



3.4	UC Audio and Video Conference System .....	3-73
3.4.1	Introduction.....	3-74
3.4.2	System Description .....	3-75
3.4.2.1	Overall System Description .....	3-75
3.4.2.2	System Architecture.....	3-75
3.4.2.3	Information Assurance.....	3-75
3.4.3	Service.....	3-76
3.4.3.1	Service Description.....	3-76
3.4.3.2	Integrated Services.....	3-80
3.4.3.3	Interoperability.....	3-82
3.4.3.4	Assured Services.....	3-89
3.4.4	Service Performance .....	3-91
3.4.4.1	Quality.....	3-91
3.4.4.2	Capacity .....	3-92
3.4.5	Service Management.....	3-94
3.4.5.1	System Management.....	3-94
3.4.5.2	Online Directory .....	3-99
3.4.5.3	Registration System .....	3-99
3.4.5.4	Scheduling System.....	3-100
3.4.5.5	Accounting and Billing.....	3-101
3.5	General Mass Notification Warning System (MNWS) .....	3-102
3.5.1	Standby MNWS Platform.....	3-104
3.5.2	[Optional] Mobile MNWS Platform.....	3-105
3.5.3	MNWS Database .....	3-106
3.5.4	Notifications Across MNWSs.....	3-107
3.5.5	MNWS Operator.....	3-107
3.5.6	Web Interface for Operators and Subscribers.....	3-109
3.5.7	Client Software for Subscribers.....	3-110
3.5.8	Event Sources.....	3-111
3.5.8.1	External IP-Enabled Event Sources .....	3-111
3.5.8.2	Internal IP-Enabled Event Sources .....	3-111
3.5.9	SMTP Delivery .....	3-112
3.5.10	External Delivery Systems and Services .....	3-112
3.5.10.1	Telephony Alerting Service .....	3-112
3.5.10.2	Short Message Service (SMS) Aggregation Service .....	3-113
3.5.10.3	Existing IP-Enabled Alert Delivery Devices .....	3-113
3.5.10.4	Installed Unified Communication (UC) Systems .....	3-114
3.5.10.5	Non-IP Delivery Systems .....	3-115

3.5.10.6	Integration With Giant Voice Systems .....	3-115
3.5.10.7	Integration With Indoor Voice Systems .....	3-116
3.5.10.8	Integration With Fire Alarm Systems .....	3-116
3.6	E911 Management System .....	3-117
3.6.1	Scope, Assumptions, and Terms .....	3-117
3.6.2	General E911 Management System.....	3-119
3.6.3	Automatic Location Identification (ALI) Information .....	3-120
3.6.4	End Instrument Location at Registration .....	3-121
3.6.5	Support for ELIN Query at 911 Call.....	3-122
3.6.6	SC Interfaces With E911 Management Systems .....	3-123
3.6.7	On-Site Notification of 911 Call.....	3-124
3.6.8	IPv6 Support .....	3-124
3.6.9	Information Assurance.....	3-124
3.6.10	OAM&P .....	3-124
3.7	Customer Premises Equipment.....	3-125
3.7.1	General Description .....	3-125
3.7.2	Requirements .....	3-125
3.8	DOD Secure Communications Devices.....	3-127
3.8.1	General Description .....	3-127
3.8.2	Requirements .....	3-127

**LIST OF FIGURES**

<b><u>FIGURE</u></b>		<b><u>PAGE</u></b>
Figure 3.2-1.	Centralized Directory (White Pages) Service .....	3-2
Figure 3.2-2.	Directory Service Attribute Information .....	3-4
Figure 3.2-3.	Directory Service Search and Display Criteria .....	3-5
Figure 3.3-1.	Routing Database Architecture: SS.....	3-7
Figure 3.3-2.	Reference Architecture for LRDBs.....	3-29
Figure 3.3-3.	Reference Architecture for MRDBs.....	3-30
Figure 3.3-4.	SS and MFS HR Call Flow Using TBCT – Part 1 .....	3-65
Figure 3.3-5.	SS and MFS HR Call Flow Using TBCT – Part 2.....	3-66
Figure 3.3-6.	SS and MFS HR Call Flow Using DSN HR .....	3-72
Figure 3.4-1.	UC Conference System Framework.....	3-74
Figure 3.6-1.	E911 Management System Architecture for UC E911 Services .....	3-118
Figure 3.6-2.	Illustrative ALI Database Records .....	3-119
Figure 3.6-3.	Message Flow at EI Registration .....	3-121
Figure 3.6-4.	911 Call Flows .....	3-122

**LIST OF TABLES**

<b><u>TABLE</u></b>		<b><u>PAGE</u></b>
Table 3.3-1.	LDAP DIT Attribute Formats .....	3-32
Table 3.7-1.	DTMF Generation and Reception From Users and Trunks .....	3-126

## SECTION 3 AUXILIARY SERVICES

### 3.1 INTRODUCTION

This section addresses required functionality, performance, capabilities, and associated technical parameters for Auxiliary Services and Systems.

### 3.2 DIRECTORY SERVICES (“WHITE PAGES”)

**AUX-000010 [Required: CVVoIP Directory Service]** The Classified Voice and Video over Internet Protocol (CVVoIP) shall have a directory service capability for searching white pages that allows subscribers to look up specific and applicable user information assigned to other CVVoIP subscribers. This is considered a requirement and is included for consideration by the CVVoIP Session Controller/Softswitch (SC/SS) product development teams.

**AUX-000020 [Required: CVVoIP Directory Service]** For security reasons, the CVVoIP directory system shall be a separate implementation from the sensitive but unclassified (SBU) Voice and Video over Internet Protocol (VVoIP) directory system.

**AUX-000030 [Required: CVVoIP Directory Service]** A centralized, multivendor supported, standards-based directory schema based on Microsoft Active Directory shall be implemented.

[Figure 3.2-1](#), Centralized Directory (White Pages) Service, illustrates the white pages directory arrangement.

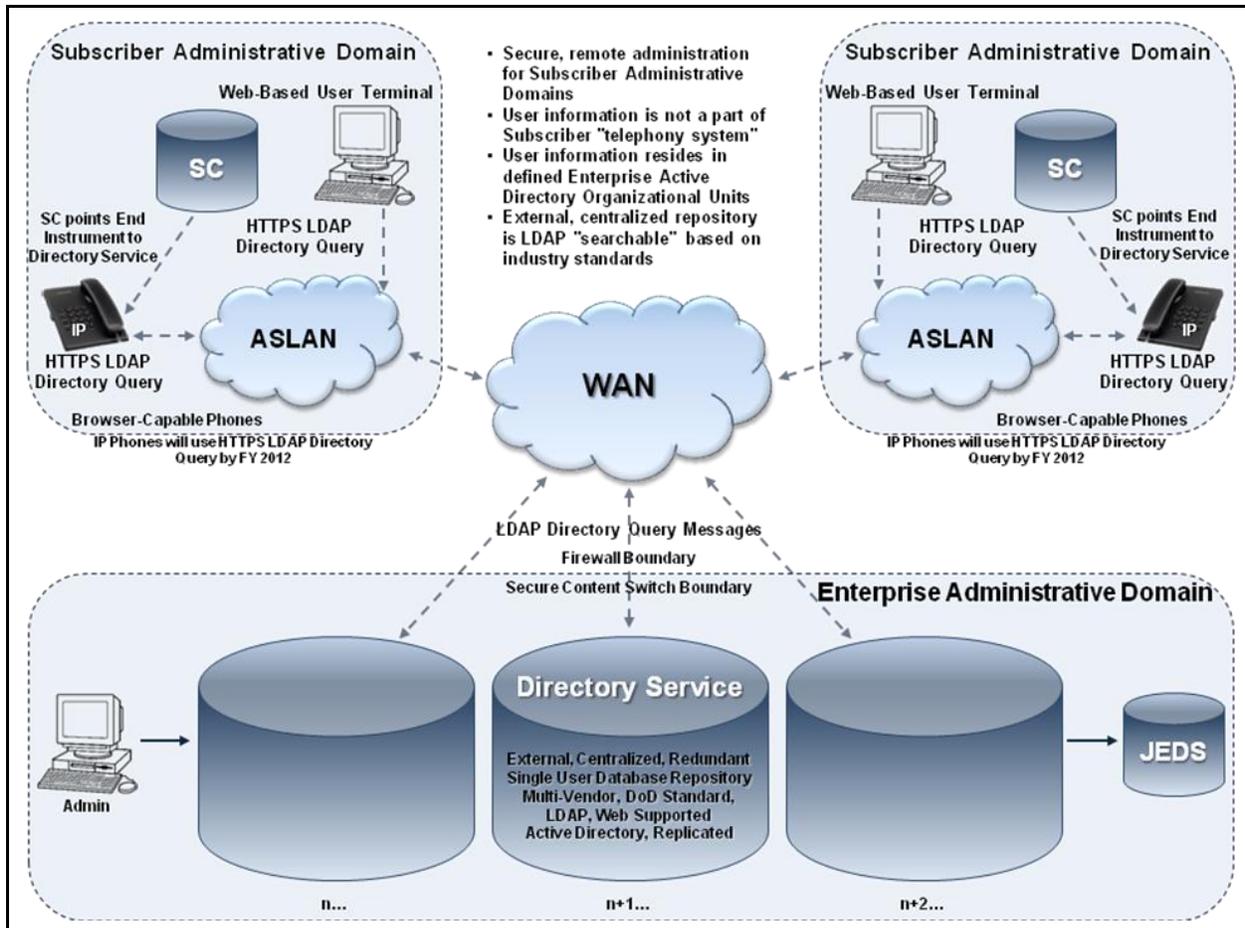


Figure 3.2-1. Centralized Directory (White Pages) Service

### 3.2.1 General Requirements for Centralized Directory (White Pages) Service

The general requirements that follow have been defined for the centralized directory (white pages) service.

#### 3.2.1.1 Use of External and Centralized "Corporate" Directory

**AUX-000040 [Required: CVVoIP Directory Service] Location and Architecture Design.** The global Directories Services architecture shall be consolidated and external to all other attached subscriber "telephony systems." The architecture shall be distributed in design to support redundancy and survivability as illustrated in [Figure 3.2-1](#). All telephony user information shall reside within the centralized Directory Services' Active Directory database.

**AUX-000050 [Required: CVVoIP Directory Service] Maintenance, Administrative, and Management Responsibility.** The overall responsibility to maintain the global Directory Services' user database structure shall reside with the Defense Information Systems Agency (DISA), with management of individual Active Directory organizational units being delegated to

---

each individual SC/SS telephony system administrator. This decentralized administrative responsibility within the Active Directory schema will ensure a constant and updated database of user information.

**AUX-000060 [Required: CVVoIP Directory Service]** Synchronization with the Local (SC/SS) and Defense RED Switch Network (DRSN) Directories. The local CVVoIP SC/SS user database for each Active Directory organizational unit shall be automatically synchronized within the larger Directory Services' Active Directory server architecture as soon as the SC/SS administrator provisions the user information within the system. Individual SC/SS administrators shall be responsible for provisioning user information at the same time the provisioning of phone devices is accomplished. This ensures a constantly maintained, real-time database repository of user information for the white pages search and lookup functionality.

The DRSN directory information shall be the responsibility of DISA and shall be statically updated as DRSN systems are modified and user information is updated from the field. At a minimum, this is expected to be accomplished at least once a year.

**AUX-000070 [Required: CVVoIP Directory Service]** Redundancy, Survivability, and Recovery. Redundancy and survivability, as well as disaster recovery, are designed into the Directory Service architecture. DISA shall be responsible for the design, maintenance, and backup of the system.

### ***3.2.1.2 Definition of Multivendor Standards Items***

**AUX-000080 [Required: CVVoIP Directory Service]** Active Directory Defined Attributes (Common Set of Fields). The CVVoIP Directory Service shall support the following Active Directory Defined Attributes, per [Figure 3.2-2](#), Directory Service Attribute Information.

AD Attribute Name	AD Attribute Description	Mandatory/ Optional/ Not Applicable	Search (PW/ BOTH)	Display (PW/ BOTH)	Comments – Layman's terminology
<b>User Attributes</b>					
givenName	First name	M		BOTH	First name
sn	Last Name (Surname)	M	BOTH	BOTH	Last name
displayName	Display-Name (first + last) or custom	NA			Automated – Combined display field of First name & Last name
initials	Initials	O			Initials
middleName	Other-Name	O			Middle name or Initial
generationQualifier	Generation-Qualifier	O			Suffix
employeeID	Employee-ID	M			EDHPI Electronic Data Interchange Person Identifier (CAC)
employeeType	Employee-Type	M			Personnel Type (e.g., Civilian, Contractor, Military)
employeeNumber	Employee-Number	O			PIN Number
title	Title	M	BOTH	BOTH	Rank
userPassword	User-Password	O			User password
mail	E-mail-Addresses	O			Email SIPR address
telephoneNumber	Telephone-Number	M		WEB	DSN/STN Telephone #
ipPhone	Phone-Ip-Primary	M		BOTH	VoSIP Telephone #
facsimileTelephoneNumber	Facsimile-Telephone-Number	NA			RESERVED
pager	Phone-Fax-Primary	NA			CMS Telephone #
otherTelephone	Phone-Office-Other	O		WEB	DSN Telephone #
otherFacsimileTelephoneNumber	Phone-Fax-Other	NA			RESERVED
otherHomePhone	Phone-Home-Other	NA			RESERVED
otherIpPhone	Phone-Ip-Other	NA			JWICS Telephone #
otherMobile	Phone-Mobile-Other	NA			RESERVED
otherPager	Phone-Fax-Other	NA			RESERVED
o	Organization-Name	M		WEB	Military Branch (e.g., AR, AF, NV, MC, DOD, CIV)
company	Company	M		WEB	COCOM/MAJCOM/DIVISION (e.g., CENTCOM, SOCOM, AMC, H <sup>3</sup> Mts, AFMC)
department	Department	M	BOTH	BOTH	Unit (e.g., 275th RNG BN, 379 <sup>th</sup> AEW, 2CSF)
physicalDeliveryOfficeName	Physical-Delivery-Office-Name	M	BOTH	BOTH	C/PS (e.g., Camp/Post/Station – MacDIA AFB, Ft Hood)
flags	Flags	M			Set to 1000 to make each OU searchable via a AD tool
userCert	User-Cert	NA			Future use - SFM
userCertificate	X509-Cert	NA			Future use - SFM
userPKCS12	PKCS #12 PFX PDU for exchange of personal identity information	NA			Future use - SFM

**Figure 3.2-2. Directory Service Attribute Information**

**AUX-000090 [Required: CVVoIP Directory Service]** Length and ASCII Characters of Each Attribute Field. ASCII characters supported by Active Directory shall be limited to characters that are supported by both SC/SS enclaves and the DRSN system. These are necessary to ensure proper display of white pages results. Alphanumeric characters that are supported shall be (0123..., abcd..., ABCD), periods (.), dashes (-), and commas (,).

Length of fields shall be set within Active Directory and shall be the basis of what is supported.

**AUX-000100 [Required: CVVoIP Directory Service]** “Ownership,” administration, and management responsibility of each organizational unit and its fields. Each individual SC/SS administrator shall “own” and be responsible for the administration and management of each user’s information governed by its telephony system. As each phone is provisioned and assigned within this system, the applicable user information shall be added to, modified in, and/or deleted from the assigned Directory Service Active Directory organizational unit within the domain. Each SC/SS administrator shall use the designed provisioning tool that DISA has developed which simplifies the task and ensures continuity of required user database information.

### **3.2.1.3 Search Criteria and Display Presentation for EIs (Computers and IP Phones**

**AUX-000110 [Required: CVVoIP Directory Service]** The CVVoIP Directory Service shall support the following Search Criteria and Display Presentation for End Instruments (EIs), per [Figure 3.2-3](#), Directory Service Search and Display Criteria.

On the IP Phone		On the Computer Web Page	
<b>Search Fields</b>	<b>Display Order</b>	<b>Search Fields</b>	<b>Display Order</b>
Layman's Terms (AD Attribute)	Layman's Terms (AD Attribute)	Layman's Terms (AD Attribute)	Layman's Terms (AD Attribute)
Last name (sn)	VoSIP Telephone # (ipPhone)	Last name (sn)	VoSIP Telephone # (ipPhone)
Unit (department)	Last name (sn)	Unit (department)	Last name (sn)
Rank (title)	First name (givenName)	Rank (title)	First name (givenName)
C/P/S (physicalDeliveryOfficeName)	Rank (title)	C/P/S (physicalDeliveryOfficeName)	Rank (title)
	Unit (department)		Unit (department)
			C/P/S (physicalDeliveryOfficeName)
			COCOM/MAJCOM/DIVISION (company)
			Military Branch (o)
			DSN/PSTN Telephone # (telephoneNumber)
			DRSN Telephone # (otherTelephone)

**Figure 3.2-3. Directory Service Search and Display Criteria**

**AUX-000120 [Required: CVVoIP Directory Service]** Lightweight Directory Access Protocol (LDAP) Criteria and Browser (Display) Functionality. Industry standard LDAP connection protocols (port 389) shall be used and supported.

Standardized browser support for computer white pages functionality (parsing and display of search results) shall be restricted to secure Web protocols [Transport Layer Security (TLS)/Hypertext Transport Protocol Secure (HTTPS)] only. This shall be part of the Directory Services architecture capability and shall ensure the privacy and security of user information to authorized viewers.

Standardized browser support for Internet protocol (IP) phone white pages functionality (parsing and display of search results) shall be mandatory, so that Web-based [Hypertext Markup Language (HTML)/Extensible HTML (XHTML)] user information can be displayed. As of calendar year (CY) 2012, display of unsecure Web protocols is no longer supported [Hypertext Transport Protocol (HTTP)]. As of CY 2012, only secure Web protocols (TLS/HTTPS) shall be supported.

**AUX-000130 [Required: CVVoIP Directory Service]** The CVVoIP Directory Service shall support the following Definitions of EI Display Fields:

- a. Browser Requirements. EIs (e.g., IP Phones) shall support HTML/XHTML-based (<http://www.w3.org/TR/xhtml1/>) rendering of content. Computers (e.g., Web browsers) with HTML-based applications, such as Microsoft Internet Explorer version 7.X, 8.X, and 9.X, are recommended.
- b. Character Fields (Attributes). See [Figure 3.2-3](#), Directory Service Search and Display Criteria, for details.
- c. Length of Attribute Fields.

- (1) Web Browsers. The length of the displayed fields on the Web interface of a computer shall be matched and validated with the limitations/policies imposed by the

- underlying directory server schema definition. Search results shall be presented in multiple lines with more display information available because of the size of the screening area. On each line, the Web browser shall display the data representing the attributes for the matched (found) entries as concatenated together using various delimiters (such as “,” “-,” “/”). The length of the information being displayed on the Web browser interface shall be configurable to be truncated to preset values on a per-attribute basis. This shall be accomplished using the Directory Service Web-based administrative interface. If attributes with additional characters are stored in the underlying directory server, then the Web-based user interface shall truncate the displayed content to the limits imposed by the Directory Service application configuration parameters. All these parameters shall be set to optimal lengths, given the size of the screening area that computers offer.
- (2) End Instruments. Search results shall be presented in multiple lines. On each line, the phone shall display the data representing the matched entries’ attributes, as concatenated together using various delimiters (such as “,” “-,” “/”) with a maximum of 64 characters per line. If attributes with additional characters are stored in the underlying directory server, then the phone user interface shall truncate the displayed content to the limits imposed by the phone device and as defined in the Directory Service application configuration parameters.
- d. How Many/Which Fields of Identification. See [Figure 3.2-3](#), Directory Service Search and Display Criteria, for details.
- e. Soft/Hard Key Functions (such as a “directory access button”). The CVVoIP SC/SS manufacturers shall provide a single action, “directory access” function, through software and/or hardware, on all supported, Joint Interoperability Test Command (JITC)-certified IP Phones. Through these methods, the action shall be a programmable, Web-based function key that can have a Uniform Resource Locator (URL). This shall allow users to have the capability to use one button to start all actions when using the Directory Service.

### 3.3 RTS ROUTING DATABASE

#### 3.3.1 Introduction

This section specifies DISA requirements for the Real-Time Services (RTS) Routing Database, the Commercial Cost Avoidance feature, and the Hybrid Routing (HR) feature.

These requirements apply to these Unified Capabilities (UC) Approved Product List (APL) Products:

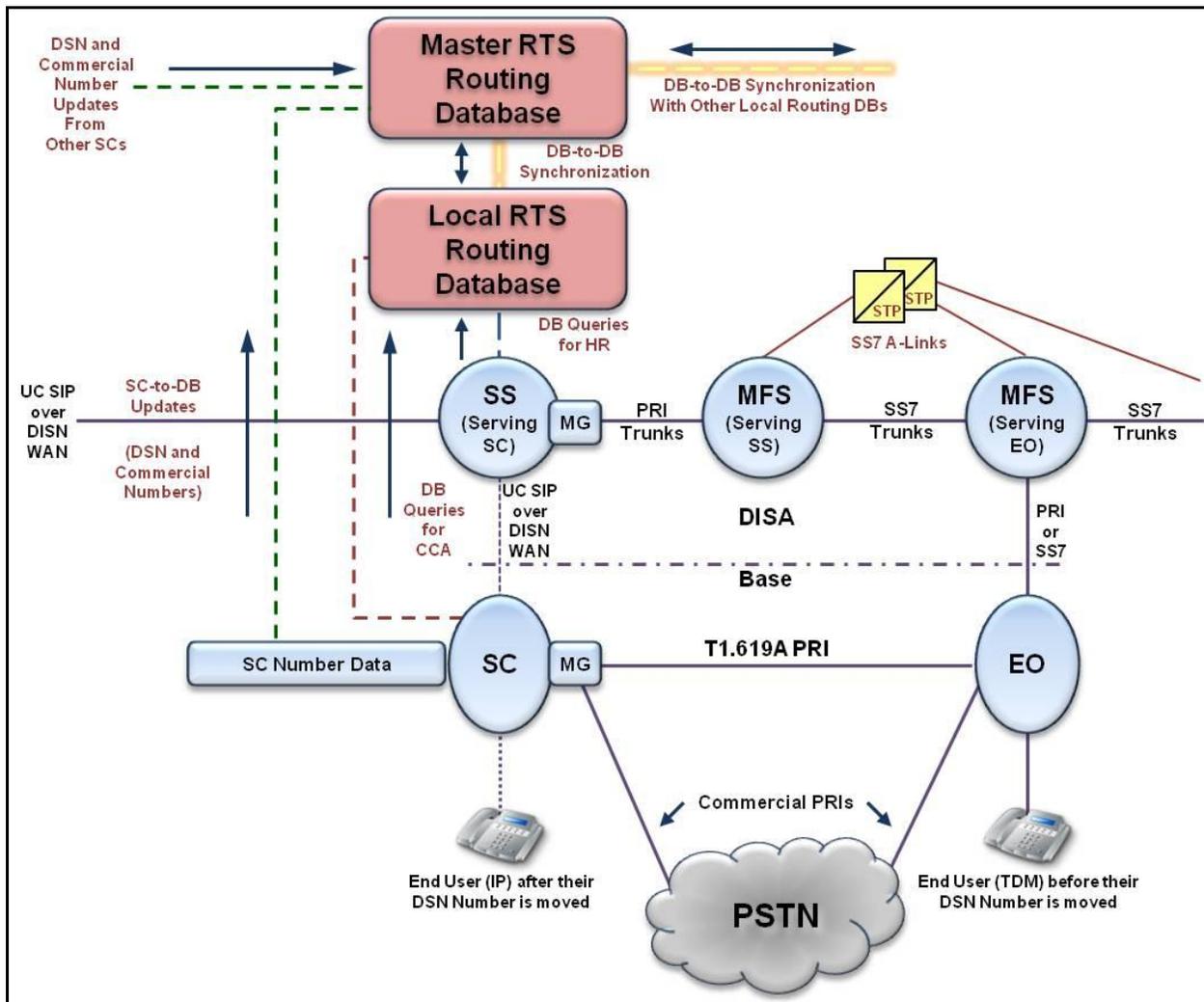
- The SS.
- The SC.
- The Local RTS Routing Database (LRDB).

- The Master RTS Routing Database (MRDB).

These requirements are organized into four areas:

- SS-to- LRDB queries for HR.
- SC-to-LRDB queries for Commercial Cost Avoidance.
- SC-to-MRDB updates [for Defense Switched Network (DSN) numbers and commercial numbers].
- LRDB and MRDB functional requirements.

[Figure 3.3-1](#), Routing Database Architecture: SS, shows the basic architecture that is used for these initial RTS Routing Database requirements. This architecture and these requirements are intended to be generic, and to support interoperability between multiple SS, SC, and Routing Database vendors. A multi-vendor interoperable protocol is used between network elements from different vendors (e.g., an SS or SC from one vendor, and an LRDB from another vendor).



**Figure 3.3-1. Routing Database Architecture: SS**

### 3.3.1.1 Assumptions

The SC, LRDB, and MRDB requirements in this section are based on the following assumptions:

- These requirements assume that a Multi-Vendor-Interoperable (MVI) Protocol is used on the following interfaces:
  - The interface between the SS and the LRDB for HR queries and responses.
  - The interface between the SC and the LRDB for Commercial Cost Avoidance queries and responses.
  - The interface between the SC and the MRDB for Database updates (transfers of DSN and commercial numbers from the SC to the MRDB).
  - The interface between the LRDB and MRDB for Database-to-Database synchronization.

The MVI Protocol used here is LDAP Version 3 (LDAPv3), as defined in the following Requests for Change (RFCs):

RFC 2251, RFC 2252, RFC 2253, RFC 2254, RFC 2255,  
RFC 2256, RFC 2829, RFC 2830, RFC 4510, RFC 4511.

- A Routing Database “data schema” is needed to specify the “information elements” that are included in the Database queries for HR (SS ↔ LRDB), the Database queries for Commercial Cost Avoidance (SC ↔ LRDB), the Database updates (SC ↔ MRDB), and the Database synchronization messages (LRDB ↔ MRDB). For these requirements, this data schema is based on LDAPv3.
- Examples of information that needs to be included in the various Database queries, Database responses, and Database updates follow:
  - The Database queries for HR need to contain the full 10-digit DSN called number.
  - The Database responses for HR need to indicate either the “number not found” or the “number found” along with an identifier for the destination SC for that DSN called number. [The SC identifier could also be absent when the number is found, meaning that the number is located on an End Office (EO)]. The responses also should contain an identifier for the primary SS that serves that SC, and an identifier for the backup SS that serves that SC. The Call Connection Agent (CCA) Identifier (CCA-ID) is the required identifier for the destination SC, the primary SS, and the backup SS in this case.
  - The Database queries for Commercial Cost Avoidance need to contain the full internationally significant commercial called number [in the format of “Country Code (CC) plus Nationally Significant Number (NSN)”].
  - The Database responses for Commercial Cost Avoidance need to either indicate “number not found,” or contain the full 10-digit DSN called number that matches the commercial called number.

- The Database updates (SC-to-MRDB) need to contain the full DSN called number, the full commercial called number, the identifier of the source SC, the identifier of the primary SS for that SC, and the identifier of the backup SS for that SC. The CCA-ID is the recommended identifier for the SC, primary SS, and backup SS in this case.

### 3.3.2 SS to LRDB Interface: Database Queries for HR

The requirements in this section apply to the SS and the LRDB. The LRDB can be located in a site that is physically remote from the SS site.

**AUX-000140 [Required: SS, LRDB]** The SS and the LRDB shall support the HR feature per the requirements in this section.

**AUX-000150 [Required: SS]** The SS shall support an interface to a LRDB to support Database queries and Database responses for the HR feature.

**AUX-000160 [Required: LRDB]** The LRDB shall support an interface to the SS to support Database queries and Database responses for the HR feature.

**AUX-000170 [Required: SS, LRDB]** The query-response interface between the SS and the LRDB shall be LDAPv3 over TLS over IP. On the SS, this LDAPv3 interface shall be compliant with RFC 4511 and all the LDAP technical specifications listed in Section 1 of RFC 4510. On the LRDB, see the LDAPv3 interface requirement ([AUX-001180](#)) in [Section 3.3.5.2.1](#), General Architecture, Protocols, and Interfaces.

**AUX-000180 [Required: SS, LRDB]** The encoding of the LDAPv3 messages and data schema used on the Database query interface between the SS and the LRDB shall follow the Basic Encoding Rules (BERs) of Abstract Syntax Notation One (ASN.1). On the SS, this encoding shall be consistent with Section 5.1, Protocol Encoding, of RFC 4511, June 2006, as referenced by RFC 4510. On the LRDB, see the LDAPv3 interface requirement ([AUX-001180](#)) in [Section 3.3.5.2.1](#), General Architecture, Protocols, and Interfaces.

**AUX-000190 [Required: SS, LRDB]** The interface between the SS and the LRDB shall be secured using TLS, consistent with the requirements for securing UC Session Initiation Protocol (SIP) messages using TLS in Section 4, Information Assurance. This security shall provide mutual authentication between the SS and the LRDB, message confidentiality for the Database query and Database response, and message integrity for the Database query and Database response.

**AUX-000200 [Required: SS, LRDB]** The interface between the SS and the LRDB shall traverse the data firewalls [and not the Session Border Controller (SBC) firewalls] at both the SS and the LRDB sites.

**AUX-000210 [Required: SS, LRDB]** The interface between the SS or SS and the LRDB shall traverse the Customer Edge (CE) Routers at both the SS and the LRDB sites, using the

Differentiated Services Code Point (DSCP) for User Signaling traffic, and the associated CE Router (CE-R) queues.

**AUX-000220 [Required: SS]** The interface between the SS and the LRDB shall terminate on the Ethernet interface used for VVoIP signaling traffic at the SS, as described in Section 4, Information Assurance.

**AUX-000230 [Required: SS]** The SS shall allow HR to be activated for all calls going through the SS. The SS also shall allow HR to be activated only for calls going through the SS to a specific set of DSN numbers. In this second case, the SS shall allow DISA to configure the set of DSN numbers for which HR is activated.

**AUX-000240 [Required: SS]** The DISA-configurable set of DSN numbers for HR shall support the following elements:

- a. Individual 10-digit numbers from the UC numbering plan.
- b. Ranges of 10-digit numbers from the UC numbering plan.

Each range shall be configurable so that DISA can specify the first and last numbers in the range.

**AUX-000250 [Required: SS]** The SS shall allow a configurable range to include one of the following:

- a. An entire DSN Area Code (first three digits specified).
- b. An entire DSN Area Code and Office Code (first six digits specified).
- c. A “thousands group” within a DSN Area Code and Office Code (first seven digits specified).
- d. A “hundreds group” within a DSN Area Code and Office Code (first eight digits specified).
- e. A “tens group” within a DSN Area Code and Office Code (first nine digits specified).

**[Optional: SS]** DISA also shall be able to independently specify the first and last numbers in a range without having to limit that range to a single Area Code, a single Office Code, a single thousands group, a single hundreds group, or a single tens group.

**AUX-000260 [Required: SS]** The SS shall allow DISA to configure the following within the set of DSN numbers for which HR is activated:

- a. Up to 20 individual DSN numbers.
- b. Up to 20 ranges of DSN numbers.

**AUX-000270 [Required: SS]** When the HR feature is activated for all calls and when the HR feature is activated for calls to a specific set of DSN numbers, the SS shall apply the HR feature on calls that enter the SS on all line or Local Area Network (LAN)-side and trunk or Wireless

---

Area Network (WAN)-side interfaces, both Time Division Multiplexing (TDM) and Voice over IP (VoIP).

### **3.3.2.1 HR Query From SS**

**AUX-000280 [Required: SS]** When the HR feature is activated for all calls, the SS shall make an HR query to the LRDB for each call that is placed to a DSN number. When the HR feature is activated for calls to a specific set of DSN numbers, the SS shall make an HR query to the LRDB for each call that is placed to a DSN number within that set of DSN numbers.

**AUX-000290 [Required: SS]** In both cases, the SS shall not make HR queries for calls that are placed to Public Switched Telephone Network (PSTN) numbers or PSTN service codes such as 911 (in the United States), 112 (in Europe), or 411 (in the United States).

**AUX-000300 [Conditional: SS]** The SS also may use cached data from a previous HR query and HR response to process an HR call, instead of making an HR query to the LRDB on that call. The SS shall associate the cached HR response data with the DSN called number for the call in this case. The SS vendor shall also support mechanisms for expiration of old cache entries and limits to the size of cached data in this case.

**AUX-000310 [Required: SS]** The HR query that the SS sends to the LRDB shall contain the full 10-digit DSN called number for that call. The HR query shall be sent in the LDAPv3 Search Request message. This Search Request message shall contain the following fields in ASCII format:

- a. Base Object field containing an LDAP Distinguished Name containing the Domain Components “uc” and “mil” (dc=uc, dc=mil).
- b. Scope field containing the value “wholeSubtree.”
- c. Filter field containing the following:
  - (1) Directory Number field containing the 10-digit DSN called number.

**AUX-000320 [Required: LRDB]** The LRDB shall accept and process the previous HR query from the SS containing the full 10-digit DSN called number.

**AUX-000330 [Required: LRDB]** The LRDB shall store the following information in its Database record for each 10-digit DSN number:

- a. CCA-ID of the SC serving that DSN number (the “destination SC”).
- b. CCA-ID of the primary SS serving the destination SC.
- c. CCA-ID of the backup SS serving the destination SC.
- d. Full internationally significant commercial number matching that DSN number (if this commercial number exists).

NOTE: The CCA-IDs may be absent from the record in cases in which the DSN and commercial numbers in the record are associated with a DSN end user who is served by a DSN EO or Private Branch Exchange (PBX).

### ***3.3.2.2 Database Response When DSN Number Is Found***

**AUX-000340 [Required: LRDB]** When the LRDB finds a database record that matches the DSN number in the HR query, the LRDB shall return an HR response to the SS containing the following information taken from that record:

- a. CCA-ID of the destination SC.
- b. CCA-ID of the primary SS serving the destination SC.
- c. CCA-ID of the backup SS serving the destination SC.
- d. Full internationally significant commercial number matching that DSN number (if this commercial number exists).

NOTE: The CCA-IDs may be absent from the record in cases in which the DSN and commercial numbers in the record are associated with a DSN end user who is served by a DSN EO or PBX.

**AUX-000350 [Required: LRDB]** The LRDB shall send this HR response in the LDAPv3 Search Result Entry and Search Result Done messages.

The Search Result Entry message shall contain the following fields in ASCII format:

- a. Object Name field containing an LDAP Distinguished Name containing the following:
  - (1) User ID component containing the commercial number (e.g., UID=7038821234).
  - (2) Domain Components “uc” and “mil” (dc=uc, dc=mil).

The commercial number in the User Identifier (UID) field may be represented in either national or international format (depending on the SC that uploads the number in the Database).

- b. Attributes field containing the following attributes:
  - (1) UID field containing the commercial number.
  - (2) Object Class field containing “mobSLR.”
  - (3) Subscriber Type field containing “asftswtch.”
  - (4) SIP Alias field containing the full commercial called number followed by “@uc.mil” (e.g., 17038821234@uc.mil).
  - (5) Sip User Name field containing the UID (i.e., commercial number) followed by “@uc.mil” (e.g., 7038821234@uc.mil).

- (6) Directory Number field containing the 10-digit called DSN number.
- (7) LSCCCAID field containing the CCA-ID of the destination SC.
- (8) SSCCAID field containing the CCA-IDs of the primary SS and the backup SS serving the destination SC, separated by a comma.
- (9) The LRDB also can include other attribute fields here that the SS may ignore.

The commercial number in the UID field may be represented in either national or international format, depending on the SC that uploads the number in the Database.

**AUX-000360 [Required: LRDB]** The Search Result Done message shall contain the following field in ASCII format:

- Result Code field indicating “Success.”

### ***3.3.2.3 Database Response When DSN Number Is Not Found***

**AUX-000370 [Required: LRDB]** When the LRDB finds no Database record that matches the DSN number in the HR query, the LRDB shall return an HR response to the SS containing a “number not found” indication.

**AUX-000380 [Required: LRDB]** The LRDB shall send this HR response in the LDAPv3 Search Result Done message. The Search Result Done message shall contain the following field in ASCII format:

- Result Code field indicating “Success.”

### ***3.3.2.4 SS Actions Based on Database Response***

**AUX-000390 [Required: SS]** In the Number Found case, the SS shall accept and process the aforementioned HR response from the LRDB containing the SC CCA-ID, the primary SS CCA-ID, and the backup SS CCA-ID.

**AUX-000400 [Required: SS]** In the Number Found case, the SS shall also accept and process HR responses from the LRDB that do not contain any CCA-IDs.

**AUX-000410 [Required: SS]** In the Number Not Found case, the SS also shall accept and process the aforementioned HR response from the LRDB containing the “number not found” indication.

**AUX-000420 [Required: SS]** In the Number Found case, if the HR response contains CCA-ID values, then the SS shall route the call to the SC specified by the SC CCA-ID in the HR response.

- a. If that SC is not subtended by the SS, then the SS shall route the call to the SS specified by the primary SS CCA-ID in the HR response.

- 
- b. If the primary SS is not accessible from the SS that sent the query and received the response (e.g., because the primary SS is out of service), then that querying SS shall route the call to the SS specified by the backup SS CCA-ID in the HR response.

**AUX-000430 [Required: SS]** The SS shall support an internal table [(configurable by DISA or the Military Department (MILDEP))] that lists the CCA-IDs of all the SCs served by that SS, and the CCA-IDs of all of the other SSs in the UC network to which this SS can route UC SIP sessions.

- a. For each CCA-ID listed in this table, this SS shall allow DISA or the MILDEP to store the DISN WAN IP address of the SBC that fronts the SC or SS associated with that CCA-ID.
- b. This SS shall use this internal table to resolve CCA-IDs returned by the LRDB into destination SC and SS SBC IP addresses on the DISN WAN.
- c. This SS shall use these destination SC and SS SBC IP addresses to route calls to the destination SCs and SSs, per the previously listed requirements.

**AUX-000440 [Required: SS]** In the Number Not Found case and in the Number Found case when the HR response does not contain a value (i.e., CCA-IDs are absent), the SS shall use the route specified in its internal routing tables for the called DSN number to route the call request to one of the following:

- a. The destination SC (by an outgoing UC SIP route).
- b. Another SS (by an outgoing UC SIP route).
- c. A Multifunction Switch (MFS) or EO connected to the Media Gateway (MG) of that SS [by an outgoing T1.619a Primary Rate Interface (PRI) route].
- d. The destination EI [UC SIP Video End Instrument (UEI), Proprietary Internet Protocol Voice End Instrument (PEI), or analog EI] served by an SC that is internal to the SS (when an internal SC is supported).

**AUX-000450 [Required: SS]** In the Number Not Found case and in the Number Found case when the HR response does not contain a value for the CCA-IDs (i.e., CCA-ID is absent),

- a. When the SS determines that the call to the DSN number previously arrived at the SS from an incoming T1.619a PRI route from an MFS,
- b. And then determines that the call should be routed back to that MFS over an outgoing T1.619a PRI route using the same PRI,
- c. The SS shall use a “route optimization” procedure on that PRI to do the following:
  - (1) Return the call to the MFS.
  - (2) Remove the incoming PRI B-Channel and outgoing PRI B-Channel from the call path so that these two B-Channels are not kept in use for the remainder of the call.

This “route optimization” procedure shall be MVI, and shall work with MFS products from other vendors (besides the SS vendor), without requiring any enhancements or software patches to the other vendors’ MFS products.

The SS vendor shall identify for DISA what this MVI route optimization procedure is, so that DISA can share it with other MFS vendors, and perform interoperability testing on it using the SS and MFS products from other vendors.

**AUX-000460 [Required: SS]** If the SS determines that it has lost connectivity with the LRDB (e.g., because that Database has failed), then the SS shall apply the Failover to Secondary LRDB procedures, per the requirements in [Section 3.3.5.2.5](#), Failover Procedures.

**AUX-000470 [Required: SS]** If the SS applies these failover procedures and does not receive the necessary routing information from the Secondary LRDB, then the SS shall use its internal routing data tables to complete the call to the DSN number.

**AUX-000480 [Conditional: SS]** If the SS supports caching of Database responses for the HR feature, and the SS loses TLS connectivity with the LRDB, then the SS shall first check the current HR cache data for Number Found information matching the called DSN number on each call in which HR treatment is required.

- a. If this current HR cache data contains Number Found information for the called DSN number, then the SS shall complete that call using the CCA-IDs (SC, primary SS, and backup SS) in that HR cache data.
- b. If this current HR cache data contains Number Found information for the called DSN number but no CCA-IDs, then the SS shall assume a Number Not Found case and apply the Number Not Found treatment described in the previous requirements.
- c. If the current HR cache data does not contain Number Found information for the called DSN number, then the SS shall assume a Number Not Found case and apply the Number Not Found treatment described in the previous requirements.

### **3.3.3 SC to LRDB Interface: Database Queries for Commercial Cost Avoidance**

The requirements in this section apply to the SC and the LRDB. The LRDB can be located in a site that is physically remote from the SC site.

**AUX-000490 [Required: SC, LRDB]** The SC and the LRDB shall support the Commercial Cost Avoidance feature per the requirements in this section.

**AUX-000500 [Required: SC]** The SC shall support an interface to an LRDB to support Database queries and Database responses for the Commercial Cost Avoidance feature.

**AUX-000510 [Required: LRDB]** The LRDB shall support an interface to the SC to support Database queries and Database responses for the Commercial Cost Avoidance feature.

---

**AUX-000520 [Required: SC, LRDB]** The query-response interface between the SC and the LRDB shall be LDAPv3 over TLS over IP. On the SC, this LDAPv3 interface shall be compliant with IETF RFC 4511 and all the LDAP technical specifications listed in Section 1 of RFC 4510. On the LRDB, see the LDAPv3 interface requirement ([AUX-001180](#)) in [Section 3.3.5.2.1](#), General Architecture, Protocols, and Interfaces.

**AUX-000530 [Required: SC, LRDB]** The encoding of the LDAPv3 messages and data schema used on the Database query interface between the SC and the LRDB shall follow the BER of ASN.1. On the SC this encoding shall be consistent with Section 5.1, Protocol Encoding, of RFC 4511. On the LRDB, see the LDAPv3 interface requirement ([AUX-001180](#)) in [Section 3.3.5.2.1](#), General Architecture, Protocols, and Interfaces.

**AUX-000540 [Required: SC, LRDB]** The interface between the SC and the LRDB shall be secured using TLS, consistent with the requirements for securing UC SIP messages using TLS in Section 4, Information Assurance. This security shall provide mutual authentication between the SC and the LRDB, message confidentiality for the Database query and Database response, and message integrity for the Database query and Database response.

**AUX-000550 [Required: SC, LRDB]** The interface between the SC and the LRDB shall traverse the data firewalls (and not the SBC firewalls) at both the SC and LRDB sites.

**AUX-000560 [Required: SC, LRDB]** The interface between the SC and the LRDB shall traverse the CE-Rs at both the SC and LRDB sites, using the DSCP for User Signaling traffic and the associated CE-R queues.

**AUX-000570 [Required: SC]** The interface between the SC and the LRDB shall terminate on the Ethernet interface used for VVoIP signaling traffic at the SC, as described in Section 4, Information Assurance.

**AUX-000580 [Required: SC]** The SC shall allow Commercial Cost Avoidance to be activated for all of the following types of calls:

- a. Originated by EIs or MGs on the SC.
- b. Placed to commercial called numbers instead of DSN called numbers.

This is the “activated for all commercial numbers” option for Commercial Cost Avoidance.

**AUX-000590 [Required: SC]** The SC shall also allow Commercial Cost Avoidance to be activated for all of the following types of calls:

- a. Originated by EIs or MGs on the SC.
- b. Placed to commercial called numbers instead of DSN called numbers.
- c. Placed to numbers within a specific set of commercial numbers.

---

In this second case, the SC shall allow DISA to configure the set of commercial numbers for which Commercial Cost Avoidance is activated.

This is the “activated for select commercial numbers” option for Commercial Cost Avoidance.

**AUX-000600 [Required: SC]** The DISA-configurable set of commercial numbers for Commercial Cost Avoidance shall support the following elements:

- a. Individual numbers from the worldwide E.164 commercial numbering plan.
- b. Ranges of numbers from the worldwide E.164 commercial numbering plan.

Each range shall be configurable so that DISA can specify the first and last numbers in the range.

**AUX-000610 [Required: SC]** The SC shall allow a configurable range to include the following:

- a. An entire E.164 CC (e.g., CC 1 for the United States and Canada, CC 49 for Germany, and CC 82 for South Korea).
- b. CC 1 and an entire three-digit Area Code (e.g., in the United States or Canada).
- c. CC 1 and an entire three-digit Area Code and three-digit Office Code.
- d. A range of numbers within CC 1, a single Area Code, and a single Office Code (e.g., a thousands group, hundreds group, or tens group within CC 1, the Area Code, and the Office Code).
- e. For countries outside CC 1, an entire E.164 CC and City Code.
- f. For countries outside CC 1, a range of numbers within an E.164 CC and City Code (e.g., a thousands group, hundreds group, or tens group within that CC and City Code).

**AUX-000620 [Optional: SC]** DISA also shall be able to independently specify the first and last numbers in a range without having to limit that range to a single Area Code, a single Office Code, a single thousands group, a single hundreds group, or a single tens group.

**AUX-000630 [Required: SC]** The SC shall allow DISA to configure the following within the set of commercial numbers for which Commercial Cost Avoidance is activated:

- a. Up to 20 individual commercial numbers.
- b. Up to 20 ranges of commercial numbers.

**AUX-000640 [Required: SC]** The SC shall support a configuration option to deactivate Commercial Cost Avoidance queries for all calls. Note that the scope of this setting is limited to interaction between the SC and the LRDB at the invocation of the Commercial Cost Avoidance feature when calls are made. It shall have no impact on the MRDB database updates performed by the SC for both Commercial Cost Avoidance and HR (as specified in [Section 3.3.4](#), SC to MRDB Interface: Database Updates for Commercial Cost Avoidance and Hybrid Routing).

### **3.3.3.1 Commercial Cost Avoidance Query From SC**

**AUX-000650 [Required: SC]** When the Commercial Cost Avoidance feature is activated for all commercial numbers, the SC shall make a Commercial Cost Avoidance query to the LRDB for each call that is placed to a commercial number. The SC shall not make Commercial Cost Avoidance queries for calls that are placed to PSTN service codes such as 911 (in the United States), 112 (in Europe), or 411 (in the United States).

**AUX-000660 [Required: SC]** When the Commercial Cost Avoidance feature is activated for a select set of commercial numbers, the SC shall make a Commercial Cost Avoidance query to the LRDB for each call that is placed to a commercial number within that DISA-configured set. The SC shall not make Commercial Cost Avoidance queries for calls that are placed to PSTN service codes such as 911 (in the United States), 112 (in Europe), or 411 (in the United States).

**AUX-000670 [Required: SC]** The SC shall query the LRDB on “99 dialed commercial PSTN number” and “98 dialed commercial PSTN number” call requests from SC end users. When the Database responds to this query with a DSN number that matches the dialed PSTN number, the SC shall route the call request over the appropriate IP (UC SIP) or TDM (T1.619A PRI) path using the DSN number returned by the Database. When the Database responds with a “Number Not Found” indication, the SC shall route the call request to the local TDM PSTN trunk group [PRI or Client Access Server (CAS)] on the SC’s MG, using the originally dialed commercial number.

**AUX-000680 [Required: SC]** The Commercial Cost Avoidance query that the SC sends to the LRDB shall contain the full internationally significant commercial called number (CC + Nationally Significant Number) for that call. The Commercial Cost Avoidance query shall be sent in the LDAPv3 Search Request message. This Search Request message shall contain the following fields in ASCII format:

- a. Base Object field containing an LDAP Distinguished Name containing the Domain Components “uc” and “mil” (dc=uc, dc=mil).
- b. Scope field containing the value “wholeSubtree.”
- c. Filter field containing the following:
  - (1) SIP Alias field containing the full commercial called number followed by “@uc.mil” (e.g., 17038821234@uc.mil).

**AUX-000690 [Required: LRDB]** The LRDB shall accept and process the Commercial Cost Avoidance queries from the SC that contain the full internationally-significant commercial called number.

**AUX-000700 [Required: LRDB]** The LRDB shall accept Commercial Cost Avoidance queries from the SC, in which this query contains the PSTN called number from the 99 dialed PSTN number or 98 dialed PSTN number call request from the SC end user. The LRDB shall be able to accept these queries for both continental United States (CONUS) “PSTN called numbers” [in

which the called number is from the 10-digit North American Numbering Plan (NANP)] and outside CONUS (OCONUS) (PSTN) called numbers (in which the called number is from either outside the NANP or within the NANP and located in Alaska, Hawaii, or the U.S. overseas territories).

**AUX-000710 [Required: LRDB]** The LRDB shall be capable of storing associations of PSTN numbers with 10-digit DSN numbers from the DSN numbering plan. The Database shall be capable of storing these associations for both CONUS and OCONUS PSTN numbers, as described in the previous requirement.

**AUX-000720 [Required: LRDB]** The LRDB shall store the following information in its database record for each commercial number:

- a. The full 10-digit DSN number matching that commercial number.
- b. The CCA-ID of the SC serving that DSN number (the “destination SC”).
- c. The CCA-ID of the primary SS serving the destination SC.
- d. The CCA-ID of the backup SS serving the destination SC.

NOTE: The CCA-IDs may be absent from the record in cases in which the DSN and commercial numbers in the record are associated with a DSN end user who is served by a DSN EO or PBX.

### ***3.3.3.2 Database Response When Commercial Number Is Found***

**AUX-000730 [Required: LRDB]** When the LRDB finds a database record that matches the commercial called number in the Commercial Cost Avoidance query, the LRDB shall return a Commercial Cost Avoidance response to the SC containing the following information, taken from that record:

- a. The full 10-digit DSN number matching the commercial number.

The LRDB shall send this Commercial Cost Avoidance response in the LDAPv3 Search Result Entry and Search Result Done messages.

**AUX-000740 [Required: LRDB]** The Search Result Entry message shall contain the following fields in ASCII format:

- a. Object Name field containing an LDAP Distinguished Name containing the following:
  - (1) User ID component containing the commercial number (e.g., UID=7038821234).
  - (2) Domain Components “uc” and “mil” (dc=uc, dc=mil).

The commercial number in the UID field may be represented in either national or international format, depending on the SC that uploads the number to the Database.

- b. Attributes field containing the following attributes:

- (1) User ID field containing the commercial number.
- (2) Object Class field containing “mobSLR.”
- (3) Subscriber Type field containing “asftswtch.”
- (4) SIP Alias field containing the full commercial called number, followed by “@uc.mil” (e.g., 17038821234@uc.mil).
- (5) SIP User Name field containing the UID (i.e., commercial number) followed by “@uc.mil” (e.g., 7038821234@uc.mil).
- (6) Directory Number field containing the full 10-digit DSN number.
- (7) LSCCAID field containing the CCA-ID of the destination SC serving the DSN number.
- (8) SSCCAID field containing the CCA-IDs of the primary SS and the backup SS serving the destination SC, separated by a comma.
- (9) Other attribute fields that the SC may ignore.

The commercial number in the UID field may be represented in either national or international format, depending on the SC that uploads the number to the Database.

**AUX-000750 [Required: LRDB]** The Search Result Done message shall contain the following field in ASCII format:

- Result Code field indicating “Success.”

### ***3.3.3.3 Database Response When Commercial Number Is Not Found***

**AUX-000760 [Required: LRDB]** When the LRDB finds no database record that matches the commercial number in the Commercial Cost Avoidance query, the LRDB shall return a Commercial Cost Avoidance response to the SC containing a Number Not Found indication.

**AUX-000770 [Required: LRDB]** The LRDB shall send this Commercial Cost Avoidance response in the LDAPv3 Search Result Done message. The Search Result Done message shall contain the following field in ASCII format:

- Result Code field indicating “Success.”

### ***3.3.3.4 SC Actions Based on Database Response***

**AUX-000780 [Required: SC]** In the Number Found case, the SC shall accept and process the Commercial Cost Avoidance response from the LRDB containing the DSN number that matches the commercial called number.

**AUX-000790 [Required: SC]** In the Number Not Found case, the SC shall also accept and process the Commercial Cost Avoidance response from the LRDB containing the “Number Not Found” indication.

**AUX-000800 [Required: SC]** In the Number Found case, the SC shall use the route specified in its internal routing tables for the digits of the returned DSN number to route the call request to one of the following:

- a. The primary or backup SS for that SC (by an outgoing UC SIP route).
- b. The DSN EO connected to the MG of that SC (by an outgoing T1.619a PRI route).
- c. A UC EI or MG served by that SC (if the returned DSN number identifies an EI on that SC or a subscriber located behind the MG of that SC).

**AUX-000810 [Required: SC]** In the Number Not Found case, the SC shall use the route specified in its internal routing tables for the original commercial called number to route the call request to the following:

- a. PSTN EO connected to the MG of that SC (by an outgoing commercial PRI or CAS trunk route).

**AUX-000820 [Required: SC]** If the SC determines that it has lost connectivity with the LRDB (e.g., because that Database has failed), then the SC shall apply the Failover to Secondary LRDB procedures, per the requirements in [Section 3.3.5.2.5](#), Failover Procedures.

**AUX-000830 [Required: SC]** On Commercial Cost Avoidance call requests that are rerouted to DSN numbers by the LRDB, the SC shall respond to SS signaling, indicating that the call attempt to the DSN number was rejected (i.e., a UC SIP 4xx, 5xx, or 6xx response to a UC SIP INVITE message) by overflowing these calls from the local UC SIP trunk group to the local TDM PSTN trunk group (PRI or CAS). The SC shall signal the originally dialed commercial number to the PSTN when overflowing this call to the PSTN trunk group.

**AUX-000840 [Required: SC]** On Commercial Cost Avoidance call requests that are rerouted to DSN numbers by the LRDB, the SC shall respond to DSN EO signaling indicating that the call attempt to the DSN number was rejected [i.e., an ISDN DISCONNECT, RELEASE, or RELEASE COMPLETE response to an Integrated Services Digital Network (ISDN) SETUP message] by overflowing these calls from the local T1.619a PRI trunk group to the local TDM PSTN trunk group (PRI or CAS). The SC shall signal the originally dialed commercial number to the PSTN when overflowing this call to the PSTN trunk group.

### **3.3.4 SC to MRDB Interface: Database Updates for Commercial Cost Avoidance and Hybrid Routing**

The requirements in this section apply to the SC and the MRDB. The MRDB can be located in a site that is physically remote from the SC site.

---

**AUX-000850 [Required: SC, MRDB]** The SC and the MRDB shall support the Routing Database update feature per the requirements in this section; in [Section 3.3.5](#), LRDB and MRDB; and in [Section 3.3.6](#), MRDB and LRDB Operations.

**AUX-000860 [Required: SC]** The SC shall support an interface to an MRDB to support Database updates for the Commercial Cost Avoidance and HR features.

**AUX-000870 [Required: MRDB]** The MRDB shall support an interface to the SC to support Database updates for the Commercial Cost Avoidance and HR features.

**AUX-000880 [Required: SC, MRDB]** The Database update interface between the SC and the MRDB shall be LDAPv3 over TLS over IP. On the SC, this LDAPv3 interface shall be compliant with RFC 4511 and all the LDAP technical specifications listed in Section 1 of RFC 4510. On the LRDB, see the LDAPv3 interface requirement ([AUX-001180](#)) in [Section 3.3.5.2.1](#), General Architecture, Protocols, and Interfaces.

**AUX-000890 [Required: SC, MRDB]** The encoding of the LDAPv3 messages and data schema used on the Database update interface between the SC and the MRDB shall follow the BER of ASN.1. On the SC, this encoding shall be consistent with Section 5.1, Protocol Encoding, of RFC 4511. On the LRDB, see the LDAPv3 interface requirement ([AUX-001180](#)) in [Section 3.3.5.2.1](#), General Architecture, Protocols, and Interfaces.

**AUX-000900 [Required: SC, MRDB]** The Database update interface between the SC and the MRDB shall be secured using TLS, consistent with the requirements for securing UC SIP messages using TLS in Section 4, Information Assurance. This security shall provide mutual authentication between the SC and the MRDB, message confidentiality for the Database updates, and message integrity for the Database updates.

**AUX-000910 [Required: SC, MRDB]** The Database update interface between the SC and the MRDB shall traverse the data firewalls (and not the SBC firewalls) at both the SC and MRDB sites.

**AUX-000920 [Required: SC, MRDB]** The Database update interface between the SC and the MRDB shall traverse the CE-Rs at both the SC and MRDB sites, using the DSCP for User Signaling traffic and the associated CE-R queues.

**AUX-000930 [Required: SC]** The Database update interface between the SC and the MRDB shall terminate on the Ethernet interface used for VVoIP signaling traffic at the SC, as described in Section 4, Information Assurance.

### ***3.3.4.1 LDAP Update Operations***

**AUX-000940** Before sending an Update operation (Add or Modify) to the Database, the SC shall send a Search operation to the Database using the Distinguished Name for the record to be updated (see [Section 3.3.5.2.3](#), Request Processing, for additional requirements). The Search operation shall be one of the following:

- The LDAP Search Request message for HR queries, specified in requirement [AUX-000310](#) in [Section 3.3.2.1](#), HR Query From SS (in this case, the Search Request message contains a Directory Number field containing the 10-digit DSN called number).
- The LDAP Search Request message for CCA queries, specified in requirement [AUX-000680](#) in [Section 3.3.3.1](#), Commercial Cost Avoidance Query From SC (in this case, the Search Request message contains a SIP Alias field containing the full commercial called number followed by “@uc.mil” [e.g., 17038821234@uc.mil]).
- If no matching record is found, then the SC shall proceed with the Update using an Add operation.
- If the matching record is found, and the CCA-ID of the requesting SC matches the SC CCA-ID in that record, then the SC shall proceed with the Update using a Modify operation.
- If the matching record is found, but the CCA-ID of the requesting SC does not match the SC CCA-ID in that record (or if there is no SC CCA-ID in that record), then the SC shall not perform the update and shall issue the necessary warnings or alerts to indicate that such an operation is not allowed until further intervention by network craftspeople or administrators.
  - For example, the network craftsperson at the requesting SC may contact another network craftsperson at the SC identified in the Database record, and ask the other craftsperson to delete the “old” SC’s record from the Routing Database so that the “new” SC’s record can be added.

#### 3.3.4.1.1 LDAP Add Operation

**AUX-000950 [Required: SC]** The SC shall send a Database update automatically to the MRDB whenever a new end user is added to the SC, unless the RTS Routing Database “opt out” indication has been made for that user.

**AUX-000960 [Required: SC]** The SC shall send this Database update automatically to the MRDB whenever the “opt out” indication for an existing user is changed from “on” to “off.”

(See [Section 3.3.4.2](#), RTS Routing Database “Opt Out” for SC End Users, for “opt out” related requirements.)

**AUX-000970 [Required: SC]** If the preceding Search request resulted in a No Record Found indication, then the SC shall perform the update using an LDAP Add operation. This operation shall contain the following:

- a. User ID (i.e., commercial number) for that end user.
- b. Full 10-digit DSN number for that end user.
- c. Full internationally significant commercial number for that end user.
- d. CCA-ID of the SC serving the DSN number.
- e. CCA-ID of the primary SS serving that SC.

- f. CCA-ID of the backup SS serving that SC.
- g. Indication that the end user, DSN number, and commercial number should be added to the Database.

The commercial number in the UID field may be represented in either national or international format, depending on the SC that uploads the number to the Database.

**AUX-000980 [Required: SC]** This Database update shall be sent in the LDAPv3 Add Request message. This Add Request message shall contain the following fields in ASCII format:

- a. An Entry field containing an LDAP Distinguished Name containing the following:
  - (1) A User ID component containing the commercial number (e.g., UID=7038821234).
  - (2) The Domain Components “uc” and “mil” (dc=uc, dc=mil).

The commercial number in the UID field may be represented in either national or international format, which will depend on the SC that uploads the number to the Database.

- b. An Attributes field containing the following attributes:
  - (1) A User ID field containing the commercial number.
  - (2) An Object Class field containing “mobSLR.”
  - (3) A Subscriber Type field containing “asftswtch.”
  - (4) A SIP Alias field containing the full commercial called number followed by “@uc.mil” (e.g., 17038821234@uc.mil).
  - (5) A Sip User Name field containing the UID (i.e., commercial number) followed by “@uc.mil” (e.g., 7038821234@uc.mil).
  - (6) A Directory Number field containing the full 10-digit DSN number.
  - (7) An LSCCAID field containing the CCA-ID of the destination SC serving the DSN number.
  - (8) An SSCCAID field containing the CCA-IDs of the primary SS and the backup SS serving the destination SC, separated by a comma.

The commercial number in the UID field may be represented in either national or international format, which will depend on the SC that uploads the number to the Database.

#### 3.3.4.1.2 *LDAP Modify Operation*

**AUX-000990 [Optional: SC]** The SC shall automatically send a Database update to the MRDB whenever an existing users’ number data (DSN and/or commercial) is modified at the SC, and the RTS Routing Database “opt out” indication for that user has not been set.

---

**AUX-0001000 [Conditional: SC]** If the SC sends this Database update, and the preceding Search request resulted in a “record found/matching SC CCA-ID” indication, then the SC shall perform the update using an LDAP Modify Replace operation. This operation shall contain the following:

- The User ID (i.e., commercial number) for that end user.
- An indication of the attribute names to be modified and the new values to be inserted.
- The commercial number in the UID field may be represented in either national or international format (which will depend on the SC that uploads the number to the Database).

**AUX-001000 [Conditional: SC]** If the SC sends this Database update, then the update shall be sent in the LDAPv3 Modify Request message containing a Replace operation. This Modify Request message shall contain the following fields in ASCII format:

- a. An Entry field containing an LDAP Distinguished Name containing the following:
  - (1) A User ID component containing the commercial number (e.g., UID=7038821234).
  - (2) The Domain Components “uc” and “mil” (dc=uc, dc=mil).
- b. The intended operation: replace.
- c. An Attributes field containing the following:
  - (1) One or more Attribute names (the ones to be modified).
  - (2) One or more Attribute values (the new values to replace the existing value).

The commercial number in the UID field may be represented in either national or international format (which will depend on the SC that uploads the number to the Database).

When adding a new SC user’s data (DSN and commercial numbers) to the MRDB, the SC may use a sequence of LDAP Add and Modify messages to add the data, instead of using a single LDAP Add Message to add the data. In this case, the following requirement applies:

**AUX-001010 [Conditional: SC]** If the SC uses a sequence of LDAP messages to add a new SC user’s data to the MRDB, then the SC shall be able to add the new SC user’s data using at least one of the following methods:

- A single Add operation containing User ID and CCA data (UID, SIP UserName, SIP Alias, DirNumber) and HR data (LSCCAID, SSCCAID).
- An Add operation containing User ID and CCA data (UID, SIP UserName, SIP Alias, DirNumber), followed by a Modify operation containing HR data (LSCCAID, SSCCAID).
- An Add operation containing User ID data (UID, SIP UserName ), followed by a Modify operation containing CCA data (SIP Alias, DirNumber) and HR data (LSCCAID, SSCCAID).

### 3.3.4.1.3 LDAP Delete Operation

**AUX-001020 [Required: SC]** The SC shall automatically send a Database update to the MRDB whenever an existing end user is deleted from the SC, unless the RTS Routing Database “opt out” indication has been made for that user.

**AUX-001030 [Required: SC]** The SC shall send a Database update automatically to the MRDB whenever the “opt out” indication for an existing user is changed from “off” to “on.”

**AUX-001040 [Required: SC]** If the preceding Search request resulted in a “record found/matching SC CCA-ID” indication, then the SC shall perform the update using an LDAP Delete operation. This operation shall contain the following:

- a. The commercial number (i.e., User ID) for that end user.
- b. An indication that the end user, DSN number, and commercial number should be deleted from the Database.

**AUX-001050 [Required: SC]** This Database Update shall be sent in the LDAPv3 Delete Request message. This Delete Request message shall contain the following field in ASCII format:

- a. An LDAP Distinguished Name containing the following:
  - (1) A User ID component containing the commercial number (e.g., UID=7038821234).
  - (2) The Domain Components “uc” and “mil” (dc=uc, dc=mil).

**AUX-001060 [Optional: SC]** If the Search response preceding the Delete operation indicated that there was no SC CCA-ID in the record, or indicated that the SC CCA-ID in the record did not match the CCA-ID of the requesting SC, then the SC shall not send the LDAP Delete operation, but shall still delete the end user data from the SC. The SC shall issue the appropriate alerts or notification to the network craftspeople/administrators in this case, as manual intervention will be necessary to complete this operation at the Database itself.

For example, the network craftsman at the requesting SC may contact the network craftsman at the MRDB, and notify the Database craftsman that his or her request to delete the SC’s record failed. Then the Database craftsman can check the Database for all Database records that contain the SC’s deleted number, and remove any of those records that are redundant or out-of-date.

### 3.3.4.1.4 LDAP Confirmation Responses

**AUX-001070 [Required: MRDB]** The MRDB shall accept and process the Database updates from the SC for added end users, modified end users, and deleted end users, as listed in the previous requirements. In addition, the MRDB should return a confirmation response to the SC whenever a new end user is added to the Database, an existing user’s data is modified in the Database, and an existing end user is deleted from the Database.

---

**AUX-001080 [Required: MRDB]** In the “added end user” case, the MRDB shall send this confirmation response to the SC in the LDAPv3 Add Response message. The Add Response message shall contain the Result Code field in ASCII format indicating “Success.”

**AUX-001090 [Required: MRDB]** In the “modified end user data” case, if all the modifications requested to the record were successful, the MRDB shall send this confirmation response to the SC in the LDAPv3 Modify Response message. The Modify Response message shall contain the Result Code field in ASCII format indicating “Success.”

**AUX-001100 [Required: MRDB]** In the “modified end user data” case, if any modifications requested to the record were not successful, the MRDB:

- a. Shall not perform any other modification that was requested in that message.
- b. Shall send a rejection response to the SC in the LDAPv3 Modify Response message indicating the reason for failure. The Modify Response message shall contain the Result Code field in ASCII format indicating the reason for the failure (e.g., noSuchAttribute, invalidAttributeSyntax).

**AUX-001110 [Required: MRDB]** In the “deleted end user” case, the MRDB shall send this confirmation response to the SC in the LDAPv3 Delete Response message. The Delete Response message shall contain the Result Code field in ASCII format indicating “Success.”

#### *3.3.4.1.5 Multiple Database Update Interfaces to Multiple SCs*

**AUX-001120 [Required: MRDB]** The MRDB shall be capable of maintaining multiple Database update interfaces to different SCs at the same time. Each individual Database update interface shall support the requirements in this document for the protocols, data schemas, and security mechanisms used between an individual SC and the MRDB. The MRDB shall support at least 40 interfaces with multiple SCs, simultaneously.

**AUX-001130 [Optional: MRDB]** The MRDB shall also be capable of supporting 80 interfaces with multiple SCs, simultaneously.

#### *3.3.4.2 RTS Routing Database “Opt Out” for SC End Users*

It is desired that an entry in the RTS Routing Database not be made for certain UC SC end users. To support this goal, an “opt out” indication is required, as follows:

**AUX-001140 [Required: SC]** The user information maintained by an SC for an EI provisioned on that SC shall include an indication to exclude an entry for that user from the RTS Routing Database. It shall be possible to set or change this indication for an end user in the same way, and at the same time, that any other provisioning information for an end user can be set or changed.

**AUX-001150 [Required: SC]** The default state for this setting shall be “off”. That is, in the absence of explicitly making this indication, this setting should remain off, and an entry for that end user shall be included in the RTS Routing Database.

**AUX-001160 [Required: SC]** The SC shall consider the setting of this indication when performing an LDAP Add, Modify or Delete operation with the MRDB, as specified above in [Section 3.3.4.1](#), LDAP Update Operations.

**AUX-001170 [Required: SC]** The changing of this indication from “on” to “off” shall trigger an LDAP Add operation from the SC to the MRDB, as specified above in [Section 3.3.4.1.1](#), LDAP Add Operation.

**AUX-001180 [Required: SC]** The changing of this indication from “off” to “on” shall trigger an LDAP Delete operation from the SC to the MRDB, as specified above in [Section 3.3.4.1.3](#), LDAP Delete Operation.

### **3.3.5 LRDB and MRDB**

#### ***3.3.5.1 Overview and Terminology***

Each theater is expected to have two or more LRDBs handling the LDAPv3 Search operations (Commercial Cost Avoidance queries and HR queries) originating from the SCs and SSs in that theater.

The LRDB(s) will be responsible for (1) performing the Search requests from the SSs (for HR queries) and Search requests from the SCs (for Commercial Cost Avoidance queries) within the local theater, and (2) maintaining synchronization with the Primary MRDB.

One predetermined theater, CONUS (to be referred to as the primary theater), will have a Primary MRDB that will be responsible for (1) receiving Update operations (DSN and commercial number updates) from all SCs across all theaters, including its own, (2) performing the synchronization updates to all LRDBs in all theaters, and (3) performing synchronization with its Backup MRDB in that primary theater.

The requirements in this section follow the architecture described in [Figure 3.3-2](#), Reference Architecture for LRDBs, and [Figure 3.3-3](#), Reference Architecture for MRDBs.

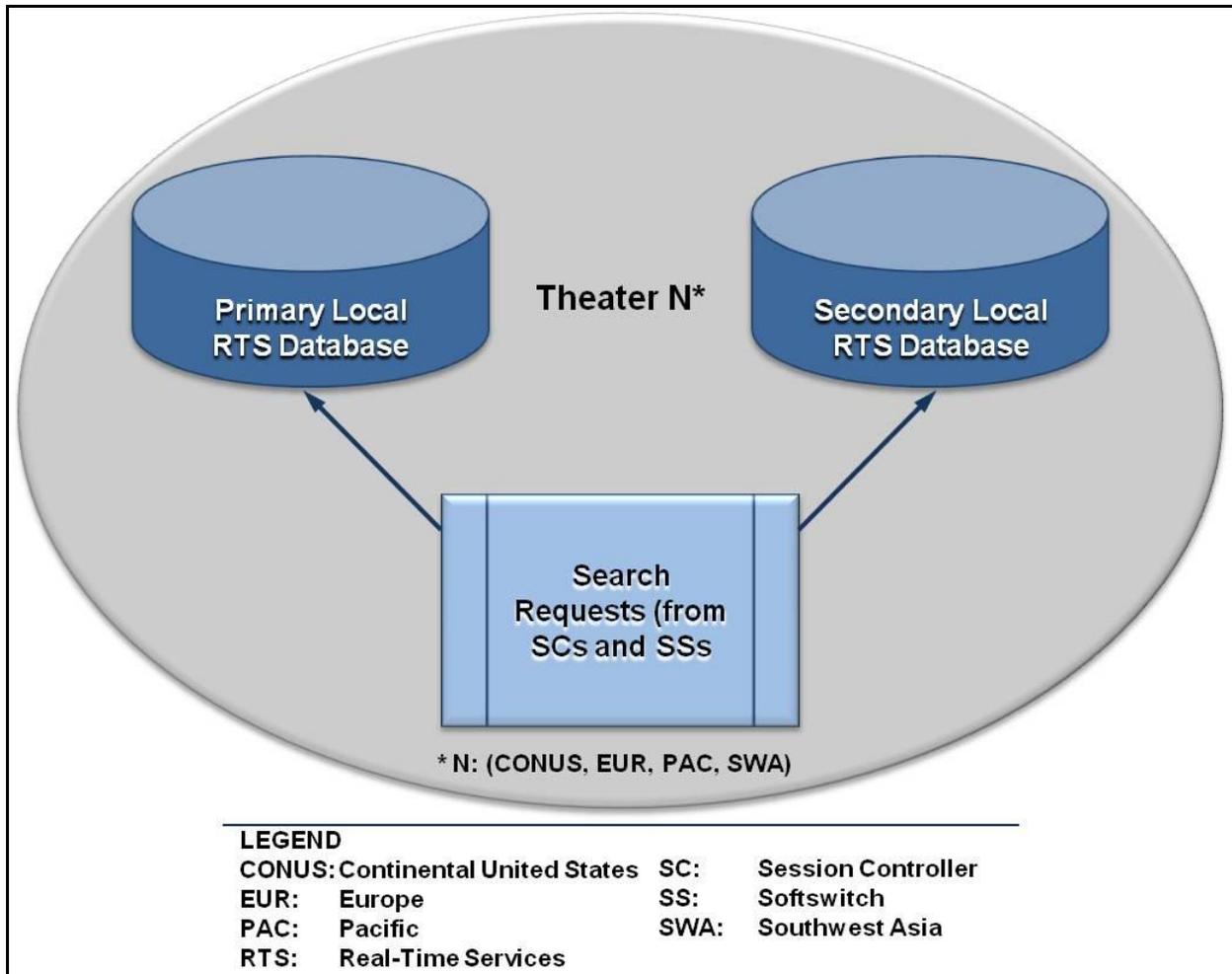
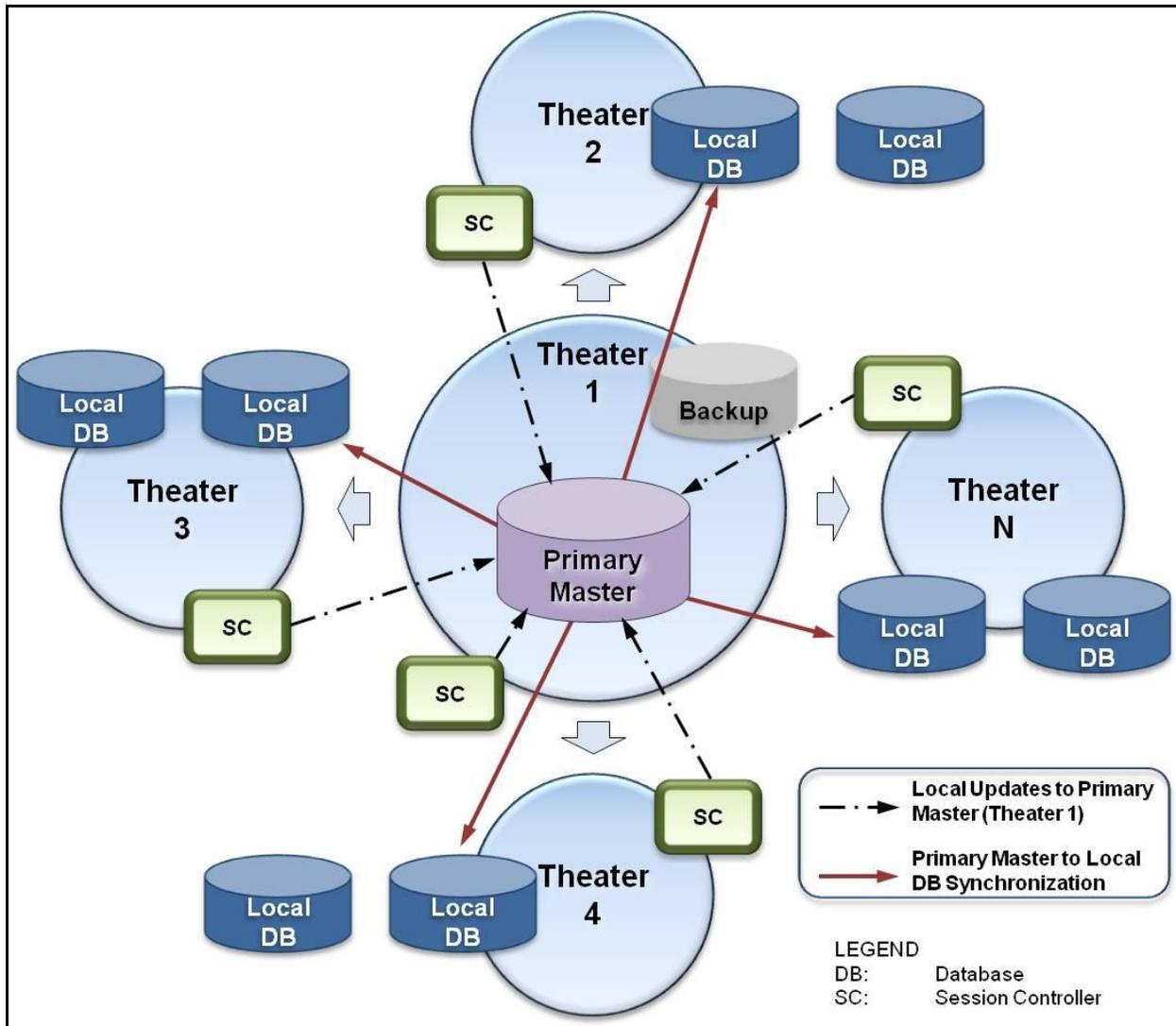


Figure 3.3-2. Reference Architecture for LRDBs



**Figure 3.3-3. Reference Architecture for MRDBs**

In the following requirements, “bulk update” refers to a method where number records are updated at the MRDB “in bulk,” rather than updated individually using LDAP Write operations (like Add, Modify, and Delete). The source of the data for the “bulk updates” may be a set of SCs containing number records, or it may be another database that is a copy of the MRDB (e.g., the Backup MRDB).

Bulk updates may be used during the initial provisioning of the MRDB (e.g., population of the MRDB from multiple SCs that already contain number records) or during full reloads of the Database (e.g., population of the MRDB from the Backup MRDB, after a loss of data at the MRDB). An example of a “bulk update” technique is transfer of LDIF files from the SCs to the MRDB, using e-mail messages or File Transfer Protocol (FTP) sessions to carry the LDIF files from the sources to the destination. LDIF file transfer implies a manual export of LDIF data at the source end (SCs or Backup MRDB) and a manual import of LDIF data at the receiving end

---

(MRDB). Other bulk update techniques can also be used, if supported by the MRDB vendor and the SC vendors.

### **3.3.5.2 Routing Database**

This section contains requirements for the LRDB and MRDB.

#### **3.3.5.2.1 General Architecture, Protocols, and Interfaces**

**AUX-001190 [Required: LRDB, MRDB]** The LRDB and MRDB shall support the following LDAPv3 RFCs:

RFC 2251, RFC 2252, RFC 2253, RFC 2254, RFC 2255, RFC 2256, RFC 2829, RFC 2830.

**AUX-001200 [Required: LRDB]** Each LRDB shall be implemented as an independent, stand-alone replica of the data in the MRDB, where that data is not distributed among several physical LRDBs.

**AUX-001210 [Required: MRDB]** Each MRDB shall be implemented as an independent, stand-alone Database, where the Database data is not distributed among several physical Databases.

#### **3.3.5.2.2 Capacity and Record Structure**

**AUX-001220 [Required: LRDB, MRDB]** The LRDB and MRDB shall be able to store up to 8 million records, where each record ranges in length from 500–2,000 characters.

It is expected that each database will grow over time, from an initial size of roughly 10,000 small records to a target size of 8 million large records. Therefore, the following requirements and objectives apply.

**AUX-001230 [Required: LRDB, MRDB]** The LRDB and MRDB shall support an initial capacity of 10,000 records.

**AUX-001240 [Required: LRDB, MRDB]** The LRDB and MRDB shall support a full capacity of 8 million records, while adhering to the same performance and availability requirements listed in this document.

**AUX-001250 [Required: LRDB, MRDB]** The LRDB and MRDB shall support the standard LDAP Directory Information Tree (DIT) format for their entries. The required attributes in each entry shall be as shown in [Table 3.3-1](#), LDAP DIT Attribute Formats.

**Table 3.3-1. LDAP DIT Attribute Formats**

ATTRIBUTE	DESCRIPTION	EXAMPLE
dn	Alphanumeric ASCII string: Distinguished Name; uid containing the commercial number, followed by dc=uc, dc=mil	uid=7038821234, dc=uc, dc=mil
uid	Alphanumeric ASCII string: Unique user ID; commercial number	7038821234
objectClass	Alphanumeric ASCII string: value is "mobSLR" for Routing Database	mobSLR
subscriberType	Alphanumeric ASCII string: value is "asftswtch" for Routing Database	Asftswtch
SIP Alias	Alphanumeric ASCII string; Full internationally significant commercial number matching the DSN number [PSTN number@uc.mil]	17038821234@uc.mil (also OCONUS commercial numbers are allowed)
SIP UserName	Alphanumeric ASCII string; UID (i.e., commercial number matching the DSN number) followed by "@uc.mil"	7038821234@uc.mil (also OCONUS commercial numbers are allowed)
dirNumber	Alphanumeric ASCII string; 10-digit DSN telephone number	3123811234 (DISA Skyline example)
LSCCAID	Alphanumeric ASCII string; CCA-ID of the SC serving the DSN number	ScottSC.uc.mil
SSCAID	Alphanumeric ASCII string; CCA-ID of the Primary and Backup SAs serving this SC	ScottSS.uc.mil, AndrewsSS.uc.mil
serverHome	null	
isMobile	false	
LEGEND		
ASCII: American Standard Code for Information Interchange		
SC: Session Controller		
SS: Softswitch		
CCA: Call Connection Agent		
OCONUS: Outside the Continental United States		
DISA: Defense Information Systems Agency		
PSTN: Public Switched Telephone Network		
DSN: Defense Switched Network		
UID: User Identifier		
ID: Identification		

### 3.3.5.2.3 Request Processing

The SCs and SAs are expected to direct their LDAP Search requests to the LRDBs for call processing purposes. The SC is expected to direct its update requests to the MRDB; it could add a new entry, delete an existing entry, or modify values of attributes in an existing entry. Adding new attributes that are not predefined in the schema is not allowed.

For the update operations, the SC must check whether the record exists in the MRDB before it inserts or deletes any records or applies any modifications.

**AUX-001260 [Required: SC]** The SC shall formulate its updates to the MRDB (or Backup MRDB) in the following sequence:

- a. Send a Search operation on the record to be updated, requesting the entire entry.

The Search operation can be one of the following:

- The LDAP Search Request message for HR queries, specified in requirement [AUX-000310](#) in [Section 3.3.2.1](#), HR Query From SS.
- The LDAP Search Request message for CCA queries, specified in requirement [AUX-000680](#) in [Section 3.3.3.1](#), Commercial Cost Avoidance Query From SC.

- b. If the entry is found and returned, then the SC shall send the intended Update operation (Delete or Modify).

- c. If the entry is not found, then the SC shall do one of the following:

- (1) Perform the intended Add operation.

- (2) Abandon the Update operation.

The requesting SC will not be allowed to perform updates on a record in which the SC CCA-ID in the record does not match its own SC CCA-ID. [Section 3.3.4.1](#), LDAP Update Operations, contains more detailed requirements.

#### 3.3.5.2.3.1 Client Time-Out

If an LDAP operation does not return results within a preset time, then the LDAP client (SC or SS) should be able to terminate (time-out) the session in a reasonable amount of time.

**AUX-001270 [Required: SC, SS]** The SC or SS shall allow the setting of an LDAP client time-out interval between 1–5 seconds, adjusted in increments of 1 second [default 2 seconds].

Setting a time-out interval helps terminate an otherwise indefinite “hang” situation.

**AUX-001280 [Required: SC, SS]** The SC or SS shall terminate the pending request (Search, Add, Delete, or Modify) via an Abandon operation, if the time-out interval expires and no response was received from the database.

#### 3.3.5.2.3.2 Bind over TLS

The LDAP standards allow for different methods of authentication:

- Anonymous access is obtained by providing no name and no password in the LDAP Bind operation.

- Unauthenticated access is obtained by providing a name but no password in the LDAP Bind operation.
- Authenticated access is obtained by providing a valid name and password in the LDAP Bind operation. With this method, the name and password may still be transported in the clear and be unprotected.

For UC, confidentiality and integrity protection are required. Transport Layer Security (TLS) (defined in RFC 5246) provides confidentiality and integrity protection. Available implementations of LDAP, such as OpenLDAP, support TLS. The name of the standard LDAP operation for initiating TLS/Secure Socket Layer (SSL) is startTLS. Upon successful completion of this LDAP operation, SSL/TLS is initiated between the LDAP Client (e.g., the SC or SS) and the LDAP Server (e.g., the LRDB or the MRDB).

All DBs and clients (SCs and SSs) are required to have valid X.509 certificates to be able to use the TLS framework. With TLS in use, none of the LDAP connections would be opened in the clear.

**AUX-001290 [Required: SC, SS]** All connections between the SC or SS to any of the DBs shall use TLS by default.

**AUX-001300 [Required: SC, SS]** An Anonymous or Unauthenticated Bind request shall be disallowed by default on all connections from the SC and SS to any of the DBs.

**AUX-001310 [Required: MRDB, Backup MRDB, LRDB]** The MRDB, Backup MRDB, and LRDB shall not accept or process an Anonymous or Unauthenticated Bind request.

The time that a TLS connection stays open is to be determined by the network administrator.

**AUX-001320 [Required: MRDB, Backup MRDB, LRDB]** The MRDB, Backup MRDB, and LRDB shall allow the setting of an Idle Time-out Timer  $T_{idle}$  (range: 5–30 minutes; increments of 5 minutes; default 10 minutes). When  $T_{idle}$  expires, the Database shall shut down the TLS connection.

#### 3.3.5.2.3.3 LRDB Request Processing

**AUX-001330 [Required: LRDB]** The LRDB shall be able to recognize and perform the following LDAP operations originating from SCs and SSs for Commercial Cost Avoidance and HR queries, respectively:

- a. Bind Request and Response.
- b. Unbind Request.
- c. Search Request and Response.
- d. Abandon Request.

---

The LRDB is not required to support Update (LDAP Add, Modify, or Delete) requests from the SCs or SSs. However, the LRDB is expected to support these Update requests for purposes of data population and provisioning through administrative LDAP interfaces, per the following requirement.

**AUX-001340 [Required: LRDB]** The LRDB shall be able to recognize and perform the following LDAP operations when received from the MRDB, a Database craftsperson station, or the Database Administrator (DBA) over an administrative LDAP interface:

- a. Bind request and response.
- b. Unbind request.
- c. Search request and response.
- d. Add request and response.
- e. Delete request and response.
- f. Modify request and response.
- g. Abandon request.

**AUX-001350 [Required: LRDB]** When the LRDB successfully locates the entry for an LDAP Search operation, it shall generate and return the appropriate LDAP response message, containing, at a minimum, the following:

- a. The dirNumber (DSN telephone number), LSCCAID, and SSCCAID values, for responses to HR queries.
- b. The dirNumber (DSN telephone number), SIP Alias (commercial number), and SIP UserName (commercial number) values, for responses Commercial Cost Avoidance queries.

**AUX-001360 [Required: LRDB]** When the LRDB fails to locate the entry for a Search operation, it shall generate and return the appropriate LDAP Result Code, which includes but is not limited to the following:

- a. Result Code 0 (indicating “Success”), with no arguments.
- b. Result Code 16, LDAP\_NO\_SUCH\_ATTRIBUTE (indicating that the specified attribute does not exist in the entry).
- c. Result Code 32, LDAP\_NO\_SUCH\_OBJECT (indicating that the Database server cannot find the entry specified in the request).

It is expected that the SCs and SSs will process the different LDAP Result Codes based on the logic for the type of call (Commercial Cost Avoidance or HR). It is expected that, if no Database entry was found or if timeouts occur at either side (the database side or the client side), or if other LDAP errors are encountered, then the Commercial Cost Avoidance logic will route the call to the commercial number. In the HR logic, if no

Database entry is found, or if timeouts occur, then the call is either (a) processed by internal SS routing tables or (b) returned to an MFS and subsequently to an End Office for call completion.

#### 3.3.5.2.3.4 MRDB Request Processing

The MRDB is required to support Update (LDAP Add, Modify, and Delete) requests from all SCs in all theaters. The MRDB is not intended to serve real-time Query requests (LDAP Searches) from SCs and SSs for HR and Commercial Cost Avoidance purposes. However, occasionally a Database craftsperson station, a DBA station, or provisioning logic in the SC or SS may launch an LDAP Search request to the MRDB to determine the existence of specific records there. As a result, the MRDB is expected to support those LDAP Search requests.

**AUX-001370 [Required: MRDB]** The MRDB shall be able to recognize and perform the following LDAP operations:

- a. Bind request and response.
- b. Unbind request.
- c. Search request and response.
- d. Add request and response.
- e. Delete request and response.
- f. Modify request and response.
- g. Abandon request.

**AUX-001380 [Required: MRDB]** When the MRDB successfully locates the entry for an LDAP Search operation, it shall generate and return the appropriate LDAP response message for that message, containing the dirNumber (DSN telephone number), LSCCAID, SSCCAID, SIP Alias (Commercial number), and SIP UserName (Commercial number) values.

**AUX-001390 [Required: MRDB]** When the MRDB fails to locate the entry for a Search operation, it shall generate and return the appropriate LDAP Result Code. Examples follow:

- a. Result Code 0 (indicating “Success”), with no arguments.
- b. Result Code 16 (indicating “Attribute not found”).
- c. Result Code 32 (indicating “Object not found”).

These Search requests are not used for routing calls (Commercial Cost Avoidance or HR); instead, they are used to verify the existence of an MRDB record. It is therefore expected that, after the Search requests are completed, SCs will use subsequent logic to launch applicable Update requests to the MRDB. For example, if no Database entry was found for a DSN number, then the SC might initiate an Add operation for that number. Conversely, if a Database entry was found for that DSN number, then the SC would not

initiate an Add operation for that number, but might instead initiate a Delete or Modify operation for that number. If other LDAP errors were encountered, then the SC LDAP logic could (a) reattempt the Update operation (Add, Delete, Modify) again for that number or (b) issue an error report, indicating multiple unsuccessful Database attempts, that requires administrative intervention.

#### 3.3.5.2.4 *Performance and Availability*

Performance characteristics of a database, such as query throughput and bulk update times, are highly dependent on the design and configuration of the hardware for that database, including but not limited to the following:

- Processor speed.
- LDAP cache (memory) size.
- Number and size of hard disks used.

The performance requirements for the LRDB and MRDB in this document can be met with various hardware configurations (e.g., processors, cache, and hard disks), as indicated previously, through optimization techniques, and other vendor-specific guidelines or products. Specifically, the MRDB needs to be optimized for processing LDAP Update requests, while the LRDB needs to be optimized for processing LDAP Search requests.

Each SC and SS is expected to direct its Search requests to a pre-specified LRDB in its theater. The load-sharing architecture for LRDBs will be determined by the DISA network engineers in each theater, based on the projected traffic volume originating from each SC or SS in that theater (i.e., the number of Search requests directed to each LRDB will vary between LRDBs, and will vary from one theater to another).

The LRDBs in each theater are expected to store a very recent image of the data stored in the MRDB. These copies should be almost identical in content, based on the time that each LRDB received its latest synchronization update from the MRDB. Creating and using these “local” copies, the LRDB in each theater should also reduce round-trip LDAP signaling latency for the SCs and SSs, and should make the routing data available to them in a reasonable amount of time.

In addition, to ensure data availability and redundancy, the architecture requires support for both a Primary MRDB and a Backup MRDB (where the Backup MRDB contains a complete copy of the Primary MRDB). While the MRDB primarily focuses on LDAP Updates, the following availability requirements apply to all of the LDAP requests (both Searches and Updates).

**AUX-001400 [Required: LRDB, MRDB]** Under normal operating conditions (i.e., there is no Database overload or scheduled downtime for Database maintenance), the LRDB and MRDB shall process 99.99 percent of all LDAP requests received (i.e., Bind, Search, Add, Modify, Delete).

**AUX-001410 [Required: LRDB]** The unavailability time for each LRDB shall not exceed 0.01 percent of 1 year (translating into 1 hour per year; approximately 5 minutes per month). The unavailable time shall apply only to failure situations and does not comprise preventive maintenance or scheduled upgrade times.

It is expected that, when one of the LRDBs in the theater is unavailable, the other LRDB(s) in the theater will be available. It is not expected that all the LRDBs in a given theater will be unavailable at the same time.

**AUX-001420 [Required: MRDB, Backup MRDB]** The unavailability time for each MRDB and Backup MRDBs shall not exceed 0.01 percent of 1 year, translating into 1 hour per year; approximately 5 minutes per month. The unavailable time applies only to failure situations and does not comprise preventive maintenance or scheduled upgrade times.

**AUX-001430 [Required: LRDB, MRDB, Backup MRDB]** The LRDB, MRDB, and Backup MRDB shall each support a minimum of 2000 LDAP Search operations per second.

**AUX-001440 [Required: LRDB, MRDB, Backup MRDB]** The LRDB, MRDB, and Backup MRDB shall each support a minimum of 200 LDAP Update (Add, Delete, and Modify) operations per second under normal operation. (Bulk updates during the initial provisioning of the database and bulk updates during full reloads of the database are not considered normal operation.)

**AUX-001450 [Required: LRDB, MRDB, Backup MRDB]** When the SC sends an LDAP Update operation to the Primary MRDB, the Primary MRDB shall relay this update to a pre-specified group of databases (configured in the Primary MRDB), including the Backup MRDB and multiple LRDBs, immediately. The total time from the initialization of a given LDAP Update by the SC, propagation of the data, and receipt of the updates in the pre-specified group of DBs shall not exceed 5 minutes.

The Primary and Backup MRDBs also support synchronization procedures of partial and full database content, with each other and with the local DBs. These procedures are discussed in [Section 3.3.5.2.7](#), Synchronization Between Primary and Backup MRDBs, and [Section 3.3.5.2.8](#), Synchronization Between LRDB and MRDB.

In both the HR and CCA applications, the Search requests serve real-time UC call setup. Therefore, the response times are important.

**AUX-001460 [Required: LRDB, MRDB, Backup MRDB]** The LRDB, MRDB, and Backup MRDB's processing time for an LDAP Bind request shall not exceed 2 milliseconds (ms). This time excludes the round-trip network delays as the Bind requests from (and Bind responses to) the SCs and SSs transit the Defense Information Systems Network (DISN).

**AUX-001470 [Required: SC, SS, SS, LRDB, MRDB, Backup MRDB]** The total LDAP Bind connect time, including all the following time intervals plus DISN transit time, shall not exceed 20 ms:

- a. Initializing the LDAP port at the SC or SS.
- b. Preparing the Bind request at the SC or SS.
- c. Processing the LDAP Bind request at the Database (authenticating the LDAP Username and password).
- d. Preparing the Bind result at the LRDB, MRDB, or Backup MRDB.
- e. Processing the Bind result at the SC, SS, or SS.

**AUX-001480 [Required: LRDB, MRDB, Backup MRDB]** The LRDB, MRDB, and Backup MRDB's processing time for an LDAP Search request shall not exceed 10 ms. This time excludes the round-trip network delays as the Search requests from (and Search responses to) SCs and SSs transit the DISN.

**AUX-001490 [Required: LRDB, MRDB, Backup MRDB]** The LRDB, MRDB, and Backup MRDB's processing time for an LDAP Update request (Add, Modify, or Delete) shall not exceed 100 ms. This time excludes the round-trip network delays as the Update requests from (and Update responses to) SCs transit the DISN.

#### 3.3.5.2.4.1 LDAP Directory Considerations

Indexing of LDAP servers reduces search times by facilitating the location of the entry without having to check every single entry for a match. Index tuning is a recommended tool that a database vendor could provide to improve performance.

Other factors that affect the performance of the database server and the processing time of a query include (a) the layout of the DIT and (b) the complexity of the Search request. The LDAP applications will perform better if simple operations are used as much as possible. Therefore, Search requests should ask only for the attributes needed and not retrieve all attributes from every entry, because doing so would slow the database processing significantly.

Some ideas for improving LDAP performance include the following practices:

- Flat directory trees yield quicker response times than deep ones:
  - One-level searches are recommended.
  - Simple search filters (exact filters) should be used more frequently than wildcard filters.

**AUX-001500 [Optional: LRDB, MRDB, Backup MRDB]** In the design of the LRDB and MRDB DIT, frequently accessed Database entries shall be placed closer to the root of the dc=uc tree to help speed access to the different Database entries and their attributes.

**AUX-001510 [Optional: SC, SS]** SC and SS Search requests launched to the LRDB, MRDB, and Backup MRDB shall be optimized to search only for the necessary CCA and HR data and to reduce the use of wildcard filters that return multiple Database entries.

#### 3.3.5.2.4.2 Data Caching

One means of boosting query throughput is to implement a memory cache for frequently retrieved data, since typically accessing the memory cache is faster than accessing a hard disk. Caches can be implemented at the client site (in this case at the SC or SS) or at the server (Database) site.

**AUX-001520 [Conditional: SC, SS]** When Database response caching is supported, the SC and SS shall implement storage buffers that are capable of supporting LDAP entry caches. This capability shall be configurable; the caching or buffering option shall be turned on or off as needed.

**AUX-001530 [Conditional: SC, SS]** When Database response caching is supported, the SC and SS shall be able to support caching at a minimum of 300 entries/records. The maximum amount of record storage (the cache size) shall be settable by DISA, based on Database utilization trends. The required memory cache size shall be provisioned accordingly.

**AUX-001540 [Conditional: SC, SS]** When Database response caching is supported, if the entry is not found in the cache, then the SC or SS shall route the Search request to the LRDB.

**AUX-001550 [Conditional: SC, SS]** If Database response caching is supported, then the cache retention period shall be settable in increments of 30 minutes and shall not exceed 48 hours. When the cache retention period expires, the contents of the cache shall be cleared/purged.

The term “cache retention period” applies to individual entries in the cache, and not to the set of cache entries as a whole. For example, if the cache retention period is 30 minutes and an individual cache entry has been in the cache for 30 minutes, then the individual cache entry should be purged. This does not mean that the whole set of cache entries should be purged every 30 minutes.

While caching offers the advantage of improving throughput, the common disadvantage is the possibility of aged data. Therefore, the network administrators, with the assistance of the vendor, should inspect the cache periodically to determine the ideal expiration time, and tune the contents of the cache accordingly.

#### 3.3.5.2.5 Failover Procedures

Under normal operations, the SC communicates the LDAP Updates directly to the Primary MRDB. The Backup MRDB is synchronized with the Primary MRDB periodically to be able to stand in for the Primary MRDB when the latter experiences downtime.

The SCs will maintain communication with both the Primary and Backup MRDBs via periodic “keep-alive” messages. Lack of response from an MRDB will indicate to the SC that the MRDB is potentially experiencing a failure. Procedures are described in this section’s requirements to help (1) minimize loss of update information intended for the MRDB, (2) automatically redirect the Update requests to an available MRDB, and (3) alert network personnel of the failed MRDB.

After the Primary MRDB has been repaired, the MRDB DBA will be able to initiate transfer of the downtime SC Update transactions from the Backup MRDB to the Primary MRDB. The administrator should ensure that the Primary MRDB is not returned to service (i.e., not re-connected to the SCs that it serves) until its data records are updated. Once the Primary MRDB is returned to service, each SC craftsperson should be able to reconnect their SC to that MRDB.

Each SC should automatically redirect its DB Update traffic (LDAP Add, Modify, and Delete messages) from the Primary MRDB to the Backup MRDB when the Primary MRDB fails. But the restoration of SC “DB Update” traffic from the Backup MRDB to the Primary MRDB requires SC craftsperson involvement, since the restoration of the Primary MRDB requires DBA involvement.

The SCs and SSs will maintain communication with Primary and Secondary LRDBs via periodic keep-alive messages. Lack of response from an LRDB will indicate to the SC or SS that the LRDB is potentially experiencing a failure. A set of procedures are described in this section’s requirements to help (1) realize the cost savings of the Commercial Cost Avoidance feature, (2) reduce call setup delays for the HR feature, and (3) automatically redirect the Search requests to an available Database for prompt processing.

NOTE: The SCs exchange keep-alive messages with all DBs (MRDB, Backup MRDB, and LRDB). The SSs exchange keep-alive messages with the LRDBs only.

**AUX-001560 [Required: SC, SS]** The SC or SS shall use keep-alive messages to verify that the MRDB (or the Backup MRDB) and the LRDBs are available.

- a. The frequency of the keep-alive messages shall be settable (Timer Ta) by the SC and SS administrators based on traffic volumes, with a default of Ta= 5 minutes.
- b. The value of Ta shall range from 0–30 minutes and shall be settable in increments of 5 minutes.

**AUX-001570 [Required: SC, SS]** The keep-alive messages sent from the SC or SS to the LRDB or MRDB shall consist of the following sequence:

- a. Bind request. (If a previous Bind request is still in effect and has not expired, then a new Bind request shall not be sent.)
- b. Search request on a predetermined LDAP Distinguished Name (DN).

When a new Bind request is sent, upon receiving a successful Bind response with resultCode = 0, the SC or SS shall issue a Search request for a predetermined LDAP DN.

When a previous Bind request is still in effect and has not expired, the SC or SS shall issue a Search request for a predetermined LDAP DN.

It is expected that the LDAP DN selected by the SC/SS administrator for these preset keep-alive messages will always be populated in each LRDB and MRDB, to avoid keep-alive failure errors.

When the SC or SS receives a Search response message indicating that the entry is found, the keep-alive message is considered successful, and the SC or SS shall complete the operation and shall reset Ta.

The SC or SS shall also reset Ta after each successful LDAP Request/Response exchange (Search, Add, Modify, or Delete) between the SC or SS and the target LRDB or MRDB.

**AUX-001580 [Required: SC, SS]** The SC or SS shall keep track of the last status (active or inactive) for each LRDB or MRDB to which it sent a keep-alive message. The status shall indicate if the Database is functional or is out of service. This status will be used in subsequent determinations of applying failover procedures.

**AUX-001590 [Required: MRDB, Backup MRDB, LRDB]** The MRDB, Backup MRDB, and LRDB shall support the processing of keep-alive messages from the SCs and SSs.

#### 3.3.5.2.5.1 MRDB Failover

During failover operation, when the Primary MRDB becomes unavailable and the Backup MRDB becomes the active MRDB, the SCs send their updates (individual or bulk) to the Backup MRDB, and the Backup MRDB queues these updates for later transmission to the Primary MRDB (i.e., when the Primary MRDB is restored to service). The Backup and Primary MRDBs support periodic synchronization procedures to ensure that their data content is consistent.

**AUX-001600 [Required: MRDB, Backup MRDB, SC]** Each SC that accesses the Primary and Backup MRDBs shall support the configuration of two DISA network IP addresses for those MRDBs: one for the Primary MRDB (used when the Primary is active) and another for the Backup MRDB (used when the Primary has failed).

##### 3.3.5.2.5.1.1 Primary Master Down, Backup Master Active

**AUX-001610 [Required: SC]** If the SC does not receive a response from the Primary MRDB within 2 seconds of sending a keep-alive message or a valid LDAP message (update or search), then the SC shall try sending another keep-alive message or resend the same LDAP message.

**AUX-001620 [Required: SC]** If no response is received from the Primary MRDB within 5 seconds of the retry attempt, then the SC shall do the following:

- a. Stop sending LDAP Updates to the Primary MRDB.
- b. Establish, if necessary, an LDAPv3 over TLS connection with the Backup MRDB.
- c. If the most recent status of the Backup MRDB is “functional,” then continue with step d. Otherwise, the SC shall withhold any updates and continue sending keep-alive messages to both Primary and Backup MRDBs until one responds.
- d. Send all subsequent LDAP Update operations (additions and deletions of DSN or commercial number pairs) to the Backup MRDB instead.

- e. Continue keep-alive messages with the Primary and Backup MRDBs.

**AUX-001630 [Required: Backup MRDB]** The Backup MRDB shall always queue the LDAP Updates it receives from the SC.

Updates received by the Backup MRDB are most likely to occur during periods of the Primary MRDB's unavailability.

**AUX-001640 [Required: SC]** The SC shall continue sending the LDAP Updates to the Backup MRDB until it receives a successful response to a keep-alive message from the Primary MRDB.

**AUX-001650 [Required: MRDB]** The Primary MRDB shall not send a successful response to any keep-alive messages until it has been loaded with the queued updates from the Backup MRDB and/or the SC. This should be ensured by the network personnel performing the necessary repairs on the MRDB before returning the MRDB back online, after the cause of failure has been resolved and the Primary MRDB has regained functionality.

**AUX-001660 [Required: MRDB, Backup MRDB]** The Primary MRDB shall support a request to transfer the downtime queued update, for a given time period specified by the network administrator, from the Backup MRDB.

Network administrators and DBAs will return the Primary MRDB to service after all the "downtime" updates have been integrated in its files successfully. The goal is to ensure that the Primary MRDB is not placed back in service until it has been updated with the recent modifications that took place while it was out of service. When the Primary MRDB is ready to handle requests, the DBA could (a) change the address in the SC from the Backup MRDB to that of the Primary MRDB, thus redirecting traffic immediately to the Primary MRDB, or (b) wait for the Primary MRDB to reply to the next keep-alive message from the SC.

**AUX-001670 [Required: SC]** The SC shall give the SC administrator the ability to change, on demand, the address to which the SC LDAP updates should be directed.

**AUX-001680 [Required: SC]** When the Database address in the SC is reset to the Primary MRDB, or when the SC receives a successful response to the keep-alive message from the Primary MRDB, the SC shall do the following:

- a. Stop sending LDAP Updates to the Backup MRDB.
- b. Reestablish an LDAPv3 over TLS connection with the Primary MRDB.
- c. Resume sending LDAP Updates to the Primary MRDB.
- d. Continue sending keep-alive messages to the Primary and Backup MRDBs according to Timer Ta.

**AUX-001690 [Required: Backup MRDB]** During failover (when the Primary MRDB is out-of-service and the Backup MRDB stands in), authorized DISA personnel (craftspeople, network

managers, DBA) shall be able to access the Backup MRDB and perform LDAP Search operations, LDAP Update operations, and LDIF file imports on it.

It is expected that the Backup MRDB will be capable of handling the LDAP Update traffic load during failover conditions.

#### 3.3.5.2.5.1.2 Primary Master Down, Backup Master Down

Although unlikely, it is possible that the Backup MRDB would do one of the following:

- Be down already when the Primary MRDB fails.
- Experience a failure shortly after it starts to stand in for the Primary MRDB.

**AUX-001700 [Required: SC]** During failover mode to the Backup MRDB, if the SC does not receive a response from the Backup MRDB within 2 seconds of sending a keep-alive message or an LDAP Update request, then the SC shall retry sending the message to the Backup MRDB.

**AUX-001710 [Required: SC]** If no response is received from the Backup MRDB for the retry message within 5 seconds (i.e., both Primary and Backup MRDBs are now out of service), then the SC shall do the following:

- a. Report alarms for a critical error to the network administrator.
- b. Queue subsequent LDAP Update operations.
- c. Initiate Ta and continue sending keep-alive messages to both Primary and Backup MRDBs until it receives notification that either the Primary or Backup MRDB has been restored to service.

**AUX-001720 [Optional: SC]** While both the Primary and Backup MRDB are down, the SC shall maintain a log of the LDAP Updates that it tried to send to the Primary and Backup MRDBs. The log shall contain the address of the destination Database, timestamps, target LDAP DN, and Update transaction.

The log will serve as a reference for audits.

#### 3.3.5.2.5.2 LRDB Failover

Each theater is expected to have one or more LRDBs serving the HR or Commercial Cost Avoidance LDAP Search requests from the SCs or SSs. In that topology, the LRDBs are expected to act as potential backups for each other. If an LRDB (e.g., Database #1) fails, then the SC will reroute LDAP requests destined for Database #1 to another LRDB (e.g., Database #2), defined here as the “Secondary.” The rerouting continues until Database #1 is returned to service.

**AUX-001730 [Required: SC, SS]** Each SC or SS that accesses LRDBs shall support the configuration of two DISA network IP addresses for those Routing DBs: one for a Primary LRDB and another for a Secondary LRDB (used when the Primary has failed).

As noted in [Section 3.3.5.2.5](#), Failover, each SC and SS shall use an independent Timer Ta to schedule sending the keep-alive messages to its Primary and Secondary LRDBs.

#### 3.3.5.2.5.2.1 Primary Local Down, Secondary Local Active

**AUX-001740 [Required: SC, SS]** If the SC or SS does not receive a response from the Primary LRDB within 0.5 seconds of sending a keep-alive message or an LDAP Search request, then the SC or SS shall send another keep-alive message or resend the same LDAP Search request.

**AUX-001750 [Required: SC, SS]** If no response is received from the Primary LRDB for the retry message within 0.5 seconds, then the SC or SS shall do the following:

- a. Stop sending LDAP Search requests to the Primary LRDB.
- b. Redirect the LDAP Search requests to the Secondary LRDB immediately.
- c. Continue keep-alive messages with the Primary and Secondary LRDBs.
- d. If the most recent status of the Secondary LRDB is “functional,” then continue with step c of [AUX-001790](#). Otherwise, the SC or SS shall utilize commercial number routing instead of performing Commercial Cost Avoidance, and utilize internal SS routing tables instead of performing HR.

**AUX-001760 [Required: SC, SS]** The SC or SS shall continue sending the LDAP Search operations to the Secondary LRDB until it receives a successful response to a keep-alive message from the Primary LRDB.

When the Primary LRDB is restored from “out-of-service” to “in-service,” the Primary LRDB should not send a successful response to any keep-alive messages from SCs or SSs until it has been updated with the latest data from the MRDB. This should be ensured by the network personnel performing the necessary repairs on the Primary LRDB before returning the Primary Database back online.

**AUX-001770 [Required: LRDB, MRDB, Backup MRDB]** The Primary LRDB shall be able to request a partial synchronization from the MRDB, specifying the start time as that time the Database went out of service. The MRDB (or Backup MRDB) shall support that request.

Network administrators or DBAs should return the Primary LRDB to service after all “downtime” updates from the MRDB have been integrated successfully in its files. The goal is to ensure that the Primary LRDB is not returned to service until it has been updated with the recent MRDB modifications that took place while it was out of service. When the Primary LRDB is ready to handle Search requests, the SC and SS administrators could (a) change the address in the SCs and SSs from the Secondary LRDB to that of the Primary LRDB, thus redirecting traffic

---

immediately to the Primary LRDB or (b) wait for the Primary LRDB to reply to the next keep-alive message from each SC and SS.

**AUX-001780 [Required: SC, SS]** The SC and SS shall give the SC and SS administrators the ability to change the address, on demand, to which the SC and SS Search requests should be directed.

**AUX-001790 [Required: SC, SS]** When the LRDB address in the SC or SS is reset to the address of the Primary LRDB, or when the SC or SS receives a successful response to the keep-alive message from the Primary LRDB, the SC or SS shall do the following:

- a. Stop sending LDAP Searches to the Secondary LRDB.
- b. Resume sending LDAP Searches to the Primary LRDB.
- c. Continue sending keep-alive messages to the Primary and Secondary LRDBs according to Timer Ta.

It is expected that the Secondary LRDB will be capable of handling the LDAP Search traffic load during failover conditions.

#### 3.3.5.2.5.2.2 Primary Local Down, Secondary Local Down

Although unlikely, it is possible that the Secondary LRDB is out of service at the same time as the Primary LRDB. In that case, the following requirements will be followed.

**AUX-001800 [Required: SC, SS]** Following the failure of the Primary LRDB, if no response is received from the Secondary LRDB within 2 seconds of sending a keep-alive message or an LDAP Search request message, then the SC or SS shall retry sending the message to the Secondary LRDB.

**AUX-001810 [Required: SC, SS]** If no response is received from the Secondary LRDB for the retry message within 5 seconds, then the SC or SS shall do the following:

- a. Report alarms for a critical error to the network administrator.
- b. Stop sending LDAP requests to the LRDBs.
- c. Start Timer Ta.
- d. Maintain keep-alive messages with both Primary and Secondary LRDBs using Ta.

The failure of both Primary and Secondary LRDBs affects HR call routing and defeats the cost savings intended from Commercial Cost Avoidance. Therefore, it is important to return at least one LRDB back to service, or to have more than one Secondary LRDB provisioned for each SC or SS. After the DBs are restored, the DBAs will notify the SC and SS administrators so that their SCs and SSs can start sending their Search requests to the appropriate LRDB.

---

**AUX-001820 [Required: SC, SS]** When both the Primary and Secondary LRDBs are out-of-service, and the SC or SS receives a successful response to the keep-alive message from the Primary LRDB, the SC or SS shall do the following:

- a. Stop sending LDAP Search requests to the Secondary LRDB.
- b. Resume sending LDAP Search requests to the Primary LRDB.
- c. Resume sending keep-alive messages to the Primary and Secondary LRDBs based on Ta.

**AUX-001830 [Required: SC, SS]** When both the Primary and Secondary LRDBs are out-of-service, and the SC or SS receives a successful response to the keep-alive message from the Secondary LRDB, the SC or SS shall do the following:

- a. Stop sending LDAP Search requests to the Primary LRDB.
- b. Resume sending LDAP Search requests to the Secondary LRDB.
- c. Resume sending keep-alive messages to the Primary and Secondary LRDBs based on Ta.

#### 3.3.5.2.6 *Provisioning*

In the following requirements, “bulk upload” refers to a method in which number records are uploaded into the LRDB or MRDB “in bulk,” rather than uploaded individually using LDAP Update operations (such as Add, Modify, and Delete). For an LRDB, the source of the data for the “bulk uploads” may be the MRDB or the Backup MRDB. For an MRDB, the source of the data for the “bulk uploads” may be a set of SCs containing number records, or it may be another database that is a copy of the MRDB (e.g., the Backup MRDB).

Bulk uploads may be used during the initial provisioning of the LRDB or MRDB (e.g., population of the MRDB from multiple SCs that already contain number records), or during full reloads of that Database (e.g., population of LRDB records from the MRDB, after a loss of data). An example of a “bulk upload” technique is transfer of LDAP Data Interchange Format (LDIF) files from an individual SC to the MRDB, using e-mail messages or FTP sessions. LDIF file transfer implies a manual export of LDIF data at the source end (e.g., SC) and manual import of LDIF data at the receiving end (e.g., MRDB). Other bulk upload techniques can also be used, if supported by the LRDB, MRDB, and SC vendors.

Commercial experience with bulk uploads for DBs containing millions of records has shown that the time needed to perform a bulk upload goes down as the size of the upload transactions (the data “chunks”) used in the bulk upload goes up. In other words, the time needed for bulk uploading records is inversely proportional to the size of the upload transactions or “chunks” used to perform the bulk-upload.

It is therefore recommended that the MRDB and LRDB include as many Database records as possible within each “bulk upload” transaction to reduce the “bulk upload” provisioning time at the LRDB or MRDB. It is also recommended that a small number of high-volume transactions be used for “bulk uploads,” instead of a large number of low-volume transactions.

**AUX-001840 [Required: LRDB]** The LRDB shall support a maximum bulk upload time of 8 hours for a Database size of 8 million records, using multiple bulk upload transactions in which each transaction contains a fraction of the 8 million records.

**AUX-001850 [Required: MRDB, Backup MRDB]** The MRDB and Backup MRDB shall be able to accept a bulk update of the full set of 8 million Database records (via LDIF file transfer or other methods) within a period of no more than 8 hours, using multiple bulk upload transactions in which each transaction contains a fraction of the 8 million records.

**AUX-001860 [Required: LRDB, MRDB, Backup MRDB]** In addition to supporting bulk uploads, the LRDB and MRDBs shall support user interfaces [e.g., a Web-based Graphical User Interface (GUI) and a text-based command line interface] that allow end users to configure and update the Database. The LRDB and MRDBs shall allow DISA to make these interfaces available to local DISA craftspeople, remote DISA craftspeople, and remote DISA Operations Systems [such as the RTS Element Management System (EMS)].

**AUX-001870 [Required: LRDB, MRDB, Backup MRDB]** The LRDB and MRDBs shall allow an authorized craftsperson, DBA, or remote DISA Operations System to access the LRDB and MRDBs for reading, writing, and updating record data.

**AUX-001880 [Required: LRDB, MRDB, Backup MRDB]** The LRDB and MRDBs shall allow an authorized craftsperson, DBA, or remote DISA Operations System to access the LRDB and MRDBs for configuring the following:

- a. Department of Defense (DOD) public key infrastructure (PKI) certificates (used with TLS authentication) for both the Database itself and the various Database clients (i.e., SCs and SSs in that theater).
- b. LDAP User Names and Passwords (used with LDAP Bind message authentication) for the various Database clients (SCs and SSs in that theater).

#### *3.3.5.2.7 Synchronization Between Primary and Backup MRDBs*

In each theater, the LRDBs are expected to act as backups for each other. The Primary MRDB also has one Backup MRDB. The purpose of this Backup MRDB is to provide a most recent duplicate of the Primary MRDB in case of an outage, data loss, or catastrophic failure at the Primary MRDB. This allows SCs sending Database updates to “fail over” from the Primary to the Backup MRDB when the Primary MRDB is out of service.

**AUX-001890 [Required: MRDB, Backup MRDB]** The Primary MRDB shall support full data updates (full data backups) to the Backup MRDB during non-busy hours (based on the Primary MRDB’s local time zone).

**AUX-001900 [Optional: MRDB]** The Primary MRDB shall support the performance requirements listed in this document (i.e., minimum operations per second and maximum processing time) during the “full data backup” process with the Backup MRDB. This means that

the Primary MRDB shall be able to support bulk updates from SCs, LDAP Search operations from SCs, and LDAP Update operations from SCs, while simultaneously performing a full data backup with the Backup MRDB.

**AUX-001910 [Required: MRDB, Backup MRDB]** The Primary MRDB shall support the performance of full data backups with the Backup MRDB on a configurable scheduled basis. The Primary MRDB shall support scheduled full data backup settable frequencies of every 6 hours, every 12 hours, and every 24 hours.

**AUX-001920 [Optional: MRDB, Backup MRDB]** The Backup MRDB shall be coupled with the Primary MRDB via redundant, physically diverse, high throughput TLS over IP connections, and shall function as a “hot standby” for the Primary MRDB. These master-to-master connections shall be secured using TLS with DOD PKI certificates, consistent with the requirements for securing exchange of LDAPv3 messages over TLS.

**AUX-001930 [Required: MRDB, Backup MRDB]** The Primary and Backup MRDBs shall give DISA the ability to initiate a “full data backup” at any time, independent of when the last scheduled full data backup was performed.

#### 3.3.5.2.8 *Synchronization Between LRDB and MRDB*

The requirements in this section apply to the LRDB and MRDB. In general, the LRDB and MRDB are located in physically separate sites.

**AUX-001940 [Required: LRDB, MRDB]** The LRDB shall support an interface to the MRDB, and the MRDB shall support an interface to the LRDB, to support Database synchronization for the Commercial Cost Avoidance and HR features.

**AUX-001950 [Required: LRDB, MRDB]** The Database synchronization interface between the LRDB and the MRDB shall be LDAPv3 over TLS over IP. This LDAPv3 interface shall be compliant with the following LDAP v3 RFCs:

RFC 2251, RFC 2252, RFC 2253, RFC 2254, RFC 2255, RFC 2256, RFC 2829, RFC 2830.

**AUX-001960 [Required: LRDB, MRDB]** The LDAPv3 Data schema used on the Database synchronization interface between the LRDB and MRDB shall include all of the following information fields:

- a. Entry field containing an LDAP Distinguished Name containing the following:
  - (1) User ID component containing the commercial number (e.g., UID=7038821234) of the end user.
  - (2) Domain components “uc” and “mil” (dc=uc, dc=mil).
- b. Attributes field containing the following attributes:
  - (1) User ID field containing the commercial number of the end user.

- (2) SIP Alias field containing the full international format commercial called number of the end user followed by “@uc.mil.”
- (3) sip User Name field containing the UID (i.e., commercial number) followed by “@uc.mil.”
- (4) Directory Number field containing the full 10-digit DSN number of the end user.
- (5) LSCCAID field containing the CCA-ID of the SC serving the end user.
- (6) SSCCAID field containing the CCA-IDs of the primary SS and the backup SS serving this SC, separated by a comma.
- (7) Object Class field containing “mobSLR.”

**AUX-001970 [Required: LRDB, MRDB]** The encoding of the LDAPv3 messages and data schema used on the Database synchronization interface between the LRDB and MRDB shall follow the BER of ASN.1.

**AUX-001980 [Required: LRDB, MRDB]** The Database synchronization interface between the LRDB and MRDB shall be secured using TLS, consistent with the requirements for securing UC SIP messages using TLS in Section 4, Information Assurance. This security shall provide mutual authentication between the LRDB and MRDB, message confidentiality for the Database synchronization messages, and message integrity for the Database synchronization messages.

**AUX-001990 [Required: LRDB, MRDB]** The Database synchronization interface between the LRDB and MRDB shall traverse the data firewalls at both the LRDB and MRDB sites.

**AUX-002000 [Required: LRDB, MRDB]** The Database synchronization interface between the LRDB and MRDB shall traverse the CE-Rs at both the LRDB and MRDB sites, using the DSCP for User Signaling traffic, and the associated CE-R queues.

**AUX-002010 [Required: MRDB]** The MRDB shall be capable of maintaining multiple Database synchronization interfaces to different LRDBs at the same time. Each individual Database synchronization interface shall support the previous requirements for the protocols, data schemas, and security mechanisms used between an individual LRDB and the MRDB.

Typically, Database synchronization methods are vendor-proprietary, and are not expected to have an effect on Database performance for this Routing Database implementation within DISA. The Primary and Backup MRDBs are expected to be the ultimate data sources available to the various LRDBs for synchronization purposes. The Database synchronization requirements call for a master-subordinate configuration, in which the MRDBs are the “masters” and the LRDBs are the “subordinates.”

**AUX-002020 [Required: LRDB, MRDB, Backup MRDB]** The MRDBs shall be able to perform their Database synchronization with the LRDBs through a “push” model, in which data records are downloaded from one MRDB to the LRDBs on a programmable schedule.

- a. Under normal operation, the data push shall be from the Primary MRDB to the various LRDBs.
- b. Under MRDB failover operation, the data push shall be from the Backup MRDB to the various LRDBs, since the Primary MRDB is out-of-service.

**AUX-002030 [Required: LRDB]** The LRDB shall be able to support SC and SS Search requests during its synchronization process with the MRDB.

**AUX-002040 [Optional: LRDB, MRDB, Backup MRDB]** The MRDBs shall be able to perform their Database synchronization with the LRDBs through a pull model, in which data records are downloaded from one MRDB to the LRDB, based on a pull request from the LRDB (e.g., in case of data loss at the LRDB).

- a. Under normal operation, the data pull shall be from the Primary MRDB to the LRDBs (as initiated by the LRDB).
- b. Under failover operation, the data pull shall be from the Backup MRDB to the LRDBs (as initiated by the LRDB), since the Primary MRDB is out-of-service.

**AUX-002050 [Required: MRDB, Backup MRDB]** The MRDB shall maintain a status on each of the LRDBs that it is responsible for synchronizing. At minimum, the status information shall include or record the following:

- a. Timestamp for the last update for each LRDB.
- b. Type of update (full or incremental).

**AUX-002060 [Required: MRDB, Backup MRDB]** The Database synchronization process between the MRDB and LRDB shall be possible through full or incremental updates. Incremental updates deliver only the records that were modified or created since the last known update.

**AUX-002070 [Required: MRDB, Backup MRDB]** The MRDB shall perform full and incremental updates according to a settable schedule or on an on-demand basis.

It is expected that incremental synchronizations will take place more frequently than full database synchronizations as the size of the database grows. Typically, full synchronizations are more appropriate in the case of a database reload after data loss, while incremental updates pose minimal effect on traffic and resources within the Database architecture.

**AUX-002080 [Required: MRDB, Backup MRDB]** The MRDB (or Backup MRDB) shall be able to synchronize its data with two LRDBs simultaneously.

**AUX-002090 [Optional: MRDB, Backup MRDB]** The MRDB (or Backup MRDB) shall be able to perform synchronization with four LRDBs simultaneously.

It is important to complete the synchronization of the MRDB with all LRDBs within a short time, in order for all Commercial Cost Avoidance and HR queries from the various clients (i.e., SCs and SSs) to receive consistent responses from all local DBs.

**AUX-002100 [Required: LRDB, MRDB, Backup MRDB]** Under normal operations (no Database failover scenarios and no Database scheduled maintenance), the simultaneous synchronization between the MRDB and every pair of LRDBs shall be completed within a period of no longer than 8 hours. The MRDB, Backup MRDB, and LRDB shall support the number of interfaces necessary to perform the synchronization within the required period.

**AUX-002110 [Required: MRDB, Backup MRDB]** If the MRDB attempts a synchronization with an LRDB, and the target LRDB is out of service at the scheduled time (e.g., a communication error is received from the LRDB), then the MRDB shall attempt the synchronization again in 30 minutes from the original scheduled time. If this second attempt fails, then the MRDB shall reattempt the synchronization one last time 60 minutes after the original start time.

**AUX-002120 [Required: MRDB, Backup MRDB]** If the MRDB's third and final attempt at synchronization with any LRDB fails, then the MRDB shall notify the DBA by issuing an alarm identifying 1) the address of the LRDB that failed to receive synchronization updates from the Primary or Backup MRDB and 2) the time of the last attempt.

If an LRDB was not available for synchronization, then the next scheduled synchronization is expected to take place during one of the following:

- a. At regularly scheduled times, after the LRDB has been repaired and returned to service.
- b. Per the LRDB administrator's request (as soon as the LRDB is repaired).

### 3.3.6 MRDB and LRDB Operations

#### 3.3.6.1 Overview

The objective of a Routing Database operations plan is to preserve Database integrity and to provide high-quality service. Operations, administration, and maintenance guidelines are provided by the Routing Database vendors and should be followed as directed for robust performance.

This section addresses the majority of the requirements for the functional areas of the Routing DBs and Signaling Appliances (Master and Local DBs, SCs, and SSs) that support the Commercial Cost Avoidance and HR features. Other sections containing related requirements are referenced throughout this section.

The functional areas are as follows:

- Trouble Detection and Reporting. The functions necessary to detect, send notification of, and log failure conditions.

- Performance Monitoring. Measurements and data collection on utilization, errors, and availability to improve capacity planning and detect traffic overload conditions.
- Routing Database Archival. The functions necessary to provision additional backup in the form of a static archive.
- Security Management. Access rights and logs.

The required approach to managing the Routing Database is using Simple Network Management Protocol (SNMP) and MIBs. The two applicable Internet Engineering Task Force (IETF) Standards are Standards 58 and 62. These two standards are composed of the following requirements.

**AUX-002130 [Required: MRDB, Backup MRDB, and LRDB]** Standard 58, Structure of Management Information Version 2 (SMIV2): RFC 2578, RFC 2579, and RFC 2580.

**AUX-002140 [Required: MRDB, Backup MRDB, and LRDB]** Standard 62, Simple Network Management Protocol Version 3 (SNMPv3): RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417, and RFC 3418.

Much of the Configuration Management (CM) requirements are covered in [Section 3.3.5](#), LRDB and MRDB. Provisioning a Routing Database, including bulk updates to initially load the database and configure security settings, is discussed in [Section 3.3.5.2.6](#), Provisioning. Requirements for synchronization of data between a Primary and Backup MRDB are in [Section 3.3.5.2.7](#), Synchronization Between Primary and Backup MRDBs. Requirements for synchronization between an LRDB and an MRDB are in [Section 3.3.5.2.8](#), Synchronization Between LRDB and MRDB.

### ***3.3.6.2 Trouble Detection and Reporting***

This section discusses Alarms, Event Logs, and Audits used by operations personnel to detect and resolve trouble conditions.

#### ***3.3.6.2.1 Alarms***

This section covers requirements for Alarms to be issued by the Routing Database or SC or SS when conditions exist on the LDAP interface between an SC or SS and a Routing Database that may be symptomatic of a hardware or software failure.

In addition to failures, alarms may be issued when there are resource or performance degradation issues caused; for example, by excessive traffic. Based on performance measurement thresholds configured by the network administrator and DBA, notifications and alarms are generated.

**AUX-002150 [Required: SC, SS]** The SC or SS shall support the generation and reporting of alarms for the following scenarios:

- a. The SC or SS detects loss of connectivity with any of the LRDBs or MRDBs (e.g., no response to an LDAP Bind): the alarm message shall contain the identity of the affected Database, timestamp, and error type, if applicable.
- b. **[Optional]** The number of LDAP error messages received from an LRDB exceeds a threshold during a 5-minute interval: the alarm message shall contain the identity of the affected Database, timestamp, and error types. The thresholds set by each network administrator will vary depending on the volume of traffic each Database is expected to support.
- c. **[Optional]** The number of LDAP error messages from the Primary or Backup MRDB exceeds a threshold during a 5-minute interval: the alarm message shall contain the identity of the affected Database, timestamp and error types. The thresholds set by each network administrator will vary depending on the volume of traffic each Database is expected to support.
- d. The SC or SS determines that it should reroute LDAP Search requests to a Secondary LRDB; i.e., a failover (refer to [Section 3.3.5.2](#), Routing Database, for detailed requirements on the conditions triggering these alarms).
- e. The SC determines that it should reroute LDAP Update requests from the Primary MRDB to the Backup MRDB (failover); this indicates that the Primary MRDB is out of service and requires attention.
- f. The SC does not receive responses to retry messages from the Backup MRDB (indicating that both the Primary and Backup MRDBs have failed).
- g. **[Optional]** The SC or SS encounters a time-out on a Search request, attempts to send the Search twice more, and the response time still exceeds the set threshold.
- h. **[Optional]** The SC encounters a time-out on a Update request, attempts to send the Update request twice more, and the response time still exceeds the set threshold.
- i. The SC or SS receives an error response LDAP\_INVALID\_CREDENTIALS (49) on three consecutive Bind attempts within 30 seconds; this error response could signal an unauthorized access attempt to the database(s).
- j. **[Optional]** The SC or SS receives an improperly formatted response from a Routing Database on the first attempt and two subsequent retries; this response could point to errors in the Database processing or Database data integrity.
- k. **[Optional]** The SC attempts an Update (Modify or Delete) in which the pilot Search result shows that the CCA-ID of the SC does not match that of the target record, or is missing.

**AUX-002160 [Required: MRDB, Backup MRDB, and LRDB]** The Primary MRDB, Backup MRDB, and LRDB shall support the generation and reporting of alarms for the following scenarios as described:

- a. A Primary or Backup MRDB fails to synchronize with an LRDB at the scheduled time and/or on reattempts: the alarm message shall contain the identities or addresses of the Primary or Backup MRDB and the LRDB in question, and the time stamp of the attempt (refer to [Section 3.3.5.2](#), Routing Database, for detailed requirements on the conditions triggering these alarms).
- b. **[Optional]** The average Routing Database LDAP response time for Search requests, measured over a 5-minute interval, exceeds a preset threshold (set by the network administrator).
- c. The number of LDAP error responses returned on Bind requests because of invalid credentials, during a 5-minute interval, exceeds a threshold (set by the network administrator).
- d. **[Optional]** The average Routing Database LDAP response time for Bind requests, over a 5-minute interval, exceeds a threshold (set by the network administrator).
- e. The Routing Database average CPU utilization for an individual processor or all processors in a given Database exceeds 90 percent for a 5-minute interval.
- f. **[Optional]** The number of LDAP requests that are not formatted properly from an SC or SS exceeds a preset threshold (set by the network administrator) during a 5-minute interval; this could point to errors in the SC or SS processing.

**AUX-002170 [Required: MRDB, Backup MRDB, and LRDB]** The Primary MRDB, Backup MRDB, and LRDB shall support Simple Network Management Protocol version 3 (SNMPv3) interfaces to remote network management systems for the reporting of alarms.

### 3.3.6.2.2 Logs

Logs capture events over a time interval. Logs can be useful for diagnostics and troubleshooting as well as other Network Management activities.

**AUX-002180 [Required: MRDB, Backup MRDB, and LRDB]** The MRDB, Backup MRDB, and LRDB shall support the generation of logs that span settable periods (default 1 week). The MRDB, Backup MRDB, and LRDB shall allow the administrators to set that period.

**AUX-002190 [Required: MRDB, Backup MRDB, and LRDB]** The MRDB, Backup MRDB, and LRDB shall support the memory requirements necessary to store log files that span a period of 6 months.

**AUX-002200 [Required: MRDB, Backup MRDB, and LRDB]** The Database Management System (DBMS) governing the MRDB, Backup MRDB, and LRDB shall support the generation of a downtime log for each Database. The downtime log shall store an event record each time a Routing Database goes out of service or returns to service. Each event shall include the following:

- a. Identity of the Database.

- b. Date and time the Database failure or restoration occurred.

**AUX-002210 [Optional: MRDB, Backup MRDB, and LRDB]** The MRDB, Backup MRDB, and LRDB shall support the generation of an LDAP Error log documenting the LDAP error response messages returned to its clients. Each log record shall include the following:

- a. Identity of the database.
- b. Identity of the LDAP client receiving the error.
- c. Type of error.
- d. Date and timestamps for each message sent.

Database access is allowed only to pre-authorized entities. Therefore, unauthorized attempts should be reported. Access logs should record key access incidents and repeated unauthorized attempts.

**AUX-002220 [Required: MRDB, Backup MRDB, and LRDB]** The MRDB, Backup MRDB, and LRDB each shall support the generation of a security access log documenting all access that requires credentials, both authorized and unauthorized access (e.g., all Bind responses in which an error response was returned because of invalid credentials). Each access log(s) record shall contain the following details:

- a. Date and time of access.
- b. User ID or system ID (e.g., SC ID).
- c. Credentials received by the Database from the accessing entity.
- d. Response sent back from Database.

It is not recommended or encouraged to perform non-standard or emergency “manual” updates to any Routing Database on a regular basis. However, if it does occur through an authorized craftsperson station or DBA station, then it is required to be sent directly to the master or backup Database (depending on which one is active at the time). For data integrity and auditing purposes, a non-standard update should be logged and promptly entered in the master Database.

**AUX-002230 [Required: MRDB, Backup MRDB, and LRDB]** The MRDB, Backup MRDB, and LRDB shall support the creation of a manual update log. Each log record shall contain the following:

- a. Time and date of manual update.
- b. Source: IP address from which the update originated.
- c. Authorization information to identify the administrator or craftsperson originating the manual update.
- d. Distinguished Name of the Database record updated.

- e. Attribute or entry updates made.

Each administrator could use the log to identify updates that originated from his or her theater and perform random checks to ensure that the updates are in effect. The MRDB DBA will be able to view the number of updates originating from each theater and perform the necessary checks to ensure that the MRDB is updated.

**AUX-002240 [Required: MRDB, Backup MRDB, and LRDB]** The MRDB, Backup MRDB, and LRDB shall support logging the following events along with the time and date for each:

- a. Synchronization attempt with another Routing Database.
- b. Synchronization result for each attempt (successful and failed attempts).
- c. Full data backups performed by DISA personnel on each Database.

**AUX-002250 [Required: SC, SS]** The SC or SS shall support logging the following events:

- a. Every failover to a Secondary LRDB and restoration to the Primary LRDB, along with the date and time of the failover or restoration and the original and alternate database addresses or identity.
- b. For SCs only, every failover to a Backup MRDB and restoration to the Primary MRDB, along with the date and time of the failover or restoration, and the original and alternate database addresses or identity.

### 3.3.6.2.3 Audits

**AUX-002260 [Optional: MRDB, Backup MRDB, and LRDB]** The MRDB, Backup MRDB, and LRDB shall be capable of performing an audit request on demand or on a scheduled basis from authorized DBAs. The audit request shall contain one of the following actions:

- a. Perform a partial comparison of entries in the MRDB and the LRDB for a range of Distinguished Names (DNs).
- b. Perform a full comparison of all entries between the MRDB and the LRDB.

While the Primary MRDB is out of service, updates are redirected to the Backup MRDB. For the purposes of audits, a separate log of those updates should be maintained by the Backup MRDB to be compared later to the actual data entries in both the Primary and Backup MRDBs.

**AUX-002270 [Optional: Backup MRDB]** The Backup MRDB shall maintain a log of all the updates received from the SCs when the Primary MRDB is out of service. The update log shall be available to authorized DBAs for viewing and auditing. Each update log record should contain the following:

- a. Data and time of the update.
- b. SC ID requesting the update.

- c. DN of the record being updated, added, or deleted.
- d. Set of attributes and values that are being updated.

#### 3.3.6.2.4 *Routing Database Archival*

The data in the MRDB is critical to the Commercial Cost Avoidance and HR services. There are several measures that have been put in place to return the DBs to service as soon as possible if a Routing Database failure occurs or if the data becomes corrupted. In addition to the redundancy, synchronization, and failover requirements discussed in [Section 3.3.5](#), LRDB and MRDB, this section recommends that a static archive be kept of the MRDB as another means of quickly restoring the data in a MRDB.

**AUX-002280 [Optional: MRDB, Backup MRDB]** The Primary and Backup MRDBs shall perform a partial or full update to the archive at least every 6 hours. The Primary and Backup MRDBs shall provide the capability to perform these updates automatically on a configurable schedule and manually on demand. The backup to the archive should be done while still meeting the MRDB throughput requirements in [Section 3.3.5](#), LRDB and MRDB.

Archival backups could be transported physically (e.g., via courier) from the Primary MRDB and Backup MRDB locations to the archival backup site. However, that could cause recovery delays of at least 1 day in case that data is needed for a total reload of the database. Electronic backup to the archival backup site would consume much less time.

**AUX-002290 [Conditional: MRDB, Backup MRDB]** If archive backups are adopted, then the Primary and Backup MRDBs shall be able to transmit the archive backup files electronically to the hardware hosting the archive over a high-bandwidth connection (via a protocol such as FTP).

**AUX-002300 [Conditional: MRDB, Backup MRDB]** If archive backups are adopted, then the Primary and Backup MRDBs shall access the archival backup copies electronically via high-bandwidth connections to restore the Database. This shall be done manually by an authorized network administrator.

It is recognized that the archives will be, at most, 6 hours out of synch with the Primary and Backup MRDBs, but could nonetheless serve as the latest available copy of the Primary MRDB in case the Primary and Backup MRDBs undergo extensive damage.

#### 3.3.6.2.5 *Performance Monitoring*

In addition to monitoring a Routing Database for failures, operations personnel need to monitor a Routing Database to ensure that it has been engineered with the resources needed to meet the traffic demands. The Routing Database needs to keep resource utilization and traffic measurements to help determine when additional capacity may be needed. Performance measurements are used to help determine when there is an impairment resulting in performance that is below expectations (e.g., slower response time). Some performance measurements have

---

associated thresholds that if exceeded, will result in an alarm being generated. DBAs can tune the database performance and resources based on the reported measurements.

**AUX-002310 [Required: MRDB, Backup MRDB, and LRDB]** The MRDB, Backup MRDB, and LRDB shall be capable of sending traffic and performance measurements to the network administrator on a predetermined schedule (as set by the DBA) or when polled by the authorized DBA.

Visual-based tools can assist DBAs in their overall management role.

**AUX-002320 [Optional: MRDB, Backup MRDB, and LRDB]** The Database Management system for the MRDB, Backup MRDB, and LRDB shall support a visual interface or Graphical User Interface (GUI) to display the performance metrics of all the databases in all the theaters.

**AUX-002330 [Optional: MRDB, Backup MRDB, and LRDB]** The following measurements and statistics for each database shall be stored and be made available for retrieval at any time by the network administrators:

- a. Disk utilization for the Database and log files, updated every 24 hours.
- b. Average “total” CPU utilization in a 5-minute interval.
- c. Average “individual” CPU utilizations in a 5-minute interval.
- d. Number of TLS connections available between the Database and its clients (SCs, SSs, and other DBs) in a period of 1 hour.
- e. Number of active TLS connections between the Database and its clients (SCs, SSs, and other DBs) in a period of 1 hour.
- f. Number of active LDAP sessions between the Database and its clients in a period of 1 hour.
- g. Number of Bind operations received in a 5-minute interval.
- h. Number of Unbind operations received in a 5-minute interval.
- i. Number of successful Binds processed in a 5-minute interval.
- j. Average LDAP Bind time (Database time to respond successfully to a Bind request) measured in a 5-minute interval.
- k. Number of LDAP Search request messages received in a 5-minute interval.
- l. Number of LDAP Search response messages sent in a 5-minute interval.
- m. Average LDAP Search response time (Database time to respond successfully to a Search request) in a 5-minute interval.
- n. Number of Database entries returned to Database clients (SCs, SSs, and other DBs) in a 5-minute interval.

- 
- o. Number of LDAP Update request messages received in a 5-minute interval, with a breakdown for the number of (a) Update Add, (b) Update Delete, and (c) Update Modify.
  - p. Number of LDAP Update response messages sent in a 5-minute interval.
  - q. Average LDAP Update response time (Database time to respond successfully to an Update request) in a 5-minute interval.
  - r. Number of LDAP Error messages returned in a 5-minute interval.
  - s. Number of pending Database synchronizations (MRDB to LRDB; Backup MRDB to LRDB; MRDB to Backup MRDB); this may point to extended outages at either the MRDB, the Backup MRDB, or the LRDB.

**AUX-002340 [Optional: SC, SS]** The following SC and SS measurements on Caching of Database Responses shall be available to the SC and SS administrators:

- a. Percentage Cache Hit Rate: Percentage of Search requests handled by the cache, updated every 24 hours.
- b. Cache Size: Actual data store in the memory cache (size of the full portion of the cache).
- c. Age of Cache Records: Time stamp when oldest cache record was written into the cache.
- d. Percentage Cache Miss Rate: Percentage of Search requests that were not served by the cache in a period of 1 hour (within that last hour).
- e. Latency: Average latency to process cache requests (time difference between receipt of cache request and return of cache response), measured and updated in 5-minute intervals.
- f. Up and Down times: Specifies the times that the cache was available (Up) or not available (Down), updated every 24 hours.
- g. Active Connections: Average number of SC and SS connections to the cache, measured and updated in 5-minute intervals.

SC and SS products may support other query- and cache-related measurements different than the ones identified above.

**AUX-002350 [Optional: SC, SS]** SC and SS measurements on Caching of Database Responses shall be collected every 1 hour. Other intervals, including 5-min, 15-min, 30-min, and daily, shall also be allowed.

**AUX-002360 [Required: MRDB, Backup MRDB, and LRDB]** The Primary MRDB, Backup MRDB, and LRDB shall support Simple Network Management Protocol version 3 (SNMPv3) interfaces to remote network management systems for the reporting of performance monitoring measurements and statistics.

### 3.3.6.2.6 *Security Management*

This section discusses some of the security features that should be provided by a Routing Database. This includes authentication and authorization of operations personnel and the SCs and SSs that send LDAP messages to the Routing Database. Both remote and local accesses to the Routing DBs are included here.

The MRDB and LRDB perform different functions. The MRDB and its Backup MRDB are primarily “write” databases, in which updates on HR and Commercial Cost Avoidance routing are centrally aggregated and managed for distribution to the LRDBs. The latter, in turn, are responsible for all the “reads” or LDAP Search requests launched by the SCs and SSs to determine the correct routing paths for HR and CCA calls.

For both types, the “read” DBs and the “write” DBs, the DBs contain important information that should be made available only to authorized DISA personnel. DBAs are expected to implement a password policy for authorized personnel and different levels of access. DBAs also create user authorization lists for each database. Only entities with credentials that match entries on the authorization list will be allowed access.

**AUX-002370 [Required: MRDB, Backup MRDB, and LRDB]** The MRDB, Backup MRDB, and LRDB shall be configured with an “authorization list” that contains authorized users and their access levels. The list shall support user IDs and passwords, as well as IP addresses and DOD PKI certificates for Database workstations, SCs, and SSs, for authorized personnel.

The DBs shall use DOD PKI certificates and negotiated TLS sessions in all their communications with Database workstations (both local and remote), SCs, and SSs.

**AUX-002380 [Required: MRDB, Backup MRDB, and LRDB]** The MRDB, Backup MRDB, and LRDB shall accept and process requests only from Database clients (SCs, SSs, and other DBs) with LDAP Bind requests containing credentials that match credentials on the “authorized” list.

**AUX-002390 [Required: MRDB, Backup MRDB, and LRDB]** The DBMS interfaces (e.g., craftsperson workstations) managing the MRDB, Backup MRDB, and LRDB shall not store, transmit, or display any LDAP client passwords in the clear.

**AUX-002400 [Required: MRDB, Backup MRDB, and LRDB]** The MRDB, Backup MRDB, and LRDB shall support the capability to provide remote, high bandwidth access to authorized craftsperson or administrator workstations. The DBAs shall be able to configure an authorization list in each MRDB, Backup MRDB, and LRDB, specifying the authorized craftsperson/DBA identities and the type of access or transactions allowed for each identity.

**AUX-002410 [Required: MRDB, Backup MRDB, and LRDB]** The MRDB, Backup MRDB, and LRDB shall support the capability to provide a visual GUI display for remote, high-bandwidth access to authorized craftsperson or administrator stations.

### 3.3.7 Hybrid Routing Requirements for Preventing PRI “Hairpin” Routes

This section provides requirements for SSs and DSN multifunction switches (MFSs) to support HR calls over T1.619A PRI interfaces. The requirements apply to SSs, SS MGs, and MFSs.

The goal of these requirements is to prevent PRI “hairpinning” of HR calls, when those calls are routed from the MFS to the SS MG (so that the SS can query the RTS Routing Database on those calls), and then routed back from the SS MG back to the MFS again for call completion. The reason that the SS returns the call to the MFS is one of the following:

- The Routing Database responds to the SS’s HR query for the DSN number and indicates “Number Not Found.”
- The Database responds to the SS’s HR query for the DSN number, and indicates “Number Found,” but provides no SC CCA-ID or SS CCA-ID values.

A routing “hairpin” would occur if the MFS routed the call to the SS MG on one ISDN PRI B-Channel, and the SS MG then routed the call back to the MFS on another ISDN PRI B-Channel. This would tie up two PRI B-Channels for the duration of each HR call that was originated on the TDM DSN, routed to an SS for access to the Routing Database, and then returned to the MFS for completion to a destination EO, Small End Office (SMEO), or PBX.

Since the goal is to not to tie up any PRI B-Channels for the duration of each TDM-originated-and-TDM-terminated HR call, a feature is needed that eliminates these routing “hairpins” on the T1.619A PRI between the SS MG and the MFS. This section provides requirements for two features that eliminate these routing hairpins:

- ISDN PRI Two B-Channel Transfer (TBCT).
- DSN HR.

Both of these features are existing MFS PRI features (or enhancements to existing MFS PRI features) that are available on DISA MFSs today.

SSs and their MGs are required to support both of these features so that they will be interoperable with the various MFSs in the DISA TDM network today for HR calls. The MFSs are required to support at least one of these features, so that they support at least one mechanism for eliminating PRI routing hairpins on MFS-to-SS-to-MFS HR calls.

**AUX-002420 [Required: SS MG, MFS]** The short marking in this section is an abbreviated version of this longer marking: [**Required: SS, SS MG, MFS**]. The longer marking means that the requirement is applicable to the SS, the SS MG, and the MFS.

**AUX-002430 [Required: SS MG, MFS]** These network appliances shall not perform any T1.619A PRI routing hairpins on HR calls that are originated on the DISA TDM network, processed by the SS using the RTS Routing Database, and then terminated on the DISA TDM network. These network appliances shall use “routing hairpin elimination” features to prevent these routing hairpins from occurring on these HR calls.

---

**AUX-002440 [Required: SS MG]** The SS and its MG shall support both of the following “routing hairpin elimination” features on its T1.619A PRIs (the PRIs between the MG and the MFS):

- ISDN PRI TBCT (per the SS requirements in [Section 3.3.7.1](#), SS and MFS Requirements for TBCT).
- DSN HR (per the SS requirements in [Section 3.3.7.2](#), SS and MFS Requirements for DSN HR).

**AUX-002450 [Required: SS MG]** The SS and its MG shall support these features on both Routine and Precedence calls. The SS and its MG shall also allow these Routing and Precedence calls to be pre-empted by the PRI multilevel precedence and preemption (MLPP) feature when these “routing hairpin elimination” features are in use on these calls.

**AUX-002460 [Required: MFS]** The MFS shall support at least one of the following “routing hairpin elimination” features on its T1.619A PRIs (the PRIs between the MFS and the SS MG):

- ISDN PRI TBCT (per the MFS requirements in [Section 3.3.7.1](#), SS and MFS Requirements for TBCT).
- DSN HR (per the MFS requirements in [Section 3.3.7.2](#), SS and MFS Requirements for DSN HR).

**AUX-002470 [Required: MFS]** The MFS shall support these features on both Routine and Precedence calls. The MFS shall also allow these Routing and Precedence calls to be pre-empted by the PRI MLPP feature when these “routing hairpin elimination” features are in use on these calls.

**AUX-002480 [Required: MFS]** Any preexisting MFS restrictions that prevent the PRI TBCT feature from being used with Precedence calls or the PRI MLPP feature shall be removed for HR calls so that the aforementioned requirements can be met.

### ***3.3.7.1 SS and MFS Requirements for TBCT***

#### ***3.3.7.1.1 SS Requirements for TBCT***

**AUX-002490 [Required: SS MG]** The SS and its MG shall support the ISDN PRI TBCT feature, per the following Telcordia requirements document:

- GR-2865-CORE, Generic Requirements for ISDN PRI Two B-Channel Transfer, Issue 3, March 2000.

**AUX-002500 [Required: SS MG]** The SS and its MG shall support these requirements for both Routine and Precedence calls. The SS and its MG shall also allow these Routine and Precedence calls to be pre-empted by the PRI MLPP feature when the TBCT feature is in use on these calls.

**AUX-002510 [Required: SS MG]** The SS and its MG shall also support these requirements on the DISA T1.619A PRI, even though the requirements were originally written for commercial U.S. National ISDN PRIs.

**AUX-002520 [Required: SS MG]** GR-2865-CORE describes TBCT operation on two sides on the ISDN PRI: the “network side” [the “Stored Program Control Switch (SPCS)”] and the “user-side” (the “TBCT controller”). The SS and its MG shall follow the GR-2865-CORE requirements for the “user-side” of the PRI TBCT feature (the MFS operates as the “network-side”).

**AUX-002530 [Required: SS MG]** The SS and its MG shall also support the “user-side” TBCT requirements for the “TBCT controller” in the following Telcordia document:

- SR-4994, 2000 Version of National ISDN Primary Rate Interface (PRI) Customer Premises Equipment Generic Guidelines, Issue 1, December 1999:
  - Section 11.5, PRI Two B-Channel Transfer.

The SR-4994, Section 11.5 “user-side” TBCT requirements are more specific than the GR-2865-CORE “user-side” TBCT requirements.

#### *3.3.7.1.2 MFS Requirements for TBCT*

The requirements in this section are Conditional for the MFS. If the MFS supports the ISDN PRI TBCT feature as a mechanism for eliminating PRI routing hairpins, then the following requirements apply.

**AUX-002540 [Conditional: MFS]** The MFS shall support the ISDN PRI TBCT feature, per Telcordia GR-2865-CORE.

**AUX-002550 [Conditional: MFS]** The MFS shall support these requirements for both Routine and Precedence calls. The MFS shall also allow these Routine and Precedence calls to be pre-empted by the PRI MLPP feature when the TBCT feature is in use on these calls.

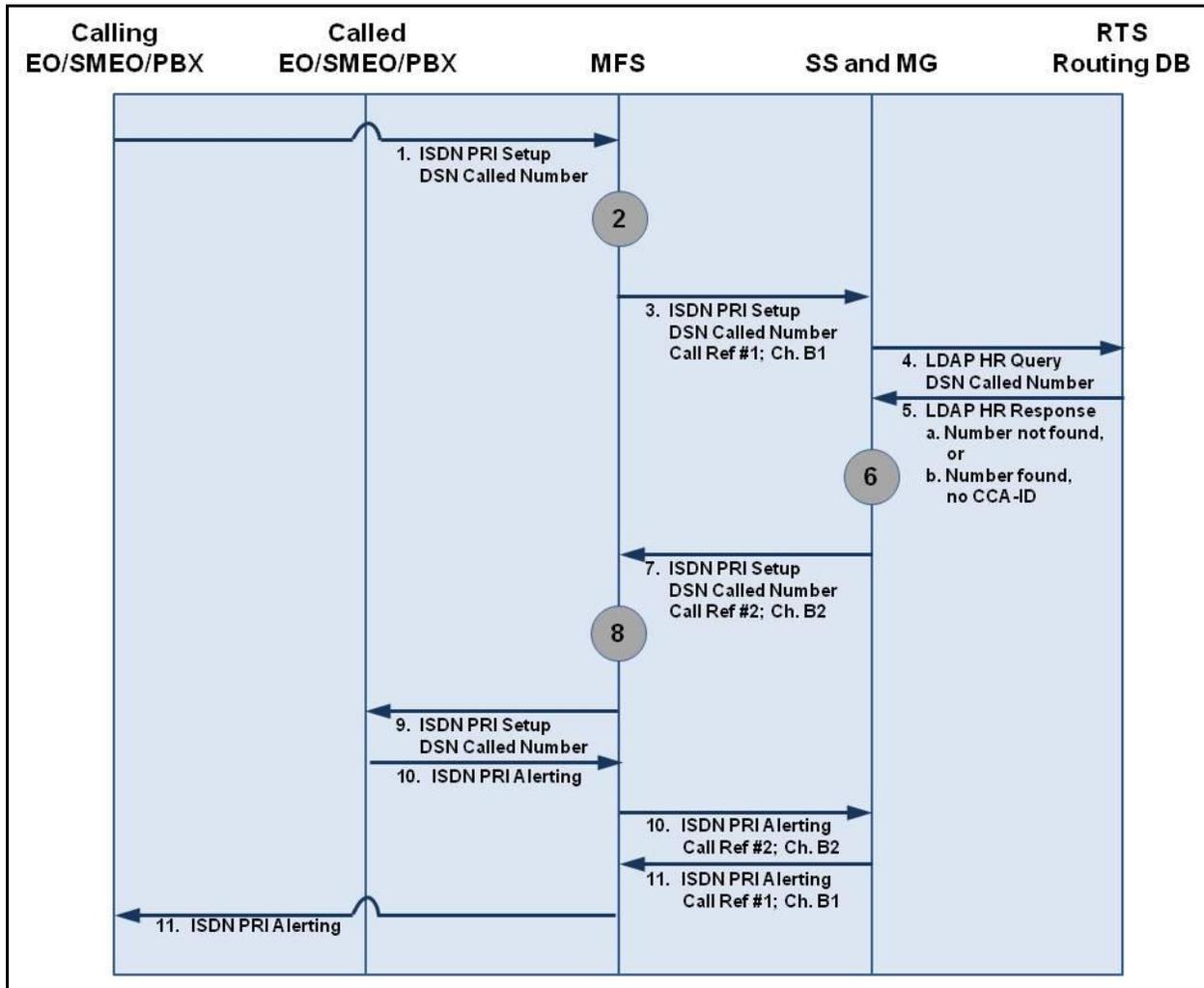
**AUX-002560 [Conditional: MFS]** The MFS shall also support these requirements on the DISA T1.619A PRI, even though the requirements were originally written for commercial U.S. National ISDN PRIs.

**AUX-002570 [Conditional: MFS]** GR-2865-CORE describes TBCT operation on two sides on the ISDN PRI: the “network side” and the “user side.” The MFS shall follow the requirements for the “network-side” of the PRI TBCT feature (the SS and its MG operate as the “user-side”).

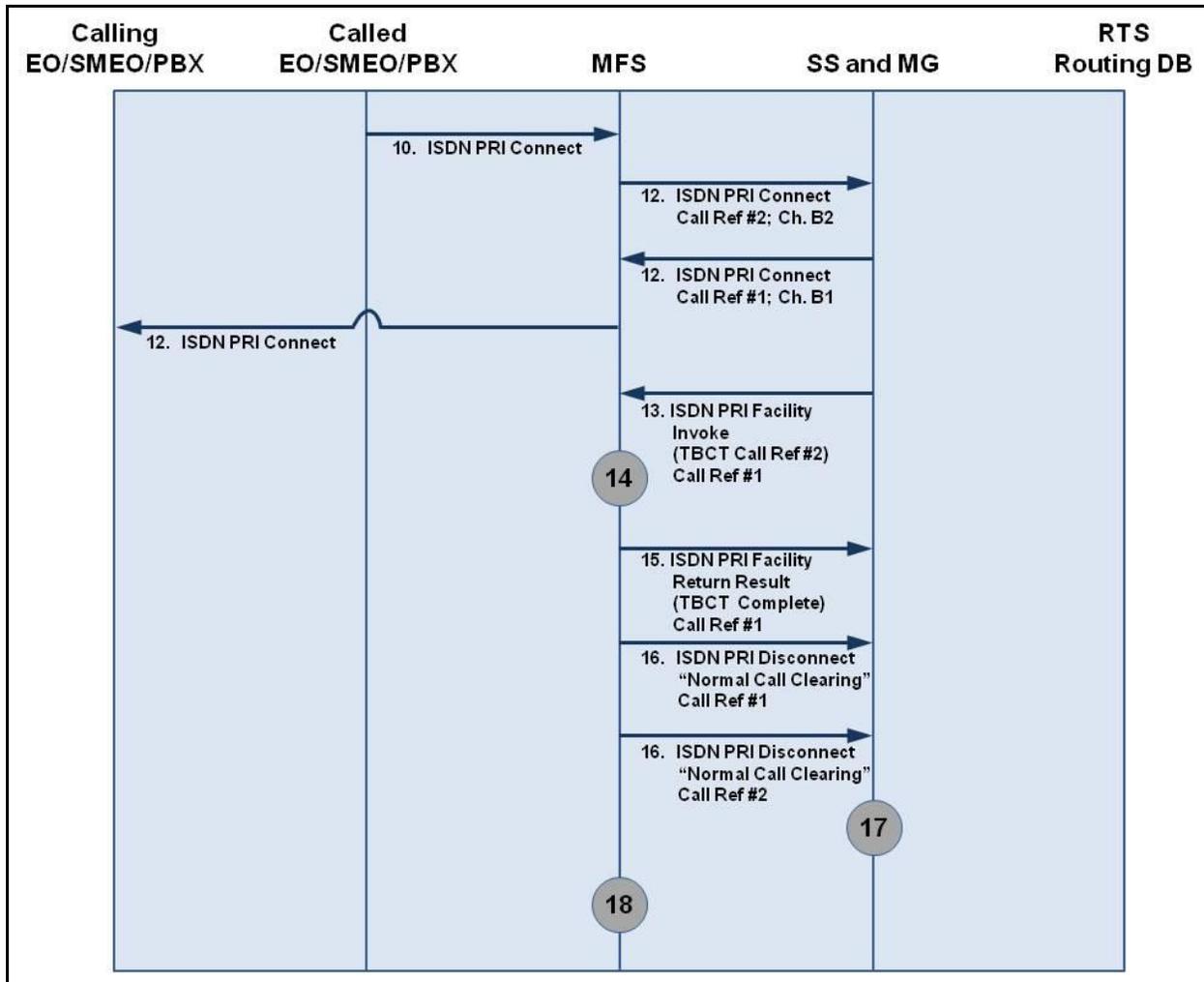
#### *3.3.7.1.3 SS and MFS HR Call Flow Using TBCT*

The following requirements apply when PRI TBCT is used between the SS (and its MG) and the MFS to prevent routing hairpins. The MFS is assumed to support the ISDN PRI TBCT feature in this case.

**AUX-002580 [Required: SS MG, MFS]** The SS, the SS MG, and the MFS shall support the entire following call flow for completion of HR calls and hairpin prevention using PRI TBCT. The call flow consists of both the following figures and the numbered steps that follow the figures. [Figure 3.3-4](#) and [Figure 3.3-5](#) show the first part of the SS and MFS HR call flow using TBCT.



**Figure 3.3-4. SS and MFS HR Call Flow Using TBCT – Part 1**



**Figure 3.3-5. SS and MFS HR Call Flow Using TBCT – Part 2**

1. The MFS receives an incoming call to a DSN number from a calling party on a line-side interface or a trunk-side interface that is different from the T1.619A PRI trunk group that connects the MFS and the SS MG.
2. The MFS checks its routing tables for the called DSN number, for the case in which the call arrived on a line-side interface or a trunk-side interface that is different from the T1.619A PRI connecting the MFS and the SS MG. The MFS then determines that the outgoing route for that number is the T1.619A PRI trunk group that connects the MFS and the SS MG.
3. The MFS routes the call request to the SS MG using this T1.619A PRI trunk group. This “first leg” of the call request is established using an ISDN SETUP message and uses one ISDN B-Channel and one ISDN call reference on that T1.619A PRI.
4. The SS MG accepts this call request from the MFS and directs the call request to the SS for further routing. The SS inspects the called number value and determines that an HR query to the RTS Routing Database is required. The SS performs this HR query per the requirements in [Section 3.3.2](#), SS to LRDB Interface: Database Queries for HR.

- 
5. The RTS Routing Database responds to the HR query with one of the following two results:
    - a. Number not found.
    - b. Number found, but no SC CCA-ID or SS CCA-ID is available.
  6. In both cases, the SS determines that the HR call needs to be returned to the SS MG, T1.619A PRI, and MFS for call completion, since the Database response indicated that the called number was not served by an SC on the UC network. The SS then returns the call to the SS MG.
  7. The SS MG routes the call request back to the MFS using the same T1.619A PRI trunk group on which the call entered the MG. This “second leg” of the call request is established using a second ISDN SETUP message and uses a second ISDN B-Channel and a second ISDN call reference on that T1.619A PRI.
  8. At this point, the MFS receives an incoming call to the called DSN number from the T1.619A PRI trunk group that connects the MFS and the SS MG. From the MFS standpoint, this is a completely separate call request from the previous call request that it directed to the SS MG, even though the two call requests have the same DSN called number.

The MFS then checks its routing tables for the called DSN number, for the case in which the call arrived on a trunk-side interface that is the T1.619A PRI connecting the MFS and the SS MG.

This means that the MFS must maintain two distinct outgoing routes for calls to the DSN called number: one for use when the call enters the MFS on a line-side interface or a trunk-side interface that is different from the MFS-to-SS-MG PRI, and another for use when the call enters the MFS on a trunk-side interface that is the MFS-to-SS-MG PRI.

The MFS needs to maintain these two distinct outgoing routes independent of whether it supports PRI TBCT or DSN HR. The first outgoing route is used to route calls from the MFS toward the RTS Routing Database. The second outgoing route is used to route calls from the MFS to the destination EO, SMEO, or PBX in the DISA TDM network after the RTS Routing Database has processed the call.

The second outgoing route is also used (and is needed) in the case in which an IP end user on an SC in the UC network calls the DSN number. The call is routed to the SS by UC SIP trunks; the SS sends an HR query to the RTS Routing Database; the Database indicates “Number Not Found” (or “SC and SS CCA-ID” not found); the SS routes the call over to the DSN MFS for call completion; and the MFS routes the call to the destination EO, SMEO, or PBX. Note that there is no need to use either PRI TBCT or DSN HR in this case because the call originates on the UC network and completes on the DISA TDM network.

9. After checking its routing tables for the second call request to the DSN called number, the MFS determines that the outgoing route for that number is a route toward the destination EO, SMEO, or PBX on the DISA TDM network (which is different from the T1.619A PRI route

---

back toward the SS MG). This destination EO, SMEO, or PBX may be directly accessible from the MFS, or it may be accessible from another MFS (or pair of MFSs) in the DISA TDM network. In the latter case, the MFS then has to route the second call request toward this destination via that other MFS in the network.

10. Once the second call request is routed to the destination EO, SMEO, or PBX, that EO/SMEO/PBX will return an ISDN ALERTING or PROGRESS message (indicating that the call is ringing), followed by an ISDN CONNECT message (indicating that the call is answered). The MFS providing TBCT receives these ISDN messages back from the destination EO, SMEO, or PBX, and then relays them to the SS MG using the second ISDN call reference on the T1.619A PRI between the MFS and the SS MG.
11. Once the SS MG receives an ISDN ALERTING or PROGRESS message from the MFS using the second ISDN Call reference, it relays that ISDN ALERTING or PROGRESS message back to the MFS using the first ISDN call reference. (The ISDN ALERTING message is analogous to the UC SIP 180 Ringing response. The ISDN PROGRESS message is analogous to the UC SIP 183 Session progress response.)
12. Once the SS MG receives an ISDN CONNECT message from the MFS using the second ISDN Call reference, it relays that ISDN CONNECT message back to the MFS using the first ISDN call reference. (The ISDN CONNECT message is analogous to the UC SIP 200 OK response.)
13. Since the two PRI call legs are both “answered,” the SS MG now requests TBCT by sending an ISDN FACILITY message to the MFS. This message contains a Facility Information Element that contains an Invoke component which contains the “TBCT” operation (the “enhancedExplicitEctExecute” operation), per GR-2865-CORE and SR-4994, Section 11.5.  
  
If the SS MG sends this FACILITY message using the first ISDN call reference, then the TBCT operation must contain a “link ID” parameter that contains the value of the second ISDN call reference.  
  
If the SS MG sends this FACILITY message using the second ISDN call reference, then the PRI TBCT operation must contain a “link ID” parameter that contains the value of the first ISDN call reference.  
  
(PRI TBCT requires at least one of the two call legs to be answered before the two call legs can be transferred together. For HR calls, it is simpler if both call legs are answered before the two call legs are transferred together, since an answer condition on one call leg immediately causes an answer condition on the other call leg.)
14. Upon receipt of the ISDN FACILITY message from the SS MG containing the “TBCT” operation, the MFS internally transfers the two call legs together. Specifically, the MFS transfers the first call leg (established MFS-to-MG, using the first ISDN B-Channel and the first ISDN call reference) and the second call leg (established MG-to-MFS, using the second

ISDN B-Channel and the second ISDN call reference) together, using an internal MFS transfer capability.

At this point, the signaling and media paths for the end-to-end call are completely within the DISA TDM network, and the two PRI call legs can be removed from the T1.619A PRI between the MFS and the SS MG.

15. The MFS returns a second ISDN FACILITY message to the SS MG containing a Facility Information Element containing a Return Result component. This Return Result component indicates the successful completion of the “TBCT” operation. The MFS sends this second ISDN FACILITY message to the SS MG using the same ISDN call reference on which the first MG-to-MFS ISDN FACILITY message was received.
16. The MFS then returns a first ISDN DISCONNECT message to the SS MG using the first ISDN call reference, and at the same time returns a second ISDN DISCONNECT message to the SS MG using the second ISDN call reference. Both ISDN DISCONNECT messages contain Cause Code #16, “Normal Call Clearing.”

If the MFS-to-MG DISCONNECT message sent on the first call reference is followed by the receipt of an MG-to-MFS DISCONNECT message on the same call reference, then the MFS has to be able to resolve the two competing DISCONNECT messages and still disconnect that call leg.

If the MFS-to-MG DISCONNECT message sent on the second call reference is followed by the receipt of an MG-to-MFS DISCONNECT message on the same call reference, then the MFS has to be able to resolve the two competing DISCONNECT messages and still disconnect that call leg.

17. After receipt of the first ISDN DISCONNECT message from the MFS using the first ISDN call reference, the SS MG completes the disconnection of the MFS-to-MG call leg on its side of the T1.619A PRI.

After receipt of the second ISDN DISCONNECT message from the MFS using the second ISDN call reference, the SS MG completes the disconnection of the MG-to-MFS call leg on its side of the T1.619A PRI.

18. Once the two call legs between the MFS and the SS MG have been disconnected, the SS and its MG are removed from the end-to-end answered call to the DSN called number. This end-to-end call is now completely within the DISA TDM network, and the signaling and media paths for that call are completely within the DISA TDM network.

### 3.3.7.2 SS and MFS Requirements for DSN HR

#### 3.3.7.2.1 SS Requirements for DSN HR

**AUX-002590 [Required: SS MG]** The SS and its MG shall support the DSN HR feature. The details of DSN HR feature operation are in [Section 3.3.7.2.3](#), SS and MFS HR Call Flow Using DSN HR.

The key differences between DSN HR and PRI TBCT are as follows:

- DSN HR uses a single ISDN call leg, single ISDN B-Channel, and single ISDN call reference between the SS MG and the MFS.
- DSN HR uses an ISDN DISCONNECT message with Cause Code #1, Unallocated (unassigned) number, in the SS-MG-to-MFS direction. There is no SS-MG-to-MFS SETUP message (establishing a second call leg) or SS-MG-to-MFS FACILITY message (transferring two call legs together) in this case.
- In DSN HR, MFS routing of the call request toward the destination EO, SMEO, or PBX is based on the receipt of the ISDN DISCONNECT message with Cause Code #1 from the SS MG, instead of receipt of a second ISDN SETUP message with the DSN called number from the SS MG.
- DSN HR requires that the MFS support an “Alternate Routing” capability, in which the primary MFS route for the DSN called number is the T1.619A PRI between the MFS and the SS MG, and the alternate MFS route for the DSN called number is the DISA TDM network route from that MFS to the destination EO, SMEO, or PBX.

Calls leave the MFS for the MG using the primary route and are “route advanced” to the alternate route (toward the destination EO/SMEO/PBX) upon receipt of the ISDN DISCONNECT message with Cause Code #1 from the MG. The “alternate route” may also be an ordered set of routes (secondary route, tertiary route, etc.) that lead to different TDM network paths from the “DSN HR” MFS toward the destination EO, SMEO, or PBX.

Alternate routes are typically used in cases in which the primary route is busy or out of order, and the call needs to be routed using an alternate route. In the DSN HR feature, alternate routes are also used when the call is offered to the primary route, and the primary route returns an indication that the call attempt has been rejected because the called number is unallocated/unassigned (ISDN DISCONNECT message, Cause Code #1).

- In DSN HR, the MFS-to-SS MG call leg is cleared by the ISDN DISCONNECT message that the SS MG sends to the MFS, using the single ISDN call reference on the single ISDN call leg. In PRI TBCT, the MFS is responsible for clearing both the ISDN call legs, using two separate MFS-to-MG ISDN DISCONNECT messages on two separate ISDN call references.

**AUX-002600 [Required: SS MG]** The SS and its MG shall support the DSN HR requirements for both Routine and Precedence calls. The SS and its MG shall also allow these Routine and

---

Precedence calls to be pre-empted by the PRI MLPP feature when the DSN HR feature is in use on these calls.

**AUX-002610 [Required: SS MG]** The SS and its MG shall support the DSN HR requirements on the DISA T1.619A PRI. The DSN HR feature is not applicable to commercial U.S. National ISDN PRIs.

#### *3.3.7.2.2 MFS Requirements for DSN HR*

The requirements in this section are all Conditional for the MFS. If the MFS supports the DSN HR feature as a mechanism for eliminating PRI routing hairpins, then the following requirements apply.

**AUX-002620 [Conditional: MFS]** The MFS shall support the DSN HR feature. The details of DSN HR feature operation are in [Section 3.3.7.2.3](#), SS and MFS HR Call Flow Using DSN HR.

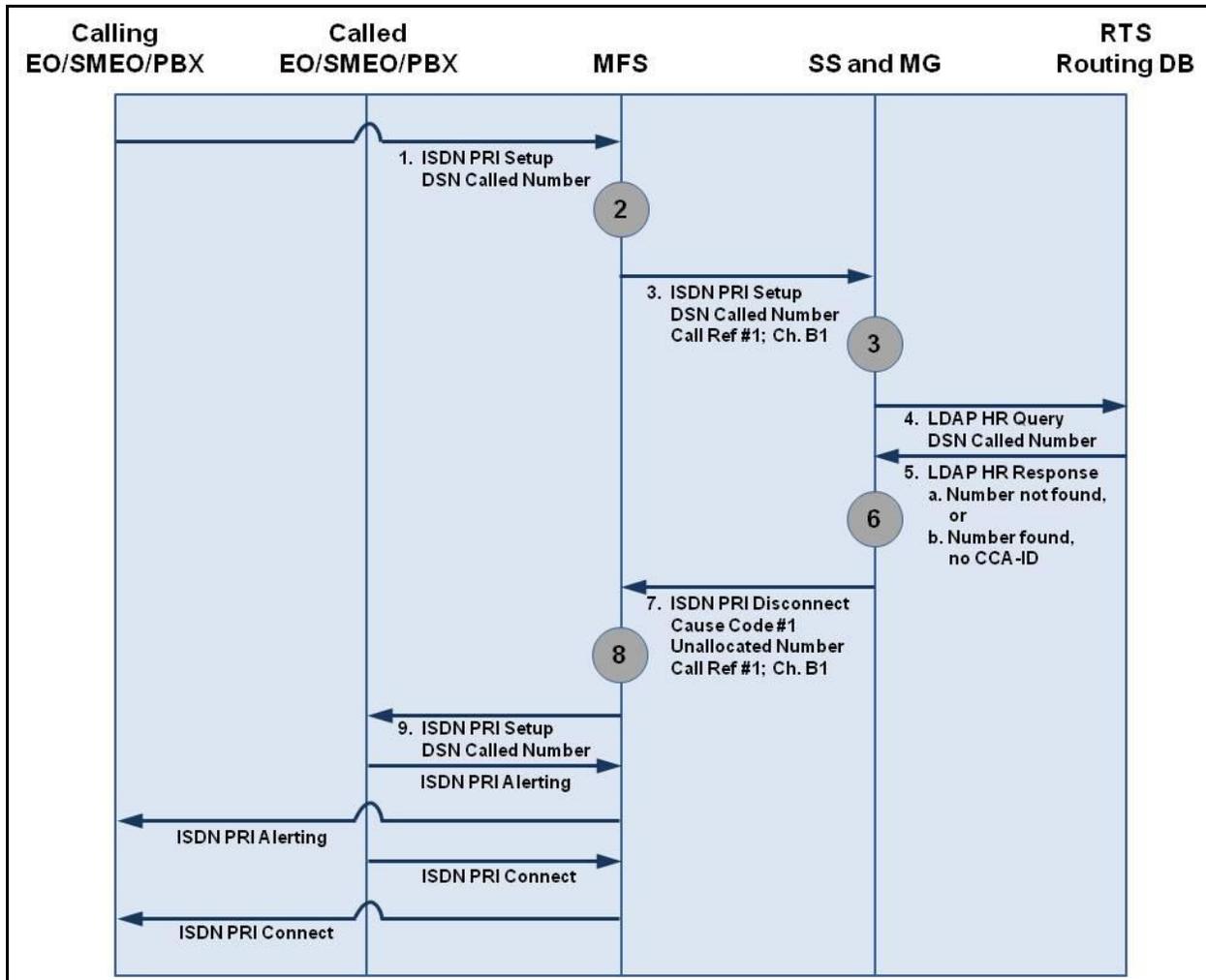
**AUX-002630 [Conditional: MFS]** The MFS shall support the DSN HR requirements for both Routine and Precedence calls. The MFS shall also allow these Routine and Precedence calls to be pre-empted by the PRI MLPP feature when the DSN HR feature is in use on these calls.

**AUX-002640 [Conditional: MFS]** The MFS shall support the DSN HR requirements on the DISA T1.619A PRI. The DSN HR feature is not applicable to commercial U.S. National ISDN PRIs.

#### *3.3.7.2.3 SS and MFS HR Call Flow Using DSN HR*

The following requirements apply when DSN HR is used between the SS (and its MG) and the MFS to prevent routing hairpins. The MFS is assumed to support the DSN HR feature in this case.

**AUX-002650 [Required: SS MG, MFS]** The SS, the SS MG, and the MFS shall support the entire following call flow for completion of HR calls and hairpin prevention using DSN HR. The call flow consists of both [Figure 3.3-6](#) and the numbered steps that follow it.



**Figure 3.3-6. SS and MFS HR Call Flow Using DSN HR**

Steps 1 through 6 in this call flow are identical to Steps 1 through 6 in the PRI TBCT call flow in [Section 3.3.7.1.3](#), SS and MFS HR Call Flow using TBCT. The last three paragraphs from Step 8 in the TBCT call flow also apply.

- The SS MG returns the call to the MFS by sending the MFS an ISDN DISCONNECT message containing Cause Code #1, unallocated (unassigned) number. The MG sends this ISDN DISCONNECT message on the SS-MG-to-MFS PRI, using the same ISDN call reference that the MFS used to send the previous ISDN SETUP message to the MG. The MG also disconnects from the MFS-to-MG call leg on its side of the T1.619A PRI.

This ISDN DISCONNECT message removes the HR call request from the MFS-to-MG interface, and returns the call to the MFS for further routing. At this point, the SS and the SS MG are completely removed from the call request to the DSN called number.

8. Upon receipt of the ISDN DISCONNECT message with Cause Code #1, the MFS “DSN HR” feature uses the MFS “Alternate Routing” feature to route the call request toward the destination EO, SMEO, or PBX in the DISA TDM network.

The “Alternate Routing” feature is set up so that the primary MFS route for the DSN called number is the T1.619A PRI between the MFS and the SS MG, and the alternate MFS route for the DSN called number is the TDM network route from that MFS toward the destination EO, SMEO, or PBX. The “alternate MFS route” may also be an ordered set of routes that represent different TDM network paths from the “DSN HR” MFS toward the destination EO, SMEO, or PBX.

This destination EO, SMEO, or PBX may be directly accessible from the MFS, or it may be accessible from another MFS (or pair of MFSs) in the DISA TDM network. In the latter case, the MFS then has to route the call request toward this destination via the other MFS in the network.

If the DSN HR feature was not used in the MFS, then the receipt of the ISDN DISCONNECT message with Cause Code #1 from the SS MG would result in rejection of the call request on the DISA TDM network, and the playback of a call denial announcement to the calling party (e.g., “Your call cannot be completed as dialed. Please check the number and try again.”). The use of DSN HR in MFS allows call requests receiving these “DISCONNECT/Cause Code #1” treatments to be “route advanced” to other network routes using Alternate Routing, instead of being rejected and connected to a call denial announcement.

9. The MFS then routes the call request to the destination EO, SMEO, or PBX on the DISA TDM network. The call request is handled on the DISA TDM network from this point forward and may be answered, forwarded, diverted to an attendant, or rejected at the called party interface. The signaling and media paths for this call remain completely within the DISA TDM network, because the SS MG removed the UC network from the call request when it returned the ISDN DISCONNECT message to the MFS.

### **3.4 UC AUDIO AND VIDEO CONFERENCE SYSTEM**

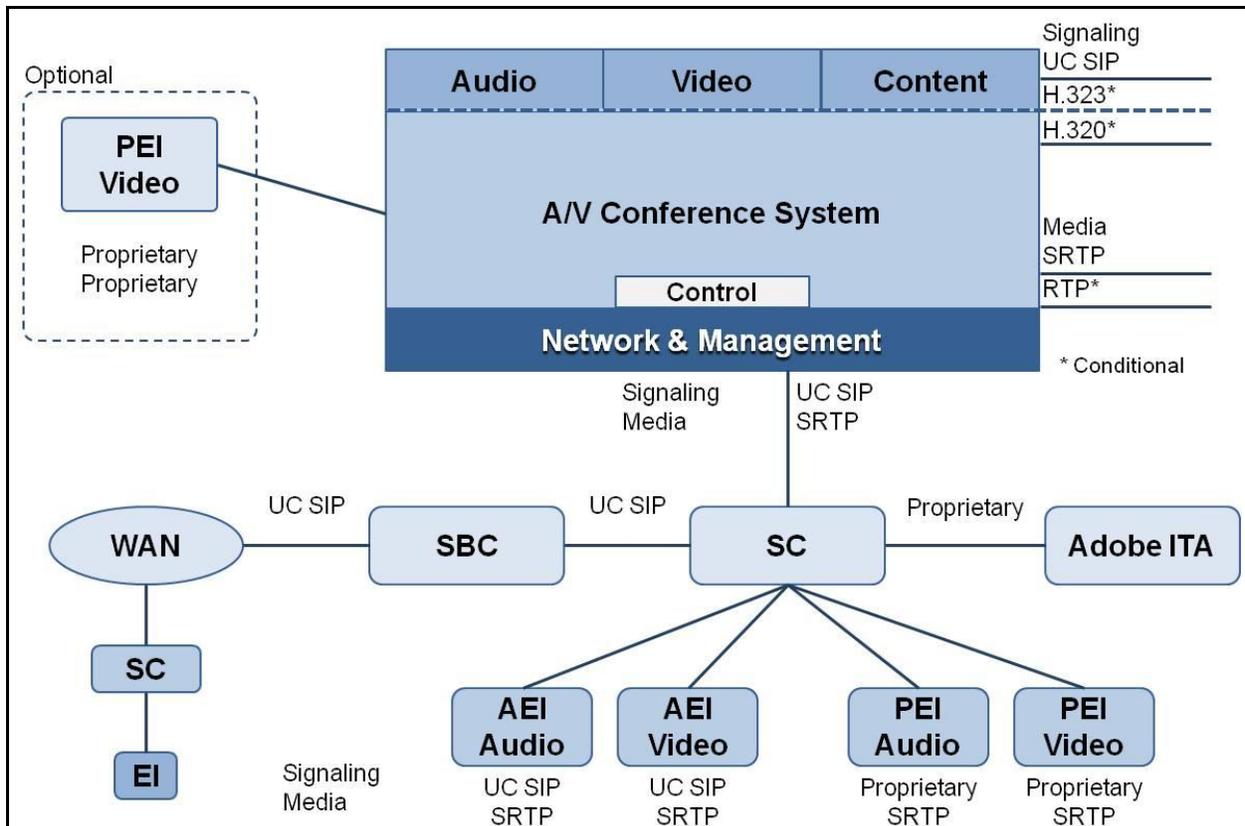
UC Conference System (UCCS) requirements in this section that are marked “AO” apply to systems that support conferences for only audio end instruments (i.e., voice phones).

Requirements that are marked “VO” apply to systems that support conferences only for video end instruments (i.e., video terminals). Requirements for systems that support conferences for both audio and video end instruments are marked “A/V.” Requirements that apply to all types of conference systems are marked “All UCCS.”

NOTE: An audio/visual (A/V) conference system can be implemented as an integrated audio and video product, or as a combination of an audio conference system and a video conference system.

### 3.4.1 Introduction

This section addresses required functionality, performance, capabilities, and associated technical parameters for the assured services audio and video conference system components of the DISN VoIP and Video over IP services. This section's focus is real-time conferencing functions and features that meet the operational needs of the Warfighter and the Government. The concept for including conference systems into the UC DISN voice and video assured services framework is depicted in [Figure 3.4-1](#), UC Conference System Framework.



**Figure 3.4-1. UC Conference System Framework**

The conference system can be viewed as a peripheral device to the SC. At the vendor's option, it can be implemented as a standalone appliance; i.e., as its own System Under Test (SUT) or as an integrated part of the SC SUT. The primary difference between the two options is that a proprietary interface may be used when the network interface component is an integral part of the SC in the same SUT. When implemented as a standalone SUT, UC SIP will be the required interface between the conference system and the SC. When made part of an existing APL SC, the SC will require a new APL certification. The acquisition agent working with the vendors will decide whether to acquire the conference system's network interface as a standalone appliance or as part of an SC. There are no hardware packaging requirements or restrictions on how the vendor chooses to implement the UCCS. A standalone audio conference system can be deployed, a standalone video conference system can be deployed, an audio conference system product can

---

be combined with a separate video conference system product, or an integrated audio/video product can be deployed. H.320 and H.323 gateway devices may be used, but are not required.

Note that Proprietary Video EIs (Proprietary Signaling, Proprietary Media/codecs) can be supported on the “line side” of Video Conference System in cases where the Proprietary Video EI and the Video Conference System are from the same vendor. It is assumed that these Proprietary Video EIs are connected directly to the Video Conference System over IP in this case, and that there is no SC in the signaling path between the Video EI and the Video Conference System. The Video Conference System can provide “normalization” from the proprietary protocol on the EI side to UC SIP on the SC side, in this case.

Proprietary Video EIs and Video Conference Systems can also communicate through an SC using proprietary protocols, if the Video EI, Video Conference System, and SC all support the same proprietary protocol.

Proprietary Video EIs and Video Conference Systems can also communicate with each other through a set of SCs and SSs, but the SCs must provide “normalization” from the proprietary protocol to UC SIP, in this case.

## **3.4.2 System Description**

### ***3.4.2.1 Overall System Description***

The UCCS is intended to provide global real-time audio and video conferencing service capabilities for the DOD. Services include non-secure audio add on, video recording, archive and retrieval, bandwidth management, and seamless connectivity of users and resources. Furthermore, the conference system shall provide reservation and reservationless based scheduling conferencing management capabilities.

### ***3.4.2.2 System Architecture***

**AUX-002660 [Required: All UCCS]** The conference system shall provide, as a minimum, an Ethernet-based interface to the network.

### ***3.4.2.3 Information Assurance***

**AUX-002670 [Required: All UCCS]** The conference system shall meet the Information Assurance requirements of all applicable DISA Security Technical Implementation Guidelines (STIGs).

[Section 3.4.5.1.6](#), Security Management, contains conference system security management requirements.

### 3.4.3 Service

This section describes the service requirements of the conference system.

#### 3.4.3.1 Service Description

This subsection describes the service requirements for the conference system. The system provides a range of conferencing services that allow two or more locations to communicate by means of audio and/or video.

##### 3.4.3.1.1 Registration

**AUX-002680 [Required: All UCCS]** All EIs, external and internal systems, and devices directly utilizing the conferencing system shall be required to register with the system in order to use conferencing services.

This registration requirement is not meant to exclude non-registered EIs and external parties from participating in a conference to which they have been invited by the registered subscriber that scheduled the conference.

[Section 3.4.5.3](#), Registration System, contains conference services registration system requirements.

##### 3.4.3.1.2 Point-to-Point Conferencing

**AUX-002690 [Required: All UCCS]** The conference system shall provide IP-based point-to-point conferencing. Point-to-point conferencing consists of two participants with fully interactive audio and/or video capabilities. The system shall support EIs that are registered with the system to initiate point-to-point, fully interactive audio and video capability communications. This capability shall be supported through conferencing services that enable the resolution of resource conflicts by calendaring and scheduling system application programming interfaces (APIs) with enterprise scheduling systems. It is desired that the UCCS shall provide real-time conferencing status capability; e.g., busy, online, offline.

**AUX-002700 [Required: All UCCS]** The conference system shall support IP-based solutions using UC SIP, **[Optional]** H.323, and **[Optional]** dial-up ISDN H.320 endpoint support.

**AUX-002710 [Required: All UCCS]** The conference system shall support interactive conferences using IP and **[Optional]** ISDN transport. These conferences may consist of Proprietary and UC SIP EIs only, **[Optional]** H.323 EIs only, **[Optional]** H.320 EIs only, or **[Optional]** a combination of H.323 EIs, Proprietary and UC SIP EIs, and H.320 EIs.

NOTE: ISDN transport applies only to conferences involving non-IP EIs.

### 3.4.3.1.3 *Multipoint Conferencing*

**AUX-002720 [Required: All UCCS]** The conference system shall provide multipoint conferencing. A multipoint conference consists of three or more EIs in a conference call and shall include the following functions and features.

**AUX-002730 [Required: All UCCS]** The conference system shall distribute fully interactive video and/or audio streams among multiple participants according to the channel bandwidth of each participant.

**AUX-002740 [Required: VO CS, A/V CS]** The conference system shall accommodate users on the same conference at different video rates, resolutions, and frame rates according to EI capability and not at the lowest common denominator level.

**AUX-002750 [Required: All UCCS]** The conference system shall provide interactive, multipoint conferences using IP transport and [**Optional**] ISDN transport. These conferences may consist of Proprietary and UC SIP EIs only, [**Optional**] H.323 EIs only, [**Optional**] H.320 EIs only, or [**Optional**] a combination of H.323 EIs Proprietary and UC SIP EIs, and H.320 EIs.

NOTE: ISDN transport applies only to conferences involving non-IP EIs.

### 3.4.3.1.4 *Video Performance*

This section describes the criteria and metrics required to ensure audio/video quality during multi-party conferences as well as point-to-point calls.

For planning purposes, the conference system should be designed in accordance with the following guidelines.

**Bit Error Rate.** It is essential for the system to control bit error rate at the lowest possible level.

**Packet Loss.** The end-to-end network design guideline for packet loss percentage is less than 1 percent and may include the use of packet loss concealment.

NOTE: The 1 percent packet loss design guideline is also supported by industry standard document Telecommunications Industry Alliance (TIA)/Electronic Industries Alliance (EIA)/TSB116.

**Latency.** International Telecommunications Union – Telecommunication (ITU-T) Recommendation G.114 recommends that no more than 50 milliseconds be allocated for each of the national and international segments of network transmission. In the international case, there is one originating and one terminating national segment, as well as one international segment resulting in the end-to-end one-way delay limit of 150 milliseconds. In the domestic case, there is one originating and one terminating national segment, resulting in the end-to-end one-way delay limit of 100 milliseconds for domestic connections.

The end-to-end one-way delay guideline is as follows:

- Less than 150 milliseconds for international connections.
- Less than 100 milliseconds for domestic connections.

Jitter. Jitter buffers that temporarily store arriving packets in order to minimize delay variations shall be employed.

#### 3.4.3.1.5 *In-Conference Control*

**AUX-002760 [Required: All UCCS]** The conference system shall provide in-conference control. In-conference control shall include the following functions and features.

**AUX-002770 [Required: VO CS, A/V CS]** The conference system shall provide a banner for each conference.

**AUX-002780 [Required: All UCCS]** The conference system shall provide notification of participants joining and leaving a conference, and provide an end-of-conference warning to all participants.

**AUX-002790 [Required: All UCCS]** The conference system shall provide the ability to extend conferences, without disruption, to conferences in progress.

**AUX-002800 [Required: VO CS, A/V CS]** The conference system shall support presentation capability for different screen layouts locally, manageable by each individual host.

**AUX-002810** The conference system shall provide the following conferencing chair control functionality:

- a. **[Required: VO CS, A/V CS]** Voice-activated switching.
- b. **[Required: All UCCS]** Broadcast mode.
- c. **[Required: All UCCS]** Lecture mode.
- d. **[Required: VO CS, A/V CS]** Video switching with H.243 control.
- e. **[Required: VO CS, A/V CS]** Continuous presence.
- f. **[Required: All UCCS]** Mute – audio/video.

#### 3.4.3.1.6 *Transcoding*

Transcoding converts audio and video media streams, allowing conference participants to communicate with each other even though their EIs are equipped with different encoding/decoding capabilities.

**AUX-002820 [Required: VO CS, A/V CS]** The conference system shall provide transcoding availability regardless of the data speeds; the number of concurrent video calls; and the number of concurrent conferences, video sizes, frame rates, and conference modes (voice switching or

---

continuous presence) without downgrading the conference to a lowest common denominator protocol.

**AUX-002830 [Required: VO CS, A/V CS]** The conference system shall provide automatic video transcoding without downgrading the conference to a lowest common denominator protocol.

**AUX-002840 [Required: AO CS, A/V CS]** The conference system shall provide automatic audio transcoding without downgrading the conference to a lowest common denominator protocol.

#### *3.4.3.1.7 Variable Data Rates*

**AUX-002850 [Required: VO CS, A/V CS]** The conference system shall provide support for variable data rates, the rate at which data (bits) is transmitted, usually expressed in bits per second (bps) per Conferencing Terminal Unit (CTU). The system shall support data rates of at least 64 kilobits per second (kbps) per CTU. The system shall provide speed matching and down speeding to facilitate adjustable data rates. The system shall provide bandwidth management of IP services through gatekeeper policies to restrict the bandwidth used by active call connections to the bandwidth installed and available in the network access connections.

#### *3.4.3.1.8 Audio Add-On*

**AUX-002860 [Required: A/V CS]** The conference system shall provide audio add-on features for audio-only participants in video conferences and support an external VoIP audio conference connecting to the video conference session.

#### *3.4.3.1.9 Interactive Graphics Exchange*

**AUX-002870 [Optional: VO CS, A/V CS]** The UCCS shall provide content sharing capability for participants to interact during video teleconferencing (VTC) sessions that allow participants to view and display the same presentation material at the same time. The system shall provide a dedicated live video stream and a presentation video stream and still-frame graphics as specified in [Section 3.4.3.3.1](#), Compression Algorithms and Audio/Video Protocols. The system shall provide Interactive Graphics Exchange with the following functions and features.

**AUX-002880 [Optional: VO CS, A/V CS]** The conference system shall provide a means to allow participants to interactively view images from external sources with all or any of the participants in the conference.

**AUX-002890 [Optional: VO CS, A/V CS]** The conference system shall provide real-time participation of any combination of EIs. The system shall provide still image exchange as specified in [Section 3.4.3.3.1](#), Compression Algorithms and Audio/Video Protocols.

---

**AUX-002900 [Optional: VO CS, A/V CS]** Interactive graphics exchange capabilities shall include the following:

- a. Point-to-point and multipoint conferencing services.
- b. Interoperability with different vendor EIs and variable graphic resolutions.
- c. Connections among participants using any video EIs, connection types, and at any rates.

#### *3.4.3.1.10 Audio Conferencing*

The conference system shall be able to support audio conferencing and provide the following functions and features.

**AUX-002910 [Required: A/V CS]** The system shall be capable of accepting audio-only participants into a conference call for both scheduled and ad hoc video conferences.

**AUX-002920 [Required: VO CS, A/V CS]** The system shall provide an interface to an external audio conferencing system to allow cascading between a multi-point VTC call with a multi-point audio call through the use of the interface to an external audio conferencing system.

**AUX-002930 [Required: AO CS, A/V CS]** The system shall provide internal conferencing capabilities for the support of audio-only participants.

#### *3.4.3.2 Integrated Services*

This subsection describes services that are to be integrated in a means that provides the customer a user-friendly presentation, request, and access.

##### *3.4.3.2.1 Web Access to Conference System*

**AUX-002940 [Required: All UCCS]** The conference system shall provide a Web-based portal for customer access to the UC conferencing services, features, and capabilities. As the conferencing services change, the Web-based portal shall reflect those changes. Additionally, the conferencing services Web portal shall provide the following:

- a. An enterprise-wide service for the identification and other pertinent information about users, conferencing services, and resources, and makes it accessible from any place at any time.
- b. Awareness of relevant, accurate information about the conferencing service to users at all levels (strategic, operational, and Tactical).
- c. An integrated scheduling system that provides users the ability to schedule one or a combination of video and audio conference services in one Web interface.

### 3.4.3.2.2 *Recorded Content Retrieval and Management*

The following subsections describe the Video and Audio Conferencing Recorded Content Retrieval and Management services to be provided by the system.

#### 3.4.3.2.2.1 Video Conferencing Recorded Content Retrieval

**AUX-002950 [Optional: VO CS, A/V CS]** The conference system shall provide a video conferencing recorded content request and retrieval system in accordance with (IAW) the following requirements.

**AUX-002960 [Optional: VO CS, A/V CS]** The system shall provide the user the ability to view and listen to the recorded video conferences using a Web browser to retrieve streaming video.

**AUX-002970 [Optional: VO CS, A/V CS]** The system shall provide a Web-based system for the meeting moderator to access the recorded video conference call.

**AUX-002980 [Optional: VO CS, A/V CS]** The system shall inform the meeting moderator of the recorded video conference access information immediately after the completion of the video conference.

**AUX-002990 [Optional: VO CS, A/V CS]** The system shall provide Web-based interfaces for users to search recorded content based on the combination of the following information: meeting topic, meeting date/time, keywords provided by meeting moderators, meeting leader name, meeting language, and meeting leader organization.

**AUX-003000 [Optional: VO CS, A/V CS]** The Web interface shall provide a link to the content retrieval launch page.

**AUX-003010 [Optional: VO CS, A/V CS]** The content retrieval launch page shall authenticate the users using PKI and prompt users to enter passwords defined by the meeting moderators during the meeting scheduling phase.

**AUX-003020 [Optional: VO CS, A/V CS]** The content retrieval launch page shall maintain a record of every content request. The record of each request shall include the name, email address, and E.164 number or IP address of the requester; the identification of the recording; and the date and time of the request.

**AUX-003030 [Optional: VO CS, A/V CS]** The content retrieval launch page shall allow users to choose which format of the supported streaming media formats to use when playing back the retrieved content.

**AUX-003040 [Optional: VO CS, A/V CS]** The system shall provide the end user controls during streaming to pause/resume and select segments to play.

**AUX-003050 [Optional: VO CS, A/V CS]** The content retrieval launch page shall allow users to download the stored content of a conference meeting, if this option is permitted by the meeting's moderator.

**AUX-003060 [Optional: VO CS, A/V CS]** The streaming shall comply with the Streaming Service Protocol Requirements described in [Section 3.4.3.3.1](#), Compression Algorithms and Audio/Video Protocols.

**AUX-003070 [Optional: VO CS, A/V CS]** The system shall ensure the compatibility of stored content with the latest versions of media player clients.

#### 3.4.3.2.2.2 Audio Conferencing Recorded Content Management

**AUX-003080 [Optional: AO CS, A/V CS]** The conference system shall provide a content management system IAW the following requirements.

**AUX-003090 [Optional: AO CS, A/V CS]** The content management system shall comply with DOD 5200.1R with clear marking and labeling.

**AUX-003100 [Optional: AO CS, A/V CS]** The content management system shall maintain recorded audio conferencing content ready for users to retrieve anytime for a period of 30 days after the completion of the conferences.

**AUX-003110 [Optional: AO CS, A/V CS]** The content management system shall archive recorded audio conferencing content into permanent storage after 30 days.

**AUX-003120 [Optional: AO CS, A/V CS]** The content management system shall allow users to request stored content from archive. The wait time to retrieve archived material shall be less than one working day.

**AUX-003130 [Optional: AO CS, A/V CS]** The archive material shall be kept at the same fidelity levels of the original recordings. Compression techniques that cause a loss of fidelity are not acceptable encoding schemes for archive material.

### ***3.4.3.3 Interoperability***

**AUX-003140 [Required: All UCCS]** This subsection describes the system's interoperability requirements. The system shall maximize the use of standards-based interfaces. The system shall use functions, protocols, and formats that are publicly available.

**AUX-003150 [Optional: VO CS, A/V CS]** For video equipment, the conference system shall adhere to Federal Telecommunications Recommendation 1080B-2002 (FTR-1080B).

#### ***3.4.3.3.1 Compression Algorithms and Audio/Video Protocols***

**AUX-003160 [Required: VO CS, A/V CS]** The conference system shall support the following audio and video standards for video conferencing:

AUDIO PROTOCOLS	VIDEO PROTOCOLS
G.711	H.261 [Optional]
G.722	H.263-2000
G.722.1	H.264
G.723.1	H.264 (SVC) [Optional]
G.728	
G.729/G.729A	

**AUX-003170 [Required: AO CS, A/V CS]** The conference system shall support the following audio standards for audio-only conferencing:

AUDIO PROTOCOLS
G.711
G.722
G.722.1
G.723.1
G.728
G.729/G.729A

**AUX-003180 [Required: All UCCS]** The conference system shall provide interoperability for all end point devices to support UC SIP, [Optional] H.320, and [Optional] H.323 during call setup.

**AUX-003190 [Required: VO CS, A/V CS]** The conference system, including any proprietary Video EIs, shall support the following:

- a. Sub-Quarter Common Intermediate Format (SQCIF).
- b. Quarter Common Intermediate Format (QCIF).
- c. Full Common Intermediate Format (FCIF, also called CIF).
- d. 4 Full Common Intermediate Format (4FCIF, also called 4CIF).
- e. [Optional] 16 Full Common Intermediate Format (16FCIF, also called 16 Common Intermediate Format (16CIF)).
- f. [Optional] SD and HD video resolution formats for H.261, H.263, and H.264 codecs.

VIDEO FORMAT STANDARDS	VIDEO RESOLUTION
SQCIF	128 x 96
QCIF	176 x 144
SIF(525)	352 x 240
CIF/SIF(625)	352 x 288
4SIF(525)	704 x 480

VIDEO FORMAT STANDARDS	VIDEO RESOLUTION
4CIF/4SIF(625)	704 x 526
16CIF	1408 x 1152
DCIF	528 x 384
SD	720 x 480
HD(720p)	1280 x 720
HD (1080p)	1920 x 1080

**AUX-003200 [Required: VO CS, A/V CS]** The conference system shall ensure that the freeze-frame image feature is compliant with ITU-T H.239 and with H.261 Annex D.

**AUX-003210 [Required: VO CS, A/V CS]** The system's freeze-frame image size shall support 4FCIF (4CIF), VGA, SVGA, XGA, HD, SVTGA, and WSXGA+ when using H.239. When using H.261 Annex D, the freeze-frame image size shall support 4FCIF (4CIF).

#### 3.4.3.3.2 H.320 and H.323 Protocols

**AUX-003220 [Optional: VO CS, A/V CS]** The conference system that supports H.323/H.320 protocols shall meet the following ISDN/PRI, H.323 V4, chair control, serial interfaces, content sharing VTC endpoint protocol requirements:

- a. ISDN PRI on ISDN interfaces (including Alcatel-Lucent 5ESS PRI, GENBAND DMS PRI, and National ISDN PRI).
- b. European E1 ISDN standards.
- c. ISDN bonding up to 1.5 Mbps on T1 and 2 Mbps on E1 per International Organization for Standardization (ISO) 13871.
- d. H.323/320 V4.
- e. Far end camera control (FECC) H.281 and H.323 Annex Q.
- f. Resource Availability Indicator (RAI)/Resource Availability Confirmation (RAC) for load balancing.
- g. Chair control messages per H.246, H.242/H.243.
- h. Direct, H.225 routed, and H.225-H.245 routed modes of H.323 gatekeeper operations.
- i. Quality of Service (QoS) support using DSCP marking of IP packets.
- j. Automatic downspeed to available ISDN/IP bandwidth.
- k. Automatic rate detection to match incoming video calls.
- l. V.35/RS-449/EIA-530 Data Terminating Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) interfaces (The implementation shall use EIA-530 interfaces, and the use of V.35 and RS-449 interfaces shall be phased out where multiple

interfaces are supported in equipment. RS-366 interfaces shall also be supported for dial signaling bypass devices).

m. H.239 for additional video channels or still images.

#### 3.4.3.3.3 UC SIP

The system shall ensure that all conferencing equipment meets the following protocol requirements:

**AUX-003230 [Required: All UCCS]** The UC SIP audio and video signaling conferencing requirements are specified in UC SIP Section 10, Audio and Video Conference Services.

**AUX-003240 [Optional: VO CS, A/V CS]** FECC H.281 and H.323 Annex Q.

**AUX-003250 [Optional: VO CS, A/V CS]** Chair control messages per H.246, H.242/H.243.

**AUX-003260 [Required: All UCCS]** QoS support using DSCP marking of IP packets.

**AUX-003270 [Required: VO CS, A/V CS]** Automatic downspeed to available IP bandwidth.

**AUX-003280 [Required: VO CS, A/V CS]** Automatic rate detection to match incoming video calls.

**AUX-003290 [Optional: All UCCS]** Support T.140 for text messages.

**AUX-003300 [Optional: VO CS, A/V CS]** H.261 Annex D for still images.

#### 3.4.3.3.4 Video Mixing Modes

The conference system shall ensure that all video mixing modes meet the following standards.

**AUX-003310 [Required: VO CS, A/V CS]** Video Switching Mode. The system shall ensure that the system supports video switching according to H.243 and H.323. The design shall minimize the time to switch and the disruption of video when switching from one video source to another.

**AUX-003320 [Required: VO CS, A/V CS]** Video Mixing (Picture Composition or Continuous Presence Mode). The system shall ensure that the system supports video mixing functions according to H.243 and H.323. The system shall support enhanced continuous presence multiple video mixing to include the 7 plus 1 format.

#### 3.4.3.3.5 In-Conference Chair Control

The conference system shall ensure that the system supports chair control standards as defined in H.230, H.246, H.242, H.243 and H.245, including standards supporting Broadcast and Lecture mode capabilities. The following shall be supported:

**AUX-003330 [Optional: VO CS, A/V CS]** H.320 chair control messages and procedures as defined in H.230, H.242, H.243 and H.245.

**AUX-003340 [Optional: VO CS, A/V CS]** H.323 multipoint conferencing units (MCUs) shall support chair control messages and procedures as defined in H.323 and as carried forward to H.323 from H.243.

**AUX-003350 [Optional: VO CS, A/V CS]** H.323 – H.320 gateways shall follow the H.246 message translation tables related to chair control functions.

#### 3.4.3.3.6 *Audio Conferencing*

The conference system shall ensure audio systems support the following requirements:

**AUX-003360 [Required: AO CS, A/V CS]** Audio systems shall support in-dial and out-dial IAW the DISN World Wide Numbering Plan and the PSTN North American dialing plans.

TDM requirements include the following:

**AUX-003370 AUX-003260 [Optional: AO CS, A/V CS]** The audio system's PSTN interfaces shall support T1/E1 (AT&T TR62411 or Telcordia TR-NWT-000170).

**AUX-003380 AUX-003270 [Optional: AO CS, A/V CS]** The audio system's CAS interfaces shall support Alcatel-Lucent 5ESS and GENBAND DMS switches.

**AUX-003390 AUX-003280 [Optional: AO CS, A/V CS]** The audio system's T1 PRI interfaces shall support Non-Facility Associated Signaling (NFAS) and D-channel backup, if the audio system supports more than two PRIs.

**AUX-003400 AUX-003290 [Optional: AO CS, A/V CS]** The audio system's T1 interface shall support extended super frame (ESF) framing and with bipolar with eight-zero substitution (B8ZS)/ Alternate Mark Inversion (AMI) coding.

**AUX-003410 AUX-003300 [Optional: AO CS, A/V CS]** The audio system's PSTN signaling module shall support ISDN PRI (5ESS, DMS, and National ISDN), and the PRI flavors of foreign countries such as Germany, Japan, and Korea.

**AUX-003420 AUX-003310 [Optional: AO CS, A/V CS]** The audio system shall support the Dialed Number Identification Service (DNIS) feature where the original dialed numbers are presented as generic address parameters (GAPs).

**AUX-003430 AUX-003320 [Optional: AO CS, A/V CS]** The audio system shall support the automatic number identification (ANI) feature and use it to identify a calling party, if applicable.

VoIP requirements include the following:

**AUX-003440 [Required: AO CS, A/V CS]** The audio system IP interfaces shall support static assignment of the IP address, mask, default router, and Domain Name Service (DNS) entries.

**AUX-003450 [Required: AO CS, A/V CS]** The audio system shall support multiple DNS entries. If the primary DNS server does not respond to a DNS request, then a secondary DNS server shall be queried.

**AUX-003460 [Required: AO CS, A/V CS]** The audio system shall support configurable transmission control protocol (TCP) ports for UC SIP messaging.

**AUX-003470 [Required: AO CS, A/V CS]** The audio system shall be able to set the IPv4/IPv6 Precedence Field bits of the Type of Service (TOS) byte and DSCP bits for media streams and signaling streams.

**AUX-003480 [Required: AO CS, A/V CS]** The audio system shall support Network Time Protocol (NTP), version 3 [RFC 1305].

**AUX-003490 [Required: AO CS, A/V CS]** The audio system shall support SNMPv3 [RFC 3414].

**AUX-003500 [Required: AO CS, A/V CS]** The audio system shall support Secure Real-Time Transport Protocol (SRTP) and Secure Real-Time Transport Control Protocol (SRTCP) [RFC 3711].

**AUX-003510 [Required: AO CS, A/V CS]** The audio system shall support SRTCP and accurately report jitter, delay, and packet loss information to the far end using Real-Time Transport Protocol (RTP) Control Protocol Extended Reports (RTCP XR) [RFC 3611].

**AUX-003520 [Required: AO CS, A/V CS]** The audio system's UC SIP signaling module shall support RFC 3261 including loose route.

**AUX-003530 [Required: AO CS, A/V CS]** The audio system's UC SIP signaling module shall allow UC SIP URLs for both incoming and outgoing calls. This includes all alphanumeric characters allowed in legal SIP URLs.

**AUX-003540 [Required: AO CS, A/V CS]** The audio system's UC SIP signaling module shall support Session Description Protocol (SDP) as defined in RFC 2327.

**AUX-003550 [Required: AO CS, A/V CS]** The audio system's UC SIP signaling module shall implement user "hold" feature by using a=inactive or a=sendonly, or by sending a mid-call INVITE that includes a session description that is the same as in the original request, but the "c" destination addresses for the media streams to be put on hold are set to zero:c=IN IP4 0.0.0.0.

**AUX-003560 [Required: AO CS, A/V CS]** The UC SIP signaling module shall support UC SIP Digest Authentication [RFCs 3261 and 3310].

**AUX-003570 [Required: AO CS, A/V CS]** The UC SIP signaling module shall be able to reject incoming INVITE messages when the message does not come from pre-provisioned proxies.

**AUX-003580 [Required: AO CS, A/V CS]** The UC SIP signaling module shall support call transfer as specified in UC SIP Section 9.6, Call Transfer.

**AUX-003590 [Required: AO CS, A/V CS]** Audio systems shall support electronic numbering (ENUM) service registration for SIP (UC SIP) Addresses-of-Record [RFC 3764].

Voice medium requirements include the following:

**AUX-003600 [Required: AO CS, A/V CS]** The audio system shall support DTMF Generation/Recognition per Telcordia GR-181-CORE.

**AUX-003610 [Required: AO CS, A/V CS]** The audio system shall support G.711  $\mu$ /A law [pulse code modulation (PCM)] and G.729.

**AUX-003620 [Required: AO CS, A/V CS]** The audio system's total media processing time shall be less than 50 ms including delays from jitter buffer, transcoding, mixing, packetization, and algorithm look ahead.

**AUX-003630 [Required: AO CS, A/V CS]** The audio system shall support G.168 compliance echo canceller (EC) with 128 ms echo path.

**AUX-003640 [Required: AO CS, A/V CS]** The audio system shall support Audio and Video Transport (AVT) payload type 0 and 8. [G.711 a/ $\mu$  law].

**AUX-003650 [Required: AO CS, A/V CS]** The audio system shall support AVT payload 18 [G.729].

**AUX-003660 [Required: AO CS, A/V CS]** The audio system shall be able to accept in-band DTMF tones.

**AUX-003670 [Required: AO CS, A/V CS]** The audio system shall be able to send DTMF specified by RFC 2833.

**AUX-003680 [Required: AO CS, A/V CS]** The audio system shall be able to conceal 1 percent of packet loss without appreciable quality degradation.

**AUX-003690 [Required: AO CS, A/V CS]** The audio system shall be able to tolerate 40 ms of jitter for audio without appreciable quality degradation.

**AUX-003700 [Required: AO CS, A/V CS]** The audio system shall implement adaptive jitter buffers instead of static fix jitter buffers.

**AUX-003710 [Required: AO CS, A/V CS]** All hardware shall meet Network Equipment Building System-3 (NEBS-3) requirements.

#### 3.4.3.3.7 *Reduced Maximum Transmission Unit IP Environment*

**AUX-003720 [Required: VO CS, A/V CS]** This subsection addresses the Maximum Transmission Unit (MTU) requirements for an IP network environment. An MTU is the maximum size of an IP packet that will be accepted for transmission without fragmenting it into a smaller datagram. The MTU size shall be configurable to optimize video traffic. As a result of devices such as encryption units, the typical MTU size shall be changed to minimize the effect of fragmentation due to the additional overhead of the encryption.

**AUX-003730 [Required: All UCCS]** The conference system shall ensure that all conferencing services provide signaling and media streams, and are capable of configuring the MTU.

**AUX-003740 [Required: All UCCS]** The conference system shall ensure that all supporting services to video and audio services, including, but not limited to, reservation, monitoring, billing, administration, operator interface, and meeting control, are capable of working in the configurable MTU IP environment.

#### 3.4.3.3.8 *IPv6 Support*

**AUX-003750 [Required: All UCCS]** The conference system shall comply with the IPv6 requirements contained in Section 5, IPv6.

#### 3.4.3.3.9 *UC SIP Support*

**AUX-003760 [Required: All UCCS]** The conference system shall comply with the UC SIP requirements contained in UC SIP 2013, Section 4, SIP Requirements for UC SIP Signaling Appliances and UC SIP EIs.

### 3.4.3.4 *Assured Services*

This subsection describes assured services as the set of capabilities which ensure that mission-critical calls are set up and remain connected.

#### 3.4.3.4.1 *Quality of Service*

**AUX-003770 [Required: All UCCS]** The system or network device shall be able to set DSCPs on both signaling packets and media streams for both IPv4 and IPv6 as specified in Section 6.2.2, Differentiated Services Code Point.

#### 3.4.3.4.2 *Assured Service*

The conference system shall ensure that the design and services satisfy the following requirements.

#### 3.4.3.4.2.1 Congestion Response

**AUX-003780 [Required: All UCCS]** The system shall provide measures to monitor bandwidth resource usage and to activate congestion management as needed within a timely fashion.

#### 3.4.3.4.2.2 Accounting

**AUX-003790 [Required: All UCCS]** The system shall maintain a call summary of conference sessions. This will include the conference attendee identification, access methods, IP address, E.164 numbers, time and date of the call, call duration, and total number of participants. The summaries shall be maintained for 30 days or IAW Information Assurance security requirements.

#### 3.4.3.4.2.3 Multilevel Precedence and Preemption

**AUX-003800 [Optional: All UCCS]** The system shall operate IAW the MLPP rules and procedures specified in Section 2.26.2, Multilevel Precedence and Preemption (inclusive as applies).

**AUX-003810 [Optional: All UCCS]** Preset Conferencing. Each conferee shall be dialed at its designated precedence level. Each conferee may have a different precedence level. The conference host must be dialed at the highest precedence level of any conferee.

**AUX-003820 [Optional: All UCCS]** Meet-Me Conferencing. When a priority session requests connection to a conference that is at conference maximum, then one of the lowest precedence conferees shall be preempted, selected through any deterministic method. (Conference maximum is the maximum number of conferees authorized for the same conference.) When a priority session requests connection to a conference that is not at conference maximum, but the system is at system maximum, then one of the lowest precedence conferees on another conference will be preempted, selected through any deterministic method. Note that the selection method shall not consider any ad hoc conferees for preemption, if an allocation of system resources dedicated to ad hoc conferences has been configured per requirement [AUX-003880](#) in [Section 3.4.4.2.1](#), Video Conference Capacity. (System maximum occurs when the maximum number of ports or resources are provisioned on the system.) Preempted conferees shall receive a preemption notification tone and be preempted. All remaining conferees on the system shall receive a conference disconnect tone (see Table 2.9-2, UC Information Signals).

**AUX-003830 [Optional: All UCCS]** Ad hoc Conferencing. When either party of a two-party session brings in a third party, an ad hoc conference is created at the highest precedence level of the dialed conferees. Thereafter, any party of an ad hoc conference can attempt to add an additional conferee at any time. If that party is dialed at a precedence level higher than any of the current conferees, then the conference precedence level shall be elevated to a higher precedence level. If an allocation of system resources dedicated to ad hoc conferences has been configured per requirement [AUX-003880](#) in [Section 3.4.4.2.1](#), and there are no ad hoc system resources

available to add on a conferee, then a conferee from the lowest precedence ad hoc conference will be preempted so that the conferee can be brought into the higher precedence ad hoc conference. If an allocation of system resources dedicated to ad hoc conferences has not been configured, but the system is at system maximum, then one of the lowest precedence conferees on another conference will be preempted, selected through any deterministic method, so that the conferee can be brought into the higher precedence ad hoc conference.

**AUX-003840 [Optional: All UCCS]** Ad hoc Conferencing. When a higher precedence session (i.e., higher than the conference precedence level) is placed to any of the conferees, that conferee receives a preemption notification tone (see Table 2.9-2, UC Information Signals). The other remaining conferees shall receive a conference disconnect tone, as described in Table 2.9-2. This tone indicates to the other parties that one of the conference call participants is being preempted.

### 3.4.4 Service Performance

**AUX-003850 [Required: All UCCS]** This section provides the service performance criteria and metrics for the system. The service performance criteria shall apply during simultaneous operation of the respective EIs. The system shall design and implement redundancy, failover, and fault tolerance at the component, subsystem, and system levels to support achieving service availability requirements in the presence of failures at the component, subsystem, and system levels. The system shall meet the requirements specified in Section 2.8, Product Physical, Quality, and Environmental Factors.

#### 3.4.4.1 Quality

##### 3.4.4.1.1 Video Conference Quality

For video conferencing services implemented and provided by the conference system, video quality requirements (that are based on commercial standards for supporting video conferencing) are as follows.

**AUX-003860 [Required: VO CS, A/V CS]** The conference system shall ensure that all video equipment used in designs can operate in the presence of minimal packet loss without degrading video quality below acceptable levels.

**AUX-003870 [Required: VO CS, A/V CS]** The conference system shall ensure that all video equipment used in the design provides adequate jitter buffer sizing to ensure an optimal end-to-end (E2E) video conferencing performance.

##### 3.4.4.1.2 Audio Conference Quality

For audio conferencing services provided by the conference system, voice quality requirements are as follows.

**AUX-003880 [Required: AO CS, A/V CS]** The conference system shall ensure that the Mean Opinion Score (MOS) on the voice path meets the MOS requirements in Section 6, Network Infrastructure End-to-End Performance.

**AUX-003890 [Required: AO CS, A/V CS]** The conference system shall ensure that the implemented design possesses the adequate performance capacity and resources to support conference access processing requirements identified in [Section 3.4.4.2](#), Capacity.

**AUX-003900 [Optional: AO CS, A/V CS]** The conference system shall ensure the time needed to compile polling statistics to adequately support the audio conference capability.

### **3.4.4.2 Capacity**

This subsection describes the capacity requirements of the conference system.

#### **3.4.4.2.1 Video Conference Capacity**

**AUX-003910 [Required: VO CS, A/V CS]** The number of concurrent conferences shall be limited only by available ports, regardless of access methods, features, or number of participants in each conference.

**AUX-003920 [Required: VO CS, A/V CS]** The system shall have the capacity to support at least 1,000 concurrent 384 kbps video calls.

**AUX-003930 [Required: VO CS, A/V CS]** The system shall provide sufficient speed matching capacity to support that capability regardless of the access methods, algorithms, speeds, or the feature sets being used.

**AUX-003940 [Required: VO CS, A/V CS]** The system shall provide enough transcoding capacity to support that capability regardless of the access methods, algorithms, speeds, or feature sets being used.

**AUX-003950 [Optional: VO CS, A/V CS]** The system shall provide sufficient H.323 gateway capacity to support that capability regardless of the access methods, algorithms, speeds, or feature sets being used.

**AUX-003960 [Required: VO CS, A/V CS]** The system shall provide enough H.239 capacity to support that capability regardless of the access methods, algorithms, speeds, or feature sets being used. The system shall provide enough H.261 Annex D capacity to support that capability regardless of the access methods, algorithms, speeds, or feature sets being used.

**AUX-003970 [Required: VO CS, A/V CS]** The system shall support a minimum of 200 EIs for each multipoint conference.

**AUX-003980 [Required: A/V CS]** The system shall provide at least four audio added-on ports for each conference without the use of external audio systems or by cascading conference

systems. The system shall ensure that audio added-on does not compromise other capacity requirements.

**AUX-003990 [Optional: VO CS, A/V CS]** A configurable percentage (0 to 100 percent, default 20 percent) of system ports/resources shall be allocated for ad hoc video conferences. Meet-me conferences shall not use resources allocated to ad hoc conference, and vice versa.

#### *3.4.4.2.2 Audio Conference Capacity*

The conference system shall provide the following audio conferencing capacity.

**AUX-004000 [Required: AO CS, A/V CS]** The system shall be capable of scaling up to 2,500 concurrent audio calls.

**AUX-004010 [Required: AO CS, A/V CS]** The system shall support up to 200 participants in a single conference session.

**AUX-004020 [Required: AO CS, A/V CS]** The system shall be capable of scaling up to 500 concurrent conferences and more than 500 conference control Web sessions.

**AUX-004030 [Required: AO CS, A/V CS]** The audio conference system shall be capable of scaling to support more than 10,000 reservations.

**AUX-004040 [Optional: AO CS, A/V CS]** The audio conference system shall support more than 50 concurrent recordings.

**AUX-004050 [Optional: AO CS, A/V CS]** A configurable percentage (0 to 100 percent; default 20 percent) of system ports and resources shall be allocated for ad hoc audio conferences. Meet-me conferences shall not use resources allocated to ad hoc conferences, and vice versa.

NOTE: Scaling can be provided by deploying multiple systems and provisioning or load sharing between systems.

#### *3.4.4.2.3 Registration, Admission, Status, and Routing Function*

**AUX-004060 [Required: All UCCS]** The conference system shall have the capability to provide bandwidth management, EI registrations, admissions, status, and routing functions. Furthermore, the system shall be capable of scaling to support at a minimum of 1,000 concurrent conference calls and 10,000 concurrent registrations of EIs.

NOTE: Scaling can be provided by deploying multiple systems and provisioning or load sharing between systems.

#### *3.4.4.2.4 Scalability*

The conference system shall support a nominal growth of services without requiring major overhaul or major replacement of equipment.

**AUX-004070 [Required: VO CS, A/V CS]** The system architecture supporting the dedicated IP-based video services capability shall be able to scale to accommodate increased growth in dedicated IP-based video services EIs.

**AUX-004080 [Required: VO CS, A/V CS]** The system architecture supporting the dial-up video services capability shall be designed to support up to a 50 percent increase in dial-up video services.

**AUX-004090 [Optional: VO CS, A/V CS]** The system shall be able to scale to accommodate increased growth to support increases in connections to ISDN networks. Additional capacity in regards to this item will only be used to support ISDN dial-up video traffic.

**AUX-004100 [Required: AO CS, A/V CS]** Audio add-on and audio conference service shall be able to scale to accommodate increased growth in call volume and EIs.

### **3.4.5 Service Management**

This section describes service management. The conference system shall provide reservation, scheduling, and registration services. The conferencing system service applications shall integrate or provide interfaces with Government network services and management applications. The conference system shall provide management functions to ensure continuous operations and accessibility of services with a data feed into the Government network services systems. The equipment and software applications shall be configurable to allow alarm and log file transmissions to be selective with the activation of a specific feature set.

#### ***3.4.5.1 System Management***

##### ***3.4.5.1.1 General System Management***

**AUX-004110 [Required: All UCCS]** The conference system shall provide services management and monitoring for the Operation, Administration, Maintenance, and Provisioning (OAM&P) of conferencing services.

**AUX-004120 [Required: All UCCS]** The conference system shall provide a service monitor and management system to actively monitor elements and critical components within the system.

**AUX-004130 [Required: All UCCS]** Report data shall be in a form that is capable of being managed by the Government network services applications and network elements, which are based on commercial and industry standards. The data transmitted shall comply with industry standard management protocols and/or data formats. Such industry standard protocols for data exchange include, but are not limited to, Syslog, Common Object Request Broker Architecture (CORBA), SNMPv3, Transaction Language 1 (TL1), Java 2 Platform Enterprise Edition (J2EE), and Extensible Markup Language (XML).

---

**AUX-004140 [Required: All UCCS]** The conference system shall be responsible for managing and monitoring the following services and related resources. Furthermore, the system shall provide real-time, read-write continuous Network Management capabilities. The level of monitoring shall be sufficient to be able to track the status, through standard interfaces and protocols, of individual discrete hardware and software components used to deliver the service to enable visibility of individual incidents affecting the service delivery:

- a. Equipment and associated services.
- b. Point-to-point and multipoint video services.
- c. Audio services.
- d. Reservation and scheduling.
- e. Gateways and interfaces.
- f. Conferencing center Web site.
- g. Support systems.

**AUX-004150 [Required: All UCCS]** The conference system shall furnish and maintain a service monitor and management system with external interfaces or feeds into Government management application and monitoring systems. These interfaces shall provide the Government the capability to monitor the performance and status of video and audio services. These interfaces shall provide for the importing and exporting of video and audio management services and monitoring information. The Government shall have real-time access to all video and audio services management and monitoring data collected and stored by the system. These interfaces are further specified in Section 2.17.2, General Management.

#### *3.4.5.1.2 Fault Management*

**AUX-004160 [Required: All UCCS]** The conference system shall provide fault management for services and resources. The system shall provide the Government with all the fault information needed electronically to effectively manage all conferencing services.

**AUX-004170 [Required: All UCCS]** The fault management system shall include the following minimum requirements:

- a. Power status shall be provided for individual shelf, rack, or controller units.
- b. Functional/Fault/Online/Offline status.
- c. Input/loss of input signal, or signal below working threshold.
- d. Output/loss of output signal.
- e. Input/output signal outside of specified range.
- f. Intrusion detected.

---

**AUX-004180 [Required: All UCCS]** The fault management function shall perform the following:

- a. Detect and identify faults. The fault management service provided shall monitor dedicated and dial-up video services resources, audio conferencing service status, support services status, and conduct alarm surveillance, maintain error logs, and analyze monitored or logged errors or events to anticipate faults:
  - (1) Faults shall be detected within 10 seconds of their occurrence.
  - (2) Faults shall be identified within 10 seconds of being detected.
  - (3) Faults shall be correlated within 10 seconds of identification.
  - (4) The Government shall be notified of service affecting faults within 10 seconds of fault correlation.
- b. Isolate faults to include correlation of alarms. The fault management service provided shall initiate diagnostic testing and evaluate diagnostic results to determine the nature, severity, and specific cause(s) of the fault and isolate the fault to the video, audio, and support services at a component level.
- c. Temporary corrective action when a fault occurs. The fault management service provided shall reroute a conference call or service request to other hubs, circuits, or equipment in the case of a fault, including through the use of redundancy and failover capabilities.
- d. Correct faults. The fault management service provided shall implement corrective actions on faults to restore services to proper working order and complete resource/service restoration when the fault is with equipment or services provided by the conference system. This process shall incorporate backup and recovery capabilities to restore configurations and services to operational service.

#### *3.4.5.1.3 Fault Management Information*

**AUX-004190 [Required: All UCCS]** The conference system shall provide the Government with real-time monitoring of service-affecting events related to hardware and software components and subcomponents that compose the conference system. These service-affecting events impacting the scheduling and operation of system services include, but are not limited to, the following:

- a. Outages for all conferencing services elements to be exported into the existing trouble tracking system.
- b. Any hazardous condition, as specified in DISA Circular 310-55-1, that may cause loss of service.

**AUX-004200 [Required: All UCCS]** The conference system shall be able to update all service management thresholds, as required.

---

**AUX-004210 [Required: All UCCS]** The conference system shall maintain historical records of all fault alarm data and be able to export this data into the Government management application systems.

#### *3.4.5.1.4 Performance Management*

**AUX-004220 [Optional: All UCCS]** The conference system shall provide a performance management system. The performance management system shall monitor and control all service performance and the quality of the services and features supporting the conference system. Performance management shall perform the following functions.

**AUX-004230 [Optional: All UCCS]** Monitor, analyze, and characterize performance. The conference system shall monitor, analyze, and gather performance-related data to detect and characterize normal and degraded performance and be able to trend this data over time for metrics purposes. [Section 3.4.4](#), Service Performance, defines normal performance requirements. The system shall provide notification if the service resources are being stressed with excess traffic loads.

**AUX-004240 [Optional: All UCCS]** Tune and control performance in areas of control: the conference system shall activate controls to tune all services performance to restore degraded resources/services to acceptable performance levels. If control actions will cause any user service disturbance, then these actions shall be approved by the Government before execution.

**AUX-004250 [Optional: All UCCS]** Maintain all services supporting the conference system through an operations database. The conference system shall maintain a database or be exportable to a Government network management tool supporting all conferencing services operational information, both real-time and historical, including, for example, traffic characterization data, performance data, and information on usage of resources/services. Historical records shall be kept of all performance data for a designated period of time.

**AUX-004260 [Optional: All UCCS]** Evaluate performance of services and features. The conference system shall continuously assess and monitor the performance of all conferencing services and features, according to the performance parameters identified in [Section 3.4.4](#), Service Performance, to ensure that the performance levels of Government services and features meet the specification requirements of [Section 3.4.3](#), Service, and [Section 3.4.4](#), Service Performance.

#### *3.4.5.1.5 Government Performance Management Information*

This subsection describes Government performance management information requirements.

**AUX-004270 [Optional: All UCCS]** The conference system shall provide notification of events, exceptions, or measures related to the performance of services' resources, and associated service-affecting conditions to Government platforms as required. Performance degradation notification shall include, at a minimum, the following.

The conferencing services are composed of servers, applications and network services, appliances, and network devices responsible for supporting video services globally throughout the DOD community. The conferencing service is of a time-sensitive nature and one of the services that is being offered with the convergence of IP on the backbone.

There are two parts to the network management of this service: transport monitoring and video stream monitoring. First, the underlying network elements and servers need to be included in fault management and performance management activities at the physical layers and IP layers. Second, the video service needs to have instrumentation included that would be able to monitor the conferencing user's experience, in order to isolate problems and reveal if the video service is meeting specific service-level requirements.

**AUX-004280 [Optional: VO CS, A/V CS]** The performance management toolset should be able to collect information from the video device managers. The information it should collect would include, but not be limited to, the number of participants, duration of a session, video burst measurements, and capacity measurements.

#### *3.4.5.1.6 Security Management*

This subsection describes the security management requirements.

**AUX-004290 [Required: All UCCS]** Certification and Accreditation. The conference system shall ensure that all systems and subsystems in UC conferencing undergo Certification and Accreditation (C&A) IAW the DOD Information Assurance Certification and Accreditation Process (DIACAP) and associated audits.

**AUX-004300 [Required: All UCCS]** Best Security Practices. The conference system shall incorporate best security practices such as single sign-on, public key encryption (PKE), smart card, and biometrics in system security design of DOD information, but does not limit to certain security mechanisms.

**AUX-004310 [Required: All UCCS]** Enterprise Security Management. The conference system shall implement enterprise management of security devices and applications such as the following:

- a. Firewalls and boundary protection.
- b. Intrusion detection systems.
- c. Operating systems, network devices, and applications security.
- d. Vulnerability management.

**AUX-004320 [Required: All UCCS]** Security Configuration Specifications. The conference system shall comply with DOD reference documents such as STIGs or security recommendation guides from the DISA Facility Security Officer (FSO) that are pertinent to the UCCS or subcomponents.

### **3.4.5.2 Online Directory**

**AUX-004330 [Required: VO CS; Optional: AO CS, A/V CS]** The system shall provide an online directory service to support scheduling that shall include general information about all registered DOD video and audio users including, but not limited to, a user's point of contact, location, supported data rates, organization name, unit capabilities, and software versions.

**AUX-004340 [Required: VO CS; Optional: AO CS, A/V CS]** The system shall update the online directory within 24 hours of learning of a new EI receiving service, a change in an existing EI's service status, or notification by DISA of any other change with regard to an EI.

**AUX-004350 [Required: VO CS; Optional: AO CS, A/V CS]** The system shall provide a secure Web interface that implements a public key enablement application, allowing registered users with a valid DOD PKI or External Certification Authority (ECA) certificate and Internet connectivity to access the online directory.

**AUX-004360 [Required: VO CS; Optional: AO CS, A/V CS]** The online directory shall support more than 1 million data entries and shall support more than 500 concurrent users at the same time.

**AUX-004370 [Required: VO CS; Optional: AO CS, A/V CS]** The online directory shall be Web-based using modern and open technologies and provide interfaces, such as XML, Simple Object Access Protocol (SOAP), Web Service Description Language (WSDL), and Universal Discovery Description Interface (UDDI), allowing external data sources from others to perform directory lookups, queries, and updates as specified by "Horizontal Fusion Standards and Specifications," 3 November 2004, and DOD Joint Technical Architecture, Version 6, Volumes I and II, 3 October 2003.

**AUX-004380 [Required: VO CS; Optional: AO CS, A/V CS]** The online directory shall support the discovery service that provides processes for discovery of information content or services that exploit metadata descriptions of information technology resources stored in directories, registries, and catalogs (to include search engines) as specified by "Horizontal Fusion Standards and Specifications," 3 November 2004, and "DOD Joint Technical Architecture," Version 6, Volumes I and II, 3 October 2003. Directory services shall be designed to meet Protected Personal Information/Personally Identifiable Information protection requirements and Privacy Act requirements.

**AUX-004390 [Required: VO CS; Optional: AO CS, A/V CS]** The system shall provide an online directory service to allow authorized registered users to search system-wide for other authorized, registered service users in the directory and/or to update data entries.

### **3.4.5.3 Registration System**

**AUX-004400 [Required: All UCCS]** UCCS customers will be required to follow a registration process to subscribe to the service. One component shall be an automated registration system

---

that prospective customers can access online using a standard Web browser. All data shall be encrypted using Secure Socket Layer (SSL)/TLS technology, as a minimum, with DOD PKI certificate authentication and validation.

**AUX-004410 [Required: All UCCS]** The automated registration system shall collect all data necessary to comply with provisioning requirements.

**AUX-004420 [Required: All UCCS]** The automated registration system shall collect all data necessary for connection approval by the program office.

**AUX-004430 [Required: All UCCS]** The automated registration system shall collect all data necessary to authorize users for access to operational systems including scheduling and reservations.

**AUX-004440 [Required: All UCCS]** The automated registration system shall collect all data necessary to support the operational requirements of UC conferencing services. Upon connection approval and completion of verification and interoperability tests, all data shall be available to the operational systems for the scheduling and activation of conferences.

**AUX-004450 [Required: All UCCS]** The automated registration system shall be the authoritative source of conference subscribers' data. The system shall provide the necessary tools to allow authorized users to maintain and update user and endpoint information. The system shall support Privacy Act statements as required by Information Assurance policy.

#### ***3.4.5.4 Scheduling System***

**AUX-004460 [Required: All UCCS]** The primary component for requesting a conference shall be by an automated scheduling system that authorized users can access online using a standard Web browser. All data shall be encrypted using SSL/TLS technology, as a minimum, with DOD PKI certificate authentication and validation.

**AUX-004470 [Required: All UCCS]** The automated scheduling system shall resolve the availability of all requested participants and conferencing resources. The customer shall be able to schedule a conference immediately or schedule it for some time in the future. Immediate start requests for conferences shall be activated in less than 5 minutes of confirmation of available resources and participants. The system shall support scheduling conferences with the conference size larger than the number of initially invited or scheduled endpoints. A unique identification number shall be assigned to each conference event to facilitate conference control and management. E-mail notifications shall be provided to all conference participants to facilitate event coordination. E-mail content shall be editable as a configuration feature. The system shall support encrypted e-mail for notifications. Scheduled conference information also shall be available through the scheduling Web interface.

**AUX-004480 [Required: All UCCS]** The original requester shall serve as the conference manager for all conferences. The system shall have the capability to assign other system users to

act as surrogates for the original requester. This may include peers and/or workflow superiors. Conference management and control shall include the ability to make changes to a scheduled or active conference. Supported changes to active conferences shall include, but not be limited to, the addition or deletion of participants, early termination of a conference, and extension of the conference beyond the originally scheduled end time. Additions, deletions, and extensions of conferences shall occur without interruption to the existing conference, other than preemptive precedence calls. Additions and extensions to conferences shall be executed in less than 5 minutes of confirmation of available resources. Deletions and terminations of conferences shall be executed in less than 5 minutes of the request by the conference manager. The system shall support scheduling of recurring conferences.

### ***3.4.5.5 Accounting and Billing***

**AUX-004490 [Required: All UCCS]** The conference system shall provide an Accounting Management function. The Accounting Management function will serve two purposes:

- a. Provide accounting information to the Government regarding all conferencing services provided.
- b. Provide all conferencing services data to the Government at a level of detail that allows the Government to bill conferencing services customers based on usage.

**AUX-004500 [Required: All UCCS]** The Accounting Management function shall enable charges to be established for the use of dedicated and dial-up conferencing services resources.

**AUX-004510 [Required: All UCCS]** The conference system Accounting Management function shall provide for the collection, aggregation, storage, and reporting of all conferencing service usage data. The accounting management function shall consist of systems to activate and monitor customer accounts and to collect, aggregate, and report on usage data.

**AUX-004520 [Required: All UCCS]** The conference system shall provide the capability to perform the following Accounting Management functions:

- a. Collect usage data from a Call Detailed Record (CDR) (i.e., at the level of the authorization code).
- b. Aggregate and combine data for generating reports as specified by the Government.
- c. Maintain conference records per individual customer's account.
- d. Ensure continuous (24x7) monitoring, processing, and recording for all video services-related events and customer activity data.
- e. Maintain a database of various conference reports per individual customer account, including conference detail summary, completion summary, and exception reports.
- f. Archive data for possible later retrieval by the Government (e.g., in response to customer inquiries or to audit the data).

**AUX-004530 [Required: All UCCS]** The conference system shall provide the capability to transmit usage data to the EMS. The frequency of data transfer shall be determined by the Government based on volume of data collected. The system shall maintain all accounting data for at least one billing cycle.

### 3.5 GENERAL MASS NOTIFICATION WARNING SYSTEM (MNWS)

See UC Framework 2013, Section 3.4.2, for a description of the MNWS.

The MNWS shall provide the following functionality:

**AUX-004540 [Required]** Alert activation. The MNWS shall provide dissemination of alert notifications to target authorized subscribers by means of multiple notification devices, including, but not limited to, the following:

- a. Personal devices. Includes networked desktop popups, PKI signed emails, text messaging, pagers, voice telephone calls, and other existing communication infrastructure such as UC/VoIP systems.
- b. Mass notification devices. Includes Giant Voice system; indoor voice systems; Land Mobile Radios (LMRs); and integration with AM/FM/TV broadcast systems, fire/evacuation systems, and social networks.

**AUX-004550 [Required]** Tracking and reporting. The MNWS shall track and report alert delivery in real time, track and report subscriber responses to alert notifications in real time, and report on the operational status of delivery devices and services.

**AUX-004560 [Required]** Database. MNWS shall establish and maintain a comprehensive database of subscribers served by the installation's MNWS.

**AUX-004570 [Required]** Group Management. The MNWS shall offer unfettered flexibility to place target subscribers into groups that can then be targeted for specified alerts. The types of groups that can be created include, but are not limited to, groups based on organization, rank, roles and responsibilities, location, device delivery preference, phone number, and IP address. In addition, the groups can be static ("rosters") or dynamic (based on subscriber data attributes).

**AUX-004580 [Required]** Permission Management. Access to MNWS functions, assets, and resources are governed by the permissions assigned to each operator and subscriber. The MNWS shall be capable of assigning permissions on a group-wide role basis such that each member of the group receives identical permission to MNWS functions, assets, and resources.

**AUX-004590 [Required]** Delivery Device Management. The MNWS shall ensure operational status of delivery devices, provide appropriate data to delivery devices in order for delivery devices to send the desired alerts to the correct set of designated target subscribers, and track performance of delivery devices in conjunction with alert notifications.

**AUX-004600 [Required]** Self-service. The MNWS shall support the ability for subscribers to update their personal information to ensure up-to-date contact information for purposes of emergency alert notification.

**AUX-004610 [Required]** The MNWS shall be Section 508 compliant and provide effective alerting to members of the special needs community.

**AUX-004620 [Required]** The MNWS shall comply with all pertinent DOD information assurance and security requirements including, for example, CAC-enabled devices, PKI servers, and prohibition on group passwords:

- a. The MNWS shall archive all alerts that are sent in order to maintain an audit trail in compliance with all DOD information assurance requirements, including logins, failed logins, data updates, and alert activations.
- b. In the case of OCONUS deployments, the MNWS shall meet host nation requirements for emergency systems.

**AUX-004630 [Required]** The MNWS shall be capable of delivering installation-wide alert notification to all targeted personnel at a minimum of within 10 minutes, per DOD Instruction (DODI) 6055.17 requirements or, as needed, at a faster delivery time per the specific needs of the installation.

**AUX-004640 [Required]** The MNWS service shall be capable of delivering regional alert notification to all targeted personnel at least within 10 minutes, per DODI 6055.17 requirements or, as needed, at a faster delivery time per the requirements of the specific region.

**AUX-004650 [Required]** The MNWS service shall scale to support Command-wide alert notifications involving over 500,000 subscribers at over 100 installations.

**AUX-004660 [Required]** The MNWS service shall be capable of delivering Command-wide alert notification to all personnel within 10 minutes per DODI 6055.17 requirements or, as needed, at a faster delivery time per the requirements of the Command.

**AUX-004670 [Required]** The MNWS shall provide a high availability service having a complete set of redundant primary and standby platforms, and this redundant configuration shall have an availability of 99.95 percent.

**AUX-004680 [Required]** The MNWS shall support the use of standard and open protocols including the Common Alerting Protocol (CAP) and XML in order to interface with various event sources and delivery devices.

**AUX-004690 [Required]** The MNWS shall meet all applicable STIGs and have current and applicable information assurance C&A.

---

**AUX-004700 [Required]** The MNWS shall provide supervision and a monitoring capability of MNWS components and of delivery systems, and provide operators with notification of a failure of an MNWS component or delivery system within 200 seconds of the occurrence of the failure.

**AUX-004710 [Required]** The MNWS shall be IPv6 compliant per the requirements in Section 5, IPv6.

### 3.5.1 Standby MNWS Platform

**AUX-004720 [Required]** An MNWS system shall have both a primary MNWS platform and a standby MNWS platform.

NOTE: In this context, a “platform” refers to a complete working instance of MNWS equipment and may consist of a number of distinct physical boxes or elements including, for example, application servers and database servers.

**AUX-004730 [Required]** The standby MNWS platform shall be deployed at a geographically diverse location from the primary MNWS platform.

**AUX-004740 [Required]** The standby MNWS platform shall fully replicate the hardware, software, database, and connectivity to event sources and delivery devices of the primary MNWS platform.

**AUX-004750 [Required]** The standby MNWS platform shall maintain standby connections with the complete set of event sources and delivery devices to which the primary MNWS platform is connected.

**AUX-004760 [Required]** When the standby MNWS platform loses contact with the primary MNWS platform and is unable to reestablish connectivity within a pre-configured time interval (default = 60 seconds), then the standby MNWS platform shall notify a predefined list of operators that the standby MNWS platform has lost connectivity to the primary MNWS platform. The standby MNWS platform shall periodically attempt to reconnect with the primary MNWS platform.

NOTE: The operators contacted by the standby MNWS platform confirm the status of the primary MNWS platform. If the primary MNWS platform is operational, then the operators keep the standby MNWS platform in standby status and address the loss of connectivity between the primary MNWS platform and standby MNWS platform. If the operators determine that the primary MNWS platform has failed, then the operators notify the standby MNWS platform that it is now the acting primary MNWS platform, and the standby MNWS platform replaces the primary with respect to all operations and functionality.

NOTE: When the primary MNWS platform fails, then the existing sessions of all operators and subscribers logged into the primary MNWS platform will fail. It is

recommended that the client software and Web-based user interface automatically redirect a login request to the standby MNWS platform in the event that the client software or Web-based user interface is unable to reach the primary MNWS platform. Once an authorized operator has notified the standby MNWS platform that the standby MNWS platform has temporarily assumed the role of the primary MNWS platform, then subscriber attempts to log in to the standby MNWS platform will succeed.

**AUX-004770 [Required]** When the primary MNWS platform comes back up and a connection is reestablished between the primary MNWS platform and the standby MNWS platform (temporarily acting as the primary MNWS platform), then the primary MNWS platform shall resynchronize its database to the database of the standby MNWS platform and reestablish connections with the complete set of event sources and delivery devices.

**AUX-004780 [Required]** When the two MNWS platforms are fully synchronized, the designated operators direct the fail-back to the primary MNWS platform. Operators currently using the standby MNWS platform are notified of the pending fail-back prior to execution of fail-back. Upon fail-back, the standby MNWS platform will once again continuously synchronize with the primary MNWS platform.

### 3.5.2 [Optional] Mobile MNWS Platform

**AUX-004790 [Optional]** The vendor shall offer a mobile instance of the MNWS software designed to run on a ruggedized laptop or equivalent mobile platform.

**AUX-004800 [Optional]** The mobile MNWS platform shall periodically synchronize its database with the active MNWS platform (i.e., the primary MNWS platform unless the primary is currently failed over to the standby MNWS platform).

**AUX-004810 [Optional]** The communication between the mobile MNWS platform and the primary MNWS platform or the mobile MNWS platform and the standby MNWS platform shall be secured using Secure HTTP employing a two-way exchange of certificates or an alternative security protocol providing at least equivalent authentication, confidentiality, and integrity mechanisms.

**AUX-004820 [Optional]** The mobile MNWS platform shall have at least a Federal Information Processing Standards (FIPS) 140-2 Level 1 compliant encrypted hard drive, and it is of particular importance that the subscriber database on the mobile MNWS platform be encrypted.

**AUX-004830 [Optional]** In the event that the primary MNWS platform and standby MNWS platform are both inaccessible or inoperative, then the mobile MNWS platform shall interface remotely with the telephony, e-mail, and Short Message Service (SMS) in order to deliver alert notifications. Recommended network connectivity methods for the mobile MNWS platform include LAN, 802.11b/g/n, broadband, and satellite.

**AUX-004840 [Optional]** The communication between the mobile MNWS platform and the external delivery devices and services, specifically telephony alerting services, MNWS Simple Message Transfer Protocol (SMTP) server, and SMS aggregators, shall be secured using Secure HTTP employing a two-way exchange of certificates or an alternative security protocol providing equivalent or better authentication, confidentiality, and integrity mechanisms.

**AUX-004850 [Optional]** The controller at the mobile MNWS platform is required to generate the alerts to the various remote delivery devices. There is no requirement that operators on remote computers be able to access the mobile MNWS platform.

**AUX-004860 [Optional]** The mobile MNWS platform shall track alert delivery progress and collect alert responses.

### 3.5.3 MNWS Database

**AUX-004870 [Required]** The MNWS shall maintain a comprehensive database of subscribers including all contact information necessary for the MNWS to send alert notifications to the subscribers.

NOTE: A representative but non-exhaustive list of the types of information maintained for each subscriber includes personal information such as name, usernames, group profiles identifying the groups to which the subscriber belongs for alert notification purposes, organizational affiliations, rank, categories of roles and responsibilities, a list of preferred and mandatory delivery devices and the contact information necessary to reach the subscriber via each delivery device, location, and categories of alerts applicable to the subscriber. In addition, subscriber information shall include a Date Eligible for Return From Overseas (DEROS) expiration date so that subscribers can be automatically removed from the alert notification set when they leave the theater.

**AUX-004880 [Required]** The MNWS database shall integrate with the relevant existing subscriber databases such as the Military Personnel Data System (MilPDS) and the Civilian Personnel Data System (CivPDS) in order to periodically synchronize subscriber data, including subscriber attributes and contact details, and to ensure accurate and up-to-date targeting of the appropriate subscriber population.

**AUX-004890 [Required]** The frequency with which the MNWS synchronizes its database with other relevant existing DOD databases shall be configurable. At a minimum, it is anticipated that synchronization will occur on a daily basis unless the local Command specifies otherwise.

**AUX-004900 [Required]** The MNWS shall be capable of accessing Active Directory databases and shall support the Lightweight Directory Access Protocol (LDAP).

**AUX-004910 [Required]** MNWS system access to the existing subscriber databases shall be read-only.

---

**AUX-004920 [Required]** Operators having the requisite authorization shall be able to define any number of subscriber attributes and contact information fields for the MNWS subscriber database including user attributes and contact details, organizational hierarchy, groups, and distribution lists.

**AUX-004930 [Required]** Operators having the requisite authorization shall be able to manually add subscribers to the database, update the contact information, update the mandatory and preferred delivery devices for a given subscriber and other fields of a subscriber record, and remove subscribers from the MNWS database.

**AUX-004940 [Required]** The MNWS shall be capable of storing database tables in an external, installation-provided database server.

### 3.5.4 Notifications Across MNWSs

**AUX-004950 [Required]** An MNWS shall be able to convey alerts to other MNWSs to support cross-organizational alert notifications, multiple installation alert notifications, regional alert notifications, and Command-wide alert notifications. In addition, an MNWS belonging to one service shall have the capability to convey alerts to one or more MNWSs belonging to one or more different services, and Combatant Command (COCOM) MNWSs shall be able to cascade appropriate alerts to their Service component MNWSs.

**AUX-004960 [Required]** Connections between MNWSs shall be secured using Secure HTTP employing a two-way exchange of certificates or an alternative security protocol providing at least equivalent authentication, confidentiality, and integrity mechanisms.

**AUX-004970 [Required]** MNWSs that share notifications shall exchange distribution lists of subscriber groups and associated targeting details including location and organizational affiliation.

**AUX-004980 [Required]** Operator roles and permissions will dictate whether an operator can share a notification with a particular peer MNWS, the nature of the alerts that the operator is allowed to share with a peer MNWS, and the target groups belonging to the peer MNWS that the operator is authorized to alert.

**AUX-004990 [Required]** An MNWS that publishes an alert to a second MNWS shall collect alerting tracking data and subscriber responses from the second MNWS.

### 3.5.5 MNWS Operator

**AUX-005000 [Required]** Operators authorized to perform group management tasks shall be able to create groups, assign individual subscribers to new or existing groups, assign groups of subscribers to new or existing groups, remove subscribers and groups from existing groups, and delete groups without deleting the subscribers and groups composing the deleted group:

- a. Operators authorized to perform group management tasks shall be able to define Static subscriber groups composed of a selected list of subscribers (“roster”) that may include nested static groups.
- b. Operators authorized to perform group management tasks shall be able to define Dynamic subscriber groups composed of lists of subscribers based on data queries on their database attributes.

**AUX-005010 [Required]** Operators having the requisite authorization shall be able to assign preferred and mandatory delivery devices to be used when alerting a subscriber or a group.

**AUX-005020 [Required]** Operators having the requisite authorization shall be able to generate predefined alert notification scenarios for subscribers and groups. These scenarios include the content of the alert, multiple response options for the subscriber to choose from, target subscribers and mass communication devices, and preferred and mandatory personal delivery devices to be used when alerting the target subscriber(s) and/or group(s).

**AUX-005030 [Required]** Operators having the requisite authorization shall be able to manually activate predefined alert scenarios to trigger alert notification. The operator shall be able to specify the timing of the alert (e.g., immediately, at a certain time, on a recurring basis).

**AUX-005040 [Required]** Operators having the requisite authorization shall be able to create and activate alerts on the fly:

- a. When an operator creates an alert on the fly, then the operator designates the target subscribers and/or groups, the preferred and mandatory delivery devices, the contents of the alert message, and the timing of the alert (e.g., immediately, at a certain time).

**AUX-005050 [Required]** Operators having the requisite authorization shall be able to target subscribers for alert notification based on organizational structure, distribution lists, physical location [over a Geographical Information System (GIS) map or by specifying zone code(s) or location name(s)], individual name, dynamic database query, roles and responsibilities, phone number, IP address, etc.

**AUX-005060 [Required]** Operators having the requisite authorization shall be able to block or remove subscribers or groups from a pre-built alert notification scenario or from a pending alert notification.

**AUX-005070 [Required]** Operators having the requisite authorization shall be able to define scheduled activation of test alerts.

**AUX-005080 [Required]** Operators having the requisite authorization shall be able to track the delivery of events and subscriber multiple responses.

**AUX-005090 [Required]** For any given alert, operators having the requisite authorization shall be able to retrieve and display the count of targeted recipients, the actual number of recipients, and the number of recipients who acknowledged receipt of the alert.

**AUX-005100 [Required]** For any given alert, operators having the requisite authorization shall be able to retrieve and display the count of targeted recipients and view the coverage of existing contact details per the selected notification devices against the count of targeted recipients prior to activating the alert.

**AUX-005110 [Required]** Operators having the requisite authorization shall be able to geo-target alert notification by selecting geographic areas, perimeters, and locations on electronic maps.

### 3.5.6 Web Interface for Operators and Subscribers

**AUX-005120 [Required]** The MNWS shall have a Web-based operator interface for operators to publish and track alerts and perform administrative tasks including, but not limited to, the management of subscribers, delivery devices and pre-built alert scenarios:

- a. The operator Web-based interface shall be role and permission based, and only those capabilities allowed by the operator's authorization will be available.
- b. All operator activities, including failed logins, shall be centrally audited. At a minimum, the audit trail shall record the following details per action: login-id, object type, action taken, and source IP address. Web-based audit reports shall be available only to authorized operators. Audit trail reports shall be exportable.

**AUX-005130 [Required]** The MNWS shall have a Web-based subscriber interface for subscribers ("self-service") to view alerts and view and update their personal information including their contact information and device preferences relating to event notification.

**AUX-005140 [Required]** Using the Web-based subscriber interface, a subscriber shall be able to view the alerts to which he or she is subscribed as well as the list of all the alerts for which the subscriber is eligible but not subscribed. The subscriber shall be able to opt-in to types of alerts for which the subscriber is eligible but not subscribed and opt-out of non-mandatory types of alerts for which the subscriber is subscribed.

**AUX-005150 [Required]** The Web-based user interface shall work on personal computers running DOD-approved operating systems and on DOD-approved Web browsers.

**AUX-005160 [Required]** The Web-based session between the browser and the MNWS Web server shall be secured using Secure HTTP. The MNWS Web server is required to authenticate itself to the operator or subscriber using its server certificate.

**AUX-005170 [Required]** Operators shall authenticate to the MNWS Web server using username and strong password. The session times out after a configurable period of inactivity, and the operator shall establish a new Web-based session with the MNWS Web server.

**AUX-005180 [Required]** Subscribers shall authenticate to the MNWS Web server either using a Common Access Card (CAC) or Active Directory Windows authentication or using an authentication method that is at least as secure as either of the two previous methods.

### 3.5.7 Client Software for Subscribers

**AUX-005190 [Required]** The MNWS shall provide client software that runs on subscriber computers, the purpose of which is to furnish alert notifications.

**AUX-005200 [Required]** When an alert occurs that is intended for the subscriber, then the client software shall provide an audio alert accompanied by a persistent visual display of the alert message on the computer until the alert is canceled; no user action will be required to receive desktop notifications.

**AUX-005210 [Required]** When the client software receives multiple concurrent alerts, then the alert notifications are displayed vertically and horizontally on the desktop in a tiered fashion.

**AUX-005220 [Required]** If a subscriber logs into the computer and runs the client software after one or more alerts have been sent but while the alert or alerts are still active, then the client software provides an audio alert accompanied by a persistent visual display of the currently active alert message(s) on the computer until the subscriber responds to the alert(s).

**AUX-005230 [Required]** When the client software displays an alert on the computer, the subscriber shall be presented with response options enabling the subscriber to select a response option. When the subscriber selects a response option, the client software shall transmit the subscriber response to the MNWS server. The MNWS server stores the subscriber response, and the subscriber response is accessible to authorized operators.

**AUX-005240 [Required]** The connection between the MNWS client and MNWS server shall be secured using Secure HTTP. The MNWS server is required to authenticate itself to the client using its server certificate. The subscriber shall authenticate to the MNWS server using a CAC card or Active Directory Windows authentication or using an authentication method that is at least as secure as either of the two previous methods.

**AUX-005250 [Required]** The MNWS service shall furnish warning notification applications for mobile devices commonly used by subscribers (e.g., warning notification apps for iPhone, Android, Blackberry, iPads):

- a. The applications shall provide audio and visual warning notifications to the user of the mobile device.
- b. The applications shall provide for user response.
- c. The applications shall use device location (subject to all applicable privacy rules) to perform real-time, location-based alert targeting and tag user alert responses with real-time location information.

### 3.5.8 Event Sources

**AUX-005260 [Required]** For any particular event, operators having the requisite authorization shall be able to define that, upon notice of occurrence of the particular event by an event source, the MNWS is to implement one of the following behaviors:

- a. The MNWS shall automatically trigger alert notification to target subscribers.
- b. The MNWS shall test the event data against a predefined rule set, and, if the event conforms to the requirements of the rule set, then the MNWS shall trigger alert notification to target subscribers.
- c. The MNWS shall test the event data against a predefined rule set, and, if the event conforms to the requirements of the rule set, then the event shall be reported to the authorized operators who in turn will decide the action to be taken.

#### ***3.5.8.1 External IP-Enabled Event Sources***

**AUX-005270 [Required]** The MNWS shall support automatic activation by IP-enabled external sources (such as the National Weather Service, local and regional security forces Really Simple Syndication (RSS), and local and state emergency Common Alerting Protocol (CAP) feeds).

**AUX-005280 [Required]** The MNWS shall monitor external sources for new events. If an event from an external source meets predefined emergency criteria, then the default action is for the MNWS to inform operators of the event. The operators qualify the event and, when appropriate, initiate an alert to the pertinent target subscribers.

#### ***3.5.8.2 Internal IP-Enabled Event Sources***

**AUX-005290 [Required]** The MNWS shall be capable of interfacing with internal IP-enabled event sources such as fire alarms, video surveillance, data collection systems, and chemical detectors.

**AUX-005300 [Required]** The MNWS shall monitor IP-enabled internal sources for new events. For any given IP-enabled internal event source, either the MNWS queries the event source to determine when an event occurs or the event source notifies the MNWS that an event has occurred, in which case the MNWS shall authenticate the alert before acting on it.

**AUX-005310 [Required]** For each IP-enabled internal event source, the MNWS shall specify either that the MNWS trigger an alert upon detection or notification of an event from the given source or that the MNWS process the event information from the given source against a predefined rule set such that an alert is triggered only when the event meets the criteria set forth in the rule set.

### 3.5.9 SMTP Delivery

**AUX-005320 [Required]** The MNWS shall include an SMTP server that sends outbound e-mail alerts to the installation's host SMTP servers which, in turn, employ SMTP relay to deliver the e-mail alerts to the set of target subscribers.

**AUX-005330 [Required]** The MNWS SMTP server shall do the following:

- a. Send PKI-signed e-mail alerts to subscribers via host SMTP servers using SMTP relay.
- b. Send e-mail alert cancellation messages to either a subset of subscribers or all subscribers as appropriate via host SMTP servers using SMTP relay.
- c. Receive incoming e-mail responses (selecting one of multiple response options) from subscribers via host SMTP servers.

**AUX-005340 [Required]** The MNWS shall do the following:

- a. Report e-mail alert delivery events.
- b. Report on the operational status of the MNWS SMTP server.

**AUX-005350 [Required]** The MNWS SMTP server shall authenticate to the host SMTP server before sending outbound alert messages.

**AUX-005360 [Required]** The host SMTP server shall authenticate to the MNWS SMTP server before the MNWS server will accept inbound messages from the host SMTP server. Alternatively, incoming SMTP traffic may be routed directly to the MNWS SMTP server by designated multiplexer (MX) record.

### 3.5.10 External Delivery Systems and Services

#### *3.5.10.1 Telephony Alerting Service*

**AUX-005370 [Required]** The MNWS shall be capable of interfacing with external commercial telephone alerting services (i.e., "dialers") for the following purposes:

- a. Sending telephony alerts to a set of target subscribers.
- b. Canceling alerts to specific recipients or to all recipients.
- c. Obtaining reports of event alert delivery and subscriber responses.
- d. Obtaining reports of the operational status for the telephony alerting service.

**AUX-005380 [Required]** The connection between the MNWS and the external telephone alerting service shall be secured using Secure HTTP employing a two-way exchange of certificates or an alternative security protocol providing equivalent or better authentication, confidentiality, and integrity mechanisms.

---

**AUX-005390 [Required]** In order to instruct the telephony alerting service to send phone alerts, the MNWS shall provide the minimum set of data items necessary for telephony alert dissemination including user names, phone numbers, and (optionally) PINs for user authentication to the telephony alerting service.

**AUX-005400 [Required]** The telephony alerting service shall anonymize and then delete the contact information provided by the MNWS once the alert notification has been disseminated.

### ***3.5.10.2 Short Message Service (SMS) Aggregation Service***

**AUX-005410 [Required]** The MNWS shall be capable of interfacing with SMS aggregation services for the following purposes:

- a. Sending text message alerts to a set of target subscribers.
- b. Sending text messages canceling alerts to specific recipients or to all recipients.
- c. Obtaining reports of event alert delivery and obtaining subscriber responses to text alerts (selecting one of multiple response options).
- d. Obtaining reports of the operational status for the SMS aggregation service.

**AUX-005420 [Required]** The connection between the MNWS and the SMS aggregation service shall be secured using Secure HTTP employing a two-way exchange of certificates or an alternative security protocol providing equivalent or better authentication, confidentiality, and integrity mechanisms.

**AUX-005430 [Required]** In order to instruct the SMS aggregation service to send text alerts, the MNWS shall provide the minimum set of data items necessary including user names and SMS addresses (e.g., mobile phone numbers).

**AUX-005440 [Required]** The MNWS shall be capable of sending at least 10,000 SMS messages per minute.

### ***3.5.10.3 Existing IP-Enabled Alert Delivery Devices***

**AUX-005450 [Required]** The MNWS shall integrate with the existing IP-enabled alert delivery devices at the installation including telephony alerting systems associated with existing IP PBXs, IP-enabled Large Voice systems, LMRs, and digital displays.

**AUX-005460 [Required]** The MNWS shall be able to create RSS feeds that are delivered to RSS aggregators such as enterprise Web portals deployed at the installation.

**AUX-005470 [Required]** The MNWS shall support, at a minimum, XML, CAP, and RSS over secure HTTP in order to integrate with existing IP-enabled alert delivery devices.

**AUX-005480 [Required]** The MNWS shall interface with existing IP-enabled alert delivery devices for the following purposes:

- a. Sending alerts to a set of target recipients.
- b. Canceling an alert to a recipient or to all recipients.
- c. Reporting event alert delivery and subscriber responses.
- d. Reporting on the operational status of a delivery device.

#### ***3.5.10.4 Installed Unified Communication (UC) Systems***

**AUX-005490 [Required]** The MNWS shall interface with installed UC systems in order to deliver alert notifications in the form of voice calls and instant messages, and by means of other collaboration tools or capabilities available on the UC system that prove useful for disseminating alerts to the target subscribers.

NOTE: It is recognized that the MNWS will most likely need to employ different protocols and interface to a different set of APIs for each UC system. However, in each case, the communication between the MNWS and the UC system shall provide for authentication, authorization, integrity, and confidentiality.

**AUX-005500 [Required]** The MNWS shall do the following:

- a. Send alerts to sets of recipients or devices.
- b. Cancel a specific alert to a recipient or to all recipients.
- c. Report on event alert delivery and subscriber responses.
- d. Obtain the operational status for the UC system and the various functional components the MNWS is relying on to deliver the alerts.
- e. In the event of a theater-wide alert, the MNWS shall have the capability to instruct the UC systems to initiate up to 10,000 simultaneous "99" phone calls theater-wide.
- f. MNWS shall be compatible with the Installation Information Infrastructure Modernization Program (I3MP) selected system.

**AUX-005510 [Optional]** The UC system shall provide a panic button that enables subscribers to send real-time alerts to the MNWS. There shall be no indication or response in the subscriber's environment to the use of the panic button. The use of the panic button is by its very nature a secret act. The MNWS shall immediately notify authorized operators as to the specific panic button that has been activated, and the MNWS runs any pre-built alert notification scenarios designed for this event.

**AUX-005520 [Optional]** The UC system shall support remote viewing of Web cameras by UC display devices and by authorized operators logged into the MNWS.

**AUX-005530 [Optional]** The UC system shall support remote viewing of UC device cameras by authorized operators logged into the MNWS.

NOTE: This would occur only in the context of an emergency event.

### ***3.5.10.5 Non-IP Delivery Systems***

**AUX-005540 [Required]** The MNWS shall interface with the legacy non-IP delivery systems located at an installation such as non-IP Giant Voice systems, public address (PA) systems, and non-IP land mobile radio systems.

**AUX-005550 [Required]** The MNWS shall interface with the non-IP delivery systems for the following purposes:

- a. Sending alerts.
- b. Canceling alerts.
- c. Reporting on alert delivery status.
- d. Reporting on the status of the non-IP delivery system.

**AUX-005560 [Required]** The MNWS shall connect to the non-IP delivery devices using legacy physical interfaces such as the following:

- a. Serial interface (RS-232, RS-485).
- b. Dry contacts.
- c. Audio-out.
- d. Dual-Tone Multifrequency (DTMF).

### ***3.5.10.6 Integration With Giant Voice Systems***

**AUX-005570 [Required]** The MNWS shall be able to connect with an installation's IP and non-IP Giant Voice systems:

- a. In case of IP-based integration, the Giant Voice system and the APIs on both systems shall comply with all required information assurance certifications.
- b. In case of non-IP integration, the requirements of Section 2.13.4, CCA Support for Admission Control, shall apply.

**AUX-005580 AUX-005470 [Required]** The MNWS integration with Giant Voice systems shall not replace the existing Giant Voice activation method, but rather augment it for unified notification scenarios.

**AUX-005590 AUX-005480 [Required]** The MNWS integration with Giant Voice systems shall enable authorized operators to specify the message to be activated, including pre-recorded voice/tone and text-to-speech:

- a. If a Giant Voice system supports activation of specific zones/speakers, then authorized MNWS operators shall have the ability to activate specific zones/speakers of the Giant Voice system.

**AUX-005600 [Required]** The MNWS integration with Giant Voice systems shall comply with the Unified Facilities Criteria (UFC) requirements for Mass Notification Systems (MNS) integration.

### ***3.5.10.7 Integration With Indoor Voice Systems***

**AUX-005610 [Required]** The MNWS shall be able to connect with an installation's IP and non-IP Indoor Voice systems:

- a. In case of IP-based integration, the Indoor Voice system and the APIs on both systems shall comply with all required information assurance certifications.
- b. In case of non-IP integration, the requirements of Section 2.13.4, CCA Support for Admission Control, shall apply.

**AUX-005620 [Required]** The MNWS integration with Indoor Voice systems shall not replace the existing Indoor Voice activation method, but rather augment it for unified notification scenarios.

**AUX-005630 [Required]** The MNWS integration with Indoor Voice systems shall enable authorized operators to specify the message to be activated, including pre-recorded voice/tone and text-to-speech:

- a. If an Indoor Voice system supports activation of specific zones/speakers, then authorized MNWS operators shall have the ability to activate specific zones/speakers of the Indoor Voice system.
- b. Authorized MNWS operators shall have the ability to activate the strobe lights (if available).

**AUX-005640 [Required]** The MNWS integration with Indoor Voice systems shall comply with the UFC requirements for MNS integration.

### ***3.5.10.8 Integration With Fire Alarm Systems***

**AUX-005650 [Required]** The MNWS shall be able to connect with an installation's IP and non-IP Fire Alarm systems:

- a. In case of IP-based integration, the Fire Alarm system and the APIs on both systems shall comply with all required information assurance certifications.
- b. In case of non-IP integration, the requirements of Section 2.13.4, CCA Support for Admission Control, shall apply.

**AUX-005660** The MNWS integration with Fire Alarm systems shall not replace the existing Fire Alarm activation method, but rather augment it for unified notification scenarios

**AUX-005670** The MNWS integration with Fire Alarm systems shall enable authorized operators to specify the message to be activated, including pre-recorded voice/tone and text-to-speech:

- a. If a Fire Alarm system supports activation of specific zones/speakers, then authorized MNWS operators shall have the ability to activate specific zones/speakers of the Fire Alarm system.
- b. Authorized MNWS operators shall have the ability to activate the strobe lights (if available).

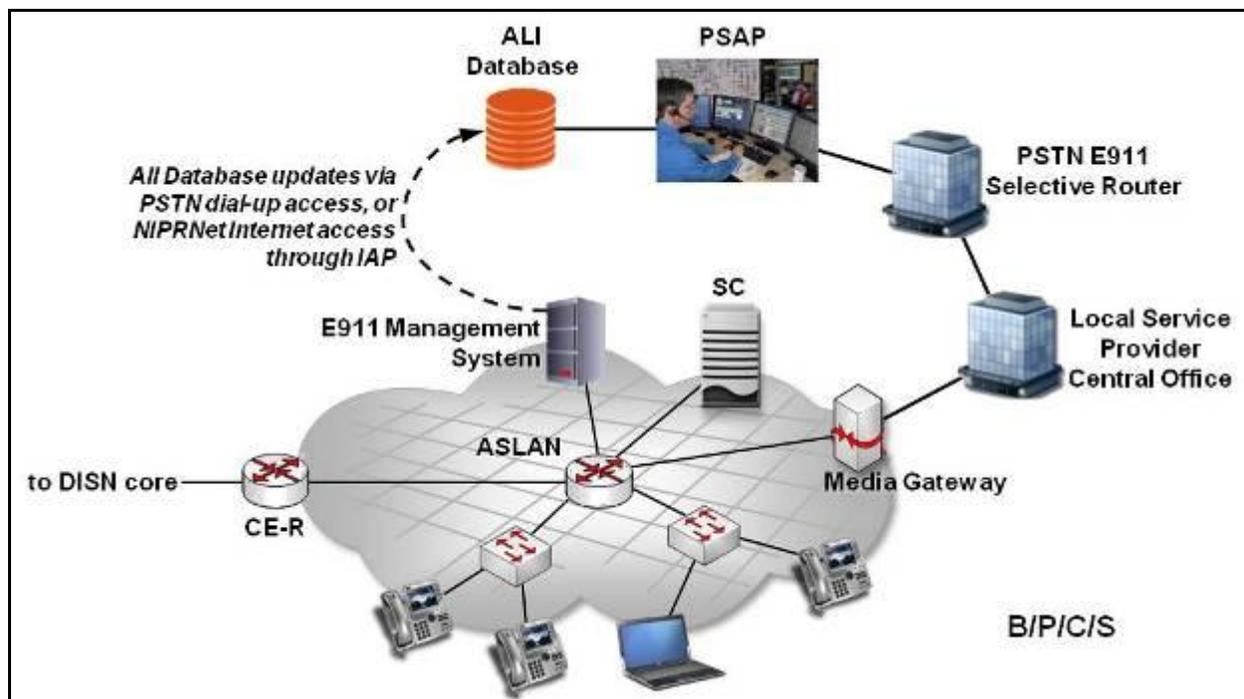
**AUX-005680** The MNWS integration with Fire Alarm systems shall comply with the UFC requirements for MNS integration and with National Fire Protection Association (NFPA) 72, National Fire Alarm and Signaling code.

## **3.6 E911 MANAGEMENT SYSTEM**

Standalone E911 Management Systems are UC appliances that enable a reliable user location to be provided to emergency response dispatch centers when a 911 call is made from a UC EI.

### **3.6.1 Scope, Assumptions, and Terms**

As illustrated in [Figure 3.6-1](#), E911 Management System Architecture for UC E911 Services, E911 Management Systems are intended to support wireline E911 service, including support for UC subscribers using softphones and subscribers connected via wireless LAN interfaces, such as Institute of Electrical and Electronics Engineers (IEEE) 802.11b/g/n.



**Figure 3.6-1. E911 Management System Architecture for UC E911 Services**

Public Safety Answering Point (PSAP) is the term used in these requirements for any emergency response dispatch center that is a terminating point for a 911 call, including those operated by a MILDEP.

The term Automatic Location Identification (ALI) database is used for any database of location information queried by a PSAP to determine the location of a 911 caller, regardless of who operates the database or of the database's implementation details.

As shown in [Figure 3.6-2](#), Illustrative ALI Database Records, each record in an ALI database is assumed to include, at a minimum, a location—composed of a street address and Emergency Response Location (ERL)—and an associated Emergency Location Identification Number (ELIN). An ERL identifies a specific physical location, area, or zone at the street address to which an emergency responder can be sent; e.g., the northeast quadrant of the third floor. An ELIN is a 10-digit telephone number that uniquely identifies the location (i.e., each ELIN is associated with one and only location).

Location Name	Street Address	ERL	ELIN
Joint Base ABC	123 Main St. Salem IL	3FLNE	618-555-1212
Joint Base ABC	123 Main St. Salem IL	3FLSE	618-555-1213
Joint Base ABC	123 Main St. Salem IL	3FLSW	618-555-1214
etc.			

**Figure 3.6-2. Illustrative ALI Database Records**

A PSAP attempts to match the calling party number received with an ELIN in the ALI database. If there is a match, then the associated street address/ERL information is used as the location of the 911 caller. Properly constructed and maintained ALI databases enable reliable location information to be determined based on the calling party number.

These requirements assume that a Default Location ALI database entry will be defined and maintained for each SC. A Default Location, and associated ELIN, identifies a location to which emergency responders can be sent in circumstances when a more precise location for an EI cannot be determined.

Base/post/camp/station (B/P/C/S) 911 services supported by E911 Management Systems should comply with Federal, state, and local 911 regulations for the regions where these systems are deployed. This compliance may require additional capabilities beyond what is required in this section. For example, state and local agencies serving a B/P/C/S location may impose certain rules regarding the format of location and ELIN data stored in their ALI databases.

### 3.6.2 General E911 Management System

**AUX-005690 [Required: E911 Management System]** The E911 Management System shall support signaling interfaces to UC SC products from at least two different vendors, and shall use these interfaces for signaling with those SCs for EI registrations and processing of 911 calls from EIs.

NOTE: A system that interoperates with only a single SC can be certified as part of the SC, but, since it has not demonstrated multivendor interoperability, it cannot be certified as a standalone product.

**AUX-005700 [Conditional: E911 Management System]** If the UC SC product supports a proprietary signaling interface for E911 Management System interconnection, then the E911 Management System shall support that interface, per the SC vendor's proprietary interface specifications.

**AUX-005710 [Conditional: E911 Management System]** If the UC SC product supports a standardized signaling interface for E911 Management System interconnection, then the E911

---

Management System shall support that interface, per standardized interface specifications identified by the SC vendor.

### 3.6.3 Automatic Location Identification (ALI) Information

**AUX-005720 [Required: E911 Management System]** The E911 Management System shall maintain, for each SC to which it interfaces, an appropriate set of location data and corresponding ELINs that identify the physical locations of each of the EIs served by the SC.

NOTE: The level of detail in the location data depends on the B/P/C/S or enclave's E911 wiremap and the approach chosen by the 911 administrator for mapping physical locations to ERLs.

**AUX-005730 [Required: E911 Management System]** The E911 Management System shall also maintain any additional data items required by the ALI databases supporting the PSAPs serving the B/P/C/S or enclave. These PSAPs are responsible for handling 911 calls from the EIs served by the SCs to which the E911 Management System interfaces.

NOTE: Sources for the ALI data maintained by the E911 Management System may include the SCs with which it interfaces, SC service provisioning systems, and direct manual entry.

**AUX-005740 [Required: E911 Management System]** The E911 Management System shall be capable of exporting, to a file, ALI data in .csv or National Emergency Number Association (NENA), Version 2.0 or later, formats.

**AUX-005750 [Conditional: E911 Management System]** If the B/P/C/S or enclave requires that ALI data be provided in a proprietary format, then the E911 Management System shall be capable of exporting, to a file, the ALI data in the required proprietary format.

If the E911 Management System supports direct, secure electronic transfer of ALI data to a target ALI database (or to an intermediary application or service that in turn updates the ALI database), and the B/P/C/S or enclave supports and allows such a transfer, then a direct electronic export of ALI data may be made in lieu of exporting the data to a file.

**AUX-005760 [Required: E911 Management System]** The E911 Management System shall be capable of exporting ALI data:

- a. On a periodic, scheduled basis.
- b. In response to a configurable event (i.e., the creation of a new ERL and ELIN in the system).
- c. In response to an administrator's request, on an ad hoc basis.

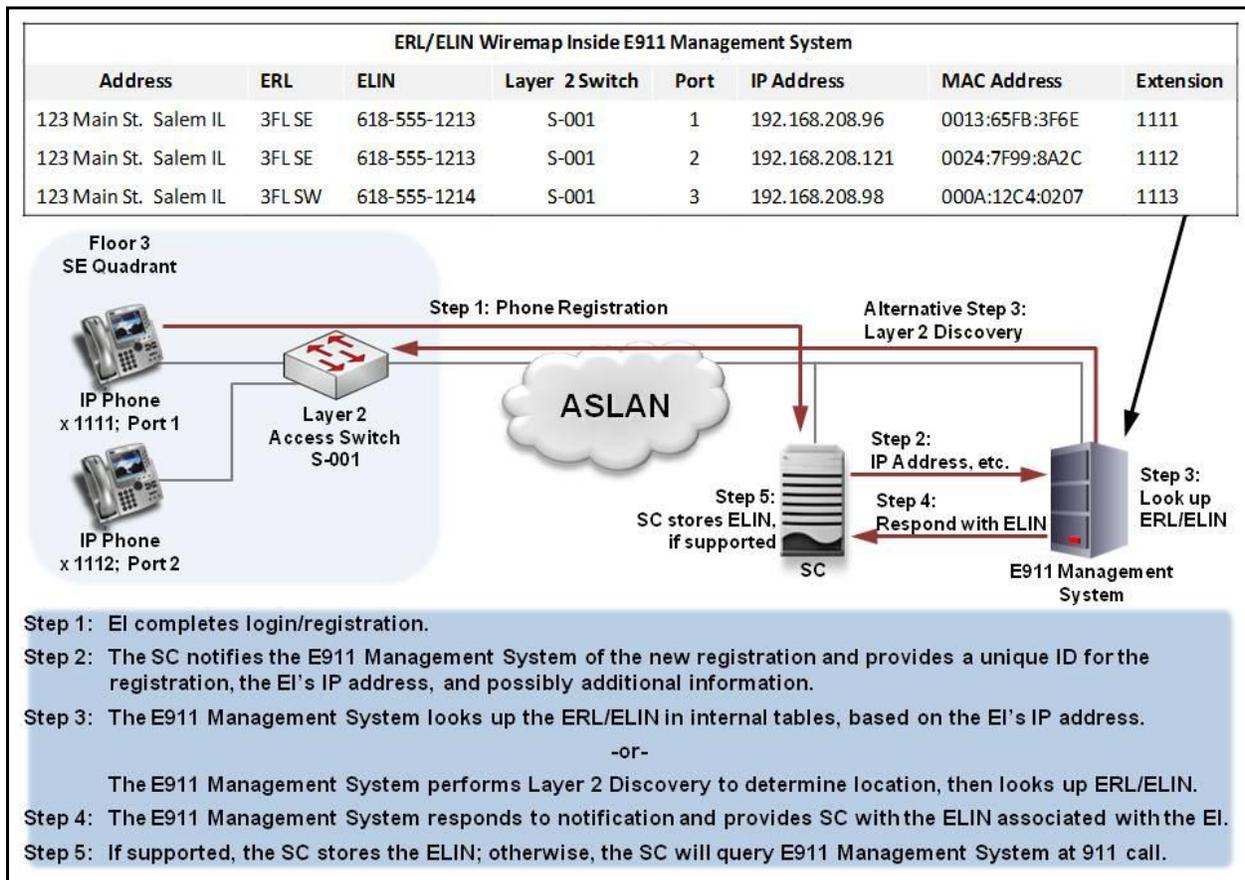
### 3.6.4 End Instrument Location at Registration

**AUX-005770 [Required: E911 Management System]** When notified by an SC of an EI registration, the E911 Management System shall do the following:

- a. Determine the physical location of the EI, based on IP address assigned to the EI and any additional information provided by the SC at registration notification.
- b. Determine the ERL assigned to that location.
- c. Keep an internal record of the EI registration that includes the ELIN for the ERL assigned to the EI's location.
- d. Acknowledge receipt of the registration notification to the SC, and include the EI's ELIN in that acknowledgement.

How the E911 Management System determines the physical location of a registered EI is not specified in these requirements. It may use network endpoint discovery techniques, it may reference an internally maintained mapping of IP addresses to locations/zones, or it may use some other approach provided that the B/P/C/S or enclave fully supports the approach used.

The message flow at EI registration is shown in [Figure 3.6-3](#), Message Flow at EI Registration.



**Figure 3.6-3. Message Flow at EI Registration**

If the E911 Management System is unable to determine the location of a registered EI, then it shall use the ELIN of the Default Location assigned to the notifying SC as the EI's ELIN, for both its internal record of the EI's registration and in the notification acknowledgement response.

NOTE: The ELIN associated with an EI, as determined by the E911 Management System, will be used by the SC as the calling party number in the event that a 911 call is made from that EI while it is registered with the SC. The SC may maintain the ELIN received in the notification acknowledgement or it may query the E911 Management System for the ELIN as part of processing a 911 call. The 911 call flows are illustrated in [Figure 3.6-4](#).

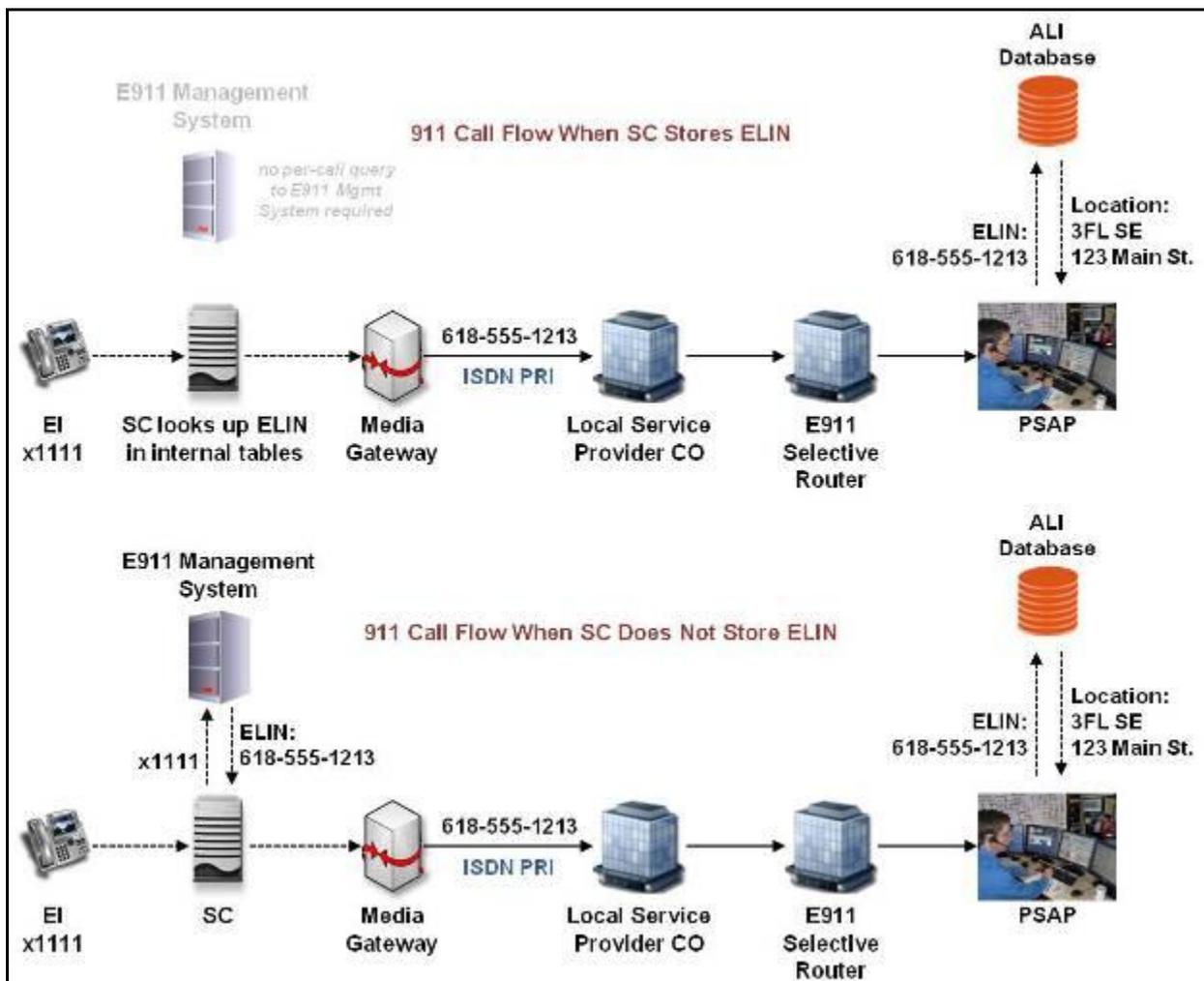


Figure 3.6-4. 911 Call Flows

### 3.6.5 Support for ELIN Query at 911 Call

**AUX-005780 AUX-005680 [Required: E911 Management System]** When queried by an SC processing a 911 call from a registered EI, the E911 Management System shall provide the SC with the ELIN associated with that EI in its internal record.

### 3.6.6 SC Interfaces With E911 Management Systems

SCs are not required to support interfaces to standalone E911 Management Systems. The burden is on the E911 solution to interface to the SC.

If an SC does support interfaces to E911 Management Systems, then the requirements in this section apply. Furthermore, the requirements in this section apply only to SCs that are connected to an active E911 Management System.

**AUX-005790 [Required: SC]** The SC shall notify the E911 Management System whenever an EI registers with the SC. The SC shall provide the EI's IP address and a unique identifier for the registration to the E911 Management System with the registration notification.

The SC may provide additional information, such as the EI's Move, Add, Change (MAC) address, to the E911 Management System with the registration notification.

**AUX-005800 [Conditional: SC]** If the SC supports receiving and storing, at the EI level, an ELIN provided by an E911 Management System in a response message to a registration notification, then the SC shall do the following:

- a. Receive the ELIN provided and store it as part of the information maintained for that EI with respect to the registration process.
- b. Populate the Calling Party Number information element in the ISDN PRI setup message that is sent over the commercial PRI from the SC's MG to the PSTN, with that ELIN, if a 911 call is made from that EI.

If the E911 Management system does not respond to an EI's registration notification, or does not provide a valid ELIN in its response, and a 911 call is made from that EI, then the SC shall populate the Calling Party Number information element with the ELIN configured to identify the Default Location for that SC.

**AUX-005810 [Conditional: SC]** If the SC supports querying an E911 Management System during 911 call processing in order to determine the ELIN for the EI from which the 911 call was made, then the SC shall do the following:

- a. Request the E911 Management System to provide the ELIN for that EI, based on the unique identifier for that EI provided at registration notification.
- b. The SC shall receive the ELIN provided by the E911 Management System, and populate the Calling Party Number information element in the ISDN PRI setup message, that is sent over the commercial PRI from the SC's MG to the PSTN, with that ELIN.

If the E911 Management system does not provide a valid ELIN within a configurable time period, then the SC shall use the ELIN that was configured to identify the Default Location for that SC as the Calling Party Number information element.

**AUX-005820 [Required: SC]** If a 911 call is made from an unregistered EI, then the SC shall populate the Calling Party Number information element in the ISDN PRI setup message that is sent over the commercial PRI from the SC's MG to the PSTN, with the ELIN configured to identify the Default Location ERL for that SC.

### 3.6.7 On-Site Notification of 911 Call

**AUX-005830 [Conditional: E911 Management System, SC]** If the E911 Management System supports notification of a 911 call to a configurable entity within the B/P/C/S or enclave other than a PSAP, such as a front desk or security command center, and the SCs to which the E911 Management System interfaces support notifying the E911 Management System when processing a 911 call, then the E911 Management System shall provide a notification message to a configured non-PSAP entity when a 911 call is made.

Allowed notification methods include automated voice call, e-mail, and text messaging.

### 3.6.8 IPv6 Support

**AUX-005840 [Required: E911 Management System]** Conformant with Section 5, IPv6, the E911 Management System shall support dual IPv4 and IPv6 stacks (i.e., support both IPv4 and IPv6 in the same IP end point) as described in RFC 4213.

**AUX-005850 [Required: E911 Management System]** The E911 Management System shall meet all of the IPv6 protocol requirements for Network Appliances and Simple Servers (NA/SS) products in Section 5, IPv6, including the requirements in Table 5.2-4, UC Network Appliances and Simple Servers (NA/SS).

### 3.6.9 Information Assurance

**AUX-005860 [Required: E911 Management System]** E911 Management Systems shall meet the Information Assurance requirements of all applicable DISA STIGs.

### 3.6.10 OAM&P

**AUX-005870 [Required: E911 Management System]** The E911 Management System shall allow an administrator to read, add, delete, and modify the ERL/ELIN entries maintained in the system.

**AUX-005880 [Required: E911 Management System]** The E911 Management System shall allow an administrator to configure authentication credentials so that the system can authenticate the SCs to which it interfaces, and the SCs can authenticate the E911 Management System.

**AUX-005890 [Conditional: E911 Management System]** If the E911 Management System supports direct, secure electronic transfer of ALI data to a target ALI database, then the E911 Management System shall allow an administrator to configure the address of an ALI database,

along with authentication credentials, so that the system can authenticate the ALI database and the ALI database can authenticate the E911 Management System.

Note that, in this requirement, “target ALI database” means the database proper, or any intermediary application or service that in turn updates the target ALI database.

## 3.7 CUSTOMER PREMISES EQUIPMENT

### 3.7.1 General Description

A wide variety of customer premises equipment (CPE) manufactured and sold by many sources was connected to the line (subscriber) side of a DSN switching system. Such varieties include industry “American National Standards Institute – European Telecommunications Standards Institute (ANSI-ETSI) Standards” based digital and analog devices, and non-standards based proprietary digital devices. During the transition period between TDM and IP-based technologies, some locations may have a requirement to interface the legacy CPE to an SC. As a result, most SC vendors provide an optional Integrated Access Device (IAD) to permit the use of CPE until it is replaced.

The CPE devices may include answering machines, voice mail systems, automated call distributors, proprietary telephone sets, standards-based telephone sets, facsimile machines, voice-band modems, ISDN Network Termination 1 (NT1) devices and Terminal Adapters (TAs), and certain devices that are deemed mandatory for local or host nation telecommunications network compliance (i.e., 911 emergency service).

### 3.7.2 Requirements

All CPE devices are required to meet the following requirements:

**AUX-005900 [Conditional]** If a CPE device supports MLPP, then that device shall do so in accordance with the requirements listed in Section 2.25.2, Multilevel Precedence and Preemption, and shall not affect the DSN interface features and functions associated with line supervision and control.

**AUX-005910 [Required]** All DSN CPE, at a minimum, must meet the requirements of Part 15 and Part 68 of the Federal Communications Commission (FCC) Rules and Regulations, and the Administrative Council for Terminal Attachments (ACTA).

**AUX-005920 [Conditional]** If a CPE device supports autoanswer, then that device shall have an “autoanswer” mode feature allowing the autoanswer mode to be set to a “time” more than the equivalency of four ROUTINE precedence ring intervals, in accordance with Section 2.25.2, Multilevel Precedence and Preemption, before “answer” supervision is provided.

**AUX-005930 [Conditional]** If a CPE device is required to support precedence calls above ROUTINE precedence, then that device shall respond properly to an incoming alerting (ringing)

precedence call cadence, as described in Section 2.9.1.2.1, UC Ringing Tones, Cadences, and Information Signals.

**AUX-005940 [Conditional]** If a CPE device can “out dial” DTMF and/or dial pulse (DP) digits (automatic and/or manual), then that device shall comply with the requirements as specified in Telcordia Technologies GR-506-CORE, LSSGR: Signaling for Analog Interfaces, Issue 1, June 1996, paragraph 10. That device shall also be capable of outputting and interpretation of DTMF digits on outgoing and two-way trunks as specified in Telcordia Technologies GR-506-CORE, LSSGR: Signaling for Analog Interfaces, Issue 1, June 1996, paragraph 15, and [Table 3.7-1](#).

**Table 3.7-1. DTMF Generation and Reception From Users and Trunks**

LOW GROUP FREQUENCIES	NOMINAL FREQUENCY IN HZ	HIGH GROUP FREQUENCIES NOMINAL FREQUENCY IN HZ			
		1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	FO (A)	
770 Hz	4	5	6	F (B)	
852 Hz	7	8	9	I (C)	
941 Hz	*	0	A or #	P (D)	

**AUX-005950 [Conditional]** If a CPE device contains a modem or facsimile machine, then that modem or facsimile machine shall be compatible with ITU and Telcordia standards, as applicable.

**AUX-005960 [Conditional]** If a CPE device contains a facsimile device, then that facsimile device, at a minimum, shall meet the requirements in accordance with applicable DOD Information Technology (IT) Standards Registry (DISR) standards.

**AUX-005970 [Conditional]** If Configuration Management and/or Fault Management is provided by the CPE device so that it can be managed by the Advanced DSN Integrated Management Support System (ADIMSS) or other management systems, then the management information for that CPE device shall be provided by one or more of the following serial or Ethernet interfaces:

- a. Serial interfaces shall be in accordance with one of the following standards:
  - (1) ITU-T Recommendation V.35.
  - (2) TIA-232-F.
  - (3) EIA-449-1.
  - (4) TIA-530-A.
- b. Ethernet interfaces shall be in accordance with IEEE 802.3-2002.

**AUX-005980 [Conditional]** If a CPE device supports 911 and E911 emergency services, then, at a minimum, the 911 and the E911 (tandem) emergency services shall have the capability to “hold” (prevent) the originating subscriber or caller from releasing the call, via the “switch

supervision interaction for line and trunk control by the called party” feature, in accordance with Telcordia Technologies GR-529-CORE. Additionally, the FCC regulations regarding 911 and E911 must be considered.

## 3.8 DOD SECURE COMMUNICATIONS DEVICES

### 3.8.1 General Description

This section describes the requirements that will be used to certify DOD Secure Communications Devices (DSCDs) when directly connected to or otherwise traversing the DSN, PSTN, or DRSN Gateway to or from the DSN.

This section applies to the secure mode operation of any DSCD that either directly connects to the DSN, the PSTN, or the DRSN Gateway or traverses these networks in the course of conducting a secure communications session, regardless of where the telephone call originates or terminates. The certification test environment for DSCDs shall include configurations that realistically simulate fixed networks (i.e., DSN, DRSN via the DSN Gateway, PSTN) and deployed networks, such as digital voice exchange (DVX) systems and other configurations as defined by the Executive Agent for Theater Joint Tactical Networks, or any combination thereof.

### 3.8.2 Requirements

The JITC will validate all the features and capabilities of a DSCD device, including voice, data, and facsimile transmission.

**AUX-005990 [Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD]** The enabled DSCD shall be only those that are type approved by the National Security Agency (NSA) and are listed on the NSA Secure Product Web site. Each DSCD must support at least one NSA-approved secure protocol. If the DSCD supports more than one secure protocol, then it must meet all the requirements for at least one of the secure protocols and must minimally support the other protocols that are provided on the DSCD.

**AUX-006000 [Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD]** The DSCD devices that use a two-wire analog or basic rate interface (BRI) shall meet the EI requirements as specified in [Section 3.7](#), Customer Premises Equipment. The DSCD devices that use an IP interface shall meet the EI requirements as specified in Section 2, Session Control Products, of UCR 2013. DSCD devices that support DSN trunk interfaces [PRI or IP (UC SIP)] shall meet the interface requirements defined in the following:

- a. Section 2, Session Control Products, MG Support for ISDN PRI Trunks, of UCR 2013, for PRI.
- b. UC SIP 2013 document for UC SIP.

**AUX-006010 [Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD]** A DSCD device that supports one of the required signaling modes shall interoperate with and establish

secure sessions with other compatible devices with at least an 85 percent secure call completion rate.

**AUX-006020 [Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD]** The DSCD shall be capable of using the protocol(s) provided to establish a secure session within 60 seconds and must maintain secure communications for the duration of the secure portion of the call.

**AUX-006030 [Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD]** The DSCD shall operate in a network that has an E2E latency of up to 600 milliseconds.

**AUX-006040 [Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD]** The DSCD shall achieve and maintain a secure voice connection with a minimum MOS of 3.0.

**AUX-006050 [Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD]** Once connected to the rekey center, the DSCD shall obtain a new key and properly process that new key with a 95 percent rekey completion rate.

**AUX-006060 [Conditional: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD]** If the DSCDs can establish secure sessions on a Continuously Variable Slope Delta (CVSD) switch and terminate on a CVSD switch without ever traversing or otherwise interacting with the DSN, DRSN, or PSTN, then that DSCD must do so with a 50 percent completion rate.

**AUX-006070 [Conditional: FNBDT/SCIP Enabled DSCD]** If the DSCDs can establish secure sessions on IP networks using Future Narrowband Digital Terminal (FNBDT)/Secure Communications Interoperability Protocol (SCIP), then that DSCD shall satisfy all the DSCD end point requirements described in NSA documents SCIP-215 and SCIP-216.

**AUX-006080 [Required: STE Enabled DSCD, FNBDT/SCIP Enabled DSCD]** The DSCD devices shall support a minimum data rate and facsimile transmission rate of 9.6 kbps.