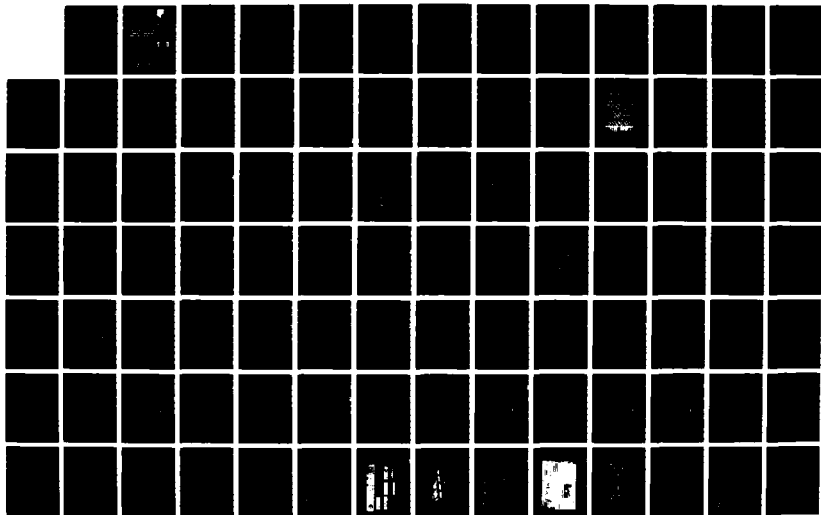
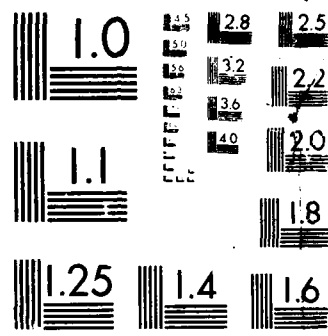


AD-A195 374 PROCEEDINGS OF THE COMMUNICATIONS NETWORK MANAGEMENT 1/3
WORKSHOP (1987) HELD. (U) ROME AIR DEVELOPMENT CENTER
GRIFFISS AFB NY J J SALERNO ET AL. NOV 87
UNCLASSIFIED RADC-TR-87-231 F/G 25/4 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963

AD-A195 374

RADC-TR-87-231
In-House Report
November 1987



12

DTIC FILE COPY

PROCEEDINGS OF THE 1987 COMMUNICATIONS NETWORK MANAGEMENT WORKSHOP

John J. Salerno, Anthony Martin and Brad Tippler

DTIC
ELECTE
MAY 02 1988
S D
COH

APPROVED FOR PUBLIC RELEASE, DISTRIBUTION UNLIMITED.

ROME AIR DEVELOPMENT CENTER
Air Force Systems Command
Griffiss Air Force Base, NY 13441-5700

88 5_02 034

This report has been reviewed by the RADC Public Affairs Office (PA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

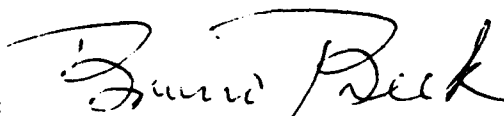
RADC-TR-S7-231 has been reviewed and is approved for publication.

APPROVED:



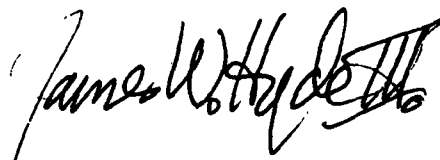
DANIEL J. MCAULIFFE
Ass't Chief, Telecommunications Division
Directorate of Communications

APPROVED:



BRUNO BEEK
Technical Director
Directorate of Communications

FOR THE COMMANDER:



JAMES W. HYDE, III
Directorate of Plans & Programs

If your address has changed or if you wish to be removed from the RADC mailing list, or if the addressee is no longer employed by your organization, please notify RADC (DCLD) Griffiss AFB NY 13441-5700. This will assist us in maintaining a current mailing list.

Do not return copies of this report unless contractual obligations or notices on a specific document require that it be returned.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

ADA195374

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188		
1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED			1b. RESTRICTIVE MARKINGS N/A			
2a. SECURITY CLASSIFICATION AUTHORITY N/A			3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited			
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A						
4. PERFORMING ORGANIZATION REPORT NUMBER(S) RADC-TR-87-231			5. MONITORING ORGANIZATION REPORT NUMBER(S) N/A			
6a. NAME OF PERFORMING ORGANIZATION Rome Air Development Center		6b. OFFICE SYMBOL (If applicable) DCLD	7a. NAME OF MONITORING ORGANIZATION N/A			
6c. ADDRESS (City, State, and ZIP Code) Griffiss AFB NY 13441-5700			7b. ADDRESS (City, State, and ZIP Code) N/A			
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Rome Air Development Center		8b. OFFICE SYMBOL (If applicable) DCLD	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER N/A			
8c. ADDRESS (City, State, and ZIP Code) Griffiss AFB NY 13441-5700			10. SOURCE OF FUNDING NUMBERS			
			PROGRAM ELEMENT NO. 63789F	PROJECT NO. 2317	TASK NO. 06	WORK UNIT ACCESSION NO. P1
11. TITLE (Include Security Classification) PROCEEDINGS OF THE 1987 COMMUNICATIONS NETWORK MANAGEMENT WORKSHOP						
12. PERSONAL AUTHOR(S) John J. Salerno, Anthony Martin (UK), Brad Tippler (CA)						
13a. TYPE OF REPORT In-House		13b. TIME COVERED FROM Jun 87 TO Aug 87		14. DATE OF REPORT (Year, Month, Day) November 1987		
15. PAGE COUNT 414						
16. SUPPLEMENTARY NOTATION N/A						
17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)			
FIELD	GROUP	SUB-GROUP	Communications Networks, Routing Network Management Voice and Data Networking, 4			
25	04					
25	05					
19. ABSTRACT (Continue on reverse if necessary and identify by block number) This report presents the results of the 1987 Communications Network Management Workshop sponsored by the Rome Air Development Center in cooperation with The Technical Cooperative Program (TTCP) Sub-Group 5. The results were also presented at the last STP-5 meeting held in Malvern, UK during the period 13-17 July 1987.						
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☐ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT ☐ DTIC USERS			21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED			
22a. NAME OF RESPONSIBLE INDIVIDUAL John J. Salerno			22b. TELEPHONE (Include Area Code) (315) 330-7751		22c. OFFICE SYMBOL RADC (DCLD)	

DD Form 1473, JUN 86

Previous editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED

ACKNOWLEDGEMENTS

The STP-5 Panel wishes to thank all those who took time out to participate in the workshop. We are especially grateful to Dr. Virgil Eveliegh and his staff, Carol Dougherty, Donna McCammon, Sue Craig, Norma Feldman, Petty VanArnum and Lois Applegate for the outstanding support in organizing and coordinating the workshop. Special thanks is also in order to those companies who allowed their employees to give briefings. A list of those companies and people is provided in Appendix A, Agenda.



Accession For	
NTIS GRA&I	☒
DTIC TAB	☐
Unannounced	☐
Justification _____	
By _____	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

TABLE OF CONTENTS

1.0 Introduction

2.0 Proceedings

- 2.1 The Management of Heterogeneous Networks
- 2.2 Stability of Routing Algorithms
- 2.3 Security
- 2.4 Knowledge-based Systems
- 2.5 Macro and Micro Management

3.0 Areas of Future Work

4.0 Summary

APPENDIX A: Agenda

APPENDIX B: Attendees

APPENDIX C: Hardcopy of presentation material

1.0 Introduction

The Technical Cooperation Program (TTCP) is a joint program, between the Governments of Australia, Canada, New Zealand, the United Kingdom and the United States of America, to share the results of military research and development. The program is split into various Subgroups of which Subgroup S is concerned with Communications. Subgroup S has various Technical Panels and STP-5 (Communications Networks Architectures) has been tasked with addressing the issue of Communications Network Management.

At the 19th meeting held at the Naval Ocean Systems Center, STP-5 concluded that a Network Management Workshop should be conducted. The USA (Rome Air Development Center) undertook to organize the 1987 Communications Network Management Workshop which was held on 30th June - 2nd July at the Sheraton University Conference Center, Syracuse, NY.

2.0 Proceedings

The presentations were structured into the following sessions:

- Overview of US Department of Defense Networking Problems
- Link Management
- Node Management
- Network Management
- User Management.

It is not proposed to describe in detail the proceedings of the workshop as the agenda may be found in Appendix A, the list of attendees in Appendix B and the materials provided by the presenters in Appendix C.

Some themes emerged, however, which were discussed throughout the workshop and which merit further discussion:

- Management of Heterogeneous Networks
- Stability of Routing Algorithms and new research techniques for investigating adaptive routing
- Security
- Knowledge-Based Systems
- The distinction between Macro and Micro Management of Networks.

2.1 The Management of Heterogeneous Networks

The management of heterogeneous networks is a difficult task. The management system must be able to deal with a variety of manufacturer's products as well as a variety of networking technologies (e.g. packet, voice) and multiple transmission media (e.g. fiber, HF, etc.). A single manufacturer's solution will not be viable due to the existence of an installed base of diverse equipment and to laws against such non-competitive activity. This is a real problem now as the military uses public networks, each with its own proprietary management systems. Network Management standards are part of the long term answer to such problems but current timetables predict that the majority will not reach Draft International Standard (DIS) status until about 1990.

The various network management systems forming an internetwork must work in a cooperative manner. Correlation of exceptions across networks to aid the management process is one area which has received little attention. It would be useful, for instance, to be able to detect co-ordinated attacks on the different networks used to communicate with a particular site.

2.2 Stability of Routing Algorithms

To date, algorithms used for activities, such as routing, have concentrated on optimality with respect to certain assumptions applicable to commercial networks. The requirements of military scenarios have not necessarily been considered. Management activities should be able to deal with:

1. mobile network nodes.
2. extreme traffic surges and variations by being responsive and stable.
3. rapid reconstitution and reconfiguration of available communications assets (currently it is difficult to determine the current state of a failing network).
4. coordinated attacks in a highly survivable manner. The network should be more offensive and less reactive. For example, upon detecting a degraded channel it could use the channel for voice rather than data. It should report details of the jamming and in extreme cases continue to send dummy traffic.

Adaptive routing research should continue. The idea of marrying perturbation analysis and simulation has developed a useful technique for modelling routing. Several of the routing algorithms which are currently being used (as well as new ones) should be compared in terms of stability and speed.

2.3 Security

The topic of Network Security was frequently raised. Two issues emerged. Firstly, the Security Services of the network need to be managed. Secondly, the network management service must be secured as must the information used within the network to make routing decisions. The ISO standards committees are concentrating only on the second¹ of these and require more technical input in this area. A related topic is that of centralized versus distributed management. Centralization provides a more complete view of network operations but creates a vulnerable point for attacks.

2.4 Knowledge-Based Systems

Knowledge-based systems continue to attract interest. They are viewed as potential aids in reducing the complexity and data volume of managing networks. They must, however, be capable of assimilating subtle trends like daily traffic patterns if they are to be useful as diagnostic and management aids.

2.5 Macro and Micro Management

It was clear that on many network management issues there were two points of view. Firstly, the user's high-level generally long term policy requirements for the performance of the network (Macro Management). Secondly, the network implementor's automatic, low-level, immediate mechanisms for network management (Micro Management). The Micro Management activities should implement the Macro Management policy.

The workshop ended with a discussion period centered around the questions:

- What is Military Network Management to a military commander?
- What is Military Network Management to a network maintainer/provider?
- What is Military Network Management to an equipment manufacturer?

The nature of the questions reflect the fact that the military needs for network management need to be better understood. Once this is achieved it is hoped that the manufacturers will provide products which better meet those needs.

¹The March 1987 draft of ISO 7498/Part2 - Security Architecture addresses the management of the Security Service

3.0 Areas of Future Work

As a result of the workshop it was agreed that the following areas would benefit from the application of more Research and Development:

1. The Management of Heterogeneous Hardware, Network Technologies and Transmission Media. This implies the need for:

- Flexible generic tools which can be configured to manage diverse existing equipments to provide a homogeneous Management Interface
- International Network Management Standards
- An Open Network Management Architecture
- The ability to exercise Network control and monitoring across networks
- The ability for "peer level" management entities to negotiate.

2. The Differentiation and Integration of Macro and Micro Network Management. Not only in the area of routing but also, for instance, the gathering of Statistics, the issues of Global Views versus Detailed Granularity.

3. The issue of low-level routing and network control would benefit from the application of the marriage of perturbation analysis and modelling. Concerns in this area include the control of extreme traffic load variations, fragmentation and reconstitution of networks and the stability of networks.

4. The application of Knowledge-based Technology to Network Management.

5. What will be the impact of Photonics (the replacement of electronic devices by Optical processing components) on network management?

6. The Security of networks - both the Security of the Management Information and the Management of the Security Service Methods to recognize sophisticated attacks on networks.

7. Support should be given to the standards making bodies in the form of technical input, to ensure that standards for the management of Network Security are both timely and useful. This issue is urgent due to the long timescale of the standards making process and the small window of opportunity which exists to influence the next standard.

4.0 Summary

The 1987 Network Management Workshop was very successful as evidenced by the fact that approximately 100 people attended. In all, over 30 presentations were given by government, industry and academia. Because of its success, it is proposed that this event should be held annually.

AGENDA

of the

1987

Communications

Network

Management

Workshop

APPENDIX A

1987 Communications Network Management Workshop
June 30 - July 2, 1987

Agenda

29 June 1987

19:00 Pre-Registration
(Social Hour)

30 June 1987

08:00 Registration

09:00 Administrative Remarks

09:15 Welcome

09:40 Forecast II: Survivable Comm Networks

10:00 Technology of Evolution for Distributed C3 Systems

10:20 Air Defense Initiative

10:40 **BREAK**

11:00 21st Tactical Air Command

11:20 Strategic Adaptive Planning Experiment

11:40 Emerging Standards in Network Management

12:00 **LUNCH**

13:30 - 16:00 LINK/NODE MANAGEMENT

13:30 Issues in Link Management

13:50 Network Survivability through Connectivity
Optimization

14:10 Multi-Commodity Routing Algorithms

14:30 Multi-Media Network Simulator

14:50 **BREAK**

16:10 Multi-Layered Networks

16:30 Survivability of Communications in Europe

16:50 Node Management

17:10 Wideband Sat Network - Link Management

Mr. John Salerno

Dr. Fred Diamond

Mr. Daniel McAuliffe

Dr. Casper DeFiore, DCA

Capt. Harvey Leister

Mr. Jerry Dussault

Mr. Dick Metzger

Mr. Stan Ames

Mr. Tom Labarre

MITRE

Mr. Jim Hoffmeyer
ITS

Mr. Kris T. Newport
MITRE Corporation

Dr. Jeff Kennington
SMU

Dr. Hugo de Pedro
GTE

Mr. Peter Steensma
ITT - DCD

Mr. Walter Kinzinger
MITRE Corporation

Thomas Clark
Northern Telecom Inc.

Mr. Steve Bluementhal
Bolt Beranek Newman, Inc.

1 July 1987

08:30 - 16:30 NETWORK MANAGEMENT

08:30	Netview Enhancements	Mr. Ellis Gregory, IBM
09:30	Voice & Data Network Design	Mr. Bill Gilkburg, IBM
10:10	<i>BREAK</i>	
10:25	Shock Analysis	Dr. Nicholas Duchon Martin Marietta Labs
10:45	Sensitivity Analysis	Dr. Chris Cassandras University of Massachusetts
11:05	Routing Across Uni-directional Links and to Receive only Nodes	Mr. Jim Stevens Rockwell International
11:30	Network Management for Space	Mr. Alan Martin Harris GSS
12:00 - 13:30	<i>LUNCH</i>	
13:30	Functions of the Network Lab at Martin Marietta	Mr. Rich Wiley Martin Marietta Corp.
14:00	Network Management - Northern Telecom	Mr. H. Paul Brant Northern Telecom Inc.
14:30	<i>BREAK</i>	
14:50	Distributed Network Management	Dr. Robert Meyer Clarkson University
15:20	Network Control Center for DCTN	Mr. Tom Whalen, ATT
15:50	Dynamic Network Reconstitution	Mr. Robert Fish Network Equip Tech
17:30	<i>COCKTAIL HOUR (No Host)</i>	
18:00	<i>DINNER (Guest Speaker - Col. Raymond French, AFCC/Al)</i>	

2 July 1987

08:30 - 10:00 NETWORK MANAGEMENT (Cont'd)

08:30	Network Management	Ms. Christine King, GTE
08:50	Network Management for the DCS	Dr. Harold M. Heggstad Lincoln Labs - MIT
9:10	Automated Network Management	Mr. James C. Ong Bolt Beranek Newman, Inc.
09:30	<i>BREAK</i>	
09:45 - 10:25	USER MANAGEMENT	
09:45	Communication Between a Distributed Operating System and the Network Management System of a Wide Area Network	Mr. William T. Euter QRS Associates
10:05	An Intelligent C3 Terminal Concept	Mr. James W. Forgie Lincoln Labs
10:30 - 12:00	Panel Discussion and Conclusion	

ATTENDEES
of the
1987
Communications
Network
Management
Workshop

APPENDIX B

A T T E N D E E S

of the
1987 Communications Network
Management Workshop

Major Mike Adams
RADC/DCLD
Griffiss Air Force Base
Rome, NY 13441-5700

Mr. M. Paul Brant
Northern Telecom
P.O. Box 13010
Research Triangle Park, NC 27709
919/992-8810

Edwin Addison
Westinghouse Corporation
Box 1897, Mail Stop 903
Baltimore, MD 21203
301/765-3828

Christos G. Cassandras
Dept. of Elec. & Comp. Engineering
University of Massachusetts
Amherst, MA 01003
413/545-1340

Ms. A'isha Ajayi
IBM/North-Central Marketing
Division
One Park Place
300 South State Street
Syracuse, NY 13202
315/424-2146

Robert H.G. Chan
Manager/Skill Center
RCA Corporation
Government Communications Sys. Div.
Camden, NJ 08120
609/338-4062

Al Akins
RADC/DCLD
Griffiss Air Force Base
Rome, NY 13441-5700

Edwin Cobb
Westinghouse Corp., D & EC
Box 1897, Mail Stop 903
Baltimore, MD 21203

Elsa Angrist
J. G. VanDyke Associates
5510 Cherokee Ave.
Suite 300
Alexandria, VA 22312
703/354-4857

Lt. John Columbi
RADC/DCLD
Griffiss Air Force Base
Rome, NY 13441-5700

Thomas Blake
RADC/DCCR
Griffiss Air Force Base
Rome, NY 13441-5700

Mr. James Countryman
SUNY/College of Technology
Vice President for Academic Affairs
P.O. Box 3050
Utica, NY 13504-3050

Steven H. Blumenthal
BBN Laboratories
10 Moulton Street
Cambridge, MA 02138
617/497-3197

Harold Crowley
RADC/DC
Griffiss Air Force Base
Rome, NY 13441-5700

Cass DeFlore
Defense Communications Agency
11440 INS-North
Reston, VA 22090
703/437-2506

Dr. Hugo DePedro
GTE Corporation
Bldg. 17
77 "A" Street
Needham Hts., MA 02194

Dr. Fred Diamond
RADC
Griffiss Air Force Base
Rome, NY 13441-5700

John Donahue
Hughes Aircraft Company
Manager, Automated Comm. Control
Project
P.O. Box 3310-Bldg. 675/2221
Fullerton, CA 92634
714/441-9498

Nicholas Duchon
Martin Marietta Labs
1450 South Rolling Road
Baltimore, MD 21227-3898
301/247-0700

Gerard J. Dunleavy
c/o RADC - John Salerno
Griffiss Air Force Base
Rome, NY 13441-5700

Mr. Bill Etter
QRS Associates
P. O. Box 4297
Rome, NY 13440
315/736-0212

John Evanowsky
RADC/DCLD
Griffiss Air Force Base
Rome, NY 13441-5700

Martin Falmlen, Jr.
Honeywell Inc.
Defense Comm. & Production Div.
10901 Malcolm McKinley Drive
Tampa, FL 33612
813/972-6392

Bud Fantera
RADC/DCCL
Griffiss Air Force Base
Rome, NY 13441-5700

Mr. Robert Fish
Network Equipment Technologies
400 Penobscot Drive
Redwood City, CA 94063
703/556-7740

Mr. James Forgie
Massachusetts Institute of
Technology
Lincoln Laboratories
244 Wood Street
Lexington, MA 02173-0073
617/863-5500

Colonel Ray French
AFCC
c/o RADC - John Salerno
Griffiss Air Force Base
Rome, NY 13441-5700

Dr. William Glikbarg
IBM Corporation
GD67
9200 Corporate Boulevard
Rockville, MD 20850

Mr. Steve Goodheart
Network Equipment Technologies
8300 Boone Boulevard
Suite 290
Vienna, VA 22180
703/556-7740

Franz Haas
RADC/DCLD
Griffiss Air Force Base
Rome, NY 13441-5700

William K. Hale
Defense Communications
Engineering Ctr.
ADDRESS UNKNOWN
703/437-2344

Dr. Henry D. Hall
MITRE Corporation
MS Z-270
7525 Colshire Drive
McLean, VA 22102

Jeffrey Kennington
Southern Methodist Univ.
Operations Research Dept.
Dallas, TX 75275
214/692-3099

Dr. Harold Heggestad
MIT Lincoln Laboratories
244 Wood Street
Lexington, MA 02173-0073
617/863-5500X7719

Ms. Christine King
GTE Corp.
Bldg. 17
77 "A" Street
Needham Heights, MA 02194

Mr. James Hoffmeyer
Nat'l Telecommunications
& Information
325 Broadway
Boulder, CO 80303-3328
303/497-3140

Nick Kowalchuk
RADC/DCLD
Griffiss Air Force Base
Rome, NY 13441-5700

Mr. William C. Hughes
General Electric
Bldg. K-1, Room 4029
P. O. Box 8
Schenectady, NY 12301
518/387-5502

Mou-Laing Kung
Norfolk State University
2401 Corprew Ave.
Norfolk, VA 23504
804/623-8650

John Warrti
RADC John Salerno
RADC/Hazeltine
Griffiss Air Force Base
Rome, NY 13441-5700

Mr. Lee LaBarre
MITRE Corporation
Network Systems Analysis
Bedford, Massachusetts 01730
617/271-8507

Robert M. John
RADC/DCLD
Griffiss Air Force Base
Rome, New York 13441-7751
315/330-7751

Mr. Douglas J. Lain
Martin Marietta Corporation
Information & Communications Systems
P.O. Box 1260 - Mail Stop XL1659
Denver, CO 80201-1260
303/977-0968

Brian Kaldenback
RADC/DCCR
Griffiss Air Force Base
Rome, NY 13441-5700

Capt. Harvey Leister
RADC/DCCL
Griffiss Air Force Base
Rome, NY 13441-5700

Jack Kelly
RADC/DCL
Griffiss Air Force Base
Rome, NY 13441-5700

Al Lisnevsky
AFCC
Griffiss Air Force Base
Rome, NY 13441-5700

Mr. A. R. Martin
Manager, Sector Technology
Harris Corporation
P.O. Box 37
Melbourne, FL 32902
305/729-7353

A. S. Martin
c/o British Embassy
Washington, D.C.
202/462-1340

Albert R. Martin
Harris Corporation
P.O. Box 37, MS 2/1971
Palm Bay, FL 32902
305/729-7353

Daniel McAuliffe
RADC/DCLD
Griffiss Air Force Base
Rome, NY 13441-5700

Mr. Dick Metzger
RADC/XPY
Griffiss Air Force Base
Rome, NY 13441-5700

Professor Robert A. Meyer
Clarkson University
Electrical & Computer Engineering
Potsdam, NY 13676
315/268-6541

Darryl Morris
MITRE Corporation
Washington C3I Operations
7525 Colshire Drive
McLean, VA 22102-3481
703/883-7456

Kris T. Newport
MITRE Corporation
RADC/TOF
Griffiss Air Force Base
Rome, NY 13441-5700
315/336-4966

Steven Olenick
CMC Electronics
20 Meridian Road
Eatontown, NJ 07724
201/389-2522

James Ong
BBN Laboratories

Mary Beth Panock
MITRE Corporation
Bedford, Massachusetts 01730
617/271-2000

Mr. Charles N. Pateros
CONTEL Federal Systems
Spacecom Division
1300 Quince Orchard Blvd.
Gaithersburg, MD 20878
301/258-6875

Alan Pease
Rome Research Corp.
Griffiss Air Force Base
Rome, NY 13441-5700

Robert V. Perkins
RCA Corporation
Government Communications
Systems Division
Mail Stop 2-4
Camden, NJ 08102
609/338-4563

Chris Perry
MITRE Corporation
Communications Engineering
7525 Colshire Drive
McLean, VA 22102-3481
703/883-6235

Mr. Joseph Podvojsky
MITRE Corporation
Mail Stop B-270
Bedford, MA 01730
617/271-2000

Col. Robert Rahme
RADC/DC
Griffiss Air Force Base
Rome, NY 13441-5700

Ms. Nancee Rozicka
Martin Marietta Corporation
Info. & Comm. Systems
P.O. Box 1260 - MS XL9058
Denver, CO 80201-1260
303/97-0410

Ray Sadlmyer
RADC/DC/D
Griffiss Air Force Base
Rome, NY 13441-5700

John Salerno
RADC
Griffiss Air Force Base
Rome, NY 13441-5700

John F. Sawyer
MITRE Corporation
Box 925
Fr. Huachuca, AZ 85613

Robert A. Shade
Research Laboratories
Hazeltine Corporation
Greenlawn, NY 11740
516/261-7000

Peter D. Steensma
ITT
Defense Communications Div.
492 River Road
Nutley, NJ 07110
201/284-2792

Mr. James Stevens
Rockwell International
3200 E. Renner Road
Richardson, TX 75081

Larry Suez
RADC/DC/D
Griffiss Air Force Base
Rome, NY 13441-5700

Bill Sweeney
RADC/DC/D
Griffiss Air Force Base
Rome, NY 13441-5700

Mr. Edward S. Talley
MITRE Corporation
1820 Dolley Madison Boulevard
McLean, VA 22102
703/893-5573

Brad Tipler
Software Kinetics Limited
65 Iber Road
P.O. Box 680
Stittsville, Ontario
Canada, K0A 3G0
613/831-0888

Sgt. L. Walberg
AFCC/RADC
Griffiss Air Force Base
Rome, NY 13441-5700

Arthur E. Walsh
GTE Government Systems Corp.
Dept. 3310, Bldg. 10
77 "A" Street
Needham, MA 02194
617/453-5287

Craig R. Warren
Network Systems Corp.
251 New Karner Road
Albany, NY 12205
518/452-2626

Mr. Richard Wiley
Martin Marietta Corporation
Info. & Comm. Systems
P.O. Box 1260 - MS XL8058
Denver, CO 80201-1260
303/977-0410

Jack Zdilla
Technical Studies & Analysis
112 Buffie Road
Tabb, VA 23602-4758
804/867-8630

PROCEEDINGS

of the

1987

Communications

Network

Management

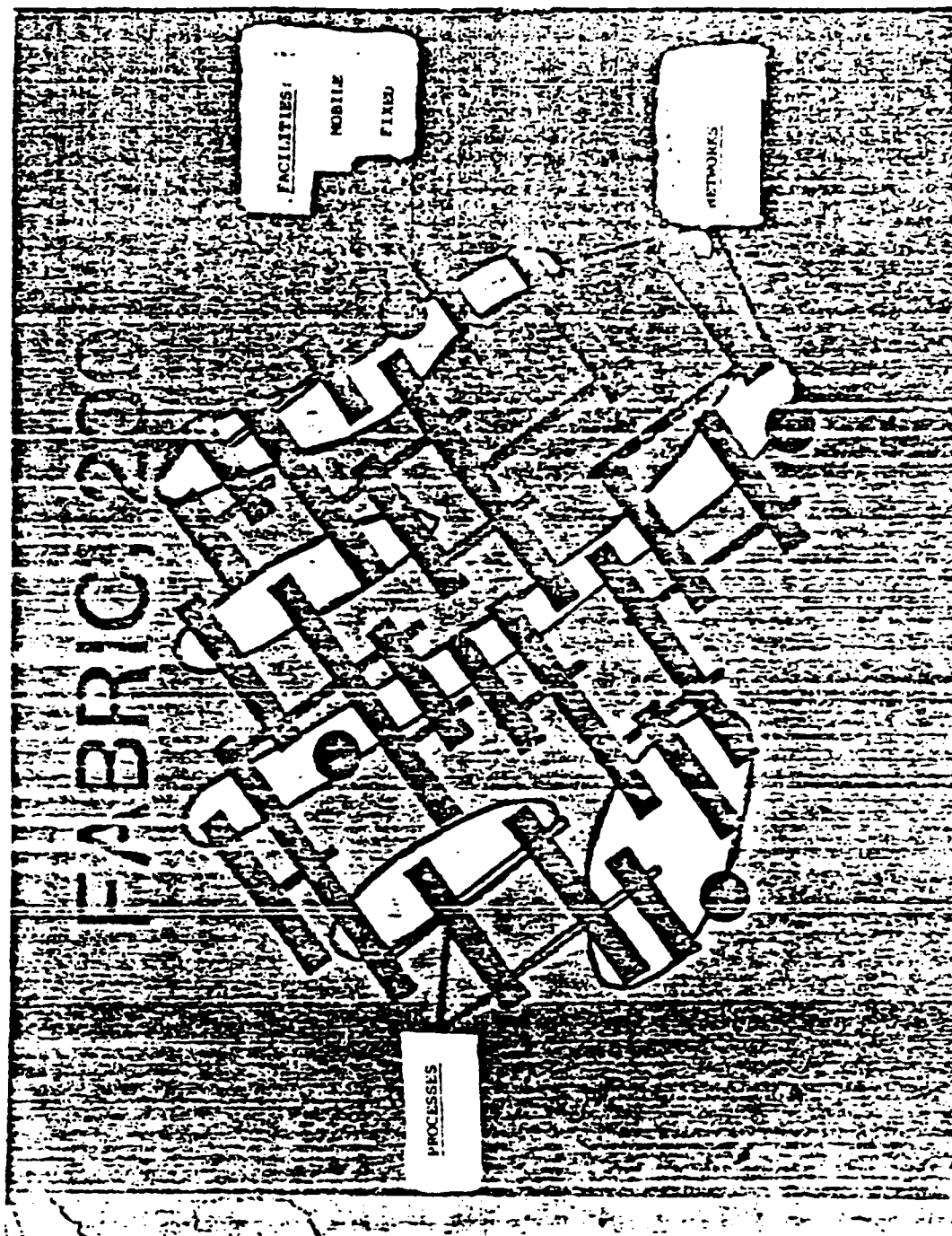
Workshop

APPENDIX C

TECHNOLOGY OF EVOLUTION FOR DISTRIBUTED C3 SYSTEMS

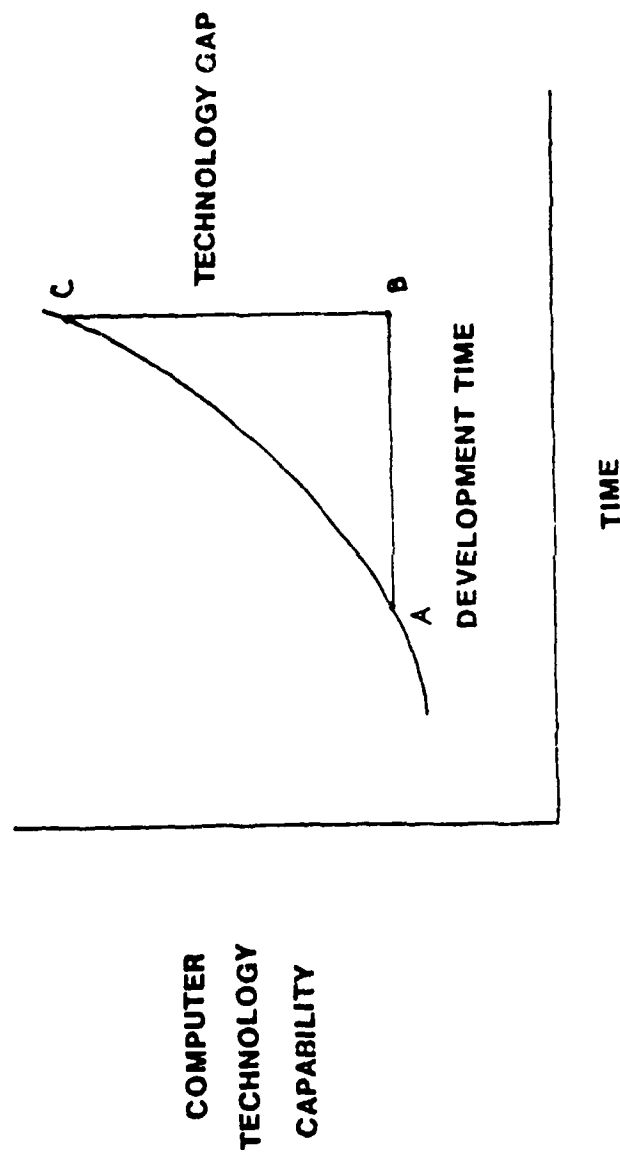
• DCA-C3 TECHNOLOGY PROJECTION AND ASSESSMENT

- CONFERENCE 17 NOVEMBER 1987
- SOME CONCLUSIONS
 - PROVIDE DISTRIBUTION OF C3 ASSETS FOR SURVIVABILITY
 - USE TECHNOLOGY IN GROWING C3 CAPABILITIES IN PLACE IN CONTRAST TO BUILDING C3 TURNKEY SYSTEMS
 - COPE WITH SECURITY VULNERABILITIES
- C3 ARCHITECTURAL FEATURES (FABRIC)
 - GEOGRAPHICALLY DISTRIBUTED COMMAND CENTERS CONSISTING OF COMPUTERS, WORK STATIONS ETC.
 - INTERCONNECTED BY MULTIPLE (REDUNDANT) MULTIMEDIA COMMUNICATIONS
 - DISTRIBUTED CONTROL



WHY EVOLUTIONARY ACQUISITION FOR C3 SYSTEMS

- ADVANCES IN CERTAIN TECHNOLOGIES ARE RAPID (E.G. COMPUTERS)
 - DARPA ESTIMATES AN ORDER OF MAGNITUDE ADVANCEMENT IN COMPUTER TECHNOLOGY EACH YEAR FOR AT LEAST THE NEXT SIX YEARS
 - CONVENTIONAL SEQUENTIAL DEVELOPMENT METHODOLOGY RESULTS IN TREMENDOUS TECHNOLOGY GAP BY THE TIME SYSTEMS ARE DEPLOYED (ESTABLISH REQUIREMENTS, CONCEPT DEVT, BREADBOARD, DEVT MODEL, PERFORMANCE TESTING, ADVANCED DEVT, PRE-PRODUCTION, OPERATIONAL TESTING, PRODUCTION/DEPLOYMENT)
 - NEED TO INSERT TECHNOLOGY QUICKLY AND AT FREQUENT INTERVALS TO MAINTAIN FORCE MULTIPLIER OF OUR C3 SYSTEMS



COMPUTER TECHNOLOGY CAPABILITY VS TIME

DISTRIBUTED SYSTEMS CHARACTERISTICS

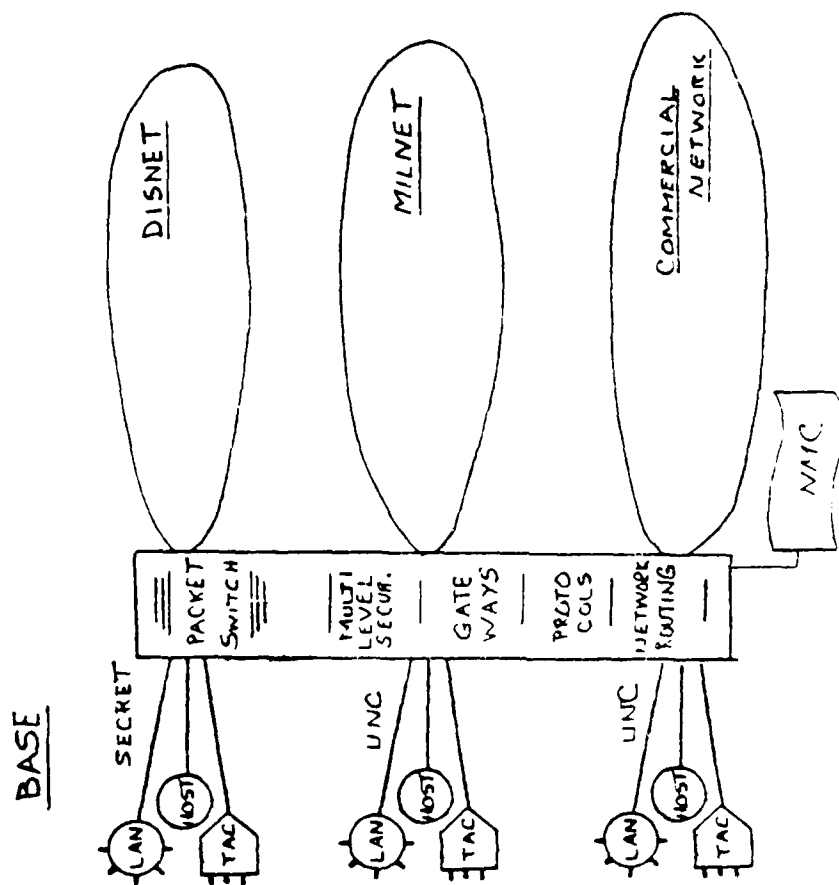
- BEGINNING TO APPEAR IN COMMERCIAL SYSTEMS
(COST, RELIABILITY, EFFICIENCY)
 - LACK KEY MILITARY REQUIREMENTS
- NATURAL TRANSITION PATH TO MORE CAPABLE SYSTEMS
 - ALLOWS TECHNOLOGY INSERTION AT USERS PACE AND DESIRE
 - MAINTAIN CURRENT SERVICE WHILE UPGRADING
- LEADS TO CONCEPT OF EVOLUTIONARY ACQUISITION
 - ADAPT TO CHANGING REQUIREMENTS (REQUIREMENTS PULL)
 - USE OF MOST EFFECTIVE TECHNOLOGY (TECHNOLOGY PUSH)

WHAT IS NEEDED

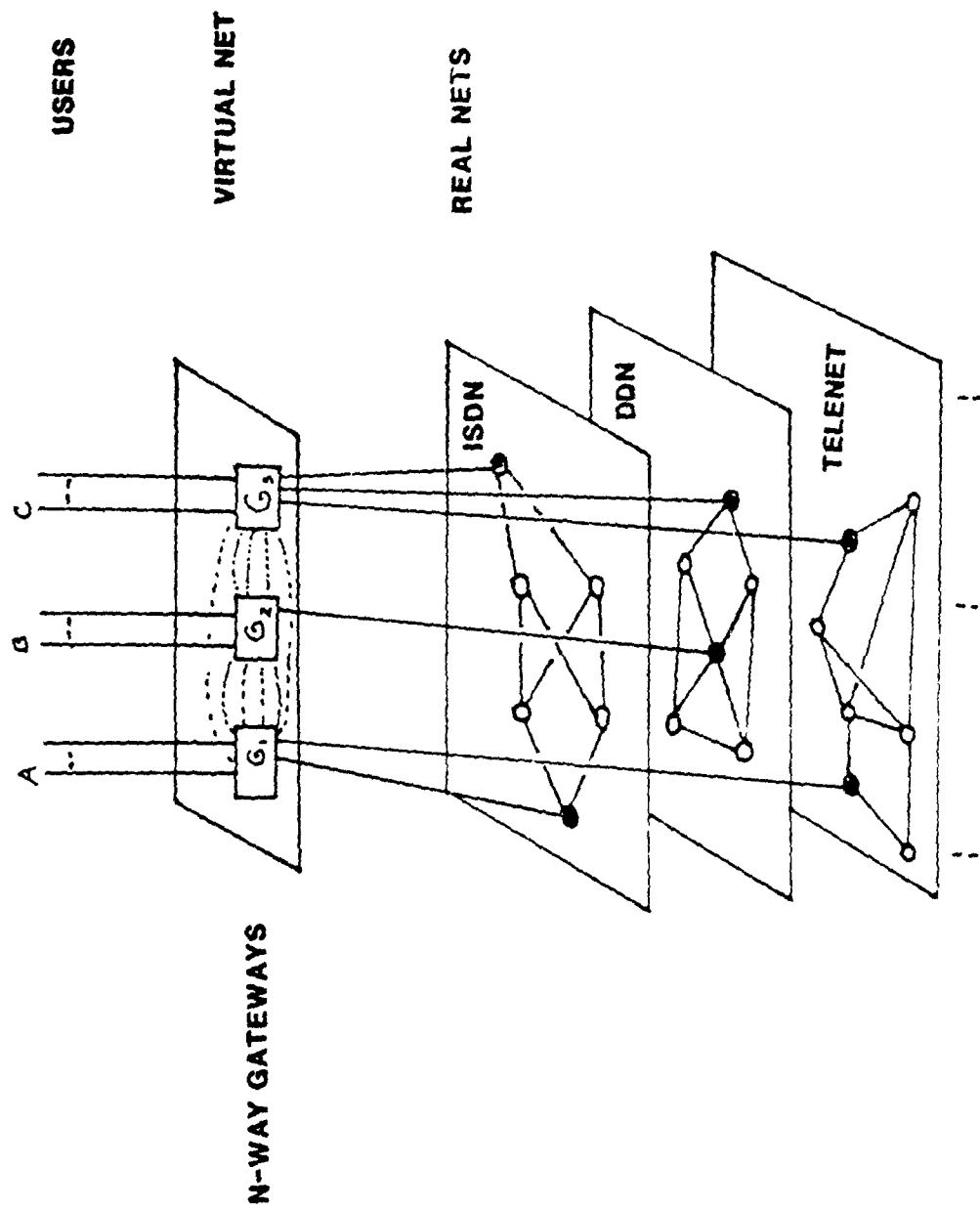
- LEVERAGE ON COMMERCIAL SYSTEMS (NON-DEVELOPMENTAL ITEMS)
- LOOK TO SERVICE, NOT NECESSARILY "OWNING" SYSTEMS
- SURVIVABLE COMMUNICATION IS THE SUMMATION OF ALL NETWORKS AND MEDIA
- CONCEPT OF ON-LINE "PATCH" CAPABILITY

APPROACH TO SOLUTION

- KEY, N-WAY GATEWAY/PACKET SWITCH THAT FORMS THE BASIS FOR A VIRTUAL NETWORK (SIMILAR TO RADIC MULTINET GATEWAY)

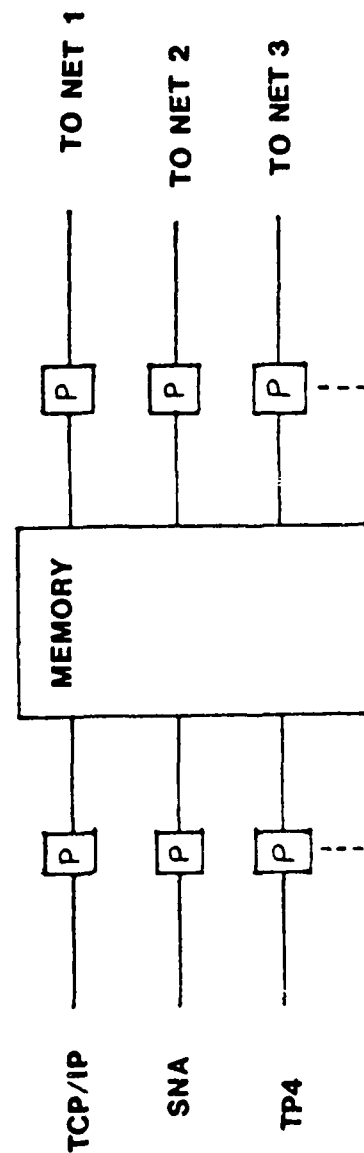


GATEWAY ARCHITECTURE



VIRTUAL NETWORK CONCEPT

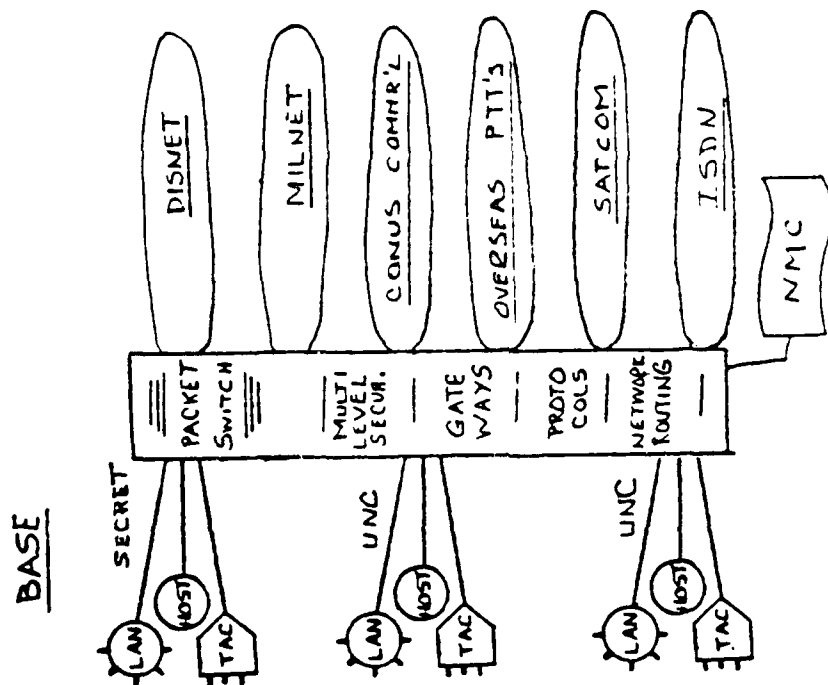
ACCESS AREA



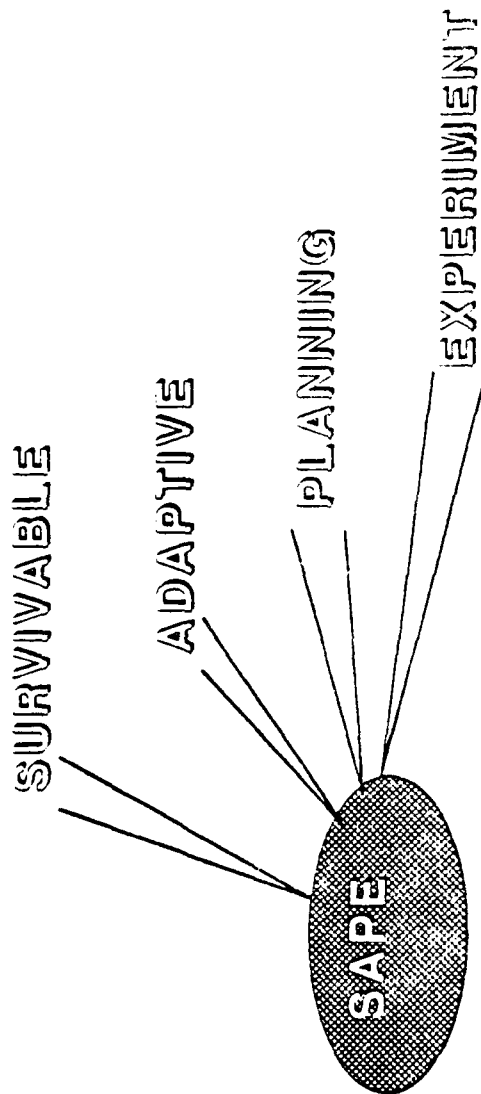
N-WAY GATEWAY MODULAR ARCHITECTURE

BENEFITS OF THIS ARCHITECTURE

- RESULTS IN A VIRTUAL NETWORK (INTERNET) THAT PROVIDES GREATER SURVIVABILITY
- PROVIDES THE MECHANISM FOR THE RAPID INSERTION OF TECHNOLOGY INTO C3 SYSTEMS (EVOLUTIONARY ACQUISITION)
- DEVICE PERFORMS TOTAL VIRTUAL NET MONITORING FUNCTION
- ALLOWS THE UTILIZATION OF ALL AVAILABLE NETS INCLUDING COMMERCIAL NETS BOTH IN DAY-TO-DAY OPERATION AND DURING CRISIS
- THE N-WAY GATEWAY CAN IF NECESSARY PROVIDE USER-TO-USER INTEROPERABILITY BY MAPPING THE PROTOCOL SUITE OF ONE USER TO ANOTHER (E.G.. SNA TO DOD PROTOCOLS)
- PROTOCOLS/GATEWAYS/NETWORK ISSUES ARE CENTRALIZED UNDER ONE AUTHORITY SEPARATE FROM THE NETWORK THEMSELVES
- USERS THEMSELVES ARE THE INTERFACE AUTHORITY, PHYSICALLY, FUNCTIONALLY AND ADMINISTRATIVELY FOR THE GATEWAY
- THE EXTENSION OF THIS CONCEPT PROVIDES A TOTAL ARCHITECTURE THAT ALLOWS FOR THE INTEGRATION OF ADDITIONAL NETWORKS AND CAPABILITIES SUCH AS OVERSEAS PTT'S AND SATCOM



EXTENDED VIRTUAL NET ARCHITECTURE



RICHARD A. METZGER
ROME AIR DEVELOPMENT CENTER
COMMAND AND CONTROL DIRECTORATE

SURVIVABLE ADAPTIVE PLANNING EXPERIMENT (SAPE)

JOINT PROGRAM: RADC,DARPA,SAC,JSTPS

INITIATED FY87

**OBJECTIVE IS TO DEVELOP AND DEMONSTRATE TECHNOLOGY
TO SUPPORT SURVIVABLE ADAPTIVE PLANNING FUNCTIONS
IN A TRANS AND EARLY POST ATTACK STRATEGIC ENVIRONMENT.
CONCENTRATION WILL BE ON PROVIDING A HIGH PERFORMANCE,
RECONFIGURABLE , DISTRIBUTED PROCESSING AND COMMUNICATIONS
ENVIRONMENT TO SERVE AS A BACKBONE FOR ADVANCED AI
PLANNING TOOLS AND TECHNIQUES**

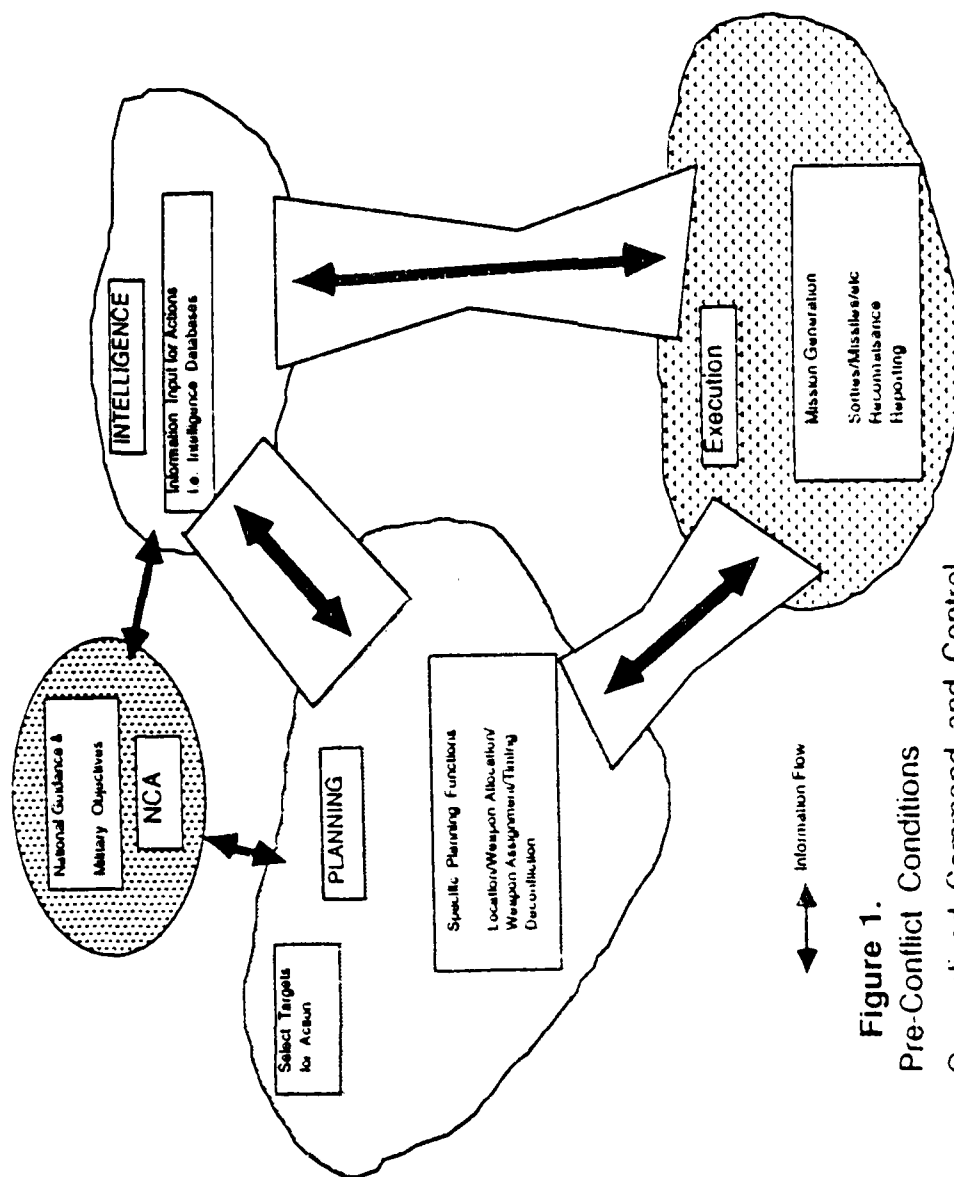


Figure 1.
Pre-Conflict Conditions
Generalized Command and Control

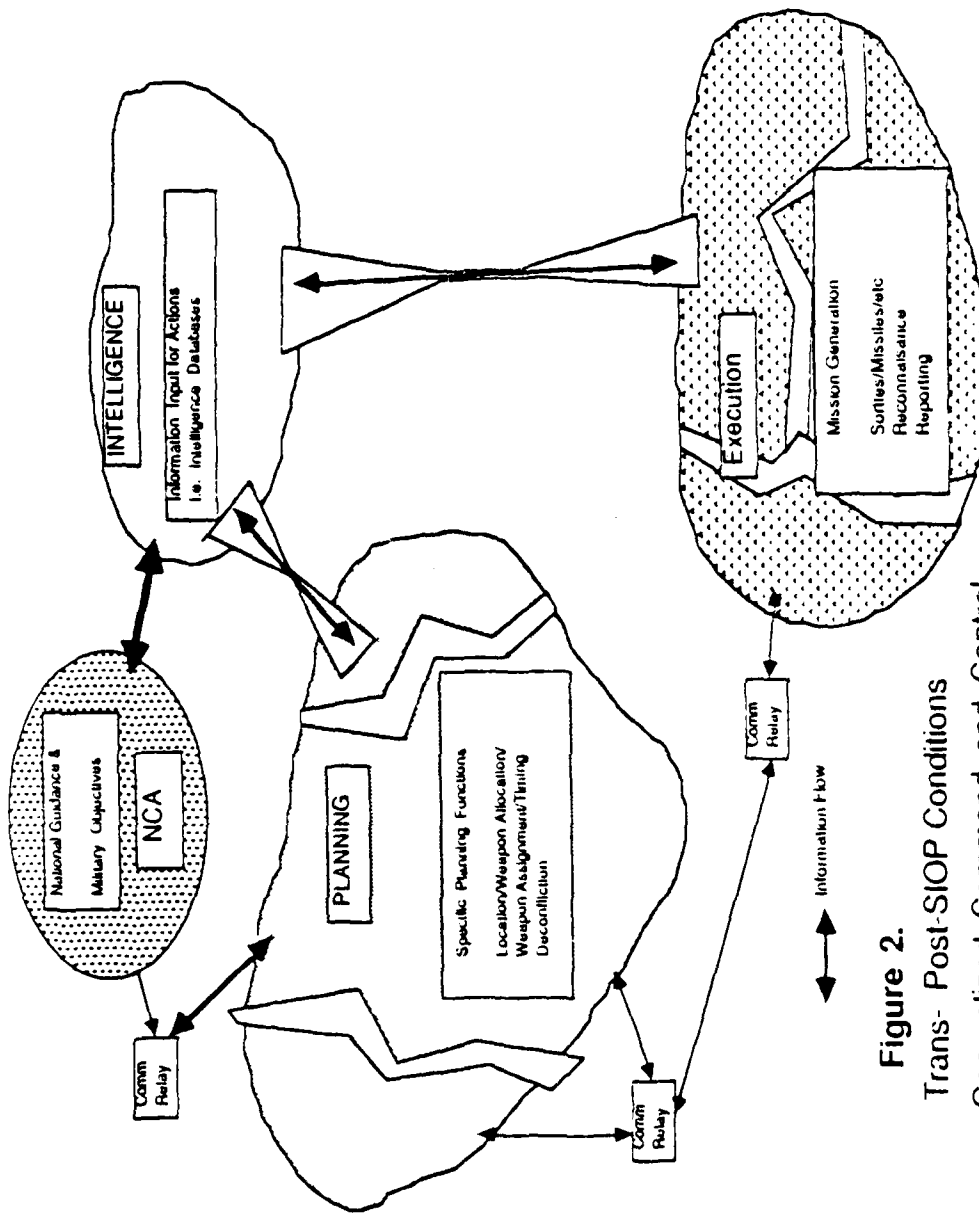
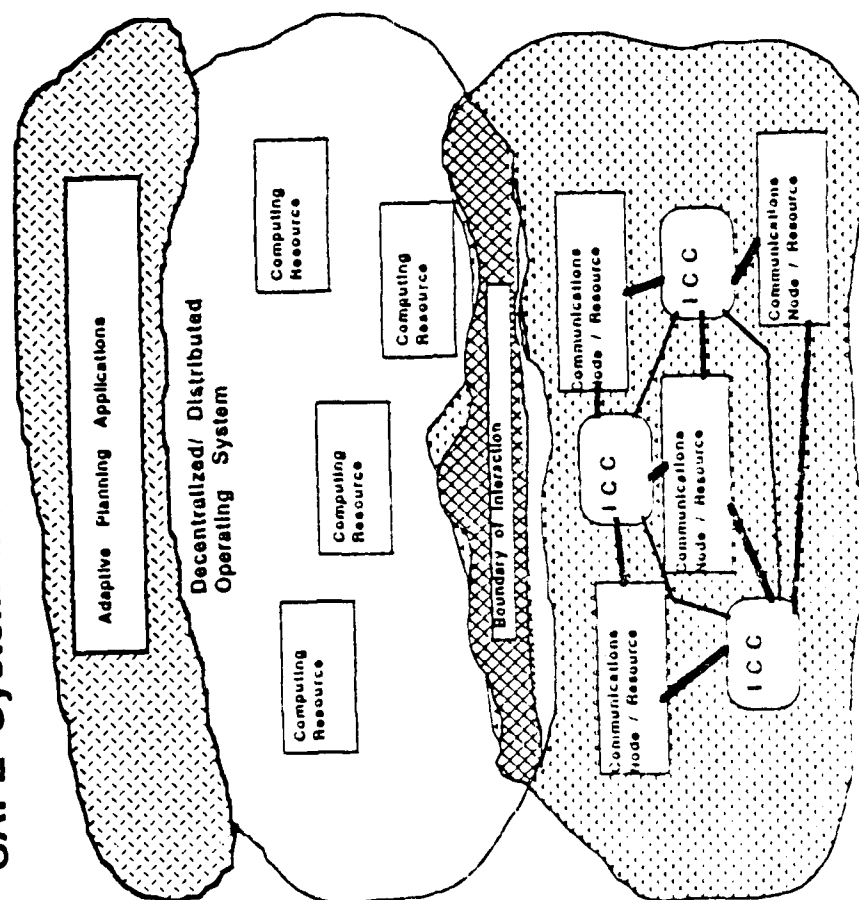


Figure 2.
Trans- Post-SIOP Conditions
Generalized Command and Control

One Possible SAPE System Model



System Level Issues

Research Areas

Sequential vs Non-sequential Architectures

System Evolvability

Security of System Level Operation

Technology Areas

Application of Dedicated Machines

Development and Evolution of Testbed

Integration of Communications and Processing

SAPE PROGRAM STRUCTURE

- * SURVIVABLE COMMUNICATIONS**
 - INTELLIGENT MULTIBAND COMMUNICATIONS**
 - AUTOMATIC RECONSTITUTION OF THE NETWORK**
- * DISTRIBUTED PROCESSING**
 - GEOGRAPHIC DISTRIBUTION OF PROCESSING**
 - CONTROL AND DISTRIBUTION OF PLANNING**
- * ADAPTIVE PLANNING**
 - DISTRIBUTED PROBLEM SOLVING**
 - ADAPTING TO CHANGING TARGET AND FORCE BASE**

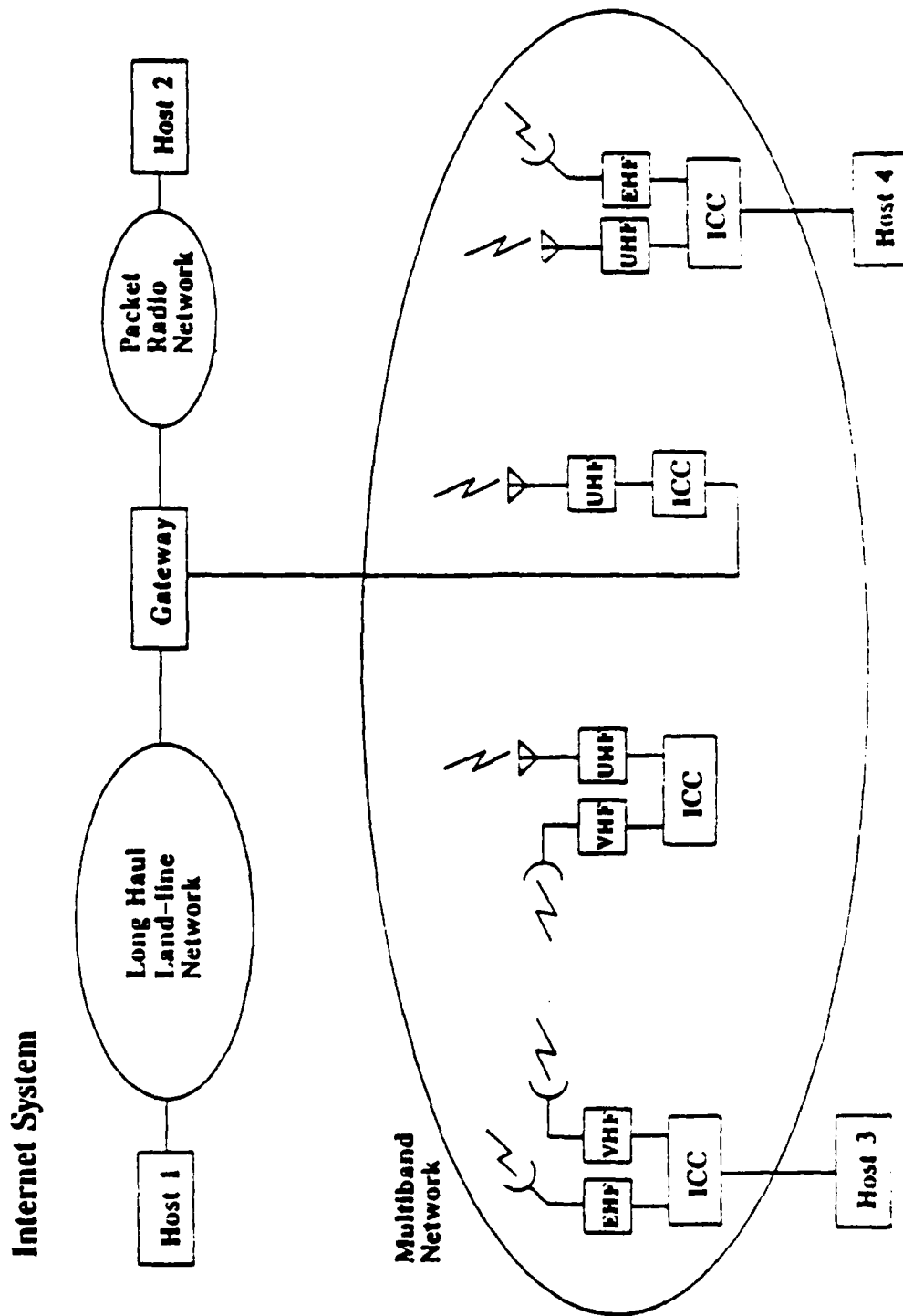
Intelligent Multiband Communications

Concept:

- Utilize all available communication media (e.g. tropo, HF, phone line, satellite, etc.) in combination to achieve highly survivable communications

Approach:

- Intelligent Communications Controller (ICC) placed at nodes where two or more existing communication systems are collocated
- Use digital section of LPR or other existing processor
- Network protocols select communication system for forwarding packets in real time, based on:
 - Propagation conditions
 - Packet size
 - Message priority
 - System loading
 - Internode connectivity
 - Et cetera



Communications Issues

Intelligent Communications Control

- Dynamic Environment and Resources
- Nearly Autonomous Operation
- Self Awareness for Resource Management
- Dynamic Reconfiguration under Stress
- Close Coupled to Distributed Operating System

Multi-Media / Multi-Band Communication Capability

- Focus on In House Design of Physical and Link Layer Interfaces
- Operation over Multiple RF Bands/Bandwidths
- Endpoint and Store and Forward Operation
- Ground, Airborne, and Space Platforms

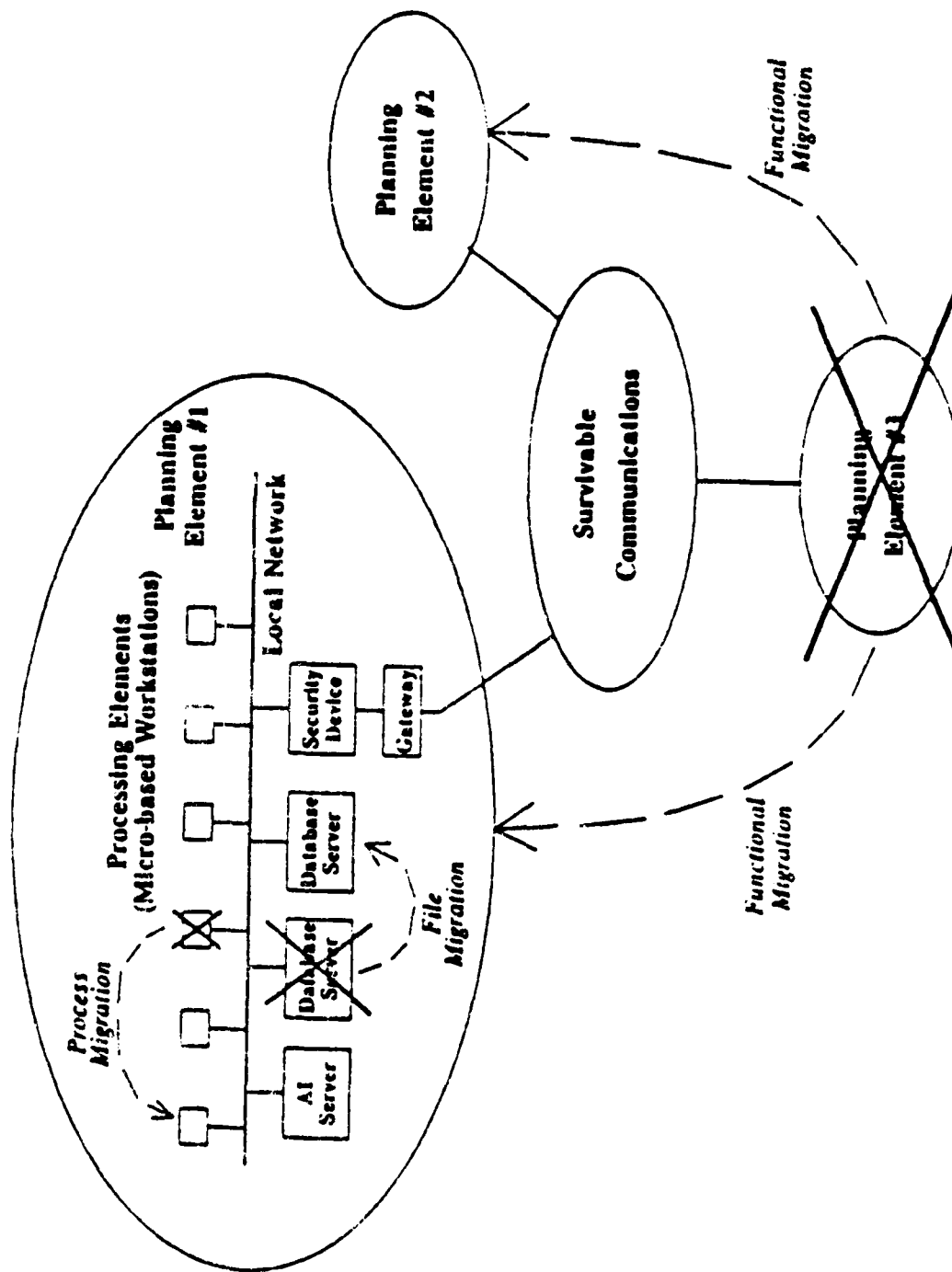
Survivable Distributed Processing

Concept:

- **Provide survivable adaptive planning by geographic distribution of processing facilities**

Approach:

- **Build a testbed of internetworked processing elements**
- **Integrate utility programs and an internet operating system to provide automated resource management, data distribution, and failure recovery for distributed applications**
- **Demonstrate survivable adaptive planning by installing and exercising adaptive planning software in the distributed processing testbed**



Distributed Processing Issues

Research Areas

- **Decentralized Distributed Operating Systems**
- **Heterogeneous Resource Bases**
- **Wide Geographic Separation of Resources**
- **Distributed Database Management**
- **Process and Data Migration Methods**

Technology Issues

- **Upward Scalability of Complex Systems**
- **Modularity of System Components**
- **Integration with Intelligent Communications System**

Software for Rapid Adaptive Planning

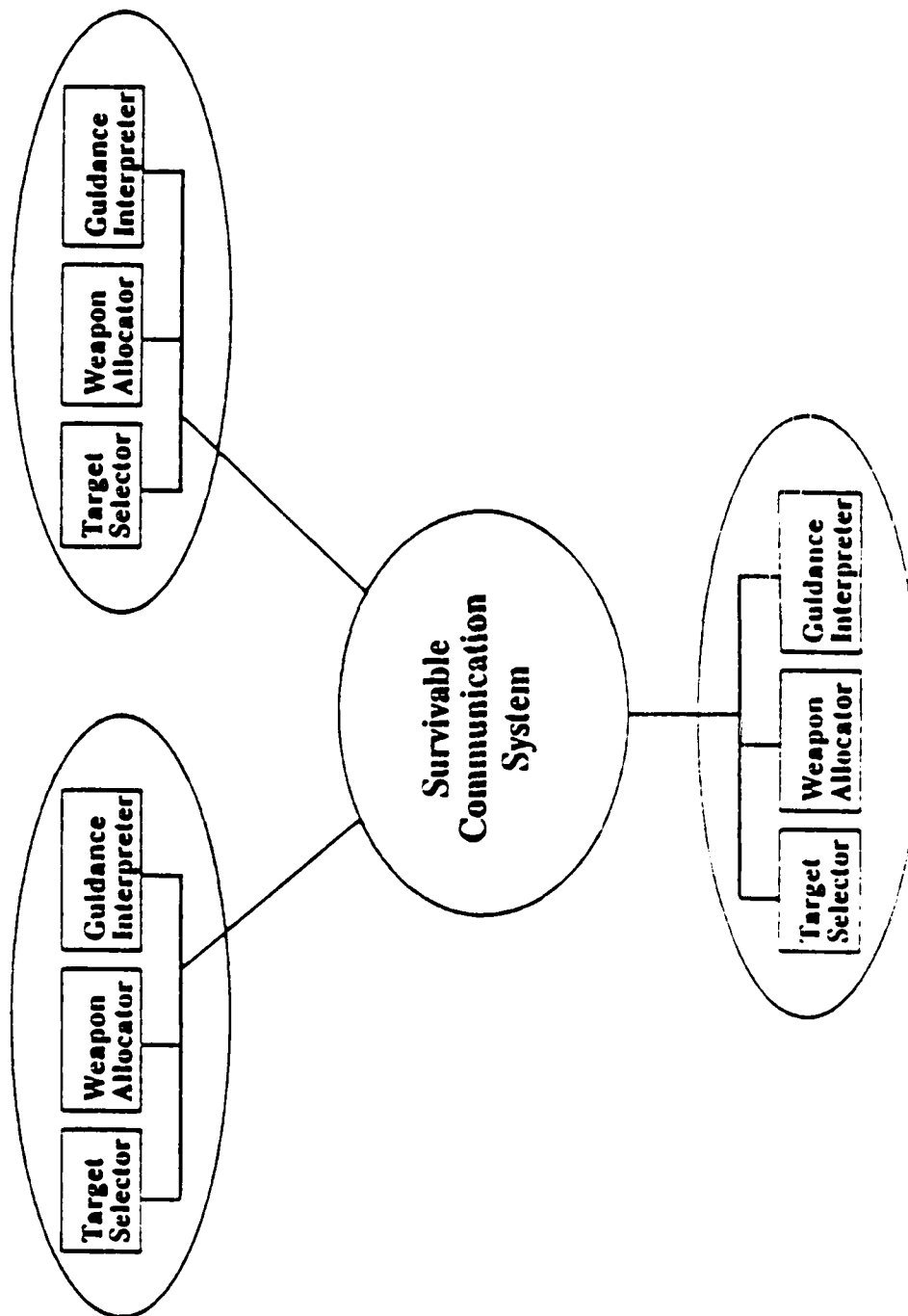
Concept:

- **Apply emerging information processing technologies to develop elements of a trans/post-attack adaptive planning system**

Approach:

- **Using recent advances in computer graphics and knowledge-based and natural language systems, design and build automated software systems to facilitate adaptive planning**
- **Apply current AI planning research results to implement a demonstration system which can:**
 - **Use plan "templates" rather than reasoning from first principles**
 - **Key amount of lookahead to available time frames**
 - **Use a plan knowledge representation that facilitates replanning**
- **Develop prototype systems in cooperation with an active user community, and demonstrate/evaluate results in field exercises using the survivable distributed processing testbed**

Adaptive Planning Functional Decomposition



Adaptive Planning Issues

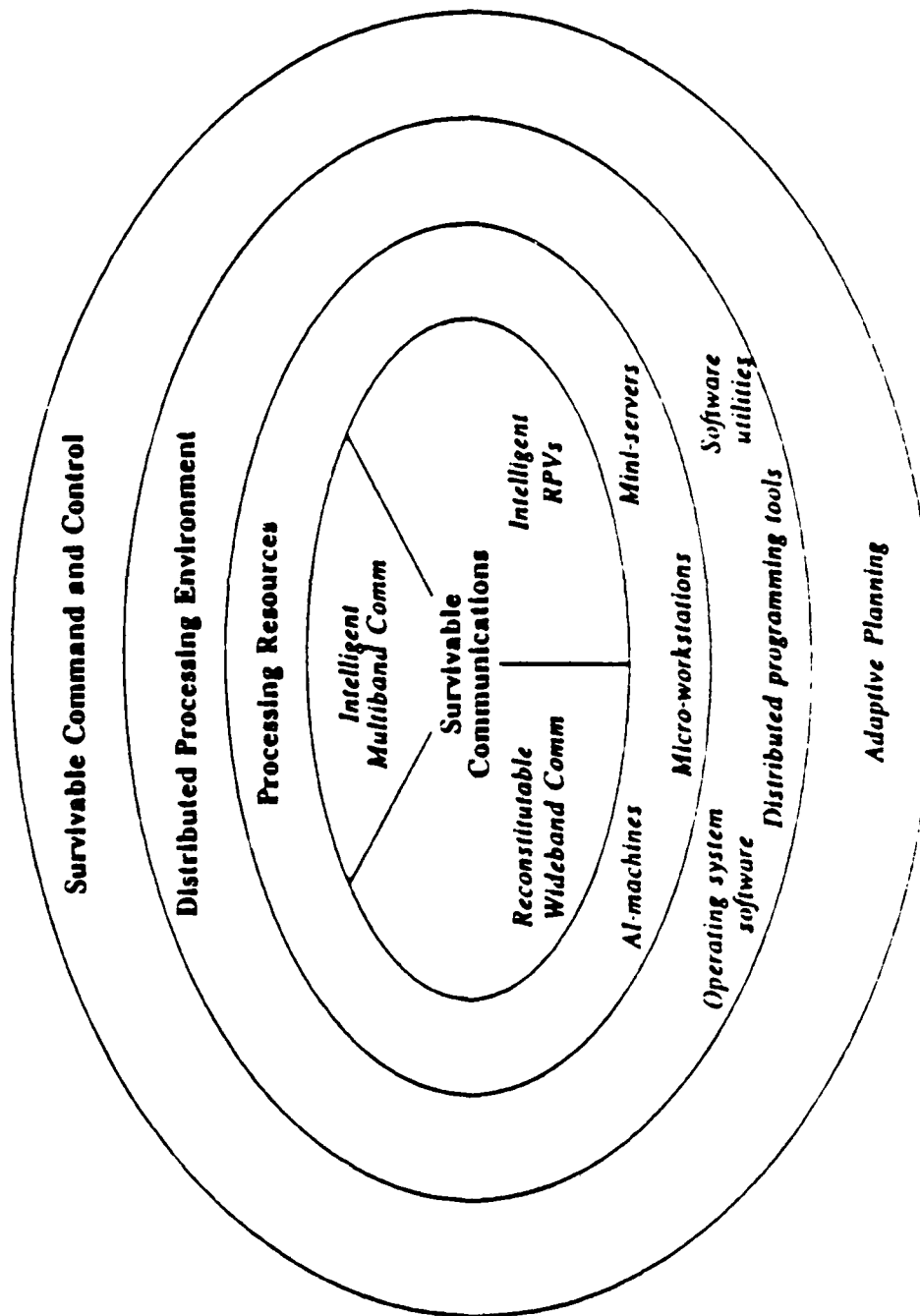
Research Areas

- Understanding Adaptive Planning Concepts
- Reasoning in Dynamic and Uncertain Environment
- Definition of Algorithms for Planning/Replanning

Technology Concerns

- Abstraction and Representation of Data
- Operation in a Distributed Environment
- Performance Measures : Speed and Correctness
- Nature of Computing Resource Base Needed

Survivable Adaptive Planning Architecture



Survivable Adaptive Planning Experiment

Phased Program Approach

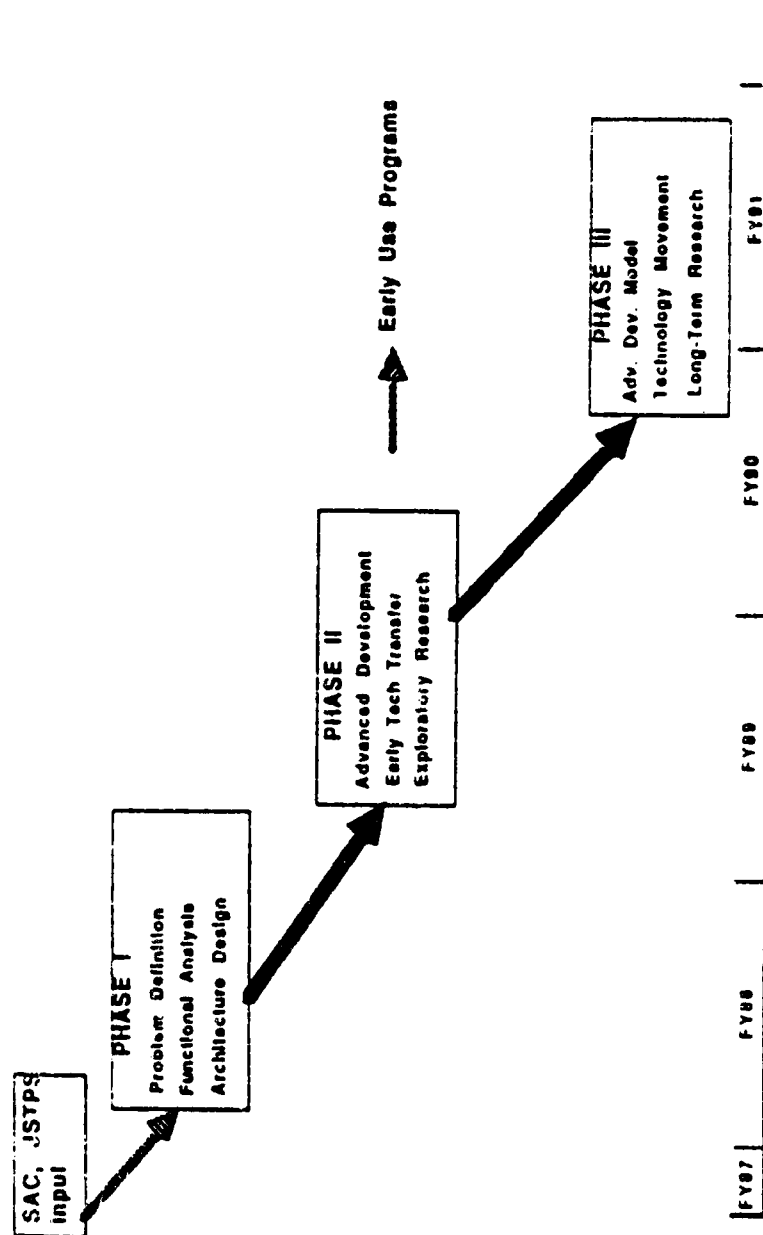


Figure 4.

EMERGING STANDARDS

IN

NETWORK MANAGEMENT

**C. E. LaBarre
The MITRE Corporation**

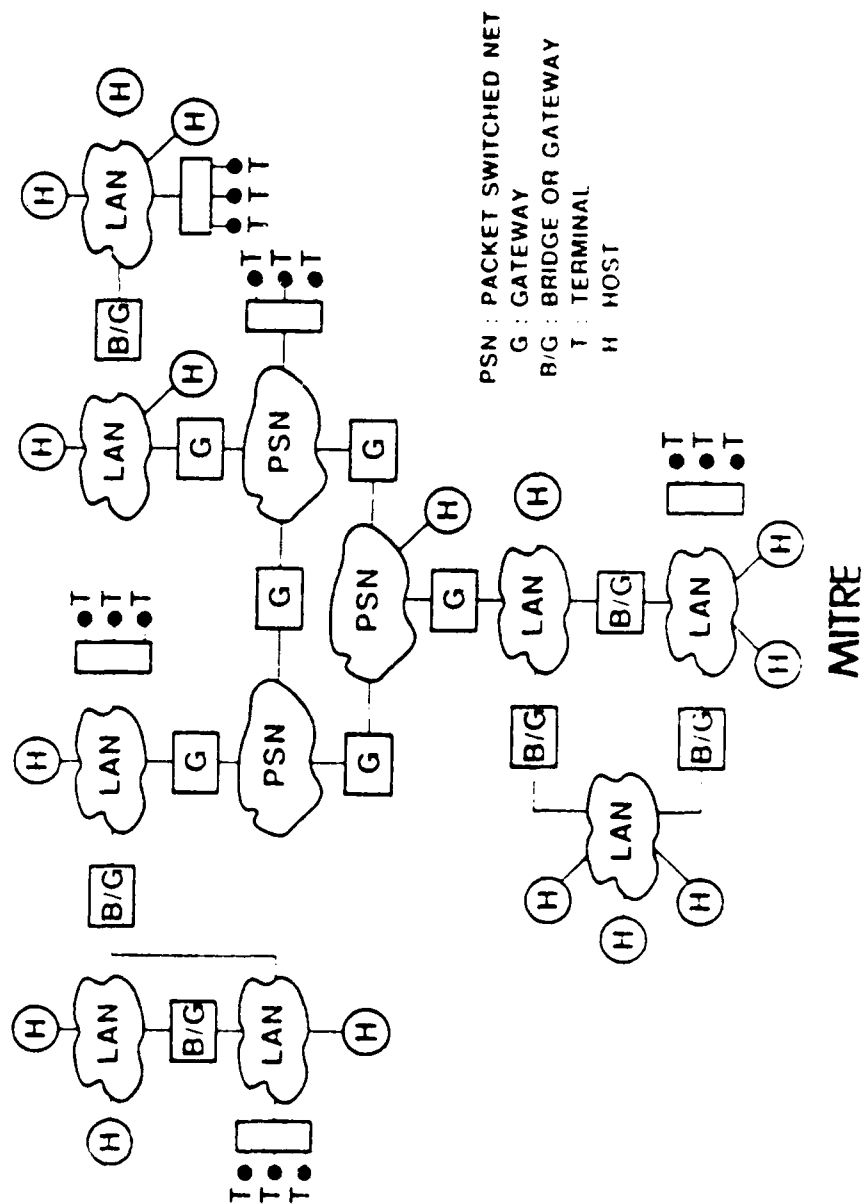
MITRE

Presentation Objectives

- Goals of network management standards
- ISO management standards
 - Model
 - Status
- CCITT management activities
- TCP/IP (DoD) management standards

MITRE

Environment



- Goals

- Interoperable net management products
- Allow vendor creativity, differentiation

- Strategy

- Develop standards for tools allowing multiple vendor managers to interoperate with multiple vendor OSI resources/device

Standard management reference model

Standard protocol(s)

Standard management information

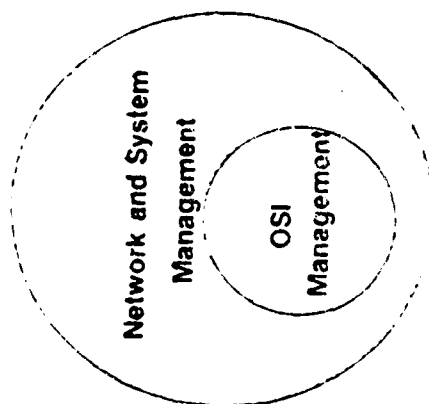
- How management is accomplished is not standardized

MITRE

OSI MANAGEMENT STANDARDS

MITRE

Scope of OSI Management



- What OSI Management is
 - Management for the OSI - relevant parts of open systems
 - A proper subset of network management
- What OSI Management is not
 - A total solution to network management

MITRE

NETWORK NODE
OR
OSI RESOURCE MANAGER

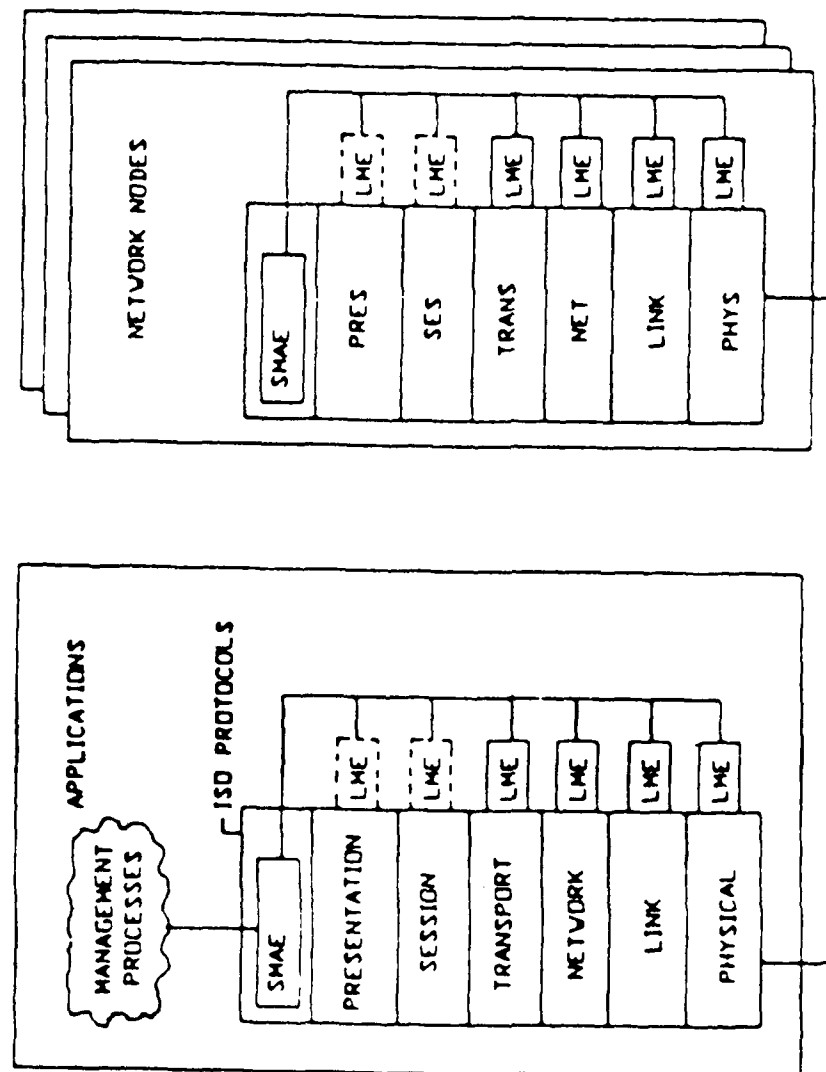


Figure 1: Overview ISO Management Reference Model

MITRE

Common Management Information Services/Protocols

- Event notification
 - Errors
 - Statistics reports
- Monitoring
 - Get { a,b,c} where AND (GE(X,1000)LE(X,5000)) best effort.
- Control
 - Create, delete instance of resource
 - Set {(a,10)(b,1)(c,0)} where {GE.(x,1000)} atomic
 - Action (e.g., execute diagnostic, trace, loopback)

MITRE

Structure of Management Information

- Status
- Counter
- Gauge (or meter)
- Tidemark
- Threshold
- Internal event information
- Report control information
- Log
 -
 -
 -

MITRE

Specific Management Information Services

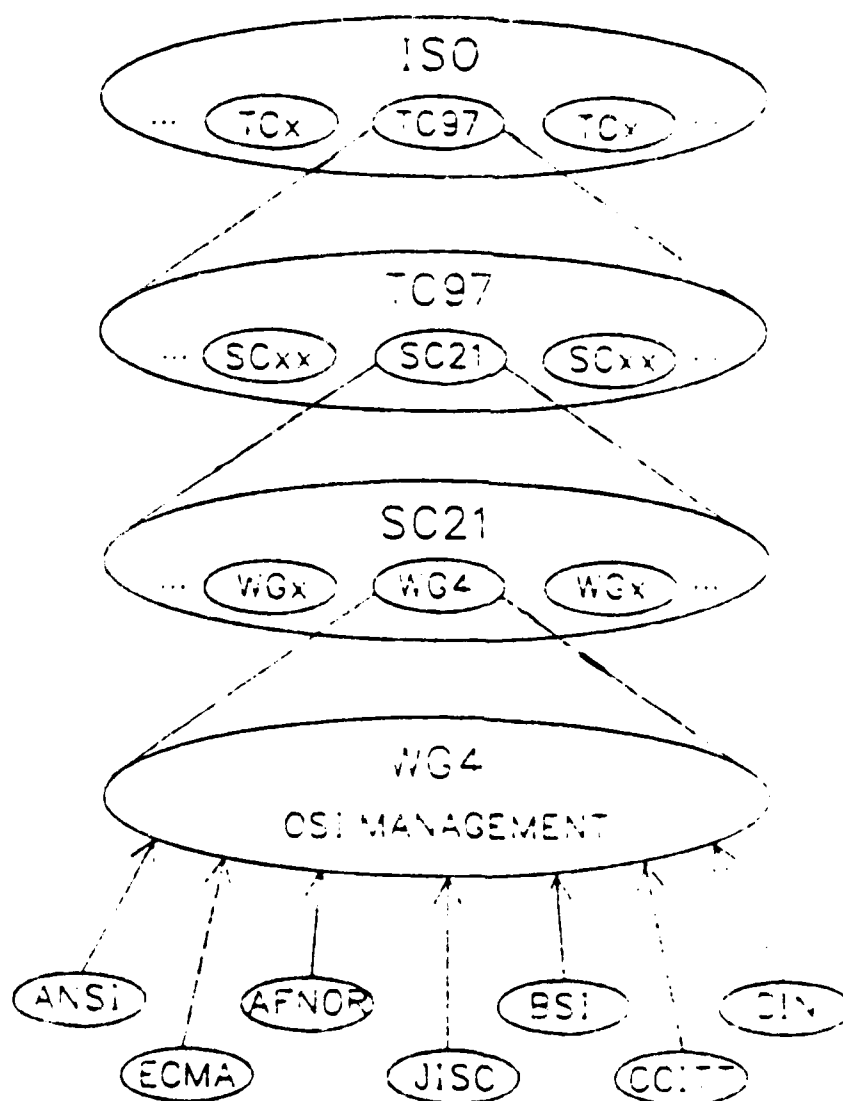
- Configuration
- Fault
- Performance
- Security
- Accounting

MITRE

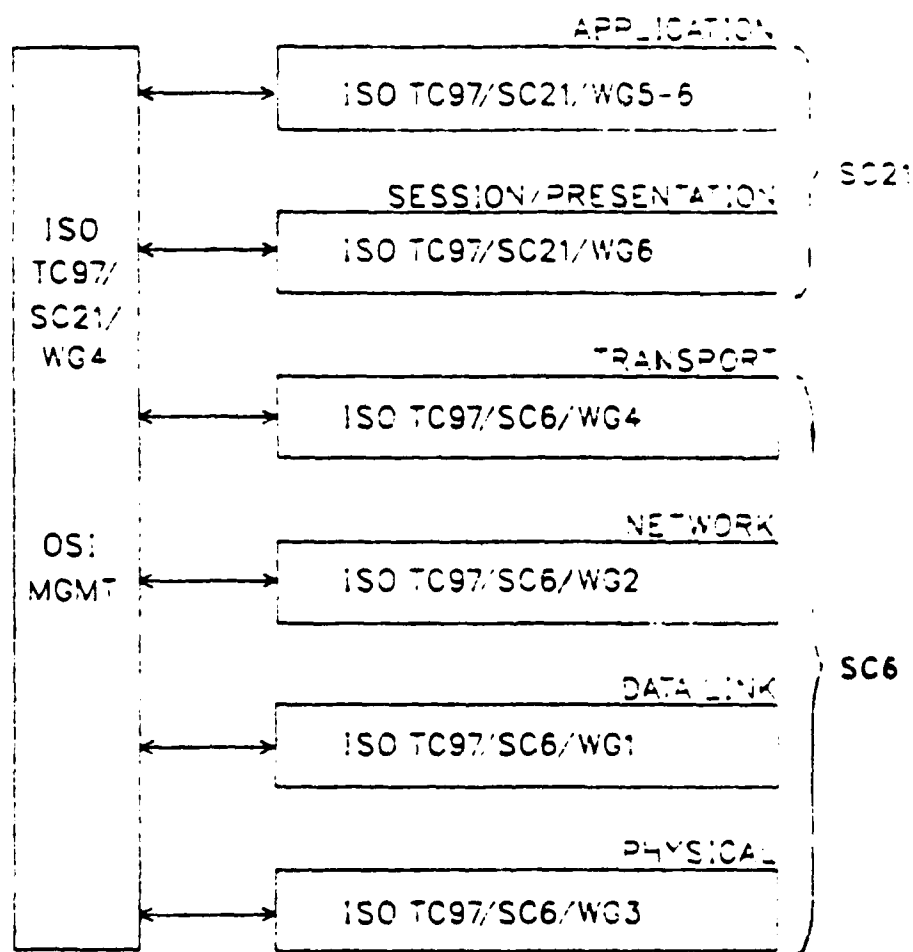
STATUS OF OSI STANDARDS

MITRE

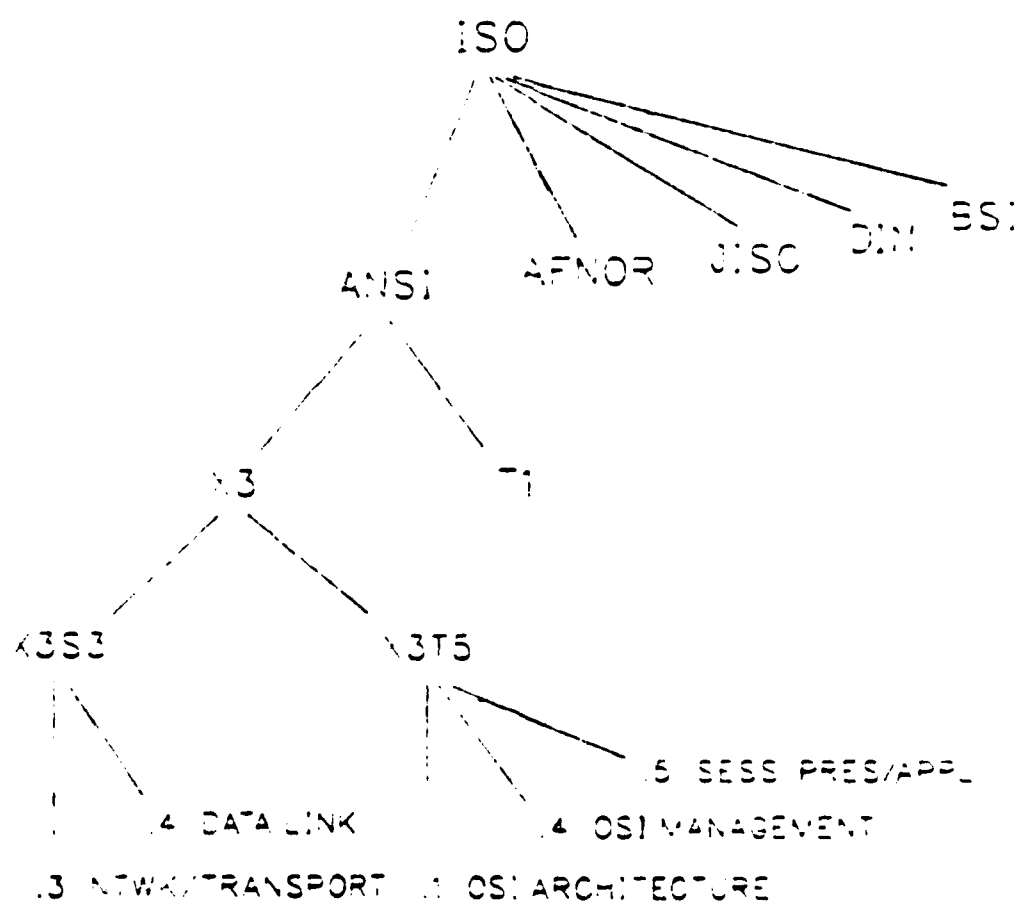
OSI MANAGEMENT RESPONSIBILITY



LAYER MANAGEMENT RESPONSIBILITY



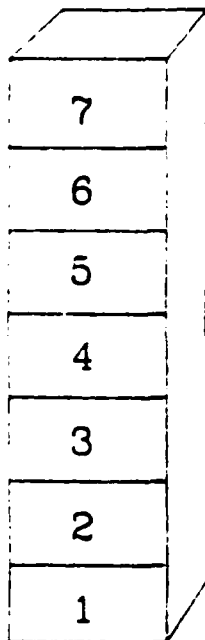
U.S. REPRESENTATION TO ISO



COS NMSC TUTORIAL

4/87

OSI REFERENCE MODEL



INTERNATIONAL STANDARD
ISO 7498

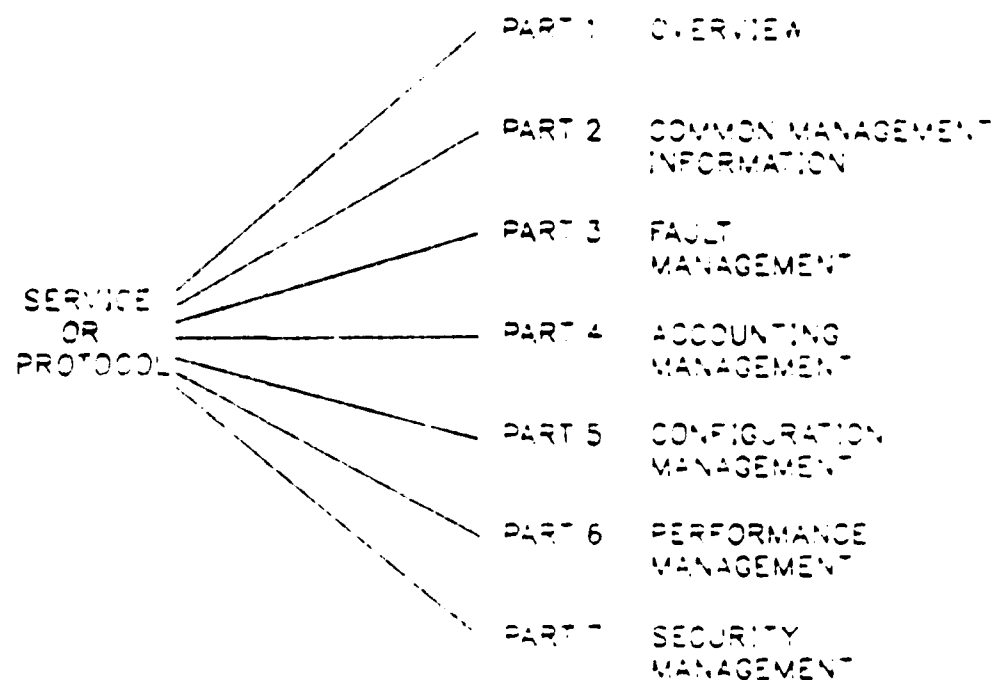
ADDENDA:

- /1 CONNECTIONLESS
- /2 SECURITY
- /3 NAMING AND ADDRESSING
- /4 OSI MANAGEMENT FRAMEWORK
 - SYSTEMS MANAGEMENT
 - LAYER MANAGEMENT ENTITIES
 - MIB
 - SMAP
 - SMAE
 - SMI ?

OSI SYSTEMS MANAGEMENT

DP 9595 - MANAGEMENT INFORMATION SERVICE DEFINITION

DP 9596 - MANAGEMENT INFORMATION PROTOCOL SPECIFICATION



Management Standards Schedule

<u>Title</u>	<u>DP</u>	<u>DIS</u>	<u>IS</u>	<u>Status</u>
OSI Management Framework DIS 7498/4	9/86	6/87	6/88	Dis
OSI Management Information Service and Protocol				
Part 1 - Overview				
Service Definition (DP 9595/1)	9/86	1/88	10/88	DP (second)
Protocol Spec. (DP 9596/1)	9/86	-----	-----	Suspended
Part 2 - Common Management				
Service Def. (CMIS) (DP 9595/2)	9/86	1/88	10/88	DP (second)
Protocol Spec. (CMIP) (DP 9596/2)	9/86	1/88	10/88	DP (second)

Mitre

Management Standards Schedule (Cont'd)

<u>Title</u>	<u>DP</u>	<u>DIS</u>	<u>IS</u>	<u>Status</u>
Part 3 -- Fault Mgmt.	2/88	2/89	12/89	WD *
Part 4 -- Accounting Mgmt.	11/88	11/89	9/90	WD
Part 5 -- Configuration Mgmt.	2/88	2/89	12/89	WD *
Part 6 -- Performance Mgmt.	11/88	11/89	9/90	WD
Part 7 -- Security Mgmt.	2/88	2/89	12/89	WD *
Part -- Structure of Mgmt. information	11/88	11/89	9/90	WD *

* Dates possibly changed as result of rapporteurs meeting in October.

MITRE

Directory Services Schedule

<u>Title</u>	<u>DP</u>	<u>DIS</u>	<u>IS</u>	<u>Status</u>
Directory Services (DP 9594/*)	9/86	11/87	6/88	DP (second)
Part 1 - Overview	"	"	"	"
Part 2 - Information Framework	"	"	"	"
Part 3 - Access and System Service Devinition	"	"	"	"
Part 4 - Procedures for Dist. Operation	"	"	"	"
Part 5 - Access and System protocol spec.	"	"	"	"
Part 6 - Selected Attribute types	"	"	"	"
Part 7 - Selected Object Classes	"	"	"	"
Part 8 - Directory Authentication	"	12/87	"	"

MITRE

Conclusions on DIS Schedules

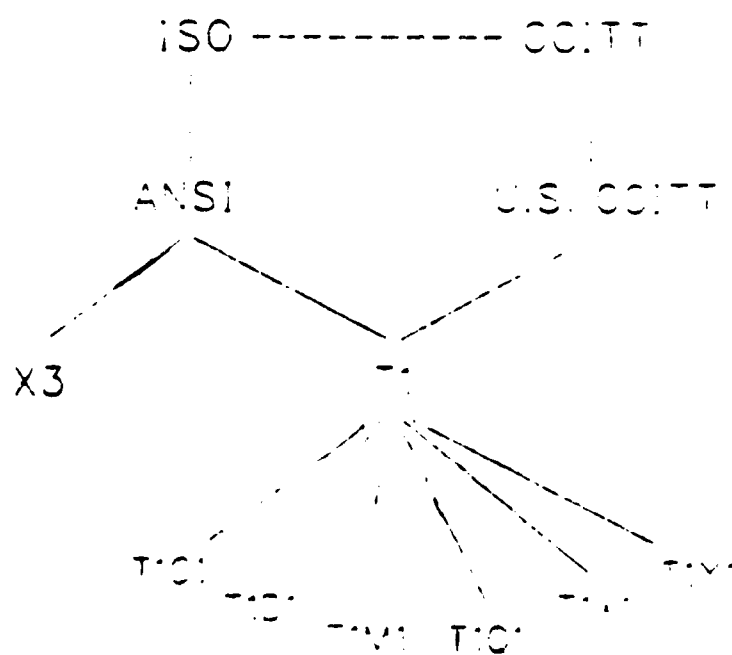
OSI Management Standards (Excluding layer specific management information)	1989
Lower layer management information standards	1990
Upper layer management information standards	1991

MITRE

CCITT MANAGEMENT ACTIVITIES

MITRE

TELECOMMUNICATION MANAGEMENT ACTIVITIES

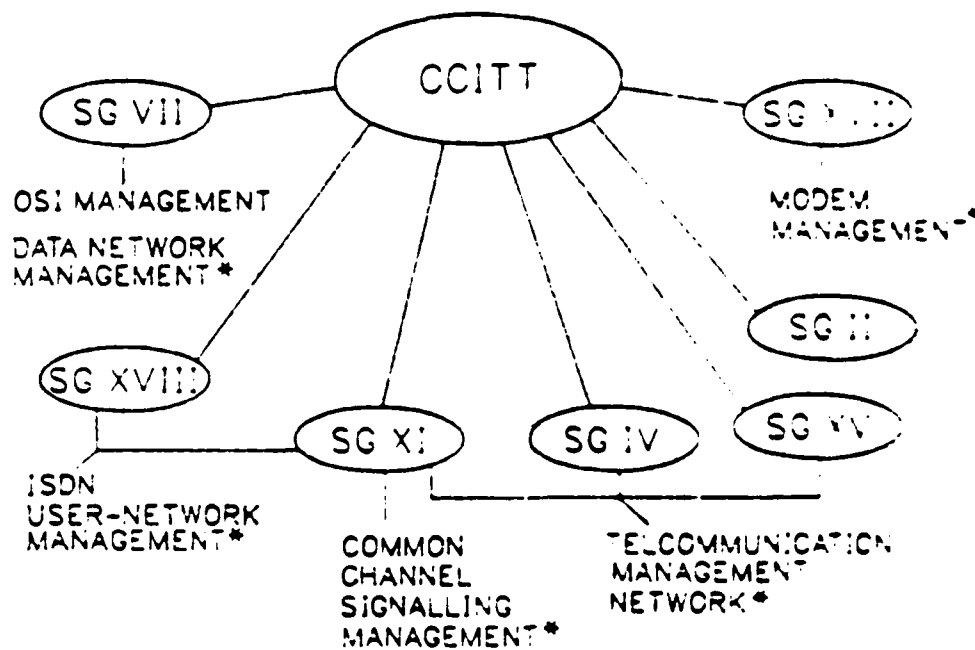


T1M1, CCITT - Telecommunication Management Network

T1M1, T1D1, CCITT - ISDN Management

T1X1, CCITT - Common Channel Signaling Management

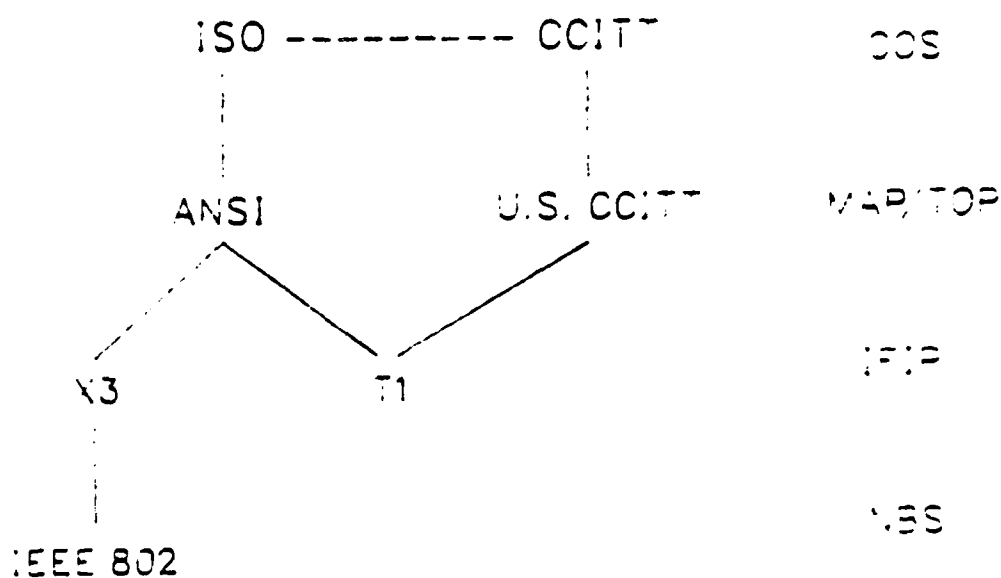
CCITT MANAGEMENT ACTIVITIES



* POTENTIAL APPLICATIONS OF OSI MANAGEMENT

SG II - OPERATIONS
 SG IV - MAINTENANCE
 SG VII - DATA COMMUNICATIONS NETWORKS
 SG XI - SWITCHING AND SIGNALLING
 SG XV - TRANSMISSION
 SG XVII - DATA OVER TELEPHONE NETWORKS
 SG XVIII - DIGITAL NETWORKS

OTHER RELATED ORGANIZATIONS



IEEE 802 - LAN Management

COS - Network Management Subcommittee

MAP/TOP - Network Management Requirements Specification

IFIP - Network Management Working Group

NBS - Likely formation of Network Management SIG

LAYER-SPECIFIC MANAGEMENT SPECIFICATIONS
 (LOWER LAYERS)
 ANSI, IEEE, MAP/TOP Work in Progress

	CONFIG.	FAULT	PERF.	SECURITY	ACCT.
TRANSPORT					
CLASS 0	XJ53.3	XJ53.3	XJ53.3		
CLASS 4	XJ53.3 MAP/TOP	XJ53.3 MAP/TOP	XJ53.3 MAP/TOP		
NETWORK					
CLNP	XJ53.3 MAP/TOP	XJ53.3 MAP/TOP	XJ53.3 MAP/TOP		
X.25	MAP/TOP	MAP/TOP			
DATA LINK					
LLC	802.2 MAP/TOP	802.2 MAP/TOP	802.2 MAP/TOP		
LAPB					
PHYSICAL					
CSMA/CD LAN	802.3 MAP/TOP	802.3 MAP/TOP	802.3 MAP/TOP		
TOKEN BUS LAN	802.4 MAP/TOP	802.4 MAP/TOP	802.4 MAP/TOP		
TOKEN RING LAN	802.5	802.5	802.5		

LAYER-SPECIFIC MANAGEMENT SPECIFICATIONS (UPPER LAYERS)

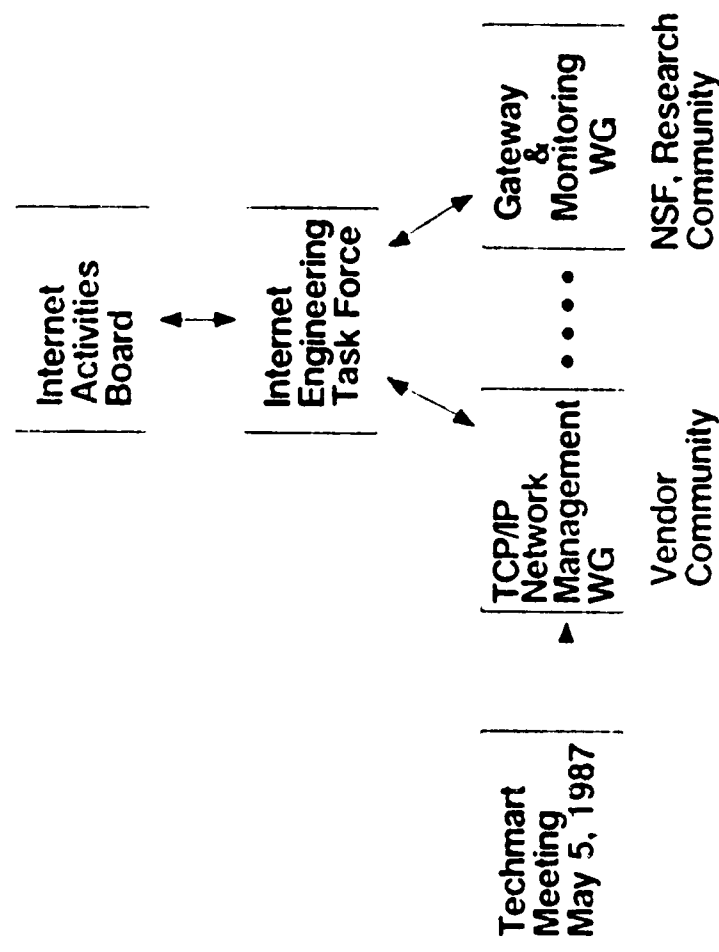
IEEE, MAP/TOP Work in Progress

	CONFIG.	FAULT	PERF.	SECURITY	ACCT.
APPLICATION					
ACSE	MAP/TOP	MAP/TOP	MAP/TOP		
FTAM					
MHS					
SMAE	802.1 MAP/TOP				
PRESENTATION					
KERNEL	MAP/TOP	MAP/TOP	MAP/TOP		
SESSION					
KERNEL	MAP/TOP	MAP/TOP	MAP/TOP		

**Internet (TCP/IP SUITE)
Management Standards**

MITRE

Background



MITRE

TCP/IP Network Management Schedule

- Working draft August 1987
- Initial draft RFCs December 1987
- Revised RFCs (if necessary) May 1987

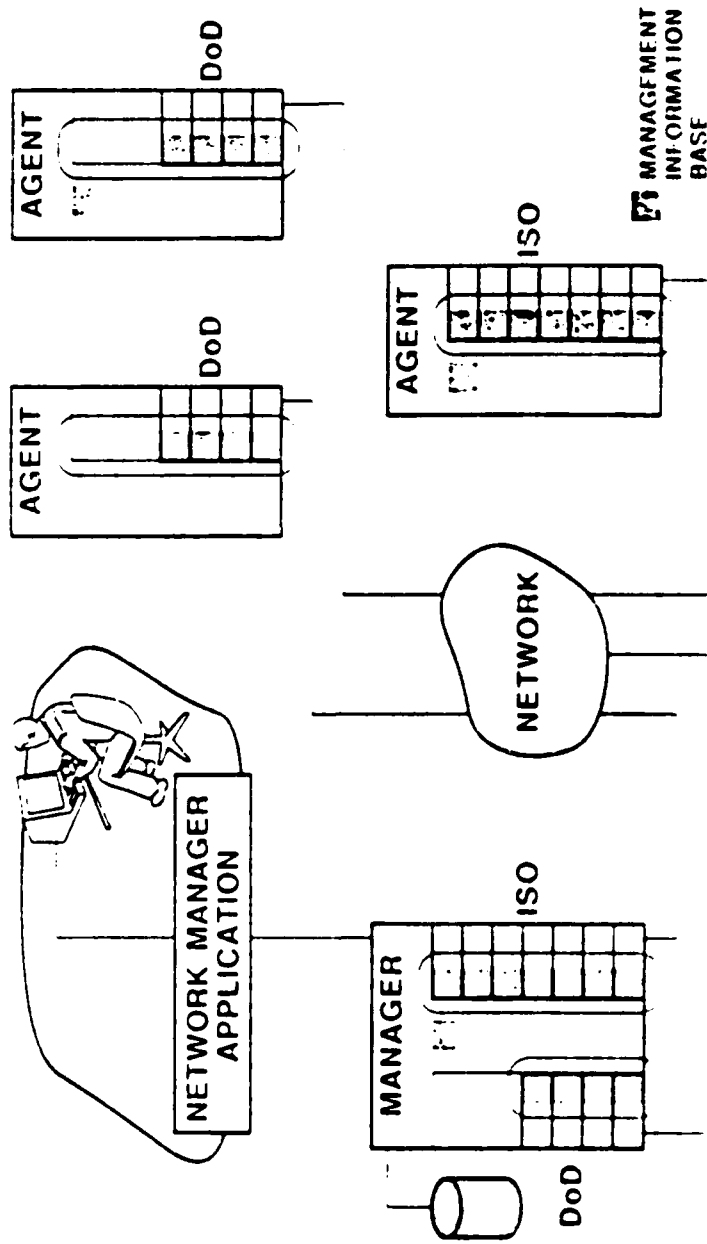
MITRE

TCP/IP Network Management

- Effort parallel to ISO efforts
- Uses ISO management framework
- Defines management protocol
- Defines parameters for
 - TCP/IP
 - Layers below IP (e.g. use IEEE 802)
 - FTP, TELNET, SMTP
- Network management WG & G + M WG
 - Activities overlap
(Convergence is in progress)

MITRE

Integrated ISO/DoD Network Management



MITRE

NBS Workshop Network Management Sig

**Chair: Dr. P. J. Brusil – The MITRE Corporation
(617) 271-7632**

TCP/IP Network Management WG

**Chair: C. E. LaBarre – The MITRE Corporation
(617) 271-8507**

ISSUES IN LINK MANAGEMENT

J. A. Hoffmeyer
Department of Commerce
Institute for Telecommunication Sciences
Boulder, Colorado 80303

The Institute for Telecommunication Sciences has had a long history in propagation research and transmission systems engineering. Much of this activity has been in support of military communications systems design, development, and testing. Although numerous technical issues remain in these areas, new research programs are now needed in the area of adaptive networks which provide survivable, endurable communications under a variety of operational conditions.

The subject of adaptive network design is both broad and complex. The viewgraphs provided are relevant to only one part of the problem--that of link management. The ITS does not currently have an ongoing research program which addresses the many problems in adaptive link management. However, there are several programs at ITS which are relevant to some of the key issues in link management.

The first two viewgraphs (ITS-1 and ITS-2) serve the purpose of introducing both the topic and the Institute for Telecommunication Sciences. This is followed by three viewgraphs (ITS-3 through ITS-5) that provide one view of the objectives and key issues in link management. The general objective is to develop communications links that are survivable, reliable and provide adequate service performance, and that can adapt to the operational environment. This can be achieved through the use of multimedia transmission links, distributed intelligence at the network nodes, the use of artificial intelligence, adaptive routing, etc.

Key issues include the definition of requirements, the design and development of adaptive algorithms for use at the intelligent nodes, and the testing of these algorithms. Testing must be preceded by the definition of performance measures to be used. Some examples of different types of performance measures are provided in viewgraph ITS-6.

The next five viewgraphs (ITS-7 through ITS-11) describe some ongoing programs at ITS which are believed to be relevant to the issues described in the preceding viewgraphs. ITS has developed a line-of-sight microwave channel simulator that is capable of simulating multipath fading conditions (see References 1 and 2). We have also developed the Transmission Monitor and Control Software (see viewgraph ITS-10 and References 1 and 4), and an algorithm which models the error distributions of a variety of channels (see viewgraph ITS-11 and References 5 and 6).

The ITS is currently developing a link simulation facility (viewgraph ITS-12) which is believed to be pertinent to the investigation of link management issues (viewgraph ITS-13). The outline of a suggested link management research program is provided in viewgraph ITS-14.

REFERENCES

1. J. Hoffmeyer, L. Pratt and T. Riley, "Performance Evaluation of LOS Microwave Radios," IEEE 1986 Military Commun. Conf., Monterey, CA, Paper No. 4.3.
2. J. Hoffmeyer and L. Vogler, "Measurement, Modeling, and Simulation of Line-of-Sight Microwave Channels," NATO AGARD Conf. Proc. No. 419, Scattering and Propagation in Random Media, Rome, Italy, May 1987.
3. J. Farrow and R. Skerjanec, "Transmission Monitoring and Control of Strategic Communication Systems," IEEE 1985 Military Commun. Conf., Boston, MA, Paper no. 26.4.
4. J. Farrow and R. Skerjanec, "Transmission Monitoring and Control of Strategic Communication Systems," IEEE Journal on Selected Areas in Communications, Vol. SAC-4, No. 2, March 1986, pp. 308-312.
5. L. Vogler, "Comparisons of the Two-State Markov and Fritchman Models as Applied to Bit Error Statistics in Communication Channels," NTIA Report 86-193, May 1986.
6. L. Vogler, "An Extended Single-Error-State Model for Bit Error Statistics," NTIA Report 86-195, July 1986.

OBJECTIVES OF LINK MANAGEMENT

SURVIABLE, ENDURABLE, RELIABLE, WIDEBAND COMMUNICATIONS

ADAPTIVE COMMUNICATIONS

AUTOMATION OF THE NETWORK OPERATOR'S SYSTEM CONTROL FUNCTIONS

ARTIFICIAL INTELLIGENCE FOR TECH CONTROL

DISTRIBUTED INTELLIGENCE

INTELLIGENT NODES

ISSUES IN LINK MANAGEMENT

DEFINITION OF REQUIREMENTS

IDENTIFICATION OF PERFORMANCE PARAMETERS

NODE

LINK

NETWORK

USER-ORIENTED

DESCRIPTION OF MEASUREMENT METHODOLOGY FOR PERFORMANCE PARAMETERS

DISTRIBUTED INTELLIGENCE AT THE LINK NODES

DEFINITION OF INFORMATION NEEDED AT THE SWITCHES

DEFINITION OF INFORMATION NEEDED AT THE NODES

ALGORITHMS

ISSUES IN LINK MANAGEMENT (CONTINUED)

ADAPTIVE MODULATION AND CODING

ADAPTIVE ROUTING

MULTIMEDIA TRANSMISSION

NETWORK INTEROPERABILITY

COMMUNICATIONS STANDARDS

BUILT IN TEST EQUIPMENT

MODELING OF INTEGRATED SERVICES TRAFFIC

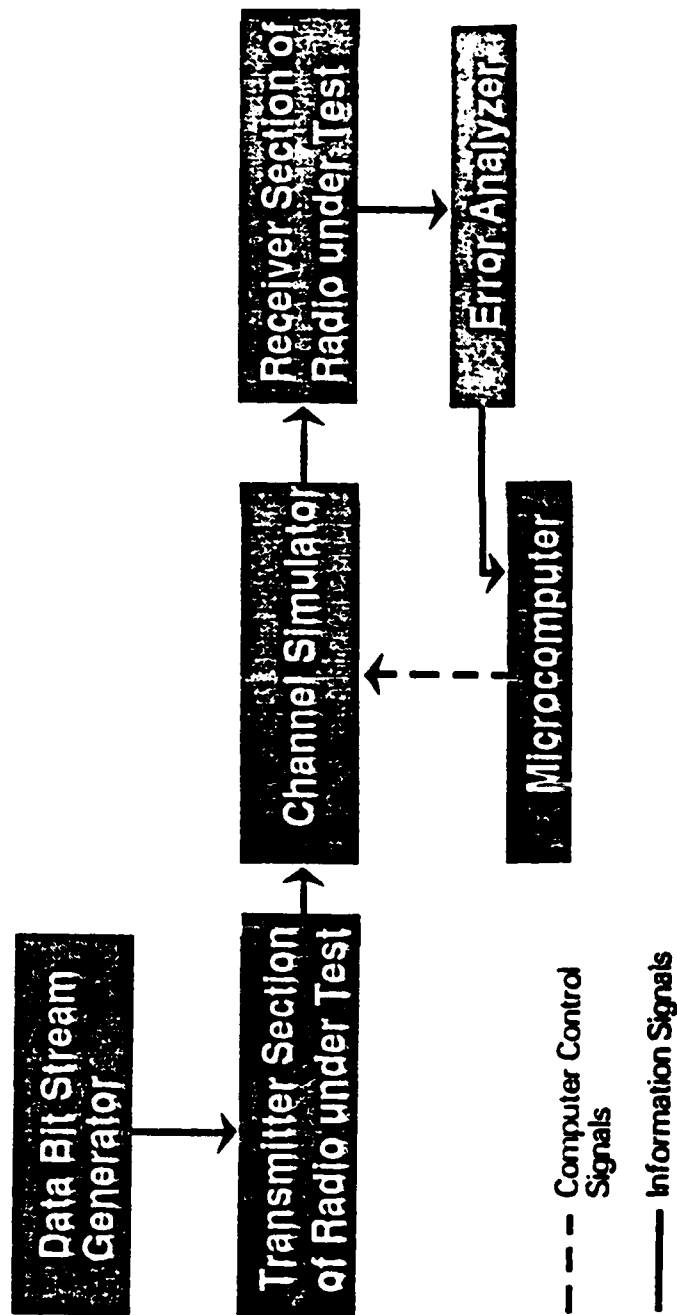
EXAMPLES OF PERFORMANCE MEASURES

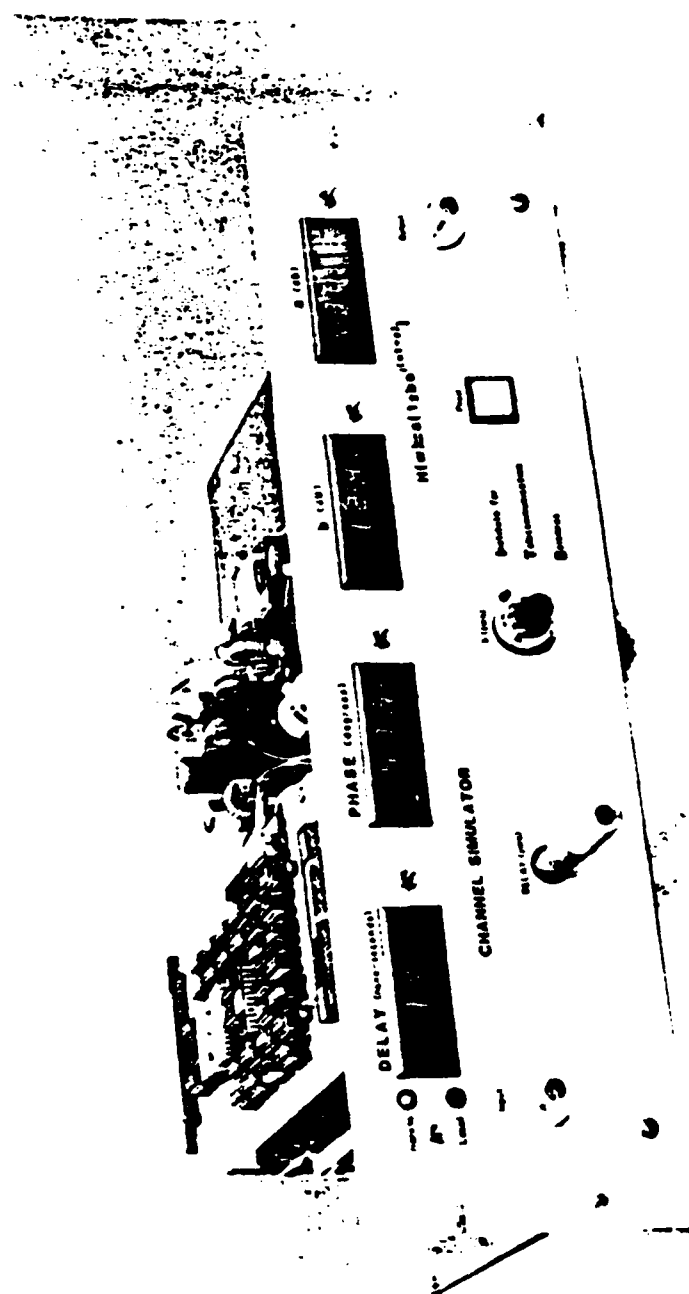
	NODE	LINK	NETWORK
USER ORIENTED	—	—	* BLOCK TRANSFER TIME • BIT ERROR PROBABILITY • BIT LOSS PROBABILITY • •
NETWORK OPERATOR ORIENTED	• EQUIPMENT RELIABILITY • DELAY • • •	• LINK ERROR PERFORMANCE • FRI • EYE OPENING • • •	• NETWORK THROUGHPUT • OVERALL NETWORK ERROR PERF. • ROUTING EFFICIENCY • • •

• FROM ANS X3.102



Radio Testing using a Channel Simulator

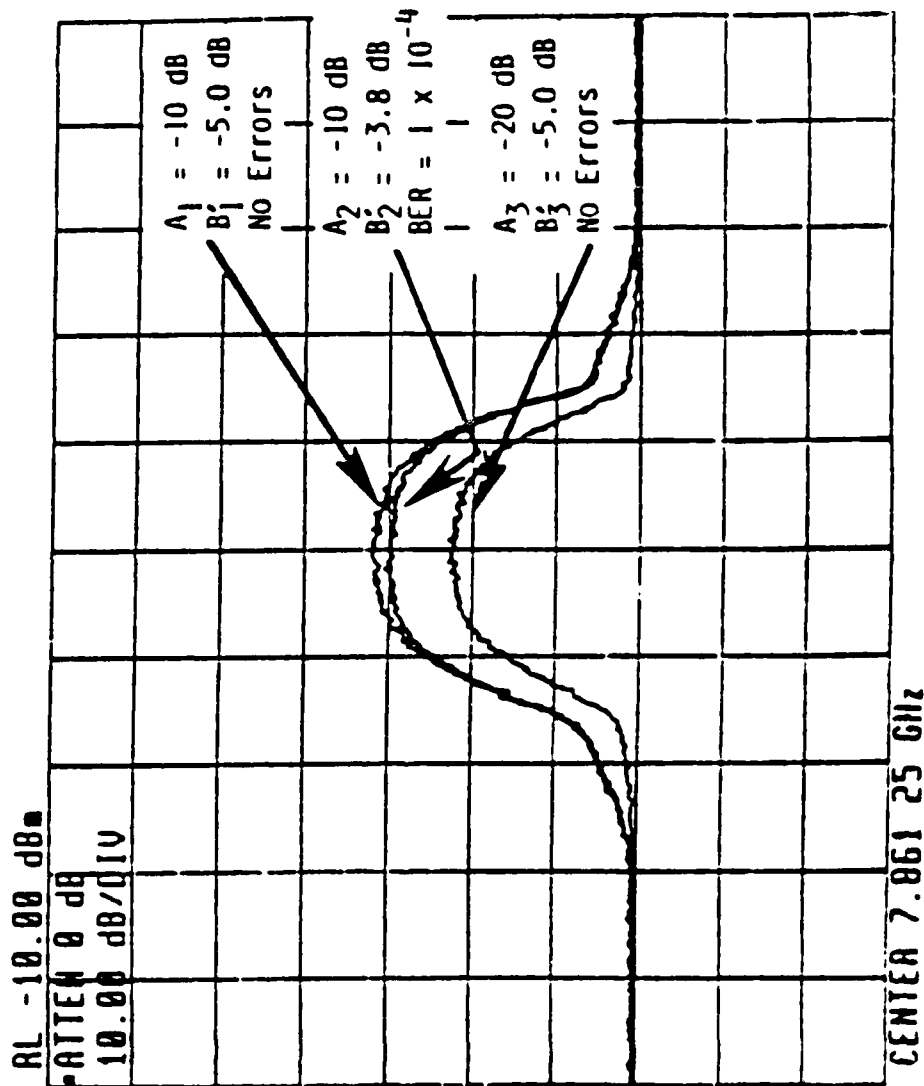




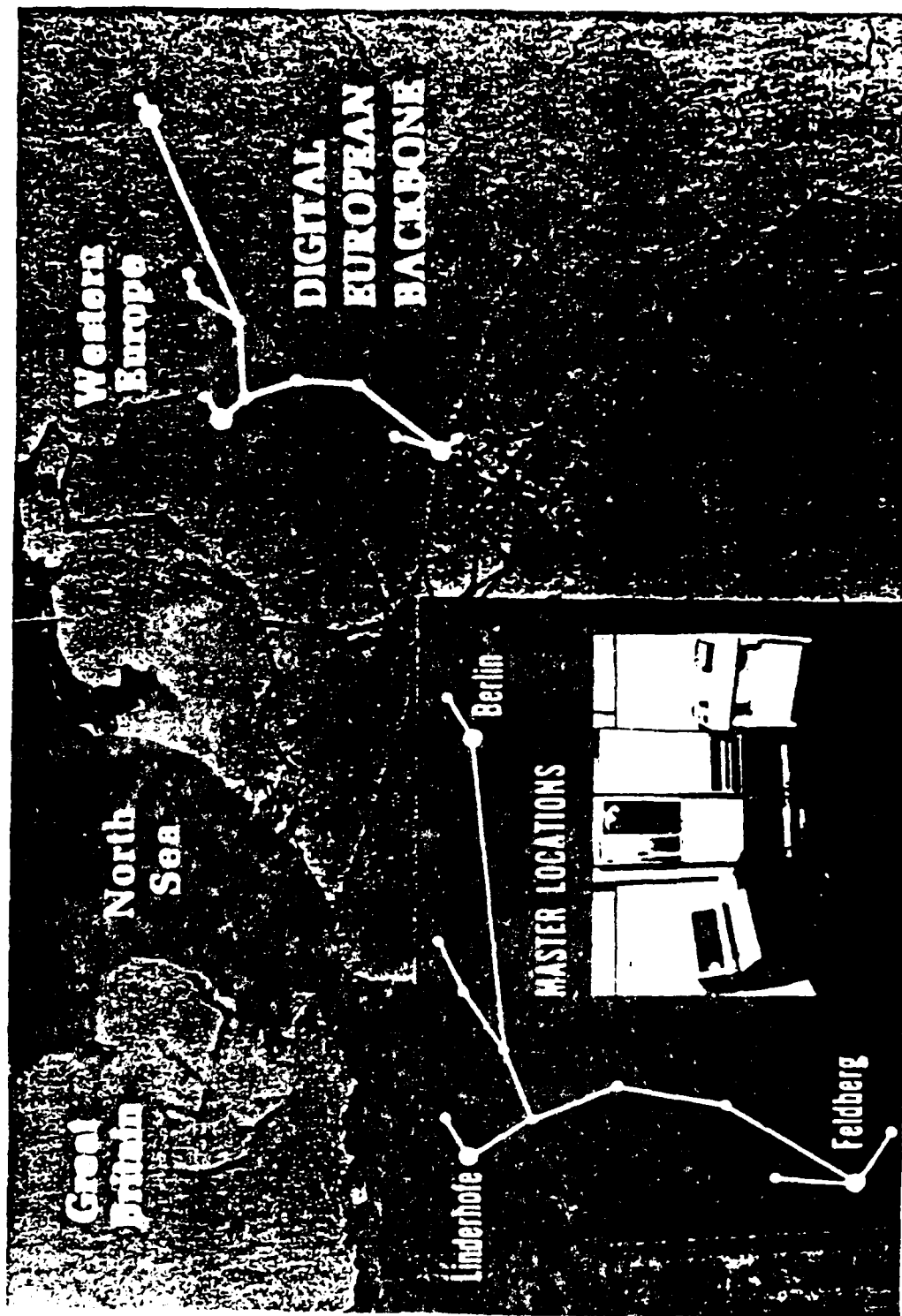
line-of-sight channel simulator.



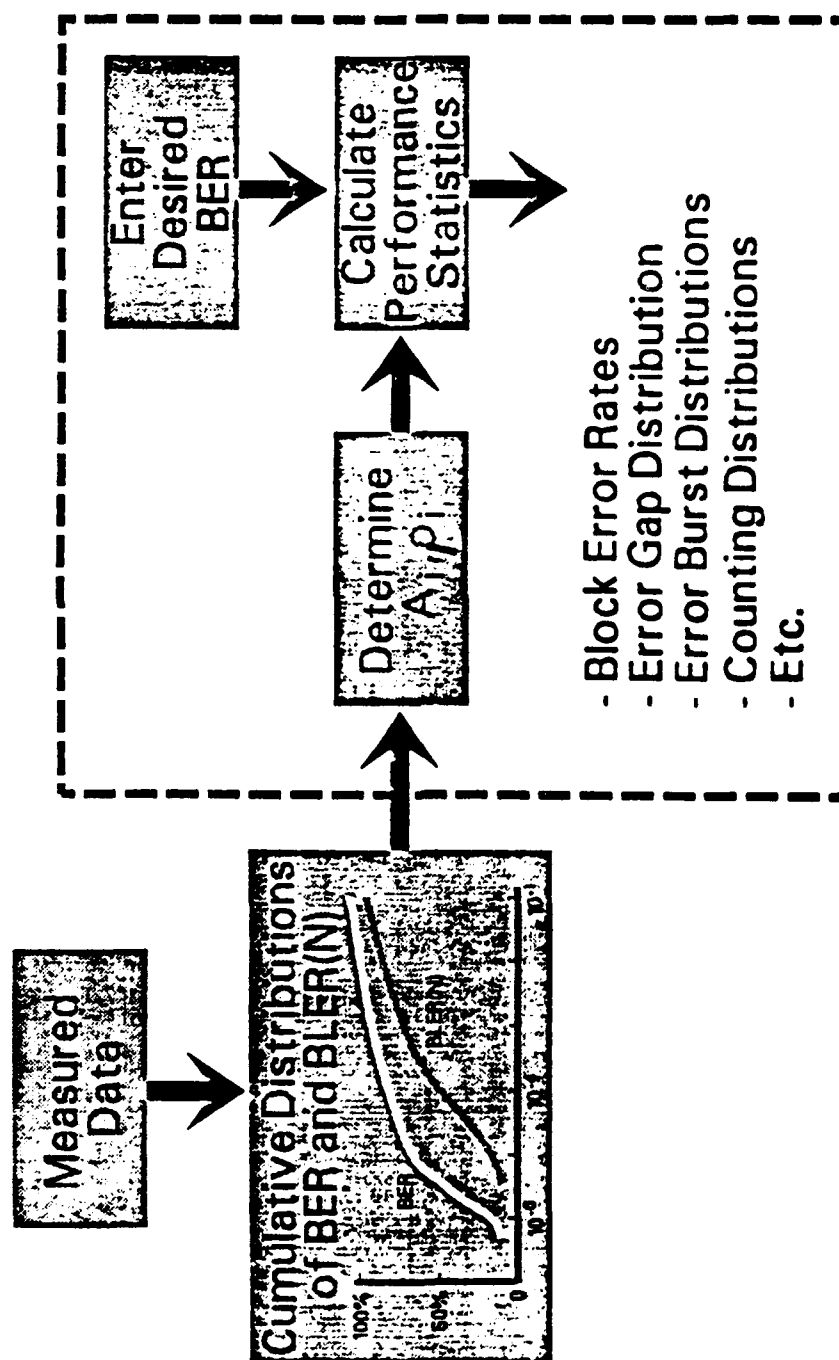
SIMULATOR OUTPUT



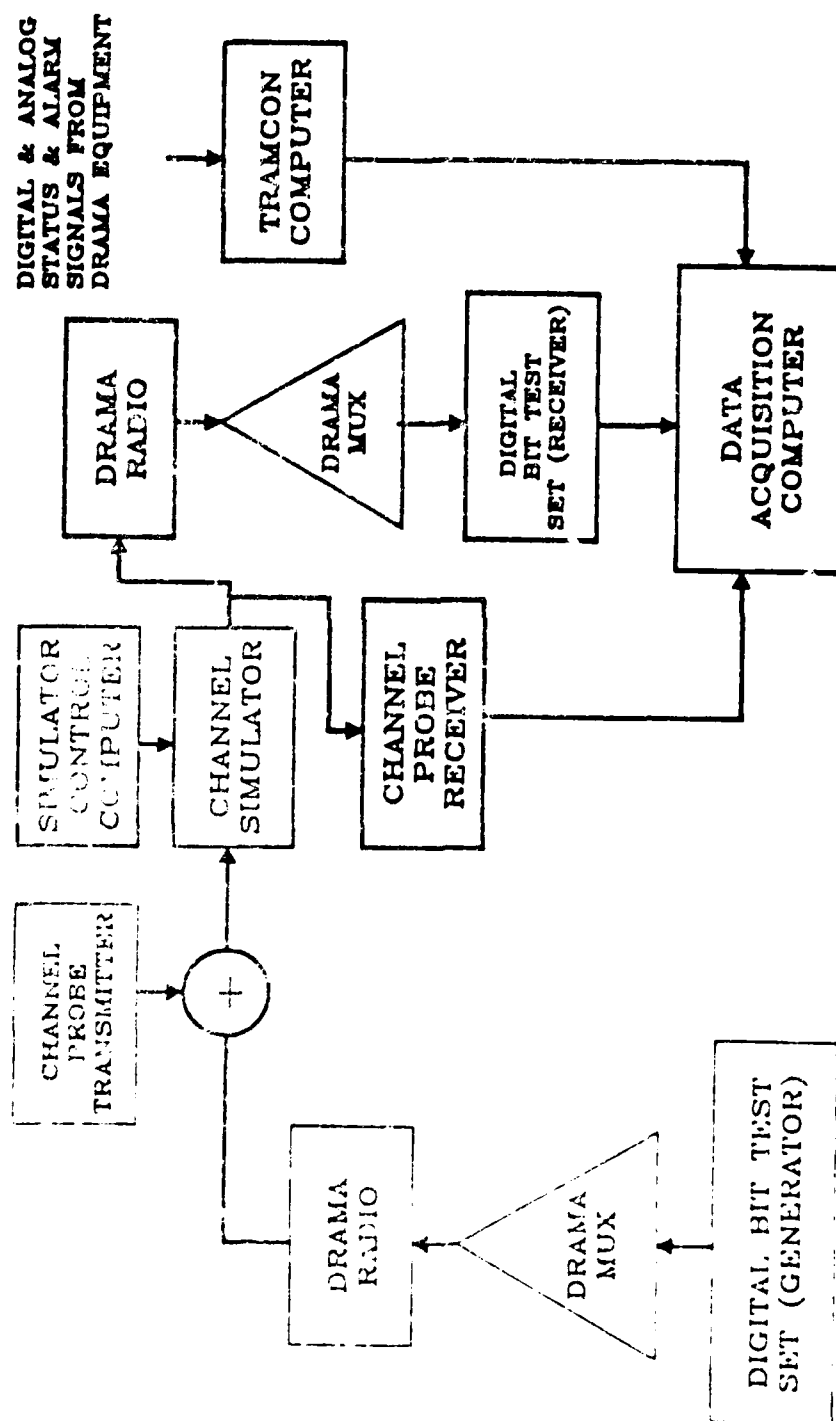
$\tau = 12$ ns
 $\phi = 289.7^\circ$



Extended Single Error State (SES) Model

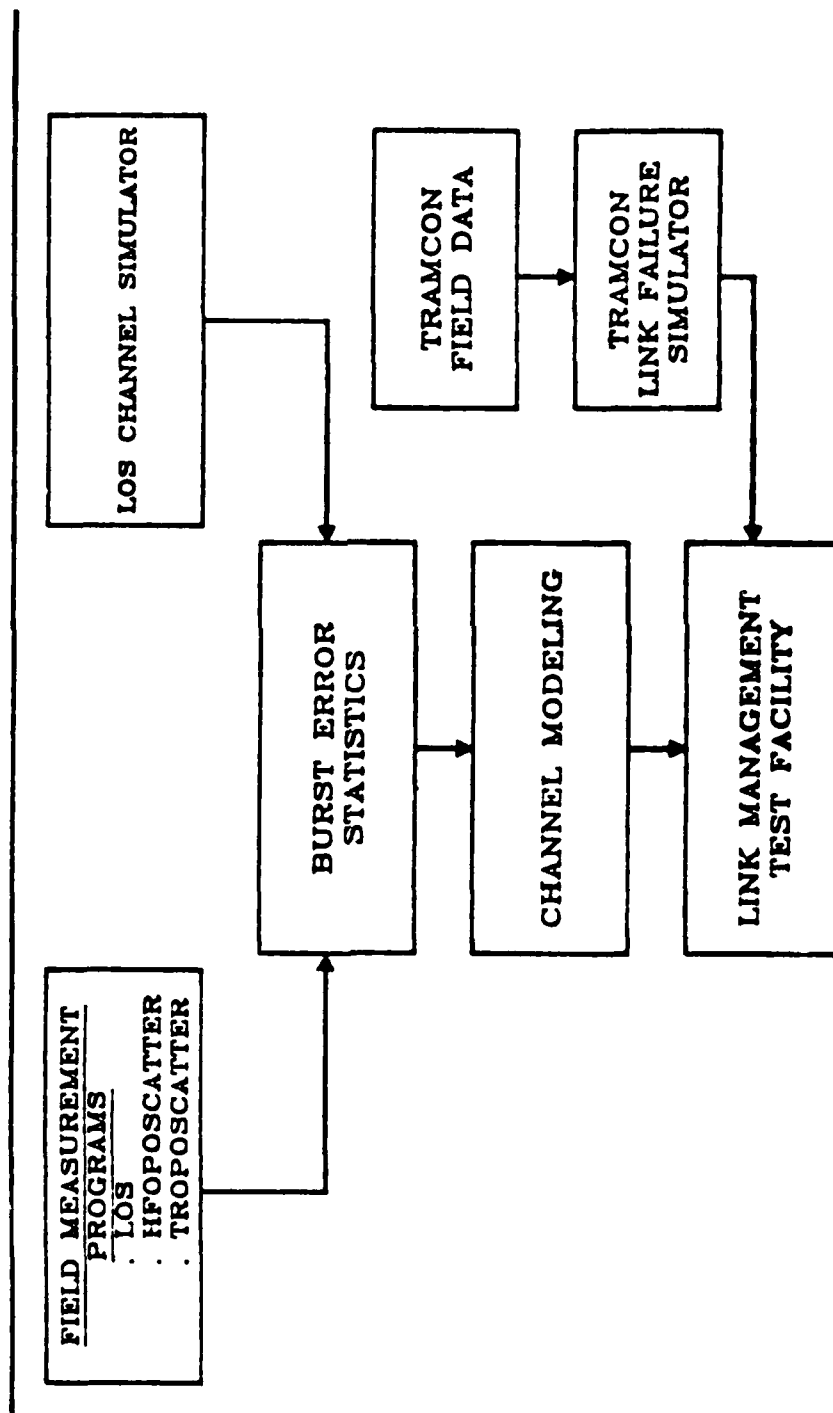


ITS LINK SIMULATION FACILITY

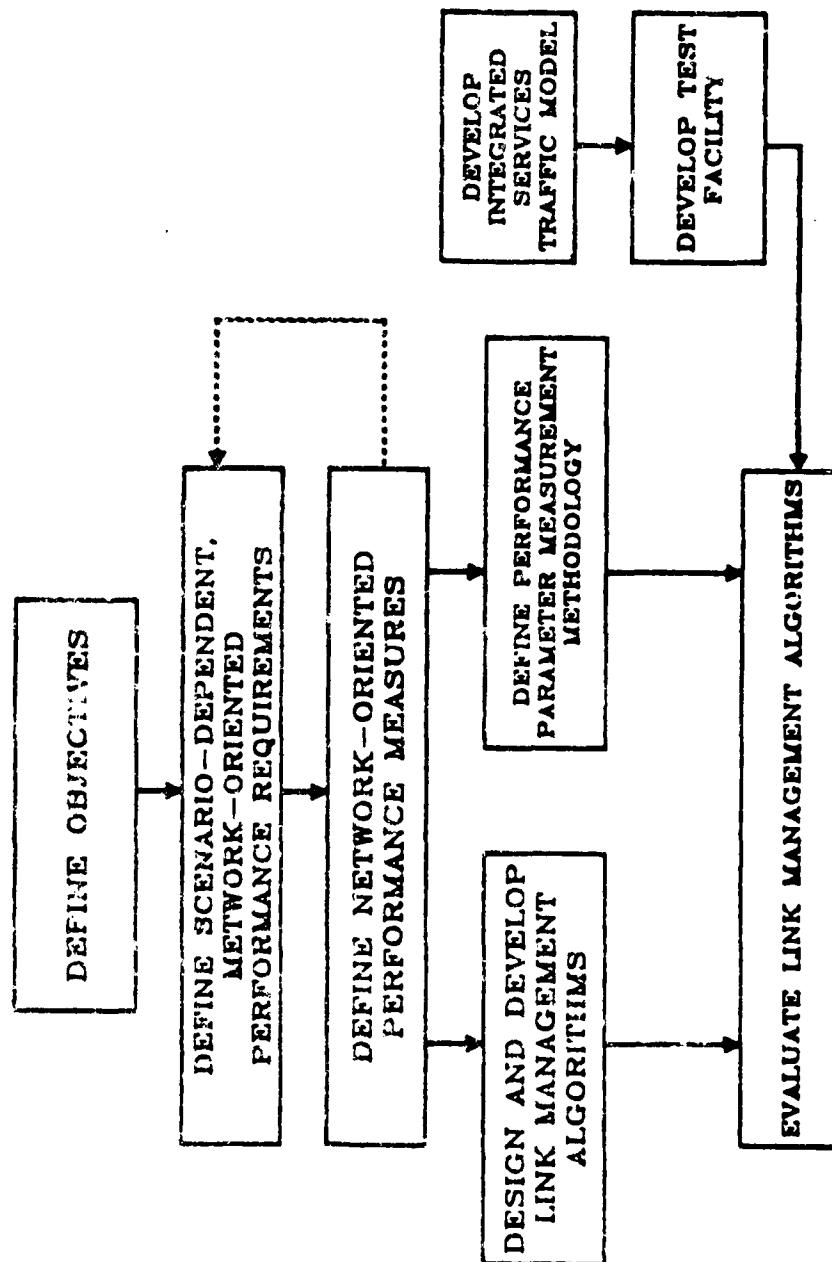




APPLICATION OF LINK SIMULATION FACILITY TO LINK MANAGEMENT ISSUES



OUTLINE OF LINK MANAGEMENT PROGRAM



AD-1193 374

PROCEEDINGS OF THE COMMUNICATIONS NETWORK MANAGEMENT
WORKSHOP (1987) HELD. (U) ROME AIR DEVELOPMENT CENTER
GRIFFISS AFB NY J J SALERNO ET AL. NOV 87

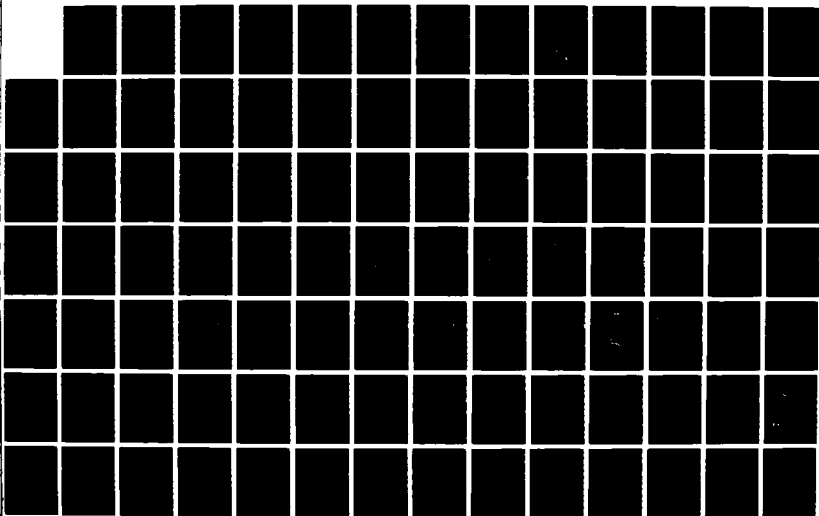
275

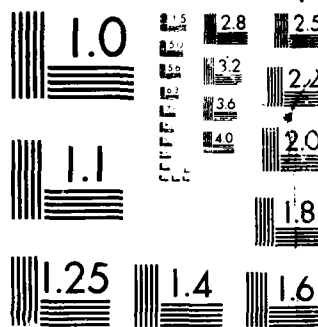
UNCLASSIFIED

RADC-TR-87-231

F/G 25/4

NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963

NETWORK SURVIVABILITY THROUGH CONNECTIVITY OPTIMIZATION*

Dr. Michael A. Schroeder, Mr. Kris T. Newport

The MITRE Corporation
RADC/TOFM
Griffiss AFB, New York 13441-5700

ABSTRACT

The potential degradation of a network composed of communications links and processing nodes into a set of disconnected, stand-alone elements is a driving concern of all system designers. This paper formulates a quantitative, graph-theory-based methodology for measuring network connectivity. Extending past efforts, primarily geared towards simple node-pair analysis, this methodology investigates connectivity from a global, network-wide perspective. It provides a measure of how well nodes within a network are initially interconnected and to what degree the network maintains that connectivity when faced with critical resource losses. Using this methodology, different initial network configurations can be compared, potential resource loss sequences evaluated, and possible real-time reconfiguration schemes suggested.

This work was funded by the Air Force Electronic Systems Division, AFSC, under contract F19628-86-C-0001. The project office for the work is located at the Rome Air Development Center.

*Previously presented at the IEEE International Conference on Communications '87 held June 7-10 in Seattle, WA. Article published in volume 1 of conference proceedings.

Network Survivability Through Connectivity Optimization

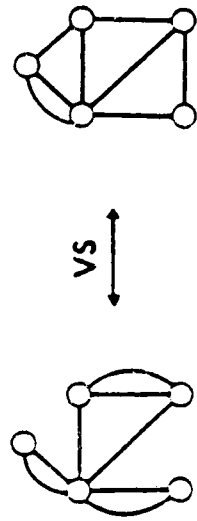
Michael A. Schroeder
Kris T. Newport

MITRE

Outline

- The Problem
- Theoretical Background
- Connectivity Measures
- Design Implications
- Monitoring/Reconfiguration

The Problem

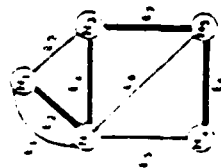
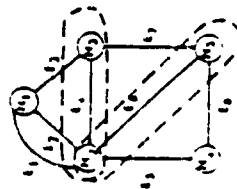
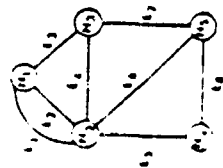


- NETWORK DESIGN
CURRENTLY OPTIMIZED TO MEET PROCESSING/
PERFORMANCE GOALS
- SHORTCOMING
OFTEN RESULTS IN POOR CONNECTIVITY
BASED SURVIVABILITY
- AUGMENTATION OF DESIGN PROCESS
BALANCE PROCESSING/PERFORMANCE GOALS WITH
TOPOLOGICAL STABILITY CONSIDERATIONS

Connectivity Measures

- Global, Network-Wide Perspective
- Multiple Levels of Decomposition
- Physical (Node) and Electronic (Link) Stability

Theoretical Baseline



"Labeled Graph" G
<N,E,M,I>

N = {N₁, N₂, N₃, N₄, N₅
E = {E₁, E₂, E₃, E₄, E₅, E₆, E₇, E₈}

E	1	2	3	4	5	6	7	8
M (I)	(1,2)	(1,2)	(1,3)	(2,3)	(2,4)	(2,5)	(3,5)	(4,5)

E	1	2	3	4	5	6	7	8
I (E)	A	B	C	D	E	F	G	H

CUTSET:
THE MINIMUM NUMBER OF NODES AND ASSOCIATED LINKS WHICH MUST BE REMOVED FROM A GRAPH TO MAKE IT A DISCONNECTED GRAPH

{N₂, N₃}, {N₂, N₅}

SPANNING TREE:
A SET OF LINKS OF A GRAPH THAT CONNECTS ALL THE NODES TOGETHER WITHOUT FORMING A CLOSED PATH

{E₂, E₄, E₇, E₈}

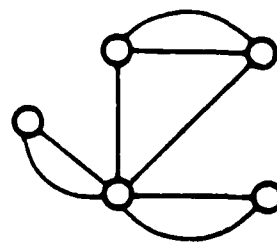
Node Connectivity Factor

$$NCF = \sum_{i=1}^{N_T} N_i \cdot P(N_i)$$

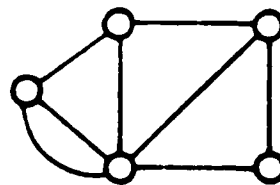
WHERE N_i = NUMBER OF CRITICAL NODES REMOVED IN i^{TH} DECOMPOSITION PATH

$P(N_i)$ = LIKELIHOOD OF THE i^{TH} DECOMPOSITION PATH OCCURRING

N_T = TOTAL PATHS IN DECOMPOSITION DIAGRAM

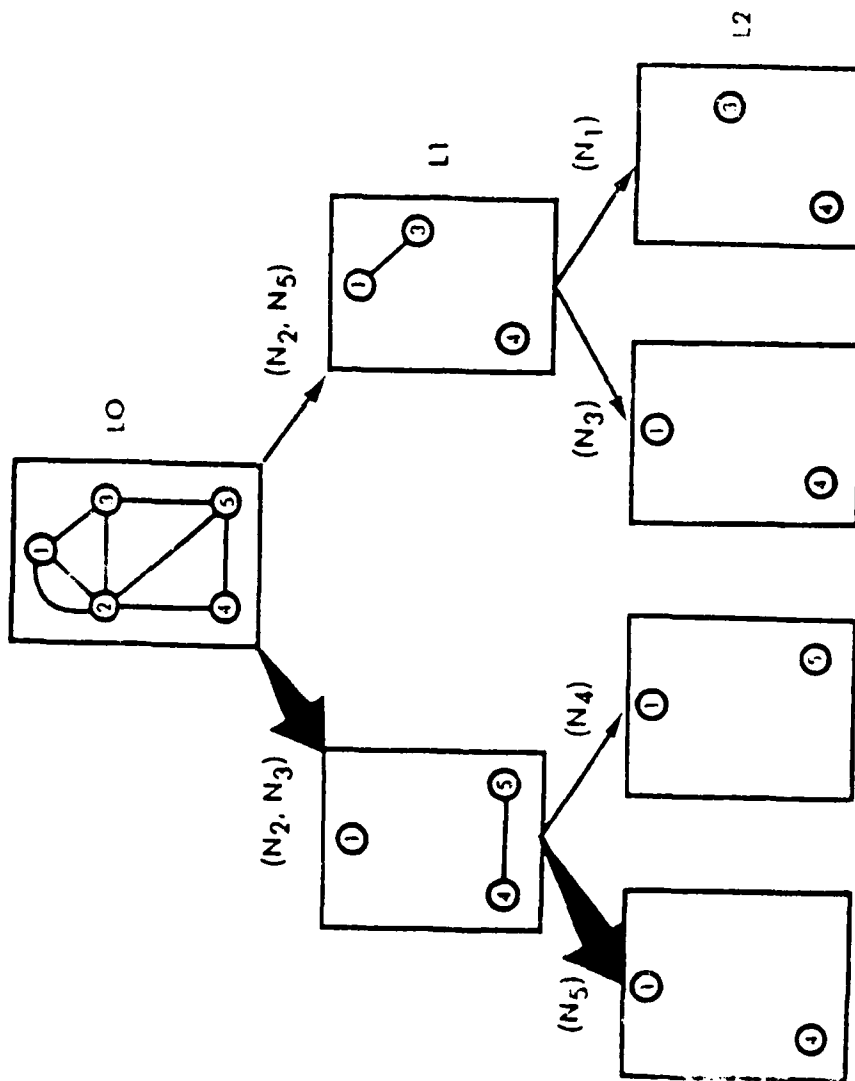


NCF = 2.00



NCF = 3.00

NCF Computation Example



$$NCF = 3(0.25) + 3(0.25) + 3(0.25) + 3(0.25) = 3.00$$

Link Connectivity Factor

$$LCF = \sum_{I=1}^N \frac{T_I * (N_I - 1) * S_I}{E_I * S}$$

WHERE T_I = TOTAL NUMBER OF SPANNING TREES IN COMPONENT I

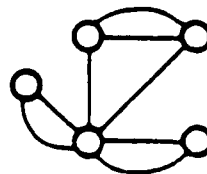
S_I = NUMBER OF LINKS IN MINIMUM SPANNING TREE FOR COMPONENT I

S = NUMBER OF LINKS IN MINIMUM SPANNING TREE FOR GRAPH

E_I = TOTAL EDGES IN COMPONENT I

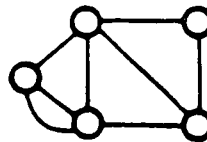
N_I = TOTAL NODES IN COMPONENT I

N = TOTAL COMPONENTS IN GRAPH



SPANNING TREES = 20

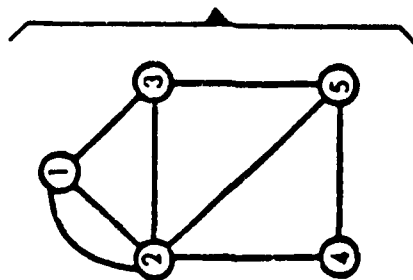
LCF = 10.00



SPANNING TREES = 34

LCF = 17.00

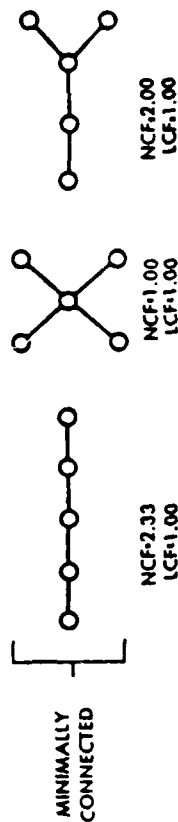
LCF Computation Example



$$T_1 = 34 \quad N_1 = 5 \quad E_1 = 8 \quad S_1 = 4 \quad S = 4$$

$$LCF = \frac{T_1 \cdot (N_1 - 1) \cdot S_1}{S \cdot E} = \frac{34(4)(4)}{4(8)} = 17.00$$

Design Implications



CASE	GRAPH CONFIGURATION	# LINKS	# TREES	NCF	LCF
C1	O-O-O-O-O	4	2	2.33	1.40
C2	O-O-O-O-O	6	3	2.33	2.00
C3	O-O-O-O-O	7	4	2.33	2.39
C4	O-O-O-O-O	8	5	2.33	2.50

CONCENTRATED LINKS

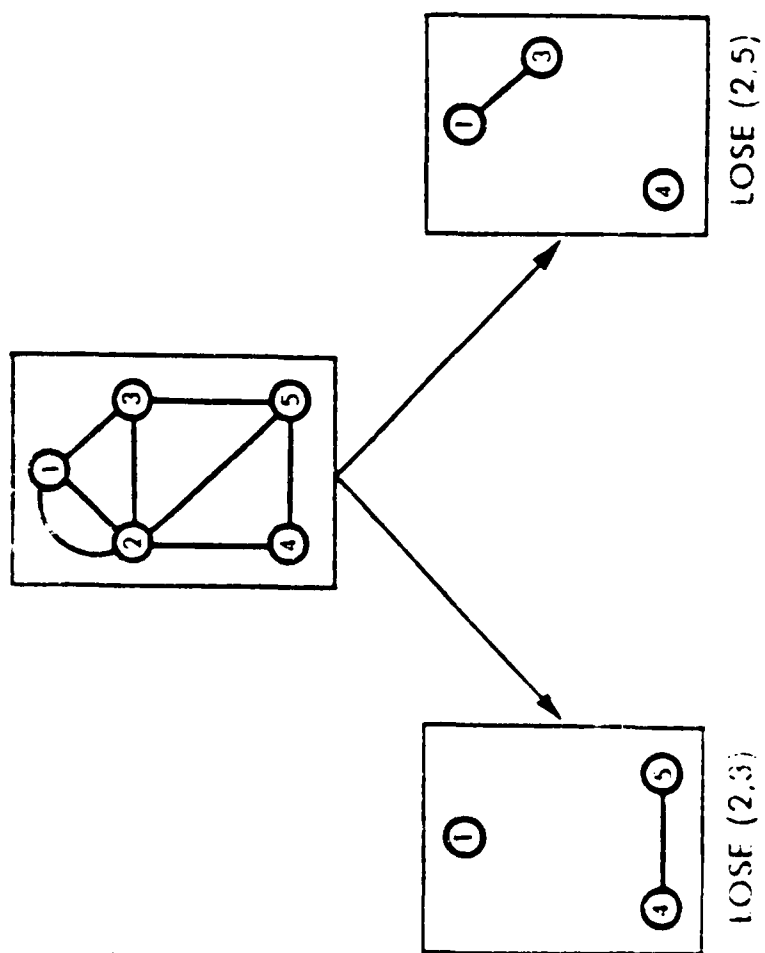
D1	O-O-O-O-O	6	4	2.33	2.67
D2	O-O-O-O-O	7	6	2.33	4.37
D3	O-O-O-O-O	8	16	2.33	8.00

DISTRIBUTED LINKS

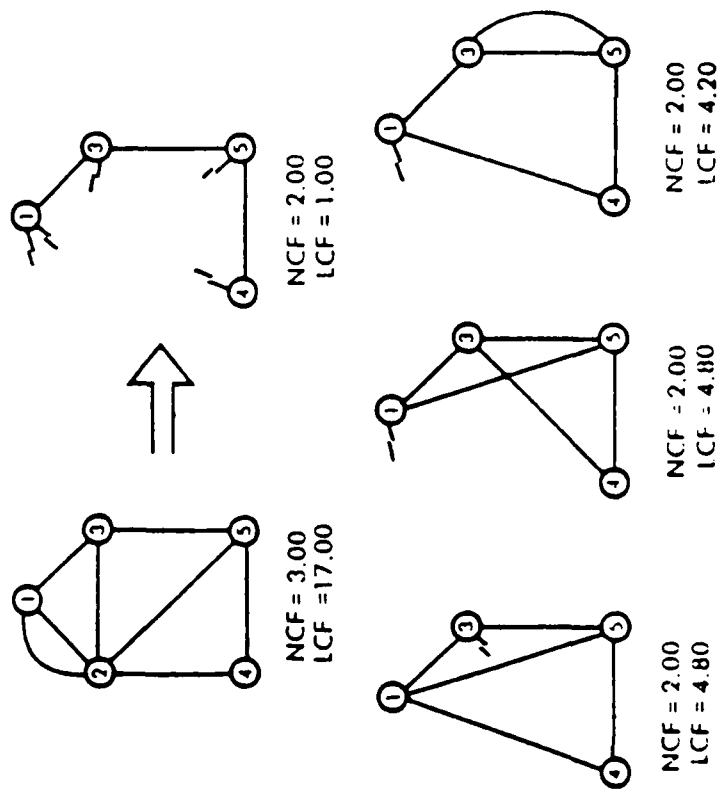
B1	O-O-O-O-O	5	3	3.00	2.40
B2	O-O-O-O-O	5	3	2.00	2.40
B3	O-O-O-O-O	6	9	3.00	6.00
B4	O-O-O-O-O	7	21	3.00	12.00
B5	O-O-O-O-O	8	4	2.00	3.20
B6	O-O-O-O-O	6	12	2.00	8.00
B7	O-O-O-O-O	5	3	3.00	4.00
B8	O-O-O-O-O	6	11	3.00	7.33

BRIDGING LINKS

Real-Time Monitoring



Action State Reconfiguration



Summary And Conclusions

- NETWORK CONNECTIVITY QUANTIFIED

$$NCF = \sum_{I=1}^{N_T} N_I \cdot P(N_I)$$

$$LCF = \sum_{I=1}^N \frac{T_I \cdot (N_I - 1) \cdot S_I}{E_I \cdot S}$$

- NETWORK DESIGN TOOL
- REAL-TIME DEGRADATION MONITORING
- PRE-DECOMPOSITION RECONFIGURATION

PARALLEL PROCESSING
and
OPTIMIZATION

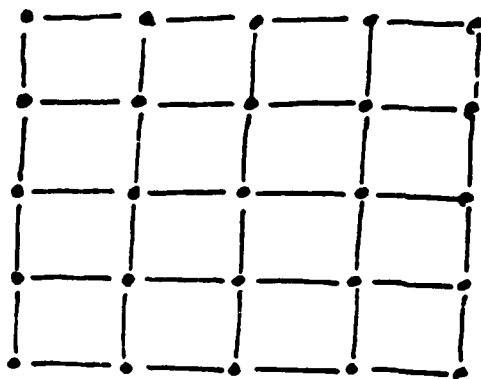
Lt. John Colombi	}	DCPL
John Salerno		RADC

Dick Barr	}	OR Dept
Dick Helgason		SMU
Jeff Kennington		

PARALLEL PROCESSING

Minimal Spanning Tree

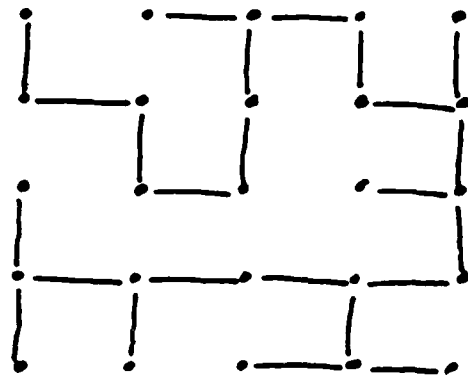
Given : Graph



Given : Edge Costs

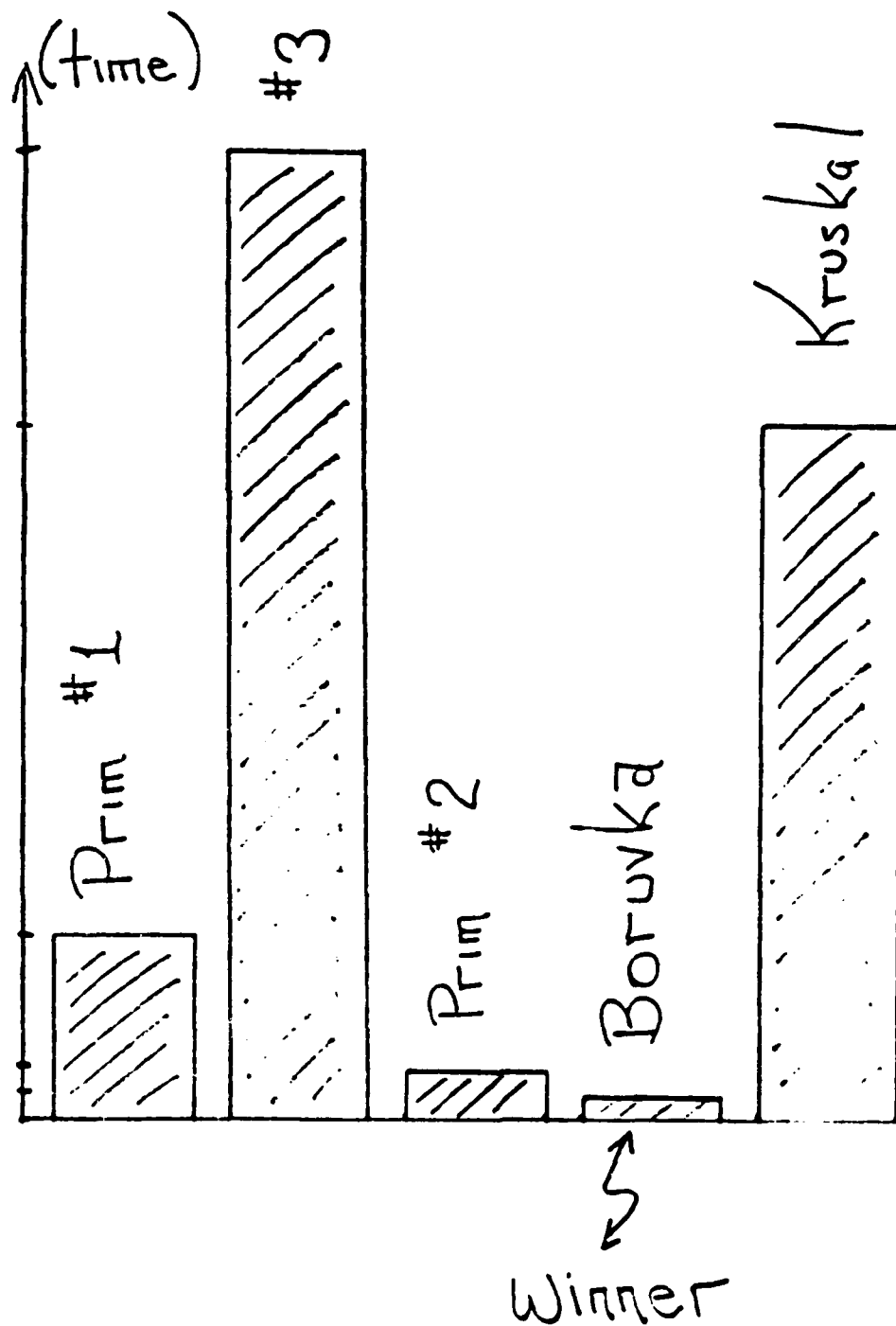
Find : Tree With Minimum
Total Cost

Answer



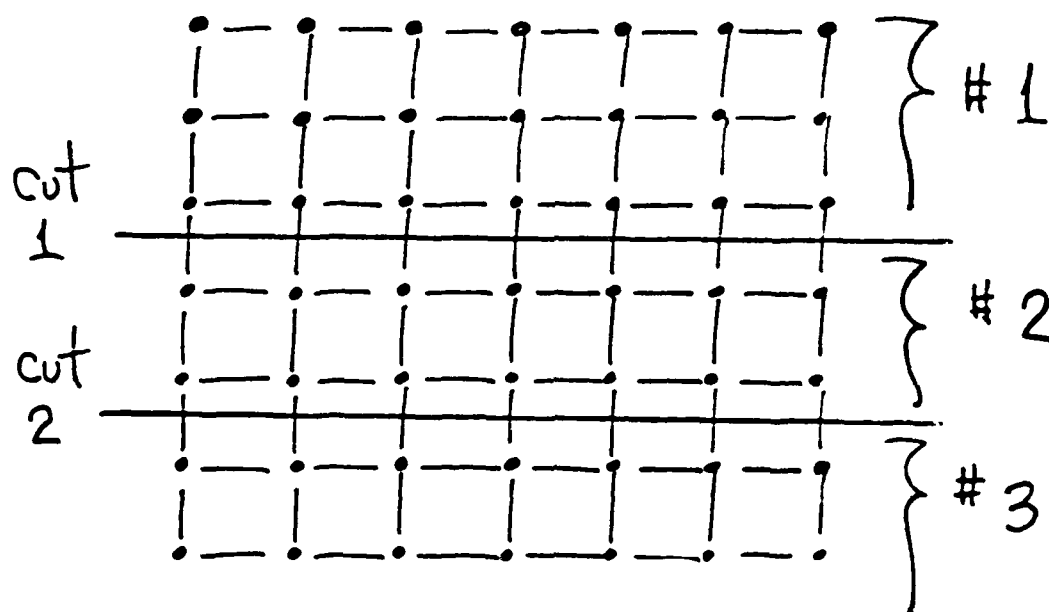
Total Cost Is Sum Of
All Edge Costs

SEQUENTIAL ALGORITHMS



DATA PARTITIONING

Partitions



Parallel Boruvka

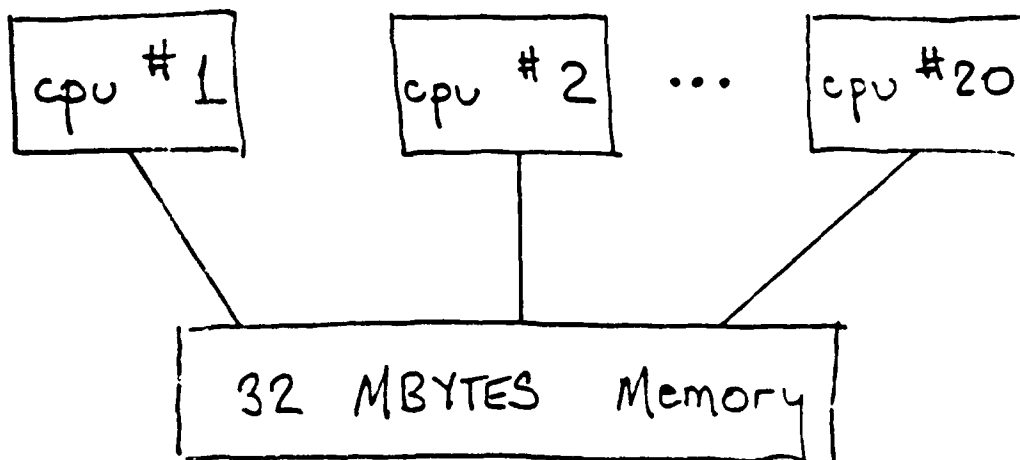
1. Use 3 cpu's to work on each partition.
2. Use 2 cpu's to work on cuts.

PARALLEL COMPUTER

Sequent Computer Systems, Inc.

Balance 21000

Shared Memory (MIMD)



NS32032

UNIX

FORTRAN

C, PASCAL

COST

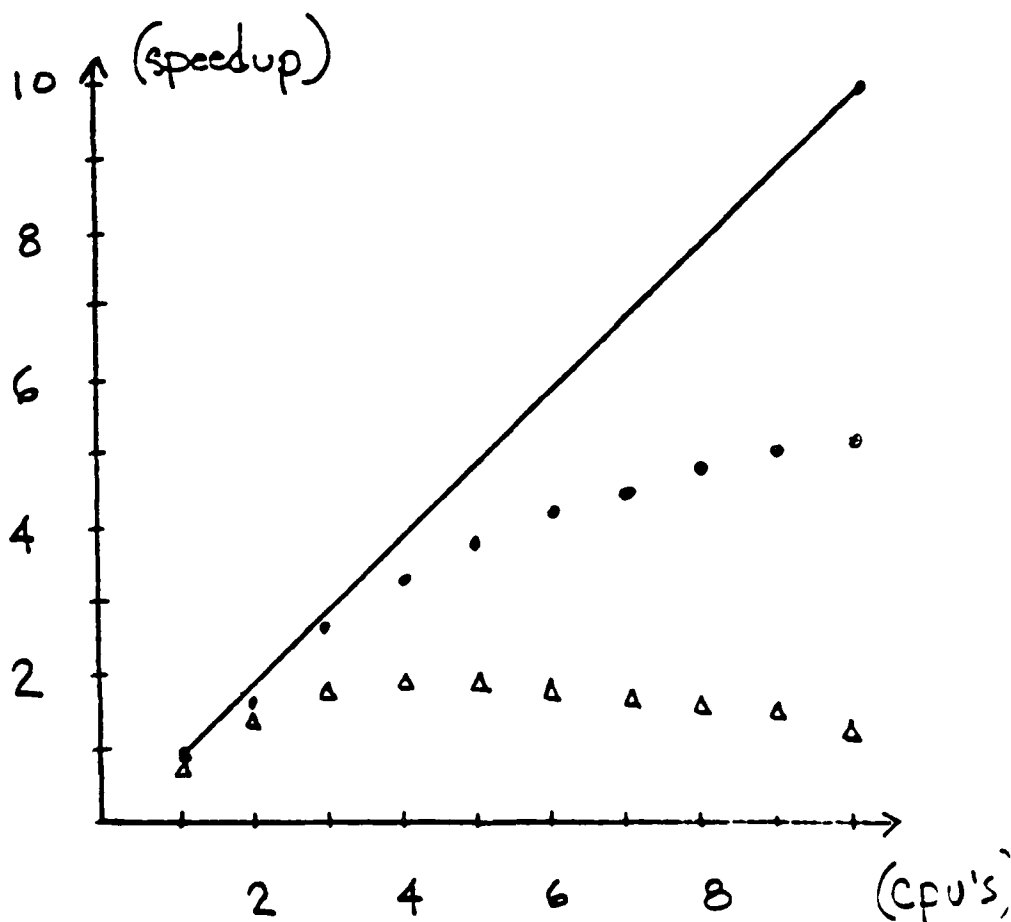
\$ 200 K - 500 K

Parallel Boruvka

200 x 200 grid

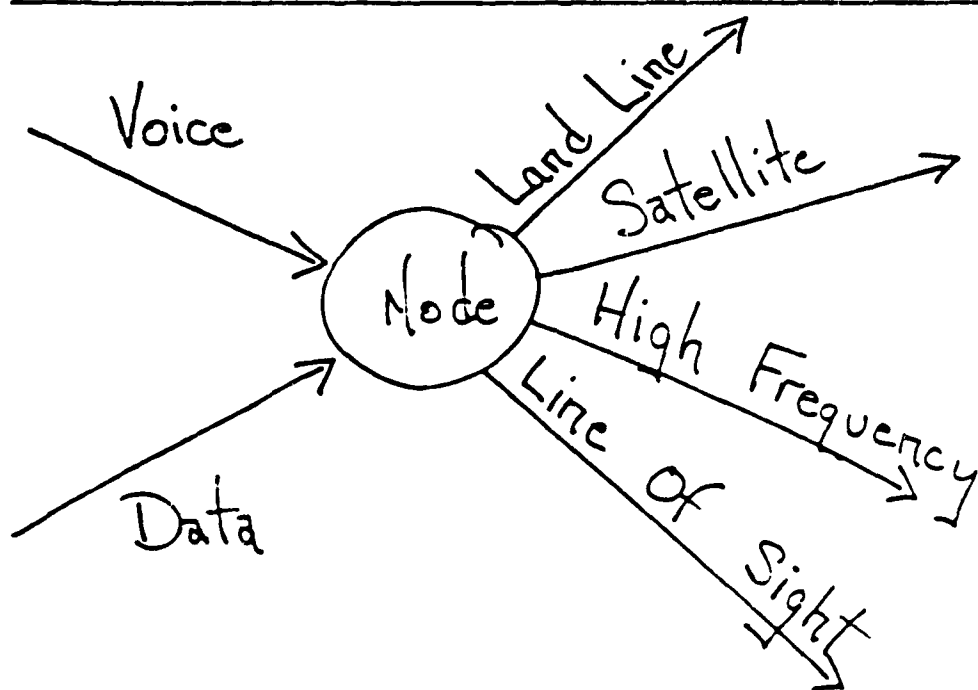
• - excludes process creation

Δ - includes all overhead



OPTIMAL TRUNK ASSIGNMENT

MODEL



Problem

As requests arrive at a node, assign them to a trunk in an "optimal" manner.

THE MODEL

Subscript

i - denotes a trunk

Constants

$\bar{d}$ - max allowable delay of
requested service
(micro-secs)

$\bar{c}$ - required capacity of
service
(K bits/sec)

d_i - delay of i th trunk
(micro-secs.)

c_i - capacity of i th trunk
(K bits/sec)

a_i - availability of i th trunk
(%)

u_i - current usage of i th trunk
(K bits/sec)

v_i - unit cost for i th trunk
\$/ (K bits/sec)

Decision Variables

$x_i = 1$ if the service is
assigned to trunk i
and 0, otherwise.

CONSTRAINTS

(Trunk Capacity)

$$\bar{c} x_i \leq c_i a_i - u_i \quad ; \quad (\text{all } i)$$

(Delay)

$$d_i x_i \leq \bar{d} \quad ; \quad (\text{all } i)$$

(Select One)

$$\sum_i x_i = 1$$

(Integrality)

$$x_i = 0, 1 \quad ; \quad (\text{all } i)$$

OBJECTIVE FUNCTION

$$\text{minimize } \sum_i v_i x_i$$

References :

1. Minimal Spanning Trees
Tech Report 87-OR-02
2. Optimal Trunk Assignment
Tech Report 87-OR-01

Jeff Kennington
Operations Research Dept
SMU

Dallas, TX 75275

MULTIMEDIA COMMUNICATIONS

JUNE 30, 1987
1987 COMMUNICATION NETWORK
MANAGEMENT WORKSHOP

DR. HUGO E. DE PEDRO
GTE GOVERNMENT SYSTEMS CORP.
77 "A" STREET, NEEDHAM HEIGHTS, MA

SURVIVABLE SYSTEM CONSIDERATIONS

- **INTEROPERABILITY OF COMMUNICATIONS**
 - TYPE OF SERVICE
 - MESSAGE CHARACTERISTICS
 - PROTOCOL TRANSLATION
 - DEGREE OF TRANSPARENCY
- **SURVIVABILITY**
 - ROBUST TOPOLOGY
 - DISTRIBUTED ADAPTIVE INTERNET CONTROL
 - MOBILE OPERATIONS
 - AUTOMATIC MONITORING
- **INTERNETTING PROTOCOL ISSUES**
 - NETWORK ACCESS
 - ADDRESSING SCHEMES
 - GATEWAY TO GATEWAY CONTROL
 - SEGMENTATION AND REASSEMBLY

SURVIVABLE SYSTEM CONSIDERATIONS (CONT.)

- **ADAPTIVE PROTOCOLS**
 - ROUTING SCHEMES
 - FLOW CONTROL
 - CHANNEL UTILIZATION/ACCESS
 - SECURE TRANSMISSION
- **MULTIMEDIA ARCHITECTURES**
 - TYPE OF SERVICE
 - LEVEL OF PROTOCOL INTERACTION
 - GLOBAL CONTROL
 - PERFORMANCE GOALS
- **NETWORK RECONSTITUTION**
 - INITIALIZATION
 - RECONFIGURATION/PARTITION NETWORK RECOVERY
 - GLOBAL CONTROL AND STATUS EXCHANGE
 - GATEWAY SUPPLIED CONTROL TO LOCAL NETWORK

MULTIMEDIA COMMUNICATIONS

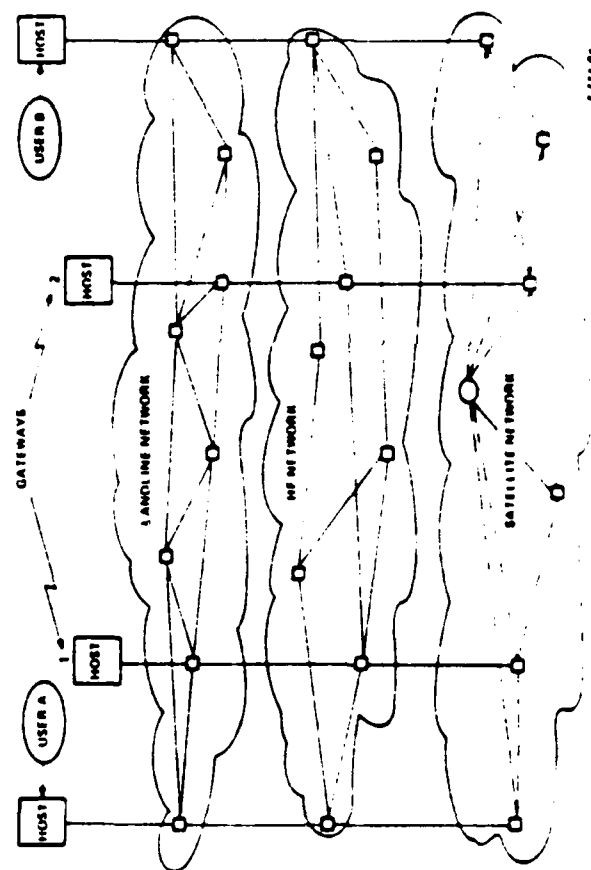
- POST-ATTACK OPERATION OF MULTIPLE PARTITIONED NETWORKS
FUNCTIONING AS AN INTEGRATED MULTIMEDIA NETWORK

- LANDLINES
- SATELLITE
- HF
- METEOR BURST

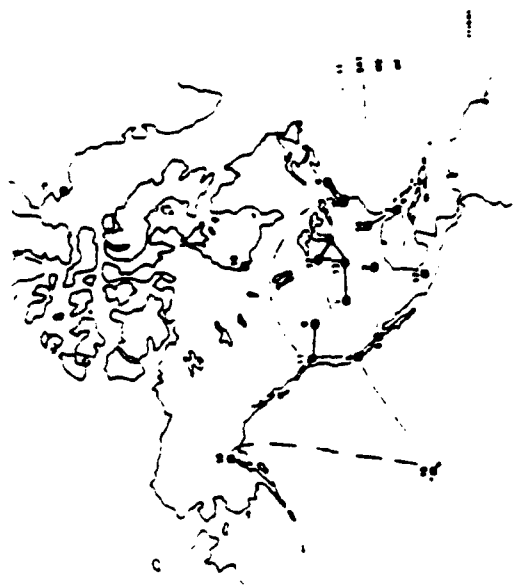
- ISSUES

- MULTIMEDIA NETWORK CONNECTIVITY
- END-TO-END LOWEST NETWORK MESSAGE DELAY
- MULTIMEDIA MESSAGE ROUTING STRATEGIES
- CHANNEL SELECTION ALGORITHMS

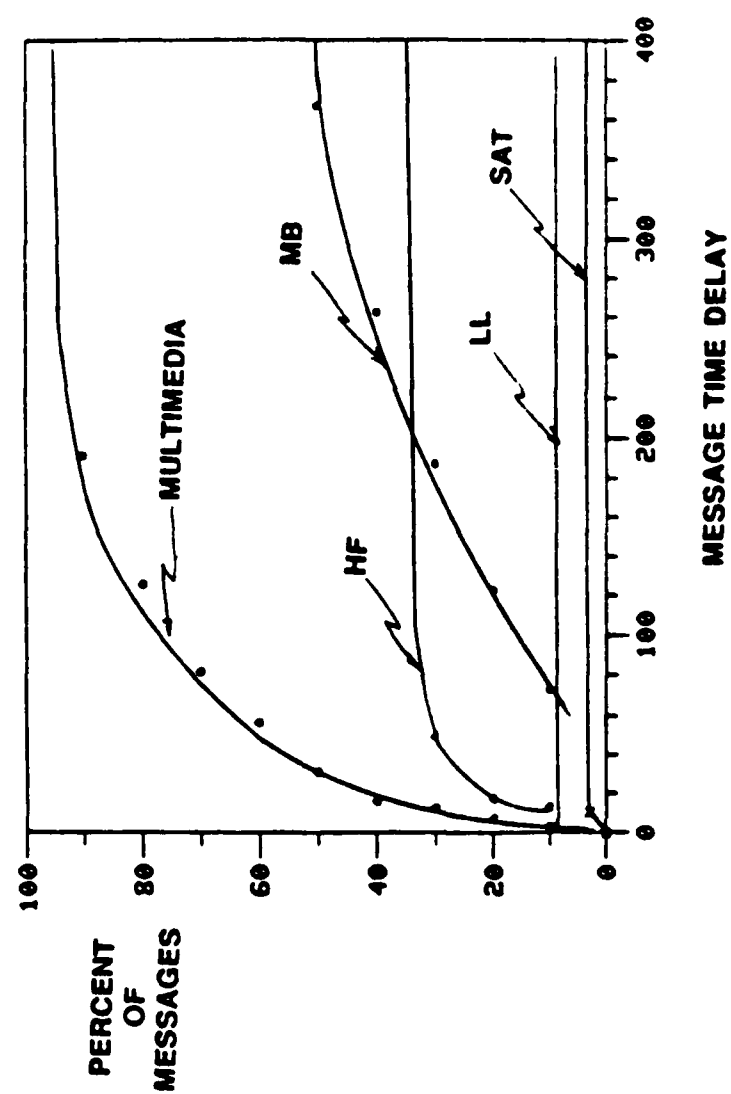
MULTIMEDIA CONFIGURATION



SAMPLE MULTIMEDIA NETWORK



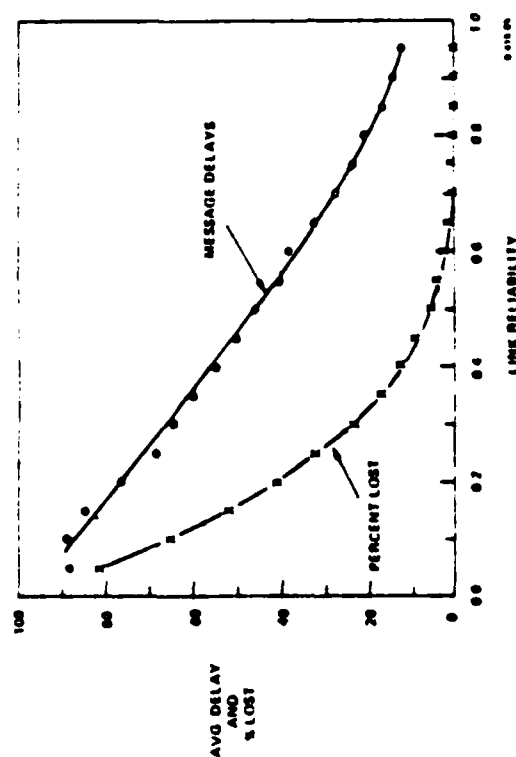
PERFORMANCE OF INDIVIDUAL NETWORK AND MULTIMEDIA NETWORK ARCHITECTURES



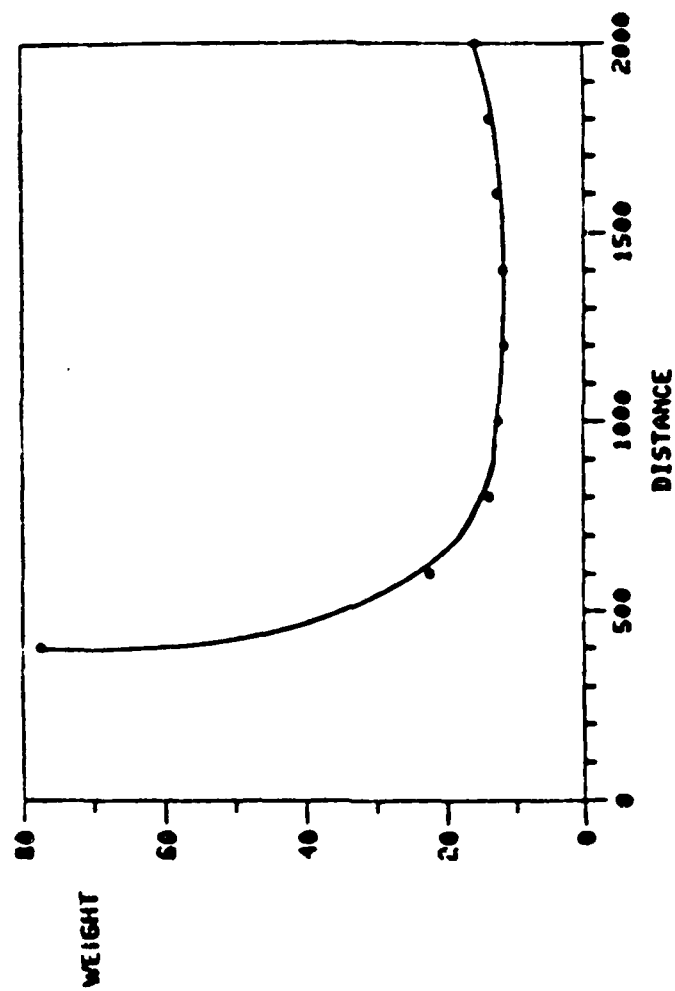
CHANNEL SELECTION ALGORITHM EXAMPLE

- **MINIMUM DELAY SELECTION STRATEGY USING ASSIGNMENT OF WEIGHTS TO INDIVIDUAL MEDIA LINKS**
 - **LANDLINE AND SATELLITE LINKS ARE ASSIGNED FIXED WEIGHTS PROPORTIONAL TO MESSAGE TRANSMISSION DELAYS**
 - **HF LINKS ARE ASSIGNED WEIGHTS BASED ON ESTIMATED LINK RELIABILITY**
 - **MB LINKS ARE ASSIGNED WEIGHTS BASED ON AVERAGE METEOR BURST WAITING TIME**
- **WEIGHT ASSIGNMENTS DEPEND ON DESIRED SYSTEM PERFORMANCE AND SPECIFIC NETWORK PROTOCOLS**

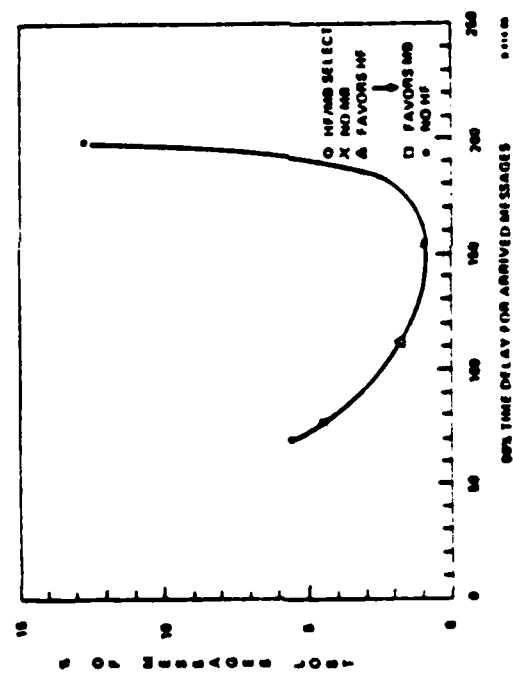
HF PROTOCOL PERFORMANCE **AVERAGE MESSAGE DELAY AND MESSAGES LOST** **AS A FUNCTION OF HF LINK RELIABILITY**



**MIB PROTOCOL PERFORMANCE
WEIGHT ASSIGNMENT AS A FUNCTION OF LINK DISTANCE**



HF VS. MB MEDIA SELECTION WEIGHT TRADE-OFF IN TERMS OF MESSAGE DELAY AND NUMBER OF LOST MESSAGES



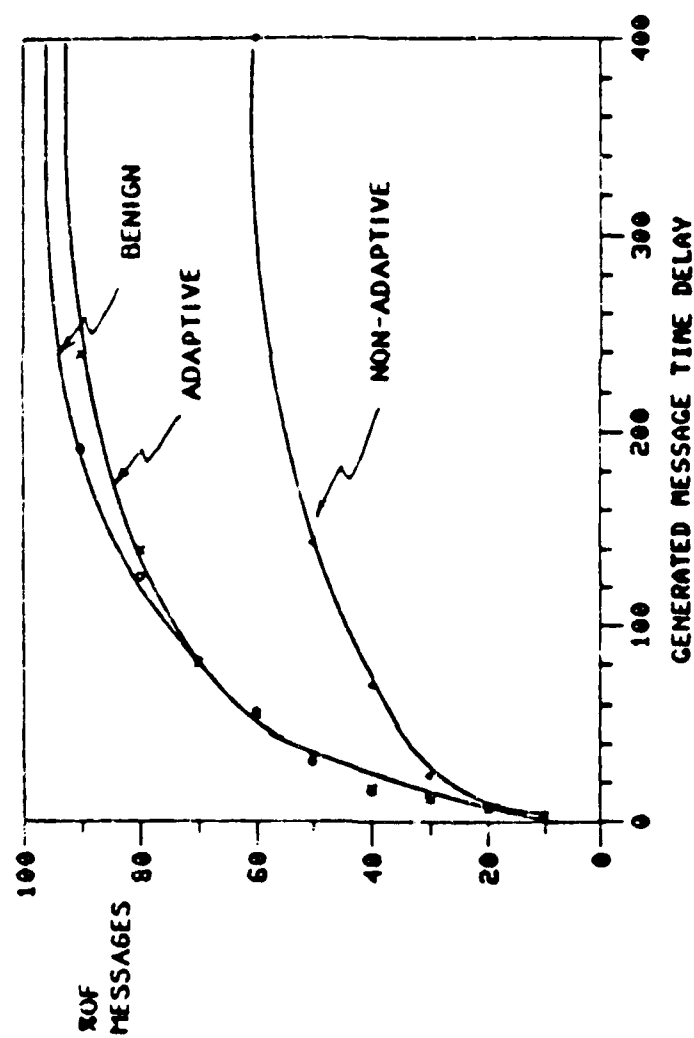
MULTIMEDIA ROUTING ISSUES

- ROUTING UPDATES NOT DISTRIBUTED WITH UNIFORM SPEED
- LOAD SPLITTING AMONG MEDIA MAY CAUSE REASSEMBLY DELAYS AND LOSS OF BUFFER SPACE
- VARIANCE OF DELAYS DIFFERENT FOR DIFFERENT MEDIA
- DIVERSION OF TRAFFIC TO RADIO LINKS WILL INCREASE COLLISION INTERFERENCE
- INTERNET ROUTING
 - ALL PROBLEMS ABOVE
 - DISTINGUISH BETWEEN PARTITIONS AND GATEWAY FAILURES

HF NETWORKING

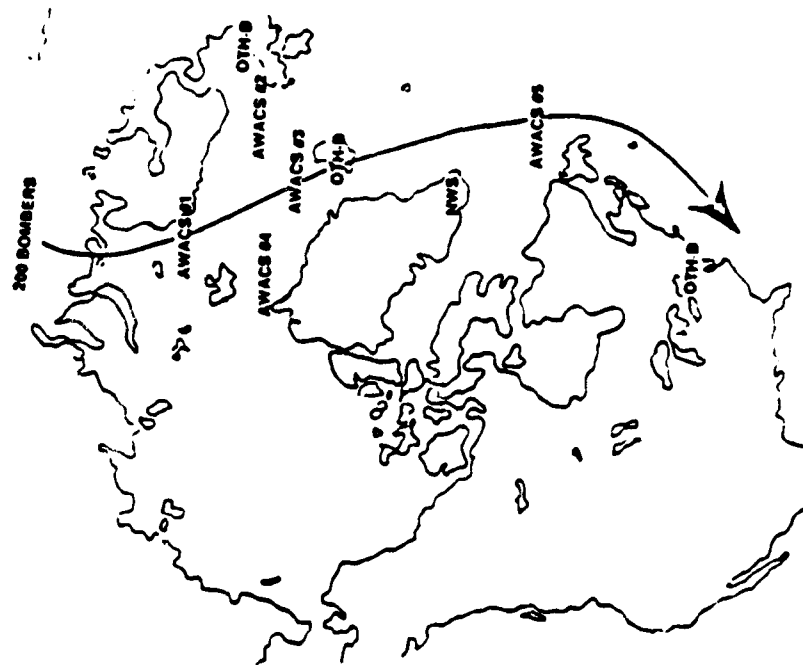
- BACKBONE HF
 - MULTIPLY CONNECTED
 - HIGHLY RELIABLE LINKS
 - OTHER NODES CONNECT INTO THE BACKBONE
 - 6-9 NODES IN THE BACKBONE
- NUMBER OF FREQUENCIES
 - AS LOW AS THREE IN BENIGN ENVIRONMENTS
- CHANNEL SELECTION
 - COORDINATION NOT REQUIRED
- ROUTING
 - CONNECTIVITY TO A SECOND LEVEL
- JAMMING
 - FAR AWAY JAMMERS VIA SKYWAVE
 - ONLY SOME FREQUENCIES PROPAGATE
 - JAMMER SHOULD DISTRIBUTE POWER ACROSS THE BAND
 - ADAPTIVE HF ENHANCES CONNECTIVITY, REDUCES DELAY

MULTIMEDIA NETWORK IN HF ECM ENVIRONMENT ONE FREQUENCY JAMMED



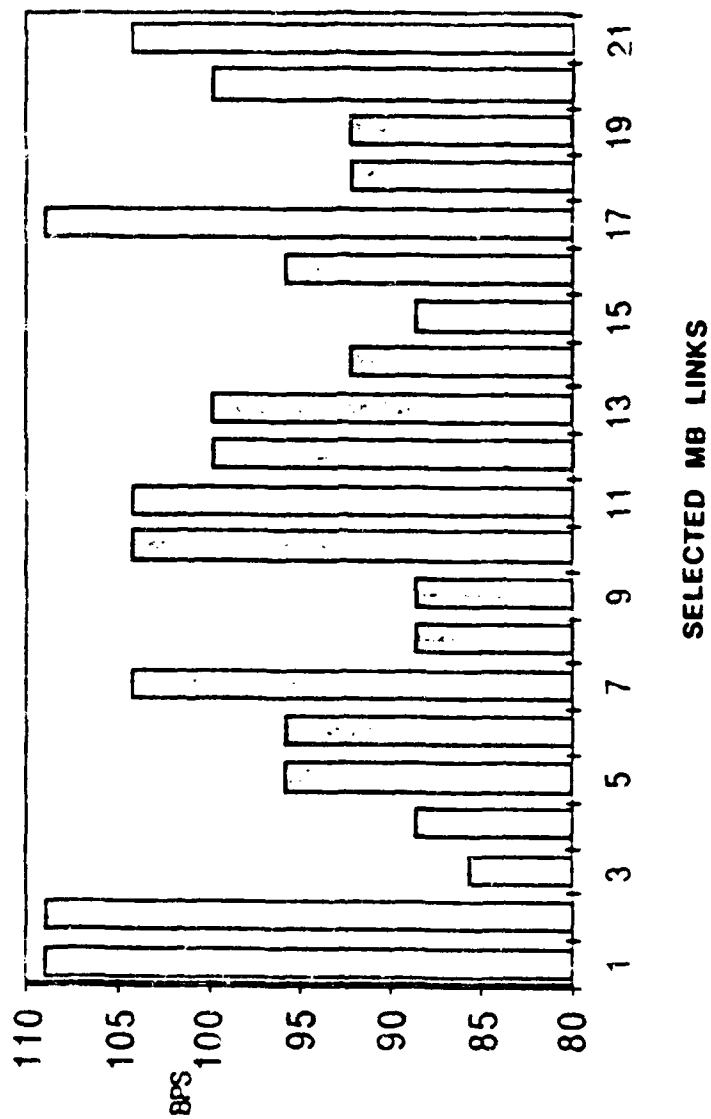
ADI APPLICATION EXAMPLE

- ENGAGEMENT SCENARIO
 - BOMBER ATTACK, CRUISE MISSILE CARRIERS
 - SURVEILLANCE ELEMENTS
 - AWACS
 - OTH-B
 - NWS
 - C2 ELEMENTS
 - ROCCS
 - GEPS
 - CMC
 - COMMUNICATIONS
 - HF
 - MB
 - UHF LOS
 - LL

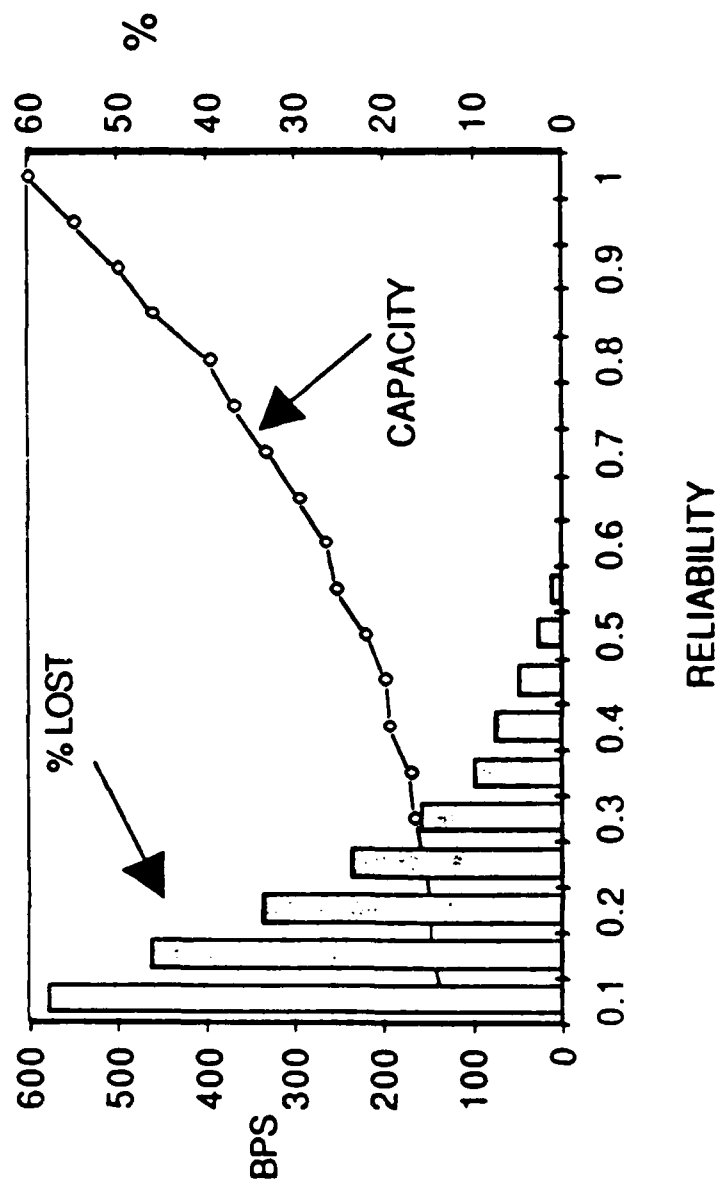


[illegible]

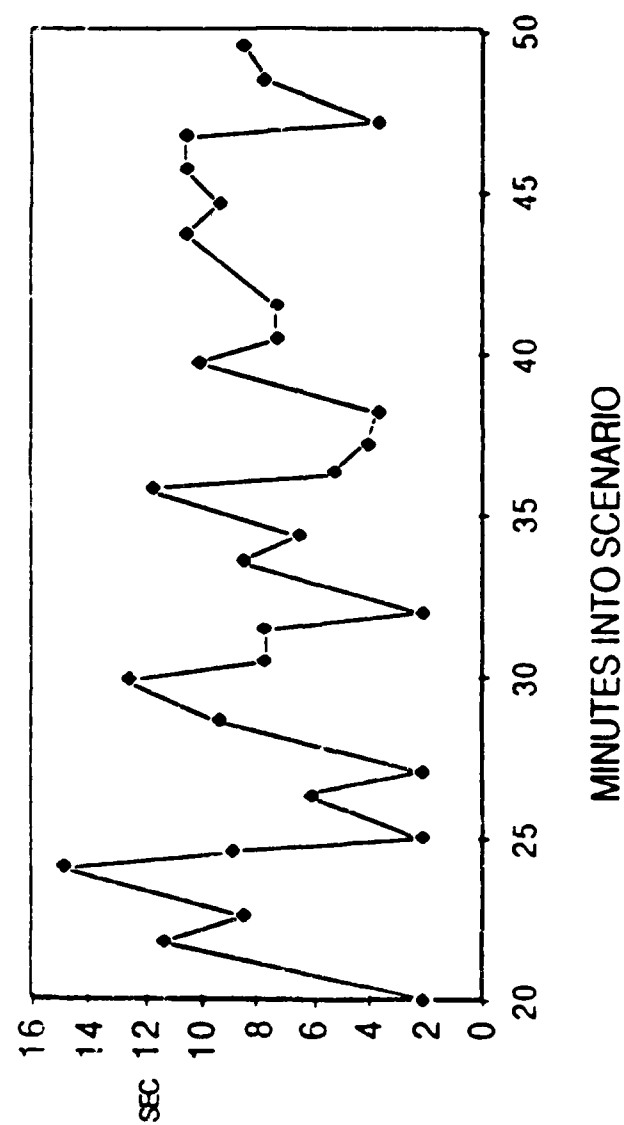
MB PROTOCOL PERFORMANCE



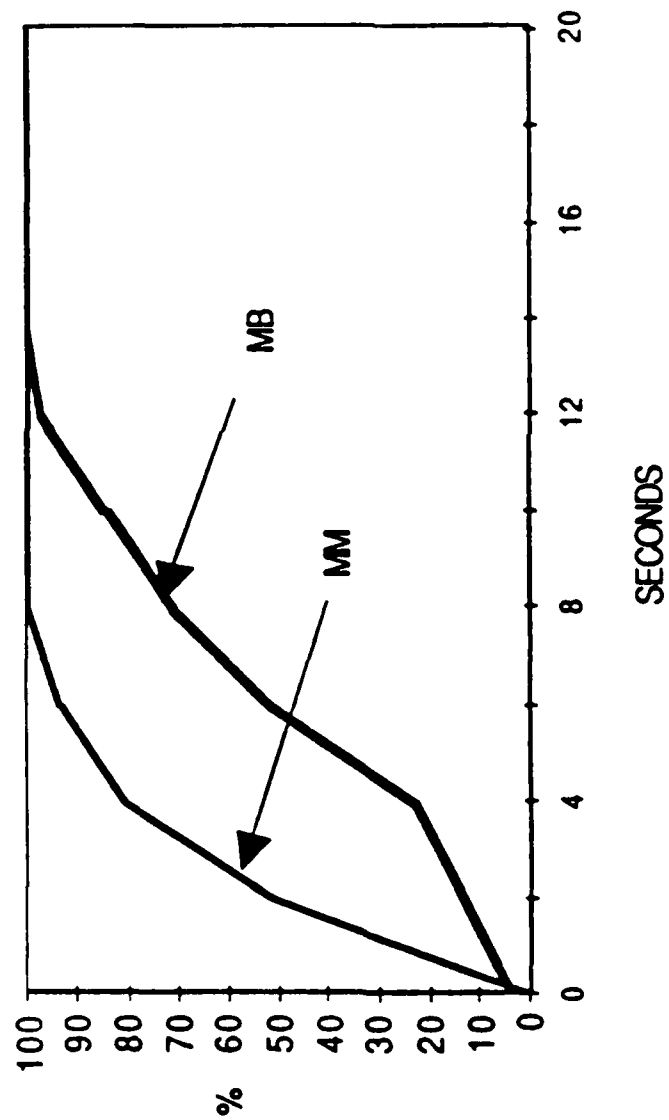
HF PROTOCOL PERFORMANCE



STATUS FUNCTION AWACS-AWACS



**DELAY DISTRIBUTION
STATUS FUNCTION AWACS-AWACS**

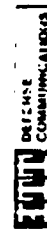


CONCLUSIONS- MULTIMEDIA NETWORKS

- **A MULTIMEDIA NETWORK CONFIGURATION PROVIDES SIGNIFICANTLY ENHANCED CONNECTIVITY OVER INDIVIDUAL MEDIA NETWORK CONFIGURATIONS**
- **ALL REMAINING COMMUNICATION ASSETS SHOULD BE USED, EVEN THOSE PROVIDING VERY SPARSE CONNECTIVITY**
- **THERE EXISTS A TRADE-OFF IN THE SELECTION OF HF AND MB LINKS IN THE NETWORK THAT DEPENDS ON THE PARTICULAR SYSTEM REQUIREMENTS AND ON THE NETWORK PROTOCOLS USED**
- **ADAPTIVE TECHNIQUES GREATLY ENHANCE NETWORK OPERATION IN ECM ENVIRONMENTS**

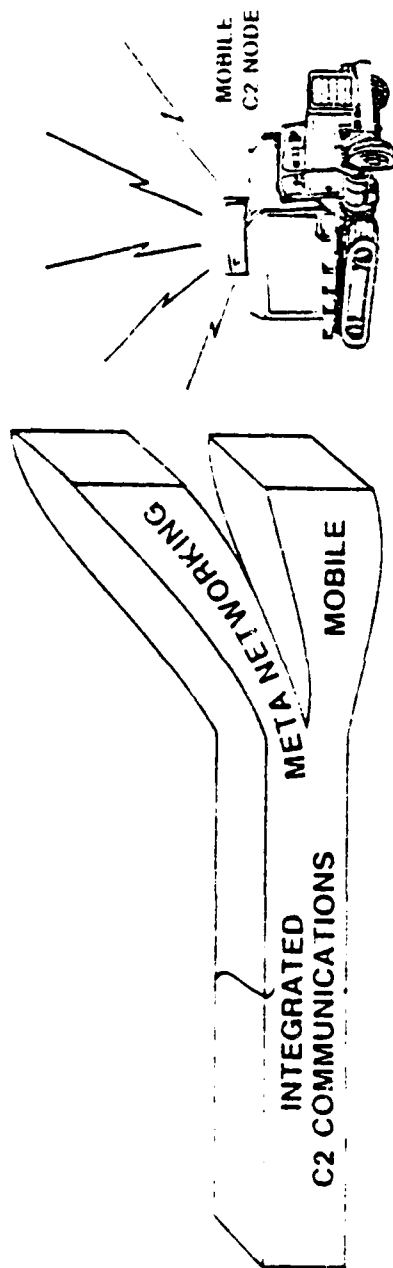
MULTI MEDIA META NETWORKS

**P. STEENSMA
ITT DEFENSE COMMUNICATIONS
NUTLEY, NEW JERSEY**



A(0) 01

History and Evolution



COMMUNICATION INTEGRATION

FUNCTIONALITY

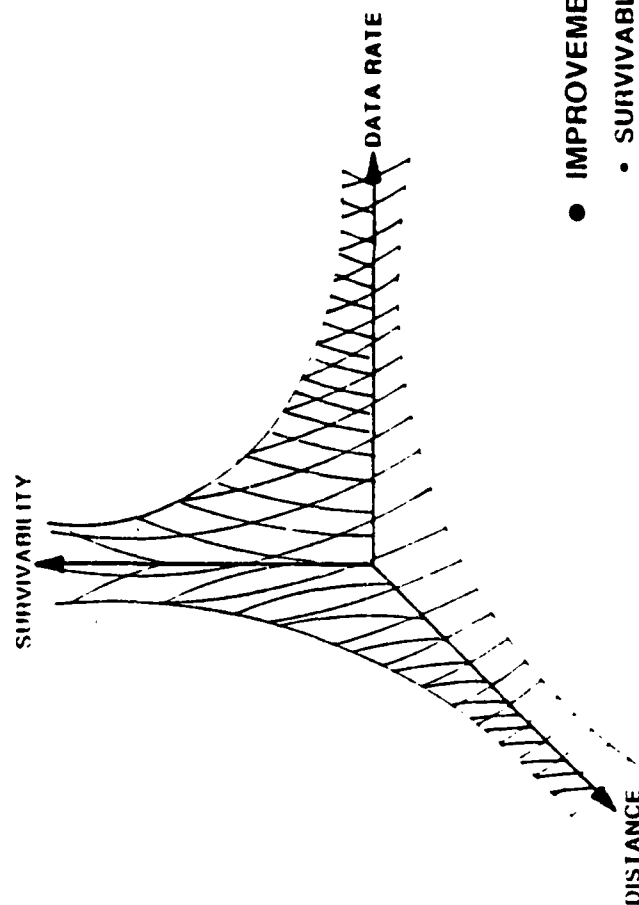
- EAM RECEIPT
- C2 TRAFFIC
- MULTI-LEVEL SECURE (TCB)
- SURVIVABLE MEDIA (HF) DOD NETS (LAND)
- 16 BIT PROCESSOR
- RAD HARD/EMP/TEMPEST
- HOT STANDBY
- CAMP INTEGRATION
- HI CAPACITY C2 TRAFFIC
- MULTI-PROCESSOR TCB
- NEW MEDIA
- MULTIPLE NETS
- 32 BIT CO PROCESSOR
- INCREASED RAD HARDNESS
- FAULT TOLERANT PROCESSING
- DISTRIBUTED NETWORKING ALGORITHMS
- RESOURCE ALLOCATION
- INTEGRATED MODEM/COMSEC
- INTEGRATED RADIO
- INTEGRATED COMSEC

SECURITY

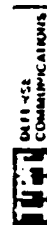
INTERFACES

HARDWARE

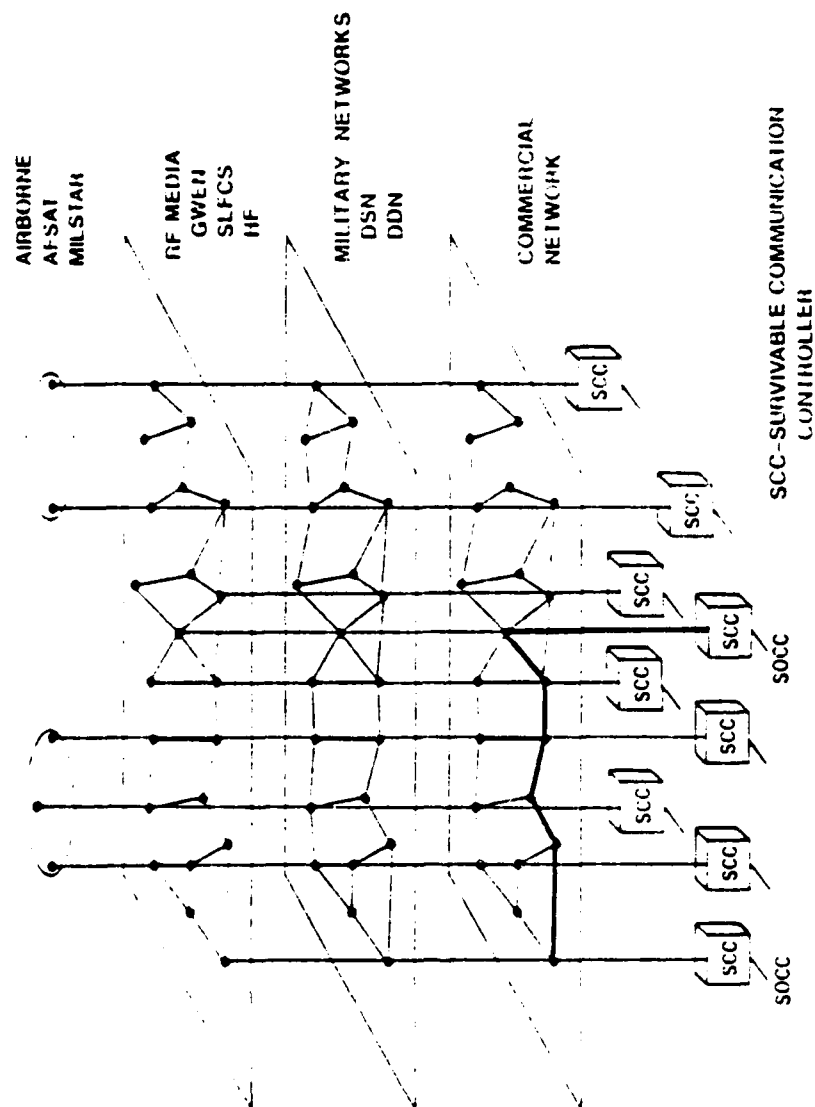
Single Link Survivability Problem



- IMPROVEMENT TECHNIQUES
 - SURVIVABLE SATELLITES
 - PROLIFERATION OF RELAYS
 - MULTIDIMENSIONAL CONNECTIVITY

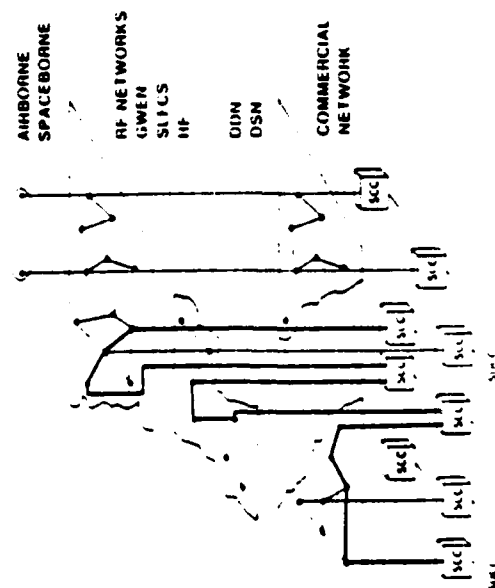


Multiple Media Meta Network

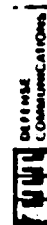
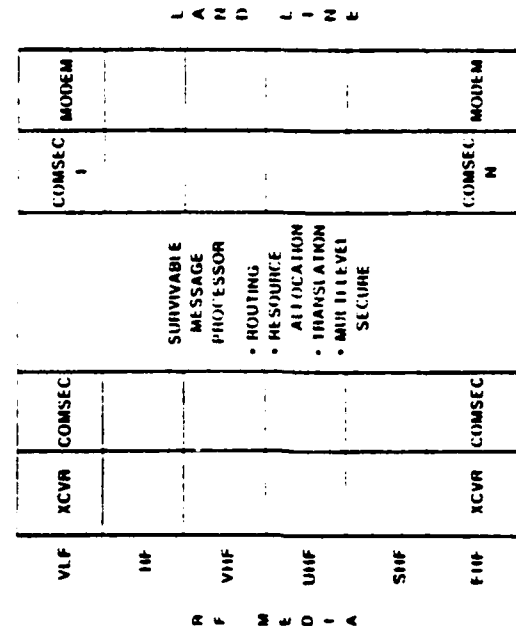


Multiple Media META Network Concept

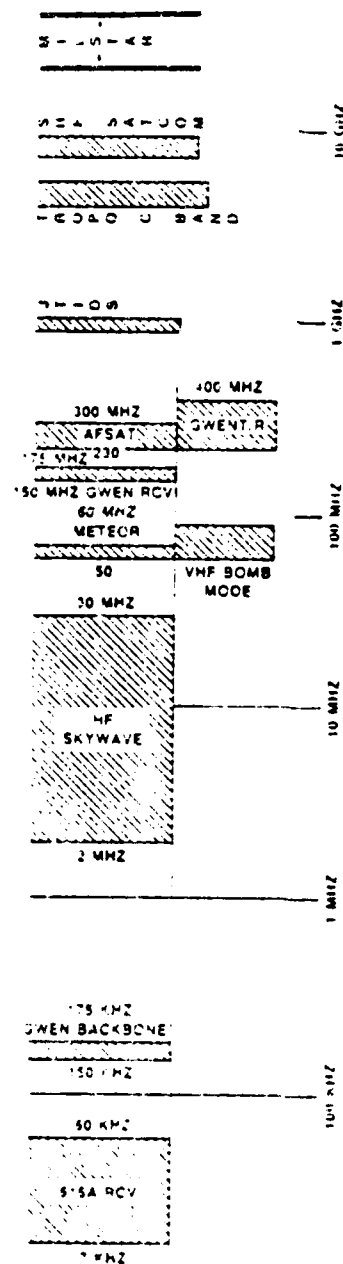
FRACTURED NETWORK ROUTING



SURVIVABLE COMMUNICATION CONTROLLER



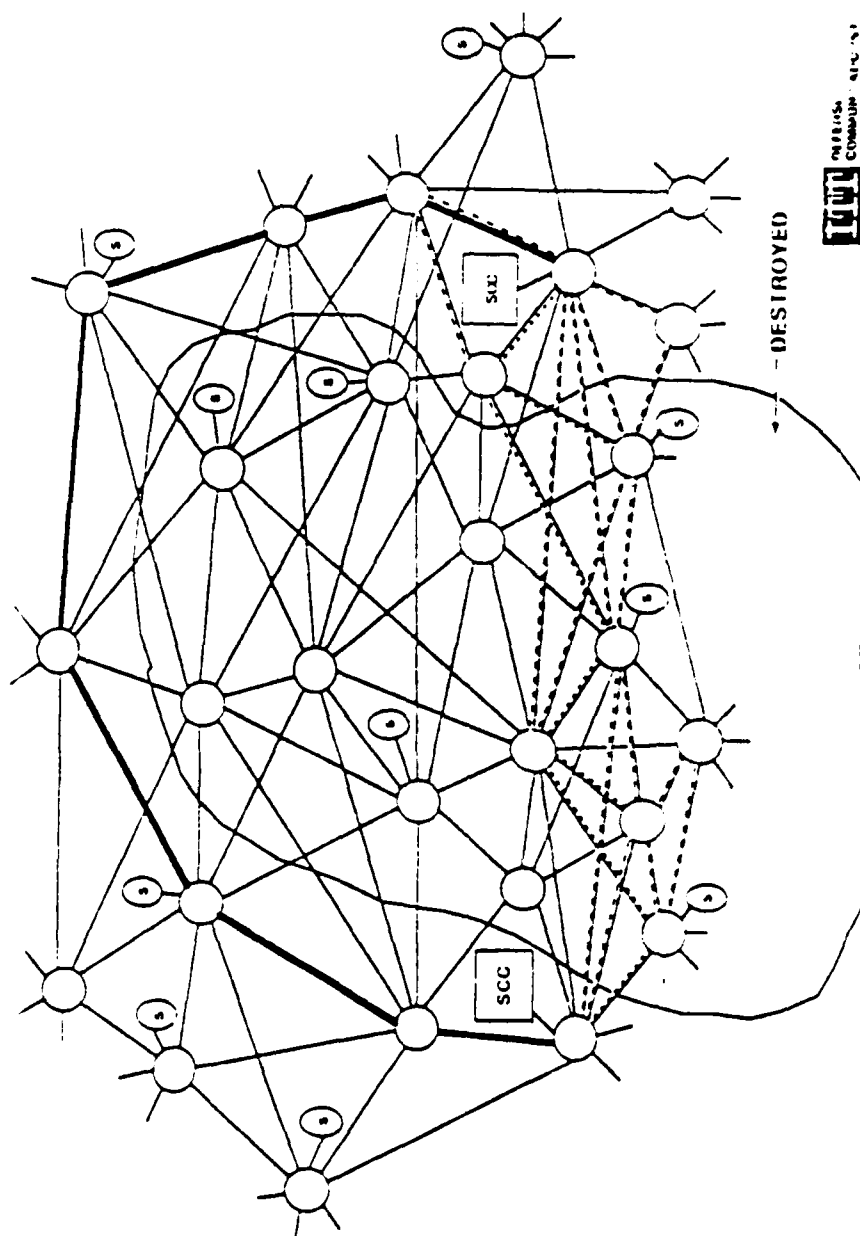
A Broad Spectrum of Connectivity



INT
OFFICE
COMMUNICATIONS

144

Connectivity Restoral Using DACS in Telephone Network

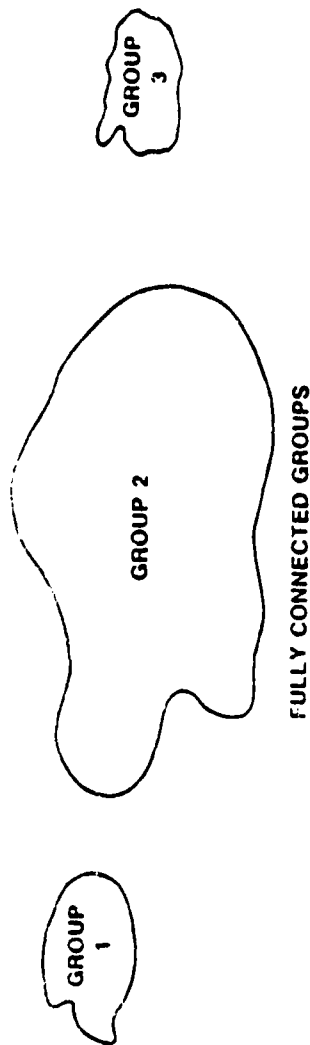


14-00000
OFFICE
COMMUNICATIONS
SECTION

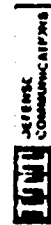
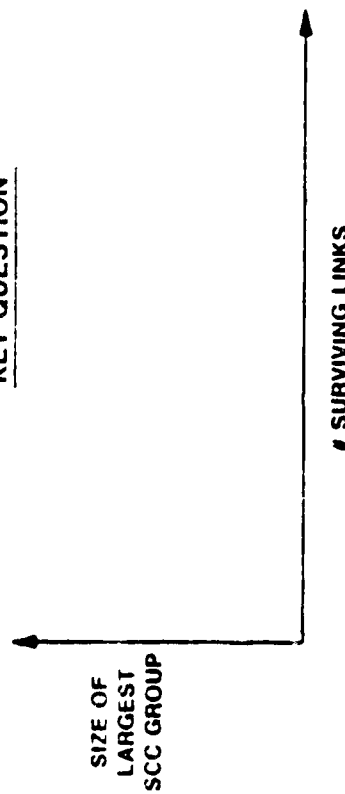
AUG 05

Connectivity Survival Study

RECONSTRUCTED NETWORK



KEY QUESTION



Study Approach

METHODOLOGY

- CONNECTIVITY SIMULATION
- MATHEMATICAL/GRAPH THEORY STUDY

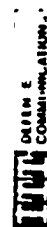
LINK MODES

CHARACTERISTICS

- RANDOMLY PLACED DIRECT CONNECT
- MULTI-HOP
 - FAILURE α (DISTANCE)²
- 2 HOP
 - FAILURE α (DISTANCE)
- SINGLE HOP
 - RANDOM FAILURE

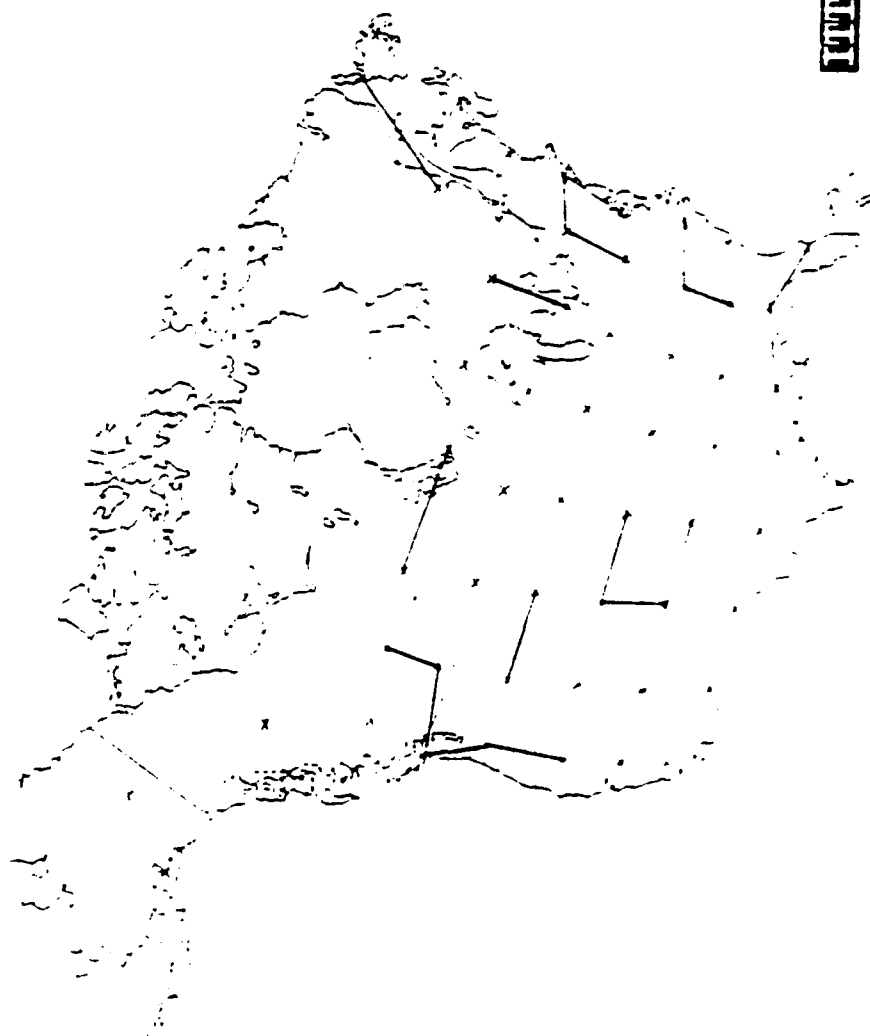
EXAMPLE

- SATELLITE
- HF
- TROPO
- LOS



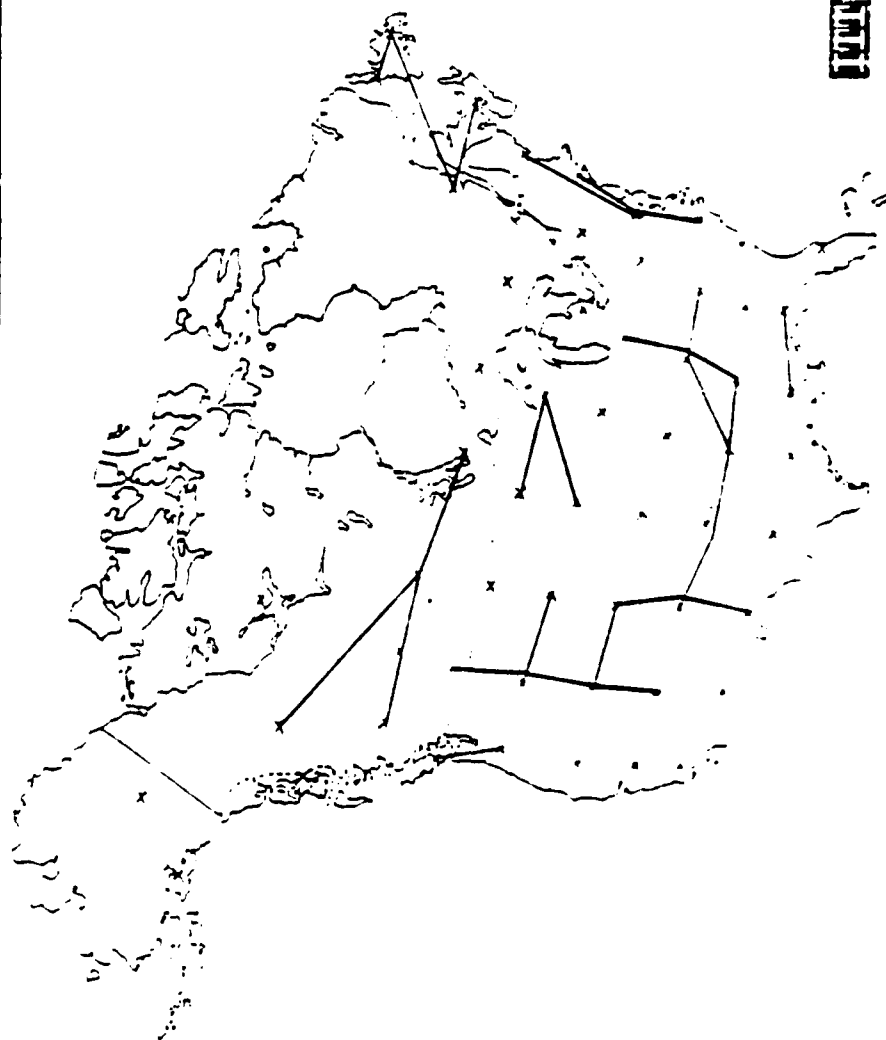
AD1-07

Single Hop Survival



AD108

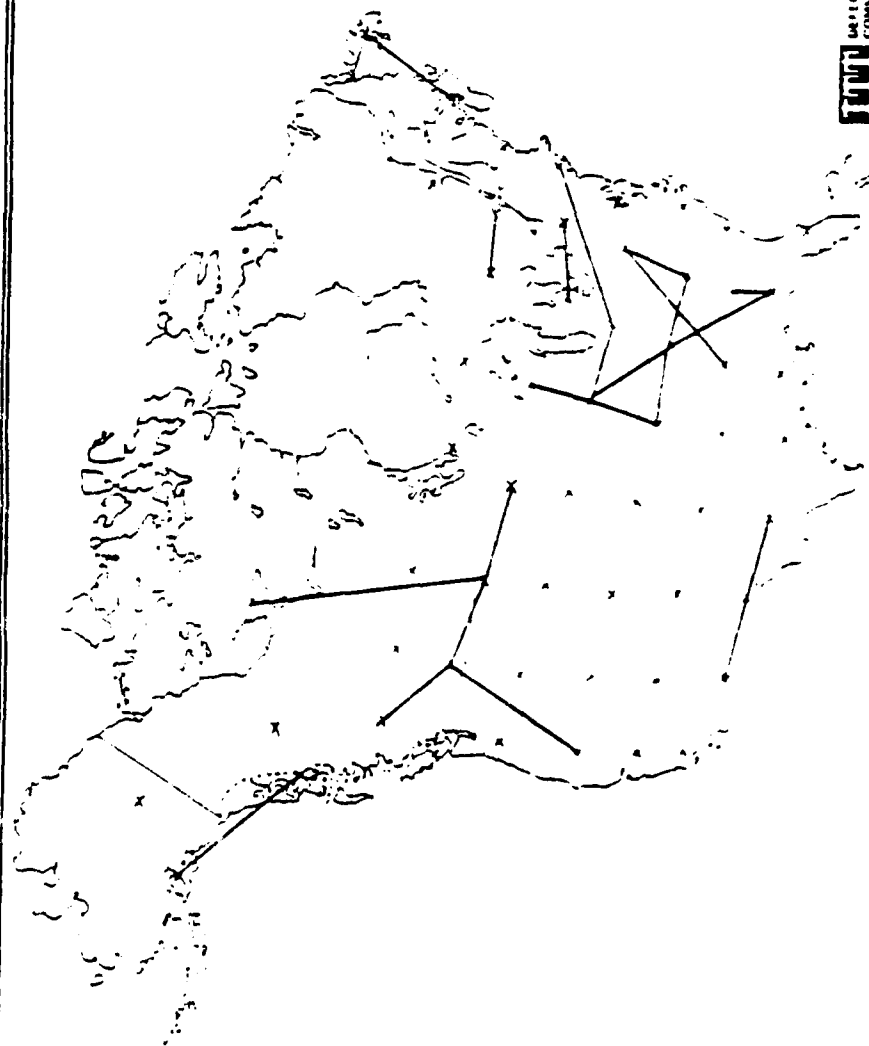
2 Hop Links - Failure α Distance



DE L'INFORMATION

ALM 009

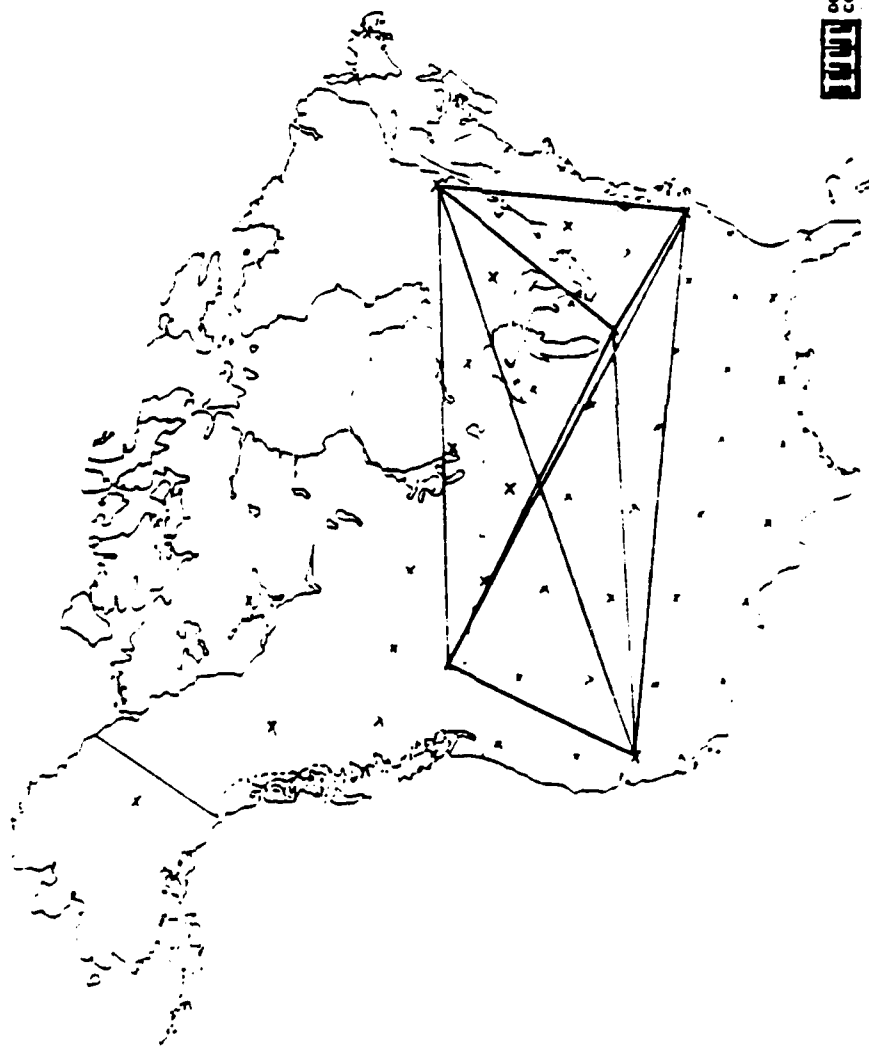
3 Hop Survival Failure α (Distance)²



US FLEET
COMBINED ATOMS

4/11/10

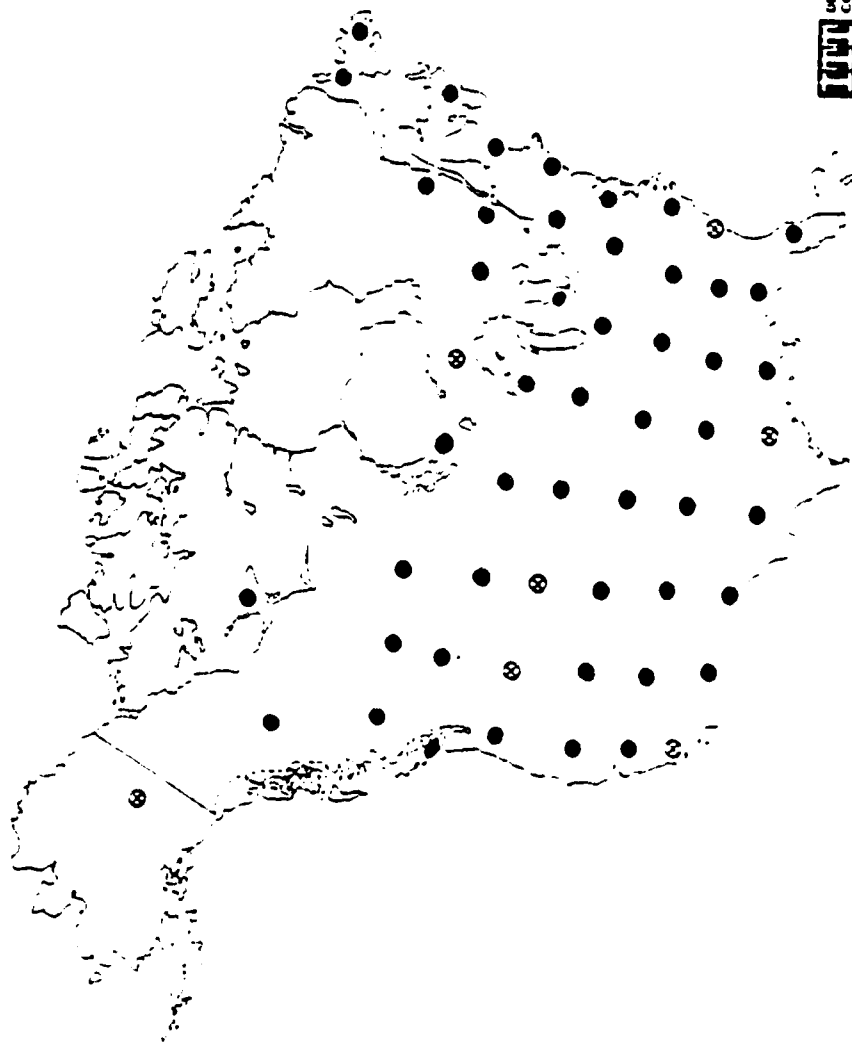
Direct Hop Connectivity



ITW DEFENSE COMMUNICATIONS

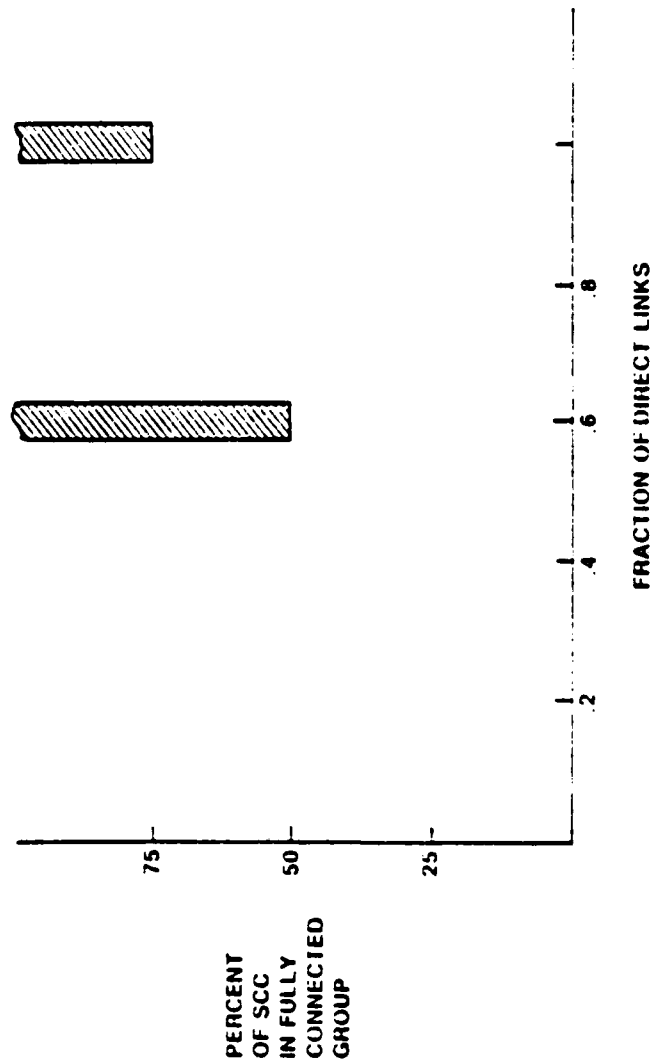
AUTH 1-1

Fully Connected Group



DEFENSE
COMMUNICATIONS
GROUP

Heuristic Simulation Result



DEFENSE
COMMITMENT ATIONS

ADD 1.2

The following paragraph is an abstract or introduction to the paper.

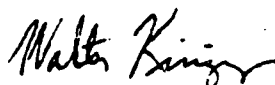
SURVIVABILITY OF COMMUNICATIONS IN EUROPE

by

Walter C. Kinzinger
The MITRE Corporation
McLean, Virginia 22102

This paper addresses the survivability of the U.S. Defense Communications System (DCS) in Europe. The DCS is a multi-country, theater-wide network that provides backbone communications among the major U.S. headquarters and also connects to the CONUS. The DCS includes the AUTOVON, AUTODIN, AUTOSEVOCOM and more recent programs such as DEB, ETS, DSN, and DDN. This paper responds to a growing concern that the DCS be capable of meeting the challenge of a wartime role. The issue is whether or not, within affordable budgets, there is a fixed communications network architecture structure that will provide adequate user connectivity in a major European theater conflict. Although the analysis addresses the European theater, the conclusions derived apply more broadly.

Thank you for this opportunity to discuss publicly some of the basic ideas that need to be incorporated into combat-ready military network design.



Walter C. Kinzinger
Associate Department Head
Worldwide Communications Systems
(703) 883-7475

WCK/1ac

MITRE

REQUEST FOR PUBLIC RELEASE OF UNCLASSIFIED TECHNICAL INFORMATION

Instructions:

- Complete form after referring to instructions on reverse side, P&P F2.c. and MITRE Security Procedures, Vol. 1, Sect. 8.
- Submit form intact to the responsible Technical Release Office. • Allow 6 weeks for routine processing.

1 No. Copies Attached Original + 3 copies	2 Subject/Title Survivability of Communications in Europe	3 MITRE Doc. No. (if any)
4 Date of Document 2 August 1982	5 Project Number 381A	6 Contract Number F19628-82-C-0001
7 Author(s) Walter C. Kinzinger		8 Dept. W-32
9 Proj. Officer/Symbol (if none, cognizant Government representative) D. Israel PSI		
10 Explain if Government release not required		
11 Approval Requested for ☐ Oral (and Visual) Presentation Only (no written publication) ☐ Written Publication of the Abstract (Summary) ☒ Written Publication of the Complete Paper		12 Release Deadline Dates (allow six weeks)
13 To be Submitted to (Editor/Chairman Name and Address) Bernard DeMarinis Booz, Allen & Hamilton		14 For Publication in or Presentation to: AFCEB Symposium at Fort Monmouth New Jersey
15 Has any portion of this material been formally released previously (including abstract)? Explain, including date, title, and release authority. No		
16 The attached material has been reviewed by the author(s) and is hereby approved to be disclosed. No proprietary or copyright information is included; any information relating to disclosures to the MITRE Patent Committee or other Government formally related to another Government contract is discussed in an attached memorandum.		
Author Walter Kinzinger		Date 1-1-82
APPROVED for Public Release		
Approval Signatures		
17 Project Leader Walter Kinzinger		Date 1-1-82
18 Department Head Harold Allen		Date 1-1-82
19 Tech. Director/Corp. Officer (for processing for presentation/publication in a foreign country)		Date
20 Vice President (or independent work)		Date
21 Technical Release Office		Date
white - Tech. Rel. Off. blue - Library		pink - Tech. Rel. Off. yellow - Author
		OSR No. W81-81

MCF 210 1/82

SURVIVABILITY OF COMMUNICATIONS IN EUROPE

- DESIGN OBJECTIVES
- PROBLEM QUANTIFICATION
- LESSONS LEARNED
- RECOMMENDED OVERALL STRATEGY

MITRE

DESIGN OBJECTIVES

- SELECT NETWORK ARCHITECTURES THAT PROVIDE GREATEST CONNECTIVITY AS CONFLICT ESCALATES
- MAKE BEST USE OF MILITARY – OWNED NETWORKS AND LEASED CIRCUITS

MITRE

PROBLEM QUANTIFICATION

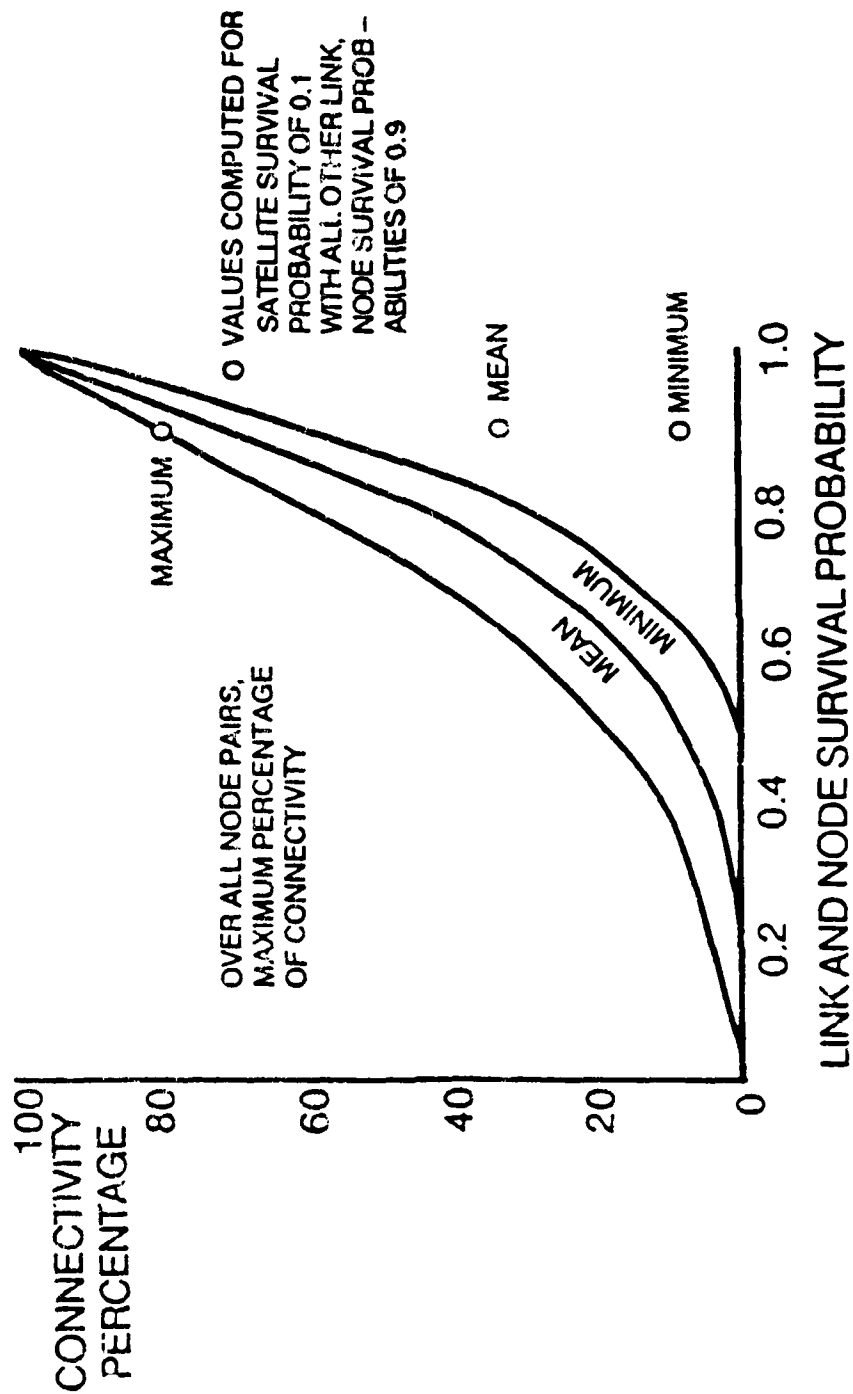
- DEVELOPMENT OF DATA BASE (ABOUT 10,000 REQUIREMENTS PLUS NODE AND LINK DEFINITIONS FOR EACH NETWORK)
- COMPUTER MODEL THAT RELATES CONFLICT LEVEL TO LINK AND NODE SURVIVABILITY AND WITH USER - USER CONNECTIVITY
- AUTOMATED ROUTER THAT ASSIGNS REQUIREMENTS TO TRANSMISSION SYSTEMS EFFICIENTLY AND PROVIDES USER - USER CONNECTIVITY
- APPLIED TECHNIQUES TO DCS SATELLITE OPTIONS, AUTOVON, IVSN, ETS AND INTERCONNECTS WITH PTT, GRUNDNETZ

MITRE

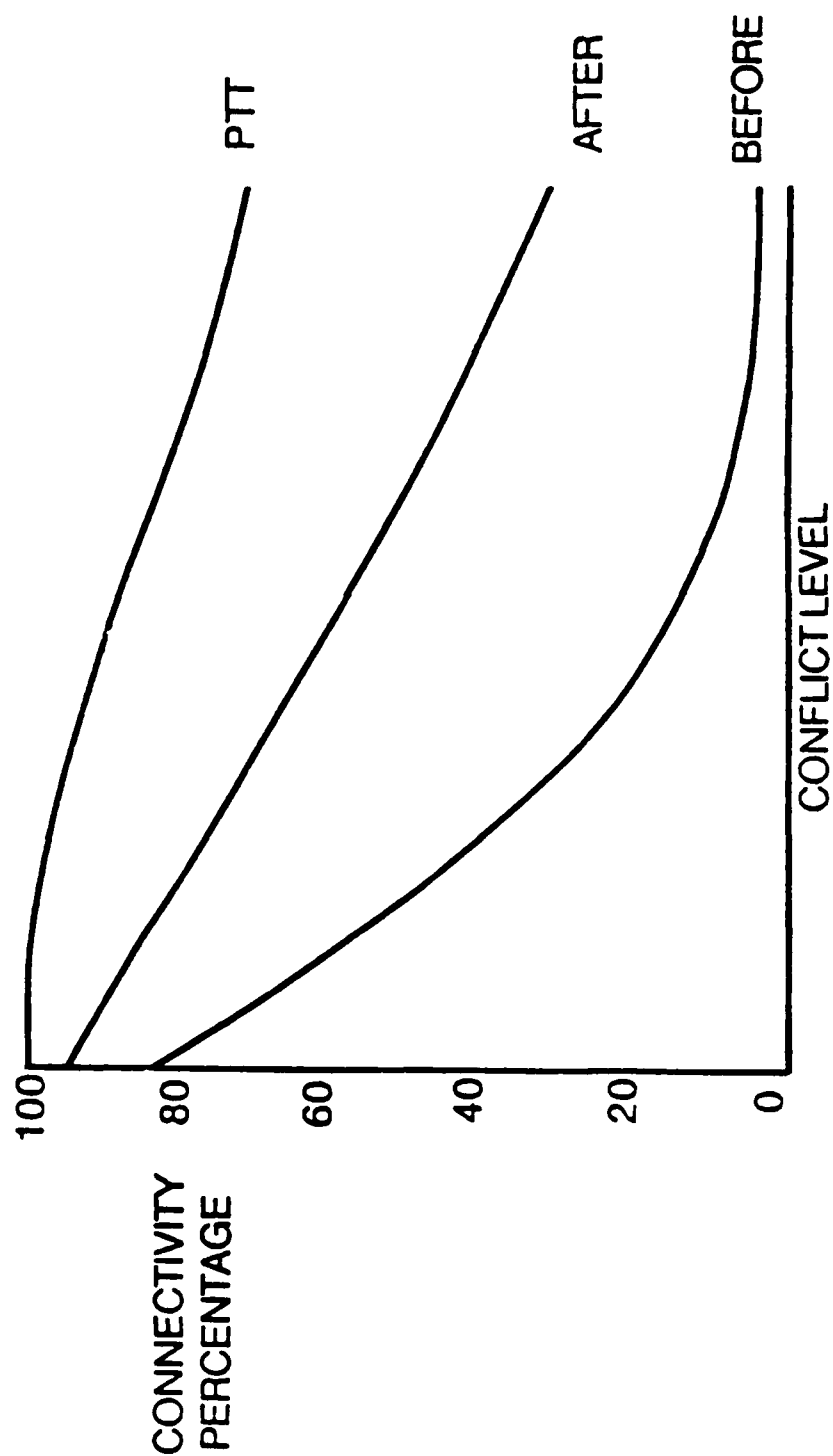
ENHANCED SURVIVABILITY FOR SINGLE NETWORKS

- AVOID CHOKE POINTS, HIERARCHICAL ROUTING
- PROVIDE HIGH LINK TO NODE RATIO (RICHLY CONNECTED TOPOLOGY)
- INCREASE NO. OF ASSETS (DISTRIBUTED TANDEM SWITCHES)
- PROVIDE DUAL HOMING OF USERS
- USE ASSOCIATED COMMON CHANNEL SIGNALING
- USE ALL SURVIVING CONNECTIVITY
- DISTRIBUTE SYSTEM CONTROLS
- MAXIMIZE THE NUMBER OF INDEPENDENT PATHS THROUGH THE NETWORK

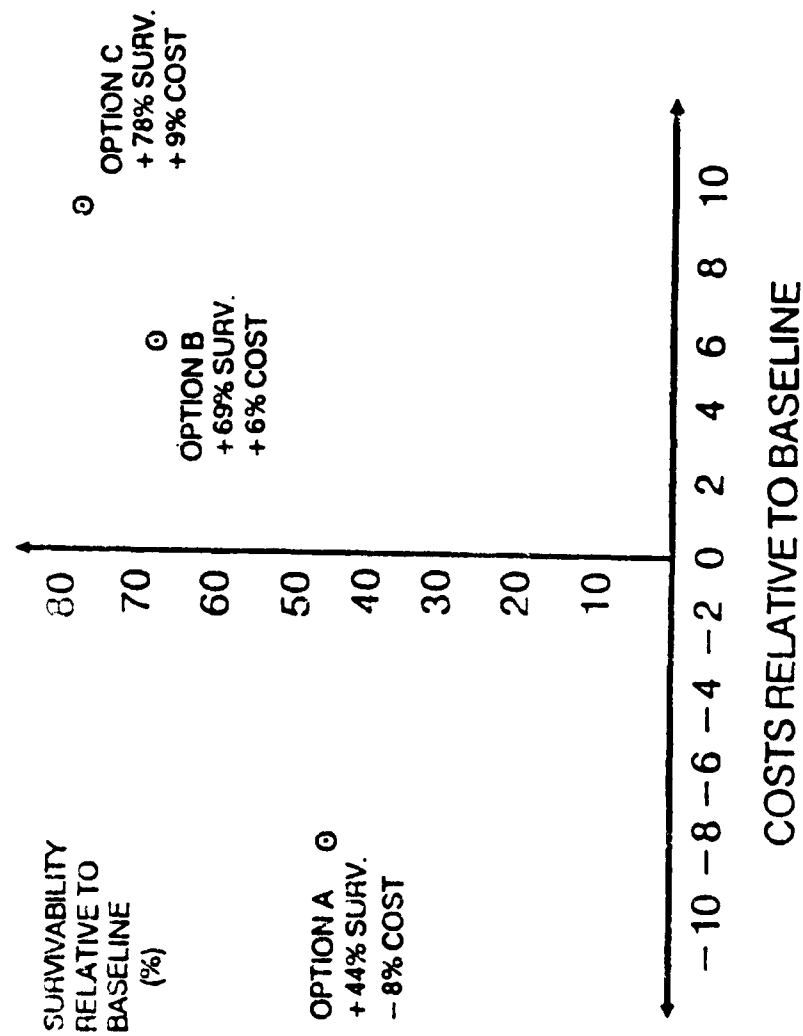
PERCENTAGE OF CONNECTIVITY FOR NODE PAIRS



COMMUNICATIONS CONNECTIVITY



EXAMPLE OF SURVIVABILITY IMPROVEMENT RESULTS



SURVIVABILITY SUMMARY

- ADEQUATE SURVIVABILITY MODEL DEVELOPED TO COMPARE NETWORK ARCHITECTURES ACROSS CONFLICT SPECTRUM
- ACCESS TO PARALLEL NETWORKS WITH LARGE NUMBERS OF ASSETS PROVIDES MAJOR SURVIVABILITY INCREMENTS
- ANALYSIS OF COMBINED NETWORKS VITAL TO ASSURE SURVIVABILITY GAIN (EFFECTS OF TOPOLOGY, TIE POINT LOCATIONS)
- REAL TIME REROUTING PAYS OFF, BUT REQUIRES PLANNING

RECOMMENDED OVERALL STRATEGY

- USE PARTNER NETWORKS
 - PTT (VOICE AND MESSAGE SUPPORT)
 - IN FRG TRADE DEB CAPACITY FOR RICHER LEASED GRIDING
 - ELSEWHERE IMPLEMENT PTT LATTICE
 - EXPAND MILITARY NETWORK INTERCONNECT ARRANGEMENTS
 - NICS, GRUNDNETZ, ASCON, STARRNET
- DISTRIBUTE ASSETS
 - USE ETS AND RELATED DEB IMPROVEMENTS AS OPPORTUNITY
 - GREATER ROUTING FLEXIBILITY TO AVOID BACKBONE
 - RICHER ETS GRIDING
 - DISTRIBUTED SYSTEM CONTROL
 - DEVELOP DSN USING DISTRIBUTED CAPABILITIES AND MAXIMUM TRANSMISSION REDUNDANCY
- PROVIDE REPLACEMENT ASSETS
 - E.G., ADDITIONAL DEB RESTORAL UNITS

LOOKING AHEAD

MILCOM '87, OCTOBER 19 - 22, 1987, WASHINGTON, D.C.

THEATER COMMUNICATION ARCHITECTURES SESSION (CLASSIFIED)

CONNECTIVITY AND ACCESSIBILITY OF EUROPEAN MILITARY
TELECOMMUNICATIONS NETWORKS

HENRY A. NEIMEIER

8:30 - 11:30 AM THURSDAY OCTOBER 22, 1987

**MONITORING AND CONTROL FOR THE
WIDEBAND PACKET SATELLITE NETWORK**

Steven Blumenthal

Manager, Network Technology Dept.

BBN Laboratories, Inc.

Cambridge, MA

OUTLINE OF TALK

- Overview of Packet Satellite Network Technology
- Topology and Description of the Wideband Network
- Earth Terminal and Satellite Modem/Codec Characteristics
- Wideband Network Monitoring Data
- Wideband Network Control
- Wideband Network Fault Isolation and Repair

PACKET SATELLITE NETWORK TECHNOLOGY

- Satellite channel:
shared multi access uplink - broadcast downlink
- Channel capacity is efficiently demand assigned on a packet-by-packet basis using the PODA reservation protocol
- Supports pure datagram service for bursty traffic and connection oriented "stream" service for constant duty cycle real-time traffic such as sensor data and packet voice and video
- Dynamic broadcast group addressing
- Multiple levels of transmission reliability via variable-rate FEC coding
- Multiple levels of priority for both datagram traffic and stream allocations
- Pre-emption of lower-priority stream allocations by new higher-priority allocation requests

PACKET SATELLITE NETWORKS

DARPA Atlantic Packet Satellite Network (SATNET)

- Two independent 64kb/s shared broadcast channels
- Operates on INTELSAT Atlantic Ocean Major Path I
- Uses BBN C/30 packet switch
- Provides Internet connectivity to ARPANET for many European research groups
- Used to support NATO C2 interoperability experiments.

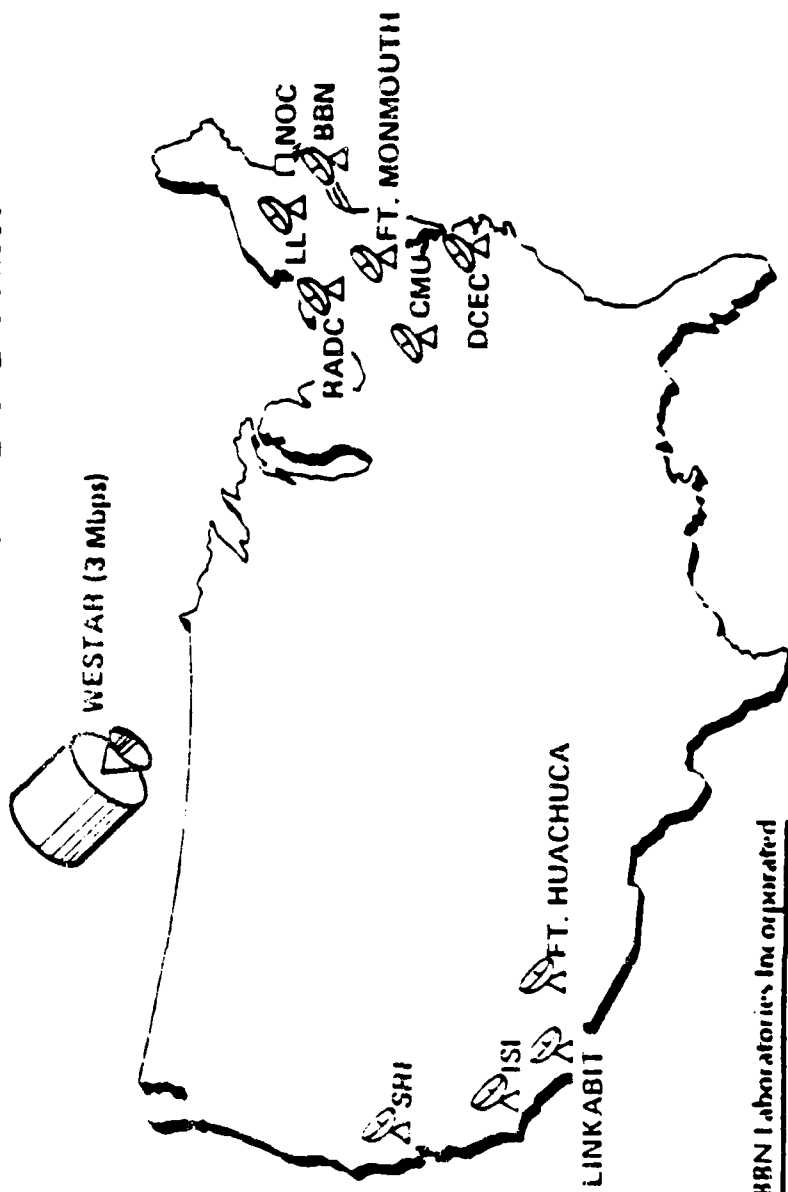
DARPA Wideband Packet Satellite Network

- 3 Mb/s shared broadcast channel
- Operates on WESTAR IV domestic satellite
- Uses BBN Butterfly Multiprocessor packet switch
- Supports multimedia (voice/video/text/graphics):
 - conferencing and high speed computer data communication
- Provides alternative to ARPANET for long-haul domestic traffic

NAVELEX Mobile Access Terminal Network (MATNET)

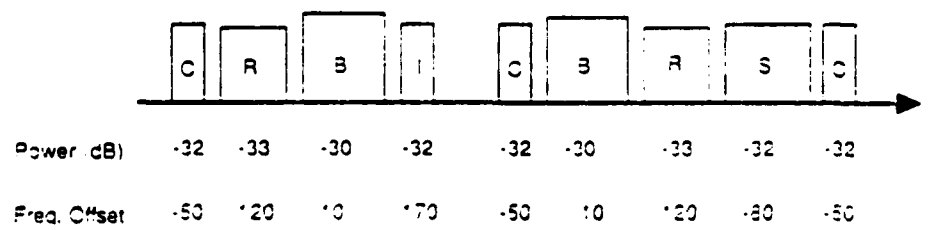
- 19.2Kb/s FLTSATCOM UHF shared broadcast channel
- Uses standard shipboard antennas, COMSEC equipment, and AN/WSC-3 radios
- Uses BBN C/30 packet switch
- Provides secure ship-to-shore and ship-to-ship C2 communication

EISN/WIDEBAND NETWORK SATELLITE SUBSYSTEM

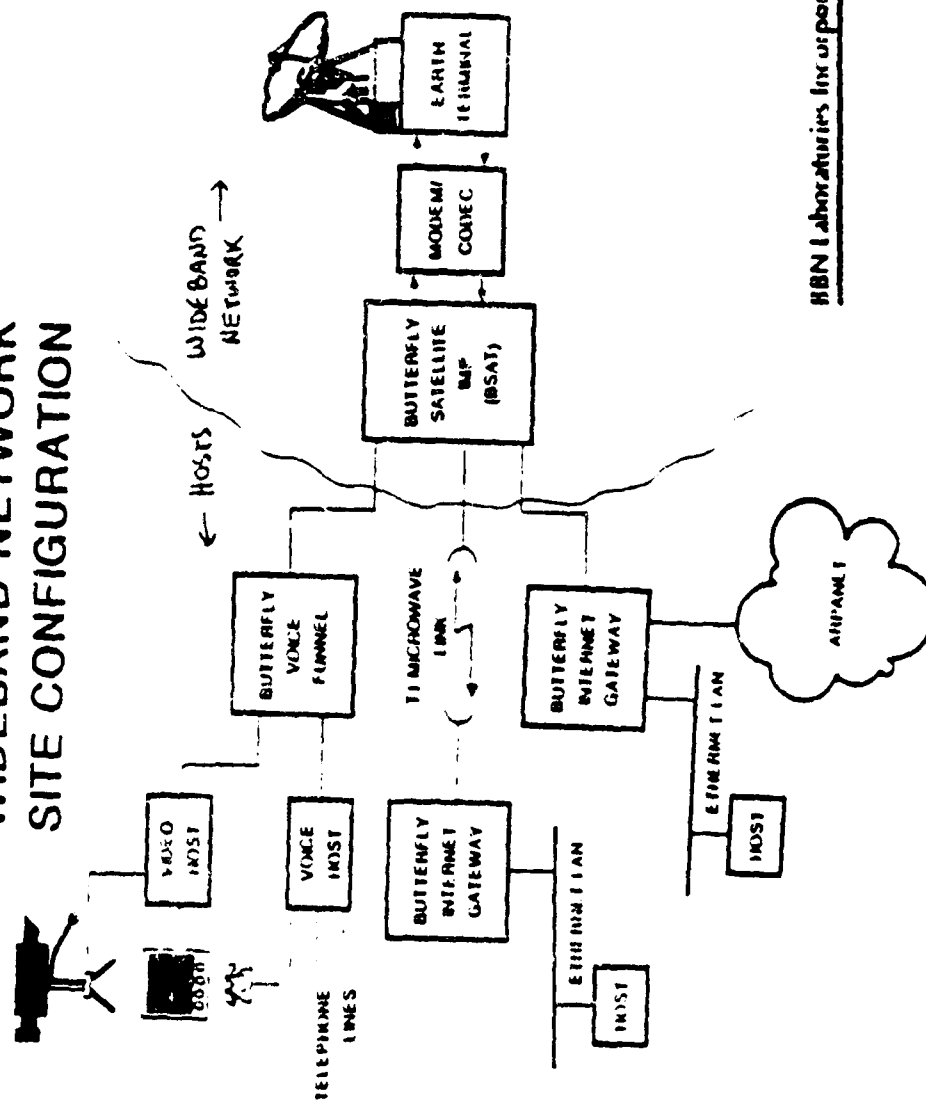


BBN Laboratories Inc. operated

Bursts on the Wideband Network Satellite Channel



WIDEBAND NETWORK SITE CONFIGURATION



HBN Laboratories Inc. operated

EARTH TERMINAL SPECIFICATIONS

Earth Terminal - Scientific Atlanta Model 8010C

- 7 meter, C-band, $G/T = 26.0 \text{ dB/}^{\circ}\text{K}$
- Receiver: 100°K Ga As FET Low Noise Amplifier
- Transmitter: 125W TWT High Power Amplifier
- Single crystal up/down converters
- RF frequencies: xmt= 6151.5 MHz rcv= 3926.5 MHz
- IF frequency = 34 MHz

BURST MODEM / CODEC SPECIFICATIONS

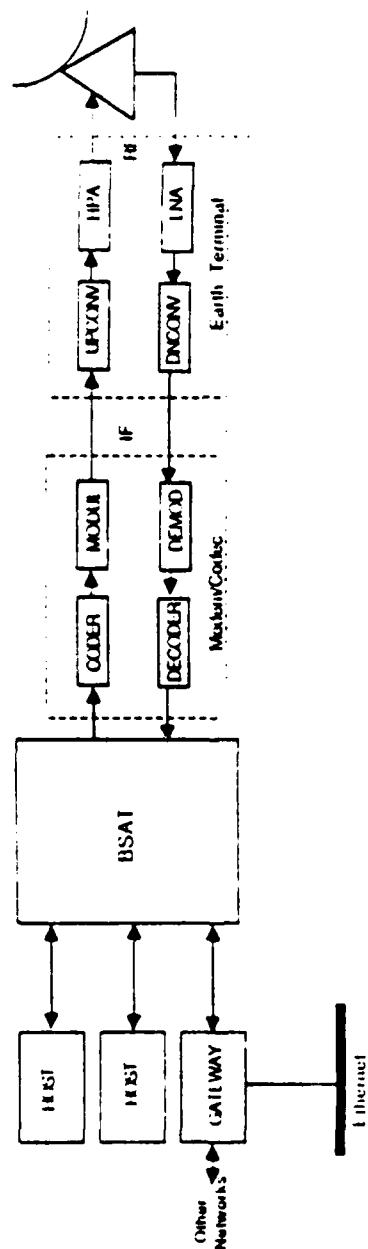
Burst Modem: M/A-COM Linkabit Model LBM36A

- Data rate: 193, 386, 772, 1544 Ksymbols/sec
- Modulation types: QPSK or BPSK
- IF frequency range: 52.000 - 87.995 MHz in 5KHz steps
- Burst-to-burst frequency tolerance: ± 500 Hz at 1.544 Msym/sec
- Long term input power range: -30dBm $\pm 10\text{dB}$
- Burst-to-burst input power range: $\pm 5\text{dB}$
- Can be operated as stand-alone "Burst Test Modem"

Codec: M/A-COM Linkabit Model LCC36B

- Convolutional Encoder
- Sequential Decoder
- Coding rates: 1/2, 3/4, 7/8, 1 (uncoded)

WIDEBAND NETWORK EQUIPMENT CONFIGURATION



NETWORK OPERATIONS CENTER (NOC)

- Located at BSN in Cambridge, MA
- Provides network monitoring, control, fault isolation, and repair facilities for:
 - ARPANET
 - MILNET (back up)
 - Internet Gateways
 - SATNET
 - Wideband Network
 - Other commercial X.25 networks
- Staffed 24 hours/day, 365 days/year
- Operates host computer facilities used for collecting real-time status, statistical, and exception data from networks, for exercising control over the networks, and for assistance in network trouble shooting
- Redundant monitoring and control paths are provided wherever possible
- Dispatches and coordinates repair services for leased phone lines, satellite channel equipment, modems, hosts, and packet-switching nodes

WIDEBAND NETWORK MONITORING DATA

Status data - periodically transmitted to the NOC by every BSAT:

- Hardware and software configuration
- Satellite channel interface state (e.g., synchronized, looped, etc.)
- Site parameter settings
- Host computer link state (e.g., up, down, looped, etc.)
- Earth Terminal and Modem/Codec status

WIDEBAND NETWORK MONITORING DATA (CONT'D)

Statistical data - periodically transmitted to the NCC by
every BSAT:

- Traffic statistics:
 - messages to/from hosts
 - messages to/from channel
 - bursts to/from channel
- Modem/Codec Test and Monitor Data - each of the
following is collected at all BSATs separately
for every BSAT heard on the satellite channel:
 - number of received bursts
 - frequency offset
 - received power
 - Es/No estimates
 - bits corrected by decoder

Wideband Frequency Offset (Hz)

Tuesday, 16 April 1985-18:31:02 GMT

From:

At:	ISI	Lincoln	DCEC	SRI	HADC	Ft Mun	Ft Hise	MACOM	CMU	BBN
ISI	20	40	70	20	200	0	140	80	0	130
Lincoln	30	-20	-60	50	240	-50	50	-20	0	60
DCEC	-120	-90	-210	-90	40	-200	-110	-160	0	-110
SRI	-50	40	-20	80	310	-30	130	60	0	90
HADC	-90	10	-40	30	180	-40	90	40	0	60
Ft Mun	-160	-220	-100	20	160	-110	20	-60	0	10
Ft Hise	-230	-90	-210	-30	170	-110	-10	-40	0	-60
MACOM	-100	0	-40	70	240	-60	60	30	0	40
CMU	0	0	0	0	0	0	0	0	0	0
BBN	20	30	-30	70	220	50	70	10	0	10

WIDEBAND NETWORK MONITORING DATA (CONT'D)

Trap data - spontaneously transmitted to the NCC by a
BSAT in response to exceptional conditions such as:

- Changes in BSAT, Modem/Codec, Earth Terminal, or
host link status
- High satellite channel or host link error rates
- BSAT or Modem/Codec throughput overloads
- Satellite channel protocol or host protocol
exceptions
- Program exceptions

WIDEBAND NETWORK CONTROL

Remote control of any BSAT can be exercised from NCC host computer facilities or from any BSAT console.

Control messages sent to a BSAT modify the BSAT's "external parameters". Actions that can be performed via the external parameters include:

- Looping/unlooping the satellite channel interface at various points in the BSAT, Modem/Codec, or Earth Terminal
- Looping/unlooping host computer interfaces
- Enabling/disabling/resetting satellite channel or host interfaces
- Reconfiguring BSAT software to drive redundant I/O devices
- Invocation of built-in diagnostic test procedures
- Generation of artificial test traffic
- BSAT built-in bit error rate testing
- Uplink frequency adjustment
- Modification of Modem/Codec parameters (e.g., FEC coding rate, modulation type, channel symbol rate)
- Modification of protocol parameters
- Informational requests

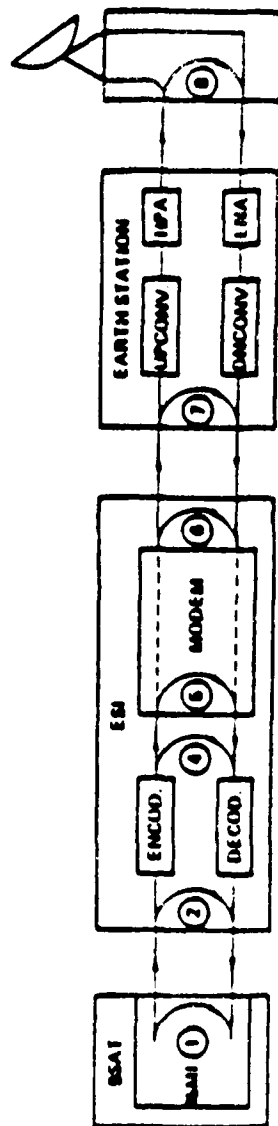


Figure 4 Midband Network Site Loopback Mode

WIDEBAND NETWORK FAULT ISOLATION AND REPAIR

- Fault isolation is performed by means of NOC computer control of the BSAT external parameters along with inspection of the received network monitoring data

- Additional diagnostic facilities are provided by:

Burst Test Modem

Remote monitoring and control of Earth Terminal status by CONTEL ASC

- Long-term drifts and/or degradations in satellite channel performance can be detected via:

Test and Monitor Data collection

Automated scanning of the satellite channel downlink received at BBN

Equipment adjustment or replacement can be initiated before performance becomes unacceptable.

- Repairs and adjustments are dispatched from BBN, Cambridge as required

SUMMARY

The DARPA Wideband Packet Satellite Network is characterized by:

- Widely distributed unattended network sites
- Connectivity via a single shared satellite channel using a demand-assigned TDMA protocol
- Satellite channel equipment which can drift in power and frequency
- Satellite Modem/Codec unit performance degradations in the face of large intersite power and frequency differences

Automated real-time network monitoring, control, and fault diagnosis systems and techniques have been developed and successfully applied resulting in the provision of stable network operations.



Telecommunications Complex Systems Organization

Federal Systems Division

Complex Systems Organization — (CSO)

Telecommunications Mission:

- **Develop and Market Solutions for Accounts with Diverse, Integrated Systems Requirements**
- **Enhance Sales of IBM Products and Services**
- **Serve as Center of Competence for Systems Integration within IBM**

AD-A195 374

PROCEEDINGS OF THE COMMUNICATIONS NETWORK MANAGEMENT
WORKSHOP (1987) HELD. (U) ROME AIR DEVELOPMENT CENTER
GRIFFISS AFB NY J J SALERNO ET AL. NOV 87

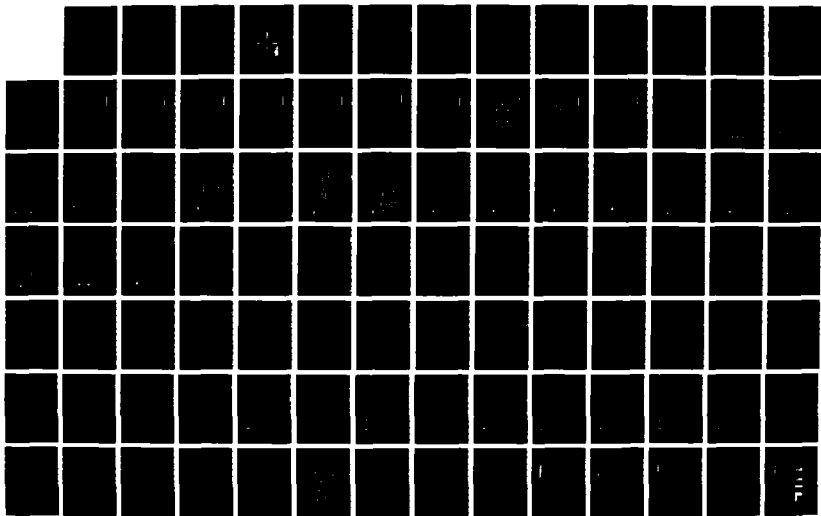
3/5

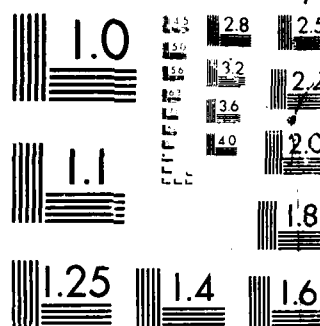
UNCLASSIFIED

RADC-TR-87-231

F/G 25/4

NL

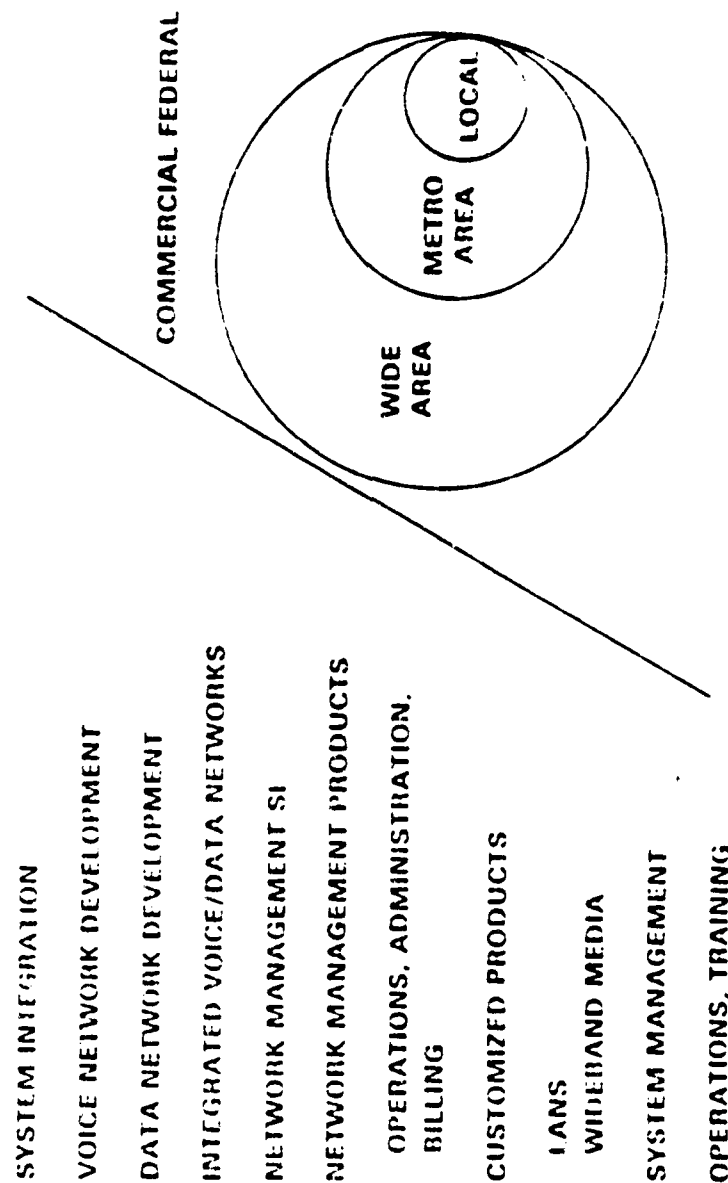




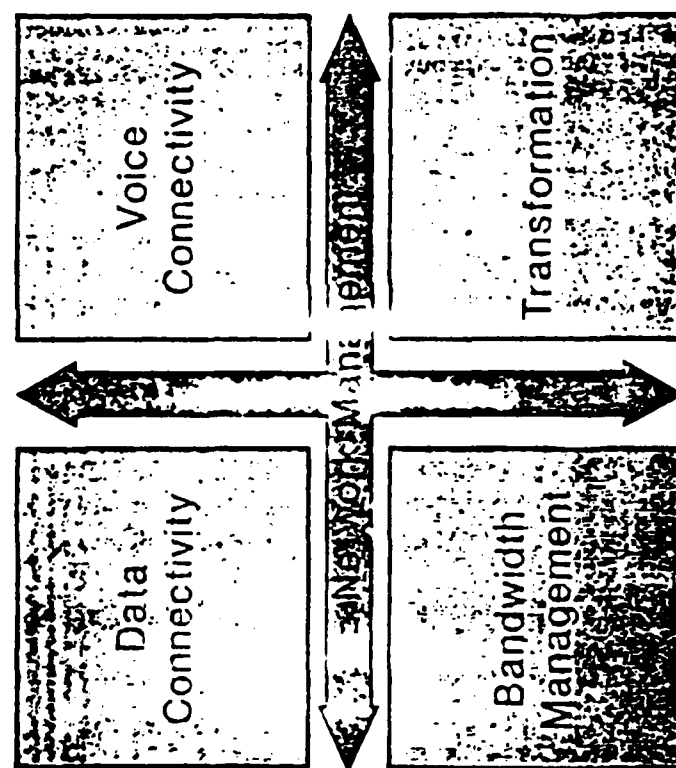
CSO Telecommunications Unit

- Formed in Mid-1985
- 200 People; 90% Technical
- Experienced Cadre
 - Large Scale Program Management
 - Systems Engineering
 - Commercial Marketing
 - Programming
 - Network Management
 - Network Design
- Recruited From:
 - Products Organizations
 - Satellite Business Systems
 - Traditional FSD
 - Marketing Divisions
 - Common Carriers

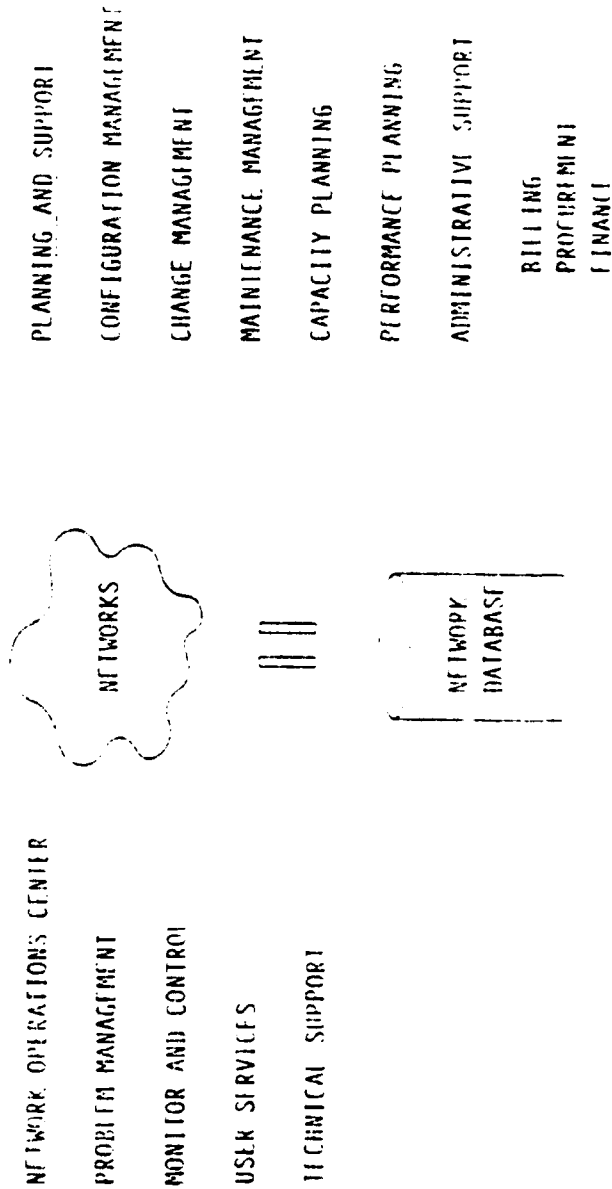
CSO TELECOMMUNICATIONS / CAPABILITIES



STRATEGIC NETWORK FUNCTIONS



NETWORK MANAGEMENT FUNCTIONAL DEFINITION



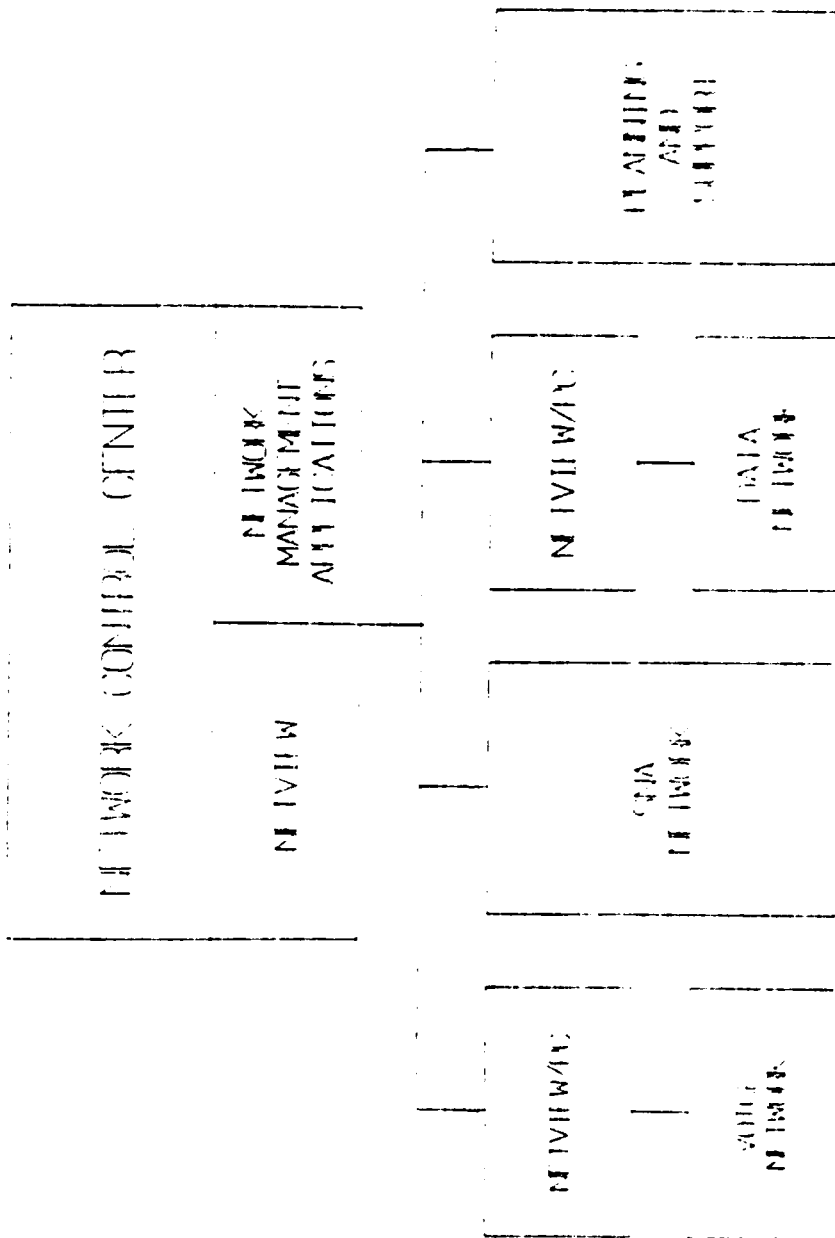
13480005, 1X1

NETWORK MANAGEMENT SOLUTION PROCESS

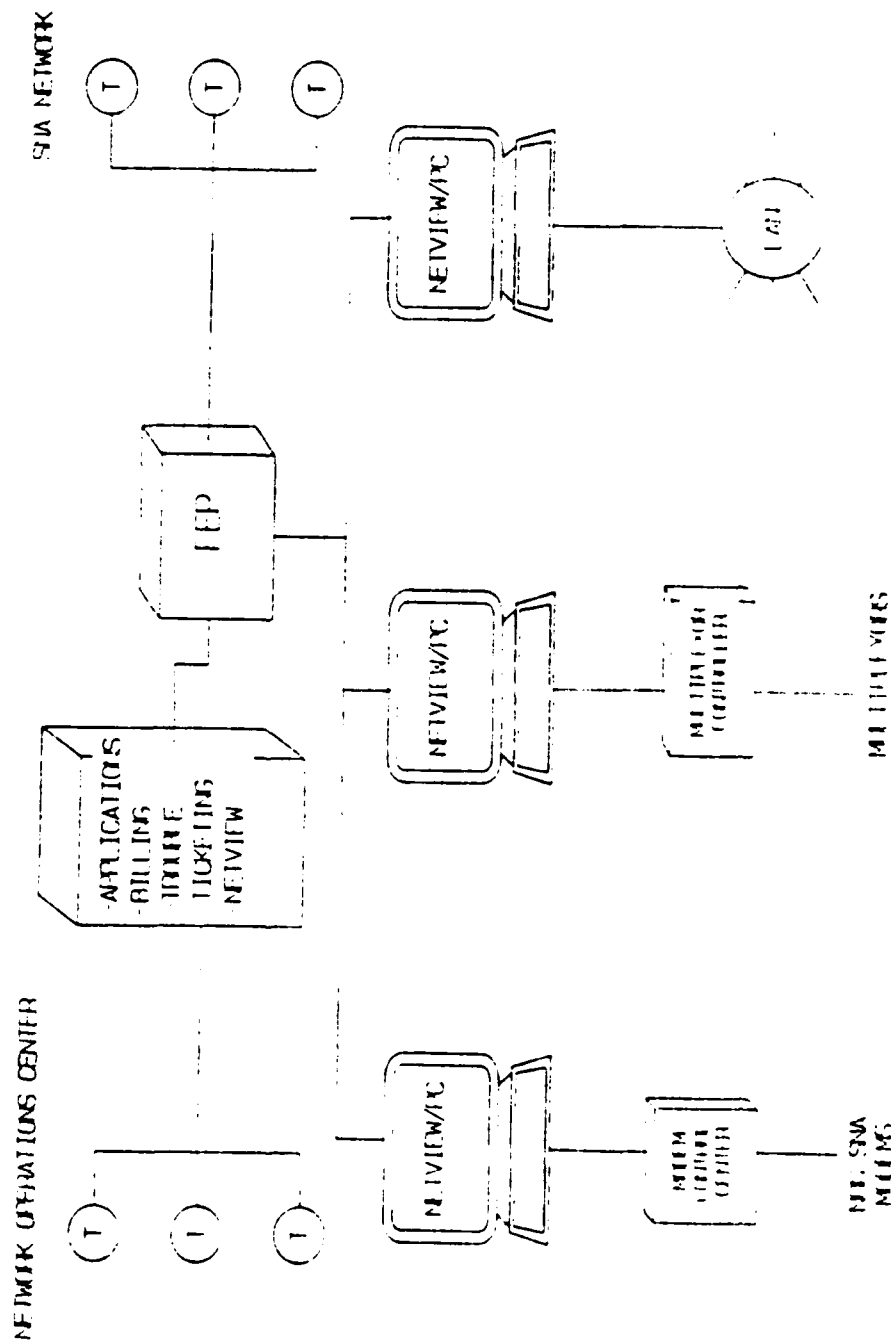
- 0 REQUIREMENTS ANALYSIS
 - SELECTED NETWORKS
 - FUNCTIONAL NEEDS
 - MIGRATION CONSTRAINTS
 - STRATEGIC DIRECTIONS
 - GROWTH EXPECTATIONS
 - DATA PROCESSING ENVIRONMENT
- 0 SYSTEM DESIGN
 - TRANSACTION SCENARIOS
 - DEVELOP BASE ARCHITECTURE
 - SPECIFY UNIQUE SOFTWARE AND HARDWARE
- 0 PRIORITIZATION AND PHASING
 - BUSINESS CASE
 - STRATEGIC ANALYSIS
 - TACTICAL NEEDS
- 0 IMPLEMENTATION AND DEPLOYMENT
 - PROCURE STANDARD EQUIPMENT
 - DEVELOP UNIQUE SOFTWARE AND HARDWARE
 - INTEGRATE
 - TEST
 - INSTALL

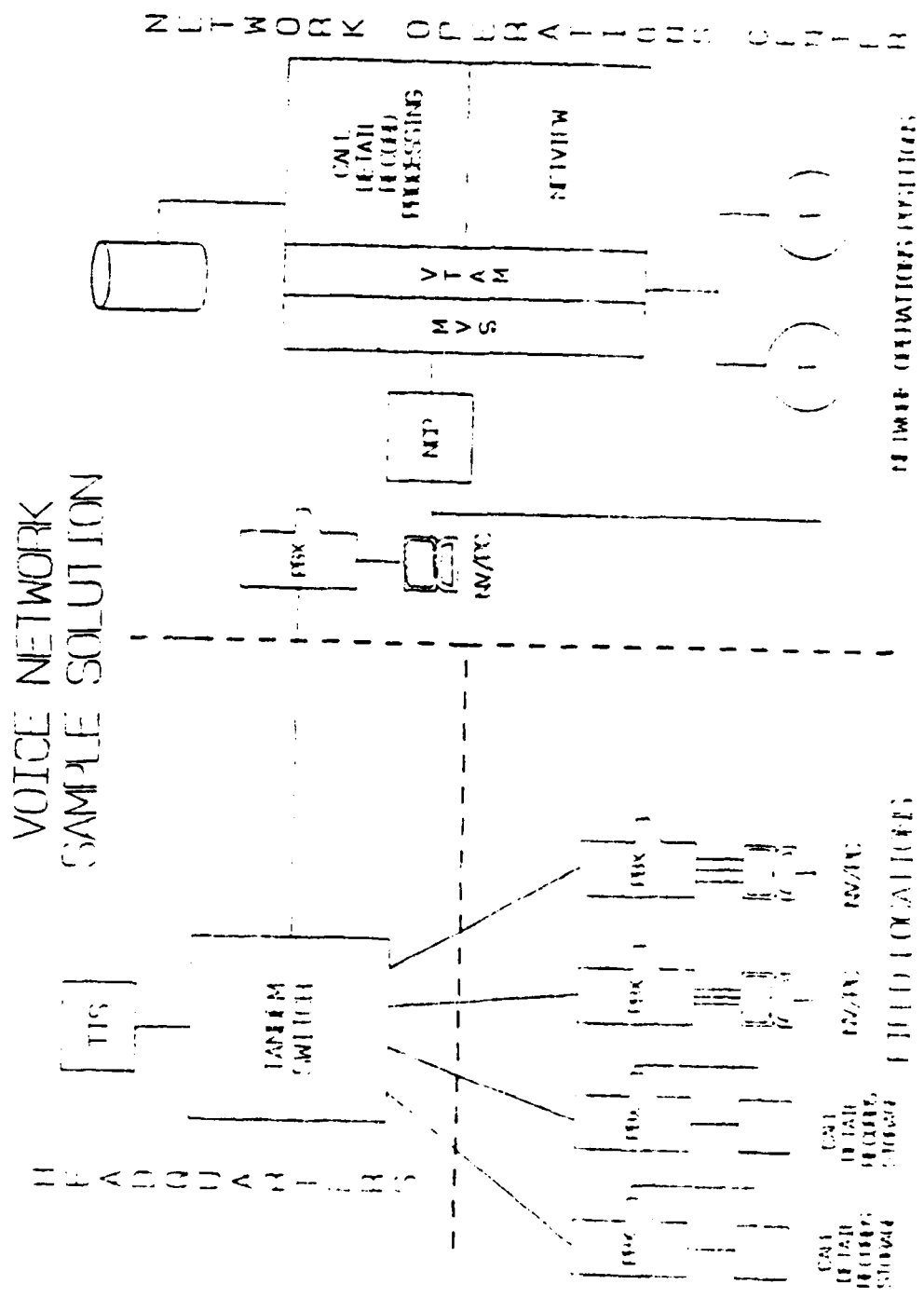
13080005, TXI

NETWORK MANAGEMENT ARCHITECTURE



DATA NETWORK SAMPLE SOLUTIONS





SUMMARY

NETVIEW/PC WITH NETVIEW PROVIDES THE BASIS FOR CONSTRUCTING A
SINGLE NETWORK MANAGEMENT SYSTEM ACROSS MULTIPLE NETWORKS

0 VOICE

0 DATA

- SNA

- NON-SNA

0 INTEGRATED

0 FUTURES

- OTHER EQUIPMENT

- MANAGEMENT SUPPORT FUNCTIONS

13880005.TXT

Summary

- IBM Offering
 - Turnkey / Custom Solutions
 - Long Term Relationships
 - Joint Development
- Telecommunication Application Knowledge
 - Network Management
 - Modernization / Integration
 - Unique Requirements
- Turnkey Solution Elements
 - Requirements Methodology
 - System Architecture / Design
 - System Assurance
 - System Implementation

Shock Analysis of Communications Networks

Dr. Nicholas Duchon

Digital Communications Department
Martin Marietta Laboratories
1450 South Rolling Road
Baltimore, Maryland 21227
(301) 247-0700

July 1987

Phenomena:

1. High demand over short periods of time
2. Loss of physical resources
 - Destruction of nodes and links
 - Jamming
 - Interference from natural sources
3. Examples:
 - war
 - natural disasters
 - cultural events

070187 DC - 2

MARTIN MARIETTA

Goals

1. Classification
2. Models
3. Heuristics
4. Application in intelligent network controller

Network Characteristics:

1. Packet switching queueing
2. Signalling for problem detection
3. Adaptive routing
4. Dynamic reconfiguration

Network Variables:

1. Quiescent loading
2. Shock loading: amount, direction and replies
3. Destruction and reconfiguration
4. Routing algorithms
5. System hardware configuration

Topology

Queue sizes

Link characteristics

07/0187 DC 5

MARTIN MARIETTA

Measures of Performance:

1. Delay:
 - End to end
 - In a subnet
 - Mean, variance and maximum
2. Queue sizes
 - Mean, variance and maximum
3. Reliability
 - Lost, garbled and mis-directed messages
4. Network utilization

Optimization vs. Adequacy:

1. Packetized voice:

Faster than reconstruction time not useful

Some packet loss tolerable

Packets time-out

Time critical

2. Data:

Loss of packets not acceptable

Packets may time-out

Generally delay not critical

Problem of undeliverable data

Local and Global control:

1. Global control advantages:

Allows network optimization

Maintains complete connectivity information

2. Global control problems:

Getting information to a central location

Time required to optimize network

Distribution of results

Network status may have changed during update

Vulnerability of network to control center loss

3. Local control problems:

No network wide optimization

Packets may go to dead end subnets for a while

May accept messages for disconnected nodes

Looping of messages in network

Special Vulnerabilities:

1. Time-dependent jamming
2. Flooding network with unauthorized messages
3. Protocol attacks

If an acknowledgement protocol is used,
the enemy may insert nack's, e.g.

Research Methods:

1. Simulation
 - Event oriented
 - Interactive
 - Small networks
2. Analysis with approximations guided by observations

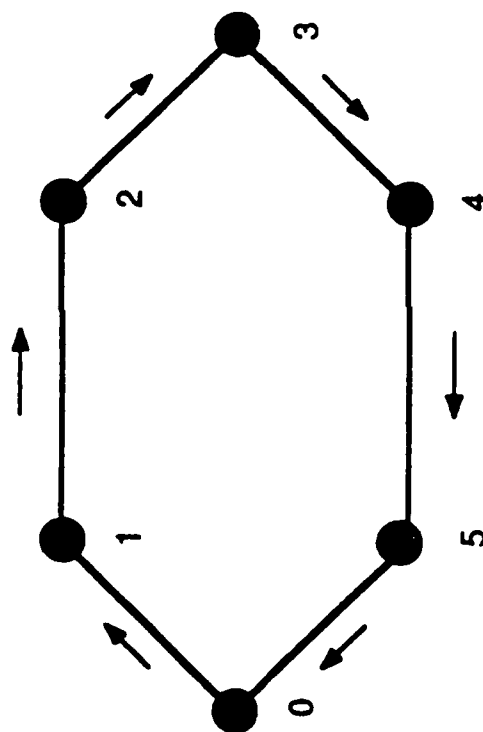
Observations:

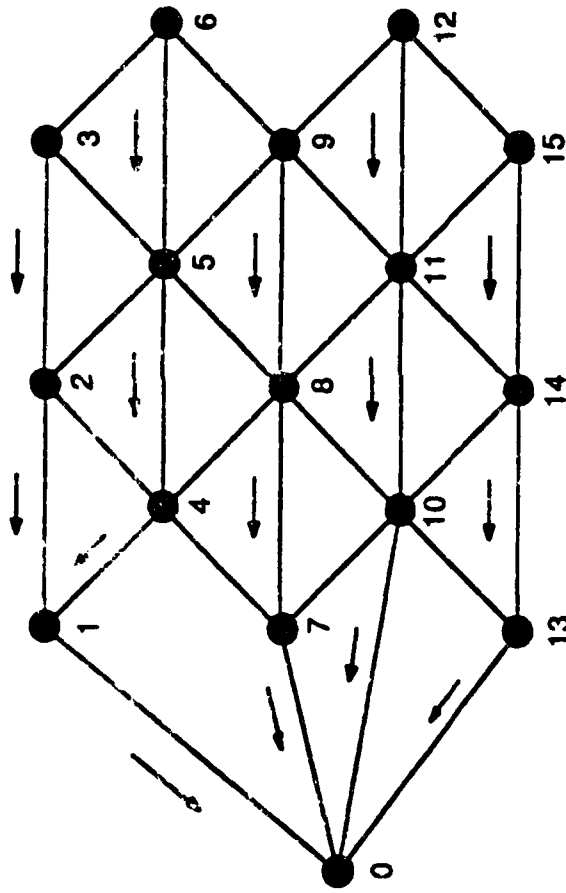
1. Ring network
2. Field/HQ example

079187-DC-10

MARTIN MARIETTA

The Ring Network





The Field-Headquarters Example
Routing from the field to HQ

Some Mathematical results (Werner Furth):

1. Arrival rate greater than service rate

Distribution of max queue sizes

Error in Tackacs on mean

Calculation of higher moments

2. Closed ring network

Lumpy queue result: If all service rates are equal then the most probable number of packets in any given queue is zero.

Packet Radio Routing Across Unidirectional Links and to Receive-Only Nodes

SURAN Technical Note #46

August 13, 1986

Jim Stevens, Rockwell International Corporation

Work performed under contract # MDA903--85-C-0205

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Defense Advanced Research Projects Agency, or the U. S. Government.

Approved for public release, Distribution is unlimited

Network Management for SURAN

Jim Stevens, Rockwell International Corporation

- Present one area of management in depth instead of broad overview.
- Present management to support unidirectional links and receive – only nodes.
- Note that management support must be provided at multiple protocol layers.

● Types of link connectivity

(1) bidirectional (bi-link)



(2) unidirectional (uni-link)



(3) no link (no-link)



● Unidirectional Links

- 1 node can reliably hear another node, yet 2nd node cannot hear 1st.
- Caused by RF propagation, topology, and/or different transmit power levels.

● Receive – Only Nodes

- A node can passively receive data, yet cannot or will not transmit data.
- Caused by failures or operational requirements.

● Types of route connectivity

(1) 2-way route (2-way)



(2) 1-way route (1-way)



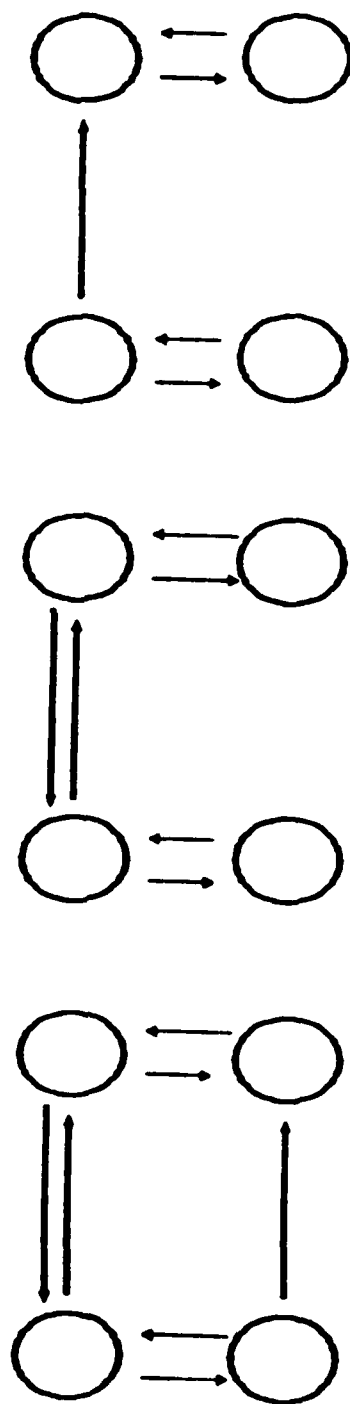
(3) no route (no-way)



Link / Route Connectivity Combinations



(1) bi-link, 2-way (2) uni-link, 1-way (3) no-link, no-way

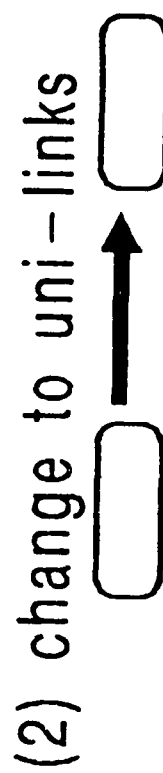
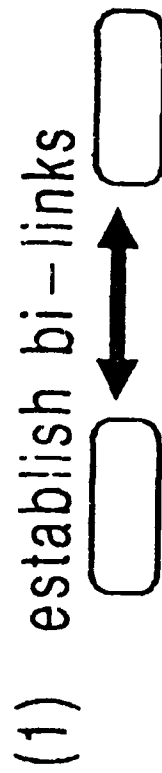


(4) uni-link, 2-way (5) no-link, 2-way (6) no-link, 1-way

LINK ESTABLISHMENT PROTOCOLS

generally require bidirectional links.

● Bi-links that change to uni-links:



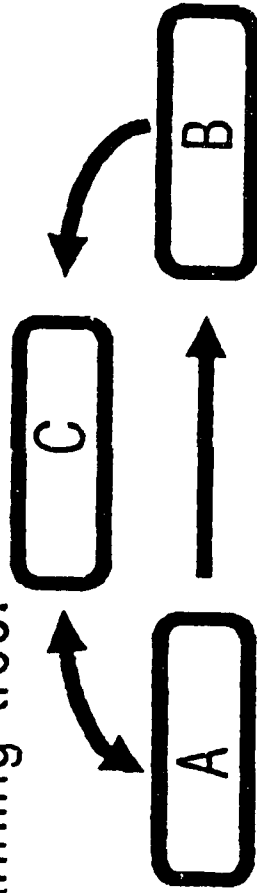
PROBLEM WITH UNIDIRECTIONAL LINKS AND RECEIVE – ONLY NODES:

- (1) Most link and network protocols require bi – directional links
- (2) Most transport and above protocols require immediate end – to – end acknowledgments for reliability

LINK ESTABLISHMENT PROTOCOLS

- Distributed uni--link establishment protocol:

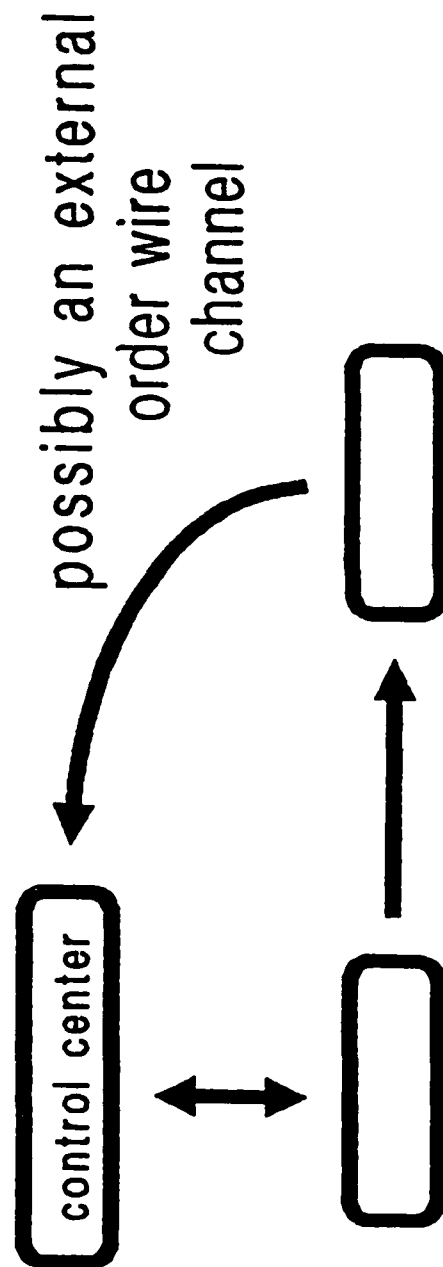
- (1) nodes broadcast out their minimal hearing spanning tree.



- (2) nodes eventually get broadcast pkt that indicates some node can hear them.
- (3) nodes then send a source--routed pkt to nodes that can hear them to establish link.

LINK ESTABLISHMENT PROTOCOLS

- Control center which all nodes can talk to or which knows position location of nodes and thus can tell nodes of uni-links.



ROUTE ESTABLISHMENT PROTOCOLS

- Network with uni-links and 2-way routes:
 - (1) nodes find uni-links through link establishment protocols above.
 - (2) routes found either through centralized control or distributed algorithm and source-routed packets which contain route information.

ROUTE ESTABLISHMENT PROTOCOLS

generally require bidirectional links.

- Network with uni-links and 1-way routes:

- (1) nodes find uni-links through link establishment protocols above.
- (2) nodes consider themselves 1-hop distance away from nodes that can hear them.
- (3) use normal network routing algorithm

FORWARDING PROTOCOLS

- Forwarding to receive – only nodes:
 - if receive – only node has multiple neighbors with uni – links to it, then send packet to each of these neighbors so that they can transmit to it to increase probability of success.

FORWARDING PROTOCOLS

generally have link acks (e.g. ARQ)

- Forwarding across uni-links.
 - use Forward Error Correction (FEC)
 - transmit packets multiple number of times to get high probability of success.

TRANSPORT & HIGHER LEVEL PROTOCOLS

- Network with routes that are 1 – way most of time and 2 – way part of time:
 - build application to act as surrogate for receive – only node.
 - * surrogate performs normal handshaking
 - * surrogate stores information as well as sending info to node unreliably.
 - * when node is 2 – way, it gets missing packets from surrogate.

TRANSPORT & HIGHER LEVEL PROTOCOLS
generally require immediate end-to-end
acks for reliability.

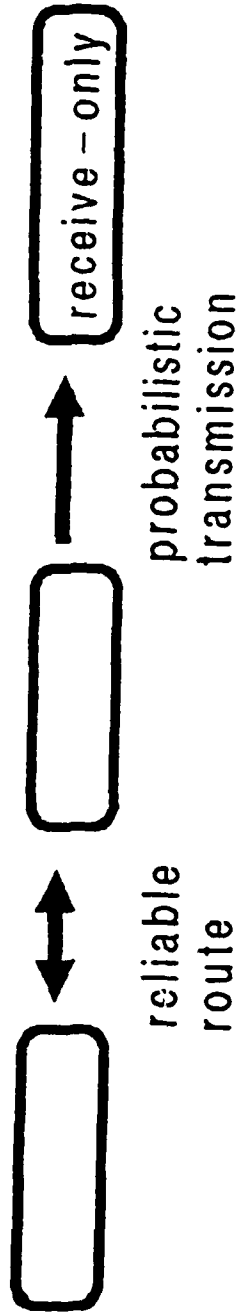
- Network with routes that are 1-way most
of time and 2-way part of time:
 - Modify protocols to accept low duty
cycle responses:
 - * large windows,
 - * no connection open negotiation,
 - * no connection keep alive pkts.

TRANSPORT & HIGHER LEVEL PROTOCOLS

- Network with routes that are 1 -- way :
 - Use transport level FEC
interleave message over several
packets such that message can still
be recovered even if some packets
were lost.

TRANSPORT & HIGHER LEVEL PROTOCOLS

- Network with routes that are 1-way :
 - Get pkts as close as possible to receive only node and then use probabilistic transmission scheme.



CONCLUSIONS for workshop:

- Management to provide many network services must span multiple protocol layers.
- Management of some protocol layers, such as link and network, often require services of higher layer protocols, such as reliability of transport.

CONCLUSIONS to paper:

- Communications across unidirectional links and to receive-only nodes can be supported with changes to today's protocols.

PACKET RADIO ROUTING ACROSS UNIDIRECTIONAL LINKS
AND TO RECEIVE-ONLY NODES

SRNTN 46

August 13, 1986

Prepared by: Jim Stevens
Rockwell International
Collins Defense Communications
High Frequency Communications Division

Prepared for: Dr. Dennis Perry
Defense Advanced Research Projects Agency
1400 Wilson Boulevard
Arlington, Virginia 22209-2308

Mr. Paul Sass
US Army GECOM
Attention: AMS2L-COM-AF-2
Fort Monmouth, New Jersey 07703-5202

Sponsored by Defense Advanced Research Projects Agency (DoD)
Information Sciences and Technologies Office
Survivable Radio Networks (SURAN) Program
ARPA Order No. 4747/8
Issued by E. Clark under Contract # MDA903-85-C-0205

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Defense Advanced Research Projects Agency, or the U. S. Government.

Approved for public release
Distribution is unlimited

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0187
Exp. Date: Jun 90

1a REPORT SECURITY CLASSIFICATION Unclassified			1b RESTRICTIVE MARKINGS		
2a SECURITY CLASSIFICATION AUTHORITY DD Form 254 dated 4 January 1986			3 DISTRIBUTION AVAILABILITY OF REPORT		
2b DECLASSIFICATION/DOWNGRADING SCHEDULE CG-45			Approved for Public Release Distribution Unlimited		
4 PERFORMING ORGANIZATION REPORT NUMBER(S) SURAN-205-6			5 MONITORING ORGANIZATION REPORT NUMBER(S) SRNTN 46		
6a NAME OF PERFORMING ORGANIZATION Rockwell International Collins Defense Communication		6b OFFICE SYMBOL (If applicable) M/S 460-340	7a NAME OF MONITORING ORGANIZATION Defense Advanced Research Projects Agency Information Sciences and Technologies Off		
6c ADDRESS (City, State, and ZIP Code) 3200 E. Renner Road Richardson, Texas 75081-6209			7b ADDRESS (City, State, and ZIP Code) 1400 Wilson Boulevard Arlington, Virginia 22209-2308		
8a NAME OF FUNDING/SPONSORING ORGANIZATION DARPA		8b OFFICE SYMBOL (If applicable) ISTO	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER Contract No. MDA-903-85-C-0205		
8c ADDRESS (City, State, and ZIP Code) 1400 Wilson Boulevard Arlington, Virginia 22209-2308			10 SOURCE OF FUNDING NUMBERS		
			PROGRAM ELEMENT NO 62708E	PROGRAM CODE ST10	TASK NO 4747/B
11 TITLE (Include Security Classification) Packet Radio Routing Across Unidirectional Links and to Receive Only Nodes					
12 PERSONAL AUTHOR(S) James A. Stevens					
13a TYPE OF REPORT SRNTN		13b TIME COVERED FROM 1985 TO 1986		14 DATE OF REPORT (Year, Month, Day) 1986 August 13	
15 PAGE COUNT 27					
16 SUPPLEMENTARY NOTATION					
17 COSAT CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)		
FIELD	GROUP	SUB-GROUP			
17	02	1	Protocols, Packet Radio, Unidirectional Routing, Receive-Only		
19 ABSTRACT (Continue on reverse if necessary and identify by block number)					
Network protocols are examined that allow packets to be routed across unidirectional links and to nodes within a network that are in a receive-only mode of operation. Support is still provided to these receive-only nodes to allow them, at a moment's notice, to transmit a packet into the network and go back into either the receive-only mode or the normal mode of operation. This paper presents adaptations to the current DARPA Packet Radio link and network layer protocols, suggests changes required to the transport and application layer protocols, and shows how such protocols could be used in other areas. Related areas examined are multi-channel networks (internets), network reconstitution, multi-level secure networks, networks that contain areas of dense connectivity, and network expressways (backbones).					
20 DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS			21 ABSTRACT SECURITY CLASSIFICATION Unclassified		
22a NAME OF RESPONSIBLE INDIVIDUAL			22b TELEPHONE (Include Area Code)		22c OFFICE SYMBOL

DO FORM 1473, 84 MAR

83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

PREFACE

The material in this paper was presented in an earlier form at the May 86 SURAN Implementers Meeting and at the May 86 Tactical Internet Task Force. This paper hopefully clarifies some of the questions and incorporates some of the comments that arose at these two meetings.

1. INTRODUCTION

Often, either due to failures or operational requirements, a node within a network cannot transmit any data. The node can still passively receive data, but can no longer transmit data, acknowledge any data reception, or even continue to participate in the normal network routing protocols. In addition, it is more likely, especially in a radio network, that one node can reliably hear another node, yet the second node cannot hear the first. In other words, there can be a unidirectional link between two nodes instead of a bidirectional link.

This paper examines the current DARPA Packet Radio Network (PRNET) link connectivity, tier routing, and packet forwarding protocols and describes how they can be adapted to support unidirectional links as well as bidirectional links. Problems and adaptations at the transport and application protocol layers are also examined.

Any network area that could have unidirectional links or receive-only nodes could use the adapted network and transport protocols described in this paper. Areas examined within this paper are multi-channel networks (internets), network reconstitution, multi-level secure networks, networks that contain areas of dense connectivity, and network expressways (backbones).

2. TYPES OF LINK CONNECTIVITY

This paper will use the terminology from this section for the link and network routing connectivity.

There are 4 types of link connectivity possible between 2 nodes, say node A and node B. The 4 types along with the terminology used within this paper are:

- * bidirectional link between A and B (bi-link),
- * unidirectional link from A to B (uni-link),
- * unidirectional link from B to A (uni-link), and
- * no link between A and B (no-link).

Uni-links can occur for several reasons. Packet Radio (PR) can have uni-links because PRs could be transmitting at different transmission power levels or else using antennas with different gains. In addition, if a PR network is using frequency diversity, then the frequency channel from PR A to PR B might be temporarily cut off while the channel from B to A might still be operational on another frequency. In addition, PRs may for operational reasons, for example to conserve power, may go into a mode of operation where they would still receive but would not longer transmit thus causing uni-links. Many conventional routing protocols consider uni-links to be equivalent to no-links.

There are 4 types of network routing connectivity possible between 2 nodes, say node A and node B. The 4 types along with the terminology used within this paper are:

- * two-way route between A and B (2-way),
- * one-way route from A to B (1-way),
- * one-way route from B to A (1-way), and
- * no route between A and B (no-way).

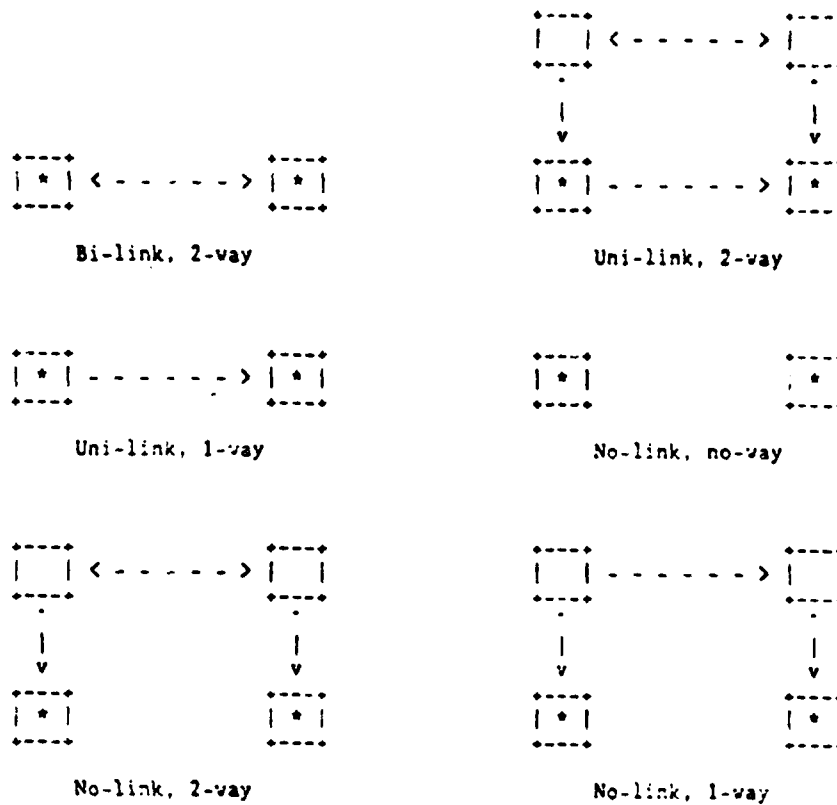
All 1-way routes are caused by uni-links but not all uni-links cause 1-way routes. Conventional transport protocol consider 1-way routes to be equivalent to no-way routes.

Figure 1 lists the possible combinations of link and network routing connectivities while Figure 2 shows an example of each possible combination.

LINK CONNECTIVITY		NETWORK ROUTING CONNECTIVITY		TYPE OF LINK AND NETWORK CONNECTIVITY
A can hear B	B can hear A	A has route to B	B has route to A	
Yes	Yes	Yes	Yes	Bi-link, 2-way
Yes	No	Yes	Yes	Uni-link, 2-way
Yes	No	Yes	No	Uni-link, 1-way
No	Yes	Yes	Yes	Uni-link, 2-way
No	Yes	No	Yes	Uni-link, 1-way
No	No	Yes	Yes	No-link, 2-way
No	No	Yes	No	No-link, 1-way
No	No	No	Yes	No-link, 1-way
No	No	No	No	No-link, no-way

FIGURE 1

ALL POSSIBLE COMBINATION OF LINK AND NETWORK CONNECTIVITY TYPES



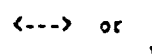
NOTE: PRs are represented by boxes:



PRs that demonstrate the possible link and network connectivity types are represented by:



Bi-links are represented by:



Uni-links are represented by:



FIGURE 2

EXAMPLES OF ALL POSSIBLE LINK AND NETWORK CONNECTIVITY TYPES

3. ADAPTATION OF CURRENT DARPA PACKET RADIO NETWORK PROTOCOLS

3.1 CURRENT DARPA PACKET RADIO NETWORK PROTOCOLS

The DARPA Packet Radio Network (PRNET) measures link connectivity and calculates routes in a distributed manner [JUBI 86], [JUBI 85], [WEST 82]. Normally host devices are attached to some of the packet radios (PRs), however routing packets to devices is omitted from this paper since it is the same as routing packets to the PRs that the devices are attached to. (Packets are routed to devices by routing across the PRNET to the PR that the devices are attached to.)

Figure 3 shows a typical PRNET. Each PR maintains two types of network information:

- * a neighbor table containing information about the link between itself and the PRs that it can directly receive from and transmit to,
- * a tier table containing network routing information.

3.1.1 PRNET LINK CONNECTIVITY ALGORITHM

Each PR determines that a link exists between it and another PR (called a neighboring PR) when it receives a packet. The packet header's transmitting PR ID is used to determine the neighboring PR ID. Note that due to the broadcast nature of the PRNET, PRs receive both packets addressed to them and overheard packets addressed to other PRs. The measured link quality from PR L to its neighbor PR M is the ratio of packets actually transmitted by PR L to the total number of packets actually received by PR M. This link quality (of the uni-link from L to M) is smoothed and hysteresis is applied to determine its good/bad rating. Periodically each PR transmits a control packet that lists the number of packets that it has transmitted and the receive link quality from each of its neighboring PRs. For example, if PR L transmits 80 packets in a given period of time and PR M receives 50 of them, then the uni-link quality from PR L to PR M is $5/8$, which is just high enough for a good rating. The bi-link to/from PR L from/to PR M is judged good enough to route packets over when both uni-links PR L to PR M and PR M to PR L are rated good.

3.1.2 PRNET TIER ROUTING ALGORITHM

The routing information in the PRNET is maintained in a distributed manner by each PR in its tier table. There is one tier table entry per PR in the network. Each entry contains the following information:

- * destination PR ID,
- * ID of the next-PR (i.e. neighbor PR) that is on the route to the destination PR,
- * length of the route to the destination PR (in tier levels), and
- * mechanisms for determining if the route is good or bad.

For the network shown in figure 3, PR L's tier routing table is shown in figure 4. The distance between a PR and its neighboring PRs is defined to be 1 tier level also called "1 hop" in the literature.

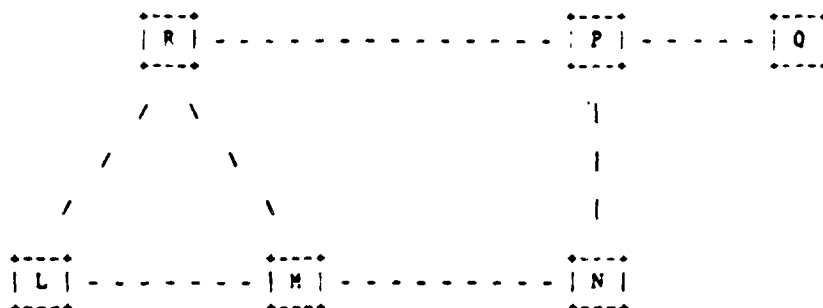


FIGURE 3
AN EXAMPLE PACKET RADIO NETWORK CONFIGURATION

PR TIER TABLE		
DESTINATION PR ID	ID OF NEXT-PR IN ROUTE	ROUTE LENGTH
L	L	0
M	M	1
N	M	2
P	R	2
Q	R	3
R	R	1

FIGURE 4
TYPICAL TIER ROUTING TABLE FOR PR L IN FIGURE 1

PRs maintain their tier routing tables as follows:

- (1) A PR always puts itself into its tier table with zero route length.
- (2) PRs periodically transmit a control packet containing each destination PR with its corresponding route distance. The receiving neighbor PRs can then use this information to update their tier table.
- (3) PRs can also update their tier tables from information in the routing header portions of overheard data packets.

The goal of the tier table is to always maintain the best information about how to get to destination PRs. Currently, the best route is defined to be the shortest route (in number of tier levels) with good bi-link connectivity between each PR on the route. Therefore the tier table can be updated only when certain conditions are met. The tier table is updated when the received packet in (2) or (3) above was received from a neighbor PR across a good bi-link and any one of the following conditions is also met:

- * there is no stored tier entry for that destination PR,
- * the route length plus one from the received packet is strictly less than the stored route length for that destination PR, or
- * the PR which transmitted the received packet is stored in the tier table as the next-PR in the route for that destination PR.

The update consists of creating a new tier entry if required and then setting the next-PR in the route equal to the PR that transmitted the received packet and setting the route length equal to the route length plus one from the received packet.

When the link quality to a neighbor PR (say the link from PR L to PR M) goes "bad", then all the routes in PR L's tier table which show PR M as the next-PR in the route are also considered to be bad. This signifies that PR M can no longer provide a reliable way for PR L to send packets to the destination PR and a new next-PR should be chosen. Thus, a new good route can be formed even if it is longer than the old bad one. The news of the bad tier information is distributed in the control packet with the good tier information. This spreading of bad route information and other mechanisms break up possible route loops and ensure that obsolete data does not override the up-to-date data.

3.1.3 PRNET PACKET FORWARDING ALGORITHM

A PR uses data from its tier table to route packets through the network. Some PR, say PR L, originates a packet for some destination, say PR N. The source PR looks up the destination entry in the tier table and copies the destination PR ID and next-PR in the route into the packet header. The source PR then transmits the packet to the next-PR in the route. The next-PR in the route receives the packet, determines that it is not the packet's destination, looks up the destination entry in its tier table, copies the next-PR in the route into the header, and transmits the packet on to its next-PR in the route. This process continues until the packet

reaches the destination PR. Figure 5 shows the forwarding of a packet from PR L to PR N. Mechanisms exist to stop packets from looping and detect packet duplicates.

PRs continue to retransmit a packet either until they hear an acknowledgement from the next-PR in the route or until they have transmitted the packet a predetermined number of times. The acknowledgement normally consists of overhearing the next-PR forwarding the packet on. For example, in figure 5, PR L overhears PR M transmit the packet to N. This overhead packet is an acknowledgement. For special cases, such as when the packet reaches the destination, a specific acknowledgement is transmitted back. For example, in figure 5, PR N transmits a specific acknowledgment back to PR M.

If a PR does not receive an acknowledgment within a certain number of transmissions, then it starts asking for help in finding an alternate route to the destination PR. Thus, in figure 3, if PR L does not receive an acknowledgment from PR M within three transmissions, then PR L asks for alternate routing help and PR R would help route the packet on to PR N. Mechanisms exist to stop packets from looping forever around the network via this alternate routing help and also to damp out packets traveling to the destination along multiple routes (i.e. the route PR L to PR M to PR N and the route PR L to PR R to PR P to PR N).

3.2 CHANGES TO SUPPORT UNIDIRECTIONAL LINKS WITHIN THE PRNET

Changes must be made in the link connectivity, tier routing, and packet forwarding algorithms to support unidirectional links. Currently the PRs will only use bi-links for routing purposes. This section shows how to use uni-links.

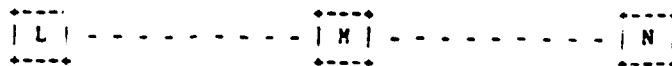
3.2.1 CHANGES TO PRNET LINK CONNECTIVITY ALGORITHMS

This section describes 4 methods of determining when a good uni-link exists between two PRs. Examples reference figure 3 where PR M is in a receive-only mode of operation and all of the other PRs are in a normal receive and transmit mode of operation.

3.2.1.1 LINK CHANGE 1

The change to the PRNET link connectivity algorithms suggested in this section would work for a PR that established normal bi-link with its neighbors and then changed to uni-links with its neighbors and with either 2-way or 1-way network routing connectivity.

A PR could come up and participate in the normal PRNET link connectivity algorithms until it has good bi-links with some number of PRs. Then this PR would tell some or all of its neighbor PRs that it is about to change to receive-only mode. These neighbor PRs would then freeze their good uni-link qualities to the receive-only PR until some future time. This future time could be quite far off if the radio connectivity is not expected to change, as for example, when the receive-only PR and its chosen set of neighbors are not



1.
PR L originates
packet for PR N.
PR L looks up the
tier entry for
PR N and finds
that PR M is the
next-PR in the
route to N.
PR L transmits the
packet to PR M.

2.
PR M receives
packet from PR L.
PR M determines
that it is not
the destination.
PR M looks up the
tier entry for
PR N and finds
that PR N is the
next-PR in the
route to N.
PR M transmits the
packet to PR N.
This transmission is
the acknowledgement
for PR L.

3.
PR N receives
packet from PR M.
PR N determines
that it is the
destination.
PR N transmits a
specific
acknowledgement
back to PR M.

FIGURE 3
FORWARDING A PACKET

mobile. If the receive-only PR expects to be mobile, then it could tell its neighbor PRs how long it expects to stay in connectivity before the uni-link quality goes bad. Also, if a neighbor PR moves, it would set its uni-link quality to bad. For example, PR M could tell PR L and PR N that it is about to go to receive-only mode. PR L and PR N would then freeze their uni-link quality to PR M at a good rating. Since PR R was not notified, it would continue to use the normal link algorithm and conclude that PR M is no longer a neighbor PR.

3.2.1.2 LINK CHANGE 2

The change to the PRNET link connectivity algorithms suggested in this section would work for a PR that has uni-links with its neighbors.

Suppose that a control center exists in the network capable of predicting the radio connectivity of the network by knowing the position of all the PRs in the network along with terrain data for the geographic area. Then the control center could tell some PR that it has a good uni-link to a neighboring receive-only PR. For example, a control center could tell PR L that it has a good uni-link to PR M. Then PR L would consider PR M to be a neighbor PR and set its uni-link to PR M at a good rating.

3.2.1.3 LINK CHANGE 3

The change to the PRNET link connectivity algorithms suggested in this section would work for a PR that has uni-links with its neighbors and also (in one sense) has only a 1-way network route to its neighbors (and in an external sense has some sort of 2-way network route.)

Suppose that there exists some communication channel external to the PRNET, for example Meteor Burst [GEOR 84]. Then the receive-only PRs could have some other means of communicating with the control center. The receive-only PR could determine that it has a good receive uni-link from some neighbor PR and relay this information to the control center. The control center would then relay this information on to the neighbor PR. For example, if PR M determines that it has a good receive uni-link from PR L and PR N, then PR M would relay this information to the control center and the control center would then relay this information on to PR L and PR N. PR L and PR N would then store the fact that they have a good transmit uni-link to PR M.

3.2.1.4 LINK CHANGE 4

The change to the PRNET link connectivity algorithms suggested in this section would work for a PR that has uni-links with its neighbors and also has 2-way network routes.

It is possible that some PRs could be in such a network environment (possibly due to transmission power imbalances) that one PR could hear another PR yet the converse is not true. Thus, there

is an uni-link from the first PR to the second. If there still exists some other path between the two PRs, then packets could still be routed from the second PR to the first PR. A distributed algorithm has already been published that describes how to spread uni-link connectivity information within such a network [GERL 83], although the algorithm would have to be modified slightly to account for the broadcast nature of packet radio.

3.2.2 CHANGES TO PRNET TIER ROUTING ALGORITHMS

The current tier routing algorithms would work in a network with uni-links with only minor changes. First, the definition of the tier route must change from meaning the best route with good bi-link connectivity between each PR on the route to meaning the best route with good uni-link connectivity toward the destination PR. Best route could either still imply shortest route without regard to whether the links are bi-link or uni-link, or it could be a function of route length and number of uni-links. For example, bi-links could have a weight of one and uni-links could have a weight of 3. Thus the best route would be the route with the smallest total weight. Tier routing information would still be updated as before, except that now the link to the next-PR in the route would only have to be a good uni-link instead of a good bi-link.

3.2.2.1 TIER CHANGE 1

The change to the PRNET tier routing algorithms suggested in this section would work for a PRNET that has all bi-links except for uni-links to PRs that have only 1-way network routes, i.e. except for PRs that are in a receive-only mode of operation.

This section assumes that one of the PRNET link connectivity changes 1-3 has been implemented. Thus the neighbors that have good transmit uni-links to the receive-only PR would list the receive-only PR as tier data at a distance of 1 tier level. Tier tables would then continue to get updated as before using the PROP mechanism.

3.2.2.2 TIER CHANGE 2

The change to the PRNET tier routing algorithms suggested in this section would work for a PRNET that has all uni-links or bi-links as long as all of the PRs have 2-way network routes.

This section assumes that the PRNET link connectivity change 4 has been implemented. Thus the neighbors that have good transmit uni-links to the receive-only PR would list the receive-only PR as tier data at a distance of 1 tier level. A distributed algorithm has already been published that describes how to spread tier routing information around a network with uni-links [GERL 83] although this algorithm does not work for a network with receive-only nodes. (Note however, that tier change 1 could be incorporated into this change so that PRs that keep a receive-only node permanently within their neighbor table would also keep this receive-only permanently in their tier table as well.)

3.2.3 CHANGES TO PRNET PACKET FORWARDING ALGORITHMS

PRs would continue to forward packets by using the tier table to look up the next-PR in the route. However, since the forwarding PR could not receive an acknowledgment back across a uni-link, the forwarding PR would have to transmit the packet a number of times, possibly a function of the (predicted) uni-link quality. In addition, the forwarding PR would no longer request alternate routing help when acknowledgments are not heard.

3.2.3.1 FORWARDING CHANGE 1

Adaptive Forward Error Correction (FEC) is being designed for the current bi-link forwarding protocols. The proposed adaptive FEC algorithms could be modified so that packets are transmitted across a uni-link using a strong FEC rate.

3.2.3.2 FORWARDING CHANGE 2

If there are several PRs with uni-links to the same receive-only PR, i.e. a PR that has only 1-way network routes toward it, then the probability of getting a packet to this receive-only PR would be improved if more of these neighboring PRs were to transmit the packet. Thus, each neighboring PR should know which other PRs also have uni-links to the same receive-only PR. This scheme would work as follows:

- (1) A packet is forwarded to the receive-only destination until it reaches a neighboring PR to the receive-only node.
 - (2) This neighboring PR then transmits the packet toward the receive-only destination and also sends a copy of the packet (with a flag set to indicate that no other copies should be made) to the other neighboring PRs.
 - (3) When a copy of the packet reaches another neighboring PR, the packet is transmitted toward the destination PR.
- Thus, the probability is increased that the receive-only PR will receive the packet.

4. PROBLEMS WITH END-TO-END ACKS AND SOME SOLUTIONS

Problems exist at the transport layer within the OSI Model [ZIMM 80] when there is no way for an end-to-end (ETE) acknowledgment to go from the destination back to the source. Probably the worst of these problems is providing a reliable delivery of packets. This problem does not automatically occur just because a network has uni-links, instead this problem occurs whenever there is one node that can send packets to another node in the network yet the second node cannot send any back, i.e. a node only has 1-way network routes. This problem can occur whenever the destination of a packet is in a receive-only mode or a network is partitioned into subnets so that there exist only one-way uni-links from one subnet to the other subnet(s). Some solutions to this problem are described below.

4.1. ETE ACK CHANGE 1

If a receive-only node could occasionally go from having 1-way network routes to having 2-way network routes and then go back to having 1-way network routes, then some transport application protocols could be modified to tolerate this occasional feedback. The transport and application protocols should require neither lengthy handshaking to open a connection nor connection keep alive packets. In addition, the protocols should be able to transmit packets for a long time before getting any acknowledgment indication. The receive-only node would store up the acknowledgments or non-acknowledgments until it gets a whole packet full or until some long period of time has elapsed, 1/2 hour for example, before transmitting the stored up acknowledgment information back to the source. While this scheme could be used to support file transport, it obviously does not support applications such as interactive computer terminals.

4.2 ETE ACK CHANGE 2

Some method of message store and forward could be implemented if a receive-only node were to repeat a pattern of going from 1-way network routes to 2-way network routes [NGUY 86]. For example, PR L could act as a message store and forward server for PR M which is in receive-only mode. The other PRs would route their packets for PR M to PR L. When PR L received a packet for PR M, it would forward the packet on to PR M as an unreliable datagram, store the packet in its memory, and provides the needed ETE acknowledgment back to the source. When PR M goes back to normal mode of operation, it would then request PR L to send it the packets that it had not received. Note that this message store and forward scheme asks quite a lot of a packet switch, and probably requires special hardware such as disk storage.

This message store and forward scheme is similar to the time-staged delivery networks for mail implemented by IBM and Tandem Computers [EDVA 86]. IBM's implementation is called Systems Network Architecture Delivery Systems (SNADS) and has been implemented in IBM's Distributed Office Support System (DISOSS). Tandem's implementation is called Transfer and is part of Tandem's

electronic-mail and facsimile transport products.

4.3 ETE ACK CHANGE 3

If no feedback to the transport or application protocol layers can be obtained from a receive-only node with 1-way routes, then a probabilistic retransmission scheme could be used. This scheme assumes that the probability of the receive-only node receiving a single datagram is known or could be predicted. For example, if there is a 50 % probability that the receive-only node will receive a single datagram and a packet is to be delivered to the receive-only node with 99.5 % reliability, then the packet would be retransmitted 8 times. This probabilistic retransmission scheme could be implemented either at the application, transport, or link layer.

- (1) Implementing the scheme at the transport layer requires knowing or predicting both the uni-link quality to the receive-only node and the probability that the datagram will be delivered from the source to the neighbor of the receive-only node. The source application layer would then retransmit the packet the required number of times.
- (2) Implementing the scheme at the link layer requires only knowledge of the uni-link quality, but violates layering. The application layer at the source PR would reliably deliver the packet to the application layer of the neighbor PR using some established transport protocol that relies on ETE acks. Then the neighbor PR would transmit the packet the required number of times to obtain the desired probabilistic reliability.

4.4 ETE ACK CHANGE 4

Transport level FEC could be used when the data that is to be sent to the receive-only node with 1-way network routes is so large that it must be fragmented into multiple packets. The data could be interleaved over the multiple packets and some form of FEC applied so that the receive-only node could still de-code the data even if it lost a packet or two of the message.

5. RELATED AREAS

5.1 MULTI-CHANNEL (INTERNET) OPERATION

A multi-channel network is made up of nodes that are connected via multiple types of channels. An example of a multi-channel network is an internet made up of several subnets using different types of channels. In other words the multi-channel network is the concatenation of several subnets using incompatible channels. Normally, subnets are assumed to be interconnected by bi-links, however subnets could be interconnected by uni-links as well.

Interconnecting a multiple access channel subnet to another subnet could be cost effective using receive-only nodes. For example, figure 6 shows an internet consisting of a PRNET and a SINGARS (SINGle Channel Ground/Air Radio Systems) network. The two subnets could be connected only by uni-links, yet there are 2-way network routes, the transport and above layers would not need to be modified. The link and network routing protocols would have to be modified as described above. If the cost of building nodes that could receive-only is less than half the cost of building nodes that can both transmit and receive, then the same amount of interconnection (i.e. number of links between the two subnets) could be realized for less total cost using receive-only nodes.

In addition, there are some internets where most of the data flows from one subnet to the other. These subnets could be connected by some number of bi-links and some number of uni-links to handle the excess of data flowing from one subnet into the other. Figure 7 shows an example remote sensor network where most of the data flows in from the remote sensors to processing centers. Thus, there need to be more links to allow data to flow into the LAN from the PRNET than there are to allow data to flow from the LAN into the PRNET. The use of PRs that can receive-only could be a cost effective way of providing these extra uni-links from the PRNET to the LAN. In addition, by adding PR M to the PRNET, the data from PR L and PR R could arrive at the LAN in a more timely fashion since there would be less PRs in the path to add forwarding delays. Note that 2-way network routes are needed to go from the LAN to the PRNET to provide feedback to the PRNET about the link connectivity and tier routing, and possibly to allow control commands to go from the processing centers to the remote sensors.

5.2 RECONSTITUTION OF NETWORKS

Networks are often required to reliably deliver packets, even in the face of failure of a network's resources. Network reconstitution is the act of restoring partial network capability following some failures, especially failures that partition the network into separate subnets.

The failure of a network's resources means failure of either a network node or link. Note that nodes or links can have partial or complete failures. Unfortunately for many current networks such as the PRNET and the ARPAnet, the remaining functionality of partially

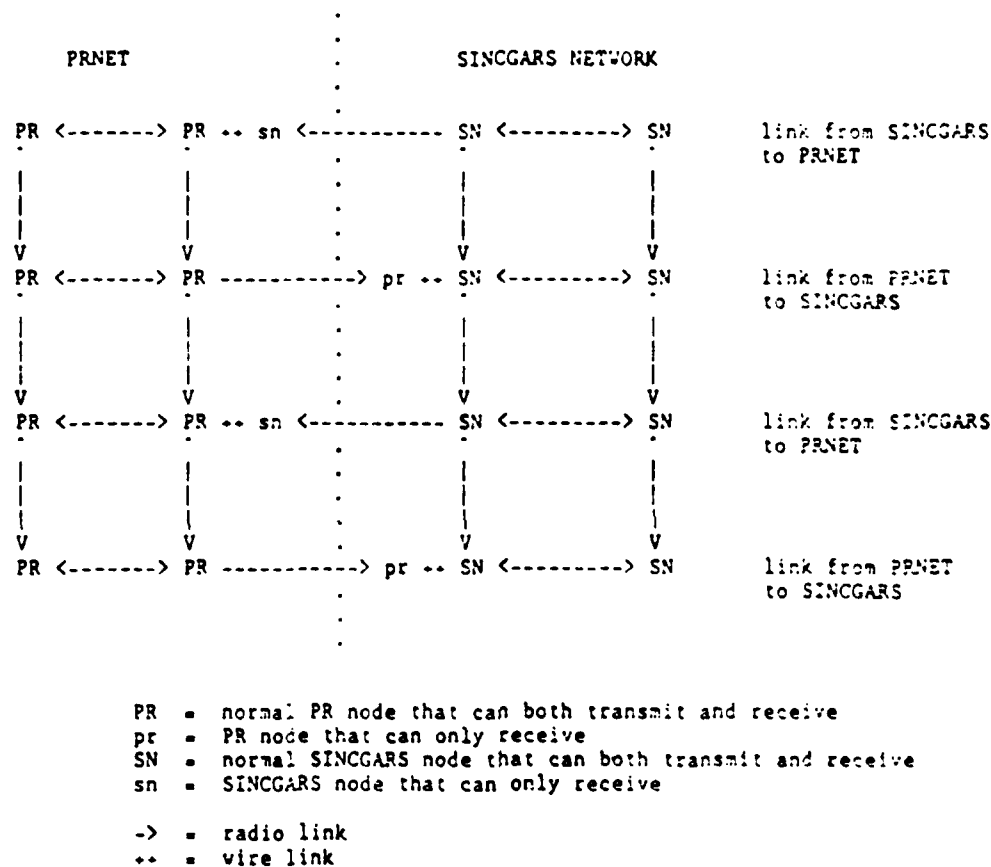


FIGURE 6
PRNET AND SINGGARS NETWORK

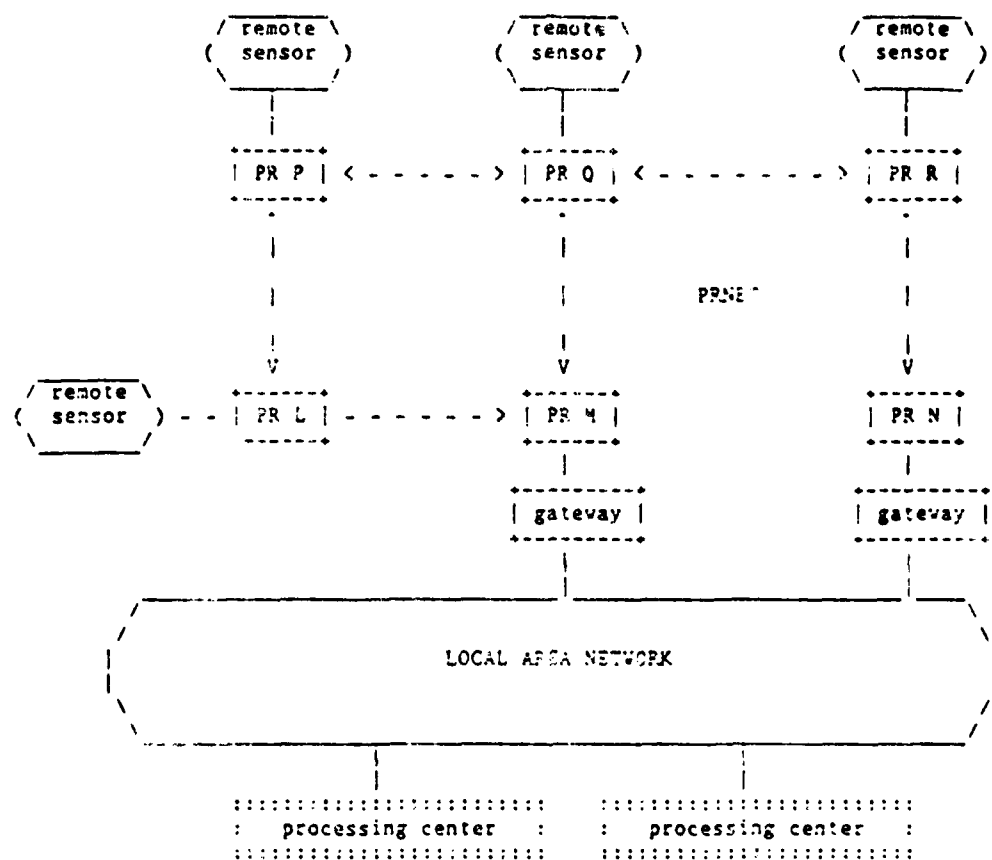


FIGURE 7
EXAMPLE REMOTE SENSOR INTERNET

failed nodes or links cannot be used. For example, if a PR fails so that it can only transmit or receive instead of being able to both transmit and receive, then it can no longer participate in the PRNET. Similarly links that are damaged so that they are now only uni-links instead of bi-links can no longer be used within the APPANet. If the PRNET and the ARPANet supported uni-links, then the networks would automatically be able to reconstitute themselves and use their partially failed links and nodes. Further reconstitution ability is provided if the networks could use 1-way network routes as well.

Experiments have been performed using the PRNET and the APPANet to simulate linking together partitioned islands of communications [DesB 84]. These experiments have used the flexibility of the PRNET protocols to adjust to changes in network connectivity. Thus the PRNET can detect partially and completely failed nodes and modify the tier routes to go around these failed nodes. Modifying the PRNET protocols to support uni-links would add robustness and allow partially failed nodes to still aid in routing packets.

In addition, the use of inexpensive receive-only PRs could be used as backups for normal PRs. For example, suppose that the PRNET is attached to the ARPANet via several gateways. Now let one of the PRs that is connected to the gateway have a complete failure. The failed PR could be quickly pulled out and a receive-only PR could quickly be inserted to at least allow data to flow from the PRNET to the APPANet. The receive-only PR would let the PRNET know that about its uni-link(s) by sending control packets to the PRNET via an existing 2-way network route via one of the existing gateways between the PRNET and the ARPANet.

5.3 MULTI-LEVEL SECURE NETWORKS

Multi-level secure networks have special problems when implementing a Trusted Computing Base (TCB) [CSC 83]. The *-property (star property) of the Bell-LaPadula security model means that a lower classified process can send data to a higher or equal classified process but that a higher classified process cannot send data to a lower classified process [SUMM 84]. Thus process A (operating at Secret) on host 1 could transmit packets to process B (operating at Top Secret) on host 2, however process B cannot acknowledge the packet since the acknowledgement could be used as an illegal data path, allowing the potential transfer of sensitive information from a higher to a lower level [WALK 85]. Process B on Host 2 then appears to be a receive-only node to process A on Host 1. One possible solution could be to use the transport protocol layer changes described above.

A solution to this problem has been published [WALK 85]. For example, process A described above could transmit packets reliably to a process B' (operating at Secret) on host 2, and process B' could transmit the packet on to process B (operating at Top Secret) with high reliability without requiring any acknowledgment since processes B and B' reside in the same host computer. This lack of acknowledgment from process B' to process B is equivalent to the transport layer performing a system call to send a message to an

application layer without requiring an acknowledgment back from the application layer.

Although the published solution satisfies common transport protocols, occasions could exist where processes might want to use transport protocols that support a receive-only mode. In other words, there may be times when process A on host 1 does not want any secret process on host 2 to be able to read the message. For example, suppose that Tom (who can log onto host 1 at Secret) wants to send a critical message about Dick (who can log onto host 2 at Secret) to Harry, Dick's supervisor (who can log onto host 2 at Top Secret). Since Tom wants to make sure that Dick cannot read this critical message, Tom would want to send the message directly to Harry, without ever letting the message be stored at a level that Dick could access. Sending Tom's message directly to Harry would be equivalent to sending the message to a receive-only mode.

5.4 NETWORKS THAT CONTAIN AREAS OF DENSE CONNECTIVITY

A problem with broadcast radio networks is adjusting the radio transmit power control so that an optimum amount of nodal connectivity is achieved. This is not a problem for uniformly distributed nodes, however, networks in the real world usually have areas with dense nodal connectivity and areas with sparse nodal connectivity. Networks characterized by large nodal connectivity have high levels of interference and low throughput [KLEI 78].

The current PRNET protocol has each PR transmit with the same default constant power level. Changes have been proposed so that the transmit power level would still be the same at each PR in the PRNET, although this PRNET wide transmit power level could be changed as the PRNET is running. Although a decrease in transmit power reduces the high connectivity in dense areas of the network, the same decrease in transmit power within the sparse areas of the network might isolate some nodes from the rest of the network. A better solution would be to decrease the transmit power level in the dense areas of the network while leaving it alone or increasing it in the sparse areas of the network. However, now that there are nodes transmitting with different power levels, the links between nodes would no longer be symmetrical and there would be some uni-links. Modifying the PRNET protocols as described in this paper would let the PRNET utilize these resultant uni-links, unless there were no paths in the reverse direction.

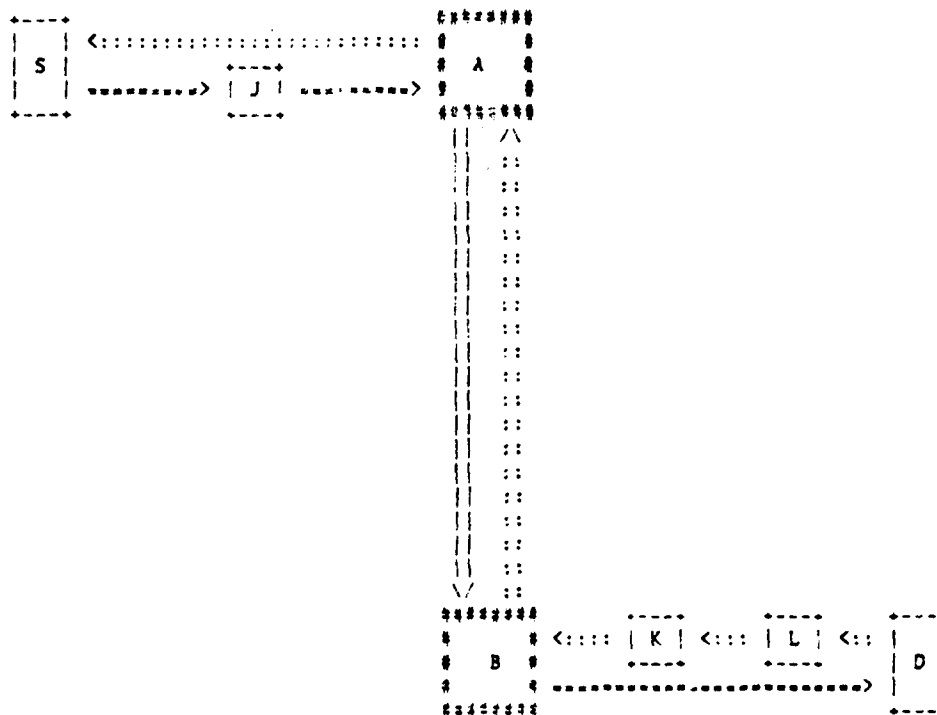
Changes have been proposed for dense neighborhoods so that the power level is not reduced but rather a PR will only keep a limited logical neighborhood [MILL 86]. This change solves the problem of a limited memory in PRs in which to store neighbor PR information. The change however can cause logical uni-links to occur. Thus although, the PR forwarding algorithms would not have to change, the PR tier routing algorithms would have to change as described in this paper.

5.5 NETWORK EXPRESSWAYS (BACKBONES)

When more and more nodes are added to networks, the average

number of nodes that packets have to travel through from source to destination increases. Normally this increases the average forwarding delay of packets and lowers the average throughput. Broadcast radio networks such as PRNET could increase the transmit power level of each PR so that they can be heard for a longer distance. Unfortunately, this increases the average connectivity in the network which increases the interference and lowers the throughput.

Network expressways or backbones are another solution to this problem. The network expressway would be made up of a few PRs that transmit at a high power level and thus could be heard for a long distance. The rest of the PRNET would transmit at a much lower power level and thus could not be heard as far away. Each PR that is part of the expressway would have a neighborhood of PRs transmitting at lower power that could hear it although they could not be heard. Thus there would be a uni-link from the expressway PRs to their neighborhood PRs. Reference figure 8. PR S in PR A's neighborhood wants to transmit a packet to PR D in PR B's neighborhood. PR S transmits the packet to PR J which transmits the packet to PR A. PR A then transmits the packet to PR B and PR B transmits the packet to PR D. If the expressway did not exist, then the packet would have gone through many more PRs and thus there would have been a larger delay.



NOTES:

PRs transmitting at low power are represented by boxes like

The range of PR transmitting at low power is
|----->

PRs transmitting at high power, thus implying that they are part of the network expressway are represented by boxes like * *

The range of PR transmitting at high power is
|----->

The path of the message being forwarded from the source PR (S) to the destination PR (D) is represented by ----->

The path of the end-to-end acknowledgement from the destination PR (D) to source PR (S) is represented by>

FIGURE 8
EXAMPLE NETWORK EXPRESSWAY

6. CONCLUSION

Current network routing protocols can be modified to allow packets to be routed across uni-links as well as bi-links and to destination nodes have 1-way network routes as well as 2-way network routes. The destination nodes may be in a receive-only mode of operation or may be part of a partitioned subnet. A receive-only node is still allowed, at a moment's notice, to transmit a packet into the network and either go back into the receive-only mode or the normal mode of operation. Adaptations to the current DAPPA Packet Radio tier routing were shown. Problems and some solutions to the problem caused by no end-to-end acks were also described. These modified network routing, transport, and application protocols were shown to be of use in other areas such as multi-channel networks (internets), network reconstitution, multi-level secure networks, networks that contain areas of dense connectivity, and network expressways (backbones).

REFERENCES

- [CSC 83] DoD Security Computer Center, "Department of Defense Trusted Computer System Evaluation Criteria", CSC-STD-001-83, Aug. 1983.
- [DesB 84] Gregory DesBrisay, Boyd Fatt, and Michael Frankel, "Airborne Communications Reconstitution Experiments", IEEE EASCON '84, pp. 311-319.
- [EDWA 86] Jeri Edwards, "Time-staged delivery networks save time, enhance productivity", Data Communications, Feb. 1986, pp. 147-150.
- [GERL 83] M. Geria, L. Kleinrock, and Y. Afek, "A Distributed Routing Algorithm For Unidirectional Networks", IEEE GLOBECOM '83, Dec. 83, Vol. 2, pp.654-658.
- [GEOR 84] Robert A. George and Harris F. Rush, "Meteor Burst Systems", Defense Science 2002+, Dec. 1984, pp. 40-45.
- [JUBI 85] John Jubin, "Current Packet Radio Network Protocols", IEEE INFOCOM '85, Mar. 1985, pp. 86-92.
- [JUBI 86] John Jubin and Janet Tornow, "The DARPA Packet Radio Network", to be published in IEEE Proceedings, Nov. 1986.
- [KLEI 78] L. Kleinrock and J. Silvester, "Optimum Transmission Rate For Packet Radio Networks Or Why Six Is A Magic Number", IEEE NTC '78, Dec. 1978, pp. 4.3.1-4.3.5.
- [MILL 86] Bill C. Miller, "Limiting Logical P2 Neighborhood Size", SNTN 43, Jun. 1986.
- [NGUI 86] Binh Nguyen and Raphael Rom, "Communication Services Under EMCON", ACM SIGCOM '86, Aug. 1986.
- [POST 81] J. Postel, "Transmission Control Protocol", RFC-793, USC/Information Sciences Institute, Sep. 1981.
- [SUMM 84] R. C. Summers, "An Overview of Computer Security", IBM Systems Journal, Vol. 23, No. 4, 1984.
- [WALK 85] Stephen T. Walker, "Network Security Overview", IEEE Proceedings of the Security and Privacy Conference, Apr. 1985, pp. 62-66.
- [WEST 82] Jim Westcott and John Jubin, "A Distributed Routing System for a Broadcast Environment", IEEE MILCOM '82, Oct. 1982, Vol. 3, pp. 10.4.1-10.4.5.
- [ZIMM 80] A. Zimmermann, "OSI Reference Model", IEEE Transactions on Communication, Apr. 1980, pp. 425-432.

SRMTN DISTRIBUTION LIST

Bolt Beranek and Newman, Inc. (2)
ATTN: Greg Lauer
10 Moulton Street
Cambridge, MA 02238

Defense Advanced Research (2)
Projects Agency/ISTO
ATTN: Dennis Perry
1400 Wilson Boulevard
Arlington, VA 22209

MIT Lincoln Laboratories
ATTN: Richard Ralston
Box 73, Room C-117
Lexington, MA 02173

Naval Warfare Systems Command
ATTN: Barry Hughes
Code 611
Washington, D.C. 20363-5100

Polytechnic Institute
ATTN: Bob Boorstyn
333 Jay Street
Brooklyn, NY 11201

SRI International (2)
ATTN: Janet Tornow
Office EJ131
333 Ravenswood Avenue
Menlo Park, CA 94025

SRI International
ATTN: Mike Frankel
Office EJ347
Menlo Park, CA 94025

UCLA
Computer Science Dept.
ATTN: Leonard Kleinrock
3732 BH
Los Angeles, CA 90024

USC-ISI
ATTN: Jon Postel
4676 Admiralty Way
Marina Del Rey, CA 90292-6695

Naval Research Lab
ATTN: J.E. Wieselthier
Code 7520
Washington, D.C. 20375

Paul Sass
US Army CECOM
ATTN: AMSEL-CCM-AF-2
Fort Monmouth, NJ 07703

Hazeltine Corporation (2)
Building 1
ATTN: Jeff Markel
Cuba Hill Road
Green Lawn, NY 11740

National Security Agency
ATTN: S743, S. Spano
Fort George Meade, MD 20755

Naval Ocean Systems Center
ATTN: Dan Leonard
271 Catalina Boulevard
San Diego, CA 92152

Rockwell International (2)
Collins Defense Communications
ATTN: John Jubin
M/S 460-340
3200 E. Renner Road
Richardson, TX 75081

Horst Clausen
Electrical and Computer Engineer
University of Kansas
1013 Learned Hall
Lawrence, KS 66045-2229

Stanford University
Computer Systems Laboratory
ATTN: Fouad Tobagi
Stanford, CA 94305

University of Illinois
CSL
ATTN: Mike Pursley
1101 W. Springfield Road
Urbana, IL 61801

Rome Air Development Center
ATTN: Dan McAuliffe
DICEF-Section (DCLS)
Griffiss AFB, NY 13441

Linkabit Corporation
ATTN: Richard Binder
3033 Science Park Road
San Diego, CA 92121

[15 Aug 86]



1987 COMMUNICATION NETWORK
MANAGEMENT WORKSHOP

NETWORK MANAGEMENT FOR SPACE

AT
HARRIS CORPORATION
GOVERNMENT SYSTEMS SECTOR

BY
A. R. MARTIN



HARRIS
Government Systems, Inc.

NETWORK MANAGEMENT

- **Outline**
 - **Background and perspective**
 - **Generic problem description**
 - **Supportive programs at Harris**
 - **Future directions**



HARRIS

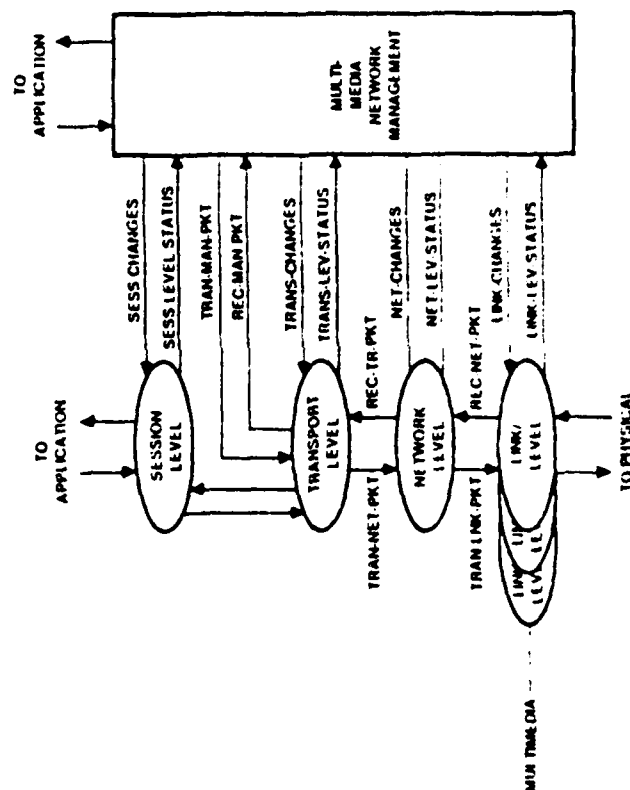
United Communications Corporation

NETWORK MANAGEMENT

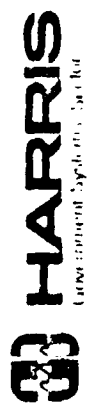
- Background and Perspective
 - Point-point, fixed networks, e.g., ARPANET
 - Broadcast, quasi-static networks, e.g., PR Network
 - Point-point, dynamic networks
 - Point-point multimedia dynamic networks

“Current research emphasis is on these 3rd and 4th generation network models”

Functional interfaces



63719 04(M)

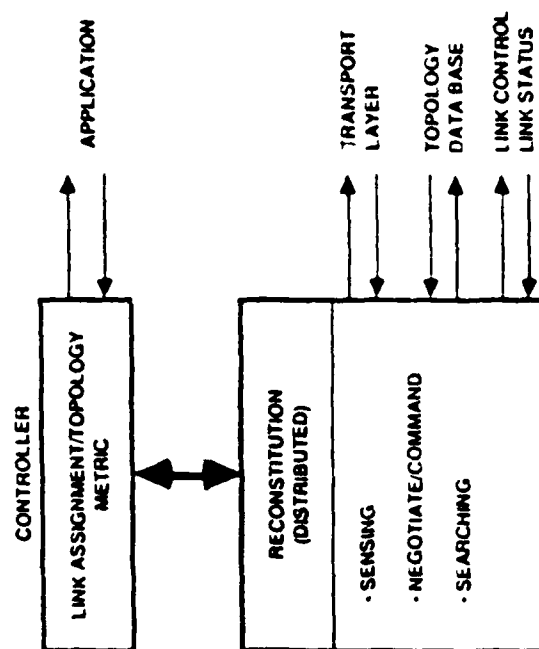


NETWORK MANAGEMENT Generic Problem

Functional decomposition

- Reconstitution (link assignment)
- Topology update (synchronization)
- Adaptive routing
- Flow control

**FUNCTIONS AND
INTERFACES-RECONSTITUTION**

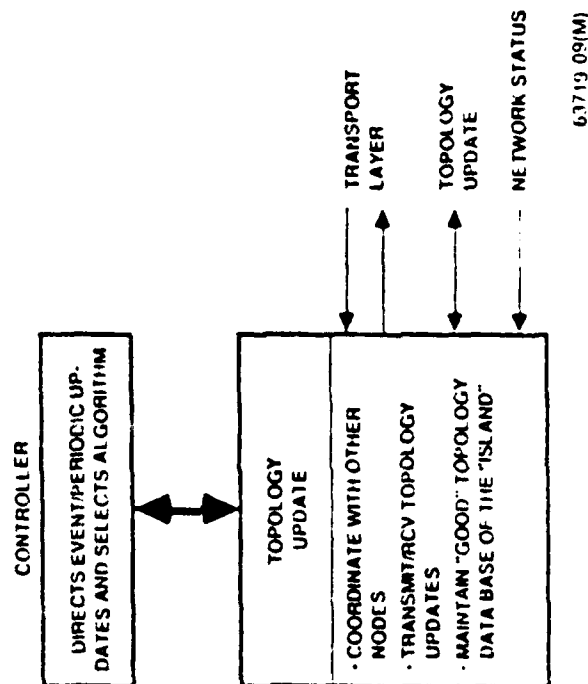


63/19 08(M)

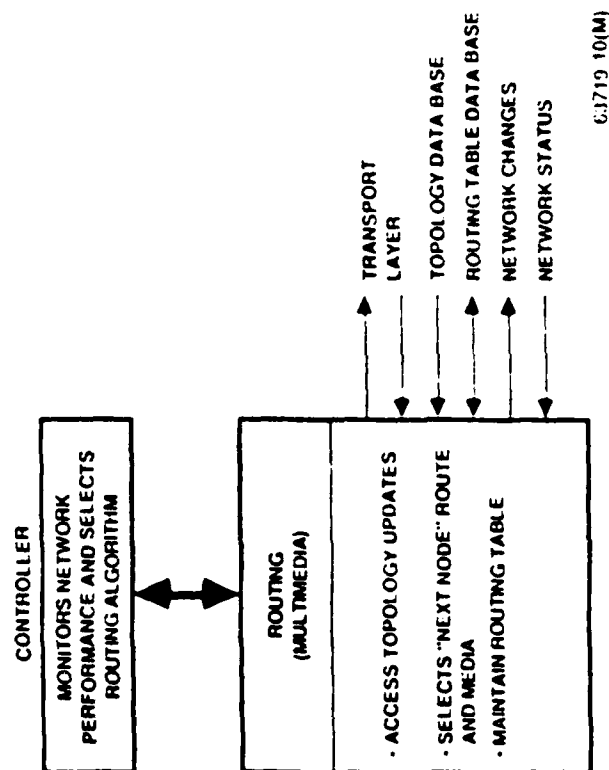


NETWORK MANAGEMENT GENERIC PROBLEM

FUNCTIONS AND INTERFACES-TOPOLOGY UPDATE



**FUNCTIONS AND
INTERFACES-ADAPTIVE ROUTING**

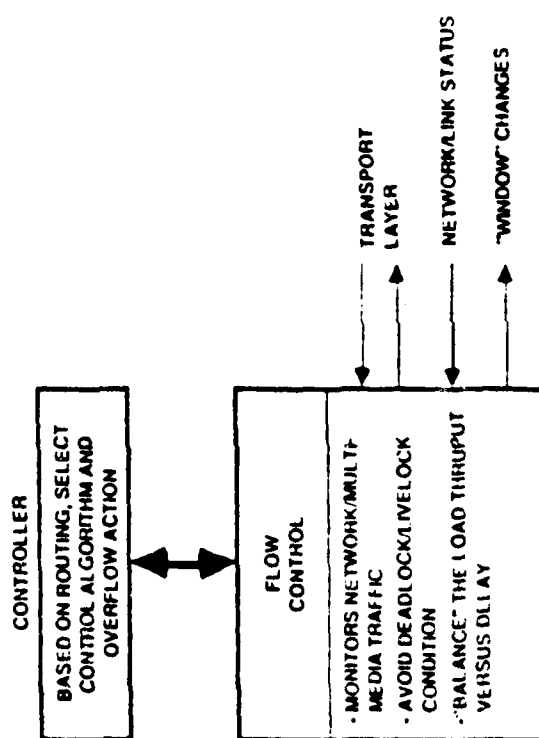




HARRIS
Government Systems, Inc.

NETWORK TECHNOLOGY GENERIC PROBLEM

FUNCTIONS AND INTERFACES-FLOW CONTROL



63719 11(M)



HARRIS
Government Systems, Inc. for

**NETWORK MANAGEMENT
GENERIC PROBLEM**

Applications/Scenarios

- Space Defense Initiative
- Multiple Satellite System
- Air Defense Initiative
- Space Systems Internetting
- Air Warfare C³I
- Unified Network Technology
- etc.



HARRIS
Government Systems Division

NETWORK MANAGEMENT HARRIS PROGRAMS

BM/C³ Communication Network Design*

- Customer: RADC/DCC, Tom Blake
- Program: 13 MY 30 MO program to develop methodology/design and simulation of BM/C³ communications network
- Output: contract CDRL's including methodology handbook, specification network design, and simulation results

*Previous program—"Communication Networking for SDI Application," RADC Final Report, April 1987 by Harris GASD

Related program—"Earth Space Links," Study for RADC by Harris GCSD

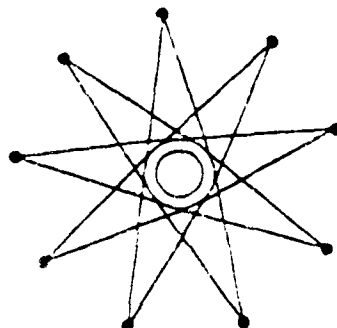
BM/C³ Communication Network Design (Continued)

- Evaluation/simulation of
 - Three topology link assignment algorithms
 - ADNMS algorithm
 - K-nearest neighbor
 - Grid constrained
 - Six adaptive distributed routing strategies
 - ARPANET (new)
 - PRNET hierarchical
 - ADNMS (Harris)
 - Codex routing
 - Other
 - Minimum hop
 - Standard protocols—HDLC, TCP/IP, TP/IP, SDLS
- Simulation models
 - KEWSTAR and BOOSTAR engagement
 - GENESIS network simulation

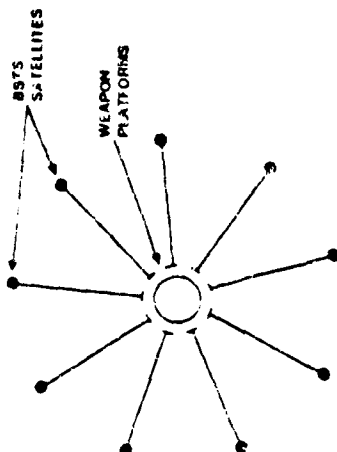


NETWORK MANAGEMENT HARRIS PROGRAMS

BM/C³ Communication Network Design



**CASE 1:
BSTS
BROADCASTS
TO WEAPON
PLATFORMS**



**CASE 2:
POINT-TO-
POINT LINKS
BETWEEN
BSTS AND
WEAPON
PLATFORMS**

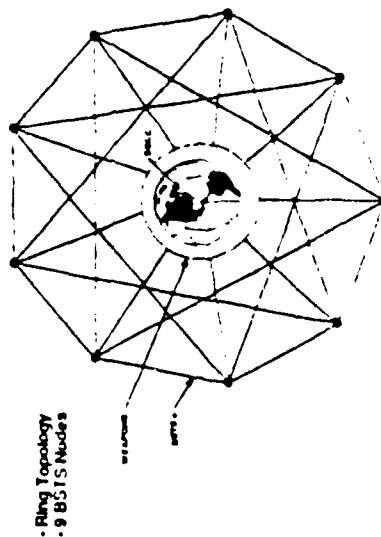
- SIMPLER DOWNLINK COMM

- JAM RESISTANT
- POSSIBLE LASER LINKS
- LOWER POWER
- LP
- NO (UP/LINK) CONTENTION

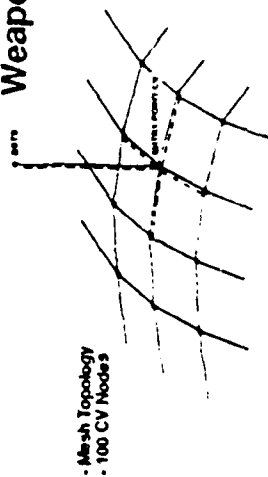
1/7/9 13(M)

BM/C³ Communication Network Design

BSTS NET



Weapon Net



811017-100



NETWORK MANAGEMENT HARRIS PROGRAMS

**ADNMS: Adaptive Distributed Network Management System,
Contract N00014-86-C-2056**

- Customer: NRL Information Technology Division; Steve McBurnett, Ed Althouse
- ADNMS goals: establish technical feasibility of SDI survivable communication networks by developing/testing critical network management algorithms
- Schedule: Phase 1—20 Feb 1986 to 20 Feb 1987, Phase 2/ECP start 20 Feb 1987
- Outputs: Contract CDRL's (e.g., Algorithm Research Report); Papers*

*Cain, J. B., et al., "A distributed Link Assignment Algorithm for SDI Networks" and Cain, J. B., et al., "A 'Near-Optimum' Multiple Path Routing Algorithm for SDI Networks")

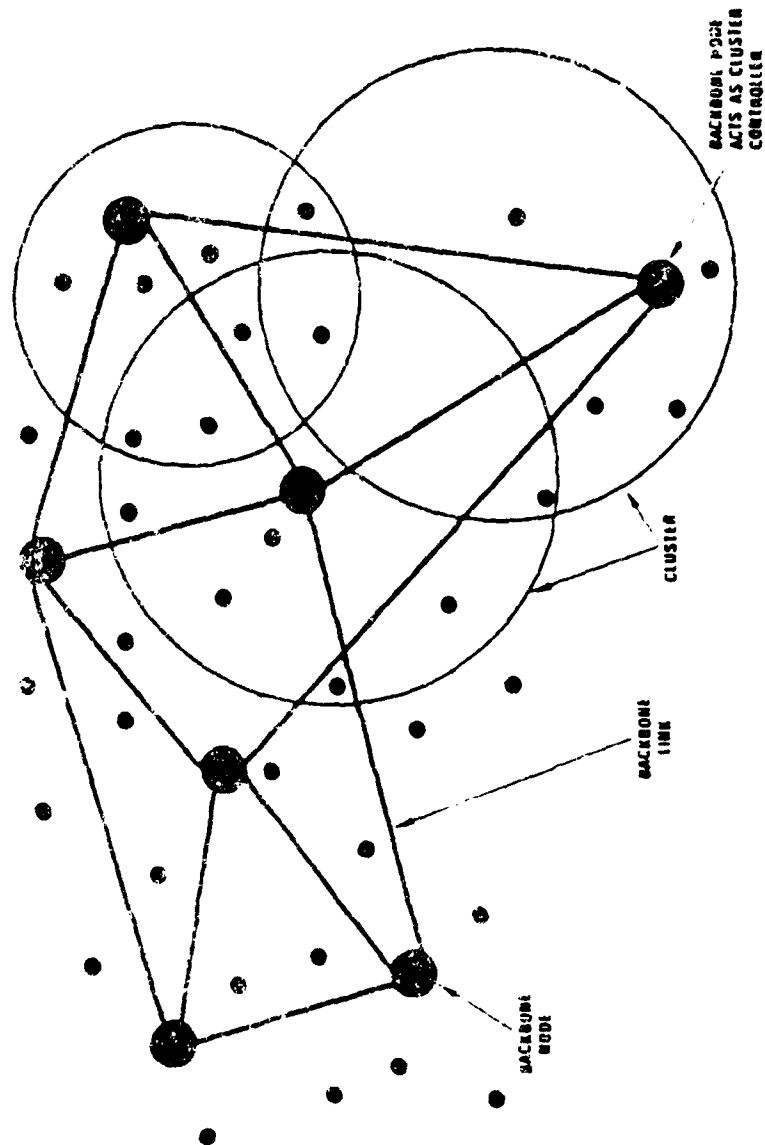
ADNMS (continued)

- **Status**
 - Designed and implemented initial link assignment/reconstitution and adaptive routing algorithms
 - Tested algorithms using Harris-designed simulator
- **Plans**
 - Assess benefits of parallel processing for ADNMS algorithms
 - Refine algorithms
 - Develop/evaluate large network algorithms



NETWORK MANAGEMENT HARRIS PROGRAMS

ADNMS Architecture

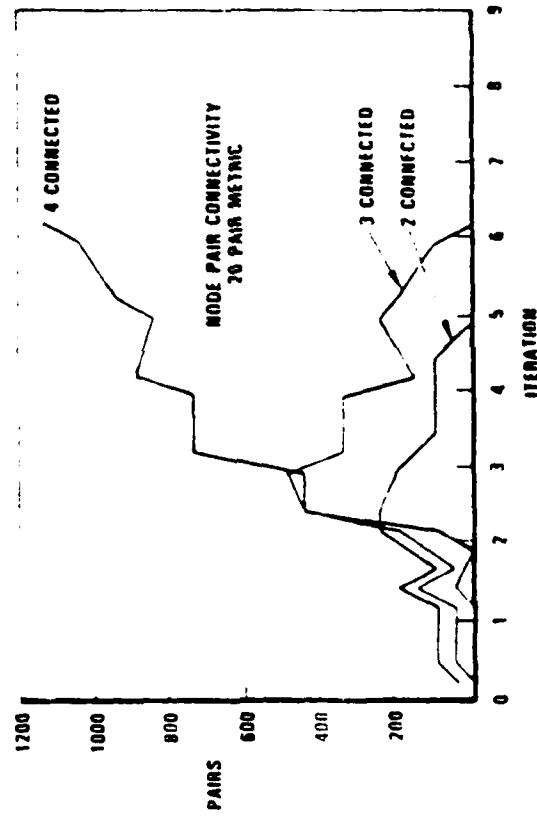




HARRIS
Communication Systems Corporation

NETWORK MANAGEMENT HARRIS PROGRAMS

Link Assignment Algorithm Example





HARRIS

Communications Systems Division

NETWORK MANAGEMENT

Future Directions

- More point-point versus broadcast applications
- Beam hopping versus multiple beam tradeoffs
- Continued reconstitution algorithm work
- Network security requirements/models/designs
- More simulation and testing



NETWORK MANAGEMENT HARRIS PROGRAMS

IR&D

- Stressed Communications (Project 4165)
 - Parallel processing simulation of HF network
 - Multimedia models and algorithms
 - "Large" HF network designs
- Survivable Communications (Project 4299)
 - Communication vulnerability (dependent node failures)
 - Simulation development (GENESIS)
 - Routing algorithm research; viz. DABF split flow versus Gallagher's
 - Emulation design
- Survivable Space-based Network Management (Project 4001)

MARTIN MARIETTA

INFORMATION & COMMUNICATIONS SYSTEMS

Information Network Laboratory

(INL)

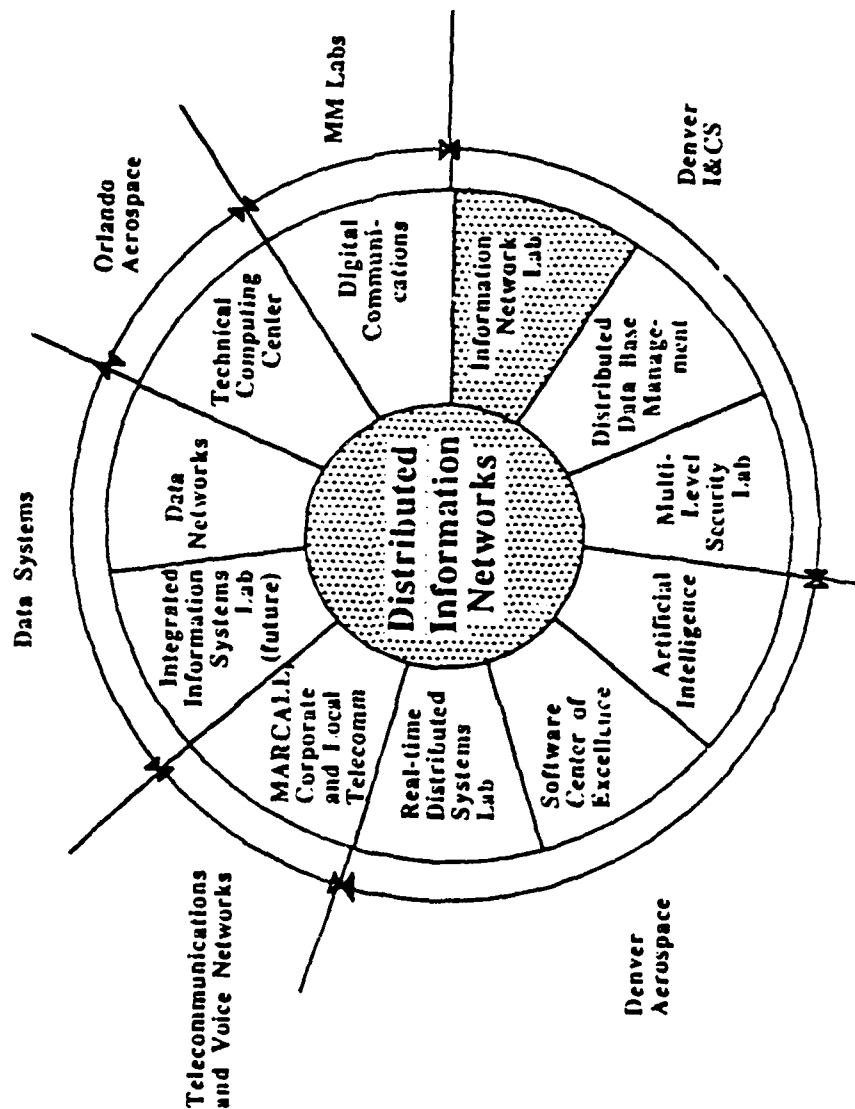
By Rich Wiley

INFORMATION NETWORK LABORATORY

MARTIN

INFORMATION & COMMUNICATIONS SYSTEMS

THE INL IS THE STRATEGIC TECHNOLOGY LEAD FOR NETWORK DESIGN AND THE DEVELOPMENT OF AN INTEGRATED INFORMATION SYSTEM ENVIRONMENT



INFORMATION NETWORK LABORATORY



INFORMATION & COMMUNICATIONS SYSTEMS

INL PURPOSE AND APPROACH

PURPOSE

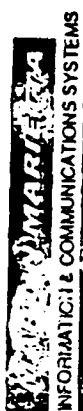
- PROVIDE INFORMATION NETWORKING EXPERTISE
- INTEGRATE/COORDINATE TECHNOLOGY APPLICATIONS ACROSS CORPORATE ENTITIES
- CREATE COMPETITIVE ADVANTAGE
 - Risk reduction
 - Performance optimization

APPROACH

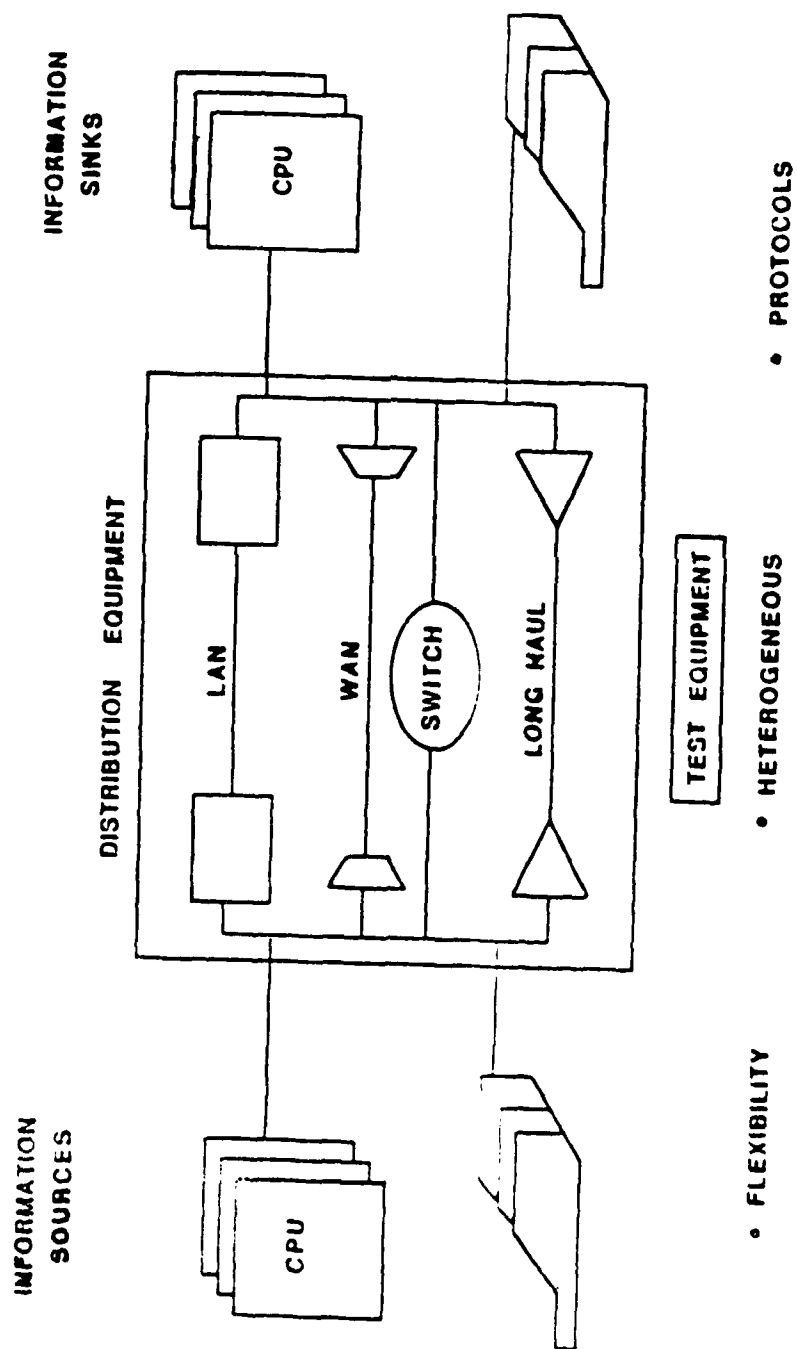
- DEDICATED FACILITY AND PERSONNEL
- SUPPORT COMPLETE LIFE-CYCLE OF SYSTEMS
- ENCOMPASS HETEROGENEOUS EQUIPMENT AND PROTOCOLS
- EMPHASIZE INTEGRATED NETWORK MANAGEMENT
- DEVELOP EXPERTISE THRUSTS TO RESPOND TO SPECIFIC CORPORATE ENTITIES NEEDS

* Local Issues (e.g., MMDA, MMD3-CRLA:IDO, DENVER I&CS,
BALTIMORE-AEROSPACE)

INFORMATION NETWORK LABORATORY



Hardware Architecture



Protocols Compared via ISO Model

APPL					APPLICATION		
PRES	TELNET or FTP		VIRTUAL TERMINAL PROTOCOL		NET MGMT		
SESS					NET APPL		
TRANS	TRANSPORT CONTROL PROTOCOL		SPP		SESSION PROTOCOL		
INT					END COMMUNICATION PROTOCOL		
NTWK	INTERNET PROTOCOL		INTERNET DATAGRAM PROTOCOL				
LINK	IEEE 802.3 (ETHERNET)		IEEE 802.3 (ETHER- NET)	PACKET LEVEL	ROUTING		HDLC/ SDLC
PHYS					DDCMP		IEEE RS232C IEEE RS449 ANSI V.35
					IEEE RS232C		
					X.25		DECNET
					TCP/IP		HDLC/SDLC

AD-A195 374

PROCEEDINGS OF THE COMMUNICATIONS NETWORK MANAGEMENT
WORKSHOP (1987) HELD. (U) ROME AIR DEVELOPMENT CENTER
GRIFFISS AFB NY J J SALERNO ET AL. NOV 87

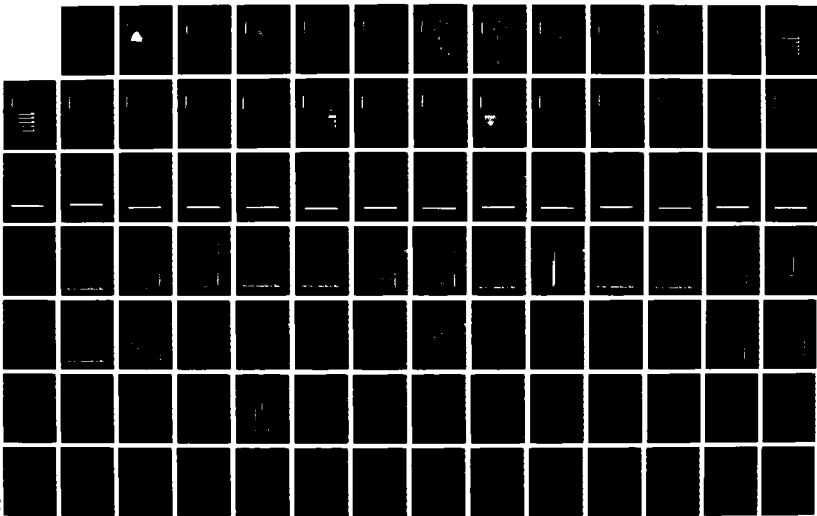
475

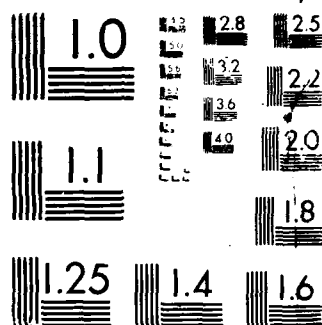
UNCLASSIFIED

RADC-TR-87-231

F/G 25/4

NL



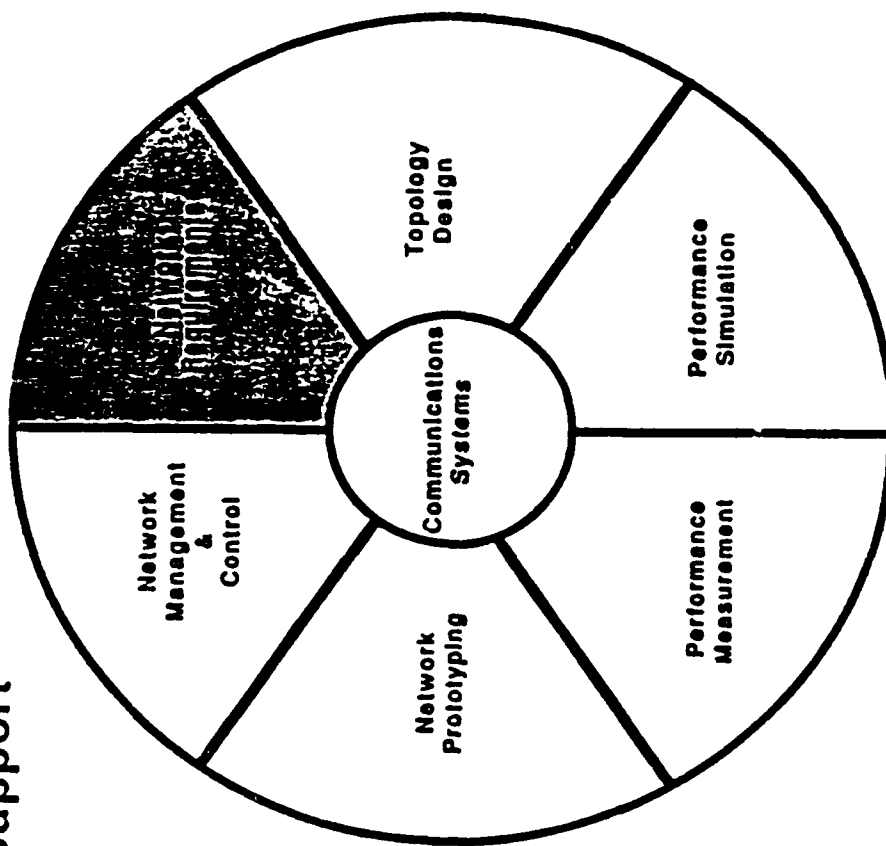


MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

INFORMATION NETWORK LABORATORY

MARTIN MARIETTA
INFORMATION & COMMUNICATIONS SYSTEMS

Life Cycle Support



Progress in Functional Requirements Decomposition

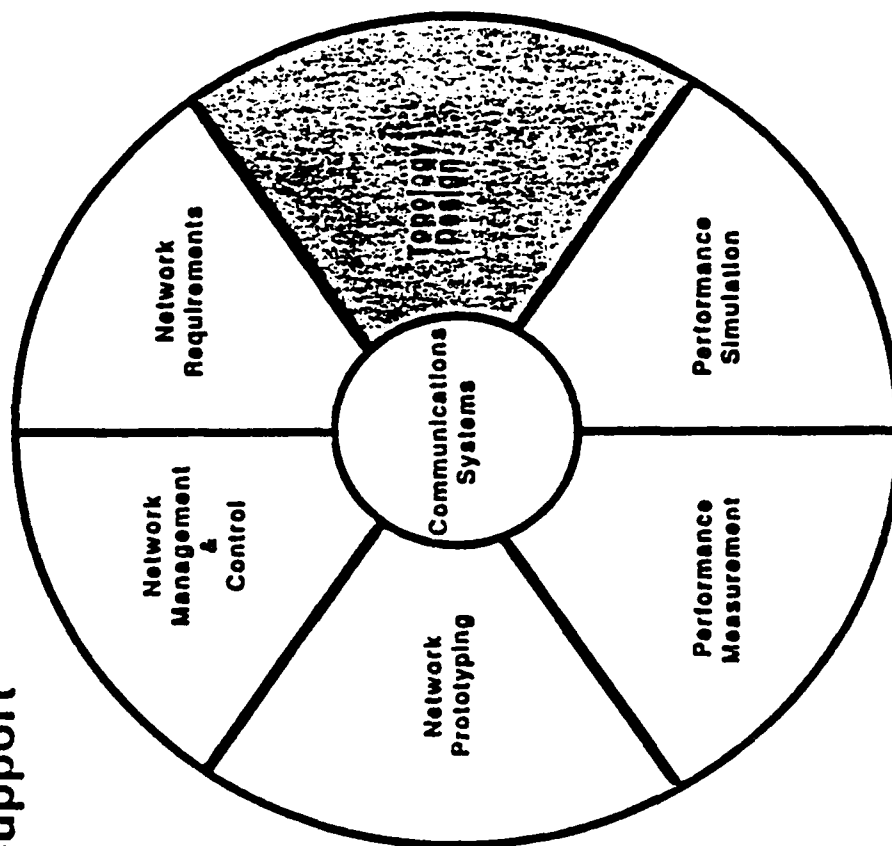


INFORMATION NETWORK LABORATORY

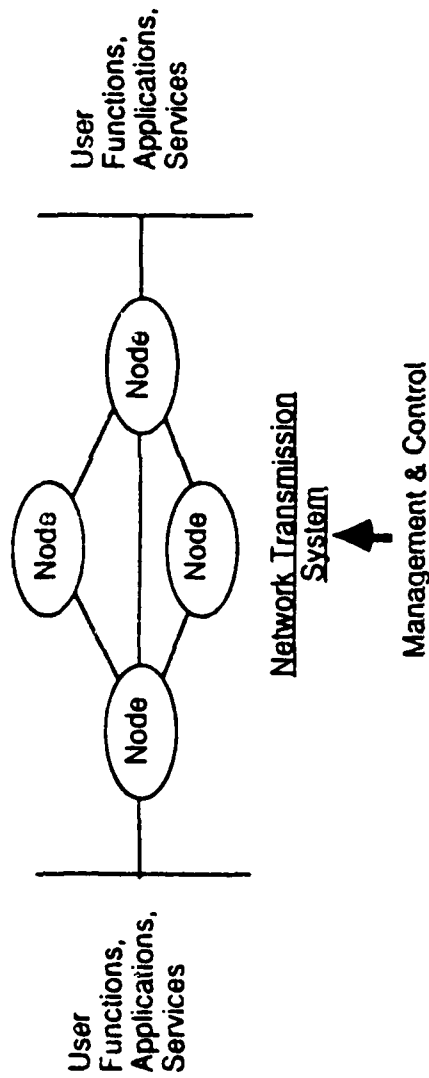
MARTIN MARIETTA

INFORMATION & COMMUNICATIONS SYSTEMS

Life Cycle Support



THE TOPOLOGY PROBLEM



OPTIMAL CONFIGURATION(S) OF NODES AND LINKS TO MEET

USER REQUIREMENTS FOR:

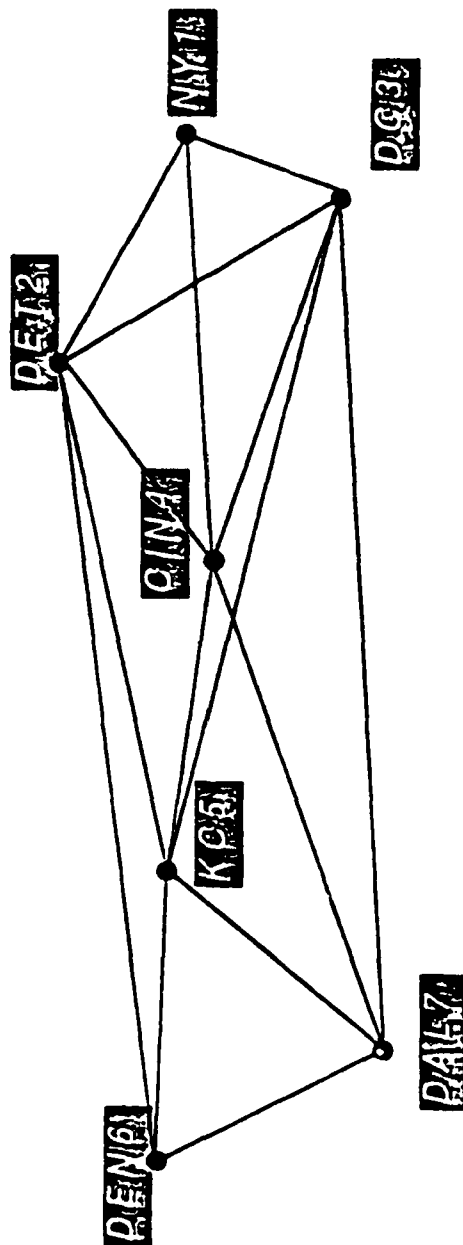
- THROUGHPUT / CAPACITY
- RESPONSE TIMES / DELAYS
- MESSAGE CLASSES
- TRAFFIC MATRICES
- ROUTING
- EXISTING NETWORK ELEMENTS

NETWORK TOPOLOGY DESIGN MODEL CAPABILITIES

- SOFTWARE TOOL FOR PACKET SWITCHED NETWORK DESIGN
- USER FRIENDLY I/O INTERFACE WITH IBM PC/XT COLOR GRAPHICS
- CONCISE EASY TO READ REPORT (COLOR MONITOR OR LISTING)
 - LINKS SELECTED BY THE MODEL
 - NODES SELECTED BY THE MODEL
 - EXPECTED TRAFFIC ON SELECTED LINKS AND THROUGH SELECTED MODEL
 - EXPECTED TRAFFIC ON EACH ROUTE
 - CONNECTIVITY OF EACH INDIVIDUAL ROUTE
 - ACTUAL COST FOR EACH LINK CHOSEN
 - ACTUAL COST FOR EACH NODE CHOSEN
 - TOTAL COST BOTH FIXED AND VARIABLE FOR THE MODELS CONFIGURATION
- CAN BE USED TO MODIFY AN EXISTING NETWORK OR CREATE A NEW DESIGN

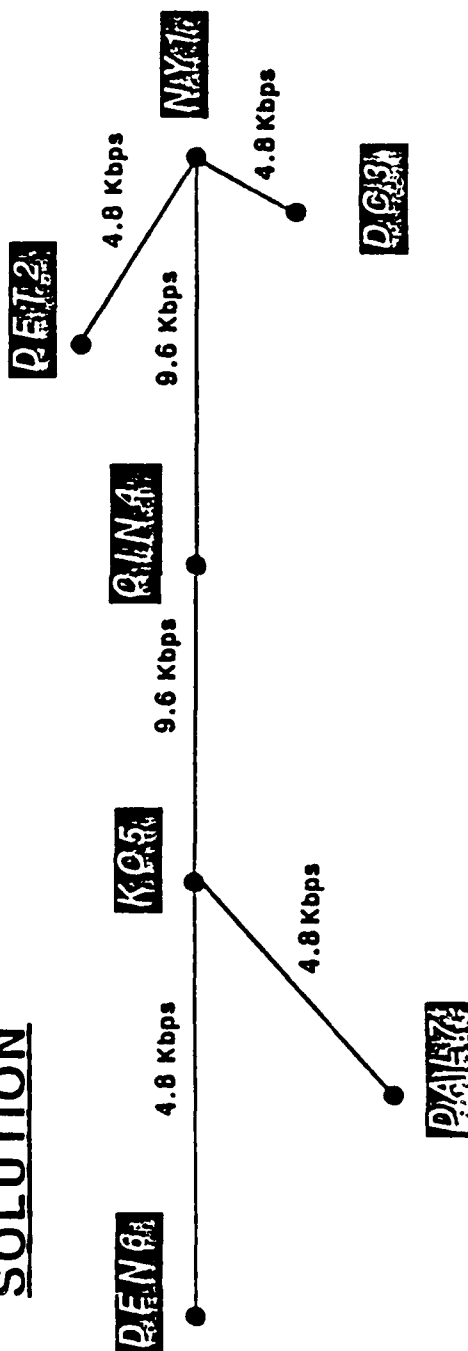
Network Topology Optimization

SEVEN NODE EXAMPLE DATA



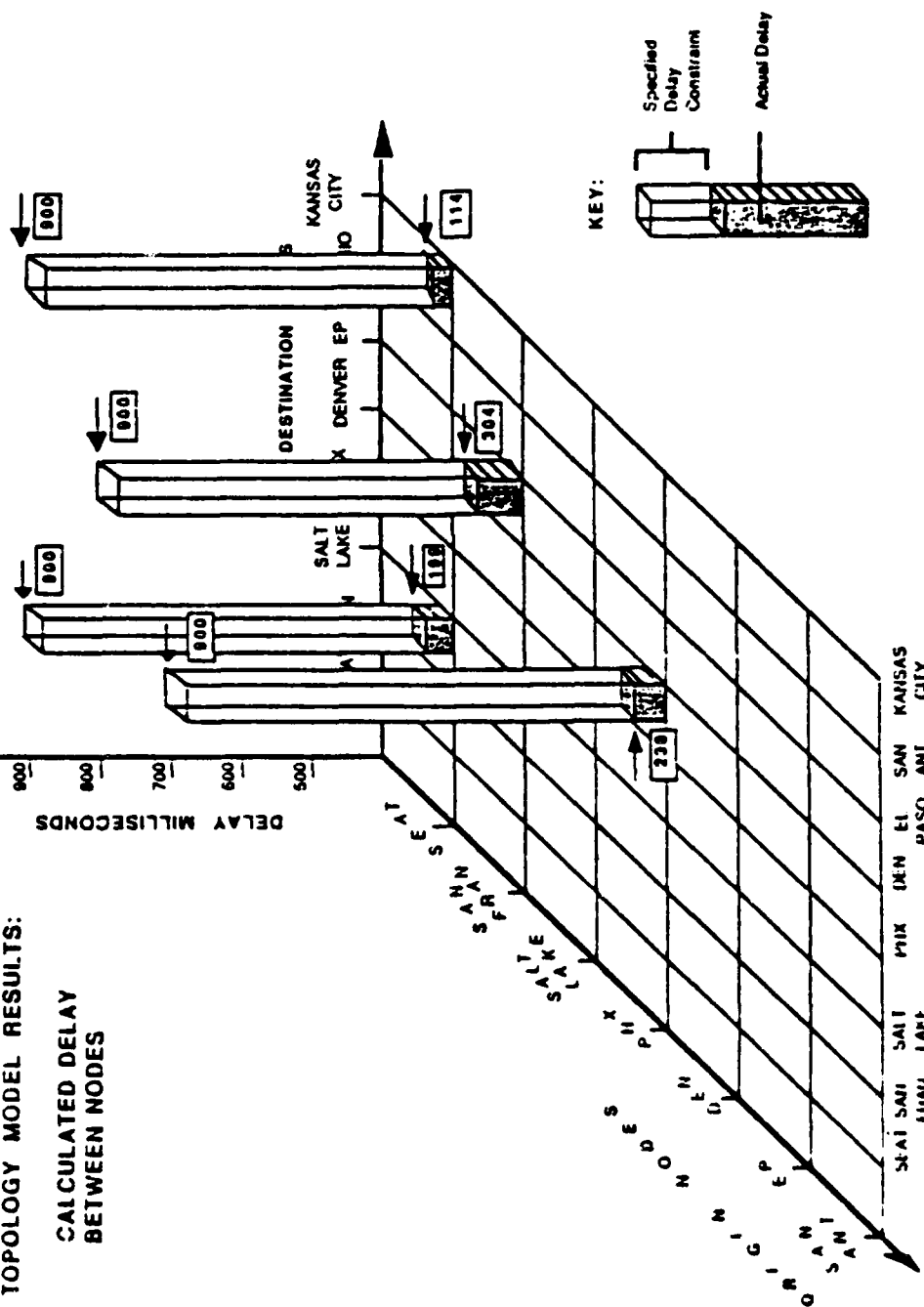
Network Topology Optimization

SEVEN NODE EXAMPLE SOLUTION



TOPOLOGY MODEL RESULTS:

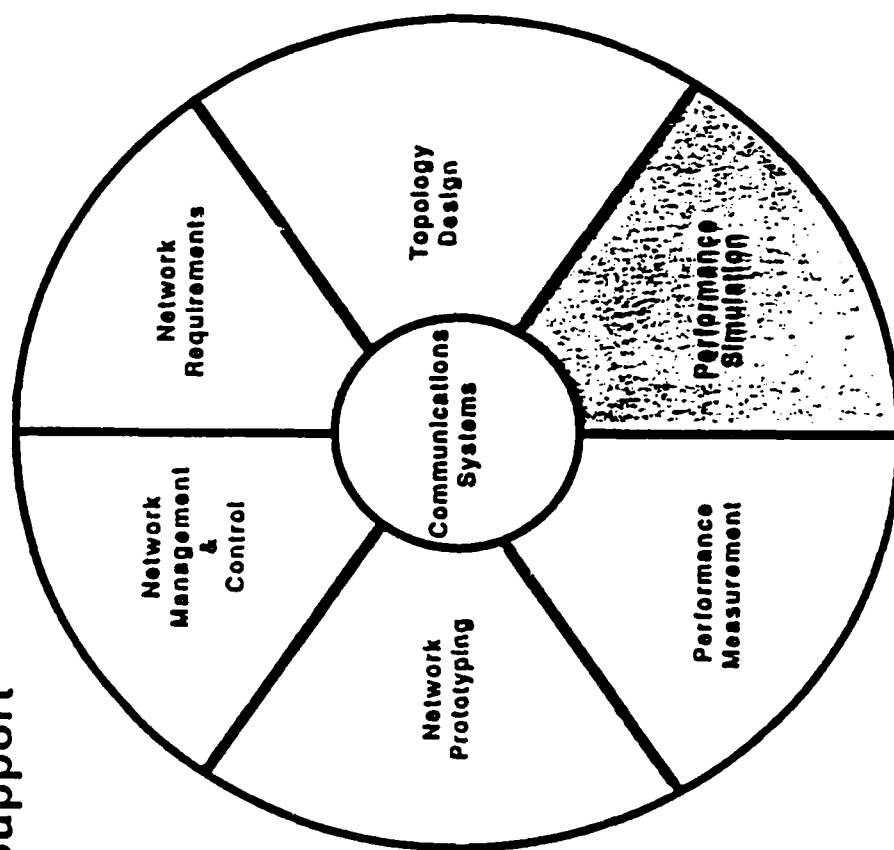
CALCULATED DELAY BETWEEN NODES



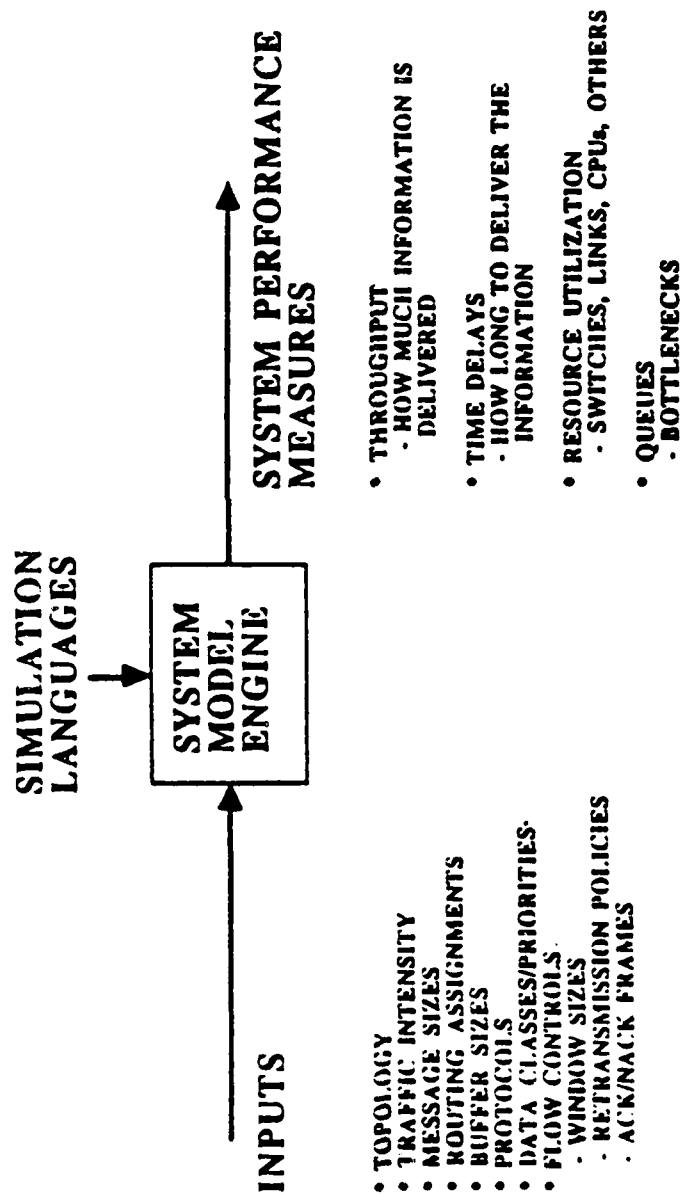
INFORMATION NETWORK LABORATORY

MARTIN MARIELLA
INFORMATION & COMMUNICATIONS SYSTEMS

Life Cycle Support



NETWORK PERFORMANCE ANALYSIS PROCESS

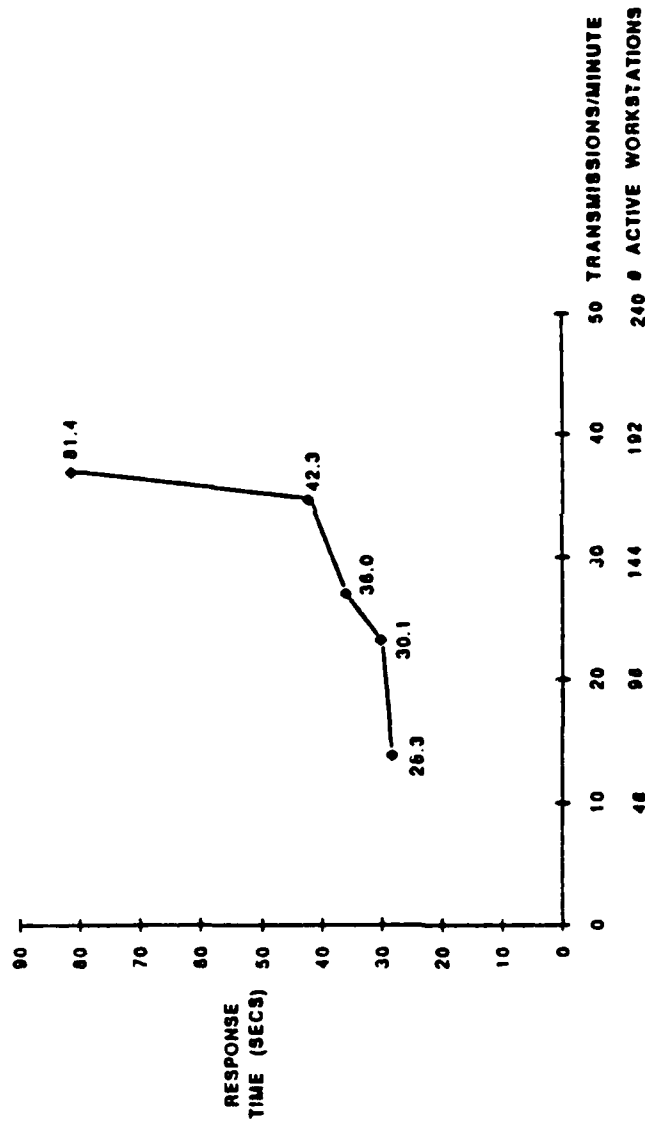


INFORMATION NETWORK LABORATORY

MARTIN MARJETTA

INFORMATION & COMMUNICATIONS SYSTEMS

Impact of Added Workstations on End-to-End Network Response Performance



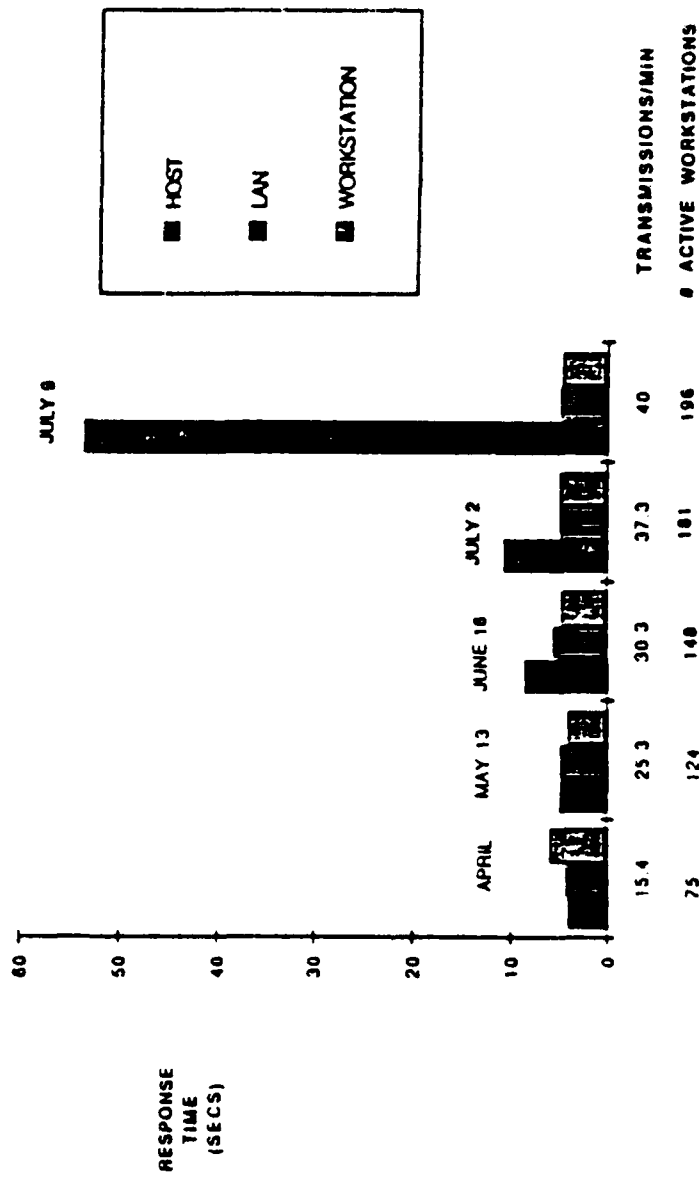
Inferences:

Network Performance Saturates at approx. 175 Active Workstations

INFORMATION NETWORK LABORATORY

MARTIN MARIETTA
INFORMATION & COMMUNICATIONS SYSTEMS

Decomposed End-to-End Response Time



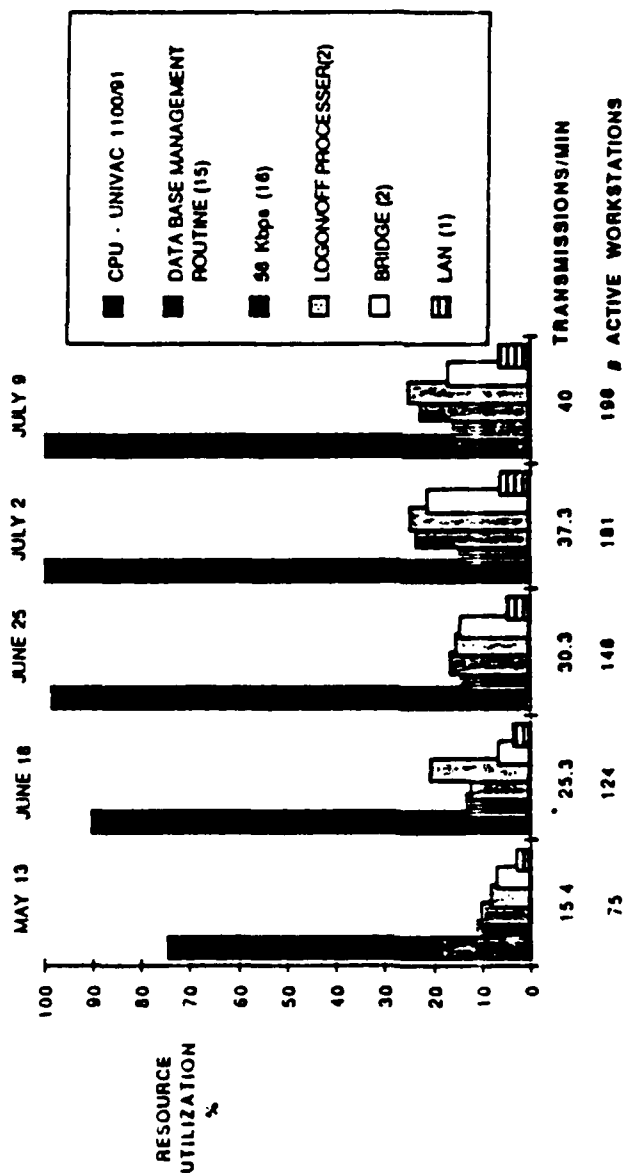
Inferences:

RESPONSE TIME DECOMPOSITION INDICATES THAT CONTENTION DELAY IS
RESIDENT IN THE HOST

INFORMATION NETWORK LABORATORY

MARTIN MARIETTA
INFORMATION & COMMUNICATIONS SYSTEMS

Impact of Added Workstations on Resource Utilization

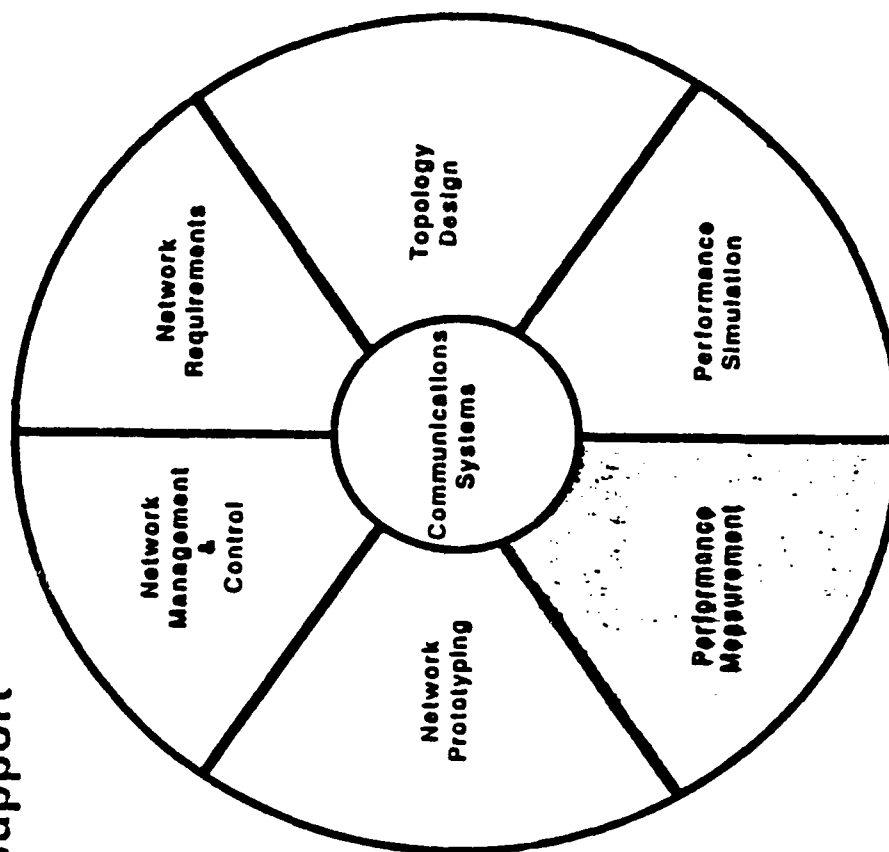


Inferences:
WITHIN THE HOST, THE INSTRUCTION PROCESSING UNIT IS A RESOURCE BOTTLENECK

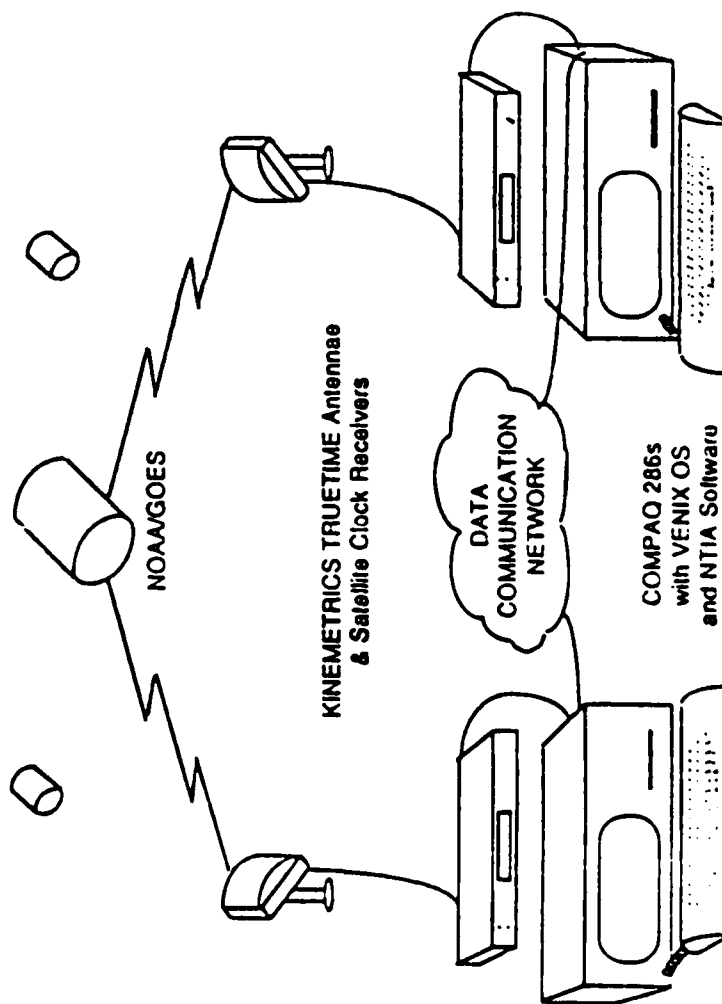
INFORMATION NETWORK LABORATORY

MARTIN MARIETTA
INFORMATION & COMMUNICATIONS SYSTEMS

Life Cycle Support



Performance Measurement Overview



**INL NETWORK PERFORMANCE MEASUREMENT CAPABILITIES:
END-TO-END NETWORK MEASUREMENTS (WITH ANS X3.102)**

Characteristics:

- defined set of parameters and measurement methods
- user oriented
- system independent
- speed, accuracy, and reliability parameters for each function

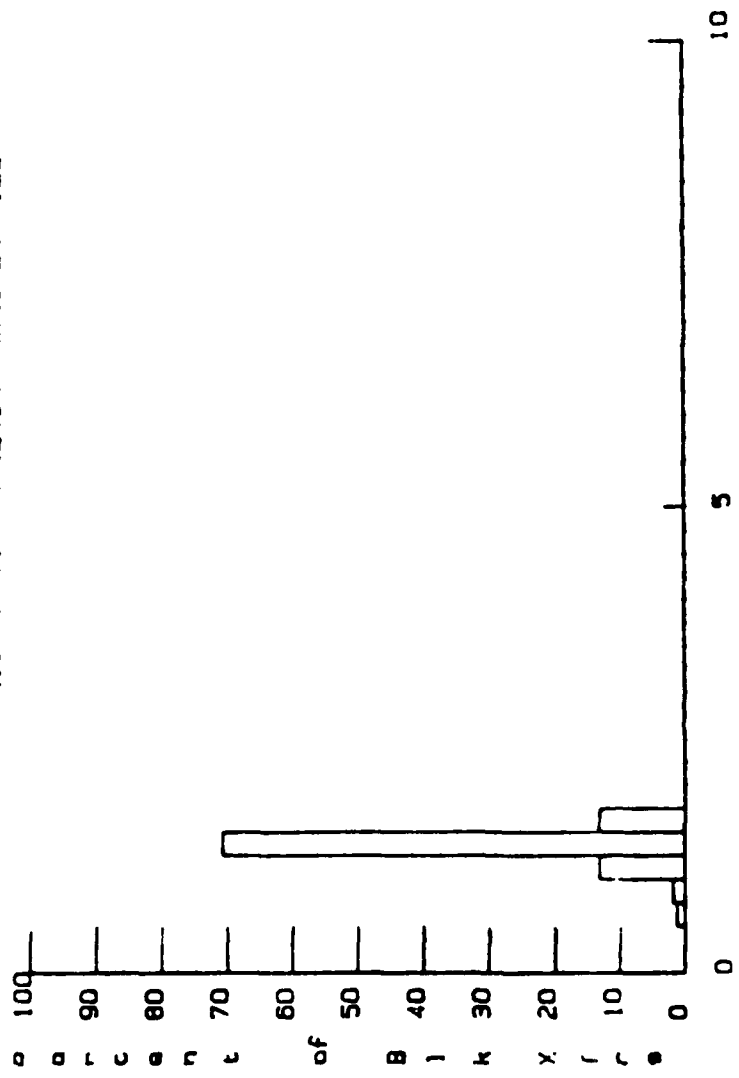
Four Major Measurement Types:

- (1) Access
 - begins upon access request signal
 - ends when first data bit input to system
- (2) Information transfer
 - includes effects of: formatting, transmission, storage, error control
media, conversion, retransmissions
- (3) Disengagement
 - begins with disengagement request
 - ends when user able to initiate new access
- (4) Ancillary parameters:
 - identify entity (user/system) most responsible for delays

INFORMATION NETWORK LABORATORY



HISTOGRAM FOR BLOCK TRANSFER FILE



Transfer time in seconds

Test of x.25 Dial-up Using x3.102

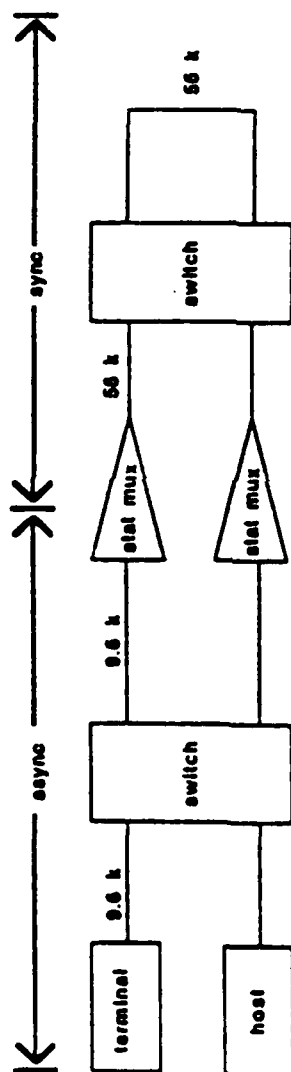
Place of test :	Denver, Colo.	Standard Deviation	-	0.153
Date of test:	Jan 20, 1987	Mean Time	-	1.38
Test #:	105	Minimum Time	-	0.71
x25 connect		Maximum Time	-	1.59
64 byte blocks		Number of transfers	-	180

Performance Estimation vs Prototype Measurement

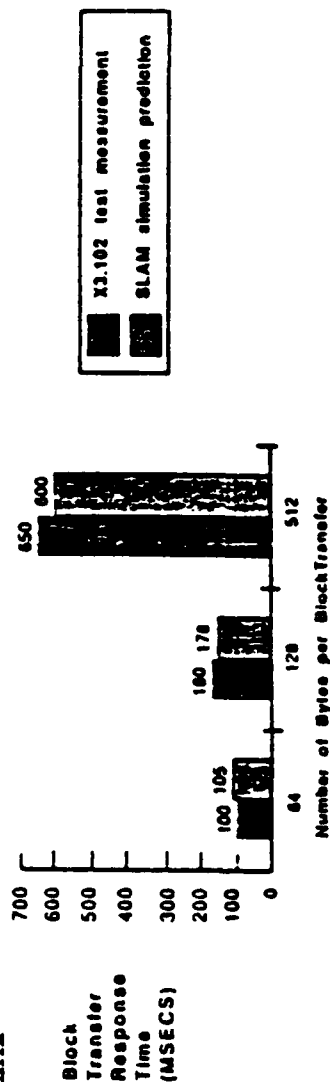
Objective

Verify simulation results through actual network measurements

Network Configuration

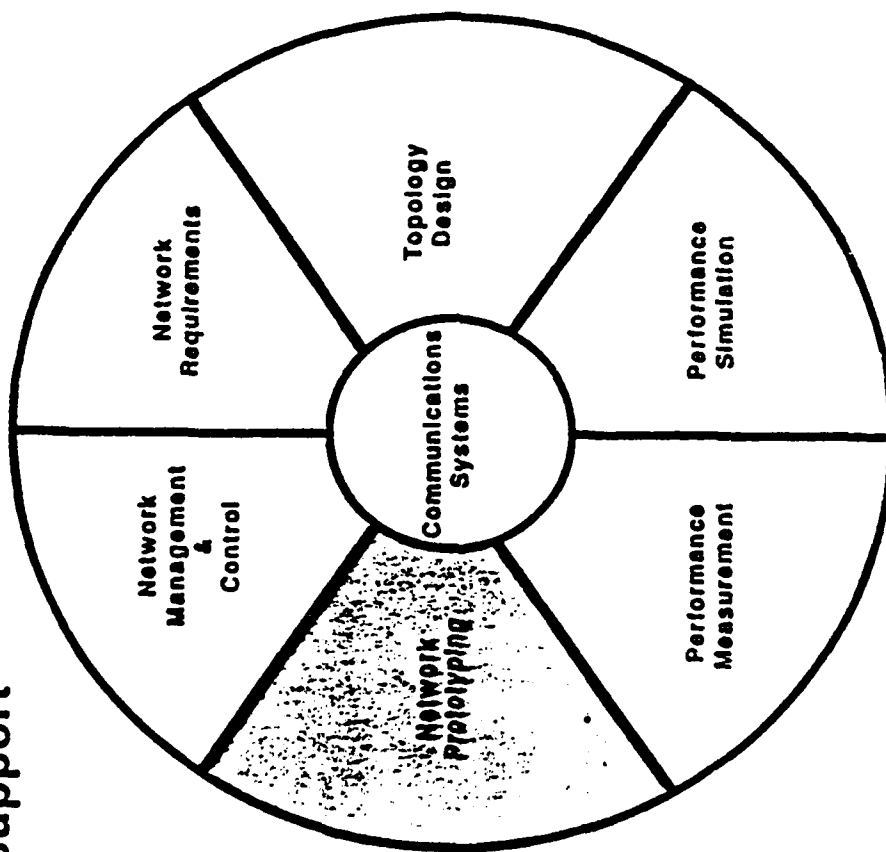


Results



INFORMATION NETWORK LABORATORY

Life Cycle Support



PROTOTYPING OVERVIEW

- **DEVELOPMENT AND TESTING OF APPLICATIONS SOFTWARE IN A DISTRIBUTED ENVIRONMENT USING TXP**

- **PROTOTYPING OF SYSTEMS IN A:**

- **LABORATORY ENVIRONMENT**

- **HARDWARE SIMULATED STRESS ENVIRONMENTS**

- **DIGITAL**

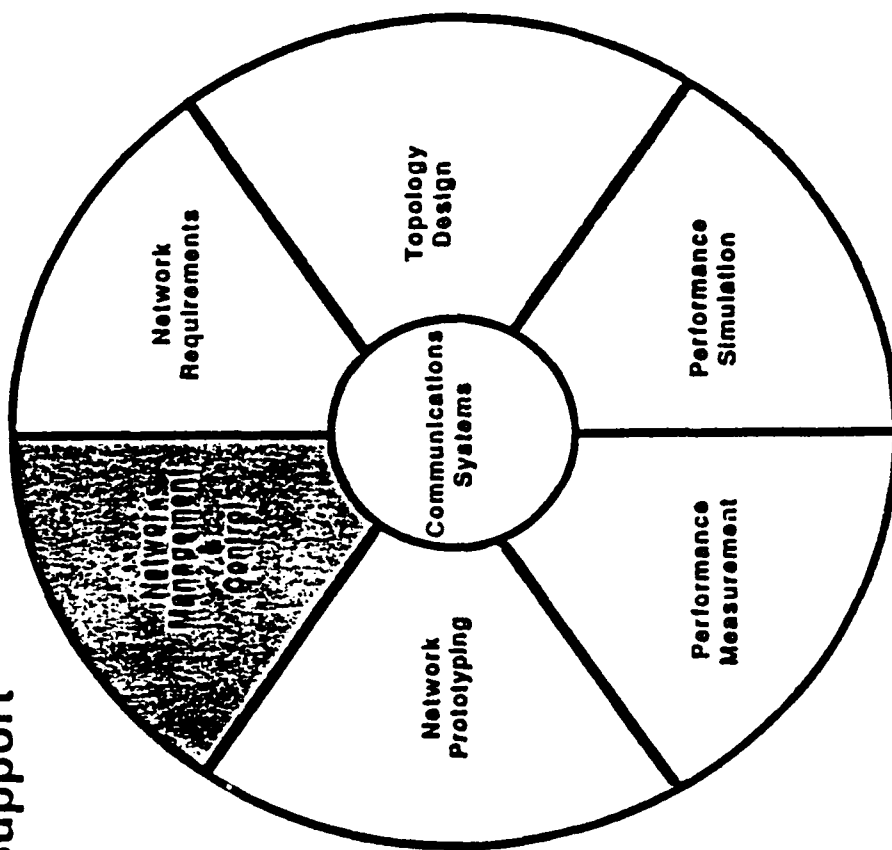
- **ANALOG**

INFORMATION NETWORK LABORATORY

MARTIN MARIETTA

INFORMATION & COMMUNICATIONS SYSTEMS

Life Cycle Support

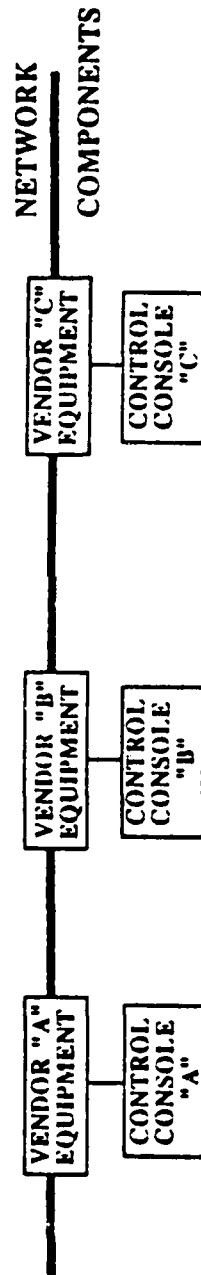


Problem

- O I&CS Customer Requirements Illustrate Need for Integrated Management Capability in Complex, Heterogeneous Communications Networks.
- O Current State-of-the-Art Consists of Stand-Alone, Vendor-Dependent Network Management Packages/Capabilities for Each Communications Resource which are:
 - Costly
 - Disjointed
 - Overlapping
 - Non-interoperable
 - Incompatible
 - Inadequate
 - Inflexible
 - Inefficient
 - Labor-Intensive
 - Unfriendly
- O Network Management Design Techniques and Development Tools are Lacking

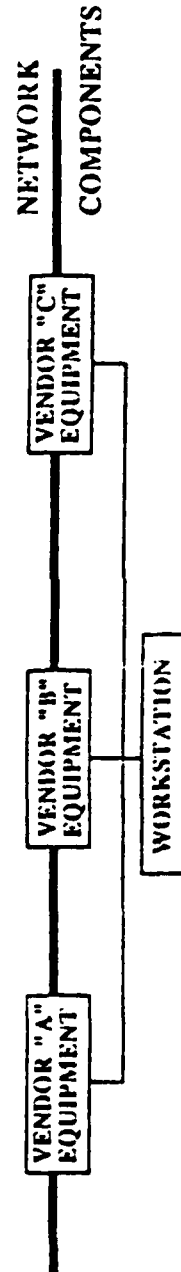
INTEGRATED NETWORK MANAGEMENT AND CONTROL OVERVIEW

* STATE-OF-THE ART



- VENDOR DEPENDENT
 - QUERY LANGUAGE
 - COLLECTED/MONITORED INFORMATION
 - ALARMS AND DISPLAYS
- DEDICATED CONSOLE
- MULTIPLE OPERATORS/STATIONS

* INTEGRATED



- COMMON QUERY LANGUAGE AND DISPLAYS
- SINGLE MONITOR AND CONTROL STATION
- COMMON FORMATS, WINDOWS

INFORMATION NETWORK LABORATORY

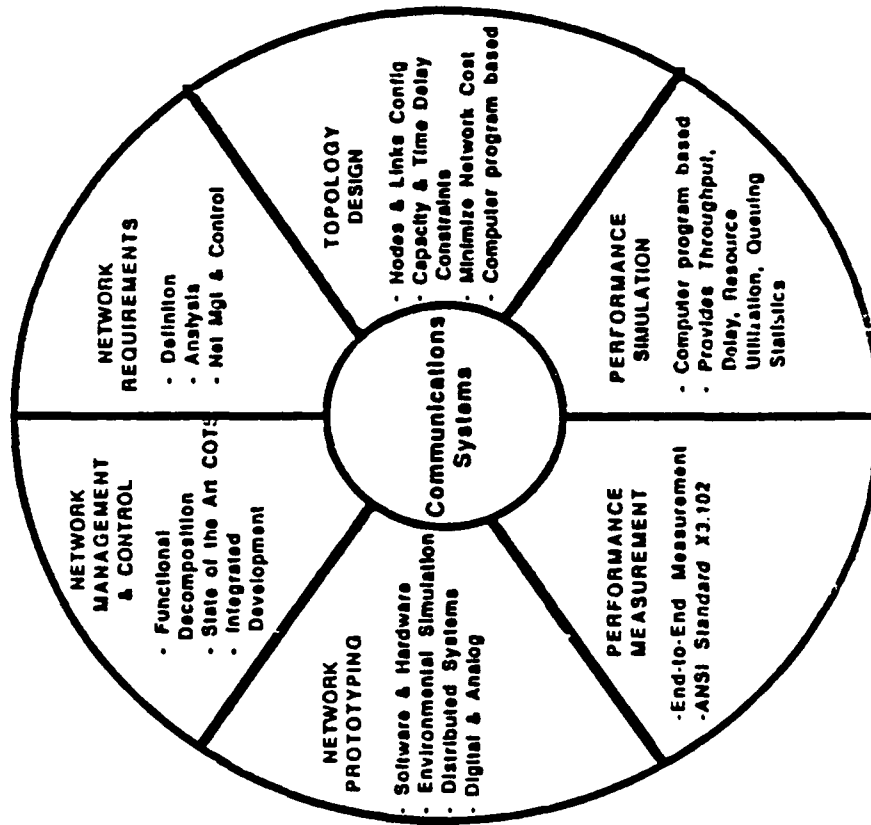
MARTIN MARIETTA

INFORMATION & COMMUNICATIONS SYSTEMS

Payoffs

- **REDUCED OPERATIONAL COSTS**
 - Single Workstation
 - Common User-Friendly Command Language
 - Simplified Training
 - Automation of labor-intensive operations
- **RAPID RECONFIGURATION RESPONSE TO**
 - Failures
 - Events
 - Traffic Loading
 - Mission Changes
- **MORE EFFICIENT USE OF COMMUNICATIONS RESOURCES**
- **GREATER FLEXIBILITY IN NETWORK CONFIGURATION**
- **HIGHER RELIABILITY AND AVAILABILITY**

Distributed Information System Technologies



FUTURE INL SERVICES

- VIDEO TELECONFERENCING
- VOICE SWITCH NETWORKS
- TRANSMISSION PROPOGATION MODELS
(MICROWAVE, SATELLITE)
- TRAFFIC SIMULATORS
- LAN SECURITY CAPABILITIES
- NETWORK DESIGNS INCORPORATING MULTILEVEL
SECURITY CAPABILITIES
- NETWORK DESIGN METHODOLOGY
- ISDN

DISTRIBUTED
NETWORK MANAGEMENT

Robert A. Meyer

C l a r k s o n U n i v e r s i t y

RESEARCH GOALS

Identify problems in network management
appropriate for application of
artificial intelligence techniques

Increase our understanding of
fundamental problems which arise in
the design of intelligent systems
distributed over a network

Develop new techniques for achieving
cooperation among intelligent
systems and demonstrate their
application to real world problems

C l a r k s o n U n i v e r s i t y

DOMAIN CHARACTERISTICS

Nodes are geographically distributed

No node has accurate and complete
knowledge about global system state

Nodes have limited bandwidth for
communication with one another

No central locus of control is assumed
(for survivability)

C l a r k s o n U n i v e r s i t y

TASKS IN NETWORK MANAGEMENT

STATUS ASSESSMENT - determine, at a high level, network status and impact of events

FAULT ISOLATION - when trouble occurs, determine its specific cause

SERVICE RESTORAL - determine plans for restoring service to as many critical users as possible

C l a r k s o n U n i v e r s i t y

PROBLEM SOLVING REQUIREMENTS

Performance assessment - (PA)
data interpretation
situation assessment

INPUTS:

equipment alarms
traffic data
transmission monitors
user complaints

OUTPUTS:

system and network status
failure detection and its impact

C l a r k s o n U n i v e r s i t y

PROBLEM SOLVING REQUIREMENTS

Fault isolation - (FI)
diagnostic activity

identify location and cause of failures,
degradation, or intermittent outages

INPUTS:

failure indication and probable
location (from PA)
equipment alarms
circuit, trunk, link status
additional test results, as needed

OUTPUTS:

location (at equipment level) of
failure, if known

or

request for additional tests to
resolve ambiguities

C l a r k s o n U n i v e r s i t y

PROBLEM SOLVING REQUIREMENTS

Service restoral - (SR)

generate and select plans
for allocation of scarce resources
to restore service to disrupted users

INPUTS:

requests for restoral action (from PA)
circuit, trunk, and link status
system configuration and topology

OUTPUTS:

set of feasible restoral plans.
indicating circuits to be restored
(and those that can not be), and
equipment re-allocations needed
to accomplish these plans

C l a r k s o n U n i v e r s i t y

ROLE OF A DISTRIBUTED NETWORK MANAGEMENT SYSTEM

As an operator aid -

- reduce the "data overload" problem

- recommend restoral and
diagnostic actions

- reduce the training period

As a distributed controller -

- enhance survivability by eliminating
dependence on a single control node

- provide coordination and cooperation
among distinct control centers

- perform satisfactorily in the
event of missing or erroneous data

C l a r k s o n U n i v e r s i t y

RATIONALE

Highly complex problems

Need for a "good" solution within a
reasonable time

Insufficient time for finding an optimal
solution, if it exists

Observed data and (non-local) knowledge
may be errorful and uncertain

Human experts are available for some
problems and have significant insight
based on many past years of experience

C l a r k s o n U n i v e r s i t y

DISTRIBUTED CONTROL SYSTEM ARCHITECTURE

Geographic distribution

- observed data
- control points
- localized knowledge of configuration
and status

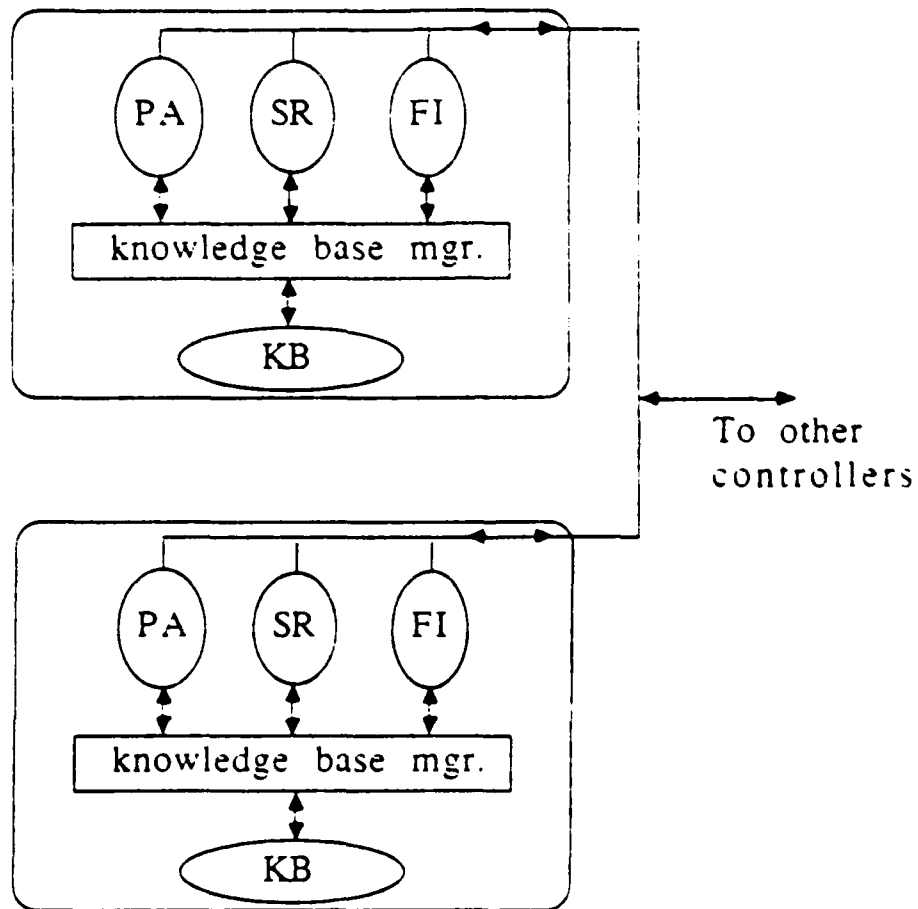
Functional distribution

- performance assessment (PA)
- fault isolation (FI)
- service restoral (SR)

"Pure" distributed control, with
no locus of control activity and
no locus of decision making is
required to reduce vulnerability
and enhance survivability.

C l a r k s o n U n i v e r s i t y

A DISTRIBUTED KNOWLEDGE - BASED
PROBLEM SOLVING SYSTEM



C l a r k s o n U n i v e r s i t y

DAISY - DISTRIBUTED AI SYSTEM

A testbed environment for developing
and experimenting with distributed
artificial intelligence systems.

HARDWARE:

a network consisting of a mixed set
of LISP machines

SOFTWARE:

SIMULACT - a generic simulation tool
for simulating multiple,
semi-autonomous actors on one or
more machines

GUS - a graphical user interface for
describing structural knowledge
about communications systems

Clarkson University

RESEARCH STATUS

Domain Analysis

completed implementation of tool for
acquisition of structural knowledge

completed initial stage of knowledge
acquisition for a DCS model network

near completion of problem solving
specifications

System Design

completed high-level architecture

developed problem solving strategy
for cooperative service restoral
based on "multistage negotiation"

investigating issues of distributed
knowledge base maintenance

C l a r k s o n U n i v e r s i t y

APPLICATION AREAS

Communications Systems

Defense Communications System (DCS)

packet switched network control

circuit switched network control

SDI communication system control

Manufacturing Process System Control

Distributed Resource Allocation

C l a r k s o n U n i v e r s i t y

DYNAMIC SERVICE RECONSTITUTION
in a
DIGITAL BACKBONE NETWORK

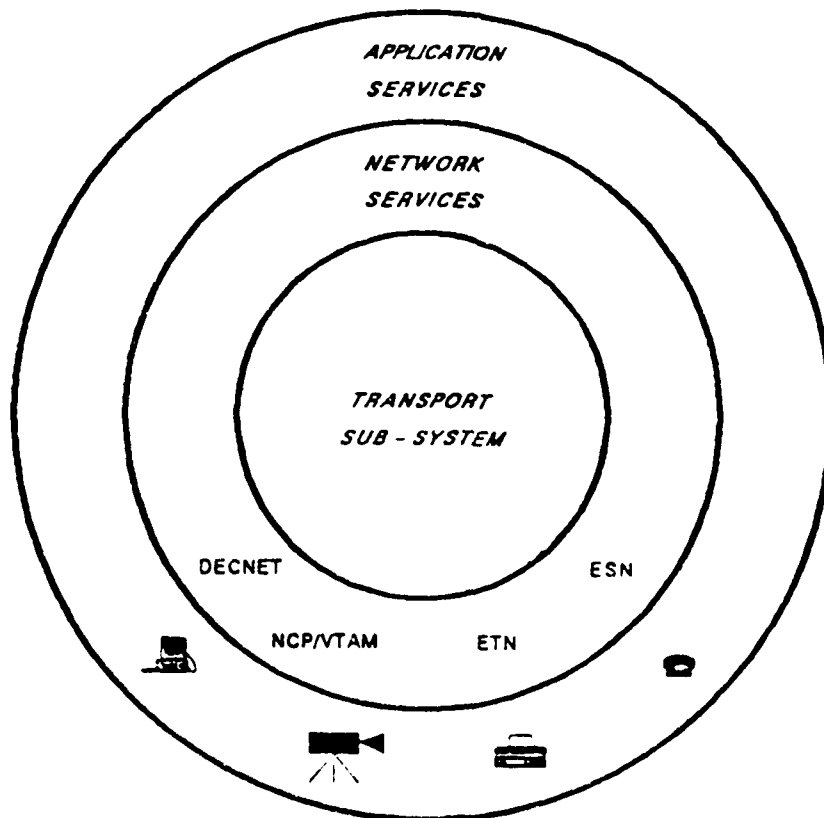
RADC

July 1, 1987

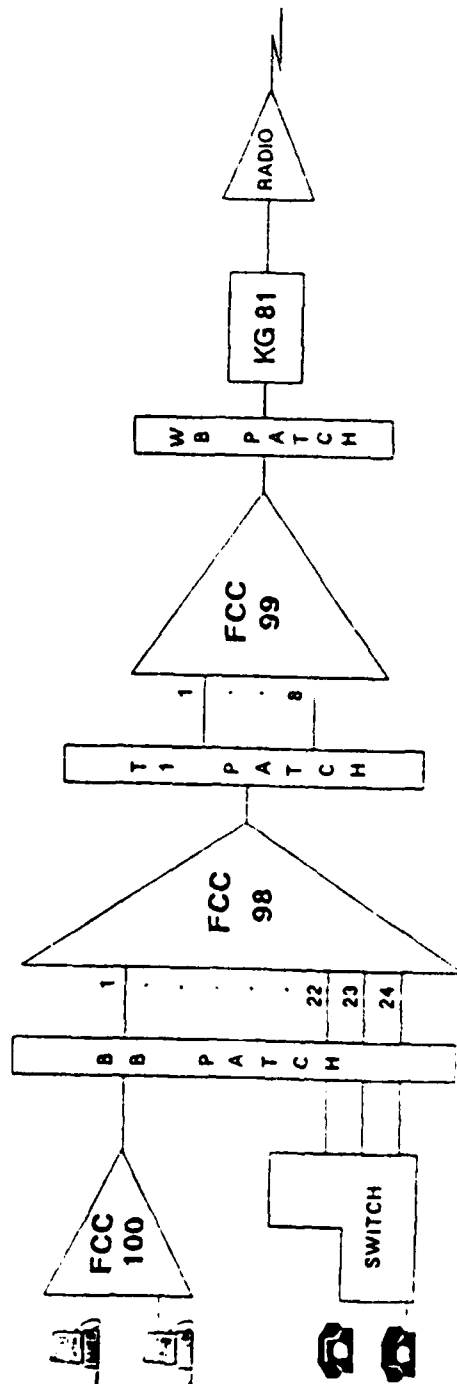
Robert Fish
Director of Systems Engineering
Federal Systems Division

Network Equipment Technologies
8300 Boone Blvd Ste. 280
Vienna, Va 22180
703 - 556 - 7740

MAJOR LOGICAL LAYERS of an IDN



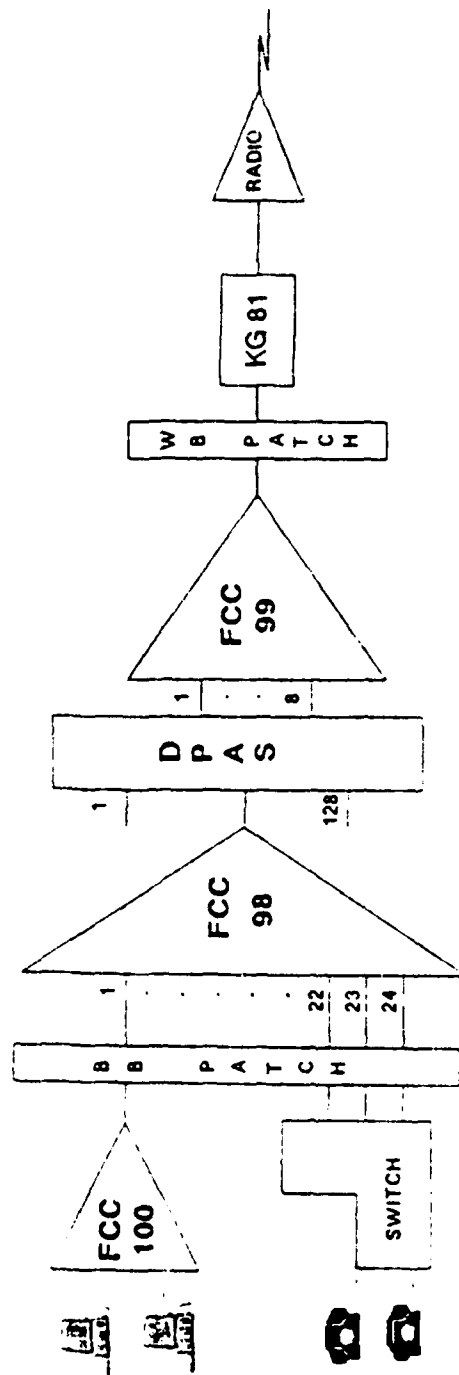
Fundamental Components of a DRAMA Based TSS.



C-311



Fundamental Components of a DRAMA/DPAS Based TSS.



COMMUNICATIONS SYSTEMS MANAGEMENT FUNCTIONS

PLANNING

- needs analysis (user, network, etc)
- technology tracking & assessment
- network design

OPERATIONS

- network monitoring
- service restoral
- problem tracking

MANAGEMENT

- configuration control
- service provisioning
- service level monitoring

ADMINISTRATION

- accounting
- inventory tracking
- contracts support



TRANSMISSION RESOURCE MANAGER

A computer controlled, high – speed
circuit switching device that combines
the following elements:

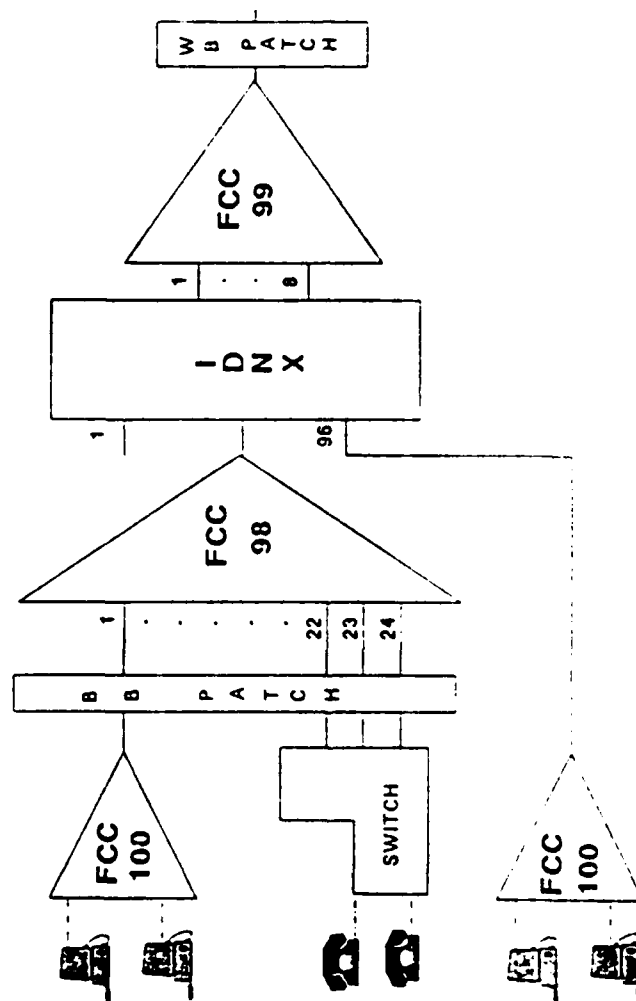
- time division multiplexing
- matrix switching
- digital cross – connection
- voice processing

to allow maximum bandwidth utilization
for voice, data, image, and video applications.

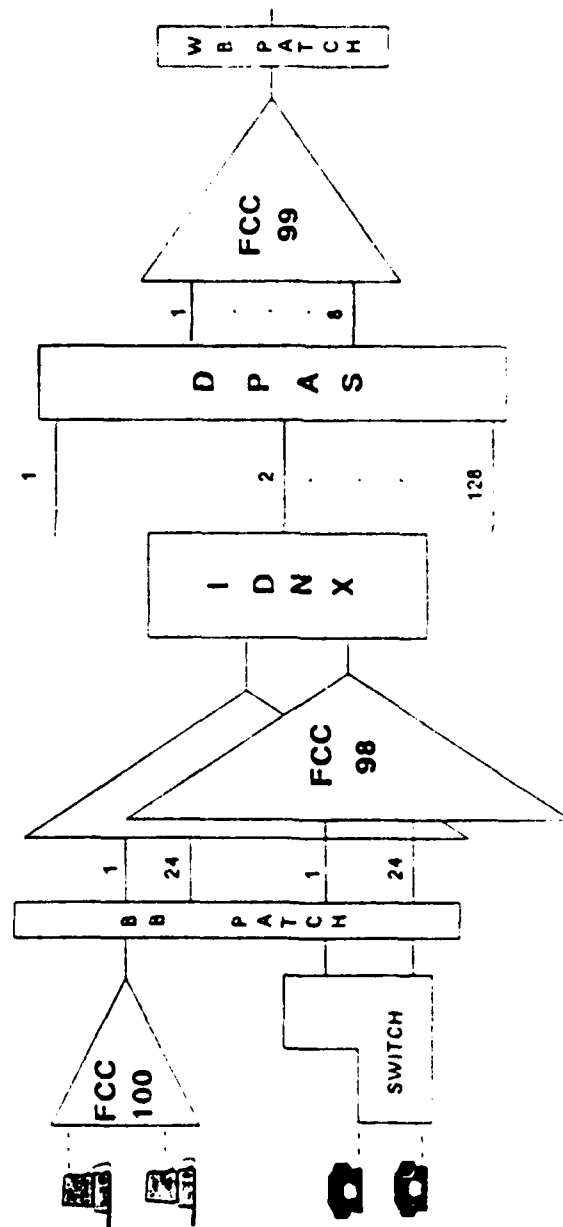


Fundamental Components

of a DRAMA/IDNX Based TSS.



Fundamental Components of a HYBRID Based TSS.



ESSENTIAL HARDWARE DESIGN CHARACTERISTICS of a SURVIVABLE TRM.

ROBUST ARCHITECTURE

- failure compartmentalization
- redundancy of critical components
- ease of maintenance
- ease of expansion

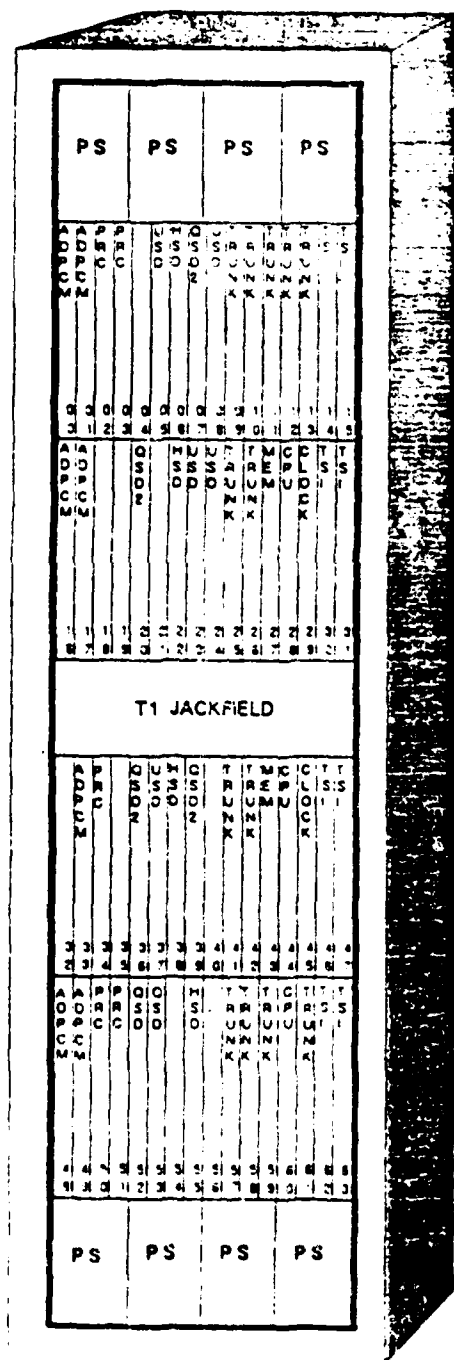
DISTRIBUTED PROCESSING

- onboard computer
- multi – processor
- EAROM configuration database
- downline loadable software

CENTRALIZED CONTROL

- simplified operator interface
- realtime alarm reporting
- board level remote diagnostics
- comprehensive statistics





TIME SLOT INTERCHANGE
ARCHITECTURE
PROVIDES *TELCO* LEVELS
of RELIABILITY

ESSENTIAL LOGIC CAPABILITIES

of a SURVIVABLE TRM.

Sophisticated Operating System

- self – checking
- fault tolerant
- rapid call processing
- extensive diagnostic hooks

Software Defined Configuration

- node parameters
- port characteristics
- trunk attributes

Efficient Bandwidth Management

- demand assigned circuits
- channel prioritization (with preemption)
- integral voice compression
- sub – rate data multiplexing

Common Channel Signaling

- realtime topology maintenance
- look – ahead call setup
- ISDN positioning



CALL CONTROLLER TASKS

CIRCUIT ESTABLISHMENT

- recognize port activation
- determine port speed/routing requirements
- determine optimal path
- establish circuit

CIRCUIT RESTORATION

- teardown affected circuits
- prioritize according to port parameters
- determine optimal new path
- establish circuit

TOPOLOGY MAP MAINTENANCE

- monitor attached links
- pass on own TM checksum
- update TM based on received checksum



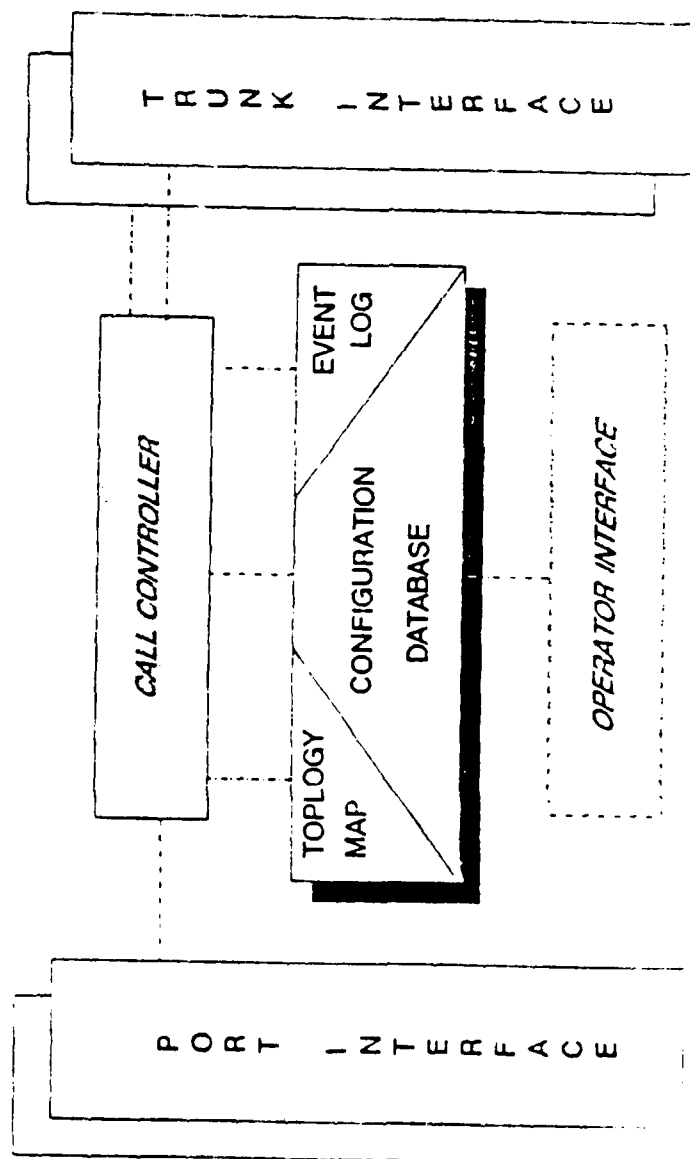
CONFIGURATION DATABASE

PARAMETERS

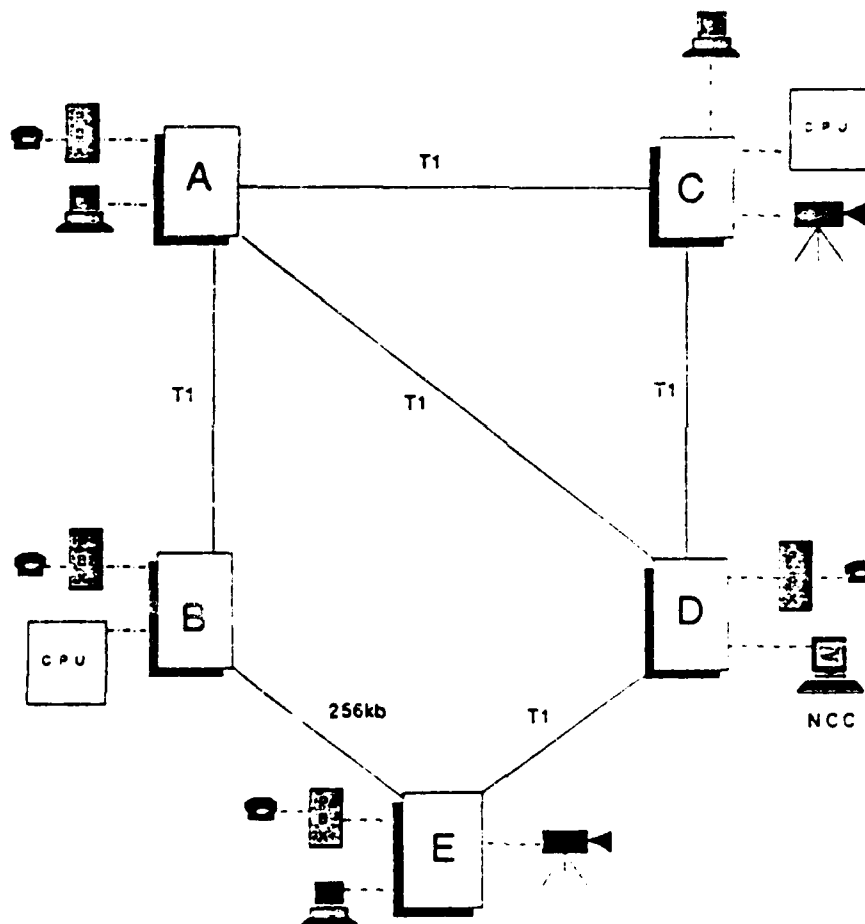
NODE	PORT	TRUNK
time zone	orig/ans mode	neighbor node
event log	destination port	type
clock sources	normal priority	routing attributes
max calls	preempt priority	redundant card
max hops per call	speed (data)	zero suppression
CDR enable	speech compression (voice)	alarm wait time
reconnect period	activation criteria	alarm percentage
attached links	routing requirements	



CALL PROCESSING LOGIC FLOW

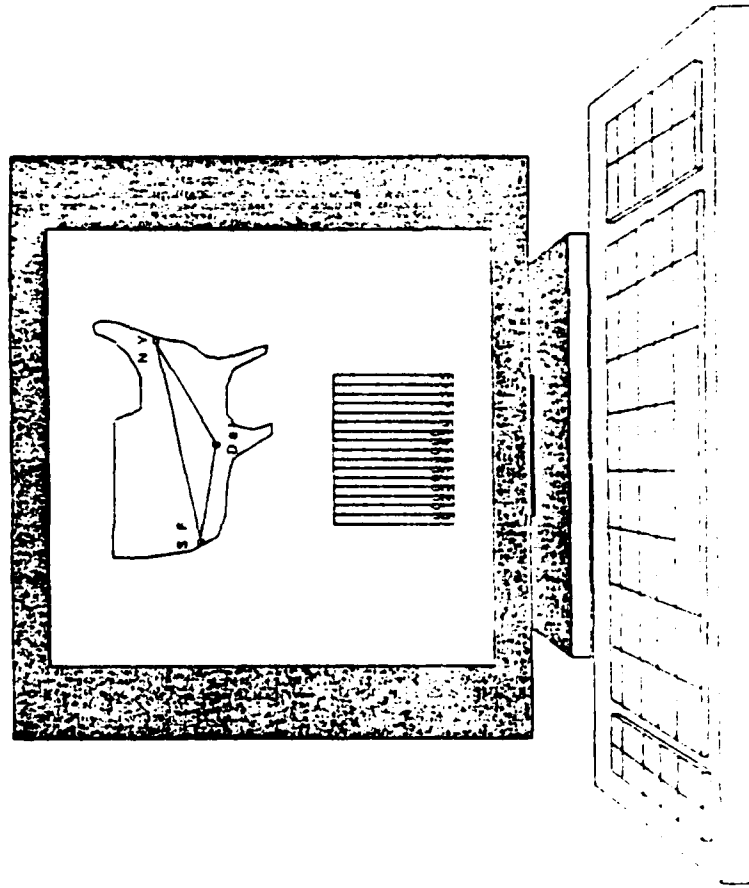


Example IDNX Network



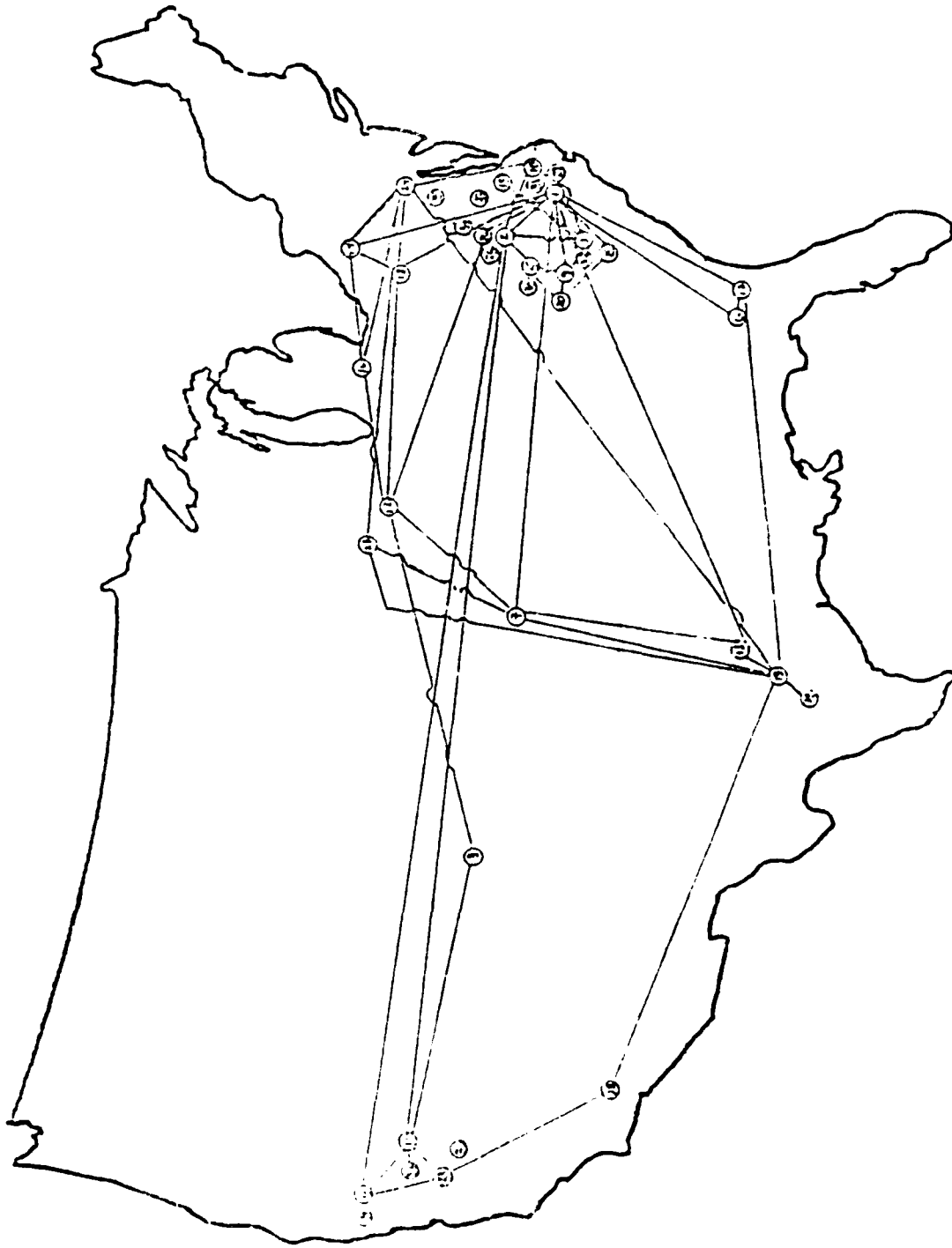
NETWORK **FEDERAL**
EQUIPMENT TECHNOLOGIES SYSTEMS DIVISION

SIMPLIFIED (graphics based) OPERATOR WORKSTATION



NEWARK
EQUIPMENT TECHNOLOGIES
FEDERAL
SYSTEMS DIVISION

MCI T1 BACKBONE NETWORK



Network Management for the DCS

H. M. Heggestad
M.I.T Lincoln Laboratory

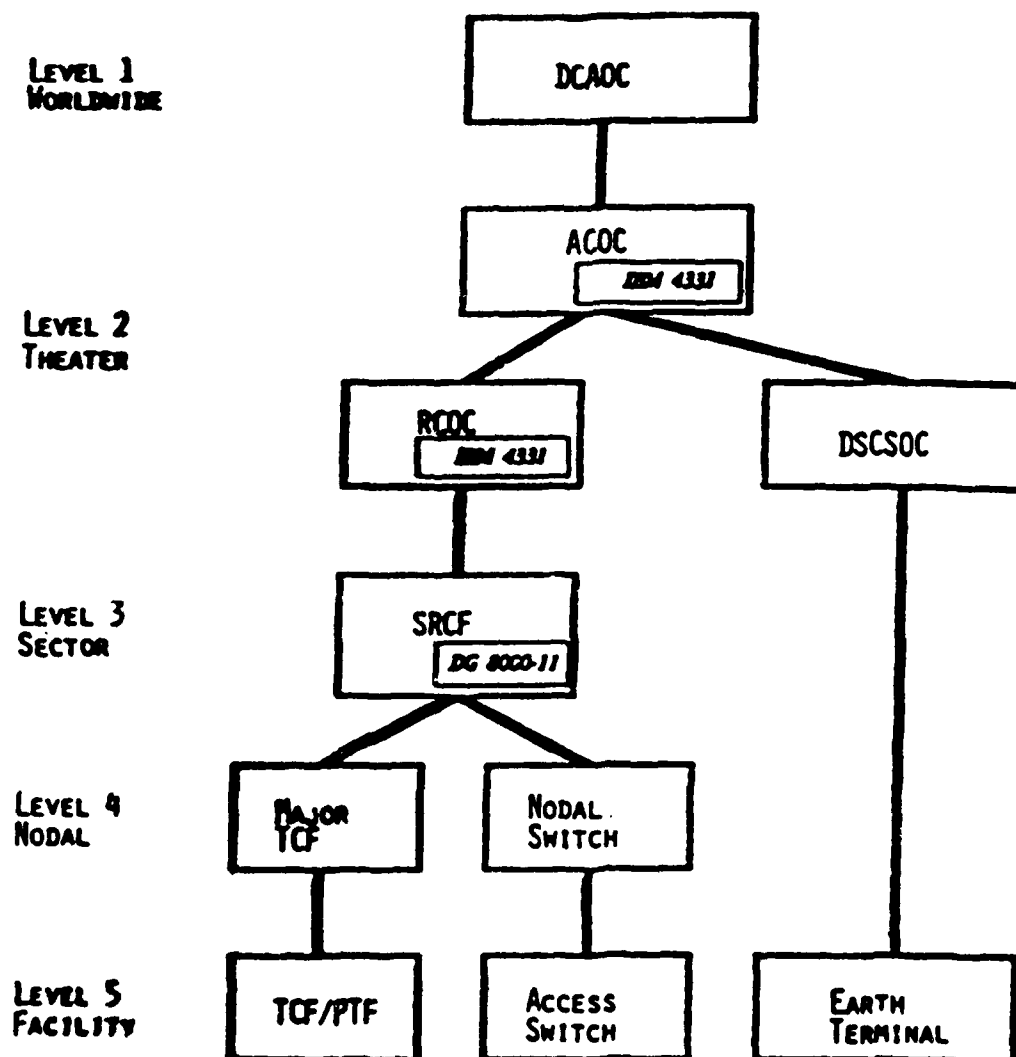
Network Management for the DCS

- System description, environment
- The Expert Tech Controller
- Management of the Defense Switched Network

The Defense Communications System

- Worldwide comm services for MilDeps
 - Circuit-switched voice system
 - AUTOVON (since 1950s)
 - Now in transition to DSN
 - Dedicated circuits
 - Defense Data Network
 - Various special networks
- Dual objectives
 - Reliable crisis, wartime communications
 - Economical peacetime operation
- Hierarchical worldwide control structure
 - Greatly improved status, performance data gathering system in development
 - Serious needs for n/w management aids

DCS OPERATIONS SUPPORT SYSTEM (DCOSS)



Glossary of Terms

DCAOC: DCA Operations Center (Washington, DC)

ACOC: Area Communications Operations Center
(e.g., European, Pacific theaters)

RCOC: Regional OC (e.g., about 15-20 in Eur)

SRCF: Sub-Regional OC (several per region)

DSCSOC: Defense Satellite Communications OC

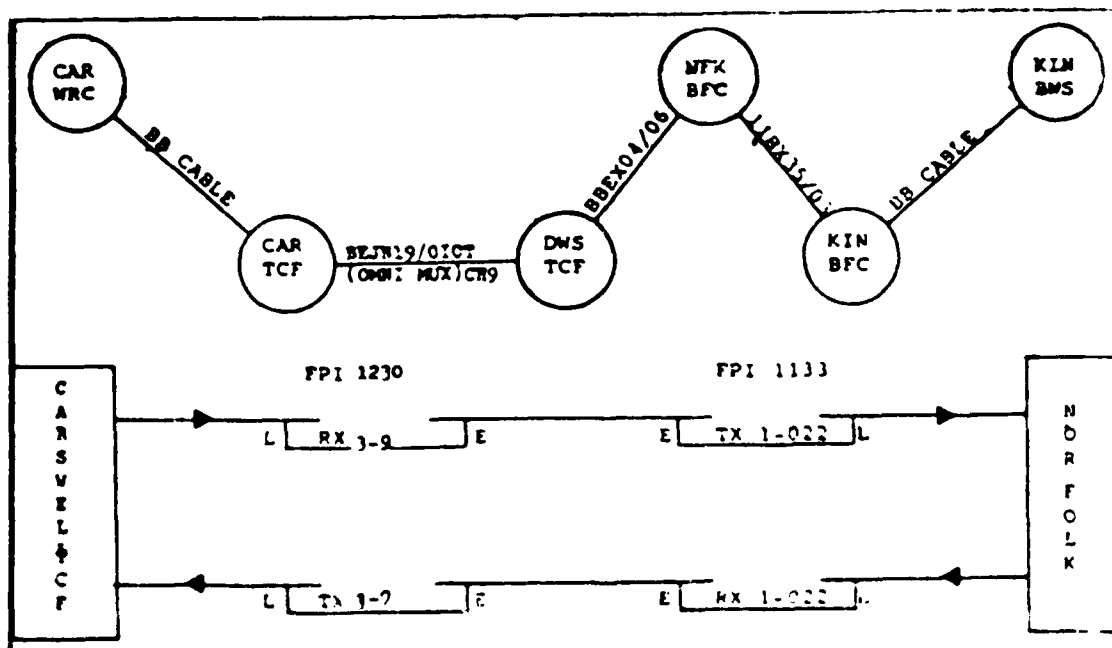
DCS Net Management Problem Areas

- Complexity of modern nets, equipment
- Enormous data reduction, interpretation load
 - Recognition of incipient problems
- Shortage, loss of skilled personnel
 - Cost of training
 - Lure of civilian jobs

Application of Expert Systems Technology in NM

- Tech Control
 - Foundation layer of control hierarchy
 - Highly skill-, manpower-intensive
- Defense Switched Network management
 - Regional, sub-regional levels
 - Network currently being implemented
 - Much greater range of net mg't options
 - No experience base

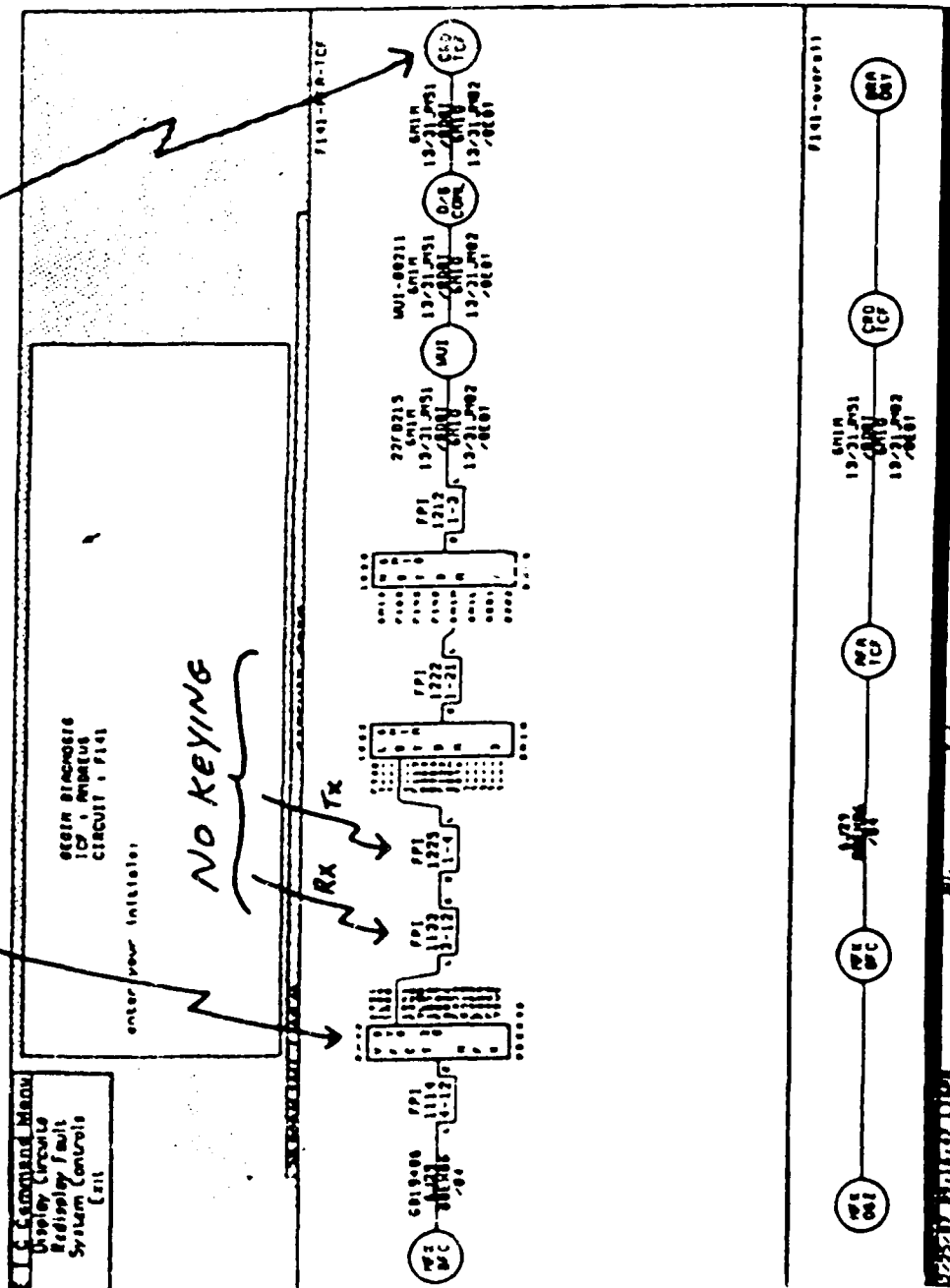
DD FORM 1207, 1 JAN 66						CIRCUIT DATA	
CCSO	LANDLINE/CHAN NO	TERMINALS	CONTROL FACILITIES		MCS NP		
BWXA7DUM	BEJN19 -0107	CARSWELL WRC	CARSWELL TCF		3A		
SEN STATION	OPERATING AGENCY	USER TERM EQUIPMENT		USER CONTACT			
TEXAS	U.S. NAVY	UNSPECIFIED		CARSWELL TCF(V)739-7809			
TERM STATION	OPERATING AGENCY	USER TERM EQUIPMENT		USER CONTACT			
BERMUDA	U.S. NAVY	UNSPECIFIED		NORFOLK O/W			
TYPE CIRCUIT	USE	CCO INCOI	MODULATION RATE		CRYPTO SERVICE		
N2. FP. FD	SEE RMKS.	CARSELL TCF	75 BAUD		NONE		
ACTIVATION AUTHORITY		DATE AND TIME INSTALLED		CMT MODIFICATION/CONTINUED ON REVERSE SIDE			
CEO: W90371/7DUM		032030ZSEP69					
DEACTIVATION AUTHORITY		DATE AND TIME CEASED		AUTHORITY			
				DATE AND TIME COMPLETED			
				TSO-W12222/7DUM 02 161217FFB73			
				TSO-W53144/7DUM 03 1613257FFB75			
CONDITIONING EQUIPMENT				REMARKS			
PAD				1. TSO: X41344/7DUM-05 2. FOR CIRCUIT ROUTING AND LAYOUT SEE REVERSE. 3. USE: NAVY WEATHER AS STATED IN DCAC 310-65-1, CHAP. 14.			
REPEAT COILS							
LINE AMPLIFIER							
DELAY EQUALIZER							
AMPLITUDE EQUALIZER							
REGENERATING REPEATER (YES)							
CROSS-CHINE CROSS							
CROSS-TERMINAL SET							
ECHO SUPPRESSOR							
OTHER							
CCSO	LANDLINE/CHAN NO	TERMINALS	CONTROL FACILITIES		MCS NP		
BWXA7DUM	BBEX04/006	BERMUDA BWS	BERMUDA BFC		3A		





FAULT: BAD RECEIVE CHANNEL

COMPLAINT: RECEIVING MARK
(NO KEYING)



DSN System Control: Simulation Techniques
and Expert Systems

- Requirements and Objectives
 - Environment
 - Functionality
- Use of existing Call-by-Call Simulator
- Expert System for network management

New Elements in the DSN Control Environment

- Large numbers of switches, various types
 - More complex topology than AUTOVON
 - More connectivity choices for alt routing
 - Greater tolerance for loss of switches
- Stored program control (SPC)
 - Extensive performance data collection
 - Flexible routing, preemption mechanisms
 - Large repertoire of control options
- Common-channel signalling (CCS)
 - Ample bandwidth for monitoring, control
- DCOSS structure

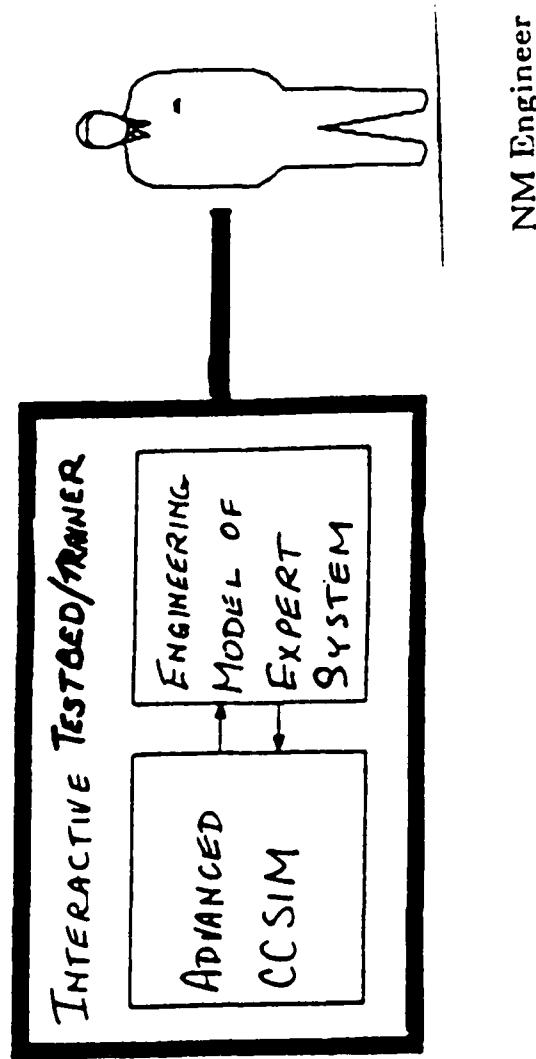
The Problems

- We do not know how to control the DSN
 - Cannot extrapolate from AUTOVON
 - Highly skill- and judgment-intensive req'ts
 - Analyze information flow from DCOSS
 - Recognize problems before they become significant
 - Understand, apply correct controls
 - Remove controls as soon as possible
- We cannot risk slowly learning by experience
 - DSN is already being implemented
 - Disastrous failures are possible
- When we do develop skilled controllers, we will be unable to retain them

Work in Progress Toward Solutions

- Major enhancements of Call-by-Call Simulator
 - Originally developed for routing studies
 - Congestion, failure models now being added
 - Incorporation of system control facilities
- Experimental development of DSN control knowledge
 - Creation of crisis/damage scenarios
 - Identification of premonitory patterns of failure
 - Exploration of control actions, effects
- Permanent retention, presentation of the knowledge in an Expert System
 - Initial application: operate simulator
 - Subsequent role: aid DSN managers

Interactive Testbed/Trainer



NM Engineer

Automated Network Management

BBN Laboratories Inc.

NOC Workstation
Automated Network Management

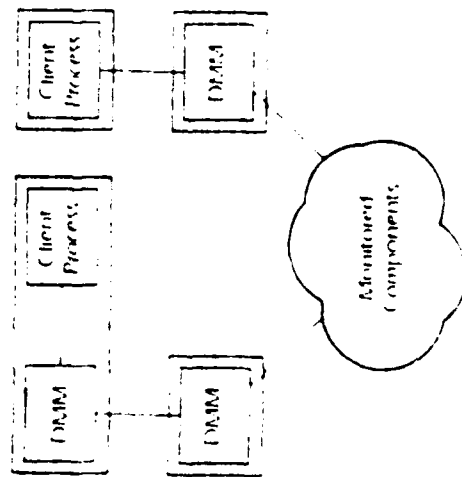
Automated Network Management

- Goals
- ANM System Architecture
- Network Components
- Distributed Management Modules
- Client Processes
- Network Management Protocol

Automated Network Management Goals

- Diverse Components
- Distributed Architecture
- Intelligent Assistance
- User-Friendly Interface

ANM System Architecture



Network Components

- Current Capabilities
 - Mobile Packet Radios
 - G411™ and Butterfly™ Gateways
 - DEDX™ Hosts
 - G40™ Packet Switch Nodes
- Planned Capabilities
 - XNetband Network
 - Multiple Satellite System (MSS)/Cooperating Space Systems (CSs)
 - Internet Private Line Interfaces (IPLIs)

Distributed Management Module Functions

- Translates and Forwards Queries and Control Commands to Commands
- Forwards Queries and Control Commands to Other DMMs When Necessary
- Stores Data Collected From Components and Other DMMs
- Archives Network Management Data
- Maintains Data Catalogs to Support Distributed System

Distributed Management Module Architecture

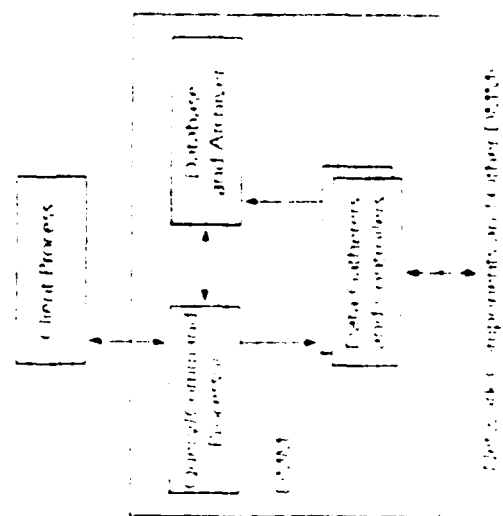


Figure 1. Distributed Management Module Architecture

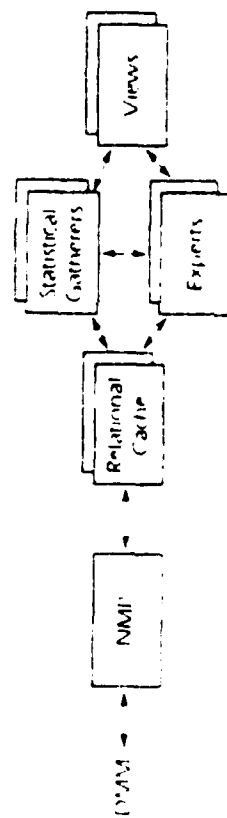
Client Process -- User Interface

- Retrieval
- Presentation
- Alerting
- Explanation

Client Process--Data Analysis

- Arithmetic Calculations
- Statistical Analyses
- Network Algorithms
- AI-Based Reasoning

Intelligent Network Manager



Network Management Protocol

Query Response Protocol (QRP)	Network Component Control Protocol (NCCP)
Management Session Protocol (MSP)	
A Reliable Transport Protocol	

- Supports ANM's Distributed Architecture
- Protocol Specifies
 - ... Command or Query
 - ... Network Components
 - Time of Execution

ANM Status

- Release 2.0
 - Delivered in Winter '87
 - In System Test at SRI
 - Monitors SUN™ Workstations, LSI-11™ Gateways, Packet Radios, and Packet Radio Stations
- Release 3.0
 - Will Deliver in Summer '87
 - Contains New User Interface
 - Adds Monitoring for C/30 PSNs

**Communication Between a Distributed Operating System
and the Network Management System of a
Wide Area Network**

This presentation will discuss the problems involved with using a Wide Area Network (WAN) for communications in a Distributed Operating System (DOS). The methodology for approaching this problem will be presented along with a description of the DOS and how the WAN fits into the system. Protocol relationships between the DOS and WAN will be presented along with a discussion of approaching the intercommunications needs using the Network Management System (NMS). Finally example uses of the WAN by the DOS along with the potential for NMS information will be described.

Presented By: William T. Etter
QRS Associates
P.O. Box 4297
Rome, NY 13440
(315)736-0212

**Communication Between a Distributed Operating System
and the Network Management System of a Wide Area Network**

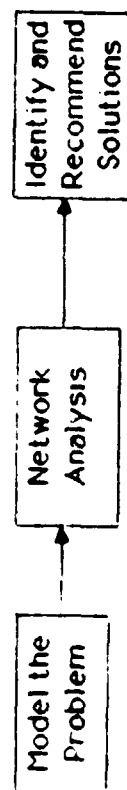
Contract # F19628-86-D-0006

This work is being performed for the Rome Air Development Center
by Dynamics Research Corporation

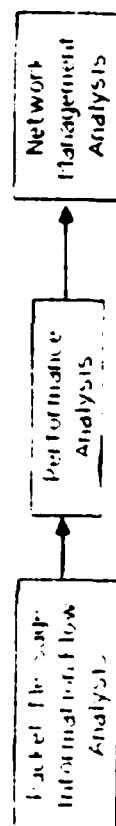
Presented By William T. Etter
QRS Associates
P O Box 4297
Rome, NY 13440
(315) 736-0212

Objective

Determine what information needs to be transferred between a DOS and a WAN to make effective use of the WAN for DOS communications.



Objective: Identify Dos/Wan potential for information transfer



Objective: Network Analysis

Generalized Models not specific implementations

- Identify problems that are representative of the overall system
- Avoid identifying problems that are due to a specific system implementation
- Prepare results that can be used in more detailed follow on work

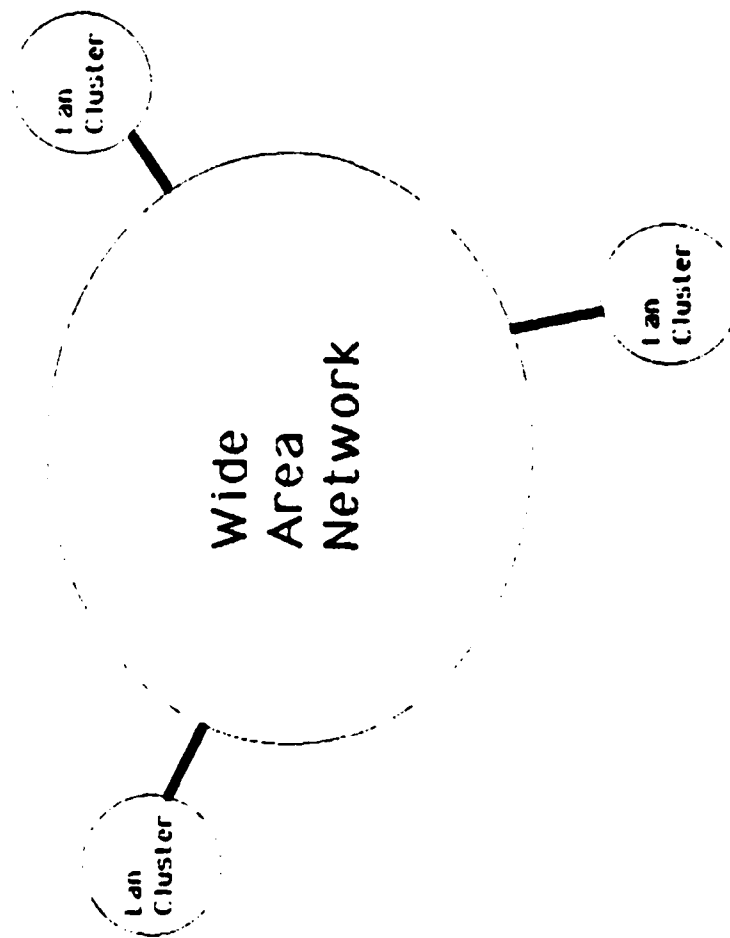
Using a layered concept of protocols & services

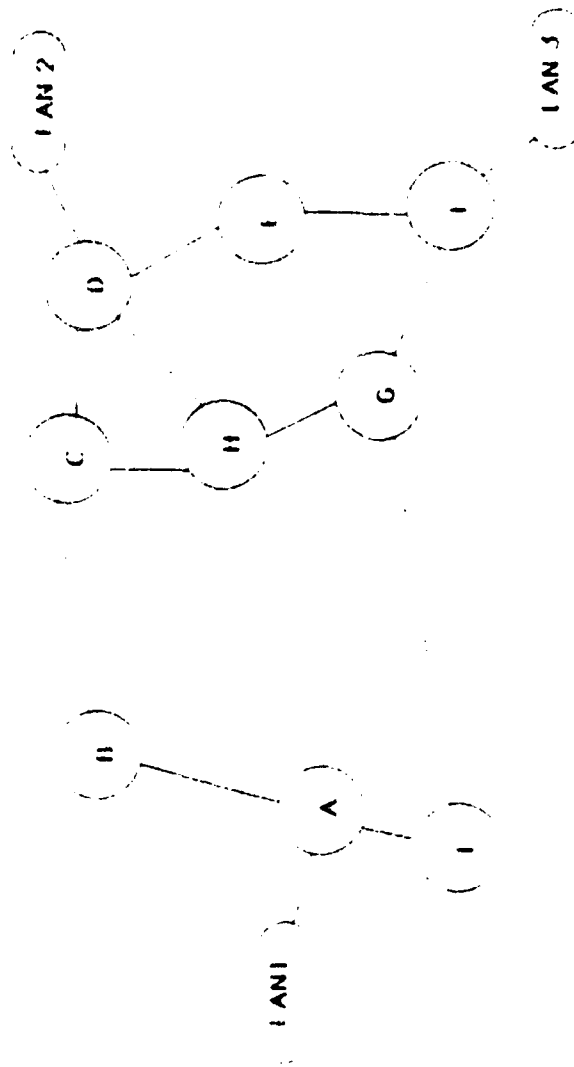
- **DOD Reference Model**
- **Emphasize layer services and functions commonly available in DoD**
- **Specific protocol and algorithm implementations will be avoided**

Distributed Operating System (DOS)

- Operating System
- Distributed among heterogeneous computer systems
- Local Cluster of computers connected by Local Area Network (LAN)
- Can be distributed over a large geographical area using WAN

The DOS/WAN System Concept





WAN Connectivity

AD-A195 374

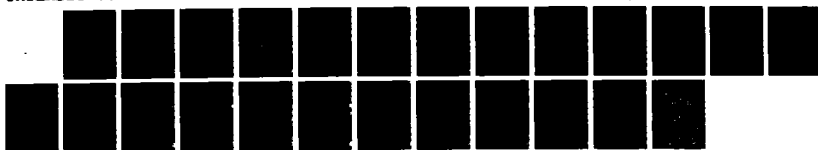
PROCEEDINGS OF THE COMMUNICATIONS NETWORK MANAGEMENT
WORKSHOP (1987) HELD. (U) ROME AIR DEVELOPMENT CENTER
GRIFFISS AFB NY J J SALERNO ET AL. NOV 87
RADC-TR-87-231

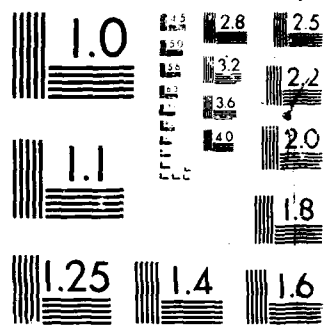
5/5

UNCLASSIFIED

F/B 25/4

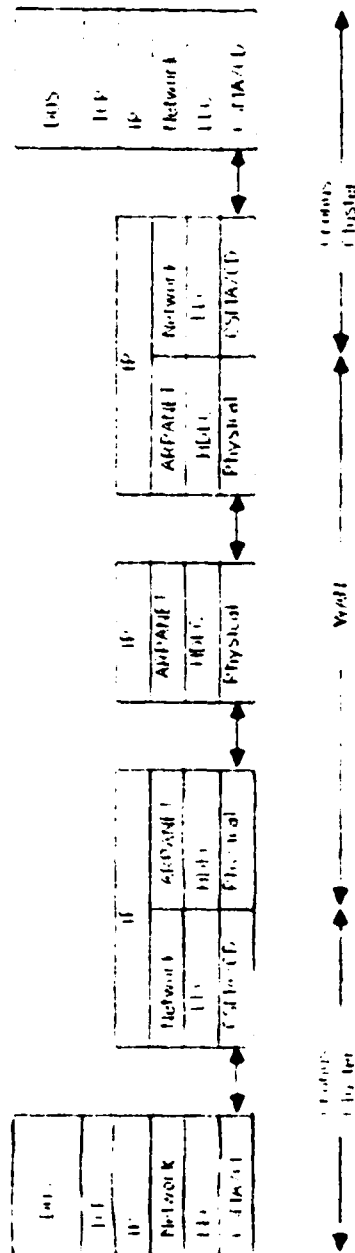
NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

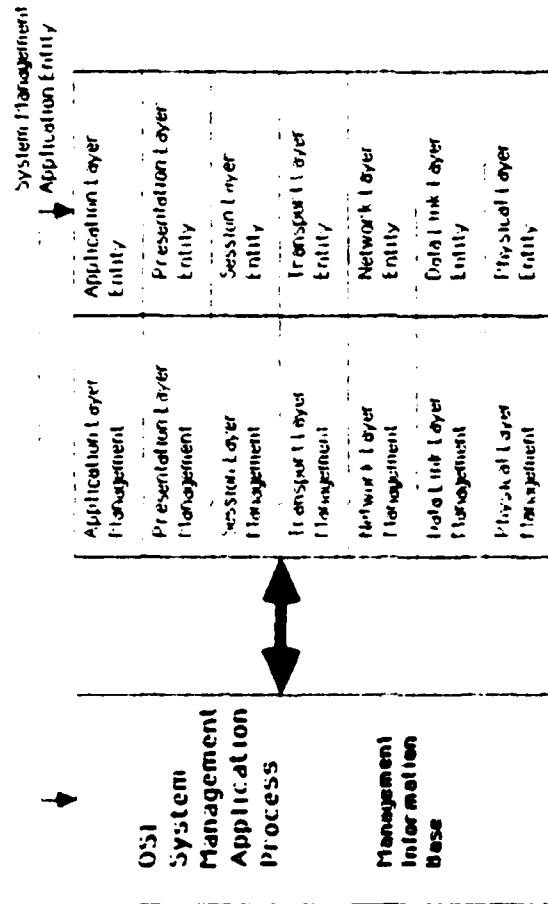
DOS/WAN Protocol Relationships



Network Management

- **Current Network Management**
 - Network Control Center (NCC)/Network Operations Center (NOC)
 - Network Utility (NU)
- **Developing Network Management**
 - OSI

OSI Management Concept



The DOS Model

- **Object Based Client-Server Model**

- Clients

Make requests for resources or services

- Servers

Objects

- **Object Manager**

- Proper operations invoked on proper objects

- Resource Managers

Represents and controls given resources

Both an object and type manager

Could be centralized or distributed

Distributed File Sharing Scenario

- **Common Functions**
 - Updating Files
 - Synchronization
 - Acquiring new storage sites in different LANs
 - Remote Reads or Writes
 - Moving files to another host in another LAN
 - Obtaining Status Information

Busy Paths

Overloaded Gateways

- **File Manager Decisions about WAN**

- From WAN Status, File Manager decides

Which LAN to access for a remote read

Which Network to choose for a backup copy of a file

Whether to delay a large file transfer until a more
lightly loaded period

Scenario: Updating a File Across a WAN

- **Operations**
 - Open a File
 - Read and Write
 - Close
- **Maintenance Functions**
 - Multicast Communications
 - Invoked Asynchronously and/or periodically
 - Could be a function of WAN traffic conditions
 - Load generated by maintenance is a parameter of WAN study
- **Concurrency Control**
 - Supports Distributed Transactions
 - Concurrency Control protocols
 - Commit and recovery protocols

Other DOS/WAN Applications

- Remote Login
- Process Scheduling
- Electronic Mail
- I/O Sharing
- Inter-Process Communication
- Monitor and Control System

Summary

- Sharing resources of WAN is theoretically feasible
- Practically it will not be as highly integrated as using just a LAN
- A large amount of information exchange between DOS and WAN is not expected
 - It is desirable to keep this to a minimum
 - It is desirable to acquire it at a low cost
- Information from WAN may result in a major performance gain
 - We need to determine which information to provide to DOS
- Cost of sophisticated schemes will probably outweigh gains
- In most cases the DOS really needs end-to-end information rather than WAN information

AN INTELLIGENT C3 TERMINAL CONCEPT

**J. W. FORGIE
MIT LINCOLN LABORATORY
2 JULY 1987**

INTELLIGENT C³ TERMINAL

- OBJECTIVE

- PROVIDE A PROFOUND IMPROVEMENT IN THE ABILITY TO COMMUNICATE AND PROCESS INFORMATION ACROSS A BROAD SET OF C³ SYSTEMS THROUGH ALL STRESS LEVELS

- APPROACH

- DEVELOP INTELLIGENT C³ TERMINAL FOR INTERNETTING OVER VARIETY OF COMMUNICATION NETWORKS; ACT AS COMMUNICATIONS EXPERT TO SUPPORT THE COMMANDER:

UNDER NORMAL CONDITIONS —

PROVIDE SECURE DIGITAL VOICE, LOW RATE DIGITAL VIDEO, AND GRAPHICS

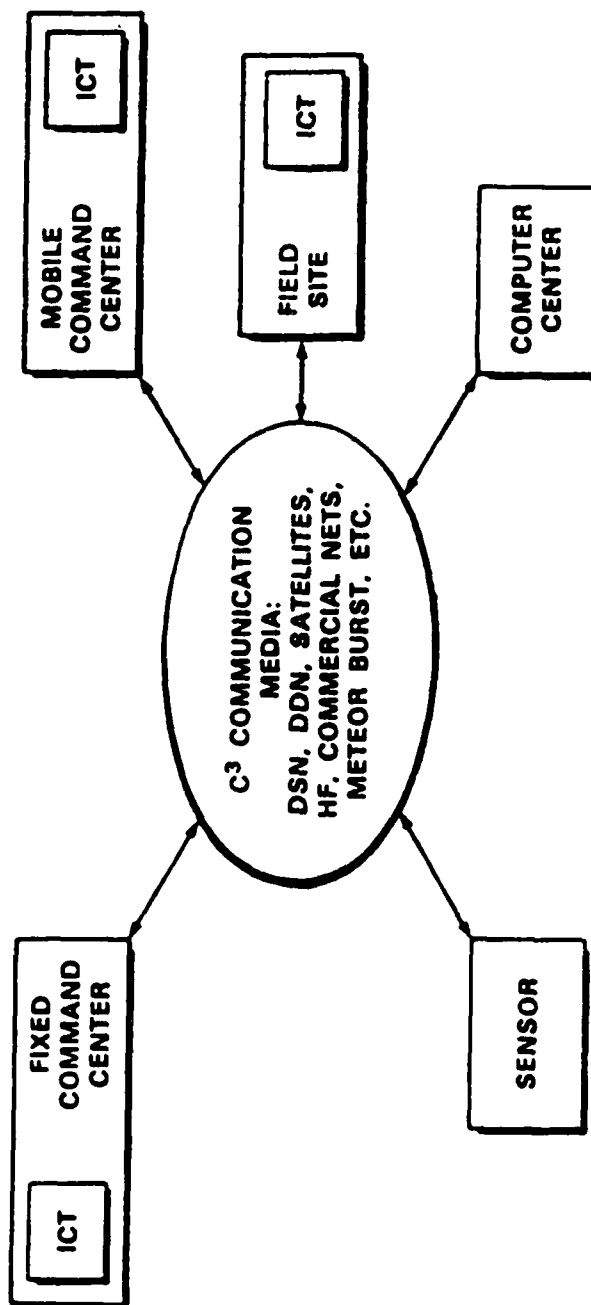
UNDER STRESSED CONDITIONS WITH JAMMING AND NETWORK DAMAGE —

PROVIDE LOW RATE DATA COMMUNICATIONS

UNDER MORE FAVORABLE BUT DEGRADED NETWORK CONDITIONS —

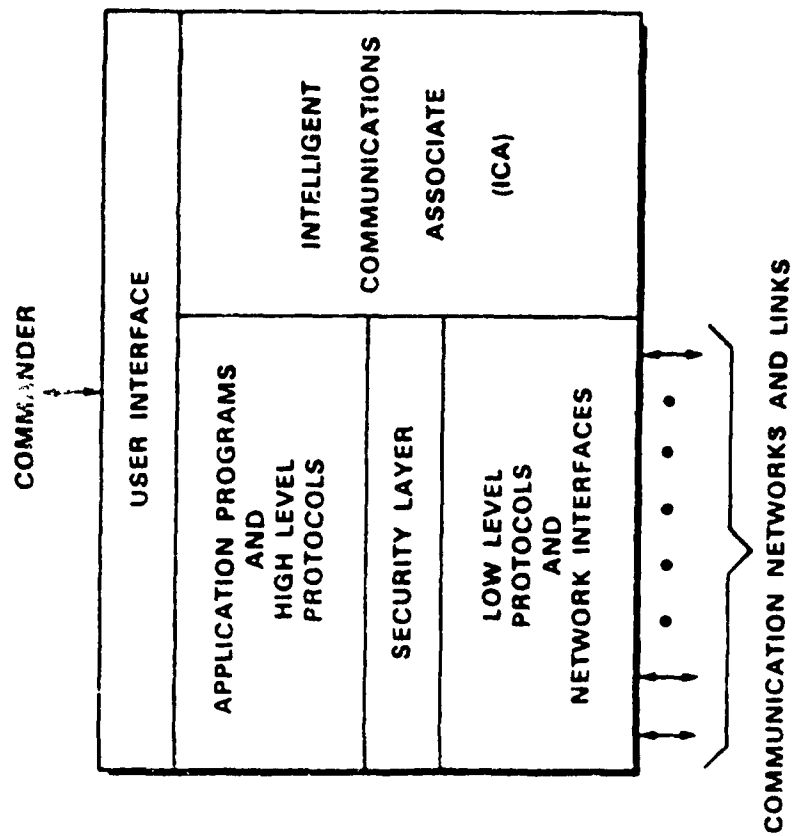
PROVIDE MORE INTERACTIVE COMMUNICATIONS, INCLUDING ULTRA LOW RATE VOICE

C³ SYSTEM ENVIRONMENT FOR INTELLIGENT C³ TERMINAL



ICT = INTELLIGENT C³ TERMINAL

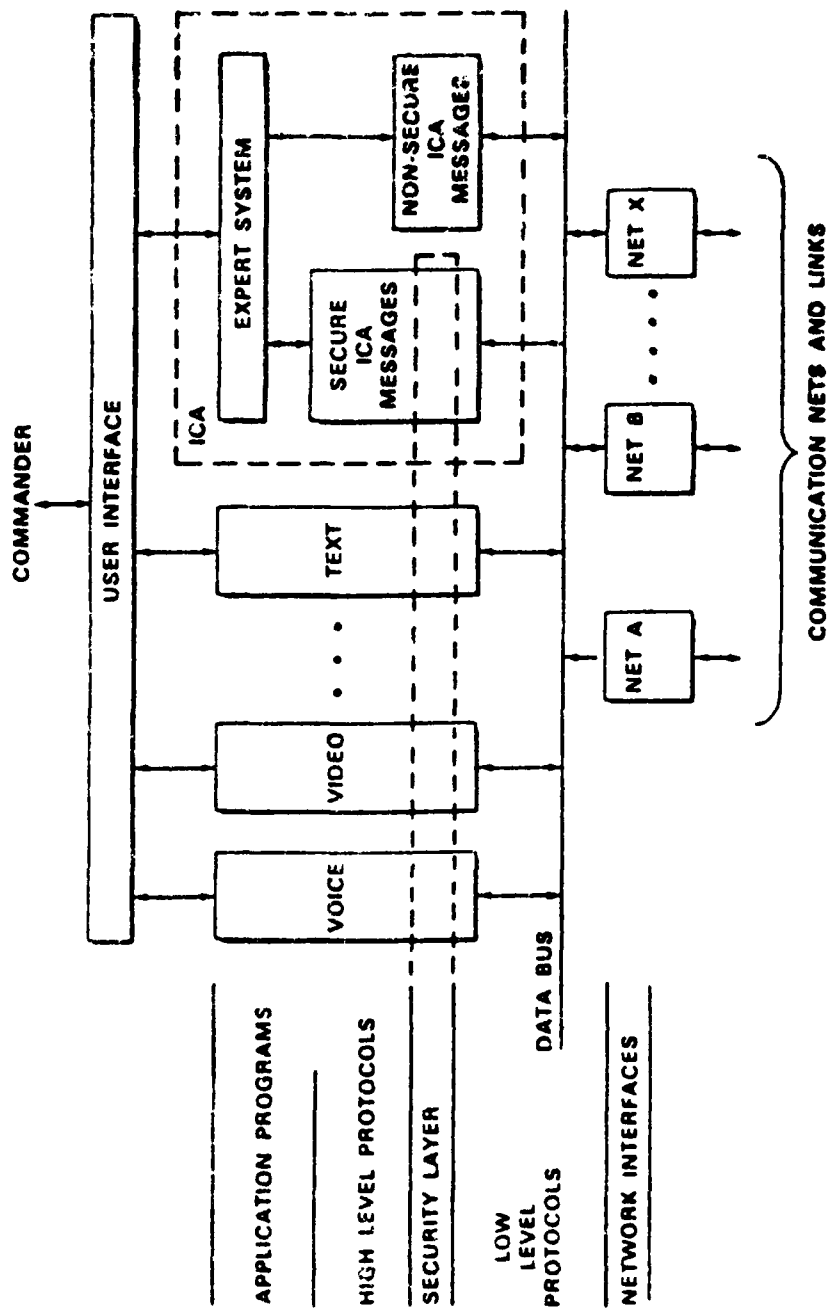
THE INTELLIGENT C³ TERMINAL (ICT)



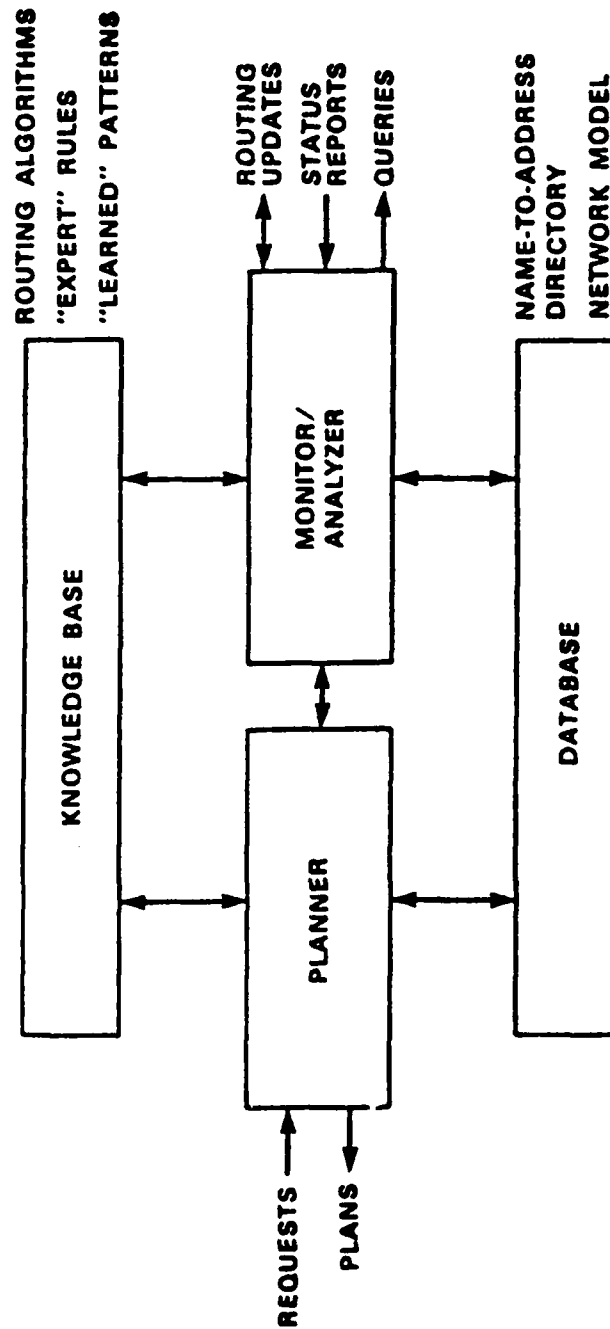
ICA FUNCTIONS

- PROVIDE PLANS FOR ACHIEVING COMMUNICATION GOALS
 - NAME-TO-ADDRESS TRANSLATION
 - ORDERED LIST OF POSSIBLE PATHS WITH CAPACITY ESTIMATES
- MONITOR AND ANALYZE ON-GOING ICT COMMUNICATIONS
 - MODIFY PLANS IF SITUATION CHANGES
- FORWARD TRAFFIC FOR OTHER ICTs
- MAINTAIN ICA KNOWLEDGE BASE AND DATABASE USING:
 - MESSAGES FROM OTHER ICAs
 - SUCCESS/FAILURE OF COMM ATTEMPTS
 - STATUS REPORTS FROM NETS, LINKS, AND APPLICATIONS
 - OTHER INFORMATION (Weather Reports, Intelligence, etc.)

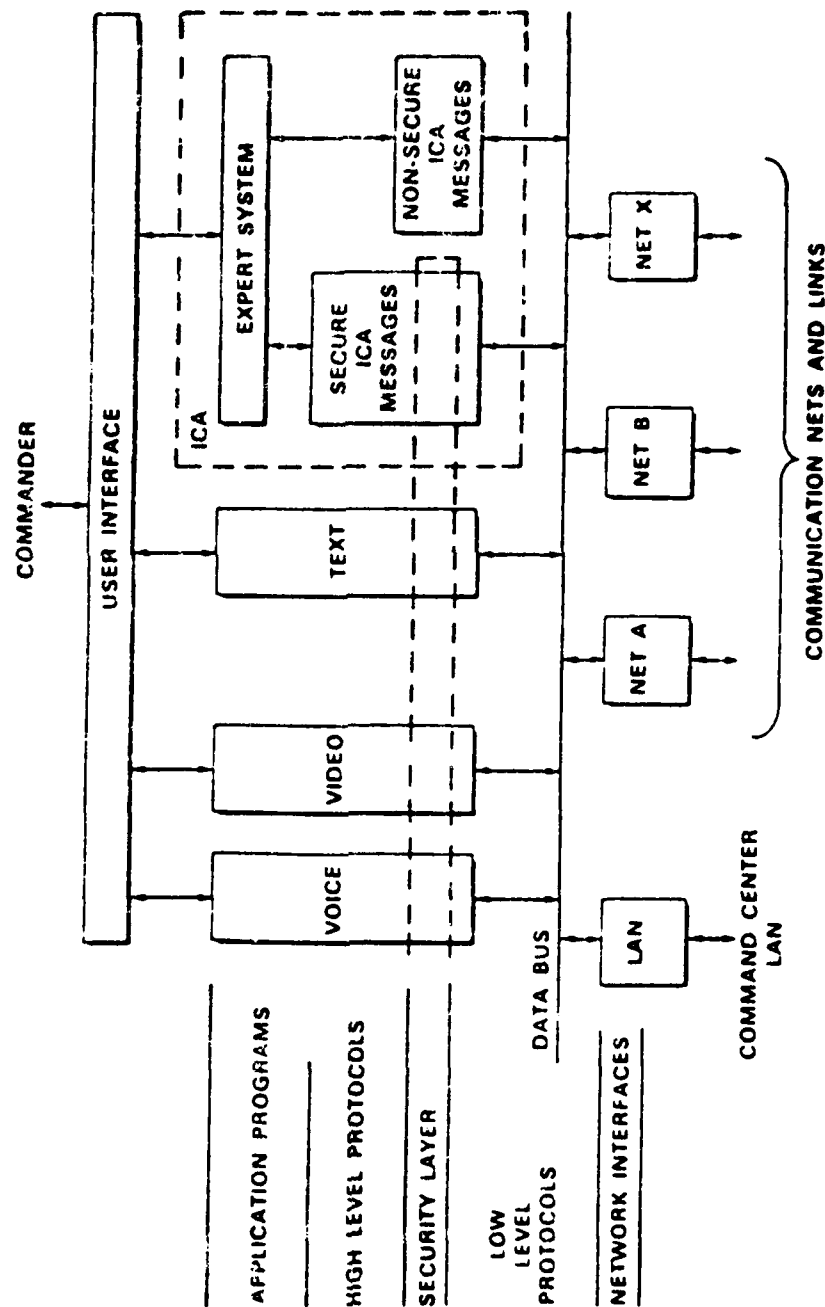
INTELLIGENT C³ TERMINAL ARCHITECTURE



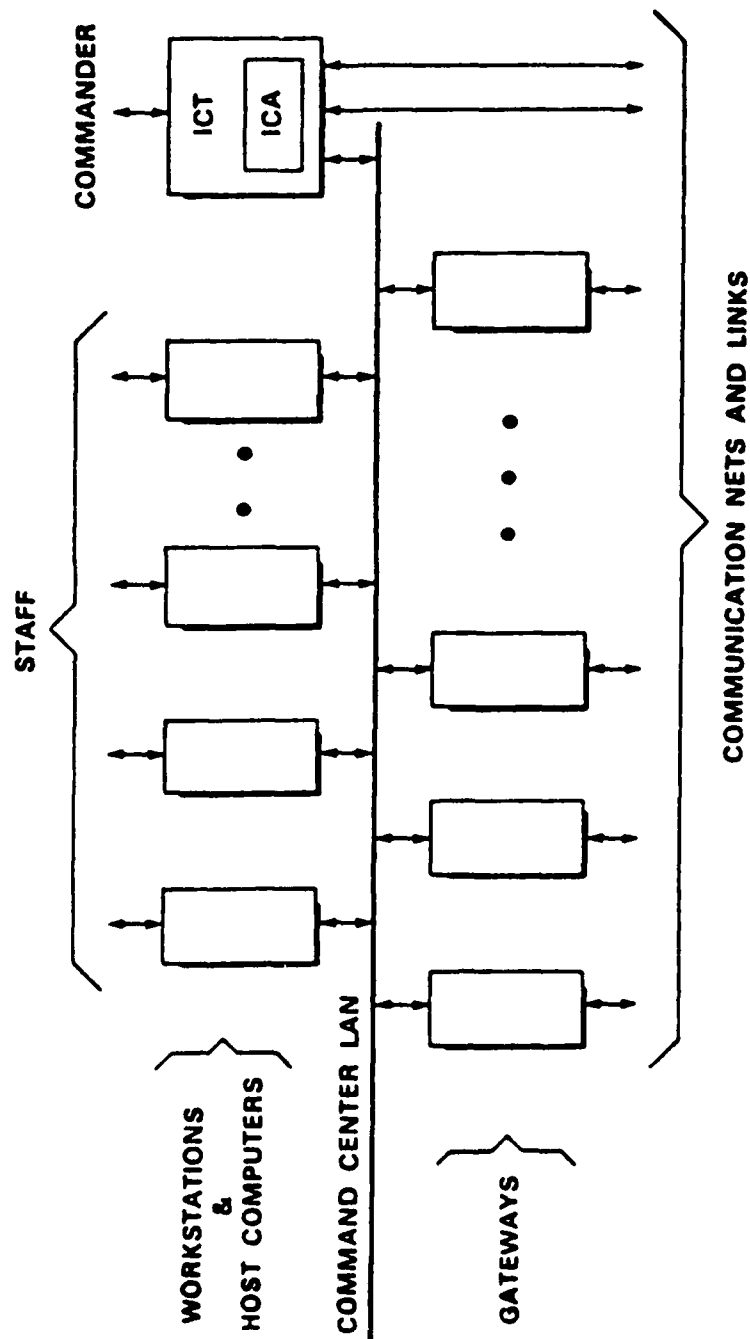
ICA "EXPERT SYSTEM" BLOCK DIAGRAM



EXTENDED ICT ARCHITECTURE FOR COMMAND CENTER APPLICATION



COMMAND CENTER EXTENSION OF ICA CONCEPT



PROTOCOL ISSUES

- **COMMON PROTOCOL WOULD SIMPLIFY ICT DESIGN**
- **EXISTING PROTOCOLS**
 - **ADEQUATE FOR TEXT AND CONTROL**
 - **INADEQUATE FOR VOICE AND VIDEO**
- **PROBLEM IS DELAY VARIABILITY**
 - **QUEUE BUILDUP IN DATAGRAM NETS**
 - **LOW LEVEL RETRANSMISSION IN VIRTUAL CIRCUIT (VC) NETS**
- **VIRTUAL CIRCUIT CONCEPT CAN BE EXTENDED TO SOLVE THE PROBLEM**
 - **DEMONSTRATED IN DARPA PACKET SPEECH EXPERIMENTS**
 - **RESEARCH NEEDED ON EFFECTS OF DAMAGE TO VC NETS**

SECURITY ISSUES

- **KEY DISTRIBUTION**
 - **SECURE COMMUNICATION AMONG MANY PARTIES**
 - **OVERHEAD UNDER STRESSED CONDITIONS**
- **NEED VARIETY OF TECHNIQUES AND RAPID SWITCHING**

RATE-ADAPTIVE COMMUNICATIONS ISSUES

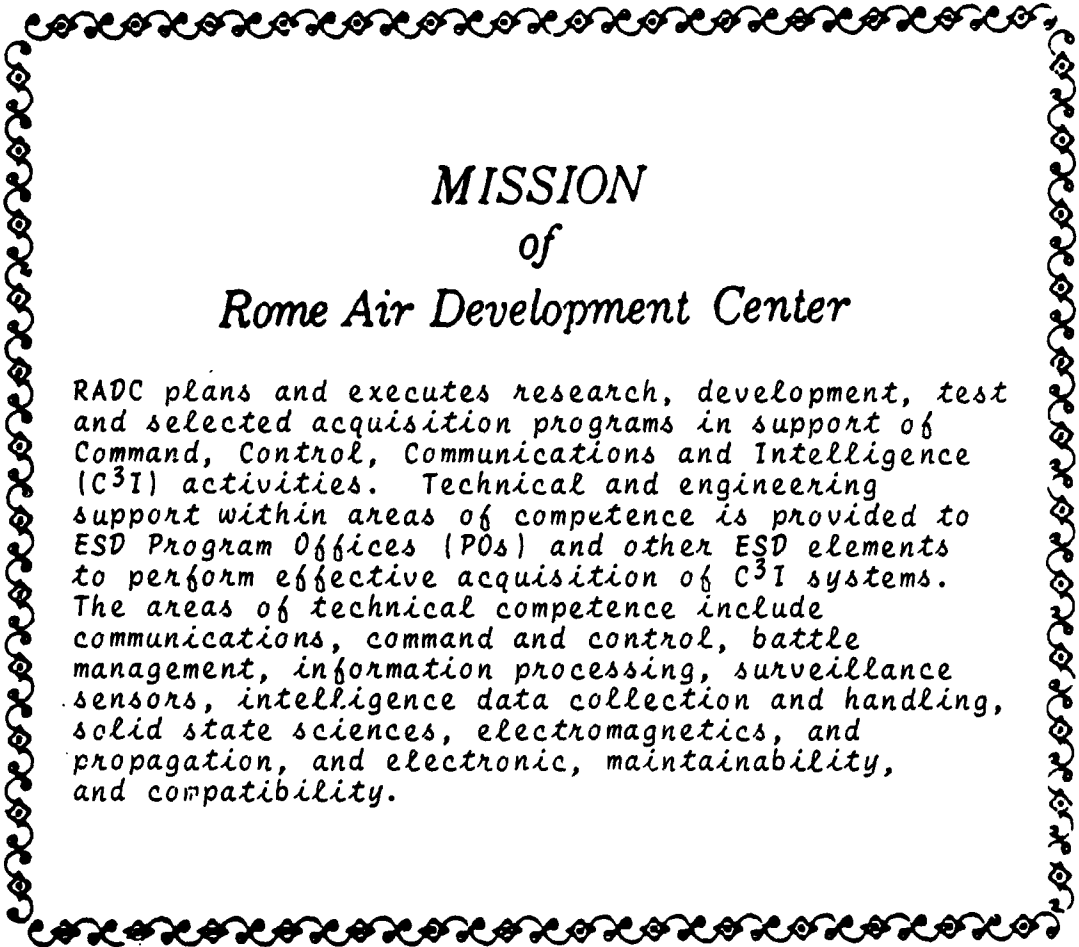
- **SENSING OF NETWORK CAPACITY TO DETERMINE AVAILABLE BIT RATE**
- **DEVELOPMENT OF MULTIRATE SPEECH CODER/SYNTHESIZER**
- **DEVELOPMENT OF ULTRA-LOW-RATE CODING TECHNIQUES INCLUDING VOICE RECOGNITION/SYNTHESIS AT <100 bps**
- **PRIORITIZATION OF DATA TRANSFERS UNDER CRISIS CONDITIONS TO MAXIMIZE EFFECTIVENESS OF INFORMATION TRANSFER**

ICA ISSUES

- ICA IS NOT A CLASSICAL EXPERT SYSTEM
 - NO HUMAN EXPERT TO EMULATE
 - NEED TO COMBINE ALGORITHMS, EXPERT KNOWLEDGE AND LEARNING
- ROUTING UNDER MULTIPLE CONSTRAINTS IS A MATHEMATICALLY INTRACTABLE PROBLEM
 - USUAL NETWORK ROUTING USES SIMPLE COST FUNCTIONS
 - ICA ROUTING WILL REQUIRE HEURISTIC SEARCH
 - PERFORMANCE CANNOT BE ACCURATELY PREDICTED
- ICA MUST LEARN FROM ITS EXPERIENCE
 - NETWORK MODEL WILL VARY FROM ONE ICA TO ANOTHER
 - DESIGNERS CANNOT BUILD IN ALL REQUIRED KNOWLEDGE
 - NEED FOR KNOWLEDGE ACQUISITION UNDER FIELD CONDITIONS POSES AN ADDITIONAL DESIGN CHALLENGE

SYSTEM ISSUES

- **MUST SUPPORT ALL COMMUNICATION NEEDS OF A COMMANDER**
 - **BENEFITS MUST OUTWEIGH COST TO LEARN**
- **MUST OFFER ADVANTAGES IN PEACETIME TO ENCOURAGE USER PROFICIENCY**
 - **USER INTERFACE FEATURES SHOULD HELP**
- **MUST BE INTEGRATED INTO OVERALL C3 ENVIRONMENT**
 - **WILL REQUIRE CHANGES IN OTHER SYSTEMS TO ACHIEVE FULL BENEFIT**



MISSION of Rome Air Development Center

RADC plans and executes research, development, test and selected acquisition programs in support of Command, Control, Communications and Intelligence (C³I) activities. Technical and engineering support within areas of competence is provided to ESD Program Offices (POs) and other ESD elements to perform effective acquisition of C³I systems. The areas of technical competence include communications, command and control, battle management, information processing, surveillance sensors, intelligence data collection and handling, solid state sciences, electromagnetics, and propagation, and electronic, maintainability, and compatibility.

END

DATE

FILMED

8-88

DTIC