Local Session Controller: Cisco's Solution for the U.S. Department of Defense Network of the Future

What You Will Learn

The future of the Department of Defense's (DoD) networks focuses on the integration of voice, video and data services. This converged network approach goes beyond the traditional methodology of the past that only included time-division multiplexing (TDM) systems. Today, it joins together content-rich, collaborative services such as voice, video, chat, mail applications, as well as web-based conferencing services with shared resources. Cisco is committed to enabling this network evolution with its enterprise-proven products and solutions. This document illustrates the Cisco® Local Session Controller (LSC) solution with the objective of providing a high-level understanding of the architecture and the components involved.

Introduction

To address the needs of the DoD community, the Defense Information Systems Agency (DISA) has created unified capabilities requirements for an IP-enabled communications architecture that improves interoperability and security that will be transported over its data networks, to include its TDM infrastructures. The goal is to provide end-to-end unified capabilities that include voice, video and data services across highly available networks regardless of vendor or technology. The set of published public specifications that govern the policy and requirements is known as the DISA Unified Capabilities Requirements (UCR).

The UCR has been divided into several categories, which represent distinct components of the overall architecture. Any vendor who wants to sell a product or solution to DISA controlled networks must first go through a rigorous certification process. This certification process consists of two phases: Information Assurance (IA) and Interoperability (IO), where IA focuses on the security of the product's components, and IO concentrates on conformance of functional requirements amongst the different vendor's products. Vendors who pass both tests and are awarded certification letters by the Defense Security Accreditation Working Group (*DSAWG*), and are placed on the Approved Products List (APL)

Traditional Architecture

Today, the unclassified DISA voice architecture, known as the Defense Switch Network (DSN), is still heavily dependent on TDM technology. However, progress has been made and isolated implementations of UCR certified, IP-enabled, voice communications using Voice over IP (VoIP) solutions do exist. Hierarchically any VoIP solution that is installed must be connected to the larger voice (DSN) network through the use of traditional TDM technology as previously defined by the Generic Switching Center Requirements (GSCR). Figure 1 provides a high-level overview of the major components.

Figure 1.   DoD Defense Switched Network
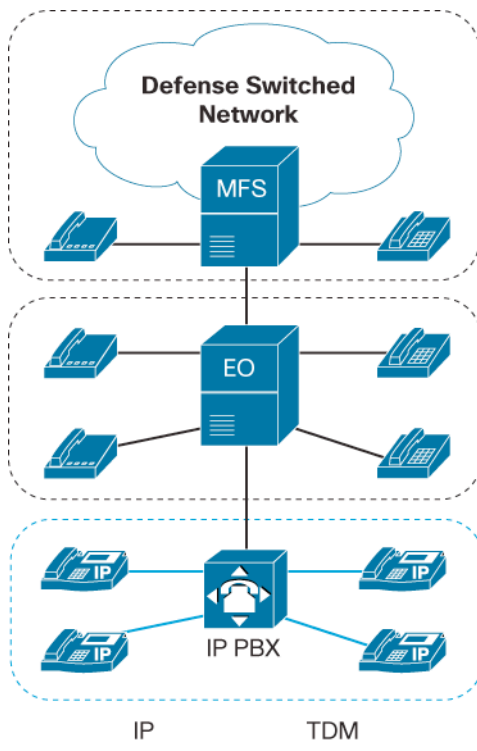
At the top tier, the Core of the DISA TDM architecture, are telephone switches known as Multi-Function Switches (MFS) that are responsible for the end-to-end connectivity across the entire DSN fabric. The common signaling used amongst these switches has been the Signaling System 7 (SS7) protocol, which is also used by the world Public Switched Telephone Network (PSTN).

At the immediate layer are the End Office (EO) or Small End Office (SMEO) telephony switches. These too are still largely comprised of TDM-based technology and are installed by individual military departments (often referred to as MILDEPS). It is typical for a MILDEP to own and operate its own EO or SMEO switching infrastructure and they connect it to the DSN through the MFS.

The last layer of the hierarchy is where IP-based Private Branch eXchanges (PBXs) can be integrated into this traditional architecture. Internet Protocol-based PBXs cannot connect directly to the Core of the DSN fabric without first being connected to an EO or SMEO at the MILDEP level. Under the DISA UCR, there are two types of IP PBX certifications: PBX1 and PBX2. The key distinction between these two certifications is PBX1-certified products

provide Command and Control (C2) requirements, such as Multi-Level Priority and Preemption (MLPP) functionality where PBX2 certified solutions do not.

Cisco Unified Communications Manager (CUCM), combined with Cisco routers, switches, and voice gateways, is certified as a PBX1 solution and is listed on the DISA APL. Cisco has maintained this certification for many years and has a large installed base of more than 550,000 VoIP handsets.

Current Architecture

DISA's current architecture is similar to the traditional architecture discussed in the preceding section, although its tiered model has several important improvements. Figure 2 presents a high-level diagram of the architecture. A more detailed diagram, outlining more of the components, is discussed in this document in subsequent sections.

Figure 2.   Current DISA Architecture: High-Level Diagram
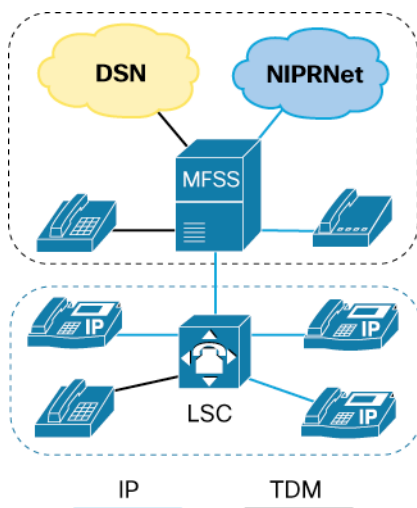
At the Core of the DSN fabric, a Multi-Function SoftSwitch (MFSS) has now replaced the MFS. The MFSS is an extension to the traditional MFS, as it still can connect to the DSN through TDM. However, a MFSS adds the capability to connect voice calls (VoIP) over the DoD Non-classified Internet Protocol Routed Network (NIPRNet), its unclassified data network, using IP. The key improvement to a MFSS over a MFS is the ability to connect to IP, as well as the TDM network as a single system. This direction also led DISA to extend the IP-based Session Initiation Protocol (SIP) to meet the DoD's unique call-control requirements to facilitate open-standard IP voice communications. This SIP extension only ported key TDM functional requirements, which were defined in the legacy GSCR, into the UCR. Hence, DISA now refers to this extended SIP capability as Assured Services SIP (AS-SIP), thus dropping TDM-based language such as MLPP. The key capability of AS-SIP is Resource Priority Headers (IP-based version of MLPP) and standardized Quality of Service (QoS) network traffic markings by all certified vendors.

A variation of the MFSS, known as a WAN SoftSwitch (WAN-SS), may be used in the Core when TDM connectivity to the DSN is not required. A WAN-SS connects only to the NIPRNet and only through what is defined as an AS-SIP trunk. TDM connectivity (trunks or line-side) to the DSN is not supported by a WAN-SS.

A finite number of MFSS and WAN-SS devices will be deployed within the DISA architecture and all these assets are owned and operated by DISA. Although an MFSS or WAN-SS can service individual end instruments (sometimes called EIs), the primary function of these devices is to act as the core of the network.

The next layer of the architecture is where the LSC is implemented. Local Session Controllers replace the EO and SMEO requirements within the traditional architecture. Historically, under the GSCR, DISA had multiple categories for the classes of telephone switches as defined by specific carrier-based requirements that mirrored the PSTN Service Provider market (e.g., MFS, EO, SMEO, PBX). With the change in direction toward IP-based telephony solutions, DISA reorganized their requirements and renamed the telephony switch groups to better align their functional capabilities. An example is the PBX, EO and SMEO individual classes and requirements, which are now identified under the UCR, simply as LSC requirements. DISA also elected to retain a PBX requirement where full LSC functionality and capability is not warranted. So, an LSC can be thought of as an IP-based EO or SMEO or PBX. Previously, IP-based voice solutions could connect to the DSN only through an EO or a SMEO using TDM trunks. In contrast, an LSC connects directly to the MFSS or WAN-SS through IP-based AS-SIP trunks. The need for TDM connectivity to the DSN through an EO or SMEO is no longer required.

Understanding Assured Services

The definition of assured services is constantly evolving. DISA has been refining the definition as it responds to both changing end-user requirements and changes in commercially available products, services, and architectures. For the purposes of voice communications, "assured services" refers primarily to the ability to guarantee service for C2 users. In times of critical need, certain users must be guaranteed that their calls will arrive at the desired destination. This assurance is accomplished two ways: in the underlying IP network and in the VoIP equipment and technologies on top of that infrastructure.

Assured Services Networking

DISA has designed the network architecture to help ensure end-to-end quality-of-service (QoS) delivery. The UCR outlines an extremely detailed QoS differentiated services code point (DSCP) marking policy for all the applications and services that will be using the shared IP medium. The UCR also includes strict performance, end-to-end delay, latency, security, and other requirements that were created to meet the needs of mission-critical applications. The main components of the assured services network topology are briefly explained in the next section.

Assured Services SIP

To help ensure the end-to-end delivery of critical telephone calls, DISA created Assured Services SIP. AS-SIP extends basic SIP by adding the following:

- Multilevel priority and preemption (MLPP) based on RFCs 4411, 4412, and 5478
- DSCP marking of media traffic based on MLPP priority levels
- Signaling encryption using Transport Layer Security (TLS)
- Media encryption using Secure Real-Time Transport Protocol (SRTP)
- Detailed call admission control (CAC)

Note that these AS-SIP requirements relate primarily to audio calls. Video calls may be subject to fewer, or more, requirements. Additionally, some of these requirements may be waived for audio calls depending on the specific mission requirements. For example, products used by tactical users, who operate in highly dynamic deployments, may be exempt from some of these requirements. However, in general, a device that is said to be AS-SIP compliant will provide the capabilities listed here.

Detailed Architectural Overview

The DISA architecture introduces several new certification categories. Each major element of the architecture is individually certifiable. As a result, a fully functional deployment can be achieved using equipment from multiple vendors, if desired. Figure 3 shows the major components. Note this is a logical depiction of the topology. Each major component may consist of multiple, redundant components that provide a guaranteed uptime level with high availability known in the industry as the "five 9s" or 99.999 percent availability as required by the UCR.

Figure 3. Major Components of the DISA Architecture
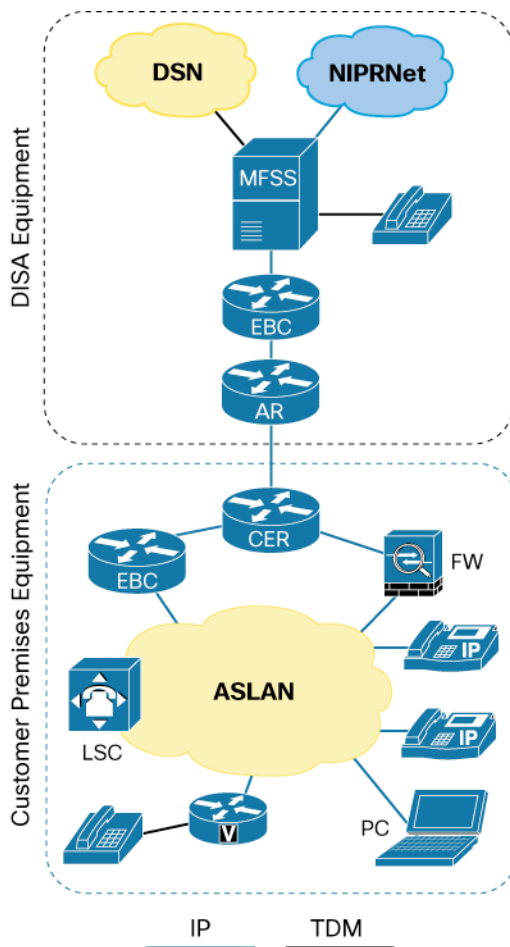
- Aggregation router (AR): The aggregation router is located at the core. It is the IP aggregation point of multiple military departments.
- Assured Services LAN: The AS-LAN provides the local network infrastructure over which assured services applications are delivered. The primary components of this certification category are Ethernet switches. Routers can also be certified within this category.
- Customer-edge router (CER): The CER is located on the edge of the AS-LAN and the NIPRNet. The CER serves as the connection point between the AS-LAN and the WAN.

- Firewall (FW): The firewall is located between the CER and the AS-LAN. Its purpose is the same as any other data firewall: to protect the AS-LAN from external threats. All data traffic should flow through the firewall on its way to the CER and the NIPRNet .
- Edge boundary controller (EBC): The EBC is located between the CER and the AS-LAN. Its primary function is to perform voice and video firewall stateful inspection requirements. An EBC must be in front of every LSC. All calls that enter or leave an LSC must pass through the EBC. An EBC also is located in front of every MFSS or WAN-SS in the core. Two interfaces connect the EBC to the network: on the inside interface, the EBC connects to the AS-LAN; on the outside interface, the EBC connects to the CER. The EBC should not be connected behind the data firewall and Cisco's preferred preference is to place it on the DMZ of its Firewall products.

Understanding the Cisco Local Session Controller Solution

Cisco provides a fully certified LSC. The makeup of a Cisco LSC is not significantly different from that of a certified Cisco PBX1 solution. A Cisco Unified Communications Manager cluster is still the main component. An LSC differs from a PBX1 with the addition of the Cisco Integrated Services Router (ISR) platform running Cisco Unified Border Element (CUBE). This CUBE instance, with regards to functionally within the scope of a LSC, is known as an InterWorking Gateway (IWG).

InterWorking Gateway

The IWG is a mandatory component of the Cisco LSC architecture. Typically, an IWG is deployed as a pair of Cisco ISRs running in a redundant configuration. It provides a single, Hot Standby Router Protocol (HSRP)– controlled, virtual IP address that is reachable both from the servers of the Cisco Unified Communications Manager cluster and from the inside interface of the local EBC.

DISA's requirements dictate that an LSC must be reachable through a single IP address. A traditional Cisco Unified Communications Manager cluster is composed of several servers, each with a unique IP address. These servers cannot be assigned a shared IP address. An IWG solves this requirement and is used to provide this capability. Figure 4 shows the logical call flow.

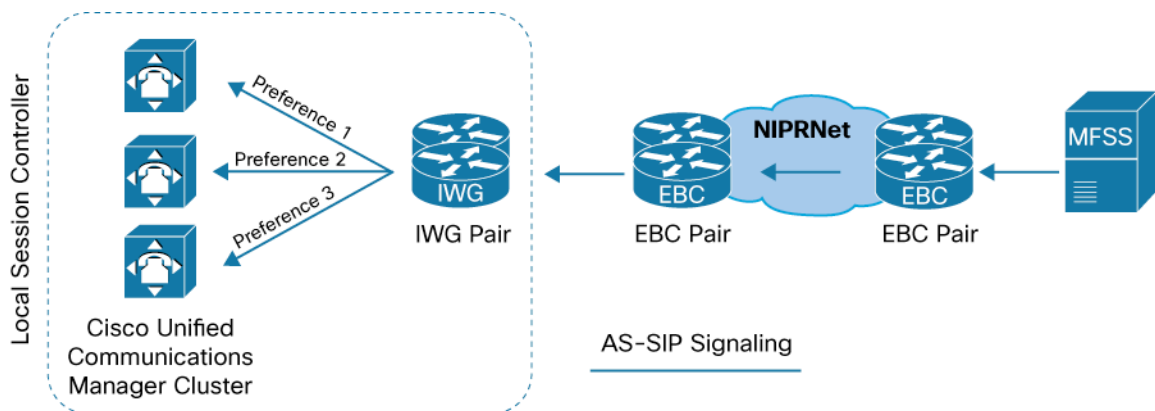**Figure 4.**　LSC Logical Call Flow

Figure 4 shows a single logical LSC, composed of a Cisco Unified Communications Manager cluster and a pair of redundant IWGs. Incoming calls from NIPRNet enter through the EBC pair. That EBC sends AS-SIP signaling to

the shared HSRP IP address of the IWG. The IWG processes the call and directs it to one of the Cisco Unified Communications Manager servers with which it is configured to interact.

Combined Operation

When deploying both a Cisco LSC and a Cisco EBC, the functions of the IWG and EBC can be combined into a single device. A combined IWG-EBC uses two interfaces. The inside interface connects to the Cisco Unified Communications Manager cluster, and the outside interface connects to the EBC in front of the MFSS or WAN-SS. Figure 5 shows an example.

Figure 5.   Combined IWG-EBC
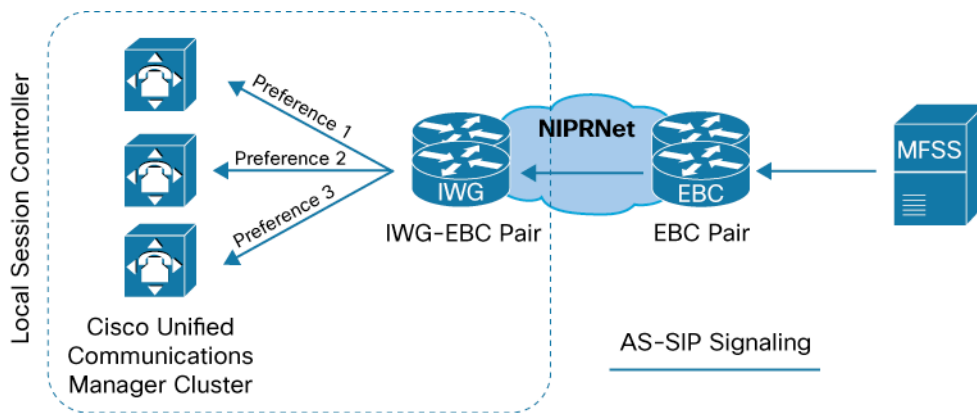
As shown in Figure 5, a combined deployment simplifies the overall the topology while providing the same functions.

Security Architecture

An LSC also differs slightly from a PBX1 installation in its security architecture. Nearly all traffic that crosses the network infrastructure is encrypted, including all call signaling, media traffic, and intracluster communications. Figure 6 shows the types of encryption used.

Figure 6.   Types of Encryption Used in LSC Security Architecture
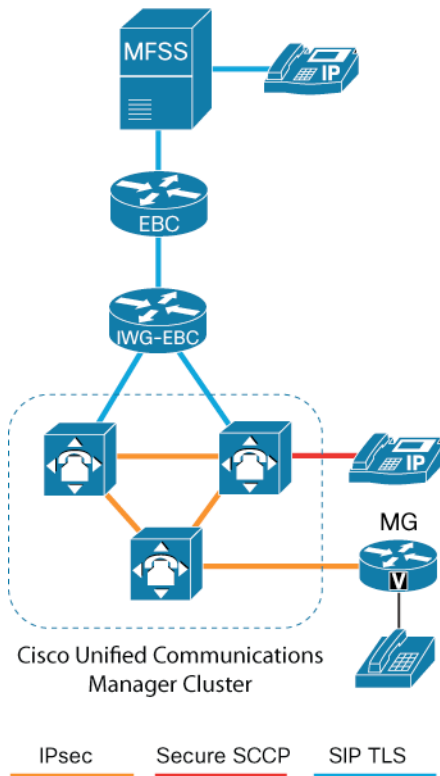
- SIP TLS: The AS-SIP signaling between the MFSS, EBC, IWG-EBC, and AS-SIP–capable IP phones is secured using TLS. Every AS-SIP TLS connection must use DISA-issued X.509 certificates. TLS encrypts the entire signaling contents. No SIP content is visible on the network.

- IP Security (IPsec): IPsec tunnels are used to secure IP connectivity between the Cisco Unified Communications Manager nodes that make up the LSC cluster. Each node is configured with IPsec tunnels to the other nodes in the cluster. Additionally, connectivity between Cisco media gateways (MG) and the LSC cluster is also secured through IPsec tunnels.

- Secure SCCP: The SCCP signaling between the Cisco IP phones and the nodes of the LSC cluster is secured through secure Skinny Client Control Protocol (SCCP). Secure SCCP uses TLS for encryption. As with SIP TLS, the contents of TLS-encrypted SCCP messages are not visible on the network. For ease of deployment and management, the Cisco Unified Communications Manager server itself, not DISA, generates the X.509 certificates used by the IP phones. Cisco Unified Communications Manager issues each phone a unique certificate, and this certificate is pushed to the phone as part of the phone provisioning process.

- SRTP (not shown): All VoIP bearer traffic is secured using SRTP with an Advanced Encryption Standard (AES) 128 cipher. With SRTP, the SRTP header is visible on the network; however, the actual SRTP payload is encrypted. The SRTP headers must remain unencrypted for synchronization purposes.

Signaling and Media Flow

Figure 7 shows the types of signaling used, and the locations, on a point-to-point call made between two Cisco LSC systems.

Figure 7.　　Signaling and Media Flow Between Cisco LCS Systems
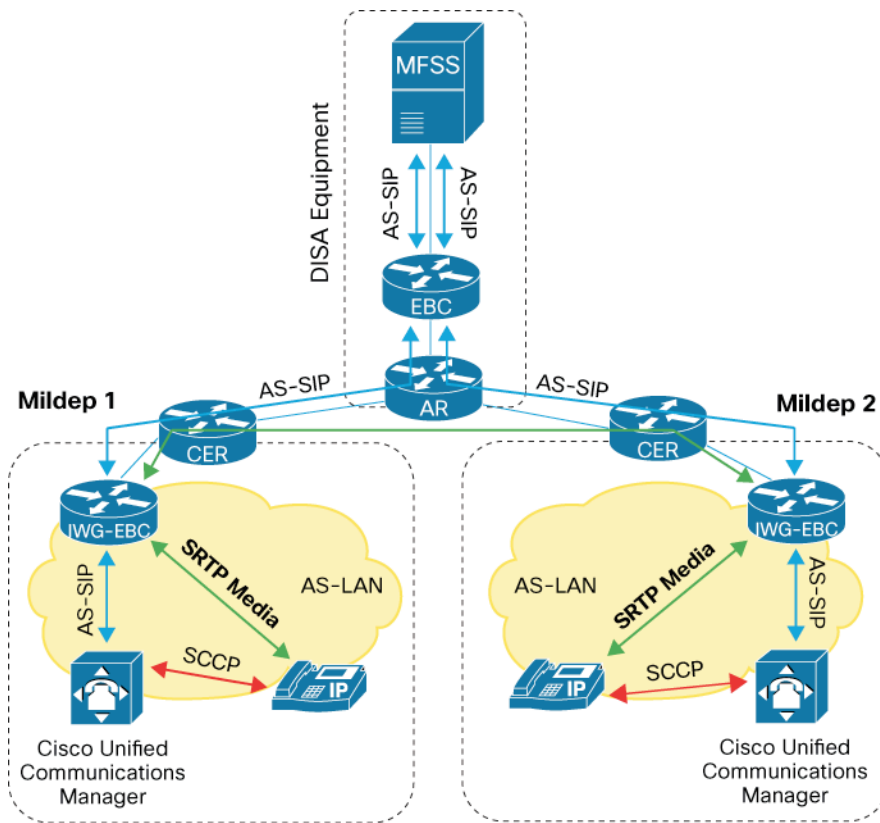
- Cisco's secure SCCP signaling occurs between Cisco IP Phones and the LSC. The phones can be within the same AS-LAN or located elsewhere in a distributed environment.
- AS-SIP signaling, also within the AS-LAN, occurs between the LSC and the inside interface of the IWG-EBC pair.
- AS-SIP signaling across NIPRNet occurs between the outside interface of the IWG-EBC pair and the outside interface of the EBC pair in front of the MFSS in the core.
- AS-SIP, within the core, exists between the inside interface of the EBC and the MFSS.
- SRTP encrypted media flows directly between military departments through NIPRNet. Each IP phone sends its media to the inside interface of the IWG-EBC pair, and the IWG-EBC at each military department forwards those media packets to the IWG-EBC pair at the destination military department. All media traffic traverses the CER for proper QoS at each military department.

Migration Options from Public Branch eXchanges 1 & 2 to a Local Session Controller

DISA fully supports PBX1 to LSC, SMEO to LSC, and EO to LSC interconnection through TDM trunks. This support is extremely useful for MILDEPs that have existing TDM-based solutions installed and operational. A PBX1, PBX2, EO, or SMEO deployment can coexist with an LSC during the migration period. Figure 8 shows this topology.

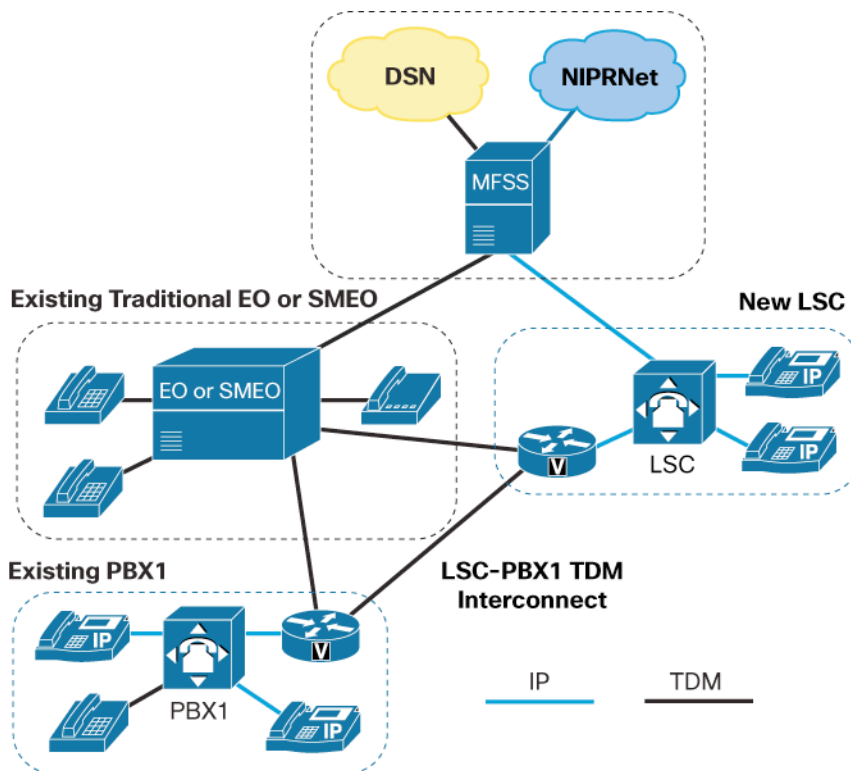**Figure 8.**   EO or SMEO and PBX1 Topology and LSC Migration

Figure 8 shows an existing EO, SMEO or PBX1 topology. A new LSC installation is brought online and connected to the MFSS through AS-SIP IP trunking. Additionally, a TDM connection, through the media gateway at both the LSC and the PBX1, is brought online, enabling connectivity between the LSC and PBX1. After this connection is made the LSC can provide all the functions of the existing EO switch. End users can be gradually transitioned from PBX1 to the LSC with little effect on operations. The LSC can also be interconnected to the EO or SMEO if the military department desires such a connection. The interconnect technique used is the same; TDM trunks are connected to a media gateway on both the EO or SMEO and the LSC.

Conclusion

The communications architecture for future DoD customers creates a converged voice, video, and data IP network. The transition and direction towards this architecture scales beyond the simple TDM voice replacement requirements, to include video, messaging, web collaboration, and much more. These expanded capabilities will continue to evolve the effectiveness of the warfighter and business communities within the DoD.

The Local Session Controller is the foundation of this transition. By providing all the necessary building blocks, Cisco's LSC can be leveraged for the deployment of additional IP applications and services, capitalizing on its position as the gateway to the converged network. As the leader in DISA APL-certified products for unified communications, Cisco gives its Federal customers Commercial Off-The-Shelf (COTS) products that are enterprise-proven with comprehensive features that meet the rigorous certification requirements set by the DoD.

For More Information

For more information about Cisco Unified Communications solutions, global government solutions, and services for defense, space, and homeland security, visit http://www.cisco.com/go/government or contact your local Cisco representative.

You can also consult the following resources:

- DISA Unified Capability Requirements: http://www.disa.mil/ucco/ucr.html
- Cisco Unified Communications System solution reference network design guides: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_uc_mgr.html
- Cisco Global Government Certifications: http://www.cisco.com/web/strategy/government/sec_cert.html