Next Generation Enterprise Branch Security CVD System Assurance Guide

Cisco Validated Design

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

The Cisco Validated Design Program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit www.cisco.com/go/validateddesigns.

Next Generation Enterprise Branch Security Design: Cisco Validated Design II

Preface

The aim of this document is to accelerate customer deployments of the Next Generation Enterprise Branch Security Design.

It presents results and recommendations for all the deployment architectures outlined in the *Next Generation Enterprise Branch Security Design Guide*.

Table 1 Modification History

Date	Comment
Feb, 2008	Initial Release

Definitions

This section defines words, acronyms, and actions which may not be readily understood.

Table 2 Definitions

Term	Definition
CVD	Cisco Validated Design
VPN	Virtual Private Network: A secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone.
MPLS	Multi-protocol Label Switching
WAN	Wide Area Network
SPA	Shared Port Adapters
SIP	SPA Interface Processor
NHRP	Next Hop Resolution Protocol
LDP	Label Distribution Protocol
802.11	The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) Wireless LANs operating in the 2.4-GHz band.

Table 2 Definitions

Term	Definition
802.11b	The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps Wireless LANs operating in the 2.4-GHz frequency band.
802.11g	The IEEE standard that specifies carrier sense media access control and physical layer specifications for Wireless LANs operating in the 2.4-GHz frequency band.
802.11af	The IEEE standard that specifies a mechanism for Power over Ethernet (PoE).
802.1q	IEEE 802.1Q was a project in the IEEE 802 standards process to develop a mechanism to allow multiple bridged networks to transparently share the same physical network link without leakage of information between networks (i.e. Trunking).
AP	Access Point
DMVPN	Dynamic Multipoint VPN
EAP	Extensible Authentication Protocol
MDRR	Modified Deficit Round Robin
mGRE	multipoint GRE
OIB	Operationally Impacting Bug
PEAP	Protected Extensible Authentication Protocol
Roaming	A feature of some access points that allows users to move through a facility while maintaining an unbroken connection to the LAN
SSID	Service Set Identifier (also referred to as Radio Network Name)
WDS	Wireless Domain Services
WEP	Wired Equivalent Privacy
WLSE	Wireless LAN Solutions Engine
WPA	Wi-Fi Protected Access
VoIP	Voice over IP
IPS	Intrusion Prevention System
CISF	Catalyst Integrated Security Features
SCCP	Skinny Call Control Protocol
SIP	Session Intiations Protocol
MQC	Modular QoS CLI

CONTENTS

FIGURES

This page is intentionally left blank

TABLES

CHAPTER 1

Executive Summary

Thix document describes the CVD System Assurance of the *Next Generation Enterprise Branch Security Design Guide*.

The Cisco® Validated Design Program (CVD) consists of systems and solutions that are designed, tested, and documented to facilitate faster, more reliable and more predictable customer deployments. These designs incorporate a wide range of technologies and products into a broad portfolio of solutions that meet the needs of our customers. For more information on the Cisco CVD program please refer to:

http://cisco.com/en/US/partner/netsol/ns741/networking_solutions_program_home.html

This test activity supports the goals of the Cisco Validated Design program by extending coverage of CVDs, combining CVDs and exploring interactions between them, as well as developing sustaining to extend the lifecycle of Network Systems in a customer representative environment. The extended coverage of designs, combined with the sustaining capability result in recommended releases that ensure improved quality and a successful customer deployment experience.

The test program was executed by following a formal test process that ensures consistency of operation, quality of results and value for our customers.

The following are key aspects of the test process:

- All collateral is reviewed and updated for general deployment
- Solution requirements are tested and results are documented according to a formal process that includes a cross-functional team of stakeholders.
- High quality standards are met (Zero observable operationally impacting defects within the given test parameters, that is, no defects that have not been resolved either outright or through software change, redesign, or workaround (refer to reference test plan for specific details)
- A detailed record of the testing conducted is generally available to customers and field teams, which provides:
  - Design baseline that provides a foundational list of test coverage to accelerate a customer deployment
  - Software baseline recommendations that are supported by successful testing completion and product roadmap alignment
- Detailed record of the associated test activity that includes configurations, traffic profiles, memory and CPU profiling, and expected results as compared to actual testing results. Design recommendations and test results undergo detailed review by Subject Matter Experts (SMEs) within each technology area.

The *Next Generation Enterprise Branch Security Design Guide* offers guidelines and best practices for the Enterprise Branch Network and lays the foundation for integration of advanced services into the Enterprise Branch Architecture. Three baseline branch architectural profiles; Single-Tier, Dual-Tier, and

Multi-Tier branches are described to address various customer requirements: balancing cost, security, availability, and manageability. The core components for all three branch profiles are WAN, LAN, High Availability (HA), Routing, Quality of Services (QoS), and Security.

The assurance test activity, tested the core components in a large scale, multi-platform, multi-release, system test environment in Single-Tier, Duel-Tier, and Multi-Tier profiles. In addition, CVD System Assurance efforts included Multicast, Wireless, Voice over IP (VoIP) and DMVPN scalability

The primary focus of the *Next Generation Enterprise Branch Security Design Guide* (CVD) is WAN, LAN, Network Fundamentals and security services of the Branch network. In addition, CVD System Assurance efforts included Multicast, Wireless, Voice over IP (VoIP) and DMVPN scalability. As an integral part of the CVD System Assurance program, an automated sustaining validation model was created for on-going validation of deployment architectures for future Internetworking Operating System (IOS) releases. With this automated sustaining validation capability, the sustaining team can validate the design in any upcoming software releases on the targeted platforms. Sustaining validation greatly extends the useful life of the design guide, and significantly increases customer confidence and reduces deployment time.

During testing, there were a number of software defects encountered, The symptoms, conditions and workarounds of each defect are described.

Table 1-1, outlines the summary of certification and validation status of the Next Generation Enterprise Branch Security Design.

Table 1-1 Certification and Validation Summary

Design	Status
Next Generation Enterprise Branch Security Design	Pass

CHAPTER 2

CVD System Assurance Test Coverage

CVD System Assurance test coverage was derived from the *Next Generation Enterprise Branch Security Design Guide*. However, to test the customer representative network, additional services were introduced.

The Next Generation Enterprise Branch Security Design consists of three distinctive profiles: Single-Tier, Dual-Tier, and Multi-Tier. In each profile, the following Cisco ISR routers are recommended: 2800 and 3800. High availability, infrastructure protection, secure WAN connectivity, and threat defense are addressed in each of these profiles.

Although the entire contents of the *Next Generation Enterprise Branch Security Design Guide* are not in the scope of this document, a summary of the design is included in the following sections.

2.1 Core Architecture

This section describes the following Branch Architectures:

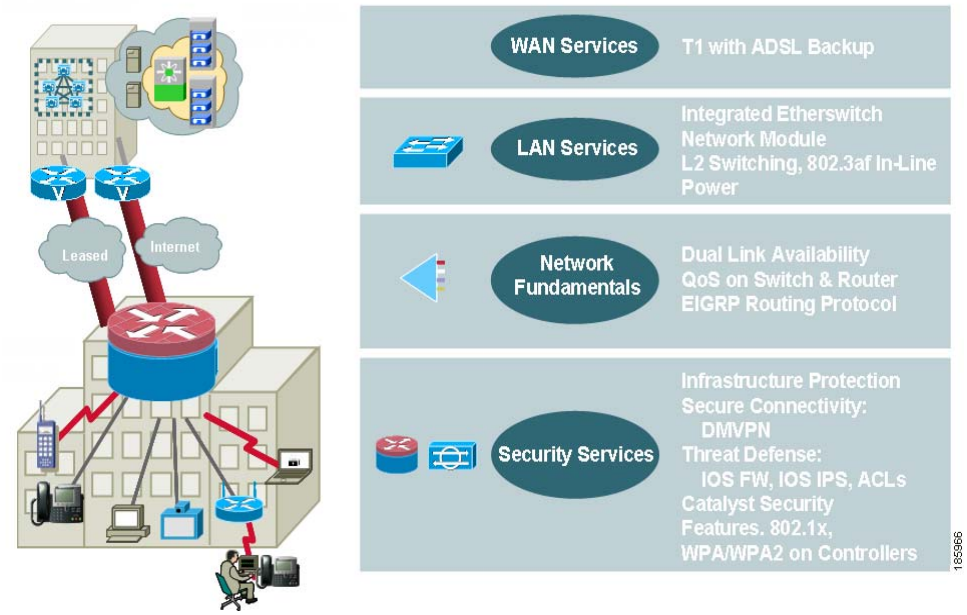
- Single-Tier Branch
- Dual-Tier Branch
- Multi-Tier Branch

2.1.1 Single-Tier Branch

The Single-Tier Branch profile mimics a small branch office with less than 50 users. It consists of an Integrated Services Router (ISR) as the access router with an Integrated EtherSwitch network module for LAN, WAN connectivity and security services. High Availability is achieved using redundant WAN links.

Figure 2-1 illustrates a Single-Tier Branch profile with associated services, and relative positioning of various devices, and services.

Figure 2-1 Single-Tier Branch Profile with Associated Services



Based on the Single-Tier profile that was described in the design guide, the following platforms were tested for CVD System Assurance: 3845, 3825, 2821 and 2811.

Additionally the following platforms were tested to expand the platform coverage: 3745,1801 and 877.

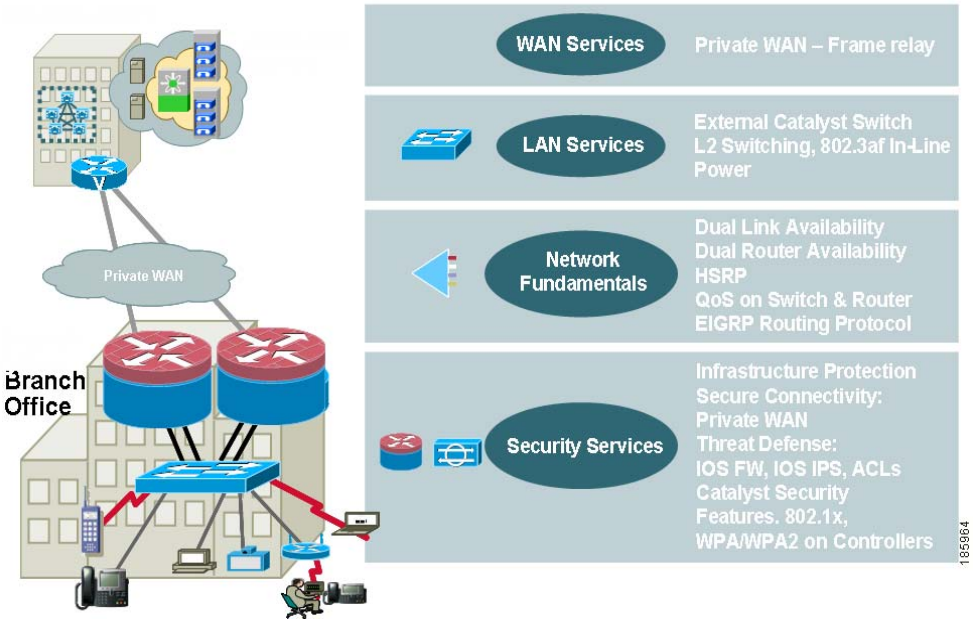
2.1.2 Dual-Tier Branch

The Dual-Tier Branch profile represents a medium-size branch office of 50-100 users. It has dual routers connected to a Catalyst 3750 switch and dual WAN links which provide high availability. The Dual-Tier Branch profile separates network functionality into separate device layers. The tiers in this profile are WAN termination, security services (firewall, IPS) services termination using ISR routers and LAN functionality and security services (CISF) achieved using desktop switches

The access routers use integrated Gigabit Ethernet ports to connect to the Catalyst 3750 and the WIC slots for WAN connectivity.

Figure 2-2 illustrates a Dual-Tier Branch profile with associated services.

Figure 2-2 Dual-Tier Branch Profile with Associated Services



Based on the Dual-Tier Branch profile that was described in the design guide, the following platforms were tested for CVD System Assurance:Cat 3750, Cat 3560, 2851, and 2801.

Additionally the following platforms were tested to expand platform coverage: 7206 VXR

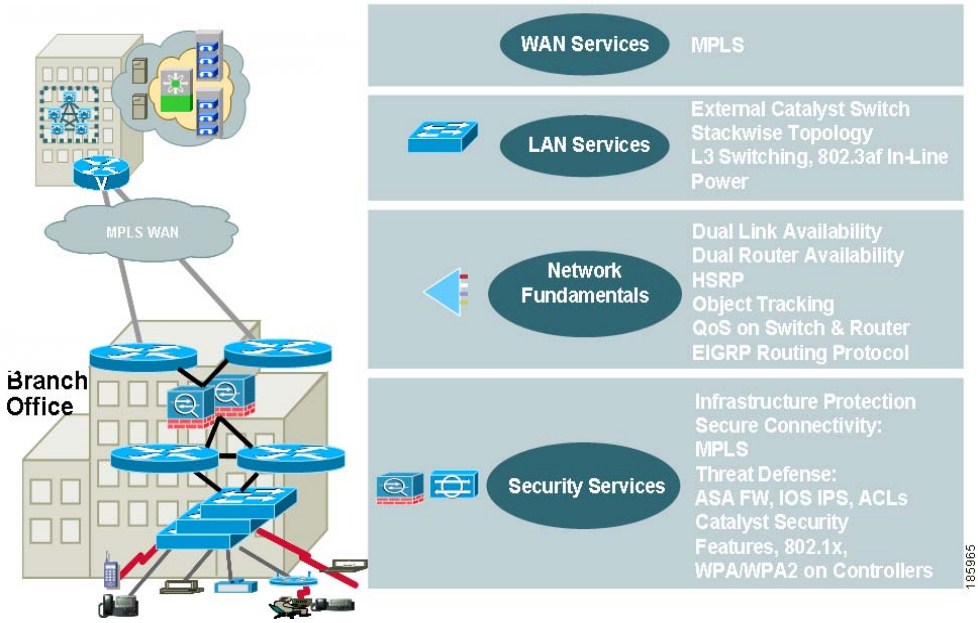
2.1.3 Multi-Tier Branch

The Multi-Tier Branch profile represents a large branch office of 100-200 users. The Multi-Tier Branch profile separates network functionality into separate device layers. The tiers in this profile are WAN termination, firewall functionality, services termination, and LAN functionality.

This profile consists of dual routers for WAN termination, dual ASA appliances for security, dual routers for service integration, and stackable switches to provide the maximum level of redundancy and high availability in the network.

Figure 2-3 illustrates a Multi-Tier Branch profile with associated services.

Figure 2-3 *Multi-Tier Branch Profile with associated services*



Based on the Multi-Tier Branch profile that was described in the design guide, the following platforms were tested for CVD System Assurance: 3845, 3825, 2851, ASA 5510 and Cat 3750G

2.2 Services

The *Next Generation Enterprise Branch Security Design Guide* breaks down the coverage into the following service layers:

- WAN Services
- LAN Services
- Network Fundamentals
- Security Services

2.2.1 WAN Services

The *Next Generation Enterprise Branch Security Design Guide* recommends T1 and DSL connectivity for Single-Tier branch connecting through the Internet, ATM/FR leased line private WAN for the Dual-Tier branch and MPLS for the Multi-Tier branch profile. CVD System Assurance testing followed these recommendations closely, with a few exceptions for fixed configuration routers which do not support T1 connectivity. 877 and 1801 are two examples of Fixed Configuration routers.

2.2.2 LAN Services

LAN services provide end device connectivity to a corporate network within a branch office. With the convergence of services in a single network infrastructure, devices such as computers, telephones, video cameras and many other devices must be connected to the corporate network over the LAN.

Following were the list of desktop switches validated as described in the *Next Generation Enterprise Branch Security Design Guide*:

- Single-Tier: Integrated switches on fixed configuration routers and NME switch modules on ISR 2800 and 3800 routers
- Dual-Tier: Cat 3750 and 3560
- Multi-Tier: Cat 3750G

2.2.3 Network Fundamentals

In the *Next Generation Enterprise Branch Security Design Guide*, Network Fundamentals refer to the basic services that are required for network connectivity. These services include High Availability (HA), IP Addressing, IP Routing, and Quality of Services (QoS). Regardless of WAN or LAN deployment model chosen for the branch architecture, Network Fundamentals are required to provide a foundation for any service to be overlaid onto the branch network.

HA was tested on the three Branch profiles using 7206VXR, 3845, 3825, 3745, 2851, 2821, 2811,and 2801.

Dual-Tier profile uses HSRP for redundancy on the LAN side. HSRP and Object Tracking are used in the Multi-Tier Profiles.

For IP routing, the focus of CVD System Assurance efforts was EIGRP and for QoS testing the focus was on classification, congestion management, congestion avoidance, traffic shaping, policing and the scavenger class, with one exception for MDRR, due to hardware constraints.

2.2.4 Security Services

Security services protect the device and network from intrusion, tampering, manipulation (data integrity), secure data transport, and Denial of Service (DoS).

CVD System Assurance testing achieved infrastructure protection according to *Next Generation Enterprise Branch Security Design Guide's* recommendations.

For secure connectivity, ATM/FR and MPLS L3 VPN were used to achieve traffic separation. For additional security, DMVPN was used for data encryption. For secure WAN transport, DMVPN Phase 3 was tested and found to be an improved solution over the recommendations in the *Next Generation Enterprise Branch Security Design Guide*.

Threat defense detection and mitigation were achieved with software based Intrusion Prevention System (IPS) features on ISR routers. For Stateful firewall features, Context Based Access Control (CBAC) was configured on the routers for Single-Tier and Dual-Tier Branch profiles. ASA security appliances were used in the Multi-Tier Branch profile. For additional LAN Security, Catalyst Integrated Security Features (CISF) such as Port Security, DHCP Snooping, Dynamic ARP Inspection and IP Source Guard were tested on Cisco Catalyst switches and switch modules on ISR routers.

2.3 Additional Services

To achieve a feature rich, customer representative network, additional features were tested in the network. Following are the list of features that were also tested, which are not discussed in the *Next Generation Enterprise Branch Security Design Guide* (CVD):

- Multicast
- Wireless
- Voice over IP

2.3.1 Multicast

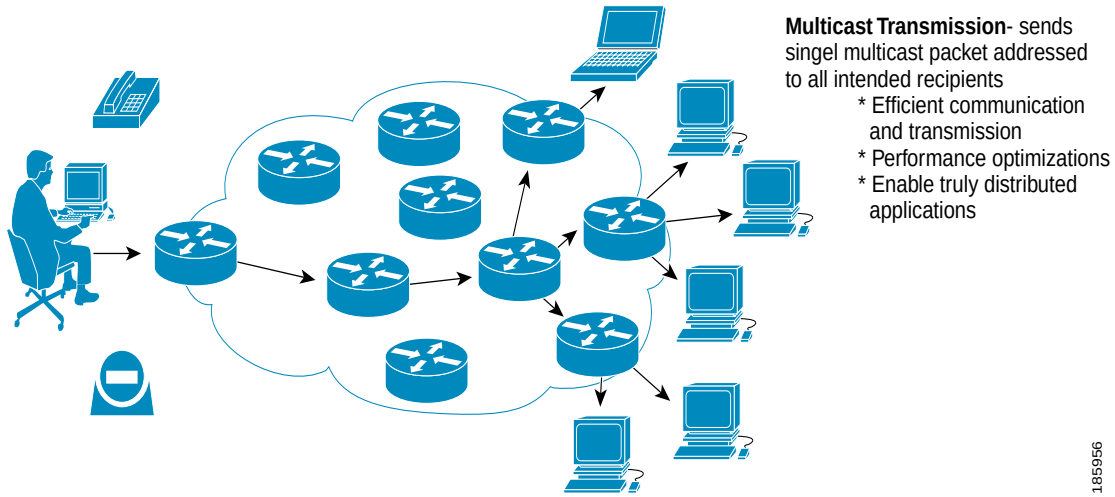
IP multicast allows for a streamlined approach to data delivery whenever multiple hosts need to receive the same data at the same time. Applications that deliver their data content using IP Multicast include Video conferencing, Cisco IP/TV broadcasts, file distribution or software packages, real-time price quotes of securities trading, news, and even video feeds from IP video surveillance cameras.

The distribution of large data files to all branches by means of a mass update is an efficient way to distribute parts lists, price sheets, or inventory data. Commercial software packages are available to optimize this file replication process by using IP Multicast as the transport mechanism. The corporate server sends one IP Multicast stream, and the networked routers replicate these packets so that all remote locations receive a copy of the file. The software can detect packet loss and at the end of the transfer, request an IP unicast stream of the missing portions to ensure the file is complete and valid.

2.3.1.1 Multicast Forwarding

IP multicast delivers source traffic to multiple receivers using the least amount of network resources as possible without placing additional burden on the source or the receivers. Multicast packets are replicated in the network by Cisco routers and switches enabled with Protocol Independent Multicast (PIM) and other supporting multicast protocols.

Figure 2-4 Basic Multicast Service



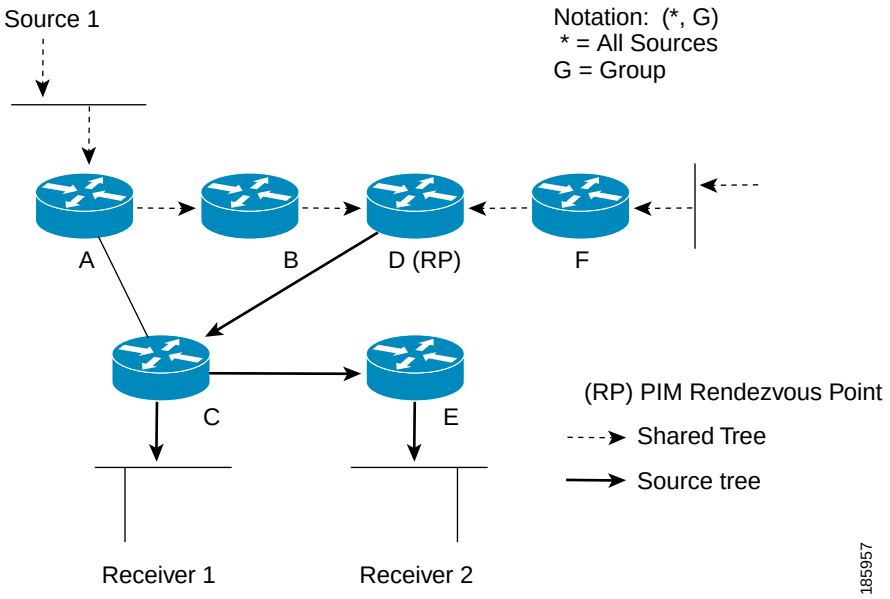
Multicast capable routers create “distribution trees” that control the path that IP Multicast traffic takes through the network in order to deliver traffic to all receivers. PIM uses any unicast routing protocol to build data distribution trees for multicast traffic.

The two basic types of multicast distribution trees are source trees and shared trees:

- Source trees—the simplest form of a multicast distribution tree is a source tree with its root at the source and branches forming a tree through the network to the receivers. Because this tree uses the shortest path through the network, it is also referred to as a shortest path tree (SPT).
- Shared trees—unlike source trees that have their root at the source, shared trees use a single common root placed at some chosen point in the network. This shared root is called a Rendezvous Point (RP).

In Figure 2-5, the RP has been informed of Sources 1 and 2 being active and has subsequently joined the SPT to these sources.

Figure 2-5 Shared Distribution Tree



PIM uses the concept of a designated router (DR). The DR is responsible for sending Internet Group Management Protocol (IGMP) Host-Query messages, PIM Register messages on behalf of sender hosts, and Join messages on behalf of member hosts.

2.3.1.2 IP Multicast Features

The primary difference between multicast and unicast applications lies in the relationships between sender and receiver. There are three general categories of multicast applications:

- One to many - when a single host sends to two or more receivers.
- Many-to-one - refers to any number of receivers sending data back to a (source) sender via unicast or multicast. This implementation of multicast deals with response implosion typically involving two-way request/response applications where either end may generate the request.
- Many-to-many, also called N-way multicast, consists of any number of hosts sending to the same multicast group address, as well as receiving from it.

One-to-many are the most common multicast applications. The demand for many-to-many N-way is increasing with the introduction of useful collaboration and videoconferencing tools. Included in this category are audio-visual distribution, Webcasting, caching, employee and customer training, announcements, sales and marketing, information technology services and human resource information. Multicast makes possible efficient transfer of large data files, purchasing information, stock catalogs and financial management information. It also helps monitor real-time information retrieval as, for example, stock price fluctuations, sensor data, security systems and manufacturing.

2.3.1.3 PIM Sparse Mode

The PIM Sparse Mode is a widely deployed IP Multicast protocol and is highly scalable in Enterprise networks. It is suitable for one-to-many (one source and many receivers) applications for Enterprise and Financial customers.

PIM Sparse Mode can be used for any combination of sources and receivers, whether densely or sparsely populated, including topologies where senders and receivers are separated by WAN links, and/or when the stream of multicast traffic is intermittent.

- *Independent of unicast routing protocols*—PIM can be deployed in conjunction with any unicast routing protocol.
- *Explicit-join*—PIM-SM assumes that no hosts want the multicast traffic unless they specifically ask for it via IGMP. It creates a shared distribution tree centered on a defined “rendezvous point” (RP) from which source traffic is relayed to the receivers. Senders first send the data to the RP, and the receiver’s last-hop router sends a join message toward the RP (explicit join).
- *Scalable*—PIM-SM scales well to a network of any size including those with WAN links. PIM-SM domains can be efficiently and easily connected together using MBGP and MSDP to provide native multicast service over the Internet.
- *Flexible*—A receiver’s last-hop router can switch from a PIM-SM shared tree to a source-tree or shortest-path distribution tree whenever conditions warrant it, thus combining the best features of explicit-join, shared-tree and source-tree protocols.

In a PIM-SM environment, RPs (Rendezvous Point) act as matchmakers, matching sources to receivers. With PIM-SM, the tree is rooted at the RP not the source. When a match is established, the receiver joins the multicast distribution tree. Packets are replicated and sent down the multicast distribution tree toward the receivers.

Sparse mode's ability to replicate information at each branching transit path eliminates the need to flood router interfaces with unnecessary traffic or to clog the network with multiple copies of the same data. As a result, PIM Sparse Mode is highly scalable across an enterprise network and is the multicast routing protocol of choice in the enterprise.

2.3.1.4 Rendezvous Point (RP) Deployment

There are several methods for deploying RPs.

- RPs can be deployed using a single, static RP. This method does not provide redundancy or load-balancing and is not recommended.
- Auto-RP is used to distribute group-to-RP mapping information and can be used alone or with Anycast RP. Auto-RP alone provides failover, but does not provide the fastest failover or load-balancing.
- Anycast RP is used to define redundant and load-balanced RPs and can be used with static RP definitions or with Auto-RP.

In the PIM-SM model, multicast sources must be registered with their local RP. The router closest to a source performs the actual registration.

2.3.1.5 Internet Group Management Protocol (IGMP)

IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP messages to their local multicast router. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

IGMP versions are described in the following sections:

2.3.1.6 IGMP Version 1

The specification of IGMP version 1 is described by RFC 1112, Host Extensions for IP Multicasting. Following are the two messages that exist in IGMP version 1:

- Membership query
- Membership report

Hosts send out IGMP membership reports of a particular multicast group to indicate that they are interested in joining that group. When a multicast application opens up a multicast socket, the TCP/IP stack on a host automatically sends the IGMP Membership report. The IGMP membership query is send periodically by the router to verify that at least one host on the subnet is still interested in receiving traffic directed to that group. When there is no reply to three consecutive IGMP membership queries, the router times out the group and stops forwarding traffic directed toward that group.

2.3.1.7 IGMP Version 2

IGMPv.2 is described by RFC 2236, Internet Group Management Protocol, Version 2. It is backward compatible with IGMPv1. Following are the four messages that exist in IGMP version 2:

- Membership query
- Version 1 membership report
- Version 2 membership report
- Leave group

IGMP Version 2 works exactly the same way as Version 1, except that there is an additional leave group message. With this message, the hosts can actively communicate to the local multicast router that they intend to leave the group. The router then sends out a group-specific query and determines if any remaining hosts are interested in receiving the traffic. If there are no replies, the router times out the group and stops forwarding the traffic. The addition of the leave group message in IGMP Version 2 greatly reduces the leave latency compared to IGMP Version 1. Unwanted and unnecessary traffic can be stopped much sooner. Therefore, version 2 is widely used if and when the choice is available.

2.3.1.8 IGMP Version 3

As of writing this document IGMP Version 3 (IGMPv3) is the latest IGMP version available. The key advantage of IGMPv3 is that it adds support for "source filtering," which enables a multicast receiver host to signal to a router to received multicast traffic from a specific source of a specific group. This membership information enables Cisco IOS software to forward traffic from only those sources from which receivers requested the traffic.

In IGMPv3, the following types of IGMP messages exist:

- Version 3 membership query
- Version 3 membership report

IGMPv3 supports applications that explicitly signal sources from which they want to receive traffic. With IGMPv3, receivers signal membership to a multicast host group in the following two modes:

- INCLUDE mode—in this mode, the receiver announces membership to a host group and provides a list of source addresses (the INCLUDE list) from which it wants to receive traffic.

- EXCLUDE mode—in this mode, the receiver announces membership to a multicast group and provides a list of source addresses (the EXCLUDE list) from which it does not want to receive traffic. The host will receive traffic only from sources whose IP addresses are not listed in the EXCLUDE list. To receive traffic from all sources, which is the behavior of IGMPv2, a host uses EXCLUDE mode membership with an empty EXCLUDE list.

The current specification for IGMPv3 can be found in the Internet Engineering Task Force (IETF) draft titled “Internet Group Management Protocol, Version 3” on the IETF website http://www.ietf.org. One of the major applications for IGMPv3 is Source Specific Multicast (SSM), which is described next.

2.3.1.9 IGMP Snooping

IP multicast uses the host signaling protocol IGMP to indicate that there are multicast receivers interested in multicast group traffic.

Internet Group Management Protocol (IGMP) snooping is a multicast constraining mechanism that runs on a Layer 2 LAN switch. IGMP snooping requires the LAN switch to examine some Layer 3 information (IGMP join/leave messages) in the IGMP packets sent between the hosts and the router. When the switch hears the “IGMP host report” message from a host for a multicast group, it adds the port number of the host to the associated multicast table entry. When the switch hears the “IGMP leave group” message from a host, the switch removes the host entry from the table.

2.3.1.10 Source Specific Multicast (SSM)

SSM, an extension of the PIM protocol, allows for an efficient data delivery mechanism in one-to-many communications. SSM enables a receiving client, once it has learned about a particular multicast source through a directory service, to then receive content directly from the source, rather than receiving it using a shared RP.

SSM removes the requirement of MSDP to discover the active sources in other PIM domains. An out-of-band service at the application level, such as a web server, can perform source discovery. It also removes the requirement for an RP.

In traditional multicast implementations, applications must "join" to an IP multicast group address, because traffic is distributed to an entire IP multicast group. If two applications with different sources and receivers use the same IP multicast group address, receivers of both applications will receive traffic from the senders of both the applications. Even though the receivers, if programmed appropriately, can filter out the unwanted traffic, this situation still would likely generate noticeable levels of unwanted network traffic.

In an SSM-enhanced multicast network, the router closest to the receiver will "see" a request from the receiving application to join to a particular multicast source. The receiver application then can signal its intention to join a particular source by using the INCLUDE mode in IGMPv3.

The multicast router can now send the request directly to the source rather than send the request to a common RP as in PIM sparse mode. At this point, the source can send data directly to the receiver using the shortest path. In SSM, routing of multicast traffic is entirely accomplished with source trees. There are no shared trees and therefore an RP is not required.

The ability for SSM to explicitly include and exclude particular sources allows for a limited amount of security. Traffic from a source to a group that is not explicitly listed on the INCLUDE list will not be forwarded to uninterested receivers.

SSM also solves IP multicast address collision issues associated with one-to-many type applications. Routers running in SSM mode will route data streams based on the full (S, G) address. Assuming that a source has a unique IP address to send on the internet, any (S, G) from this source also would be unique.

For CVD System Assurance, Multicast features such PIM Sparse mode, AutoRP, SSM and IGMP v3 were tested based on the recommendations in the *Multicast over IPSec VPN Design Guide*.

2.3.2 Wireless

The Cisco Unified Wireless Network solution unifies the wired and wireless networks to provide enterprises with a secure, scalable, and manageable platform for delivering mobility services. With this innovative solution, unification occurs at all levels, including hardware, software, and services. The Cisco wireless solution takes a comprehensive approach that enables mobility from the application layer to the client device.

Following are the three basic elements required to build secure, successful enterprise-class WLANs:

- Client Devices
- Lightweight Access Points
- Wireless LAN Controllers

Additional optional elements to the solution, such as Cisco Wireless Control System (WCS), Cisco WCS Navigator, and Cisco Wireless Location Appliance can be added as the wireless networking requirement grows.

WCS is management software that can be used to manage WLC devices and provide advanced management tools like wireless coverage display and location-based services. WCS uses SNMP to manage WLC devices, so the WLC devices need to have SNMP configured correctly.

Additional details on WCS can be found from the following location:

http://www.cisco.com/en/US/products/ps6305/products_qanda_item0900aecd802570dc.s html

The Cisco Wireless Location Appliance is the industry's first location solution that simultaneously tracks thousands of devices from within the WLAN infrastructure, bringing the power of a cost-effective, high-resolution location solution to critical applications such as:

- High-value asset tracking
- IT management
- Location-based security

For additional details, please refer to the following link:

http://www.cisco.com/en/US/products/ps6386/index.html

The Cisco Wireless Control System (WCS) Navigator delivers an aggregated platform for enhanced scalability, manageability, and visibility of large-scale implementations of the Cisco Unified Wireless Network. This powerful software-based solution gives network administrators cost-effective, easy access to information from multiple, geographically diverse Cisco WCS management platforms. It supports partitioning of the unified wireless network at the management level.

http://wwwin.cisco.com/ewtg/wnbu/products/wlm/wcs_navigator/index.shtml

For CVD System Assurance, a Centralized Wireless deployment was tested with 2006, 4404 and 3750G Wireless controllers, Cisco Wireless LAN Controller Modules (WLCMs) in different branch profiles. For Lightweight AP, HWIC-APs were used to verify Hybrid REAP and Dot1x authentication. Clients authenticate using Dot1x with Cisco Secure ACS Radius server as the authentication server. The supplicant on the clients was Cisco Secure Services Client (CSSC).

The Cisco Unified Wireless Network (CUWN) architecture centralizes WLAN configuration and control by a device called a WLAN Controller (WLC). This allows the WLAN to operate as an intelligent information network and support advanced services, unlike the traditional 802.11 WLAN infrastructure

that is built from autonomous, discrete entities. The CUWN simplifies operational management by collapsing large numbers of managed end-points—autonomous access points—into a single managed system comprised of the WLAN controller(s) and its corresponding, joined access points.

In the CUWN architecture, APs are “lightweight”, meaning that they cannot act independently of a WLC. APs are “zero-touch” deployed and no individual configuration of APs is required. The APs learn the IP address of one or more WLC via a controller discovery algorithm and then establish a trust relationship with a controller via a “join” process. Once the trust relationship is established, the WLC will push firmware to the AP if necessary and a configuration. APs interact with the WLAN controller via the Lightweight Access Point Protocol (LWAPP).

2.3.2.1 Cisco Wireless LAN Controllers

The Cisco 4400 Series Wireless LAN Controller provides system wide wireless LAN functions for medium to large-sized facilities. By automating WLAN configuration and management functions, network managers have the control, security, redundancy, and reliability needed to cost-effectively scale and manage their wireless networks as easily as they scale and manage their traditional wired networks.

The Cisco 4400 Series Wireless LAN Controller works in conjunction with Cisco Aironet access points, the Cisco Wireless Control System (WCS), and the Cisco Wireless Location Appliance to support business-critical wireless data, voice, and video applications. It provides real-time communication between access points and other wireless LAN controllers to deliver centralized security policies, wireless intrusion prevention system (IPS) capabilities, award-winning RF management, quality of service (QoS), and mobility.

The Cisco 4400 Series Wireless LAN Controller is available in two models. The Cisco 4402 Wireless LAN Controller with two 1 GB Ethernet ports comes in configurations that support 12, 25, and 50 access points. The Cisco 4404 Wireless LAN Controller with four 1 GB Ethernet ports supports 100 access points. The Cisco 4402 controller provides one expansion slot. The Cisco 4404 controller provides two expansion slots that can be used to add VPN termination as well as enhanced functionality in the future. In addition, each Cisco 4400 WLAN Controller supports an optional redundant power supply to ensure maximum availability.

2.3.2.2 Cisco Wireless LAN Controller Modules

Cisco Wireless LAN Controller Modules (WLCMs), supported on the Cisco Integrated Services Routers (ISR), provide an easy to deploy, cost-effective branch office or Small to Medium Business wireless solution. As a component of the Cisco Unified Wireless Network, the Cisco WLCMs give network administrators the visibility and control necessary to effectively and securely manage business-class wireless LANs and mobility services, such as enhanced security, voice, guest access, and location services. WLCMs work in conjunction with Cisco lightweight access points and the Cisco Wireless Control System (WCS) to provide centralized wireless LAN management and monitoring. The modules manage 6, 8 or 12 Cisco Aironet lightweight access points and are supported on Cisco 2800 and 3800 Series Integrated Services Routers and Cisco 3700 Series Multiservice Access Routers.

The Cisco Catalyst 3750 Integrated Wireless LAN Controller combines Cisco's Unified Wireless LAN functionality with Cisco's Catalyst 3750 stackable switches and delivers WLAN security, mobility, and ease of use for business critical wireless LANs.

Depending on the number of AP support, following are the two models available:

- The Cisco Catalyst WS-C3750G-24WS-S25, with 24 10/100/1000 PoE ports, 2 SFP module slots, and an integrated Cisco wireless LAN controller supporting up to 25 Cisco Access Points
- The Cisco Catalyst WS-C3750G-24WS-S50, with 24 10/100/1000 PoE ports, 2 SFP module slots, and an integrated Cisco wireless LAN controller supporting up to 50 Cisco Access Points

The Cisco Catalyst 3750G Integrated Wireless LAN Controllers deliver secure, enterprise wireless access to midsize organizations and enterprise branch offices requiring support for 50 to 200 access points in one logical unit. A logical unit is a stack of up to nine 3750G switches.

The Cisco Catalyst 3750G Integrated Wireless LAN Controllers delivers centralized security policies, wireless intrusion prevention system (IPS) capabilities, award-winning RF management, QoS, and Layer 3 fast secure roaming for WLANs.

For CVD System Assurance, wireless features were tested based on recommendations in the *Enterprise Mobility 3.0 Design Guide*.

2.3.3 Voice over IP (VoIP)

To implement Voice over IP, the following design guides were used together to reflect the implementation of complex designs in the field:

- *Cisco Unified Communications SRND Based on Cisco Unified CallManager 5.x*
- *Cisco Unified CallManager Express Solution Reference Network Design Guide*
- *Guide to Cisco Systems' VoIP Infrastructure Solution for SIP*
- *Cisco IOS SIP Configuration Guide*

Combinations of the listed design guides were the design basis for the CVD System Assurance voice test suite. Skinny Call Control Protocol (SCCP) and Session Initiation Protocol (SIP) voice were tested both with Cisco Unified Communication Manager and Cisco Unified Call Manager Express.

The Cisco Unified Communications System delivers fully integrated communications by enabling data, voice, and video to be transmitted over a single network infrastructure using standards-based Internet Protocol (IP).

The foundation architecture for Cisco IP Telephony includes of the following major components:

- Cisco IP network Infrastructure
- Call Processing Agent
- Communication End Points

2.3.3.1 Cisco IP Network Infrastructure

The Enterprise Branch Security design provides support for multiple clients such as hardware Cisco IP phones and video phones.

Proper Branch and WAN infrastructure design is extremely important for proper IP telephony operation on a converged network. Proper WAN infrastructure design requires deploying end-to-end QoS on all WAN links.

WAN deployments for voice networks may be hub-and-spoke or an arbitrary topology. A hub-and-spoke topology consists of a central hub site and multiple remote spoke sites connected into the central hub site. In this scenario, each remote or spoke site is one WAN-link hop away from the central or hub site and two WAN-link hops away from all other spoke sites. An arbitrary topology may contain multiple WAN links and any number of hops between the sites. In this scenario there may be many different paths to the same site or there may be different links used for communication with some sites compared to other sites. The simplest example is three sites, each with a WAN link to the other two sites, forming a triangle. In that case there are two potential paths between each site to each other site.

Topology-unaware call admission control requires the WAN to be hub-and-spoke, or a spoke-less hub in the case of MPLS VPN. This topology ensures that call admission control, provided by Unified Communication Manager's locations or a gatekeeper, works properly in keeping track of the bandwidth available between any two sites in the WAN. In addition, multiple hub-and-spoke deployments can be interconnected via WAN links.

WAN links should, when possible, be made redundant to provide higher levels of fault tolerance. Redundant WAN links provided by different service providers or located in different physical ingress/egress points within the network can ensure backup bandwidth and connectivity in the event that a single link fails. In non-failure scenarios, these redundant links may be used to provide additional bandwidth and offer load balancing of traffic on a per-flow basis over multiple paths and equipment within the WAN. Topology-unaware call admission control normally requires redundant paths to be over-provisioned and under-subscribed to allow for failures that reduce the available bandwidth between sites without the call admission control mechanism being aware of those failures or the reduction in bandwidth. Topology-aware call admission control is able to adjust dynamically to many of the topology changes and allows for efficient use of the total available bandwidth.

Voice and data should remain converged at the WAN, just as they are converged at the LAN. QoS provisioning and queuing mechanisms are typically available in a WAN environment to ensure that voice and data can interoperate on the same WAN links. Attempts to separate and forward voice and data over different links can be problematic in many instances because the failure of one link typically forces all traffic over a single link, thus diminishing throughput for each type of traffic and in most cases reducing the quality of voice. Furthermore, maintaining separate network links or devices makes troubleshooting and management difficult at best.

Because of the potential for WAN links to fail or to become oversubscribed, it is recommended to deploy non-centralized resources as appropriate at sites on the other side of the WAN. Specifically, media resources, DHCP servers, voice gateways, and call processing applications such as Survivable Remote Site Telephony (SRST) and Cisco Unified Communications Manager Express (Unified CME) should be deployed at non-central sites when and if appropriate, depending on the site size and how critical these functions are to that site. Keep in mind that de-centralizing voice applications and devices can increase the complexity of network deployments, the complexity of managing these resources throughout the enterprise, and the overall cost of a the network solution; however, these factors can be mitigated by the fact that the resources will be available during a WAN link failure.

When deploying voice in a WAN environment, Cisco recommends that you use the lower-bandwidth G.729 codec for any voice calls that will traverse WAN links because this practice will provide bandwidth savings on these lower-speed links.

Finally, recommendation G.114 of the International Telecommunication Union (ITU) states that the one-way delay in a voice network should be less than or equal to 150 milliseconds. It is important to keep this in mind when implementing low-speed WAN links within a network. Topologies, technologies, and physical distance should be considered for WAN links so that one-way delay is kept at or below this 150-millisecond recommendation.

The deployment of an IP Communications system requires the coordinated design of a well structured, highly available, and resilient network infrastructure as well as an integrated set of network services including Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), and Network Time Protocol (NTP).

2.3.3.2 Call Processing Agent

Cisco Unified Communications Manager (Unified CM) is the core call processing software for Cisco IP Telephony. It builds call processing capabilities on top of the Cisco IP network infrastructure. Unified CM software extends enterprise telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, voice gateways, and multimedia applications.

Typically, Cisco Unified Communications Manager (Unified CM) cluster servers, including media resource servers, reside in a data center or server farm environment.

For CVD System Assurance, Multi-site WAN with Centralized Call Processing is used. The Multisite WAN model with centralized call processing consists of a single call processing agent that provides services for many sites and uses the IP WAN to transport IP telephony traffic between the sites. The IP WAN also carries call control signaling between the central site and the remote sites. The remote sites rely on the centralized Unified CM cluster to handle their call processing. Applications such as voicemail and Interactive Voice Response (IVR) systems are typically centralized as well to reduce the overall costs of administration and maintenance.

The multi-site model has the following design characteristics:

- Single Unified CM or Unified CM cluster.
- Maximum of 30,000 Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP) IP phones or SCCP video endpoints per cluster.
- Maximum of 500 H.323 devices (gateways, Mucks, trunks, and clients) per Unified CM cluster.
- PSTN for all external calls.

Connectivity options for the IP WAN include:

- Leased lines
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- ATM and Frame Relay Service Inter-Working (SIW)
- Multi-protocol Label Switching (MPLS) Virtual Private Network (VPN)
- Voice and Video Enabled IP Security Protocol (IPSec) VPN (V3PN)

Routers that reside at the WAN edges require quality of service (QoS) mechanisms, such as priority queuing and traffic shaping, to protect the voice traffic from the data traffic across the WAN, where bandwidth is typically scarce. In addition, a call admission control scheme is needed to avoid oversubscribing the WAN links with voice traffic and deteriorating the quality of established calls.

2.3.3.3 Centralized Call Processing Model Best Practices:

Following are the guidelines and best practices when implementing the Multisite WAN model with centralized call processing:

- Minimize delay between Unified Communication Manager and remote locations to reduce voice cut-through delays (also known as clipping).
- Use the locations mechanism in Unified Communication Manager to provide call admission control into and out of remote branches.
- The locations mechanism works across multiple servers in Cisco Unified CM Release 3.1 and later. This configuration can support a maximum of 30,000 IP phones when Unified CM runs on the largest supported server.
- The number of IP phones and line appearances supported in Survivable Remote Site Telephony (SRST) mode at each remote site depends on the branch router platform, the amount of memory installed, and the Cisco IOS release.

2.3.3.4 Communication Endpoints

A communication endpoint is a user instrument such as a desk phone or even a software phone application that runs on a PC. In the IP environment, each phone has an Ethernet connection. IP phones have all the functions you expect from a telephone, as well as more advanced features such as the ability to access World Wide Web sites.

In this design, Cisco IP phones and Video telephones are being used for endpoint.

Under this infrastructure, SCCP phones and SIP phones are connected to ISR routers and access switches, with IP addresses routable to Cisco Unified Communications Manager. These phones are registered with Cisco Unified Communications Manager and a route plan is devised in Cisco Unified Communications Manager to be able to find and connect to numbers dialed.

In this design validation effort, PSQM voice quality measurement, jitter and delay are measured for the combination of difference call types.

This page is intentionally left blank

CHAPTER 3

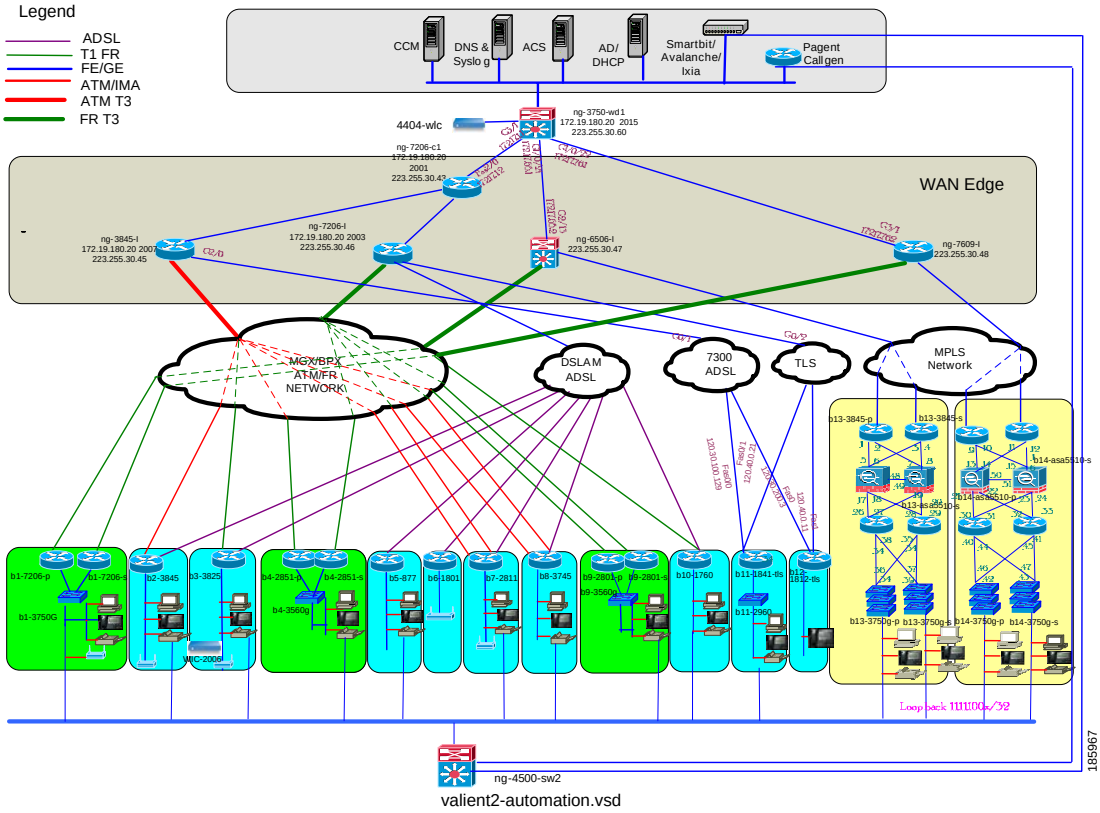
CVD System Assurance Test Strategy

This section explains the overall strategy of the test-bed setup, types of system tests, and sustaining strategy.

3.1 Test Topology

A large scale branch system test environment was built consisting of three branch profiles as shown in Figure 3-1.

Figure 3-1 *Automation Test Bed Setup for NG Branch CVD System Assurance*



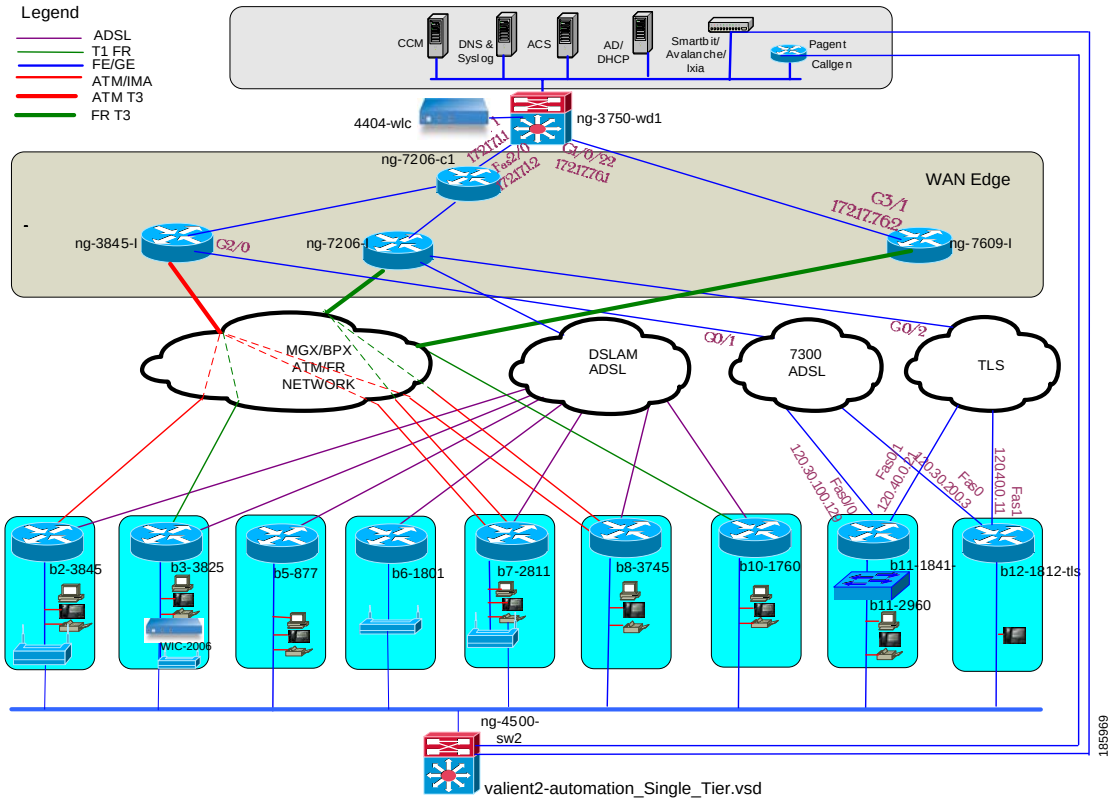
According to the *Next Generation Enterprise Branch Security Design Guide*, different WAN connections were established to satisfy different customer needs. The WAN aggregation portion of enterprise campus was created to terminate WAN connections to the branches. In an effort to create a truly customer representative network, services such as VoIP, Multicast, Wireless were provisioned. Traffic tools were used to generate voice, Multicast, data and Wireless users traffic.

As shown in Figure 3-1, 14 branches were constructed among which nine were Single-Tier, three were Dual-Tier, and two were Multi-Tier. MGX/BPX was used for the ATM/FR cloud and DSLAM was used for the ADSL cloud. An MPLS L3VPN network was built for Multi-Tier Branch profile.

Four Enterprise WAN Edge devices: 7206VXR, Cat 6509, 3845, and C7600 were placed on WAN Edge of a simulated Campus network. The Enterprise WAN Edge devices allow branches to terminate DMVPN connections. The Campus network was simulated with a Cat 3750 switch. The data center, where all the applications such as ACS Server, Cisco Call Manager reside were connected to a Cat 3750 switch.

The Single-Tier branch profiles were connected to the Enterprise WAN Edge device (DMVPN hubs) through Frame-relay and ATM clouds (MGX/BPX) as shown in Figure 3-2. The back-up links were connected through an ADSL cloud (DSLAM).

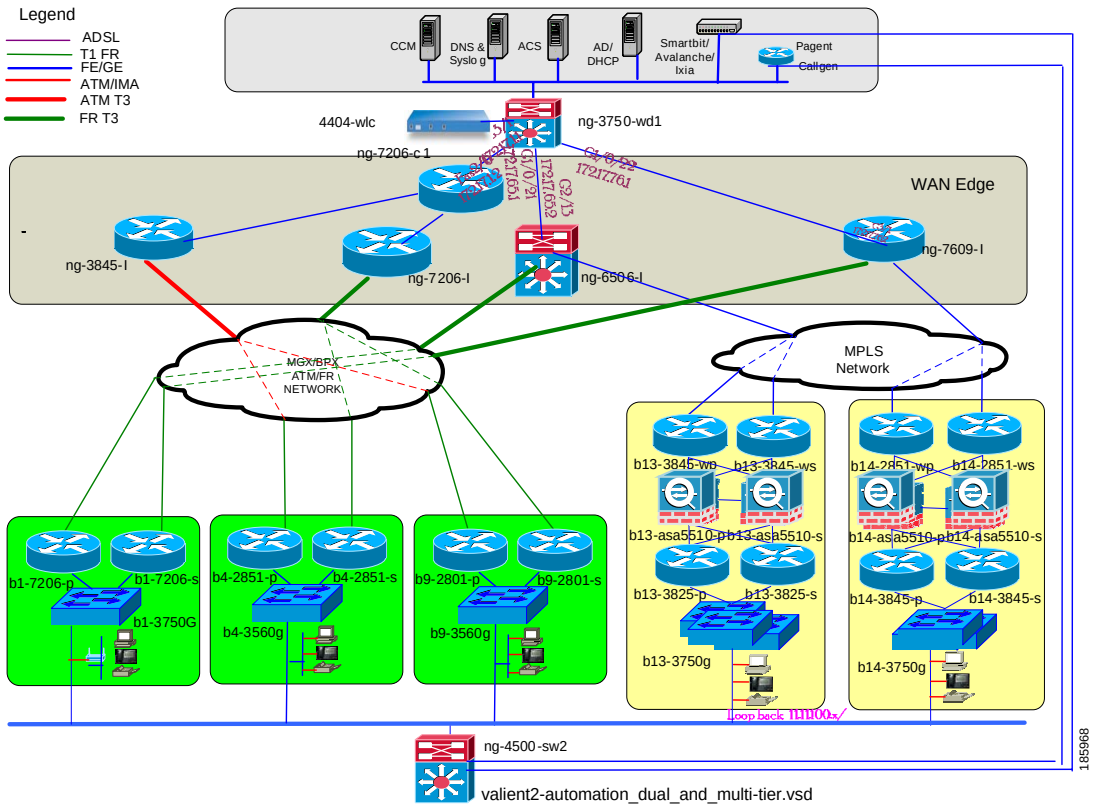
Figure 3-2 Automation Test Bed Setup for NG Single-Tier Branch Profiles



The Dual-Tier used a Frame Relay private WAN deployment model. The primary and the back-up access routers are connected to Campus Edge routers via Frame Relay PVC configured over T1 link. Dual-Tier branches that are constructed for Automation test bed are shown in Figure 3-3.

The Multi-Tier Branch profiles were connected to the MPLS L3VPN cloud to provide high availability and reliability. Multi-Tier Branch profiles that were tested and automated are shown in Figure 3-3.

Figure 3-3 Automation Test Bed Setup for NG Dual-Tier & Multi-Tier Branch Profiles



The EIGRP Routing protocol was used for IP routing in all the three profiles. The Dual-Tier profile used HSRP for network redundancy. In the Multi-Tier profile, static routing was used on ASA firewall.

VoIP testing included Cisco Unified Communications Manager that sits on the data center. VoIP also includes CCME (configured on ISR Routers on the Branches), and IP Phones, and the VoIP testing tool Abacus was used to generate traffic. SIP, SRST, SCCP, voice jitter, delay, and packet loss were tested.

The Branch traffic profiles consisted of stateful (such as http, telnet, and ftp), background UDP, Multicast (both Sparse-mode and SSM) traffic, video over wireless, and VoIP traffic. Unicast, PIM-SM, and SSM Multicast traffic were generated using SmartBits. SmartBits was also used for CISF security feature testing. For QoS testing, Unicast traffic was generated by setting multiple DSCP values. Abacus was used for VoIP testing. Stateful traffic was generated using Avalanche to test the Cisco IOS Intrusion Prevention System (IPS) on the ISR routers. IxVPN was used to generate 400-800 DMVPN spokes per DMVPN hub. For wireless testing, IxLoad combined with IxWLAN were used to generate wireless sessions, verify authentication, and access web pages.

Configurations of a Single-Tier, Dual-Tier, and Multi-Tier Branch Profiles are shown in Appendix E.

3.2 Test Types

Validation tests are divided into the following types:

- System Integration Test
- Scalability Test
- Negative/Redundancy Test
- Reliability Test

3.2.1 System Integration Tests

System Integration has two major components, feature combination and feature interaction. Feature combination focuses on testing a feature when various combinations of other features are enabled. An example of Feature combination test is when ARP inspection is tested along with base-line configuration on the switch. Feature interaction tests were conducted to verify dependencies between features. An example of a Feature Interaction test is DMVPN with dynamic routing protocol such as EIGRP.

For the System Integration test, following were the features configured in Single-Tier, Dual-Tier, and Multi-Tier Branch profiles: DMVPN, EIGRP Routing Protocol, QoS, Multicast, Security, Wireless, and VoIP. Traffic flow between Branch to Branch, and Branch to Campus were generated to test these services individually while ensuring all services were provisioned in the devices.

3.2.1.1 DMVPN Test Suite

DMVPN Phase three was tested with Hierarchical Hub topology for scalable spoke to spoke tunnels.

Following are the types of test cases performed in the DMVPN Hierarchical Hub Network:

- Hierarchical Topology Verification
- Spoke to Spoke DMVPN tunnel
- Summarization of EIGRP Routing Protocol
- Lifetime
- AES

All DMVPN test cases were sequentially executed with background traffic and baseline features.

3.2.1.2 Routing Test Suite

The routing test suite was targeted to deploy and verify the Enterprise NG Branch Design using EIGRP as the routing protocol. The EIGRP routing protocol was used for IP routing in all the three profiles. The Dual-tier profile used HSRP for network redundancy. In the Multi-Tier profile, static routing was configured in the ASA firewall

The EIGRP routing protocol had to be configured correctly before Multicast, VoIP, Security, QoS, and Convergence test suites could be executed. Following are the types of test cases performed in the Routing Test Suite:

- EIGRP Neighbors Authentication
- EIGRP Stub Routing
- EIGRP Route Filters

- EIGRP Neighbor Stability

All routing test cases were executed in parallel with background traffic and baseline features.

3.2.1.3 Security Test Suite

The security test suite focused on Cisco Integrated Security Feature (CISF) on the NME-16ES-1g-p module. Following are the types of test cases in the security test suite:

- CISF Port Security
- CISF DHCP Snooping
- CISF Dynamic ARP Inspection
- CISF IP Source Guard

All the test cases were executed sequentially.

3.2.1.4 QoS Test Suite

QoS on the branch network was configured using Modular QoS CLI (MQC) and a 10-class QoS model.

Following are the types of test cases in the QoS test suite:

- QoS Scavenger Class
- QoS Frame Relay Traffic Shaping
- QoS MQC Queuing
- QoS Spoke Prioritization

All QoS test cases were executed sequentially.

3.2.1.5 Wireless Test Suite

Wireless testing included WPA2 and Roaming. Security features such as VPN Client Authentication, dot1x authentication were tested. A centralized Wireless infrastructure mode was used. Cisco Secure ACS was used to authenticate clients using 802.1x with EAP tunnel protocol.

Data, VoIP, Video, and Multicast traffic were verified to function properly together between Wireless clients and the Branch network.

Following are the types of test cases in the Wireless test suite:

- 2006 Wireless Controller Verification
- 4404 Wireless Controller Verification
- 3750G Wireless Controller Verification
- Wireless LAN Controller Modules (WLCMs) Verification
- HWIC-AP WLAN Module Verification
- Hybrid Reap
- Dot1x Auth

All test cases executed sequentially.

3.2.1.6 Multicast Test Suite

The Multicast test suite focused on verifying Multicast functionality such as PIM Sparse Mode, SSM and IGMP v3 over the DMVPN network. The tests were performed on ISR 3845 and 7206 VXR hub routers. Multicast via a DMVPN mGRE interface is not supported on the Cat 6500 or C 7600 router and therefore was not tested.

Following are the types of test cases in the Multicast test suite:

- Multicast delivery using PIM Sparse Mode
- PIM Sparse Mode Auto-RP listener
- Multicast Delivery using SSM
- IGMP v3

All test cases were executed sequentially.

3.2.1.7 VoIP Test Suite

The primary focus of the VoIP test suite was to test the Cisco Unified Communications Manager (Version 5.0), Cisco Call Manager Express (Version 4.0) and SRST on different ISR routers. Session Initiation Protocol (SIP) and Skinny Client Control Protocol (SCCP) were the VoIP protocols tested. Performance tests such as RTP Jitter, Delay and PSQM Voice Quality were executed for Branch routers using Cisco Unified Communications Manager and Cisco Unified Call Manager Express.

Following are the types of test cases in the VoIP test suite:

- Intra Branch SIP to SIP with CCM
- Inter Branch SIP to SIP with CCM
- Intra Branch SCCP to SCCP with CCM
- Inter Branch SCCP to SCCP with CCM
- Inter Branch SIP to SCCP and SIP to SCCP with CCM
- Inter Branch Media Transport Delay with CCM
- Inter Branch Jitter with CCM
- Inter Branch SRTP with CCM
- Inter Branch Quality of Voice with CCM
- Intra Branch SIP Video Phone with CCM
- SRST with CCM
- Intra Brach SCCP to SCCP with CME
- Intra Branch SIP to SIP with CME
- Inter Branch SCCP to SCCP with CME
- Inter Branch SIP to SIP with CME
- Inter Branch Jitter with CME
- Inter Branch Media Transport Delay with CME
- Inter Branch PSQM test with CME
- Inter Branch test between SCCP and SIP with CME

All test cases were executed sequentially.

3.2.2 Scalability Test Suite

Scalability testing measures the limit of a particular variable when all others are constant in a system level environment. For example, the number of EIGRP neighbor a DMVPN hub can support. The purpose of this test suite was to scale 400 DMVPN spokes on Cat 6509 and 800 DMVPN spokes on 3845, 7206, and 7609 DMVPN hub routers. IxVPN was used for this testing.

The focus of this test suite was to verify the number of NHRP mappings the Hub can cache, and the number of DMVPN spokes that can be built successfully on various hubs. It is important to note that, scaling number of EIGRP Neighbor per hub is as important as scaling number of DMVPN spokes. The lowest number between DMVPN spokes, and EIGRP neighbors that hub can support should be used for designing a scalable DMVPN network. Due to tool limitation, hub was scaled for number of DMPVN spokes only without turning on EIGRP routing protocols.

All test cases were executed sequentially.

3.2.3 Negative Test Suite

Negative testing concerns error handling and robustness. Erroneous inputs can be applied at the system level to verify behavior against error handling specifications. Unspecified inputs or conditions, including fault injection, can be applied to assess the system level robustness. **Redundancy Testing** is placed under the negative test suite and it primarily pertains to testing network availability, e.g. validation of redundant WAN links.

The Negative test suite was executed on the Enterprise NG Branch Single-Tier, Dual-Tier and Multi-Tier profiles with some test scenarios that validate that under different failure conditions, the network functions normally.

Each negative test case introduced certain conditions or failures to the network that made other positive test cases fail. Therefore, negative test cases were grouped together in a separate test suite for better test management.

Following are the types of test cases in the Negative test suite:

- Convergence Tests with Link failures
- Convergence Tests with Router failures
- High Availability test with ASA failover
- IPSec Tunnel Shut – no Shut
- Adding and deleting ACL's

All test cases were executed sequentially.

3.2.4 Reliability Test Suite

System reliability is the probability that the system will work without failure for a specified period of time.

A 120-hr reliability test case was performed after all the system integration, negative and scalability testing passed. During the duration of 120 hours reliability testing, all the traffic including stateful (http, telnet, ftp etc.), background UDP, Multicasting, Video streams, VoIP and Wireless traffic, were running on the Enterprise NG Branch network infrastructure. Every 10 hours, the following test suites were executed: DMVPN, Routing, Security, QoS, Multicast, VoIP, Wireless, and Negative to ensure that the network was functioning properly. After these test suites were executed the following were analyzed: memory utilization, CPU hog, up time, traceback, alignment, Syslog, packet errors and crashes.

3.3 Sustaining Coverage

All the test cases in the System Integration Test described in B.1 System Integration Tests, page B-2 were included in the automation scripts. The automation test solution includes following components:

- The automated test scripts for each automation test cases
- The common library for managing the test-bed, collecting and reporting the test results
- The automated procedures to capture the manual execution results

All the real applications used in the manual validation phase, Cisco Unified Communications Manager server and IP phones were not automated. Instead, the traffic tools were used to generate simulated traffic on the network.

This page is intentionally left blank

CHAPTER 4

Results and Recommendations

This section presents a summary of validation results and outlines CVD System Assurance recommendations for Single-Tier, Dual-Tier, and Multi-Tier Branch Profiles on Branch routers, and the Hub routers based on the observation during the validation for the project, and Cisco best practices recommendation. For additional details on test results, please contact your account team.

4.1 DMVPN

Following are some of the recommendation for the DMVPN implementation:

4.1.1 MTU Recommendation

It is highly recommended to fragment the packets using the GRE tunnel interface. When GRE tunnel interface fragments the data IP packets, it encapsulate the individual fragments in GRE/IP packets. Then when IPSec sees the "not-fragmented" GRE/IP packets, it doesn't fragment the packet again. If IPSec needs to do fragmentation, then this causes higher CPU utilization on the other end (hubs). To avoid this, the GRE tunnel is set with the **IP mtu to 1400**. Consequently, all of the IP reassembly that is done by the receiving router can be avoided.

Following is an example of how to setup the MTU value to 1400 on the tunnel interface on the spokes:

```
interface Tunnel38
ip mtu 1400
```

It is highly recommended to turn on Pre-fragmentation on the IOS router. Pre-fragmentation for IPSec VPNs is enabled by default. To make sure to disable Post-fragmentation, use the following command in the configuration mode of the router:

```
no crypto ipsec fragmentation after-encryption
```

For additional details on how to address the MTU issue, please refer to the following link:

http://www.cisco.com/warp/public/105/pmtud_ipfrag.html

4.1.2 NHRP Hold Time Tuning for Dynamic Spoke to Spoke Tunnels

In a DMVPN network, the dynamic spoke to spoke tunnels are brought up only when there is traffic that needs to go to the network behind other spoke routers. The spoke to spoke tunnels are designed to be transitory and therefore must be refreshed if data traffic is still using the spoke to spoke tunnel. This

means that there are NHRP resolution request/reply packets to refresh the tunnel. This mechanism is performed in the background and does not directly affect the data traffic. However, it does increase the CPU load slightly on the routers. In DMVPN Phase 2 networks, both spokes and hubs see this traffic. In DMVPN phase 3 networks, only the two spokes see this traffic. If theDMVPN network is designed to be 100% dynamic spoke to spoke then this traffic can have some impact on the CPU and the whole network. To reduce the amount of traffic, the only option available is to increase the NHRP hold time. Increasing the hold time will refresh the spoke to spoke tunnel less often. This however poses problems with keeping a spoke to spoke tunnel up longer even when it is no longer being used. The recommended value for the NHRP hold time under these circumstances depends on the size of the DMVPN network, and the ratio of dynamic spoke to spoke tunnels.

4.1.3 Black-Holing Mitigation Technique for Dynamic Spoke to Spoke Tunnels

In DMVPN spoke to hub deployments, tunnels are continuously monitored by the routing protocol that is running over them. Therefore, if something in the middle breaks the tunnel, it is noticed fairly quickly and routing switches traffic to the other spoke to hub tunnel. In the case of spoke to spoke, however, tunnels are not monitored with a dynamic routing protocol. Therefore, if something in the middle breaks the tunnel, it may not be noticed and the spoke to spoke traffic may be black-holed for an extended period of time. It will likely be detected the next time the spoke to spoke tunnel is refreshed. To reduce the length of time of black-holing, decrease the NHRP hold time. The NHRP hold time under these circumstances depends on the stability, and resiliency of the underlying network upon which the DMVPN network is overlaid.

4.1.4 CA Server Deployment

The CA Server must be available for the DMVPN spokes before the tunnel between the DMVPN spokes and hubs can be established if a certificate is used for the IKE Phase 1 authentication. Therefore, the CA Server is best placed in the subnet connected behind the management VPN gateway. Initially the spokes can be enrolled with CA as part of in-house provisioning before shipment to the remote location. If PKI certificates have expired or become invalid, the tunnel cannot be set up for corporate access. Keeping the CA Server under the management subnet will give the spokes secure access through management tunnel for new enrollment or reenrollment if the certificates expire or become invalid. If the certificate from the same CA Server is used to set up secure connections with the management and data gateways and the certificate in the spoke becomes invalid, the management tunnel will also fail. Therefore, it is recommended that different CA Servers be used to set up secure connections with management and data gateways. There are a number of CA Server choices available such as Cisco IOS routers, Microsoft or VeriSign. While most of the CA Servers work with Cisco IOS routers for DMVPN, it is easier to implement a Cisco IOS Certificate Server without any plug-ins.

4.2 Routing

4.2.1 Choosing Routing Protocol for the DMVPN network

Selection of the routing protocol over a DMVPN network depends on the specific need based on the deployment scenarios. Table 4-1 summarizes the characteristics of various routing protocol options for the DMVPN network.

Table 4-1 DMVPN Routing Protocol Options

Routing Protocol	Network Type	Routing Control	Convergence	CPU	Scaling	Comment
EIGRP	Hub to Spoke spoke to spoke	Good	Faster	High	Lower	
OSPF	Hub to Spoke spoke to spoke	Fair	Faster	High	Lower	Restricted to single Area
BGP	Hub to Spoke spoke to spoke	Good	Slower	Medium	Medium	Static neighbor
RIP (Passive)	Hub to Spoke	Fair	Slower	Low	Higher	Need IP SLA
ODR	Hub to Spoke	None	Slower	Low	Higher	Default Route Only

Based on Table 4-1, with the BGP Route Server farm behind the hub, it is possible to scale higher DMVPN spokes. However, convergence is slower than the EIGRP and OSPF routing protocol. RIP (Passive), and ODR can scale higher spokes with the expense of slower convergence and less route control. Besides, with RIP (Passive), and ODR, only Hub to Spoke is possible unless DMVPN phase 3 is implemented.

EIGRP is the protocol of choice when it comes to routing flexibility for DMVPN networks. EIGRP is a distance-vector protocol, and it works better on NBMA types of networks unlike OSPF, which is a link-state protocol.

Using EIGRP, it is easier to load-share, and load balance the spokes with the hubs. Using EIGRP, it is easy to manipulate the routing metrics, which allow some spokes to use one hub (hub1) as the primary and the other hub (hub2) as the backup while other spokes do the reverse, while still preserving symmetrical routing in both directions over the tunnels. With OSPF some spokes will end up having asymmetrical routing in one direction or the other over the tunnels.

Using DMVPN Phase 2, EIGRP has a number of advantages over OSPF. In dynamic spoke to spoke deployments, using OSFP, only 2 hub routers can be configured because OSPF **broadcast network type** needs to be configured so that the routes on the spoke routers will have the correct IP next-hop (remote spoke). OSPF **broadcast network type** require that a DR and BDR (the hub routers) is elected, and it is required that the DR and BDR see the same set of spoke routers as well as each other. There is no provision for a BBDR. However, using EIGRP, more hub routers can be bundled together to increase the number of spoke routers on the DMVPN network. Spokes are typically connected to two hubs for redundancy and all of the spokes are evenly spread across all of the hubs. For example, for 600 spokes, with redundancy, 1200 spoke-hub tunnels must be built, which means there will be 3 hubs with 400 spokes each. There is no theoretical limits on hub routers, however the practical limit is around 6-10 hub routers.

When deploying a DMVPN Phase 2 Hub to Spoke topology, spokes can be setup as stub routers when EIGRP is used. Consequently, EIGRP doesn't send queries to all the spokes when a spoke router goes up or down. With the changes to the EIGRP protocol, configuring stub and non-stub neighbors on the same interface is possible. However, using OSPF, all of the tunnels and spokes must be in the same area. If however, multiple mGRE interfaces (multiple DMVPN clouds) are configured on the Hub router, then each one can be in a different OSPF area. All spoke routers within the same area are notified (LSAs sent, etc.) whenever a spoke router goes up or down. Another advantage of EIGRP is that summarizing routes at the hub is possible when advertising spoke routes back out to the spokes. Using OSPF. summarizing routes within an area is not possible. Therefore, all spokes within a DMVPN cloud will have all routes for networks behind other spokes. Just like the dynamic spoke to spoke deployment model, using

EIGRP, it is possible to deploy as many hub routers as necessary to support a large number of spokes in the DMVPN network. If more than 2 hub routers need to be deployed using OSPF, a point-mulitpoint network type must be configured. In this case, the special /32 routes for tunnel IP addresses must be blocked so that they do not get into the routing table. Otherwise it is possible that a spoke router brings up only 1 spoke to hub tunnel. The other spoke-hub tunnel will fail to come up.

For **DMVPN Phase 3 with either hub-and-spoke only or dynamic spoke to spoke, t**he scaling of EIGRP and OSPF will be similar to their respective scaling of the when using DMVPN Phase 2 hub-and-spoke only.

4.2.2 EIGRP Routing Protocol Recommended Configuration

4.2.2.1 EIGRP Stub Routing

It is highly recommended to configure EIGRP stub routing on the DMVPN spoke routers. Configuring the EIGRP stub feature on the spoke routers prevents the hub routers from sending downstream queries which helps convergence time.

```
router eigrp 100
eigrp stub connected
```

With this configuration branch routers will advertise only the connected networks to the hubs across the DMVPN tunnel.

http://www.cisco.com/en/US/customer/docs/ios/12_0t/12_0t7/feature/guide/fceigrps.html

4.2.2.2 EIGRP Route Filters

EIGRP route filters on the hub must be configured in such a way that branch router never re-learns the connected network that was advertised by the branch routers to the hubs with the **eigrp stub connected** command on the Branch. Configure the following commands on the head-end to accomplish this (assuming that the connected network on the branch that was advterised to the hub was 10.1.1.0):

```
router eigrp 100
distribute-list default out GigabitEthernet3/3
!
ip access-list standard default
deny 10.1.1.0
permit any
```

4.3 Security

Many of the network security attacks and violations that occurred in the past in an enterprise network is from the LAN segment of the Campus and Branch. Hence, proper security mechanism needs to be implemented on typically trusted side of the network, which is LAN. CISF features can be enabled on the NME module of the ISR routers or the low end switches such as Cat 3750, or Cat3560 to mitigate some of the attacks that can be originated from the LAN side of the Branch networks. The impact of these attacks can be significant, and propagate all the way to Campus, if not mitigated timely manner.

4.3.1 Catalyst Integrated Security Features (CISF)

Port Security:

Port security is used to restrict input to an interface by limiting and identifying MAC addresses of the stations that are allowed access to the port. When assigning secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If the number of secure MAC addresses is to one and assigned a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port.

Dynamic ARP Inspection (DAI):

DAI uses the binding information that is built by DHCP snooping to enforce the advertisement of bindings to prevent "man-in-the-middle" attacks. These attacks can occur when an attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entries in a communication association. DAI adds an extra layer of security to Address Resolution Protocol (ARP) inspection by verifying that the ARP packet's MAC address and IP address match an existing DHCP snooping binding in the same VLAN. The basic functionality and packet flow of ARP inspection remains unchanged except for the addition of checks to ensure that a DHCP binding exists. Turn on DAI to “Man-in-the-middle” attachk attacks on the LAN facing interface of the Branch LAN switches or the NME modules on the ISR routers. You must have the DHCP Snooping turned on to have DAI feature on the LAN Switches or the NME modules on the ISR.

DHCP Snooping:

DHCP snooping provides security against DoS attacks that are launched using DHCP messages by filtering the DHCP packets and building and maintaining a DHCP-snooping binding table. DHCP snooping uses both trusted and untrusted ports. DHCP packets that are received from a trusted port are forwarded without validation. Typically, trusted ports are used to reach a DHCP server or relay agent. When the switch receives the DHCP packets from an untrusted port, DHCP snooping validates that only the DHCP packets from the clients are allowed and verifies that no spoofing of information is occurring. It will also block any DHCP server response on untrusted port to prevent Rogue DHCP server response. The DHCP-snooping binding table contains the MAC address, IP address, lease time in seconds, and VLAN port information for the DHCP clients on the untrusted ports of a switch. The information that is contained in a DHCP-snooping binding table is removed from the binding table once its lease expires or DHCP snooping is disabled in the VLAN. Turn on DHCP snooping to prevent DoS attacks on the LAN facing interface of the Branch LAN switches or the NME modules on the ISR routers. This feature must be turn on to add the IP Source Guard feature which is described next.

IP Source Guard:

The IP source guard feature prevents IP spoofing by allowing only the IP addresses that are obtained through DHCP snooping on a particular port. Initially, all IP traffic on the port is blocked except for the DHCP packets that are captured by DHCP snooping. When a client receives a valid IP address from the DHCP server, a port access control list (PACL) is installed on the port that permits the traffic from the IP address. This process restricts the client IP traffic to those source IP addresses that are obtained from the DHCP server. Any IP traffic with a source IP address other than that in the PACL's permit list is filtered out. This filtering limits the ability of a host to attack the network by claiming a neighbor host's IP address. It is strongly recommended to enable IP Source Guard on the LAN facing interfaces of the Branch LAN network switches, or the NME on the ISRs.

Following is a sample CISF configuration on the cat 3750. The same configuration is applicable for the NME modules on the ISR routers:

```
! 3750 Global Commands for DHCP snooping and DAI c3750-i5-mz.122-20.SE.bin
ip dhcp snooping vlan 100
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan 100
! Error recovery timer set to one second for Port Security and DAI
errdisable recovery cause psecure-violation
errdisable recovery cause arp-inspection
errdisable recovery interval 60
! Interface commands for Port Security and IP Source Guard
interface GigabitEthernet1/0/2
switchport access vlan 100
switchport mode access
switchport port-security
switchport port-security maximum 3
switchport port-security aging time 2
switchport port-security aging type inactivity
ip verify source
ip dhcp snooping limit rate 15
! Interface Commands to Trust DHCP snooping and DAI
interface GigabitEthernet1/0/3
switchport access vlan 100
switchport mode access
ip arp inspection trust
ip dhcp snooping trust
```

4.3.2 IOS Router Integrated Security Features

IPS - To protect a Branch network from external attacks or intrusion, IPS features must be turned on the WAN facing interfaces of the ISR routers.

CBAC - For single-Tier, and Dual-Tier branch IOS FW features such as CBAC was configured on the IOS router to attain the stateful firewall functionality which enhances the security for the branch network significantly by reducing the chances for attacks from the intruders. For multi-tier branch ASA 5510 is recommended to configure to attain the stateful firewall capability. This offloading of security feature into a dedicated appliance such as ASA 5510 scales very well.

4.4 QoS

Successful implementation of per tunnel QoS on the hubs is critical for designing a scalable hub and spoke DMVPN network. If the GRE tunnel addresses for the spokes are static and known then they can be used to classify traffic per spoke for traffic shaping and then the IP TOS field can be used to classify traffic within this shaping for policing. The QoS classification is statically defined and applied on the physical interface.

Alternatively, if the data networks behind the spoke are known then that can be used to classify unicast-traffic that is destined for that spoke. This classification can be used in shaping on the outbound physical interface and a "child" policy can be used to police traffic within this shaping. Note that this will not be able to classify any multicast traffic per spoke since all multicast traffic would have the same source and destination IP address no matter which spoke it was destined for.

4.5 Wireless

Multicast over Wireless network:

When multicast is configured with PIM Sparse mode in a wireless network, the “ip pim parse-mode” command should be configured under both Management interface VLAN of Wireless LAN Controller (4404) and AP VLAN on Cat 6500. This allows the AP to join the 4404 Wireless Controller Multicast group. Otherwise, Multicast group join will not take place.

Hybrid REAP:

The Hybrid REAP solution is recommended for branch-office and remote-office deployments. It allows configuring and controlling two or three access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The Hybrid REAP access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller.

4.6 Multicast

PIM Sparse mode must be used over the DMVPN network for IP Multicast traffic. Because PIM bi-dir mode is not supported in point-multipoint interfaces deployment. The underlying routing protocol can be any IGP, however for the CVD System assurance testing EIGRP routing protocol was used.

IP multicast over DMVPN stresses hub routers, because hub routers need to replicate each IP multicast packet, one for each spoke that want to receive the packet. This replication takes place prior to GRE encapsulation and IPSec encryption. For example, a multicast stream of 256 Kbps traffic for 100 spokes would require encapsulating, encrypting of 25.6 Mbps of traffic by the hub routers. Multicast is not supported over dynamic spoke to spoke tunnel. Hence all multicast traffic traverses through the hubs either Hub to Spoke or spoke to spoke deployment models.

When running IP multicast over DMVPN you will need the following commands in addition to any other appropriate multicast commands:

Configure the following command on the tunnel interface of the spokes:

```
ip pim dr-priority 0
ip pim nbma-mode
ip pim sparse-mode
```

Configure the following command on the tunnel interface of the Hub routers:

```
ip pim dr-priority 2
ip pim nbma-mode
ip pim sparse-mode
```

If the multicast sources are behind the hub routers, then there is no special treatment required for the multicast deployment. However, if the IP multicast source is behind a spoke, then you must set it up so that the multicast packets go to the hub or through the hub and then turn around to go back out the hub, so the hub can do the replication and send it to the other spokes that want the multicast stream. For this, you must place the Rendezvous Point (RP) at or behind the hub.

If you have at least one source behind the spoke, you must enable the following global configuration commands on hub, and spokes:

Global configuration of the spokes:

To configure static RP configure the following command to define RP:

```
ip pim rp-address 192.168.1.1
```

Alternatively dynamic RP can be configured with the following command:

```
ip pim autorp listener
```

Disable switching to source-tree with the following command

```
ip pim spt-threshold infinity
```

Global Configuration command on the hubs:

To configure static RP, configure the following command:

```
ip pim rp-address 192.168.1.1
```

Alternatively dynamic RP can be configured with the following command:

```
ip pim autorp listener
```

If all IP multicast sources are behind the hubs, then the above commands are not required on the hubs or spokes. If the DMVPN deployment requires IP Multicast support, then do not configure DMVPN directly on the Cat6500 or C 7600 with MSFC or Sup720. Multicast traffic over DMVPN is not supported on the 6500/7600 when running DMVPN directly on the MSFC/Sup720. IP multicast traffic, however, to/from the 6500 and 7600 (Ex: Routing protocol traffic) is supported. However for scalable IPSec encryption if the design requires using Cat6500 or C7600, then use other platforms such as 7200VXR with NPE-G2 to perform mGRE, NHRP and routing protocol, while 6500/7600 is used to perform IPSec encryption.

4.7 VoIP

For successful VoIP deployment, proper Branch and WAN infrastructure design is extremely important. Deploying end-to-end QoS on all WAN links is critical for higher quality Voice.

WAN links should, when possible, be made redundant to provide higher levels of fault tolerance. Because of the potential for WAN links to fail or to become oversubscribed, it is recommended to deploy non-centralized resources as appropriate at sites on the other side of the WAN. Specifically, media resources, DHCP servers, voice gateways, and call processing applications such as Survivable Remote Site Telephony (SRST) and Cisco Unified Communications Manager Express (Unified CME) should be deployed at non-central sites when and if appropriate, depending on the site size and how critical these functions are to that site. Keep in mind that de-centralizing voice applications and devices can increase the complexity of network deployments, the complexity of managing these resources throughout the enterprise, and the overall cost of a the network solution. However, these factors can be mitigated by the fact that the resources will be available during a WAN link failure.

When deploying voice in a WAN environment, Cisco recommends the lower-bandwidth G.729 codec for any voice calls that will traverse WAN links because this practice will provide bandwidth savings on these lower-speed links.

Finally,the recommendation of the G.114 of the International Telecommunication Union (ITU) states that “the one-way delay in a voice network should be less than or equal to 150 milliseconds”. It is important to keep this in mind when implementing low-speed WAN links within a network. Topologies, technologies, and physical distance should be considered for WAN links so that one-way delay is kept at or below this 150-millisecond recommendation.

The deployment of an IP Communications system requires the coordinated design of a well structured, highly available, and resilient network infrastructure as well as an integrated set of network services including Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), and Network Time Protocol (NTP).

Cisco Unified Communications Manager (Unified CM) is the core call processing software for Cisco IP Telephony. It is best to place Cisco Unified Communications Manager (Unified CM) cluster servers, including media resource servers, in a data center or server farm environment.

4.8 Hardware and Software Device Information

Table 4-2 shows the Hardware platforms, Line cards, and software releases that were tested for the CVD System Assurance.

Table 4-2 Platform, Release and Service Modules

Harware Platform	Software Version	Line Cards/Interface
7206VXR w/ NPE-G2	12.4(15)T3	
Calyst 3750G	12.2(35)SE1	
3845 ISR router	12.4(15)T3, 12.2(35).SE2 on NME	NME-16ES-1G-P
3825 ISR router	12.4(15)T3, 12.2(35).SE2 on NME	NME-16ES-1G-P
2851 ISR router	12.4(15)T3	
Calyst 3560E	12.2(35)SE1	
877 ISR router	12.4(15)T3	
1801 ISR router	12.4(15)T3	
2811 ISR router	12.4(15)T3, 12.2(35).SE2 on NME	NME-16ES-1G-P
3745 ISR router	12.4(15)T3, 12.2(35).SE2 on NME	NME-16ES-1G-P
2801 ISR router	12.4(15)T3	
2821 ISR router	12.4(15)T3, 12.2(35).SE2 on NME	NME-16ES-1G-P
1841 ISR router	12.4(15)T3	
1812 ISR router	12.4(15)T3	
Calyst 2960G	12.2(35)SE1	
Calyst 6509	12.2(18)SXF12a	
Calyst 7609	12.2(33).SRC	
CSSC	4.1	
WLAN controller & module	4.1.171.0	
HWIC-AP-G-A	12.3.8-JA	
ASA	7.2(2)	

CHAPTER 5

References

The following design guides are used to design and configure the NG Branch test bed.

Next Generation Enterprise Branch Security Design Guide

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a00807593b6.pdf

Multicast over IPSec VPN Design Guide

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008074f26a.pdf

Enterprise Mobility 3.0 Design Guide

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/ccmigration_09186a00808118de.pdf

Cisco Unified Communications SRND Based on Cisco Unified CallManager 5.x

http://www/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a0080783d84.html

Cisco Unified CallManager Express Solution Reference Network Design Guide

http://www/en/US/products/sw/voicesw/ps4625/products_implementation_design_guide_book09186a00805f05db.html

Guide to Cisco Systems' VoIP Infrastructure Solution for SIP

http://www/en/US/tech/tk652/tk701/technologies_configuration_guide_book09186a00800eaa0e.html

Cisco IOS SIP Configuration Guide

http://www/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_book09186a00807517b8.html

This page is intentionally left blank

APPENDIX **A**

Test Coverage Matrix

A.1 Test Coverages Matrix

Table A-1 below clearly outlines of what was covered in CVD versus CVD System Assurance. The table lists all the features, platforms, and software versions for a Secured NG Branch Network.

Table A-1 CVD vs. CVD System Assurance coverage

Enterprise Branch Security Design	CVD	CVD System Assurance
Features		
Singele-Tier Branch	✓	✓
Dual-Tier Branch	✓	✓
Multi-Tier Branch	✓	✓
DMVPN	✓	✓
Hierarchical DMVPN Hub (Phase 3)		✓
Routing Protocol (EIGRP)	✓	✓
QoS: LLQ, CBWFQ, WRED	✓	✓
Multicast		✓
VoIP		✓
Redundancy	✓	✓
Wireless		✓

Table A-2 CVD vs. CVD System Assurance coverage Platform and Software coverage

CVD		
Role	**Platform**	**Software**
Hub	7206VXR	N/A
Hub	ISR 3845	N/A
Hub	C7600	N/A
Hub	Cat 6509	N/A
Spoke	ISRs	12.4(7.7)T

Catalyst Switches	Cat 3750	12.2(25)SEE
Firewall	ASA 5510	7.0(4)
CVD System Assurance		
Hub	7206VXR	12.4(15)T3
Hub	ISR 3845	12.4(15)T3
Hub	Cat 6509	12.2(18)SXF12a
Hub	C6700	12.2(33)SRC
Spoke	R Routers & 7206VXR	12.4(15)T3
Catalyst Switches	Cat 3750 & 3560	122-35.SE1
Firewall	ASA 5510	7.2(2)

APPENDIX **B**

Test Case Descriptions and Results

Table B-1 summarizes the test results for the Next Generation Enterprise Branch Security Design.

Table B-1 Test Results Summary for NG Branch network CVD System Assurance testing

Test Type	Test Cases	Test Results		
		Pass	Pass with Exception	Fail
Feature Combination	48	48	0	0
Feature Interactions	43	40	0	1
Negative	21	21	0	0
Scalability	4	4	0	0
Reliability	1	1	0	0
Total	117	114	0	1
	100%	97%	0%	1%

B.1 System Integration Tests

All test cases that were executed under the Systems Integration Test suite are listed in Table B-2.

Table B-2 System Integration test cases and results

Test	Manual Test Case	Defects	Automation Test Case	Defects
DMVPN Test Suites				
DMVPN Route Summary The test case objective is to verify the summarization of the routing protocol updates from hub to spokes as described in [6]. According to the DMVPN phase3 guidelines, the spokes are no longer required to maintain an individual route (with an IP next-hop of the tunnel IP address of the remote spoke) for the Networks that access all the other spokes. This way, each spoke can use summarized routes or specific routes (with an IP next-hop of the tunnel IP address of the hub) in order to build direct spoke-to-spoke tunnels. The immediate benefit of the summarization is noticeable on the distribution hub routers that are no longer required to advertise all the individual spoke routes. Instead of the distribution hub router is advertising a summary route to each spoke. The test configures the hubs and spokes and verifies the spoke IPSec tunnels and routing performed by the distribution hubs.	Pass	—	Pass	—
DMVPN Hierarchical Architecture This test case verifies that DMVPN hub and spoke architecture is operating correctly in a DMPVN Phase 3 Hierarchical network. This test case is only applicable to DMVPN cloud spokes connected to a 7206 or 3845 DMVPN hub. This test case is run in a Branch test network environment setup and will be run sequentially with other test cases within this test suite. Device configuration used for this test case will have feature combination and feature interaction with configuration from other test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—

DMVPN Spoke to Spoke This test verifies the spoke-to-spoke dynamic tunnel creation and direct path accessibility wih VoIP traffic for spokes that are part of the same DMVPN cloud, for both "same hub spokes" and "different hub spokes" cases. This test case is run in a Branch test network environment setup and will be run sequentially with other test cases within this test suite. A Device configuration used for this test case will have feature combination and feature interaction with configurations from other test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—
DMVPN Lifetime The objective is to verify the correct setup for the IKE and IPSec Security Association lifetime. We plan to set the IKE SA lifetime to 8 hours (28800 seconds) and the IPSec SA lifetime to 4 hours (14400 seconds) for all the DMVPN hubs and spokes. This test case is run in a Branch test network environment setup and will be run sequentially with other test cases within this test suite. A device configuration used for this test case will have feature combination and feature interaction with configurations from other test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—
DMVPN AES This test verifies the utilization of the Advanced Encryption Standard (AES) and the hardware accelerator encryption engine (AIM-VPN/SSL-X, where X is a hardware dependent integer) throughout the DMVPN cloud (hub and spokes). The test case applies to the entire DMVPN cloud (hubs and spokes) covered by the following hubs: 3845i, 7206i, 6506i, and 7609i.	Pass	—	Pass	—
Routing Protocol Test Suite				

EIGRP Neighbors Authentication This test case will set up and verify that the EIGRP neighbor relationship is established between each adjacent router across the network. This test case runs in parallel with other test cases within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Voice and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—
EIGRP Stub Routing This test case will set up and verify EIGRP stub routing on the DMVPN spoke routers. In the Enterprise NG Branch design, configuring the EIGRP stub feature on the spoke routers prevents the hub routers from sending downstream queries, which helps the convergence time. This test case run in NG Branch test network environment and will run in parallel with other test cases within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as Voice and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—
EIGRP Route Filters This test case will set up and verify that the EIGRP route filtering is applied on the head-end routers to ensure that the branch router has a default route (gateway) to the remote network as well as a reduced routing table. This test case runs in parallel with other test cases within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Voice and Multicast test suites. This test case will run With traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—

EIGRP Neighbors Stability This test case will set up and verify that a stable EIGRP neighbor relationship is established. This test case runs in parallel with other test cases within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Voice and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—
Security Test Suite				
CISF Port Security Port security is used to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed access to the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port. Port Security will be tested on all access ports, but will not be tested on voice ports. This is because VoIP traffic will be simulated with Abacus tools with random MAC address, which generate Security violation when port security is turned on. To avoid these false positives VoIP ports will not be tested for Port Security. This test case is run in the Branch test network environment setup and will be run in serial within this test suite. A Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, multicast traffic, and voice traffic.	Pass	—	Pass	—

CISF – Dynamic ARP Inspection The purpose of this test is to verify the functionality of the Dynamic ARP Inspection (DAI) feature. DAI uses the binding information that is built by DHCP snooping to enforce the advertisement of bindings to prevent "man-in-the-middle" attacks. These attacks can occur when an attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entries in a communication association. DAI adds an extra layer of security to Address Resolution Protocol (ARP) inspection by verifying that the ARP packet's MAC address and IP address match an existing DHCP snooping binding in the same VLAN. The basic functionality and packet flow of ARP inspection remains unchanged except for the addition of checks to ensure that a DHCP binding exists. This test case is run in the Branch test network environment setup and will be run in serial within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, multicast traffic, and voice traffic	Pass	—	Pass	—

CISF – DHCP Snooping DHCP snooping provides security against DoS attacks that are launched using DHCP messages by filtering the DHCP packets and building and maintaining a DHCP-snooping binding table. DHCP snooping uses both trusted and untrusted ports. DHCP packets that are received from a trusted port are forwarded without validation. Typically, trusted ports are used to reach a DHCP server or relay agent. When the switch receives the DHCP packets from an untrusted port, DHCP snooping validates that only the DHCP packets from the clients are allowed and verifies that no spoofing of information is occurring. It will also block any DHCP server response on untrusted port to prevent Rogue DHCP server response. The DHCP-snooping binding table contains the MAC address, IP address, lease time in seconds, and VLAN port information for the DHCP clients on the untrusted ports of a switch. The information that is contained in a DHCP-snooping binding table is removed from the binding table once its lease expires or DHCP snooping is disabled in the VLAN. This test case is run in the Branch test network environment setup and will be run in serial within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, multicast traffic, and voice traffic.	Pass	—	Pass	—
CISF – IP Source Guard The purpose of this test is to verify the functionality of the IP source guard feature. The IP source guard feature prevents IP spoofing by allowing only the IP addresses that are obtained through DHCP snooping on a particular port. Initially, all IP traffic on the port is blocked except for the DHCP packets that are captured by DHCP snooping. When a client receives a valid IP address from the DHCP server, a port access control list (PACL) is installed on the port that permits the traffic from the IP address. This process restricts the client IP traffic to those source IP addresses that are obtained from the DHCP erver. Any IP traffic with a source IP address other than that in the PACL's permit list is filtered out. This filtering limits the ability of a host to attack the network by claiming a neighbor host's IP address.	Pass	—	Pass	—
QoS Test Suite				

QoS – Scavenger Class The test will verify correct operability of Network Based Application Recognition (NBAR) to identify scavenger applications and use the MQC feature to set the appropriate DSCP value and limit the Scavenger Class to a bandwidth of 1%. This test case is run in branch test network environment setup and will be run in serial within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configuration information from other test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic,multicast traffic, and voice traffic.	Pass	—	Pass	—
QoS – Frame Relay Traffic Shaping This test will verify the correct operability of Class-Based Frame Relay Traffic-Shaping. Class-Based Frame relay traffic-shaping will be implemented on the Frame Relay WAN links. The CIR will be set to 95% of the PVC due to the fact that the FRTS mechanism does not take the Frame Relay overhead (headers and CRCs) into account in its calculations. This test case is run in branch test network environment setup and will be run in serial within this test suite. A Device configuration information used for this test case will have feature combination and feature interaction with configuration information from other test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, multicast traffic, and voice traffic.	Pass	—	Pass	—
QoS Lifetime On the DMVPN hubs (3845, 7206), Per Site QoS will be configured to manage congestion and guarantee bandwidth to a specific site. A class-map will be used to match a peer destination address. This test case is run in branch test network environment setup and will be run in serial within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configuration information from other test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, multicast traffic, and voice traffic.	Fail	CSCsj33060	Fail	CSCsj33060

QoS – MQC Verify that the modular QoS CLI is working correctly on the various branch platforms by demonstrating the correct operability of the arious queueing mechanisms. Traffic will be generated with the appropriate DSCP values for a specific map-class and the bandwidth percentage on the policy map verified. This test case is run in branch test network environment setup and will be run in serial within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configuration information from other test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, multicast traffic, and voice traffic.	Pass	—	Pass	—
DMVPN Spoke QoS On the DMVPN hubs (3845, 7206), Per Site QoS will be configured to manage congestion and guarantee bandwidth to a specific site. A class-map will be used to match a peer destination address. This test case is run in branch test network environment setup and will be run in serial within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configuration information from other test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, multicast traffic, and voice traffic.	Pass	—	Pass	—
Wireless Test Suite				

2006 Verification This test case will configure the 2006 controller and verify that it functions as expected. The Cisco 2006 Wireless LAN Controller works in conjunction with Cisco Lightweight Access Points to provide system-wide Wireless LAN functions. It controls up to six lightweight access points for multi controller architectures typical of enterprise branch deployments. It may also be used for single-controller deployments for small- and medium-sized business environments. This test case is run in the NG Branch test network environment setup and will be run in parallel within this test suite. Device configuration used for this test case will have feature combination and feature interaction with configurations from the Routing andMulticast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—
4404 Controller Verification This test case configures the 4404 Wireless Controller and verifies that it functions as expected. It works in conjunction with the Cisco Lightweight Access Points protocol (LWAPP) to support Wireless data, voice, and video applications. This test case will verify that the 4404 Wireless Controller can manage the LWAPP access points. This test case is run in the NG Branch test network environment setup and will be run in parallel within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from the Routing and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—

3750G Wireless Controller Verification The Cisco 3750G Integrated Wireless LAN Controller integrates Wireless LAN controller functions into the Cisco Catalyst 3750G Series Switches and delivers centralized security policies, Wireless intrusion prevention system (IPS) capabilities, RF management, QoS, and Layer 3 fast secure roaming for WLANs. This test case configures the 3750G Wireless Controller verifies that it can manage the LWAPP access points and support Wireless data, voice, and video applications. This test case is run in the NG Branch test network environment setup and will be run in parallel within this test suite. Device configuration used for this test case will have feature combination and feature interaction with configurations from the Routing andMulticast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—

Wireless LAN Controller Modules (WLCMs) Verification Cisco Wireless LAN Controller Modules (WLCMs), supported on the Cisco Integrated Services routers (ISR), provide an easy-to-deploy, cost-effective branch office or small- to medium-business Wireless solution. As a component of the Cisco Unified Wireless Network, the Cisco WLCMs give network administrators the visibility and control necessary to effectively and securely manage business-class Wireless LANs and mobility services. This test case configures the WLCM controller and verifies that it works in conjunction with the Cisco Lightweight Access Points protocol (LWAPP) to support Wireless data, voice, and video applications. This test case is run in the NG Branch test network environment setup and will be run in parallel within this test suite. Device configuration used for this test case will have feature combination and feature interaction with configurations from the Routing and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—

HWIC-AP WLAN Module Verification The Cisco HWIC-AP 802.11G and HWIC-AP 802.11A/B/G are Wireless LAN interface cards in the High-Speed WAN Interface Card (HWIC) form factor that provide integrated access point functionality in the Cisco 1800 (Modular), Cisco 2800, and Cisco 3800 Integrated Services Routers. Enterprise branch office and small- to medium-business customers can run concurrent services of Layer 3 routing, security, Layer 2 switching, and now IEEE 802.11 Wireless LAN functionality in a single platform. This combination offers ease of configuration, deployment, and management while delivering high performance, security, and rich set of services. This test case verifies that HWIC-AP modules work in conjunction with Cisco Wireless Controllers to provide system-wide Wireless LAN functions anddata/voice/video traffic. This test case is run in the NG Branch test network environment setup and will be run in parallel within this test suite. Device configuration used for this test case will have feature combination and feature interaction with configurations from the Routing and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—

Hybrid REAP Verification Hybrid REAP is a solution for branch-office and remote-office deployments. It enables customers to configure and control two or three access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The Hybrid REAP access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller. This test case will verify that Hybrid REAP works as expected in the enterprise branch networks. This test case is run in the NG Branch test network environment setup and will be run in parallel within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from the Routing and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—
Dot1x Authentication This test case verifies that a CSSC client can successfully authenticate using Dot1x protocol and can transmit/received Wireless data traffic across a branch network. This test case is run in the NG Branch test network will be run in parallel within this test suite. Device configuration used for this test case will have feature combination and feature interaction with configurations from the Routing and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—
Multicast Test Suite				

Multicast PIM Sparse-mode Test The purpose of this test is to verify the successful delivery of Multicast PIM Sparse-Mode Traffic via a DMVPN Hierarchical network to a branch router. The Multicast traffic will be sent on group 239.254.200.1 at a rate of 100 pps.This test case runs in parallel with other test cases within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Voice and QoS test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—
AutoRp Listener Test The objective of this test is to verify that the RP for a Multicast group can be dynamically learned for the branch network using the “ip pim autorp listener” command. This test will not occur for branches connected to 6500 or 7600 hubs due to platform limitations. This test case runs in parallel with other test cases within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Voice and QoS test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—
Multicast SSM Test The purpose of this test is to verify the correct reception of SSM Multicast traffic on a DVMPN branch router. This test case runs in parallel with other test cases within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Voice and QoS test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—

Multicast IGMP v3 access list The objective of this test is to verify thecorrectoperability of IGMP v3 and controlling access to SSM Groups. This test case runs in parallel with other test cases within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Voice and QoS test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—
VOIP Test Suite				
Inter Branch CCME Failover Test CCME Failover is executed with Intra Branch VoIP calls using Cisco Call Manager Express (CCME) with Skinny Client Control Protocol (SCCP) are executed in Branches 8, 10, and 13. In this test, the Abacus VoIP traffic/quality generation/verification test tool Branch 13 routers are configured as Cisco Call Manager Express using SCCP protocol. The endpoints are configured as follows: - 10 SCCP end-points (IP phones) for b13-3825 primary - 10 SCCP endpoints (IP phones) for b13-3825 secondary Out of the 10 endpoints, 5 are set up as originating and 5 as terminating endpoints. The Branch routers will also have configurations from other test suites, such as Routing, QoS, Security, and Multicast. There will be background traffic including stateful, stateless, and multicast traffic.	Pass	—	Pass	—

Inter Branch Delay Measurement with CME Average one-way delay measurements are executed on Inter Branch VoIP calls using Cisco Call Manager Express (CCME) with Skinny Client Control Protocol (SCCP). Branches 8, 10 and 13 routers are configured as Cisco Call Manager Express using SCCP protocol. The endpoints are configured as follows: - 10 SCCP end-points (IP phones) for b8-3745 - 10 SCCP end-points (IP phones) for b10-2821 - 10 SCCP end-points (IP phones) for b13-3825 The Branch routers will also have configurations from other test suites, such as Routing, QoS, Security, and Multicast. There will be background traffic including stateful, stateless, and multicast traffic. Abacus ICG card will set up VoIP traffic channel streams as follows: Channel 1: 10 SCCP calls between b8-3745 and b10-2821 Channel 2: 10 SCCP calls between b10-2821 and b13-3835	Pass	—	Pass	—

Inter Branch Jitter Measurement with CME Jitter measurements are executed on Inter Branch VoIP calls using Cisco Call Manager Express (CCME) with Skinny Client Control Protocol (SCCP). Branches 8, 10, and 13 routers are configured as Cisco Call Manager Express using SCCP protocol. The endpoints are configured as follows: - 10 SCCP end-points (IP phones) for b8-3745. - 10 SCCP end-points (IP phones) for b10-2821. - 10 SCCP end-points (IP phones) for b13-3825. The Branch routers will also have configurations from other test suites, such as Routing, QoS, Security, and Multicast. There will be background traffic including stateful, stateless, and multicast traffic. Abacus ICG card will set up VoIP traffic channel streams as follows: Channel 1: 10 SCCP calls between b8-3745 and b10-2821 Channel 2: 10 SCCP calls between b10-2821 and b13-3835	Pass	—	Pass	—

Inter Branch Jitter with CCM Device configuration information used for his test case will have feature combination and feature interaction with configurations from other test suites, such as the Routing, QoS, Security, and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, and multicast traffic. RTP jitter is measured during the interval between the sending of two RTCP packets. In this test, the Abacus VoIP traffic/quality generation/verification test tool will be used to emulate: - 5 SIP end-points (IP phones) for b1-7206 - 5 SIP end-points (IP phones) for b2-3845 - 5 SIP end-points (IP phones) for b6-1801 - 5 SIP end-points (IP phones) for b7-2811 Abacus will also generate corresponding number of VoIP call signaling and Real-Time Transport Protocol (RTP) traffic streams between branches for 10 times. - 5 SIP end-points (IP phones) between b1-7206 and b6-1801 - 5 SIP end-points (IP phones) between b2-3845 and b7-2811 Average RTP jitter should be less than 50 ms. To achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in branch should be working and functioning properly.	Pass	—	Pass	—

Inter Branch Media Transport Delay with CCM This test case will run in the Enterprise Branch test network environment setup. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Routing, QoS, Security, and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, and multicast traffic. One-Way Delay (OWD) measures time interval between the time a voice pattern leaves the transmitting device and the time reaches the receiving device. The accuracy of this measurement is A±2 ms, and the resolution is 1. In Simplex mode, the number of measurements for one-way delay on a channel should equal the number of PSQM values. In this test, Abacus VoIP traffic/quality generation/verification test tool will be used to emulate: - 5 SIP end-points (IP phones) for b1-7206 - 5 SIP end-points (IP phones) for b2-3845 - 5 SIP end-points (IP phones) for b6-1801 - 5 SIP end-points (IP phones) for b7-2811 Abacus will also generate corresponding number of VoIP call signaling and Real-Time Transport Protocol (RTP) traffic streams between branches for 10 times. - 5 SIP end-points (IP phones) between b1-7206 and b6-1801 - 5 SIP end-points (IP phones) between b2-3845 and b7-2811 Average one-way delay should be less than100 ms. To achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in branch should be working and functioning properly.	Pass	—	Pass	—

Inter Branch PSQM Quality of Voice with CCM This test case will run in the Enterprise Branch test network environment setup. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Routing, QoS, Security, and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, and multicast traffic. The PSQM algorithm uses a psychoacoustic model that aims to mimic the perception of sound in real life. The algorithm functions by comparing the original signal with the signal that was sent and received. PSQM provides an output in the range 0 to 6.5, where 0 indicates a good channel, and 6.5 indicates a very bad channel. If the input and output are identical, the algorithm is designed to produce a perfect score. Similarly, the objective is that if the input and output have inaudible differences, the score should not be degraded. In this test, the Abacus VoIP traffic/qualitygeneration/verification test tool will be usedto emulate: - 5 SIP end-points (IP phones) for b1-7206 - 5 SIP end-points (IP phones) for b2-3845 - 5 SIP end-points (IP phones) for b6-1801 - 5 SIP end-points (IP phones) for b7-2811 Abacus will also generate corresponding number of VoIP call signaling and Real-Time Transport Protocol (RTP) traffic streams between branches for 10 times. - 5 SIP end-points (IP phones) between b1-7206 and b6-1801 - 5 SIP end-points (IP phones) between b2-3845 and b7-2811 Total Call Success Rate (CSR) should be greater than 99%. To achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in branch should be working and functioning properly.	Pass	—	Pass	—

Inter Branch PSQM Voice Quality Measurement with CME Perceptual Speech Quality Measurements (PSQM) are executed on Inter Branch VoIP calls using Cisco Call Manager Express (CCME) with Skinny Client Control Protocol (SCCP). Branches 8, 10 and 13 routers are configuredas Cisco Call Manager Express using SCCP protocol. The endpoints are configured as follows: - 10 SCCP end-points (IP phones) for b8-3745. - 10 SCCP end-points (IP phones) for b10-2821. - 10 SCCP end-points (IP phones) for b13-3825. The Branch routers will also have configurations from other test suites, such as Routing, QoS, Security, and Multicast. There will be background traffic including stateful, stateless, and multicast traffic. Abacus ICG card will set up VoIP traffic channel streams as follows: Channel 1: 10 SCCP calls between b8-3745 and b10-2821 Channel 2: 10 SCCP calls between b10-2821 and b13-3835	Pass	—	Pass	—

Inter Branch SCCP to SCCP with CCM This test case will run in the Enterprise Branch test network environment setup and will run in parallel with "Intra Branch SCCP to SCCP with CCM". Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Routing, QoS, Security, and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, and multicast traffic. In this test, Abacus VoIP traffic/quality generation/verification test tool will be used to emulate: - 5 SCCP end-points (IP phones) for b1-7206 - 5 SCCP end-points (IP phones) for b2-3845 - 5 SCCP end-points (IP phones) for b6-1801 - 5 SCCP end-points (IP phones) for b7-2811 Abacus will also generate corresponding number of VoIP call signaling and Real-Time Transport rotocol (RTP) traffic streams between branches for 10 times. - 5 SCCP end-points (IP phones) between b1-7206 and b6-1801 - 5 SCCP end-points (IP phones) between b2-3845 and b7-2811 Total Call Success Rate (CSR) should be reater than 99%. To achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in branch should be working and functioning properly.	Pass	—	Pass	—

Inter Branch SCCP to SCCP with CME Inter Branch VoIP calls using Cisco Call Manager Express (CCME) with Skinny Client Control Protocol (SCCP) are executed in Branches 8, 10, and 13. In this test, the Abacus VoIP traffic/quality generation/verification test tool Branches 8, 10, and 13 routers are configured as Cisco Call Manager Express using SCCP protocol. The endpoints are configured as follows: - 10 SCCP end-points (IP phones) for b13-3825 The Branch routers will also have configurations from other test suites, such as Routing, QoS, Security, and Multicast. There will be background traffic including stateful, stateless, and multicast traffic. Abacus ICG card will set up VoIP traffic channel streams as follows: Channel 1: 10 SCCP calls between b8-3745 and b10-2821 Channel 2: 10 SCCP calls between b10-2821 and b13-3835	Pass	—	Pass	—

Inter Branch SCCP to SIP Testing with CME Inter Branch VoIP calls are executed between Cisco Call Manager Express (CCME) configured with Skinny Client Control Protocol (SCCP) and Cisco Call Manager Express (CCME) configured with Session Initiation Protocol (SIP). Branches 8, 10, and 13 routers are configured as Cisco Call Manager Express using SCCP protocol. The endpoints are configured as follows: - 1 SCCP end-points (IP phones) for b8-3745 - 1 SCCP end-points (IP phones) for b10-2821 - 1 SCCP end-points (IP phones) for b13-3825 Branches 9 and 14 routers are configured as Cisco Call Manager Express using SIP protocol. A SIP IP phones are registered on each of the branch routers. The Branch routers will also have configurations from other test suites, such as Routing, QoS, Security, and Multicast. There will be background traffic including stateful, stateless, and multicast traffic. Abacus ICG card will set up VoIP traffic channel streams as follows: Channel 1: 1 SCCP calls to b8-3745 Channel 2: 1 SCCP calls to b10-2821=	Pass	—	Pass	—

Inter Branch SIP to SCCP and SIP to SCCP with CCM This test case is run in the Enterprise Branch test network environment setup and will run in serial with other test cases within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Routing, QoS, Security, and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, and multicast traffic. In this test, Abacus VoIP traffic/quality generation/verification test tool will be used to emulate: - 5 SCCP end-points (IP phones) for b1-7206 - 5 SCCP end-points (IP phones) for b2-3845 - 5 SCCP end-points (IP phones) for b6-1801 - 5 SIP end-points (IP phones) for b3-3825 - 5 SIP end-points (IP phones) for b4-2851 - 5 SIP end-points (IP phones) for b11-1841 Abacus will generate 10 SIP-to-SCCP and 5 SCCP-to-SIP VoIP call signaling and Real-Time Transport Protocol (RTP) traffic streams over the campus for 10 times. Total Call Success Rate (CSR) should be greater than 99%. To achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in branch should be working and functioning properly.	Pass	—	Pass	—

Inter Branch SIP to SIP with CCM Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Routing, QoS, Security, and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, and multicast traffic. In this test, the Abacus VoIP traffic/quality generation/verification test tool will be used to emulate: - 10 SIP end-points (IP phones) for b3-3825 - 5 SIP end-points (IP phones) for b4-2851 - 5 SIP end-points (IP phones) for b11-1841 Abacus will also generate corresponding number of VoIP call signaling and Real-Time Transport Protocol (RTP) traffic streams between branches for 10 times: - 5 SIP calls between b3-3825 and b4-2851 - 5 SIP calls between b3-3825 and b11-1841 Total Call Success Rate (CSR) should be greater than 99%. To achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in branch should be working and functioning properly.	Pass	—	Pass	—
Inter Branch SIP to SIP with CME Device configuration information used for this test case will have feature combinationand feature interaction with configurations from other test suites, such as the Routing, QoS, Security, and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, and multicast traffic. The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. SIP clients use TCP or UDP typically using port 5060 to connect to SIP servers and other SIP endpoints. SIP is primarily used in setting up and tearing down voice or video calls. However, it can be used in any application where session initiation is a equirement. These include event subscription and notification, terminal mobility, and so on.	Pass	—	Pass	—

Inter Branch SRTP with CCM This test case will run in the Enterprise Branch test network environment setup and will run in serial with other test cases within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Routing, QoS, Security, and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, and multicast traffic. The Secure Real-time Transport Protocol (or SRTP) defines a profile of Real-Time Transport Protocol (RTP), intended to provide encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast application. For encryption and decryption of the data flow (hence providing confidentiality of the data flow), SRTP (with SRTCP) standardizes utilization of only a single cipher. This cipher is AES and it can be used in two cipher modes, which turn the original block AES cipher into a stream cipher: To authenticate the message and protect its integrity, the HMAC-SHA1 algorithm (defined in RFC 2104) is used, which produces a 160-bit result that is then truncated to 80 bits to become the authentication tag appended to the packet. In this test, the Abacus VoIP traffic/quality generation/verification test tool will be used to emulate: - 10 SIP end-points (IP phones) for b3-3825 - 5 SIP end-points (IP phones) for b4-2851 - 5 SIP end-points (IP phones) for b11-1841 Abacus will also generate corresponding number of VoIP call signaling and Real-Time Transport Protocol (RTP) traffic streams between branches for 10 times: - 5 SIP calls between b3-3825 and b4-2851 - 5 SIP calls between b3-3825 and b11-1841 Total Call Success Rate (CSR) should be greater than 99%. To achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in branch should be working properly	Pass	—	Pass	—

Intra Branch SCCP to SCCP with CCM This test case will run in the Enterprise Branch test network environment setup. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Routing, QoS, Security, and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, and multicast traffic. SCCP (Skinny Client Control Protocol) is a proprietary terminal control protocol owned and defined by Cisco Systems, Inc. as a messaging set between a skinny client and the Cisco Call Manager. Examples of skinny clients include the Cisco 7900 series of IP phone and the 802.11b wireless Cisco 7920. Skinny is a lightweight protocol that allows for efficient communication with Cisco Call Manager. Call Manager acts as a signaling proxy for call events initiated over other common protocols such as H.323, SIP, ISDN, and/or MGCP. A skinny client uses TCP/IP to and from one or more Call Managers in a cluster. RTP/UDP/IP is used to and from a similar skinny client or H.323 terminal for the bearer traffic Real-Time audio stream). In this test, the Abacus VoIP traffic/quality generation/verification test tool will be used to emulate: - 240 SCCP end-points (IP phones) for b1-7206 - 240 SCCP end-points (IP phones) for b2-3845 - 18 SCCP end-points (IP phones) for b6-1801 - 36 SCCP end-points (IP phones) for b7-2811 Abacus will also generate corresponding number of VoIP call signaling and Real-Time Transport Protocol (RTP) traffic streams within branches for 10 times. Total Call Success Rate (CSR) should be greater than 99%. To achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in branch should be working andfunctioning properly.	Pass	—	Pass	—

Intra Branch SCCP to SCCP with CME Intra Branch VoIP calls using Cisco Call Manager Express (CCME) with Skinny Client Control Protocol (SCCP) are executed in Branches 8, 10, and 13. In this test, the Abacus VoIP traffic/quality generation/verification test tool	Pass	—	Pass	—
Intra Branch SIP to SIP with CCM Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Routing, QoS, Security, and Multicast test suites. This test case will run with traffic streams flowing in the background that includes statefultraffic, stateless traffic, and multicast traffic. The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. SIP clients use TCP or UDP typically using port 5060 to connect to SIP servers and other SIP endpoints. SIP is primarily used in setting up and tearing down voice or video calls. However, it can be used in any application where session initiation is a requirement. These include event subscription and notification, terminal mobility, and so on. In this test, the Abacus VoIP traffic/quality generation/verification test tool will be used to emulate: - 168 SIP end-points (IP phones) for b3-3825 - 96 SIP end-points (IP phones) for b4-2851 - 18 SIP end-points (IP phones) for b11-1841 Abacus will also generate corresponding number of VoIP call signaling and Real-Time Transport Protocol (RTP) traffic streams within branches for 10 times. Total Call Success Rate (CSR) should be greater than 99%. To achieve the goal, all technology aspects of layer 2, IP routing, QoS, and security in branch should be working and functioning properly.	Pass	—	Pass	—

Intra Branch SIP to SIP with CME Intra Branch VoIP calls using Cisco Call Manager Express (CCME) with Session Initiation Protocol (SIP) are executed in Branches 9 and 14. In this test, regular Cisco SIP Phones are used to test calls. Branches 9 and 14 routers are configured as Cisco Call Manager Express using SIP protocol. The Branch routers will also have configurations from other test suites, such as Routing, QoS, Security and Multicast. There will be background traffic including stateful, stateless, and multicast traffic. Two SIP IP phones are registered on each of the branch routers SIP phones are used to make calls as follows: - 5 SIP calls are executed between the sip phones on b9-2801 - 5 SIP calls are executed between the sip phones on b14-3845	Pass	—	Pass	—

Intra Branch SIP Video with CCM This test case will run in the Enterprise Branch test network environment setup and will run in serial with other test cases within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Routing, QoS, Security, and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, and multicast traffic. H.264/AVC/MPEG-4 Part 10 contains a number of new features that allow it to compress video much more effectively thanolder standards and to provide more flexibility for application to a wide variety of network environments. H.264 is supported with Cisco 7900 Video IP Phones. In this test, the Abacus VoIP traffic/quality generation/verification test tool will be used to emulate: - 10 SIP end-points (IP phones) for b3-3825 - 10 SIP end-points (IP phones) for b4-2851 - 2 SIP end-points (IP phones) for b11-1841 Abacus will also generate corresponding number of SIP Video call signaling and H.264 Real-Time Transport Protocol (RTP) traffic streams within branches for 10 times. Total Call Success Rate (CSR) should exceed 99% and packet loss should be less than 5%. To achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in branch should be working and functioning properly.	Pass	—	Pass	—

Intra Branch SRST This test case will run in the Enterprise Branch test network environment setup. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Routing, QoS, Security, and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, and multicast traffic. Survivable Remote Site Telephony (SRST) provides Cisco Call Manager with fallback support for Cisco IP phones that are attached to a Cisco router on your local network. Cisco SRST enables routers to provide call-handling support for Cisco IP phones when they lose connection to remote primary, secondary, or tertiary Cisco Call Manager installations or when the WAN connection is down. In this test, the Abacus VoIP traffic/quality generation/verification test tool will be used to emulate: - 240 SCCP end-points (IP phones) for b1-7206 - 240 SCCP end-points (IP phones) for b2-3845 - 18 SCCP end-points (IP phones) for b6-1801 - 36 SCCP end-points (IP phones) for b7-2811 After CCM becomes unavailable, Abacus will also generate corresponding number of VoIP call signaling and Real-Time Transport Protocol (RTP) traffic streams within branches for 10 times. Total Call Success Rate (CSR) should be greater than 99%. To achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in branch should be working and functioning properly.	Pass	—	Pass	—

B.2 Scalability Tests

Table B-3 shows the DMVPN Hubs scalability results with the corresponding test cases.

Table B-3 DMVPN scalability test cases and results

Test	Manual Test Case	Defects	Automation Test Case	Defects
DMVPN Scalability Test Suite				
3845 DMVPN Scalability The objective of this test is to verify that 800 DMVPN spokes have been successfully established on a DMVPN hub.	Pass	—	Pass	—
7206 DMVPN Scalability The objective of this test is to verify that 800 DMVPN spokes have been established on a DMVPN hub.	Pass	—	Pass	—
6506 DMVPN Scalability The objective of this test is to verify that 400 DMVPN spokes have been established on a MVPN hub.	Pass	—	Pass	—
7609 DMVPN Scalability The objective of this test is to verify that 800 DMVPN spokes have been established on a DMVPN hub.	Pass	—	Pass	—

B.3 Negative Tests

Table B-4 shows the results for Negative test suite.

Table B-4 Negative test cases and results

Test	Manual Test Case	Defects	Automation Test Case	Defects
Negative Test Suites				
Convergence Tests with Link Failures The purpose of this test is to determine, when the primary WAN link fails, what level of disruption of network connectivity occurs on the device and the network when switchover takes place. In addition, the system experiencing a link that goes down and up should still have normal CPU utilization and there should be no memory leak, traceback, or CPU hog etc. This test case is run in NG Branch test network environment setup and will be run in serial within this test suite. Device configuration used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Routing and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—

Convergence Tests with Router Failures The purpose of this test is to determine, if the primary branch router goes down, how long it will take for the backup branch router to take over and what level of disruption of network connectivity occurs on the branch network. The expected result is that after the primary branch router comes back up, the routing table will resume. In addition, the system experiencing the switchover scenario should still have normal CPU utilization and there should be no memory leak, traceback, or CPU hog etc. This test case is run in NG Branch test network environment setup and will be run in serial within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Routing and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—
High Availability Test with ASA Failover The purpose of this test is to determine, when the primary ASA firewall goes down, how long it will take for the secondary ASA to take over and what level of disruption of network connectivity occurs on the network. The expected result is that after the primary ASA comes back up, the routing table will resume. In addition to that, the systems experiencing the ASA switchover scenario should still have normal CPU utilization and there should be no memory leak, traceback, or CPU hog etc. This test case is run in NG Branch test network environment setup and will be run in serial within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configuration information from other test suites, such as the Routing and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	N/A	—

IPSec Tunnel Shut - No Shut The purpose of this test is to determine, if the primary IPSec tunnel goes down, how long it will take for the secondary IPSec tunnel to take over and what level of disruption of network connectivity occurs on the branch network. The expected result is that after the primary IPSec tunnel comes back up, therouting table will resume. In addition, the systems experiencing the IPSec tunnel down-up scenario should still have normal CPU utilization and there should be no memory leak, traceback, or CPU hog etc. This test case is run in NG Branch test network environment setup and will be run in serial within this test suite. Device configuration information used for this test case will have feature combination and feature interaction with configuration information from other test suites, such as the Routing and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—
Adding and Deleting ACLs The purpose of this test is to verify that adding/deleting the ACLs won't disrupt network connectivity on the branch network. The expected result is that the systems experiencing the add/delete ACLs should stillhave normal CPU utilization and there should be no memory leak, traceback, or CPU hog etc. This test case is run in NG Branch test network environment setup and will be run in serial within this test suite. Device configuration used for this test case will have feature combination and feature interaction with configurations from other test suites, such as the Routing and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic.	Pass	—	Pass	—

B.4 Reliability Tests

Table B-5 shows the results of 120 Hour Reliability test case.

Table B-5 Reliability test case and results

Test	Manual Test Case	Defects	Automation Test Case	Defects
Reliability Test Suites				
120 Hour Reliability Test This test will verify the reliability of the Enterprise NG Branch Network design. During the duration of 120 hours reliability testing, all the traffic including stateful traffic (http, telnet, ftp, etc.), background UDP traffic, multicasting traffic, video streams, voice calls, and wireless traffic, will be running on the Enterprise NG Branch network infrastructure. With this traffic, every 10 hours, some tests will be performed on the routers to ensure the network is still a healthy environment and all the major features of the network are still functioning properly. The test cases that will be performed every 10 hours are: dmvpn test suite, routing test suite, security test suite, QoS test suite, multicast test suite, voice test suite, wireless test suite, and negative test suite. Refer each test suite spec for more detail. The checking processes that will be performed every 10 hours are: router's memory utilization, CPU hog, router's up time, traceback errors, alignment errors, syslog errors, and packet errors and crashes.	Pass	—	N/A	—

APPENDIX **C**

Defects

C.1 CSCsj82794

MQC policing not working and drop rate displaying in wrong class

Component: QoS

Severity: Severe:

Symptom:

- MQC policing is NOT policing the traffic correctly. It's NOT just a cosmetic issue.
- The "exceeded" match counter in the policing class is showing zero.
- "show policy-map interface ..." shows that the drop rate is showing up in the wrong class (in "default" class in our case).

Conditions:

The issue is seen on a Cisco 1801 and a Cisco 877.

Workaround:No work-around

Status: Assigned (A)

Found In: 12.4(11)T02

Integrated In: N/A

Verified:Fix verified in IOS release 12.4(15)T3

C.2 CSCsj33060

Packet marked with qos-group does not match shaping policy on tunnel.

Component: QoS

Severity: Moderate

Symptom:

The problem is observed with the IPSec tunnel scenario. The inbound packets are marked with certain qos-group through the "police_1" policy-map. The outbound packets are matched through the "shape_2" policy-map which is applied to the traffic entering the IPSec tunnel (qos pre-classify is configured).

In the marking policy (police_1), show policy-map interface shows the packets are being marked but on the shaping policy (shape_2), none of the marked packets matched the class that has "match qos-group".

Conditions:

DMVPN hub router configured with per spoke QoS based on classifying/matching qos-group

Workaround: Mark/match base on ip precedence instead of match qos-group

Status:Assigned (A)

Found In: 12.4(11)T02

Integrated In: N/A

Verified: N/A

C.3 CSCsg83151

DMVPN: QOS enabled on physical outbound interface stops packet forwarding.

Component: QoS

Severity: Severe

Symptom:

A router may fail to forward packets via a tunnel interface.

Conditions:

This symptom is observed when the tunnel interface is

Configured for Dynamic Multipoint VPN (DMVPN) and QoS.

Workaround:No work-around

Status: Resolved (R)

Found In: 12.4(11) T2

Integrated In: 12.4(11) T3

Verified: Fix verified in IOS release 12.4(15)T3

C.4 CSCsj32241

QoS: Router reloads with DMA out of range error

Component: QoS

Severity: Severe

Symptom:

```
Router Reloads with the following message:

Router Reload after "Fatal error, DMA out of range error  "
####################
Jun 15 16:06:51: %IPPHONE-6-REG_ALARM: 10: Name=SEP0003E3631476
Load=7.1(2.0) Last=TCP-timeout
Jun 15 16:06:51: %IPPHONE-6-REGISTER: ephone-1:SEP0003E3631476
IP:172.16.127.11 Socket:1 DeviceType:Phone has registered.
```

```
%ERR-1-GT64120 (PCI-0): Fatal error, DMA out of range error
GT=0x24000000, cause=0x0500E083, mask=0x0ED01F00, real_cause=0x04000000
      ...
```

Conditions:

Policy map is configured, and services policy is applied on the interface.

Workaround:Remove Policy map, and service policy

Status:

Fixed in 12.4(11) T3 and later.

Found In: 12.4(11) T2

Integrated In: 12.4(11) T3

Verified: Fix verified in IOS release 12.4(15)T3

C.5 CSCsj14847

“crypto connect” command dropped after reload on unchannelized 2CT3+

Component: DMVPN

Severity: Severe

Symptom:

The crypto connect command on a channelized T3 WAN card (serial interface in the non-channelized mode) is lost after the chassis reload or on the WAN card reload.

Conditions:

Chassis reload with crypto connect command in the startup configuration for a serial interface.

Reload of the WAN card with the crypto connect command configured on the serial interface.

Workaround:Reconfigure the crypto connect command.

Status: Resolved (R)

Found In: 12.2(18)SXF9 on Cat 6K, and 12.2(33)SRB1 on Cisco 7609

Integrated In: 12.2(18)SXF11 on Cat 6K (integrated), and 12.2SRC on Cisco 7609 (will be integrated)

Verified: Fix verified in IOS release 12.2(18)SXF12a on Cat 6500, and 12.2(33)SRC in C7600 platforms.

C.6 CSCsi65242

DMVPN: disabling AIM-VPN/SSL-3 leads to tracebacks.

Component: DMVPN

Severity: Moderate

Symptom:

Entering the command "no cry eng aim 0" leads to following tracebacks and continuous error messages.

```
Apr 25 02:13:49: %VPN_HW-6-INFO_LOC: Crypto engine: aim 0  State changed
to: Disabled
Apr 25 02:13:49: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0  State
changed to: Enabled
Apr 25 10:13:49.809: IPSECcard: an error coming back 0x10F1
Apr 25 02:13:49: %SYS-2-BADSHARE: Bad refcount in datagram_done,
ptr=C0830CCC, count=0,  -Traceback= 0x616D1CB4 0x605FF810 0x6395468
4 0x639567EC 0x6394E7B8 0x6392B484 0x6335EB80 0x6335ECE0 0x6392BED4
0x639312B4 0x632299EC 0x63242480 0x63242EB0 0x63242D8C 0x63241B6
0 0x632434A8
```

Conditions:

When "no cry eng aim 0” command is executed on the router.

Workaround:Do not turn off HW encryption

Status:Assigned (A)

Found In: 12.2(11)T2

Integrated In: N/A

Verified: N/A

C.7 CSCsd19181

“Crypto connect” command is dropped from serial interface after reload.

Component: DMVPN

Severity: Severe

Symptom:

Crypto connect command is lost on T3 interfaces when using a 6500. This command is lost after a reload. All connectivity using encryption on this interface will be disrupted.

Conditions:

Command will be lost after a reload or image upgrade.

Workaround: Re-enter the command after reloading the router

Status:Resolved (R)

Found In: 12.2(18)SXF07

Integrated In: 12.2(18)SXF08

Fix verified in IOS release 12.2(18)SXF12a on Cat 6500 platform.

C.8 CSCsi65686

“Crypto connect vlan” command is dropped on Serial wan after reload

Component: DMVPN

Severity: Severe

Symptom:

c7600 has crypto connect command configured on serial interface. The serial interface is 2CT3+ on an enhanced flexwan module. The command is dropped after a reload causing all crypto sessions to fail.

Conditions:

Command will be lost after a reload or image upgrade.

Workaround:Re-enter the command after reloading the router

Status:Resolved (R)

Found In: 12.2(32)SRB1

Integrated In: 12.2(33)SRB1

Verified: Fix verified in release 12.2(33)SRC in C7600 platforms

C.9 CSCsi00105

Traceback generated at router boot-time at udp_internal_Multicast

Component: Multicast

Severity: Severe

Symptom:

At router boot-time a traceback is generated to console.

Conditions:

This behavior may be observed on an IOS router installed with an IOS specified

or implied by the "First Fixed-in" field of bug ID CSCsd78066 "socket_sendto()

to a Multicast address does not consider the VRF setting".

Workaround:There is no known workaround to this issue.

Status:Resolved (R)

Found In: 12.4(11)T2

Integrated In: 12.4(13.9)T

Verified: Fix verified in IOS release 12.4(15)T3

C.10 CSCsi36011

c870 & c180x Watchdog timeout crash

Component WAN

Severity: Moderate

Symptom:

A router running Cisco IOS may experience a crash due to watchdog timeout..

Conditions:

This applies only to 870 and 180x series routers with ATM interfaces. When trying to shutdown the atm interface or "clear int atm0" the router may crash.

Workaround:

None, other than avoiding the shut and clear commands mentioned above.

Status:Resolved (R)

Found In: 12.4(11)T2

Integrated In: 12.4(17.06)T

Verified: Fix verified in IOS release 12.4(15)T3

C.11 CSCsj25679

%SYS-4-CHUNKMALLOCFAIL: Could not allocate chunks for CEF: arp throt

Component WAN

Severity: Moderate

Symptom:

%SYS-2-CHUNKMALLOCFAIL messages on c7200 router while

sending traffic.

Conditions:

%SYS-2-CHUNKMALLOCFAIL messages on c7200 router can be

seen while box is so much stress with traffic with higher size of packets.

(>=512bytes).

Workaround:No work-around

Status:Resolved (R)

Found In: 12.4(11)T2

Integrated In: 012.004(016.013) 12.4(15)T02 12.4(16.13)T 12.4(16a)

Verified: Fix verified in 12.4(15)T3.

C.12 CSCsj95947

%DATACORRUPTION-1-DATAINCONSISTENCY: copy error

Component: Miscellaneous

Severity: Moderate

Symptom:

The following message is seen on the router:

```
*Aug  6 16:34:47.188: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error,
-PC=
0x8005EC50,  -Traceback= 0x809971F4 0x809B9C2C 0x809DD8A4 0x8005EC50
0x800651E4 0x800652A8 0x809E42D4 0x809C4A38 0x800652EC 0x809C4BA0
0x809E42D4 0x80A0854C 0x800DB8C0 0x800DEE48.
```

Conditions:

Not applicable

Workaround: No work-around

Status:Resolved (R)

Found In: 12.4(15)T1

Integrated In: 012.003(024.002) 012.004(017.006) 12.4(03i) 12.4(06)T10 12.4(09)T07 12.4(13e) 12.4(15)T02 12.4(15)XN 12.4(16b) 12.4(17.02)T

Verified: Fix verified in 12.4(15)T3.

This page is intentionally left blank

APPENDIX **D**

Technical Notes

Following are the technical notes produced during the system assurance testing:

D.1 Technical Note

Wireless Multicast Test - "ip pim parse-mode" command should be configured under both Management interface VLAN of Wireless LAN Controller (4404) and AP VLAN on Cat 6500:

To perform Multicast over a Wireless infrastructure testing, the 4404 Wireless LAN Controller is connected to a Catalyst 6500 switch. While testing, it was observed that "ip pim sparse-mode"

MUST be configured on both the Controller management VLAN and the AP VLAN that are configured on the Catalyst 6500. This allows the AP to join the 4404 Wireless Controller Multicast group. Otherwise, Multicast group join will not take place.

D.2 Technical Note

Link Convergence Test - Provisioning sub-interface produce faster routing convergence than that of Main interface for Frame-relay network:

Routing convergence is much faster when frame relay sub-interfaces are provisioned for frame-relay network. While testing, it was observed that when main interface was provisioned for frame-relay network, the routing convergence outcome was 180 seconds, while the same configured on sub-interface produced the routing convergence in 15 seconds.

D.3 Technical Note:

Wireless LAN Controller Image Upgrade needs to be done in Sequence

Couple of observation deserves attention while considering to upgrade the Wireless LAN Controller image:

1. Sizes of some of the images may be larger than 32meg, hence need to make sure TFTP server used for the upgrade can support larger file transfer
2. Images need to be upgraded in sequential manner as some of images require some previous image before upgrade can take place. A simple example is version A may need to be upgraded before proceeding with version B upgrade.

D.4 Technical Note

High CPU utilization on ISRs after failure:

While performing the negative testing, some ISR routers show high CPU utilization (> 50%) right after failure. This has been interpreted as part of the convergence. Generally after a short period of time (around 1 min) the CPU utilization drops down to normal.

APPENDIX E

Configurations

In this section an example of branch router configuration shown from Single-Tier, and Dual-Tier profiles.

E.1 Single-Tier Branch Profile Configuration

This section shows the configuration of the following devices for Branch 2:

- "b2-3845
- "b2-3845-esm

```
b2-3845#show running-config
Load for five secs: 2%/0%; one minute: 3%; five minutes: 2%
Time source is NTP, 23:18:55.977 PST Mon Oct 22 2007
Building configuration...

Current configuration : 22481 bytes
!
! Last configuration change at 18:41:46 PST Mon Oct 22 2007 by campus
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime localtime
no service password-encryption
!
hostname b2-3845
!
boot-start-marker
boot system flash:c3845-adventerprisek9-mz.124-11.T2
boot-end-marker
!
logging count
logging buffered 64000
logging rate-limit 5
enable secret 5 $1$H3bz$YX4zN77ufaMEP2Es3m1ij/
enable password lab
!
aaa new-model
!
!
aaa authentication login default local enable
!
```

```
!
aaa session-id common
clock timezone pst -8
clock summer-time PST recurring
no network-clock-participate wic 0
no network-clock-participate wic 2
network-clock-participate wic 3
no network-clock-participate aim 1
!
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
   17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
   B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
   5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
   FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
   50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
   006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
   2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
   F3020301 0001
  quit
!
crypto pki trustpoint TP-self-signed-2027467210
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2027467210
 revocation-check none
 rsakeypair TP-self-signed-2027467210
!
!
crypto pki certificate chain TP-self-signed-2027467210
 certificate self-signed 01
  30820246 308201AF A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32303237 34363732 3130301E 170D3037 30353133 31333530
  34305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 30323734
  36373231 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100BF31 8CD14B8B 39EDD1BE 8B2ADDB7 B413FD76 9553E6EF D3FC09A0 A8A8904C
  9D22A448 0C14DB13 4BDC6342 BFB94BFE CF1751A8 688A59B5 A098A2E3 846BDC1C
  0D68E43C CE478B7D 6A45E53D D8519EE5 9BC6A012 88F5E8F2 DE4080CD 3AFFBE0F
  CE3098E6 31BADEE9 8B588C68 5C4DA3B2 F21D174B D7F59CF9 C1D495A8 E5DD21C4
  65C30203 010001A3 6E306C30 0F060355 1D130101 FF040530 030101FF 30190603
  551D1104 12301082 0E62322D 33383435 2E65662E 636F6D30 1F060355 1D230418
  30168014 36FE374D 51C96056 2752622E A3DB9C30 DE520B00 301D0603 551D0E04
  16041436 FE374D51 C9605627 52622EA3 DB9C30DE 520B0030 0D06092A 864886F7
  0D010104 05000381 8100724F E7BEC87D 66BB3229 F2C0EB2D F643EC9C D27C7562
  E4CE20F4 1B42956A 4BCC5D0C 84D80B51 9C8216B7 FA9AD059 48F3EAAF 97C6F624
  4A8142E1 04787ECE EDE0726B 234D3D06 FC8D9A3D 34D3FB39 8919DC15 9A080C55
  20576310 41D46313 0977E02A 32755313 1D73CFA6 1C41107D BC759853 59843C55
  7B38A430 58E009AC A0ED
        quit
!
!
crypto isakmp policy 20

encr aes 256
```

```
 authentication pre-share
 group 2
 lifetime 28800
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10 periodic
!
!
crypto ipsec transform-set secureAES esp-aes 256 esp-sha-hmac
!
crypto ipsec profile $ipsec_profile
 set security-association lifetime seconds 14400
!
crypto ipsec profile dmvpn_aes
 set security-association lifetime seconds 14400
 set transform-set secureAES
!
!
no ip source-route
ip cef
!
!
ip nbar port-map custom-04 udp 1024 1025
ip nbar port-map custom-03 tcp 5554 9996
ip nbar port-map custom-02 udp 1434
ip nbar port-map custom-01 tcp 3200 3201 3202 3203 3600
ip nbar port-map netbios udp 135 137 138 139 445
ip nbar port-map netbios tcp 137 139 445
no ip dhcp use vrf connected
ip dhcp excluded-address 172.16.36.0 172.16.36.100
ip dhcp excluded-address 172.16.37.1 172.16.37.100
!
ip dhcp pool ap_pool
   network 172.16.36.0 255.255.255.0
   default-router 172.16.36.1
   domain-name ef.com
   option 60 ascii "Cisco AP c1240"
   option 43 hex f104.ac10.230a
!
ip dhcp pool wireless_users_pool
   network 172.16.37.0 255.255.255.0
   default-router 172.16.37.1
   domain-name ef.com
!
!
no ip bootp server
no ip domain lookup
ip domain name ef.com
ip multicast-routing
ip ips config location flash:/ipsstore/ retries 1
ip ips name ips1
ip ips name dmvpn-ips
!
ip ips signature-category
  category all
   retired true
  category ios_ips advanced
   retired false
!
```

```
!
multilink bundle-name authenticated
!
isdn switch-type primary-5ess
voice-card 0
 dspfarm
!
!
!
key chain valient
 key 1
   key-string cisco123
!
!
voice service voip
!
voice class h323 1
  call start fast
!
!
username ent-3845-w1 password 0 lab
username cisco privilege 15 secret 5 $1$h6dB$YfQ/kREZY/PkSM.vTQGjo.
username scriptman password 0 lab
username campus privilege 15 password 0 lab
archive
 log config
  hidekeys
!
!
controller T1 0/0/0
 shutdown
 framing esf
 clock source internal
 linecode b8zs
!
controller T1 0/0/1
 shutdown
 framing esf
 linecode b8zs
!
controller T1 0/2/0
 shutdown
 framing esf
 linecode b8zs
!
controller T1 0/2/1
 shutdown
 framing esf
 linecode b8zs
!
controller T1 0/3/0
 framing esf
 clock source line primary
 linecode b8zs
!
controller T1 0/3/1
 framing esf
 linecode b8zs
```

```
!
ip ssh logging events
!
class-map match-all BRANCH-BULK-DATA
 match access-group name BULK-DATA-APPS
class-map match-all SQL-SLAMMER
 match protocol custom-02
 match packet length min 404 max 404
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol sqlnet
 match protocol http url "*cisco.com"
 match protocol custom-01
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
class-map match-any WORMS
 match protocol http url "*.ida*"
 match protocol http url "*cmd.exe*"
 match protocol http url "*root.exe*"
 match protocol http url "*readme.em1*"
 match protocol exchange
 match protocol netbios
 match protocol custom-03
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol telnet
 match protocol nfs
 match protocol dns
 match protocol icmp
 match protocol tftp
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
 match protocol custom-04
class-map match-any CALL-SIGNALING
 match ip dscp cs3
 match ip dscp af31
class-map match-all NET-MGMG
 match ip dscp cs2
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
!
!
```

```
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
  set cos dscp
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMG
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
   police cir 8000 bc 8000 be 8000
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN_EDGE_FRTS
 class class-default
  shape average 1460000 14600 0
  service-policy BRANCH-WAN-EDGE
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
 class BRANCH-SCAVENGER
  set ip dscp cs1
 class WORMS
   drop
!
!
!
interface Loopback0
 ip address 172.16.32.1 255.255.255.255
 ip pim sparse-mode
!
interface Loopback5
 description Tunnel source interface
 ip address 45.1.2.1 255.255.255.255
!
interface Tunnel38
 description Used for DMVPN spoke network
 bandwidth 1000
```

```
 ip address 10.0.0.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nbar protocol-discovery
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 valient
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco
 ip nhrp map 10.0.0.252 39.1.1.1
 ip nhrp map multicast 39.1.1.1
 ip nhrp map 10.0.0.253 39.1.1.2
 ip nhrp map multicast 39.1.1.2
 ip nhrp network-id 100
 ip nhrp holdtime 360
 ip nhrp nhs 10.0.0.252
 ip nhrp nhs 10.0.0.253
 ip nhrp cache non-authoritative
 ip nhrp shortcut
 ip nhrp redirect
 ip ips dmvpn-ips in
 ip route-cache flow
 ip tcp adjust-mss 1360
 load-interval 30
 qos pre-classify
 cdp enable
 tunnel source Loopback5
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile dmvpn_aes
!
interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
 no ip address
 ip ips dmvpn-ips in
 duplex auto
 speed auto
 media-type rj45
 no keepalive
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no keepalive
!
interface GigabitEthernet0/1.1
 description Ixia (data/multicast) traffic
 encapsulation dot1Q 24
 ip address 220.22.1.1 255.255.255.0
 ip pim sparse-dense-mode
 ip ips dmvpn-ips in
 ip virtual-reassembly
 ip igmp version 3
!
interface GigabitEthernet0/1.2
 description VoIP (callgen/IP phone) traffic
```

```
 encapsulation dot1Q 25
 ip address 197.2.5.1 255.255.255.0
 ip ips dmvpn-ips in
!
interface GigabitEthernet0/1.3
 description IPSec (Smartbit avalanche) traffic
 encapsulation dot1Q 26
 ip address 220.41.1.1 255.255.255.0
 ip ips dmvpn-ips in
!
interface ATM0/1/0
 mtu 1450
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
 cdp enable
 max-reserved-bandwidth 100
 hold-queue 224 in
!

interface ATM0/1/0.111 point-to-point
 bandwidth 256
 no snmp trap link-status
 cdp enable
 pvc 1/11
  vbr-nrt 256 256
  tx-ring-limit 3
  encapsulation aal5snap
  service-policy output BRANCH-WAN-EDGE
  max-reserved-bandwidth 100
  pppoe-client dial-pool-number 1
 !
!
interface GigabitEthernet1/0
 ip address 1.1.1.1 255.255.255.0
 ip nbar protocol-discovery
 ip ips dmvpn-ips in
 load-interval 30
!
interface GigabitEthernet1/0.18
 encapsulation dot1Q 18
 ip address 223.255.30.121 255.255.255.0
 ip ips dmvpn-ips in
!
interface GigabitEthernet1/0.27
 encapsulation dot1Q 27
 ip address 172.16.27.1 255.255.255.0
 ip nbar protocol-discovery
 ip pim sparse-mode
 ip ips dmvpn-ips in
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet1/0.28
 encapsulation dot1Q 28
 ip address 172.16.28.1 255.255.255.0
 ip pim sparse-mode
```

```
 ip ips dmvpn-ips in
 ip igmp access-group ssm_group
 ip igmp version 3
!
interface GigabitEthernet1/0.29
 encapsulation dot1Q 29
 ip address 172.16.29.1 255.255.255.0
 ip ips dmvpn-ips in
!
interface GigabitEthernet1/0.31
 encapsulation dot1Q 31
 ip address 172.16.31.1 255.255.255.0
 ip ips dmvpn-ips in
!
interface GigabitEthernet1/0.36
 encapsulation dot1Q 36
 ip address 172.16.36.1 255.255.255.0
!
interface GigabitEthernet1/0.40
 encapsulation dot1Q 40
 ip address 172.16.40.3 255.255.255.0
!
interface GigabitEthernet1/0.41
 encapsulation dot1Q 41
 ip address 172.16.41.3 255.255.255.0
!
interface ATM2/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 no scrambling-payload
 cdp enable
 max-reserved-bandwidth 100
!
interface ATM2/0.1 point-to-point
 description to ng-3845-i
 bandwidth 3072
 ip address 220.12.0.1 255.255.255.252
 ip ips dmvpn-ips in
 no snmp trap link-status
 cdp enable
 pvc 10/203
  vbr-nrt 1536 1536
  tx-ring-limit 3
  encapsulation aal5snap
  service-policy output BRANCH-WAN-EDGE
  max-reserved-bandwidth 100
 !
! Removed rest of the ATM interface configuration as are unused.

interface wlan-controller3/0
 ip address 172.16.35.1 255.255.255.0
!
interface wlan-controller3/0.37
 encapsulation dot1Q 37
 ip address 172.16.37.1 255.255.255.0
!
interface Dialer1
```

```
 ip address 72.1.100.102 255.255.255.0
 ip ips dmvpn-ips in
 encapsulation ppp
 load-interval 30
 dialer pool 1
 dialer-group 1
 ppp authentication chap callin
 ppp chap hostname cisco111
 ppp chap password 0 cisco
!
router eigrp 10
 network 10.0.0.0 0.0.0.255
 network 172.16.27.0 0.0.0.255
 network 172.16.28.0 0.0.0.255
 network 172.16.29.0 0.0.0.255
 network 172.16.30.0 0.0.0.255
 network 172.16.31.1 0.0.0.0
 network 172.16.37.0 0.0.0.255
 network 172.16.0.0
 no auto-summary
 eigrp router-id 10.0.0.2
 eigrp stub connected
!
ip route 39.1.1.1 255.255.255.255 220.12.0.2
ip route 39.1.1.2 255.255.255.255 72.1.100.1
ip route 39.1.1.100 255.255.255.255 220.12.0.2
ip route 39.1.1.100 255.255.255.255 72.1.100.1
ip route 72.1.1.0 255.255.255.0 72.1.100.1
ip route 72.1.1.0 255.255.255.0 220.12.0.2
ip route 220.17.0.0 255.255.255.0 220.12.0.2
ip route 223.255.0.0 255.255.0.0 223.255.30.1
!
!
no ip http server
ip http authentication local
ip http secure-server
ip pim autorp listener
ip pim ssm default
ip nat pool overload-entvw2 220.22.0.1 220.22.0.1 prefix-length 30
ip nat inside source list 30 pool overload-entvw2 overload
!
ip access-list extended ssm_group
 permit igmp host 172.17.70.52 host 232.0.0.1
!
!
map-class frame-relay FRAME_MAP_T1
 service-policy output WAN_EDGE_FRTS
logging source-interface GigabitEthernet0/0
logging 223.255.254.243
logging 223.255.20.25
access-list 30 remark ixia-ipnat
access-list 30 permit 220.22.1.0 0.0.0.255
access-list 30 permit 197.2.5.0 0.0.0.255
access-list 101 deny   eigrp any any
access-list 101 permit ip any any
access-list 110 remark Multicast
access-list 110 permit ip any 239.192.0.0 0.0.255.255
access-list 110 permit ip any 239.232.0.0 0.0.255.255
```

```
access-list 110 remark Multicast
access-list 122 remark GRE-to-entw2
access-list 122 permit gre host 220.22.0.1 host 220.22.0.2
access-list 122 remark GRE-to-entw2
access-list 130 remark fwlist
access-list 130 deny   tcp any any log
access-list 130 permit udp any host 224.0.1.39
access-list 130 permit udp any host 224.0.1.40
access-list 130 permit udp host 11.10.2.3 239.0.0.0 0.255.255.255
access-list 130 permit ospf any any
access-list 130 permit gre any any
access-list 130 permit esp any any
access-list 130 permit pim any any
access-list 130 permit icmp any any echo log
access-list 130 permit icmp any any echo-reply log
access-list 130 permit icmp any any traceroute log
access-list 130 permit icmp any any unreachable log
access-list 130 permit eigrp any any
access-list 130 permit udp any eq 1719 any
access-list 130 remark fwlist
access-list 160 remark CoPP ACL for Critical traffic
access-list 160 permit tcp any any precedence internet
access-list 160 permit tcp any any precedence network
access-list 160 remark CoPP ACL for Critical traffic
access-list 161 remark CoPP ACL for Important traffic
access-list 161 permit tcp any any established
access-list 161 remark CoPP ACL for Important traffic
access-list 162 remark CoPP ACL for Normal traffic
access-list 162 permit icmp any any ttl-exceeded
access-list 162 permit icmp any any port-unreachable
access-list 162 permit icmp any any echo-reply
access-list 162 permit icmp any any echo
access-list 162 remark CoPP ACL for Normal traffic
access-list 163 remark CoPP ACL for Undesirable traffic
access-list 2021 remark Lotus
access-list 2021 permit tcp any range 8000 8999 any
access-list 2021 permit tcp any any range 8000 8999
access-list 2021 remark Lotus
access-list 2022 remark Oracle
access-list 2022 permit tcp any range 5000 5999 any
access-list 2022 permit tcp any any range 5000 5999
access-list 2022 remark Oracle
access-list 2031 remark GateKeeper
access-list 2031 permit udp any eq 1719 any
access-list 2031 permit udp any any eq 1719
access-list 2031 remark GateKeeper
access-list 2032 remark H225
access-list 2032 permit tcp any eq 1720 any
access-list 2032 permit tcp any any eq 1720
access-list 2032 remark H225
access-list 2033 remark H245
access-list 2033 permit tcp any range 11000 11999 any
access-list 2033 permit tcp any any range 11000 11999
access-list 2033 remark H245
access-list 2034 remark SCCP
access-list 2034 permit tcp any range 2000 2002 any
access-list 2034 permit tcp any any range 2000 2002
access-list 2034 remark SCCP
```

```
access-list 2035 remark MGCP
access-list 2035 permit tcp any eq 2427 any
access-list 2035 permit tcp any any eq 2427
access-list 2035 remark MGCP
access-list 2036 remark telnet
access-list 2036 permit tcp any range 6000 6999 any
access-list 2036 permit tcp any any range 6000 6999
access-list 2036 remark telnet
access-list 2037 remark ftp
access-list 2037 permit tcp any range 7000 7999 any
access-list 2037 permit tcp any any range 7000 7999
access-list 2037 remark ftp
dialer watch-list 1 ip 220.27.5.1 255.255.255.255
dialer watch-list 1 delay disconnect 20
dialer-list 1 protocol ip list 101
snmp-server engineID local 1234560000000000000000
snmp-server enable traps ipmulticast
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-messa
ge
!
!
tftp-server flash:SWISMK9-4-1-171-0.aes alias wlc.aes
tftp-server flash:AIR-WLCM-K9-4-0-217-0.aes alias WLCM.aes
radius-server host 172.17.50.3 auth-port 1645 acct-port 1646 key cisco123
!
control-plane
!
!
dial-peer voice 1001 voip
 description to ent-7206-vw ccme
 destination-pattern 1001...
 session target ipv4:220.31.5.1
 codec g711ulaw
!
dial-peer voice 3003 voip
 description to ent-3825-vw ccme
 destination-pattern 3003...
 session target ipv4:220.20.0.250
 codec g711ulaw
!
dial-peer voice 4004 voip
 description to ent-2851-vw ccme
 destination-pattern 4004...
 session target ipv4:220.24.0.250
 codec g711ulaw
!
dial-peer voice 2009888 pots
 description Digital T1 phones
 destination-pattern 2009888
!
dial-peer voice 2009999 pots
 description Analog T1 phone
 destination-pattern 2009999
!
dial-peer voice 3009 voip
 description to ent-3825-vw Ana/Digi phones
 destination-pattern 3009...
 session target ipv4:220.20.0.250
```

```
 codec g711ulaw
!
!
gateway
 timer receive-rtp 1200
!
!
!
telephony-service
 load 7910 P00403020214
 load 7960-7940 P00303020214
 load 7905 CP79050101SCCP030530B.sbin
 max-ephones 240
 max-dn 720
 ip source-address 197.2.5.1 port 2000
 time-format 24
 max-conferences 8 gain -6
 web admin system name administrator password cisco
 web admin customer name cisco password cisco
 dn-webedit
 time-webedit
 transfer-system full-consult
 create cnf-files version-stamp 7960 Oct 15 2007 11:05:45
!
!
ephone-dn  1
 number 2002001
!
!
ephone-dn  2
 number 2002002
!
!
ephone-dn  3
 number 2002003
!
!
ephone-dn  4
 number 2002004
!
!
ephone-dn  5
 number 2002005
!
!
ephone-dn  6
 number 2002006
!
!
ephone-dn  7
 number 2002007
!
!
ephone-dn  8
 number 2002008
!
!
ephone-dn  9
```

```
 number 2002009
!
!
ephone-dn  71
 number 2002071
!
!
ephone-dn  72
 number 2002072
!
!
ephone-dn  73
 number 2002073
!
!
ephone-dn  74
 number 2002074
!
!
ephone-dn  75
 number 2002075
!
!
ephone-dn  76
 number 2002076
!
!
ephone-dn  77
 number 2002077
!
!
ephone-dn  78
 number 2002078
!
!
ephone-dn  79
 number 2002079
!
!
ephone  1
 device-security-mode none
 mac-address 0000.2002.0001
 button  1:1
!
!
!
ephone  2
 device-security-mode none
 mac-address 0000.2002.0002
 button  1:2
!
!
!
ephone  3
 device-security-mode none
 mac-address 0000.2002.0003
 button  1:3
!
```

```
!
!
ephone  4
 device-security-mode none
 mac-address 0000.2002.0004
 button  1:4
!
ephone  5
 device-security-mode none
 mac-address 0000.2002.0005
 button  1:5
!
!
!
ephone  6
 device-security-mode none
 mac-address 0000.2002.0006
 button  1:6
!
!
!
ephone  7
 device-security-mode none
 mac-address 0000.2002.0007
 button  1:7
!
!
!
ephone  8
 device-security-mode none
 mac-address 0000.2002.0008
 button  1:8
!
!
!
ephone  9
 device-security-mode none
 mac-address 0000.2002.0009
 button  1:9
!
!
!
ephone  71
 device-security-mode none
 mac-address 0000.2002.0071
 button  1:71
!
!
!
ephone  72
 device-security-mode none
 mac-address 0000.2002.0072
 button  1:72
!
!
!
ephone  73
 device-security-mode none
```

```
 mac-address 0000.2002.0073
 button  1:73
!
!
!
ephone  74
 device-security-mode none
 mac-address 0000.2002.0074
 button  1:74
!
!
!
ephone  75
 device-security-mode none
 mac-address 0000.2002.0075
 button  1:75
!
!
!
ephone  76
 device-security-mode none
 mac-address 0000.2002.0076
 button  1:76
!
!
!
ephone  77
 device-security-mode none
 mac-address 0000.2002.0077
 button  1:77
!
!
!
ephone  78
 device-security-mode none
 mac-address 0000.2002.0078
 button  1:78
!
!
!
ephone  79
 device-security-mode none
 mac-address 0000.2002.0079
 button  1:79
!
!
alias exec esm service-module Gi 1/0 sess
!
line con 0
 exec-timeout 0 0
 transport preferred none
 stopbits 1
line aux 0
 stopbits 1
line 66
 no activation-character
 no exec
 transport preferred none
```

```
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
line 194
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 password lab
 exec prompt timestamp
 transport preferred none
 transport input telnet ssh
line vty 5 15
 exec-timeout 15 0
 privilege level 15
 password lab
 exec prompt timestamp
 transport preferred none
 transport input telnet ssh
line vty 16 25
 exec-timeout 0 0
 privilege level 15
 transport input telnet ssh
!
scheduler allocate 20000 1000
ntp clock-period 17179735
ntp update-calendar
ntp server 223.255.10.1 prefer
ntp server 223.255.19.1

!
webvpn cef
!
end

b2-3845#
```

The NME configuration of the same router for Branch 2 is shown below:

```
b2-3845-esm#show running-config
Load for five secs: 5%/0%; one minute: 5%; five minutes: 5%
Time source is NTP, 22:30:15.840 pst Mon Oct 22 2007

Building configuration...

Current configuration : 9785 bytes
!
! Last configuration change at 15:22:26 pst Mon Oct 22 2007 by scriptman
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime localtime
no service password-encryption
!
hostname b2-3845-esm
!
logging count
logging buffered 64000 debugging
logging rate-limit 5
enable password lab
!
username cisco privilege 15 password 0 lab
username scriptman password 0 lab
username campus privilege 15 password 0 lab
aaa new-model
aaa authentication login default local enable
!
aaa session-id common
clock timezone pst -8
system mtu routing 1500
ip subnet-zero
no ip domain-lookup
ip domain-name ef.com
ip host syslog 223.255.22.8
ip dhcp smart-relay
ip dhcp excluded-address 172.16.40.1 172.16.40.10
!
ip dhcp pool CISF-VLAN-40
   network 172.16.40.0 255.255.255.0
   default-router 172.16.40.1
   domain-name ef.com
!
ip dhcp snooping vlan 27-30,40-41
ip dhcp snooping database flash:dhcp.txt
ip dhcp snooping database timeout 10
ip dhcp snooping
ip arp inspection vlan 27-30,40
ip arp inspection validate src-mac dst-mac ip
ip arp inspection log-buffer entries 100
ip arp inspection log-buffer logs 20 interval 120
!
mls qos map policed-dscp  0 10 18 24 25 34 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
```

```
mls qos srr-queue output cos-map queue 1 threshold 3  5
mls qos srr-queue output cos-map queue 2 threshold 1  2 4
mls qos srr-queue output cos-map queue 2 threshold 2  3
mls qos srr-queue output cos-map queue 2 threshold 3  6 7
mls qos srr-queue output cos-map queue 3 threshold 3  0
mls qos srr-queue output cos-map queue 4 threshold 3  1
mls qos srr-queue output dscp-map queue 1 threshold 3  46
mls qos srr-queue output dscp-map queue 2 threshold 1  16 18 20 22 25 32 34 36
mls qos srr-queue output dscp-map queue 2 threshold 1  38
mls qos srr-queue output dscp-map queue 2 threshold 2  24 26
mls qos srr-queue output dscp-map queue 2 threshold 3  48 56
mls qos srr-queue output dscp-map queue 3 threshold 3  0
mls qos srr-queue output dscp-map queue 4 threshold 1  8
mls qos srr-queue output dscp-map queue 4 threshold 3  10 12 14
mls qos queue-set output 1 threshold 2 70 80 100 100
mls qos queue-set output 1 threshold 4 40 100 100 100
mls qos
!
crypto pki trustpoint TP-self-signed-807466368
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-807466368
 revocation-check none
 rsakeypair TP-self-signed-807466368
!
!
crypto pki certificate chain TP-self-signed-807466368
 certificate self-signed 01
  3082028E 308201F7 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  53312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 38303734 36363336 38312130 1F06092A 864886F7 0D010902
  16126232 2D333834 352D6573 6D2E6566 2E636F6D 301E170D 39333033 30313030
  30303530 5A170D32 30303130 31303030 3030305A 3053312E 302C0603 55040313
  25494F53 2D53656C 662D5369 676E6564 2D436572 74696669 63617465 2D383037
  34363633 36383121 301F0609 2A864886 F70D0109 02161262 322D3338 34352D65
  736D2E65 662E636F 6D30819F 300D0609 2A864886 F70D0101 01050003 818D0030
  81890281 8100BC08 703A42FC F103265F A207C847 F06D4655 30412BFD 49D0840A
  BCA06A9C E2E228F4 975E3757 B970B84A 18C05D7B 09BF90BC C04404C4 5130E6B2
  D5CFAF36 14842EBA EFFECD7D 590A573F 40B9784E 32C34969 A2588420 4FF0F826
  FCD2F0F8 75274B04 18C826F6 3511C558 555602E5 6FD9464A AFDE2712 688C96CC
  34AAC264 6FBB0203 010001A3 72307030 0F060355 1D130101 FF040530 030101FF
  301D0603 551D1104 16301482 1262322D 33383435 2D65736D 2E65662E 636F6D30
  1F060355 1D230418 30168014 8D4E20F1 C8C04AB5 DC9E1547 3D0A3C16 CC044935
  301D0603 551D0E04 1604148D 4E20F1C8 C04AB5DC 9E15473D 0A3C16CC 04493530
  0D06092A 864886F7 0D010104 05000381 81006DDA 6032D70C 0EC35D41 0BD38DFB
  F2BF8963 7080CD52 F1178CD6 767E11A4 F0D6E065 83C268B8 D1E5DAE6 F6DF70AB
  71D120A0 8BB4EBDA 239F0BA1 D01DD6EE 26783CBD 934A183E 4FCFE3FC 92918EE0
  B33636A7 B3C41373 0806422C 3F9D1ADF 5F726954 71EF9109 6C3D6428 E1B8CCF9
  AFCE57E0 1D7D1BB7 279FCDFE ACA1010F 2CB8
  quit
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
class-map match-all DVLAN-TRANSACTIONAL-DATA
```

```
  match access-group name DVLAN-TRANSACTIONAL-DATA
class-map match-all DVLAN-PC-VIDEO
  match access-group name DVLAN-PC-VIDEO
class-map match-all DVLAN-MISSION-CRITICAL-DATA
  match access-group name DVLAN-MISSION-CRITICAL-DATA
class-map match-all VVLAN-VOICE
  match access-group name VVLAN-VOICE
class-map match-all VVLAN-ANY
  match access-group name VVLAN-ANY
class-map match-all DVLAN-BULK-DATA
  match access-group name DVLAN-BULK-DATA
class-map match-all VVLAN-CALL-SIGNALLING
  match access-group name VVLAN-CALL-SIGNALLING
!
!

policy-map IPPHONE+PC
  class VVLAN-VOICE
   set dscp ef
    police 128000 8000 exceed-action drop
  class VVLAN-CALL-SIGNALLING
   set dscp cs3
    police 32000 8000 exceed-action policed-dscp-transmit
  class VVLAN-ANY
   set dscp default
    police 32000 8000 exceed-action policed-dscp-transmit
  class DVLAN-PC-VIDEO
   set dscp af41
    police 49500 8000 exceed-action policed-dscp-transmit
  class DVLAN-MISSION-CRITICAL-DATA
   set dscp 25
    police 5000000 8000 exceed-action policed-dscp-transmit
  class DVLAN-TRANSACTIONAL-DATA
   set dscp af21
    police 5000000 8000 exceed-action policed-dscp-transmit
  class DVLAN-BULK-DATA
   set dscp af11
    police 5000000 8000 exceed-action policed-dscp-transmit
!
!
!
interface FastEthernet1/0/1
 switchport access vlan 27
 load-interval 30
 speed 100
 duplex full
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape  3  0  0  0
 priority-queue out
 mls qos trust dscp
!
interface FastEthernet1/0/2
 switchport access vlan 27
 speed 100
 duplex full
!
interface FastEthernet1/0/3
 switchport access vlan 28
```

```
 speed 100
 duplex full
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape  3  0  0  0
 priority-queue out
 mls qos trust dscp
!
interface FastEthernet1/0/4
 switchport access vlan 28
 speed 100
 duplex full
!
interface FastEthernet1/0/5
 switchport access vlan 29
 speed 100
 duplex full
!
interface FastEthernet1/0/6
 switchport access vlan 29
 speed 100
 duplex full
!
interface FastEthernet1/0/7
 switchport access vlan 30
 speed 100
 duplex full
!
interface FastEthernet1/0/8
 switchport access vlan 30
 speed 100
 duplex full
!
interface FastEthernet1/0/9
 switchport access vlan 31
 speed 100
 duplex full
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape  3  0  0  0
 priority-queue out
 mls qos trust dscp

interface FastEthernet1/0/10
 switchport access vlan 31
 speed 100
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape  3  0  0  0
 priority-queue out
 mls qos trust dscp
!
interface FastEthernet1/0/11
!
interface FastEthernet1/0/12
!
interface FastEthernet1/0/13
 description connection to Pagent_7206VXR_1 e1/1 for CISF testing
 switchport access vlan 40
 switchport mode access
 spanning-tree portfast
```

```
 ip verify source
 ip dhcp snooping limit rate 20
!
interface FastEthernet1/0/14
 description connection to pagent-7206vxr-1 e3/1 for CISF testing
 switchport access vlan 41
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security violation restrict
 load-interval 30
 speed 10
 spanning-tree portfast
!
interface FastEthernet1/0/15
 description connection to pagent-7206vxr-2 e1/0 for CISF testing
 switchport access vlan 40
 switchport mode access
 ip arp inspection limit rate 20
 load-interval 30
 spanning-tree portfast
 ip dhcp snooping limit rate 20
!
interface FastEthernet1/0/16
 description airespace aps
 switchport access vlan 36
 speed 100
!
interface GigabitEthernet1/0/1
 switchport access vlan 18
 switchport mode access
!
interface GigabitEthernet1/0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,18,27-31,35-37,40,41
 switchport mode trunk
 load-interval 30
!
interface Vlan1
 ip address dhcp
 no ip route-cache
 no ip mroute-cache
!
interface Vlan18
 ip address 223.255.30.122 255.255.0.0
 no ip route-cache
 no ip mroute-cache
!
interface Vlan40
 description used for CISF testing
 ip address 172.16.40.1 255.255.255.0
 ip helper-address 172.16.40.1
 ip helper-address 116.4.40.1
 no ip route-cache
 no ip mroute-cache
!
interface Vlan41
 description used for CISF testing
```

```
 ip address 172.16.41.1 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
ip default-gateway 223.255.30.1
ip classless
ip http server
ip http secure-server
!
!
ip access-list extended DVLAN-BULK-DATA
 permit tcp any any eq 143
 permit tcp any any eq 220
ip access-list extended DVLAN-MISSION-CRITICAL-DATA
 permit tcp any any range 3200 3203
 permit tcp any any eq 3600
 permit tcp any any range 2000 2002
ip access-list extended DVLAN-PC-VIDEO
 permit udp any any range 16384 32767
ip access-list extended DVLAN-TRANSACTIONAL-DATA
 permit tcp any any eq 1352
ip access-list extended VVLAN-ANY
 permit ip 10.173.1.128 0.0.0.127 any
ip access-list extended VVLAN-CALL-SIGNALLING
 permit tcp 10.173.1.128 0.0.0.127 any range 2000 2002 dscp af31
 permit tcp 10.173.1.128 0.0.0.127 any range 2000 2002 dscp cs3
ip access-list extended VVLAN-VOICE
 permit udp 10.173.1.128 0.0.0.127 any range 16384 32767 dscp ef
!
radius-server source-ports 1645-1646
!
control-plane
!
alias exec return Ctrl^x ; esm clear
!
line con 0
 exec-timeout 15 0
 transport preferred none
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 password lab
 exec prompt timestamp
 transport preferred none
 transport input telnet
line vty 5 15
 exec-timeout 15 0
 privilege level 15
 password lab
 exec prompt timestamp
 transport preferred none
 transport input telnet
!
ntp clock-period 36029427
ntp server 223.255.9.1
ntp server 223.255.19.1
end
```

```
b2-3845-esm#
```

E.2 Dual-Tier Branch Profile Configuration

This section shows the configuration of the following devices for Branch 4 (shown in figure 6):

- b4-2851-p
- b4-2851-p-esm
- b4-3560g

```
b4-2851-p#show running-config
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is NTP, 23:41:48.007 PST Mon Oct 22 2007

Building configuration...

Current configuration : 11281 bytes
!
! Last configuration change at 18:44:05 PST Mon Oct 22 2007 by campus
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime localtime
no service password-encryption
!
hostname b4-2851-p
!
boot-start-marker
boot system flash:c2800nm-adventerprisek9-mz.124-15.T2.fc4
boot-end-marker
!
logging count
logging buffered 64000
logging rate-limit 5
enable password lab
!
aaa new-model
!
aaa authentication login default local enable
!
!
aaa session-id common
clock timezone pst -8
clock summer-time PST recurring
no network-clock-participate wic 0
!
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
   17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
   B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
```

```
   5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
   FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
   50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
   006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
   2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
   F3020301 0001
                            quit
!
crypto isakmp policy 20
 encr aes 256
 authentication pre-share
 group 2
 lifetime 28800
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10 periodic
!
!
crypto ipsec transform-set secureAES esp-aes 256 esp-sha-hmac
!
crypto ipsec profile $ipsec_profile
 set security-association lifetime seconds 14400
!
crypto ipsec profile dmvpn_aes
 set security-association lifetime seconds 14400
 set transform-set secureAES
!
no ip source-route
!
!
ip nbar port-map custom-04 udp 1024 1025
ip nbar port-map custom-03 tcp 5554 9996
ip nbar port-map custom-02 udp 1434
ip nbar port-map custom-01 tcp 3200 3201 3202 3203 3600
ip nbar port-map netbios udp 135 137 138 139 445
ip nbar port-map netbios tcp 137 139 445
ip cef
!
!
no ip bootp server
no ip domain lookup
ip domain name ef.com
ip multicast-routing
ip ips name dmvpn-ips
!
ip ips signature-category
  category all
   retired true
  category ios_ips advanced
!
multilink bundle-name authenticated
!
isdn switch-type basic-5ess
!
voice-card 0
 no dspfarm
!
!
key chain valient
```

```
 key 1
   key-string cisco123
!
username ent-3845-w1 password 0 lab
username scriptman password 0 lab
username campus privilege 15 password 0 lab
username cisco privilege 15 password 0 lab
archive
 log config
  hidekeys
!
controller T1 0/0/0
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24
!
controller T1 0/0/1
framing esf
 linecode b8zs
!
ip ssh logging events
!
!
class-map match-all BRANCH-BULK-DATA
 match access-group name BULK-DATA-APPS
class-map match-all SQL-SLAMMER
 match protocol custom-02
 match packet length min 404 max 404
class-map match-all BULK-DATA
 match ip dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match ip dscp af41  af42
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol sqlnet
 match protocol http url "*cisco.com"
 match protocol custom-01
class-map match-all BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
                          class-map match-any WORMS
 match protocol http url "*.ida*"
 match protocol http url "*cmd.exe*"
 match protocol http url "*root.exe*"
 match protocol http url "*readme.em1*"
 match protocol exchange
 match protocol netbios
 match protocol custom-03
class-map match-all VOICE
 match ip dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match ip dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol telnet
 match protocol nfs
 match protocol dns
```

```
 match protocol icmp
 match protocol tftp
class-map match-all ROUTING
 match ip dscp cs6
class-map match-all SCAVENGER
match ip dscp cs1
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
 match protocol custom-04
class-map match-any CALL-SIGNALING
 match ip dscp cs3
 match ip dscp af31
class-map match-all NET-MGMG
 match ip dscp cs2
class-map match-all TRANSACTIONAL-DATA
 match ip dscp af21  af22
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
  set cos dscp
policy-map BRANCH-WAN-EDGE
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
class CALL-SIGNALING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMG
  bandwidth percent 2
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class SCAVENGER
   police cir 8000 bc 8000 be 8000
 class class-default
  bandwidth percent 25
  random-detect
policy-map WAN_EDGE_FRTS
 class class-default
  shape average 1460000 14600 0
  service-policy BRANCH-WAN-EDGE
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-MISSION-CRITICAL
  set ip dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class BRANCH-NET-MGMT
  set ip dscp cs2
 class BRANCH-BULK-DATA
  set ip dscp af11
```

```
 class BRANCH-SCAVENGER
  set ip dscp cs1
 class WORMS
   drop
!
interface Loopback0
 ip address 172.16.64.1 255.255.255.255
 ip pim sparse-mode
!
interface Loopback28
ip address 192.168.4.1 255.255.255.255
!
interface Tunnel38
 description Used for DMVPN spoke network
 bandwidth 1000
 ip address 10.0.0.4 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nbar protocol-discovery
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 valient
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco
 ip nhrp map 10.0.0.252 39.1.1.1
 ip nhrp map multicast 39.1.1.1
 ip nhrp network-id 100
 ip nhrp holdtime 360
 ip nhrp nhs 10.0.0.252
 ip nhrp cache non-authoritative
 ip nhrp shortcut
 ip nhrp redirect
 ip ips dmvpn-ips in
ip tcp adjust-mss 1360
 load-interval 30
 qos pre-classify
 cdp enable
 tunnel source Serial0/0/0:0.1
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile dmvpn_aes
!
interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
 no ip address
 ip ips dmvpn-ips in
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.1
 description Ixia (data/multicast) traffic
 encapsulation dot1Q 44
 ip address 220.24.1.1 255.255.255.0
```

```
 ip pim sparse-dense-mode
 ip nat inside
 ip ips dmvpn-ips in
 ip virtual-reassembly
 ip igmp version 3
!
interface GigabitEthernet0/1.2
 description VoIP (callgen/IP phone) traffic
 encapsulation dot1Q 45
 ip address 197.4.5.1 255.255.255.0
 ip ips dmvpn-ips in
!
interface GigabitEthernet0/1.3
 description IPSec (Smartbit avalanche) traffic
 encapsulation dot1Q 46
!
interface Serial0/0/0:0
 description Interface SHUTDOWN for phase5c EIGRP test suite
 no ip address
 ip pim sparse-mode
 encapsulation frame-relay IETF
 load-interval 30
 cdp enable
 frame-relay lmi-type cisco
!
interface Serial0/0/0:0.1 point-to-point
 description to ng-3845-i
 bandwidth 1536
 ip address 220.14.0.1 255.255.255.252
 ip ips dmvpn-ips in
 snmp trap link-status
 frame-relay interface-dlci 306
  class FRAME_MAP_T1
!
interface BRI0/2/0
 ip address 220.10.1.4 255.255.255.0
 ip ips dmvpn-ips in
 encapsulation ppp
 dialer idle-timeout 30
 dialer wait-for-carrier-time 10
 dialer map ip 220.10.1.1 name ent-3845-w1 broadcast 4088888888
 dialer map ip 220.27.5.1 name ent-3845-w1 broadcast 4088888888
 dialer watch-disable 20
 dialer watch-group 1
 dialer-group 1
 isdn switch-type basic-5ess
 isdn point-to-point-setup
 ppp authentication chap
 ppp chap hostname ent-2851-vw
 ppp chap password 0 lab
!
interface GigabitEthernet1/0
 ip address 1.1.1.1 255.255.255.0
 ip nbar protocol-discovery
 ip ips dmvpn-ips in
!
interface GigabitEthernet1/0.18
 encapsulation dot1Q 18
```

```
 ip address 223.255.30.141 255.255.255.0
!
interface GigabitEthernet1/0.30
 encapsulation dot1Q 30
!
interface GigabitEthernet1/0.59
 encapsulation dot1Q 59
 ip address 172.16.59.1 255.255.255.0
 ip nbar protocol-discovery
 ip pim dr-priority 10
 ip pim sparse-mode
 ip ips dmvpn-ips in
 standby version 2
 standby 59 ip 172.16.59.3
 standby 59 timers 1 3
 standby 59 preempt
 standby 59 track Serial0/0/0:0.1 15
 service-policy input BRANCH-LAN-EDGE-IN
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet1/0.60
 encapsulation dot1Q 60
 ip address 172.16.60.1 255.255.255.0
 ip pim dr-priority 10
 ip pim sparse-mode
 ip ips dmvpn-ips in
 ip igmp access-group ssm_group
 ip igmp version 3
 standby version 2
 standby 60 ip 172.16.60.3
 standby 60 timers 1 3
 standby 60 preempt
 standby 60 track Serial0/0/0:0.1 15
!
interface GigabitEthernet1/0.61
 encapsulation dot1Q 61
 ip address 172.16.61.1 255.255.255.0
 ip ips dmvpn-ips in
!
interface GigabitEthernet1/0.62
 encapsulation dot1Q 62
 ip address 172.16.62.1 255.255.255.0
 ip ips dmvpn-ips in
!
interface GigabitEthernet1/0.63
 encapsulation dot1Q 63
 ip address 172.16.63.1 255.255.255.0
 ip ips dmvpn-ips in
!
router eigrp 10
 network 10.0.0.0 0.0.0.255
 network 172.16.59.0 0.0.0.255
 network 172.16.60.0 0.0.0.255
 network 172.16.61.0 0.0.0.255
 network 172.16.62.0 0.0.0.255
 network 172.16.63.0 0.0.0.255
 network 172.16.0.0
 network 192.168.4.0
```

```
 no auto-summary
 eigrp router-id 10.0.0.4
 eigrp stub connected
!
ip forward-protocol nd
ip route 39.1.1.1 255.255.255.255 220.14.0.2
ip route 39.1.1.100 255.255.255.255 220.14.0.2
ip route 220.17.0.0 255.255.255.0 220.14.0.2
ip route 223.255.0.0 255.255.0.0 223.255.30.1
!
!
no ip http server
no ip http secure-server
ip pim autorp listener
ip pim ssm default
ip nat pool nat-entvw4 220.24.0.1 220.24.0.1 prefix-length 30
ip nat inside source list 30 pool nat-entvw4 overload
!
ip access-list extended ssm_group
 permit igmp host 172.17.70.52 host 232.0.0.1
                              !
ip radius source-interface Loopback0
!
map-class frame-relay FRAME_MAP_T1
 service-policy output WAN_EDGE_FRTS
!
map-class frame-relay fr_t1
access-list 130 permit icmp any any echo log
access-list 130 permit icmp any any echo-reply log
access-list 130 permit icmp any any traceroute log
access-list 2036 remark telnet
access-list 2036 permit tcp any range 6000 6999 any
!
radius-server host 172.17.50.3 auth-port 1645 acct-port 1646 key cisco123
!
control-plane
!
voice-port 0/1/0
!
voice-port 0/1/1
!
!
line con 0
 exec-timeout 0 0
 transport preferred none
 stopbits 1
line aux 0
 stopbits 1
line 66
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 password lab
```

```
 exec prompt timestamp
 transport preferred none
 transport input telnet ssh
line vty 5 15
 exec-timeout 15 0
 privilege level 15
 password lab
 exec prompt timestamp
 transport preferred none
 transport input telnet ssh
!
scheduler allocate 20000 1000
ntp clock-period 17180332
ntp server 223.255.9.1
ntp server 223.255.19.1

!
webvpn cef
!
end
```

The following configuration is taken from NME fro Branch 4:

```
b4-2851-p-esm#show running-config
Load for five secs: 4%/0%; one minute: 4%; five minutes: 4%
Time source is NTP, 22:42:21.526 pst Mon Oct 22 2007

Building configuration...

Current configuration : 2697 bytes
!
! Last configuration change at 15:22:26 pst Mon Oct 22 2007 by scriptman
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime localtime
no service password-encryption
!
hostname b4-2851-p-esm
!
logging count
logging buffered 64000 debugging
logging rate-limit 5
enable password lab
!
username cisco privilege 15 password 0 lab
username campus password 0 lab
username scriptman privilege 15 password 0 lab
aaa new-model
aaa authentication login default local enable

aaa session-id common
clock timezone pst -8
system mtu routing 1500
ip subnet-zero
no ip domain-lookup
ip domain-name ef.com
```

```
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet1/0/1
 switchport access vlan 59
 speed 100
interface FastEthernet1/0/2
 switchport access vlan 59
 speed 100
 duplex full
!
interface FastEthernet1/0/3
 switchport access vlan 60
 speed 100
 duplex full
!
interface FastEthernet1/0/4
 switchport access vlan 60
 speed 100
 duplex full
!
interface FastEthernet1/0/5
 switchport access vlan 61
 speed 100
 duplex full
!
interface FastEthernet1/0/6
 switchport access vlan 61
speed 100
 duplex full
!
interface FastEthernet1/0/7
 switchport access vlan 62
 speed 100
 duplex full
!
interface FastEthernet1/0/8
 switchport access vlan 62
 speed 100
 duplex full
!
interface FastEthernet1/0/9
 switchport access vlan 63
 speed 100
 duplex full
!
interface FastEthernet1/0/10
 switchport access vlan 63
 speed 100
 duplex full
!
interface FastEthernet1/0/11
!
```

```
interface FastEthernet1/0/12
!
interface FastEthernet1/0/13
!
interface FastEthernet1/0/14
!
interface FastEthernet1/0/15
!
interface FastEthernet1/0/16
!
interface GigabitEthernet1/0/1
 switchport access vlan 18
 switchport mode access
!
interface GigabitEthernet1/0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,18,59-63
 switchport mode trunk
 load-interval 30
!
interface Vlan1
ip address dhcp
!
interface Vlan18
 ip address 223.255.30.142 255.255.255.0
!
interface Vlan30
 no ip address
!
ip default-gateway 223.255.30.1
ip classless
ip http server
ip http secure-server
!
!
radius-server source-ports 1645-1646
!
control-plane
!
!
line con 0
 exec-timeout 15 0
 transport preferred none
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 password lab
 exec prompt timestamp
 transport preferred none
 transport input telnet
line vty 5 15
 exec-timeout 15 0
 privilege level 15
 password lab
 exec prompt timestamp
 transport preferred none
 transport input telnet
```

```
!
ntp clock-period 36029452
ntp server 223.255.9.1
ntp server 223.255.19.1
end
```

The following configuration is taken from the LAN switch on Branch 4:

```
b4-3560g#show running-config
Load for five secs: 22%/0%; one minute: 21%; five minutes: 21%
Time source is NTP, 22:42:44.961 pst Mon Oct 22 2007

Building configuration...

Current configuration : 9653 bytes
!
! Last configuration change at 15:44:08 pst Mon Oct 22 2007 by campus
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime localtime
no service password-encryption
!
hostname b4-3560g
!
logging count
logging buffered 64000 debugging
logging rate-limit 5
enable password lab
!
username campus privilege 15 password 0 lab
username scriptman privilege 15 password 0 lab
username cisco privilege 15 password 0 lab
aaa new-model
aaa authentication login default local enable
aaa session-id common
clock timezone pst -8
system mtu routing 1500
ip subnet-zero
no ip domain-lookup
ip domain-name ef.com
ip host tftp 223.255.20.5
ip dhcp smart-relay
!
ip ssh logging events
ip igmp snooping vlan 60 mrouter interface Gi0/26
!
crypto pki trustpoint TP-self-signed-1664220544
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1664220544
 revocation-check none
 rsakeypair TP-self-signed-1664220544
!
!
crypto pki certificate chain TP-self-signed-1664220544
 certificate self-signed 01
30820287 308201F0 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
```

```
  51312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31363634 32323035 3434311E 301C0609 2A864886 F70D0109
  02160F62 342D3335 3630672E 65662E63 6F6D301E 170D3933 30333031 30303031
  32395A17 0D323030 31303130 30303030 305A3051 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 36363432
  32303534 34311E30 1C06092A 864886F7 0D010902 160F6234 2D333536 30672E65
  662E636F 6D30819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100AE9B 98563140 609B40BD FE70D96F 00639470 46898532 00C3CC12 3F98C90B
  F8F43668 00597BD8 22AC75E4 6EFD8738 90CC4BA9 510CF94E C011F933 984D777F
  0969DE9F 9EE12C56 A8114A91 4909AD8C 30ABD25F 976280FF 8E815CC9 DE1887C8
  9E287EA5 2A2D3A1A A052A562 2166034A 2FE32BD6 4EF463D5 CE64EF84 6A096C99
  21050203 010001A3 6F306D30 0F060355 1D130101 FF040530 030101FF 301A0603
  551D1104 13301182 0F62342D 33353630 672E6566 2E636F6D 301F0603 551D2304
  18301680 14C7A5B9 AC6B1F77 6D9855AD F1B98BF2 DE365F6A A1301D06 03551D0E
  04160414 C7A5B9AC 6B1F776D 9855ADF1 B98BF2DE 365F6AA1 300D0609 2A864886
  F70D0101 04050003 818100AE 29B05CA7 01A34C88 4F823BB5 EDB41720 3B5B547A
  06E6224F EEB7C4CC 5CDB3C23 E25AEF72 6E1D69CB A40D45B9 15C9FCFB 656CDC50
  412690A4 4B0C91A6 3C41FB94 D984036A 1F85392A 935896B0 52A243AF 38BB76DE
  4D454CFA 16B1025B 6D61C3FF 140A8E43 6D165F76 97884A55 C3046067 4BC96DCB
  143B2C73 DAB2301A 08D2EE
  quit
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface GigabitEthernet0/1
 switchport access vlan 59
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection trust
 ip arp inspection limit rate 100
 load-interval 30
 speed 100
 duplex full
 spanning-tree portfast
 ip dhcp snooping limit rate 100
                          !
interface GigabitEthernet0/2
 switchport access vlan 59
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 load-interval 30
 speed 100
 duplex full
 ip verify source
```

```
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/3
 switchport access vlan 60
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 load-interval 30
 speed 100
 duplex full
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/4
 switchport access vlan 60
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 load-interval 30
 speed 100
 duplex full
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/5
 switchport access vlan 61
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 load-interval 30
 speed 100
 duplex full
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/6
 switchport access vlan 61
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
                            ip arp inspection limit rate 100
 load-interval 30
 speed 100
```

```
 duplex full
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/7
 switchport access vlan 62
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 load-interval 30
 speed 100
 duplex full
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/8
switchport access vlan 62
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 load-interval 30
 speed 100
 duplex full
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet0/9
 switchport access vlan 63
 load-interval 30
 speed 100
 duplex full
!
interface GigabitEthernet0/10
 switchport access vlan 63
 load-interval 30
 speed 100
 duplex full
!
interface GigabitEthernet0/11
 switchport access vlan 63
 switchport mode access
 load-interval 30
 speed 100
!
interface GigabitEthernet0/12
 switchport access vlan 63
 switchport mode access
 load-interval 30
 speed 100
!
```

```
interface GigabitEthernet0/13
 switchport access vlan 63
 switchport mode access
 load-interval 30
 speed 100
!
interface GigabitEthernet0/14
 load-interval 30
 interface GigabitEthernet0/15
 load-interval 30
!
interface GigabitEthernet0/16
 load-interval 30
!
interface GigabitEthernet0/17
 load-interval 30
!
interface GigabitEthernet0/18
 load-interval 30
!
interface GigabitEthernet0/19
 load-interval 30
!
interface GigabitEthernet0/20
!
interface GigabitEthernet0/21
!
interface GigabitEthernet0/22
!
interface GigabitEthernet0/23
                            !
interface GigabitEthernet0/24
 no switchport
 ip address 223.255.30.145 255.255.255.0
!
interface GigabitEthernet0/25
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 59-63
 switchport mode trunk
 load-interval 30
 speed 100
!
interface GigabitEthernet0/26
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 59-63
 switchport mode trunk
 load-interval 30
 speed 100
!
interface GigabitEthernet0/27
!
interface GigabitEthernet0/28
!
interface GigabitEthernet0/29
!
interface GigabitEthernet0/30
!
interface GigabitEthernet0/31
```

```
!
interface GigabitEthernet0/32
!
interface GigabitEthernet0/33
!
interface GigabitEthernet0/34
!
interface GigabitEthernet0/35
!
interface GigabitEthernet0/36
!
interface GigabitEthernet0/37
!
interface GigabitEthernet0/38
 no switchport
 no ip address
!
interface GigabitEthernet0/39
interface GigabitEthernet0/40
!
interface GigabitEthernet0/41
!
interface GigabitEthernet0/42
!
interface GigabitEthernet0/43
!
interface GigabitEthernet0/44
!
interface GigabitEthernet0/45
!
interface GigabitEthernet0/46
!
interface GigabitEthernet0/47
!
interface GigabitEthernet0/48
!
interface GigabitEthernet0/49
!
interface GigabitEthernet0/50
!
interface GigabitEthernet0/51
!
interface GigabitEthernet0/52
!
interface Vlan1
 no ip address
!
ip default-gateway 223.255.18.1
ip classless
ip route 223.255.0.0 255.255.0.0 223.255.30.1
ip route 223.255.0.0 255.255.0.0 223.255.18.1
ip http server
ip http secure-server
!
!
cdp timer 5
snmp-server community valient1 RW
snmp-server community valient2 RW
```

```
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps entity
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps rtr
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server host 172.17.50.2 version 2c valient1
snmp-server host 223.255.18.215 version 2c valient1
snmp-server host 172.17.50.3 version 2c valient2
radius-server source-ports 1645-1646
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 password lab
 transport preferred none
 stopbits 1
line vty 0 4
 exec-timeout 0 0
privilege level 15
 password lab
 exec prompt timestamp
 transport preferred none
 transport input telnet
line vty 5 15
 exec-timeout 15 0
 privilege level 15
 password lab
 exec prompt timestamp
 transport preferred none
 transport input telnet
!
ntp clock-period 36029035
ntp server 223.255.19.1
end
b4-3560g#
```

This page is intentionally left blank