Space Packet Network Architectures Trade Space and Potential Solutions

March 6, 2023

Joseph D. Touch

Information Systems and Cyber Division
Engineering and Technology Group

Prepared for:
Space Development Agency
1670 Air Force Pentagon
Washington, D.C. 20330

Contract No. FA8802-19-C-0001

Authorized by: Defense Systems Group

Abstract

This presentation describes the considerations in designing the architecture of a space-based packet network. It addresses the various protocols and mechanisms that define such networks and the ways in which choices affect overall network properties. There are a few dominant architectures that support a wide variety of uses; however, there is no single answer for network design. In most cases, an architectures is defined by the links that interconnect its nodes and whether it supports edge or backbone (cross-network) traffic. Network endpoints and internetwork connections should use the Internet Protocol (IP), enabling ubiquitous information exchange, but an individual network domain can and should use the architecture that matches its link properties best.

Space Packet Network Architectures Trade Space and Potential Solutions

Dr. Joseph D. Touch
Principal Scientist
The Aerospace Corporation

March 6, 2023

Overview

- Satellite communications (SATCOM) packet networks can leverage a few existing ground network architectures
  - *All are commercial off-the-shelf (COTS) and used in existing SATCOM programs*
  - *All support network integration (i.e., interconnecting separately-managed networks)*

- Backbones typically match Multiprotocol Label Switching (MPLS)
  - *Most are multinode, multihop systems based on point-to-point links that align with MPLS*
  - *No need to match or coordinate directly with other MPLS networks, either space or ground*

- Edges vary
  - *Link 16 is its own ground-hosted network that space can join*
  - *Beam-based ground coverage matches Ethernet (MEF) due to broadcast coverage*
  - *Internal space vehicle (SV) matches Ethernet for simplicity and capacity*

- There are some key issues to develop and track
  - *Crosslink interoperation with other COTS and government program systems*
  - *Crosslink design properties*
  - *Internetworking support within the network edges (e.g., the need for IP routing for interdomain transit)*

Some details to be filled in, but a mostly COTS approach is sufficient

General SATCOM Network Architecture Options

- Edge protocols
  - *All support IPv4; many also support IPv6—both enable ubiquitous interoperability with ground systems*
  - *Some also support Explicit Congestion Notification (ECN), critical to latency and jitter minimization, but not always available*

- Backbone protocol (forwarding technology)
  - *Dominant choices are MPLS and Ethernet (direct and two-level encapsulated); others include Synchronous Optical Network (SONET) and IP*
  - *Choices depend on link topology (point-to-point vs. multiaccess), timing requirements (asynchronous vs. synchronous), and network topology (hierarchical tree, spanning tree, regular mesh, irregular)*
  - *Choices vary in size, weight, and power (SWaP) and technology readiness level (TRL)*

- Routing protocol
  - *Options include distributed partial-view dynamic (Ad hoc On-demand Distance Vector [AODV], Routing Information Protocol [RIP]), distributed global-view dynamic (Border Gateway Protocol [BGP], Open Shortest Path First [OSPF]), centralized dynamic (Software-Defined Networking [SDN]-based), and time-varying static*
  - *Each routing protocol will vary in stability, convergence time, and bandwidth (BW) overhead*
  - *All can be on demand or precomputed/predistributed (almanac), which reduces impact of predictable change*

- Backbone topology (SV-SV and SV-ground links)
  - *Multiple node-independent paths (at least two, preferably three) for node and link resilience*
  - *Can otherwise be topology agnostic (can optimize for other properties [i.e., angular diversity, signal strength, dilution of precision [DOP] minimization, etc.])*
  - *Heuristic search methods may be costly or risk inefficient results;*
    geographic routing (Voronoi diagrams) may be more efficient and deterministic ($O(N^2)$) computation cost using open-source algorithms

Network Trade-of-trades Spaces

Use Case Properties						
Mission	**Traffic**	**Message Latency**	**User BW**	**Comm Mode**	**User Location**	**Availability**
Combat cloud	C2	Very Low (<100 ms)	1–500 Kbps	Unicast	Ground	Persistent
Space backhaul	TT&C	Low (<5 sec)	1–500 Mbps	Multicast	LEO	On demand
Air backhaul	Interactive	High (10–50 sec)	1–3 Gbps	Geocast	MEO	Scheduled
Ground backhaul	Teleconferencing	Unbounded	5–10 Gbps	Pub/sub	GEO	
Ground exchange	Streaming		40+ Gbps		Beyond GEO	
ISP	Bulk					

User Constraints						
User Link	**Client Protocols**	**TRANSEC**	**Robustness**	**Connectedness**	**Network Scale**	**Orbits**
RF directed	PPP/PPPoE	LPI/LPD	Strategic	Connected	Tens or fewer	LEO
RF omni	SONET	AJ	Tactical	Disconnected	Hundreds	MEO
Optical directed	Ethernet		Space weather		Thousands	Tundra
Optical diffuse	IP				Unbounded	GEO
Quantum	Link 16					Beyond GEO
	Other (MILCOM)					

Platform Properties				
Payload	**SWaP**	**Power**	**Asset Control**	**Internal Links**
Custom	Low (150 kg)	Low (150 W)	Government	RF directed
COTS	Med (500 kg)	Med (1K W)	Commercial	RF omni
	High	High (10 KW)	Community	Optical directed
				Quantum

Derived Network Properties						
Topology Function	**Naming**	**Routing**	**Autonomy**	**Internal Protocols**	**Management Plane**	**Provisioning Time**
Backbone	Broadcast	Fixed	None	Circuits	NETCONF/YANG	Minutes
Tail/Edge/Stub	Multicast	Scheduled	Partial	SONET	SNMP/MIB	Hours
Peer to peer	Fixed (table)	Dynamic	Full	Ethernet	SDN	Days
Ad hoc				IP		Weeks

Comparison of Typical Satellite Packet Network Architectures

	Property	SONET	IP	Ethernet	MPLS	Ad Hoc Mesh ("MANET")	Success Metric
Mechanisms	Link Traffic Type	Unicast	Unicast or fixed-topology broadcast	Fixed-topology broadcast	Unicast	Topology-selecting broadcast	Match dominant link/traffic type
	End-to-end Protocol	IP	IP	IP	IP	IP	Interoperability
	Backbone Protocol	SONET	IP	MEF (varies, typ. MAC-in-MAC Ethernet)	MPLS	IP	COTS
	Control Plane	Centralized	Central or distributed	Central or distributed	Centralized	Distributed (e.g., AODV)	Central optimizes better
	Forwarding	Preconfigured circuit	IP longest-prefix match	Flat address match	Per-hop label ops (push, pop)	IP longest-prefix match	SWaP and speed
	Routing vs. Orbital Dynamics	Not applicable (GEO)	Scheduled	Scheduled	Scheduled	Automatic, slow convergence	Rapid convergence
Capabilities	Multipath Flow Management	No	No (esp. if using IPsec or HAIPE)	No/difficult	Yes	No	Aggregate capacity
	VLAN (mission separation)	Inherent (circuits)	No	Yes	Yes	No	Mission separation
	Supports Traffic Policing/Shaping	Not applicable	Yes	Yes	Yes	No	Safe from overloading
	Shares Unused Capacity	Limited (VCAT/LCAS)	Yes	Yes	Yes	Yes	Flexibility
	Adapts to Node/Link Losses	No/limited	Yes	Yes	Yes	Yes	Fault tolerance

Most important factor

Cells are colored green when their values are desirable, as per their row's corresponding success metric.

Primary SATCOM Network Architecture Decisions

Three key choices with answers (in red), of which only one is typically local/internal to satellite constellation

- Core link protocol decision (lowest multihop protocol) — *– determined by satellite link type or traffic patterns*
  - *If link types are known or constrained:*
    - If links are point to point or multiswitch, **use MPLS**
    - If links are multiparty (especially 1:many [e.g., down horns], especially if star [single switch]), **use Ethernet**
    - If traffic is already highly aggregated and links are point to point and stable over time, can **use SONET** instead of MPLS
    - NOTE: This topology compatibility supports the link medium access control (MAC) protocol (if needed), whether using standard or custom MAC protocols
  - *If links are part of the design space:*
    - Pick the link above to match the traffic pattern
  - *Use diffsrv to support prioritization*
    - Keep the user-specified diffsrv priority levels to seven or less
    - Rely on edge enforcement (like rush-hour highway metering traffic lights) rather than path-related state (like train rail schedules)
- Tactical edge link protocol decision — *– determined by your edge users*
  - ***Use what your users already use**, if known (e.g., Link 16)*
  - *Otherwise, extend the core link protocol to them, if possible*
  - *Applies to both in-theater and reach-back edges*
- Network layer for interoperability and internetworking — *– determined by "everyone else"*
  - ***Use IPv4***
  - *Include support for IPv6 as dual stack (all IPv4 or all IPv6), assuming endpoint preference or Domain Name System (DNS) preload and "happy eyeballs" choice*
  - *Do NOT try to support IPv4/IPv6 interoperation (IPv4 over IPv6, the converse, NAT64, etc.)*

Most of a satellite packet network architecture is determined by the satellite links and traffic

Typical Point-to-point Network Architecture

- Edge protocols
  - *IPv4, preferably also IPv6 (dual stack with application preference or DNS preload)*
  - *May also include IP routers for interdomain transit*
  - *ECN for low latency and low jitter*

- Backbone protocol
  - *MPLS to support point-to-point links with multipath provisioning*
  - *Quality of service (QoS) and ECN support at intermediate hops to support prioritization with low-delay transit*
  - *IP edge routers for interdomain networking*

- Routing protocol
  - *Almanac based: precomputed and predistributed*
  - *Include simple backup routes for localized failure*
  - *Include potential to use dynamic routing for automatic recovery for nonlocalized failure*
  - *Dynamic routing should support almanac-like (time-varying) context caching and shifting*

A little more automation than ground networks, but basically COTS otherwise

MPLS vs. IP vs. Ethernet Provider Backbone Bridged Network (PBBN) as Backbone Protocols

Property	IP	Ethernet PBBN	MPLS	Success Metric
Addressing	4- or 16-byte hierarchical	6-byte flat	2.5-byte flat	Smaller is better Flat is simpler
Packet Forwarding	Destination address	Egress address	Per-hop label	Per-hop is more flexible
Loop Avoidance	8-bit TTL/hopcount	None (no transient loops) or use TRILL TTL shim	8-bit TTL	Support complex routing and transient loops
Forwarding Table Size	Number of end users	Number of egresses	Number of switch ports	Smaller is better
VPN Size	No limit	4K	1M	Higher is better
QoS (for priority service)	64 levels	8 levels	8 levels	At least 4 for management, high-priority, messaging, bulk transfer
ECN (for low latency)	Yes; independent of QoS	Yes; shared with QoS	Yes; shared with QoS	Avoid queuing delays
Impact of Path Changes	Local	Local	Global	Local impact adapts to changes more quickly

Cells are colored green when their values are desirable, red when undesirable, and orange when in between, as per their row's corresponding success metric.

In some cases, these can be combined (e.g., IP or Ethernet edge with MPLS backbone)

MPLS vs. IP vs. Ethernet

- Firmware – ubiquitous globally at network edge (hosts, services, user devices)
  - *Packet does not change along the path (except to decrement hop count)*
  - *Longest match of destination address prefix (higher SWaP)*
  - *Load balancing or path changes require context indexing (additional SWaP)*

- Ethernet – ubiquitous locally at the network edge
  - *Maps natively to broadcast and multicast*
  - *Supports high-capacity interconnect*
  - *Emerging as onboard alternate to SpaceWire*

- MPLS – widely used in network backbones
  - *Packet is prefixed by tag that can change at each hop (lookup, push, pop)*
  - *Fixed-size tag lookup (low SWaP)*
  - *Load balancing or path changes use packet tag context (no additional SWaP)*

- All
  - *Widely deployed and stable*
  - *Numerous implementations (including software, hardware, and field-programmable gate array [FPGA] IP)*
  - *Numerous test suites*
  - *All CAN be used at edge or as wide-scale interconnect, with varying efficiency depending on link properties and scale*

Other Space Network Protocol Concerns

- Limiting accumulated latency: AQM and ECN
  - *Ensure low-latency transfer, especially through large numbers of hops*
  - *Active Queue Management (AQM) = queuing that doesn't wait until it's full to start "dropping" packets*
  - *Explicit Congestion Notification (ECN) = queueing that flags packets as "would have been dropped"*
  - *AQM + ECN allows endpoints to react to emerging congestion BEFORE packets are dropped (more efficient, avoids retransmission delays, avoids congestion collapse)*

- Link error correction: FEC vs. ARQ
  - *Forward Error Correction (FEC) = transcode that increases delay and BW to allow receivers to recover without needing retransmission; compensates for known delays, but always "burns" overhead*
  - *Automatic Repeat ReQuest (ARQ) = receiver detects losses and requests retransmission; recovery and overhead is adaptive, but results in much larger and more variable delay*
  - *Long multihop systems should optimize for FEC over ARQ*

- Routing choices: path state routing (per-hop label swap) vs. source/segment routing vs. destination address routing
  - *All can be useful; MPLS supports all natively; IP and Ethernet support destination routing easily; IP supports source/segment routing, but can be expensive*

Principles of Protocol Design and Use

Similar to the rules of supervising children

- Don’t ask a question if you don’t NEED to know the answer
  - *Routing protocols exchange information to discover changes, then adapt to those changes*
  - *All routing protocols treat all changes as “surprises” (i.e., unanticipated)*
  - *Satellite network meshes have topologies that evolve very predictably*
  - *That evolution TRIPS UP routing protocols, which require BW and time to recover*
  - *SOLUTION: use an “almanac” of precomputed starting points*
  - *Most of the time, that almanac is sufficient (especially if it includes simple alternate backups)*
  - *If needed, run dynamic routing with the almanac as its starting point*

- Don’t do anything once you don’t want to do a thousand times
  - *Any solution that doesn’t anticipate predictable change will be continually restarting*
  - *That restart will continue until it is predicted (it can’t converge on a moving target)*

J. Touch 2015, with permission.

Principles of Satellite Routing

- Consider the difference between provisioning and routing
  - *Ad hoc "routing" determines the topology AND routes simultaneously*
  - *Ad hoc "routing" works only when "possible" links can be discovered (e.g., via broadcast media)*

- Match the link and routing protocol to the native link properties
  - *For crosslinks and individual downlinks (GEP, airborne, etc.)*
    - Optical links are beginning to dominate space crosslink designs
    - Where optical is not used, highly directional RF with similar limitations is often used for crosslinks
    - Link closure requires precise pointing (optical requires more precise than RF)
    - Link closure requires time (currently 10–100 sec)
    - Both types of links are point-to-point (unicast) and are inefficient for broadcast-based routing protocols (RIP)
    - Both types of links are established before being useful and thus inappropriate for ad hoc routing protocols (AODV)
    - Both types of links match MPLS, ATM, etc.
  - *For ground theater coverage*
    - Broad RF beams are dominant, to increase number of ground users
    - Broad RF is native broadcast, matching Ethernet

General Network Cybersecurity Approach

- Use stable COTS protocols
  - *Available cyber test suites*
  - *Leverage best current practices for cybersecurity*

- Disable capabilities that are not needed
  - *IP options, extension headers (except IPv6 IP security [IPsec] extension header)*
  - *Internet Control Message Protocol (ICMP) messages (except during testing)*
  - *Dynamic routing*
  - *Ethernet tags and encapsulation*
  - *Ethernet signaling (except within an SV)*

- Harden capabilities that are needed
  - *Line-rate processing of IP packets, MPLS tags*
  - *Add application authentication within red network*
  - *Net management using fine-grain access control and locking*
  - *Maintain network boundary between untrusted ground or partner payloads*

- Use a High-Assurance IP Encryptor (HAIPE) boundary to protect everything else
  - *Management plane (behind HAIPE or over telemetry, tracking, and command [TT&C])*
  - *IP signaling needed for endpoint discovery (Address Resolution Protocol [ARP], Neighbor Discovery [ND]) via explicitly managed caches where possible*

Network Control

These in-band protocols should be disabled for security

- MPLS
  - *Label Distribution Protocol (LDP) and MPLS Traffic Engineering (MPLS TE) for peer-based path distribution*

- Ethernet
  - *Bridge Protocol Data Units (BPDUs) for topology discovery*
  - *Address learning for PBBN ingress encapsulation*
  - *Port learning to manage backbone flooding*
  - *Internet Group Management Protocol (IGMP) snooping for multicast configuration*

- IP
  - *IP header options*
  - *ICMP messages*
  - *IGMP and Multicast Lister Discovery (MLD) for multicast endpoint membership*
  - *Protocol Independent Multicast-Sparse Mode (PIM-SM) for multicast router configuration*
  - *Routing protocols (RIP, OSPF, Intermediate System to Intermediate System [IS-IS])*
  - *ARP/ND for Layer 2 address discovery*
  - *Router advertisement (RA) for configuration*

- Upper layer
  - *Interdomain routing (BGP)*
  - *Dynamic Host Configuration Protocol (DHCP) for configuration*
  - *DNS for IP address discovery*
  - *Network Time Protocol (NTP) for time coordination (unless via encrypted tunnel with a security-based hierarchy)*

Use these protocols sparingly, if at all

Cybersecurity Issues

Protocol/System Component	**Corresponding Cybersecurity Approach**
• Internet layer	
– *Options and extension headers disabled (except IPv6 IPsec extension header)*	*- IP extensions **disabled** (except as needed for HAIPE)*
– *No on-path fragmentation (IPv4 DF=1)*	*- IP in-network functions **disabled***
– *Differentiated Services Code Point (DSCP), ECN per HAIPE specification*	*- Cross-domain solution for IP path signaling as per **HAIPE***
– *ARP for IPv4 link address discovery*	*- IP discovery within **red network** only*
– *ICMP (signaling) limited or disabled (except during testing)*	*- IP signaling within **red network** only and largely **disabled***
– *Routing protocols not used*	*- IP routing **disabled**; management distributes routes (HAIPE protected)*
• Link layer	
– *MPLS label distribution not used*	*- MPLS control plane **disabled***
– *Ethernet pause frames for flow control within SV only*	*- Ethernet signaling **local** within SV only*
– *Ethernet switching within SV only*	*- Ethernet learning and port discovery **local** within SV only*
– *No Q-tags (VLANs, PBNs) or MAC-in-MAC (PBBNs) encapsulation*	*- Ethernet extensions **disabled***
• Application layer	
– *Endpoint identity authentication to differentiate multiple host/service endpoints*	*- **Application authentication** within/behind HAIPE tunnel e.g., Transport Layer Security (TLS) or Datagram TLS (DTLS)*
• Management	*- Management plane within **red network** only*
– *Centralized, in the spirit of SDN (but not SDN protocols)*	*- Avoid services not needed; use open Internet standards*
– *NETCONF protocol, YANG data model*	*- NETCONF provides fine-grained **access control and locking***
• Performance (general)	
– *Support for line rate at the minimum packet size, as is typical for Ethernet, MPLS, IP*	*- General performance requirements avoid data plane denial of service*

Network Data Transfer Issues

- Throughput
  - *Command and control*
  - *Operation*
  - *Partner services*
- Latency
  - *Data delivery delay*
  - *Variation in data delivery delay (jitter)*
- Information protection
  - *Authentication, nonrepudiation, and integrity protection*
  - *Privacy*
- Resilience (capability protection)
  - *Multiple network paths to operate through node and link failures*

Lots of Ideas that Can/Do Apply

But there's not much about how any of this should drive architecture

• SDN/central management	Separation of control/data planes has been around for decades, including Simple Network Management Protocol (SNMP) and NETCONF; this is just its newest variant
• Pseudowire	Many methods for circuit emulation, but use only when absolutely needed
• IPv4 vs. IPv6	Use IPv4 or consider dual stack; avoid trying to combine directly and focus low-latency applications on explicit selection or preloaded DNS for "happy eyeballs" choice (RFC 8305)
• DiffServ vs. IntServ	DiffServ is the industry standard and scales, but does not reserve resources; IntServ should be avoided as brittle and not scalable
• TOR/onion routing	Hiding routing info and endpoint activity can be interesting, but always requires a conventionally addressed network underneath (i.e., these are "applications")
• COTS protocols	Generally should be assumed, though may want to use limited variants (fewer options/extensions). Nearly never useful to mandate particular protocols beyond the data plane.
• Overlays	Supported in nearly all network core protocols; useful for provisioning; these are typically relevant for only the black core, not red edges and they should not be relied upon for information separation.

Issues, Approaches, and Buzzwords to Avoid – and Why

Avoid solutions that solve problems unique to other people/domains

• “for satellites”	Satellite Internets have existed since 1972, commercial since 2003, and widely since 2011
• “for pLEO”	Proliferated low Earth orbit (pLEO) is similar to ground nets (not much difference)
• IP backbone	IP routing is useful at the network edge, not typically in the core
• TCAMs	These are widely used for deep packet inspection (DPI), not packet forwarding
• MANET	This is useful for omni RF with link connectivity choices, but not for preoriented two-party links
• OSPF, BGP	These are unnecessary as a primary routing mechanism due to predictability of orbits; “don’t ask questions when you already know answers”
• Geographic routing	This doesn’t work due to the “corridor problem,” except in very particular and limited constellations
• Segment routing	This reinvents source routing, which is just MPLS that only pops tags (doesn’t push tags enroute)
• DTN	This is used when connectivity gaps are hours/days and reinvents a mechanism email provides
• SDN/OpenFlow	This is useful to avoid vendor hardware lock-in, but not much otherwise
• ICN/CCN	This is not a network layer; at best, it’s distributed web caching at the application layer
• NFV/NSV	These are ways of implementing services at the application layer, not forwarding link/network packets

Acronyms

AJ	anti-jam, the ability of an information signal to prevent interference either by avoidance (passive) or direct response (active)
AODV	Ad hoc On-demand Distance Vector, a MANET routing protocol
ARP	Address Resolution Protocol, maps IP addresses to Ethernet addresses
ARQ	Automatic Repeat ReQuest, a mechanism for error recovery using retransmission after errors are detected
ATM	Asynchronous Transfer Mode, a Layer 2 protocol based on fixed-size, very small (53 byte) cells
BGP	Border Gateway Protocol, a routing protocol used between network domains
BPDU	Bridge Protocol Data Unit, the control protocol that enables Ethernet switches to automatically configure their routing
BW	bandwidth, a unit of information transfer capacity per unit time (bits per second)
C2	command and control, types of information based on short, reliable exchanges
CDS	cross-domain solution, a mechanism that allows information to transit from high (more secure) to low (less secure), based on limited types of content
COTS	commercial off-the-shelf, often implying ubiquitous adoption by a vendor or user community
DF	don’t fragment, a signal bit in an IPv4 packet that prohibits on-path refragmentation
DHCP	Dynamic Host Configuration Protocol, a mechanism for automatic configuration of end-host IP address, routing, DNS, etc.
DIFFSRV	differentiated services, an approach to QoS based on edge policing and internal prioritization, but not internal or on-path resource reservation
DNS	Domain Name System, a mechanism that maps human-readable names into IP addresses
DOP	dilution of precision, a model for error propagation in satellite navigation
DOS	denial of service, the effect of overwhelming resources to prevent others access
DSCP	Differentiated Services Code Point, a bitfield in an IP header that indicates the priority of a packet
DTLS	Datagram TLS, a mechanism for authenticating and protecting the integrity of individual messages (typically within one packet)
DTN	Delay/Disruption Tolerant Networking, a protocol that allows message paths that are discontinuous, where messages stop as needed (similar to email)

Acronyms

ECN	Explicit Congestion Notification, a mechanism where network congestion can be avoided before packets are dropped and a key capability to reducing latency
FPGA	field-programmable gate array, a type of reconfigurable hardware
GEO	geosynchronous Earth orbit
GEP	ground entry point, the location where satellite information transits from space to ground (or the converse)
HAIPE	High-Assurance IP Encryptor, a standard based on a subset of IPsec used to support communications security
ICMP	Internet Control Message Protocol, the signaling protocol for the Internet that indicates when and how errors occur
ICN	Information-Centric Networking, an application-layer mechanism to associate information with its index inside a network; also known as NDN
IGMP	Internet Group Messaging Protocol, a protocol that manages how IPv4 multicast works in edge networks (see MLD)
INTSRV	integrated services, an approach to QoS based on internal or on-path resource reservation
IP	Internet Protocol (e.g., IPv4 [version 4] or IPv6 [version 6])
IPsec	IP security, the protocol extensions by which IP packets are encrypted, authenticated, and integrity protected
IS-IS	information system to information system routing protocol, a routing protocol used within a network domain
ISP	Internet service provider, a generic term for a system that provides Internet connectivity to its users
LCAS	link capacity adjustment scheme, a SONET mechanism for dynamically modifying circuit BW (often used with VCAT)
LDP	Label Distribution Protocol, a mechanism by which MPLS switches can self-configure
LPI/LPD	low probability of intercept/low probability of detection, goals for communications security that involve receiving or interfering with the signal itself
MAC	Medium Access Control, a protocol for shared access to a multiparty communications medium, but also a nickname for an Ethernet address or header
MANET	mobile ad hoc network, a mechanism that both provisions and routes among a set of nodes typically interconnected via multiparty communication links
MEF	Metro Ethernet Forum, a standards body and their standards for communal configuration of Ethernet networks to enable internetworking
MEO	medium Earth orbit

Acronyms

MIB	management information base, a database of network configuration parameters managed using SNMP
MILCOM	military communications, sometimes MILSATCOM (“SAT” for satellite)
MLD	Multicast Listener Discovery, a protocol that manages how IPv6 multicast works in edge networks (see IGMP)
MPLS	Multiprotocol Label Switching, a protocol that swaps fixed labels based on path information stored at switches
MPLS TE	MPLS Traffic Engineering, a protocol and mechanisms for coordinating resources along an MPLS path
NAT64	network address translation between IPv6 and IPv4, a stateful mechanism that rewrites IP headers to enable interoperation between IPv4 and IPv6 endpoints
ND	Neighbor Discovery, the address lookup in IPv6 that replaces ARP
NDN	Named Data Networking, a synonym for ICN
NETCONF	Network Configuration Protocol, the more modern variant of SNMP used with YANG models
NFV	network functions virtualization, a mechanism that deploys functions and services inside the network
NSV	network service virtualization, a synonym for NFV
NTP	Network Time Protocol, a distributed application that synchronizes host time
OSPF	Open Shortest Path First, a routing protocol used inside a network domain
PBBN	Provider Backbone Bridge Network, an Ethernet VLAN based on MAC-in-MAC encapsulation
PBN	Provider Bridge Network, a network that connects a PBBN to a customer network
PIM-SM	Protocol Independent Multicast-Sparse Mode, a protocol for configuring multicast between edge networks
pLEO	proliferated low Earth orbit, a constellation composed of a large number of satellites at low Earth orbit
PPP	Point-to-Point Protocol, a generic protocol for carrying packets over two-party links
PPPoE	PPP over Ethernet, a protocol for using PPP inside Ethernet packets
pub/sub	publish/subscribe, a service architecture in which information is distributed (published) to receivers indicating interest (subscribers)

Acronyms

QoS	quality of service, a traffic prioritization mechanism based on traffic labels and differential queueing
RA	route advertisement, a protocol message used in IPv6 for endpoint self configuration
RF	radio frequency, referring to any signal using photons, but not based on lasers
RFC	request for comments, a protocol standards or operational advice document of the Internet
RIP	Routing Information Protocol, a routing protocol used inside a network domain
SATCOM	satellite communications
SDN	Software-Defined Networking, a network management method based on centralized control of distributed devices; may also refer to specific protocols therein
SNMP	Simple Network Management Protocol, a protocol for configuring and monitoring network devices using MIBs
SONET	Synchronous Optical Network, a protocol for time-coordinated virtual circuits
SV	space vehicle
SWAP	size, weight, and power, the primary constraints for space-based devices
TCAM	ternary content-addressable memory, an indexing device that allows three values—0, 1, and X (don’t care)
TLS	Transport Layer Security, a protocol for encrypting the contents of TCP connections
Tor	The Onion Router, a mechanism for VPNs based on many layers of protocol encapsulation
TRILL	Transparent Interconnection of Lots of Links, a protocol layered between Ethernet headers that adds a TTL field, allowing use of other routing protocols
TRL	technology readiness level, a measure of the maturity of a technology, especially for operational use in space
TT&C	telemetry, tracking, and command, a very-low-BW channel used for SV initialization, monitoring, and recovery
TTL	time-to-live, an IP header field that decrements based on both time and hop count
VCAT	virtual concatenation, a mechanism in SONET for aggregating capacity across virtual circuits
VLAN	virtual local area network, a network whose traffic is labeled or encapsulated to allow several concurrent networks to share links
VPN	virtual private network, a network composed of (or extended by) encrypted links
YANG	Yet Another Next Generation, a model for representing network configuration information used with NETCONF

External Distribution

REPORT TITLE

Space Packet Network Architectures Trade Space and Potential Solutions

REPORT NO.	PUBLICATION DATE	SECURITY CLASSIFICATION
TOR-2023-00848	March 31, 2023	UNCLASSIFIED

Dr Michael Pagels
SDA
Pagels, Michael A CIV OSD OUSD R-E (USA)
<michael.a.pagels.civ@mail.mil>

David R McKeeby
SDA
David R McKeeby, CTR OSD OUSD R-E(USA)
<david.r.mckeeby.ctr@mail.mil>

Timothy Mudge
SDA
Timothy B Mudge CIV OSD OUSD R-E(USA)
<timothy.b.mudge.civ@mail.mil>

Rick Oleszczuk
SDA
Oleszczuk, Rick K CTR (USA)
<rick.k.oleszczuk.ctr@mail.mil>

LtC Daniel Dierks
SDA
Dierks, Daniel A LCDR USN USSF SDA (USA)
<daniel.a.dierks.mil@mail.mil>

Maria-Dolores Wong
SDA
maria-dolores.wong.civ@mail.mil

APPROVED BY_____ DATE_____
(AF OFFICE)

AEROSPACE REPORT NO.
TOR-2023-00848

Space Packet Network Architectures Trade Space and Potential Solutions

Cognizant Program Manager Approval:

Jack B. Clarke, PRINCIPAL DIRECTOR
NATIONAL SPACE SYSTEMS ENGINEERING
DEFENSE SYSTEMS OPERATIONS
DEFENSE SYSTEMS GROUP

Aerospace Corporate Officer Approval:

Martin Whelan, SENIOR VP DEFENSE SYSTEMS GROUP
OFFICE OF EVP

SQ0521

AEROSPACE REPORT NO.
TOR-2023-00848

Space Packet Network Architectures Trade Space and Potential Solutions

Content Concurrence Provided Electronically by:

Joseph D. Touch, PRINCIPAL ENGINEER/SCIENTIST
INFORMATION SYSTEMS & CYBER DIVISION
ENGINEERING & TECHNOLOGY GROUP

Technical Peer Review Performed by:

Goran Scuric, SENIOR ENGINEER SPECIALIST
NETWORK SYSTEMS DEPT
COMMUNICATION & NETWORK ARCH SUBDIV
ENGINEERING & TECHNOLOGY GROUP

Robert M. Liang, SENIOR ENGINEER SPECIALIST
COMMUNICATION SYSTEMS ENGINEERING DEPT
COMMUNICATION & NETWORK ARCH SUBDIV
ENGINEERING & TECHNOLOGY GROUP

Howard D. Feil, SENIOR PROJECT LEADER
CYBERSECURITY AND ADVANCED PLATFORMS
INFORMATION SYSTEMS & CYBER DIVISION
ENGINEERING & TECHNOLOGY GROUP

SQ0521

AEROSPACE REPORT NO.
TOR-2023-00848

Space Packet Network Architectures Trade Space and Potential Solutions

Timothy A. Goff, SENIOR ENGINEER SPECIALIST
CYBER ENGINEERING DEPARTMENT
CYBERSECURITY AND ADVANCED PLATFORMS
ENGINEERING & TECHNOLOGY GROUP

Xinyu Wang, SENIOR PROJECT LEADER
NETWORK SYSTEMS DEPT
COMMUNICATION & NETWORK ARCH SUBDIV
ENGINEERING & TECHNOLOGY GROUP

SQ0521