TABLE OF CONTENTS

LIST OF FIGURES

<u>**FIGURE**</u> <u>**PAGE**</u>

<div align="center">

SECTION 3
AUXILIARY SERVICES

</div>

This Section contains explanatory text on some of the Auxiliary Services Requirements in Unified Capabilities Requirements (UCR) 2013, Section 3, Auxiliary Services. It also contains explanatory text on other Auxiliary Services in the Unified Capabilities (UC) Network, including Services provided by Required Ancillary Equipment, and Services provided by UC Gateways (such as Centralized Connections to Commercial Voice Internet Service Providers, Centralized Secure Connections to Wireless Providers, and Allied Network Interfaces).

3.1 REGIONAL HUB DESIGN FOR REQUIRED ANCILLARY EQUIPMENT (RAE)

Operation of UC products requires management/security support from server functions that normally are not part of a Softswitch (SS), Session Controller (SC), or Session Border Controller (SBC) product. These functions/severs are referred to as Required Ancillary Equipment (RAE) and must be made available at the site to support the SS, SC and SBC. The RAE support includes Authentication, Authorization, and Accounting (AAA) servers; access to a Domain Name Service (DNS) server; SYSLOG server; Network Time Protocol (NTP) server; Dynamic Host Configuration Protocol (DHCP) server; and Department of Defense (DoD) Public Key Infrastructure (PKI) certificate verification, including access to an Online Certificate Status Protocol (OCSP) responder.

As a companion project associated with relocating SSs from DoD Components to the Defense Information Systems Agency (DISA) network domain and security enclaves, DISA is in the process of procuring and installing RAE to support the SS nodes. To simplify management, minimize staffing and equipment cost centralized RAE hubs will be installed at Hickam, Scott, and Vaihingen. The three RAE hubs will provide support to the SSs within each theater. The RAE hub components will reside within the Defense Information Systems Network (DISN) network domain and DISA security enclaves. The operational concept for the regional RAE hub arrangement is illustrated in .
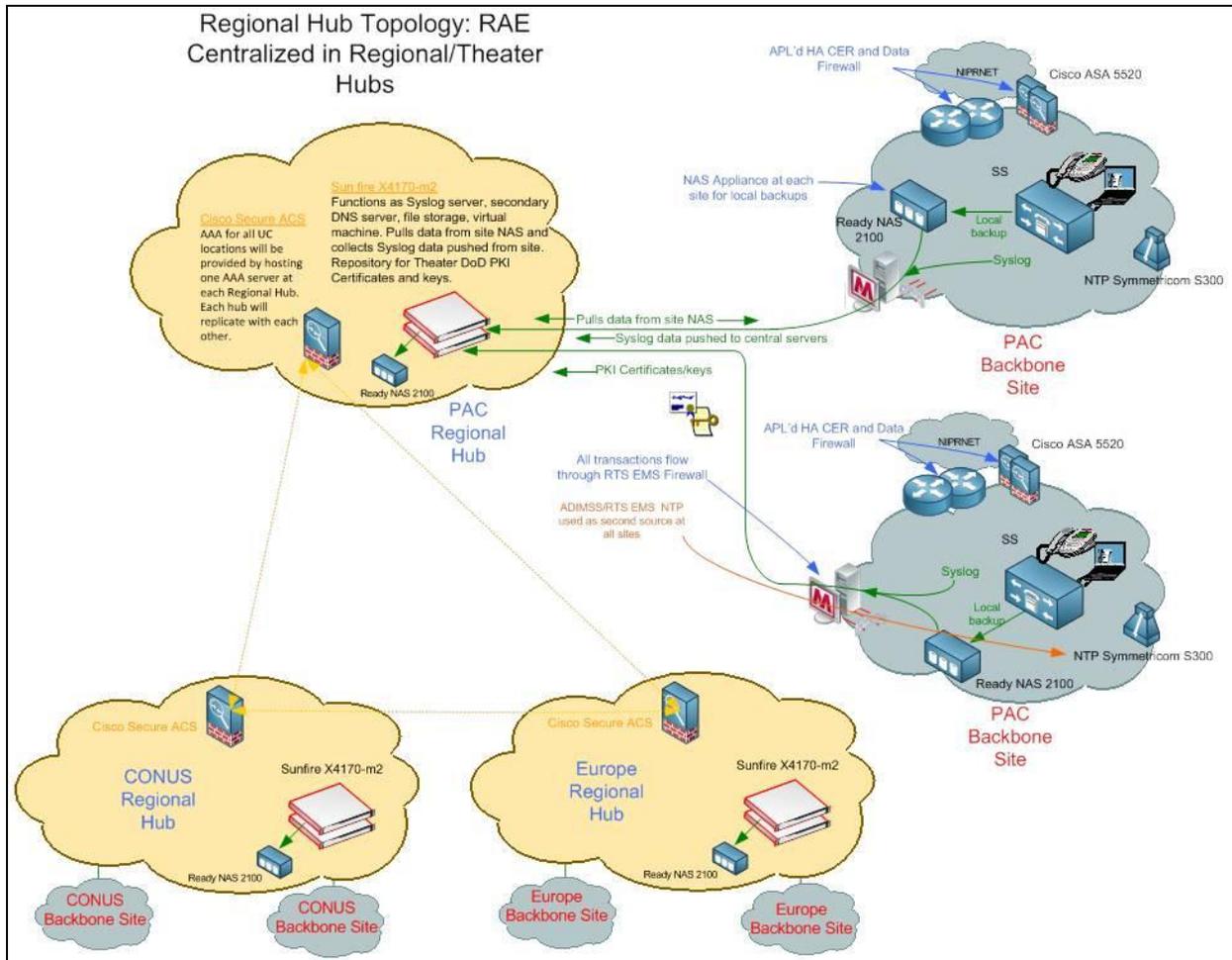
Figure 3.1-1. Regional RAE Hub Topology

1. Each SS in the network will have a 1 rack unit Network Attached Storage (NAS) appliance installed at the local site. The local on-site NAS provides a method to meet the local backup requirement without hosting a server. The on-site SS servers will push complete disk images to the local NAS and the central hub-based servers will pull the images from each NAS on a regular basis. The local file storage capability will be provided by a NETGEAR Ready NAS 2100 with 4 Terabytes (TB) of storage capacity.

2. The regional hubs will be equipped to provide off-site system backup storage, Authentication, Authorization, and Accounting (AAA) Services, SYSLOG, secondary DNS service, and storage of Internet Protocol (IP) Detail Records (IPDRs). The following equipment will be installed at each regional hub:

   a. AAA Services will be provided by one (1) Cisco 1121 Access Control System appliance with Cisco Secure Access Control System 5.2. The Cisco Access Control Server (ACS) will be configured to provide centralized AAA services to all other DISN UC Backbone locations/equipment (SS, SBCs, Firewalls [FWs], Customer Edge [CE] Routers [CE-Rs], Access Switches, etc.) within the theater by invoking either Remote Authentication Dial-

in User Server/Service (RADIUS) or Terminal Access Controller Access Control System (TACACS).

Additionally, the ACS servers will be configured to replicate with the other regional ACS servers located at the two other hub locations.

b. Centralized Services will be provided to support off-site system backup storage, SYSLOG, secondary DNS service, and storage of Internet Protocol Detail Record's (IPDR) will be provided centrally by a server located at each regional hub. The centralized services will be provided by two Oracle Sun Fire X4170-m2 servers, one active and one backup.

3.2 COMMERCIAL COST AVOIDANCE AND HYBRID ROUTING FEATURE

The Routing Database (DB) is a DISA-owned and DISA-operated DB that contains records of the Defense Switched Network (DSN) numbers, commercial (Public Switched Telephone Network [PSTN]) numbers, SC identifiers, and SS identifiers for UC end users served by SCs. This DB may also contain records of DSN numbers and commercial numbers for individual DSN end users served by DSN End Offices (EOs) and Private Branch Exchanges (PBXs). The DB records may be populated automatically by SCs, whenever end users' numbers are added to an SC during activation of that end user on the SC. The DB records also may be populated manually by a DISA craftsperson, using DSN and commercial number information from an SC site or DSN EO or PBX site.

The SSs that support the Hybrid Routing (HR) feature query the Routing DB to determine whether there is an SC identifier, a primary SS identifier, and a backup SS identifier stored there that matches the dialed DSN number on a UC call that enters the SS. Figure 3.2-1, Hybrid Routing Feature Operation in the Network, illustrates how the Hybrid Routing Feature operates in the network.
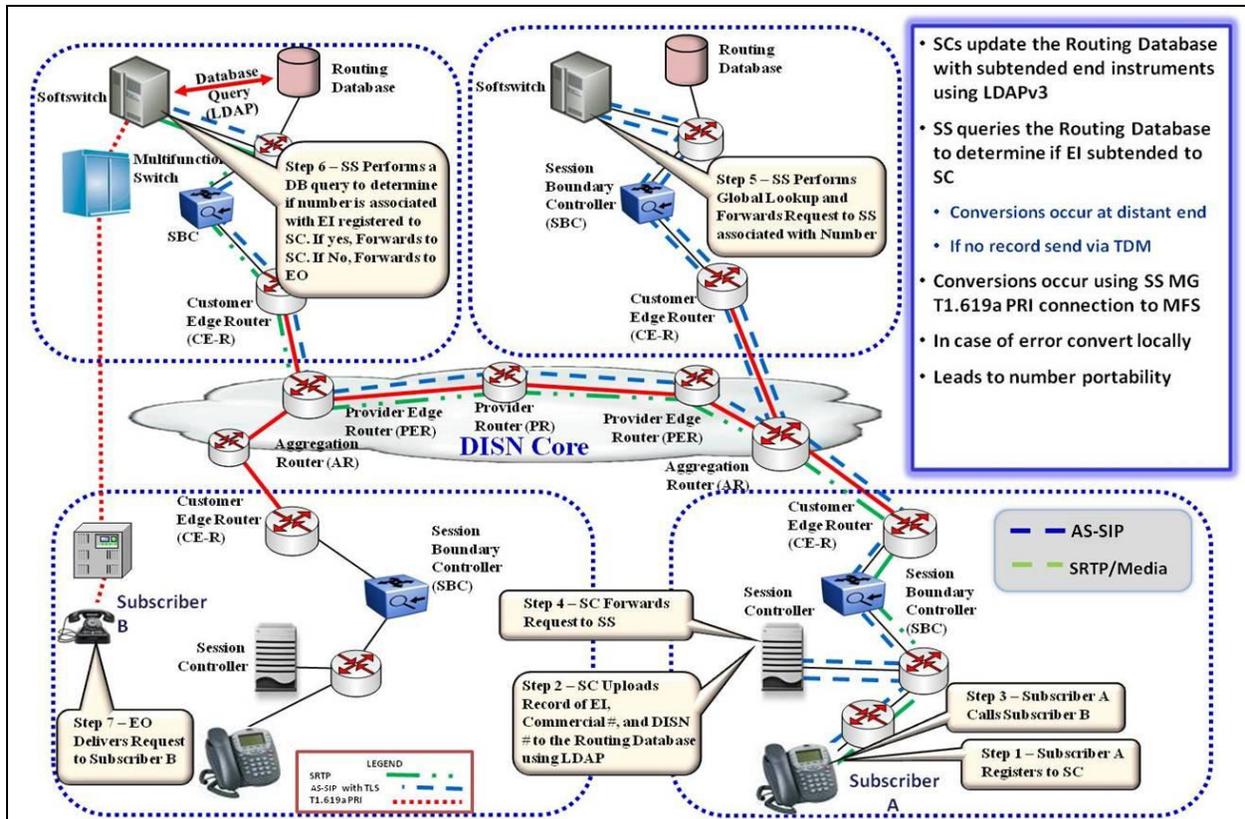
Figure 3.2-1. Hybrid Routing Feature Operation in the Network

The SCs that support the Commercial Cost Avoidance feature query the Routing DB to determine whether there is a DSN number stored there that matches the dialed commercial number on a commercial call from the SC (e.g., a 9+9 call, or a 9+8 call). Figure 3.2-2, Commercial Cost Avoidance Feature Operation in the Network, depicts how the Commercial Cost Avoidance feature operates in the network.

The protocol that SCs and SSs use to query and update the Routing DB is Lightweight Directory Access Protocol (LDAP) version 3 (LDAPv3), secured using Transport Layer Security (TLS), and signaled via IP over the DISN Wide Area Network (WAN).
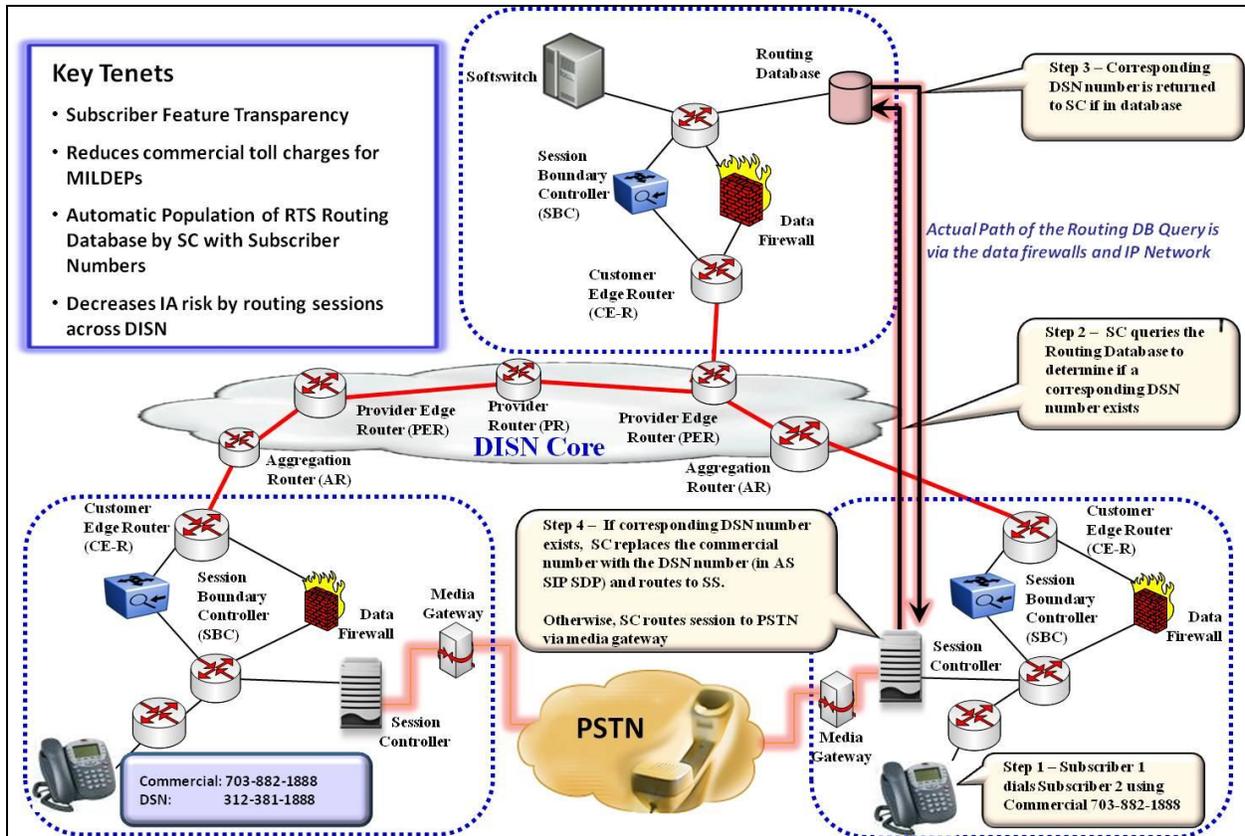
Figure 3.2-2. Commercial Cost Avoidance Feature Operation in the Network

3.3 INTERFACE TO EMERGENCY RESPONSE SYSTEMS

This section addresses two emergency response products that must be supported at DoD locations and must interface DoD UC products. These two systems are the E911 Management System and the Mass Notification Warning System.

3.3.1 Enhanced 911 Interface

Access to Enhanced 911 is available from SC/Media Gateways using the dial plan. This interface is Time Division Multiplexing (TDM) because of Information Assurance requirements. E911 Management Systems interface with SCs to provide reliable user locations to Public Safety Answering Points (PSAPs), including cases where DoD components host a PSAP for E911 services.

3.3.2 Mass Notification Warning System Interface

The Mass Notification Warning System will be used to meet the DoD's requirements to provide Association of Public-Safety Communications Officials (APCO) – International, Project 25, systems at DoD locations. The Mass Notification Warning System is a product that monitors event sources and if an event from an event source meets pre-defined emergency criteria then the

default action is for the Mass Notification Warning System (MNWS) to inform system operators of the event. The operators qualify the event and when appropriate instructs the system to initiate alerts. The system then initiates alerts via interfaces to alert delivery systems.

Currently all local access to any public network such as PSTN service; E911; and APCO – International, Project 25, systems must be via TDM and cannot be transmitted over IP, because of Information Assurance requirements. The only connection to the PSTN is through a TDM interface using Primary Rate Interface (PRI) or Channel Associated Signaling (CAS), so there is no interaction between the Voice and Video over IP (VVoIP) system and commercial VVoIP IP networks.

3.4   OTHER AUXILIARY SERVICES

Other auxiliary services that are included in UCR 2013 are as follows:

- UC audio and video conferencing systems.
- Customer premises equipment.
- DoD secure communications devices.