control Traffic

Part of the overhead is network control traffic. The heterogeneous network can consist of a large number of nodes. For the flat architecture, the signaling overhead will be large. For proactive routing schemes the link information should flow between all nodes with a high enough frequency to keep track of the topology changes induced by the transmission technology that experience the highest rate of link breaks. A heterogeneous network can also hold low data-rate narrow band transmission technologies. These cannot sustain the same amount of signaling traffic that is needed to support routing over a transmission technology that experiences much topology changes (e.g., a wideband transmission technology). If the same amount of network control traffic is distributed in the whole network, the presence of narrow band transmission technologies will typically limit the network size to a very small number. Our experiment with OLSRv2 used on a medium band (250 kHz, 175 kbps) transmission technology in the Anglova scenario shows that for a

configuration with Multi-Point Relay (MPR) plugin, this scales to a network of a few tenths of nodes when frequent network control messages are utilized (see Ref. [32] for more information). A reactive routing protocol in a flat architecture has similar scalability concerns. Routing techniques such as hierarchical routing e.g., Ref. [33], or fisheye routing [34] can improve the scalability. A common effect of all techniques to reduce the overhead is that some characteristics of the network will suffer to give lower connectivity and/or robustness and/or resource efficiency, and/or reduced flexibility.

E.5.2.3.2 Tailoring of Network Control Traffic

The flat architecture is likely to cause reduced throughput in some transmission technologies. Most state-of-the-art military radios today include a proprietary routing protocol that is tuned for best performance of the network. Particularly low data-rate transmission technologies need close collaboration between the routing protocol and the lower layers of the transmission technology to achieve optimal throughput. When one common routing protocol is used over many different transmission technologies, it is not possible to tailor the protocol for optimal performance within each technology. This can be mitigated somewhat when real time information from the transmission technology is made available to the routing layer via the IEI-M interface. This can be used to configure the protocol slightly different for different transmission technologies, or to aid the protocol metric. All tailoring of the common protocol will increase the configuring complexity and increase the risk of protocol instability or loops [35]. No mature protocols exist that use the information over the IEI-M to configure the protocol differently for dissimilar transmission technologies.

E.5.2.3.3 Overhead from Suboptimal Paths

Another share of the overhead comes from an extra number of transmissions due to suboptimal paths or due to retransmissions over bad links. For the flat network architecture, it will often be possible to find the best path (according to the chosen metric), and the overhead due to suboptimal routing paths is therefore negligible. Regarding retransmissions over bad links, it is the routing protocol that must try to avoid the bad links thus this performance is independent of the chosen routing architecture. However, the flat architecture gives the routing protocol the highest number of link choices in order to find the best links.

E.5.2.4 Resource Efficiency and QoS

E.5.2.4.1 QoS Routing

The flat routing architecture knows all links in the network. Given that the IEI-M interface is available this architecture can easily support QoS routing as long as a routing protocol with the wanted QoS functionality is provided. In Ref. [31] OLSRv2 with the airtime metric is used for some QoS functionality in heterogeneous networks.

E.5.2.4.2 Providing Multiple Paths

Two different schemes for multiple paths between source and destination can be beneficial for resource efficiency and QoS:

- Equal cost paths (load balancing); and
- Link quality specific paths (differentiated characteristics).

If an IEI-M interface that provides information about the link characteristics is available, and a protocol that supports such functionality is installed, this requirement can easily be fulfilled. Only experimental protocols with such functionality exist (e.g., Multi-Topology routing [29]).

E.5.2.4.3 Network Policies

Network policies that involve the whole heterogeneous network can be supported well by the flat routing architecture. Supporting network policies that concern one or a few of the transmission technologies utilized in the heterogeneous network will increase the network control traffic and the complexity of the protocol. Such protocol does not exist today.

E.5.2.5 Configuration and Management

E.5.2.5.1 Protocol and Configuration Complexity

The flat architecture in its basic (non-optimized) form is easy to understand, easy to configure and requires detailed knowledge of only one single routing protocol and the process can easily be automated. There is no need for protocol information exchange interfaces (IEI-R/IEI-RO) between different protocol domains. However, an IEI-M interface will prove beneficial. On the other hand, it can be hard to find the optimal parameters for a network that consists of diverse transmission technologies. Also, as soon as the protocol needs to be tuned differently for different transmission technologies¹, the configuration of the protocol becomes more complicated. Nevertheless, the network manager only has to handle one protocol with one set of configuration options. Thus, the required education and risk of routing protocol misconfiguration is relatively low for this architecture.

Configuration of a common routing protocol across different coalition partners requires agreement on many parameters. A common routing protocol profile must be defined, and a common name space for configuration parameters must be agreed on. Here is a high risk for configuration errors that can lead to loss of the network service. On the other hand, when all nations use the same configuration, they can copy from each other and share best practices which reduce the chance of error.

It is easy to add new network segments to the common heterogeneous network on the fly when the chosen configuration such as profile and network name spaces for the operation is known.

E.5.2.5.2 Remote Management

Management of a flat architecture is easy since only one common routing protocol domain needs to be managed. It also simplifies traffic management and traffic engineering since it has fewer interfaces for these mechanisms to adhere to / utilize.

E.5.2.6 Ease of Deployment

The flat architecture requires that one common routing protocol must be agreed upon by the nations and used by all transmission technologies in the network. Most military radios do not allow the user to install new routing protocols on the radio. It is unrealistic to expect all vendors to include the same routing protocol in their radios but a standardized IEI-M interface (e.g., Ref. [20]) for radios that do not include routing, can be agreed on. For some transmission technologies (e.g., wideband technologies) it might also be realistic to get radio products that allow the user to bypass the internal routing if this is asked for by the customer. Such radios could include an IEI-M interface as well. If the vendor allows the customer to use the vendor specific routing protocol when desired, or using a common protocol on an external tactical router (bypassing the internal routing protocol) when desired, the radios can be used in a flat architecture for scenarios where this is beneficial and with optimized internal routing in an interconnect architecture for other scenarios. Also support for Software Defined Networking (SDN) in military radios can provide an interface for the customer to install country specific or coalition specific routing functionality in the future.

Rapid integration of an IEI-M interface requires a clear business case. Such driver should come from MoD requirements related to end-to-end information exchange capabilities and system and coalition

interoperability, when acquiring new tactical communications equipment. With respect to routing inside or outside the radio; radio vendors have generally invested a lot to get the most out of the available bandwidth for local communication. Different waveforms are needed for different purposes, and many vendors deliver radio-specific routing protocols accordingly. If the flat architecture is the target for achieving interoperability, this comes at the cost of a lower performance in terms of data throughput over the transmission technology. However, applying optimized radio-specific routing protocols can prevent the level of interoperability that can be achieved by applying the flat routing architecture. Currently, industry leans towards the radio-specific routing solutions. As long as this remains the case it will be very difficult to deploy a common routing protocol of choice on all transmission technology domains in both a national and a coalition heterogeneous networking environment.

Open standard and open source protocols exist to implement the flat routing architecture for a few metric-types.

E.5.2.7 Conclusion

This architecture can support many of the requirements if it is used either on a heterogeneous network where the different transmission technologies have similar characteristics (e.g., data-rate, and transmission delay), or on small networks where also narrow band transmission technologies can support the signaling overhead. It provides the best end-to-end connectivity for traffic crossing several transmission technology domains at the cost of reduced local network efficiency. This cost is higher for a heterogeneous network that incorporates transmission technologies with very different characteristics than for a more homogeneous network. In the latter case it is easier to tailor the protocol for good performance in the network. The architecture including the IEI-M interface is very flexible and futureproof. It allows for easy deployment of new functionality as soon as a routing protocol is available that provides the necessary functionality. Mature protocols that support much of the discussed functionality do not exist today. It remains to be seen if scalable advanced protocols will become available. It might be difficult to deploy this architecture on a large scale since it needs direct access to L2 in the radios or the common routing protocol of choice installed in L3 radios. If it is used on a large network, scalability and network stability can be a problem. This architecture is the best choice for quite homogeneous networks or fairly small networks of medium to high data-rate and where end-to-end traffic is prevalent.

E.5.3 Interconnect-Flat

The interconnect-flat architecture represents an architecture where different routing protocol domains are interconnected in a flat manner. Figure E-16 shows a situation where embedded routing protocols are used in the different transmission technology domains but one or more of the routing protocol domains in this architecture can also be a heterogeneous network running a flat routing protocol as described in the flat architecture (Section E.5.2). In that situation we have a hybrid architecture with elements from both the flat and the interconnect-flat architecture. In order for any routing information to flow between the different routing protocol domains in this situation, there must be interconnection platforms where two or more routing protocol domains are present and with routers with an IEI-R over which some information is shared between the protocols running in the different protocol domains. The military platforms represented with the dotted circles in Figure E-16 represent interconnection platforms. Each router color represents a routing protocol domain. For the Anglova scenario, the two grey routers are using the same transmission technology for two separate frequency bands.

In the following section, the main characteristics and tradeoffs of this architecture are explained in the context of the requirements given in Section E.2.

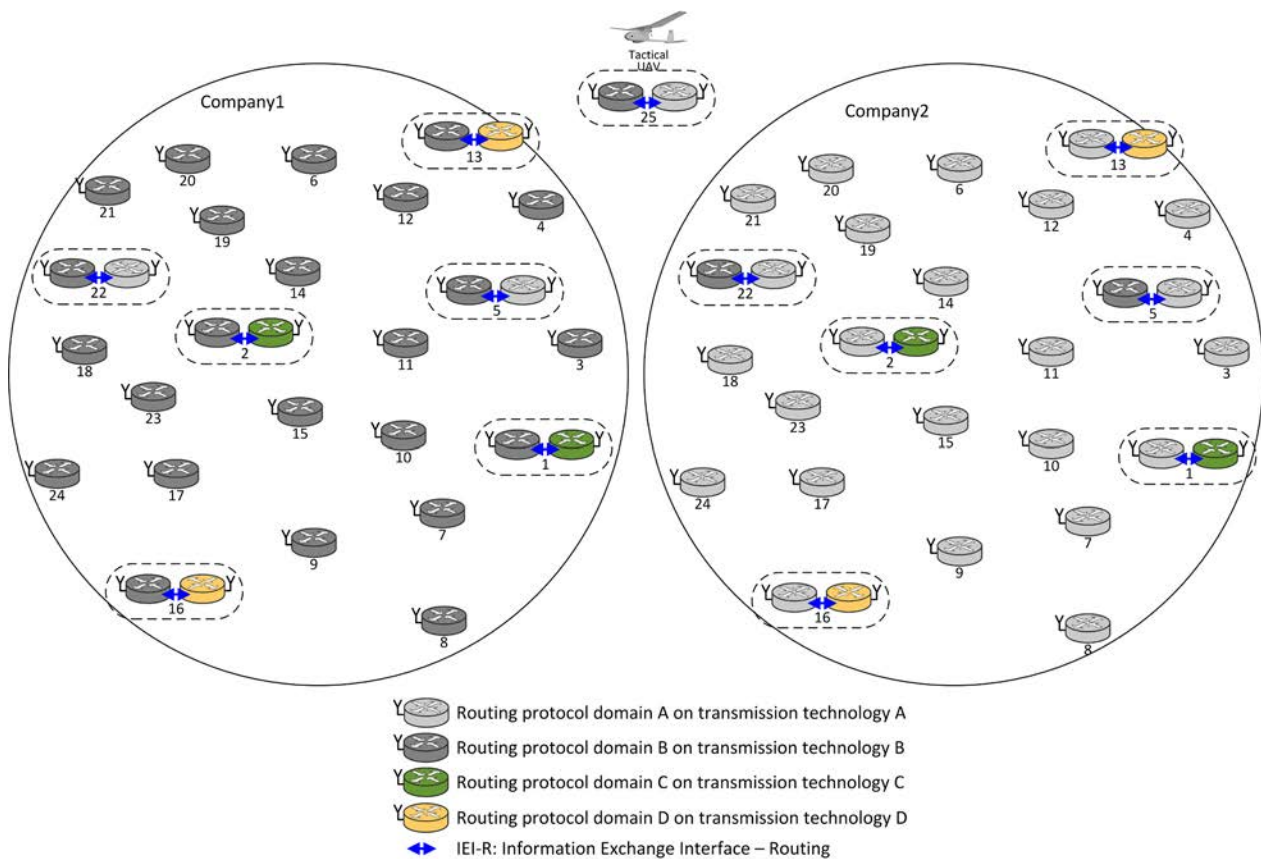


Figure E-16: A Situation with an Interconnect Architecture with Flat Protocol Interaction for the Two Companies.

E.5.3.1 Heterogeneous Network Routing

E.5.3.1.1 Connectivity

Connectivity internal to the different interconnected network segments is assumed to be very good for this architecture since either a tailored embedded protocol, or a well-designed flat architecture is assumed to be used in the different routing protocol domains. End-to-end connectivity on the other hand depends on information exchange over IEI-Rs between the routing protocol domains, and on the different routing protocols' ability to distribute the shared information in the routing protocol domain. In Section E.4.4 we suggest a list of information elements to share over IEI-R and discuss some of these. If the forwarding table or more detailed topology information is shared periodically, then end-to-end connectivity can be good. Only the manufacturer-specific route redistribution function exists for this information exchange today.

The time required from a route is requested, until it is found, depends on the protocol design and protocol timers. Most likely the route redistribution function operates at a lower frequency than internal signaling thus the time to find a route is likely to be longer than for a flat architecture.

It is very difficult to support end-to-end connectivity in a network that uses reactive and proactive protocols in different routing protocol domains of the heterogeneous network. This case has received very little attention of the research community.

E.5.3.1.2 Radio Silence

To which effect the network can support radio silence depends on the different routing protocol domains. If one routing protocol domain supports radio silence, that network segment will stop transmitting, however in order for other parts of the network to keep sending traffic to the domain in radio silence, the radio silence information must be signaled over the IEI-R and the other protocol domains must have support for continued transmission to the network domains in radio silence.

E.5.3.2 Robustness

E.5.3.2.1 Detect Link Break and Find New Route

It is assumed that route repair capabilities internal to the different transmission domains are good. For end-to-end paths (given IEI-R) the architecture can also respond to failures (e.g., partitioned network segment) by rerouting traffic via an adjacent routing protocol domain. Metric information must be shared over IEI-R in order for the architecture to do more advanced rerouting such as avoiding transmission technologies that are being jammed or that experience flaky connections for other reasons. This support over IEI-R does not exist today. The time it takes from the moment the trouble is being detected until the end-to-end route is repaired, depends on the redistribution and the frequency of information exchange between routing protocol domains.

E.5.3.2.2 Multiple Paths

For added robustness the availability of multiple paths allows quicker rerouting times after link breaks as well as providing parallel paths over which redundant copies of the information can be sent. For the interconnected-flat architecture it is difficult to support multiple paths since routing decisions are made internally in each routing protocol domain independent on the decision made in adjacent domains. Thus, it is difficult to force separate paths crossing several routing protocol domains.

E.5.3.2.3 Network Stability and Vulnerability

This architecture comes with a big risk of routing loops and suboptimal paths. Care must be taken to never advertise a network prefix back into the routing protocol from which it originally came. In a heterogeneous network with many interconnection platforms this is difficult to avoid. Methods to avoid loops with existing routers include route tagging, filtering, or modifying administrative distances. In Ref. [21], the problem is well described and a model is proposed that can help network designers to check if their configuration has a risk for routing loops. Today there is no standard that defines the IEI-R and the methods to avoid loops. Standardized mechanisms that are available in all affected protocols must be in place to be able to avoid misconfiguration.

Instability in one routing protocol domain will not spread in the heterogeneous network as quickly as for the flat architecture. How visible the instability of one routing protocol domain will be depends on the level of detail of the information that is shared over the IEI-R. When little information is shared, the instability will hardly be visible to other parts of the network. On the other hand it might be beneficial for the rest of the network to know that a certain routing protocol domain experiences instabilities in order to avoid routing via this domain. When much routing information is shared, the instability will propagate into neighboring routing protocol domains but with smaller volume and with a smaller pace than for the flat architecture. Information can also be stopped by filters in the IEI-R, to further strengthening the stability.

E.5.3.2.4 Cyber Resiliency

Attacks by adversaries to confuse one routing protocol domain will not severely degrade another routing protocol domain thus it is difficult to disrupt the service of the complete heterogeneous network with this architecture. On the other hand, monitoring and detection of cyber threats as well as reacting to cyber threats may be more complicated because of the separated domains.

E.5.3.3 Scalability

E.5.3.3.1 Overhead from Network Control Traffic

In this architecture it is assumed that the routing protocol that is used in the different routing protocol domains is optimized for the respective transmission technologies, thus the internal signaling overhead is as low as it can be for best performance. In addition to locally produced network control traffic there will also be network control traffic that comes from the other router protocol domains and is being shared over the IEI-R. This latter control traffic is difficult to optimize. This traffic can be substantial and is dependent on the number of interconnection platforms and on the details and update frequency of the information shared over the IEI-Rs. Sometimes the static network prefix information for the complete routing protocol domain is used instead of redistribution forwarding information to single nodes. This greatly reduces the overhead but also greatly reduces the connectivity. In this situation network partitions internally in the different routing protocol domains will not be visible to external networks and these cannot avoid these protocol domains, or help connecting the partitioned network. This means that the interconnect-flat architecture scales well with few interconnection platforms and redistribution of only network prefix information. Possible narrow band network segments will limit the network size to a small number.

To our knowledge, connecting different routing protocol domains that are running reactive protocols has not been studied in the literature yet, thus we will not speculate here on the overhead and performance for such design.

The overhead in this architecture is assumed to be lower (in most cases) than in the flat architecture however this should be studied further with different configuration parameters with simulation or emulation.

E.5.3.3.2 Tailoring of Network Control Traffic

It is likely that most routing protocol domains in this architecture correspond with the transmission technology domains. This means that a protocol that is tailored for the transmission technology can be used for optimal local performance. However, the routing protocol domain also has to carry network control traffic to distribute topology information learned over IEI-R. It is difficult to tailor this information since it might come from network segments with different characteristics (e.g., frequent topology changes).

E.5.3.3.3 Overhead from Suboptimal Paths

For traffic internal to the different routing protocol domains it is assumed that the best path (according to the chosen metric) can be found, thus the overhead due to suboptimal routing paths are negligible for this case. For end-to-end paths, it is expected that a good path can be found (given some topology sharing over IEI-R) but since each routing protocol domain makes local routing decisions and might not even use the same metric, the paths cannot be expected to be optimal. This leads to some overhead due to suboptimal paths.

E.5.3.4 Resource Efficiency and QoS

E.5.3.4.1 QoS Routing

In many cases this architecture will have many routing protocol domains with different protocols (some proprietary and some standard) and it will be difficult to find and agree on a common metric. In the unlikely situation that the different routing protocol domains use identical metrics, and metric information is shared over IEI-R, then specific QoS paths can be found.

E.5.3.4.2 Providing Multiple Paths

Two different schemes for multiple paths between source and destination can be beneficial for resource efficiency and QoS:

- Equal cost paths (load balancing); and
- Link quality specific paths (differentiated characteristics).

Providing multiple paths end-to-end requires support for this functionality by all routing protocol domains in the heterogeneous network, as well as metric information shared over the IEI-R, thus it is very unlikely that this can be supported throughout the tactical network.

E.5.3.4.3 Network Policies

Network policies that involve a single routing protocol domain can be supported well by the interconnect-flat architecture. For network policies that involve the whole network, all routing protocol domains must support functions to implement a common set of policies. Even if this can be done, it is not certain that this results in the expected end-to-end behavior since the different routing protocol domains make local decisions and nodes cannot control the complete end-to-end path.

E.5.3.5 Configuration and Management

E.5.3.5.1 Protocol and Configuration Complexity

This architecture is easy to understand. One by one, the different routing protocol domains are easy to configure, but the architecture requires expert knowledge of many different protocols. In addition, as soon as the different routing protocol domains start sharing and redistributing information over the IEI-Rs for end-to-end connectivity, care must be taken to avoid routing loops and to control the overhead from network control traffic. This requires expert knowledge and tight coordination between coalition partners participating in the heterogeneous network.

Configuration is needed when a new network segment (routing protocol domain) is added to the network.

E.5.3.5.2 Remote Management

Management of the interconnect-flat network is difficult. There are many different systems to manage and most likely different protocols to use for the management. It is also difficult to do traffic management and traffic engineering since each routing protocol domain (most likely) has its own interfaces for these mechanisms to adhere to.

E.5.3.6 Ease of Deployment

The information flow and the mechanisms to avoid routing loops in such configuration is vendor specific thus it will be very difficult to ensure a correct configuration in a heterogeneous network with equipment from many different vendors.

The interconnect-flat architecture is the one that is easiest to deploy in current military networks. It assumes that existing routing protocols internal to the different transmission technologies (L3 IP radio networks) can be used. It requires that an IEI-R is available for redistribution and it requires that mechanisms are available to avoid routing loops. If dynamic information over an IEI-R is not available, static routes can also be used. Common practice for most current military radios is that they only redistribute via the IEI-R, the network prefix of the wireless domain and do not expose detailed routes on the wireless interface to the wired interface. Some radios might not redistribute any information from the wireless domain but only share the network prefix of networks that can be reached via the wireless routing protocol domain (e.g., attached LANs).

Current practice of radio manufacturers is that they use one routing protocol on the wireless network and another on the wired interface with an internal IEI-R (the vendor specific route redistribution function), as shown in Figure E-17, this leads to a long chain of routing protocol domains and IEI-Rs for connectivity information to flow from the routing protocol for one transmission technology to another. As long as nonstandard routing protocols are used on the wireless interface, the redistribution must go via standard routing protocols that both routers (e.g., Router A and Router B in Figure E-17) support for interoperability. In the figure there is a need for three IEI-Rs on an interconnection platform to have a connected network that can support dynamic routing for the mesh topology approach. With the availability of an external IEI-R, the external router could be removed from Figure E-17.

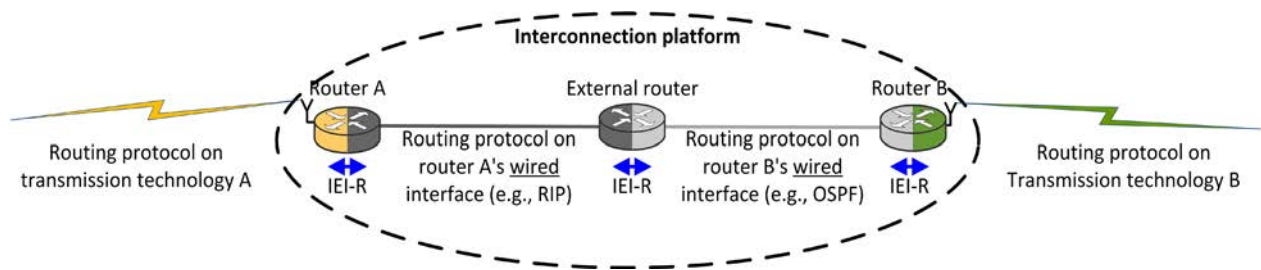


Figure E-17: An Example of the Chain of Different Routing Protocols that Might be Needed to Connect Two Different Military IP Radios with the Interconnect-Flat Architecture.

E.5.3.7 Conclusion

The interconnect-flat architecture is a well-known intranet architecture that is often used when several routing protocols are deployed in the intranet (e.g., university campus network). This can work well if only a few networks with few connection points are connected. If care is taken to avoid routing loops and only network prefix information is redistributed, then this is a scalable solution that supports end-to-end connections out of the box with many existing IP radios. This is a no-frills architecture that does not give much flexibility. If support for QoS, added robustness or other policy parameters are needed, or automated configuration is preferable, this is not the architecture of choice. As long as IEI-Rs and guidelines for how to avoid routing loops are not standardized, this is an architecture that is difficult to use in a coalition setting with equipment from many different vendors and multiple network administrators.

E.5.4 Interconnect-Overlay

Interconnect-overly represents an architecture where an extra routing protocol domain is installed in an overlay network where a subset of the nodes in the whole network participates. The purpose of the overlay is to connect the different network segments that make up the heterogeneous network. Figure E-18 shows an example with the two companies from the Anglova scenario. The overlay spans the whole heterogeneous network and connects the separate routing protocol domains. The overlay uses the different routing protocol domains to carry the traffic of the overlay links. BGP is a well know protocol that uses similar principles. For the remainder of this section we call the routing in the overlay network for the overlay routing protocol domain and the routing in the different network segments that make up the heterogeneous network for local routing protocol domains. The military platforms that are elected to be interconnection platforms must participate in the overlay network and must have the routing protocol of the overlay installed.

The overlay network has the following characteristics:

- It uses an extra layer of routing on top of the local routing protocol domains (that make up the heterogeneous network). The routing messages of the overlay routing protocol domain are sent

between the overlay nodes. This can be solved, e.g., with tunnels across the different local protocol domains, or by utilizing an end-to-end transport protocol.

- Each local routing protocol domain must have (or be reachable from) one or more router(s) that participate in the overlay.
- All routes traversing several local routing protocol domains must be routed via the overlay. The routing protocol internal to the local routing protocol domains only distributes internal topology information; there is no direct interaction between the routing protocols running in the different local domains.
- It is advantageous if there is an IEI-RO over which the overlay routing protocol domain can learn about the current network topology of the connected local routing protocol domain. In Table E-1 we suggest a list of information elements to share over IEI-RO and discuss some of these.
- Since the local routing protocol domains only have local topology information, an overlay link can never traverse several local routing protocol domains. The overlay links will then have the properties of the path in the local routing protocol domain.
- The chosen routing technique in the overlay will define the end-to-end characteristics of the heterogeneous network such as scalability/overhead, ability to do QoS routing and traffic management.

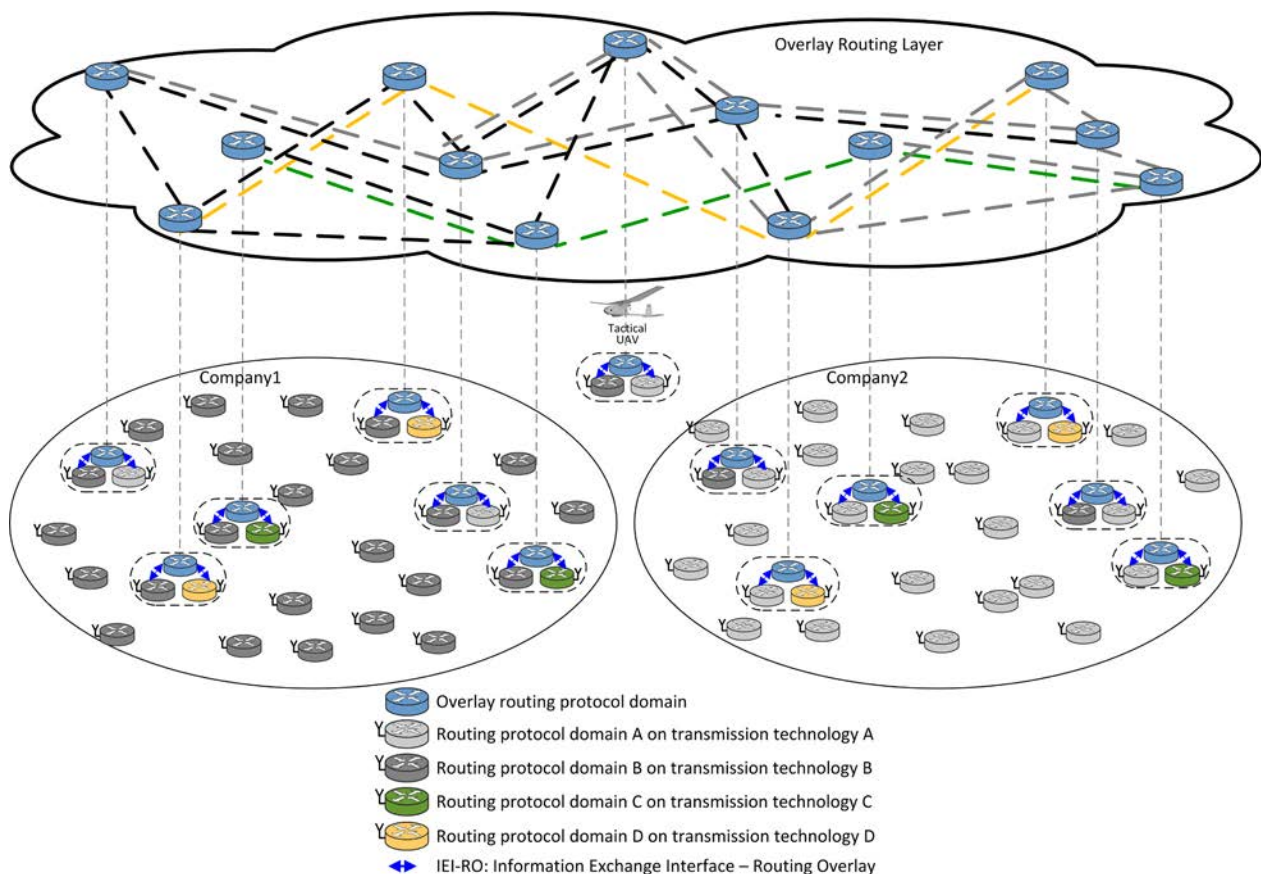


Figure E-18: A Heterogeneous Network Utilizing an Overlay Routing Protocol Domain to Provide Routes Across Several Local Routing Protocol Domains.

This architecture aims to provide much flexibility for the end-to-end routing function in the heterogeneous network. Depending on the number of overlay nodes, the number of overlay links, the level of information exchange between the local routing protocol domains and the overlay, and the type of protocol that is used in the overlay, it is possible to tune both the overhead and the functionality of the network to fit many different scenarios and requirements. This type of routing architecture running a reactive policy enabled protocol in the overlay is reported on in Ref. [36].

In order for the overlay routing protocol domain to be able to connect the different local domains, there must be interconnection platforms where two or more local routing protocol domains are present and where there is also an overlay route. The interconnection platforms are represented by the dotted circles in Figure E-18. One important design consideration in this type of architecture is the election of the overlay nodes. A simple design is to require that all military platforms that have more than one local routing protocol domain should participate in the overlay network. The color of the links in the overlay network shown in Figure E-18 indicates which local routing protocol domain that carries the overlay link in the example. Each local routing protocol domain can use one transmission technology or multiple transmission technologies as in the flat architecture. In the latter case the result is a hybrid architecture with both flat and interconnect-overlay properties.

E.5.4.1 Heterogeneous Network Routing

E.5.4.1.1 Connectivity

In this architecture the different local routing protocol domains maintains local routing only. All end-to-end routing is done by the overlay protocol. There must be one or more interconnection platform(s) that connects the local routing protocol domain to the overlay. Usually there are at least two interconnection platforms in each local routing protocol domain to allow the overlay to build a link over the local routing protocol domain to use for overlay signaling and transit traffic.

Connectivity internal to the local routing protocol domains is assumed to be very good for this architecture. The architecture also allows for good end-to-end connectivity. The different local routing protocol domains strive to find the best path for the overlay links (route the tunnels). The overlay finds the best path through the overlay to the destination local routing protocol domain. If the overlay can access the forwarding table of the different local routing protocol domains via IEI-RO, then partitioned local routing protocol domains can be taken into consideration when choosing which interconnection platform to choose for delivering the traffic to the destination local routing protocol domain. A standard Internet or MANET protocol in connection with some gateway functionality in the interconnection platforms, can be used in the overlay for basic connectivity, however the performance is expected to be better with a specific protocol developed for the overlay. No mature protocol designed specifically for the interconnect-overly architecture exists today.

The time required from a route is requested, until it is found, depends on the protocol design and protocol timers of both the protocols in the local routing protocol domains and the overlay protocol. Since here the routing information is maintained with two protocols with their own timers it is likely that the time to find a route is longer than for the flat architecture.

E.5.4.1.2 Radio Silence

To which effect the network can support radio silence depends on the different local routing protocol domains and the protocol in the overlay. It is not likely that the overlay will be in radio silence, but selected local routing protocol domains might be. The overlay will automatically stop using a local routing protocol domain that is in radio silence for transit traffic since the overlay links will time out. In order for the overlay to keep sending traffic to the segment in radio silence, the radio silence information must be signaled over the IEI-RO and the overlay protocol must have support for continued transmission to the domain in radio silence.

E.5.4.2 Robustness

E.5.4.2.1 Detect Link Break and Find New Route

Routing in this architecture is done in two layers, the local layer and the overlay. The local layer tries to find the best path internal to the local routing protocol domain. The overlay, that sees the complete heterogeneous network, tries to find the best overlay path from the local routing protocol domain of the source to the local routing protocol domain of the destination. The robustness is good, the local domain will detect and repair link breaks internally and the overlay will detect and avoid network partitions (tunnel break). Due to the two levels of protocols, there will be longer response time for end-to-end paths than for the flat architecture. It is possible for the overlay to either get information about the network state of a local routing protocol domain via the IEI-RO or monitor the quality of the path over the local routing protocol domain with network state estimation tools. In that situation it is possible to avoid transmission technologies that are being jammed or that experience flaky connections for other reasons.

E.5.4.2.2 Multiple Paths

For added robustness the availability of multiple paths allow quicker rerouting times after link breaks as well as providing parallel paths over which redundant copies of the information can be sent. A protocol that supports multiple paths can be installed in the overlay and make the forwarding in the overlay more robust. Protocols that support multiple paths can be available in the different local routing protocol domains to make local forwarding more robust. These can also be combined but that is more challenging and requires that the IEI-RO can convey the necessary information.

E.5.4.2.3 Network Stability and Vulnerability

With this architecture, local traffic and end-to-end traffic is handled by two different protocols. Stability problems in one local routing protocol domain can be kept local. The instability of the local routing protocol domain can be visible in the overlay as a flaky link or with extra network control traffic if the overlay must frequently alter the choice of interconnection platform to deliver traffic to a certain destination to. Overall, the stability should be good.

E.5.4.2.4 Cyber Resiliency

Attacks by adversaries to confuse one local routing protocol domain will mainly affect local traffic. If the overlay routing protocol domain is attacked this will affect end-to-end traffic, but not the local traffic. Monitoring and detection of cyber threats as well as reacting to cyber threats may be more complicated because of the separated domains as well as two layers of routing.

E.5.4.3 Scalability

E.5.4.3.1 Overhead from Network Control Traffic

In this architecture it is assumed that the routing protocol that is used in the local routing protocol domains is optimized for the respective transmission technologies, thus the internal signaling overhead is as low as it can be for best performance. In addition to locally produced network control traffic there will also be network control traffic on the tunnels that are used by the overlay. Some topology information from the overlay might also be distributed by the local routing protocol domain, but this is not absolutely necessary.

If a proactive protocol is used in the overlay, then there will be periodic network control traffic, however since the overlay links are assumed to break seldom (the underlying local routing protocol domains strive to keep the overlay connection up) the timers can be set to long intervals. Additionally the control traffic only traverses the tunnels and is not flooded from all-to-all in the local routing protocol domain. If it is assumed

that most traffic is local and only a small portion of the traffic needs to enter the overlay, proactive protocols can be used in the local routing protocol domains and a reactive protocol can be the best choice in the overlay. Such protocol can be tailored to have very little overhead. The network control overhead in this architecture is assumed to be lower (in most cases) than for the two other architectures, however this should be studied further with different configuration parameters with simulation or emulation.

E.5.4.3.2 Tailoring of Network Control Traffic

Similar to the interconnect-flat architecture, this architecture also allows local routing protocol domains that are tailored for a specific transmission technology. However, the local routing protocol domain also has to carry network control traffic of the overlay tunnels. This is difficult to optimize but the local protocol domain can, e.g., inform the overlay via IEI-RO of a maximum capacity that it allows the overlay to use for signaling, as suggested in Section E.4.4.

E.5.4.3.3 Overhead from Suboptimal Paths

For traffic internal to the different routing protocol domains it is assumed that the best path (according to the chosen metric) can be found, thus the overhead due to suboptimal routing paths are negligible for this case. For end-to-end paths, traffic is routed via the overlay. The efficiency of this path depends on the number of overlay nodes and the mesh of tunnels. For overlay nodes on all interconnection platforms and a full mesh of tunnels, the end-to-end paths can be the best possible (according to the chosen metric). For scalability concerns it is beneficial to reduce the number of overlay links, which may come at the cost of introducing some suboptimal paths. More simulation or emulation is necessary to better understand this tradeoff.

The end-to-end traffic that crosses several network segments must be forwarded by the tunnels of the overlay. This creates additional overhead. Some header compression algorithm (e.g., Robust Header Compression (ROHC) [37]) can reduce this overhead. The tunnel overhead can be removed if the local routing protocol domains can be told to route via the next hop overlay router which next, identifies the next hop overlay router and so on. This requires modification of the routing protocols for the local domains.

E.5.4.4 Resource Efficiency and QoS

E.5.4.4.1 QoS Routing

QoS routing can be supported in the local routing protocol domains and/or in the overlay if protocols that support QoS are installed. Supporting QoS routing in the local domain will have only local effects. Supporting QoS routing in the overlay can be beneficial also without QoS support in the local routing protocol domains e.g., traffic can be blocked when it enters the overlay if the overlay knows that it does not have a path with required quality to the destination's local routing protocol domain. It is possible for the overlay to collect the network state of an overlay link via the IEI-RO or monitor the quality of the link with own network state estimation tools (see Ref. [36] for an example QoS routing protocol for the overlay). Local and overlay QoS routing can also be combined but that is more challenging and requires common metrics and an IEI-RO that can convey the necessary information.

E.5.4.4.2 Providing Multiple Paths

Two different schemes for multiple paths between source and destination can be beneficial for resource efficiency and QoS:

- Equal cost paths (load balancing); and
- Link quality specific paths (differentiated characteristics).

This is similar to the QoS routing case, if the local protocol or the overlay protocol can support multiple paths, this can easily be utilized for local traffic or for the end-to-end transport. For a combination of both, the protocols must be interoperable and the IEI-RO must be able to provide the necessary information.

E.5.4.4.3 Network Policies

The interconnect-overlay architecture is a nice framework for supporting network policies. Network policies for local traffic should be supported by the local routing protocol domain and routing policies for end-to-end traffic must be supported by the overlay. If the local routing protocol domains want to restrict the access to the domain, this must be communicated over the IEI-RO to the overlay for the overlay to take such policies into account for end-to-end decisions.

E.5.4.5 Configuration and Management

E.5.4.5.1 Protocol and Configuration Complexity

The local routing protocol domains must be configured to handle local traffic. The overlay protocol must be configured for best end-to-end connection. This layering of protocols reduces the complexity and makes it easier to make good choices both for local traffic and for end-to-end traffic. One by one, the different local routing protocol domains are easy to configure. The overlay might be more complicated to configure since this will always be a heterogeneous network where the different links can have very different properties, on the other hand this can be automated since it is a single protocol. The architecture requires expert knowledge of many different protocols but typically the network sizes will be small. This reduces the risk for configuration error.

When a new local routing protocol domain is added to the network during an operation, the local routing protocol domain must be configured as usual in standalone fashion. The interconnection platform(s) must be identified and included in the overlay. As for the flat routing architecture this configuration requires agreement on many parameters (e.g., profile, namespace, etc.) among all coalition partners that participate in the network with network segments that carry overlay links. Here is a risk for configuration errors that can lead to loss of end-to-end connectivity. Note that local traffic will not be influenced by this. The overlay network is expected to be much smaller than the network of the flat architecture, since only overlay routers participate in this network, thus it is easier to detect and fix configuration errors in the overlay network.

E.5.4.5.2 Remote Management

Management of the Interconnect-overlay network is complex. There are many different systems to manage and most likely different protocols to use for network management. The overlay architecture provides a framework where it is possible to focus on traffic management and traffic engineering by installing a protocol in the overlay that supports this. The overlay also provides a common interface that can enable coherent coalition management. In the local protocol domain, these functions must be handled by local functions.

E.5.4.6 Ease of Deployment

In its basic form with no dynamic information flowing over the IEI-RO and manual configuration of the tunnels that form the overlay links, this architecture can technically be used today to connect many existing IP enabled military radio networks. An external router must be introduced to the interconnection platforms to run the protocol of the overlay routing protocol domain. A standard Internet or MANET routing protocol can be used in the overlay, although current protocols are not efficient enough for use over VHF connections. The vendor specific route redistribution function (see Section E.4.4) can be used to support the IEI-RO. This architecture can also work without dynamic topology information made available over IEI-RO.

Installing a more specialized routing protocol to, e.g., cater for QoS needs or scalability concerns can also easily be done for the overlay network. This requires a router on the interconnection platform that can run the protocol, the availability of a protocol with the needed characteristics and a common agreement between the coalition partners on which protocol to use. The local routing protocol domains can be left as is. For better performance the availability of IEI-RO could be good.

Deployment of an overlay routing domain in a coalition network requires that a common routing protocol for the overlay must be agreed upon by the nations and that there is an agreement on using the interconnect-overlay architecture.

E.5.4.7 Conclusion

This interconnect-overlay architecture is a compromise architecture that aims to provide the network designer with similar flexibility and functionality as the flat architecture but with less overhead. The architecture allows optimized embedded routing protocols to run in the (often small) local routing protocol domains and focuses on making good choices for the traffic that need to traverse several local routing protocol domains. One or several local protocol domain can also be small heterogeneous networks running a flat architecture. This results in a hybrid architecture. Due to overhead concerns it is expected that these local routing protocol domains are quite small. Since only a few nodes of each local protocol domain participate in the overlay, it is expected that the overlay network will also be quite small. It is probable that the links in the overlay are quite stable since the underlying protocol strives to keep the local network connected, and with that the tunnel(s) between the interconnection platforms that forms the links in the overlay.

This architecture resembles very much the structure from the Internet of interior-gateway-protocol domains (local routing protocol domain) that are connected by exterior gateway protocols (overlay routing protocol domain). However, since the nature of mobile tactical network differs from fixed networks, traditional protocols such as BGP are not suitable to play this role in the tactical environment. (e.g., Ref. [38]). The Interconnect-overlay architecture described here has low maturity and it must be studied further how well this architecture performs. In the section describing state-of-the-art protocols (E.10) we point to a few protocol proposals that could be used for this architecture.

E.6 ARCHITECTURE COMPARISON

In this section we will compare the different architectures for each of the requirement categories listed in Section E.5.1.1. The terms in **bold** indicate the performance parameters that are discussed in more detail in Section E.5.

E.6.1 Heterogeneous Network Routing

The goal of the heterogeneous network routing requirements is to ensure that connectivity between nodes is arranged between all users that want to exchange information.

For the **flat architecture**, since it forms a single routing protocol domain across all transmission technologies, all possible routing paths in the network can be found and used. Therefore this architecture gives in theory very good **connectivity** and the time required from a route is requested, until it is found, is expected to be short (depends on the choice of routing protocol). Support for **Radio Silence** in selected transmission technologies increases the complexity of the protocol. Such protocol does not currently exist.

For the **interconnect-flat architecture** local **connectivity** is good. With a routing protocol tailored for each transmission technology, it might be better than for the flat architecture. The discovery of paths across different routing protocol domains depends on the level of detail of topology information that is shared over

the IEI-R and the different protocols' ability to carry the shared information. If full connectivity (the forwarding table) is shared, paths to all destinations in the network segments should be discoverable. The route discovery time may be longer than for the flat architecture. **Radio silence** can be handled in selected routing protocol domains. In order for adjacent domains to keep forwarding traffic to the domain in radio silence, there IEI-R and adjacent routing protocols must support this.

For the **interconnect-overlay architecture**, local **connectivity** is the same as for the flat architecture. End-to-end connectivity is expected to be similar to the interconnect-flat, but this architecture does not require IEI-RO in order to provide dynamic end-to-end paths. **Radio silence** can be handled in selected domain. The IEI-RO and the overlay protocol should be radio silence aware. Such protocol does not exist today.

E.6.1.1 Conclusion

In terms of basic heterogeneous connectivity, the flat routing architecture seems to meet the requirements the best. The interconnect architectures have similar capabilities, with the interconnect-overlay having the advantage of being functional without the availability of IEI-RO and having a generically better overview of end-to-end connectivity than the interconnect-flat architecture.

E.6.2 Robustness

The goal of the robustness requirements is to ensure that the availability of the network for the users is as high as possible, and that disruptions in communications streams and data exchange between users are prevented.

The **flat routing architecture** allows for the fastest **link break detection and repairs** that is possible (decided by the choice of protocol). The architecture requires the IEI-M interface in order to implement advanced routing functions that require extra information about the links. Introduction of, e.g., a new routing metric requires modification of at most one protocol. **Network stability** for a large flat network can be a concern (see scalability). Frequent topology changes in one part of the network can reduce the stability in other parts of the network, the same goes for traffic from configuration errors / malicious node. A single routing protocol also introduces a **cyber-vulnerability**, since an attack or malfunction in one part of the network will most likely affect the whole network. On the other hand, network monitoring, threat detection and mitigation may be easier to handle in a flat architecture because there are fewer network boundaries.

For the **interconnect-flat architecture**, **link breaks are detected and repaired** very quickly in the local domain. For paths traversing several protocol domains, topology information has to be carried across multiple IEI-Rs, which introduces additional detection and reaction time. With IEI-Rs (sharing topology information) on every interconnection platform then in theory the same paths can be found as in the flat architecture. Introduction of e.g., a new routing metric is difficult; it requires modification of all protocols in the network. **Network instability** in one routing protocol domain can be better controlled than for the flat architecture. However this architecture is very vulnerable to routing loops. It should not be used on a heterogeneous network with many interconnection platforms without a plan for how to avoid loops. A **cyber-attack** on one routing protocol will only influence part of the network.

The **interconnect-overlay architecture** will have **link break detection and repair** times similar to the interconnect-flat architecture both for local traffic and for end-to-end traffic. However this architecture provides a better control of the end-to-end path with the overlay. Introducing a new metric for end-to-end paths is similar to the flat architecture, for the local traffic it is similar to the interconnect-flat. **Network instability** in local protocol domains appears in the overlay simply as a flaky path. If there is a **cyber-attack** on the overlay routing protocol, the local routing domains will not be affected, and an attack of one local domain will only affect the overlay paths carried by the attacked domain.

E.6.2.1 Conclusion

In terms of robust connectivity, the flat architecture seems to be the most robust one, followed by the interconnect-overlay architecture. The interconnect-overlay architecture is likely to be most stable and interconnect-flat is least vulnerable to cyber-attacks.

E.6.3 Scalability

The goal of the scalability requirements is to make sure that large numbers of military platforms can successfully exchange information via the heterogeneous network.

A key consideration of the **flat architecture** is its scalability. For most routing protocols the **network control traffic** increases in proportion to the size of the network, since every router in the network must learn about paths to all (relevant) destinations. The timers of the protocol must also be set to keep up with the topology changes of the least robust transmission technology. Although optimization mechanisms exist, the scalability is limited, especially when low-bandwidth links are involved. Mechanisms exist to decrease the routing signaling overhead, but the scalability still remains limited as shown in e.g., Ref. [32], or the performance of the protocol degrades as shown in Ref. [35]. Besides routing signaling, this architecture doesn't introduce other overhead, such as tunneling. This architecture cannot easily be **tailored to the underlying transmission technology** but the **overhead due to suboptimal** end-to-end paths are low.

The **interconnect-flat architecture** is expected to be more scalable (in terms of **network control traffic** overhead) than the flat architecture, since local **routing can be tailored** for respective routing protocol domains, and only a route summary (the details of the summary are dependent on the details of the information that is shared over the IEI-R) is propagated to other network segments. The main drawback of this approach is the difficulty of controlling how the route summary information is propagated which also leads to a high risk of routing loops. There might also be some **overhead due to suboptimal** end-to-end paths.

The **interconnect-overlay** depends on two layers of routing. Local **routing that can be tailored** for the transmission technology is done in the respective local routing protocol domains where we expect that the network size and protocol overhead is tuned to a scalable solution. Additional **network control traffic** is generated by the protocol running in the overlay that does the end-to-end routing. User traffic traversing several local routing protocol domains must be forwarded by the overlay tunnels, this also creates some overhead. The architecture is flexible and the overhead can be tuned by changing the number of overlay links and the frequency and details of the information signaled in the overlay. In Ref. [14], a scalable reactive protocol is proposed to be used in the overlay network. More experiments are needed to compare the scalability of such an approach to that of an efficient routing protocol in the flat architecture. A consequence of keeping a small size of the overlay network is that there might be some **overhead due to suboptimal** end-to-end paths. The interconnect-overlay may make more optimized routing decisions than the interconnect-flat architecture, since the overlay routing protocol has a network-wide view.

E.6.3.1 Conclusion

The interconnect-overlay architecture seems to be the most scalable solution, followed by the interconnect-flat (must be used with care for mesh network constellations).

E.6.4 Resource Efficiency and QoS

The goal of the resource efficiency requirements is to maximize the user data that can be exchanged between users via the heterogeneous network given a certain time span, and to provide QoS.

The **flat architecture** needs the IEI-M interface to collect correct metric information from the transmission technology in order to do **QoS routing**. Standardization among the information provided via the

IEI-M interface is needed to interpret them correctly. With this interface in place, is easy to install protocols that can support **multiple paths** or provide specific metrics for **QoS routing**. The architecture can easily support **network policies** (given that protocols with the necessary functionality is available) that involve the whole network. It requires additional complexity to support routing policies that involve one or a few transmission technologies.

In order for the **interconnect-flat architecture** to be able to do **QoS routing** and **provide multiple paths**, all routing protocol domains must support compatible metrics and the IEI-R must be able to convey the metric information. This is difficult to achieve. **Network policies** that involve a single routing protocol domain can be supported easily. Network policies for the whole network are not so easy to support.

For the **interconnect-overlay architecture**, **QoS routing** and support for **multiple paths** in the overlay can be installed independent of **QoS routing** in the local routing protocol domains, thus protocol changes in all local routing protocol domains are not necessary. **Network policies** for both single routing protocol domains and/or the whole network can be easily supported.

E.6.4.1 Conclusion

In terms of resource efficiency and QoS, the flat architecture has the most potential in terms of global QoS routing, but the interconnect-overlay architectures is very flexible and can be tailored to support different network policies.

E.6.5 Configuration and Management

The goal of the configuration and management requirements is to minimize the effort needed to configure and maintain the network and reduce the need for human intervention in the network to ensure correct operations in different and changing circumstances.

The **flat architecture** allows for a high degree of automation, since the routing intelligence is in one single protocol. It requires a standardized IEI-M interface for optimal use, but no IEI-R or IEI-RO are needed. Proprietary interfaces can be used instead of IEI-M if the router and modem function is embedded in the radio and delivered by the same vendor. The latter option reduces the flexibility of the architecture. It might be a complex task **to best configure** the protocol for the different transmission technologies. There is also a need for tight coordination between nations to correctly configure the common routing protocol. **Remote management** only requires one management interface.

The **interconnect-flat** is also relatively simple **to configure**, as long as the number of routing protocol domains that have to be selected are limited. However, automation is a bit more complex, since there are multiple IEI-Rs and multiple protocols that must be configured. Care must be taken to configure the information flow over the IEI-R in such manner to avoid routing loops and suboptimal routes. **Remote management** is more difficult since many interfaces must be supported.

The **interconnect-overlay** is more complex **to configure**, because it has two layers of routing. For the overlay routing protocol domain, automation is similar to that of the flat architecture. **Remote management** of both the local routing protocol domains and the overlay must be available.

E.6.5.1 Conclusion

The flat architecture is the easiest to configure and manage globally. For the interconnect-flat architecture with many individual configuration interfaces it is difficult to do coherent management for the coalition. The interconnect-overlay might have slightly better coalition management via the common overlay.

E.6.6 Ease of Deployment

We also consider deployment challenges in the discussion in order to assess how easy it is to realize the architecture design with state-of-the-art military communications equipment.

To **deploy** the **flat architecture** the transmission technologies must be made available without embedded routing functionality or the common protocol must be embedded in the device running the transmission technology.

The **interconnect-flat** architecture is the simplest to deploy. This architecture can be **deployed** connecting any IP network as long as the IEI-R is available.

Given the availability of interconnection platforms where the overlay routing protocol is installed, the **interconnect-overlay** architecture can be easily **deployed**. For this situation, any existing IP network can be connected. It is beneficial but not necessary to have IEI-RO available.

E.6.6.1 Conclusion

The interconnect architectures are easiest to deploy. On the other hand, no technical reasons prohibit vendors to offer products that fit the flat architecture as well.

E.6.7 Impact on Coalition Interoperability

When teams consist of units from multiple nations, they need to be interoperable. The goal is also to be able to share information between the units of different nations, as if they were in the same nation's network. In Section E.4.2 the following IEIs were defined:

- The IEI-M interface;
- The IEI-R between the routing protocol domains of different network segments; and
- The IEI-RO between the routing protocol domain of a network segment and the overlay routing domain.

These are IEIs for efficient routing or routing interoperability. In terms of mobile coalition operations these IEIs may or may not coincide with the nation's IOPs.

Deploying a **flat architecture** across a multi-national network requires that either the radios are modems without any embedded routing that can be connected to a router that runs the routing protocol of choice, or the radios have the chosen routing protocol embedded. Radios that act as modems should provide the IEI-M interface for improved performance. In this situation the IEI-M can be a coalition interface. That is, if one nation borrows another nation's transmission technology (modem) and connects it to his national tactical router. There is no need for IEI-Rs or IEI-ROs between the nations' units in this architecture. On the other hand, configuration of a common protocol across different coalition partners requires agreement on the protocol to use and many protocol parameters. A common protocol profile must be defined and a common name space for many configuration parameters must be agreed on. Configuration errors can lead to loss of the network service.

The **interconnect-flat** architecture would be the easiest way to combine two nations' mobile networks into a heterogeneous network today. Any IP network can be used to build the heterogeneous network. The IEI-R is needed for this architecture. IEI-R is a coalition interface if the routers (with or without a wireless transmission technology) of two different nations are connected via a point-to-point connection on an interconnection platform. There is no standard implementation of IEI-R today but vendor specific route redistribution functions exist. If this function is used in a heterogeneous network with many interconnection platforms and a chain of networks, there is a high risk of routing loops. For a collation, the partners must

agree on the necessary common guidelines for configuration, on order to avoid loops. This is challenging as long as a standard does not exist.

The **interconnect-overlay** architecture introduces a common (coalition) overlay protocol, that makes use of the different local routing protocol domains to forward its routing messages. Any IP network can be used as the local routing protocol domain. The overlay must be installed on the interconnection platforms. Similar to the flat architecture, configuration of a common protocol across different coalition partners requires agreement on many parameters. A common protocol profile must be defined and a common name space for many configuration parameters must be agreed on. However the overlay protocol is only needed on the interconnection platform and the overlay network is not expected to be very big. It is beneficial if an IEI-RO is supported for information to flow between local routing protocol domain and the overlay. This IEI-RO will be a coalition interface in the same situation as for the interconnect-flat architecture.

E.6.7.1 Conclusion

All the architectures are dependent on enough inter-nation connections to work well. The interconnect-flat architecture can be used for basic connectivity today but should not be the choice for the future since it is difficult to configure to a coherent network, and is very vulnerable to routing loops. The interconnect-overlay is less intrusive than the flat network since it can incorporate existing IP radios, however both the interconnect-overlay and the flat architecture require nations to agree on a common routing protocol and install this on all interconnection platforms or on all routers.

E.6.8 Conclusions

Table E-3 shows the relative score of each of the architectures based on the comparison in the previous sections. The table presents expert opinions by the authors. Some experiments back up some of the scores but more experiments are needed to proof the correctness of most of the scores. Note also that there are many parameters that control the performance of the architectures. One architecture might be best for one requirement in one scenario whereas another architecture is best for the same requirement in another scenario. For some of the requirements, there are no mature protocols with the necessary support. For those cases the rating represents a probability that a stable and scalable protocol can be designed for the architecture and installed in the network.

Table E-3: Relative Performance¹ of the Different Architecture Approaches on the Requirements.

Requirement	Flat	Interconnect-flat	Interconnect-overlay
Heterogeneous networking routing:	***	*	**
• Connectivity	***	*	**
• Radio silence	**	**	***
Robustness:	**	*	***
• Detect link break and find new route	***	*	**
• Multiple paths	***	*	**
• Network stability and vulnerability	*	**	***
• Cyber resiliency	**	*	**

Requirement	Flat	Interconnect-flat	Interconnect-overlay
Scalability:	*	*	**
• Overhead from network control traffic	*	*	***
• Tailoring of the network control traffic	*	**	**
• Overhead from suboptimal paths and tunnels	***	**	*
Resource efficiency and QoS:	***	*	**
• Optimized routes and QoS routing	***	*	**
• Providing multiple paths	***	*	**
• Network policies	**	**	***
Configuration and management:	***	**	**
• Protocol and configuration complexity	**	**	**
• Remote management	***	*	**
Ease of deployment	*	***	**

¹Three stars (***) indicates best score on the subject; one star (*) indicates lowest score on the subject. Three stars (***) indicate best performance compared to the other architectures. The stars do not attempt to describe how well the requirement is fulfilled.

Note: We Assess the Importance of Some Sub-Categories to be Higher the Others, Thus the Overall Character for the Category is Not Necessarily an Average of the Subcategories. See Section E.5 for the argumentation behind the rating.

Overall, it can be seen from the table that no single architecture scores the best overall and combinations of architectural approaches may be necessary in practice. Generically speaking the flat architectures perform well in terms of heterogeneous connectivity, robustness and simplicity while the interconnect architecture may be more scalable, more cyber resilient and, especially the flat-interconnect, more compatible with existing equipment.

E.7 IMPLICATION OF SECURITY DESIGN

“IST-124 Heterogeneous Networks, Security Architecture” [16] presents possible security measures and considerations related to protecting network control and user plane data in mobile tactical networks. It focuses on the general problem of securing data in a network that consists of multiple routers and radios, in which the radio could have different configurations, both in terms of communication functionality as well as in terms of security capabilities. This effectively results in the creation of different approaches to create so-called red-black separations. In this section we will look at the presented alternatives in the security document and go into more detail on how they would impact the three presented routing architectures.

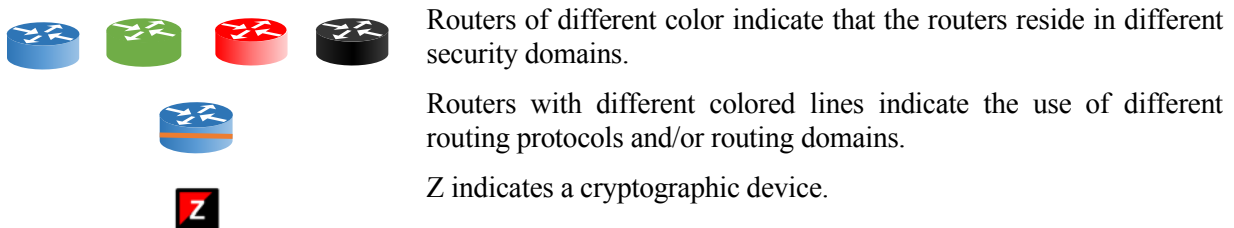
For the routing architecture, in this section, our main concern is the impact of security approaches to the information exchange interfaces that were identified in Section E.4.4, namely the IEI-M, the IEI-R and the IEI-RO interfaces. Signaling between applications and the network, e.g., for Quality of Service, is out of scope for this annex. The two main security approaches from the security architecture report that are relevant for our discussion are:

- Security architecture based on combined application-level/end-host encryption and link encryption; and
- Security architecture based on network-level encryption.

The first approach introduces two layers of encryption, since application-level encryption does not enable protection of network control data which, according to the IST-124 Security architecture, is needed, especially in the case of wireless networks. The second approach protects both user and control data using a single level of encryption.

In the remainder of this section we will discuss per routing architecture the impact of these different security approaches. Note that in the figures we depict the OSI-layer implications for the application-level encryption only, and not those of the host-level encryption, since both have similar impact on the routing architecture IEIs. For the security solution as a whole however, it does matter whether the end-to-end encryption occurs at the application level, or at the network or host-level, e.g., for key distribution and security capabilities of applications. Those aspects of security are discussed in the security architecture report.

Note that due to the additional aspect of security, we use slightly different router symbols in this section than we do for the figures in other sections of this annex. Also, in the figures of this section, radios are depicted either with or without a router inside. These are implementation views, indicating either a radio device with an embedded router inside, or a radio device without layer-three functionality:



E.7.1 Security Implications of the Flat Routing Architecture

The flat routing architecture as described in Section E.5.2 assumes that radio and routing functionality are conceptually separated. Please note that this still allows for the integration of the routing functionality into one of the radios, as long as the other external radios operate in layer-two mode. All routers run the same (flat) routing protocol and communicate directly using routing protocol messages. When looking at the application-level with link-crypto solution, which is visualized in Figure E-19, no implications on the flat routing architecture IEIs are introduced. The only relevant interface is the router-to-modem IEI-M interface (in green) which in this security approach resides fully in the grey security domain and does not cross any security boundaries. In case QoS signaling between the application and the network is needed, a security boundary (red-to-grey) has to be crossed. However, this interface is out of scope for the discussion in this annex. An advantage is that this approach enables the blue router to route traffic that originates from multiple security domains, since all traffic arrives encrypted at the blue router. This is under the assumption that the separation between different security domains is done inside or directly next to the end hosts. It should be noted that for the case of application-level security this brings along challenges to key management logistics.

The other alternative that is presented in the security architecture report is the network-level encryption approach. In this approach there are two choices that can be made, either the encryption device is located between the hosts and the router (the flat router is in the black domain and all hosts are behind a single network crypto), or the encryption device is located between the router and the radio (the flat router is in the red domain). When the crypto device is located between the host and the router the IEI-M interface does not cross a security border and the flat architecture is not impacted. This is shown in Figure E-20. However, when the network crypto is located between the router and the radio, the IEI-M interface is impacted, as is visualized in Figure E-21. The red router in the figure runs the flat routing protocol.

The advantage of the latter approach is that all routing control information is protected. The drawback is that optimized routing is difficult since black-side information cannot be obtained by the flat routing protocol.

A way to still realize this would be to enable some form of strictly controlled information exchange through the red-black separation. The operational security impact of such a design would have to be assessed to determine if it can actually be applied operationally. Another drawback is that with this approach a router can only route traffic from a single security domain, since all traffic is routed when it is plain text. Since the flat router belongs to the red security domain it cannot do the routing for hosts that are located in another security domain on the same military platform, without introducing additional encryption measures leading to additional (tunneling) overhead.

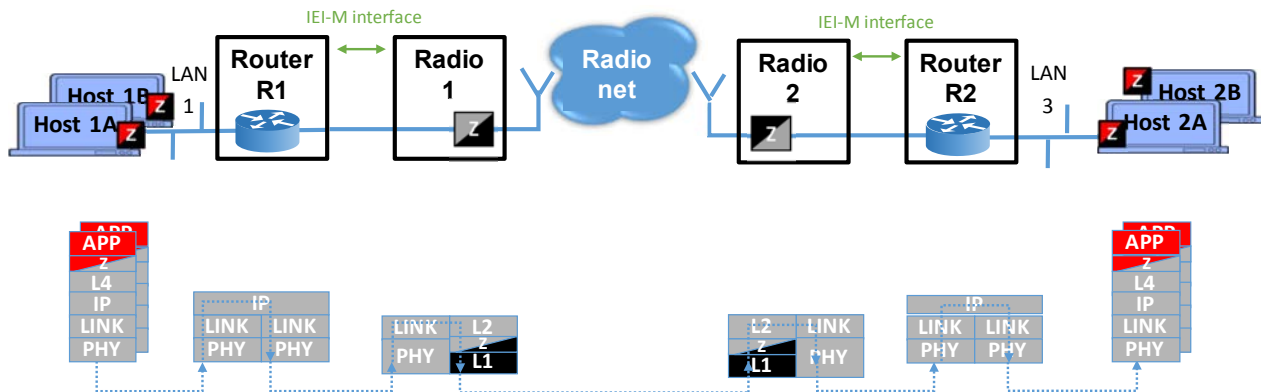


Figure E-19: Application-Level with Link Encryption in the Flat Routing Architecture.

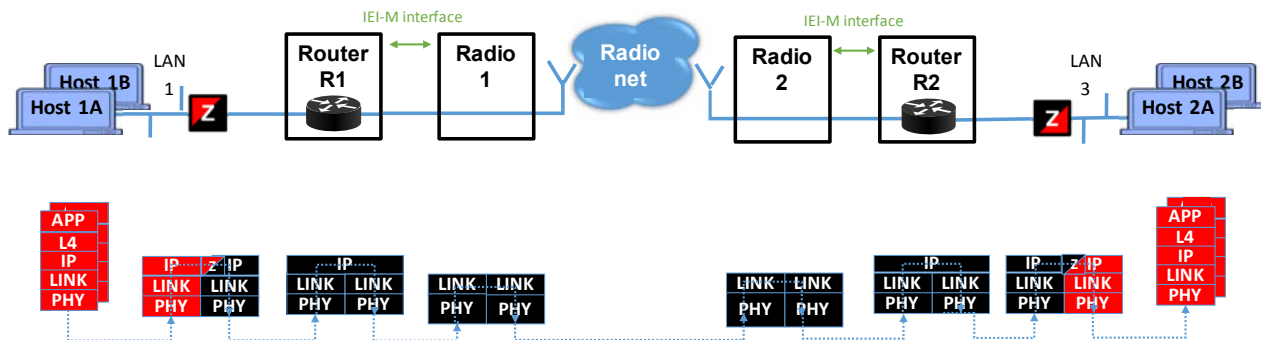


Figure E-20: Network-Level Encryption in the Flat Routing Architecture, Where the Crypto is Between Hosts and the Router.

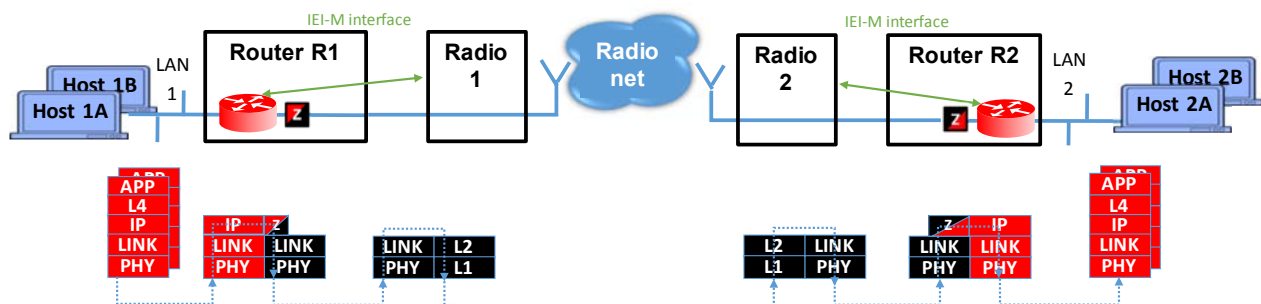


Figure E-21: Network-Level Encryption in the Flat Routing Architecture, Where the Crypto is Between the Router and the Radios.

In addition, encryption at the network layer can also be used to provide for generic link-level protection, instead of doing actual link layer encryption on each (layer-two) radio device. In this approach, network layer encryption is added hop-by-hop between each node, keeping the router effectively in the red domain. This leaves the freedom to still add application-level protection on top of that for end-to-end security and to allow for multiple security domains on the military platform. This results in a setting similar to Figure E-19, except that IEI-M still has to cross a security boundary as was the case in Figure E-21. Also, the overhead due to added encryption tunneling may be somewhat higher. An example realization of this approach is described in Ref. [39] and visualized in Figure E-22. In order to limit the additional overhead, Ref. [39] proposes to use IPsec in transport mode for link-level protection enforced through hop-by-hop network-layer encryption.

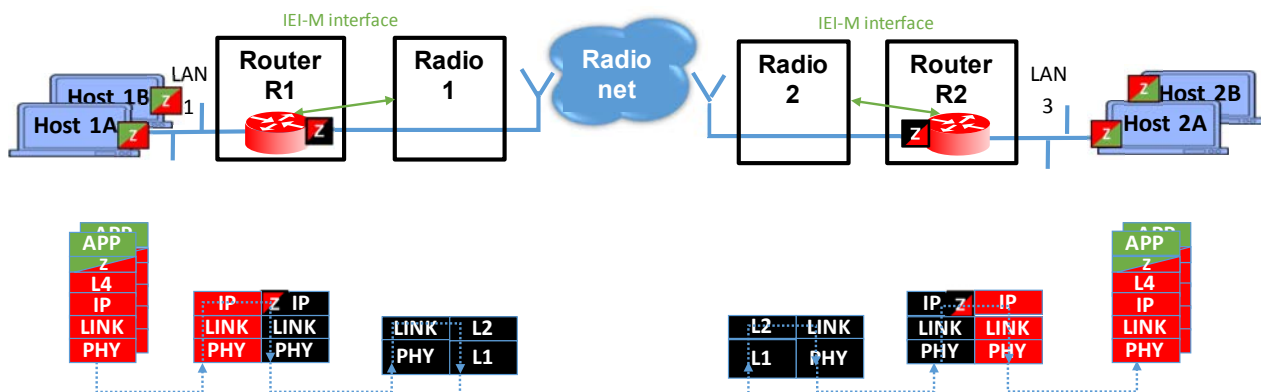


Figure E-22: Network-Level Encryption Used as Generic Link Encryption in the Flat Routing. Adapted from Ref. [39].

E.7.2 Security Implications of the Interconnect-Flat Routing Architecture

The interconnect-flat architecture as described in Section E.5.3 connects routers from different routing domains directly to each other using an interface called IEI-R. In this concept two or more routing protocols that form different routing domains, each with their own set of transmission technologies, meet on a single military platform (an interconnection platform). Figure E-23 shows an interconnection platform that runs two routing protocols that form different routing domains (blue routers with either a yellow or orange line). The orange line routing function is embedded in a radio device (making it a layer-three radio), while the yellow line routing function resides in a tactical router that is connected to a layer-two radio. The focus here is on the IEI-R between the routers. In the application-level with link-level encryption solution the IEI-R is not impacted. The only limitation occurs in case the network needs to exchange information with the application, but this is out of scope for the analysis in this annex.

When applying the network-level encryption approach to the interconnect-flat architecture, there is the choice where to put the crypto device. There are three options:

- Both routers are on the red side.
- Both routers are on the black side
- The routers are in different security domains.

In the first two options, there is no impact on the IEI-R interface and the concerns are similar to the ones mentioned for the application-level with link encryption solution. However, the third option has an impact on IEI-R as is shown in Figure E-24; the IEI-R crosses a security boundary. In the picture this is shown as a red-black separation and red-green separation, since it should be noted that in a multi-national interoperability setting the routers may be in different domains, preferably of comparable security level (e.g., one is Nation A restricted,

the other is Nation B restricted). When looking at the case where a host on military platform 2 (e.g., Host 2A) wants to exchange data with a host on military platform 3 (e.g., Host 3B) and need to route via the interconnection platform on military platform 1, it should be investigated if this means that the IEI-R needs some kind of additional release mechanism for the exchange of routing information between the security domains. It should be noted that to fulfill the requirement for a heterogeneous tactical coalition network, both national networks should allow traffic from other nations and security domains to be carried by their networks. This will only be achievable when the security levels of the traffic that is transported are equal to each other.

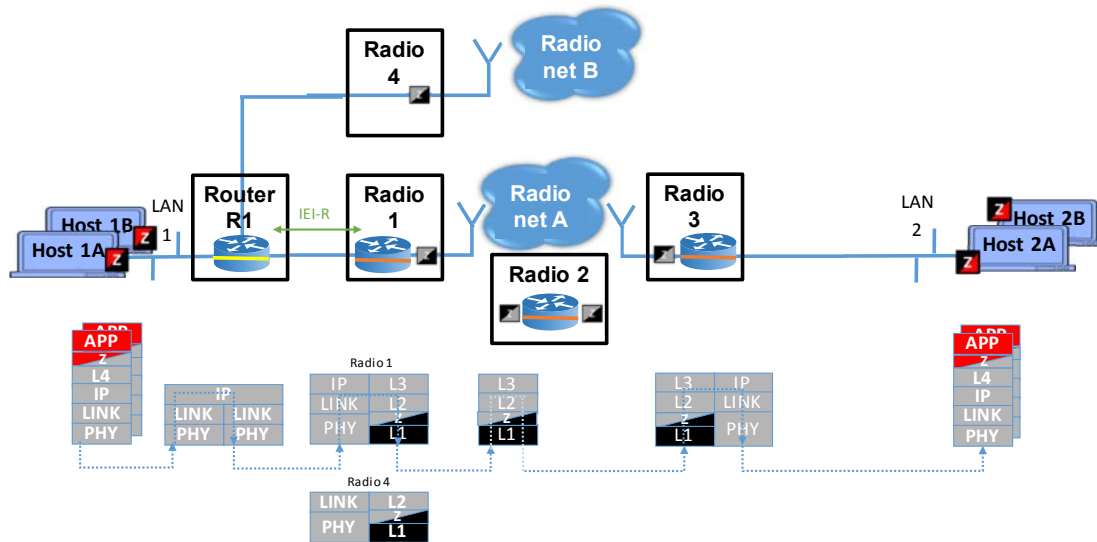


Figure E-23: Application-Level with Link Encryption in the Interconnect-Flat Routing Architecture.

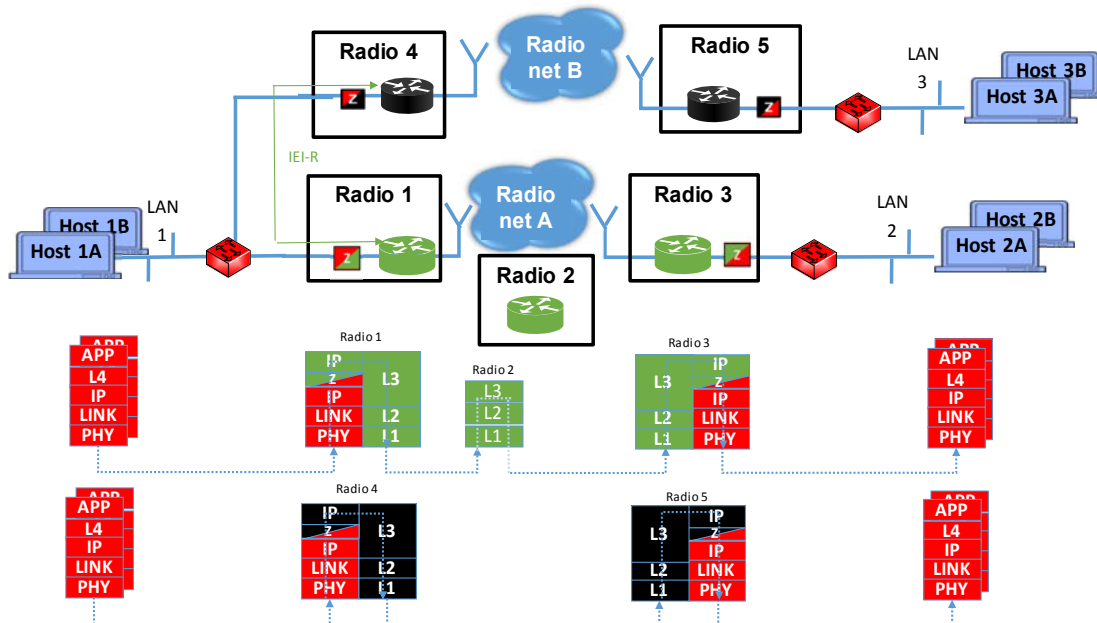


Figure E-24: Network-Level Link Encryption in the Interconnect-Flat Routing Architecture, Where Both Routers are in Different National Domains, Preferably of Comparable Security Level.

E.7.3 Security Implications of the Interconnect-Overlay Routing Architecture

The interconnect-overlay routing architecture is described in Section E.5.4 and has the key characteristic that routing domains are not interconnected directly as is the case for the interconnect-flat, but via an overlay routing protocol domain. This means that if two routing domains need to be connected, a military platform (interconnection platform) doing this typically runs three or more routing protocols. The security asset protection considerations are very similar to those of the interconnect-flat architecture as can be seen in Figure E-25, which shows the application-level with link-level encryption approach. The yellow-ribbon routing domain and the orange-ribbon routing domain are interconnected via the blue overlay routing domain (R1 and R2). The main difference with the interconnect-flat is that there is always an overlay router in between local routing domains, while for interconnect-flat this typically is not the case.

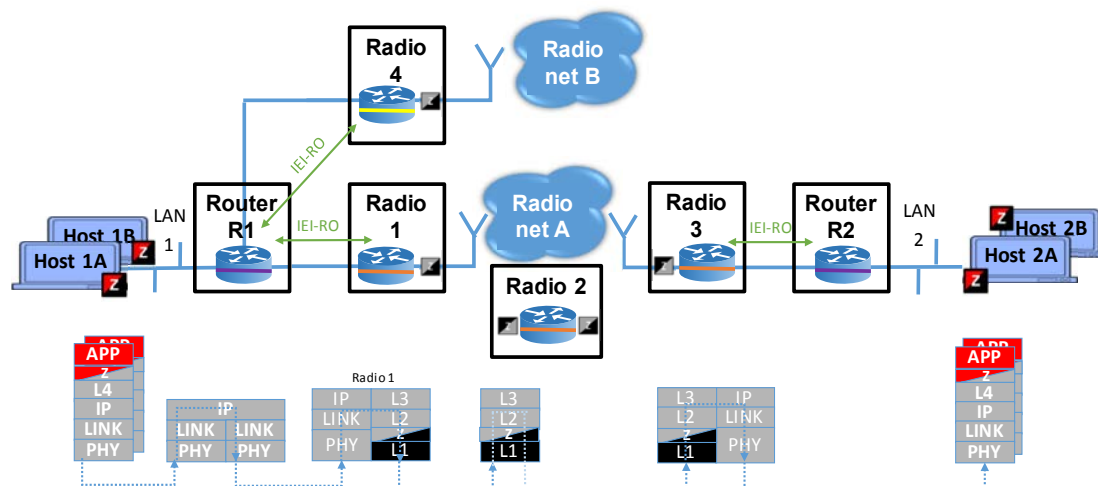


Figure E-25: Application-Level Encryption with Link Encryption in the Interconnect-Overlay Routing Architecture. Router R1 and R2 are overlay routers.

Applying network encryption to this scenario has the same options as the interconnect-flat architecture:

- The sub-routing domain router and overlay router are both in red domain.
- The sub-routing domain router and overlay router are both in the black domain.
- The overlay router is in the red domain and the sub-routing domain routers are in the black domain.

For the first two options, there is no impact on the IEI-RO, since it resides fully in either the red or black domain. For the third option, the IEI-RO crosses a Z-device as is shown in Figure E-26.

E.7.4 Additional IEI: Realizing a Flat Routing Architecture in Case of a Hybrid Black and Red Router Configuration

One of the figures of the security document shows the figure that is presented in Figure E-27, in which a flat architecture is aimed for, but some radios are capable of encryption and others are not. Such a scenario could be introduced by the fact that in some operational deployments headsets, that may not have the required (cryptographic) security capabilities, are directly connected to the radio instead of to the vehicle LAN. Although such a configuration is not desired from both a routing and security perspective, they may be present in practice. The IST-124's Security Architecture elaborates on this aspect [16]. This particular setting brings complications along in terms of flat routing, because there is no single router that has the full view over all radios that are available on the military platform: the black router R2 can make better routing decisions for the networks Radio A and B are part of, while the red router R1 can make better routing

decisions for the networks Radio C and Radio D are part of. In order for this to work optimally from a routing perspective, Router R1 and Router R2 should share information about their networks, ideally synchronizing their routing information, or at least become part of the same routing domain, resulting effectively in a flat routing architecture. This asks for an IEI between Router R1 and R2 (IEI-RH), which has to be strictly controlled, since it allows for information to flow between the black and the red domain. Note that an alternative option is to only inform the Router R1 of the information of R2 and trust R1 fully with the routing decision. In this case routing information should flow from the black to the red domain only. Also note that a similar situation may occur for the flat-overlay architecture. A third option is to connect Radio A and Radio B via an IEI-M to Router R1, but this has to be done via a cryptographic device and is therefore only possible when this information is allowed to cross the black-red separation.

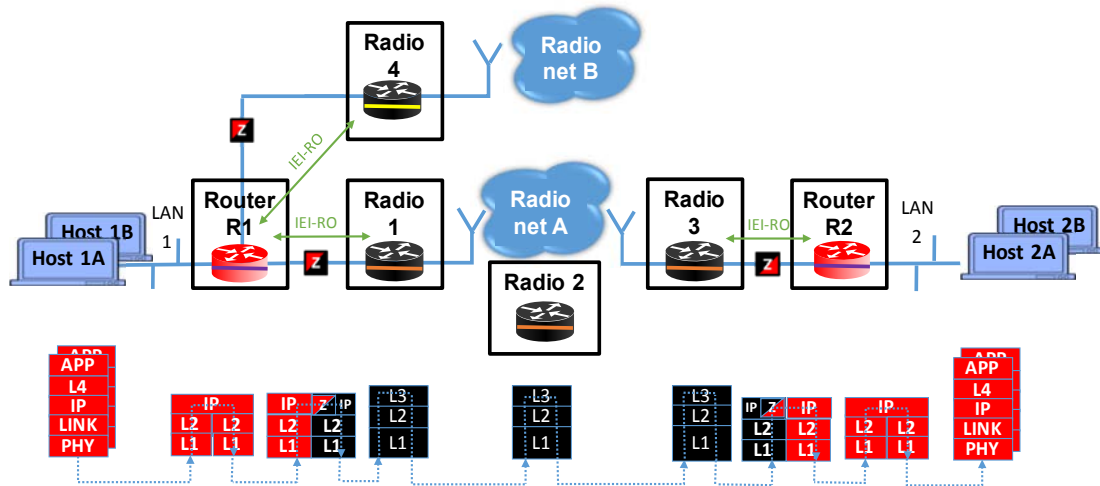


Figure E-26: Network-Level Encryption Between the Overlay and Local Routing Domains in the Interconnect-Overlay Routing Architecture.

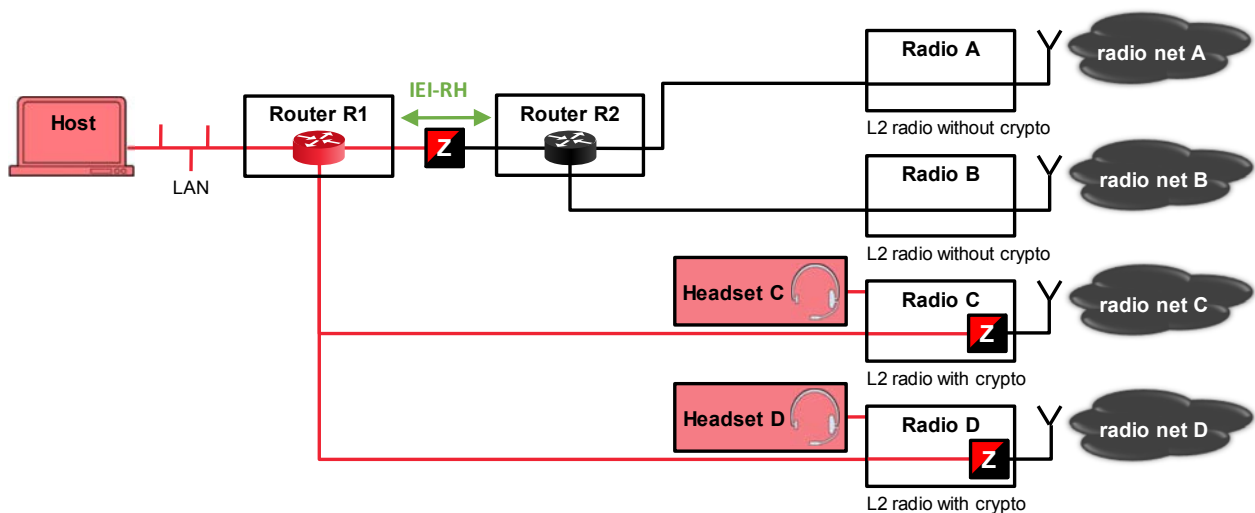


Figure E-27: Hybrid Approach in Which Some Radio Devices are Only Visible to the Red Router and Others Only to the Black Router. The red and the black router both run the common flat routing protocol and the aim is to create a flat architecture, meaning they have to form one common routing domain.

This situation is further complicated in Figure E-28 where two radios (Radio B and Radio D) that have the common routing protocol embedded is included in the picture. Radio D includes encryption whereas Radio B doesn't. Also in this case the routing messages must flow between the different routers on the platform in order for these to form a common routing protocol domain. For this scenario IEI-RH is needed also internally in Radio D. For the sake of completeness the figure also shows the necessary IEI-M interfaces. It should be noted that from a routing configuration point of view, for the case when Router R2 and Radio B both run the common flat routing protocol, it is better to shut down the routing service in one of them and let the other do the routing for both devices. Preferably the routing protocol instance that is the least central in the platform architecture should be shut down (this means Radio B in Figure E-28). Albeit undesired, it may turn out in practice to be impossible to shut down the routing protocol in the radio (because a product may not allow this), therefore this case is included in Figure E-28.

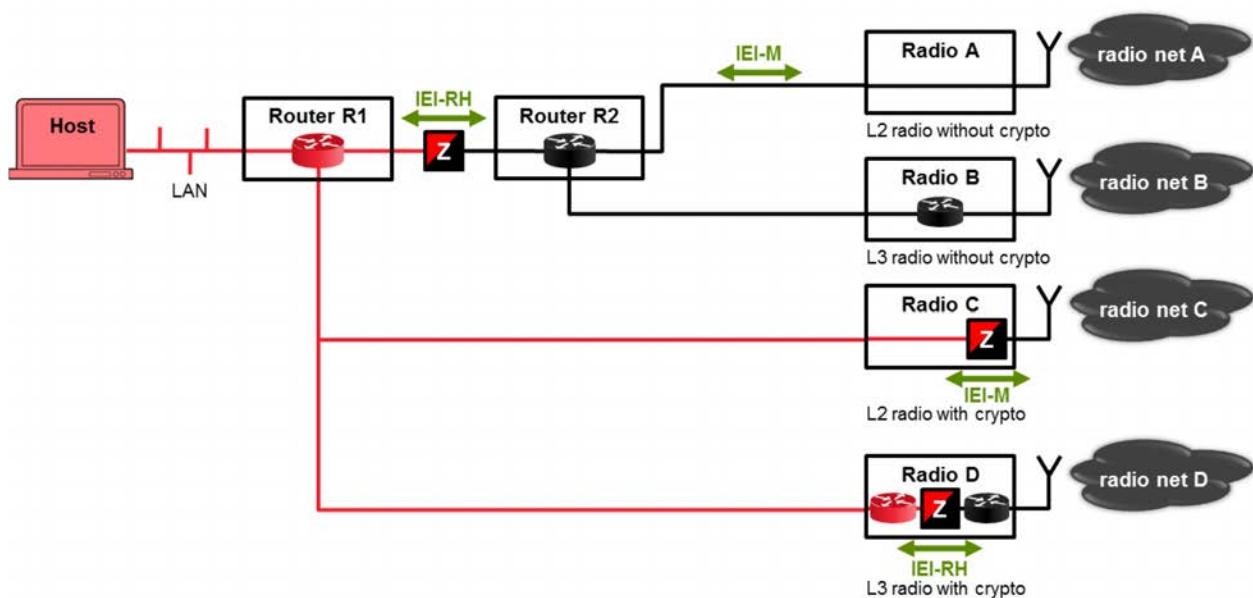


Figure E-28: Information Exchange Interfaces that are Needed to Achieve a Flat Routing Architecture in Case of a Hybrid Platform Configuration in Which Some Radio Devices are Only Visible to the Red Router and Others Only to the Black Router and Where Radios B and D Have the Routing Protocol Used by R1 and R2 Embedded.

E.7.5 Conclusive Remarks on Security

In general, because of the limited availability of bandwidth on wireless links in the military mobile domain, the overhead should be minimized as much as possible in the tactical environment. Concerning security in tactical edge networks the main aim is to minimize the tunnel overhead that is introduced by the security solution, for example by reducing the number of tunnels, and keep the overhead introduced by each tunnel as low as possible. To attenuate the overhead, additional means like Robust Header Compression (ROHC) can be used [37]. Another issue is that with respect to the routing architectures some security approaches lead to the need to send some, strictly controlled, routing information (IEIs) through a red-black separation. Allowing such routing information exchange can weaken the red-black separation between security domains. It depends on the situation whether this is acceptable: both the communication capability improvement that is achieved by these measures and the additional risk that comes with it need to be carefully assessed. IPsec transport mode also weakens the red-black separation in the sense that it leaves the original IP header unprotected and needs to transfer the header from the red to the black side. Transport mode can be used to protect single end hosts. It has less overhead than IPsec tunnel mode. Tunnel mode is used to protect

multiple end hosts. Transport mode could also be used to protect multiple hosts if it is combined with, for example, a GRE tunnel, but it then produces more overhead than tunnel mode. A link-level encryption potentially may have less overhead than both IPsec transport and tunnel mode without further optimizations. A data centric, or application-level encryption mechanism combined with link-level encryption has preference in terms of achieving good routing performance and interoperability while at the same time protecting the network control traffic. It is worth mentioning that a generic link-level encryption can also be realized with IPsec and the appropriate tunnels (e.g., GRE). Application-level encryption requires more cryptographic keys compared to for instance an IPsec device or link-level encryption that protects multiple applications using the same key. Key exchanges and distribution of more keys add overhead.

E.8 PROPOSED HETEROGENEOUS NETWORK DESIGN

From the discussion in this report it is clear that there is no single architecture that suits all needs for all scenarios. As indicated in Section E.4.5 there are a lot of tradeoffs leading to different choices for different scenarios. We believe it is necessary that the future brings a tactical network that allows the network planner to choose between different architectures and be able to pick one, or a combination, that suits the operation the best. In the following we suggest some guidelines of when the different architectures suit best.

Flat routing is best suited for:

- Heterogeneous network where the different transmission technologies have similar characteristics such as data-rate and transmission delay, or where the networks are small enough to allow also narrow band transmission technologies to support the signaling overhead.
- Scalability tests should be used to find the acceptable network size for scenarios with for example different transmission technologies and different targets for network control traffic.
- Scenarios where end-to-end traffic crossing different transmission technologies are prevalent. For these cases it is important to optimize for end-to-end performance at the cost of reduced throughput internal to each transmission technology. This cost is higher for a heterogeneous network that incorporates transmission technologies with very different characteristics than for a more homogeneous network. In the latter case it is easier to tailor a common protocol for good performance in the whole network.
- Networking in a congested space or in very difficult terrain for channel propagation. In this situation, the robustness available with a protocol that can take information about all links of all transmission technologies into account when searching for a route might be necessary.
- Networking with advanced transmission technologies that support cognitive radio and topology control. For this more long-term case that foresees full flexibility in the use of frequency spectrum and coding techniques, the network layer must be equally flexible.

Flat routing is not suited for:

- Large networks that also include low data-rate transmission technologies.
- Heterogeneous security design that enforces the presence of multiple routing protocol domains, since the routing architecture is per definition not flat anymore.
- Near term networks where transmission technologies with embedded no standardized routing (L3 radios) are prevalent. These are difficult to include in the flat routing architecture.
- Scenarios with transmission technologies that do not provide the IEI-M interface. This will work, but the routing performance will be degraded. That is, unless the IEI-M interface is embedded in the radio and the routing function and modem function originate from the same vendor.
- Scenarios where the traffic local to one transmission technology is prevalent.

Interconnect-flat is well suited for:

- Simple heterogeneous network where only a few different routing protocol domains are connected via few interconnection platforms in such manner that there is no risk for loops.
- Local traffic internal to the different routing protocol domains is prevalent and there is no need for optimized end-to-end paths or end-to-end robustness/QoS routing.
- For near term networks where some network segments cannot support either of the two other routing architectures.

Interconnect-flat is not suited for:

- Any future proof more advanced heterogeneous networks that want to support the mesh topology and that want to exercise some control over the end-to-end path establishment and overhead.

Interconnect-overlay is well suited for:

- Scenarios that require the application of different network policies for local traffic in some network segments (local routing protocol domains) than for the end-to-end traffic in the whole heterogeneous network.
- When traffic local to a transmission technology is prevalent, then we want to optimize traffic internal to a transmission technology at the cost of less optimal end-to-end traffic. The architecture can still provide predictable end-to-end performance and overhead.
- Networks that are large, or that incorporate transmission technologies with very different characteristics. For these scenarios, the flat architecture does not scale and the interconnect-overlay attempts to provide a compromise between overhead and network flexibility. The overlay architecture aims to support most of the requirements that the flat architecture supports, but with somewhat reduced performance for traffic traversing several network segments.
 - More simulation or emulation experiments are needed in order to understand the scalability versus performance of this architecture.
- Near term networks where transmission technologies with embedded, not standardized, routing (L3 radios) are prevalent.
- As a hybrid architecture when each nation runs a flat architecture internally but it is either not scalable to run the flat architecture across the nations, or the different nations have chosen different protocols for the flat architecture.

Interconnect-overlay is not suited for:

- Small networks where the flat architecture is well suited.
- Near term networks with interconnection platforms where it is not possible to introduce a new overlay router or install the overlay routing protocol SW on existing HW.

Given the fact that the flat architecture does not scale to a large network size and that the information exchange requirements do not always require optimized end-to-end performance, we propose a network design with a hybrid interconnect-overlay architecture that connects smaller network segments using the flat architecture and/or some network segments with embedded routing tailored for the transmission technology (Figure E-29). We don't recommend to plan for extended use of the interconnect-flat architecture since it is very difficult to control the end-to-end performance as well as the overhead with this architecture, however we think it is useful to have some standardized IEI-R interface for those situations where quick interoperability using interconnect-flat can provide an intermediate solution.

The suggested hybrid architecture is not well studied and simulation or emulation experiments are needed to better understand the performance and be able to suggest the best size of the local routing protocol domains and the size of the resulting overlay network. For all discussion in this annex we have aimed for a fully meshed architecture where topology information is shared between the different transmission technologies. These routing architectures for the mobile domain should be viewed in conjunction with the deployed networks that will be present in an operation. Some information will be shared via the mobile mesh links, while other information will be shared via the deployed coalition network. Especially for very large networks, the role of the deployed network is expected to be significant. If the deployed backbone is available to lower tactical levels, then the mobile networks can be smaller and the meshed routing architectures as discussed in this annex are adequate. If the deployed backbone does not reach this far, then the mobile networks must be larger and aspects such as route aggregation and hierarchical routing approaches will be necessary for scalability reasons. These aspects are left for future work.

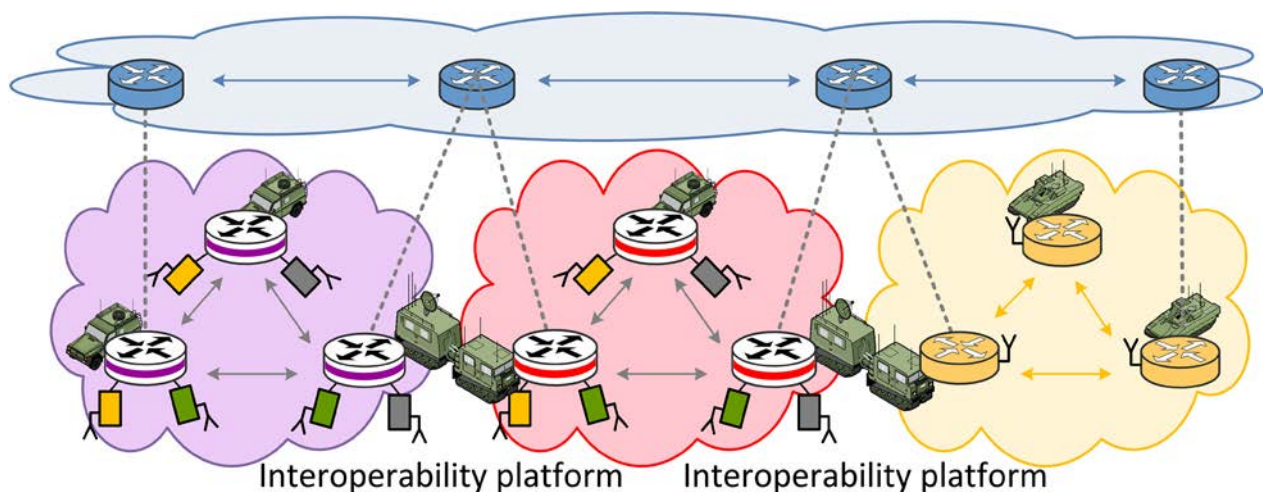


Figure E-29: A Hybrid Architecture with the Flat Architecture and the Interconnect-Overlay Architecture Combined.

E.9 CONCLUSIONS AND NEXT STEPS

In this document we discuss considerations and provide guidelines for realizing robust connectivity in mobile tactical networks, in coalition context. These mobile networks must be treated differently than static and deployed networks, in order to perform well, thus we propose to take the considerations and guidelines of this document into account when specifying FMN for mobile tactical (edge) networks. We have presented and characterized three different routing architectures which can all be used when designing the mobile tactical networks of the future, flat, interconnect-flat and interconnect-overlay. Each of these routing architectures aim to connect the military platforms that participate in an operation, into a common heterogeneous tactical network, while benefitting from the robustness of utilizing different kinds of transmission technologies. Accompanying the routing architectures, three Information Exchange Interfaces (IEI) have been identified:

- The IEI-M describes information flow between the modem representing a transmission technology, and the routing function. The interface aims at a standard way to connect transmission technologies to a common routing protocol domain in the heterogeneous tactical network, while providing the routing layer with necessary information to optimally use and select the available transmission technologies in the network.

- The IEI-R and IEI-RO interfaces describe information flow between two routing domains. The interface aims at realizing a standard way to connect multiple routing domains into a common tactical network. The routing domains can represent networks of radios with embedded proprietary routing protocols, or national heterogeneous mobile tactical networks using tactical routers that form a common national routing domain.

These Information Exchange Interfaces (IEIs) between different routing protocols and between the routing function and the modems must be specified in a common standard, which is lacking today.

The analysis of the routing architectures in this report revolves around achieving a set of performance requirements: heterogeneous network routing, robustness, scalability, resource efficiency and QoS, configuration and management and ease of deployment. The analysis shows that a general design that works well for all requirements in all terrains and all for scenarios, does not exist. The only way to improve the capacity, robustness and coverage to better match what is sought by mobile tactical forces, is to provide flexible heterogeneous network designs that can be tailored for the different operations. Mobile heterogeneous tactical networks can be very complex and consist of transmission technologies with different characteristics. A very heterogeneous network with a wide range of different transmission technology can be very robust and serve many different needs. On the other hand the heterogeneity will lead to scalability and stability concerns that are difficult to solve. A toolbox of architectures, protocols and network policies should be made available to the network planner in order to allow him to choose the best network architecture and policy for the most important network requirements of the operation, and accept the cost of the choice on other less important requirements.

We suggest to start filling the toolbox with solutions for a hybrid coalition routing architecture that uses the interconnect-overlay architecture to connect smaller network segments using the flat architecture and/or some network segments with embedded routing tailored for specific transmission technologies (Figure E-29). This is a future proof design that has room for much flexibility. One consideration, which is related to flexibility, innovation and realizing vendor independence, is the option to bypass proprietary layer-three functionality of radios and allow a tactical router to provide the routing function for the flat architecture domains. MoDs should take such aspects into account when designing their future mobile tactical networks.

We have shown that different security architectures pose challenges for optimal operation by the different routing architectures, because of red-black separations that impact the information exchange interfaces and the additional overhead that security solutions introduce. An application-level encryption mechanism combined with link-level encryption is beneficial in terms of achieving good routing performance and interoperability while at the same time protecting the network control traffic. The overhead of the application-level encryption and cost of a high number of cryptographic keys deems that sometimes this must be combined with other security solutions that is likely to degrade heterogeneous network connectivity.

Given the drive in civilian network research and development to automate network configuration and maintenance, we believe that the future will show an increased automation of both network configuration prior to an operation and reconfiguration during an operation. As the network complexity increases, eventually a human will not be able to make good choice; some variant of artificial intelligence will do much better in most cases. In order for the automation to work well, a toolbox of mechanisms and architectures must be made available, and the different designs must be well understood and characterized in order for an automation process to be able to select the best mechanisms to build the network of choice.

In terms of future work, the following topics have been identified by IST-124 with respect to the routing architecture:

- Study more how narrow band links can best be included in the heterogeneous tactical network, both routed and non-routed approaches.

- Further definition of the different IEs and experimentation with them, most notably the IEI-R and IEI-RO, for which no standards are currently available.
- Compare the performance of the different routing architectures for different scenarios in a simulation or network emulation environment (e.g., IST-124 emulation environment with the Anglova scenario) to better understand when to use which architecture.
- Multicast, and group communications in general, in heterogeneous tactical edge networks and the impact on the presented routing architectures and their information exchange interfaces. This will be addressed in the new IST-161 “Efficient Group and Information-Centric Communications for Mobile Military Heterogeneous Networks”.
- Identification and development of scenarios for automation both prior to an operation as well as during an operation, and investigation of mechanism that can support such flexibility.

E.10 STATE-OF-THE-ART, RELATED WORK

Most work related to Mobile Ad Hoc Networks (MANETs) has been done studying a homogeneous environment with one transmission technology (typically 802.11). In recent years some work that also considers a heterogeneous MANET that consists of several transmission technologies, has been published. In this review, first we point at some useful general references that describe the challenges with MANET formation as well as some work that point at long-term goals for heterogeneous networks. Next we list related work that discusses different routing architectures for heterogeneous networks and finally we review different routing protocol proposals that might be useful for the different routing architectures.

Ref. [40] gives a well-structured list of challenges in order to provide survivable mobile wireless networks. The paper is 15 years old, but unfortunately still very relevant. The paper considers homogeneous MANETs but all the challenges are even more problematic for heterogeneous MANETs. The paper “Cognitive Tactical Network Models” [41] provides a nice list of steps required to build and maintain a heterogeneous tactical network. The design rules, point at a future network target that is very flexible, where choice of frequency ranges, topology control, and routing protocols cooperate to build the best network given the available resources and scenario. Also, Ref. [5] points at cognitive radios with tight topology control as an important research topic to improved mobile military networks. We have aimed for a nearer term network architecture and have neither considered cognitive networks nor topology control in this discussion. Incorporating support for cognitive radios and topology control is a natural next step for a routing architecture for heterogeneous mobile networks as soon as we have a good solution that can handle the level of heterogeneity that is assumed in this annex.

Only a few studies that we are aware of have looked into the problem of identifying a good routing architecture for heterogeneous networks. In Ref. [15], the authors discuss the advantages and disadvantages of tree-based architectures versus mesh architecture. They look at different reasons for why the tree-based solution is the prevalent and also discuss non-technical issues. We believe that a mesh architecture is necessary in order to fulfill important requirements, thus we have looked into different routing architectures that all fulfill the mesh topology. In Ref. [42], the authors compare different routing architectures for MANETs with an airborne backbone network. Flat routing, hierarchical routing and BGP variants are compared. They have studied only mature protocols and have listed some of the same advantages and disadvantages as we have considered in this document. One conclusion is that the scalability and deployments concerns with flat routing are a major problem for this architecture. In our discussion we have compared the architectures conceptually with experimental protocols in mind and also considered functionality where protocols or protocol functionality does not currently exist.

In the following we give a brief literature review of proposed routing protocols that can be used to implement the different architectures. The work we are aware of can be grouped in three groups:

- 1) Proposals for new inter-domain protocols suitable for mobile environment;
- 2) Proposals for modifications to make BGP better suitable for mobile networks; and
- 3) Proposals of adaptive, hybrid, hierarchical or composite routing that handles both internal and external routing.

Both 1) and 2) describe protocols that suit the overlay routing architecture, whereas 3) describes protocols that suit the flat routing architecture.

A reactive protocol that uses depth first search to do routing in an overlay tying many MANETs is reported on in Ref. [36]. The protocol is designed to have low intrusiveness on low data-rate MANETs/links and to give the network planners and operators the means to steer the traffic based on a range of different policies. An Inter-Domain Routing for MANET (IDRM) protocol is proposed in Ref. [43], which supports many of the needed features for an inter-domain protocol: 1) Partition and merge of domains; 2) Membership announcements; and 3) Support for policy based routing.

The protocol allows existing local routing protocols to be used (also reactive) and uses an overlay of gateways to connect the different MANET domains. In Ref. [44], the protocol (now called InterMR) is improved with fisheye routing [34] to reduce the overhead of the propagation of distance vector information. Bloom filter of the node names in a MANET without hierarchical IP address is used to address a domain. In a recent paper, InterMR is implemented and used for an airborne backbone and compared with a flat routing solution as well as a BGP variant [45]. A Cluster-based Inter-Domain Routing protocol (CIDR) is proposed in Ref. [46]. This protocol exploits group affinity during cluster formation to handle frequent network topology changes. It also uses bloom filters and fisheye techniques to handle dynamic group memberships and reduce overhead. In Ref. [47], an early simple proactive beacon protocol is used to interconnect several MANETs. It seems to be assumed that all domains use a single 802.11 common channel, thus it is not very useful for heterogeneous networks. However, they show that it is necessary to use a hierarchy of protocols to allow interconnected MANETs to scale; one protocol for internal routing in single MANETs, optimized with regards to use and operating environment, and another that is used to tie the MANETs together.

There are also some proposals that aim to improve BGP for a mobile environment. Arguments for this are that BGP is a well-studied protocol, and we can assume that most problems with the protocol are already well described. It can also be easier to support connectivity between a modified BGP protocol and the BGP protocol running in the backbone. All the mentioned papers list some of the known challenges with using BGP to interconnect MANET. In addition, Ref. [48] also describes with the use of an example, how it is difficult to use common guidelines as used in the Internet to ensure BGP route convergence in a mobile environment. In Ref. [49], the problem of AS-split is treated. A dynamic AS reconfiguration is proposed. The paper also raises the discussion if the original policy should follow a deployed (and split) AS, or not. In Ref. [50], BGP with Mobility Extensions (BGP-MX) solves the two problems of dynamic BGP-peer discovery and slow convergence time of BGP. A distributed peering broker service is implemented, and the BGP peers announce their mobility (stationary, low, medium, high) in order to select more stable paths. In Ref. [42], virtual routers are used with BGP to avoid the AS-split problem in a two tier network with multiple MANET domains connected via an aerial backbone. It is noted that configuring the virtual routers will be complex and memory consuming for large networks with many domains. In Ref. [51], a testbed is built in order to study BGP's performance in mobile environments better. The authors also study two improvements of BGP; the use of IPv6 neighbor discovery to support dynamic BGP-peer discovery, and the optimization of BGP signaling overhead by utilizing a Connected Dominated Set (CDS). A more recent BGP – MANET Routing (BGP-MR) is proposed in Ref. [52]. The authors argue that it is better to modify the well-known BGP protocol than to implement a brand-new inter-domain protocol. Thus, they modify BGP to

improvements of BGP; the use of IPv6 neighbor discovery to support dynamic BGP-peer discovery, and the optimization of BGP signaling overhead by utilizing a Connected Dominated Set (CDS). A more recent BGP – MANET Routing (BGP-MR) is proposed in Ref. [52]. The authors argue that it is better to modify the well-known BGP protocol than to implement a brand-new inter-domain protocol. Thus, they modify BGP to have similar gateway functionality as in the InterMR [44] protocol as well as a method to avoid loops. The modified BGP protocol is used to connect MANETs and fixed networks.

All the work presented above allows each MANET to preserve its internal standard or legacy routing protocol and use an additional routing function or extra layer or routing to connect the different domains. Some work is also done to study the use of one protocol in a very heterogeneous environment like the flat routing architecture studied in this report. In these works, a scenario with many small MANETs of different characteristics is assumed. Instead of requiring a protocol for inter-domain connection, the same IP layer protocol (but different MAC and PHY protocols) is tried utilized in all nodes. In Ref. [30], a design is proposed that use several optimized instances of OLSR to support routing in a network with very dissimilar link characteristics. In Ref. [35], it is shown that when different protocol timers are used and/or there are varying transmission delays in the network, (as will always be the case in heterogeneous networks) there is an increased risk of getting routing loops in a heterogeneous MANET. In Ref. [29], OSPF-MT is used as the common protocol in a heterogeneous network to provide support for admission control and QoS. OLSRv2 with the Directional Airtime (DAT) metric is discussed and tested for a heterogeneous community network in Ref. [53] and for a mobile tactical network in Ref. [31]. The DAT metric considers the link speed and the expected transmission count of each link in a heterogeneous network order to find a path that should yield the shortest total transmission time for path. This metric automatically incorporates the different characteristics of different transmission technologies. OLSR is also the basis for a routing protocol for multiple transmission technologies as described in Ref. [54]. In this work where mainly civilian transmission technologies are used, the OLSR functionality is amended with a score function that performs the route calculation for different policies (e.g., optimize energy consumption, capacity, etc.). It is also shown that it is important to tailor the OLSR signaling rates to the underlying technologies. In Ref. [55], OLSR and OSPF-MDR is combined in composite routing. OSPF-MDR is a mobility extension to OSPFv3 and interoperates natively with OSPF. In this architecture, OLSR is used in each MANET, and can be tuned to the MANET's properties. OLSR and OSPF-MDR are merged and use OSPF-MDR's functionality to interact with OSPF. OSPF ties the different MANETs together. A Hybrid protocol based on the Zone Routing protocol (ZRP) [56] and that builds a virtual backbone, is presented in Ref. [57]. The protocol combines proactive routing for the local zones, with reactive routing in the virtual backbone. Thus, a situation similar to the overlay architecture with reactive protocol in the overlay is here built into one protocol. The protocol assumes a homogeneous MANET environment, but with some added work, the concept can also be used for a flat protocol in a heterogeneous environment. MM-Backs presented in Ref. [58] is an extension of M-Backs [59] for heterogeneous networks. These protocols form an internal backbone in order to improve the scalability. It is not clear how traffic is routed and forwarded in nodes that are not part of the backbone. A range of techniques to improve the scalability of flat routing protocols for a homogenous environment have been proposed. We don't review these here. The focus of this review has been to show work that has considered heterogeneous environments.

E.11 REFERENCES

- [1] Hallingstad, G. and Oudkerk, S., "Protected Core Networking: An Architectural Approach to Secure and Flexible Communications," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 35-41, 2008.
- [2] Federated Mission Networking (FMN) Portal, Available: [https://tide.act.nato.int/tidepedia/index.php/Federated_Mission_Networking_\(FMN\)_Portal](https://tide.act.nato.int/tidepedia/index.php/Federated_Mission_Networking_(FMN)_Portal) (NATO UNCLASSIFIED).

- [3] Eggen, A., Hauge, M., Hedenstad, O.E., Lund, K., Legaspi, A., Seifert, H., Sevenich, P., and Simon, P., “Coalition Networks for Secure Information Sharing (CoNSIS) (Invited Paper),” *Proceedings IEEE MILCOM*, San Diego, CA, USA, pp. 354-359, Nov. 2013.
- [4] CoNSIS, www.consis.info. [accessed 16.11.2017].
- [5] Chapin, J.M. and Chan, V.W.S., “The Next 10 Years of DOD Wireless Networking Research,” *Proceedings MILCOM*, pp. 2238-2245, Baltimore, MD, USA, Nov. 2011.
- [6] Kreutz, D., Ramos, F.M.V., Verissimo, P.E., Rothenberg, C.E., Azodolmolky, S., and Uhlig, S., “Software-Defined Networking: A Comprehensive Survey,” *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14-76, 2015.
- [7] Jain, S., Kumar, A., Mandal, S., Ong, J., Poutievski, L., Singh, A., Venkata, S., Wanderer, J., Zhou, J., M., Zolla, J., Hözl, U., Stuart, S., and Vahdat, A., “B4: Experience with a Globally-Deployed Software Defined Wan,” *Proceedings ACM SIGCOMM*, Hong Kong, China, pp. 3-14, 2013.
- [8] Phemius, K., Seddar, J., Bouet, M., Khalifé, H., and Conan, V., “Bringing SDN to the Edge of Tactical Networks,” *Proceedings IEEE MILCOM*, pp. 1047-1052, 2016.
- [9] Spencer, J. and Willink, T., “SDN in Coalition Tactical Networks,” *Proceedings IEEE MILCOM*, pp. 1053-1058, 2016.
- [10] Network Functions Virtualisation, Available: <http://www.etsi.org/technologies-clusters/technologies/nfv> [accessed 04.09.2018].
- [11] Radius Staff, “The Strategic Direction: NFV and Manx Telecom,” in *Radius: Network Function Virtualization and SDN*, Feb. 23, 2017. Available: <https://www.vmware.com/radius/nfv-manx-telecom/>.
- [12] Jacobson, V., Smetters, D.K., Thornton, J.D., Plass, M.F., Briggs, N.H., and Braynard, R.L., “Networking Named Content,” *Proceedings ACM CoNEXT*, Rome, Italy, pp. 1-12, 2009.
- [13] Kutscher, D., Eum, S., Pentikousos, K., Psaras, I., Corujo, D., Saucez, D., Schmidt, T., and Waehlich, M., “Information-Centric Networking (ICN) Research Challenges,” IETF, *RFC7927*. July 2016. Available: <http://www.ietf.org>.
- [14] Menezes, A.J., v.Oorschot, P.C., and Vanstone, S.A. *Handbook of Applied Cryptography*, Boca, FL, USA: CRC Press, 1997.
- [15] Shake, T. and Gibbons, T., “Architectural Consequences of Domain Formation in Tactical Edge Networks,” *Proceedings IEEE MILCOM*, San Diego, CA, USA, pp. 647-654, Nov. 2013.
- [16] Hegland, A.M., Buchin, B., Holtzer, A., Hauge, M., and Peukhuri, M., “NATO IST-124 Heterogeneous Networks, Security Architecture”, STO-TR-IST-124-Part-II, 2019, NATO UNCLASSIFIED.
- [17] Cheng, B. and Berger, L. “DLEP Multi-Hop Forwarding Extension,” IETF, *draft-cheng-manet-dlep-multi-hop-extension*, February 2017. Available: <http://www.ietf.org>.
- [18] Li, L., Rutagemwa, H., Hu, J., Hugg, P., Vigneron, P., Brown, C., Kunz, T., “Networking for Next Generation NBWF Radios,” *Proceedings IEEE MILCOM*, 2015.
- [19] Cheng, B.N., Wheeler, J., and Veytser, L., “Radio-to-Router Interface Technology and its Applicability on the Tactical Edge,” *IEEE Commun. Mag.*, vol. 50, no. 10, pp. 70-77, 2012.

- [20] Ratliff, S., Jury, S., Satterwhite, D., Taylor, R., and Berry, B. “Dynamic Link Exchange Protocol (DLEP),” IETF, *RFC8175*. June 2017. Available: <http://www.ietf.org>.
- [21] Le, F., Xie, G.G., and Zhang, H., “Understanding Route Redistribution,” *Proceedings IEEE ICNP*, Beijing, China, pp. 81-92, 2007.
- [22] Rogge, H. and Baccelli, E. “Directional Airtime Metric Based on Packet Sequence Numbers for Optimized Link State Routing Version 2 (OLSRv2),” IETF, *RFC7779*. Apr. 2016. Available: <http://www.ietf.org>.
- [23] Hanzo II, L. and Tafazolli, R., “Admission Control Schemes For 802.11-Based Multi-Hop Mobile Ad Hoc Networks: A Survey,” *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 78-108, 2009.
- [24] Berry, B., Ratliff, S., Paradise, E., Kaiser, T., and Adams, M. “PPP Over Ethernet (PPPoE) Extensions for Credit Flow and Link Metrics,” IETF, *RFC5578*. Feb. 2010. Available: <http://www.ietf.org>.
- [25] Barz, C. and Rogge, H., “Improved Community Network Node Design Using a DLEP Based Radio-To-Router Interface,” *Proceedings IEEE WiMob*, Barcelona, Spain, pp. 636-642, 2012.
- [26] Hinden, R., and Haberman, B., “Unique Local IPv6 Unicast Addresses,” IETF, *RFC4193*. Oct. 2005. Available: <http://www.ietf.org>.
- [27] NATO Codification Bureaux (NCB), <https://www.nato.int/structur/AC/135/welcome.htm>, (Accessed: 05.01.2018)
- [28] Open Network Automation Platform (ONAP). Available: <https://www.onap.org/> (Accessed: 05.01.2018).
- [29] Hauge, M., Brose, M.A., Sander, J., and Andersson, J., “Multi-Topology Routing for QoS Support in the CoNSIS Convoy MANET,” *Proceedings MCC*, Gdansk, Polen, pp. 1-8, Oct. 2012.
- [30] Landmark, L., Øvsthus, K., and K. Ø, “Routing Trade-Offs in Sparse and Mobile Heterogeneous Multi-Radio Ad Hoc Networks,” *Proceedings IEEE MILCOM*, San Jose, CA, USA, pp. 2229-2236, Nov. 2010.
- [31] Barz, C., Fuchs, C., Kirchhoff, J., Niewiejska, J., and Rogge, H., “Extending OLSRv2 for Tactical Applications,” *Proceedings ICMCIS*, Brussels, Belgium, pp. 1-8, 2016.
- [32] Marcus, K., Barz, C., Kirchhoff, J., Rogge, H., Nilsson, R., in ‘t Velt, J., Suri, N., Hansson, A., Sterner, U., Hauge, M., Lee, K., Holtzer, A., Buchin, B., Peuhkuri, M. and Mısırlıoğlu, L., “Evaluation of the Scalability of OLSRv2 in an Emulated Realistic Scenario,” *Proceedings ICMCIS*, Oulu, Finland, 26 June 2017.
- [33] Ying, G., Lamont, L., and Villasenor, L., “Hierarchical OLSR – A Scalable Proactive Routing Protocol for Heterogeneous Ad Hoc Networks,” *Proceedings IEEE WiMob*, Montreal, Canada, pp. 17-23, Vol. 3, 2005.
- [34] Guangyu, P., Gerla, M., and Tsu-Wei, C., “Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks,” *Proceedings IEEE ICC*, New Orleans, LA, USA, pp. 70-74 vol.1, 2000.

- [35] Landmark, L., Hauge, M., and Øivind, K. "Routing Loops in Mobile Heterogeneous Ad Hoc Networks," *Proceedings IEEE MILCOM*, San Diego, CA, USA, pp. 112-118, Nov. 2013.
- [36] Landmark, L., Larsen, E., Hauge, M., and Kure, "Resilient Internetwork Routing Over Heterogeneous Mobile Military Networks," *Proceedings IEEE MILCOM*, Tampa, FL, USA, pp. 388-394, Oct. 2015.
- [37] Sandlund, K., Pelletier, G., and Jonsson, L.-E. "The Robust Header Compression (ROHC) Framework," IETF, *RFC5795*. March 2010. Available: <http://www.ietf.org>.
- [38] Gibbons, T., Hook, J.V., Wang, N., Shake, T., Street, D., and Ramachandran, V., "A Survey of Tactically Suitable Exterior Gateway Protocols," *Proceedings IEEE MILCOM*, San Diego, CA, USA, pp. 487-493, Nov. 2013.
- [39] Barz, C. and Quinkert, F., "Advanced Security Gateways for Heterogeneous Tactical Ad Hoc Networks," *Proceedings ICMCIS*, Cracow, Poland, 2015.
- [40] James, P.G.S., Rajesh, K., Regina, R.H., Alden, W.J., David, L., Ram, R., and John, Z., "Survivable Mobile Wireless Networks: Issues, Challenges, and Research Directions," *Proceedings ACM Workshop on Wireless Security*, pp. 31-40, Atlanta, GA, USA, Sept. 2002.
- [41] Younis, O., Kant, L., McAuley, A., Manousakis, K., Shallcross, D., Sinkar, K., Chang, K., Young, K., Graff, C., and Patel, M., "Cognitive Tactical Network Models," *IEEE COMMAG*, vol. 48, no. 10, pp.70-77, Oct. 2010.
- [42] Wang, J.N., Narula-Tam, A., and Byan, R., "Interconnecting Heterogeneous MANET Networks at the Tactical Edge," *Proceedings IEEE MILCOM*, Baltimore, MD, USA, pp. 1152-1159, Oct. 2014.
- [43] Chau, C.-K., Crowcroft, J., Lee, K.-W., and Wong, S. H.Y., "Inter-Domain Routing for Mobile Ad Hoc Networks," *Proceedings MobiArch*, pp. 61-66, Seattle, WA, USA, Aug. 2008.
- [44] Lee, S.-H., Wong, S.H.Y., Chau, C.-K., Lee, K.-W., Crowcroft, J., and Gerla, M., "InterMR: Inter-MANET Routing in Heterogeneous MANETs," *Proceedings MASS*, pp. 372-381, San Francisco, CA, USA, Nov. 2010.
- [45] Wang, J.N., Hook, J.V., and Deutsch, P., "Inter-Domain Routing for Military Mobile Networks." *Proceedings IEEE MILCOM*, Tampa, FL, USA, pp. 407-412, Oct. 2015.
- [46] Zhou, B., Cao, Z., and Gerla, M., "Cluster-Based Inter-Domain Routing (cidr) Protocol for MANETs." *Proceedings WONS*, Snowbird, UT, USA, pp. 19-26, Feb. 2009.
- [47] Chandrashekar, K., Morera, R., McAuley, A., and Baras, J., "Domain Based Hierarchical Routing for Large Heterogeneous MANETs," *Proceedings IEEE MILCOM*, Atlantic City, NJ, USA, pp. 1284-1290, Vol. 2, Oct. 2005.
- [48] Sorteberg, I., "BGP Convergence in Military Coalition Networks," *Proceedings IEEE MILCOM*, Monterey, CA, USA, pp. 649-655 Vol. 2, Oct. 2004.
- [49] Hares, S. and White, R., "BGP Dynamic AS Reconfiguration," *Proceedings IEEE MILCOM*, Orlando, FL, USA, pp. 1-7, Oct. 2007.
- [50] Kaddoura, M., Trent, B., Ramanujan, R., and Hadynski, G., "BGP-MX: Border Gateway Protocol with Mobility Extensions," *Proceedings IEEE MILCOM*, Baltimore, MD, USA, pp. 687-692, Nov. 2011.

- [51] Carl, G., Arbiv, S., and Ward, D., “Performance of BGP Among Mobile Military Networks,” *Proceedings MILCOM*, pp. 679-686, Baltimore, MD, USA, Nov. 2011.
- [52] Okundaye, I., Kunz, T., and Gulder, S., “Inter-Domain Routing for Tactical Mobile Ad-Hoc Networks,” *Proceedings IEEE VTC2014-Fall*, Vancouver, Canada, pp. 1-6, Sept. 2014.
- [53] Barz, C., Fuchs, C., Kirchhoff, J., Niewiejska, J., and Rogge, H., “OLSRv2 for Community Networks: Using Directional Airtime Metric with External Radios,” *Computer Networks*, vol. 93, no. Part 2, pp. 324-341, 2015.
- [54] Sadok, D.F.H., Rodrigues, T.G., Amorim, R.D., and Kelner, J., “On the Performance of Heterogeneous MANETs,” *Wireless Networks*, vol. 21, no. 1, pp. 139-160, 2015.
- [55] Fang, J., Goff, T., and Pei, G., “Comparison Studies of OSPF-MDR, OLSR and Composite Routing,” *Proceedings IEEE MILCOM*, San Jose, CA, USA, pp. 989-994, Nov. 2010.
- [56] Pearlman, M.R. and Haas, Z.J., “Determining the Optimal Configuration for the Zone Routing Protocol,” *J-SAC*, vol. 17, no. 8, pp. 1395-1414, 1999.
- [57] Liang, B. and Haas, Z.J., “Hybrid routing in Ad Hoc Networks with a Dynamic Virtual Backbone,” *IEEE Trans. Wireless Commun.*, vol. 5, no. 6, pp. 1392-1405, 2006.
- [58] Basagni, S. and Nanni, M.A., “Using Multiple Radios for Ad Hoc Backbone Construction and Maintenance,” *Proceedings IEEE MASS*, Valencia, Spain, pp. 170-172, Oct. 2011.
- [59] Nanni, M.A. and Basagni, S., “M-Backs: Mobile Backbones for Multi-Hop Wireless Networks,” *Proceedings IEEE WCNC*, Cancun, Quintana Roo, Mexico, pp. 944-949, 2011.



Annex F – INTERCONNECTION PLATFORMS IN VIGNETTE 2

Jan Nilsson and Ulf Sterner
Swedish Defence Research Agency (FOI)
SWEDEN

F.1 INTRODUCTION

In all heterogeneous networks that consist of two or more different radio networks there must be interconnection platforms that establish physical connection between the different radio networks (see also Annex E: “Routing architecture considerations for heterogeneous tactical networks”). The required number of interconnection platforms needed to get full connectivity in the heterogeneous network is an important parameter. This parameter impacts both the performance and complexity of the network design and is investigated in this annex. We consider a heterogeneous network based on Vignette 2 of the Anglova scenario (see Annex A: “Operational Perspective for IST-124”, Annex B “Emulation Based Experimentation and the Anglova Scenario”, Annex C “Experimentation Environment and Tools” and Annex D: IST-124 “Experimentation Execution” as well as Refs. [1], [2], and [3]) where each company form a Company Network (CN). To connect the companies, we select a number of nodes in each company to have an extra radio and take the role of the interconnection platform. This second radio might be identical to the other one (but using a different frequency band) or it might be a different radio with other characteristics. The interconnection platform nodes form an Inter-company Network (IN). We consider a heterogeneous network consisting of four companies (with a total of 96 nodes) in the Anglova scenario. To investigate the number of required Interconnection Platforms (ICPs) we have made connectivity calculations. The connectivity is calculated for all connections between every pair of nodes in the network. That is, not only between the ICPs. For the purpose of the experiments described here, a time interval of the two-hour scenario, from 5500 seconds to 6501 seconds, was selected. The primary reason for selecting this interval is that the networks are reasonably well connected during this timeframe and do not need to use the UAV for connectivity. Furthermore, the four mechanized companies are denoted Company 1, 2, 3 and 4. The chosen time interval is also used in Ref. [2].

F.2 INTERCONNECTION PLATFORM SELECTION

In a practical case the ICPs are probably spread out among the platoons in the company, i.e., not all ICPs are in the same platoon. In this analysis we select the ICPs in the following way. First, in each company, six groups are formed; the four platoons form four groups, the two command nodes is one group and the support vehicles is one group. For an experiment with up to six ICPs in each company, the first ICP is selected randomly, the second is selected randomly but not from the group containing the first ICP and so on, until at most one ICP per group are selected. In an experiment with more than six ICPs, the selection process is repeated until the desired total numbers of ICPs are selected in each company. For example, for seven ICPs, one of the six groups in each company contains two ICPs. When 12 ICPs are investigated, each of the six groups in each company contains two ICPs. For an experiment with a given number of ICPs, 64 realizations of how the ICPs are selected, are made. That is, in different realizations the numbers of ICPs are the same but which of the 96 nodes that are selected as ICPs are different.

F.3 WAVEFORMS

We define the radio system gain G_{sys} to be equal to the maximum possible path loss from transmitter to receiver for connections that satisfy a given error requirement. That is, a radio system with good transceiver performance has a larger system gain than transceivers with low performance. We study different network options for the inter-company network and the company networks, based on combinations of three defined

ANNEX F – INTERCONNECTION PLATFORMS IN VIGNETTE 2

waveforms NB (Narrow Band), MB (Medium Band) and WB (Wide Band) with different settings of bandwidth W , data rate R and radio system gain G_{sys} :

- Waveform NB: $W = 25$ kHz, $R = 17.5$ kbit/s, $G_{sys} = 156$ dB;
- Waveform MB: $W = 250$ kHz, $R = 175$ kbit/s, $G_{sys} = 146$ dB; and
- Waveform WB: $W = 1.25$ MHz, $R = 875$ kbit/s, $G_{sys} = 139$ dB.

Furthermore, the waveforms can be used on different frequency bands:

- 50 MHz; or
- 300 MHz.

As the used frequency band is important for the performance, we both analyze the case that the inter-company network uses the lower frequency band (50 MHz) and the higher frequency band (300 MHz). The waveform NB is only used for the inter-company network and at the frequency band 50 MHz. The waveform MB is analyzed for the inter-company network both at 50 MHz and 300 MHz. The company network uses either MB or WB at the 300 MHz band. In total, 6 system options are investigated.

F.4 RESULTS

Figure F-1 and Figure F-2 show how the connectivity varies over time for the different network combinations in case of two and four ICPs per company, respectively. For example, almost full connectivity is reached during most of the test period by using four ICPs and the waveform MB at 300 MHz for the inter-company network. In the end of the test period, however, the connectivity drops considerably. In Figure F-3 the average connectivity over the 1000s long segment of Vignette 2 for different number of ICPs is shown.

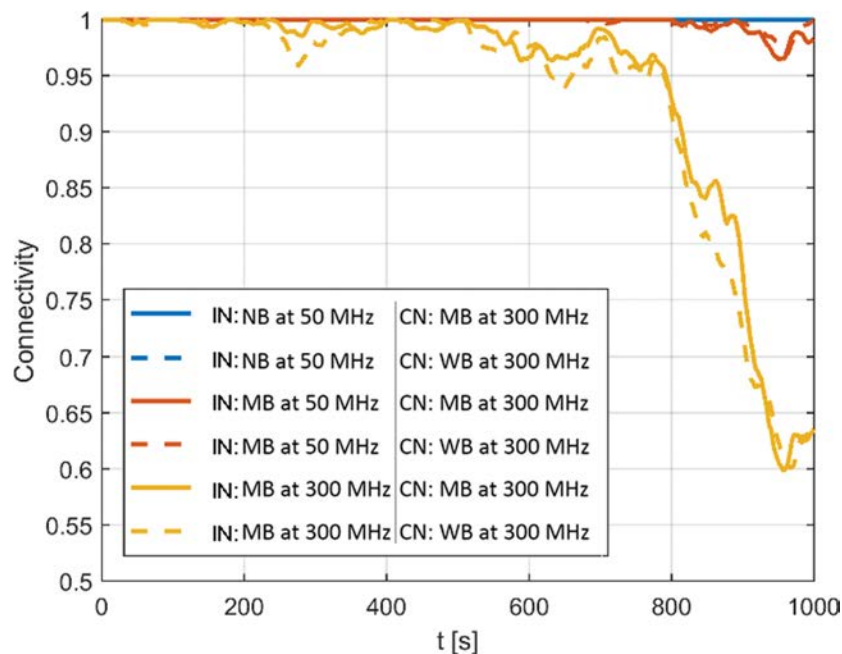


Figure F-1: Connectivity with Two ICPs Per Company for the Different Cases with Inter-Company Network (IN) and Company Network (CN) Based on the Three Waveforms, NB, MB and WB.

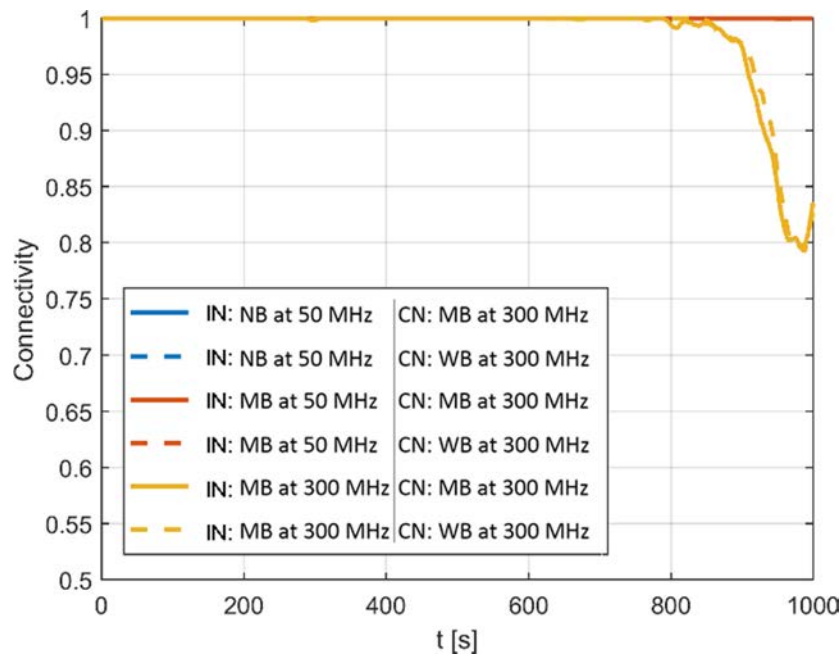


Figure F-2: Connectivity with Four ICPs Per Company for the Different Cases with Inter-Company Network (IN) and Company Network (CN) Based on the Waveforms, NB, MB and WB.

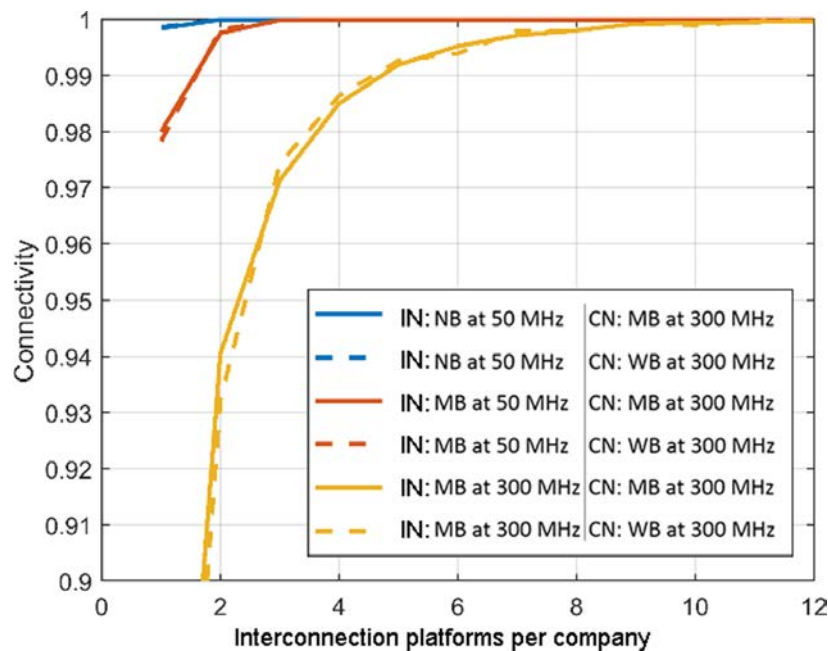


Figure F-3: Average Connectivity for Different Number of ICPs Over the Whole 1000 Second Test Period, for the Different Cases of Inter-Company Network (IN) And Company Network (CN) Based on the Waveforms, NB, MB and WB.

For the company network, the waveform WB is preferred as it has the highest data rate. The connectivity is only marginally improved if the waveform MB is used instead. The appropriate solution for the inter-company network depends on the required data capacity for communication between the companies.

As can be seen, by using the waveform NB, good connectivity is obtained, and it is sufficient with one ICP node per company. Unfortunately, the low data rate limits what can be sent between the companies considerably. Using the waveform MB at the 50 MHz band is an option but it is questionable if 250 kHz of bandwidth can be made available at the 50 MHz frequency range. The main option is therefore to use the waveform MB at the 300 MHz band for the inter-company network. For this case around 4 – 6 ICP nodes per company is needed as well as an efficient routing functionality that are able to discover the necessary paths to connect the inter-company and company networks. Note that the time interval of Vignette 2 that we chose for analysis has a fairly well-connected network for most of the time period. In other scenarios, other number of ICPs may be required. Also, in some cases it may not be possible to connect the company networks at all with the waveforms MB or WB.

F.5 REFERENCES

- [1] Suri, N., Hansson, A., Nilsson, J., Lubkowski, P., Marcus, K., Hauge, M., Lee, K., Buchin, B., Mısırlıoğlu, L., and Peuhkuri, M., “A Realistic Military Scenario and Emulation Environment for Experimenting with Tactical Communications and Heterogeneous Networks,” Proceedings of the 2016 International Conference on Military Communications and Information Systems (ICMCIS), Brussels, 2016, doi: 10.1109/ICMCIS.2016.7496568.
- [2] Marcus, K., Barz, C., Kirchhoff, J., Rogge, H., Nilsson, J., in’t Velt, R., Suri, N., Hansson, A., Sterner, U., Hauge, M., Lee, K., Holtzer, A., Buchin, B., Peuhkuri, M., and Mısırlıoğlu, L., “Evaluation of the Scalability of OLSRv2 in an Emulated Realistic Military Scenario,” Proceedings of the 2017 International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, 2017, doi: 10.1109/ICMCIS.2017.7956503.
- [3] Suri, N., Nilsson, J., Hansson, A., Sterner, U., Marcus, K., Mısırlıoğlu, L., Hauge, M., Peuhkuri, M., Buchin, B., in’t Velt, R., and Breedy, M., “The Angloval Tactical Military Scenario and Experimentation Environment,” Proceedings of the 2018 International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, Poland, 2018.

Annex G – OSPF SCALABILITY

Jimmi Grönkvist and Anders Hansson

Swedish Defence Research Agency (FOI)
SWEDEN

G.1 INTRODUCTION

Open Shortest Path First (OSPF) is one the most widely used interior Gateway Protocols (IGP) in the Internet. The purpose of this annex is to determine whether OSPF can be used as the overall IP-routing protocol for military tactical communication. An advantage with a large OSPF domain instead of several smaller, is that reconfiguring the connection of groups of nodes from one point in the network to another is easier. Also changes in network structure can be handled automatically, at least for unicast traffic. However, there are questions on whether using OSPF is possible for tactical waveforms due to their low data capacity.

We study the feasibility of using OSPF in the tactical domain by calculating how much overhead OSPF would generate in a typical battalion network. The overhead cost is then compared to the typical data capacity of a wideband tactical waveforms. Overhead is calculated for each type of message that is used by the OSPF protocol. In the calculations, some parameters are given, such as the number of nodes in a battalion and the typical data capacity of a waveform. In some cases, parameter values had to be estimated, for example the choice of some OSPF parameter settings. Other parameter values are based on results from earlier simulations, for example the stability of a radio connection for nodes moving in the terrain. The reason for estimating the overhead with the help of calculations rather than just simulating the traffic is primarily because there are no accessible simulators that both have good models of OSPF with MANET extensions as well as good models of military tactical waveforms in realistic terrains. Using the more commonly available models based on WLAN techniques and simplified path links will not give realistic results.

G.2 TACTICAL WAVEFORMS

A number of different types of radio networks are used for battalion communication. The two most relevant types of radio networks in a military battalion communication system are the wideband waveform and the narrow band waveform. We focus on the wideband waveform, because it is most suitable in a heterogeneous network. The wideband waveform is the primary waveform for battalion control. We assume that a single radio network is used to cover the entire battalion (or at least most of its vehicles as not all logistics vehicles may need all information). We therefore assume the waveform needs to handle at least 140 mobile nodes and cover a rather large area. In addition to these two types of networks there are other networks as well, but with a topology that is quite stable from an IP perspective and generate little overhead in the rest of the OSPF domain, so they are not considered further. The capacity in a wideband network is expected to be around 500 kb/s to 1 Mb/s, shared between the different applications.

G.3 DIFFERENT ROUTING ARCHITECTURES

In this annex, we describe the overall routing assumptions. We study an OSPF domain with a single OSPF area within an Autonomous System (AS), which allows us to ignore traffic from other OSPF areas. We study OSPF usage in two of the architectures described in Annex E: “Routing Architecture Considerations for Heterogeneous Tactical Networks”, the flat architecture and interconnect-overlay architecture.

G.3.1 Flat Architecture

In the flat architecture, we assume that OSPF is the routing protocol used in a single routing protocol domain handling all routing decisions. Multiple radio networks (network segments) may be a part of the routing domain, but here we are primarily studying traffic inside a single network segment covering the wideband battalion network.

Using the flat architecture, all routing functionality resides on layer three, including the ad hoc routing. This means that all link changes need to be handled by the OSPF protocol as all changes in the radio network are visible to the IP network. Figure G-1 shows the nodes in a single network. The links that exist at layer two and the links that are known to the layer-three protocol are indicated. We assume that the layer-three protocol has knowledge of the actual links at layer two. Some of the nodes are also part of other networks, as indicated by the dashed lines. In this setup, a radio is just used as a link to other radios. It is the tactical router (running OSPF) that the radio is connected to, that makes all the routing decisions. The router gets information from the radio about the link quality of its neighbors through a router to modem interface (called Information Exchange Interface – Modem (IEI-M) in Annex E. Link quality is here used in a wide sense, so it may include different parameters used to set the cost of the link, like data rate and load. The flat architecture can be seen as the default architecture for the design of OSPF with MANET extensions (see Refs. [1] [2] [3]).

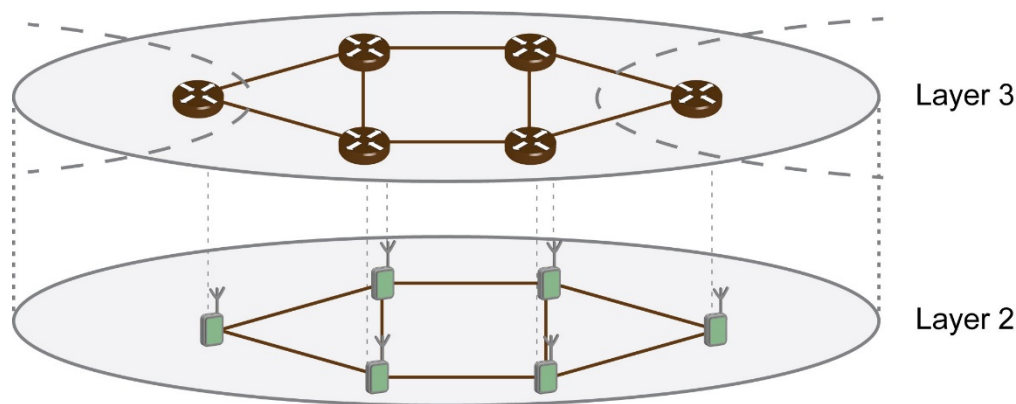


Figure G-1: Single Layer-Three Routing Protocol.

G.3.2 Interconnect-Overlay

In the interconnect-overlay architecture we assume that OSPF is used in the virtual overlay network layer, potentially covering several different networks segments. In order to simplify the local behavior of the battalion radio network segment, we assume that all internal routing functionality within the battalion radio network is located below layer three. We thereby do not need to consider tunneling cost and the network performance will be more predictable, at least for cooperative broadcast networks [4].

Some routing functionality is required on layer three in all nodes. We assume that all nodes in the battalion network segment are part of the overlay network. Therefore, OSPF is used in all tactical routers in the battalion. Because all relaying within the radio network is hidden from the IP-layer, details of the actual links are hidden from the OSPF routers. In this case, the MANET-interface primarily behave as a broadcast interface capable of handling different costs to the different nodes (due to for example hop lengths) and being capable of handling network fragmentation. This means that a message may be relayed by several radios in order to reach the destination, but to the higher layers the topology is presented like a fully connected 1-hop network. This concept is similar to the use of bridges and switches for Ethernets. The difference between the links at layer two and the visible links at the layer-three level is illustrated in Figure G-2.

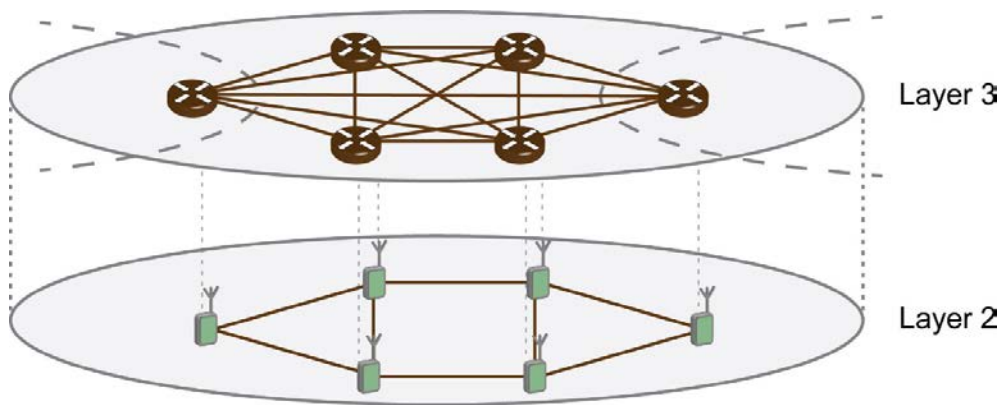


Figure G-2: Single Layer-Three Routing and MANET Routing on Layer Two.

Network fragmentation (and reassembly) is the primary change that is visible on layer three, which is caused by mobility. The interconnect-overlay architecture may require some changes of the current standards to become efficient, which is discussed in the separate message sections. The layer-two routing cause overhead traffic as well, but we do not evaluate that overhead here because the implementations are usually proprietary and difficult to analyze.

G.4 SOME CENTRAL TERMS OF OSPF

G.4.1 OSPF Areas

OSPF divides its routing domain into areas, where each area maintains separate link state databases. Within an area all routing information is flooded to all routers, while between areas route information may be summarized to reduce signaling. We focus on a single OSPF area because only changes within an area can be fully handled automatically by OSPF. The size of the OSPF area is assumed to be equal to the size of the wideband waveform network of 140 nodes.

G.4.2 Link State Advertisements

Link State Advertisements (LSAs) are used in OSPF to communicate the routers' local topology to the rest of the network. All LSAs taken together is used to form the link-state database which is used for calculating the minimum cost path to all nodes in the network. An important goal of OSPF is to ensure that all nodes have the same, updated, collection of LSAs, and therefore the same description of the network topology. There are a number of different LSA types that are used to describe different types of networks, nodes and OSPF area properties, e.g., a router LSA gives details on the node that is sending the LSA, and lists all or some of the neighbors of the sending node depending of the interface.

G.4.3 Adjacencies and Interfaces

An OSPF router does not necessarily exchange routing information with all its neighbors. Instead, the data base of a node is only synchronized with a subset of the neighbors. This subset of nodes is designated as adjacent. In order to become adjacent, the nodes, among other things, exchange copies of their link-state databases. Which nodes that chooses to become adjacent is primarily dependent on the type of attached network on an interface, as database synchronization may become inefficient on networks with many neighbors. Therefore, on broadcast interfaces database synchronization only occurs with a small subset of the nodes, for efficiency reasons. It is done by selecting one of the nodes as a designated router. All other nodes set up adjacencies with the designated router, thus reducing the signaling to an amount that is linearly

proportional to the number of nodes. In addition, the routers on the broadcast network only need to report the designated router (and a backup) in their router LSAs, which considerably reduces their size.

However, on broadcast interfaces all nodes are expected to receive from all other nodes. If that is not the case (such as in a MANET) point-to-multipoint interfaces can be used instead. In this case, designated routers cannot be used, and all nodes must be reported in the router LSAs. MANETs behave as point-to-multipoint interfaces but the rapid changes require a more efficient solution. In the MANET extensions, described in [1] [2] [3], to OSPF, efficiency improvements are:

- Reduction on the number of created adjacencies;
- More efficient neighborhood detection; and
- More efficient LSA flooding.

Both layer-three and layer-two solutions need to use IP MANET interfaces. The MANET interfaces are required because networks can fragment, and any set of nodes may end up in any fragment. This type of fragmentation is something that the standard OSPF interfaces have difficulties in handling efficiently. We assume that using MANET interfaces means that the OSPF traffic is IPv6. It may be possible to use OSPFv3 over IPv4 for IPv6 transitions [5]. In that case, all packets have 20 bytes less overhead than we assume in our assessment.

There are currently three suggested (experimental) OSPF standards for MANET: OSPF-MPR [1], OSPF-MDR [2], and OSPF-OR [3]. They differ in the details but in Refs. [6] and [7] it is shown that OSPF-MDR have the least overhead of the three algorithms, less than a fourth compared to OSPF-OR for large networks. Therefore, we use OSPF-MDR in the analysis.

G.5 OSPF OVERHEAD ANALYSIS IN A FLAT ARCHITECTURE

To assess the flat architecture, we think it is sufficient to refer to the results from Refs. [6] and [7], although the simulation results in these publications are performed only for a single radio network. No specific values for 140 nodes are given in Refs. [6] and [7] but rather for 120 and 160 nodes. For a dense network the total OSPF overhead is between 247kb/s and 418 kb/s and for a sparse network 347kb/s and 573 kb/s. A comparison of overhead for OSPF-MDR [2], OLSR [8] and composite routing is performed in Ref. [9] for smaller networks (up to 40 nodes). The comparison gives overhead values that are very high for a system with data rates between 500 kb/s and 1 Mb/s. So, it cannot be expected to be functional, especially because the simulation results are based on quite simple propagation models with fixed range and no terrain effects.

We see that rapid topology changes in a battalion network cannot be supported by OSPF in a flat architecture due to the high signaling overhead, especially if we also consider all the additional networks that generate OSPF signaling. Other protocols at layer three (for example OLSRv2) may perform better as they do not use all of the mechanisms of OSPF, such as data base updates and acknowledgements.

G.6 OSPF OVERHEAD ANALYSIS IN AN OVERLAY NETWORK

In this annex, we study the OSPF overhead in terms of signaling that occur when OSPF is used in an overlay network. For simplicity, we focus on OSPF-MDR, but we do not know whether MDR generate the least overhead of the three extensions also in a single hop network.

G.6.1 Background Assumptions

OSPF-MDR use a Connected Dominating Set (CDS) in order to reduce both the nodes that flood LSAs in the network and to reduce the number of adjacencies as links between non-CDS nodes are not considered adjacent. This is done by generalizing the Designated Router concept from broadcast networks to a CDS consisting of a

subset of nodes called MANET Designated Routers (MDR). In the same way, the backup designated routers are generalized to a subset of nodes called Backup MDRs (BMDR). Also, mechanisms are used to avoid changing MDR or BMDR nodes whenever possible, thereby further avoiding adjacency changes.

For a flat architecture OSPF-MDR [2] is appropriate to use, but for an overlay network an update to OSPF-MDR is better used, see RFC 7038 which describes its use in broadcast networks [10]. One of the purposes of RFC 7038 is the use of OSPF-MDR over layer-two routing, but allowing different costs to different nodes due to, for example, different number of (layer-two) hops to (layer-three) neighbors. We assume that the lower layer is capable of detecting link changes and that there is an information exchange interface that delivers layer-two information to layer three when the network is fragmented (nodes lost) or when new nodes appear within the network. Furthermore, we assume that the layer-two reaction to link changes is fast, and do not require fast retransmission of Hello messages. Signaling can be caused either by link changes, or by updates that occur regularly.

The idea of using an overlay network is to hide irrelevant information from OSPF so that rapid changes within single networks do not propagate to other networks nor unnecessarily triggers OSPFs database updates. With the overlay architecture there are fewer changes than with the flat architecture. As mentioned, the changes that are visible to OSPF are when the networks fragments or re-assembles. It is important that the network converge rather quickly after such changes. Otherwise, traffic might not be able to reach its destination even if the node is reachable on the lower layers. Studying results from Section 4.2 in Ref. [11] (with results based on the topology in Vignette 2 in the Anglova scenario) we see average time spans between fragmentations on the order of a hundred seconds. If updates take so long time, there is a risk that OSPF never converge. Detection of link breaks usually takes several seconds though, which limits how short we can make OSPF updates. In the analysis, we set an update requirement of 10 seconds after the lower layers report changes, in that way the OSPF network is synchronized at least for a large part of the time.

In the following four sections, we calculate the total IP packet size of different OSPF message types based on RFC specifications of message header and other message parts. From the message sizes and the number of transmissions, we then analytically estimate the signaling overhead.

G.6.2 Hello

Hello messages are sent to keep track of neighbor relationship. With efficient use of information from the radio, it should be possible for the routers to only send needed information in Hello messages. On layer three, topology changes are rare, so the OSPF Hello messages are almost empty and must not be transmitted frequently. The Hello messages are flooded through the network, not just sent to neighbors, because all network nodes are OSPF neighbors. When a fragmented network reconverges, all (virtual) links between the fragments are recreated, i.e., all nodes in both fragments see new links to all nodes in the other fragment more or less at the same time. Because the Hello message information is used to select MDRs, it usually contains information on all neighbors. In this case, the Hello message size is 644 bytes and if all nodes transmit these messages, more than 90 kB are flooded through the network before any new adjacencies can be created. Assuming four retransmissions on layer two [4] means that more than 2.8 Mbits are transmitted by the link layer every time the network reconverges.

The amount of Hello traffic can, however, be reduced, because the network is always fully connected and the only necessary topology information for appropriate routing decisions is which nodes that are MDRs and BMDRs in the different partitions. This information is contained within differential Hello messages that are used for reporting new links. With these differential messages, the total amount of data is much lower. Assuming a group of ten nodes reconverging with the network, the Hello message size is 23 kB. A greater modification to RFC 7038 would be that only links to and from the MDRs and BMDRs are included in the updates, in which case the Hello message size is less than 3 kB. It is important that the information from the radio triggers the Hello message transmission so that the (empty) differential Hello messages are sent rarely.

Otherwise, if Hello messages are sent every two seconds, the total end-to-end signaling overhead is 4 9kb/s. With four retransmissions on layer two, we get nearly 200kb/s transmitted data, which is expensive even for a wideband waveform.

G.6.3 Database Description Messages

There are probably much fewer nodes that are MDRs in an overlay network than in a flat architecture. Using the standard for single hop networks for MDR (RFC 7038 [10]), a single MDR and two backup MDRs are chosen. In a static network this should lead to a similar situation as for a broadcast network, which have a designated router and a backup designated router, except that we get two backup routers here. Mobility complicates this simple picture, though. If a small part of the network (e.g., a group or platoon) is fragmented from the main network it is likely that all MDRs and BMDRs remain in the main partition. The separate partition therefore chooses new MDRs and BMDRs locally. The overhead cost of this fragmentation is local but involves $3(m-2)$ database updates within the partition, where m is the number of nodes in the partition. As each such update may be more than 22 976 bits, a group of 10 nodes breaking away from the main network therefore need to transfer more than 550 kb in database description information to create the new adjacencies.

When the group re-merges with the main network these local adjacencies are most likely removed, and the group therefore reform adjacencies with the original MDRs and BMDRs. Then $3m$ database updates is required, each of size 22976 bits, resulting in at least 689 kbit data transfer. Whether the database updates are challenging for the network or not, depends on the delay requirements. With a delay requirement of 10 seconds, the database update requires a data transfer rate of 69 kb/s, which is expensive as it may be sent over multiple radio hops.

G.6.4 Router LSA

As a first alternative, we study the case when all of the bidirectional neighbors are included in a router LSA, which is required to correctly calculate the path costs for nodes further away. For the overlay network we have 139 neighbors in a single router LSA, i.e., at least 18464 bits (ignoring other interfaces). If the networks become partitioned all nodes need to update their router LSA. In order for the network to react reasonably fast to changes (at least in the local network) we need higher data rates. A reaction time of 10 seconds require 260 kb/s in signaling, which is too high. We therefore conclude that including all neighbors in router LSAs isn't possible.

As a second alternative, we include fewer nodes in the LSA. The minimum number to send would be the adjacent nodes, i.e., minimal LSA. In such a case, only the nodes losing (or creating at re-merge of network) adjacencies would need to generate new router LSAs, i.e., primarily the MDRs and BMDRs. If a smaller group partitions from the network (e.g., 10 nodes) and none of the MDRs or BMDRs is included in the group, all nodes in the smaller partition generate new (small) router LSAs and the three old MDR/BMDRs generate new (large) router LSAs. For a 10 seconds reaction time we get the following amount of traffic:

- Three old (B)MDR: $17184 \times 3/10 = 5155$ bits/s.
- Three new (B)MDR (in small partition): $1696 \times 3/100 = 547$ bits/s.
- Seven others: $928 \times 7/100 = 739$ bits/s.

The total end-to-end signaling overhead is 6.4 kbit/s. A wideband waveform can probably handle this amount of overhead, even if it is retransmitted several times. We should however note that the information is flooded through the entire OSPF area.

G.6.5 LSA Acknowledgement

We consider the case when each node sends one message with the combined acknowledgements of all received LSAs. Furthermore, a maximum end-to-end delay requirement of 10 seconds is assumed for the

sent messages. If minimum size router LSAs are used, 13 LSAs need to be acknowledged in the fragmented network example described above. We assume that all 13 LSAs are acknowledged in one single LSA acknowledgement message which results in a message size of around 2528 bits. This number is an approximation because the amount is slightly less for some nodes, as nodes do not need to acknowledge their own LSAs. With this approximation and for a network of 140 nodes, a total of 353920 bits are injected into the wideband network. With the assumption that all acknowledgements are received within a maximum of 10 seconds, the resulting end-to-end signaling must be at least 33 kb/s. As this overhead traffic may be sent multi-hop within the network, the overhead may be even higher, which must be considered heavy even for a wideband network. A similar number of messages are sent out at a network re-merge, although at slightly different size.

G.6.6 Discussion and Conclusions on an OSPF Overlay Network

From the above-mentioned numbers, it is clear that the wideband waveform has trouble handling the OSPF signaling also in the overlay case, at least if the radio network is multi-hop. It is interesting to note that the most expensive message type is the Database Description messages and Acknowledgements of the LSAs, both of which are not used by other protocols such as OLSR.

G.7 USING ANOTHER ROUTING PROTOCOL IN MOST RADIOS

From the previous annexes we can see that neither solution work very well if they are used as is. We describe a method that may improve the efficiency while keeping the advantages of having the same standardized routing protocol everywhere. In the overlay network description above an OSPF router is used in every node in the network. In most radio nodes, however, there are only two interfaces connected to this router, a local LAN and the wideband waveform radio leading to very simple routing decisions, which do not normally need as complicated protocol as OSPF. (Technically, there are normally more radio systems available in the node, but often these are narrow band systems with very limited capacity designed for very different purposes and not useful in a heterogeneous network, at least not as transit networks.)

Therefore, a third option is where OSPF routers are only used in nodes that have access to other high data rates communication systems. This configuration is currently only expected in interoperability platforms. The rest of the nodes can instead use a simplified protocol on layer three, that inform the OSPF capable nodes which network they have on the local LAN and route information to and from the local LAN. The OSPF capable router need on the other hand to run two separate routing protocols, potentially over separate virtual LANs one containing all nodes in the radio network and the other only the OSPF capable nodes. The simplified routing protocol can then be used to inform OSPF on accessible LANS through the radio network and take information from the OSPF overlay so other nodes can elect proper gateways into the OSPF overlay network. This third option is in practice only available for an overlay architecture. Because nodes without OSPF routers relay packets on layer two, the total connectivity of the network does not decrease (unlike a layer-three solution which would be significantly less connected).

G.8 CONCLUSIONS

We assess the use of OSPF in tactical networks, in terms of the amount of overhead that OSPF generate when a tactical wideband waveform is part of an OSPF. In order to do this, we analyze two different types of routing architectures, flat architecture and interconnect-overlay. In the first architecture, OSPF handles all changes in the ad hoc networking waveforms. This setup most closely follows the OSPF standard, with the drawback that all changes in the radio networks, primarily the wideband waveform, are visible to the entire OSPF domain, (that might also include low capacity waveforms). In the second one, interconnect-overlay, most of the rapid network changes are hidden from OSPF by using forwarding and routing below the overlay. We note that for both of the overlay architectures there is also a need for standardized Information

Exchange Interfaces (IEIs) that provide an interface for the necessary information flow between the routing protocols at the different layers.

From the results we can conclude that a flat architecture only using OSPF is generating too much signaling to be feasible for use in a large tactical network with a wideband waveform. We also see that an overlay network generates a high signaling load, although less than what is the case with a flat architecture. Further modifications of OSPF are required before it can be used over a tactical wideband waveform with 140 nodes.

Finally, we also discuss an alternative that only use OSPF in the few nodes that have more than one high capacity radio system. The rest of the nodes use a more optimized protocol that generate less overhead. This may lead to less overhead but there are practical issues that needs to be studied further as it may require some changes to the OSPF standard.

G.9 REFERENCES

- [1] Baccelli, E., Jaquet, P., Nguyen, D., and Clausen, T. “OSPF Multipoint Relay (MPR) Extension for Ad Hoc Networks”, *RFC5449*, IETF, 2009. Available: <http://www.ietf.org>.
- [2] Ogier, R. and Spagnolo, P. “Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding”, *RFC5614*, IETF, Aug. 2009. Available: <http://www.ietf.org>.
- [3] Roy, A. and Chandra, M. “Extensions to OSPF to Support Mobile Ad Hoc Networking”, *RFC5820*, IETF, 2010. Available: <http://www.ietf.org>.
- [4] Komulainen, A., Grönkvist, J., and Nilsson, J. “Comparing the Capacity of Cooperative Broadcast to Spatial Reuse TDMA in ad hoc Networks”, Proceedings International Conference on Military Communications and Information Systems (ICMCIS), May 2016.
- [5] Chen, I., Lindem, A., and Atkinson, R. “OSPFv3 over IPv4 for IPv6 Transition”, *RFC7949*, IETF, Aug. 2016. Available: <http://www.ietf.org>.
- [6] Ogier, R. “Comparison of OSPF-MDR and OSPF-OR”, *draft-ogier-ospf-manetmdr-or-comparison*, IETF, Sep. 2010. Available: <http://www.ietf.org>.
- [7] Ogier, R. “Comparison of OSPF-MDR and OSPF-MPR”, *draft-ogier-ospf-manetmdr-mpr-comparison*, IETF, Sep. 2010. Available: <http://www.ietf.org>.
- [8] Clausen, T. m.fl. “The Optimized Link State Routing Protocol Version 2”, *RFC7181*, IETF, 2014. Available: <http://www.ietf.org>.
- [9] Fang, J., Goff, T. and Pei, G. “Comparison Studies of OSPF-MDR, OLSR and Composite Routing”, Proceedings *IEEE MILCOM*, 2010.
- [10] Ogier, R. “Use of the OSPF-MDR in Single-Hop Broadcast Networks”, *RFC7038*, IETF, Oct. 2013. Available: <http://www.ietf.org>.
- [11] Örn Tengstrand, S., Hansson, A., and Grönkvist, J. “Routing Architectures for Heterogeneous Networks”, *FOI-R-4133-1942*, Swedish Defence Research Agency, Nov. 2015.

Annex H – NAVAL TASK GROUP AND ROUTING EXPERIMENTS

Levent Misirlioglu and Taner Kurtulus
MilSOFT Yazilim Teknolojileri A.Ş
TURKEY

H.1 OPERATIONAL CONTEXT FOR THE NAVAL SCENARIO

The naval task group scenario covers information exchange through heterogeneous tactical IP networks among a coalition naval task group and shore-based commanders for military operation in the Anglova scenario. The scenario and tools are described in:

- Annex A: “Operational Perspective for IST-124”;
- Annex B: “Emulation based experimentation and the Anglova Scenario”;
- Annex C: “Experimentation Environment and Tools”; and
- Annex D: IST-124 “Experimentation execution”, of this report and also in Refs. [1], [2], and [3].

H.1.1 Precondition

One Task Group is formed under the tactical command of an OTC (Officer in Tactical Command) along the coast of Anglova. The Task Group is under the operational control of Fleet Commander / Maritime Interdiction Force (MIF) Commander located in Coalition Head Quarters. The Task Group consists of one command ship holding the flag officer and 20 surface combatants. There is also one multipurpose helicopter, which will carry on MEDEVAC duties, within the Task Group.

The individual ships have basic radars, AIS (Automatic Identification System) and ESM (Electronic Support Measures) systems connected to their C2 (Command and Control) systems. The basic task of the Task Group is to conduct Surveillance and Reconnaissance missions within their responsibility area. In addition, NATO authorities ordered to employ Maritime Interception and Interdiction Operations to control the flow of arms and goods into and out of the “Anglova” country. Each of the task units perform operations within LOS of at least one other ship in order to utilize Line of Sight connectivity with the group, so that they can take advantage of V/UHF frequency band for communications. But there are sometimes inevitable positional displacements due to movement, or as the operational situation dictates; Command Authorities may order detachment of small groups under the tactical control of superior ranking commander of the detaching units for missions like patrols, search and rescue, reconnaissance missions, investigating and boarding of suspected ships, etc. In these situations, there is still a need for continuation of connectivity with HF frequencies or airborne assets to be used as relays.

The individual ships report their contacts and themselves to OTCs and other units. The group combine local pictures coming from each unit to form a Common Tactical Picture (CTP).

Individual ships also share their position and important contacts with shore as well. Normally the distances the ships perform these operations are Beyond Line Of Sight (BLOS), therefore HF frequencies or airborne relays will be used to exchange information. As expected the throughput and capacity of HF frequencies are lower than the UHF frequencies, therefore some Intelligent Tactical IP Router capability by using QoS mechanism in terms of priority, reliability and perishability, etc. is required.

ANNEX H – NAVAL TASK GROUP AND ROUTING EXPERIMENTS

Typical information exchange requirements for the Task Group are as follows:

- Blue force tracking picture.
- Local Tracks / Contacts (of merchant vessels, boats, yachts, etc.).
- Common Tactical Picture / Recognized Maritime Picture (with suspect vessels, Contacts Of Interest (COIs)).
- Text chat for coordination issues.
- E-mail and file transfer to exchange pictures, plans, etc.
- Typical Data Properties.
- Assuming a total of 250 tracks within the surveillance area, number of tracks per ship: 10 – 15.
- Size of track data:
 - 18 bytes every 12 seconds;
 - 27 bytes over each 96 seconds for air tracks; and
 - 18 bytes per 96 seconds for surface tracks.
- Size of drop track report: 9 bytes (expected roughly 5 drop tracks per minute).
- Size of free text: 250 characters long (10 messages per minute per ship can be considered).
- Size of e-mails: 100 Kb average every 20 minutes.
- Tactical track data for real time tracks has a life span of two minutes.

On all nets track with Contact of Interest (COI) statuses and initial report of suspect vessels are first priority. Periodic reports of suspect vessels and blue force information and OTC / Fleet Commander orders are the second priority.

COIs and initial report of suspect vessels and command orders along with their acknowledgements are serviced with guaranteed delivery. Ships reach out to HQ periodically to report their positions; equipment status and important contacts are also serviced with guaranteed delivery. Operators may assume the delivery method of e-mails while preparing it. The rest of the information is best effort.

Typical Services and Network Requirements for this scenario are as follows:

- Each OTC Task Group / separated group shall work on his/her own Mobile Ad Hoc Network (MANET) preferably with UHF frequency in order to utilize UHF frequencies advantages.
- 8 of the ships, MEDEVAC and HQ have HF MANET besides UHF MANET in order to perform data exchange among headquarter, OTC / Tactical Commanders, and with the rest of the Land Forces who are present in the Anglova scenario. Also the individuals who have no connection otherwise may use this MANET to communicate through routing as a backup link.
- Since the topology changes frequently, a layer 2 routing/relay capability inside the MANETs is required.
- Tactical Information routing between HF and UHF MANETs requires a layer 3 Intelligent Tactical IP routing capability.
- These MANETs should automatically organize themselves to adhere to frequent topology changes.
- End-to-end IP connectivity shall be an effective way of communications even when the detachment group switch over to HF MANET, still paths exists with the same addressing schema to send their information to their destinations independent of the network or frequency band they are in.

- IP Header Compression and TCP optimizations are selectively employed.
- Units employ a dynamic time division multiple access MAC protocol to satisfy their needs for varying payloads.

Sequence of events of the Navy through Vignette 2/3 of the Anglova scenario:

- Task Group sailed away under the command of OTC (Officer in Tactical Command) from the shore to conduct Surveillance and Reconnaissance mission. UHF MANET among each unit in the Task Group and HF MANET with the capable units are automatically established.
- Scenario starts with a topology that each ship is reachable within at most 5 hops of every other unit to test UHF MANET connectivity. HQ is away, so that communication is only possible through HF MANET and via layer 3 routing.
- Blue picture is formed automatically since the unit reports their position frequently through MANET. Units exchange their tracks and inform HQ with summary reports. Units also use text chat / free text messages for coordination purposes.
- Units in the force detect targets with its primary radar. With the help of AIS and ESM information classifies the targets and report contact information to the other units.
- Topology changes occur due to movements of the ships, the MANET's will adapt to those changes.
- One of the eastbound units locates a group of targets far away from the friendly Task Group, moving together as a convoy with suspicious appearance. Course and speed and AIS information are reported to the OTC using UHF MANET. The contacts are initially reported with suspect vessel identity.
- OTC orders a small task group consisting of one command ship with helicopter capability and four fast patrol boats to form a MIF (Maritime Interdiction Force) group to investigate and if required, boarding and searching of the targets.
- The commander on the departing command ship now called On Scene Commander (OSC) departs away eastwards with his MIF group from the rest of the task force to investigate while keeping up the connectivity with the OTC and the other remaining ships through HF MANET and routing.
- The OTC also tasks MEDEVAC Helo to take off from one of the westbound ships and sail to the MIF Command Ship in order to be prepared for any emergency call from the land forces and improve communication connectivity between the two separate groups.
- The Task Group arrives near suspect targets and positively identifies the tracks as Contact of Interest (COI) tracks and reports this message to the headquarter, OTC and rest of the fleet with a first priority message.
- The OSC also takes a photograph of the convoy using day camera and e-mails this photo to the OTC in order to give a positive indication to their identification. The e-mail goes through the network with a lower priority.
- The OTC/headquarters then takes necessary actions against the COI tracks and sends their orders with a guaranteed delivery to OSC.
- The MEDEVAC Helo lands on deck of MIF Command ship, and the MIF group takes formation one to enter into the harbour of Anglova, while the rest of the Task Group continues on the Surveillance Task.
- The MEDEVAC Helo takes off again to answer an emergency call from the Land Forces and lands in the designated helipad.

H.2 TOOLS AND UTILITIES GENERATED TO CONDUCT EXPERIMENTS

We have produced some utility programs to execute experiments on the EMANE [4] environment. The details are given in Annex C.7.

H.3 EXPERIMENTATION

H.3.1 Operational Concept and Scenario Overview

Although the Naval Component Scenario is generated for both Vignette 2 and Vignette 3 of the Anglova scenario, the experiment described in this annex is conducted for a two hour period of Naval Operation under Vignette 2, since this part includes the most interesting topology changes, separation of task forces and using an airborne relay to improve connectivity.

An IP-Based Ad Hoc Network Controller product based on STANAG 4691 [5] is tested during this operation. This product is planned to be used on V/UHF and HF networks and use of standard routing protocols among platforms employing V/UHF and HF frequencies for IP based communication is foreseen. The typical operational concept description which is defined in the scenario below is also depicted in the figure below (Figure H-1).

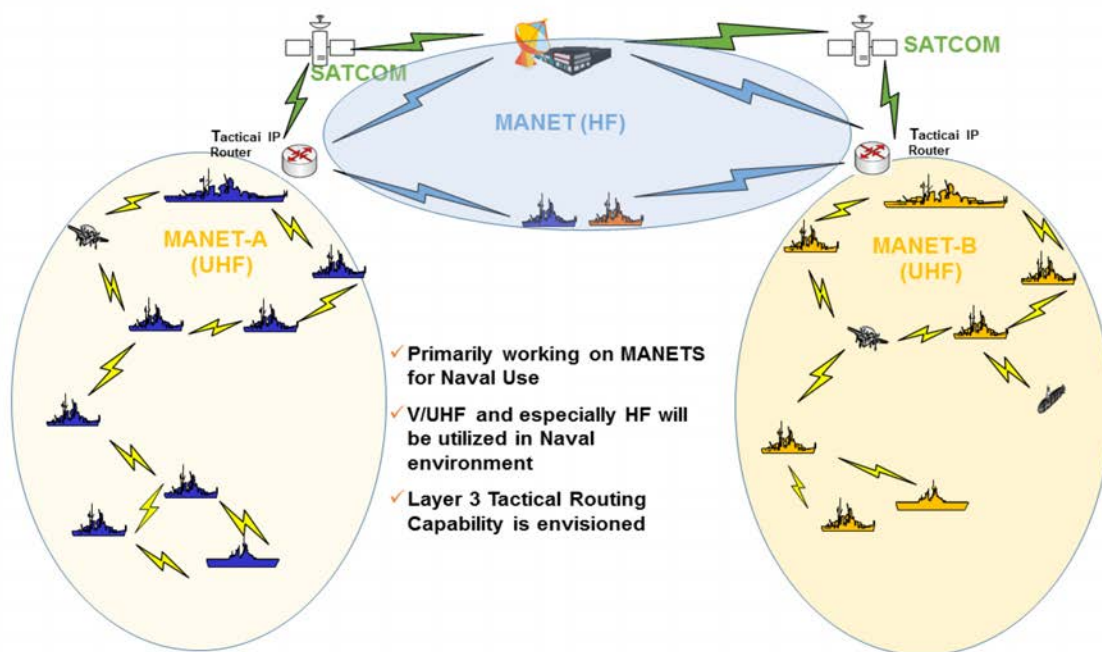


Figure H-1: Operational Concept of MARLIN Implementation.

The STANAG 4691 recommends MARLIN to be used by at most up to 16 platforms. In this experiment we have used an interesting topology to test the system in some sort of worst case condition. We have employed a total of 23 platforms, 8 of them have dual systems. The initial composition of naval units forms a topology that make use of 5 hop distance for most of the ships located in “edge” locations, to communicate with their farther-most counterparts topology changes at the initial stage occur within the UHF range, when the groups are separating the MEDEVAC Helo is made airborne to improve connectivity. There are also some units making late entries to the main networks.

For V/UHF and HF frequencies we have assumed to use the following waveforms:

- Waveform V/UHF: @25 kHz, 64 kbit/s; and
- Waveform HF: @3 kHz, 4 kbit/s.

H.3.2 Experiment Conducted for Tactical Track Dissemination

We have simulated tactical track exchange capabilities of the system. The specifics of the experimentation are listed below.

The naval part from Anglova scenario Vignette 2 is used. An overview is depicted in Figure H-2.

- Two hour scenario.
- 23 units participated (21 ships, 1 MEDEVAC Helo, 1 Shore Based Headquarter).
- 8 ships, 1 MEDEVAC Helo and 1 HQ have dual channels (both UHF and HF).
- Scenario starts with UHF connectivity through relays (except HQ).
- Topology changes occur only on UHF network. HF network is always connected.
- Two task groups depart from each other.
- At 40th minute MEDEVAC Helo is airborne to help to improve connectivity between the task groups.

OLSRv2 with MPR [6] is selected as the router between V/UHF and HF Network. The following configuration is used. In this setup “eth3” is the V/UHF MARLIN interface and “rtrcon” is HF MARLIN interface.

```
#
[global]
fork 1
plugin mpr
[interface=eth3]
hello_interval 90.0
hello_validity 450.0
ffdat_interval 20
[interface=rtrcon]
hello_interval 120.0
hello_validity 600.0
ffdat_interval 20
[neighbor_probing]
interval 90.0
[olsrv2]
ndhp_routable true
tc_interval 90.0
tc_validity 450.0
```

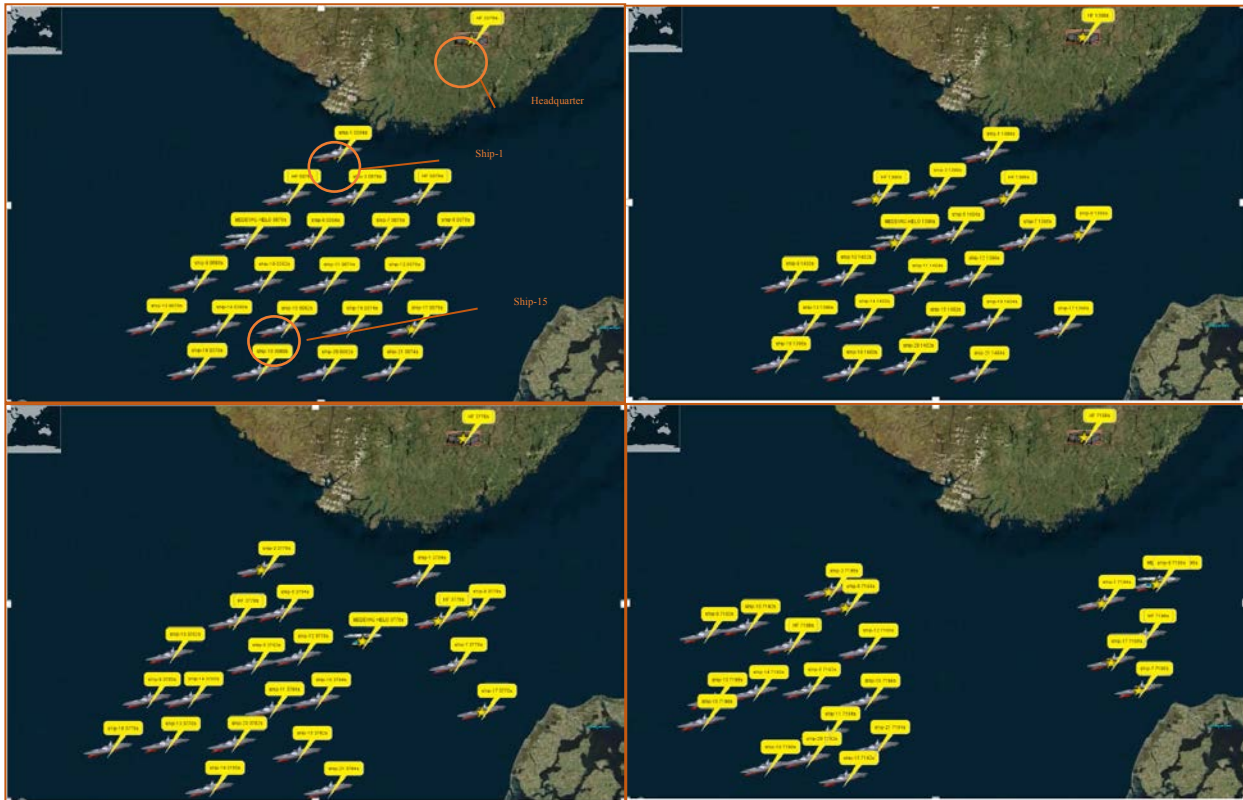


Figure H-2: Naval Component Vignette 2 Scenario Overview.

Main Objectives:

- We would like to measure the effectiveness of Tactical Track Exchange functionality on this relatively tough scenario.
- We will measure the average track delivery time and packet delivery ratio at the target.
- We have assumed the typical track stale time for such a Tactical Information Exchange System as:
 - Air Track stale time: 20 seconds.
 - Surface Track stale time: 2 minutes.
- A packet delivery ratio of 80 percent which is accepted as Standard Delivery probability of reception in Link 22 systems. But Link 22 is basically a 2 hop system. Since we are using MARLIN as a 5 hop system, achieving a PDR of 70% for more than 2 hops, is fair to consider as a success for this experiment sake.
- We would like to measure the benefits of airborne relay.
- And if any benefit is gained from our header compression implementation based on Ref. [7] (version 1.7.0).

Traffic Generation:

- Generated by the Multi-Generator (MGEN) tool:
 - Each node sends 200 bytes every 12 seconds in broadcast mode through UHF to simulate Track Exchange by using compact Link 22 track messages. Assuming basic track information via Link 22 can be expressed in 18 bytes, this corresponds to approximately 11 tracks per 12 seconds per ship.

- Each node sends 1000 byte every 96 seconds / 2 minutes through UHF to HQ to simulate track information summary.
- Since HQ is far away, routing is used to deliver that information through HF.
- Since broadcast traffic is not supported by routing protocol, broadcast traffic is distributed by underlying MARLIN implementation.
- Layer-3 routing is only used to deliver messages to HQ.

Measurement and Analysis Methods:

- The data is logged at the receiver. 3 receiver stations are selected for analysis:
 - Platform 1 is for broadcast data analysis, because of its unique position in the scenario as shown in Figure H-2 which can be considered as an edge unit for the network.
 - Platform 15 is also selected for broadcast data analysis to see the results from an intermediate unit in the network.
 - Platform 23 (HQ) is selected for p2p delivered messages.
- We have used trpr tool to extract statistics on latency.
- A simple grep function delivers the packet delivery ratio at the receiver site.
- We have generated a utility program to filter out messages delivered after the track is C, i.e., filter out the messages arriving after maximum track stale time.
- Excel is used for calculation and preparation of tables listed herein and gnuplot is used to draw Latency versus Time information.
- The experiments were conducted at least 7 times for both normal and header compression implementation. The results are averaged through all experiments.
- The results are analysed as overall (entire 2 hour period), and range (for 50 minutes duration after the Helo is airborne).

H.3.3 Measured Metrics**H.3.3.1 Broadcast Delivery Analysis at Intermediate Node (@ node-15) for Full Period**

For broadcast receive performance being an Intermediate Node, ship 15 performs very well with respect to surface track exchange requirements depicted in Table H-1. It can receive very high percentage (96.55%) of all broadcast traffic, and high percentage (84.30%) of it under 120 seconds. The PDR values varies essentially proportional to hop counts of the other nodes (nodes performing late entry such as node-17 is an exception in the Table H-1, as messages are stored and forwarded after network entry).

In the header compression experiments we see that average latency decreases from 24.39 seconds to 15.71 seconds (a 35.6% increase), at the cost of 17.46% decrease in the PDR performance. In this calculation we find the difference between the filtered PDR values for normal and header compression case and call it “significant loss”, although the packet loss between all packet cases is much higher (26.67%). Since Robust Header Compression (rohc) schema accommodates a certain amount of packet out of order reception, normally excessively late packets drops quickly. Therefore the percentage difference between all and filtered rohc packets is relatively low (2.85%). We believe that header compression case should be further investigated, with newer versions of the available library and perhaps better out of sequence packet reception recovery implementations, since the topology changes and broadcast delivery nature of the traffic suffer a lot from out of sequence reception.

ANNEX H – NAVAL TASK GROUP AND ROUTING EXPERIMENTS

Table H-1: Broadcast Delivery Analysis at Intermediate Node (@ Node-15) for Full Period.

Node	Average Latency (Seconds)					Packet Delivery Ratio (%)				
	Normal Operation		Header Comp Enabled		Latency Improvement Due To Header Compression	Normal Operation		Header Comp Enabled		Packet Loss Significant By RohC
	All	120 Seconds Filtered	All	120 Seconds Filtered		All	120 Seconds Filtered	All	120 Seconds Filtered	
10.102.0.1	59.31	31.16	25.18	18.73	39.89%	91.47%	75.75%	62.50%	60.58%	15.17%
10.102.0.2	62.73	29.54	19.69	18.24	38.26%	99.59%	83.56%	65.89%	64.90%	18.66%
10.102.0.3	56.77	31.90	19.31	15.46	51.54%	99.38%	84.38%	60.72%	59.01%	25.38%
10.102.0.4	54.60	29.90	22.94	16.48	44.89%	90.14%	75.24%	61.54%	59.52%	15.72%
10.102.0.5	48.67	27.97	23.16	17.13	38.77%	100.00%	89.76%	69.42%	66.61%	23.15%
10.102.0.6	53.58	30.03	19.68	17.70	41.05%	99.52%	85.65%	68.80%	67.67%	17.98%
10.102.0.7	51.45	30.46	23.17	17.19	43.54%	91.54%	78.84%	63.22%	61.37%	17.47%
10.102.0.8	57.26	29.28	23.67	16.54	43.53%	88.18%	72.98%	59.55%	57.47%	15.51%
10.102.0.9	58.42	24.55	21.30	15.89	35.28%	94.79%	80.82%	58.90%	57.19%	23.63%
10.102.0.10	61.08	22.96	23.56	17.03	25.82%	97.67%	82.95%	65.10%	62.95%	20.00%
10.102.0.11	32.06	18.22	27.08	16.21	11.05%	100.00%	91.30%	100.00%	91.82%	-0.51%
10.102.0.12	40.35	23.95	18.19	15.57	35.02%	99.55%	88.29%	67.12%	66.27%	22.02%
10.102.0.13	53.72	23.83	22.38	14.92	37.37%	93.25%	80.27%	59.73%	57.88%	22.40%
10.102.0.14	51.27	20.74	25.60	16.33	21.24%	98.08%	84.01%	62.05%	59.04%	24.97%
10.102.0.16	31.55	17.52	14.73	12.47	28.83%	99.55%	91.75%	78.53%	77.64%	14.11%
10.102.0.17	131.13	24.76	162.41	16.06	35.16%	94.49%	70.96%	76.95%	58.36%	12.60%
10.102.0.18	49.15	26.65	20.53	18.43	30.85%	94.42%	83.08%	61.78%	60.65%	22.43%
10.102.0.19	29.81	22.55	15.21	14.37	36.29%	99.55%	94.28%	79.04%	78.53%	15.75%
10.102.0.20	16.03	13.63	12.24	12.19	10.55%	99.90%	98.46%	94.66%	94.52%	3.94%
10.102.0.21	13.07	11.40	8.85	8.40	26.32%	98.46%	97.67%	78.39%	78.39%	19.28%
10.102.0.22	79.57	21.23	74.98	14.53	31.56%	98.08%	80.24%	73.53%	63.18%	17.05%
Overall Avr	51.98	24.39	29.71	15.71	35.60%	96.55%	84.30%	69.88%	66.83%	17.46%

Normal update rate of surface tracks is defined as 96 seconds in Link 22 unless a High Update Rate (HUR) requirement exist. Therefore in this experiment using 12 seconds update gives us a margin of 8 times to include more tracks or higher probability of reception by sending the same information more than once.

H.3.3.2 Broadcast Delivery Analysis at Intermediate Node (@ Node-15) for Range Helo Airborne

When the helicopter is used as an airborne relay, the system performs very well (Table H-2). In this case all the nodes become 1 hop or at most 2 hops away. With the dynamic bandwidth management capability of the underlying MARLIN implementation the Helo gets the necessary slots according to increasing demand for relay traffic and the network become even suitable to exchange “air track data” which has a stale time of 20 seconds and high update rate of 12 seconds.

Also rohc performs very well in this situation as expected, giving us a small performance increase.

H.3.3.3 Broadcast Delivery Analysis at Edge Node (@ node-1) for Full Period

For broadcast receive performance at an edge node, ship 1 performs well with respect to surface track exchange requirements depicted above (Table H-3). It can receive high percentage (88.38%) of all broadcast traffic, and medium percentage (74.49%) under 120 seconds. The PDR values varies essentially proportional to hop counts of the other platforms.

Table H-2: Broadcast Delivery Analysis at Intermediate Node (@ Node-15) for Range Helo Airborne.

Node	Average Latency (Seconds)					Packet Delivery Ratio (%)				
	Normal Operation		Header Comp Enabled		Latency Improvement Due To Header Compression	Normal Operation		Header Comp Enabled		Packet Loss Significant By RohC
	All	120 Seconds Filtered	All	120 Seconds Filtered		All	120 Seconds Filtered	All	120 Seconds Filtered	
10.102.0.1	11.83	11.83	10.78	10.83	8.43%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.2	10.89	10.89	10.43	10.29	5.50%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.3	11.57	11.57	10.36	10.21	11.73%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.4	10.39	10.39	10.30	10.16	2.23%	99.94%	99.94%	100.00%	100.00%	-0.06%
10.102.0.5	9.30	9.30	9.31	9.55	-2.72%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.6	10.58	10.58	10.62	10.56	0.19%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.7	11.02	11.02	11.00	10.94	0.68%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.8	10.79	10.79	11.50	11.16	-3.40%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.9	11.84	11.84	12.12	11.29	4.64%	99.20%	99.20%	99.77%	99.77%	-0.57%
10.102.0.10	11.10	11.10	11.24	11.11	-0.10%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.11	6.81	6.81	6.96	7.04	-3.49%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.12	10.61	10.61	10.74	10.77	-1.51%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.13	11.34	11.25	9.68	9.63	14.41%	98.86%	98.80%	98.80%	98.74%	0.06%
10.102.0.14	12.95	12.14	12.67	12.04	0.77%	99.94%	99.43%	100.00%	100.00%	-0.57%
10.102.0.16	9.96	9.96	9.81	9.54	4.21%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.17	11.00	11.00	10.59	10.28	6.47%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.18	13.30	13.19	12.26	12.28	6.92%	98.17%	98.11%	98.40%	98.40%	-0.29%
10.102.0.19	11.07	11.07	10.56	10.34	6.63%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.20	9.68	9.68	10.26	10.74	-10.88%	100.00%	100.00%	94.57%	94.57%	5.43%
10.102.0.21	7.76	7.76	7.16	7.14	7.98%	100.00%	100.00%	89.14%	89.14%	10.86%
10.102.0.22	6.09	3.54	4.31	3.72	-5.15%	100.00%	98.63%	100.00%	99.89%	-1.26%
Overall Avr	10.47	10.30	10.13	9.98	3.09%	99.81%	99.72%	99.08%	99.07%	0.65%

In the header compression experiments we see that average latency decreases from 22.91 seconds to 16.82 seconds (a 26.58% increase), at the cost of 8.70% decrease in the PDR performance. The difference between all rohc packets and filtered rohc packets is 4.98%, which is higher than for the intermediate node case, as expected. Being an edge node, more layer two relay/route is required to reach node-1 than node-15. This is exactly the same reason for having some lower PDR values depicted as red in the above table.

Normal update rate of surface tracks is defined as 96 seconds in Link 22 unless a High Update Rate (HUR) requirement exist. Therefore in this experiment using 12 seconds update gives us a margin 8 times to include more tracks or higher probability of reception by sending the same information more than once.

H.3.3.4 Broadcast Delivery Analysis at Edge Node (@ node-1) for Range Helo Airborne

Similar to intermediate node case, when the helicopter is used as an airborne relay, the system performs very well (Table H-4). In this case all the nodes become 1 hop or at most 2 hops away. With the dynamic bandwidth management capability of the underlying implementation the Helo gets the necessary slots according to increasing demand for relay traffic and the network become even suitable to exchange “air track data” which has a stale time of 20 seconds and high update rate of 12 seconds.

Also header compression performs very well in this situation as expected, giving us a small performance increase.

ANNEX H – NAVAL TASK GROUP AND ROUTING EXPERIMENTS

Table H-3: Broadcast Delivery Analysis at Edge Node (@ Node-1) for Full Period.

Node	Average Latency (Seconds)					Packet Delivery Ratio (%)				
	Normal Operation		Header Comp Enabled		Latency Improvement Due To Header Compression	Normal Operation		Header Comp Enabled		Packet Loss Significant By RohC
	All	120 Seconds Filtered	All	120 Seconds Filtered		All	120 Seconds Filtered	All	120 Seconds Filtered	
10.102.0.2	47.54	23.03	29.96	16.93	26.49%	86.12%	75.84%	67.16%	63.51%	12.33%
10.102.0.3	27.35	20.64	28.14	16.00	22.51%	93.89%	89.53%	86.17%	81.22%	8.31%
10.102.0.4	7.63	7.53	7.55	7.41	1.62%	99.52%	99.46%	91.78%	91.61%	7.85%
10.102.0.5	56.09	26.32	37.87	15.49	41.13%	85.02%	71.77%	62.73%	57.15%	14.61%
10.102.0.6	37.19	26.20	32.51	19.98	23.75%	92.60%	85.88%	82.88%	77.72%	8.16%
10.102.0.7	15.77	14.89	12.57	12.32	17.27%	99.41%	98.93%	87.80%	87.63%	11.30%
10.102.0.8	16.51	14.18	9.48	9.48	33.18%	95.63%	94.22%	83.22%	83.22%	11.00%
10.102.0.9	86.58	24.65	34.14	16.95	31.25%	82.23%	61.29%	56.77%	53.18%	8.12%
10.102.0.10	79.41	25.04	38.18	15.50	38.10%	83.58%	65.13%	58.03%	53.04%	12.08%
10.102.0.11	68.45	25.87	40.74	17.12	33.81%	86.61%	68.79%	68.34%	61.95%	6.84%
10.102.0.12	39.98	27.87	34.40	20.92	24.93%	92.14%	84.54%	74.96%	69.92%	14.62%
10.102.0.13	87.48	23.25	34.51	16.92	27.23%	81.32%	59.92%	56.66%	53.31%	6.61%
10.102.0.14	85.46	24.59	44.69	17.82	27.53%	83.94%	61.36%	61.64%	55.80%	5.56%
10.102.0.15	64.84	27.24	35.21	18.13	33.43%	86.01%	68.70%	65.13%	59.53%	9.17%
10.102.0.16	52.42	29.91	39.03	21.70	27.46%	90.28%	77.13%	75.61%	68.78%	8.36%
10.102.0.17	128.57	16.66	135.65	13.19	20.79%	94.31%	73.73%	85.90%	69.81%	3.92%
10.102.0.18	88.57	25.67	34.53	19.00	26.01%	81.19%	59.21%	55.56%	52.00%	7.21%
10.102.0.19	77.86	23.89	30.96	17.48	26.81%	83.17%	62.19%	58.03%	54.83%	7.36%
10.102.0.20	75.23	24.58	33.65	19.33	21.34%	85.28%	64.65%	64.14%	60.14%	4.51%
10.102.0.21	55.87	29.13	37.56	22.87	21.49%	88.24%	73.94%	73.44%	68.11%	5.82%
10.102.0.22	83.12	19.97	87.11	18.69	6.38%	85.51%	68.13%	70.24%	59.15%	8.98%
Overall Avr	61.04	22.91	38.97	16.82	26.58%	88.38%	74.49%	70.77%	65.79%	8.70%

H.3.3.5 Headquarter Delivery Analysis @ Node-23

The communication with the HQ requiring the layer-3 router performed moderate under this setup. In real life, less complex topologies with fewer number of units might give better results but we see that definitely an improvement is needed. We have made the following observations during these experiments.

- The bold case IP numbers in show the units having an HF system which directly communicates to the HQ through HF frequencies. Therefore we expect a PDR ratio of very close to 100% for those nodes. But for example, node-1 and node-8 have lesser values. During the experimentation we have observed that occasionally olsrv2 selects these nodes more frequently as routers for the non-HF units than the others. While selected by many the total load is not shared evenly and they lose even their own traffic due to heavy congestion in HF. Therefore we believe that measuring and using congestion as a router metric would be a good approach, to make better routing decisions.
- The UHF only nodes find a route to the HQ via one of the HF equipped ships, but if they are far away from the ship they have to traverse multiple UHF links to get to the HF ship, as well. In the UHF network there are two routing algorithms; in layer 2 MARLIN calculates a route and in layer 3 OLSRv2 calculates another route depending only upon its own measurements. This lack of cooperation may be the result of some packet loss.
- We expect that Dynamic Link Exchange Protocol (DLEP) [8] implementation within MARLIN to OLSRv2 will help overcome these two problems, as we can supply the layer 3 router the most recent

topology change information. Thus, OLSRv2 will react rapidly to change paths and packet loss due to wrong route calculations will decrease.

Table H-4: Broadcast Delivery Analysis at Edge Node (@ node-1) for Range Helo Airborne.

Node	Average Latency (Seconds)					Packet Delivery Ratio (%)				
	Normal Operation		Header Comp Enabled		Latency Improvement Due To Header Compression	Normal Operation		Header Comp Enabled		Packet Loss Significant By RohC
	All	120 Seconds Filtered	All	120 Seconds Filtered		All	120 Seconds Filtered	All	120 Seconds Filtered	
10.102.0.2	11.35	11.35	10.71	10.71	5.68%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.3	11.76	11.76	10.21	10.21	13.22%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.4	7.15	7.15	7.04	7.04	1.54%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.5	10.42	10.42	10.31	10.31	1.13%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.6	10.72	10.72	10.61	10.61	1.03%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.7	10.29	10.29	10.45	10.45	-1.59%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.8	8.04	8.04	9.02	9.02	-12.15%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.9	11.62	11.62	13.24	11.37	2.10%	99.03%	99.03%	99.83%	98.69%	0.34%
10.102.0.10	11.04	11.04	11.53	11.53	-4.44%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.11	10.11	10.11	10.17	10.17	-0.63%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.12	10.93	10.93	11.04	11.04	-0.95%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.13	11.48	11.38	9.69	9.69	14.90%	98.63%	98.57%	99.09%	99.09%	-0.51%
10.102.0.14	14.71	12.39	12.02	12.02	2.98%	99.94%	98.46%	100.00%	100.00%	-1.54%
10.102.0.15	10.97	10.97	10.25	10.25	6.55%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.16	11.57	11.57	10.64	10.64	8.11%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.17	10.68	10.68	10.32	10.32	3.36%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.18	13.43	13.32	12.33	12.33	7.44%	97.66%	97.60%	98.17%	98.17%	-0.57%
10.102.0.19	11.30	11.23	10.94	10.94	2.57%	100.00%	99.94%	100.00%	100.00%	-0.06%
10.102.0.20	11.38	11.38	12.56	12.30	-8.09%	100.00%	100.00%	100.00%	99.77%	0.23%
10.102.0.21	10.92	10.92	10.53	10.53	3.54%	100.00%	100.00%	100.00%	100.00%	0.00%
10.102.0.22	6.92	3.67	4.09	3.94	-7.43%	100.00%	98.46%	100.00%	99.89%	-1.43%
Overall Avr	10.80	10.52	10.37	10.26	2.51%	99.77%	99.62%	99.86%	99.79%	-0.17%

H.4 RESULTS

We have concluded the following results:

- By using this kind of experiment, some of the operational capabilities of the systems can be shown without the use of expensive actual functional flow tests conducted at sea.
- This emulation experiment shows that under given operational scenario such a system can be effectively used for exchanging of Surface Tracks, with some improvements on the router.
- Airborne relays are very useful, if there is an airborne relay in the network, the network performs very well, even sufficient enough to exchange air tactical picture over distant groups.
- Although header compression can be used in broadcast mode if latency is more important than probability of reception, we believe the improvements should be further examined.
- Some kind of perishability QoS for time sensitive data must be implemented in order to comfort queues of the relayers.
- Congestion value if measured and used can be good metric for router selection.
- DLEP implementation will improve interaction with the router and network performance.

Table H-5: Headquarter Delivery Analysis @ Node-23.

Node	Average Latency (Seconds)		Packet Delivery Ratio (%)	
	Normal Operation		Normal Operation	
	All	120 Seconds Filtered	All	120 Seconds Filtered
10.102.0.1	13.85	13.85	85.38%	85.38%
10.102.0.2	8.53	8.53	99.77%	99.77%
10.102.0.3	8.83	8.83	100.00%	100.00%
10.102.0.4	7.74	7.74	99.71%	99.71%
10.102.0.5	57.24	38.79	75.90%	68.11%
10.102.0.6	7.20	7.20	100.00%	100.00%
10.102.0.7	7.33	7.33	99.53%	99.53%
10.102.0.8	9.34	9.34	84.85%	84.85%
10.102.0.9	118.83	53.18	67.70%	48.08%
10.102.0.10	111.65	49.51	71.16%	53.82%
10.102.0.11	93.57	52.99	69.53%	53.18%
10.102.0.12	79.30	56.33	68.71%	58.34%
10.102.0.13	113.24	58.48	69.61%	50.16%
10.102.0.14	130.82	54.75	69.25%	46.69%
10.102.0.15	106.50	52.74	82.24%	60.97%
10.102.0.16	98.17	57.40	72.11%	54.65%
10.102.0.17	10.06	7.41	99.77%	98.95%
10.102.0.18	126.59	60.78	65.48%	44.68%
10.102.0.19	135.08	59.48	61.39%	41.82%
10.102.0.20	148.39	58.51	64.32%	39.18%
10.102.0.21	118.07	57.67	67.02%	47.09%
10.102.0.22	13.50	13.50	99.71%	99.71%
Overall Avr	69.27	36.11	80.60%	69.76%

H.5 REFERENCES

- [1] Suri, N., Hansson ,A., Nilsson, J., Lubkowski, P., Marcus, K., Hauge, M., Lee, K., Buchin, B., Ṁiṡiṙlioğlu, L., and Peuhkuri, M., “A Realistic Military Scenario and Emulation Environment for Experimenting with Tactical Communications and Heterogeneous Networks,” Proceedings of the 2016 International Conference on Military Communications and Information Systems (ICMCIS), Brussels, 2016, doi: 10.1109/ICMCIS.2016.7496568.
- [2] Marcus, K., Barz, C., Kirchhoff, J., Rogge, H., Nilsson, J., in’t Velt, R., Suri, N., Hansson, A., Sterner, U., Hauge, M., Lee, K., Holtzer, A., Buchin, B., Peuhkuri, M., and Ṁiṡiṙlioğlu, L., “Evaluation of the Scalability of OLSRv2 in an Emulated Realistic Military Scenario,” Proceedings of the 2017 International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, 2017, doi: 10.1109/ICMCIS.2017.7956503.

- [3] Suri, N., Nilsson, J., Hansson, A., Sterner, U., Marcus, K., Mısırlıoğlu, L., Hauge, M., Peuhkuri, M., Buchin, B., in't Velt, R., and Breedy, M., “The Angloval Tactical Military Scenario and Experimentation Environment,” Proceedings ICMCIS, Warsaw, Poland 2018.
- [4] AdjacentLink, LLC. Extendable Mobile Ad-hoc Network Emulator (EMANE) Wiki. Internet: <https://github.com/adjacentlink/emane/wiki>, [December 13, 2017].
- [5] STANAG 4691-Multi-hop IP Networking with Legacy UHF Radios: Mobile Ad Hoc Relay Line-of-Sight IP Networking (MARLIN), Edition 2, June 2016 (NATO UNCLASSIFIED).
- [6] Clausen, T., Dearlove, C., Jacquet, P., and Herberg, U. “The Optimized Link State Routing Protocol Version 2”, IETF, RFC7181. Apr. 2014. Available: <http://www.ietf.org>.
- [7] Sandlund, K., Pelletier, G., and Jonsson, L.-E. “The Robust Header Compression (ROHC) Framework”, IETF, RFC5795. March 2010. Available: <http://www.ietf.org>.
- [8] Ratliff, S., Jury, S., Satterwhite, D., Taylor, R., and Berry, B. “Dynamic Link Exchange Protocol (DLEP)”, IETF, RFC8175. June 2017. Available: <http://www.ietf.org>.



Annex I – QOS FRAMEWORK

Markus Peuhkuri

Aalto University
FINLAND

Niranjan Suri

U.S. Army Research Laboratory (ARL)
UNITED STATES

Mariann Hauge

Norwegian Defence Research Establishment (FFI)
NORWAY

It is commonly agreed that some Quality of Service (QoS) is needed in networks and especially in military networks. However, QoS is understood differently by different parties and it is good to review these different viewpoints. Implementing QoS brings additional costs to implementing and operating a network, mainly in form of increased complexity. Benefits from QoS mechanisms deployment must be well evaluated and not only based on a subjective feeling from a network manager of having additional network control.

From a network engineer's viewpoint, QoS is a set of mechanisms that can be implemented in network devices to provide a set of different traffic treatments that allow the network to comply with requirements set by an application.

A network user expects the applications to work with sufficient fidelity. How this is accomplished is irrelevant for the user unless additional actions such as payment, physical relocation or change of communication method are needed by her.

An application has some minimum requirements for the network performance that was expected when it was designed. Typically, time needed to transfer a data item (available throughput) and in some cases the delay are what matters to an application. The common network metrics such as packet loss and delay variation is often visible to the user as reduced throughput and increased end-to-end delay as an effect of the transport protocol.

From a military standpoint, QoS should make sure that the information that best serves the mission's objectives, should be available where it is needed and in time. The traffic management decisions needed to achieve this is difficult to make solely per packet using predefined priorities and allocations; a wider view is needed where more information must be taken into account. Information Objects (IO) can be assigned different value based on how informed decisions they help to make. This value depends also on other information available at a soldier or unit. Each IO is transmitted in one or multiple packets consuming network resources; if there are two IOs providing the same value but the first one can be transmitted in one packet while the other takes hundred, the network should be able to identify that the first one is the one that should be prioritized in order to utilize the network resources in the best manner (best value for the mission).

In this document we will first review QoS as it is known and applied in civilian networks. Following that we review QoS-related requirements set to heterogeneous military mobile networks. Third, we introduce three operating states of networks followed by a discussion on how Quality of Information (QoI), Value of Information (VoI), and Quality of Service relate to each other. Next we discuss QoS mechanisms and their visibility and before the conclusion, review the characteristics of the most important military applications currently expected to use the network. Existing standards and vocabulary for QoS are discussed in Annex J: "QoS Standards and Vocabulary".

I.1 PROVIDING QUALITY OF SERVICE IN CIVILIAN NETWORKS

At first sight, there is no QoS in civilian networks. There is no way a network user can ask for some of the traffic (e.g., video call) to receive shorter delay and lower packet loss ratio than other traffic types (e.g., software update

downloads in the background). Different performance objectives can be provided but in most cases require a new contract or even new connection to be installed. This might take days, weeks, or months to accomplish. However, there is a range of peer reviewed publications proposing ways to implement QoS first in Asynchronous Transfer Mode (ATM) networks and then in IP networks. There is a gap between solutions proposed by research groups and a business case for QoS. The problem is discussed in detail e.g., in Refs. [1] and [2].

While QoS is not part of the offering by Internet network providers, there is a need for QoS in military networks since the objectives in military networks differ from civilian networks. In military network the line of command should provide the common goal for an operation: the network should be configured in such manner that the applications can best serve the goal. To understand the differences, we first look at how the QoS challenge is solved in civilian networks, if solved at all.

I.1.1 Network Level QoS

Solutions deployed in commercial networks and proposed in the literature are typically based on one or more of the following features [2]:

- Increase network capacity to match the demand. This is common in corporate and operator networks where there is a 10-fold increase every 5 years or so when networking hardware including end terminals are upgraded.
- Content Distribution Networks (CDN) and caching allows shorter delays and fewer (congested) links when content is moved closer to the customer. These techniques are becoming an integrated part of the networks. For example, 5G networks will provide mobile edge processing to optimize backbone access, for lower latency, and to optimize content for consumption. Content filtering, compression, and optimization have been utilized for example with different “mini” browsers in feature mobile phones that have no capacity to render web pages designed for desktop.
- Use price controls to adapt demand. Customers are provided with different capacity tiers limiting maximum throughput by access link speed, by shaping, or setting monthly quota on transfers. This works as an effective admission control limiting used bandwidth by impacting which applications are used and how much.
- Divide traffic into different traffic classes. Each class has its maximum capacity and relative priority compared to each other. There may also be different priorities inside classes. Traffic is policed on the edge of the network to allow only predefined traffic volume. Classification is made by end devices (if they are to be trusted) or at the network edge. In addition to different capacities, classes may also receive different treatment like limiting queuing delay.
- Traffic flows are utilizing reserved capacity and well defined treatment by the network. Flows can be generated by individual application (micro-flows) or aggregate macro-flows. The latter can be considered as a dynamic variation of traffic classes. Capacity allocation can be realised using i.e., virtual private networks within network provider network.

The capacity increases in mobile networks over the generations from 2G to 5G are in part possible because of increased number of base stations and additional frequency ranges. Base stations connect to the backbone with optical links in many cases. Both are aspects that are not often feasible in military environment.

Content distribution, caching, and optimization are technologies well suited for tactical environments. Price controls are not applicable in military environment.

The last two points in the list above (classes and flow treatment) are not commonly used in civilian networks because it is difficult to sell first “inferior” basic service and charge extra for good quality service [2]. In military environment, however, it is beneficial to give different information objects different priority and treatment.

I.1.2 Non-Network Approaches for Quality of Services

In addition to the above mentioned network-centric approaches, also end systems may use methods to ensure optimal Quality of Service. Some of the following techniques are utilized in civilian networks, some in military networks, and many in both networks.

Applications may work in co-operative manner. Even without any enforcement from the network, each device can try to occupy only its fair share of resources from the network. This is a well-studied area and lots of research has been put into TCP congestion control in order to provide fair sharing of network resources.

Network devices can signal upcoming congestion to end devices by delaying packets, dropping packets, or marking packets with congestion indication like Explicit Congestion Notification (ECN) [3].

In the wireless domain with unstable connections an additional challenge is to differentiate between packet loss because of congestion and packet loss due to a bad channel (bit error). The delay may increase because of a route changes and not only because of increasing queue length due to congestion. This makes it even harder to provide fair sharing of resources. Marking packets with, for example, explicit congestion notification is helpful to understand if the loss of a packet or increased delay is due to other reasons than congestion.

In addition, non-elastic applications can try to adapt to available bandwidth. Well-known examples include hierarchical encoding of video or avoiding the use of some media altogether when there is not enough capacity. There may also be a common middleware providing these functions.

Middle-boxes like transcoders, proxies, caches and content distribution points in the network may also optimize data for low-bandwidth links by for example down sampling image data, by applying compression, and improving data transfer by combining multiple items into one download bundle. Of course, if data is to be modified in transit this must be supported also by the security architecture. A discussion on the impact of middle-boxes can be found in Ref. [4].

Some traffic types have a short validity time. For example, if a voice packet of a telephone call (VoIP) is delayed too much, it has no value for the end user any more. In military networks different types of track data (e.g., friendly force tracking) has no value if it is too old. If there is newer data from a sensor available already, there is no use in transmitting the old data but rather the network resource should be used to send the most recent instead. This functionality to discard old information is not available in standard IP routers but assumes some kind of data-aware device or middle-box functionality. Some military radios implement this functionality but in a proprietary manner. Such support should be made available end-to-end across the heterogeneous network.

Applications can also improve packet delivery reliability. By using error-correcting codes, applications can trade some bandwidth and additional delay for reliability. However, this increases the total data volume and may result in reduction of the overall utility of the network [5].

Application-level control of course assumes that users are co-operative. For example, TCP fairness will suffer if some users establish multiple parallel TCP connections. User actions may result in unwanted effects too. If a web site does not respond in time, the users often try to reload the page, even multiple times in rapid succession. This will put unnecessary load on the network and on the server, often making the situation worse for everyone using the network and the server.

In addition to misbehaving users, it is possible that a device hardware or software is malfunctioning. Examples include Push-To-Talk (PTT) button not releasing, phone not put on-hook correctly or software failing to receive acknowledgment and retransmitting unnecessary messages.

In a military environment, malicious users, devices or malware trying to overload the network must be taken into account as potential risks and the effect must be limited. In all of these cases, it should be possible to identify any abnormal state. Network Management and Cyber Defence (NMCD), a key component providing security in the Protected Core Network (PCN) model, has this function [6].

I.2 REQUIREMENTS

The goal of the heterogeneous network Quality of Service is to ensure that resources in the network are allocated such way the network can best support mission objectives.

Many requirements are shared with routing and QoS. Many of requirements described in Annex E: “Routing Architecture Considerations for Heterogeneous Tactical Networks” apply also for QoS. Following requirements are QoS-specific requirements.

I.2.1 General Requirements

The goal of the heterogeneous network Quality of Service is to ensure that resources in the network are assigned to traffic according to its importance – resulting in better utilization of the network.

- Different operations will assign different priorities and forwarding treatment for a different set of traffic. Also network capacity, number of users, and operation environment are different in each operation. Operation must be able to select the best working set of QoS mechanisms and policies for their needs.
- The network must implement an admission control to reject some traffic if the network does not have capacity to forward the traffic while maintaining priorities.
- If a mobile network is degraded and carries less traffic than planned, it must be able to adapt prioritization and admission control to match the present resources.
- The network must be able to pre-empt traffic it has no capacity to transfer a new high-priority traffic flow.
- A traffic class should not be forwarded to a path whose properties cannot provide the service that the class needs. If there is no alternative path, the traffic should be denied.
- Applications, middleware and the users should have knowledge of network state. If possible they should take advantage of the state information to modifying their behaviour (traffic generation) to better suit the current network state.
- Users should be made aware if they are using applications the network cannot support at the time.
- The terminals should indicate network state if the information does not overload the user capability.
- Various quality target values have been defined in standards including Y.1541 and STANAG 4711. See Annex J for details.

I.2.2 Robustness Requirements

- The traffic path should be sufficiently robust in characteristics so resource allocation and forwarding characteristics for a flow can be maintained for a reasonable session life-time.
- Each network segment must be able to control traffic volume and traffic classes and adapt to the available capacity and mission state independently.

- The network should adapt its control and forwarding to the present capacity.
- The network must be able to make a priority decision even if the network is partitioned.
- The QoS mechanisms shall be as straightforward as possible, because any unnecessary complexity threatens the operational efficiency and the reliability of the services.

I.2.3 Scalability Requirements

- Nodes sharing a common channel should share a common view of available network resources and implement appropriate admission control for the situation.
- There must be an efficient method to limit network state information visibility not to cause too much signalling information.

I.2.4 Resource Efficiency Requirements

- The priority of different traffic should be adapted based on the ratio of the Value of the Information (VoI) for the mission to consumed resources (i.e., if a video clip does not have much added value compared with a short message, the latter should be prioritized).
- There should exist an estimate on present network load and available capacity.
- Traffic that cannot be forwarded to the destination should be rejected/dropped as close to the source as possible.
- Traffic that has no value for the recipient because it is too old, or has been replaced with new information, should not be forwarded.
- If radio silence or Traffic Flow Confidentially (TFC) are applied, the impact of these elements must be taken into account.

I.2.5 Flexibility Requirements

- A common QoS control framework must be easily implemented based on the mission plan.
- It should be easy to reconfigure the QoS control to meet changing requirements if the environment changes. In the ideal case this should require little or no manual operation.
- The network must adapt to the available capacity. It should be possible to modify the network QoS control and policy in real time if the situation requires so – for example in case of an unforeseen Medical Evacuation (MEDEVAC) operation.

I.3 NETWORK STATES

In order to provide best possible QoS and resource management for heterogeneous mobile military networks, we believe it is necessary to identify the current operating state of the network. We propose to define three different operating states that the network can be in:

- 1) **Normal operation** is the state the network is built for. QoS mechanisms should be enforced to provide good user experience and to cater for application specific needs like low-delay delivery. The network capacity may vary within an order of magnitude of the initial capacity because of external factors like troop movement, loss of links, jamming, physical damage to points of presence, and other external factors.

- 2) In **reduced capacity** state there is a significant loss of service. Throughput may be much lower than designed and network-wide end-to-end connectivity is not consistent. The roles of the QoS mechanisms are to make sure that the most *important* services – for the *mission* – can still have the fidelity they require. Service is not provided for very resource-hungry applications.
- 3) In **last effort** state the network has capacity measured as low as tens of bits per second and very intermittent connectivity. There is no concept of flows but communication is reduced to bare essentials in individual messages mode. A node must identify this situation based on only local information: directly connected peers, links and individual datagrams it observes. QoS mechanisms must work without any signaling or access to any central service.

As indicated in the description of the states, the resource management and traffic management mechanisms and policies will be different in the different states. For example, fairness is important in the “normal operation”; the network should aim to share the resources fairly between users and services. In “reduced state” fairness is not a goal, on the contrary it is important to prioritize the most important services and users. In the “last effort” state it might be necessary to utilize all resources in order to provide one service on a very opportunistic basis. The selected method(s) for traffic control and QoS must either have some role in all these states, or be made aware of the change in state and not interfere in states where the mechanisms is not applicable, or automatically disable themselves for states where they do not provide value.

There is prior work on network survivability, for example Ref. [7]. Ref. [8] presents a measurement-based admission control for simulation models of voice and Video Teleconferencing (VTC) traffic with Multilevel Precedence and Pre-emption (MLPP). More work is necessary in order to decide on the possible mechanisms to identify when the networks are in different states, to make sure that there is a common view on the current state throughout the network, and how different applications provide best value for consumed capacity.

I.4 QUALITY OF INFORMATION, VALUE OF INFORMATION, AND RELATIONSHIP TO QUALITY OF SERVICE

I.4.1 Introduction

One of the overarching goals of the QoS framework of a mobile heterogeneous network is to make sure that the information that best serves the mission’s objectives, should be available where it is needed and in time. Identifying manually or automatically the information that best serves the mission’s objective is a difficult task. Recent research in the area of information management and information dissemination to military operators has resulted in exploiting two notions – that of Quality of Information (or QoI) and Value of Information (or VoI). This research can help identifying the important information, whereas the QoS mechanisms must make sure to bring the information to the right destination, in time.

While the two notions of QoI and VoI are inherently related in nature, QoI may be defined as a more fundamental and intrinsic attribute of the information whereas VoI is defined in the context of an individual recipient. When ascribing QoI or VoI, the metric is often applied to an individual or discrete piece of information, termed an Information Object (IO). While the notion of QoI and VoI can be extended to continuous streams of data (e.g., video), work to date has focused primarily on discrete pieces or chunks of information (which could include individual video clips).

Defined more rigorously, QoI can be said to represent an “*internal*” and *objective metric* that considers the *intrinsic characteristics* of an IO. For example, an IO containing a photograph or an image might have a QoI value defined by aspects such as level of detail (or resolution), clarity, contrast, exposure, etc. In some cases, it is possible to devise automated systems that determine the QoI of an IO by analyzing its contents. For example, IOs generated by infrared sensors will typically have higher QoIs than those generated by

visual sensors at night, and vice-versa by day. In more complex cases, such as IOs containing documents/reports, the determination of the QoI may have to rely on a human operator.

On the other hand, VoI can be said to represent an “*external*” and *subjective metric* that classifies an IO according to the *utility it provides to its consumer* – that is, to its ability to support the consumer in more effective decision making. In fact, the VoI concept originated in economic and decision-making research communities, with the purpose of investigating the advantages that additional information provided to decision makers [9], [10]. VoIs are dynamic values that change according to many factors, such as a consumer’s needs and information availability. Also note that the same IO may have different VoI values for different consumers and that an IO may have a very high QoI (for example, it may be a very accurate, recent location report for an enemy unit) but it may have a very low VoI for a particular consumer, for whom it represents irrelevant information. In other words, an IO’s VoI is a function of its QoI, of its suitability or applicability to the consumer given the consumer’s current context, as well as of the previous history of IOs sent to the consumer.

I.4.2 Overview of Approaches to VoI

Calculating the actual VoI of an IO for a particular consumer is challenging, as it requires the system to model each consumer in terms of their existing knowledge, their objectives, their information needs, and their decision-making strategy. Broadly speaking, there does not exist a general, comprehensive solutions that addresses the problem of determining VoI. Fundamental work on VoI was published by Howard in 1966, where he explored the notion from a business perspective [11]. In particular, his framework considered the Value of Information to be the price that a company would pay to reduce their uncertainty about a business decision. This approach, termed the Uncertainty Reduction approach, is the first of five typical categories of approaches taken by systems:

- 1) **Uncertainty Reduction** – Information can be ascribed value if having that information reduces the uncertainty (e.g., related to Situation Awareness) about a set of assumptions or assertions of knowledge. The greater the reduction in uncertainty, the higher the value of the information. This is directly related to Howard’s original work on this topic as mentioned earlier.
- 2) **Decision Theoretic** – A second approach to ascribing value is based on decision theory. One perspective in this category, related to military decision making, is to consider the different IOs that are necessary to make a decision and whether any of them are missing. If a decision cannot be made unless that IO is available, then that IO is assigned a value related to the importance of making that decision. Some original work in this area was published by Heckerman, Horvitz, and Middleton in the context of medical diagnosis [12], where the VoI to be gained from specific diagnostic tests was used to drive the selection of the next test(s) that should be run on a patient.
- 3) **Recommender Systems** – Another approach being explored to determine VoI is to leverage ongoing research in the area of recommender systems, which have been applied to a wide range of topics from recommending books to movies to news articles. The key challenge here is to identify other users in “similar” situations/conditions and to leverage feedback from those users about VoI of specific IOs and then compute the VoI of those IOs for a new recipient.
- 4) **Channel Capacity (Human/System)** – A slightly different perspective on determining VoI is to take into account the channel capacity, which could either be the system channel capacity (typically the network in the case of tactical networks) or the operator (i.e., the intended recipient). The channel capacity of the network is an identifiable value (e.g., in terms of Kbps) whereas the channel capacity of the recipient is much more nebulous. Recent work in this latter vein has been focused on physiological measurements in order to determine cognitive workload and current context, which then feed into the identification of valuable IOs for that recipient.
- 5) **Policy-based** – One final category of approaches to assigning VoI to IOs is a policy-based approach, which uses a set of rules encoded into the system that determine the value based on either the

metadata associated with the IO or the data within the IO. Usually, the rules are derived from Subject Matter Experts (SMEs) and encoded within the system.

It is entirely possible to have hybrid approaches that combine elements of the above five categories.

I.4.3 VoI-Based Dissemination Model

Irrespective of the approach taken to determine the VoI of an IO, the concept of using VoI fundamentally changes the system design for disseminating information. Figure I-1 shows a traditional information dissemination model using a publish-subscribe metaphor. In this model, which applies to a large number of existing systems, clients subscribe to receive IOs based on a topic or on some metadata criteria. As IOs are generated, they are published into the system, which then evaluates whether they match any of the clients that are registered/connected. If an IO matches a client, the IO is then transmitted to the client. In the example in Figure I-1, there are two clients, one of which has subscribed to both Topics A and B, whereas the second client has only subscribed to Topic A.

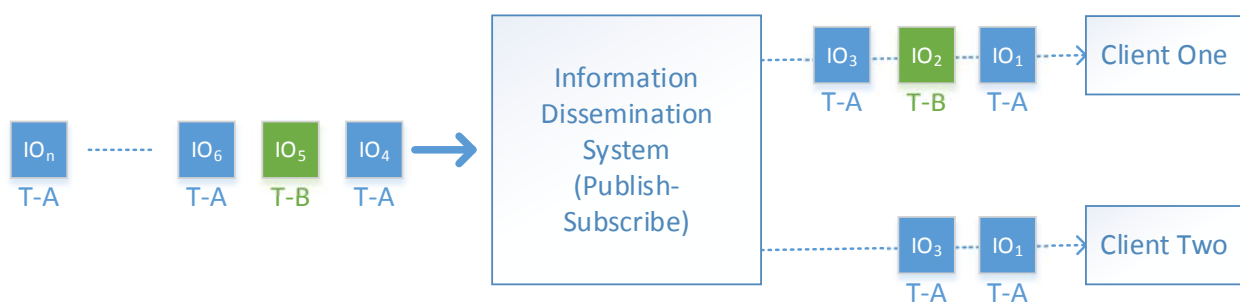


Figure I-1: Traditional Information Dissemination Model.

Note that this simple model can be enhanced with aspects such as prioritization, filtering, and a Data Store that supports query.

On the other hand, Figure I-2 shows a VoI-based information dissemination model, which has notable differences from the traditional model. In a VoI-based model, the current state of each client is represented within the dissemination system (shown as Client One Context and Client Two Context). This contextual information is updated as and when the client's context changes. The specific nature of the contextual information depends on the algorithm for determining VoI, but it could include elements such as identity, role, mission, and for mobile nodes, current position and planned routes. It could also include logistics-related information such as food, water, fuel, and ammunition levels, as well as physiological and health measures, if the client represents an individual user.

As new IOs enter the system, they are archived into a Data Store and also passed to a component termed the Information Valuator. This component is responsible for evaluating the VoI of the incoming IO with respect to any clients that are registered/connected based on the context for those clients. The outcome is an assignment of a value score for each individual client. Therefore, IO_x may have a high score for Client One and a low score for Client Two. The IO, along with the evaluated score, is sent to a Communications Module, which handles the actual transmission of IOs to clients. The Communications Module may discard the IO or otherwise prioritize it to be sent to the intended client(s).

It is important to note that if an IO is deemed to not be of value to a client and hence filtered, that valuation may change over time. In particular, it is entirely possible that an IO is deemed to not be of value at the current moment in time but may become highly valuable to a client in the future, as that client's context

changes. Therefore, all IOs are archived within a local Data Store. Whenever the context of a client changes, previously skipped IOs are re-evaluated to see if their VoI score has changed, and if it is deemed to be sufficiently high, it may be transmitted at that time.

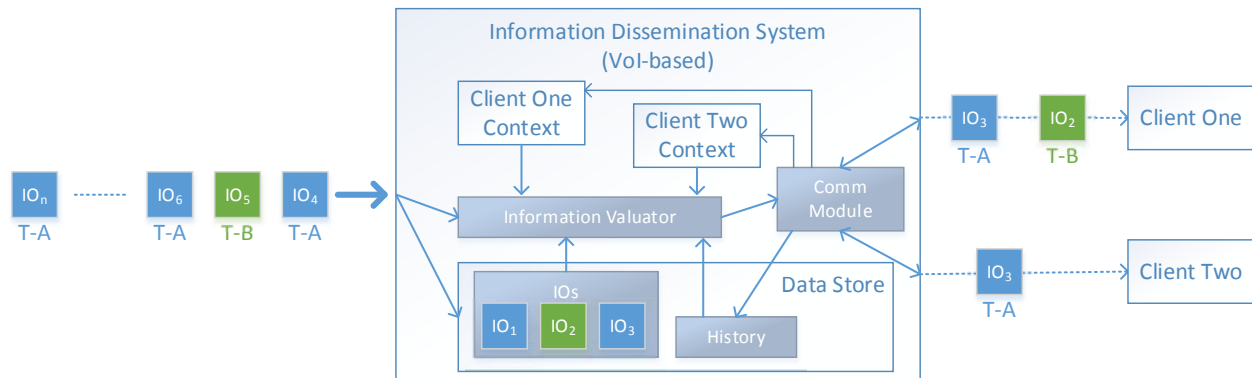


Figure I-2: Value-of-Information-Based Dissemination Model.

The History log within the Data Store plays an important role in keeping track of which clients have already received specific IOs. This is updated by the Communications Module upon successful transmission of an IO to a client. The History log is consulted by the Information Valuator when a client's context changes so that only previously skipped IOs are re-evaluated for the client.

The History log plays a second crucial role for computing the VoI. One of the aspects that impact the VoI of an IO for a client is the previously known information by that client (i.e., the IOs that have been previously sent to that client). It is entirely possible that IO_n on its own would be of high value to a client, but not if the client had already received IO_m. Therefore, the Information Valuator also consults the History Log when determining the VoI of newly arriving IOs.

I.4.4 VoI-Based Dissemination Deployment Patterns

Prior experimentation has revealed three different deployment patterns for exploiting information value-based dissemination, which are shown in Figure I-3. The first deployment pattern applies to information from a command/operations center flowing to dismounted soldiers using a tactical network. The intuition here is that the operations center is essentially an enterprise network node, with very few constraints on computation, storage, and network resources. However, not all of the information available at the operations center can be transmitted to the tactical edge given the capacity limitations. Therefore, each of the dismounted soldiers pushes their current context (denoted as the user context) to the operations center where an Information Valuator component examines the available IOs (and new incoming IOs – for example from deployed sensor networks) to determine their value, filter IOs that do not satisfy a relevance threshold, prioritize the IOs that are selected, and transmit those to dismounted soldiers. In this deployment pattern, data from sensor networks is first exfiltrated back to the operations center from one or more sensor network gateways (via a number of possible network links) before being evaluated and transmitted to dismounted users.

The second deployment pattern applies to information from the tactical network, including dismounted soldiers and sensor networks, being transmitted back to an operations center, where the consumer may be an analyst, or other tactical network users that are also connected to the operations center. In this case, the IOs are generated by sensors as well as soldiers and include tracks, detections, pictures, reports, and other potentially large objects. As discussed before, the tactical network does not have the capacity to transfer all of this data back to the operations center. Therefore, in this second deployment pattern, IOs increasingly stay where they are gathered, and are pushed out of the tactical network to the operations center based on

demand. For example, an analyst may express his or her interest in different types of IOs, which would represent their user context. These user contexts would be pushed out to sensor network gateway nodes, where valuator components would match locally generated IOs to the consumers. Again, IOs that satisfy a relevance threshold would be selected, prioritized based on their relevance, and transmitted to the consumers.

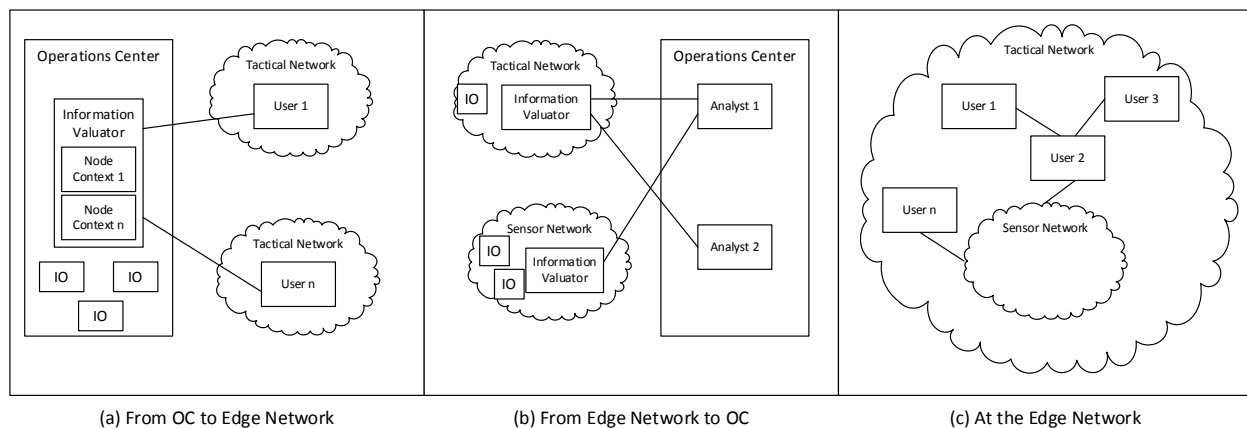


Figure I-3: Deployment Patterns for Vol-Based Dissemination.

The third deployment pattern applies to information sharing directly at the tactical edge – for example from one soldier to another or from a sensor network to a soldier. Unlike the first two cases, these peer-to-peer exchanges occur on an ad-hoc basis based on potentially opportunistic contacts between the edge users. Hence, the user contexts are not pre-shared but exchanged upon contact, at which point a node with relevant IOs would push those to the other node. While not shown in the diagram, user nodes and sensor network gateway nodes contain information valuator as well as the node contexts for connected peers/users (the word peer and user are used interchangeably – a user is represented by a node that is a peer on the network).

I.5 QOS MECHANISMS IMPLEMENTATION AND GUIDELINES

When an information object is determined to be valuable enough to be sent over the network it needs to be assigned a value that can tell the network elements how to process it compared to other information that is sent over the network. This is accomplished using a set of QoS mechanisms. In packet networks, QoS mechanisms can be implemented on five different levels:

- 1) **Transport layer and applications** (TCP, rate-adapting voice and video codecs, self-rate limiting applications) can adapt themselves to available network capacity. Usually, an application tries to utilize its fair share of available resources. If we have two bulk transfers over TCP, both of them should receive if not equal but reasonable similar performance. However, this is not guaranteed and small changes may result in starvation of one of the sessions. A background process may opt also for a lower share of the resources i.e., less-than-best effort.

In the Internet, rate control is based on feedback from packet loss or round-trip delay. In deployment scenario typical to mobile heterogeneous networks, this is not reliable as packet loss may result from a bad channel (weak signal, signal loss, or intentional jamming). Differences in congestion avoidance algorithms, initial window sizes and presence of other traffic will result in unfair allocation of capacity.

- 2) **Packet marking**, like Differentiated Services provides, can be used to differentiate the service packet by packet. [13]. Together with various queuing and scheduling methods, packet marking can produce predefined service properties if and only if offered traffic is policed to avoid network congestion. These include delay, delay variation, burst tolerance, throughput, and priority over other types of traffic.

One consideration is if users should be informed about priorities or not. If for example, voice traffic is given higher priority over data traffic by default then users may opt using the data channel in voice service¹ for data transfers to get reliable throughput. If priorities are assigned only based on the rank, it may lead to sub-optimal resource allocation from the mission perspective.

- 3) **Admission control**, flow level, or call level methods are designed to provide predictability to the service level a flow like a phone call receives. If a call is established, it will maintain the same quality throughout its life-time as there are resources allocated for it. Preferred treatment is often implemented using packet marking. Offered traffic is controlled by admission control rejecting any flows potentially exceeding available capacity.

Normal implementations prioritize existing flows over new ones. If there are multiple call priorities, higher priority ones may pre-empt existing calls. If the network capacity or quality falls below committed capacity, then the service level cannot be maintained.

- 4) **Aggregate level traffic engineering** works on a (static) set of paths i.e., set of links the traffic would travel on. An example would be Multiprotocol Label Switching (MPLS) [14] that builds virtual pipes or paths below IP level. Also other tunnelling methods can be used. Each path would have predefined capacity allocation (either strict or flexible). Signalling like for Integrated Services can implement similar functionality on individual flow level [15].

While it is easy for the network manager (or signals officer) to consider this in a set of isolated, parallel networks, it can become quite complex in a larger network with many paths. Adding backup links for fast layer 2 rerouting further complicates network management and control. When using policy-based forwarding it is possible to implement traffic engineering on strictly IP level without support from Layer 2 or using Layer 2.5 shim.

- 5) **Routing paths** can be found based on specific requirements of the packets, flows or aggregates. Normal IP routing finds a route only based on the destination address, but different metrics can be used to calculate the best path (lowest cost, shortest path, minimum air time, etc.). In multi-topology routing the cost of the path can be set different for different topologies i.e., depends on both the traffic requirements of the traffic class and the link properties. For example, a low-delay, low-bandwidth link would have low cost for real-time low bit-bitrate sensor traffic and a high-cost for bulk transfer. A high-delay, high-bandwidth satellite link would have the opposite costs (see, for example, Ref. [16] for more information). Security requirements may set some links non-preferred for sensitive information.

Routing can utilize instantaneous link states and capacities. Traffic load can be balanced over multiple paths considering specific requirements of traffic. Routing happens within network with no or little visibility of the end user.

Note that several of the mechanism above is designed based on the assumption that one flow occupies only a small portion of the link/path capacity. In mobile heterogeneous network where also very low-capacity network segments are present, one flow can occupy a major share of the path capacity. For such situations many admission control and traffic engineering techniques based on statistical multiplexing does not work very well.

In a network where a single entity (nation) can have control over each layer, utilizing all possible controls available in a coordinated manner on all layers would be a tempting idea. The main pitfall is the complexity that is involved with this approach. Often an expert is needed to consider how to use mechanism at one level, when interaction between two levels is planned, the complexity can be impossible to anticipate. For example, what is the relation of dynamic routing while there are multiple TCP connections over different round-trip times and congestion avoidance algorithms?

¹ Or even modem over voice.

The typical evaluation method where all network properties are fixed to a predefined scenario except for the mechanisms/parameter that is to be evaluated and running tests with different configuration of this mechanism will provide some results about the effect of that particular mechanism/parameter. However, this is seldom realistic and may lead to erroneous reasoning. In a real network there are continuous streams of unanticipated changes, not least from user reactions and behaviour changes. Using an emulation environment such as the one described in Annex B “Emulation based experimentation and the Anglova Scenario”, Annex C: “Experimentation Environment and Tools”, and Annex D: IST-124 Experimentation Execution” can be helpful to identify complex problems.

The following two principles should be used as guidelines when designing QoS mechanisms for a network:

- A requirement (like delay or reliability) shall be managed only by one network layer. Choose the layer that can best implement the requirement in the mission’s network. This reduces the risk for no-cooperating mechanism at different layers that might degrade the performance rather than improve the performance.
- Control loops on different layer should work on different time scales. Synchronisation effects across layers can lead to unpredictable performance [17].

If the above two principles cannot be followed for some reason, the system must be very carefully designed, evaluated, tested, and any critical parameters identified. Lastly, we must perceive the real events in the network and the descriptive models used when different actors interact with each other. Actors include both human and technical actors. For example, it cannot be assumed that demand for all other services stay unchanged if one service is disabled.

The QoS controls required from an operational perspective can be implemented by different layers as described above. Quite similar results can be achieved with diverse methods, e.g., packet marking can be used also for flow admission control. Different methods can be combined to provide the desired behaviour for the network, often resulting in a complex network configuration. However, when there is a problem and an expert is trying to understand why the system is not working as designed, very sophisticated mechanisms are a burden. Present network device configurations can have thousands of lines of near-identical configuration items and a small mistake may be easily overlooked [2].

It is expected that (partly) automated network configuration using Software Defined Networking (SDN) or configuration generation via NETCONF [18] or similar will become an integral part of future network configuration and maintenance and allow the mission planner to create more complex networks. The introduction of Network Function Virtualization (NFV) and accompanying management tools will most likely accelerate the automation process. However the knowledge of experts will still be necessary in order to understand the network problem that should be solved and the complexity of the network should be kept as low as possible.

I.5.1 Characteristics of QoS in Tactical Networks

IP Quality of Service, especially Differentiated Services, has evolved from the needs in a typical Internet topology where leaf networks have small number of flows, aggregating towards the network core where there is a bottleneck with large number of flows. This allows queuing and queue control to work well with good statistical multiplexing.

In tactical networks, the situation is different. There may not be any traffic aggregation on the IP level that results in congestion in the bottleneck queue, but the congestion takes place in the radio network. Also paths within a network segment are not many hops long (Figure I-4). Much of the packets sent by a node may be generated by the node itself.

Without knowledge of the current available capacity on the path, no resource guarantees can be made. The available capacity can also vary with an order of magnitude in an instance with a route change, when a military platform is moving out of coverage of a wideband radio network and is left with only a narrowband radio system. In these networks only prioritization can be applied resulting in a relative quality. If resource allocation (admission control) is static, i.e., there is no adaptive control; the network is very likely to behave badly if the available capacity is only a fraction of the design values.

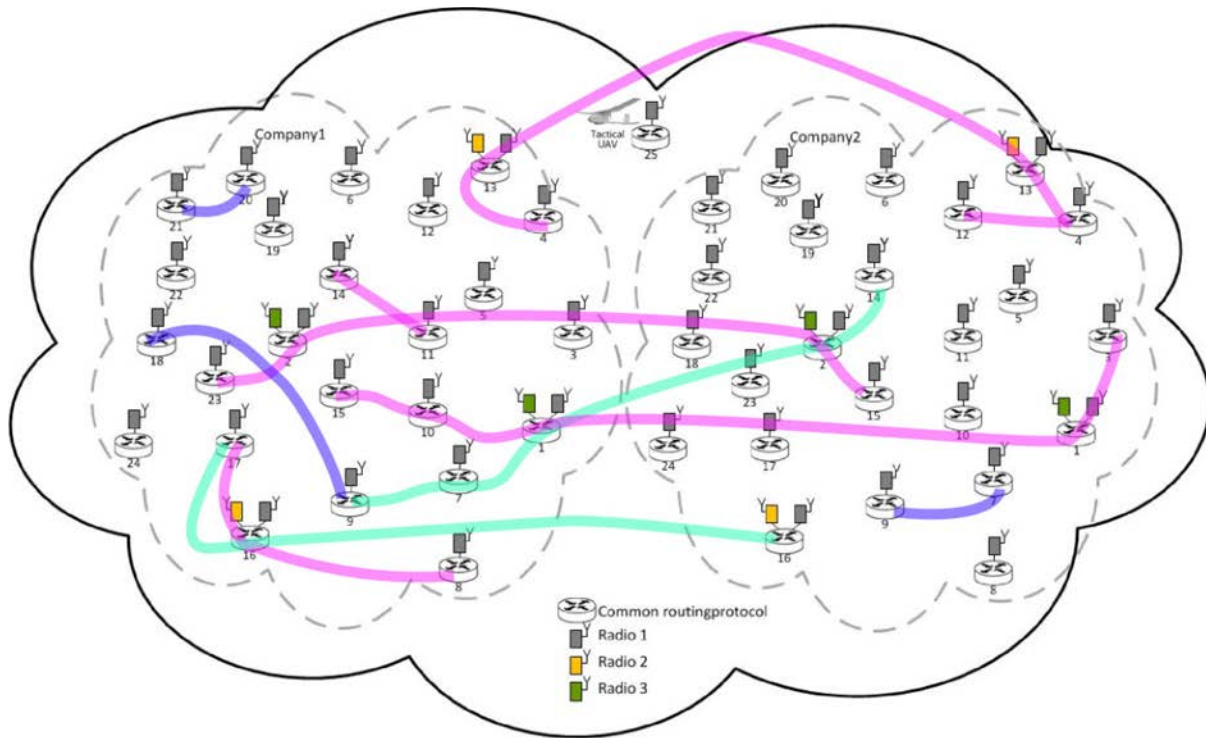


Figure I-4: Example of Short Paths without Bottleneck.

However, the stateless IP QoS mechanisms are not useless. Each node assigns traffic into different queues enforcing precedence locally. The local network may have good capacity but the uplink is congested because there is lots of traffic aggregated on it. In this case queue with priorities and capacity allocations works as intended. Discussion on different architecture's impact on can be found in Annex E.5

It is also important to note that even if not all devices and network segments are able to utilize IP QoS marking, it will be valuable in other parts. If traffic is marked according to application and priority with a common schema, other parts of the network can take appropriate actions to control traffic. Without marking there is only a single traffic class, best effort.

Traffic marking also helps with admission control. If the network capacity is severely limited, all packets with video, high-throughput data and low-priority data can be rejected before entering the network based on their Differentiated Services Code Point (DSCP) values. If multi-topology routing is used, service class marking can be used to guide traffic into right topology.

I.5.2 Visibility of Traffic Control Mechanisms

It is well known from a number of studies that user expectation will have an impact on how they perceive the service they receive [19]. This is an important aspect to remember when network services are described to users. The more accurate the estimate of expected received quality is (or if any service is received at all), the

more predictable will the user experience be. If the user selects a “wrong” application that the network cannot support, it may lead to severe degradation of the network and have a serious impact on the mission.

An example of such a situation could be a reconnaissance report. The soldier has identified an interesting target and has two options: generate a text-based description of the target or record a high-resolution video-stream. The first option can be sent as a short message while the latter will require high-bandwidth connection or a long time to transmit over a low-bandwidth connection. If the network cannot support transmission of the video, the result is that no information of the target is conveyed. See more discussion in Section I.4.

In another example, there exist two equal priority voice calls. The capacity available for voice calls is reduced for some reason, or a higher-priority call (in an MLPP environment [20]) is placed. There are not enough network resources to support both lower-priority calls. How should the network decide which of the calls to preempt? Pre-empt the one that is using most resources (longest path), one the one that has been active for the longest time, or based on some other criteria. The right answer is none of the above: the call that has the least value for the mission should be aborted. The remaining problem is to make the value of the call known to the network devices.

The policies used to make decisions must be carefully considered. For example, if there is very limited capacity and existing flows are prioritized over new ones, then there may be a temptation by the users to keep a call open to make sure a message can be delivered when needed. This is clearly a non-optimal situation for overall utilization of the resources. It should also be considered if different information objects can give the same value to the mission e.g., a reliable and in-time delivery of a short data message might be a sufficient replacement of the voice call.

I.6 SERVICE VIEW ON HETEROGENEOUS NETWORKS

There are a number of services that are desired in tactical networks. Some of these services might originate from dedicated radio networks with specific message formats but those messages are often at some point converted to IP network payloads. Each service has their own requirements but we can identify a few groups of services that share common characteristics and requirements.

In NATO C3 taxonomy, *Unified Communication and Collaboration Services* include following services [21]:

- Military Messaging Services;
- Informal Messaging Services;
- Fax Services;
- Calendaring and Scheduling Services;
- Video-based Communication Services;
- Audio-based Communication Services;
- Text-based Communication Services;
- Whiteboarding Services;
- Presence Services;
- Time Zone Data Distribution Services; and
- Application Sharing Services.

Not all of these are relevant to heterogeneous networks. Based on discussion in IST-124 group, the following groups of applications were identified (see Table I-1). Some selected services are discussed in depth later.

- **Network control** includes traffic that is necessary in order to keep the network operational. Timely, low-loss, low-delay delivery is important for routing messages. Other messages like key management or monitoring may not have as strict delay requirement.
- **Voice** is important in both full-duplex and push-to-talk modes. The former needs lower round-trip delay.
- **Video** has three functions: video-conference with similar delay requirements as full-duplex audio, live sensor streams and recorded sensor streams. Only the first one has strict delay requirements.
- **Situational awareness** includes also blue force tracking. There is no real-time requirement for delay.
- **Formal messages, real time** are typically short messages. Low-loss and low-delay are required for call for fires and similar messages using military messaging services.
- **Formal messages, non-real time** like orders and logistics messages can tolerate longer delays.
- **Informal messaging** includes chat and short messages that are low in volume. Emails may include large attachments.
- **Mass data, non-real time** such as maps, meteorology and oceanography (METOC) information, and software updates are large in data volume but they tolerate long delays and can be postponed, to wait for better connectivity.
- **Internet and remote access** to services not designed for low-capacity networks are sometimes needed. These include remote desktop sessions and/or internet services using middle-boxes to optimize for low-bandwidth networks.
- **Database queries and synchronized messages** do have delay requirements but typically lower than real time.

Table I-1: Network Characteristics Requirements for the Chosen Set of Applications in Order to Achieve Acceptable Fidelity in Heterogeneous Networks.

Service	Bandwidth	Loss	Delay
Network control	-	-	-
Voice	+	0	+
Video	++	0	0
Situational awareness	-	-	- (+)
Formal messages, real time	-	0	0 (++)
Formal messages, non-real time	+	-	--
Informal messaging	++	-	--
Mass data, non-real time	++	-	--
Internet and remote access	++	-	-
Database queries and synchronized messages	-	+	-

Key

--	< 100	20,00%	30 s
-	1000	5,00%	5 s
0		1,00%	1 s
+	16k	0,10%	< 250 ms
++	> 200k	0,01%	< 50 ms

Depending on the situation at hand, some applications provide more value for the mission than others as discussed in Section I.4. It is important to observe the impact of non-delivery of the service. Some of the applications listed above are not designed for tactical networks. They can be enterprise-type applications and not optimized for low-bandwidth connections. These may need some adaptation for low-capacity networks.

The packet loss requirement is often indicated as a single figure assuming a random loss process. Many applications and protocols can handle an isolated packet loss just fine. For example, a routing protocol using keep-alive messages typically has dead peer detection of three times the keep-alive interval. This protocol can then have up to 66% packet loss assuming every third message is reliably received. Track data has similar aspects; we can lose many messages as long there is not too long time between successful transmissions. Because the loss process is random, we set the loss percentage to a low value in the requirements to make sure that a sufficient number of messages reach their destination.

In the following section, we discuss some of the services in more detail.

I.6.1 Network Control

Transporting, e.g., routing information, is not a service by itself but because a network won't be functional without it, the network must allocate resources to carry network control traffic.

A dynamic network needs information on how it can relay messages across the network. This information is critical because if, for example, the connectivity information is wrong, messages will not reach their destination and/or consume system resources on sub-optimal routes.

Routing information and information supporting routing is collected on multiple levels:

- Link layer, e.g., radio can provide information of its peers and link quality. This information can be feed into IP routing and used as an input when calculating metrics.
- IP routing will use connectivity information. It may also use link quality and capacity as observed on the IP layer as one metric.
- Applications may form their own overlay networks on top of IP routing. Those need to exchange routing information as well and possibly collect path quality information too.

All this information exchange may result in excessive traffic if the parameters are not carefully tuned. Utilizing cross-layer information, especially IP-layer routing and application layer routing, can help as well as limiting the scope where detailed information is relayed. The amount of routing information depends on multiple aspects that are discussed in Annex E.

Another part of management traffic is related to security. This includes key management and policy updates. These are not as time-critical as routing information, but low-loss is preferred. Log messages and notifications of important network, system, and security related events can be important and time-critical.

I.6.2 Voice and Video

There are two types of military voice services with different requirements. Two-way telephony will have similar requirements as a normal phone call, although user expectations for quality may be lower by experience. In any case, the round-trip delay should be less than 500 ms. While low packet loss rate is important by itself, it is more critical that distortion free intervals are long enough, at least 1.3 seconds [22].

Another voice service is push-to-talk, where voice data is sent in real time with the same requirement for packet loss and distortion free intervals as two-way telephony but this service does not have as strict round-trip-time requirements since there is an expected delay for the peers to respond in any case.

Capacity required for voice is less than 10 kbit/s for the payload. For voice services, the impact of the added overhead of packet-based transport with encryption like IPSec can be very significant because of small payload packet sizes.

Video conferencing over tactical networks has limited use. The more common application to transport video media over tactical network is a streaming video from a surveillance camera. Acceptable delay depends on the use case: monitoring only has no strict requirements but if some counter-actions are performed, low-delay is required. Bit rates of video are typically from 64 kbit/s to megabits per second.

I.6.3 Situational Awareness

Maintaining accurate situational awareness, including positions of own troops (blue force tracking) and enemy observations does not typically have very strict delay requirements. Data may be prepared in combination with manual input to generate a recognized situational picture.

I.6.4 Sensor

Sensor data comes in many forms and can have quite varying requirements. Some sensors may require low-delay (i.e., ones tracking fast-moving targets) while others can tolerate much longer delays. Surveillance camera can send high-definition video needing large capacity while a movement detection sensor will send a short message only when it observes something. Track data is typically short messages sent with regular intervals.

In many sensor types, if there is older information that has not been yet sent before newer data is available, there is no use in sending the old data but the newest data should be sent instead. This requires the forwarding process to have an understanding about validity and relationship of data items, i.e., Quality of Information and Value of Information as discussed in Section I.4. That kind of functionality is currently not found in routers but requires some middleware or middle-boxes to interpret this information.

I.6.5 Real Time Formal Messages

Call for fire, close air support and alarms need low-delay delivery with high reliability. Application or middleware layer cannot help much if the network does not deliver the required service. Acknowledgments may take place on different levels like in the transport protocol, in the application, or even by manual action by the user. These messages are not large if there is no image or other media data associated with them. These require typically low-loss and real-time handling of the data packets in the routers.

I.6.6 Informal Messaging

Informal messaging can have similar purpose as a voice call. The delay requirements and bandwidth demand is lower than voice for chat and short messages. In some environments, chat can substitute voice as the method to communicate information. Email attachments may result in large message sizes that can be compressed with middle-boxes, e.g., by down sampling image data.

I.6.7 Non-Real Time Mass Data

This information does not have real time requirements, but has a value for the operation. Examples include map data, picture synchronization to improve situational awareness, other database updates, and software updates. The data volume may be large.

For some of these services other transport methods can be alternatives e.g., via physical media or Disruption Tolerant Networking (DTN) methods.

I.6.8 Internet and Remote Access

There may be situations where some information from the Internet or the headquarter systems are needed at the tactical edge. Low network capacity and security aspects may make it impossible to access those services directly. In most cases, there is not a direct Internet connection but the connection is established via a gateway that handles both the necessary filtering between potentially different security classifications and adaptation of the data to low-capacity transmission. This is handled as a best effort, low-priority traffic.

I.6.9 Database Queries and Synchronized Messages

Various information systems do distribute information over network using database synchronization or via remote access to databases. Those need often adaptation to work over long-delay and high-loss data channels.

I.7 SUMMARY

We can have two types of traffic in tactical and battlefield networks: one that stays always within a nation and one that will cross nation boundaries. For the former case, it is up to the nation to select a proper set of QoS mechanisms. For the latter case, it must be agreed on a joint, standards-based approach that is enforced at inter-nation points. The interconnection should be the least but sufficient common denominator of mechanisms used in participating networks. The principles for QoS management need to be aligned for this to be possible.

Wired, optical networks have very high throughput and few bit errors. Heterogeneous mobile networks typically have much more unpredictable connectivity and frequent topology changes because of relocating units, communication link failures, and enemy actions. In those networks, capacities are also much lower and it may be worthwhile to make resource reservations based on individual application flows.

Today, typically, communication from one tactical network segment in one nation to a tactical network segment in another nation happens at the Head Quarter (HQ) level following the troop's hierarchy and there is no transit traffic in tactical network segments. It can happen that all or part of a deployed unit loses its uplink towards the HQ resulting in a partitioned domain. One solution to improve robustness is to rely on the network capacity of other units as backup communication. The network designs considered in Annex E all implement a meshed network structure at the tactical edge in order to improve connectivity internal to a unit that might have teams from different coalition partners and to increase the robustness for the communication with the HQ. Consideration for separation of different networking domains and information domains will likely lead to sub-optimal routing as seen from the communication perspective. This shortcoming must be taken into account.

Different types of proxies may be designed and used to optimize the communication to be more suitable for the available network and link characteristics. While for example transcoding by each network boundary leads into inferior end-to-end quality and is discouraged, optimization for voice calls between networks may be beneficial. These can also work to interpret signalling flows between different architectures. Also mobility support, if not supported network-wide, can benefit from middle-boxes.

We recommend the following related to QoS:

- All IP traffic is marked with proper DSCP values per service class and precedence. Use of standard marking, e.g., STANAG 4711 is recommended. DSCP values can be used to disallow traffic on some links or topologies if multi-topology routing is used.
- Even if one part of the network does not need or is not able to enforce QoS treatment, it must preserve the QoS information associated with the traffic including classification, priority, and precedence. This applies to transit networks.

- Admission control must be enforced at network edges and within the network. Each service class has its own allowed capacity.
- A QoS requirement (like delay or reliability) shall be managed only by one network layer. Choose the layer that can best implement the requirement in the mission's network. This reduces the risk for no-cooperating mechanism at different layers that might degrade the performance rather than improve the performance.
- Control loops on different layer should work on different time scales. Synchronisation effects across layers can lead to unpredictable performance.
- Three states of network health (normal, reduced, last effort) are to be considered in the network design. Network device must be able to alter their configuration to match the current state autonomously by observing the network, via network control, or by the operator.
- Core network or LAN traffic may need to be adapted to a more suitable form for lower data rate channels either natively by the application or by using middle-boxes and gateways. With the latter solutions, the implications of for the security architecture must be taken into account.
- Routers must be aware of link statuses. Regarding QoS, it is important to know the present available capacity of the link and how occupied the queues are.
- There is no QoS mechanism in tactical environment that can provide 100% guarantee on commitments. The system must be able to provide a reasonable handling for different traffic.
- Situation-aware, automatic network configuration should be implemented, and it calls for more intelligent node and radio configuration. Cognitive, Software Defined Networking and Radio (SDN, SDR) may provide tools to implement this in interoperable manner.
- Recognize that many of the Resource Management (RM) and QoS mechanisms are meant for point-to-point links. Their use on common radio channel needs to be evaluated case by case.
- The information that best serves the mission's objectives, should be available were it is needed and in time. For this to happen the network must establish a notion of the QoI and VoI and convey this information to the QoS and RM mechanisms.

The overarching goal for the QoS and RM mechanisms is to make sure that the current operating state of the network is identified in order to keep the network operational and to ensure that the resources are always used to deliver the most important information for the mission to the right destinations.

1.8 REFERENCES

- [1] Armitage, G.J., "Revisiting IP QoS: Why Do We Care, What Have We Learned? ACM Sigcomm 2003 Ripqos Workshop Report," *SIGCOMM Comput. Commun. Rev.*, Vol. 33, no. 5, pp. 81-88, Oct. 2003.
- [2] X. Xiao, *Technical, Commercial and Regulatory Challenges Of QoS*. Morgan Kaufmann, 2008.
- [3] Baker, F., and Fairhurst G. (Eds.), "IETF Recommendations Regarding Active Queue Management," RFC Editor; RFC 7567 (Best Current Practice); RFC Editor, Fremont, CA, USA, pp. 1-31, July 2015.
- [4] Carpenter, B., "Middle-Boxes: Taxonomy and Issues," IETF *RFC 3234*, 2002.
- [5] Jiang, W. and Schulzrinne, H., "Comparison and Optimization of Packet Loss Repair Methods on VoIP Perceived Quality Under Bursty Loss," *Proceedings of the 12th International Workshop on Network and Operating Systems Support for Digital Audio and Video*, 2002, pp. 73-81.

- [6] Hallingstad, G., and Oudkerk, S., “Protected Core Networking: An Architectural Approach to Secure and Flexible Communications,” *IEEE Communications Magazine*, Vol. 46, Issue 11, IEEE, Nov 2008.
- [7] Heegaard, P.E. and Trivedi, K.S., “Network Survivability Modelling,” in *Computer Networks*, Vol 53, Issue 8, 2009, pp. 1215-1234.
- [8] Elmasry, G.F., McCann, C.J. and Welsh, R., “Partitioning QoS Management for Secure Tactical Wireless ad hoc Networks,” in *IEEE Communications Magazine*, Vol 43, Issue 11, pp. 116-123, Nov. 2005.
- [9] Galanis, S., “The Value of Information under Unawareness”, *Journal of Economic Theory*, Vol. 157, pp. 384-396, May 2015.
- [10] Quiggin, J., “The Value of Information and the Value of Awareness”, *Theory and Decision*, 2015, DOI: 10.1007/s11238-015-9496-x.
- [11] Howard, R.A., “Information Value Theory”, *IEEE Transactions on Systems Science and Cybernetics*, Vol. SSC-2, No. 1, August 1966, pp. 22-26.
- [12] Heckerman, D., Horvitz, E., and Middleton, B., “An Approximate Nonmyopic Computation for Value of Information”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 15, No. 3, March 1993, pp. 292-298.
- [13] Kalevi, K., *Differentiated Services for the Internet*. Macmillan Publishing Co., Inc., 1999.
- [14] Rosen E., Viswanathan, A., and Callon, R., “Multiprotocol Label Switching Architecture”, IETF *RFC 3031*, Jan. 2001, <http://www.ietf.org>.
- [15] Robert, B., Clark, D., and Shenker S. “Integrated Services in the Internet Architecture: An Overview,” IETF *RFC 1633*, 1994.
- [16] Hauge, M., Brose, M.A., Sander, J., and Andersson, J., “Multi-Topology Routing for QoS Support in the CoNSIS Convoy MANET,” *Proceedings MCC*, Gdansk, Polen, pp. 1-8, Oct. 2012.
- [17] Vikas, K., and Kumar. P.R. “A Cautionary Perspective on Cross-Layer Design,” *IEEE Wireless Communications* 12.1 (2005): pp. 3-11.
- [18] Rob, E., Bjorklund, M., and Schoenwaelder, J. “Network Configuration Protocol (NETCONF),” IETF *RFC 6241*, 2011.
- [19] Bouch, A., Kuchinsky, A., and Bhatti, N. “Quality is in the Eye of the Beholder: Meeting Users’ Requirements for Internet Quality of Service,” *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 2000.
- [20] Baker F., and Polk, J., “Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite,” IETF *RFC 4542*, 2006, <http://www.ietf.org>.
- [21] Bloebaum, T.H., Hannay, J.E., Hedenstad, O.-E., Haavik, S., and Lillevold, F., “Architecture for the Norwegian Defence Information Infrastructure (INI) – Remarks on the C3 Classification Taxonomy,” Norwegian Defence Research Establishment (FFI) Tech. Rep. FFI-rapport 2013/01729, 2013.

- [22] Bardy P., “A Statistical Analysis of On-Off Patterns in 16 Conversations,” *The Bell System Technical Journal*, Vol. 47, pp. 73-91, Jan. 1968.



Annex J – QoS STANDARDS

Daniela Ghezzi and Maurizio Bisio

Leonardo – Società per azioni
ITALY

Markus Peuhkuri

Aalto University
FINLAND

J.1 BACKGROUND

The Quality of Service (QoS) is a concept that has been associated to Communications Networks since the beginning, even if its definition and its scope have been influenced by the underlying technology: for instance, in analogue networks crosstalk was one of the major issues, while, with digital networks and even more with packet networks, the QoS issues have changed and in addition, with the introduction of the layered structure of the systems, have assumed themselves a layered structure.

Therefore, in the following we will focus on QoS issues related to IP networks and an overview of QoS standards applicable to IP networks, and in particular to Mobile IP networks, will be presented.

A very effective analysis on QoS issues applied to IP has been performed in Ref. [1], which shows that *“there are a lot of terms related to this [QoS-related terminology] issue, but they are often used inappropriately. It is clear that the confusion should be eliminated”*. This condition of uncertainty is noted also in Ref. [2], par. 5.1, where it is stated that:

“the term quality of service (QoS) is extensively used today, not just in the telecommunications world in which it has its roots, but increasingly regarding broadband, wireless and multimedia services that are IP-based. Networks and systems are gradually being designed in consideration of end-to-end performance required by user applications; however, the term QoS is usually not well defined, is used loosely, or worst of all, misused”.

As indicated in Ref. [1], there are three main standardization bodies that should be taken into account for their works on the QoS issues, namely the International Telecommunications Union (ITU), the European Telecommunications Standards Institute (ETSI) and the Internet Engineering Task Force (IETF).

Taking into account that:

- IETF RFCs also refer to the ITU-T Recs and in particular to Y.1541 as a basis for a QoS model (cf. RFC 5976); and
- In Ref. [1], it is stated that: *“the ITU and ETSI approaches to QoS-related terminology are almost the same. In fact, both organizations adopted the concepts of each other while developing the notion of QoS”*;

we will take the ITU-T Recommendations as a reference in this Annex.

As a preliminary statement, it should be noted that among various ITU-T Recs. there are different high level definitions for QoS: for instance, in Ref. [3], par. 2.2, the QoS is the *“totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service”*, while in Ref. [2], par. 3.2, the QoS is indicated as *“the collective effect of service performances, which determine the degree of satisfaction of a user of the service”*, and also the scope of the QoS in Ref. [3], par. 1.2, is enlarged, since is meant as composed by Network Performance and Non-network Performance such as *“provision time, repair time, range of tariffs and complaints resolution time”*.

On the contrary, we prefer to maintain the “QoS” term associated to the network issues, excluding the “business” aspects listed above. To this extent, we prefer to adopt the terminology adopted in Ref. [4], Figure 1, reported in Figure J-1, where instead of Network Performance the term “Network QoS” is used.

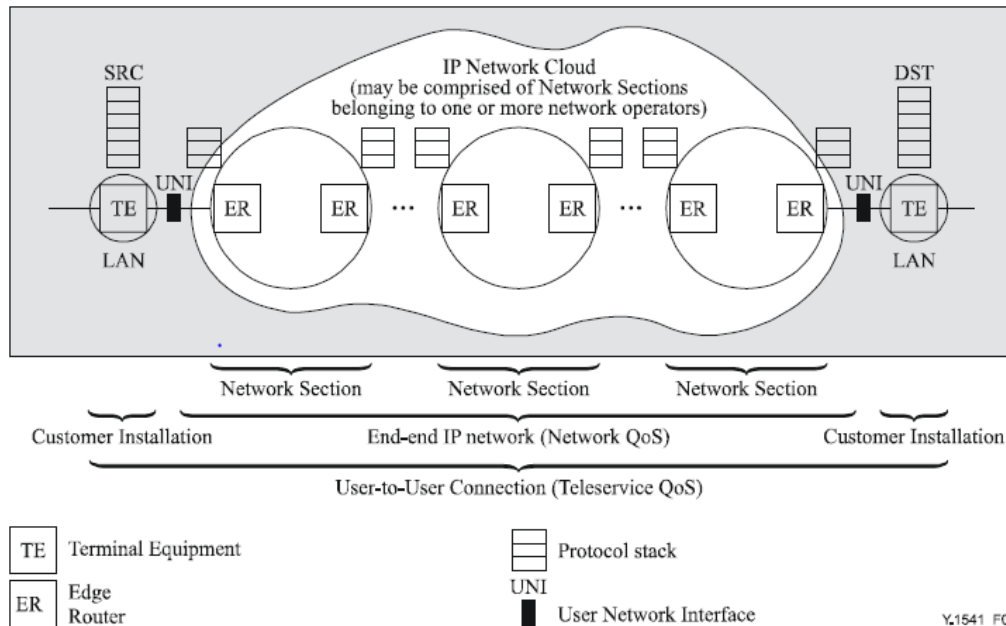


Figure J-1: UNI (User Network Interface)-to-UNI Reference Path for Network QoS Objectives.

In order to provide a more precise definition of the term “Quality of Service”, we will focus on the word “service”.

The most appropriate definition of **service** for our context can be found in Ref. [5], par. 3.2:

“IP-based service: An IP-based service is defined as a service provided by the service plane to an end user (e.g., a host (end system) or a network element) and which utilizes the IP transfer capabilities and associated control and management functions, for delivery of the user information specified by the service level agreements”.

In addition, this definition introduces the layered approach referred to previously, since an IP-based service belongs to the Application Layer (Layer 7), while the IP Transfer Capability, which “is defined as the set of network capabilities provided by the IP layer. It may be characterized by the traffic contract as well as performance attributes supported by control and management functions of the underlying protocol layers” (see Ref. [5], par. 3.4), constitutes the actual method by which an IP Network Service (Layer 3), “defined as a data transmission service in which the data passed across the interface between the user and provider is transferred in the form of IP (Internet Protocol) packets (sometimes called datagrams)” (Ref. [5], par. 3.3), is provided.

Summarizing an IP-based Service is provided by means of an IP Network Service, which in turn is implemented via an IP Transfer Capability. To avoid that these terms remain too “philosophical” and to link them to Figure J-1, IP-based services are associated to the Teleservice QoS and IP Transfer Capabilities are associated to the Network QoS.

Examples of IP-based services are listed in Ref. [5], Table 1, represented in Table J-1.

Table J-1: Examples of IP-Based Services with their Guaranteed Performance Attributes.

IP-based service class	IP-based service	Guaranteed performance attribute(s) for IP-based service
Conversational	• Internet telephony • Videoconferencing • Video telephony • Interactive games	Loss, delay and delay variation
	• Internet shopping • Electronic data exchange	Loss
	• Remote login	None
Messaging	• Voice e-mail • Internet fax • Video e-mail • Group e-mail	None
Retrieval	• Web browsing • News retrieval • File downloading	None
	• Video-on-demand	Loss and delay variation
Distribution Service without Individual presentation control	• Electronic newspaper • Internet advertising	None
	• Live broadcasting	Loss
Distribution Service with Individual presentation control	• News-on-demand • Video-on-demand	Loss and delay variation

IP Transfer Capabilities are dealt with in Ref. [6], par. 6:

“In order to offer multiple classes of QoS to multiple applications and to optimize the usage of network resources, IP-based networks should be capable of providing multiple transfer capabilities.

Three IP transfer capabilities are defined:

- *Dedicated Bandwidth (DBW) IP transfer capability.*
- *Statistical Bandwidth (SBW) IP transfer capability.*
- *Best-Effort (BE) IP transfer capability.*

This set of IP transfer capabilities are based on current IP service models and this set may be extended in the future”.

In addition a qualitative set of QoS parameters associated to each IP Transfer Capability is provided:

- *“The DBW capability can be associated with specified loss commitments (IP Loss Ratio, IPLR) and specified delay commitments (IP Transfer Delay, IPTD and IP Delay Variation, IPDV)” (Ref. [6], par. 6.1.2);*
- *“The SBW capability may be associated with a specified packet loss commitment” (Ref. [6], par. 6.2.2);*
- *“There are no QoS commitments specified” (Ref. [6], par. 6.3.2) for the BE capability.*

ANNEX J – QoS STANDARDS

In order to provide a quantitative definition of the QoS commitments stated above, in Ref. [4], Table 1, a set of 6 Network QoS Classes is defined, as represented in Table J-2, with also 2 Provisional QoS Classes (see Ref. [4], Table 3), as represented in Table J-3.

Table J-2: IP Network QoS Class Definitions and Network Performance Objectives.

Network performance parameter	Nature of network performance objective	QoS Classes					
		Class 0	Class 1	Class 2	Class 3	Class 4	Class 5 Unspecified
IPTD	Upper bound on the mean IPTD (Note 1)	100 ms	400 ms	100 ms	400 ms	1 s	U
IPDV	Upper bound on the $1 - 10^{-3}$ quantile of IPTD minus the minimum IPTD (Note 2)	50 ms (Note 3)	50 ms (Note 3)	U	U	U	U
IPLR	Upper bound on the packet loss probability	1×10^{-3} (Note 4)	1×10^{-3} (Note 4)	1×10^{-3}	1×10^{-3}	1×10^{-3}	U
IPER	Upper bound	1×10^{-4} (Note 5)					U

Table J-3: Provisional IP Network QoS Class Definitions and Network Performance Objectives.

Network performance parameter	Nature of network performance objective	QoS Classes	
		Class 6	Class 7
IPTD	Upper bound on the mean IPTD	100 ms	400 ms
IPDV	Upper bound on the $1 - 10^{-5}$ quantile of IPTD minus the minimum IPTD (Note 1)	50 ms	
IPLR	Upper bound on the packet loss ratio	1×10^{-5}	
IPER	Upper bound	1×10^{-6}	
IPRR	Upper bound	1×10^{-6}	

A guidance in associating IP-based services (i.e., Teleservices or Applications) to Network QoS Classes is provided in Ref. [4], Table 2, as represented in Table J-4.

The QoS standards analysed in Table J-4 provide qualitative definitions and quantitative performance objectives for the QoS, but do not specify how those objectives can be achieved. ITU-T Rec. Y.1291 has a central role for this purpose.

In fact, in Ref. [7], par. 5, it is stated that “*this Recommendation identifies a set of generic QoS network mechanisms and provides a structure for them. Ultimately the network mechanisms are to be used in combination to deliver the satisfactory collective effect of varying service performance required by a wide range of applications*”: it should be noted that Y.1291 is related to Network QoS.

Table J-4: Guidance for Network QoS Classes.

QoS class	Applications (examples)	Node mechanisms	Network techniques
0	Real-time, jitter sensitive, high interaction (VoIP, VTC)	Separate queue with preferential servicing, traffic grooming	Constrained routing and distance
1	Real-time, jitter sensitive, interactive (VoIP, VTC).		Less constrained routing and distances
2	Transaction data, highly interactive (Signalling)	Separate queue, drop priority	Constrained routing and distance
3	Transaction data, interactive		Less constrained routing and distances
4	Low loss only (short transactions, bulk data, video streaming)	Long queue, drop priority	Any route/path
5	Traditional applications of default IP networks	Separate queue (lowest priority)	Any route/path
NOTE – Any example application listed in Table 2 could also be used in Class 5 with unspecified performance objectives, as long as the users are willing to accept the level of performance prevalent during their session.			

These QoS network mechanisms are aimed “for controlling the network service response to a service request, which can be specific to a network element, or for signalling between network elements, or for controlling and administering traffic across a network” (Ref. [7], par. 6) and are called QoS building blocks, which “are organized into three planes:

- *Control Plane, which contains mechanisms dealing with the pathways through which user traffic travels. These mechanisms include admission control, QoS routing, and resource reservation.*
- *Data Plane, which contains mechanisms dealing with the user traffic directly. These mechanisms include buffer management, congestion avoidance, packet marking, queuing and scheduling, traffic classification, traffic policing and traffic shaping.*
- *Management Plane, which contains mechanisms dealing with the operation, administration, management aspects of the network. These mechanisms include Service Level Agreement (SLA), traffic restoration, metering and recording, and policy” (Ref. [7], par. 6).*

The QoS building blocks are depicted in Ref. [7], Figure 1, as represented in Figure J-2.

As indicated in Ref. [7], par. 10:

“A comprehensive QoS solution typically employs multiple building blocks across the Control Plane, Data Plane and Management Plane. QoS parameters therefore need to be exchanged between the various building blocks. These parameters include transaction performance at the packet level (e.g., delay and packet loss) and service reliability/availability expectations in the form of traffic priority levels for specific network functions such as admission control and traffic restoration”.

QoS signalling is a mechanism to convey these parameter values between the QoS building blocks and, more precisely, it:

“is mainly for conveying application (or network) performance requirements, reserving network resources across the network, or discovering QoS routes. Depending on whether the signalling information is part of the associated data traffic, QoS signalling may be effected in or out of band [...] depending on whether the signalling path is closely tied to the associated data path, QoS signalling may be viewed as path coupled or decoupled” (Ref. [7], par. 10.1).

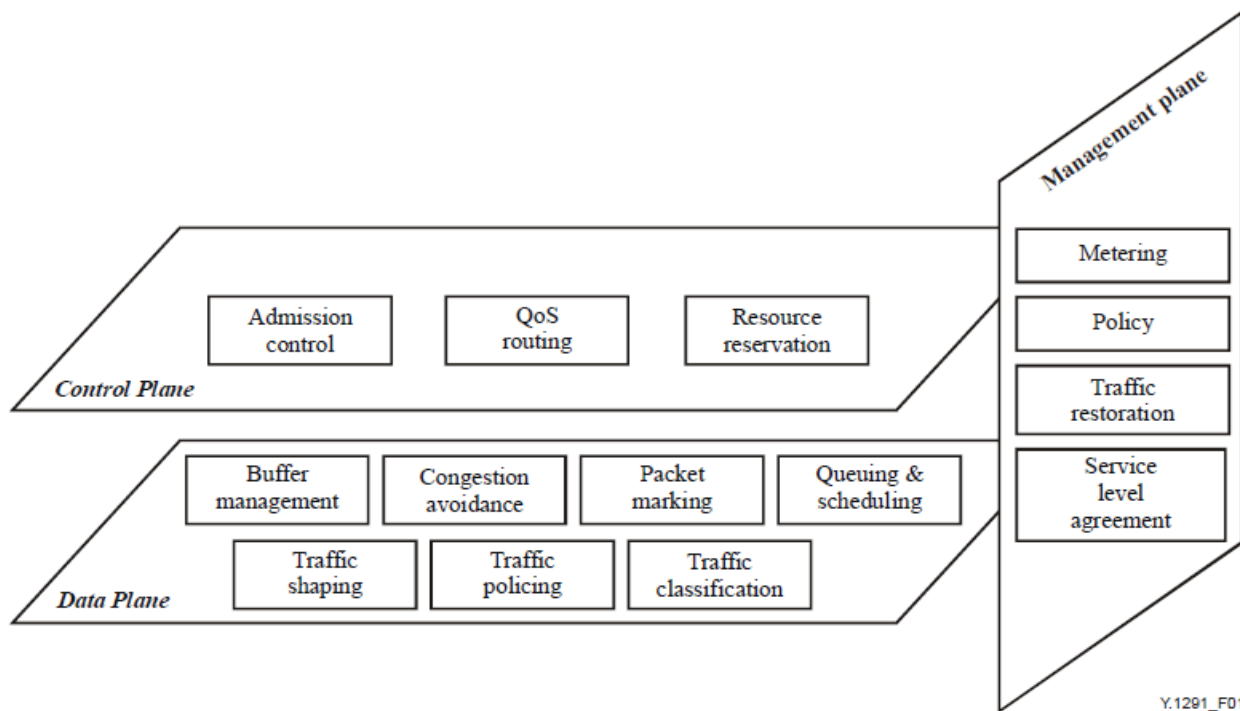


Figure J-2: QoS Building Blocks.

J.2 OVERVIEW OF MILITARY STANDARDS RELATED TO QOS

J.2.1 TACOMS STANAGS

TACOMS STANAGs “specify network protocols, interfaces, and related functionality to create a federated network. [...] The TACOMS standardization methodology consisted of [...] specification of a network QoS framework” (Ref. [8], par. 1.5).

In particular, in Ref. [8], par. 4.3, it is stated that “to support network and end-to-end user services across TFNs, a comprehensive QoS concept is defined”, with the definition of two Traffic Handling Classes (THCs): the Connectionless (CL) THC, “specified to handle IP packets”, and the Connection-Oriented (CO) THC, “specified to handle full-duplex calls, video, and multimedia”.

The CO THC is dealt with in Ref. [9], where in Appendix 7 to Annex B, par. 3.5, it is stated that “the QoS requirements of a call are derived from the call signaling. [...] Based on the H.245 call signaling, calls are divided into three distinct CO Classes of Service (CO CoS). [...] It is assumed that not all NEs will support all the CO CoS, but the voice CO CoS shall be supported”. The CO CoS are shown in Ref. [9], Table B-9, as represented in Table J-5.

It should be taken into account that, even if STANAG 4643 provides for a signalling protocol for the CO THC, this is intended only for call establishment without any resource reservation over the TACOMS IOP (Interoperability Point).

The CL THC is dealt with in Ref. [10], where it is stated in Annex D, par. 2, that “the TACOMS IP QoS is based on the Diffserv architecture” and in Appendix 3 to Annex D, par. 3.5 that “the TACOMS IP QoS specifications are concretised in three areas: Packet Marking Function, [...] Per Hop Behaviour specifications, [...] and DSCP Assignment”.

Table J-5: TACOMS CO CoS.

CO CoS	Call Characteristics Defining Each CO CoS	Network Capabilities Specifically Required for Each CO CoS	Example of User Services for Each CO CoS
Voice	A call that signals only one audio media stream in each direction, or only one at all, even if the call signals various alternative voice codecs using alternative audio capabilities.	Support of the voice coding protocols and voice trans-coding procedures specified in STANAG 4643 Annex D.	• Telephony • Voice intercom • Half-duplex telephony
Constant Bit Rate (CBR) Data	A call that signals only one data media stream in each direction, or only one at all, even if the call signals various alternatives data bit rates using alternative data capabilities.	Support of the CBR data coding protocols specified in STANAG 4643 Annex D. The actual traffic of the call may not have constant bit rate, but the network has to be prepared to support it.	• SCIP (encrypted voice and low-rate data) • Legacy tactical data
Multimedia	A call that signals one or more video or multimedia streams, or more than one media stream in at least one direction.	Support of multimedia, video and voice coding protocols specified in STANAG 4643 Annex D.	• Low-rate video • High-rate video • Still picture • Videoconference • Streaming multimedia

In particular, the DSCP (Differentiated Services Code Point) Assignment is specified in Ref. [10], Tables D-1 and D-2, as represented in Table J-6 and Table J-7.

Table J-6: DSCP Assignment for C6/7, EF (Expedited Forwarding), AF (Assured Forwarding), BE (Best-Effort) and PHBs (Per Hop Behaviour).

Type of Services	Example Flows	DSSP		Dec.
		Binary	Dec.	
Critical Network Control	• IP layer keep alive • Critical control messages	111000	56	CS6/7
Non-Critical Network Control	• Routing (e.g., RIP, OSPF, BGP) • Network services (e.g., DNS, DHCP) • High-priority management (e.g., SNMP Traps) • ICMP error messages	110000	48	

Type of Services	Example Flows		DSSP		Dec.
			Binary	Dec.	
Voice and CBR data	- VoIP - SCIP applications - Circuit emulation over IP		101110	46	EF ⁽¹⁾⁽²⁾
Time-critical data and interactive multimedia	- Time-critical app. (e.g., air traffic control, Tactical Data Links) - Multimedia conferencing	P1	100010	34	AF41 ⁽³⁾
		P2	100100	36	AF42
		P3	100110	38	AF43
Non-interactive multimedia	Multimedia streaming	P1	011010	26	AF31 ⁽³⁾
		P2	011100	28	AF32
		P3	011110	30	AF33
Transactional	- Client-server applications (DAP, LDAP, DNS, etc.) - Web-based applications	P1	010010	18	AF21 ⁽³⁾
		P2	010100	20	AF22
		P3	010110	22	AF23
Bulk transfer	- File transfer - Messaging - Replications	P1	001010	10	AF11 ⁽³⁾
		P2	001100	12	AF12
		P3	001110	14	AF13
Best Effort	Other applications		000000	0	BE

Table J-7: DSCP Assignment for Class Selector (CS) Codepoints.

Type of Services	Example Flows	DSCP			Assigned PHB
		Name	Binary	Decimal	
Critical Network Control	- IP layer keep alive - Critical control messages	CS7	111000	56	CS6/7
Non-Critical Network Control	- Routing (e.g., RIP, OSPF, BGP) - Network services (e.g., DNS, DHCP) - High-priority management (e.g., SNMP Traps) - ICMP error messages	CS6	110000	48	CS6/7

Type of Services	Example Flows	DSCP			Assigned PHB
		Name	Binary	Decimal	
Signalling	• Signalling for VoIP • Signalling for multimedia • Signalling for SCIP calls	CS5	101000	40	AF41
	Reserved	CS4	100000	32	AF31
	Reserved	CS3	011000	24	AF21
Management	• Non-critical management (e.g., SNMP, COPS, telnet)	CS2	010000	16	AF11
	Reserved	CS1	001000	8	AF12
Default (Best-Effort)	• Other applications	CS0	000000	0	BE

J.2.2 STANAG 4711 (Under Ratification)

STANAG 4711 is still under ratification and it is composed by two different documents:

- The main document that constitutes the actual STANAG 4711, where the agreement of nations to use the associated AComP publication is recorded;
- The AComP-4711 document, that contains the technical material on the “Interoperability Point QoS”.

AComP-4711 is composed of a large part of informative text, while only Chapter 3 is normative.

In Ref. [11], par. 3.2, “*the functionality needed to realize connectionless IP QoS*” is defined, and namely:

- Traffic Marking, that “*shall be done in the Differentiated Services Code Point Field of the IP header*” (Ref. [11], par. 3.2.1); the use of the DSCP field is defined as represented in Table J-8.

Unfortunately, the term “Precedence” is used instead of the term “Priority”, causing some confusion between the Military Precedence related to the operational role and the Packet Priority related to the scheduling of the packet.

Table J-8: DSCP Field Specification.

DSCP bit 1(MSB)	DSCP bit 2	DSCP bit 3	DSCP bit 4	DSCP bit 5	DSCP bit 6	ECN bit 1	ECN bit 2
ServiceClass SC0-SC7			Precedence (4 levels)		0: CL	Not used	Not used
					1: CO		

- Service Classes (SCs), “*which are based on RFC 4594 and RFC 5127. These definitions are modified to be better in line with military requirements*” (Ref. [11], par. 3.2.2). The SCs are listed in Ref. [11], Table 4, as represented in Table J-10.

However, the definition of the values of SCs to be included in the DSCP field is not formally provided, even if can be deduced from some examples in Ref. [11], par. 3.5, as represented in Table J-11.

Table J-9: Service Classes and their Quality Constraints.

Service Class	Tolerance To		
	Loss	Delay	Jitter
Circuit Emulation (TDMoIP) (SC7)	Very Low	Very Low	Very Low
Signalling, OAM, Network MGMT (SC6)	Low	Low	Medium
Voice (SC5)	Low	Low	Medium
Video (SC4)	Low – Medium	Low	Low
Transaction Messaging (SC3)	Low – Medium	Medium	Medium
Low-Latency Data (SC2)	Low	Low – Medium	High
High-Throughput Data (SC1)	Low	Medium – High	High
Low-Priority Data (SC0)	High	High	High

Table J-10: SC Values.

Service Class	BitCode
SC0	000xxx
SC1	001xxx
SC2	010xxx
SC3	011xxx
SC4	100xxx
SC5	101xxx
SC6	110xxx
SC7	111xxx

- Treatment Aggregates (TAs), that are based on RFC 5127 and “*can be used for mapping services to fewer than eight forwarding queues within network*” (Ref. [11], par. 3.2.3). 4 TAs are listed in Ref. [11], Table 5, as represented in Table J-12.

However, the definition of which SCs are associated to each TA is not provided, even if, from the tables in Ref. [11], par. 2.13.1, it can be deduced that an implicit association could be as represented in Table J-12.

- Military Precedence handling, where “*Military Precedence is handled as a transmission priority on IP layer*” (Ref. [11], par. 3.2.4): Military Precedence is mapped into the values of the IP Military Precedence Level (IP MPL), with the already described confusion between the words Precedence and Priority. The list of values is provided in Table 6, including the type of traffic (CL or CO), as represented in Table J-13.

Table J-11: Treatment Aggregates and their Quality Constraints.

Treatment Aggregate	Tolerance To		
	Loss	Delay	Jitter
Real-Time	Very Low	Very Low	Low
Near Real-Time	Low	Low – Medium	Medium
Assured Elastic	Low	Medium	High
Elastic	Medium	Medium – High	High

Table J-12: Association of SCs to TAs.

Treatment Aggregate	Service Class
Real-Time	SC5, SC7
Near Real-Time	SC4, SC6
Assured Elastic	SC2
Elastic	SC0, SC1

Table J-13: Mapping between Military Precedence Level and DSCP-Coding.

Precedence-Level	IPMPL-DSCP
CL-Flash	xxx 010
CL-Immediate	xxx 100
CL-Priority	xxx 110
CL-Routine	xxx 000
CO-Flash	xxx 011
CO-Immediate	xxx 101
CO-Priority	xxx 111
CO-Routine	xxx 001

Substantially, STANAG 4711 provides for a DiffServ QoS for CL and CO traffic, but with a mapping of DSCP values towards services, as suggested in Ref. [11], Table 7, that is different from the mapping defined in the TACOMS STANAG 4644 (e.g., “H.323/SIP signalling” is associated to DSCP 52 in STANAG 4711, whilst “Signalling for VoIP” is associated to DSCP 40 in TACOMS STANAG 4644).

In addition, even if in the informative part (Ref. [11], par. 2.13.1), STANAG 4711 defines performance targets associated to QoS Classes that are quite different from the civilian ones defined, for instance, in the ITU-T Rec. Y.1541, and are referred not to the end-to end path, but to an individual network, in the hypothesis that the end-to-end path is composed by no more than 4 individual networks.

The values are provided in Ref. [11], par. 2.13.1, Tables 2 and 3, for tactical core networks and tactical networks and represented in a “merged” table in Table J-14.

Table J-14: Performance Targets Applicable for Tactical Core Networks and Tactical Networks.

Treatment Aggregate	Service Class	QoS Target For Tactical Core Networks	QoS Target For Tactical Networks
Real-Time (1)	Circuit Equivalent	Delay (D) < 20ms Jitter (J) < 5ms Loss (L) < 0.1% MOS $\geq$ 3.9	Delay (D) < 20 ms Jitter (J) < 5ms Loss (L) < 0.1% MOS $\geq$ 3.9
Real-Time (2)	Telephony Equivalent	Delay (D) < (28 + P)ms Jitter (J) < 20ms Loss (L) < 0.5% MOS $\geq$ 3.9	Delay (D) < 40ms Jitter (J) < 15ms Loss (L) < 0.1% MOS $\geq$ 3.0
Near-Real-Time	Signalling Video	Delay (D) < (60 + P)ms Jitter (J) < 30ms Loss (L) < 1%	Delay (D) < 150 ms Jitter (J) < 50ms Loss (L) < 1%
Assured Elastic	Low-Latency Data	Delay (D) < (60 + P)ms Loss (L) < 1%	Delay (D) < (150 + P)ms Loss (L) < 1%
Elastic	High-Throughput Data Low-Priority Data	Loss (L) < 1%	Loss (L) < 2%

Finally, in the informative part (Ref. [11], par. 4), STANAG 4711 introduces a definition of the CO QoS that extends the CO paradigm defined in TACOMS, because STANAG 4711 foresees also a stateful mode to be associated to CO QoS, with signalling, resource reservation, QoS routing and military precedence and preemption.

J.3 APPLICABILITY OF QoS STANDARDS TO MOBILE SCENARIO

In order to analyse the applicability of the QoS concepts dealt with in the previous paragraphs, it should be made a distinction between mobile networks with an infrastructure, such as Universal Mobile Telecommunications System (UMTS) and Long-Term Evolution (LTE) access networks, and mobile networks without an infrastructure, such as Mobile Ad Hoc Networks (MANETs).

J.3.1 QoS for Mobile Networks with an Infrastructure

For mobile networks with an infrastructure, some specific QoS standards have been issued from standardization bodies, such as ITU-T, ETSI and IETF:

- ITU-T Rec. E.804;
- ETSI UMTS TR 22.25; and
- IETF RFC 3583.

In particular, in Ref. [12], par. 6.1.4.2, “a scenario where two mobile users are communicating with each other” is shown in Figure 6-5, which is represented in Figure J-3.

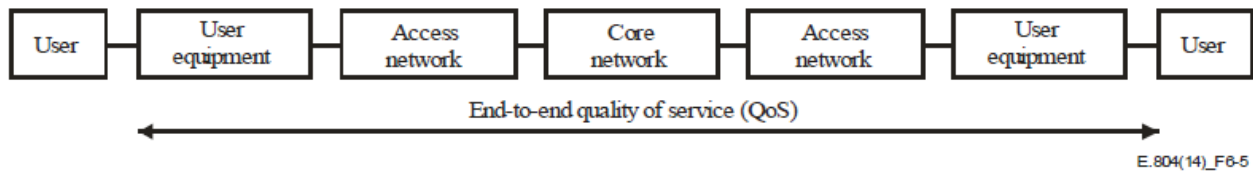


Figure J-3: Communication Between Two Mobile Users.

From the text in Ref. [12] explaining Figure J-3, and in particular the statement that each of the functional blocks in the figure “has an influence on the achievable QoS level:

- *If one of the user equipment has limited capabilities, e.g., reduced computational power, this will have an observable effect on the end-to-end QoS; and*
- *The same applies to the access networks, where, e.g., the bandwidth of the transmission link has a major effect” (Ref. [12], par. 6.1.4.2);*

it arises that specific issues related to the wireless peculiarities affect the end-to-end and Network QoS.

For instance, in Ref. [13], par. 4.1.2, the following set of specific parameters are considered basic for evaluating network performance: “Answer / Connect time-when called party accepts the call, Release time, Interruption of services”, as in Ref. [14], par. 3.1, the following performance requirements are listed: “Minimize the interruption in QoS at the time of handover, [...] Localize the QoS (re)establishment to the affected parts of the packet path in the network, [...] Releasing after handover the QoS state (if any) along the old packet path”.

However, together with these specific issues, for instance in Ref. [13], par. 5, implicit “Service Classes” are defined, such as Speech services, Data Transmission services, with the associated performance targets, such as “Delay (one way end-to-end) 40 ms” (Ref. [13], par. 5.2.2) for Speech services.

Therefore it could be affirmed that, for mobile networks with an infrastructure, the presence of an engineered (i.e., stable enough) infrastructure permits the assimilation of the wireless network to a wired functional block in the reference path of the Y.1541 shown in Figure J-1, allowing the application of the network performance objectives indicated in Table J-2.

J.3.2 QoS for MANETs

MANETs present a very different situation in comparison to the mobile networks with an infrastructure.

In Ref. [15], Introduction, an in-depth analysis is provided:

“Conventional wireless networks require as prerequisites some form of fixed network infrastructure and centralized administration for their operation. In contrast, the so-called ad hoc wireless networks, consisting of a collection of wireless nodes, all of which may be mobile, dynamically create a wireless network among themselves without using any such infrastructure or administrative support. [...] The absence of fixed infrastructure means that the nodes of an ad hoc network communicate directly with one another in a peer-to-peer fashion. The mobility of these nodes imposes limitations on their power capacity, and hence on their transmission range; indeed, these nodes often must satisfy stringent weight limitations for portability. [...] The lack of fixed base stations in ad hoc networks means that there is no dedicated agency to manage the channel resources for the network nodes. [...] All the challenges enumerated above are potential sources of service impairment in ad hoc networks, and hence may degrade the QoS seen by users of the network.”

Another important paper in the analysis of QoS issues for MANETs is Ref. [16], where, in the Abstract, it is stated that:

“In mobile ad hoc networks (MANETs), the provision of quality of service (QoS) guarantees is much more challenging than in wireline networks, mainly due to node mobility, multihop communications, contention for channel access, and a lack of central coordination”.

In fact the problem is that, on one side, the services are agnostic of underlying networks and they requires the compliance with the network performance targets that they need, independently from the involvement of MANETs in the transmission path, while, on the other side, the inherent characteristics of MANETs prevent from guaranteeing their fulfilment in a deterministic way.

As indicated in Ref. [16], “QoS routing protocols play a major part in a QoS mechanism”, and in fact MANET QoS-aware routing has been one of the main research fields, with several proposals such as QOLSR [17] and QAODV [18], as QoS-aware extensions of already existing routing protocols, and CEDAR [19] among the new QoS-aware routing protocols.

As an alternative, in the literature a few QoS solutions, independent from the routing protocol, have been proposed, namely FQMM [20], SWAN [21] and INSIGNIA [22].

However, at present, no standard solution to provide Network QoS better than best-effort in MANETs has been identified.

J.4 QoS VOCABULARY

In the following section, the definitions of the terms related to QoS are provided, in the light of the overview presented in the previous paragraphs:

<i>Admission Control</i>	A mechanism that controls the traffic to be admitted into the network. The admission criteria are typically policy driven and the decision depends on if adequate network resources are available to satisfy the QoS requirements of the newly admitted traffic.
<i>End-to-end QoS (or Teleservice QoS)</i>	The ability of a user-to-user connection to satisfy a set of performance requirements related to communications between users.
<i>IP-based Service</i>	A service provided by the service plane to an end user (e.g., a host (end system) or a network element) and which utilizes the IP transfer capabilities and associated control and management functions, for delivery of the user information specified by the service level agreements.
<i>IP Network Service</i>	A data transmission service in which the data passed across the interface between the user and provider is transferred in the form of IP packets.
<i>IP Transfer Capability</i>	The set of network capabilities provided by the IP layer. It may be characterized by the traffic contract as well as performance attributes supported by control and management functions of the underlying protocol layers.
<i>Network QoS (or Bearer QoS)</i>	The ability of a network or network portion to satisfy a set of performance requirements related to communications between users.
<i>QoS Routing</i>	The selection of a path satisfying the QoS requirements of a flow.

<i>QoS Signalling</i>	A mechanism to convey QoS parameter values between the QoS building blocks and, in particular, for conveying application (or network) QoS requirements, reserving network resources across the network, or discovering QoS routes.
<i>Resource Reservation</i>	A mechanism to reserve network resources so as to provide the required Network QoS.

J.5 REFERENCES

- [1] Gozdecki, J., Jajszczyk, A., and Stankiewicz, R., “Quality of Service Terminology in IP Networks,” *IEEE Communications Magazine*, Vol. 41, no. 3, pp. 153-159, Mar. 2003.
- [2] ITU-T Rec. G.1000, “Communications Quality of Service: A Framework and Definitions,” Nov. 2001.
- [3] ITU-T Rec. E.800, “Definitions of Terms Related to Quality of Service,” Sept. 2008.
- [4] ITU-T Rec. Y.1541, “Network Performance Objectives for IP-Based Services,” Feb. 2006.
- [5] ITU-T Rec. Y.1241, “Support of IP-Based Services Using IP Transfer Capabilities,” Mar. 2001.
- [6] ITU-T Rec. Y.1221, “Traffic Control and Congestion Control in IP Based Networks,” Mar. 2002.
- [7] ITU-T Rec. Y.1291, “An Architectural Framework for Support of Quality of Service in Packet Networks,” May 2004.
- [8] STANAG 4637, “TACOMS Phase 1 – Head STANAG,” Edition 1.
- [9] STANAG 4643, “TACOMS Phase 1 – Connection Oriented Network Protocols,” Edition 1.
- [10] STANAG 4644, “TACOMS Phase 1 – Connectionless Network Protocols,” Edition 1.
- [11] Allied Communication Publication AComP-4711, “Interoperability Point Quality of Service (IP QoS),” Edition A, Version 1 (Draft).
- [12] ITU-T Rec. E.804, “QoS Aspects for Popular Services in Mobile Networks,” Feb. 2014.
- [13] ETSI TR 22.25, “UMTS – Quality of Service and Network Performance,” version 3.1.0, Mar. 1998.
- [14] RFC 3583, “Requirements of a Quality of Service (QoS) Solution for Mobile IP,” Sept. 2003.
- [15] Chakrabarti, S., and Mishra, A., “QoS Issues in Ad Hoc Wireless Networks,” *IEEE Communications Magazine*, Vol. 39, no. 2, pp. 142-148, Feb. 2001.
- [16] Hanzo, L. II, and Tafazolli, R., “A Survey of QoS Routing Solutions for Mobile Ad Hoc Networks,” *IEEE Communications Surveys & Tutorials*, Vol.9, Issue 2, 2nd Quarter 2007.
- [17] Nguyen, D.-Q. and Minet, P., “QoS Support and OLSR Routing in a Mobile Ad Hoc Network,” ICN/ICONS/MCL, 2006.
- [18] Perkins, C.E. and Belding-Royer, E.M. “Quality of Service for Ad Hoc On-Demand Distance Vector Routing,” *IETF MANET Working Group*, Internet Draft, draft-perkins-manet-aodvqos-00.txt, Nov. 2001.

- [19] Sinha, P., Sivakumar, R. and Bharghavan, V., “CEDAR: A Core-Extraction Distributed Ad Hoc Routing Algorithm,” *INFOCOM '99*, New York, NY, USA, Vol.1., pp. 202-209, 1999.
- [20] Xiao, H., Seah, W.K G., Lo, A. and Chua, K.C., “A Flexible Quality of Service Model for Mobile Ad-Hoc Networks,” *VTC2000-Spring*, Tokyo, Vol.1., pp. 445-449, 2000.
- [21] Ahn, G.-S., Campbell, A.T., Veres, A. and Sun, L-H., “SWAN: Service Differentiation in Stateless Wireless Ad Hoc Networks,” *INFOCOM*, Vol.2, pp. 457-466, 2002.
- [22] Lee, S-B, Ahn, G-S., Zhang, X., and Campbell, A.T., INSIGNIA: An IP-Based Quality of Service Framework for Mobile ad Hoc Networks, *Journal of Parallel and Distributed Computing*, Vol. 60.4, pp. 374-406, 2000.

REPORT DOCUMENTATION PAGE			
1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-IST-124-Part-I AC/323(IST-124)TP/877	ISBN 978-92-837-2201-4	PUBLIC RELEASE
5. Originator	Science and Technology Organization North Atlantic Treaty Organization BP 25, F-92201 Neuilly-sur-Seine Cedex, France		
6. Title	Heterogeneous Tactical Networks – Improving Connectivity and Network Efficiency		
7. Presented at/Sponsored by	Final Report of NATO IST-124.		
8. Author(s)/Editor(s)	Multiple		9. Date September 2019
10. Author's/Editor's Address	Multiple		11. Pages 386
12. Distribution Statement	There are no restrictions on the distribution of this document. Information about the availability of this, and other STO unclassified publications, is given on the back cover.		
13. Keywords/Descriptors	Heterogeneous network Mobile ad hoc network Quality of service Resource management Routing		
14. Abstract	This report documents the work of IST-124/RTG-061. The group has contributed to a better understanding (through analysis, simulation, network emulation and expert opinions) on how to build interoperable heterogeneous mobile networks at the tactical edge. Challenges imposed by different security architectures are identified. Several design choices are discussed and compared to help the network planner to orchestrate the best network design for a given operation. Both mechanisms to provide end-to-end connectivity in the networks (routing) as well as solution for efficient utilization (resource management and quality of service) of the scarce network resources, has been studied. Necessary information exchange interfaces to enable heterogeneous coalition network connectivity at the tactical edge, have been identified. Monitoring of three states of network health (normal, reduced, last effort) is proposed to improve resource management and service quality in the network. The group has implemented a cloud-like shared emulated network platform for doing joint experiments. A shared network emulation environment can improve international research collaboration and speed up the time from early research results until solutions are ready to be tested for standardization. A well connected, resource efficient network can improve Training, Materiel and Interoperability.		





BP 25

F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cs0.nato.int



DIFFUSION DES PUBLICATIONS STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre et la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (<http://www.sto.nato.int/>) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE

Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE

Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

BULGARIE

Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA

DGSIST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

DANEMARK

Danish Acquisition and Logistics Organization
(DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESPAGNE

Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

ESTONIE

Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

ETATS-UNIS

Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FRANCE

O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

GRECE (Correspondant)

Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE

Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALIE

Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG

Voir Belgique

NORVEGE

Norwegian Defence Research
Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

PAYS-BAS

Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE

Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL

Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE

Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

ROUMANIE

Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI

Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE

Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIE

Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

TURQUIE

Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanlıklar – Ankara

AGENCES DE VENTE

The British Library Document
Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and
Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (<http://www.ntis.gov>).



BP 25

F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cs.o.nato.int



DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (<http://www.sto.nato.int/>) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM

Royal High Institute for Defence –
KHID/IRSD/RHID
Management of Scientific & Technological
Research for Defence, National STO
Coordinator
Royal Military Academy – Campus
Renaissance
Renaissancelaan 30
1000 Brussels

BULGARIA

Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA

DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC

Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

DENMARK

Danish Acquisition and Logistics Organization
(DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESTONIA

Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

FRANCE

O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

GERMANY

Streitkräfteamt / Abteilung III
Fachinformationszentrum der
Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GREECE (Point of Contact)

Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY

Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALY

Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG

See Belgium

NETHERLANDS

Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY

Norwegian Defence Research
Establishment, Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

POLAND

Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL

Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROMANIA

Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

SLOVAKIA

Akadémia ozbrojených síl gen
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIA

Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SPAIN

Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

TURKEY

Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanlıklar – Ankara

UNITED KINGDOM

Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down, Salisbury SP4 0JQ

UNITED STATES

Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre

Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)

National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (<http://www.ntis.gov>).