LOCKHEED MARTIN
We never forget who we're working for®

EADGE-T

Enterprise
System Design Package (SDP)

ANNEX E - COMMUNICATIONS CAPABILITIES

CDRL Data Item EADGET-SDP--C012.0 Annex E-Rev 5.0 dated 04 Jun 2020

Prepared by:
Lockheed Martin Corporation
Lockheed Martin Global, Inc (LMGI)
9970 Federal drive
Colorado Springs, CO 80921

This Page Intentionally Left Blank

Document Change Log

ISSUE/REVISION	DATE	REASON FOR CHANGE
Rev 1.0	10 Dec 2014	Initial SDR Release.
Rev 2.0	24 Apr 2015	Updated to address AIs and TBXs for SDR.
Rev 3.0	15 Jan 2016	Submission tied to L0 SDR held in Oct 2015.
Rev 4.0	11 Mar 2019	Document updated to reflect 0.7 design baseline
Rev 4.0R1	07 Aug 2019	Document updated to address AFAD provided comments
Rev 5.0	04 Jun 2020	Updated to provide additional network switching capabilities

Document To Be Determined (TBD)/To Be Required (TBR) Matrix

PARA, FIGURE, TABLE	TBD/TBR DESCRIPTION	DUE DATE
	none	

Table of Contents

List of Figures

List of Tables

1 INTRODUCTION

1.1 EADGE-T Communications Overview

The Emirates Air Defense Ground Environment - Transformation (EADGE-T) system includes a robust enterprise network and communications infrastructure, which supports communications among system elements including Command and Control (C2) facilities, military and civilian agencies, non-us coalition forces, sensors, air and ground-based weapons systems. The EADGE-T communications infrastructure provides voice and data exchange services which leverage redundant equipment and multiple links to provide resilient communications with service level guarantees that ensure the integrity of time sensitive traffic. The EADGE-T communications infrastructure uses multiple network technologies to support the current mission requirements and long-term EADGE-T objectives including adaptability and extensibility.

This annex provides the basis for the design of the EADGE-T enterprise communications capabilities including the services provided, key technologies used, architectural elements and planning and management capabilities. The communications design for EADGE-T that is described in this Enterprise Annex provides an overview which is further detailed in the Communications description provided in document C012.4.0.

1.2 EADGE-T Communications Definitions

To the maximum extent possible, EADGE-T Communications makes use of accepted industry and military terms, definitions and acronyms. Definitions used in EADGE-T are provided in EADGET-SDP-C012.0 – Enterprise SDP Annex B Integrated Dictionary AV-2.

1.3 Communications Architecture in the EADGE-T SOA

The design of the EADGE-T system makes use of modular components which support an extensible hardware and software architecture. Thus, while deployed EADGE-T sites support different functions and capabilities, communications components including redundant network routers and switches, use identical design concepts to provide resilient connectivity. The use of common components and design elements results in a system which not only provides high availability but also provides:

- Consistency – By using common hardware, software and/or firmware components the occurrence of any operational issues will be more predictable and can be more readily resolved
- Sustainability – Common maintenance and repair procedures are applicable across the EADGE-T system
- Supportability – Logistics are easier to manage given the limited number of components and Line Replaceable Units (LRUs) required.

In addition, the use of proven Internet technologies with common commercial communications components, and software elements which provide network centric and Service Oriented Architecture (SOA) interfaces, allow new communications and operational capabilities to be added to the system over time.

The modular design of the communications system supports the secure exchange of information by using access controls which protect distributed enclaves from intrusion attempts using attack prevention and detection methods, anti-virus signature scanning, data encryption and information separation. The network components selected are based on a unified family of commercial components that are scaled to meet the performance and functional requirements of each EADGE-T site and configured using structured device templates.

Software components which support the ability to manage, control and access communications capabilities are based on a structured architecture that allows the integration of new functional capabilities. The modular software design provides support for current tactical radio control functions as well as, the ability to extend radio communications capabilities in the future to support the introduction of new radio models and capabilities using software-defined radio technologies. The

modular approach to communications software supports the integration of communications functions with mission-focused command and control applications using EADGE-T Common Services.

In addition to the modular approach used in both communications hardware and software, the design of the EADGE-T network is based on relevant military and commercial standards. The use of standards-based IP packet technologies supports the convergence of voice and data services over a single network infrastructure. EADGE-T makes use of optical and other transport technologies provided by the UAE including the Al Sharyan fiber optic backbone (FOBB), the Next Generation Network, dedicated fiber connections, SATCOM, broadband, and microwave networks. These transport networks have been adapted to support IP communications which support the integration of new capabilities so that the EADGE-T system can evolve to meet future AFAD mission requirements.

1.3.1 Voice Communication as a Service

EADGE-T uses converged IP communications to provide network voice services using Voice over IP (VoIP) and Radio over IP (RoIP) technologies. Both VoIP and RoIP are based on the same core technologies, although within the EADGE-T system VoIP services generally refer to voice calls established between local and remote Operators and include IP telephony services, while RoIP technologies are used to support tactical voice communications including air/ground radio communications. Thus, RoIP services generally require explicit pre-established voice radio configuration settings to support the exchange of fixed frequency or secure voice communications and/or data communications.

In order to provide tactical radio configuration services across EADGE-T, a generalized service level interface is provided that supports a range of radio models from different manufacturers. At present radio manufacturers have not developed a common or generic interface that can be used to modify RF settings regardless of the make and/or model of a radio. Rather, it is common for different radio models from the same manufacturer to use different radio configuration interfaces, e.g., Thales TRG-5400 and F@stnet radios.

The EADGE-T communications design solves this problem by providing a service level interface that can communicate with agent software modules to support the specific configuration requirements of each radio model. Radio control service level interfaces are provided by the Tactical Radio Configuration and Control (TRCC) server and are accessible via Common Services. The TRCC is a functional component of the Network Management subsystem which supports radio control and management functions. The TRCC server provides interfaces to different radio control agents to support the specific radio commands required for each supported radio. The TRCC capabilities are shown in Figure 1-1. The IP Conversion appliances (Stream Adaptation Systems, also known as SAS boxes) shown in this figure are used when required to support custom or proprietary vendor radio interface connections.

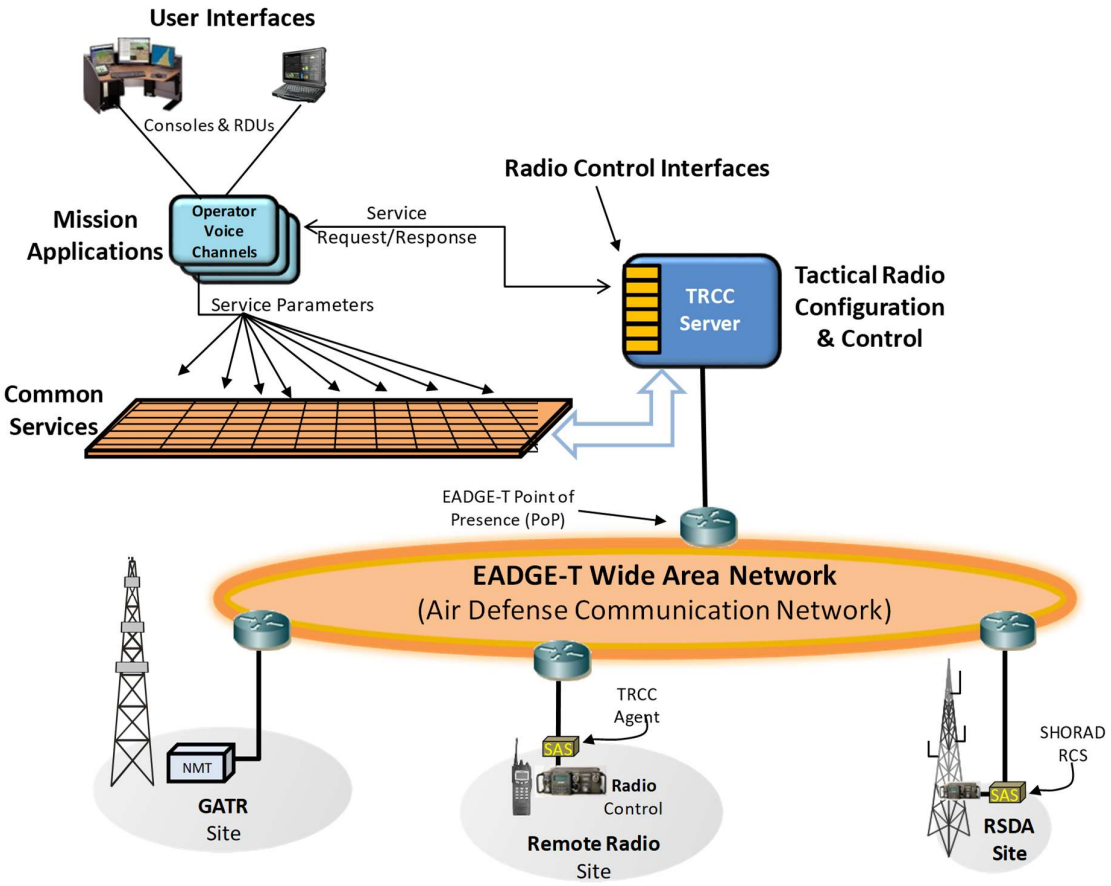


Figure 1-1: TRCC Radio Voice Control Services

The service level interfaces provided by the TRCC allow other EADGE-T applications to support radio configuration functions which reduce operator actions and eliminate the need to switch between operational and radio configuration functions. In addition, the TRCC supports voice setup functions required to make the radio conversations accessible via the audio touch panels at each operator console.

1.3.2 Data Communication as a Service

The implementation of secure and non-secure data connections leverages the same TRCC radio configuration capabilities used to support voice services. Service level interfaces provided by the TRCC server and implemented by TRCC agents, support the initial configuration, allocation and activation of data services in conjunction with the EADGE-T Site Connectivity Manager (SCM). SCM operations are described in EADGE-T Enterprise System Design Package (SDP) Annex D – Site Connectivity Management. Interfaces provided by the TRCC server allow radio configuration commands to be applied, so that tactical data links can exchange status and track information with data link interface processes that are integrated with the Multi-Source Correlator Tracker (MSCT).

TRCC data communications services provide wireless communications channels to support tactical data exchanges. Service level interfaces support the setup of each radio so that the payloads required to support higher level protocols (i.e., LU-2 and SDL) can be exchanged between the MSCT and each aircraft or weapons system.

2 REFERENCED DOCUMENTS

This section lists documents used in support of this document. Miscellaneous documents in Section 2.3 are for guidance only.

2.1 Customer Documents

- EADGE-T Concept of Operations (CONOPS)
- EADGE-T Contract - Annex 2, Statement of Work Contract Number: DP3/6/8/1/2012/69
- YAHSAT Transportable ICD, July 2011

2.2 Program Documents

- EADGET-SDP-C012.0 EADGE-T Enterprise System Design Package (SDP)
- EADGET-SDP-C012.0AnnexB EADGE-T Enterprise SDP Annex B - Integrated Dictionary (AV-2)
- EADGET-SDP-C012.0AnnexD EADGE-T Enterprise SDP Annex D – Site Connectivity Management
- EADGET-SDP-C012.0AnnexF EADGE-T Enterprise SDP Annex F - System Configurations and States
- EADGET-SDP-C012.0AnnexH EADGE-T Enterprise SDP Annex H - Security Architecture
- EADGET-SDP-C012.0AnnexL EADGE-T Enterprise System Design Package (SDP) Annex L – Tactical Data Links
- EADGET-SDP-C012.2 EADGE-T System Level System Hardware System Design Package (SDP)
- EADGET-SDP-C012.4 EADGE-T System Level Communications System Design Package (SDP)
- EADGET-ICD-C013.18 EADGE-T Interface Control Document GATR
- EADGET-ICD-C013.13 EADGE-T Interface Control Document SHORAD Pantsyr SFU
- EADGET-ICD-C013.14_SHORAD_Data_Link
- EADGET-SLST-D022 EADGE-T Site List VLAN Consolidated Baseline Workbook
- EADGET-RPT-NET-220- EADGE-T Network Model
- EADGET-RPT-DAR-225-00_Fixed Site Design Analysis Report
- EADGET-PTAL-001-Program Terms and Acronyms Listing

2.3 Miscellaneous Documents

- Unified Capabilities Requirements, US Department of Defense, 2013
- RFC 2474. Definition of the Differentiated Services Field, IETF, December 1998
- RFC 3550: RTP: A Transport Protocol for Real-Time Applications, IETF, July 2003
- RFC 3665: Session Initiation Protocol (SIP) Basic Call Flow Examples ,IETF, December 2003
- IEEE 803.2ad, Link Aggregation, IEEE Computer Society, November 2008
- ED-137/1B, Interoperability Standards for VoIP, Volume 1 Radio, EUROCAE, January 2012
- Network Management - Network Operations Center, Security Guidance At-a-Glance, Supplement of Network Infrastructure STIG, V8R1, US Department of Defense Information Systems Agency (DISA), 2010

3 EADGE-T COMMUNICATION SERVICES

The EADGE-T System / Subsystem / Component Tree includes multiple communications subsystem elements which represent a range of diverse technologies as documented in the EADGET-SDP-C012.0 Enterprise System Design Package. These elements provide a layered hierarchy to support time critical command and control operations across the EADGE-T enterprise. Together these elements can be viewed as a set of underlying services which provide the infrastructure required to meet strategic and tactical communications needs. The communications services provided include:

- Network Capability Services which provide an extensible architecture based on Internet Protocols to enable the integration and future expansion of network communications across the enterprise. Network capability services are implemented using separate sub-system elements to support wide area networking, site Edge Networks and local enclave networks
- Voice Communications Architecture to support secure and non-secure telephony, tactical radio communications and operator voice communications
- Digital Data Link Services which establish communications networks essential to supporting command and control operations and establishing a recognized air picture

This section provides an enterprise level description of each of these communications elements and how they support the operational needs of the AFAD.

3.1 Network Capability Services

Network services provided by the EADGE-T communications system provide the secure exchange of command and control information between deployed assets and mission applications. The design of the EADGE-T network infrastructure is based on converged IP technologies that provide reliable transport of data, voice and video traffic. The architecture is based on international standards and best practices (as referenced in Section 2.3), that have been adopted by commercial network service providers, the North Atlantic Treaty Organization (NATO, also called the North Atlantic Alliance) and the U.S. Department of Defense (DoD). The architecture consists of a core or backbone network which transports encrypted voice and data between enclaves located at each deployed EADGE-T site. As shown in Figure 3-1 the modular design uses the same elements at each site. As described in section 1.3, the use of common elements in the design provides consistency across the system while improving sustainability, supportability, and enforces security controls between enclaves.

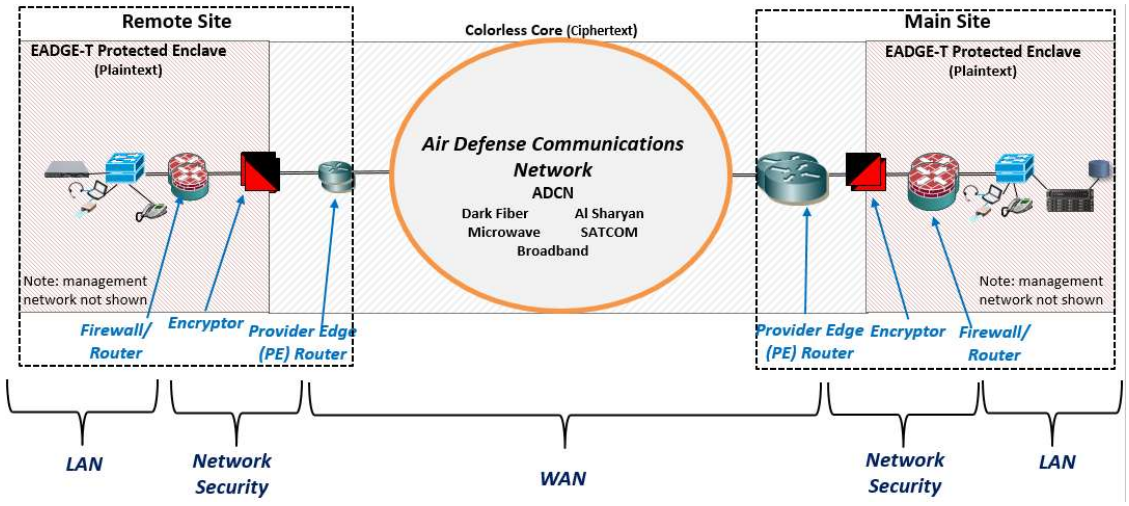


Figure 3-1:EADGE-T Site-to-Site Network Connectivity

The design of the EADGE-T communications architecture consists of three (3) primary elements or segments which provide connectivity between sites:

1. ***The EADGE-T Wide Area Network*** (WAN) is an enterprise wide network consisting of IP routers that use a combination of network transport technologies including dark fiber (i.e., direct fiber optic interconnect components), the Al Sharyan fiber optic back bone (FOBB), the High Capacity Microwave Protocol (HCUP), wireless broadband[1] and Satellite Communications (SATCOM). The ability of the EADGE-T WAN to securely transport mission critical data over the aggregation of these different technologies is referred to as the Air Defense Communication Network (ADCN). The ADCN supports the secure exchange of encrypted (ciphertext) data between deployed EADGE-T locations and includes a central core network consisting of high-speed Provider Routers (P-Routers) with additional connections to remote EADGE-T locations through the use of separate Provider Edge Routers (PE-Routers). The ADCN routes EADGE-T traffic over a wide area using Multi-Protocol Label Switching (MPLS) technologies which connect the PE-Router of one remote site with the corresponding Router located at an EADGE-T operation center.
2. ***Network Security*** provides controls at each EADGE-T location to ensure the secure transport of information over the ADCN. An EADGE-T site is a room, facility or organization which consists of one or more secure enclaves. The equipment deployed at each site typically includes a redundant pair of PE-Routers, separate In-line Network traffic Encryptors (INE) and a pair of security firewall/routers which are configured with security policies to block the exchange of any unexpected or unauthorized traffic. As shown in Figure 3-1, each firewall/router provides an interface between the encryptors and the local network equipment within the enclave. Firewall/routers are commonly referred to as Customer Edge (CE) routers by commercial network service providers. In the EADGE-T network design, firewall/routers protect the attached enclave providing signature-based network detection, security policy enforcement and local network routing functions. The graphical symbol used for an EADGE-T firewall/router includes elements to represent both security and routing functions as the hardware components used as firewalls in EADGE-T support both routing and firewall capabilities in a single device.
3. ***Local Area Networks*** (LAN) in each of the enclaves located at an EADGE-T site provides secure access to local resources and services as well as local management and monitoring. The modular design of Local area networks in each deployed enclave is designed to support the extension of EADGE-T services including the ability to add additional mission and/or tactical communications capabilities. The local area networks at each EADGE-T location also include monitoring capabilities which support the secure management of the deployed infrastructure at each site.

- Each of these segments includes, where environmental conditions permit, redundant components which support automated failover mechanisms to provide high system availability. The configuration of these elements are used as a design template that is repeated throughout the EADGE-T network. The EADGE-T wide area network makes use of network backbone transport services standards as defined by the US Department of Defense to provide secure separation of the UAE SECRET, NON-US COALITION, UAE UNCLASSIFIED, and US SECRET/RELESABLE security domains. The remainder of this section provides descriptions of these network elements. Further technical details of these elements are provided in the EADGE-T Communications System Design Package (SDP).

3.1.1 Wide Area Network

The wide area connectivity of the EADGE-T system is provided by the Air Defense Communications Network using multiple transport technologies to provide a resilient means of interconnecting the EADGE-T enclaves located at each site. Unlike the existing EADGE Integrated Communications Network, which uses switched circuit technologies, the EADGE-T ADCN uses packet technologies

[1] Where compatible broadband coverage is available

and different transport types to improve reliability and provide resilience. By using a combination of network links consisting of dark fiber, FOBB, Microwave and Satellite Communications (SATCOM), the ADCN dynamically routes information over different network transport segments to improve reliability and adapt to underlying link failures. By combining standards-based protocols including IP and MPLS with Traffic Engineering (TE), the ADCN isolates, prioritizes and routes mission critical EADGE-T traffic over multiple paths to provide reliable connectivity between sites.

3.1.2 Core Network

The EADGE-T Core Network securely transports voice and data to designated sites in the UAE enabling collaboration between government and civil authorities. Designated core nodes in the EADGE-T WAN provide the central connectivity required to transport command and control information between remote sites distributed throughout the UAE and communications centers located at designated primary, alternate, and deployable control centers. The 14 EADGE-T core sites interface to high speed optical nodes which are part of the Al Sharyan NGN (Next Generation Network). The NGN is an Optical Transport Network (OTN) which uses high speed optical switching and dense wave division multiplexing (DWDM) technologies to provide a high-speed backbone within the Al Shayan network. The EADGE-T core nodes are Provider Routers (P-Routers) which use a 10 Gbps NGN channel (referred to as a 'lambda') to transport information using Multi-Protocol Label Switching (MPLS) technologies. Connections over the NGN portion of the FOBB support a full mesh topology which allows information to be exchanged between all of the core P-Routers.

This full mesh configuration minimizes network latencies between sites and uses Quality of Service (QoS) controls to ensure that time-sensitive traffic, including voice and video data, get priority over network traffic that is less susceptible to the effects of network delays, jitter or packet loss. EADGE-T remote sites that are not directly connected to the core sites are connected to the Core network through Provider Edge Routers (PE-Routers) that are connected to the Fiber Optic Backbone (FOBB) using local fiber (Synchronous Digital Hierarchy - SDH), microwave or SATCOM links. Each PE-Router is logically connected to two different P-Routers so that once traffic from a remote site reaches the nearest P-Router it is a single network hop away from processing applications located at either Main Site or the DAOC. Figure 3-2 provides a high-level representation of the network showing the 14 P-Routers that are connected to the Optical Transport Network as well as the PE-Routers connected to the SDH.

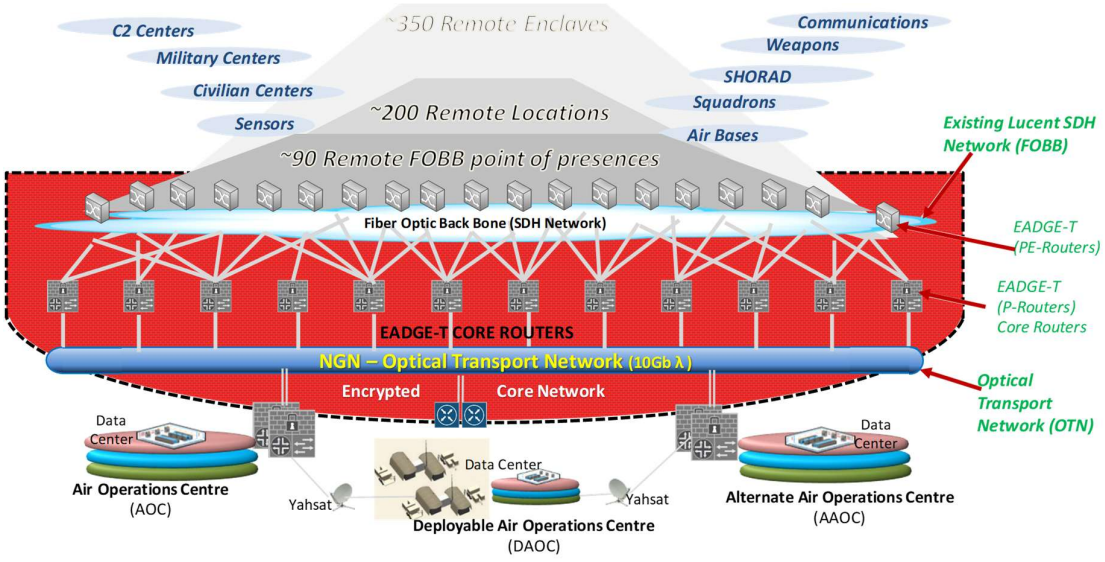


Figure 3-2: High-Level Representation of ADCN Core Network

The information exchanged between different EADGE-T sites is routed through network pathways (MPLS tunnels), known as a Label Switched Paths (LSPs) which may include several individual segments which use different network transport technologies. Each EADGE-T site is configured with dual LSP tunnels with separate pairs of LSPs for each security protection level required for the site.

The ADCN network provides a high level of availability by using multiple failover technologies along with redundant components:

1. P-Routers located at each of the core sites are configured with two power supplies and dual routing engines to provide 1+1 redundancy. The routing engines in the Juniper (MX series) routers used as ADCN P-Routers include different control and management interfaces to separate routing protocol updates from network management functions. The dual routing engines minimizes network interruptions and packet loss by using automated failover features including:
   a. Graceful Routing Engine Restart – GRES preserves the state of the Packet Forwarding Engine (PFE) during a switchover. The internal packet forwarding engine uses forwarding tables established by the routing engine to forward traffic between ports. GRES eliminates the need to restart the forwarding engine thus avoiding interrupting existing packet flows.
   b. Non-Stop Active Routing – NSR improves recovery times over the existing EADGE routers by running concurrent versions of network routing protocols in the backup as well as the primary routing engine. This minimizes the delay required for the backup routing engine to assume responsibility for routing protocols.
   c. In-Service Software Upgrade – ISSU allows for the installation of newer versions of the Juniper network operating system (JunOS) on the backup routing engine without affecting packet forwarding or routing operations occurring on the primary routing engine.

   These configuration options prevent network interruptions and packet loss even if one of the routing engines fail or is taken off line to support maintenance activities.
2. Packet forwarding from remote sites through the core network will not be affected by a link failure as long as an alternate path is available. Thus, if a remote optical interface failure prevents FOBB access at a remote site, routing updates will automatically select an alternate network route, often without the loss of any data packets.

Resilient packet forwarding in the Core Network is supported by alternate routes and protected circuits. The full mesh configuration of the core sites allows alternate routes to use Fast Re-Route (FRR) capabilities. FRR computes alternate routes around P-Routers when the failure of the primary path is detected. Typical failover times are <100 milliseconds and recovery are automatic. Fast Re-Route capabilities are discussed in the EADGE-T System Level Communications System Design Package (SDP) document.

3.1.3 Routing Between EADGE-T Sites

Connections between enclaves at the same security level is accomplished using an end-to-end overlay network which uses the WAN as an underlying network to transport information. Local area network traffic in one enclave is exchanged with other enclaves by first inserting the information into a Generic Routing and Encapsulation (GRE) tunnel formed by the local firewall/router. This tunnel forms a point-to-point link between the local and remote firewall/routers. A health check is performed by the firewall/router on each end by exchanging timing messages to ensure the integrity of the connection. If the health check fails, traffic is automatically diverted and send over the alternate (A or B) path as shown in Figure 3-3.

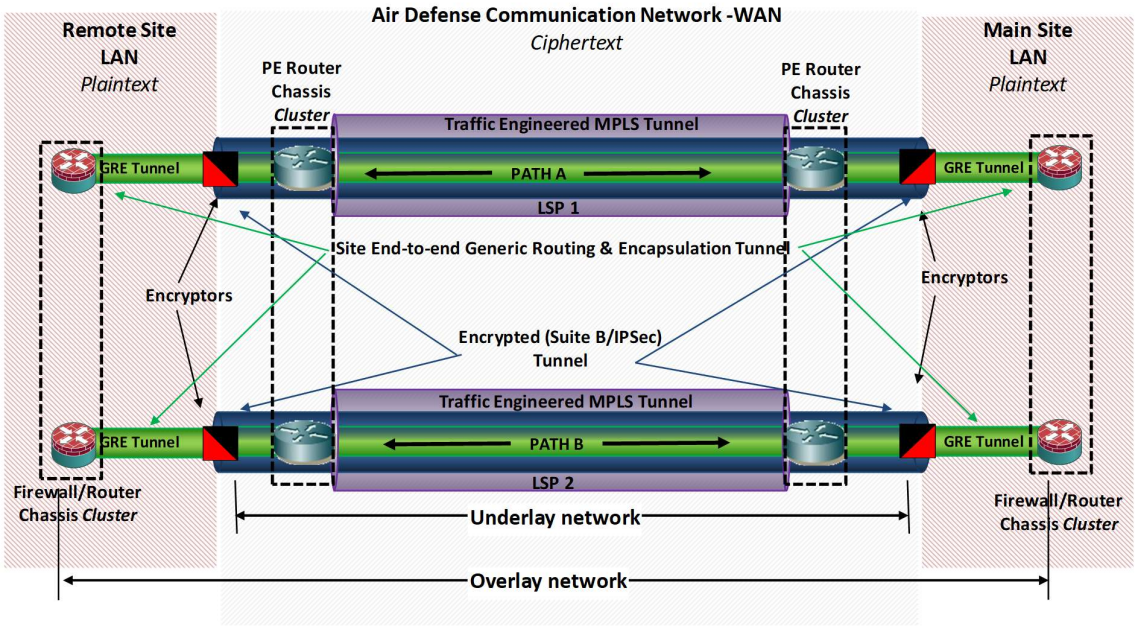


Figure 3-3: Underlay and Overlay Routing

The underlay network shown in Figure 3-3 transports data from the GRE tunnel by first encrypting the traffic using router based encryptors which use the IP security (IPSEC) protocol with Suite-B encryption algorithms. These encryptors form an end-to-end security association (SA) between the source and destination encryptors. Data in this encrypted tunnel is then routed over the MPLS WAN using LSPs defined for each enclave protection level.

3.1.4 Multi-Protocol Label Switching (MPLS)

MPLS (as described in the EADGE-T System Level Communications System Design Package - SDP) works with IP Quality of Service (QoS) mechanisms to provide an expedited pathway across the network between sending and receiving sites. MPLS LSPs provide a virtual circuit connection between the PE-Routers located at each source and destination site. MPLS works with IP protocols in accordance with the layers defined by the Open Systems Interconnection (ISO/OSI) model however, MPLS inserts a small packet header or 'shim' between the data link and network layers to form the LSP. In this way each LSP provides a virtual network tunnel through the ADCN which allows IP packets to be sent directly between the originating and destination sites. MPLS LSPs improve network performance by simplify the routing decisions normally required in IP networks and by supporting the creation of separate virtual pathways used to forward different traffic types and security requirements. Network traffic types are characterized based on their respective Quality of Service requirements (as described in Section 3.1.12.2.1 below) and grouped into 'forward equivalency classes' (FECs) to support traffic differentiation.

MPLS tunnels are established by the PE-Routers at each site which serve as a Label Edge Routers (LERs). When encrypted data is sent from an enclave at an EADGE-T site, the local PE-Router works as an LER examining the forward equivalency class of the information, adding a label, and placing it in the appropriate LSP which lead to the intended destination. Intermediate P-Routers within the Core network are known as Label Switch Routers (LSRs) as they forward traffic between the PE-Routers that are located at each end of the connection.

3.1.5 Resource Reservation Protocol (RSVP)

RSVP works with MPLS as individual LSPs are created between sites attached to the ADCN. As each LSP (tunnel) is formed, RSVP establishes bandwidth reservations on the intermediate routers (P-Routers) along the path. As multiple LSPs are created between PE-Routers, some LSPs may cross

each other and use the same intermediate routers. As each new LSP is formed, RSVP performs checks to ensure that the total bandwidth requirements of all the LSPs passing through each intermediate router do not exceed the amount of bandwidth each router can support.

3.1.6 Traffic Engineering (TE)

Traffic Engineering (TE) provides the final component ensuring that different LSPs are defined for the primary (PATH A) and secondary (PATH B) path between the operating centers and the PE-Router at each site. Thus, TE ensures that there is no single component shared between the paths which could result in a single point of failure that would affect traffic forwarding. In addition, TE plays an important part in distributing traffic to prevent directing too much traffic over a segment or component in the WAN.

3.1.7 Packet Transport Networks

The ADCN supports the secure exchange of packet information using IP protocols at Layer 3 of the ISO/OSI model. However, the connectivity between any two adjacent P- or PE-Routers relies on the presence of an underlying Layer 2 transport network which provides a point-to-point connection using media access control (MAC) protocols. P- and PE-Routers used in the ADCN include interface adapters to support these lower layer protocols so that packets between EADGE-T routers can be transported at Layer 2. Connectivity to an EADGE-T remote site depends on which Layer 2 transport networks are available at the site. However, all EADGE-T PE- and P-Routers support redundant Layer 2 interfaces which can include interface connections to dark fiber, Al Sharyan FOBB, AFAD Microwave network, wireless broadband and/or satellite networks. The EADGE-T P- and PE-Routers supplied include spare Ethernet and E1 connection ports to support additional interfaces as well as additional interface ports to support future connections using other network technologies.

Regardless of the technology and media used by these Layer 2 transport networks, all traffic sent between sites is encrypted before being sent over the ADCN. Thus, all information sent over the ADCN is deemed ‘colorless’ to indicate that the contents of the transmitted data cannot be examined during transport. In addition, a number of the transport networks used by the ADCN include TRANSEC encoding to further protect the confidentiality of data exchanges (e.g. AFAD microwave networks).

3.1.7.1 Dark Fiber

Dark fiber refers to the transport network through the colorless domain directly connected by fiber optic cabling. Where available and used by EADGE-T, dark fiber provides point-to-point Ethernet connectivity using single- or multi-mode fiber. Ethernet specifications which support distances of up to 80km with single mode fiber and the appropriate optical interfaces. Each Ethernet connection includes separate transmit and receive fibers with multiple fiber pairs that are bundled together to improve reliability and overall throughput. Within EADGE-T, dark fiber connections exist between Main Sites 1 and 2. Larger airbases include a Base Area Network (BAN) which uses dark fiber segments in a ring or spoke topology to reach distributed sites and enclaves located within the base.

3.1.7.2 FOBB

The FOBB refers to multiple fiber optic network technologies that provide connectivity between civil and military sites across the UAE. The FOBB is monitored and supported by the Army Signal Corps and has been configured in accordance with AFAD requests. The FOBB includes a centralized Optical Transport Network (OTN), the NGN, which uses Optical Carriers (OC) and Dense Wave Division Multiplexing (DWDM) technologies to provide high speed (10Gbps) connectivity between directly connected sites. Remote sites are indirectly connected to the OTN using SDH loops and Add Drop Multiplexers. The Signal Corps operates a Microwave backup network to ensure FOBB connectivity if portions of the optical network are disrupted.

3.1.7.3 Microwave

The AFAD operates a microwave network which provides connectivity between AFAD facilities in portions of the country. The HCUP microwave network supports up to 16 E1 carrier circuits and uses a point-to-point topology between main sites and selected remote EADGE-T locations. Most EADGE-T P- and PE-Routers include E1 interfaces to support connectivity to the HCUP. In addition, a dedicated point-to-point microwave connection is used between Main Sites 1 and 2.

3.1.7.4 Satellite

EADGE-T SATCOM capabilities include a mobile communications terminal used by the Mobile Air Operations Center (MAOC) to support Communications On-The-Move (COTM), and two transportable terminals that are normally located with the Deployable Air Operations Center (DAOC) for Communications At-The-Halt (CATH). SATCOM coverage is provided by YahSat which consists of secure Ka band coverage for the UAE using the YA1 and YA2 satellites. YahSat military satellite communications are supported at primary and backup Military Anchor Stations (MAS) and managed at Military Network Operations Centers (MNOCs). YahSat provides a radio relay function to support communications between deployed transportable or mobile terminals and the MAS anchor site. The MAS acts as a hub site for all SATCOM traffic and uses the FOBB to provide connectivity to other EADGE-T sites. Coordination with YahSat will be required if the AFAD wishes to change this topology to support a direct point-to-point topology.

The MAOC COTM SATCOM terminal was developed under a contract with Yahsat with terminal and antenna components from Airbus Defense and Space and General Dynamics SATCOM Technologies. The MAOC mobile satellite ground terminal (Figure 3-4) will provide EADGE-T connectivity using a 2 Axis antenna which supports a 75 cm aperture. Expected throughput of the mobile terminal is less that 2Mb/s (depending on link budget). The terminal is an integrated unit consisting of an antenna unit mounted on the MAOC and separate colorless and secure management racks each housed in transit cases.

- Antenna Subsystem
  - A General Dynamics Model 24-30L SATCOM On-The-Move Ka band antenna
  - GPS antenna and splitter
  - Inertial Reference Unit (IRU)
- Non-Secure Rack
  - A Radio Frequency Distribution Unit
  - Thales 21e Modem
  - Cisco Router
- Secure Management Rack
  - HC-7825 IP VPN Encryptor
  - Cisco Router
  - Management Server

Figure 3-4: Mobile Air Operations Center with COTM Antenna

EADGE-T encrypted traffic to/from the MAOC is exchanged via the YahSat supplied Cisco non-secure router. The non-secure router provides network switching and routing functions for the Non-secure domain. Local and remote management of the terminal is supported using the secure management rack. Remote support for the terminal is provided from the MNOC but is limited exclusively to the terminal and cannot access EADGE-T management capabilities or data. Additional details related to the COTM terminal is provided in the Communications SDP (C012.4.0).

The AFAD will supply two Transportable Satellite Ground Terminals (TRN SGTs, Figure 3-5) to support DAOC Communications At-The-Halt (CATH). Each terminal includes an optical Ethernet interface to support connectivity to EADGE-T. Each supplied transportable SGT will support up to 130 Mb/s using a 2.4-meter antenna when downlinking through the MAS. If the MAS is bypassed and the terminal is configured to support direct connections between the transportable SGTs or with the MAOC SGT, power limitations will reduce the total bandwidth available.

Figure 3-5: YahSat Transportable SGT

IP SATCOM communications using either mobile or transportable SATCOM terminals require external mechanisms to ensure that available bandwidth is used efficiently. EADGE-T uses protocol enhancing proxies (PEPs) that are located in the plaintext (unencrypted) enclaves of each site using a SATCOM terminal to provide IP acceleration for non-terrestrial connections. EADGE-T uses a combination of virtual and physical SteelHead IP acceleration appliances from Riverbed as follows:

- MAOC: virtualized SteelHead software running on virtual machines in the UAE SECRET, NON-US COALITION and UAE UNCLASSIFIED enclaves
- DAOC: virtualized SteelHead software running on virtual machines in the UAE SECRET, NON-US COALITION and UAE UNCLASSIFIED enclaves
- YahSat receiving site: PEP physical appliances in the UAE SECRET, NON-US COALITION and UAE UNCLASSIFIED enclaves

If the TRN Satellite Ground Terminals are relocated to Main Sites 1 or 2, the DAOC virtual PEP appliances will also have to be relocated and placed in the UAE SECRET, NON-US COALITION and UAE UNCLASSIFIED enclaves.

3.1.8 Communications On-The-Move (COTM)

A number of the EADGE-T systems support COTM operations. Among those are the MAOC, Client Kits (when linked to the MAOC), and Short Range Air Defense (SHORAD) Fire Units (SFUs).

3.1.8.1 MAOC

The MAOC is capable of operating the following communications systems while On-The-Move:

- SATCOM – voice and data
- Tactical Radios – voice only
- Wireless LAN – connectivity to the DAOC (while within range)
- LTE/Broadband Wireless – voice and data (where LTE coverage is available)

The network design for the MAOC is provided in Section 4.3.2.

3.1.8.2 Client Kits

The Client Kits are capable of operating the following communications systems while On-The-Move through the MAOC:

- Wireless LAN

Client Kits are discussed in Section 4.3.3.

3.1.8.3 SFU

The SFU are capable of operating the following communications systems while On-The-Move:

- Tactical Radios – voice and data
- LTE/Broadband Wireless – voice and data (where LTE coverage is available)

Aspects related to the network design used in SHORAD Fire Units are included in Section 4.3.4.

3.1.9 Communications At-The-Halt (CATH)

In addition to system elements which support either fixed or COTM, EADGE-T communications capabilities are also be supported by EADGE-T deployable system elements including the DAOC, GM200 Mobile, and SFUs. Like other elements, these systems can be connected to fixed (fiber, microwave, or wired) EADGE-T communications capabilities at a deployed location or, in the case of the DAOC, make use of dedicated SATCOM terminals.

3.1.10 Network Model

A crucial part of the ADCN design relates to the amount of bandwidth available between each site and the core network. The AFAD estimated the amount of data required to support each EADGE-T site and the Signal Corps provisioned the FOBB interfaces accordingly. However, in order to ensure that the system isn't limited by the interface rates provisioned and has sufficient room for expansion, a modeling effort was undertaken to validate bandwidth estimates. These efforts have been focused on determining the overall ADCN WAN utilization in a worst-case scenario when traffic utilization is at its peak. These modeling efforts are based on estimates of the bandwidth requirements for EADGE-T software applications. In addition, detailed information related to the specific applications and functions utilized at each EADGE-T site, has not been included in the model given the sensitivity of such information. The overall utility of the model and its ability to ensure that bandwidth utilization does not exceed the provisioned values.

3.1.10.1 Modelling Approach

The current EADGE-T bandwidth model (Version 3.1, July 2019) is implemented in Excel using a discrete analysis of the expected traffic types for each site. The sites and enclaves used to develop this model are based on the SV-2 Level 1 file (Site Type-Counts-IF-Enclaves). This SV-2 artifact contains a listing of the number and type of each site in the baseline. The model provides ADCN predictions based on several factors:

1. Protocol Characterization – Generic protocol types (flows) were created to represent major traffic flows. A total of about 20 different traffic types are used in the model including radar data, tactical voice, streaming video, network management, tactical data links, RDU web, replication, file transfers and others. Both User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) are specified.
2. Site Traffic Profiles – The network protocol types were assigned to each site type (as identified in the SV-2 Level 1 baseline) to indicate the type of network transactions occurring

at each site. Site types include agencies squadrons, radars, ground-air transmit/receive (GATR), SHORAD Deployment Area (W/RSDA) towers, HAWK batteries, Advanced Weapons, Air Operations Center/Alternate Air Operations Centers (AOC/AAOC), Deployable Air Operations Center (DAOC), Mobile Air Operations Center (MAOC), Military and Civilian Agencies. The model only includes sites expected to be active during a crisis, thus training and development facilities have not been included.

3. Traffic Rates – The traffic types assigned to each site type are defined further to indicate the number of instances (i.e., sites performing the same function), the number of active channels or sessions and an estimate of the ratio of received vs. transmitted traffic. As an example, there are 50 squadrons, each with two (2) RDUs so the assigned traffic entry for a squadron specified 50 instances with one (1) active session (on one of the RDUs) and a receive to transmit ratio of 5/1. Each traffic entry uses this parametric data to scale the traffic characterization data (from step 1 above).
4. Model Generation – The traffic entries for each site type are then summed to estimate the bandwidth (in kilobits per second); tables are produced for each site type along with graphs showing the received (ingress) and transmitted (egress) rates.
5. An additional set of graphs are provided which estimate the bandwidth requirements for each FOBB interface (PE-Router) to account for the amount of bandwidth required to support all of the EADGE-T enclaves connected to each FOBB point of presence (PoP)

A pictorial of the modeling process is shown in Figure 3-6; the associated table and graphics for the current model are provided below in Figure 3-7. Values shown in Mb/s are Megabits per second while values in MB/s are Megabytes per second.

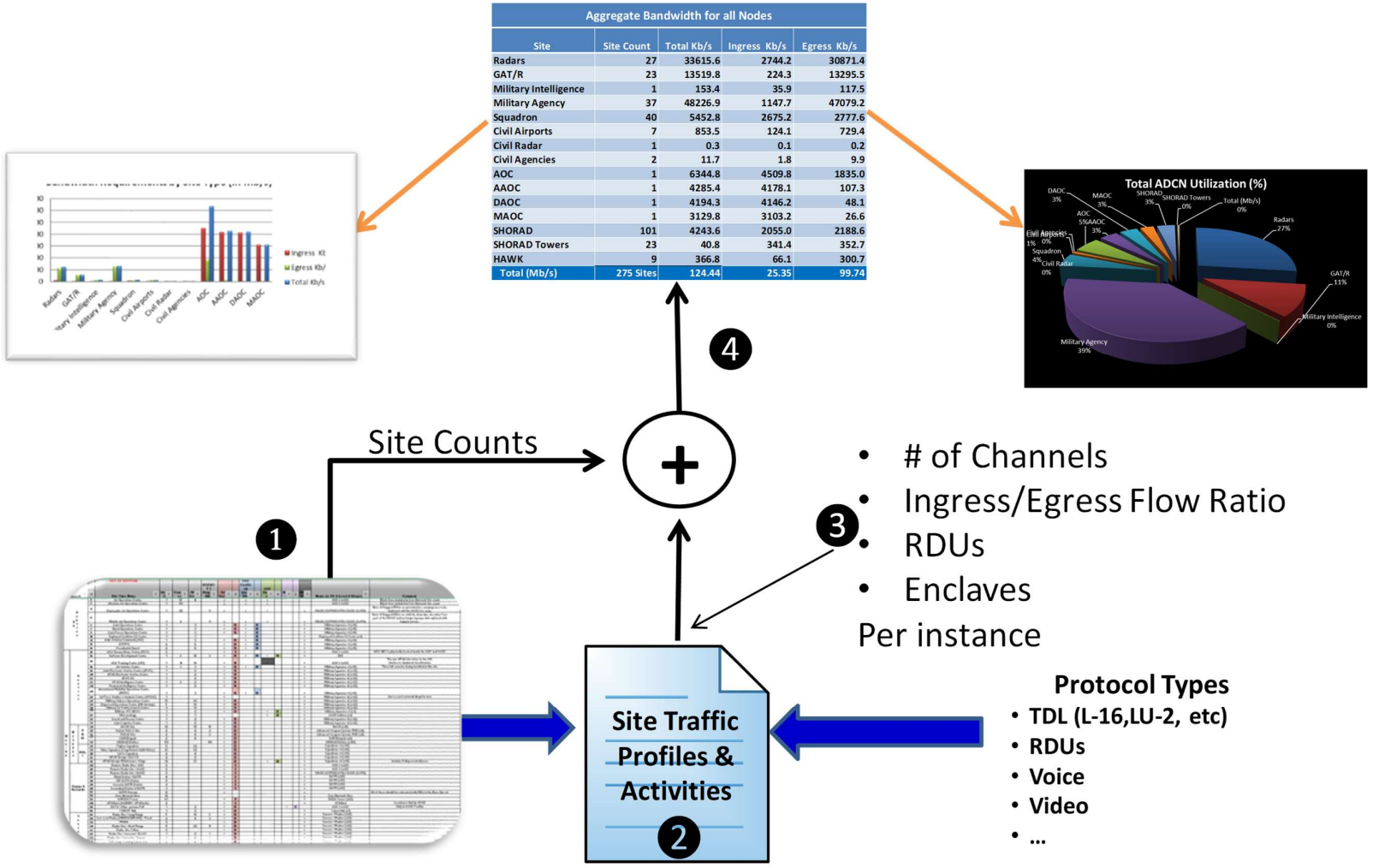
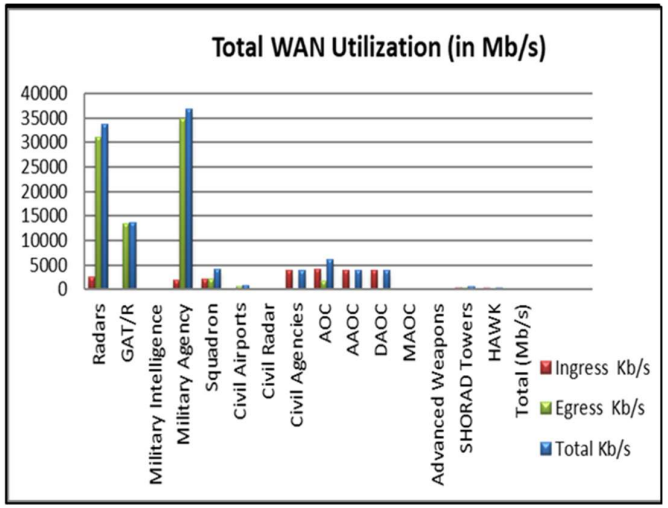
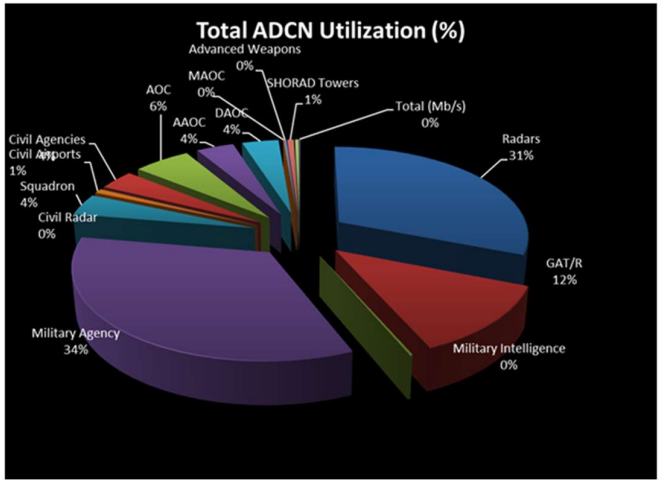


Figure 3-6: Bandwidth Model Operation

Total Bandwidth per Site Type				
Site	Site Count	Total Kb/s	Ingress Kb/s	Egress Kb/s
Radars	27	33615.6	2523.3	31092.3
GAT/R	23	13519.8	224.3	13295.5
Military Intelligence	1	220.5	107.4	113.1
Military Agency	37	36847.0	1930.7	34916.3
Squadron	40	4198.4	2057.3	2141.1
Civil Airports	7	853.5	189.8	663.8
Civil Radar	1	0.3	0.1	0.2
Civil Agencies	2	3819.6	3816.3	3.2
AOC	1	6061.2	4246.9	1814.3
AAOC	1	4001.9	3925.2	76.7
DAOC	1	3898.8	3863.4	35.4
MAOC	1	65.5	51.4	14.1
Advanced Weapons	6	216.0	180.0	36.0
SHORAD Towers	23	694.0	341.4	352.7
HAWK	9	366.8	282.1	84.7
Total (Mb/s)	180 Sites	108.38	23.74	84.64





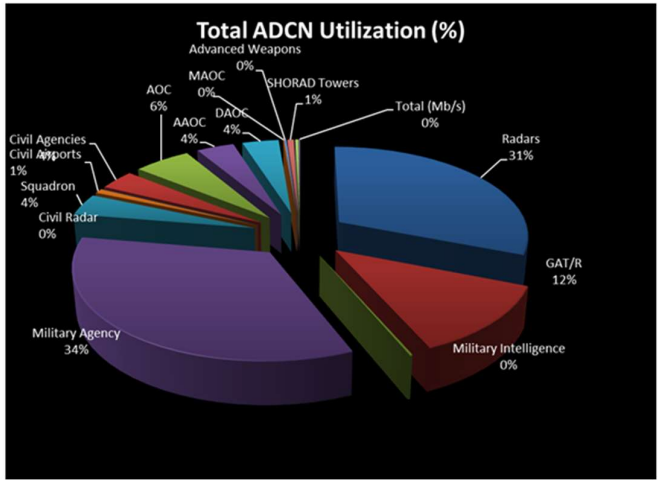


Figure 3-7: Bandwidth Model Output Graphs (in Megabytes per Second)

3.1.10.2 Model Summary

As shown in Figure 3-7, the model results provide an estimate of the ADCN network bandwidth utilized by EADGE-T. Additional information on the model and the link capacity estimates are provided in the EADGE-T System Level Communications System Design Package (EADGET-SDP-C012.4).

3.1.11 Edge Network

Each deployed EADGE-T site interfaces to the ADCN using a standardized configuration referred to an Edge Network. The configuration of the Edge Network components provides encryption and border protection for each enclave supported at the site. While most locations consist of a small number of enclaves that are directly connected to the PE-Routers, the enclaves at larger locations may be connected to the PE-Routers via a base or ring network.

The modular design of the Edge Network is shown in Figure 3-8. This network configuration is used at all deployed EADGE-T sites to ensure a consistent security profile. Juniper routers, switches and firewalls specified in the EADGE-T design have been sized appropriately to meet interface requirements by using different models of the same network devices as shown in Table 4-1, Table 4-2, and Table 4-3. Network devices selected include high speed backplanes and spare interface ports and card slots to support 50% growth in capacity and physical interfaces. In addition, the interfaces in each network device support full line rates (e.g. 1 Gbps, 100Mb/s, etc.) so that information can be exchanged between sites simultaneously at the maximum rate for each interface.

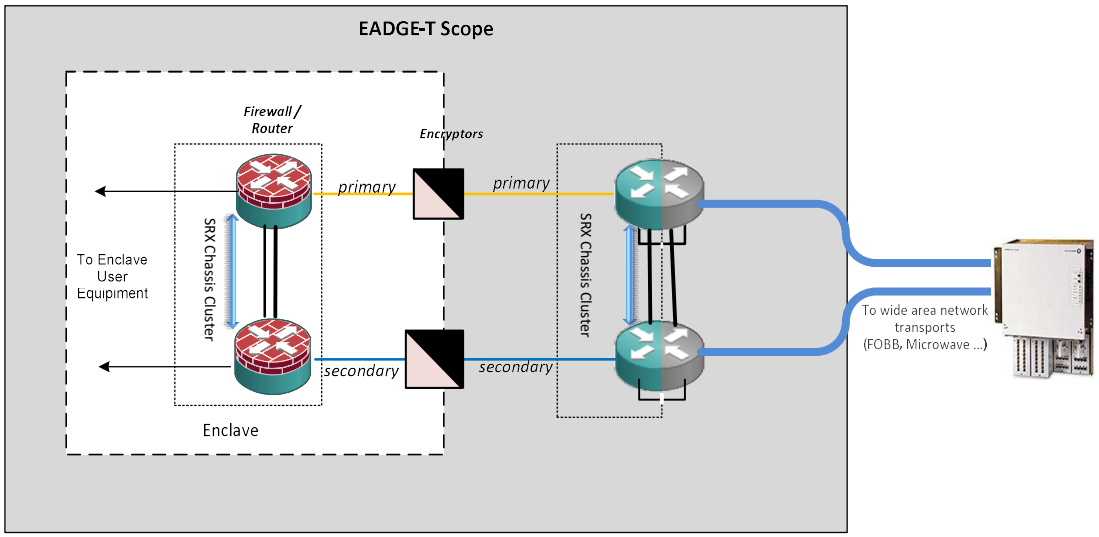


Figure 3-8: Edge Network Redundancy Design

The design of the Edge Network makes use of high availability features supported by routers and firewall devices. In particular, all devices are configured with redundant power supplies, and all fixed EADGE-T sites use a virtual chassis (also referred to as a chassis cluster) configuration, which combines the features of two independent devices so that they operate as single unit. Higher system availability is achieved in this configuration as the routing engine in the second device acts in a hot standby mode to provide sub-second failover which prevents the failure of one chassis from affecting operations. In essence, the combined chassis functions as a single, larger device with both primary and backup routing engines and a shared pool of physical interface cards and ports from both devices. The configuration uses two pairs of links to connect the separate chassis together, one as a control link to exchange configuration and state information and the second as a dedicated fabric connection to support session information as traffic traverses between the chassis. The EADGE-T network uses Juniper Networks SRX Series Services Gateways for encryption, firewall/routers and edge routing

functions. SRX gateways used as firewall/routers are a single device that provide security firewall as well as routing functions.

The dual chassis configuration supports both active/active and active/passive modes. Control operations, which support routing functions occur in one of the chassis at a time (active/passive), while data forwarding is supported on both devices. Juniper has performed extensive tests on different failure modes related to this configuration, as shown in Table 3-1.

Table 3-1: Virtual Chassis Failure and Recovery Modes

FAILURE MODE	PACKET LOSS	NOMINAL FAILOVER TIME	FAILOVER TIME (MAX)
Control Link Failure	No	0.835 msec	1 sec
Fabric Link Failure	No	0 sec	500 msec
Redundant Link Failure	Yes	4.92 sec	6 sec
Power Supply Failure	No	0 sec	500 msec
Fan Failure	No	0 sec	500 msec
Chassis Failure	Yes	2.87 sec	6 sec

Notes:

1. Failover times are provided by Juniper using SRX650 gateways and are shown in seconds (sec) or milliseconds (msec). The configuration and times shown are representative of all remote EADGE-T sites (which use a pair of SRX gateways as shown in Figure 3-8). The Nominal and Max Failover Times are better for the rest of the Juniper series.
2. The virtual chassis configuration used includes dual route processors, power supplies and fan trays.
3. Maximum failover times are typical values based on analysis.
4. Tests conducted using unacknowledged IP streams and do not include routing protocol convergence times (if applicable).

The design of Edge Network supports automated failover using the 'dual-rail' configuration shown in Figure 3-3. Plaintext traffic originating from the local area network at Site 1 or Site 2 is routed to the redundant Firewall/Routers and sent over the Generic Routing and Encapsulation (GRE) tunnel (shown previously in Figure 3-3 as the green connection). The GRE tunnel is required to allow unicast or multicast traffic to be sent to the peer firewall router. As traffic is sent through the tunnel it is routed to the encryptor which establishes an additional tunnel (shown in blue) with the peer encryptor using IP Security (IPSec) protocols. Routing tables in the PE-Routers then forward the encrypted IPSec packets over an MPLS tunnel (purple) to the destination PE-Router. This three-layer encapsulated tunnel allows the secure transfer of data between the Operating centers and each remote site. The secure tunnel also supports the exchange of routing updates so that devices connected to the LAN in each site appear to be directly connected with each other (forming network adjacencies). The dual chassis firewall/routers and PE-Routers at each site allows traffic to be exchanged over either rail (Path A or Path B).

The configuration shown in Figure 3-8 was designed to support a direct ('drop in') replacement of the encryption devices to support the integration with US or non-US coalition partners. Type 1 High Assurance IP Encryptors (HAIPE) and other encryptors (including the Thales Mistral encryptor) use a single plaintext (red) input and a single ciphertext (black) output. The design of the Edge Network in EADGE-T provides a configuration that is compatible with the encryption devices used by other coalition partners and additionally, supports a redundant dual rail approach which allows traffic to be routed over the top encryptor or the bottom encryptor. In this mode, the failure of one of the encryptors will allow traffic to be re-routed over to the alternate 'rail' to prevent a site from being isolated from the ADCN. Edge Network components provide encryption for both operations and management information at all sites.

3.1.12 Local Area Network (LAN)

Within each enclave that is connected to the Edge Network, additional high availability approaches are used to provide fault tolerance. Where the design permits, enterprise class network switching

devices used in EADGE-T are configured as a 'virtual chassis' using a high-speed interconnect cable. The virtual chassis configuration allows multiple switches to operate as a single device with up to ten (10) individual switches providing high availability. As shown in Figure 3-9, a virtual chassis link is used to interconnect multiple Juniper EX switches to protect against the failure of a single switching device. The virtual chassis also allows the 'dual-homing' of server devices using link aggregation protocols (IEEE 803.2ad). The Link Aggregation Control Protocol (LACP) is a networking standard that allows up to eight (8) individual links to be 'bonded' together to act as one high capacity link. The configuration shown in Figure 3-9 uses both LACP and virtual chassis switching to support a Multi Chassis Link Aggregation Group (LAG). This configuration not only improves the total network bandwidth provided, but also improves reliability as connectivity with the server is maintained as long as at least one of the links is functioning. Thus, in this configuration, the loss of a network interface, cable connections or even one of the switches will not affect server availability. A summary of the advantages of link aggregation is shown in **Error! Reference source not found.**.

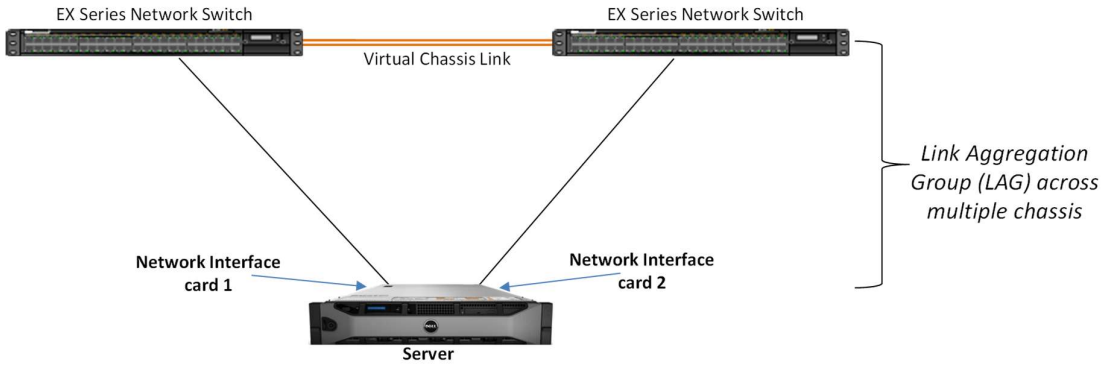


Figure 3-9: EADGE-T High Availability LAN Connections

Table 3-2: Link Aggregation Benefits

CAPABILITY	DESCRIPTION
Combines up to eight (8) links into a single link	Increases available bandwidth up to eight-fold
Supports automatic link failover	Individual link failures do not affect connectivity
Links connected to different switches	Loss of a chassis, port or cable does not affect connectivity

3.1.12.1 LAN Security

As discussed in Enterprise Annex H (Security Architecture) EADGE-T supports information protection for data at the UAE SECRET, UAE UNCLASSIFIED and NON-US COALITION protection levels. Each of these security domains actually consist of a number of separate EADGE-T enclaves located at different sites. While each of these enclaves make use of the ADCN to exchange encrypted data, they appear as separate isolated networks only allowing the exchange of information between enclaves at the same classification level. Sharing of information between security domains is only permitted if dictated by specific applications and is tightly controlled by security appliances (cross domain guards or data diodes) and established security policies.

Isolation between each domain is enforced by three separate mechanisms:

1. Traffic Filtering – Firewall / routers installed in each network enclave include firewall filters which examine network traffic outside the enclave, as well as internal enclave traffic that is sent between different network zones. These firewall rules either permit or deny traffic passing between security zones based on defined security policies. Redundant firewall / routers are used for high availability and provide network traffic inspection which block known penetration attempts and non-compliant information transfers.
2. Data Encryption – As discussed, the Edge Network equipment located in the enclaves at each EADGE-T site include a pair of INEs which provide a security boundary encrypting all plaintext information as it is sent across the ADCN wide area network. Correspondingly,

encrypted (ciphertext) data received from other EADGE-T sites are decrypted before being passed into the enclave. The security algorithms used by the encryptors are based on asymmetric block encryption keys and digital certificates so that data can only be exchanged between enclaves that exist at the same security level. Note as all traffic sent over the ADCN is encrypted, the ADCN is a colorless domain separate from the UAE SECRET, UAE UNCLASSIFIED and NON-US COALITION domains.

3. Data Separation – Information exchanged between enclaves at the same protection level is sent over the ADCN using different network paths. The virtual private networks (VPNs) established by MPLS support the separation of data for each security domain in much the same way that commercial network service providers (e.g., Du or Etisalat) support separate business customers.

3.1.12.2 Quality of Service

The technologies used for the EADGE-T enterprise-wide network support the convergence of different types of network traffic including data, voice and video from multiple applications and locations across the system. This convergence reduces overall system complexity and sustainment costs as well as making more effective use of available resources. Supporting different applications each with potentially different traffic characteristics and sensitivity to network latencies requires that network devices be configured to support Quality of Service (QoS) capabilities.

Unlike circuit-based technologies, which are the basis for EADGE communications, EADGE-T leverages Internet Protocols (IP), which allow the transport of data, voice and video services over a common network infrastructure. Rather than dedicating specific circuits exclusively to support the transfer of information between two end-points, IP allows traffic from different applications and from different devices to travel over the same circuit pathways through the network. As a result, network connections between all entities in the system can share available communications resources and avoid statically dedicating network bandwidth to support the communications between participating locations in the network.

IP is based on packet switched technologies, which use statistical multiplexing to inter-mix the network flows from different applications. This provides the most effective use of network resources as compared to Time Division Multiplexed (TDM) circuits but also means that different types of network traffic potentially share the same network resources. In order to match the service level guarantees provided by circuit switched technologies, processes have been designed into the EADGE-T local and wide area networks to ensure that time sensitive traffic is given prioritization over traffic that is less sensitive to the effects of network congestion that can result in higher levels of packet loss, delay or delay variation (jitter). This is particularly true when using IP technologies to transport time critical voice and video traffic, which can become unintelligible in the presence of network congestion. As compared to time sensitive network flows, other traffic types including web applications and file transfers are termed ‘elastic’ as they can adapt to network delays and packet loss using automatic recovery algorithms.

3.1.12.2.1 Quality of Service Standards

Commercial and Military networks have adopted converged IP technologies on a global basis using industry standard approaches which support different service levels for the network flows of different applications. The most widely accepted approach to support QoS is defined by Differentiated Services (DiffServ) standards as described in RFC 2474. These DiffServ specifications provide a scalable approach using fields in each packet header to support the classification and treatment of network QoS. Supporting QoS and traffic differentiation is particularly important in military networks due to the criticality of real time traffic and the presence of bandwidth limitations in tactical environments.

EADGE-T networks support QoS using DiffServ standards based on guidance provided in the U.S. Department of Defense (DoD) Unified Capabilities Requirements (UCR) document. While industry standards specify multiple traffic classes, the UCR provides specific requirements and settings for QoS that are used within local and wide area military networks. The UCR is a comprehensive document covering a broad range of issues, many of which are not relevant to EADGE-T. However,

the UCR provides some important insights and practical approaches, particularly regarding Quality of Service.

Network QoS for EADGE-T is based on commercial and military best practices using industry standard mechanisms, which enable consistent end-to-end performance for the network requirements of different traffic flows. In addition to DiffServ, MPLS, Resource Reservation Protocol (RSVP) and Traffic Engineering (TE) are used to provide a stable and resilient enterprise network.

3.1.12.2.2 Differentiated (DiffServ) QoS

The goal of DiffServ QoS is to provide consistent treatment of end-to-end network flows across the network. DiffServ works by enforcing the specific forwarding rules of each traffic flow in the switches and routers between the source and destination nodes. In DiffServ, applications are associated with one or more network flows, which have implicit priorities and characteristics with respect to packet loss, latency and jitter. Network flows with similar traffic characteristics are then combined into forwarding classes (FCs), where each specific FC has explicit requirements regarding how packets in the network flows are to be treated. As shown in Figure 3-10, the network flows from each application are grouped into specific FCs in the router, where application flows with similar forwarding characteristics are combined in a single forwarding class.

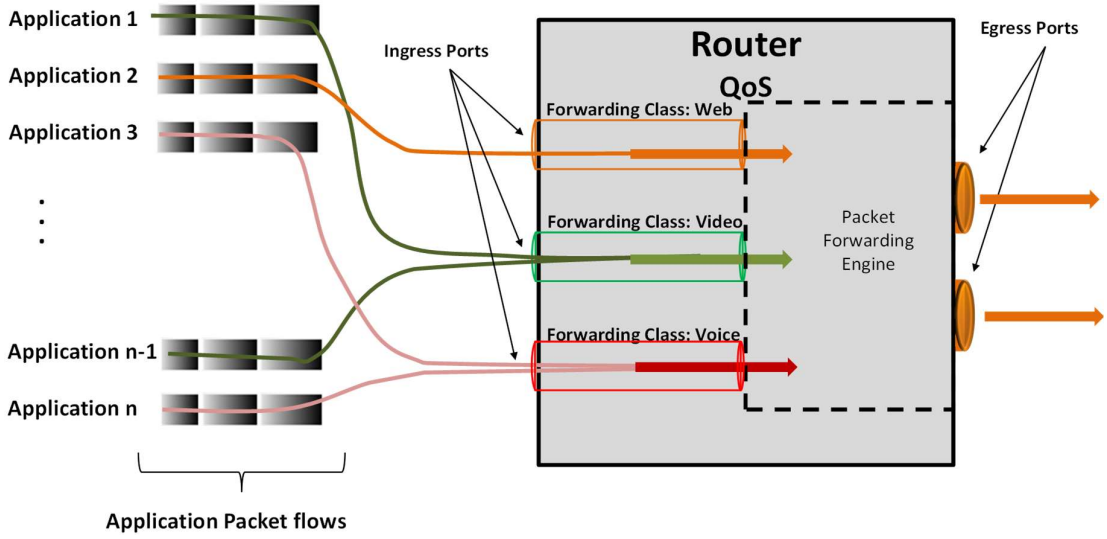


Figure 3-10: Forwarding Classes

After flows are grouped into forwarding classes, DiffServ marks (or re-marks) each packet in the flow with a pre-defined code point value (the DiffServ Code Point - DSCP) to indicate the specific FC that each packet (and flow) is assigned to. By marking the packet at the edge of the network, each router along the path from source to destination can forward the packets according to specific pre-defined rules. These rules are referred to as Per Hop Behaviors (PHB) and include the ability to define forwarding class priorities between flows, as well as how the router behaves under network congestion conditions.

The progression of events used in DiffServ QoS is shown in Figure 3-11. Each router along the path from source to destination follows these steps to provide a uniform level of service from end-to-end. The steps shown include:

- **Ingress Traffic Classification and Marking** – When packets of a flow arrive at the ingress interface, the first step is to classify the incoming traffic to categorize each flow in regard to the relative importance of each packet. Classification involves assigning each packet in the flow to a loss priority that is used later in QoS processing. Classification either occurs by examining packets previously marked (for example by examining the DSCP value in the arriving packet) or based on examining several different fields in the received packet.

- **Per-flow Rate Policing** – When required, upstream routers will examine traffic that exceeds defined burst information rates and limit the rate at which packets are forwarded to shape or limit the traffic accordingly. The rate policing can occur on both ingress and egress ports in order to reduce the effects of jitter and to prevent one flow from monopolizing channel bandwidth. (Application flows which can tolerate temporary delays or packet loss without affecting usability, like TCP/IP, are referred to as elastic and include built in recovery mechanisms for lost packets)
- **Forwarding Queues** – QoS mechanisms define queues to for each FC. Each queue provides the mechanisms to enforce the required priority, precedence, and loss for the packets in each class. If the number of packets in the queue exceed a specific threshold, values in the (DSCP) header are used to determine if a packet can be discarded and removed from the queue
- **Priority Scheduling and Congestion Avoidance** - Packets in each queue are de-queued and forwarded to the egress interface based on the priority of each queue. Different algorithms are used to de-queue packets and can vary from a strict-high priority (where as long as the queue has traffic to send it receives precedence over all other queues) to queues based on specific thresholds or traffic rates

These steps are repeated at each router along the path from source to destination. The PHBs provided align with the traffic requirements of the forwarding classes and the application flows that they contain.

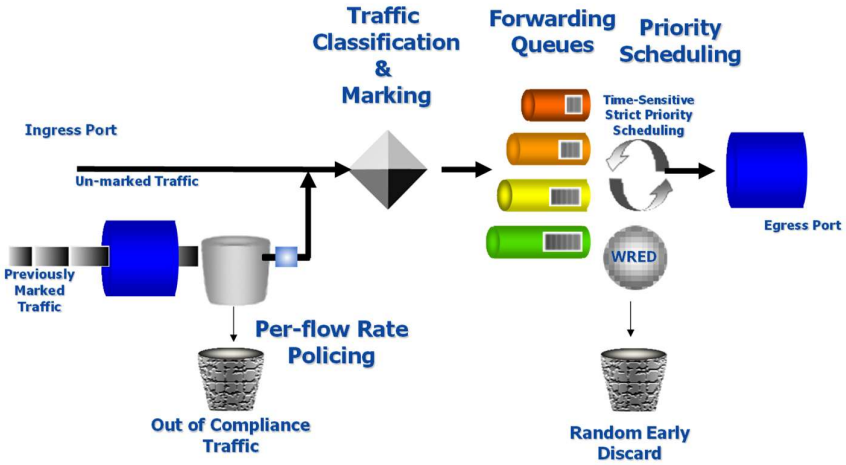


Figure 3-11: DiffServ Processes

EADGE-T QoS uses 6 separate queues that are used to differentiate traffic types sent over the network. Different meanings are assigned to these queues to support the different traffic transmitted on the network. The queues (in order of priority) are shown below. Note that within the core (colorless) network UAE Secret traffic is give priority over other Unclassified and Non-US Coalition traffic.

Table 3-3: EADGE-T QoS Queues

Queue	Description	Meaning in Core	Meaning in Enclave	PHB / DSCP Type
Q6	CONTROL_ENCLAVE	Network Management	Network Management	Expedited Forwarding (EF)
Q5	SEC-A_VVoIP	Secret Traffic	Time Sensitive VoIP	Expedited Forwarding (EF)
Q4	NA_VVoIP	Reserved	Inelastic Real-Time	Expedited Forwarding (EF)
Q3	CONTROL	Core Control (P/PE)	Reserved	Reserved
Q2	UNC-Stream	Unclassified Traffic	Stream	Assured Forwarding (AF)
Q1	COA-BestEffort	Coalition Traffic	Best Effort	Best Effort/Low Priority

Table 3-4: US DoD Unified Capabilities 6-Queue Model

QUEUE	AGGREGATED SERVICE CLASS	GRANULAR SERVICE CLASS	DSCP BASE10	DSCP BINARY	CER PHB
5	Network Control	Network Signaling (OSPF, BGP, etc.)	48	110 000	EF
4	Inelastic Real-Time	User Signaling (AS-SIP, H.323, etc.)	40	101 000	
		Short Message	32	100 000	
		Assured Voice (Includes SRTCP)	41	101 001	
			43	101 011	
			45	101 101	
			47	101 111	
			49	110 001	
		Assured Multimedia Conferencing (voice, video, and data)	33	100 001	
			35	110 011	
			37	100 101	
			39	100 111	
			51	110 011	
3	Inelastic Real-Time	Broadcast Video	24	011 000	
		Non-Assured Voice	46	101 110	
		Non-Assured Multimedia Conferencing (Non-Assured Video Conferencing)	28	011 100	
			30	011 110	
			34	100 010	
			36	100 100	
			38	100 110	
2	Preferred Elastic	Multimedia Streaming (Video Streaming)	25	011 001	AF
			27	011 011	
			29	011 101	
			31	011 111	
			26	011 010	
		Low-Latency Data: (IM, Chat, Presence)	17	010 001	
			19	010 011	
			21	010 101	
			23	010 111	
			18	010 010	
		High Throughput Data (Real-Time Data Backup, Web Hosting)	9	001 001	
			11	001 011	
			13	001 101	
			15	001 111	
			10	001 010	
		OA&M	16	010 000	
1	Elastic	Best Effort	0	000 000	BE
0	Elastic	Low Priority Data	8	001 000	

LEGEND:

AS-SIP: Assured Services Session Initiation Protocol
BE: Best Effort
CER: CE Router
EF: Expedited Forwarding
OA&M: Operations, Administration, & Maintenance
PHB: Per Hop Behavior
SRTCP: Secure Real-Time Transport Control Protocol
AF: Assured Forwarding
BGP: Border Gateway Protocol
DSCP: DiffServ Code Point
IM: Instant Messaging
OSPF: Open Shortest Path First

Figure 3-12 shows an example of the end-to-end traffic patterns between an EADGE-T C2 node and a remote site over an LSP. Forwarding classes and traffic types requiring different PHBs are sent over the LSP that connects the sites. Within the LSP, each forwarding class receives different treatment based on the sensitivity of the traffic transported. The six (6) queues shown in the figure correspond to the queues provisioned for EADGE-T and match queues established in the U.S. DoD UCR.

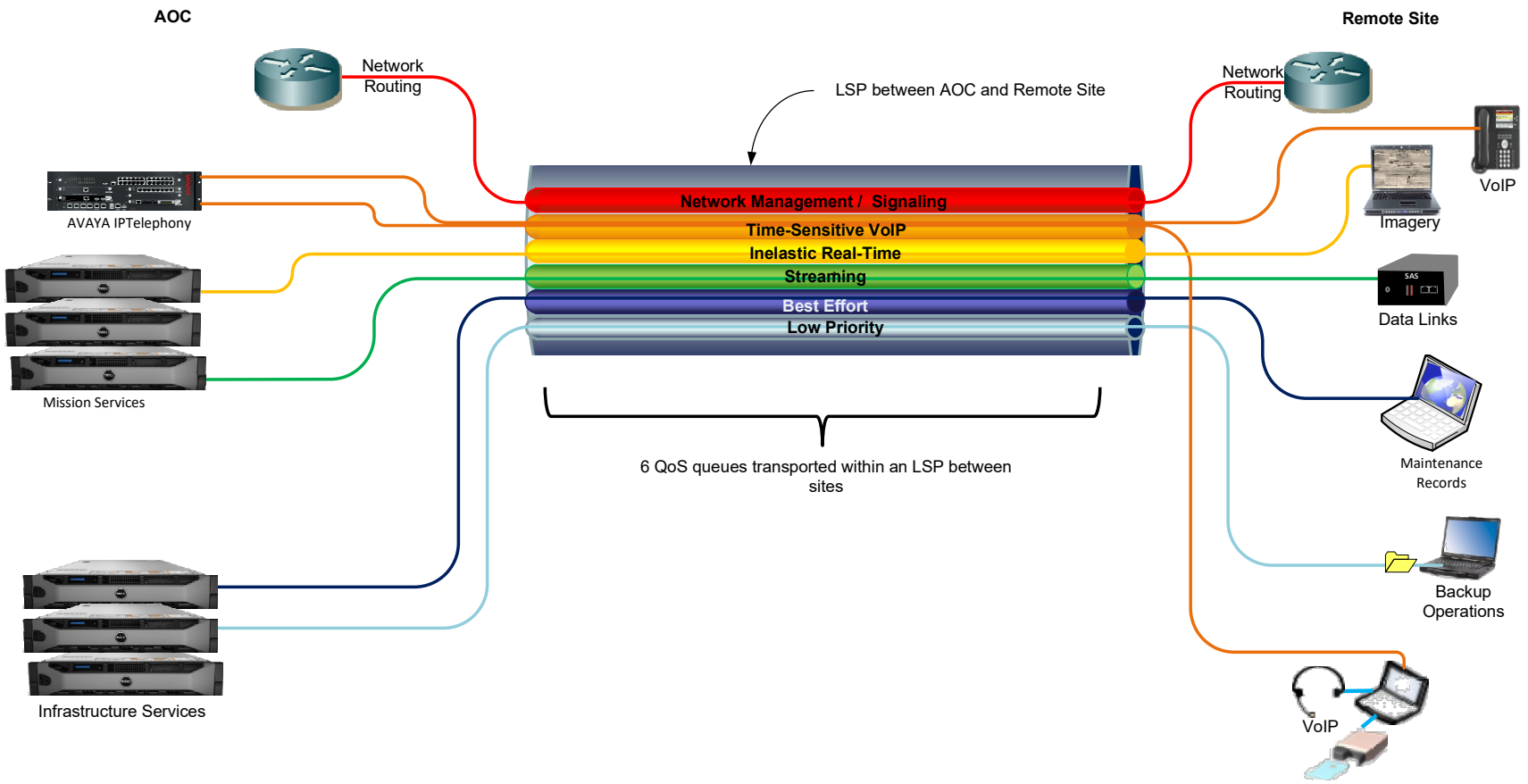


Figure 3-12: End-to-End Transport Over MPLS, RSVP and TE

3.2 Voice Communication Architecture

Reliable voice services are essential elements of AFAD operational missions providing secure and non-secure tactical communications among operators, joint forces, deployed airborne assets and ground-based weapons systems. EADGE-T integrates several tactical voice capabilities to provide a voice architecture using Voice over IP (VoIP) and Radio over IP (RoIP) technologies with QoS to prioritize time sensitive voice traffic. The solution provides voice capabilities supporting C2 Audio functions for CRC operators, a Voice Communications System (VCS) which includes tactical voice radio interfaces to support current and future voice radios, and an Enterprise scale, telephony system. The architecture is based on an end-to-end voice over IP infrastructure. Where specified in baseline requirements, distributed EADGE-T sites include radio over IP gateways to support tactical voice radios, telephony services, and RDU voice communications using a VoIP audio client voice application.
The design of the EADGE-T voice architecture is based on a set of design criteria to ensure that voice capabilities meet operational requirements for flexibility and effectiveness:

1. Standards-based – Design supports the ability to extend voice functions using standard interfaces to support interoperability between products from multiple vendors. Adopting the European Organization for Civil Aviation Equipment (EUROCAE) ED-137B interoperability standards for VoIP ATM (Air Traffic Management) supports future growth and reduces dependencies on a single vendor.
2. Compliant – Meets time critical requirements including call setup and push to talk (PTT) delays by reducing intermediate gateways between functions. Tactical communications rely on sub second response to commands. Gateways which translate signaling or voice traffic introduce delays which can affect operations.
3. Reliable – Design includes end-to-end mechanisms to detect and resolve equipment failures. Protocols used must provide built-in transactions to monitor the health of end-to-end communications.
4. Efficient – Provides required functionality by making effective use of available communications resources. Performance requirements must be met without impacting the performance of other system applications which use communications resources.
5. Manageable – Includes management and configuration interfaces to provide real-time equipment status. Provided voice communications interfaces support system monitoring and configuration utilities.

Using these design criteria as the basis for the EADGE-T voice architecture results in an integrated and interoperable voice capability which supports future system growth. The interoperability provided using international standards allows the integration of separate solutions for C2 Audio, tactical voice communications, and IP Telephony. Part 1 of the ED-137B standard is used in the EADGE-T design to not only to support vendor interoperability, but also leverage well established VoIP standards including Session Initiation Protocol (SIP), and the Real-time Transport Protocol (RTP). Session control functions included in SIP provide call establishment, routing and redundancy, while RTP transports voice packets including timestamps and headers to support radio signaling.

The design includes C2 Audio, tactical voice communications and IP Telephone services to support UAE SECRET, NON-US COALITION and UAE UNCLASSIFIED voice operations. The voice services provided in each security domain are distributed across operations centers at both Main Sites and the DAOC to provide survivability as shown in Figure 3-13. Standard time division multiplexed (TDMA) trunks are used to support calls between security domains but explicit security policies and interlocks are provided that only permit calls from a higher classification level to a lower one so that operators can make emergency calls from either the UAE SECRET or NON-US COALITION when required. So, for example, operators in the UAE SECRET domain can make voice calls to Search and Rescue personnel in the UAE UNCLASSIFIED domain but unsolicited UNCLASSIFIED calls to SECRET operators are not permitted.

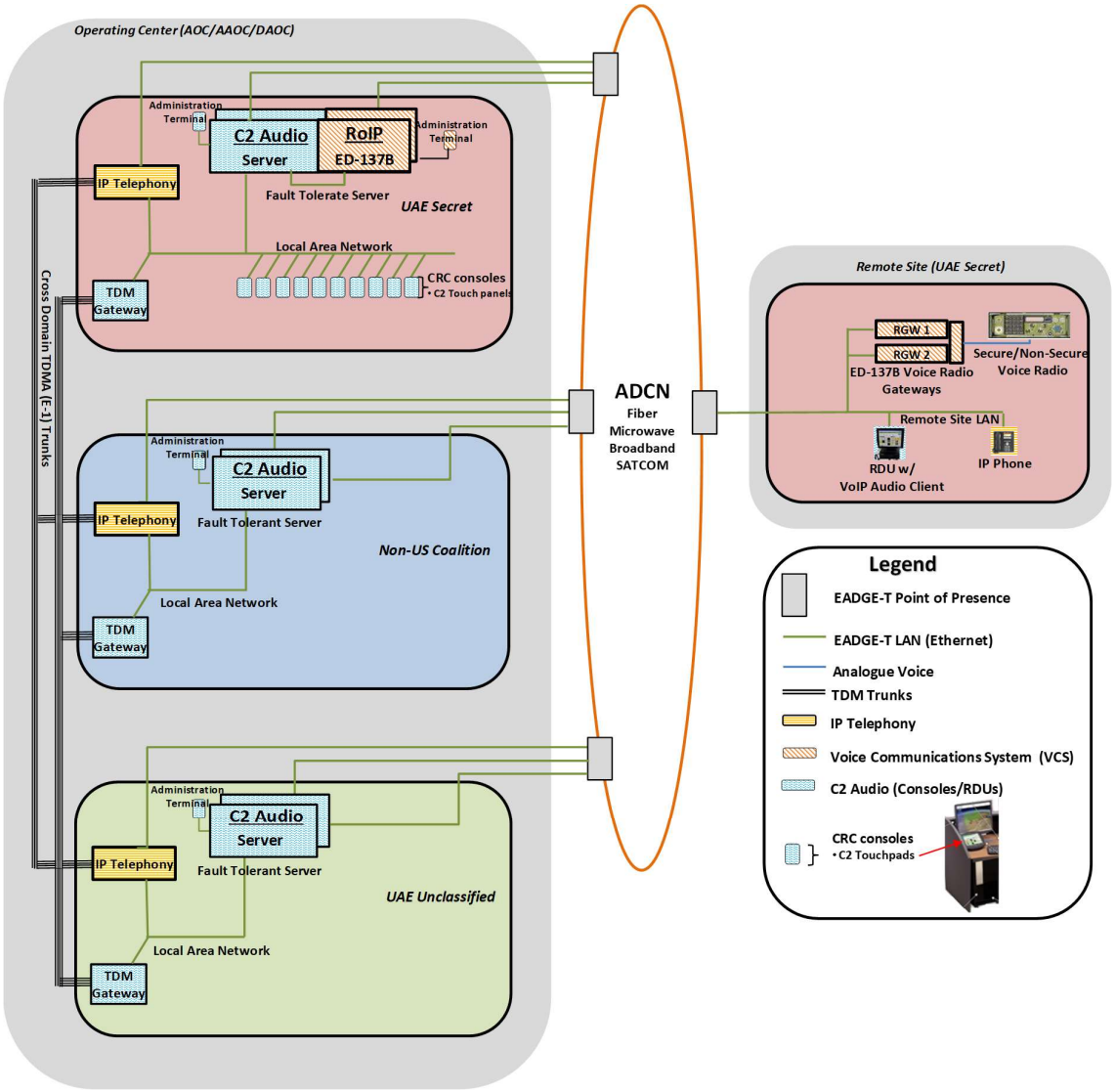


Figure 3-13: EADGE-T Voice Architecture

3.2.1 Console C2 Audio

C2 Audio functions are designed to be similar to the Communication Control Panel (CCP) used to support console operations in the EADGE system. C2 Audio fault tolerant servers in each operations center distributes VoIP communications to operator consoles using a centralized architecture similar to that of established multi-party conferencing systems based on a Multipoint Control Unit (MCU). Within each control center, the system distributes pulse code modulated (PCM) audio streams using IP protocols. In addition to distribution to consoles in the operating centers, C2-Audio supports voice calls with remote sites where RDUs are located. RDUs are configured with a C2-Audio soft client which provides remote operators with access to tactical voice calls. The C2 Audio subsystem communicates with other EADGE-T voice capabilities provided by the RoIP and IP telephony subsystems using a SIP protocol gateway. C2 Audio capabilities are described in the C012.2 System Level System Hardware SDP. Components in each console include:

- C2 Audio Thin Client supports multiple audio connections for each operator console. The thin client acts as an appliance that attaches to operator workstations and supports accessories including headphones, foot switches, speakers and an audio touch panel

- C2 Audio Touch Panel which allows operators to make phone calls using their headsets, establish or join internal ad hoc conferences with other AOC, AAOC and M/DAOC operators, and listen or talk on radio channels. The layout of each touch panel consists of multiple pages each consisting of an array of radio/call buttons that can be customized to meet the specific mission requirements for each operator
- Central processing elements of the C2-Audio system are hosted in a fault-tolerant server which ensures high system availability for voice services in each operations center
- System Administration Terminal (SAT) supports the creation of voice channels and groups as well as their association with each operator console. Once an operator logs onto their C2 audio touch panel, these settings are downloaded to the C2 Audio Thin Client and the layout and assignment of each button on the C2 Audio touch panel is displayed

Recording capabilities are provided as part of the Data Capture and Analysis subsystem to support the recording of console audio conversations.

3.2.2 Tactical Voice Radio Communications

EADGE-T integrates audio communications from remote radio transceivers using ED-137B radio gateways. Remote radios (including those in SHORAD towers and GATR stations) utilize redundant radio gateway interfaces which interface to the E&M (i.e., Ear & Mouth) analogue interface of each radio transceiver. Since radios can be configured for either voice or data, dual radio gateways are connected to all radios. Each radio is connected to a dedicated channel on a non-powered 'passive combiner' which is then connected to a main and standby radio gateway card. Each gateway card can support two separate radio transceivers. Figure 3-14 provides an example of a station equipped with two voice radio transceivers that are each connected to main and standby radio gateway cards using a passive combiner. The combiner includes six separate radio channels and each channel includes three separate E&M interfaces to the attached transceiver. This allows the transceiver to communicate with the main, and standby gateways as well as support for an existing EADGE voice communications Remote Radio Site Equipment (RRSE).

The gateways convert analogue signals into RoIP streams using RTP. The digitized voice stream that are sent using RTP include signaling flags that are included in the RTP extension header. This RTP header is used by ED-137B to support bidirectional link monitoring ('keep alives') to ensure connectivity between the operations centers and remote radio gateways.

ED-137B uses SIP to identify, locate and establish tactical communications between each radio and the VCS Server located in each operations center. SIP uses symbolic names to identify each end point (e.g., R03.LWM-G@CAP1 for the 3rd GATR radio at site LWM) and textural commands (REGISTER, INVITE, etc.) to establish calls. In the EADGE-T VCS, a tactical radio (Combat Network Radio – CNR) Push to Talk (PTT) call is established when access to a voice radio is first required (i.e., a button is assigned on a C2 Audio touch panel to a specific tactical radio). The VCS uses a Radio Server process as a concentrator so that multiple operators can connect to the same radio using a single radio gateway connection. Separate SIP sessions can be established between each radio gateway and servers located in different operations centers to support failover. Thus, in a two-site single team configuration, radio gateways can establish connections between the VCS Radio Servers located in both Main Sites 1 and 2.

Once the ED-137 voice radio session is established, RTP voice flows are exchanged between the radio and Radio Server process. During incoming (air-to-ground) communications, voice traffic received by the radio in the tower is sent to the Radio Server with the Squelch bit set in the RTP header. When an operator initiates a PTT operation, an RTP stream is sent from the console to the Radio Server and forwarded to the remote radio with the PTT bit set. Whenever voice traffic is not being sent between the server and radio gateway bidirectional keep alive messages are exchanged to ensure link availability. The call flows for call setup and a PTT operation are shown in Figure 3-15 and Figure 3-16.

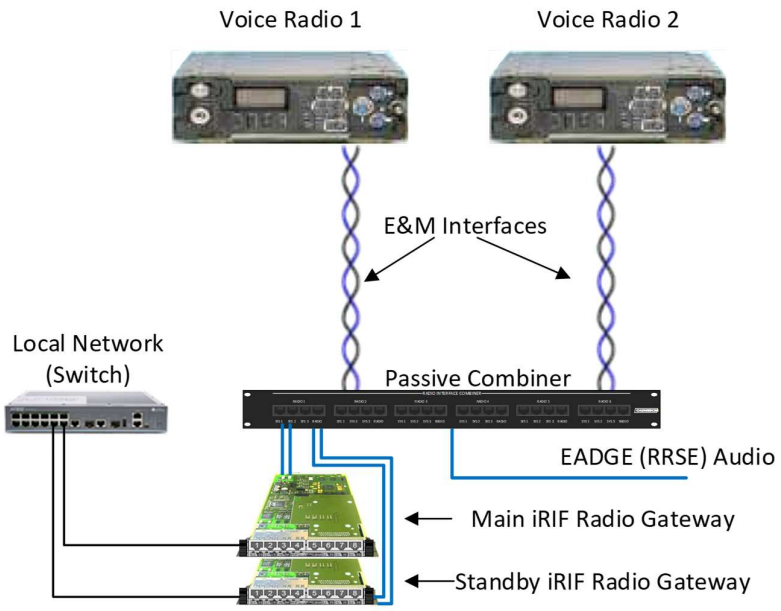


Figure 3-14: Example Remote Radio Site with Redundant Radio Gateways

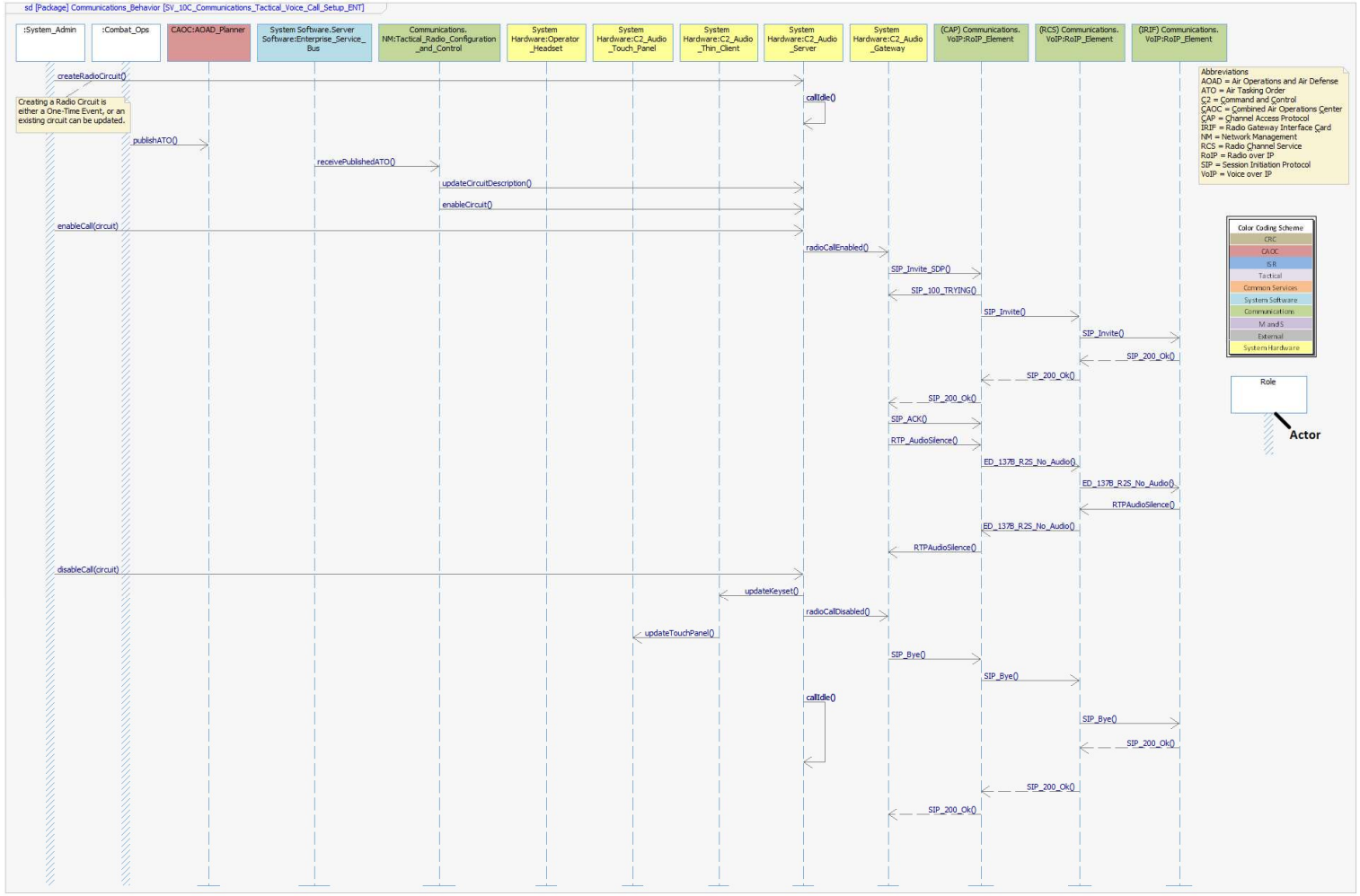


Figure 3-15: Tactical Voice Call Setup

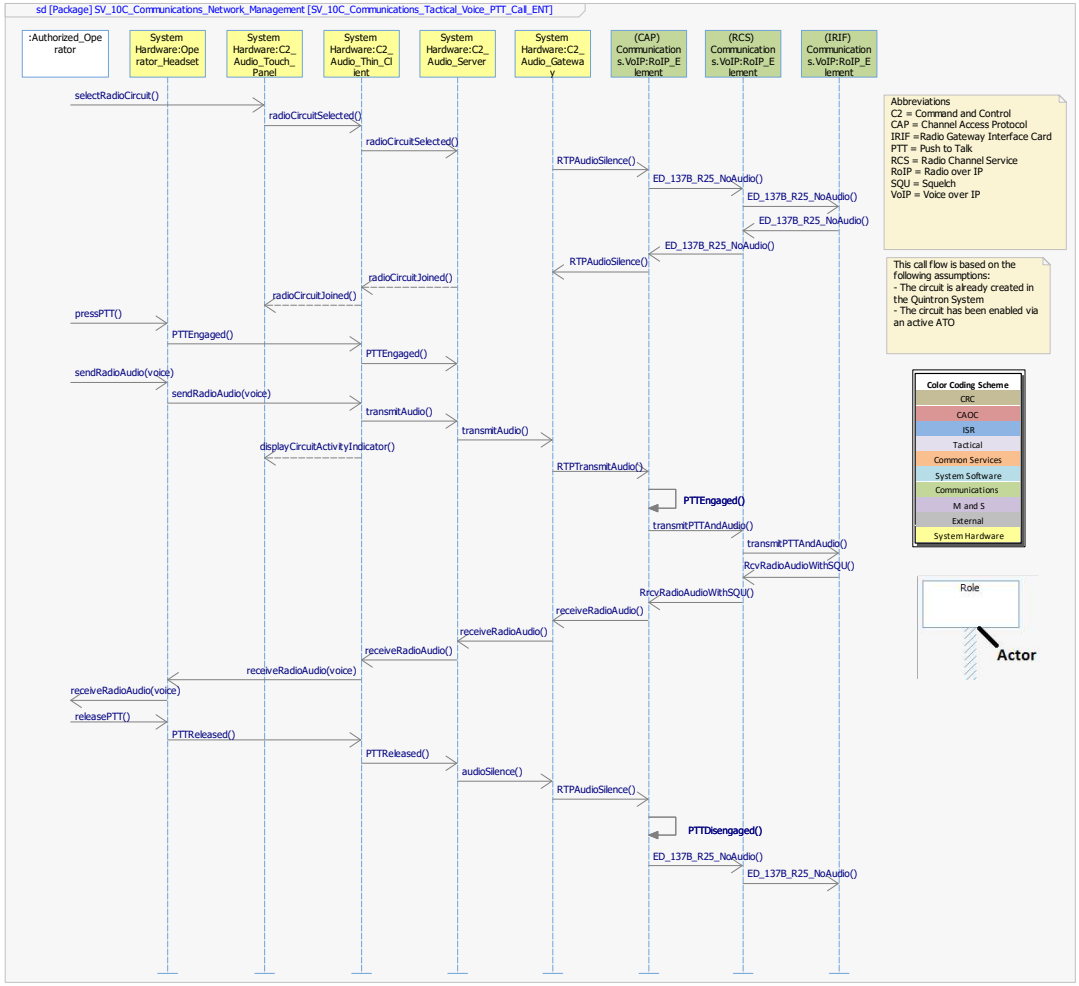


Figure 3-16: Tactical Voice PTT Call

3.2.3 IP Telephony

The EADGE-T voice design also includes a full functions business class telephony. EADGE-T telephony is based on standard VoIP technology and leverages 3G/4G concepts developed by the 3rd Generation Partnership Project (3GPP). The 3GPP is a consortium of international telecommunications providers that have promoted development of standards like the IP-Multimedia Subsystem (IMS). The architecture is based on a hierarchy of functions that is modeled after the IMS with a highly available lower tier which makes calls to higher layer functions to activate advanced services. As shown in Figure 3-17 calls initiated by distributed users at different EADGE-T sites use the SIP protocol to register and establish calls using session manager at larger sites. At this signaling layer, IP phones (user agents) register their presence to several session managers so that calling parties can contact other users across the enterprise even if a specific session manager is not available. User Agents (UAs) act a small Private Branch Exchanges (PBXs) and are able to establish simple calls between users but access to additional services including multiparty (meet-me) calls, conferencing, and call routing and directory lookup features require services provided by Layer 2, the connection layer.

The connection layer provides access to call and user parameters stored in the call manager database. Database configuration is accessed through system management terminals and includes a large number of configurable call attributes and dial plan information. Communications Managers at the connection layer are installed in duplex configurations in each Air Operations Center. These servers can also satisfy service requests for advanced functions including access to external phone systems through TDM gateways, and conferencing capabilities. Like the communications servers at layer 2, these layer 3 functions are hosted in virtual machines and include high availability features.

Independent phone systems are provided in each security domain, but the system restricts calls from higher to lower protection levels to support calls to search and rescue services (i.e., Secret to Non-US Coalition or Unclassified and Non-US Coalition to Unclassified). EADGE-T IP telephony is independent from the C2 Audio and tactical voice radios but the dial plan provided supports calling between IP phones and operators using C2 Audio services.

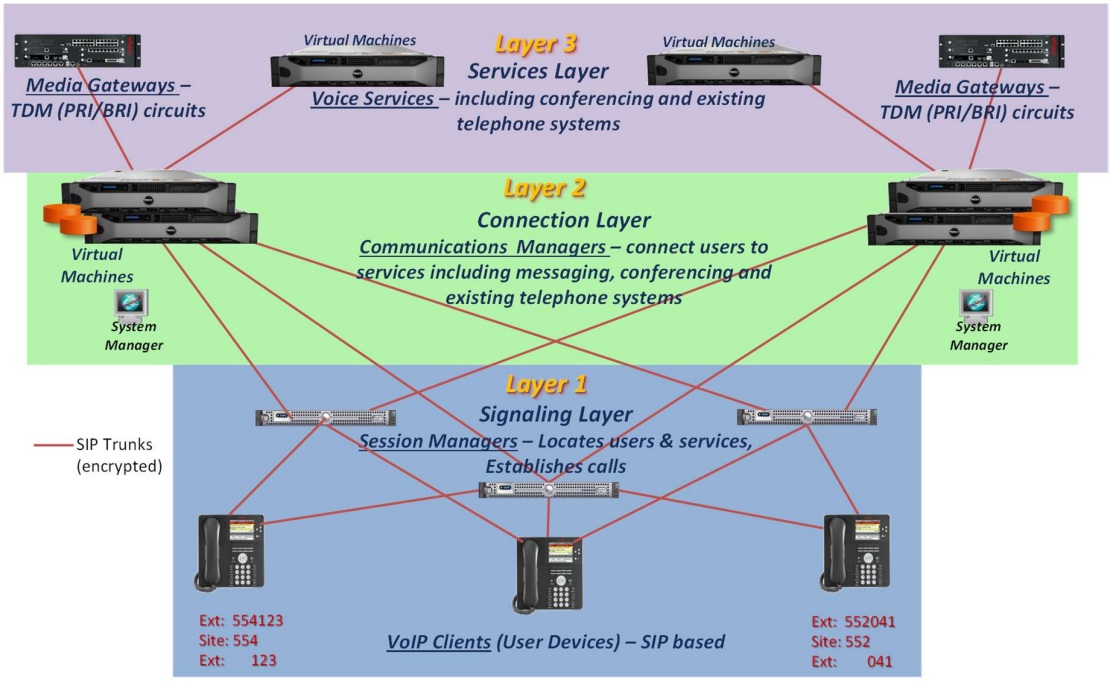


Figure 3-17: IP Telephony Design

The IP telephony design provides reliable services by installing high availability gateways at larger sites. These gateways include embedded processors which support layer 2 services and allow smaller sites to access services if larger sites are unavailable.

3.3 Digital Data Link Services

Datalink services are provided through the datalink radios in conjunction with Common Services and the Execution Manager application. Datalink radios are configured following the same sequence defined for the voice radio services. Once the radios are configured to the appropriate settings per the Network Planner allocations, the radio status in Common Services is updated so that the SCM can connect the datalink path to the MSCT server. Further details of the SCM processes and datalink operations are contained in Annex D and Annex L respectively.

3.4 Tactical Radio Configuration and Control Services

The TRCC component under the Communications Network Management System subsystem is responsible for configuration and control of the radio devices, including radio status. This component will be implemented as both TRCC Servers running as Shared Resources and with TRCC clients accessible on the servers as shown in Figure 3-18.Each TRCC Server will be configured to connect to all other TRCC servers in the AOCs and maintain a heartbeat connection to support failover. Any TRCC server can be configured as the Primary with the others being Standby. By default, the AOC will be configured as Primary with the Failover order being AOC, AAOC, DAOC and MAOC. Failovers will occur automatically if the Primary TRCC is stopped or if a manual failover is performed. The Failover hierarchy and list of TRCC servers is driven by a configuration file. This supports running the TRCC Client/Server in the operational, test and development environments.

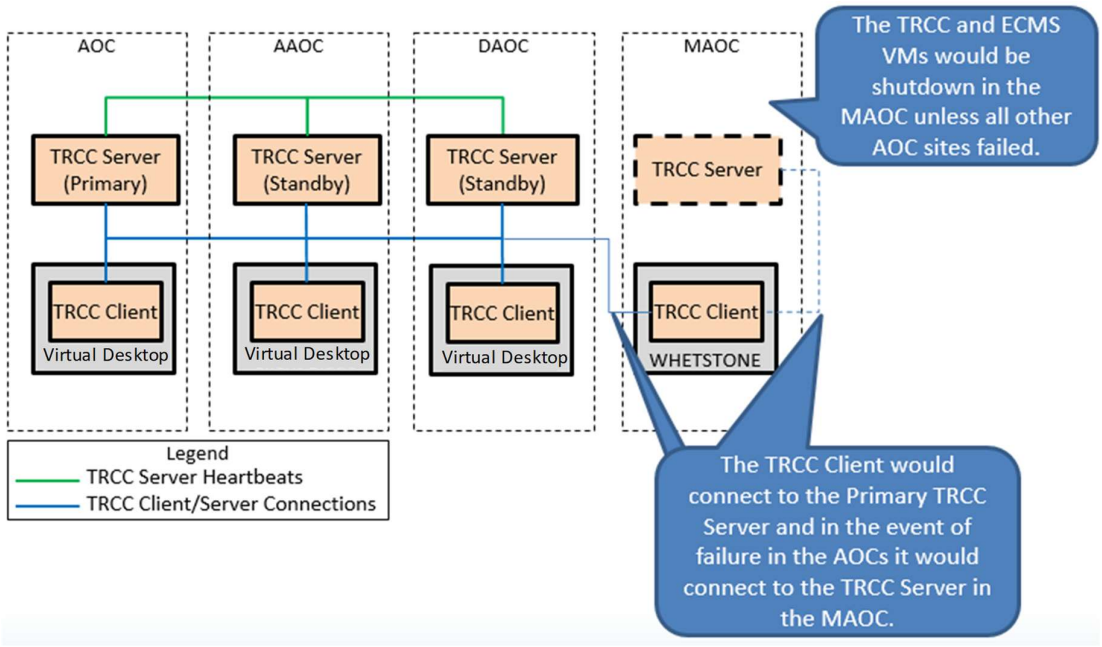


Figure 3-18: TRCC

In addition to the Failover implementation of multiple TRCC servers the VM hosting the TRCC server will be using VMware vSphere® Fault Tolerant (FT) mode, which provides availability for applications in the event of server failures by creating a live shadow instance of a virtual machine that is up-to-date with the primary virtual machine.

FT mode works by doing the following as shown in Figure 3-19:

- Creates a live shadow instance of the primary, running on another physical server

- The two instances are kept in virtual lockstep with each other using VMware vLockstep technology, which logs non-deterministic event execution by the primary and transmits them over a Gigabit Ethernet network to be replayed by the secondary virtual machine
- The two virtual machines play the exact same set of events, because they get the exact same set of inputs at any given time
- The two virtual machines access a common disk and appear as a single entity, with a single IP address and a single MAC address to other applications. Only the primary is allowed to perform writes
- The two virtual machines constantly heartbeat against each other and if either virtual machine loses the heartbeat the other takes over. The heartbeats are frequent, with millisecond intervals, insuring a failover with no loss of data, state, or network connections
- The failover to a shadow server automatically triggers the creation of a new shadow virtual machine to work with the now primary server, to ensure protection to the application
- The primary and shadow will be on different servers, but within the same Operations Center

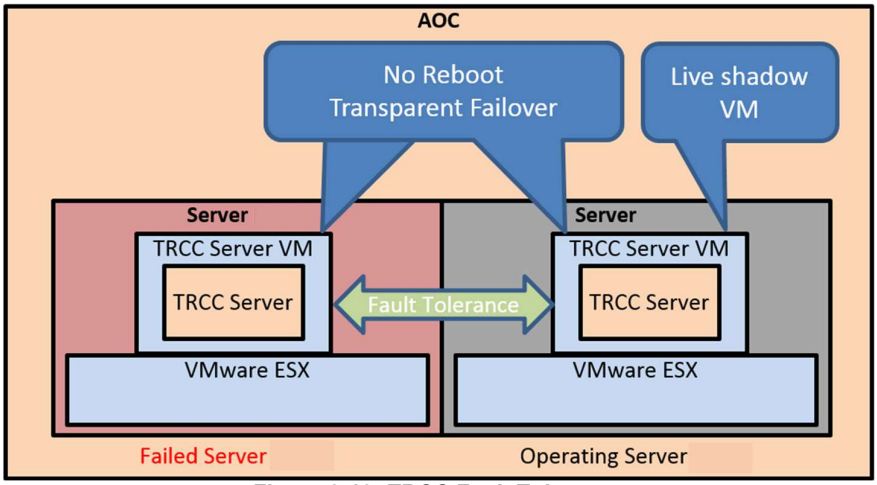


Figure 3-19: TRCC Fault Tolerance

By using VMWare Fault Tolerant mode in the TRCC server system availability for both GATR and SHORAD systems are improved. FT reduces the time required to restart a failure of the GATR Electronic Counter Countermeasure Management System / Communications Network Management (ECMS/CNMS) system thus preventing remote GATR stations from dropping their connection to the MSCT. The use of FT technology in the TRCC also maintains connectivity to the Radio Control Software (RCS) at deployed SHORAD deployment areas.

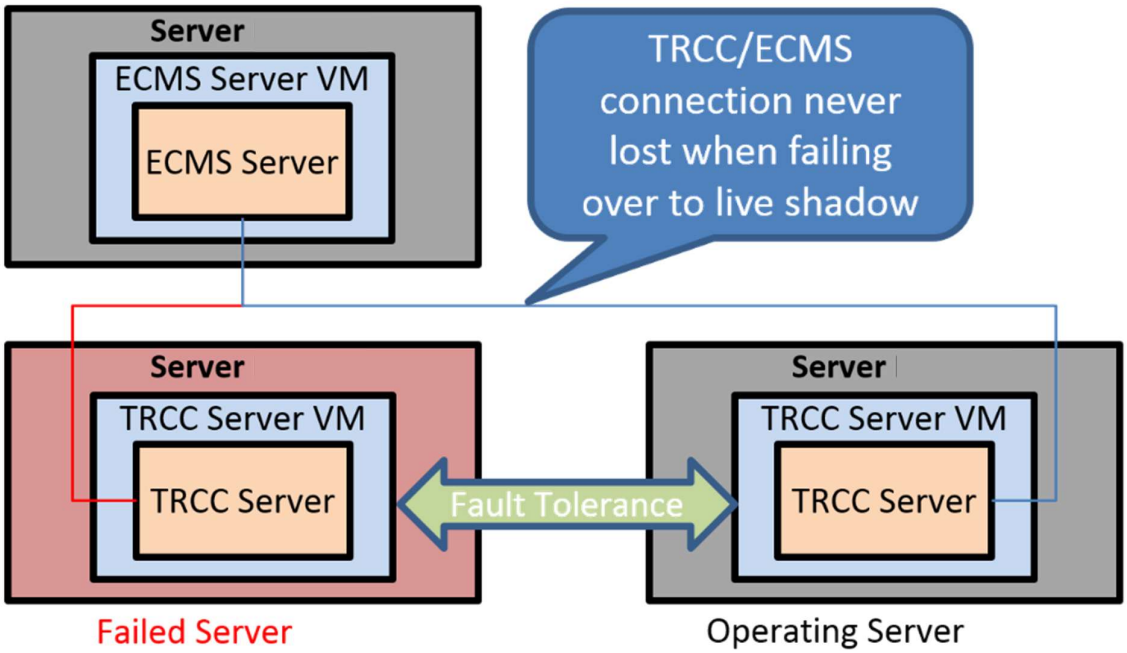


Figure 3-20: TRCC FT Failover With ECMS

TRCC supports a number of interfaces to perform its role in configuration, control, and status collection of radio devices as shown in Figure 3-21. These interfaces support both current EADGE systems and sub-systems new to EADGE-T. EADGE systems include GATR, SHORAD, and various other voice radios. TRCC will support these interfaces in the following ways:

- Maintain connections to all GATR ECMS servers to support configuration, control, and status of GATR radios via the implementation of the GATR ICD
- Maintain connections to the ported Thales RCS software running on SAS boxes at the SDA towers and remote radio sites to configure, control and status the SHORAD radios
- Deploy TRCC Agents to IP converters (SAS boxes) at the remote radio sites to control and status other voice radios supporting a Command Line Interface (CLI)
- Maintain connections to the TRCC Agent software for the Link-11 radios at the Link-11 sites to support control and status of the Link-11 radios
- Maintain connections to Common Services in the Mission Strings to update the radio status
- Sends updates to the C2 Audio system to update descriptions of the C2 audio voice circuits displayed on the CRC Operators touch panel
- Provide interfaces to support changes to the missions real-time, such as assigning new radios to support flight plan changes or to support radio replacement in event of a radio failure

The C2 Audio System Client will be used to setup the layout of the buttons on the CRC Operator touch panel. This button layout will have a reserved section of buttons that will be updated by TRCC as mission radios are configured for voice networks.

Next the VCS Management terminal can be used to remotely monitor and configure the radio gateways and will be used by the NMS system as an element manager of the Voice Communications System (VCS), which is described in more detail in Section 3.2.

Some of the radio related operational failures that can occur and how they would be conveyed to the Operators and resolved follows. First for the GATR radios, status updates are conveyed from the ECMS/NMT to the TRCC Server. For SHORAD a detailed status is received from the RCS software. In either case, the status will be displayed on the TRCC Client so that the operator can initiate further action. If a problem is resolvable remotely by rebooting the radio this can be done by remotely accessing the PDU and powering the radio off and then back on. Otherwise maintenance will need to be performed on the radio as indicated in the alert message. As described in the following sections,

the TRCC design supports future growth including adding a new instance of an existing radio, adding an additional serially connected radio, or adding a radio with a different interface.

3.4.1 Additional Like-EADGE-T Radio

In this use case a Radio Resource with controls that are identical to (in other words like) an existing radio (i.e. GATR 5400A or PR4G v2) would be added to Common Services via the Combined Air Operations Center (CAOC) Air Operations and Air Defense (AOADP) Planner as a system resource (e.g. new SFU, etc.…) as shown in Figure 3-21. Additional Like radio hardware would be installed at the site. There would be no software changes in this case. Next the C2 Audio System and the Radio Gateway (RGW) will be updated with the new voice circuit. Note that for GATR the new radio would be using one of the spare slots already available at existing GATR sites. Finally, a mission can be planned using the new radio.

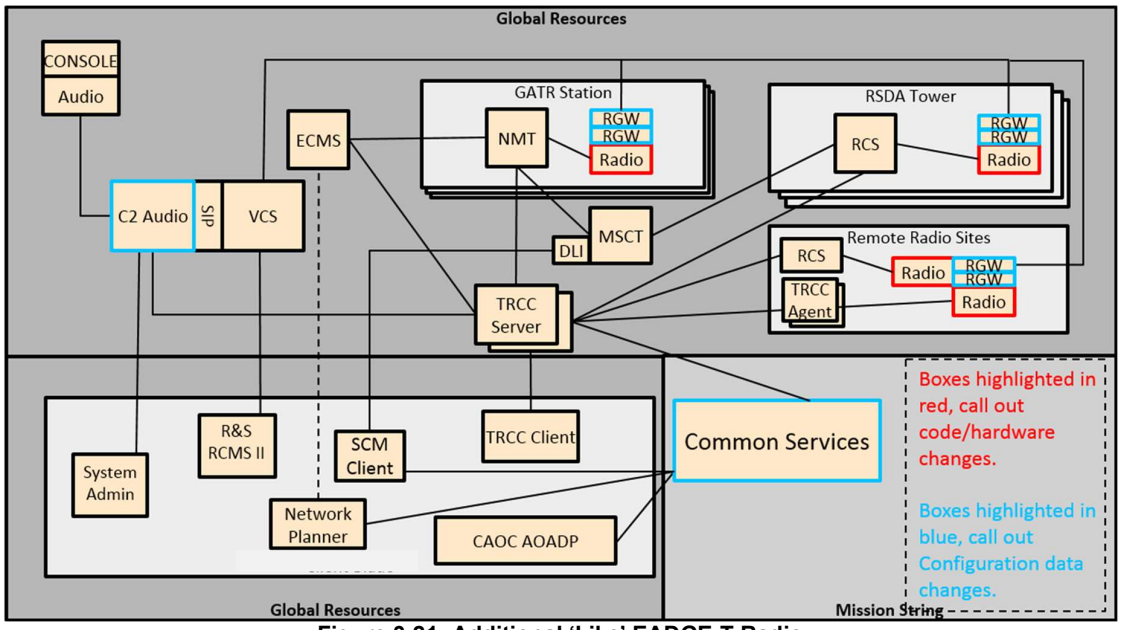


Figure 3-21: Additional 'Like' EADGE-T Radio

3.4.2 New EADGE-T Radio Model with Serial (CLI/Link-11)

When an unsupported radio is added to the EADGE-T system that supports control via a serial interface, a serial processor can be used to remotely interface to the radio. This will be the case for a Link-11 radio, for example. In this case a new SAS box would be added with a serial connection to the radio and an IP connection to the EADGE-T network as shown in Figure 3-22. Then the TRCC Agent would be installed on the IP converter box (no change to the TRCC Agent software). Next a new Radio Unit Type and Radio Planned Resource of that type would be added to Common Services via the CAOC AOADP. New radio hardware would be installed. TRCC would need to be updated to support the commands specific to the new radio and the TRCC Client would require a new panel to display the required radio parameters. Then the radio would be connected to the associated RGW and the C2 Audio System would be updated with the new voice circuit.

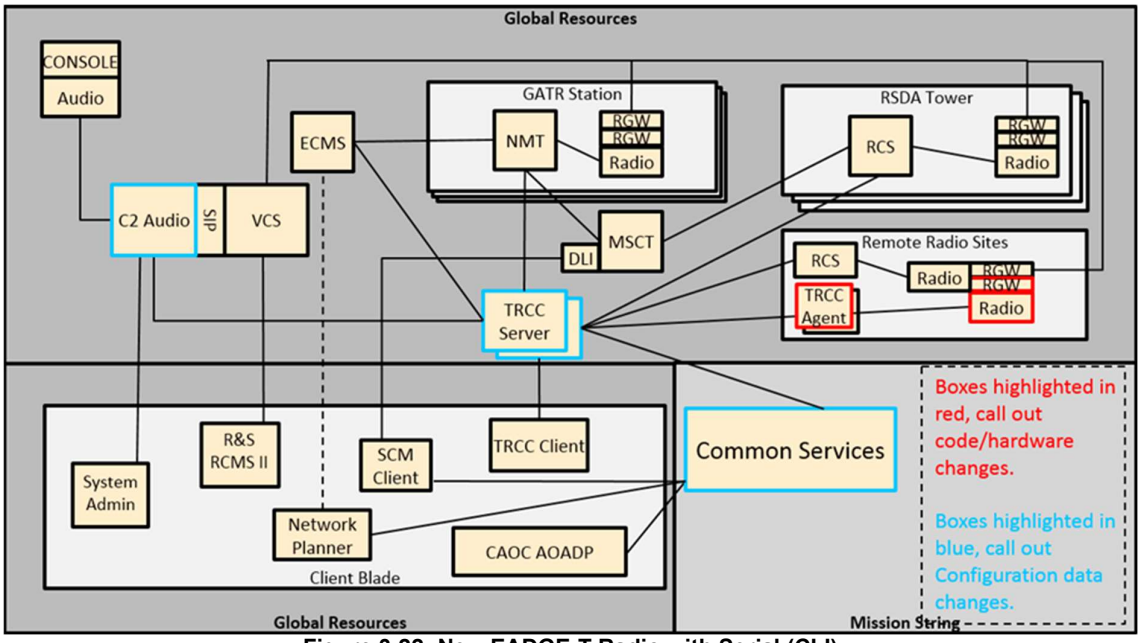


Figure 3-22: New EADGE-T Radio with Serial (CLI)

3.4.3 New Radio EADGE-T Capability at GATR/SHORAD

In this use case the Interfaces identified in the ICD would have to be implemented and added to the ECMS Server and NMT to support the new ICD (i.e. TRG-5400N) as shown in Figure 3-23. TRCC would be updated if it drove a different interface definition from baseline ICD. Then add a new Radio Unit Type and Radio Planned Resource to Common Services for the new radio. New radio hardware would be installed. Then the radio will be connected to the associated RGW and the C2 Audio System will be updated with the new voice circuit. In the case where the radio is installed at a new site a new RGW will also need to be installed.

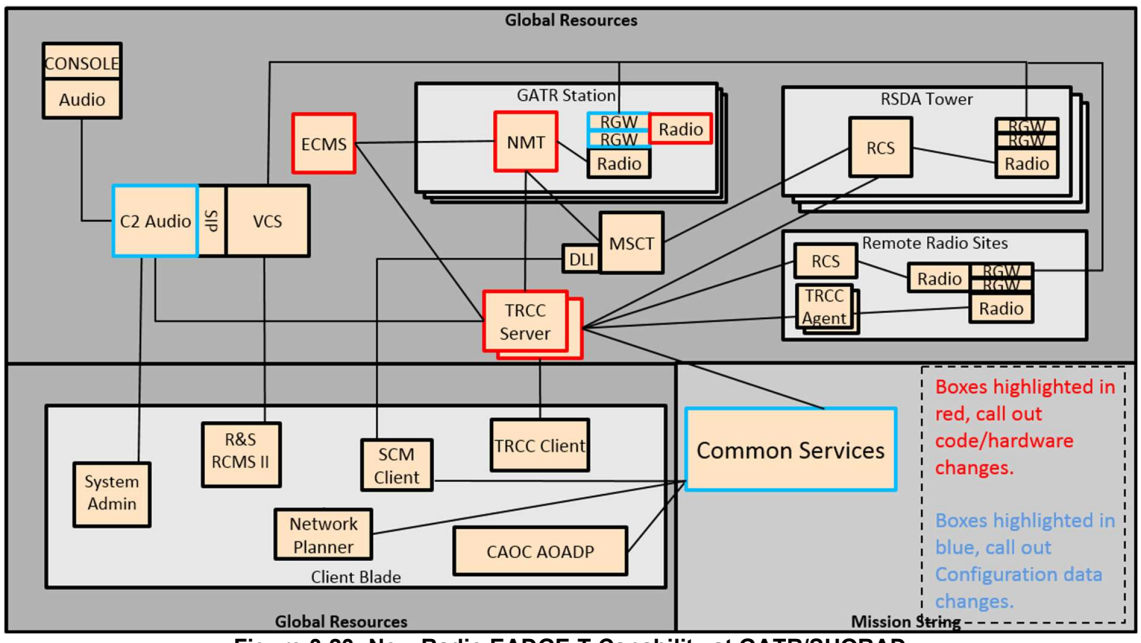


Figure 3-23: New Radio EADGE-T Capability at GATR/SHORAD

3.4.4 New Radio ICD with New Capability

In this use case the data model in Common Services needs to be updated to model the new capability as shown in Figure 3-24. Network Planner would need to be updated if one of the new capabilities affects RF network planning. TRCC will need to be updated to implement the new ICDs interfaces. TRCC client will need to be updated if there are new manual interfaces that the operator would want to access. Common Services will need to be updated to store or change existing parameters for the Radio Unit Type Configuration, which will result in display, database, and web service updates in addition to adding the new Radio Unit Type Data. The Radio Unit Type Configuration contains the list of presets that can be selected for the radio model and will only change if a new frequency plan was loaded into the radio. New radio hardware will be installed. Then the radio will be connected to the associated RGW and the C2 Audio system will be updated with the new voice circuit. In the case where the radio is installed at a new site, a new RGW would also be needed.

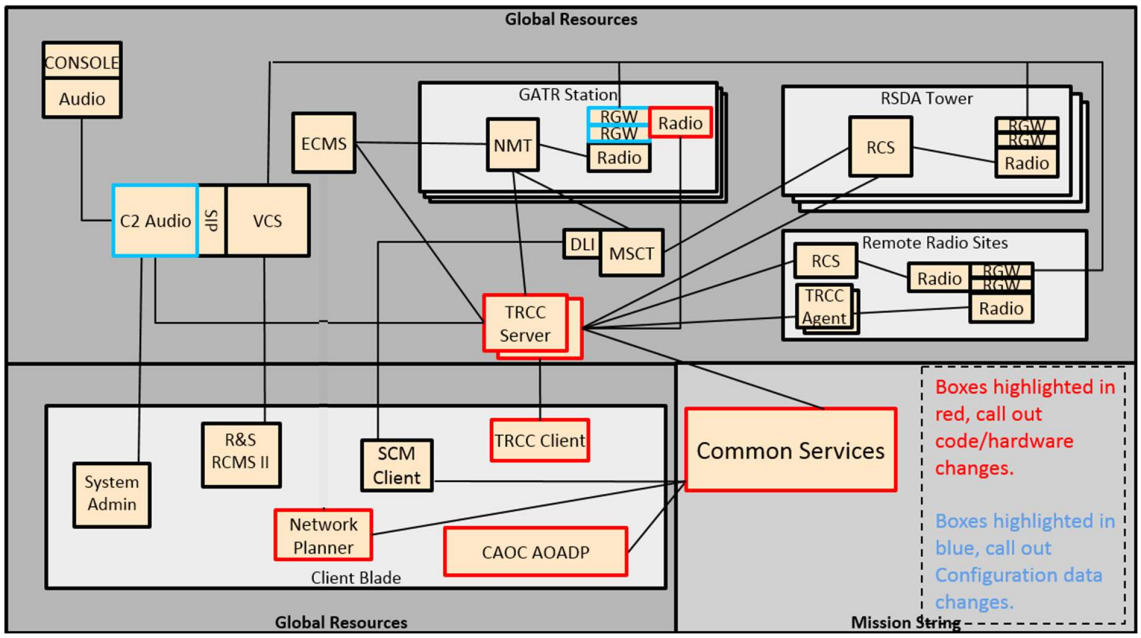


Figure 3-24: New Radio ICD with New Capability

4 EADGE-T C4ISR SITES COMMUNICATION ARCHITECTURE

EADGE-T sites are based on a structured design using common functional components. Network devices including Core Routers, Edge Network Encryptors, Firewall/Routers, Layer 2 network switches are scaled to allow for current needs with the ability to support new acquisition platforms and accommodate organizational changes for modified C3 capabilities. This section provides a summary of the network design for different fixed and mobile EADGE-T sites. While SV-2 architectural artifacts and a Bill of Materials (BOM) have been provided for the sites, site descriptions provided in this section are limited to EADGE-T communications capabilities including network devices and descriptions relevant to the network design. This information is provided to support the design and illustrate the modular elements used to support EADGE-T communications capabilities. Additional device information including the device types utilized are included in Appendix A of the Fixed Site Design Analysis Report.

4.1 Network Components

Network devices specified in the design have been assigned high level names which include a standard set of sub-assembly components. This assignment serves to associate required sub-components, supports scalability and simplifies equipment ordering. The major network components located at each site and enclave include a P- or PE-Router, and optionally an Encryptor and Firewall/Router. The devices selected for each of these network functions are discussed below. Network switches are not included below but are all based on Juniper EX series switches.

4.1.1 Routers

P- or PE-Routers provide internal and/or core routing between the enclaves at each site and the ADCN. The devices selected are based on the switch backplane performance in bits/second. Large routers support 10Gbs interfaces required at core and Main Sites while small routers are used at remote sites. The rugged models are used in the M/DAOC and SFUs. As these routers interface to the ADCN, P- and PE-Routers must support MPLS. MPLS protocols are supported natively on Juniper MX series routers. SRX security gateways can support MPLS when operated in packet mode. The following Table 4-1 contains the router models and throughput.

Table 4-1: Provider and Provider Edge Devices

PROVIDER & PROVIDER EDGE ROUTERS	JUNIPER MODEL(S)	PERFORMANCE SWITCH FABRIC
L99_PROVIDER_EDGE_SMALL	SRX550	50 Gbps
L99_PROVIDER_EDGE_ LARGE	MX480	480 Gbps
L99_PROVIDER	MX480	480 Gbps
L99_ROUTER_SMALL	SRX550	50 Gbps
L99_ROUTER_MX104 (Rugged)	MX104	80 Gbps
L99_RUGGED_ROUTER	LN1000 LN2600 RTR8GE NFX250	9 Gbps

4.1.2 Encryptors

EADGE-T encryptors support Suite B encryption profiles using approved block cipher algorithms. Encryptors pass traffic between sites using IP Security (IPSec) protocols. Thus, the IPSec (VPN) performance metrics listed below are used to select the appropriate device. The following Table 4-2 contains the encryptor models and throughput. While the routers used to support IPSEC encryption algorithms provide multiple network interfaces, a single interface is used to connect the encryptor to the ciphertext (encrypted traffic or black) side and plaintext (unencrypted or red) side of the encryptor.

Table 4-2: Enclave Encryption Devices

ENCRYPTORS	JUNIPER MODEL(S)	PERFORMANCE VPN
L99-50MBPS_IPSEC_ENCRYPTOR	SRX220	100 Mbps
L99-100MBPS_IPSEC_ENCRYPTOR_V2 **L99-OOBM_ROUTER**	SRX240	300 Mbps
L99-100MBPS_IPSEC_ENCRYPTOR	SRX550	1 Gbps
L99-1GBPS_IPSEC_ENCRYPTOR	SRX650	1.5 Gbps
L99-10GBPS_IPSEC_ENCRYPTOR	SRX5400E	35 Gbps
L99-100MBPS_IPSEC_ENCRYPTOR	LN1000 LN2600 RTR8GE NFX250	250 Mbps

4.1.3 Firewall/Routers

Traffic entering or leaving each enclave passes through a firewall/router which enforces security policies to prevent unauthorized or malicious traffic. Routing functions support local subnets and virtual local area networks (VLANs). Key features are the ability of the Firewall/Router to support security policies and known network attacks (intrusion detection and prevention). The firewall architecture of the SRX series devices support separate security partitions known as zones to separate traffic flows and apply appropriate policies. The following Table 4-3 contains the firewall/router models and throughput.

Table 4-3: Firewall/Router Devices

FIREWALL / ROUTERS	JUNIPER MODEL(S)	PERFORMANCE FIREWALL	PERFORMANCE INTRUSION PREVENTION
L99-FIREWALL_ROUTER_XSMALL	SRX220	950 Mbps	80 Mbps
L99-FIREWALL_ROUTER_SMALL_V2	SRX240	300 Mbps	230 Mbps
L99-FIREWALL_ROUTER_SMALL	SRX550	5.5 Gbps	800 Mbps
L99-FIREWALL_ROUTER_MEDIUM	SRX650	7 Gbps	1 Gbps
L99-FIREWALL_ROUTER_LARGE	SRX5400E	65 Gbps	22 Gbps
L99-RUGGED_ROUTER	LN1000 LN2600 RTR8GE NFX250	2 Gbps	250 Mbps

4.1.4 Network Switches

Network switching devices provide the enclave infrastructure for larger sites. Switches have been selected based on performance, Virtual network (VLAN) support as well as fan-out requirements. Table 4-4 includes the switching devices used in each EADGE-T enclave. Larger sites utilize Juniper EX4200 and EX4550 switches for production data networks while EX2200C switches are utilized to support the transport of management traffic as well as power over Ethernet (POE) device interfaces. A more complete breakdown of where each switching device is utilized is provided in Appendix A of the Fixed Site Design Analysis Report.

Table 4-4: Network Switching Devices

SWITCH PERFORMANCE	EX2000C-12	EX4200-48	EX4200-24	EX4200-48
Data Rate	28 Gbps	88 Gbps	136 Gbps	960 Gbps

SWITCH PERFORMANCE	EX2000C-12	EX4200-48	EX4200-24	EX4200-48
Throughput	21 Mbps	64 Mbps	101 Mbps	714 Mpps
10Mb/100Mb/1Gb Port Count	14	24	24	48
10Gb Port Count	0	2	2	48
Virtual Chassis Units Supported	8	10	10	10
MAC Addresses	16000	32000	32000	32000
IPv4 Routes	6,500	16000	16000	14000
VLAN Count	1024	4096	4096	4096
ARP Entries	2000	16000	16000	8000
Wire Speed	Yes	Yes	Yes	Yes

4.2 Fixed Sites

The fixed sites described in this subsection are provided to show the common network communications elements used at all EADGE-T sites. Figures provided in this section show portions of the Level 2 SV-2s and are included to show the modularity of the communications design and specific network elements and ADCN interfaces. The SV-2s and information provided in the Site Installation Plans should be consulted for specific site information.

4.2.1 Core Network Sites

Each of the 14 core sites are interconnected via 10Gbps links over the Al Sharyan optical network and EADGE-T equipment at all but two of the core sites (the exceptions are Main Sites 1 and 2) are hosted in Army Signal Corps facility locations. Each of these 12 core sites include the following network equipment:

- **L99_PROVIDER:** Single P-Router large chassis router
- **L99-OOBM_ROUTER:** Management Router

The P-Router forwards MPLS traffic to other P-Routers and PE-Routers at core and remote sites respectively. As shown in Figure 4-1, each core site also includes remote management capabilities consisting of a management server, IP Keyboard/Video/Monitor (KVM), console server and Power Distribution Units (PDUs). Management interfaces are monitored and controlled by the network management server over a local Out of Band (OOB) management network. OOB data is encrypted by the management router and forwarded over the 1Gbps link to the P-Router. Encrypted management information is sent to Network Monitoring stations located at the AOCs. Remote management capabilities are supported at fixed sites as described in Section 6.2 of this document.

Dual 10Gbps links connect the P-Router to the Al Sharyan OTN. These connections are aggregated so that the loss of one of the links will not affect the exchange of traffic.

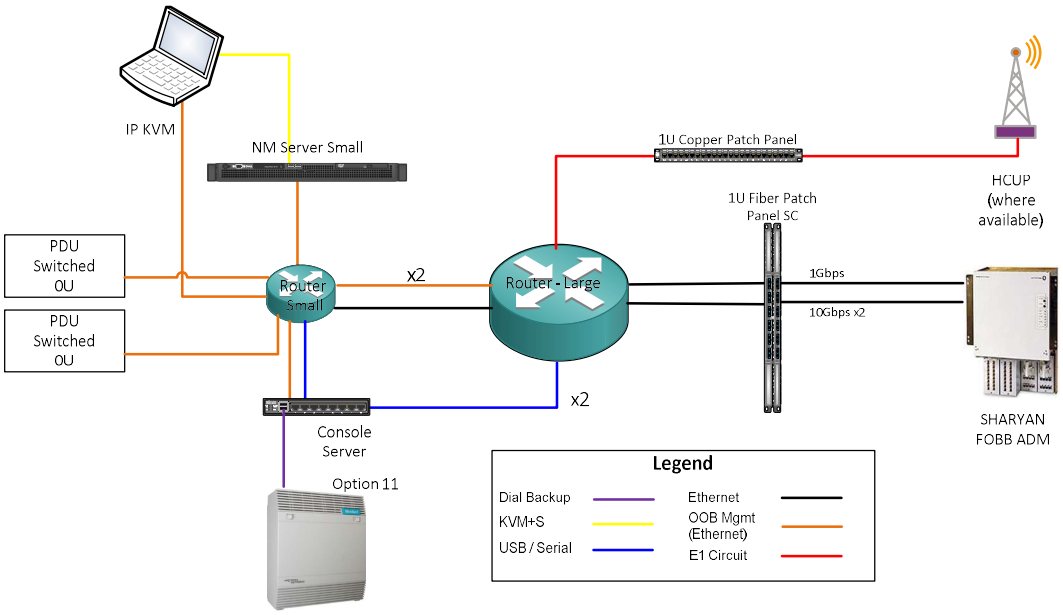


Figure 4-1: Core Site Design

4.2.2 *Main Sites*

Main Sites 1 and 2 serve as dual communications hubs that support command and control traffic between other EADGE-T sites. PE-Routers at each Main Site establish multiple MPLS tunnels to each remote site to separate secret, non-us coalition and unclassified traffic.

The network devices used in the Edge Networks of Main Sites are shown in **Error! Reference source not found.** and include:

- **L99_PROVIDER_EDGE_LARGE**: Dual PE-Routers in a high availability configuration
- **L99_OOBM_ROUTER:** Management Router & Out of Band Management Switches
- Base Ring Switches for distribution to other sites located at each Main Site.
- Port-based Network Access Controllers (PNAC) to authenticate network access
- Server stacks to support services including Network Management, & Network Time Protocol
- Interfaces which support dark fiber, and HCUP connections between sites

Main Sites 1 and 2 are considered core sites since they are inter-connected to other core sites in a full mesh topology. However, Main Sites differ from the other core sites in the following ways:

1. Main Sites are configured in a high availability cluster configuration consisting of dual **L99_ROUTER_LARGE** chassis
2. The router virtual chassis configuration at both sites are PE vs P-Routers since they are located at the edge of the ADCN and attached to multiple sites and enclaves in the Main Sites
3. The PE-Routers at Main Sites include additional ADCN interfaces including dedicated dark fiber and microwave links between the Main Sites

Main Sites have the same remote access management capabilities as core and other fixed sites.

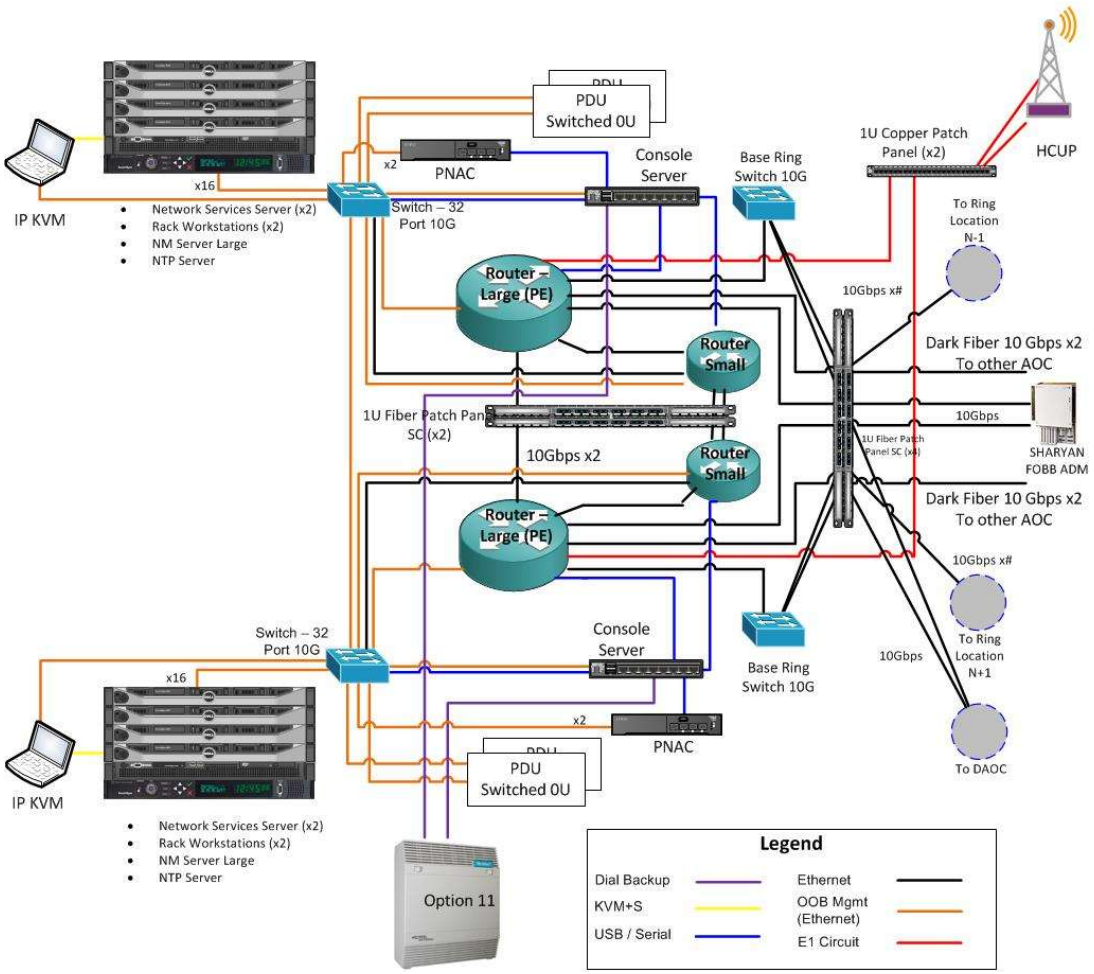


Figure 4-2: Main Site Edge Network Design

4.2.3 Base Area Networks

Where an EADGE-T location includes multiple sites that are connected to the ADCN by one or more PE-Routers, a fiber optic campus or Base Area Network (BAN) is used. BANs allow traffic between PE-Routers and distributed sites within the location to be exchanged using aggregated fiber optic links in a ring topology. BANs are installed at most AFAD air bases but also used in smaller locations, where appropriate. The design of the Main Sites shown in **Error! Reference source not found.** includes fiber optic patch panels and 10Gbps switches to support a ring network on the right side of the figure.

Base Area Networks are a logical extension of the ADCN in that the link between the Provider Edge router and the enclave is encrypted. Since the enclave encryptor is located with the enclave and not collocated with the PE-Router, information transported in the fiber optic cable between the enclave and PE-Router is protected.

The Base Area Network located at Main Site 2 is unique in that it uses a dual ring design. The BAN at Main Site 2 consists of two distributed switch clusters. Each cluster is composed of up to 10 distributed Juniper EX switches that are interconnected to form a distributed backplane. The switches form a ring and connect to enclaves and routers within an area of the base. A layer 2 link is formed over this distributed switch architecture which connects each enclave with a specific point of presence (PoP) for the Al Sharyan network.

4.2.4 Remote Sites

The network equipment at remote sites including PE-Routers and Edge Network components perform the same role as other fixed sites. Since the rate at which traffic is exchanged with the enclave LANs is ultimately limited by the amount of bandwidth provided by the ADCN interface (and particularly the FOBB), the size of the network equipment used in the design is scaled down to meet site throughput requirements with additional spare capacity for future growth. Typical remote sites include the following components as shown in **Error! Reference source not found.**:

- **L99_PROVIDER_EDGE_SMALL:** Dual PE-Router configured as a virtual chassis

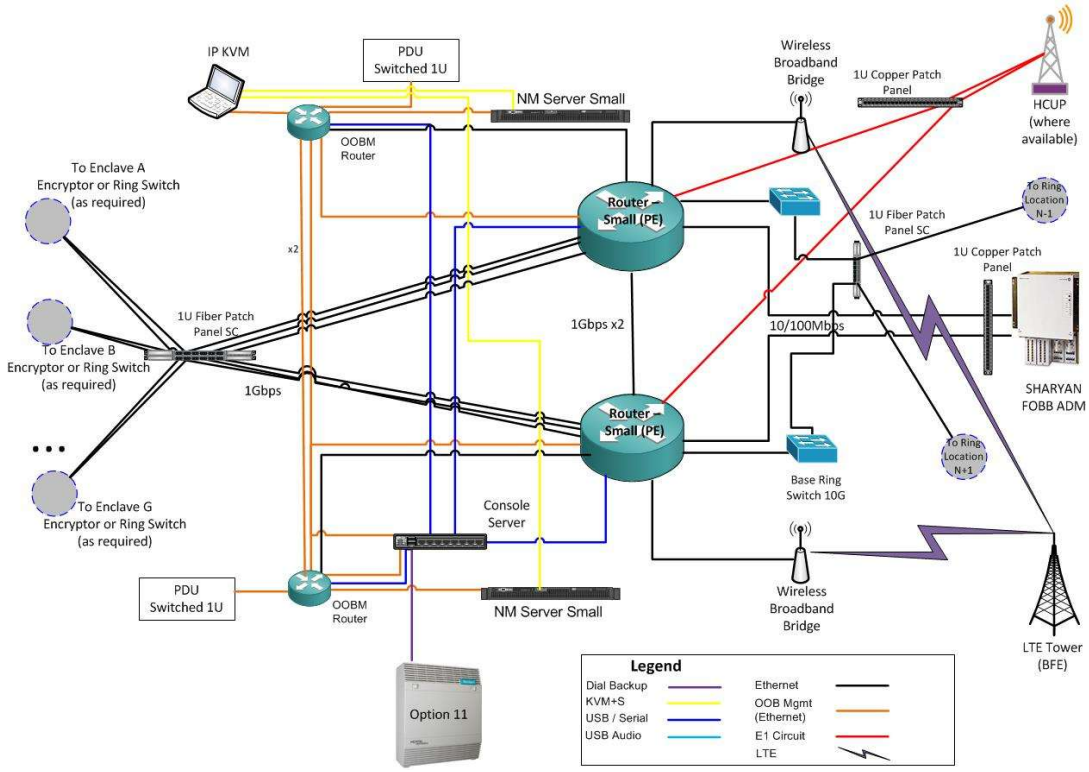


Figure 4-3: Remote Site Edge Network Design (typical)

Devices used at remote sites including PE-Routers and Edge Network equipment are functionally identical to devices used at other fixed sites. As shown in Figure 4-3, remote sites typically include additional ADCN network transport network including both LTE broadband and HCUP microwave in addition to Al Sharyan FOBB. Like other fixed sites, remote sites include an OOB management network (shown in orange) which allows equipment to be remotely monitored from the operations centers.

Local Area components used in a typical remote site enclave include the following as shown in Figure 4-4 below.

- **L99_100MBPS_IPSEC_ENCRYPTOR:** Dual Suite B encryptors per enclave
- **L99_FIREWALL_ROUTER_SMALL:** Dual Security gateway providing firewall protection and routing

The equipment hosted within each remote site will vary depending on the capabilities provided and can connect to the PE-Routers to access the ADCN using a ring network if appropriate. The site shown includes connections to Remote Data Units (RDUs). A separate OOB management network is provided to support equipment in each security domain.

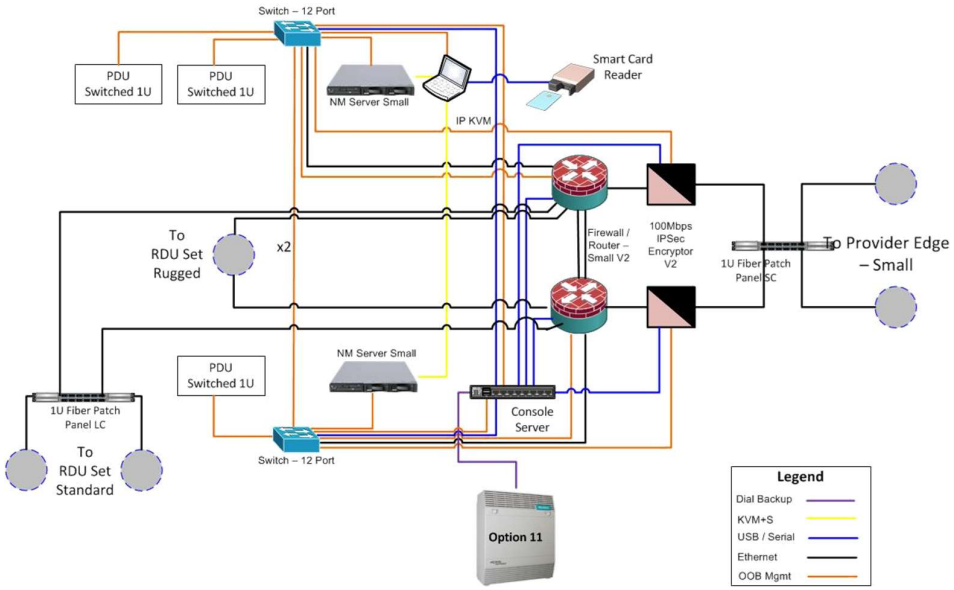


Figure 4-4: Remote Site LAN Design (typical)

4.2.5 GATR Voice and Data Architecture

Air-to-ground communications provided by current GATR capabilities are integrated into the EADGE-T architecture. Interfaces have been defined which combine existing GATR planning tools with the EADGE-T Tactical Radio Configuration and Control (TRCC) to replace the existing EADGE management elements (CNMS). The resulting communications system provides an upgrade path which is the basis for extending current air/ground communications. The new system can support a combination of new fixed and mobile LLR stations with the existing main and secondary stations.

The standard EADGE-T network design supports both centralized planning and management services along with remote stations using dedicated subnets to enforce security policies to limit system vulnerabilities. Operator or technician access to GATR management and control applications are provided through service interfaces which use rules installed in the firewall/routers to protect communications assets. The integrated GATR solution preserves existing secure and non-secure data and voice capabilities using existing radio assets while supporting the migration to newer technologies.

As described in the Communications SDP (C012.4.0), the GATR subsystem consists of planning, Electronic Counter-Countermeasure (ECCM) management and control functions located at Main Sites, with station management functions supported by the NMT at the remote stations. The centralized software management and control functions have been upgraded and re-hosted in virtualized servers. New fault tolerant virtualization techniques are being used to ensure high levels of availability and prevent loss of operational control in the event of a server fault.

Upgrades to the remote NMTs provide a normalizing layer which supports a common command set to operate each station. The upgraded NMT software and hardware will be installed at all existing

GATR sites to eliminate obsolete components and serve as a gateway to control voice and data radios. Unlike existing Message Interface Unit (MIU), data exchanges which use a single interface for all the LU-2 networks in a station, EADGE-T establishes independent CRC data link processes to support each LU-2 network. Data exchanges between the MSCT and patrol aircraft are controlled by these link interfaces with link status monitoring provided by the TRCC.

The network equipment at each GATR station consists of the following as shown in Figure 4-5:

- **L99_PROVIDER_EDGE_SMALL**: Dual SRX550's PE-Router connected via a Ring network
- **L99_100MBPS_IPSEC_ENCRYPTOR:** Dual rack mounted SRX550's
- **L99_FIREWALL_ROUTER_V2:** Dual Rack mounted and located in a building near the tower

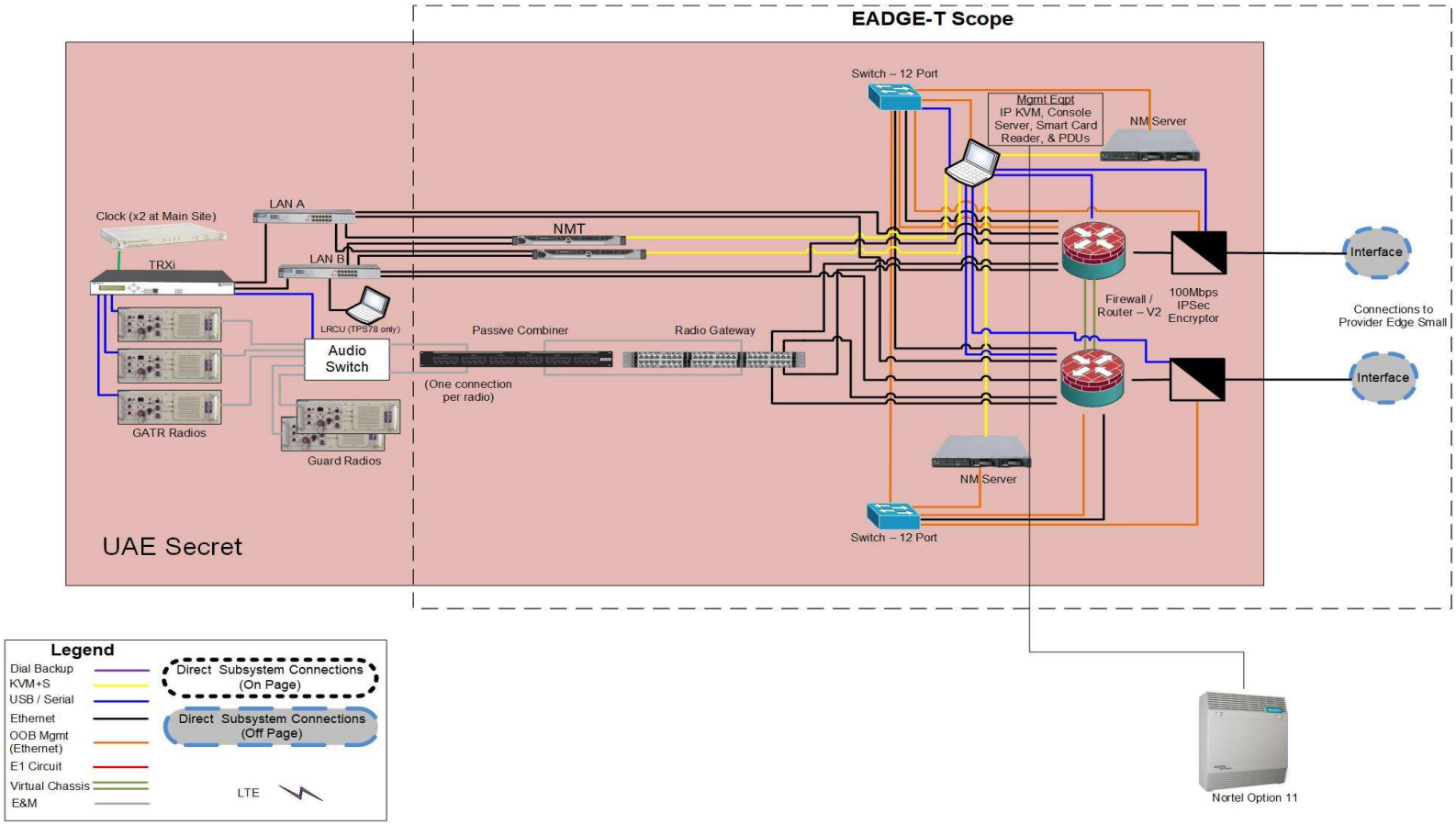


Figure 4-5: GATR Site LAN Design

4.2.6 SHORAD Voice and Data Architecture

The EADGE-T communications design supports the exchange of targeting and engagement information with SHORAD units using RF and wired technologies. Radio SHORAD Deployment Areas (RSDAs) support time based (TDMA) communications with AFAD weapons systems using the SHORAD Data Link (SDL) protocol exchanges. The EADGE-T communications design addresses reliability issues with the current EADGE system by rewriting the original centralized Versa Module Eurocard (VME) software and moving control software to each tower to reduce transport delays.

As shown in Figure 4-6, the EADGE-T communications design uses the TRCC to establish SHORAD radio configurations based on the contents of the Communication Plan. The TRCC uses control and management services provided by the Thales Radio Control Software (RCS) in each tower to define the communications mode and operating parameters for the voice and data radios (yellow arrow). The RCS software is hosted on an IP converter (SAS box) which communicates with both the voice and data radios using Thales proprietary serial protocols.

Once the TRCC has successfully established the connection with the data radio, the Site Connectivity Manager (SCM) creates a link process which allows the MSCT to exchange data with the RCS (green arrow). For voice communications, once the TRCC establishes the voice channel, the C2 audio system sets up the remote radio gateway (RGW) and appropriate operator buttons for secure or non-secure voice communications. Radio over IP communications from the radio are exchanged using ED-137B protocols.

In the SFU, radio connected Remote Situational Awareness Weapon Control Terminal (RSAWCT) rugged laptops receive and process the SDL protocol while (HF and VHF) voice radios support voice communications.

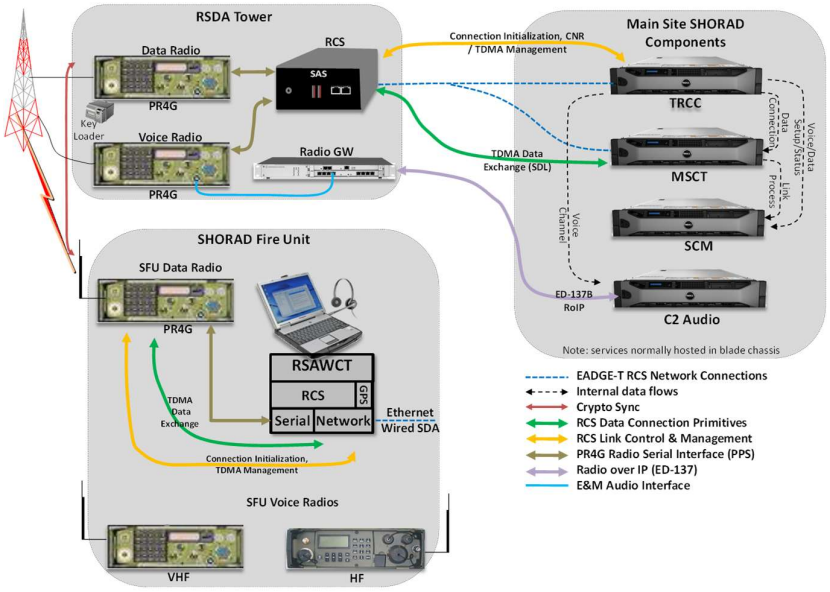


Figure 4-6: SHORAD Communications Design

The network equipment at each RSDA tower consists of the following as shown in Figure 4-7:

- **L99_PROVIDER_EDGE_SMALL:** Dual SRX550s PE-Routers connected via a Ring network
- **L99_100MBPS_IPSEC_ENCRYPTOR**: Dual rack mounted SRX550s
- **L99_FIREWALL_ROUTER_V2:** Dual rack mounted and located in a building near the tower

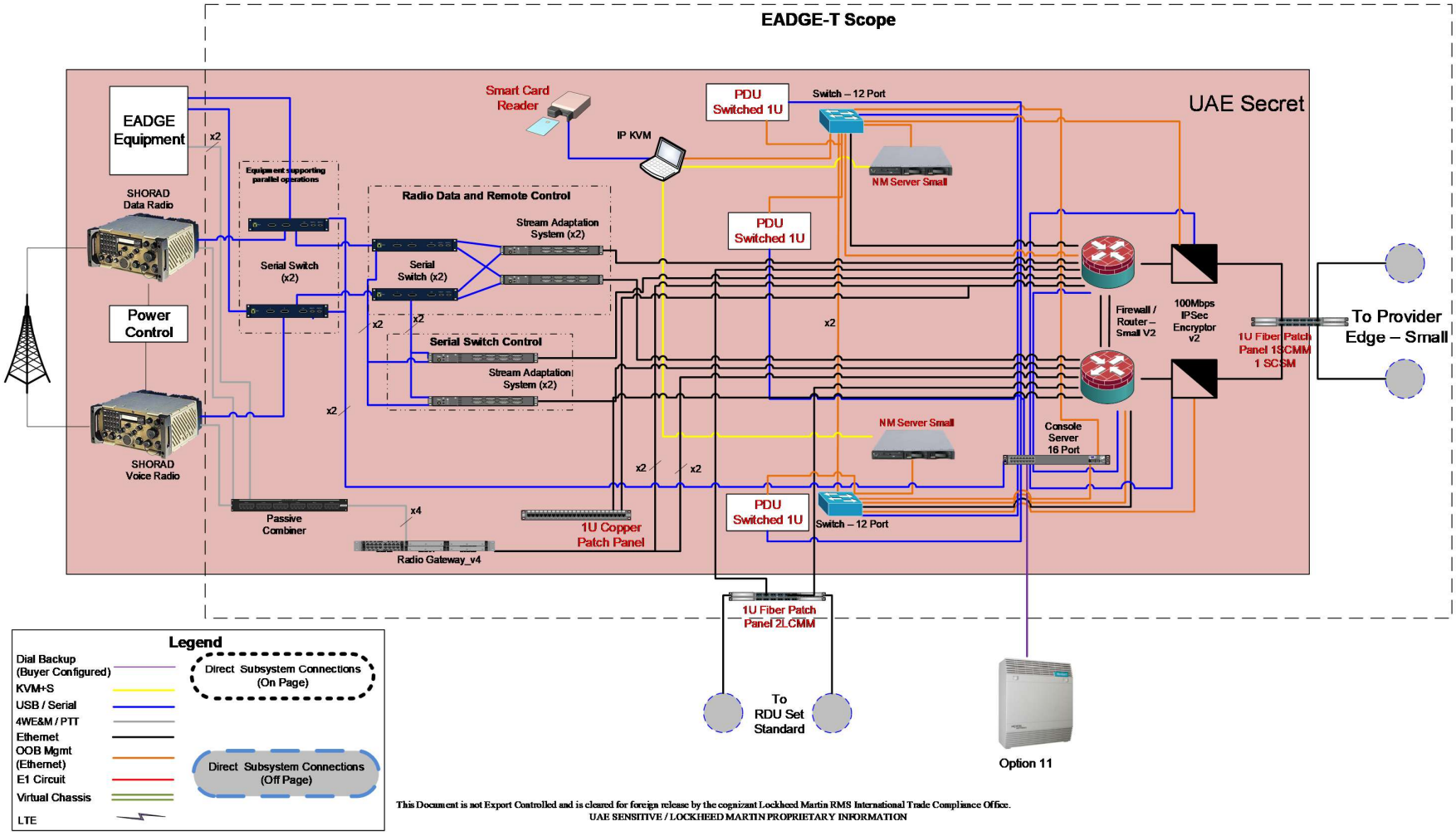


Figure 4-7: RSDA Tower Site LAN Design

4.3 Mobile/Deployed Sites

4.3.1 DAOC

The Deployable Operations Center uses the same functional elements as other sites but consists of separate shelters for communications and operations. A local high-speed fiber optic ring network connects the two communications and two operations shelters together. The communications shelters support UAE SECRET, NON-US COALITION and UNCLASSIFIED enclaves (as shown in Figure 4-8) and have been designed with identical sets of equipment to implement failover and improve survivability. The DAOC supports multiple transport networks to provide the flexibility to operate in different environments. The DAOC supports communications At-The-Halt using FOBB access, LTE broadband, IEEE 802.11n wireless, transportable SATCOM and Microwave. In addition, the DAOC includes a separate mobile enclosure, the Remote Radio Shelter, which houses Link-11, GATR, and SHORAD radios.

The DAOC has been designed to work in harsh environments and as such uses ruggedized equipment. The network devices used include rugged models of the Juniper MX and SRX routers and firewalls. The Juniper MX-104 (**L99_ROUTER_MX104**) routers support ADCN access as the PE-Router for the DAOC. Two different models for the DAOC Firewall/routers and encryptors have been specified to allow for maximum bandwidth (e.g. when connected via 10Gbps FOBB links) or ruggedized operation (over SATCOM). Thus, a combination of the Juniper SRX-5400 (**L99_10GBPS_IPSEC_ENCRYPTOR** / **L99_FIREWALL_ROUTER_LARGE**) and Juniper LN2600 (**L99_100MBPS_IPSEC_ENCRYPTOR_RUGGED** / **L99_RUGGED_ROUTER**).

As a command and control center, the DAOC supports voice and data functions either as part of a three-site single team or deployed single team configuration. Console positions located in the operations and communications shelters support command and control applications as well as access to Tactical Radio configuration and control functions to support management of available communications resources. Each communications shelter includes Link-11 (HF/VHF), GATR (UHF/VHF) and SHORAD/RSDA (VHF/HF) radios. A MIDS Link-16 terminal is supported when provided by the AFAD.

Detailed descriptions of the DAOC, MAOC and client kits are included in the System Hardware SDP (EADGET-SDP-C012.2).

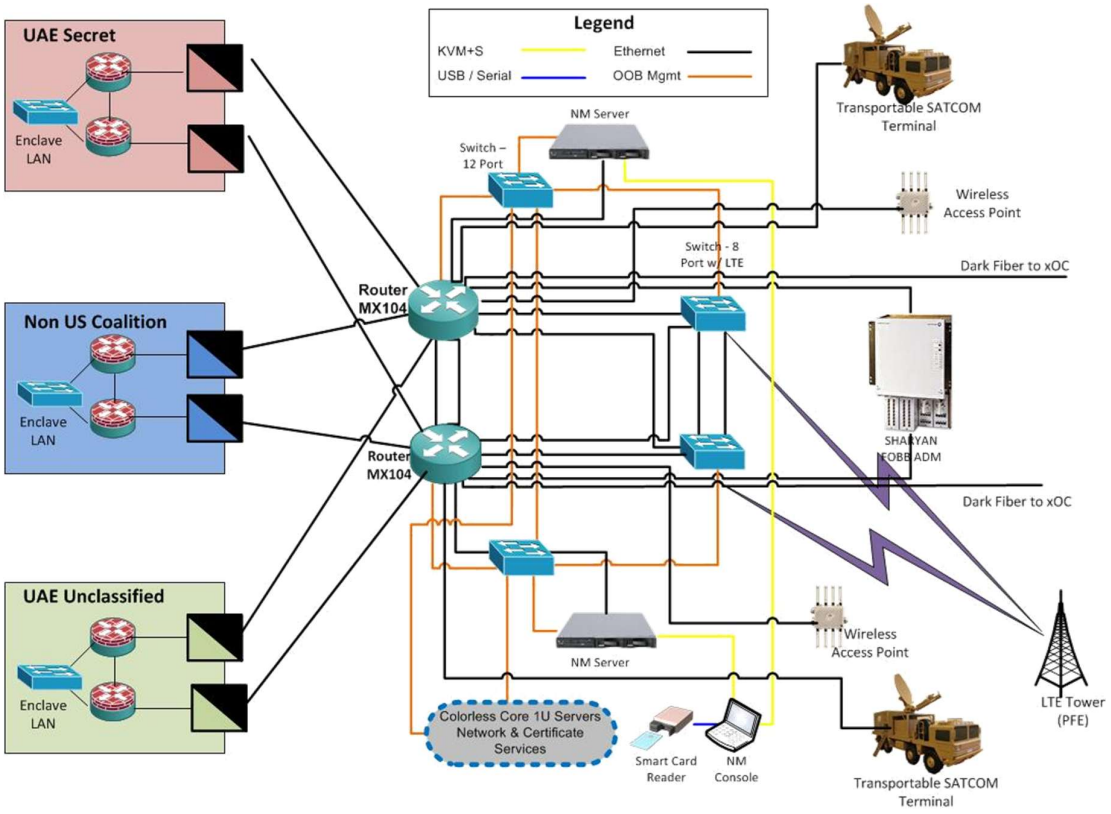


Figure 4-8: DAOC Communications Design

4.3.2 MAOC

The Mobile Air Operations Center is a flexible vehicle that supports communications On-The-Move or At-The-Halt. ADCN access is provided either through the FOBB when operating At-The-Halt or On-The-Move using SATCOM, IEEE 802.11n wireless (WiFi), or LTE broadband access. The MAOC includes rugged equipment to support operations in Secret, Non-US Coalition and Unclassified enclaves. It can operate independently, or with the DAOC as part of a three-site single team or deployed single team configuration as described in Enterprise Annex F (System Configuration and States).

The MAOC is a versatile platform that can be used by senior staff for battle management or to supplement operations. Like the DAOC, components used in the MAOC utilize ruggedized network that meet the SWAP restrictions of the MAOC. It includes an internal vehicle intercom system and supports HF, VHF and UHF voice radios. Figure 4-9 shows the colorless network components that provide access to the ADCN. The MAOC uses the same functional design as other deployed EADGE-T sites. Network components used in the MAOC include:

- **L99_ROUTER_RUGGED:** Whetstone LN1000 PE-Router
- **L99_100MBPS_IPSEC_ENCRYPTOR_RUGGED**: RTR8GE
- **L99_ROUTER_RUGGED**: Whetstone LN1000 Firewall/router

As shown in the SV-2 design artifact below, space constraints in the MAOC cause the elimination of some redundant components in the Non-US Coalition and UAE Unclassified enclaves. Please refer to the System Hardware SDP (EADGET-SDP-C012.2) for additional details.

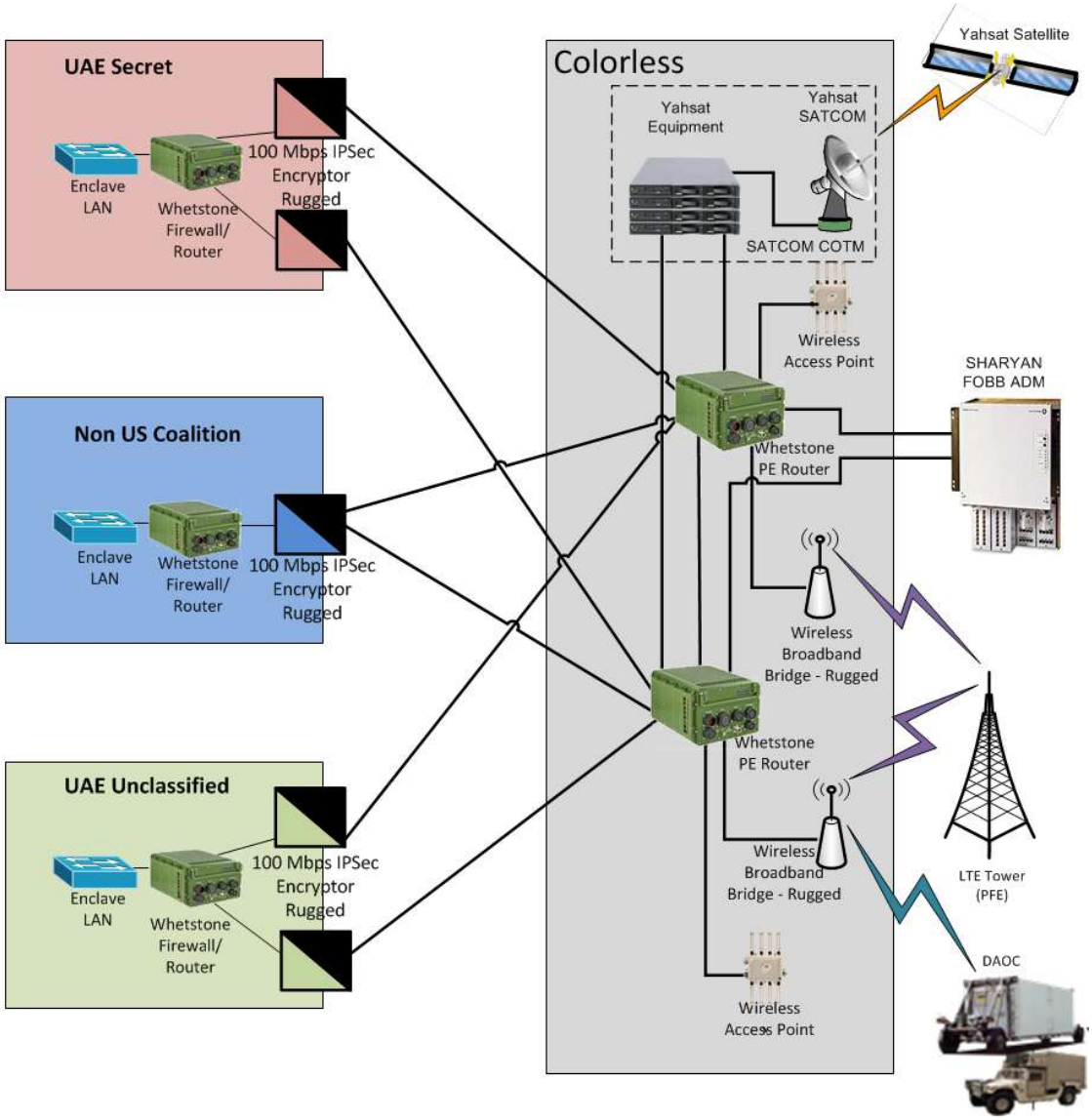


Figure 4-9: MAOC Communications Design

4.3.3 Client Kits

Client kits support the extension of M/DAOC capabilities by providing wired or wireless access for additional staff connected to the M/DAOC. As shown in Figure 4-10, each client kit includes three (3) Remote Data Unit (RDU) ruggedized notebook computers which allow access to classified RDU applications over IEEE 802.11n wireless, the FOBB or using direct fiber optic connections. Client kits can also be used for surge support and while the DAOC is in transit. Each RDU includes a VoIP audio client for voice communications. Client kits are discussed in the System Hardware SDP (EADGET-SDP-C012.2).

Rugged versions of the standard ADCN interface components including the PE-Router, encryptor and firewall/router utilize the GE RTR8GE which contains a Juniper LN1000 rugged router.

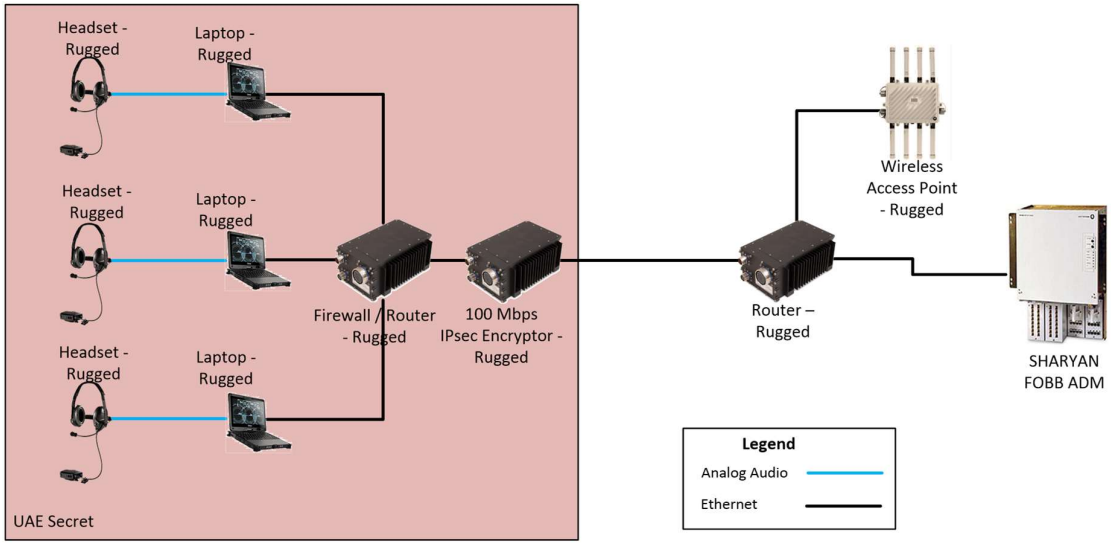


Figure 4-10: Client Kit Design

4.3.4 SHORAD Fire Units (SFU)

SFUs can be configured to communication over a direct wire connection or VHF to support engagement activities in a wired or radio SHORAD Deployment Area (WSDA/RSDA). (See section 4.2.6 above) SFUs are configured with ruggedized network equipment as shown to meet environmental, space and power requirements.

- **L99_ROUTER_RUGGED:** RTR8GE PE-Router
- **L99_100MBPS_IPSEC_ENCRYPTOR_RUGGED**: RTR8GE Encryptor
- **L99_ROUTER_RUGGED**: RTR8GE Firewall/router

RSDA communications use a TDMA cycle which nominally supports 10 SFUs per RSDA tower. Each tower site can support additional SFUs in wired mode using a 10 Mbps fiber interface between the RSDA sites' PE-Router. Both interfaces use the SHORAD Data Link (SDL) protocol as described in Annex L. For radio connected SFU's the RSDA tower includes a redundant pair of IP to serial converters running the Radio Control Software (RCS) to interface to the data and voice radios.

As shown in Figure 4-11, wire connected Pantsyr units support the UDL protocol using an IP to Serial converter which converts encapsulated UDL messages into serial commands sent to the EADGE Pantsyr KBP central computer. As the Pantsyr S1 combat vehicle does not provide direct access to a RS-232 serial interface a Frequency Shift Keying (FSK) modem will be incorporated into the design. Connectivity between EADGE-T and each wired SFU uses a fiber optic cable with attaches to the nearest WRSDA or Provider Edge site. A network switch located at the WRSDA or Provider Edge site uses DHCP (Dynamic Host Configuration Protocols) to support the connection of an SFU to the EADGE-T network.

Once wireless broadband LTE coverage becomes available, additional bandwidth will allow an increase in the number of SFUs as well as the ability to support the roaming of SFUs between towers, which is not supported in the EADGE system due to limitations in the PR4G VHF radios.

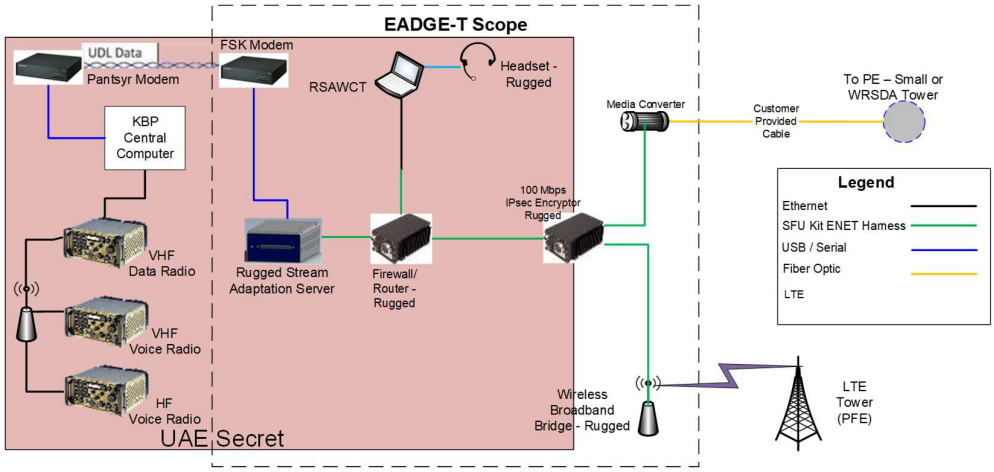


Figure 4-11: SFU Communications Design

4.3.5 *HAWK Voice and Data Architecture*

Provider Edge routers for HAWK missile sites are located in a facility at the site near the Al Sharyan (FOBB) interface rack. A portion of the SV-2 showing the ADCN interface network components is provided in Figure 4-12 below and voice and data architecture components are detailed in this section. The Provider Edge Router (PE-Router) connects to one or more HAWK command posts (CP) via fiber connections allowing command posts to be relocated and tied to the PE-Router at a different location. As the HAWK CP computer does not provide direct access to a RS-232 serial interface a Frequency Shift Keying (FSK) modem will be incorporated into the design. The HAWK secret enclave is located in or near the command post and consists of a half rack containing encryptors and firewall/routers. The secret enclave includes the standard network monitoring equipment, an RDU and a serial to IP converter which interfaces to the HAWK processor using UDL. HAWK command post key network components include:

- **L99_PROVIDER_EDGE_SMALL**: Dual SRX550s PE-Routers connected via a Ring network
- **L99_100MBPS_IPSEC_ENCRYPTOR_V2:** Dual encryptors in a half rack in HAWK Control Post
- **L99_FIREWALL_ROUTER_V2**: Dual firewalls located in a half rack in HAWK Control Post

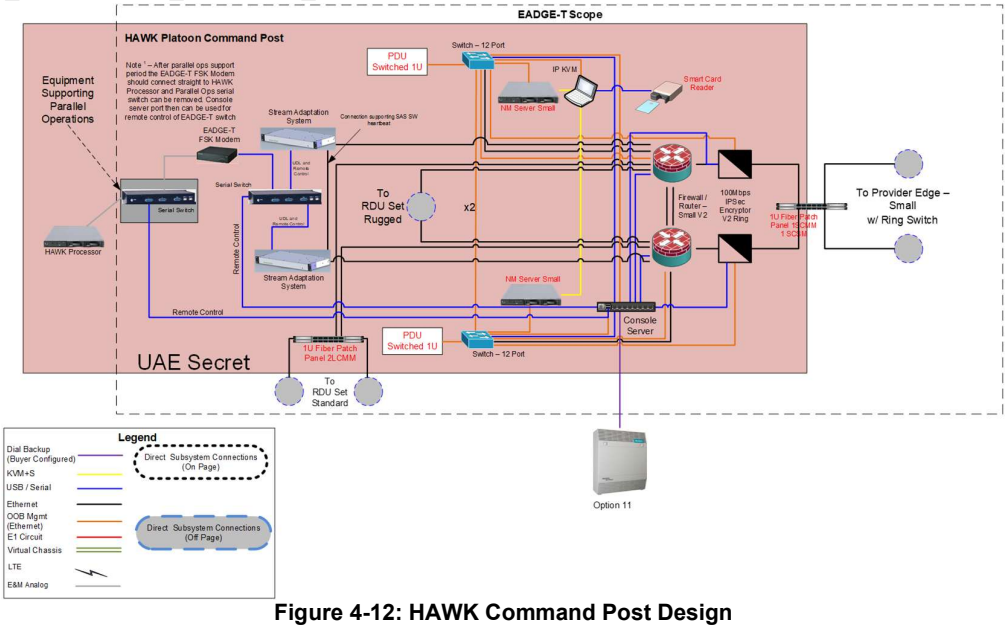


Figure 4-12: HAWK Command Post Design

In addition to the data connection to the existing HAWK processor, rugged and standard RDU terminals are provided. Both RDUs provide access to voice communications using a VoIP audio client. In addition, the standard secret RDU set provided includes an IP telephone.

5 COMMUNICATION PLANNING

5.1 Voice and Data Communication Planning

Voice and Data Communication Planning is performed as part of Air Tasking Order (ATO) planning. Voice communications are planned to support GATR, SHORAD, Link-16 radios. Data communications are planned to support GATR, SHORAD, Link-11 and Link-16 radios. In addition, manual configuration of other voice radios are supported via Command Line Interfaces (CLI).

5.2 Communication Planning Approach & Tools

Communication Planning is performed using a suite of tools. These tools include the Network Planner (NP) Client together with the GATR and SHORAD Planning software for Radio Frequency Communication Planning. Common Services and Network Management subsystems are used to store the COMPLAN and configure/status the radios. The GATR and SHORAD Planning software is used for initial loading and planning of frequencies, presets and keys. The Common Services subsystem contains the Order of Battle (ORBAT) data, which specifies the site definitions (e.g., GATR Main Site), and is available to the Network Planner Client via a web service interface. The web service interface uses XML for input/output, thus allowing maximum portability and configurability, which easily allows AFAD engineering staff to extend the NP and map display with new capabilities as the AFAD mission continues to grow. The ORBAT data also contains the Radio and Antenna definitions. The Unit Type Configurations are associated with the ORBAT data. These Unit Type Configurations are the specific configurations for radios and antenna (e.g., all of the specific attributes of the radios and antenna, such as gain and power, etc.).

The Operator performs data entry upon system installation via the CAOC AOADP, which uses Common Services to store the data. This activity includes entering the ORBAT data and the Unit Type Configuration data for all of the radios and antennas. Once the system is in use, an ATO will be stored in the Common Services subsystem as (Airspace Battle Plans) ASBPs. ATOs further divide into Missions, which are tasks assigned to specific organizations. As each organization works on creating the Missions in the ATO, they use the Network Planner Client to open the ATO, perform coverage analysis and define the RF networks needed to support the Mission. This collection of RF networks is collectively referred to as the COMPLAN and is stored using the Common Services subsystem.

The definition of the ATO and its associated RF networks is an iterative process that each organization completes until all of the Missions that need RF networks have been defined. ATO/Mission annotations can be used to indicate that Mission RF network planning is complete in the Network Planner Client. The Common Services subsystem uses these indications to ensure that an ATO is not published until it has been validated in the Network Planner Client.

After the ATO publishes, an event is generated in the Common Services subsystem that the TRCC uses to open the Communication Plan contained in the ATO as shown in Figure 5-1. During execution of the Communication Plan, the radios are configured to support the specified RF networks contained in the Communication Plan. The display will show the list of both executing and published ATOs. For the selected ATO the list of missions and associated RF networks will be displayed. After an ATO has been published, radio configuration will start automatically at the designated times.

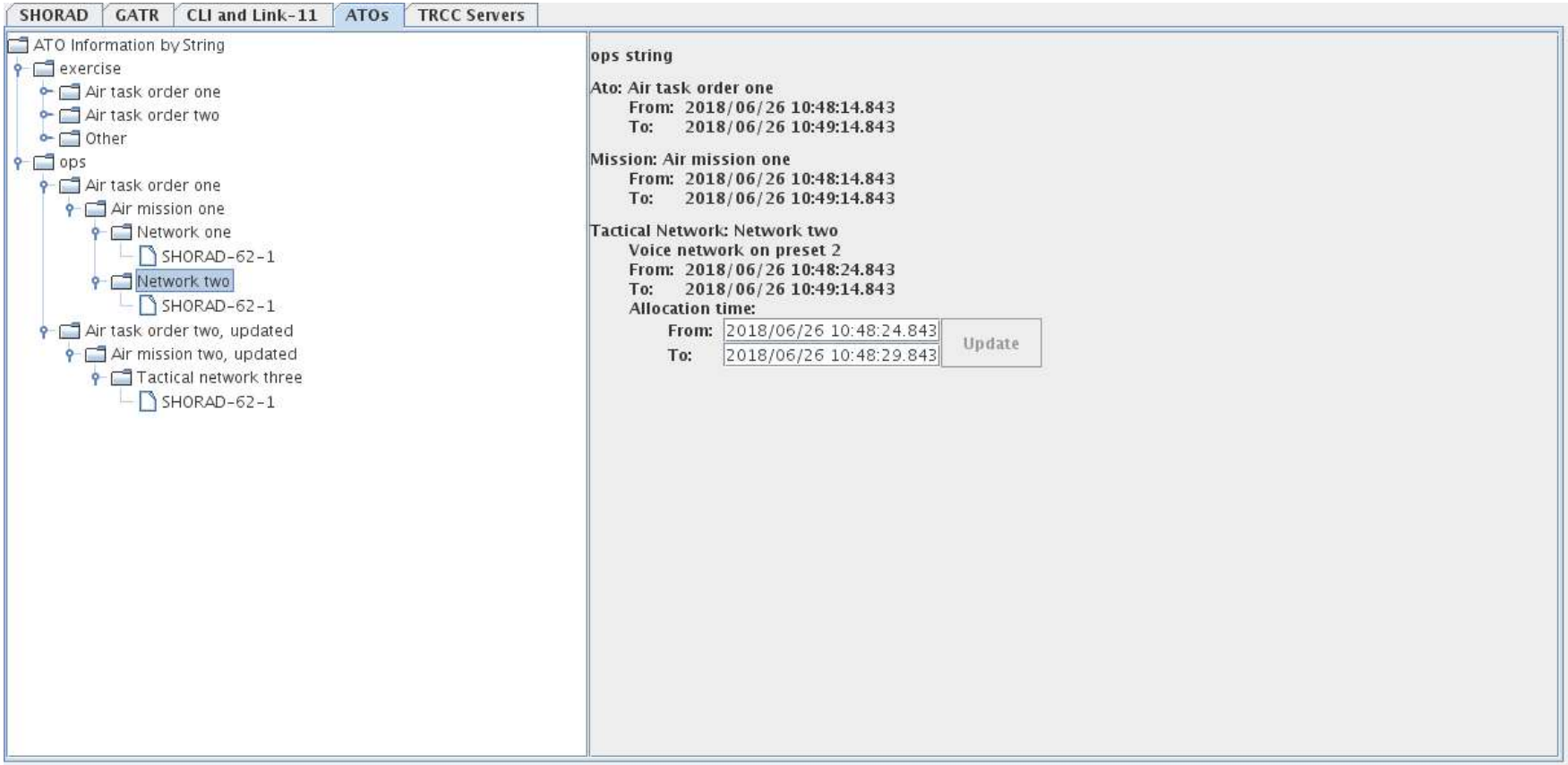


Figure 5-1: TRCC Client ATO Display

6 COMMUNICATIONS MANAGEMENT

6.1 Management and Configuration Approach

Communication Management provides an interface which supports the ability to monitor and alert operating and technical personnel so that system faults can be identified, diagnosed and resolved. The design of communication management capabilities for EADGE-T are driven by three key objectives:

1. Provide a secure, highly available communications management capability for EADGE-T that allows for the isolation and resolution of failures
2. Make use of standard management interfaces to support the deployed EADGE-T communications infrastructure as well as providing the ability to integrate new technologies and products in the future
3. Leverage available commercial management products to support unique vendor products

While commercial network management products are focused on supporting specific technologies and products, they lack the ability to support a military enterprise comprised of a range of communications components including wired and wireless networks, IP-based network technologies, security components, client and server computer systems, and tactical voice and data radio networks. Rather than relying solely on off the shelf commercial management products, EADGE-T management capabilities are based on a programmable framework provided by WebNMS which not only supports the diverse set of equipment required to support and maintain EADGE-T today but also provide the ability to introduce new functions in the future. While the customizable capabilities provided by WebNMS provides the flexibility to meet most EADGE-T management needs, the management solution provided also integrates specialized commercial management products such as VCenter, and JunOS Space, where they offer unique, vendor specific, capabilities.

6.1.1 Standards-Based Approach

The implementation of Network Management capabilities leverages standards for two primary reasons. First by supporting well defined, industry standard interfaces and protocols, management capabilities can be readily supported for the broadest range of communications devices available now and support the integration of new devices in the future. This involves adopting standards including the Simple Network Management Protocol (Versions 1,2 and 3) and PING. Adoption of these protocols ensures support for a wide range of COTS communications products.

Second, international standards such as the International Telecommunications Union – Telecommunications standardization sector (ITU-T) M.3010 and M-3400 provide high level guidance regarding the structure (element and management layers) and functions included in management capabilities (specifically Fault, Configuration, Asset, Performance and Security - FCAPS). Detailed descriptions of these standards and how they are used in the EADGE-T management solution are provided in the Subsystem Network Management System Design Package (C012.4.2).

6.1.2 Management Architecture

The EADGE-T management solution is a layered solution supporting the network management, element management and element layers in the Telecommunications Management Network (TMN) architecture (M.3010) as shown in Table 6-1:

Table 6-1: TMN Layers

LAYER	DESCRIPTION
Network Management Layer (NML)	The Network Management Layer (NML) offers a holistic view of the network and provides integration with the Element Manager (EM) software tools that allow an operator to control and monitor the EADGE-T network.
Element Management Layer (EML)	The Element Management Layer (EML) contains element managers (EM) which provide management functions (control and monitoring) for one or more of a specific type of network elements (such as routers, switches, computers, etc.).

LAYER	DESCRIPTION
	These software packages are geared towards a certain type of vendor or function and their user interfaces can be thick or thin clients (web-based). EMs in this layer interface northbound with the NMSs in the NML and southbound with devices in the Network Element Layer (NEL).
Network Element Layer (NEL)	The Network Element Layer (NEL) defines the interfaces for the network elements. For EADGE-T, network elements include network devices (e.g. routers, switches), security devices (e.g. firewalls, cryptographic equipment), computing devices (e.g. workstations, servers) and tactical radios.

In the EADGE-T management solution, FCAPS is the methodology used to implement the TMN architecture for network management. The FCAPS model is made up of five functional areas as shown in Table 6-2. Portions of each of the FCAPS functions will be performed at the different layers of the TMN architecture (Figure 6-1).

Table 6-2: FCAPS Functional Areas

FUNCTION	DESCRIPTION
Fault Management	Fault Management consists of monitoring the components in the network, detecting and logging faults, and notifying users by generating alarms in support of network recovery.
Configuration Management	Configuration Management consists of monitoring the network and system configuration information including tracking network changes, additions and deletions.
Asset Management	Asset Management consists of assets tracking, version management, inventory management and software upgrades management. *Asset Management replaces Accounting in the FCAPS model.
Performance Management	Performance Management measures and makes available various aspects of network performance for network performance monitoring and optimization. Examples of the statistics gathered include: system errors, utilization, and response time, which are used to identify system trends and plan for future use.
Security Management	Security Management provides controlled access to network resources as established by organizational security guidelines. For example, controlling access to log into a router.

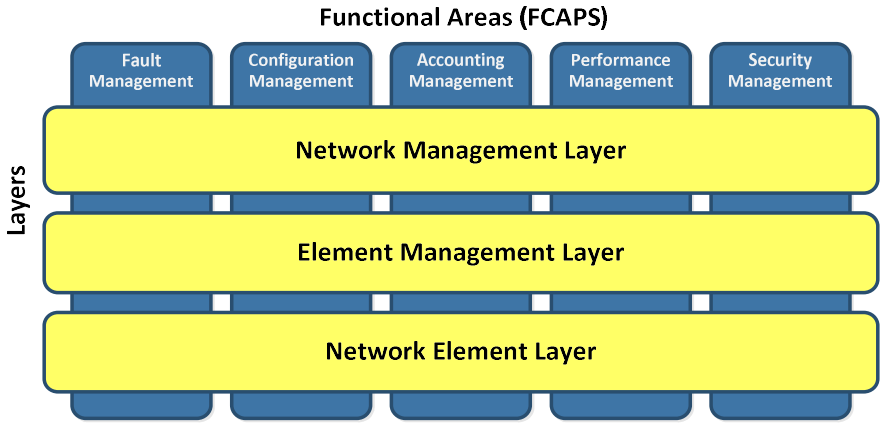


Figure 6-1: FCAPS Functional Areas vs TMN Layers

EADGE-T management capabilities support monitoring and alerting functions for supported security domains by aggregating reports from remote enclaves. Through a tiered hierarchy of management

resources, local, remote and centralized awareness of equipment faults and status is presented in a manner that allows rapid identification and diagnosis of equipment failures.

At the local level, management servers within each enclave collect, process and report metrics, including log files and faults from network and IT devices to support local problem resolution using a shared instance of the WebNMS EADGE-T management application. The local EADGE-T management servers actively collect status and management information for the deployed equipment, interface to element management applications where supported (such as Juniper Networks Junos Space application) and provide controlled access to allow troubleshooting and configuration.

Fault information collected by the management servers in each enclave are forwarded to network management consoles located at the AOC and AAOC to provide technicians with a system level view of all the enclaves within each security domain. Technicians at the network management consoles can then access the remote servers using the web-based network management application to examine detailed status information and support remote troubleshooting activities. Unlike commercial network management products which collect and send management metrics over the wide area network, the EADGE-T network management architecture performs remote data collection and only sends relevant fault information over the wide area network to reduce impacts on the ADCN. The status of equipment located in each security domain is routed through secure gateways (one-way diodes) to provide an enterprise wide management view of the EADGE-T status.

6.1.3 Out-of-Band Management

Remote management capabilities which ensure the health of the EADGE-T communications infrastructure expose sensitive interfaces which are essential in maintaining and supporting the system. While these interfaces support the ability to diagnose and resolve failures, they also represent a potential vulnerability if accessed by unqualified personnel or penetrated by an attacker. The design of the EADGE-T network infrastructure leverages security concepts specified in the US DoD Information System Agency (DISA) Network Infrastructure Security Technical Information Guide (STIG) which recommends the use of a separate network infrastructure dedicated to support the remote configuration and monitoring of connected communication devices. This network, referred to as an out-of-band (OOB) network (to differentiate it from the in-band operational network), is protected by additional security policies to prevent unauthorized accesses. Where deployed communications equipment provides dedicated management interfaces, the OOB network provides a means to isolate maintenance activities from the mission critical traffic on the (in-band) operations network in each enclave. Established security policies and access controls not only restrict access to authorized users, but also limit management protocols to the OOB network.

Within EADGE-T, an OOB network is provided within each enclave at remote sites. Management information as well as security logs are transported from remote sites to the AOCs using separate encrypted (IPSec) tunnels but information is transported over the ADCN rather than over dedicated out of band network links.

6.2 Network Configuration & Tools

The NM subsystem provides several mechanisms for an authorized technician to control and configure the various network elements (network devices, security devices and computing devices) in the EADGE-T system. Each enclave at a site provides local management capabilities via the IP KVM switches for computing devices and via console servers for network, security devices and other serial accessible devices. Element Managers resident on the network elements are accessible after logging into a computing device via the IP KVM. SSH is also available on network elements and computing devices after logging into a computing device via the IP KVM. For remote sites, these capabilities allow a local technician to troubleshoot and repair problems at the remote sites. If network connectivity exists between the AOCs and the remote sites, these same approaches are available for technicians in the AOCs to be able to remotely diagnose and repair faults in the remote sites 24x7. Table 6-3 identifies the primary mechanisms provided for controlling and configuring network elements.

Table 6-3: Management Approaches

APPROACH	LOCATION	DESCRIPTION
Element Manager	AOC AAOC DAOC MAOC Remote Sites	Element Managers are vendor specific device management applications, often residing on the network element itself, that are used for the configuration and control of the network element. The technician, using the NMS displays, navigates to a device (e.g. by visiting the device on the Alarm, Device or Topology Display) and opens the Element Manager for that particular device. NMS launches the Element Manager and the technician performs control and configuration operations.
SSH/Command Line Interface	AOC AAOC DAOC MAOC Remote Sites	SSH is an application and a protocol that provides a secure connection to a device using standard cryptographic mechanisms. The technician, using the NMS displays, navigates to a device and opens an SSH session to the device (for devices that support SSH). NMS launches a terminal window with an open SSH session. After technician login (if required), the technician can use Command Line Interface (CLI) commands to control and configure the device.
Console Server	AOC AAOC DAOC Remote Sites	Console servers are devices which, via serial ports, have secure access to the physical console port (RS-232) of the network elements connected to it. They are ideal for out of band access to network and security devices (routers, switches, firewalls, encryptors) and other local or remote critical network devices. The technician, using the NMS displays, navigates to the Console Server device (e.g. at a remote site) and opens the Console Management Console for that Console Server. The Console Management Console runs in a browser and provides a view of the Console Server Management Switch, Console Server product and all the connected equipment. Authorized technicians can use the Management Console to access and control configured devices, review port logs, use the built-in Web terminal to access serially attached consoles and control power to the connected devices. The technician can select a device connected to the Console Server and connect to that device, thereby receiving a console window to the device in which to enter commands. Alternatively, the technician, once the Console Server is selected in NMS, can open an SSH session to the Console Server. In the SSH session window, the technician can enter the port of the device to connect to. The technician would be presented with the console window to the device in which to enter commands. For fixed sites, including remote sites, the technician can use dial-up to gain access to the console server at that site, which has a built-in modem, and its capabilities. This provides another method for the technician to configure and control devices at fixed sites.
IP KVM	AOC AAOC DAOC Remote Sites	IP KVM (KVM over IP) refers to technology that allows you to connect to a CPU or KVM switch via its keyboard, monitor and mouse port using an IP connection. In EADGE-T, each IP KVM is a KVM Switch deployed at various sites that provides secure access to up to eight directly connected computing devices from within the EADGE-T network, as long as there is a network connection, using only one keyboard, monitor and mouse. Since it does not require additional software packages be loaded on the target machine (the server you are contacting via IP), IP KVM can be used for BIOS level access to the computing devices. The technician, using the NMS displays, navigates to the KVM Switch device (e.g. at a remote site) and opens the Web Based Element Manager for that KVM Switch. From the Web based Element Manager, the technician launches the Trip Lite Java Applet. From the applet, the technician can select the computing device connected to the KVM Switch they wish to access. That computer's screen will be displayed to the technician. Alternatively, the technician, from a Command Line of a Linux workstation, can run the Java Client. Once started, the main screen of the client presents the Model Name and IP Address of discovered KVM Switches in a Server List. The technician highlights the desired KVM and logs in. Once logged into the KVM Switch, the technician can select the computer connected to the KVM Switch they wish to access. That computer's screen will be displayed to the technician.

6.3 Voice/Data Communications Management

Communications Management for Voice/Data is performed by TRCC. This is done either automatically when triggered by the approved publication of an ATO or manually via the TRCC Client. Additionally,

there is a control interface exposed to support management of radios to handle real-time changes to missions. Section 3.4 describes these interfaces in detail.

Communications Management for Voice/Data is performed by a combination of TRCC, VCS, Telephony and C2 Audio administrative interfaces. TRCC handles the RF voice and data communication configuration.

Section 3.2 describes these interfaces in detail.

7 SCENARIOS

7.1 Summary

The following sections describe how Communication Plans are developed and executed, how radios are configured to support Communication Plans, and how Communication Management is performed. This involves exploring several scenarios relevant to how planning is done, missions are activated, pre-sets and keys are generated, link tests are performed, mission strings are monitored, and radio failure is handled.

7.2 Planning Scenario

The following describes the process by which the UAE Air Force and Air Defense Headquarters elaborates and disseminates the Air Force Directives for all flying units and Ground Air Defense units. The process starts with the initial creation of an ATO using the EADGE-T CAOC Planning Software. Then units will use their Remote Data Unit (RDU) terminals to enter Missions through the CAOC AOADP, as shown in Figure 7-1.

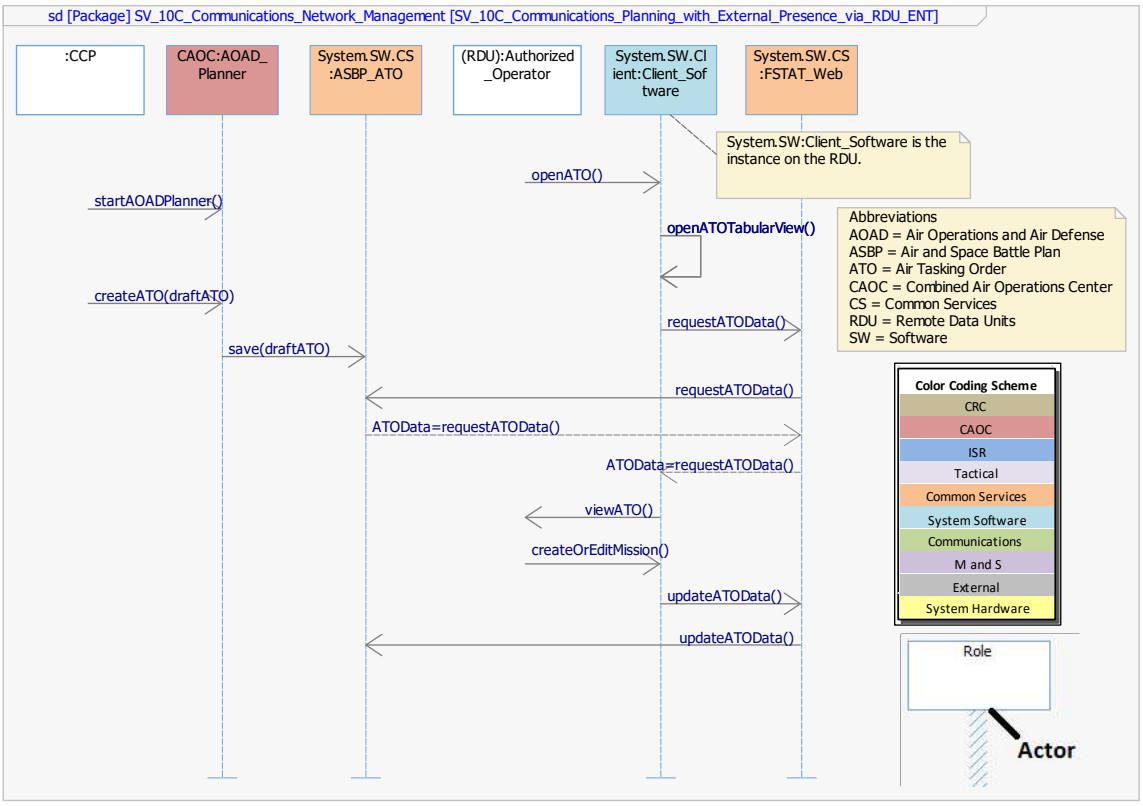


Figure 7-1: Planning with External Presence via RDU

Next the AOC Planners will elaborate and release the “Weekly Flying Schedule” (WFS). This elaboration will be done using the Network Planning Software to plan resource needed to support the mission, which includes the allocations of radios and pre-sets to missions, as shown in Figure 7-2 and Figure 7-3.

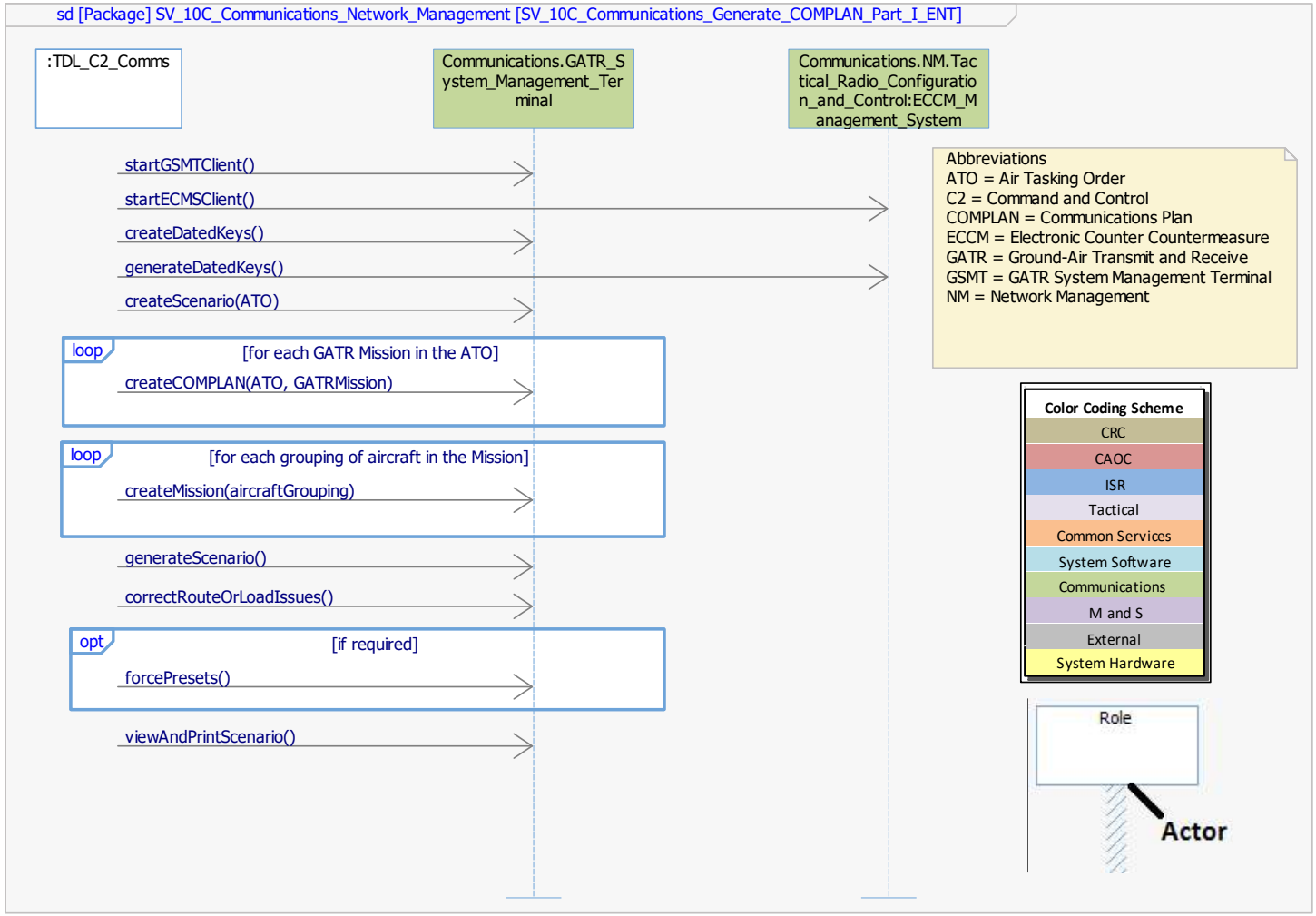


Figure 7-2: Generating COMPLAN Part I

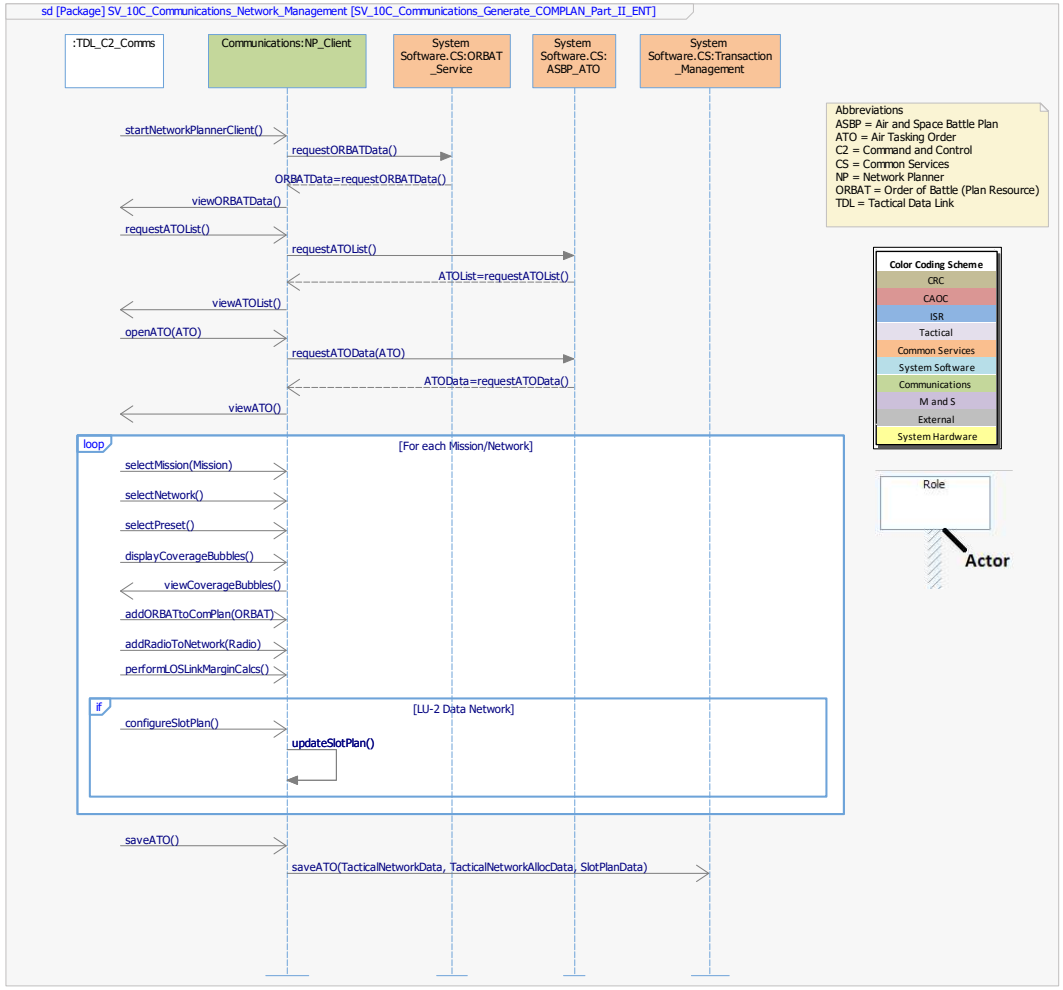


Figure 7-3: Generating COMPLAN Part II

The units can then review the mission before approval by the AOC Director and AOC Commander. At this point any changes to resource allocations needed to support operational, exercise, or non-us coalition missions would be done by allocating the radio planned resource to the appropriate EADGE-T String using Resource Allocation, as shown in Figure 7-3.

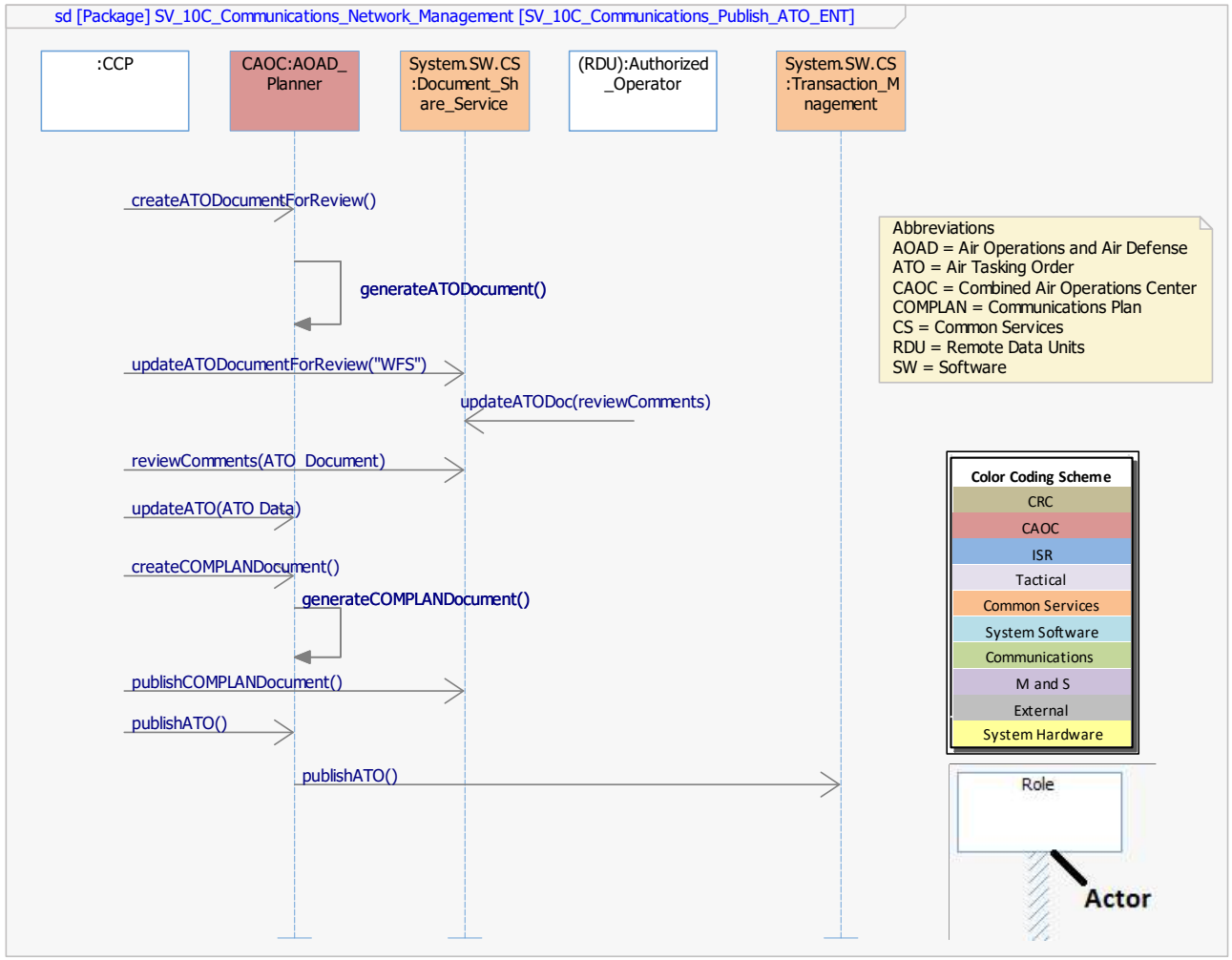


Figure 7-4: Publish ATO

Finally, the CAOC AOADP is used to publish the ATO, which in turn triggers TRCC to load an ATO for execution. Once TRCC starts executing the ATO, radios will be automatically configured to support missions. For voice networks, the desription (button labels) of the voice circuit will be configured on the CRC Operators touch panels. For data networks, SCM will configure the Data Link Interface with MSCT. Status updates for the radios are performed throughout the process and stored in Common Services to be available to all EADGE-T Sub-systems, as shown in Figure 7-5.

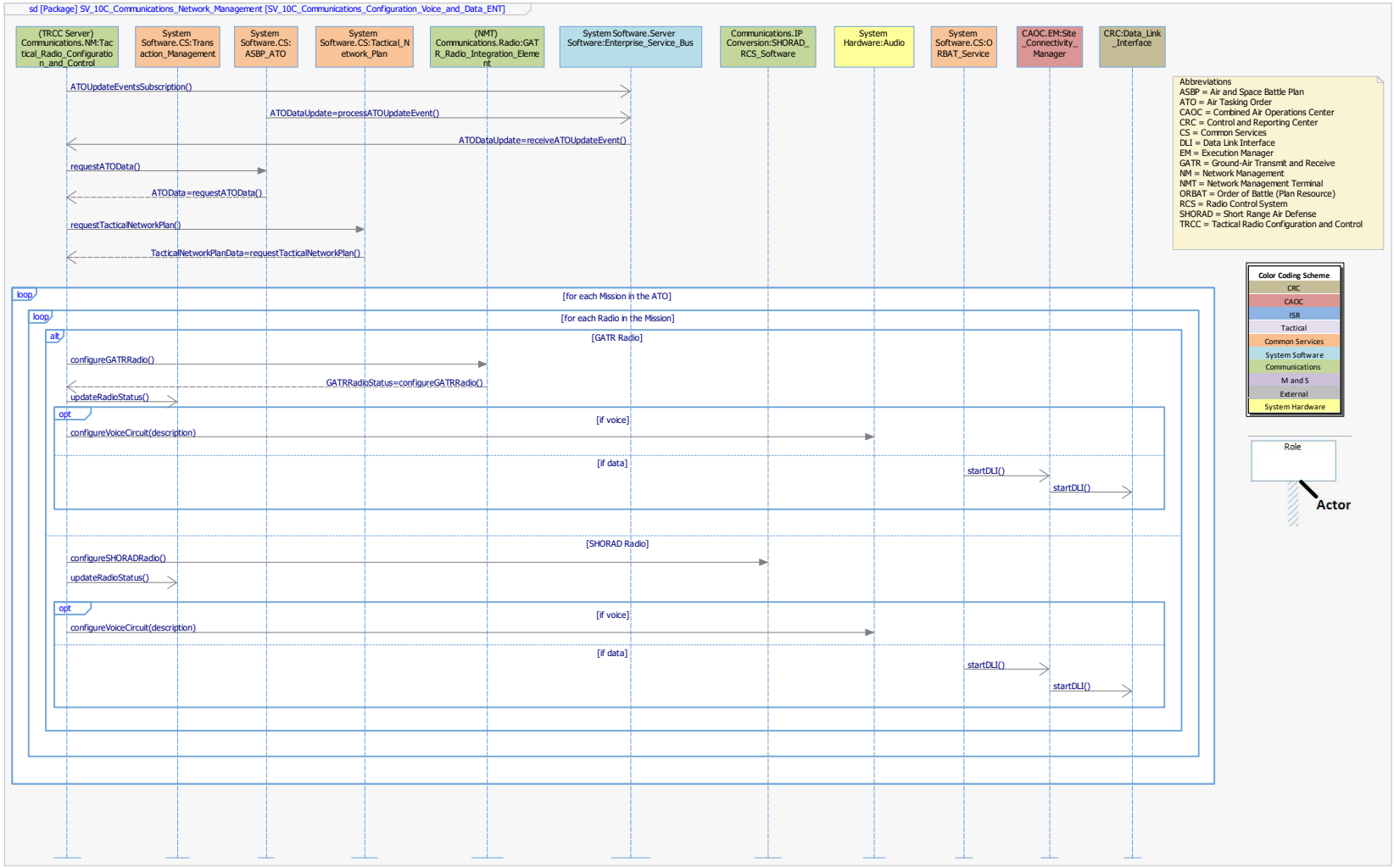


Figure 7-5: Configure Voice and Data

7.3 Configuration Scenario

7.3.1 Mission Activation

As part of ATO Execution the TRCC will configure GATR and SHORAD radios associated with each of the ATO Missions or Defense Activities. Missions and Defense Activities will contain a Planned Resource (e.g. Aircraft or SDA Tower), which will have an assigned list of Tactical Networks. Each Tactical Network will contain a list of radios that will be needed to support the mission. The TRCC will extract the configuration information for the radios from the Tactical Network Design and at Mission Start will configure the radios. Configuration differs based on the radio unit type and the type of network (e.g. data or voice). Whether it was a success or failure, the status for the radio is updated in Common Services. This status update generates a Java Messaging Service (JMS) event that SCM receives automatically. If the status indicates success and the network type is data, SCM will then use SSH to start the appropriate process on the MSCT VM for the radio.

If configuration successful and the network type is voice an Application Program Interface (API) call is made to C2 Audio system to indicate the voice circuit associated with the radio is now active.

7.3.2 Preset/Key Distribution

Keys for the GATR system are pushed daily to the GATR sites with the ECCM Management System (ECMS). Keys are generated using the GATR System Management Terminal (GSMT)/ECMS and are dated and changed each day. For SHORAD, keys are generated by using the SHORAD Frequency and Key Loading Unit (FKLU)/Frequency and Key Management Unit (FKMU) software. Since SHORAD keys are distributed via fill gun loads the keys are not changed daily. They are only changed when coordinated fill gun loads can be deployed to the SDA towers and SFUs.

Presets are generated only when a change to the allowed frequencies is made. If a change does occur, then the presets are generated via the GSMT/ ECMS or the SHORAD FKLU/FKMU software. Then the new set of presets are entered into Common Services via the CAOC AOADP as a new Radio Unit Configuration. See Figure 7-6 for details.

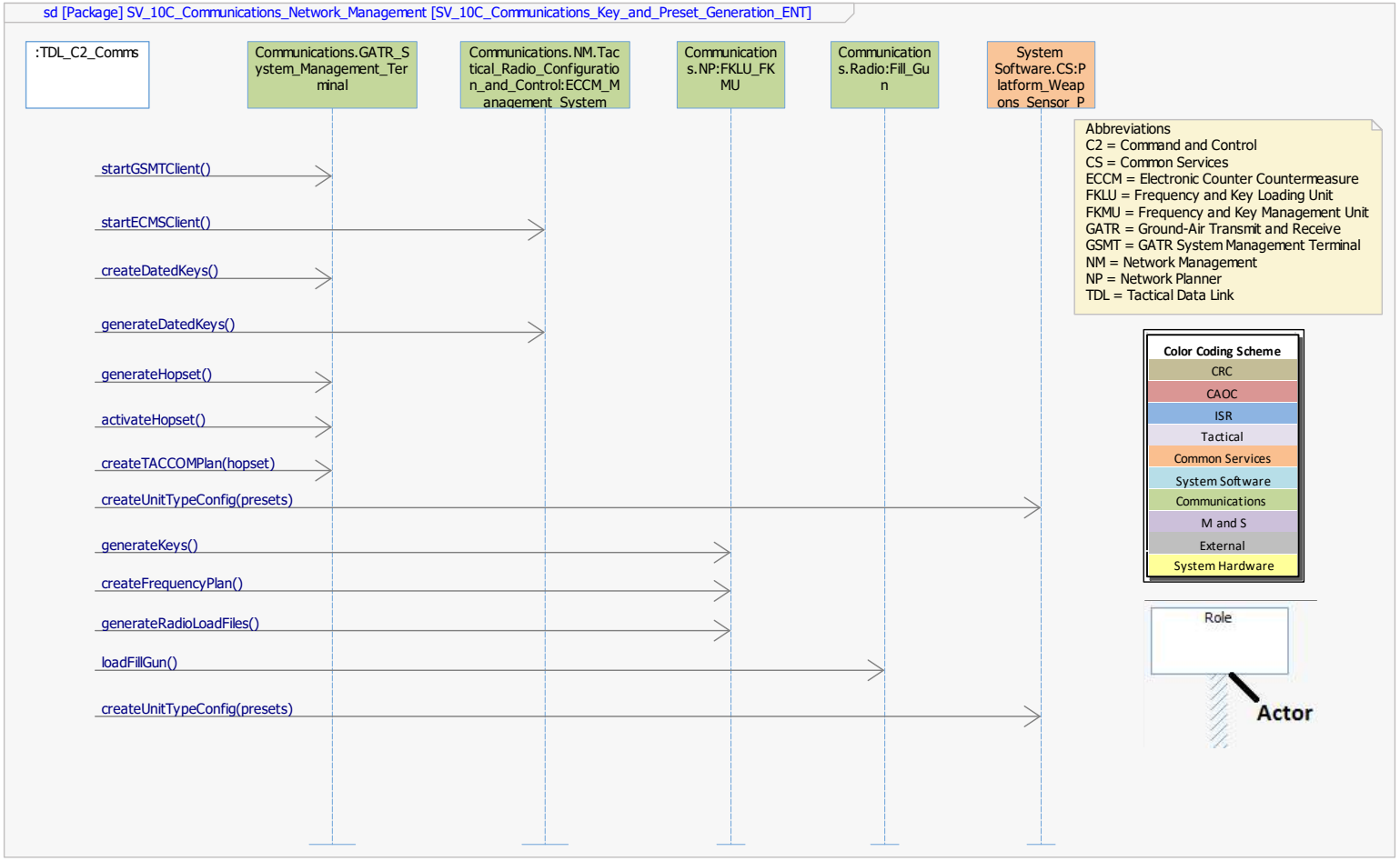


Figure 7-6: Key and Pre-set Generation

7.3.3 SFU Link Test

A link test would be initiated by the SHORAD Firing Unit (SFU) Tactical System Display (TSD) in the case were the Remote Site Weapons Controller is in voice contact with the AOC but has lost the SDL data link. In this case the AOC would request that a Link Test be performed using the TSD. A Link Test would send a message from the SFU data link radio to the SDA tower radio. If the link test is successfully received an Alert will be generated by the TRCC to indicate a link test was performed along with the status of the test. The link test status will also be displayed in the TRCC Client. See Figure 7-7 for detailed sequence.

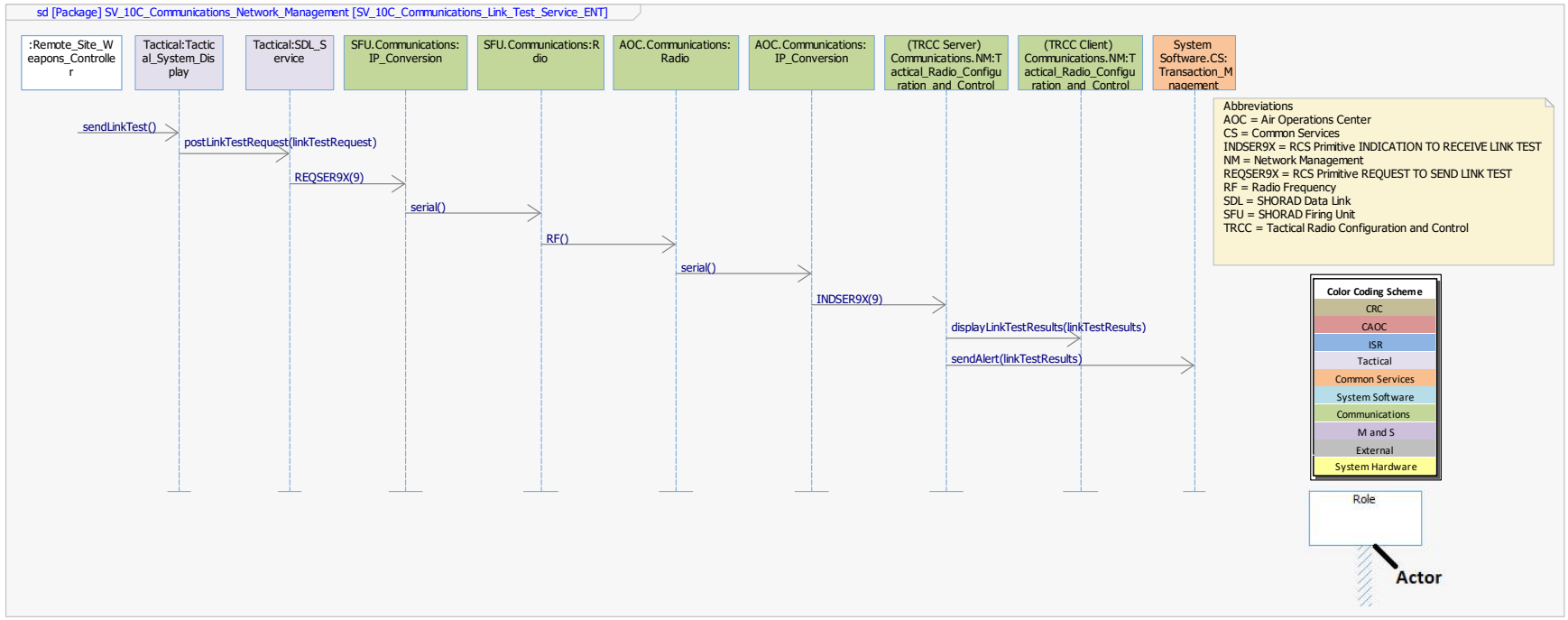


Figure 7-7: Link Test

Performing a link test is a task that can be performed for any SFU in the field to ensure there are not issues with the data link radio prior to using it to support a mission, which would also cover an initial deployment. For more information see the ICD SHORAD rev-I Sections for the REQSER9X, REPSER9X and INDSER9X messages, as well as, the Link Test service.

7.4 Communication Management Scenario

7.4.1 Mission/String Monitoring & Status

Network Management provides a holistic view of IT and Communication resources in the EADGE-T enterprise by proactively monitoring and presenting to the operator key health and performance data as well as alarms for computing, security, network and radio devices. The information presented is device specific and includes critical and non-critical metrics, such as CPU utilization, memory utilization, disk usage, interface status, dropped packets, tunnel status, temperature and fan status, and availability. In the event a fault is detected, Network Management issues a System Alert indicating the nature of the fault. The operator, based on the information provided in the Alert, can then begin troubleshooting the fault if necessary (e.g. redundant hardware or software may have a backup and require no intervention). See Figure 7-8, Figure 7-9, Figure 7-10 for detailed sequences.

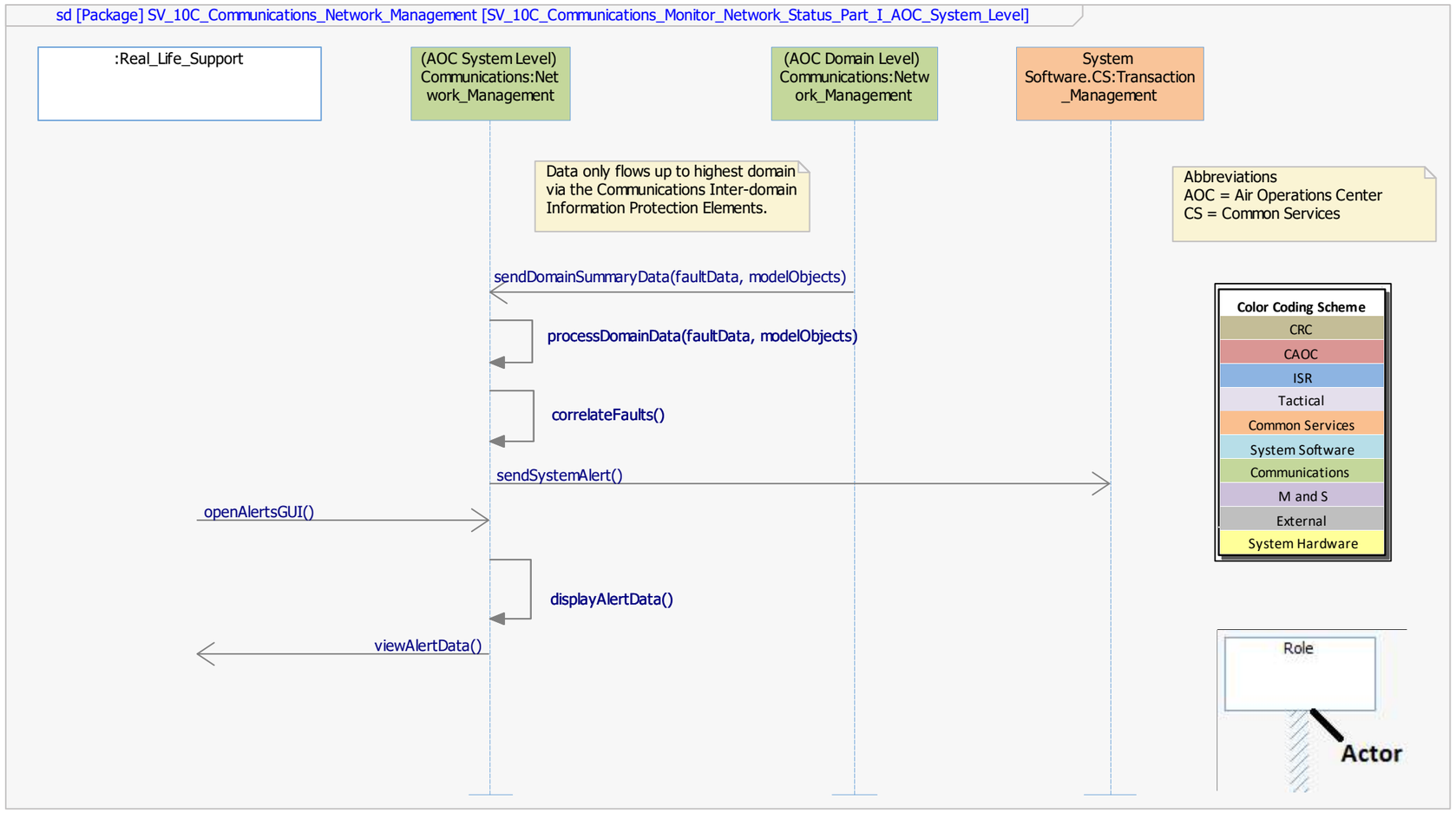


Figure 7-8: Mission/String Monitoring & Status Part I

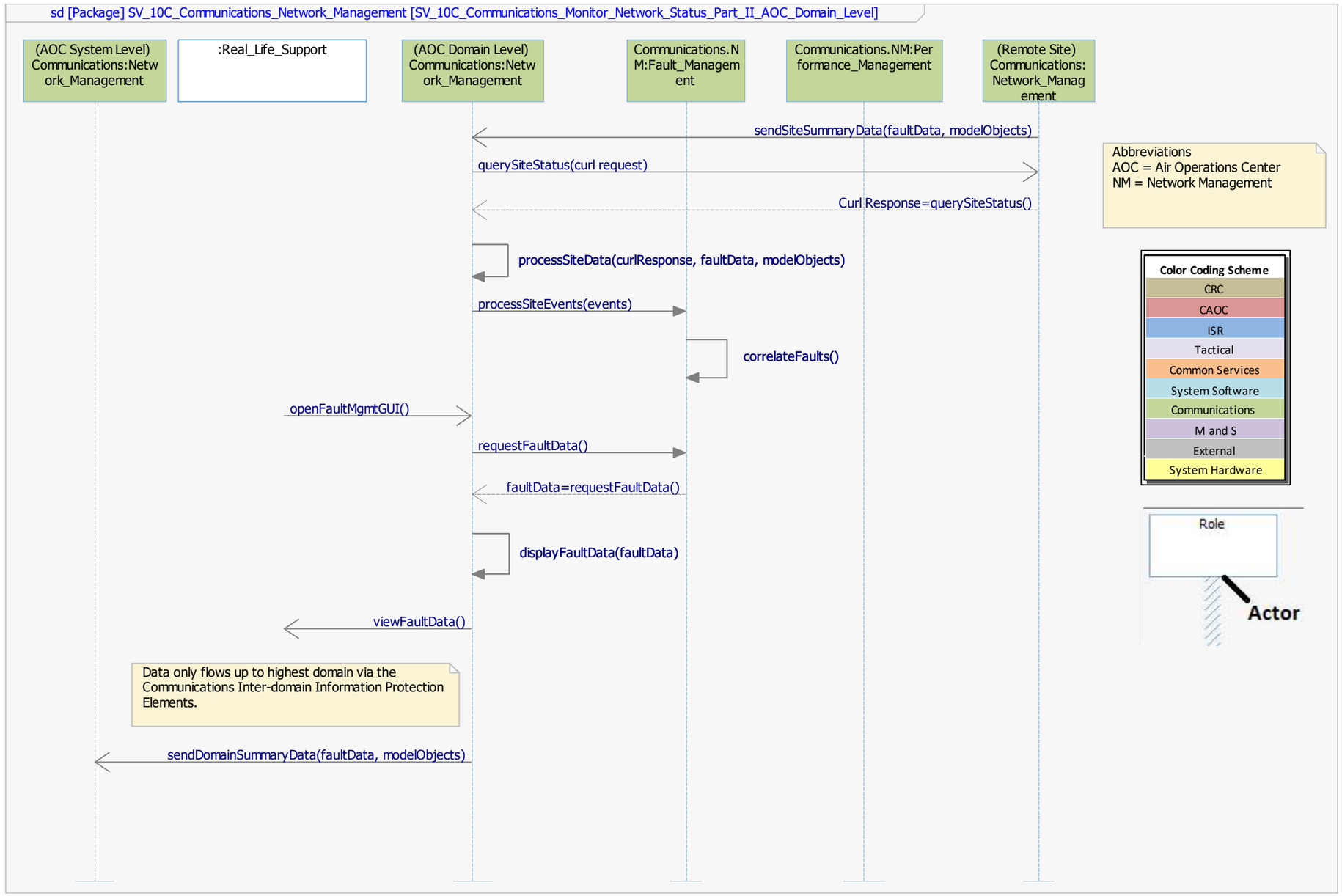


Figure 7-9: Mission/String Monitoring & Status Part II

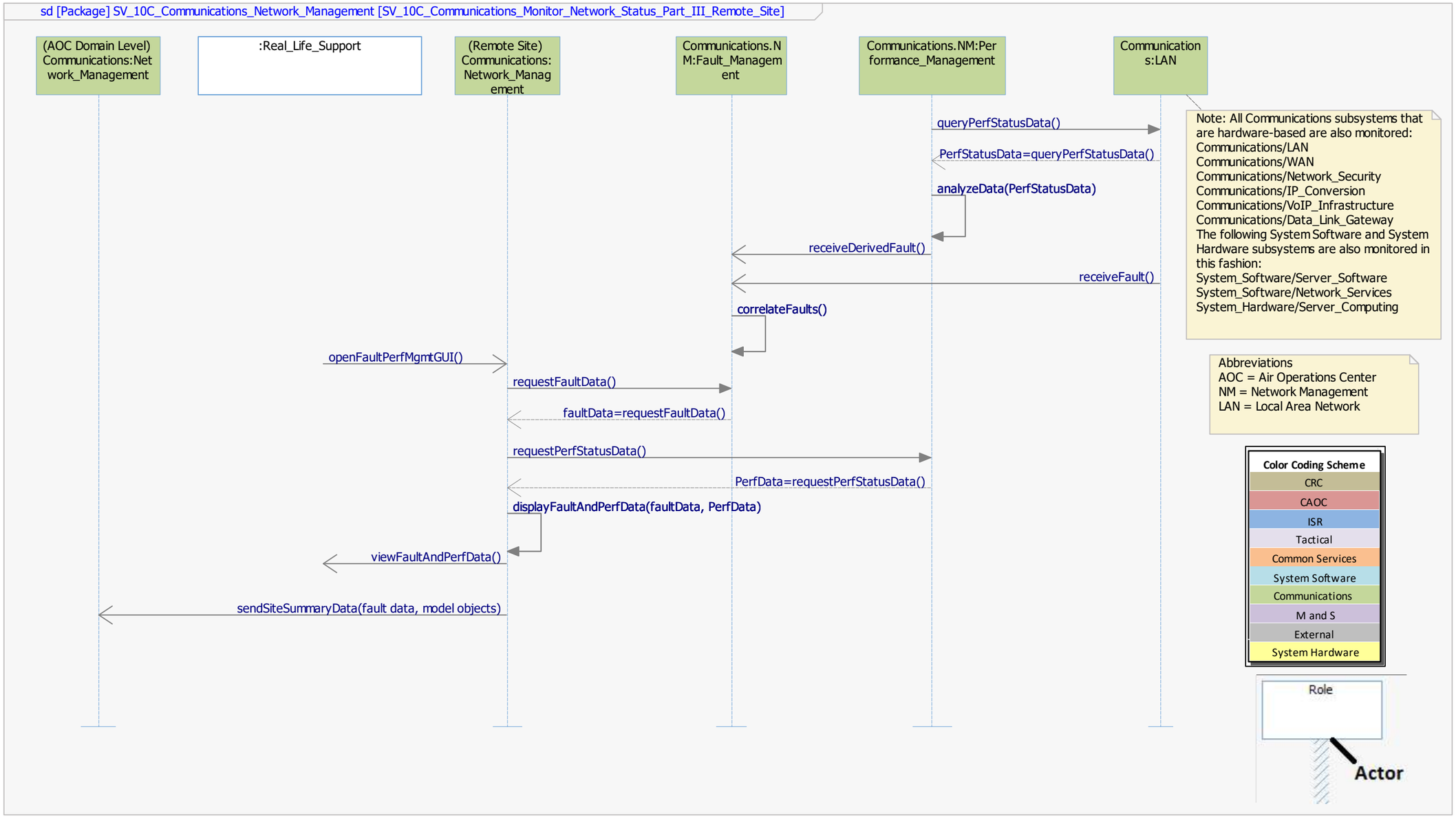
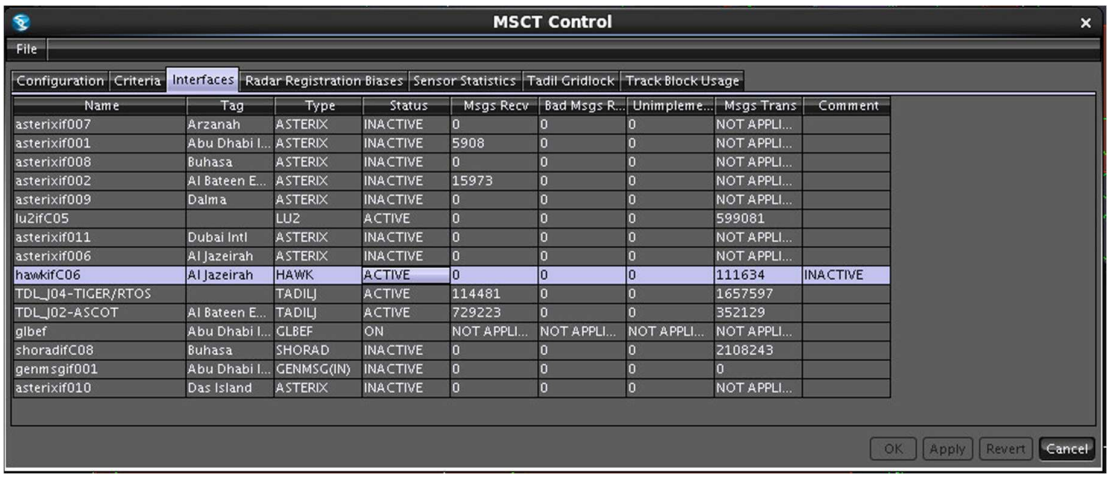


Figure 7-10: Mission/String Monitoring & Status Part III

7.4.2 Radio Failure/Replacement

The following describes the process by which the CRC Operator, upon being notified of a potential problem to a SHORAD radio currently being used in a mission, can replace that radio with an alternate SHORAD radio. The process starts with the SHORAD radio generating and sending a message to the RCS software indicating a change in the status of the radio. This results in RCS sending an asynchronous message to TRCC with a code indicating that the radio's status has changed and indicating the nature of the change. TRCC is unable to determine the impact of the change on data links or the mission and therefore generates a System Alert to inform the operator of the potential issue. It is up to the CRC operator to determine, based on the information that they have available, whether to replace the SHORAD radio with another radio, including one which may already be in use.

Upon receiving the System Alert indicating a potential problem with a SHORAD radio, the CRC operator uses the TDF display (See Figure 7-11) to check that SDL data is still being received from that radio. If it is and the operator determines that the status change does not affect the mission, then there is nothing else to do. However, if the operator sees that SDL traffic is not being received for that radio, the operator may choose to replace the SHORAD radio with another.



Name	Tag	Type	Status	Msgs Recv	Bad Msgs R...	Unimpleme...	Msgs Trans	Comment
asterixif007	Arzanah	ASTERIX	INACTIVE	0	0	0	NOT APPLI...	
asterixif001	Abu Dhabi I...	ASTERIX	INACTIVE	5908	0	0	NOT APPLI...	
asterixif008	Buhasa	ASTERIX	INACTIVE	0	0	0	NOT APPLI...	
asterixif002	Al Bateen E...	ASTERIX	INACTIVE	15973	0	0	NOT APPLI...	
asterixif009	Dalma	ASTERIX	INACTIVE	0	0	0	NOT APPLI...	
lu2ifC05		LU2	ACTIVE	0	0	0	599081	
asterixif011	Dubai Intl	ASTERIX	INACTIVE	0	0	0	NOT APPLI...	
asterixif006	Al Jazeirah	ASTERIX	INACTIVE	0	0	0	NOT APPLI...	
hawkifC06	Al Jazeirah	HAWK	ACTIVE	0	0	0	111634	INACTIVE
TDL_J04-TIGER/RTOS		TADILJ	ACTIVE	114481	0	0	1657597	
TDL_J02-ASCOT	Al Bateen E...	TADILJ	ACTIVE	729223	0	0	352129	
glbef	Abu Dhabi I...	GLBEF	ON	NOT APPLI...	NOT APPLI...	NOT APPLI...	NOT APPLI...	
shoradifC08	Buhasa	SHORAD	INACTIVE	0	0	0	2108243	
genmsgif001	Abu Dhabi I...	GENMSG(IN)	INACTIVE	0	0	0	0	
asterixif010	Das Island	ASTERIX	INACTIVE	0	0	0	NOT APPLI...	

Figure 7-11: TDF Interface Status Display

The CRC Operator uses the SCM display to delete the current Site Connection and then updates the Tower Network Participant using the Tactical Network Editor (See Figure 7-12) to add a SHORAD radio allocation to support the mission and saves the change. The CRC Operator creates a new Site Connection using the updated Tactical Network. Saving the Tactical Network results in an update being published to TRCC and triggers the new radio to be configured. Upon successful configuration of the radio, TRCC Server updates the radio planned resource status in Common Services to indicate it was configured. If the Replacement Radio was successfully configured for data, then SCM will start the Data Link IF process. The status of the data link in the TDF display changes to show that TDF is once again receiving traffic on the data link.

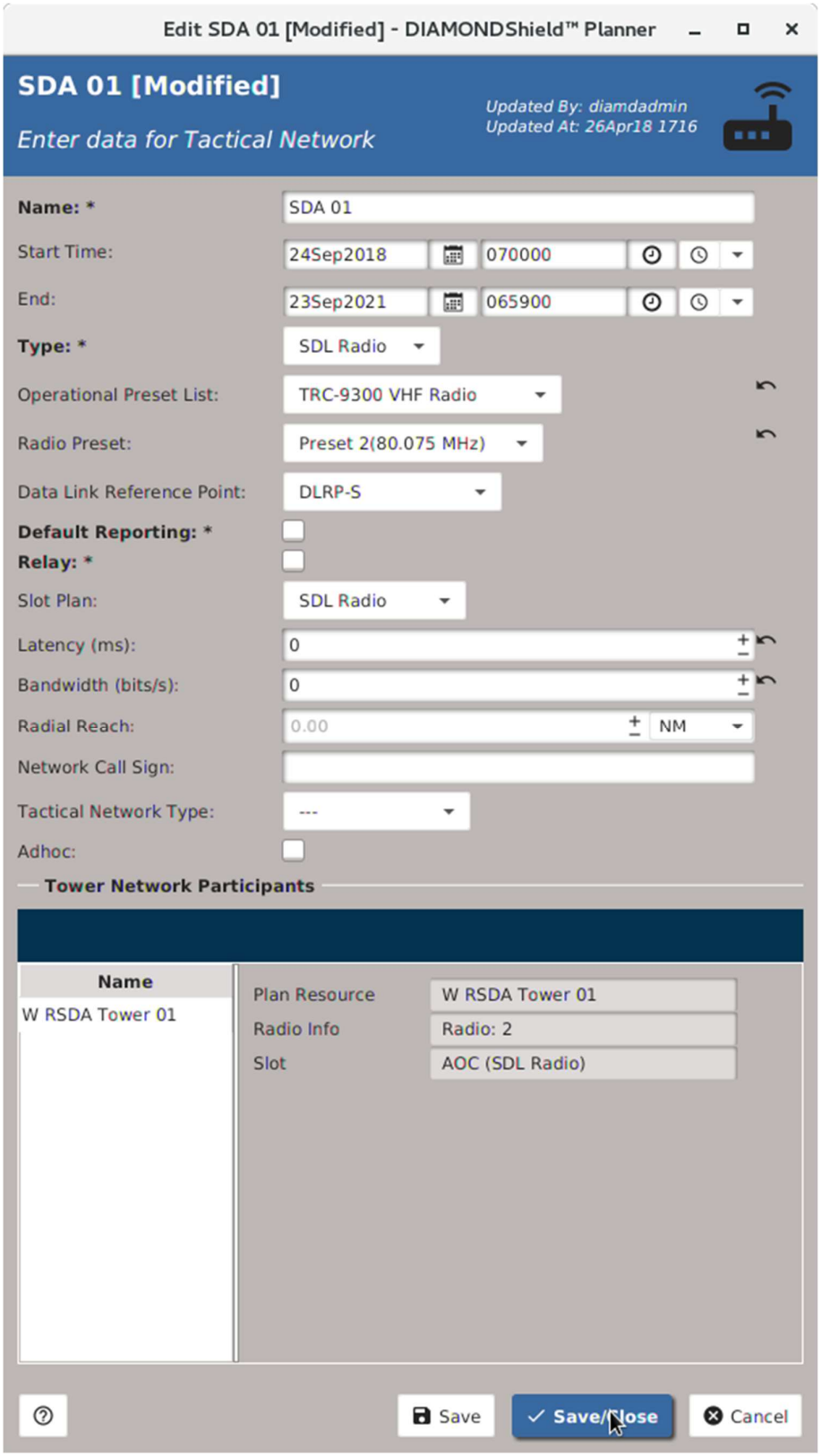


Figure 7-12:SCM Tactical Network Editor

See Figure 7-13 for a detailed sequence of this scenario.

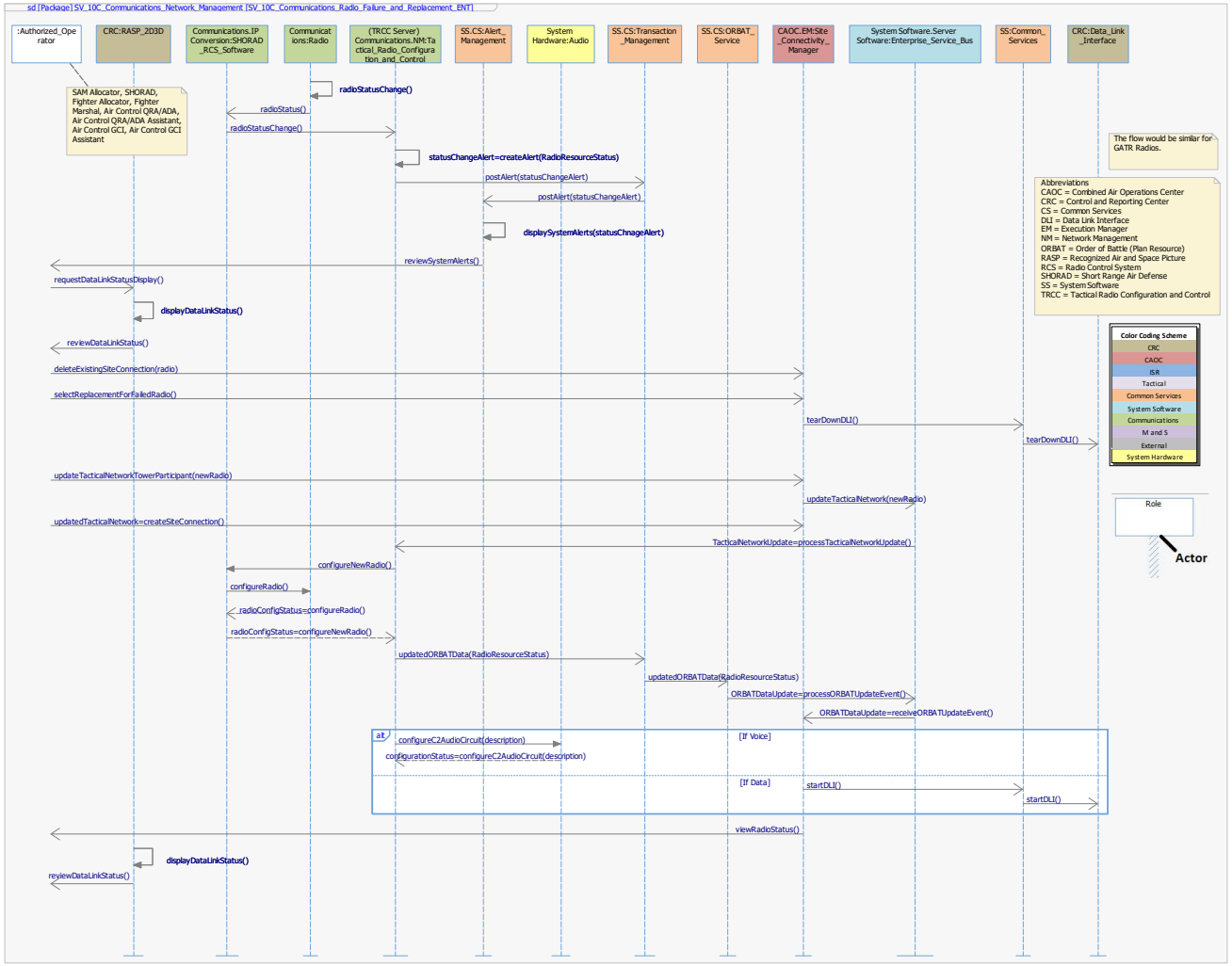


Figure 7-13: Radio Failure/Replacement

APPENDIX A REQUIREMENTS CROSS REFERENCE

The requirements listed in the following table have been verified by analysis using the Objective Qualitative Evidence (OQE) presented in this document. This summary table provides a reference for locating the requirements' analysis and supporting evidence using the Evidence Location column. The Verification Method for the requirements listed has been omitted from the Table as all requirements assessed in this Report are verification by "Analysis". All requirements listed in this table are from the C002 – Requirement Compliance and Verification Matrix.

CUSTOMER REQUIREMENT ID	EVIDENCE LOCATION
O3-019	Section 1.1
O3-021	Section 1.3
O8-001	Section 3.1
T11-01	Section 3.1
O8-029	Section 3.1.4
O8-030	Section 3.1.4
T3-110	Section 3.1.4
T3-203	Section 3.1.4
T3-117	Section 3.2
T3-135 O8-027	Section 3.2
T3-117	Section 3.2

APPENDIX B ACRONYMS

The list of acronyms contained within this document can be found in EADGET-LST-PTAL-001.docx.