Enterprise Mobility Capabilities Strategy

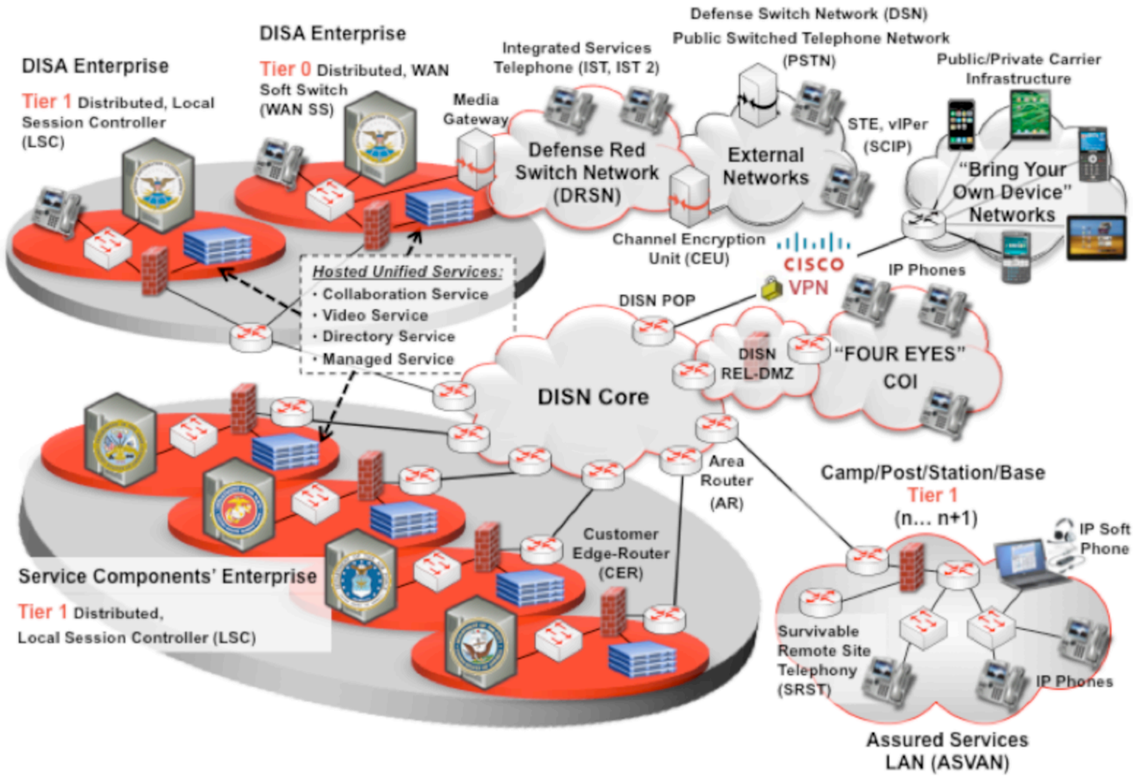
Introduction

The U.S. government, most notably the Department of Defense (DoD), is moving toward a comprehensive enterprise-level mobility solution where participating industry (commercial) smartphones and tablets can reach and access the classified government infrastructures through controlled and layered security mechanisms.

Background

On February 27, 2012, the National Security Agency (NSA) published its Mobility Capability Package (MCP) 2012, Version 1.1 document that defines the first phase of the Enterprise Mobility Architecture. The intent of this initial document is to be a living reference that focuses on the architectural components of providing a Secure Voice over Internet Protocol (SVoIP) capability using commercial-grade products. As technology and policies change over time, based on lessons learned, this reference document can be modified to accommodate these advancements. Figure 1 illustrates the current global DoD secure communications enterprise solution whereby Future Mission Networks (FMN) that use mobile devices attached through public or private infrastructures can reach the classified government infrastructure. Typically referred to as “Bring Your Own Device” (BYOD), these endpoints can be securely attached to the existing communications network of networks by following the reference MCP guidance.

Figure 1. Global DoD Classified Voice Video over IP Architecture

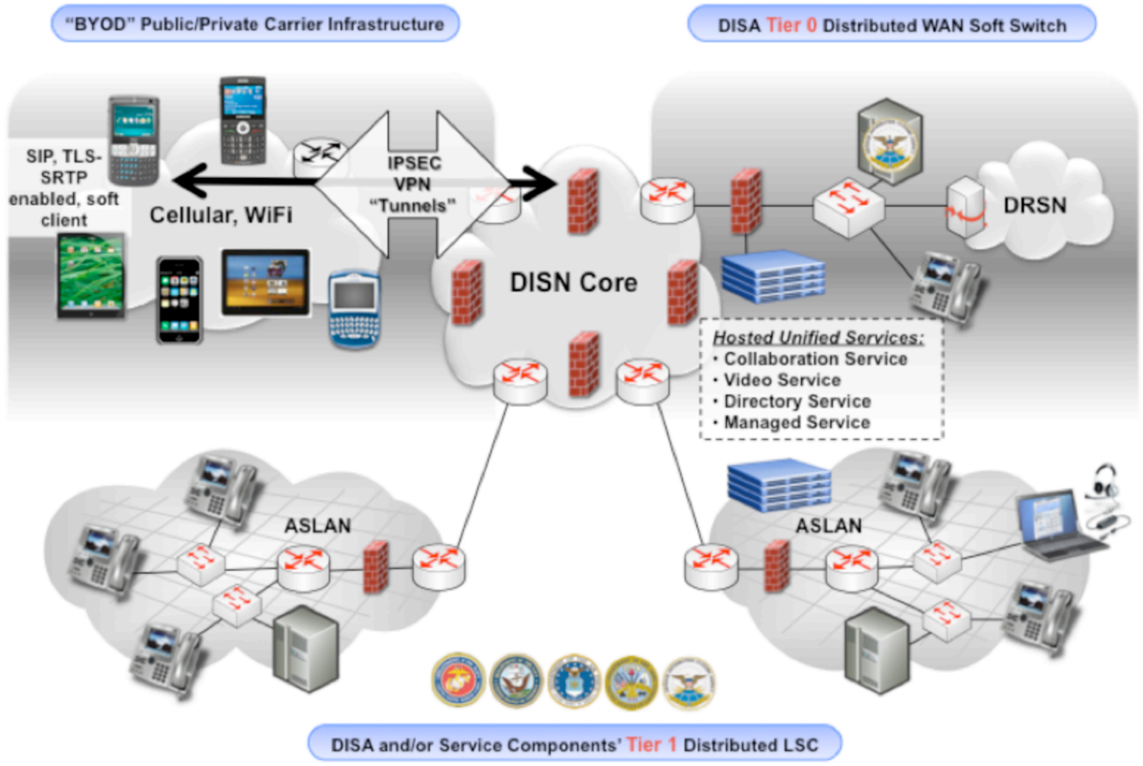

DISA Enterprise
Tier 1 Distributed, Local Session Controller (LSC)
DISA Enterprise
Tier 0 Distributed, WAN Soft Switch (WAN SS)
Media Gateway
Integrated Services Telephone (IST, IST 2)
Defense Switch Network (DSN)
Public Switched Telephone Network (PSTN)
Public/Private Carrier Infrastructure
Defense Red Switch Network (DRSN)
External Networks
STE, vIPer (SCIP)
“Bring Your Own Device” Networks
Channel Encryption Unit (CEU)
CISCO VPN
IP Phones
Hosted Unified Services:
• Collaboration Service
• Video Service
• Directory Service
• Managed Service
DISN POP
DISN REL-DMZ
“FOUR EYES” COI
DISN Core
Area Router (AR)
Camp/Post/Station/Base
Tier 1
(n... n+1)
IP Soft Phone
Customer Edge-Router (CER)
Service Components’ Enterprise
Tier 1 Distributed, Local Session Controller (LSC)
Survivable Remote Site Telephony (SRST)
IP Phones
Assured Services LAN (ASVAN)

The above special command and control Classified Voice Video over Internet Protocol (CVVoIP) architecture (commonly known as the Voice over Secure Internet Protocol [(VoSIP]) network) shown in Figure 1, has multiple network-based secure connections by both Time-Division Multiplexing (TDM) and Internet Protocol (IP) mechanisms to other secure voice communications architectures. Aggregated, the complete CVVoIP solution spans access for end-to-end communications across various Communities of Interest (COI) networks throughout the world.

“Bring Your Own Device” Strategy

Within the MCP framework, network-based encryption for BYOD is not used, and there are two key important fundamentals germane to all vendors who want to participate with a solution. The first is that the MCP reference on pages 19 and 20 for the Threshold and Objective requirements specifies that two layers of encryption will be used, and by which the BYOD applications, the Virtual Private Network (VPN) client and the Session Initiation Protocol (SIP) soft client shall be from different vendors. Further defined is that the VPN client must be of IP Security (IPsec) Advanced Encryption Standard (AES) quality (for example, Suite B), with the SIP soft client protocol using Transport Layer Security (TLS) over Secure Real-Time Protocol (SRTP). This specific requirement and reference means that vendors are limited and cannot provide a complete solution for both “access” through Virtual Private Network (VPN) tunnels and “voice” communications by Session Initiation Protocol soft clients. Cisco and other vendors will have to determine which layer of technology solution they want to provide, because the requirements within the current MCP version are restrictive.

Figure 2. Defense Information Systems Network Regional View


“BYOD” Public/Private Carrier Infrastructure
DISA Tier 0 Distributed WAN Soft Switch
SIP, TLS-SRTP enabled, soft client
Cellular, WiFi
IPSEC VPN “Tunnels”
DISN Core
DRSN
Hosted Unified Services:
• Collaboration Service
• Video Service
• Directory Service
• Managed Service
ASLAN
ASLAN
DISA and/or Service Components’ Tier 1 Distributed LSC

The second critical delimiter is that all secure voice calls can be completed only if both the called and calling parties are both VPN-connected to the government-controlled infrastructure. This requirement means that all end-to-end calls (both signaling and media flow) involving a BYOD must transit through the government architecture even though the calls are between two BYOD endpoints.

Lastly, there are other specific references to features and designs for access, authentication, monitoring, and infrastructure control requirements that vendors must build to in order to qualify and participate. However, they are secondary to the strategy decision on how Cisco will participate in this section of the FMN solution.

Solution

The concept of Cisco participation lies in a solution strategy that focuses on our core strengths. The Cisco® go-to-market strategy takes advantage of the strengths of our partners in conjunction with the breadth of our portfolio. Using these partnerships to full advantage will be a critical component to moving our strategy forward.

It is recommended that Cisco initially focus on the smartphone and tablet markets, based on the feedback and direction of our customers. Other mobile devices, such as laptops, should not be ignored, but are not the immediate focus of this strategy. Focusing on taking advantage of our core competencies (retaining the government IP telephony core or tier 0) with the smartphone and tablet market will allow us to establish focused partnerships and position win-win solutions for our government customers.

Smartphone Market

In this market, the smartphone strategy addresses two options our partners can position and our customers can adopt now based on their internal objectives. The third option is outside the scope of the current MCP requirements. This option requires further socialization and discussion with NSA officials so the MCP v1.1 release can be modified to allow direction of this strategy.

- Option 1—VPN client: The first option is rooted in the current direction to continue the build-out of the Cisco AnyConnect® (for example, Suite B) VPN product, without a SIP soft client (for example, the Cisco Jabber™ messaging integration platform). This option does not require any modifications to the Jabber® client; however, Cisco will have to review, identify capability gaps, and develop to the specific feature requirement deficiencies identified within the MCP.
- Option 2—SIP client: The second option is for partners and vendors who require a SIP soft client but prefer to use a third-party open-sourced VPN strategy other than Cisco's. With this strategy, Cisco needs to address development in the product (for example, the Jabber application) to remove the deficiencies identified within the MCP requirements document.
- Option 3—VPN and SIP client from one vendor: Further justification and "marketing" is required to adjust to this strategy, which is outside the present requirements outlined in the NSA document. The NSA MCP v1.1 requirements document is attached as an addendum to this executive paper so executives and business units can review as required in order to make informed business decisions regarding the development and execution of any or all of these strategies.

Tablet Market

This market for the customers is a little more involved, but if it is executed correctly, this strategy can specifically meet the MCP fundamental requirement for two layers of encryption with vendor separation for the VPN and SIP client support. Keep in mind that there can be permutations to the primary strategy, but if we develop our "clients"

(AnyConnect™ and Jabber clients) to the MCP requirements, those permutations will be available to cover any “one offs” not met by this strategy.

The proposed solution follows: VPN Client with Citrix and VMware Thin Client Support

The tablet strategy would take advantage of capabilities provided by Cisco, Citrix, and VMware to provide a complete partner-based solution that will meet the intent of the MCP requirement for two layers of encryption, each provided by a different vendor.

The Cisco AnyConnect VPN client product would provide the first layer of encryption. Citrix or VMware encryption for their tablet-supported Thin Client product would provide the second layer of encryption. With Citrix and VMware Thin Client support, a different vendor is providing the second layer of encryption, thus satisfying the MCP requirement. The added bonus to our customers using this solution approach is they can provision the Cisco SIP soft client (for example, the Jabber client) within their Virtual Desktop Image (VDI), where the Thin Client provisions from the government enterprise infrastructure. With this strategy, our customers’ mobility solution meets the fundamental requirements identified to support the FMN, anytime, anywhere.

Conclusion

The measures (Threshold and Objectives) used to meet the NSA MCP reference guidance for secure access and voice communications can be met with minimum disruption to the core strategies of Cisco and our partner delivery model. Careful project management along with tight business development strategies worked concurrently with both Cisco and our partners can be tailored so we can achieve and meet our customers’ expectations. This portion of the Future Mission Network objectives that use BYOD can be satisfied, thus bringing Cisco and our partners in line with the published Mobility Capability Package 2012 reference specifications.

Table 1. Summary of Market Strategies

	Smartphone Option 1	Smartphone Option 2	Tablet Proposed Solution
Layer 1 encryption	Cisco AnyConnect VPN Client	Partner VPN Client	Cisco AnyConnect Client
Layer 2 encryption	Partner SIP Client	Jabber Client	Citrix-VMware Thin Client VDI with Jabber Client

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-704013-00 03/12