



Basic Small Branch Network System Assurance Guide

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

Cisco Validated Design

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.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Basic Small Branch Network System Assurance Guide
© 2009 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface ix

Obtaining Documentation and Submitting a Service Request ix

Basic Small Branch Network Overview 1

Contents 1

Introduction 1

Small Branch Design Considerations 4

System Design 7

Topology 11

Cisco Platforms and Versions Evaluated 13

References and Recommended Reading 14

Features and Services 17

Contents 17

Branch Network Components 17

Selecting Network Components 19

WAN Services 25

Selecting WAN Service 27

Leased-line Deployment 30

Frame Relay Service Deployment 32

L3VPN Service Deployment 34

VPWS Services 36

MPLS Switched WAN Services 36

Ethernet Switched WAN Services 36

LAN Deployment Model 39

Virtual LANs 42

VLAN Trunks and VLAN Trunking Protocol 43

Power-over-Ethernet 45

Spanning Tree Protocol 45

Network Fundamentals 45

Path Redundancy, Rapid Recovery, and Disaster Recovery 46

Backup WAN Link 48

IP Addressing and IP Routing 51

Routing Protocols	53
Multicast	55
DHCP	55
NAT and PAT	55
Quality of Service	56
Classification and Marking	60
Policing and Markdown	61
Scheduling	61
Shaping	62
Scavenger Class QoS	62
Automatic QoS	62
Security Services	63
Infrastructure Protection	64
Access Control	66
Authentication	67
Authorization	68
Accounting	68
Secure Connectivity	68
Threat Protection, Detection, and Mitigation	76
Management Services	78
Cisco Configuration Professional	79
Simple Network Management Protocol	80
Syslog	81
NetFlow	81
Network Based Application Recognition	81
IP Service Level Agreement	82
Network Time Protocol	82
Cisco Configuration Engine	82
Voice Services	84
Voice Quality Considerations	85
WAN Capacity Considerations	87
IP Telephony	90
Centralized Call Control	91
Local Call Control	92
Selecting a Call Control Model	93
IP Phones	93
Voice Gateway	94
Call Admission Control	96
Conferencing and Transcoding	98

Music on Hold	98
Dial Plan	98
Voice Mail and Auto Attendant Services	99
Traditional Telephony	99
Analog Device Connectivity	99
Emergency Services	99
System Implementation	101
Contents	101
Network Topology	101
WAN Services Implementation	105
Single-Port DS-1 Interface with Frame Relay Encapsulation	105
Verification of Single-Port DS-1 Interface with Frame Relay Encapsulation	106
Single-Port DS-1 Interface with Point-to-Point Encapsulation	106
Onboard Fast Ethernet Interface	107
LAN Services Implementation	108
Edge and Distribution Layer	108
Data VLAN	108
Voice VLAN	109
DMZ VLAN	109
Management VLAN	110
Access Layer	110
VLAN Trunking Protocol Implementation	110
VLAN Implementation	111
Spanning Tree Implementation	112
Uplink to Router Implementation	113
DOT1X Services	113
QoS Implementation	114
Assigning QoS to Switch Port	117
Network Fundamental Services Implementation	118
High Availability	118
Redundant WAN Link	118
IP Addressing and IP Routing	119
Routing Protocol Implementation	119
Multicast Implementation	127
DHCP Implementation	127
NAT Implementation	128
Quality of Service Implementation	129
Security Services Implementation	136

Infrastructure Protection Implementation	136
Securing Unused Ports	136
Turning Off Unused Services	137
Routing Protocol Security	141
Additional Services Measures	142
Access Control Implementation	143
Password Management	143
Secure Connectivity Implementation	143
GETVPN Key Server	144
DMVPN Implementation	145
SSL VPN Implementation	147
Threat Defense Detection and Mitigation Implementation	150
Zone-based Policy Firewall Implementation	150
Cisco IOS IPS Implementation	162
Access Control List Implementation	163
uRPF Implementation	163
Layer 2 Security	164
Port Security Implementation	164
Dynamic ARP Inspection Implementation	165
IP Source Guard Implementation	165
DHCP Snooping Implementation	166
BPDU Guard Implementation	166
Management Services Implementation	166
NetFlow Implementation	167
SNMP Implementation	167
NTP Implementation	168
IP SLA Implementation	169
Syslog Implementation	170
Cisco Configuration Professional Implementation	170
Cisco Configuration Engine Implementation	175
Downloading and Using the Configuration Templates	177
Voice Services Implementation	181
FXO and FXS Port Implementation	182
Cisco Unified CME with SCCP Endpoints Implementation	183
Cisco Unified CME with SCCP Endpoints: Telephony Service Setup	183
Cisco Unified CME with SCCP Endpoints: IP Phone Installation and Configuration	185
Cisco Unified CME with SCCP Endpoints: H.323 Voice Gateway Implementation	187
Cisco Unified CME with SCCP Endpoints: Dial Plan Implementation	187
Cisco Unified CME with SCCP Endpoints: CAC Implementation	188
Cisco Unified CME with SCCP Endpoints: Transcoding and Conferencing Implementation	189

Cisco Unified CME with SCCP Endpoints: Music on Hold Implementation	190
Cisco Unified CME with SCCP Endpoints: Voice Mail and Auto Attendant Integration	191
Cisco Unified CME with SCCP Endpoints: Emergency Services Implementation	197
Cisco Unified CME with SCCP Endpoints Verification	198
Cisco Unified CME with SIP Endpoints Implementation	200
Cisco Unified CME with SIP Endpoints: Telephony Service Setup	200
Cisco Unified CME with SIP Endpoints: IP Phone Installation and Configuration	201
Cisco Unified CME with SIP Endpoints: SIP Voice Gateway Implementation	202
Cisco Unified CME with SIP Endpoints: Dial Plan Implementation	202
Cisco Unified CME with SIP Endpoints: CAC Implementation	204
Cisco Unified CME with SIP Endpoints: Transcoding Implementation	204
Cisco Unified CME with SIP Endpoints: Music on Hold Implementation	204
Cisco Unified CME with SIP Endpoints: Voice Mail and Auto Attendant Integration	205
Cisco Unified CME with SIP Endpoints: Emergency Services Implementation	206
Cisco Unified SRST with SCCP Endpoints Implementation	206
Cisco Unified SRST with SCCP Endpoints: Telephony Service Setup	207
Cisco Unified SRST with SCCP Endpoints: IP Phone Installation and Configuration	208
Cisco Unified SRST with SCCP Endpoints: H.323 Voice Gateway Implementation	209
Cisco Unified SRST with SCCP Endpoints: Dial Plan Implementation	211
Cisco Unified SRST with SCCP Endpoints: RSVP Implementation	213
Cisco Unified SRST with SCCP Endpoints: Transcoding and Conferencing Implementation	214
Cisco Unified SRST with SCCP Endpoints: Music on Hold Implementation	216
Cisco Unified SRST with SCCP Endpoints: Voice Mail and Auto Attendant Integration	216
Cisco Unified SRST with SCCP Endpoints: Emergency Services Implementation	217
Cisco Unified SRST with SIP Endpoints Implementation	218
Cisco Unified SRST with SIP Endpoints: Telephony Service Setup	218
Cisco Unified SRST with SIP Endpoints: Cisco Unified SRST Fallback Mode at the Branch Router	220
Cisco Unified SRST with SIP Endpoints: IP Phone Installation and Configuration	221
Cisco Unified SRST with SIP Endpoints: SIP Voice Gateway Implementation	221
Cisco Unified SRST with SIP Endpoints: Dial Plan Implementation	223
Cisco Unified SRST with SIP Endpoints: RSVP Implementation	225
Cisco Unified SRST with SIP Endpoints: Transcoding and Conferencing Implementation	225
Cisco Unified SRST with SIP Endpoints: Music on Hold Implementation	228
Cisco Unified SRST with SIP Endpoints: Voice Mail and Auto Attendant Integration	228
Cisco Unified SRST with SIP Endpoints: Emergency Services Implementation	229
Caveats	230
Configuration Verification	231
Contents	231

General Configuration Verification	232
QoS Verification	233
Routing Verification	233
Security Verification	234
Voice Verification	235
Cisco Unity Express Verification	237
Cisco Wide Area Application Services Verification	237
Additional Command Reference Documentation	239

Troubleshooting	241
Contents	241
Baseline Troubleshooting Commands	241
Voice Troubleshooting Commands	242
Cisco WAAS Troubleshooting Commands	242

System Testing	243
Contents	243
Test Result Summary	243
Traffic Profile	247
Test Setups	247
Test Cases	251
WAN Connectivity Test Cases	252
Network Services Test Cases	254
High Availability Test Cases	313
Network Management Test Cases	325
Cisco Unified CME Test Cases	327
Cisco Unified SRST Test Cases	343
Performance Test Cases	360



Preface

Revised: March 25, 2009,

This guide provides a detailed blueprint for deploying a secure, converged network at a basic small enterprise branch. It describes a single branch network design to address common connectivity, security, availability, voice, and application optimization requirements for a branch office of 100 to 240 users. The design has undergone an intensive system assurance test program. The goal of this validated blueprint is to minimize the total cost of ownership (TCO) of a branch office network by accelerating and simplifying its deployment. The focus is on networking services that directly integrate into the branch office router. This guide supplements the general Cisco enterprise branch architecture documents, which can be found at:

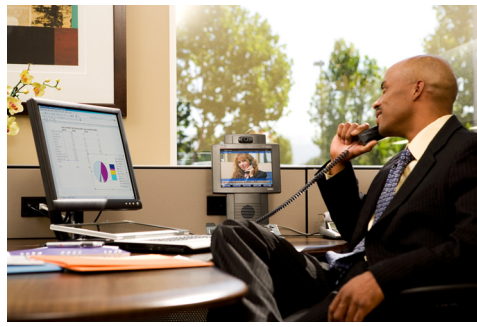
http://www.cisco.com/en/US/netsol/ns816/networking_solutions_program_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.



Basic Small Branch Network Overview

Revised: March 25, 2009

This chapter describes the Basic Small Branch Network design and components.

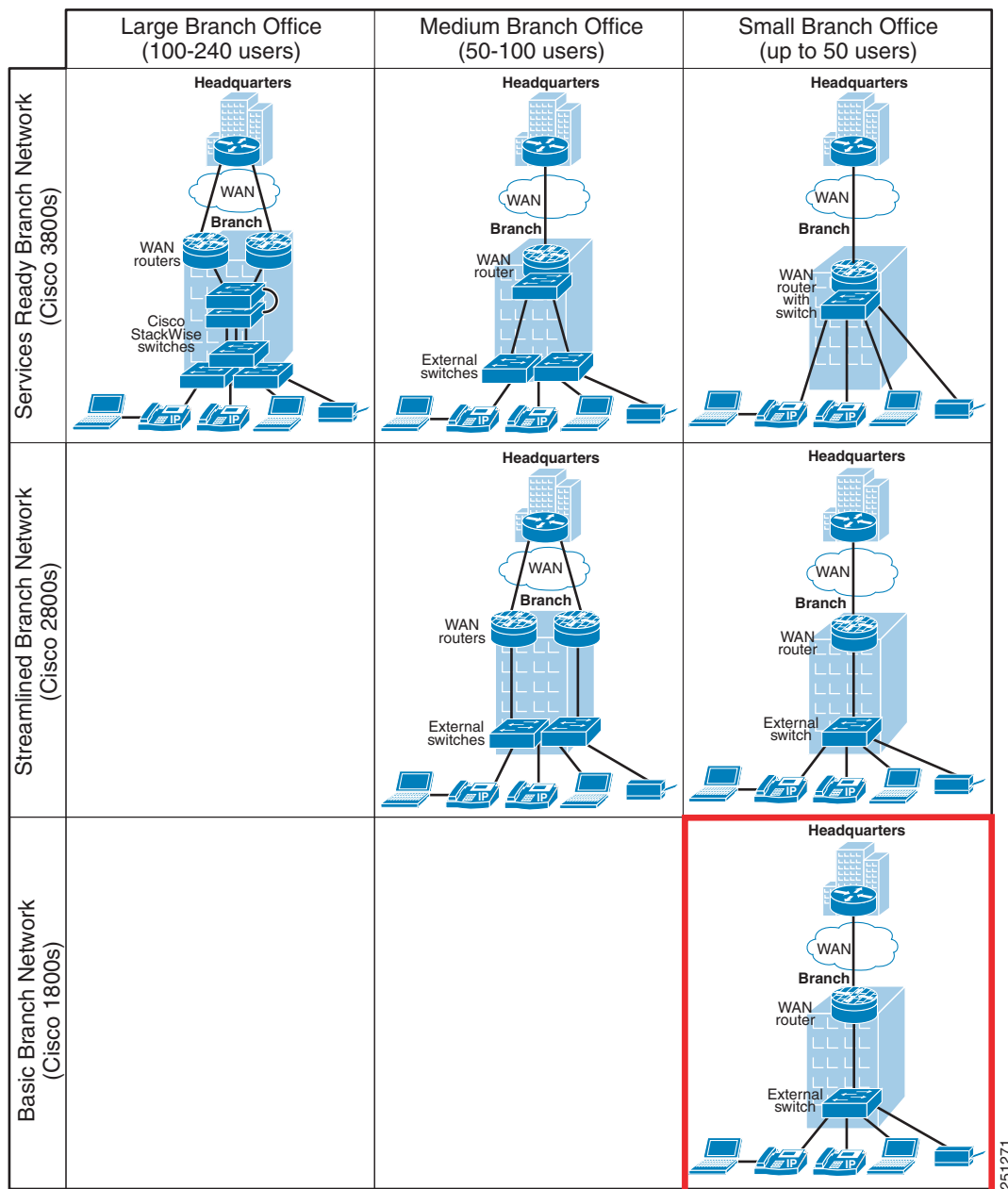
Contents

- [Introduction, page 1](#)
- [Small Branch Design Considerations, page 4](#)
- [System Design, page 7](#)
- [Topology, page 11](#)
- [Cisco Platforms and Versions Evaluated, page 13](#)
- [References and Recommended Reading, page 14](#)

Introduction

The Basic Small Branch Network enables enterprises with branch offices of up to 25 users to deploy high-value network services such as unified communication on top of a secure branch network infrastructure that is connected to a campus or data center core (central site) over a variety of WAN technologies. The goal of the Basic Small Branch Network is to make deployment of these services fast, simple, and predictable.

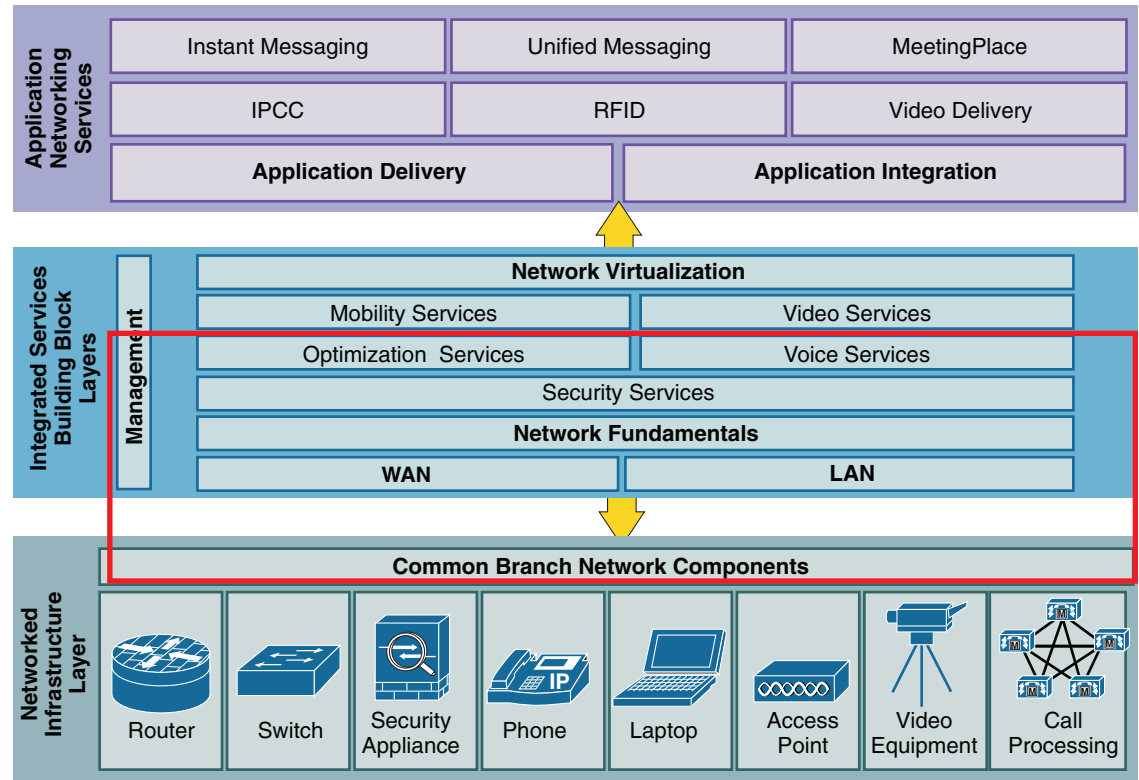
The Basic Small Branch Network is one of the Cisco Integrated Services Networks for the branch office. These networks focus on providing branch office deployment blueprints for connectivity, security, voice, and application optimization services integrated into the branch router. Integrated Services Branch Networks consist of three Services Ready Branch Networks, two Basic Branch Networks, and one Basic Branch Network, each corresponding to a different size branch office and branch router platform, as shown in [Figure 1](#).

Figure 1 *Integrated Services Branch Networks*

251271

The Integrated Services Branch Networks are implementations of the Cisco Enterprise Branch Architecture framework and focus on networking services directly integrated into the branch office router. The Framework is one component in the overall Cisco Service Oriented Network Architecture (Cisco SONA), which provides guidelines for designing advanced network capabilities into enterprise IT infrastructure. Leveraging elements of the Cisco Enterprise Branch Architecture Framework, the Cisco Integrated Services Branch Networks incorporate networking infrastructure components and the most common integrated services found in a typical branch office, as shown in the red box in Figure 2. All Integrated Services Networks have undergone an intensive system assurance test program and will be tested on an ongoing basis as individual components continue to evolve.

Figure 2 Common Integrated Services in Enterprise Branch Networks



2705991

This guide focuses on deployment of the Basic Small Branch Network. It provides design, implementation, and testing guidelines for the following features for a large branch network:

- WAN services
- LAN services
- Network fundamentals
 - IP routing and addressing
 - Quality of service (QoS)
- Security services
 - Infrastructure protection
 - Access control
 - Secure connectivity
 - Threat prevention, detection, and mitigation
- Network management
- Voice services
 - IP telephony with centralized call control
 - IP telephony with local call control
 - Traditional telephony and fax

The blueprint begins with a list of design criteria for a secure small branch office network that can be optimized for unified communications. The [“System Design” section on page 7](#) describes the network topology and network services that address these design criteria. The [“System Implementation”](#) chapter provides a step-by-step implementation of the topology and configuration of each service. Finally, testing methodology for the system is provided along with test cases and test results in the [“System Testing”](#) chapter. The [“References and Recommended Reading” section on page 14](#) lists additional detailed documents on the various technologies used in the Basic Small Branch Network.

For a list of tested platforms, interface cards, modules, and software versions, see the [“Cisco Platforms and Versions Evaluated” section on page 13](#).

Small Branch Design Considerations

Today most enterprise resources are typically located at the corporate headquarters and accessed from a branch office over a private WAN. However, certain types of applications and services continue to be deployed in the branch office. To support them, a branch network must meet additional requirements beyond basic connectivity. For the small branch office, these requirements typically include security, manageability, and telephony. The Basic Small Branch Network has been designed to meet such requirements and offers two deployment options. One provides security services for a branch office of up to 25 users. The other provides security and voice services for a branch office of up to 15 users. The following are its main design criteria:

- [Branch Network Components, page 4](#)
- [Branch Network Components for Voice-Enabled Basic Branch, page 4](#)
- [WAN Services, page 5](#)
- [LAN Services, page 5](#)
- [Network Fundamentals, page 5](#)
- [Security Services, page 6](#)
- [Network Management, page 6](#)
- [Voice Services, page 6](#)

Branch Network Components

- Up to 25 active users within the branch office
- Multiple integrated network services deployed in the branch router
- Minimal carbon footprint
- Majority of corporate resources are centrally located

Branch Network Components for Voice-Enabled Basic Branch

- Up to 15 active users within the branch office
- Multiple integrated network services deployed in the branch router
- Converged data, voice, and video network
- Minimal carbon footprint
- Majority of corporate resources are centrally located
- Telephony that supports the following use cases:
 - Moderate call volume user

- Heavy call volume user
- Decision maker
- Video-conferencing user
- Conference room

WAN Services

- Dedicated bandwidth ranging from 0.75 to 1.5 Mb/s to handle data, voice, and video traffic
- Fast Ethernet, single T1, or fractional T1 dedicated lines to WAN service providers network
- Traditional Layer 2 private WAN with various encapsulation options to guarantee privacy and reliability

or

Layer 3 Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) for increased flexibility and reduced bandwidth cost

or

Layer 2 Ethernet or MPLS VPN for greater control and simplified connectivity

LAN Services

- Hierarchical network design to simplify deployment, troubleshooting, and management
- Connectivity to branch devices at Fast Ethernet or Gigabit Ethernet speeds
- Near-wire-speed performance between all devices
- Power-over-Ethernet (PoE)

Network Fundamentals

- High availability, rapid recovery, and disaster recovery
 - Rapid recovery in case of non-redundant component failure
 - Automatic switchover to backup WAN link that has a minimum one-quarter of the bandwidth of the primary WAN link
 - Ability to restore service within 24 hours in the event of a disaster
- Quality of service (QoS)
 - Automatic application-specific traffic prioritization both within the branch office and across the enterprise WAN
 - Bandwidth management for WAN-based traffic
 - Provisions to mitigate denial of service (DoS) and worm attacks
 - Identification and classification of critical application flows for QoS
- Additional Quality of Service (QoS) for the voice-enabled branch
 - Manual application-specific traffic prioritization both within the branch office and across the enterprise WAN
 - Provisions for IP telephony, business video, critical and bulk data applications
- IP routing and addressing
 - Routing within the enterprise and between the branch and the service provider network
 - Direct Internet access from the branch

- Support for multicast applications
- Translation of private addresses and ports in order to access the Internet
- Dynamic allocation of IP addresses for end devices

Security Services

- Infrastructure protection
 - Physical securing of access to networking devices
 - Disabling of unused services that may be used to exploit the network
 - Authentication of routing protocol updates
- Access control
 - Authentication and authorization services for controlling access to network resources
 - Logging capabilities for auditing access to network devices and resources
 - Integration with global access management system to enforce access privileges
- Secure connectivity
 - Secure interoffice connectivity for full-mesh and hub-and-spoke WAN topologies
 - Secure access into the branch network for remote or home office workers
 - Voice, video, and data separation on the LAN
 - Separation of network management traffic
 - Access to the server in the branch by home office users
- Threat protection, detection, and mitigation
 - Blocking of unauthorized traffic from entering or leaving the branch
 - Access to servers in the branch by home office users
 - Verification of source addresses for incoming traffic
 - Identification and mitigation of common DoS attacks and worms
 - Prevention of malicious attacks on the branch office network from outside
 - Prevention of attacks and security breaches from within the branch office

Network Management

- Monitoring of networking services through a unified management console
- Analysis of IP services and generation of data needed for verification of service level agreements
- Ability to synchronize network time to accurately analyze network performance
- Traffic monitoring and accounting
- Common infrastructure for collecting and logging events generated by network devices
- Ability to automate initial software installation and configuration of all network devices
- Ability to automate reconfiguration of all network devices

Voice Services

- Ability to use IP-based and traditional analog telephones in the branch network
- Support for WAN-based (Toll Bypass), LAN-based (Private Exchange), and PSTN (Traditional) calling

- Ability to regulate quantity of calls placed over the WAN
- Support for voice and video calls
- Local voice mail and auto attendant
- Ability to use traditional analog fax devices
- Support for conference calling
- Transcoding of various voice codecs
- Connectivity to emergency services
- Support for multiple dial peers and plans
- Music on hold for waiting callers
- Capacity to support:
 - 5:1 user-to-active call ratio
 - 4:1 WAN-to-PSTN call ratio
 - 4:1 WAN-to-LAN call ratio
 - 2 percent of calls to be video
 - 5 percent of calls to be conferencing calls
 - 10 percent of calls resulting in a transcoding session
- Survivable central-site call control
or
Local call control

System Design

Branch network design varies greatly from one enterprise to another. Each design reflects the size, location, cost constraints, and business requirements of the corresponding branch office. However, regardless of the network architecture, a set of common branch networking elements provides:

- Network connectivity within the branch, to the Internet, and to the rest of the enterprise
- Security for data residing in the branch or crossing the network
- Unified network management and configuration
- Voice and fax services to support reliable, converged VoIP and POTS communication

To help enterprises address these common connectivity, security, management, and voice needs, the Basic Small Branch Network assembles the most important and common of these elements in a single, rigorously tested design. The goals of this design are to provide assurance that the various features interoperate and to provide a starting point for customization. The design focuses only on the services that integrate directly into the branch office router. Alternative designs that feature external appliances and provide the same functionality as the Basic Small Branch Network are equally viable.

For guidance on implementation of such designs, see the Cisco enterprise branch architecture documents at:

http://www.cisco.com/en/US/netsol/ns656/networking_solutions_program_home.html.

The following components and fundamental connectivity, security, and management services were tested in the Basic Small Branch Network:

- [Branch Network Components, page 8](#)
- [Branch Network Components for Voice-Enabled Basic Branch, page 8](#)
- [WAN Services, page 8](#)
- [LAN Services, page 9](#)
- [Network Fundamentals, page 9](#)
- [Security Services, page 9](#)
- [Management Services, page 10](#)
- [Voice Services, page 10](#)

Branch Network Components

- Cisco 1841 Integrated Services Router (ISR)
- Cisco Catalyst 2960 Switch

Branch Network Components for Voice-Enabled Basic Branch

- Cisco 1861 Integrated Services Router (ISR)
- Cisco Catalyst 2960 Switch
- Cisco Unified IP Phones 7942G, 7945G, 7961G, 7962G, 7965G, 7971G, and 7985G
- Cisco Unified IP Conference Station 7936

WAN Services

- Dedicated leased lines through service provider network
 - A T1 lines with Multilink Frame Relay, Multilink Point-to-Point Protocol (MLPPP) encapsulation
 - A ½ T1 line with PPP or Frame Relay (FR) encapsulation
 - Fast Ethernet line shaped to 1.5 Mb/s
- Virtual lines through service provider network provisioned at provider edge (PE) devices
 - Frame Relay service
 - Connectivity to service provider's PE device
 - A ½ T1 line with Frame Relay (FR) encapsulation
 - Layer 3 Virtual Private Network (L3VPN)
 - Connectivity to service provider's PE device
 - A T1 line with PPP encapsulation
 - A ½ T1 line with PPP encapsulation
 - Layer 2 Virtual Private Wire Service (VPWS)
 - Connectivity to service provider's PE device:
 - A T1 line with PPP encapsulation
 - A ½ T1 line with PPP encapsulation
 - A T1 line with Frame Relay (FR) encapsulation

A ½ T1 line with Frame Relay (FR) encapsulation

Fast Ethernet line shaped to 1.5 Mb/s

LAN Services

- Power-over-Ethernet (PoE)
- Fast Ethernet connectivity

Network Fundamentals

- High availability, rapid recovery, and disaster recovery
 - Backup WAN link with Symmetric High-Speed Digital Subscriber Line (SHDSL)
 - Routers and switches with modular, field-replaceable components
- IP addressing and routing
 - Network Address Translation (NAT)/Port Address Translation (PAT)
 - Open Shortest Path First (OSPF)
 - Enhanced Interior Gateway Routing Protocol (EIGRP)
 - Routing Information Protocol (RIP) Version 2
 - Dynamic Host Configuration Protocol (DHCP)
 - Multicast
- QoS
 - Automatic QoS (AutoQoS)
 - Shaping on the egress WAN interface
 - Class of service (CoS) to DSCP mapping with Weighted Round Robin (WRR) queuing on LAN switches
 - DSCP re-marking on LAN switches
 - Rate policing on LAN switches
 - Congestion-only queuing on LAN switches
 - Network Based Application Recognition (NBAR)
- Additional QoS for the voice-enabled branch
 - Hierarchical 8-class QoS Model using Low Latency Queuing (LLQ), Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), and Differentiated Services Code Point (DSCP)-WRED on the router
 - Policing of voice and video traffic on the egress WAN interface

Security Services

- Perimeter protection
 - Disabling of unused services
 - Console timeouts
 - Password protection
 - Secure Shell (SSH) access
 - Routing protocol security

- Access control
 - Authentication, Authorization, and Accounting (AAA) with RADIUS and TACACS+
 - Syslog
- Secure connectivity
 - Encryption with 3 DES (Data Encryption Standard) and 256-bit Advanced Encryption Standard (AES)
 - Key exchange with Diffie-Hellman Group 2
 - Data integrity with Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1)
 - Preshared key (PSK)
 - IP Security (IPsec) Dynamic Multipoint VPN (DMVPN)
 - IPsec Group Encrypted Transport VPN (GETVPN)
 - 802.1Q virtual LANs (VLANs)
 - WebVPN (SSL VPN)
- Threat Protection, Detection, and Mitigation
 - Cisco IOS Intrusion Prevention System (IPS) with advanced signature set
 - Zone-based Cisco IOS firewall
 - 802.1x
 - Port security
 - IP source guard
 - PortFast bridge protocol data unit (BPDU) guard
 - DHCP snooping
 - Dynamic Address Resolution Protocol (ARP) inspection
 - Standard and extended Access Control Lists (ACLs)
 - Unicast Reverse Path Forwarding (uRPF)
 - DoS attack and worm detection and mitigation with NBAR

Management Services

- Simple Network Management Protocol (SNMPv3)
- Cisco Configuration Professional (CCP)
- Network Time Protocol (NTP)
- IP service level agreements (SLAs)
- NetFlow version 5
- Syslog
- Cisco Configuration Engine (CCE)

Voice Services

- Cisco Unified Communications Manager (Cisco Unified CM)
- Survivable Remote Site Telephony (Cisco Unified SRST)
- Cisco Unified Communications Manager Express (Cisco Unified CME)

- Voice Gateway
- Cisco Unity Express
- Resource Reservation Protocol (RSVP) agent
- Analog lines for PSTN connectivity
- Analog device connectivity
- Emergency services
- Packet voice digital signal processing modules (PVDM)
- Fax pass-through
- Fax T.38 relay
- Transcoding
- Conferencing
- G.711 and G.729a codecs
- cRTP
- Music on hold (MOH)

Topology

The Basic Small Branch Network provides security, and network manageability for the small branch, and integrates the various network services into the branch office router. As [Figure 3](#) shows, there are two topologies.

One topology consists of a single Cisco 1861 series ISR for WAN termination, services aggregation, and LAN connectivity, and a Catalyst 2960 access switch for additional LAN connectivity. This topology features security and voice services.

The other topology consists of a single Cisco 1841 series ISR for WAN termination, services aggregation, and a Catalyst 2960 access switch for LAN connectivity. This topology only features security but supports a larger number of users.

Both topologies meet the criteria highlighted in the [“Small Branch Design Considerations”](#) section on [page 4](#).

Figure 3 Basic Small Branch Network Topology for Security and Voice Services

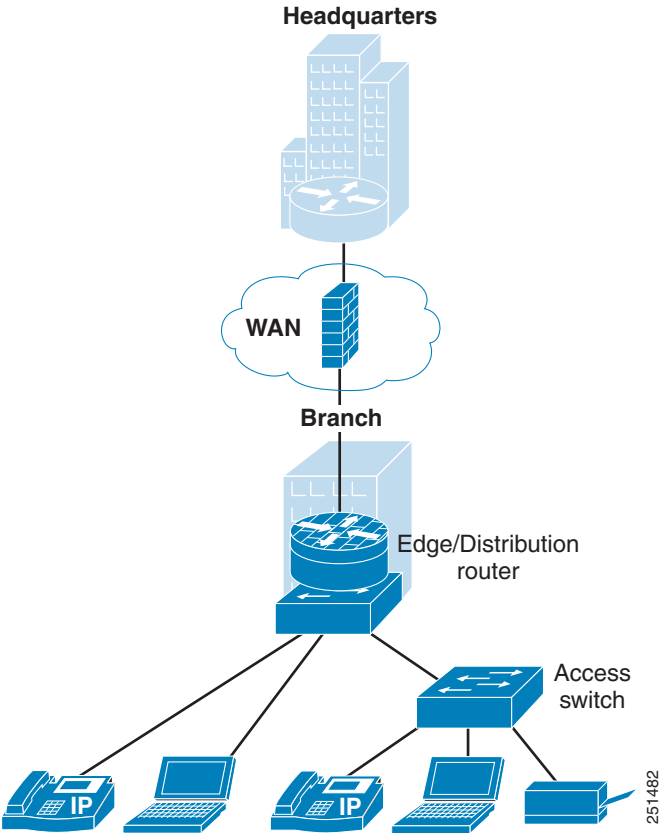
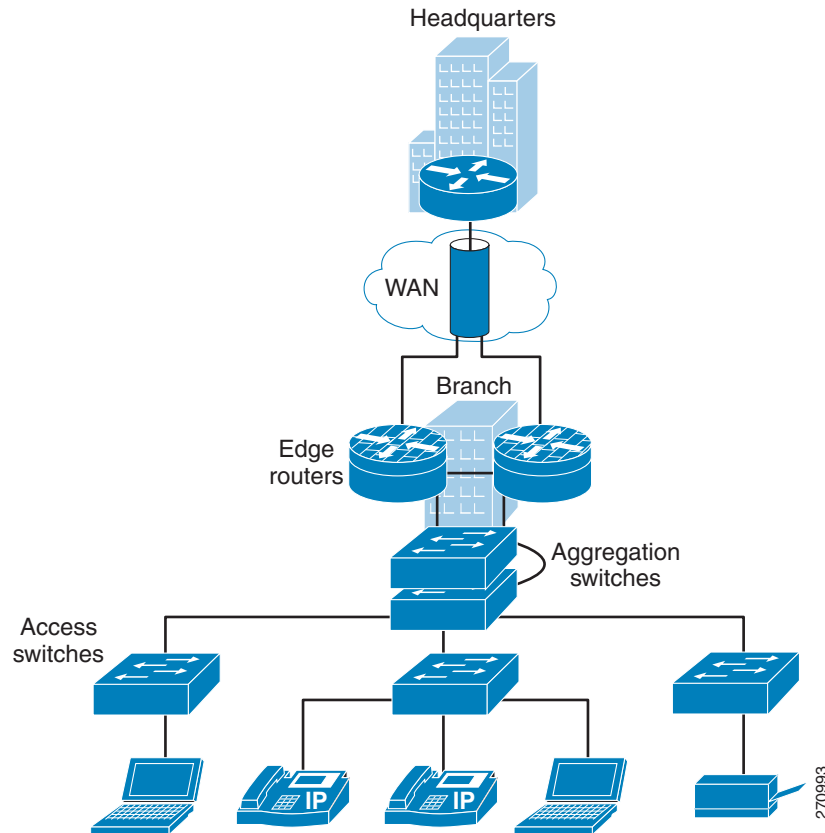


Figure 4 Basic Small Branch Network Topology for Security Services



Cisco Platforms and Versions Evaluated

The information in this document is based on the hardware and software listed in [Table 1](#) and [Table 2](#).

Table 1 Hardware Configurations

Platform	Configuration
Cisco 1861	HWIC-1T1/E1, PVDM2-32, AIM-CUE, 128 MB DRAM, 64 MB flash Cisco IOS Release 12.4(20)T2–Advanced Enterprise Services Image
Cisco 1841	HWIC-1T, HWIC-2SHDSL, AIM-VPN/SSL-2, 128 MB DRAM, 64 MB flash Cisco IOS Release 12.4(15)T7–Advanced Enterprise Services Image

Table 1 **Hardware Configurations (continued)**

Platform	Configuration
Catalyst 2960	WS-C2960G-24-TC-L, 64 MB DRAM, 32 MB flash Cisco IOS Release 12.2(25)SEE4 - IP Services Image
Catalyst 2960	WS-C2960PD-8TT-L, WS-C2960-8TC-L, 64 MB DRAM, 32 MB flash Cisco IOS Release 12.2(25)SEE4 - IP Services Image

Table 2 **Hardware and Software Versions**

Component	Version
AIM-CUE	3.1
Cisco Unified IP Phones 7942G, 7945G, 7961G, 7962G, 7965G, 7971G, 7985G	8.3.x
Cisco Unified Conference Station 7936	1.2(1)
Cisco Unified Communications Manager Express (Cisco Unified CME)	4.1
Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST)	4.1
Cisco IOS Intrusion Prevention System (Cisco IOS IPS)	5.0
Cisco Configuration Engine (CCE)	3.0

References and Recommended Reading

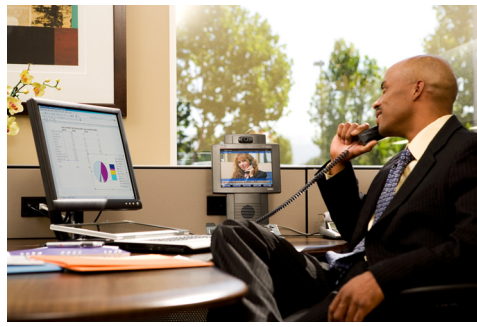
For more information on topics described in this guide, see the following documents:

- [Cisco WAFS Benchmark Tool for Microsoft Office Applications Installation and Configuration Note](#)
- [High Availability Campus Network Design—Routed Access Layer Using EIGRP or OSPF](#)
- [LAN Baseline Architecture Branch Office Network Reference Design Guide](#)
- [Enterprise QoS Solution Reference Network Design Guide](#)
- [Business Ready Teleworker Design Guide](#)
- [Enterprise Branch Security Design Guide](#)
- [Enhanced IP Resiliency Using Cisco Stateful Network Address Translation](#)
- [Stateful Failover for IPSec](#)

The following information is referenced in this guide:

- [Cisco Design Zone for Security](#)
- [Cisco IOS Configuration Fundamentals Command Reference](#)

- *Cisco IOS Debug Command Reference*
- *Cisco IOS IP Addressing Services Command Reference*
- *Cisco IOS IP Application Services Command Reference*
- *Cisco IOS IP Multicast Command Reference*
- *Cisco IOS IP Routing Protocols Command Reference*
- *Cisco IOS LAN Switching Command Reference*
- *Cisco IOS NetFlow Command Reference*
- *Cisco IOS Quality of Service Solutions Command Reference*
- *Cisco IOS Security Command Reference*
- *Cisco IOS Voice Command Reference*
- Cisco Solution Reference Network Design Guides
- *Basic Small Branch Network Quick Start Guide*
- Support—Cisco Systems



Features and Services

Revised: March 25, 2009

This chapter briefly describes all the services and features that are part of the Basic Small Branch Network design and that meet the business criteria outlined in [“Small Branch Design Considerations” section on page 4](#). The building blocks of the Cisco Enterprise Branch Architecture framework are described as they apply to the Basic Small Branch Network.

Contents

- [Branch Network Components, page 17](#)
- [WAN Services, page 25](#)
- [LAN Deployment Model, page 39](#)
- [Network Fundamentals, page 45](#)
- [Security Services, page 63](#)
- [Management Services, page 78](#)
- [Voice Services, page 84](#)

Branch Network Components

Cisco offers a broad and versatile portfolio of routers, switches, and IP Phones. There are three product lines of routers and four product lines of switches for the branch office. Each product line offers different performance and features, enabling enterprise IT departments to meet a wide range of functional requirements. [Figure 5](#) provides an overview of the various Cisco Integrated Services Routers (Cisco ISRs) that are commonly deployed in the branch office.

Figure 5 *Branch Office Integrated Services Router Portfolio*

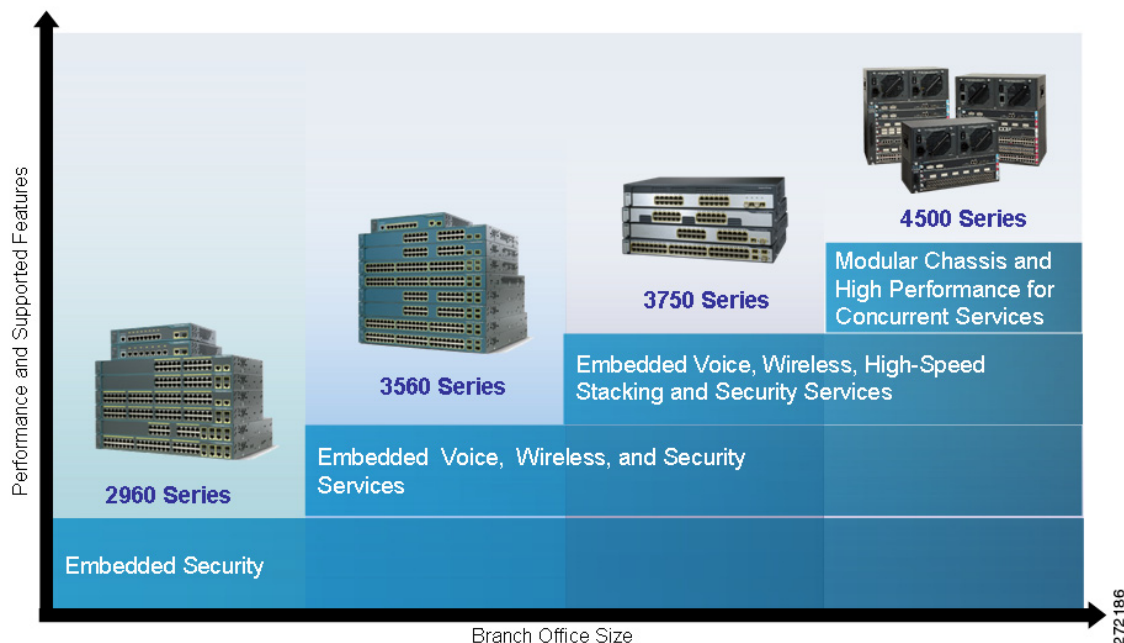


To learn more about each router product line, see the *Cisco Router Guide*:

http://www.cisco.com/en/US/prod/collateral/routers/ps5855/prod_brochure0900aecd8019dc1f.pdf

Figure 6 provides a high-level overview of the various Catalyst switches that are commonly deployed in the branch office.

Figure 6 *Branch Office Catalyst Switch Portfolio*



To learn more about each switch product line, see the *Cisco Catalyst Switch Guide*:

http://www.cisco.com/en/US/prod/switches/ps5718/ps708/networking_solutions_products_genericcontent0900aecd805f0955.pdf

There are four desktop IP Phone product lines that are suited for the branch office. Each phone offers different functions and capabilities, as shown in [Figure 7](#).

Figure 7 Branch Office Cisco Unified IP Phone 7900 Series Portfolio



To learn more about each IP Phone, visit:

http://www.cisco.com/en/US/products/sw/voicesw/products_category_buyers_guide.html#number_1

Selecting Network Components

Selecting the appropriate routing and switching platforms for a branch office involves numerous considerations. The most important considerations are:

- Branch office size: The platform must support required port densities for the expected number of end-user devices.
- Features and services: The platform must support required networking services, interfaces, and modules.
- Performance: The platform, including features and services, must handle wire speeds required by branch applications.
- Scalability: The platform must have extra slots for DRAM, flash, interface and module expansion.

In accordance with the business criteria outlined in the “[Small Branch Design Considerations](#)” section on [page 4](#), Cisco 1861 and Cisco 1841 Integrated Services Routers (ISRs) were selected for the Basic Small Branch Network.

The Cisco 1861 ISR, shown in [Figure 8](#), is ideal for small business and small enterprise branch offices. It offers embedded voice, wireless, switching, and security features. Built for converged communication, it delivers multiple concurrent services at a wire speed of up to a T1/E1/xDSL rate.

Figure 8 *Cisco 1861 Integrated Services Router*



To learn more about the Cisco 1861 ISR, visit:

<http://www.cisco.com/en/US/products/ps8321/index.html>

The Cisco 1841 ISR, shown in [Figure 9](#), offers similar performance to that of the Cisco 1861 ISR but does not support any voice features. However, it provides two High-Speed WAN Interface card slots for added modularity.

Figure 9 *Cisco 1841 Integrated Services Router*



To learn more about the Cisco 1841 ISR, visit:

<http://www.cisco.com/en/US/products/ps5875/index.html>

The Catalyst 2960 series switch was selected for the Basic Small Branch Network. Several different models are available in each product family. The selection of a specific model depends on the desired number of ports, support for PoE, and Gigabit Ethernet connectivity, and will vary from enterprise to enterprise.

The Catalyst 2960 series switch, shown in [Figure 10](#) is an ideal access layer switch for small branch-office environments. It offers Fast Ethernet and Gigabit Ethernet connectivity and concurrent QoS, ACL, port security, link aggregation, and VLAN functionality at forwarding rates of up to 39 Mb/s. For scalability, the Catalyst WS-C2960G-24-TC-L model provides up to twenty-four 10/100/1000 ports and four small form-factor pluggable (SFP) ports.

The Cisco 1861 ISR offers eight onboard switch ports. To support up to 15 users, another physically separate 8-port Catalyst 2960 switch was connected to the router. The Catalyst WS-C2960-8TC-L is a compact switch that provides concurrent QoS, ACL, port security, link aggregation, and VLAN functionality at forwarding rates of up to 2.7 Mb/s. The Catalyst WS-C2960PD-8TT-L shown in

Figure 11 adds Power over Ethernet (PoE). The main selection criterion for the Catalyst 2960 switch is to provide support for the PoE option. However, the Catalyst WS-C2960-8TC-L model was tested to provide an option for connecting devices that do not require PoE.

Figure 10 *Catalyst WS-C2960G-24-TC-L Switch*



Figure 11 *Catalyst WS-C2960PD-8TT-L Switch*



To learn more about the Catalyst 2960 switch series, visit:

<http://www.cisco.com/en/US/products/ps6406/index.html>

Cisco offers a variety of IP Phones. Selection of the appropriate phone depends on its intended usage. The most important selection criteria for Cisco Unified 7900 Series office worker IP Phones are:

- Display: The applications used on the phone determine the need for backlight, color, and touch screen.
- Line count: The expected usage determines the required number of phone lines or telephony features.
- Physical features: The amount and type of phone traffic and the applications determine the required number of buttons, the functionality of the navigation wheel, and the need to support key expansion modules.
- Video: Video conferencing requires video capabilities.

When considering an IP Phone, in general, there are numerous other features to evaluate (e.g., QoS, codec). However, all office worker Cisco 7900 Series Unified IP Phones implement the same core features required of an enterprise class IP Phone. Therefore, the above criteria are the primary considerations when selecting from the various options. To learn more about the features of the Cisco Unified IP Phones, see the *Cisco Unified IP Phone Features A - Z*:

http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/all_models/phone_a_to_z/english/user/guide/az_user.html

Business criteria outlined in the “[Small Branch Design Considerations](#)” section on page 4 specify five different use cases for IP Phones in a branch office: moderate call volume user, heavy call volume user, decision maker, video conferencing user, and conference room. For each of the first three use cases two different phones were selected.

The Cisco Unified IP Phone 7942G and Cisco Unified IP Phone 7945G, shown in [Figure 12](#), were chosen for the moderate call-volume use case. Both phones support:

- High-fidelity audio
- High-resolution display for advanced XML applications and double-byte characters/Unicode
- IEEE 803.af PoE (Class 2) or local power supply
- Access to two phone lines (or combination of line access and telephony features)
- Integrated Ethernet switch and 10/100BASE-T Ethernet connection through an RJ-45 interface for LAN connectivity
- Standards-compliant Session Initiation Protocol (SIP) support.

In addition, the Cisco Unified IP Phone 7945G phone offers Gigabit Ethernet VoIP telephony technology and a large backlit color display.

Figure 12 *Cisco Unified IP Phones 7942G and 7945G*



The Cisco Unified IP Phone 7962G GE and Cisco Unified IP Phone 7965G, shown in [Figure 13](#), were selected for the high call-volume use case. Both phones support the same features and differences as the Cisco Unified IP Phone 7942G and Cisco Unified IP Phone 7945G phones, and both phones support four additional phone lines.

Figure 13 Cisco Unified IP Phones 7962G and 7965G

The Cisco Unified IP Phone 7971G GE and Cisco Unified IP Phone 7975G, shown in [Figure 14](#), were selected for the decision-maker use case. Both phones support the following features:

- High-fidelity audio
- Gigabit Ethernet VoIP telephony technology
- Backlit high-resolution, color touch screen for easy access to communications information
- XML applications
- Integrated Ethernet switch and 10/100/1000BASE-T Ethernet connection via an RJ-45 interface for LAN connectivity
- IEEE 802.3af Power (Class 3) over Ethernet (PoE) or a local power supply
- Standards-compliant SIP phone support

In addition, the Cisco Unified IP Phone 7975G features a high-resolution screen, high-fidelity wideband audio, and Internet Low Bit Rate Codec (iLBC) support for use in lossy networks.

Figure 14 Cisco Unified IP Phones 7971G-GE and 7975G

[Table 3](#) provides a high-level feature comparison of the six IP Phone models.

Table 3 **Comparison of Cisco Unified IP Phone Models for Small Branch Offices**

Use Case	Moderate Call Volume		Heavy Call Volume		Decision Maker	
Cisco Unified IP Phone	7942G	7945G	7962G	7965G	7971G-GE	7975G
Display	Grayscale	Color	Grayscale	Color	12-bit Color	16-bit Color
Touch screen	No	No	No	No	Yes	Yes
Wideband speaker	Yes	Yes	Yes	Yes	No	Yes
Wideband handset	Yes	Yes	Yes	Yes	Accessory	Yes
Wideband headset	Supported	Supported	Supported	Supported	Supported	Supported
iLBC	Yes	Yes	Yes	Yes	No	Yes
Navigation cluster	2-way	4-way + Select	2-way	4-way + Select	4-way	4-way + Select
Gigabit Ethernet	No	Yes	No	Yes	Yes	Yes
Line keys	2	2	6 (+KEM)	6 (+KEM)	6 (+KEM)	8 (+KEM)
KEM support ¹	No	No	Yes	Yes	Yes	Yes

1. KEM: Key Expansion Module.

The Cisco Unified IP Phone 7985G, shown in [Figure 15](#), was selected for the video-conferencing use case. The phone supports personal desktop video for instant, face-to-face communications, incorporates all the components required for video calls (camera, LCD screen, speaker, keypad, and handset), provides integrated Ethernet switch and 10/100BASE-T Ethernet connection through an RJ-45 interface for LAN connectivity, and has dedicated buttons that control the video features: Self View, Picture in Picture, Video Mute, Display, and Brightness.

Figure 15 **Cisco Unified IP Phone 7985G**

The Cisco Unified IP Conference Station 7936, shown in [Figure 16](#), was selected for the conference room scenario. The conference station offers a regular telephone keypad plus three soft keys, menu navigation keys, and a backlit, pixel-based LCD display.

Figure 16 Cisco Unified IP Conference Station 7936



WAN Services

A number of WAN technologies are available to meet the diverse business requirements of an enterprise. This guide does not address considerations and issues pertaining to enterprise WAN design. However, certain aspects of WAN deployment, such as basic connectivity and routing, affect configuration of the branch office router and influence the use of specific features and services in the branch network. To ensure its relevance and applicability, the Basic Small Branch Network was validated with the most commonly deployed enterprise WANs. For detailed guidance on WAN design and implementation see the Cisco WAN design documents at:

http://www.cisco.com/en/US/netsol/ns817/networking_solutions_program_home.html.

Today enterprises have five common WAN connectivity options for the branch office. Each option, as shown in Figure 17, has its own set of benefits and trade-offs.

Private WAN

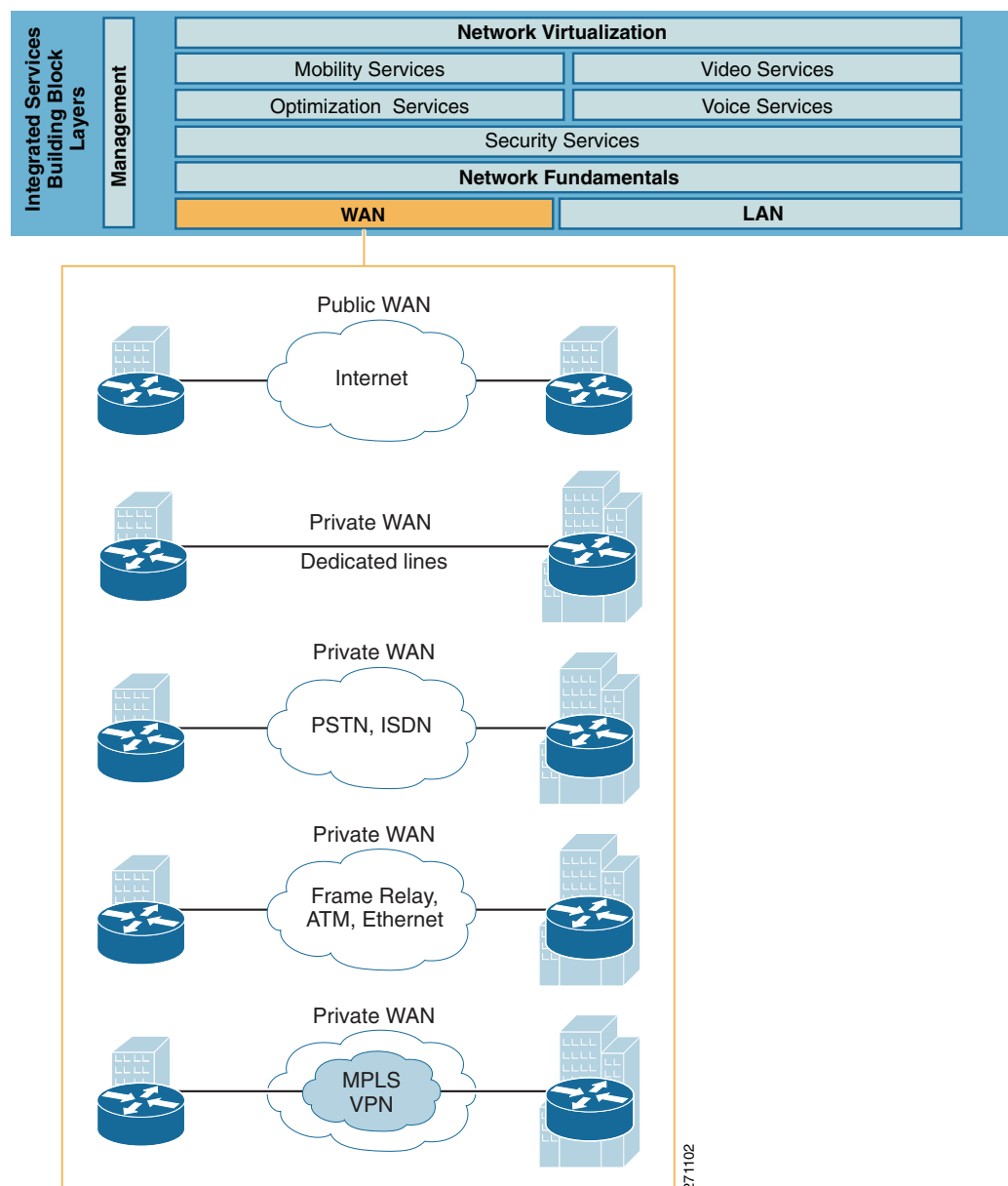
- **Dedicated leased lines:** Permanent point-to-point links connecting two fixed points across a provider network. In general, the links are based on Layer 1 (SONET/SDH, T1/E1, T3/E3, xDSL) technology. Today, because of the availability of cheaper alternatives, only branches that have special business requirements, that are geographically near a central site, or that are limited by availability of other local connection options, favor dedicated lines.
- **Circuit-switched transmission service:** Dynamically created point-to-point links over telephone wires. The links are typically based on analog dialup or ISDN technology. Today, because of bandwidth limitations and lengthy call setup, they are mainly used for voice services or as a primary link backup.
- **Packet-switched transition service:** Virtual point-to-point or point-to-multipoint links that are established over a provider-administered Layer 2 network. The provider network is based on Frame Relay, ATM, or Ethernet technology. Although this is the most widely used connectivity option for branch offices, Frame Relay and ATM as services are declining in popularity because of MPLS based alternatives. Using Ethernet implemented over SONET or using Ethernet switches is gaining popularity in the form of carrier Ethernet services (L2VPN) such as Ethernet Private Line (EPL), Ethernet Virtual Private Line (EVPL), or Ethernet-LAN (E-LAN).

- Label-switched transmission service: Virtual any-to-any links running on top of a packet or circuit-switched network. The provider network is based on MPLS technology, which is emerging as the foundation of next-generation WANs that can deliver a wide range of advanced services such as Layer 3 VPN (L3VPN), or as transport mechanisms for carrier Ethernet services (L2VPN) mentioned above.

Public WAN

- Internet broadband link: Shared any-to-any links over the Internet. This has become an attractive connectivity option in recent years for smaller branch offices as VPN technologies has matured and as broadband connectivity has become more widely available. For small branch offices, this connectivity option can be used as a primary link, as a backup link, or both. In general, broadband links are based on dialup, cable, and terrestrial or satellite wireless technologies.

Figure 17 **WAN Service Options**



Selecting WAN Service

A WAN includes transmission service available from a service provider and an access link to the service provider network. Selecting the appropriate provider network service and the access link involves many considerations. For a branch office, the most important considerations are:

- Purpose: The WAN service must provide seamless access to any site in the enterprise.
- Geographic scope: The WAN service must provide access to both regional and global sites.
- Traffic profile: For the Basic Small Branch Network, the WAN service must support up to 1.5 Mb/s of data, voice, and video traffic.
- Quality guarantee: The WAN service must provide a mechanism to ensure quality of service (QoS).
- Security: The WAN service must provide a mechanism to ensure traffic privacy.
- Existing infrastructure: The WAN service must be consistent with or must leverage existing WAN deployment.
- Availability: Selection of the WAN service must take into account local availability.
- Cost: The WAN service cost must be evaluated based on how well it meets the above considerations.

Table 4 lists advantages and disadvantages of the most commonly used WAN transmission services for a branch office.

Table 4 Common WAN Transmission Service Options for a Small Branch Office

Service Type	Advantage	Disadvantage	Appropriate for Branches
Leased Line	• Secure and private • Uncontended bandwidth • Reliable and predictable • Supports any protocol	• Expensive • Point-to-point • Fixed bandwidth	• Geographically close to campus or data center • With critical applications that require guaranteed bandwidth
Frame Relay (FR) Service	• Cost effective • Adjustable bandwidth • Extensive coverage • Secure and private • Reliable and resilient • Flexible and scalable • IP and non-IP protocols	• Variable bandwidth, latency, and jitter • Point-to-point • Inefficient QoS	• With legacy FR WAN deployment • With hub-and-spoke WAN topology • With non-IP applications

Table 4 Common WAN Transmission Service Options for a Small Branch Office (continued)

Service Type	Advantage	Disadvantage	Appropriate for Branches
Layer 3 Virtual Private Network Service (MPLS L3VPN)	• Same benefits as Frame Relay except for support of non-IP protocols • Any-to-any connectivity • QoS provisioning • Traffic engineering • Support wide variety of IP applications	• Potentially costly migration • Proprietary to service provider network • Limited global availability • Supports only IP	• Most medium and large branch offices
Layer 2 Virtual Private Wire Service (VPWS)	• Same benefits as Frame Relay • Transparent LAN integration • Low administrative overhead	• Potentially costly migration • Limited availability • Limited scalability • Point-to-point	• With enterprise control over WAN routing • With non-IP applications

In addition to these general considerations, a WAN service must meet the business criteria outlined in the “[Small Branch Design Considerations](#)” section on [page 4](#). To ensure its relevance and applicability, the Basic Small Branch Network was validated with all the WAN service options listed in [Table 4](#). Specific design considerations related to each WAN service type are described in the following sections:

- [Leased-line Deployment, page 30](#)
- [Frame Relay Service Deployment, page 32](#)
- [L3VPN Service Deployment, page 34](#)
- [VPWS Services, page 36](#)

To access the WAN service, a branch office needs a local loop to the nearest location where the provider makes the service available. Typically, this is a dedicated leased line to the edge of the provider’s network. To support up to 25 active users, the following connection types and bandwidth options are appropriate:

- A T1 or fractional T1 carrier line connected to an HWIC-1T interface, shown in [Figure 18](#)

Figure 18 1-Port Serial High-Speed WAN Interface Card (HWIC-1T) with a T1 High-Speed Serial Port



To learn more about the HWIC-1T interface card, visit:

http://www.cisco.com/en/US/prod/collateral/modules/ps5949/datasheet_c78-491363.html

Figure 19 1-Port Serial High-Speed WAN Interface Card (HWIC-1T1/E1) with a T1/E1 High-Speed Serial Port



To learn more about the HWIC-1T1/E1 interface card, visit:

http://www.cisco.com/en/US/prod/collateral/routers/ps5853/prod_data_sheet0900aecd8073cc38.html

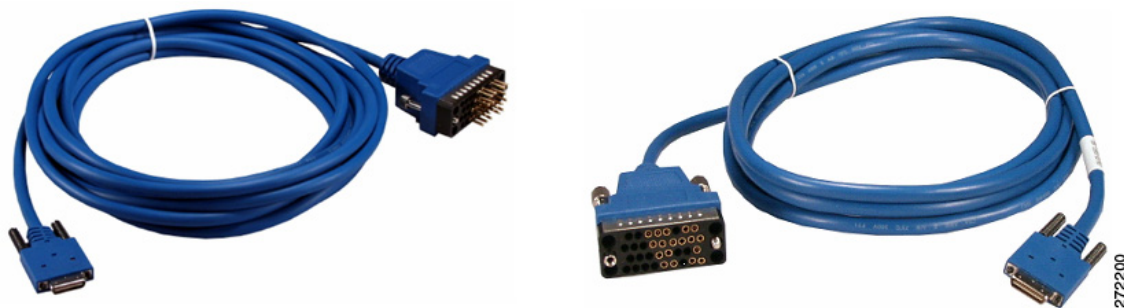
- Metro Ethernet line connected to an onboard Fast Ethernet port.

The specific selection of a WAN access link depends on the number of end user devices, the branch traffic profile, the applications used in the branch, and the available budget. The Basic Small Branch Network was validated with the two interface cards and the onboard Fast Ethernet port described previously.

Physical layer standards define the mechanical connection and electrical signaling to connect the branch router to the service provider network, which are typically done through a channel service unit (CSU)/data service unit (DSU) device that provides termination for digital signals, clocking, and synchronization, and that converts T-carrier line frames into frames that the LAN can interpret and vice versa. The branch router typically uses serial communication to connect to the CSU/DSU. The specific serial standard and socket type depend on the CSU/DSU equipment supplied by the service provider.

The Basic Small Branch Network was validated with the following serial communication specifications:

- V.35 shown in [Figure 20](#). This serial specification is typically used to connect a Cisco router to a T1/E1 and fractional T1/E1 through a CSU/DSU. A single V.35 connector can achieve up to 2.048 Mb/s speed.

Figure 20 Male (CAB-SS-V35MC) and Female (CAB-SS-V35FC) V.35 Connectors

To learn more about Cisco High-Speed Serial Interface options, visit:

http://www.cisco.com/en/US/prod/collateral/modules/ps5949/ps6182/product_data_sheet0900aecd80274416.html

Table 5 summarizes the WAN access line types, bandwidth, physical connection for the link, and ISR interface or module that provides access to the provider network.

Table 5 WAN Access Link Summary

WAN Access Line Type	Bandwidth	Physical Connection	Cisco ISR Interface or Module
1 T1 line	1.5 Mb/s	V.35 cable	HWIC-1T
1 T1 line	1.5 Mb/s	Category-5 UTP cable	HWIC-1T1/E1
½ T1 line	0.75 Mb/s	V.35 cable	HWIC-1T
½ T1 line	0.75 Mb/s	Category-5 UTP cable	HWIC-1T1/E1
Metro Ethernet line	Shaped to 1.5 Mb/s	Category-5 UTP cable	Onboard Fast Ethernet

Each deployment scenario was also validated with a backup link to the WAN. The details are described in the “Path Redundancy, Rapid Recovery, and Disaster Recovery” section on page 46.

The routing and addressing aspects of each WAN deployment are described in the IP Addressing and IP Routing, page 51.

Leased-line Deployment

When a branch office requires a permanent dedicated connection, a point-to-point leased line is used to provide a preestablished digital circuit from the branch through the service provider network to the central site. The service provider reserves the circuits for exclusive use by the enterprise. For a branch office, leased lines are typically available in fractional, full, or multiple T1/E1 or T3/E3 capacities. They are generally priced based on bandwidth and distance between the two connected endpoints. The cost of a leased-line WAN can become significant when it is used to connect a branch to many sites over increasing distance. Therefore, leased-line WANs are typically used to connect the branch to a central site, only when it is over a geographically short distance; when branch applications have critical bandwidth, latency, and/or jitter requirements; or when no acceptable alternatives are available in the geographic area. However, leased lines are used extensively to connect branches to a local point of presence (POP) that serves as an entry point into a service provider network offering other types of WAN transmission services.

Figure 21 and Figure 22 show the Basic Small Branch Network leased-line deployment scenario using the Cisco 1841 and 1861 ISRs, respectively.

Figure 21 Basic Small Branch Network Leased Line Deployment Using the Cisco 1841 ISR

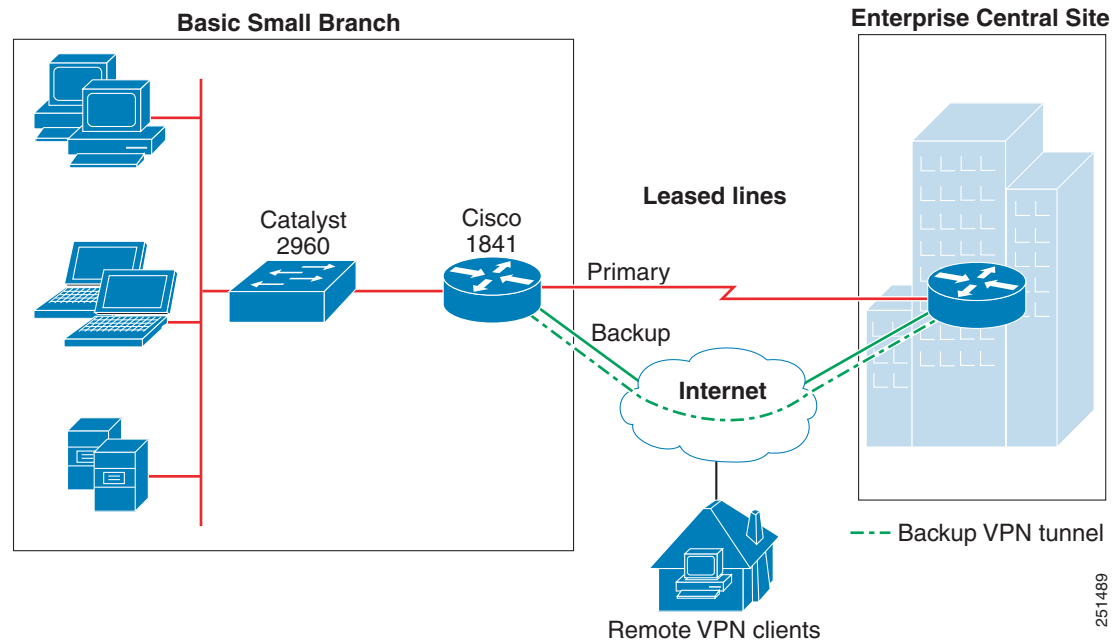
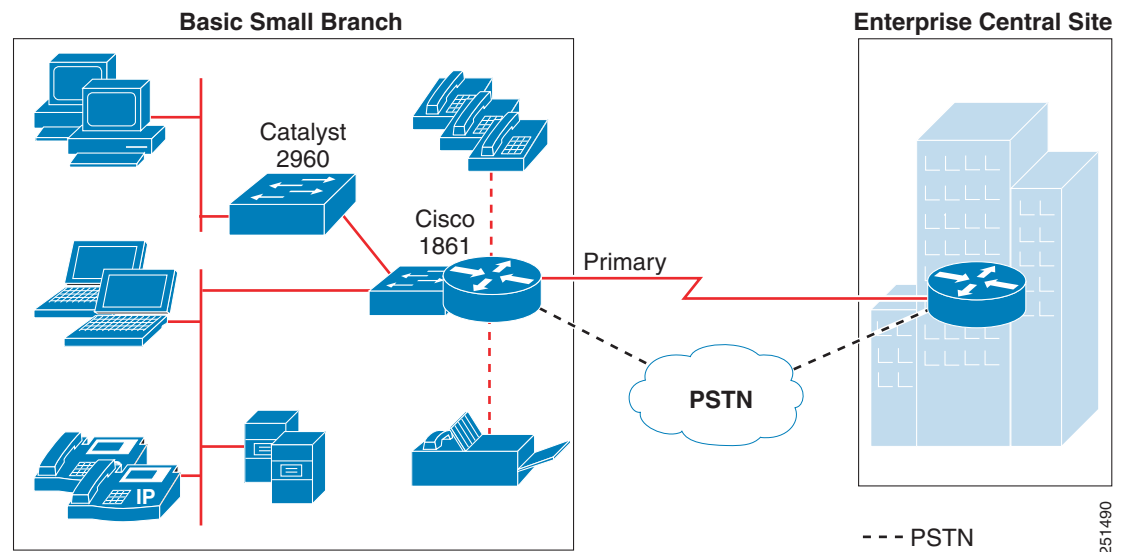


Figure 22 Basic Small Branch Network Leased Line Deployment Using the Cisco 1861 ISR



All traffic must be encapsulated by a data link layer protocol while it is crossing the WAN. The protocol defines how data is encapsulated into frames and the mechanism for transferring the frames between the branch and a central site. Selection of the data link layer protocol depends on the WAN technology and the communicating equipment in use. For leased-line WAN links, the following are the most prevalent data link protocols:

- Point-to-Point Protocol (PPP): The most popular encapsulation protocol for transporting IP traffic over point-to-point links. PPP provides asynchronous and synchronous encapsulation, network protocol multiplexing, link configuration, link quality testing, error detection, and option negotiation for capabilities such as network layer addresses or data-compression algorithms.
- Multilink Point-to-Point Protocol (MLPPP): A method for splitting, recombining, and sequencing datagrams across multiple PPP links. It combines multiple physical links into one logical link to increase available bandwidth. To learn more about PPP and MLPPP, visit:
http://www.cisco.com/en/US/tech/tk713/tk507/tsd_technology_support_protocol_home.html
- Ethernet: Various standards capable of carrying standard Ethernet frames at a rate of 100 Mb/s. Ethernet employs the same Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol, same frame format, and same frame size as its lower speed predecessors.

The Basic Small Branch Network was validated with the following combination of leased lines and encapsulation protocols:

- A T1 line with PPP
- A ½ T1 line with PPP
- Fast Ethernet

Frame Relay Service Deployment

The traditional alternative to permanent leased lines has been virtual circuits provisioned over a service provider-administered Frame Relay network. A branch office is connected to the network by attaching a point-to-point link from the branch router (DTE) to the provider's nearest Frame Relay switch (DCE). When connections are in place for both the branch and a central site, a virtual circuit is set up to allow communication between the two locations. The virtual circuit is typically configured to stay active all the time. A virtual circuit is identified by Data Link Connection Identifier (DLCI), which ensures bidirectional communication from one DTE device to another and which guarantees data privacy. A number of virtual circuits can be multiplexed into a single physical line for transmission across the network. Therefore, it is relatively easy to connect one branch office to multiple destinations.

Frame Relay is an any-to-any service over a network shared by many subscribers. The sharing allows service providers to offer lower monthly rates in comparison to dedicated leased lines. The data rate is also more flexible. Instead of one fixed rate, bursts are allowed if the network has available capacity. The downside to a shared network is a potential drop in service when traffic increases. To provide acceptable performance, service providers usually offer a minimum committed rate that is guaranteed to a subscriber. Frame Relay can provide speeds from 56 kb/s to 43 Mb/s, depending on the capability of the service provider's network.

While Frame Relay is considered legacy today, it is used extensively to implement enterprise WANs. Its primary advantages are cost and deployment flexibility. In comparison to leased lines, bandwidth is cheaper because it is shared, and only a short local loop is required to connect the branch to the nearest Frame Relay switch. Adding virtual circuits or increasing bandwidth is simple and fast.

The leased-line connection to the Frame Relay network typically uses one of the following Frame Relay encapsulation mechanisms:

- Frame Relay (FR) protocol: Specifies how data moves between the DTE and DCE over a single line. To learn more about FR, visit:
http://www.cisco.com/en/US/tech/tk713/tk237/technologies_tech_note09186a008014f8a7.shtml
- Multilink Frame Relay (MLFR): Enables multiple lines to be aggregated into a single bundle of bandwidth.

To learn more about MLFR, visit:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/17s_mfr.html

The Basic Small Branch Network was validated with the following combination of Frame Relay encapsulation protocols:

- A T1 line with Frame Relay protocol
- A ½ T1 line with Frame Relay protocol

Figure 23 and Figure 24 show the Frame Relay private WAN deployment scenario using the Cisco 1841 and 1861 ISRs, respectively.

Figure 23 *Basic Small Branch Network Frame Relay Service Deployment Using the Cisco 1841 ISR*

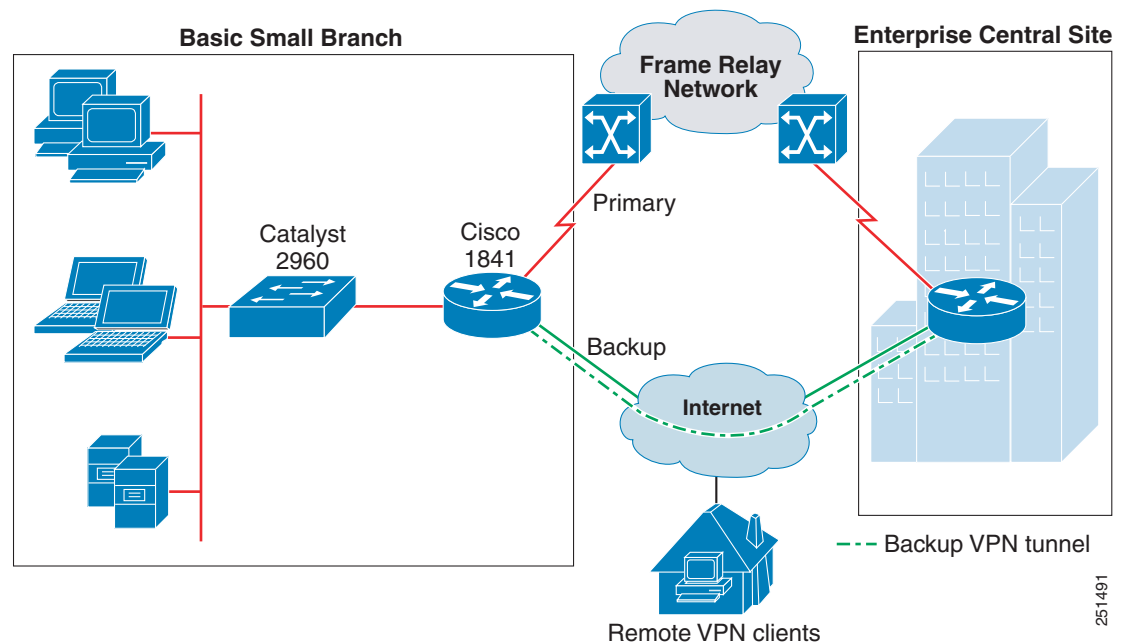
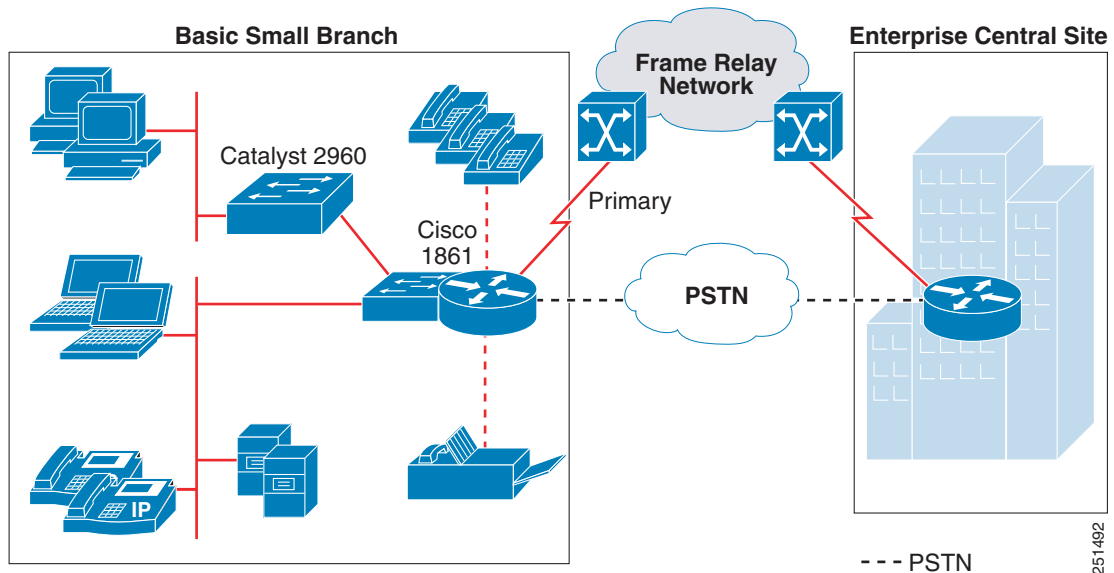


Figure 24 Basic Small Branch Network Frame Relay Service Deployment Using the Cisco 1861 ISR



L3VPN Service Deployment

Many enterprises are turning to MPLS-based WAN services because they offer cost-effective, scalable, and flexible alternatives to the traditional Frame Relay (or ATM) based private WANs. MPLS is a label-based protocol that operates between the data link layer (Layer 2) and the network layer (Layer 3). A label is imposed on a packet at the edge of the MPLS network and is removed at the other end. Label forwarding is performed by a lookup on the incoming label, which is then swapped for the outgoing label and forwarded to the next hop. Routing decisions and reachability information are based on IP addresses. Therefore, Layer 3 is also the foundation for any services offered by MPLS-based networks. Virtual Private Network (VPN) technology combined with MPLS provides traffic security and privacy. There are two general types of VPNs: enterprise-managed and service provider-managed. Layer 3 MPLS VPN (L3VPN) is a service provider-managed VPN service.

In an L3VPN WAN deployment, the provider's MPLS network routes the enterprise IP traffic. A provider edge (PE) router directly connects to the customer edge (CE) router in the branch office. The PE router communicates with the CE router via the routing protocol selected by the enterprise (RIP, OSPF, BGP, and so on). Thus, the PE router learns all of the enterprise routes and forwards the packets based on that information. The PE router also exchanges reachability information with other PE routers in the MPLS network by running Multiprotocol Border interior Gateway Protocol (M-IBGP) in the MPLS network core.

L3VPN services offer several unique advantages over traditional private WANs:

- They offer scalable any-to-any connectivity. A CE router peers with a PE router that maintains the full mesh topology. Unlike Frame Relay (or ATM), there is no complex virtual circuit topology to manage. Adding a new site to the mesh involves no other connections beyond the one connection to the PE router.
- Two branches can have overlapping address space if they are members of different VPNs.
- MPLS is IP aware and has a single control plane that matches the physical topology of the network. This allows better mapping of traffic into available resources or rapid redistribution of traffic in response to changes in the topology.

- Service providers are leveraging IP QoS to offer a full range of service guarantees for critical traffic.

The main limitation of MPLS stems from its dependence on IP. Only IP-based traffic is supported, and all other protocols must use a tunneling mechanism.

To learn more about Layer 3 MPLS VPN, visit:

http://www.cisco.com/en/US/solutions/ns340/ns414/ns465/net_design_guidance0900aecd80375d78.pdf

http://www.cisco.com/en/US/docs/net_mgmt/vpn_solutions_center/1.1/user/guide/VPN_UG1.html

The leased-line connection to the PE device typically uses one of the following data link layer encapsulation mechanisms:

- PPP: Described in the “Leased-line Deployment” section on page 30.
- MLPPP: Described in the “Leased-line Deployment” section on page 30.

The Basic Small Branch Network was validated with the following combination of access links to a PE device:

- A T1 line with PPP
- A ½ T1 line with PPP

Figure 25 and Figure 26 show the L3VPN private WAN deployment scenario using the Cisco 1841 and 1861 ISRs, respectively.

Figure 25 Basic Small Branch Network L3VPN Deployment Using the Cisco 1841 ISR

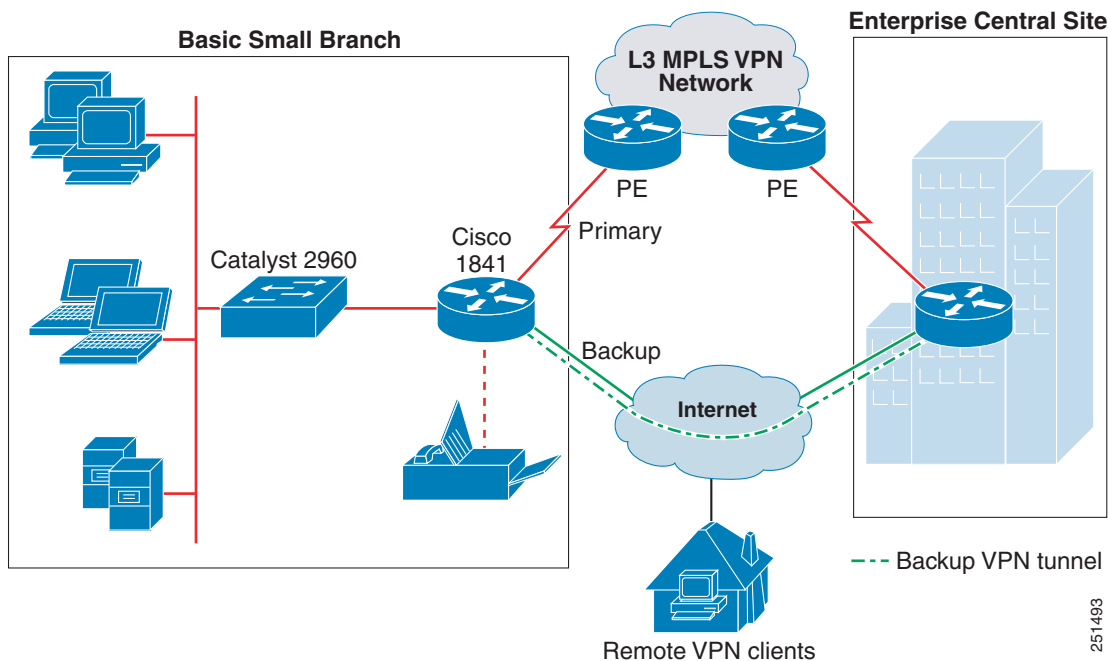
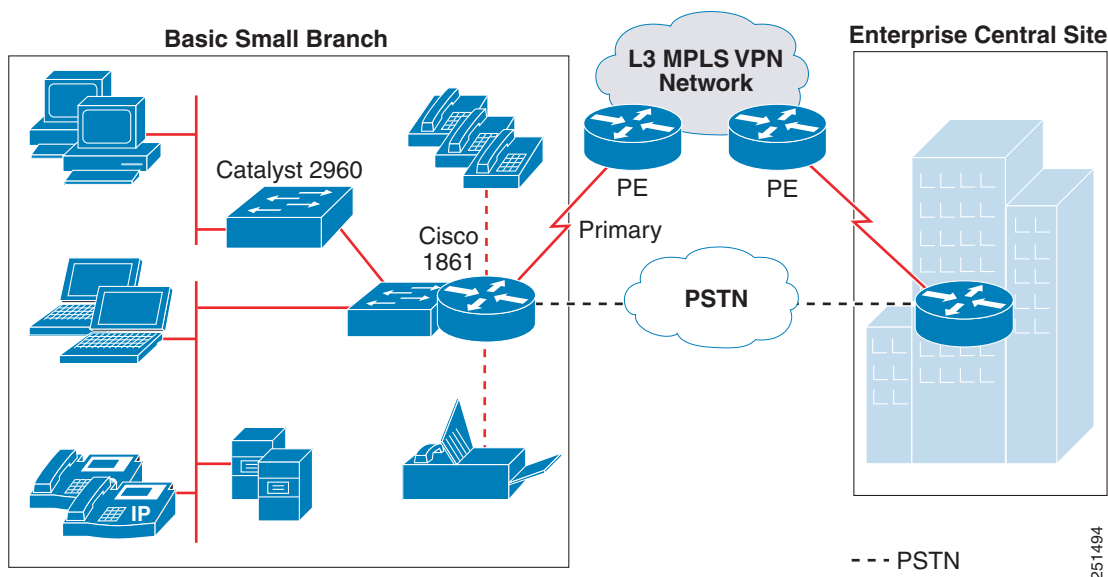


Figure 26 Basic Small Branch Network L3VPN Deployment Using the 1861 ISR



VPWS Services

For enterprises that want to retain control over Layer 2 connectivity, service providers offer Layer 2 VPNs. The following sections describe the most typically offered services.

MPLS Switched WAN Services

- Layer 3 VPNs: Described in the [“L3VPN Service Deployment”](#) section on page 34.
- Layer 2 VPNs: Emulation of Layer 2 connectivity over MPLS network
 - Virtual Private LAN Service (VPLS): The branch office Ethernet LAN is extended to the provider edge (PE) device. The provider network then emulates the function of a LAN switch to connect all customer LANs into a single bridged LAN. VPLS is a point-to-multipoint service.
 - Virtual Private Wire Service (VPWS, also called *PWE3 pseudowire*): The service provider network emulates point-to-point connections from the branch over the underlying MPLS tunnel. In general, the network emulates existing Frame Relay, ATM, Ethernet, HDLC, or PPP links. The enterprise keeps the same Layer 2 connections to the service provider, but instead of the data being carried natively over a Frame Relay or ATM service, the data is encapsulated and routed over the provider’s MPLS backbone.

Ethernet Switched WAN Services

- Permanent Point-to-Point Ethernet Line: Dedicated Ethernet circuit. The permanent point-to-point Ethernet switched WAN series are described in the [“Leased-line Deployment”](#) section on page 30.
- Virtual Ethernet Connections: Connectivity over a service provider’s shared Ethernet network.
 - E-Line: Point-to-point Ethernet services (single link configuration)

Ethernet Private Line (EPL): Dedicated point-to-point virtual line. The connection from the branch goes to a dedicated User Network Interface (UNI) device. Multiple EPLs require multiple UNIs. EPL is an alternative to dedicated leased lines.

Ethernet Virtual Private Line (EVPL): Multipoint-to-point virtual lines. A single UNI multiplexes multiple virtual connections. EVPL is an alternative to Frame Relay or ATM PVCs.

- E-Tree: Point-to-multipoint Ethernet services (hub-and-spoke configuration)

Ethernet Private Tree (EP-Tree): Single point-to-multipoint virtual lines.

Ethernet Virtual Private Tree (EVP-Tree): Multipoint-to-multipoint virtual lines.

- E-LAN: Multipoint-to-multipoint Ethernet service (full-mesh configuration)

Ethernet Private LAN (EP-LAN): Single multipoint-to-multipoint virtual lines.

Ethernet Virtual Private LAN (EVP-LAN): Multiple multipoint-to-multipoint virtual lines.

Selecting the most appropriate Ethernet-switched WAN service from this list involves several considerations. One of the first decision points is between L3VPN or L2VPN service. Table 6 provides a high-level comparison of the two options. Ultimately, the decision depends on the amount of control that the enterprise wants to retain over its WAN deployment.

Table 6 *High-Level Comparison Between L2VPNs and L3VPNs*

L2VPN	L3VPN
Provider forwards frames, based on Layer 2 information	Provider forwards packets, based on Layer 3 information
Provider involved in routing	Provider not involved in routing
Supports only Ethernet as access technology	Supports any access technology
Enterprise controls Layer 3 policies (routing, QoS)	Provider controls Layer 3 policies (routing, QoS)
Supports any Layer 3 protocol	Supports only IP
Limited scalability	Scalable

The Basic Small Branch Network was validated with Virtual Private Wire Services (VPWS). In this deployment, the service provider network acts as a Layer 2 switch. It maps incoming traffic to pseudowires based on Layer 2 headers. Figure 27 and Figure 28 show a VPWS deployment scenario using the Cisco 1841 and 1861 ISRs, respectively.

To learn more about Layer 2 MPLS VPNs, visit:

http://www.cisco.com/en/US/technologies/tk436/tk891/technologies_white_paper0900aecd80162178_ns585_Networking_Solutions_White_Paper.html

Figure 27 The Basic Small Branch Network VPWS Deployment Using the Cisco 1841 ISR

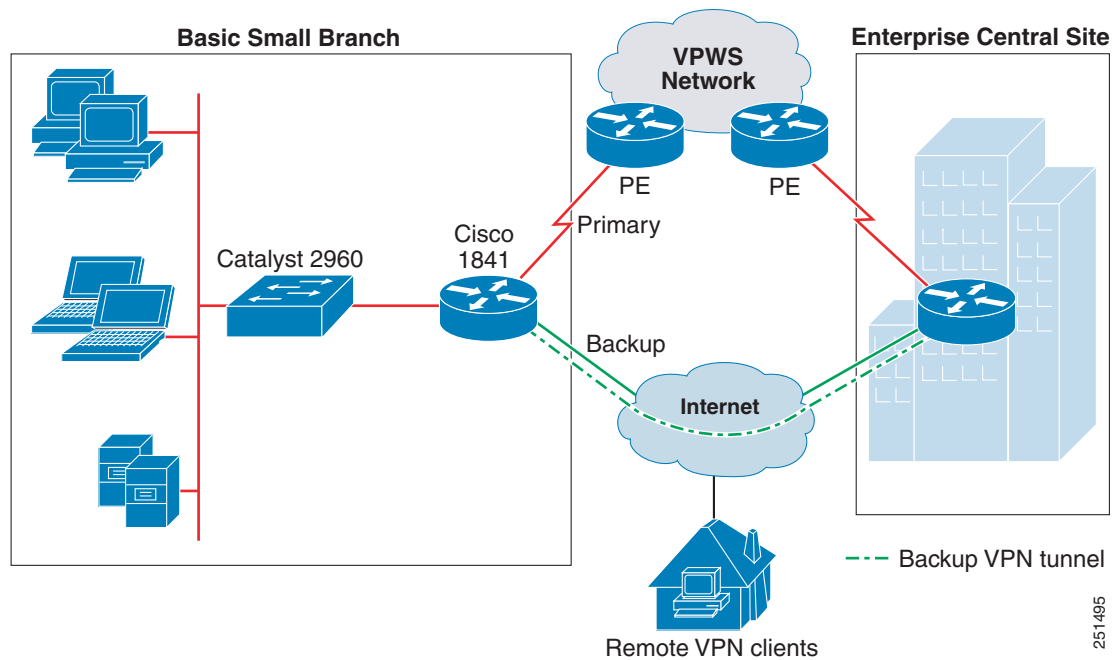
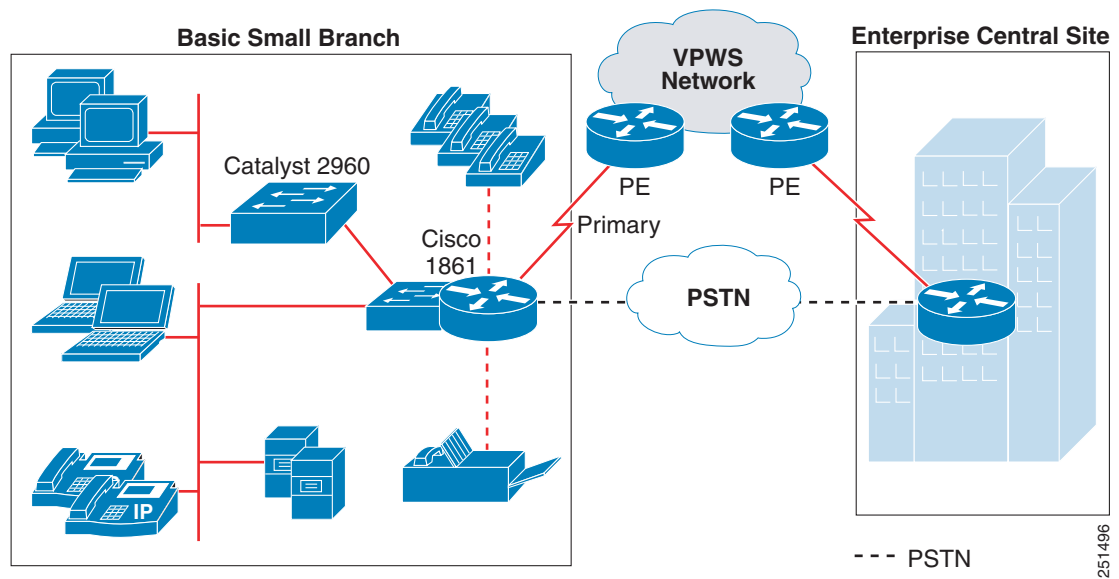


Figure 28 The Basic Small Branch Network VPWS Deployment Using the Cisco 1861 ISR



VPWS services allow the enterprise to keep its existing WAN infrastructure and to transparently connect to the service provider's Ethernet network, providing a transparent migration path to VPLS services. The leased-line connections to the PE device continue to use the typical Layer 2 encapsulation mechanism:

- PPP: Described in the [“Leased-line Deployment”](#) section on page 30.
- MLPPP: Described in the [“Leased-line Deployment”](#) section on page 30.
- Ethernet: Described in the [“Leased-line Deployment”](#) section on page 30.

The Basic Small Branch Network was validated with the following combination of access links to a PE device:

- A T1 line with PPP
- A ½ T1 line with PPP
- Fast Ethernet

LAN Deployment Model

LAN services provide connectivity for converged data, voice, and video communication. Consequently, a properly designed LAN is a fundamental requirement for performing day-to-day business functions at the branch office. Of the various ways to architect a LAN, a hierarchical design is best suited to meet the business criteria outlined in the [“Small Branch Design Considerations” section on page 4](#).

A typical hierarchical design is broken into three logical layers:

- Access layer: Interfaces with end devices, such as PCs, IP Phones, printers, and servers. The access layer provides access to the rest of the network, and it controls which devices are allowed to communicate on the network.
- Distribution layer: Aggregates the data that is received from the access layer switches, provides for data separation and forwards traffic to the core layer for routing to its final destination. It controls the flow of traffic, delineates broadcast domains, and provides resiliency.
- Edge layer: Aggregates the data that is received from the distribution layer switches and serves as an entry and exit point between the LAN and WAN. This is typically the branch router.

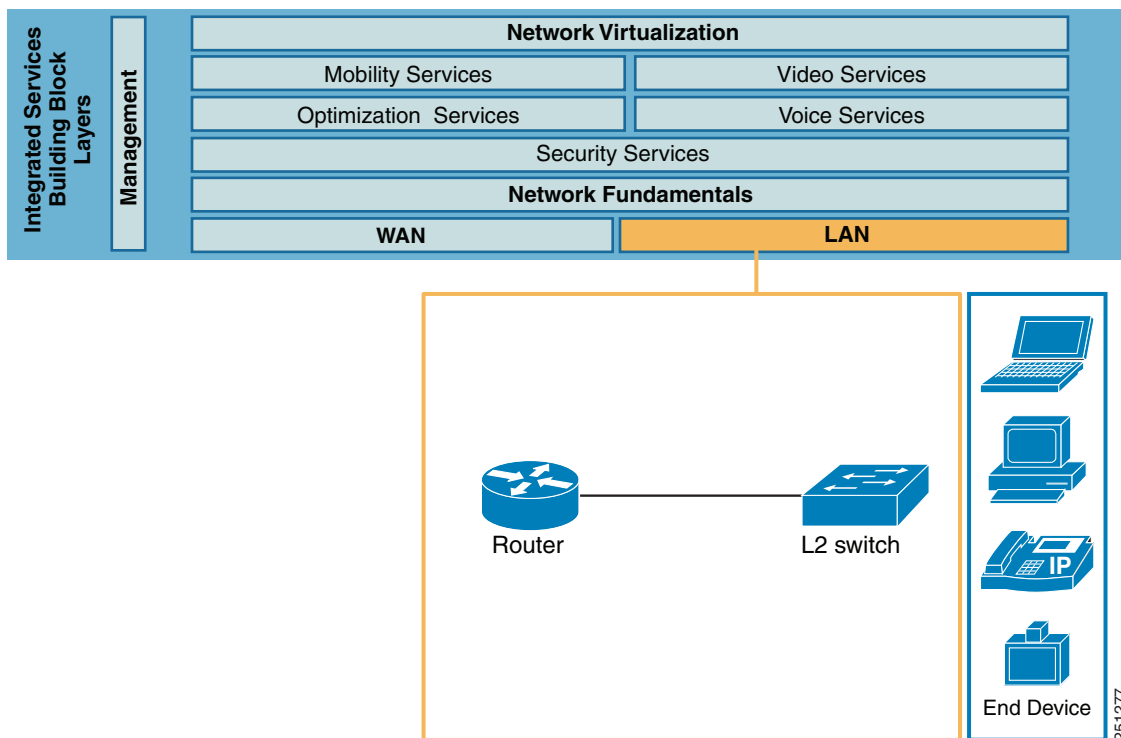
This design has the following benefits:

- Scalability: The modularity of the design provides room for easily adding devices as the network grows.
- Resiliency: Connecting the access layer switches to multiple distribution switches ensures path redundancy.
- Performance: Hierarchical layering enables fewer higher performing switches to aggregate traffic from many lower performing switches. The need for fewer higher performing switches results in both cost savings and optimal use of network devices.
- Security: Different security policies can be implemented at various levels of the hierarchy
- Manageability: All switches in one layer perform the same function, making it easy to propagate changes.

Hierarchical LAN design is only a logical layout of network devices. A Cisco ISR small branch office has three prominent physical implementation options, shown in [Figure 29](#), that map into the logical hierarchical design:

- Access router that is connected to physically separate access switch
- Access router with integrated access switch
- Access router with integrated and physically separate access switch

Figure 29 LAN Connectivity Options for Small Branch Office

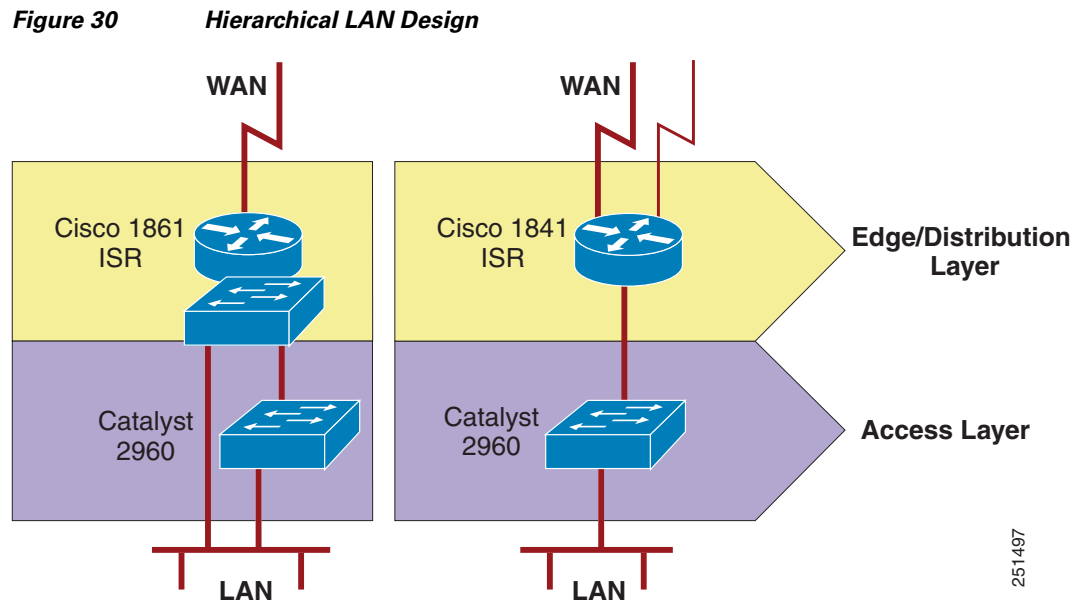


The integrated switch configuration on the Cisco 1861 provides only eight switch ports. Therefore, the router with the integrated switch implementation option does not meet the requirements highlighted in the “[Small Branch Design Considerations](#)” section on page 4. The Cisco 1841 configuration used a physically separate switch, and the Cisco 1861 configuration used a combination of an integrated switch and a physically separate switch.

For a more in-depth discussion of various branch LAN deployment options and features, see the following:

- [LAN Baseline Architecture Branch Office Network Reference Design Guide](#)
- [LAN Baseline Architecture Overview--Branch Office Network](#)

The “[Selecting Network Components](#)” section on page 19 briefly describes the Catalyst 2960 switch that was selected for the Basic Small Branch Network LAN. [Figure 30](#) shows a high-level physical topology diagram for the LAN. The Basic Small Branch Network used 1.25 end devices per user, assuming that most PCs are connected to the switch through an IP Phone. [Figure 30](#) shows one possible physical configuration for a 15- and 25-user branch office.



251497

Switches must support many features to facilitate interoffice connectivity. Features of the Catalyst 2960 switch that were leveraged by the Basic Small Branch Network are described in the following sections:

- [Virtual LANs, page 42](#)
- [VLAN Trunks and VLAN Trunking Protocol, page 43](#)
- [Power-over-Ethernet, page 45](#)
- [Spanning Tree Protocol, page 45](#)

In addition, the following features of the Catalyst switches are described in other parts of this guide:

- Layer 2 security in the [“Threat Protection, Detection, and Mitigation” section on page 76](#)
- Layer 2 Quality of Service (QoS) in the [“Quality of Service” section on page 56](#)
- Authentication services in the [“Access Control” section on page 66](#)

Access layer switches facilitate the connection of end node devices to the network. Most of these devices are equipped with a single network interface card (NIC) and therefore form only one connection to the network. If a device has multiple NICs, it can be wired to two or more access layer switches for increased resiliency. For the Basic Small Branch Network, the access layer provides the following functions:

- Voice, data, black hole, and management VLANs: Provide traffic separation and broadcast domains for voice, data, and management traffic.
- Uplink connections with VLAN Trunking Protocol (VTP) trunks to the edge and distribution layer router: Extend VLANs to the router and across the entire network.
- VTP server: Propagates VLAN information across the LAN.
- Layer 2 security: Controls the number and identity of devices that can connect to the network.
- QoS: Guarantees network resources for voice traffic and enforces proper usage of QoS by end devices.
- Authentication services: Authenticates the connecting device with RADIUS server.
- Power over Ethernet: Provides power to the connected IP Phones.
- Spanning Tree Protocol (STP): Eliminates any accidentally introduced loops from the network.

The edge and distribution layer provides:

- Connectivity, security, and management services described throughout this guide.
- Voice, data, black hole, management, and DMZ subnets: Switches interVLAN traffic.

Virtual LANs

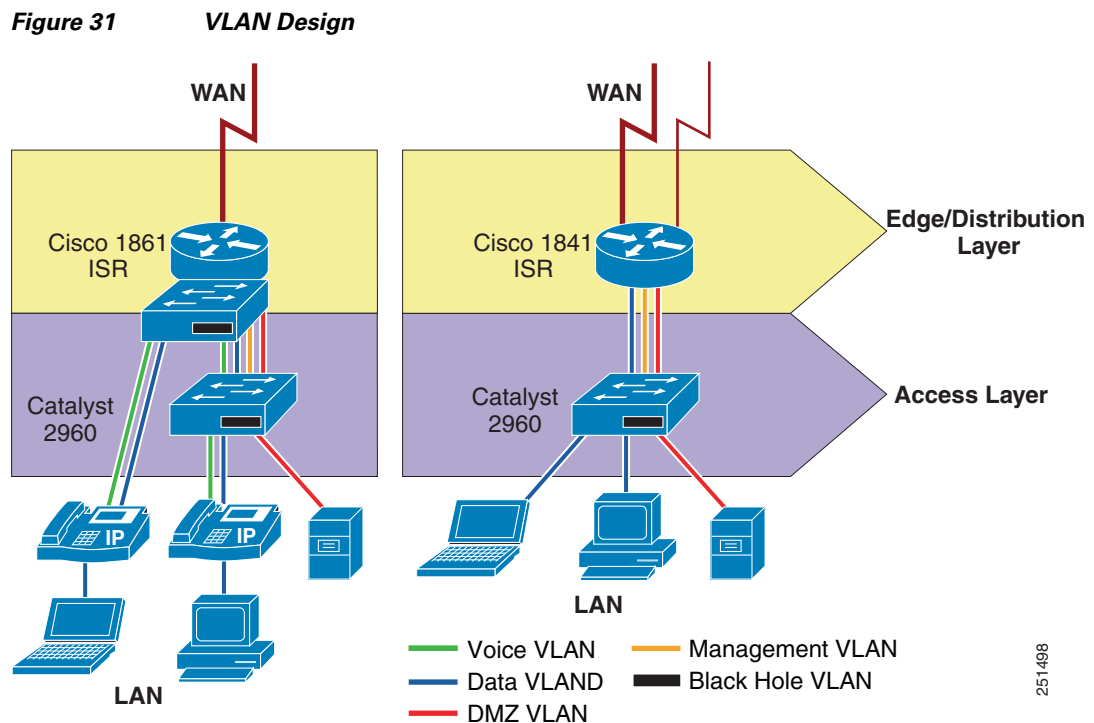
A VLAN defines a group of logically connected devices that act as an independent LAN while sharing the same physical infrastructure with other VLANs. Each VLAN is a logically separate IP subnet. A switch can carry multiple VLANs, and a VLAN can be extended across multiple Layer 2 and Layer 3 devices. VLANs offer several benefits:

- Security: Traffic in a VLAN is separated from all other traffic by Layer 2 tags.
- Performance: VLANs reduce unnecessary traffic and use bandwidth more efficiently by delimiting broadcast domains.
- Management: VLANs are managed globally, and configuration is propagated across the network.

Several VLANs were defined for the Basic Small Branch Network:

- Data VLAN: Carries traffic generated by laptops, PCs, and servers.
- Voice VLAN: Carries traffic generated by IP Phones, and singles out voice traffic for QoS.
- DMZ VLAN: Special VLAN for web, application, and database servers accessible by home office users.
- Management VLAN: Carries traffic for managing networking devices.
- Black Hole VLAN: All unused ports are assigned to this VLAN. This is a security best practice.

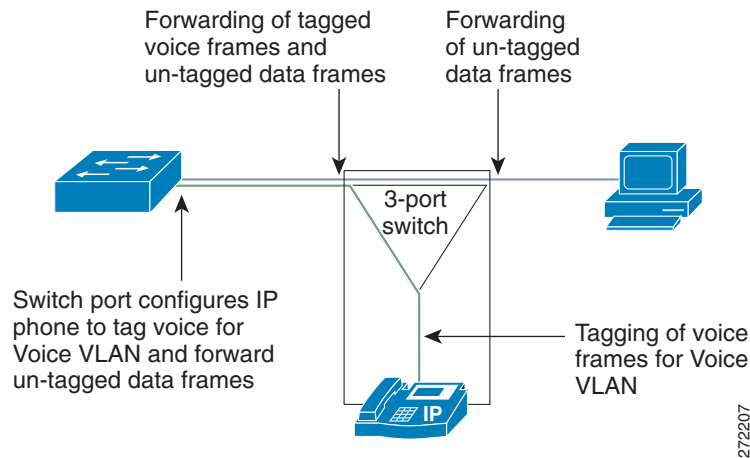
Figure 31 shows the VLAN configuration for the Basic Small Branch Network.



251498

Cisco IP Phones contain integrated three-port switches, as shown in [Figure 32](#). An access layer switch instructs the phone to tag voice traffic for voice VLAN and to forward data frames for tagging at the switch port. This allows the switch port to carry both voice and data traffic and to maintain the VLAN separation. The link between the switch port and the IP Phone acts as a trunk for carrying both voice and data traffic.

Figure 32 *Integrated Switch in Cisco Unified IP Phone 7900 Series*



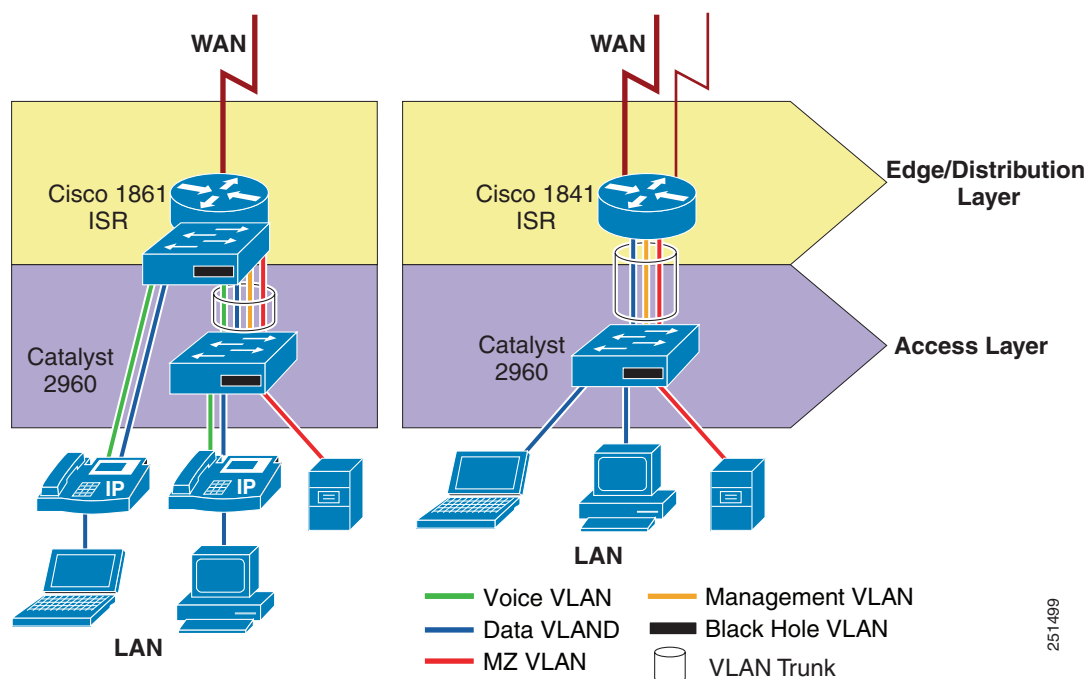
The DMZ VLAN and the black hole VLAN are described in the [“Security Services” section on page 63](#). The Management VLAN is described in the [“Management Services” section on page 78](#). In addition to the VLANs that were defined for the Basic Small Branch Network, other VLANs could be required. If the branch office has wireless access points, they should be connected to the switch and the traffic generated through these devices should be assigned to the wireless VLAN. Moreover, some networks could continue to use older equipment that does not support 802.1Q frame tagging. Isolate these devices in their own native VLAN that supports both untagged and tagged traffic.

VLAN Trunks and VLAN Trunking Protocol

VLAN trunks are point-to-point links between two Ethernet interfaces that carry traffic for multiple VLANs. They are used to extend VLANs across the entire network. VLAN Trunking Protocol (VTP) propagates VLAN information from one switch (server) to other switches in the network (clients). VTP maintains VLAN configuration consistency by managing the addition, deletion, and changes to VLANs across multiple switches.

Figure 33 shows VLAN trunks that are defined for the Basic Small Branch LAN.

Figure 33 VLAN Trunks and VTP Configuration



251499

A switch can be configured as a VTP server, as a VTP client, or in transparent mode. A VTP server distributes and synchronizes VLAN information to VTP-enabled switches. VTP clients act on that information. VTP transparent switches are unaffected, but they pass VTP advertisements to other switches. The VTP domain delimits the portion of the LAN managed by a single VTP server.

The Basic Small Branch Network consists of a single VTP domain. The access switch was configured as a VTP server as shown in Figure 33. VTP is not necessarily for a single switch network design; however, it enables the network to scale up when additional switches are introduced. In the two-switch Cisco 1861 topology, the physically separate Catalyst 2960 switch served as the VTP server to reduce the router's workload.

VTP version 2 was used in validating the Basic Small Branch Network.



Note

Always check the revision number of a new switch before bringing adding it to the network, regardless of whether the switch is going to operate in VTP client mode or operate in VTP server mode. To reset the revision number, do one of the following:

- Reboot the switch
or
- Temporarily change the domain name of the new switch and then change it back to its valid domain name.

In using VTP, it is possible to run into a “VTP bomb,” which can happen when a VTP server with a higher revision number of the VTP database is inserted into the network. The higher VTP database number will cause VLAN information to be deleted from all switches. Therefore, it is important to make sure that the revision number of any new switch introduced into the network is lower than that of the VTP server.

Power-over-Ethernet

Power-over-Ethernet (PoE) provides power to devices that are attached to the switches such as IP Phones or wireless access points. All access layer switches in the Cisco 1861 Basic Small Branch Network are provided with the PoE option. Although all access layer switches should provide PoE to support the required number of users, a non-PoE Catalyst 2960 was inserted into the Cisco 1861 Basic Small Branch Network for validation completion. The Catalyst 2960 used in the Cisco 1841 Basic Small Branch Network does not provide PoE.

Spanning Tree Protocol

Spanning Tree Protocols (STPs) are used to detect and prevent traffic loops or duplicate frames in a network with redundant paths. The Basic Small Branch Network, by design, does not have loops. However, to prevent accidental loops that frequently occur in the wiring closet or when users connect desktop switches to the network, Rapid VLAN Spanning Tree (RVST) protocol was enabled on the switch. In the two-switch Cisco 1861 topology, the physically separate Catalyst 2960 switch served as the root bridge for the protocol to reduce the router's workload

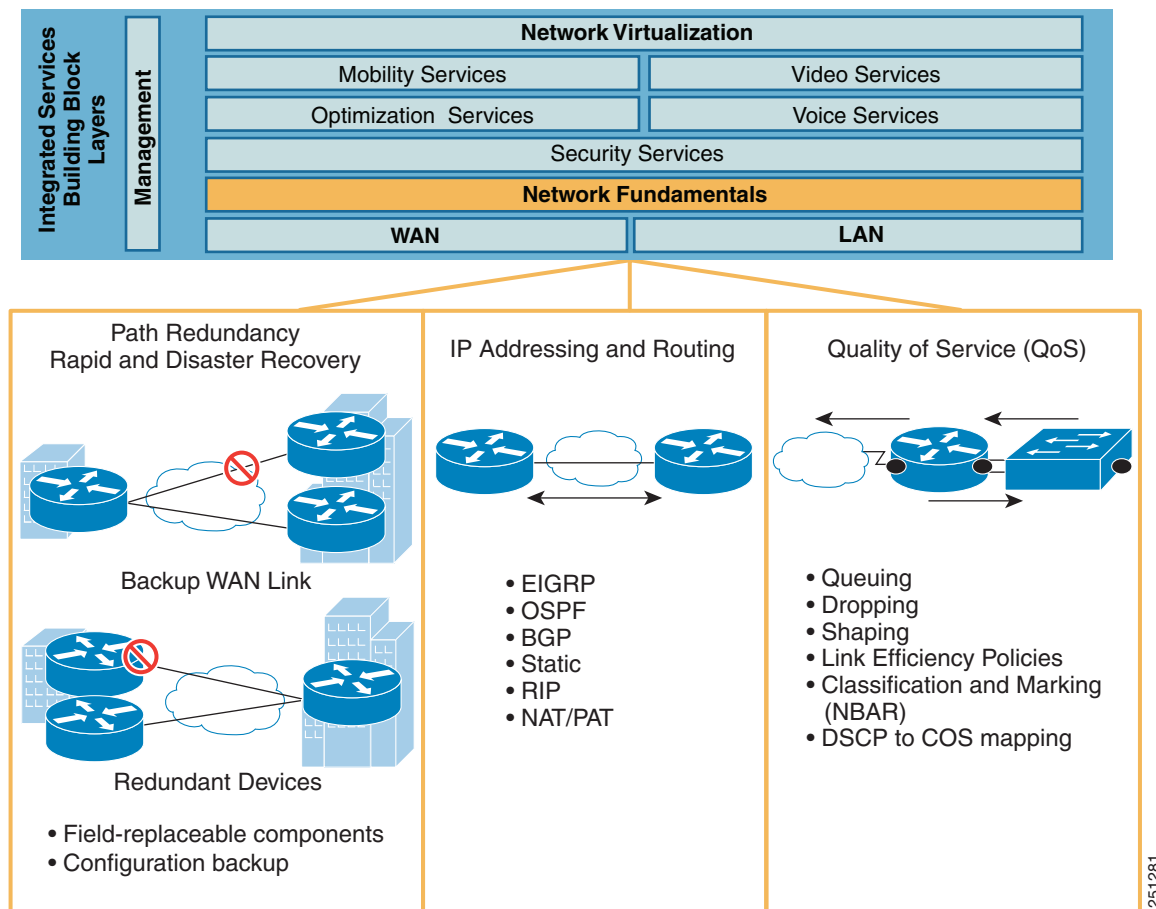
To learn more about STP, visit:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/sw_ntman/cwsi2/cwsiug2/vlan2/stpapp.htm

Network Fundamentals

Network fundamentals are the basic services required for network connectivity. These services are described in the following sections and shown in [Figure 34](#):

- [Path Redundancy, Rapid Recovery, and Disaster Recovery, page 46](#)
- [IP Addressing and IP Routing, page 51](#)
- [Quality of Service, page 56](#)

Figure 34 Basic Connectivity Services

Path Redundancy, Rapid Recovery, and Disaster Recovery

Network uptime and recovery time are critical for many types of enterprise branches. The Basic Small Branch Network achieves network availability through link redundancy. Rapid recovery is the ability of a network service to quickly recover from downtime. The Basic Small Branch Network achieves rapid recovery by using modular, field-replaceable components.

Disaster recovery is the process of restoring network services to full function after a failure-induced downtime. The Basic Small Branch Network enables disaster recovery by storing redundant copies of all device configurations on external storage devices. In addition, a Cisco SmartNet contract is recommended to provide around-the-clock, global access to the Cisco Technical Assistance Center (TAC), and 2-hour or next-business-day hardware replacement.

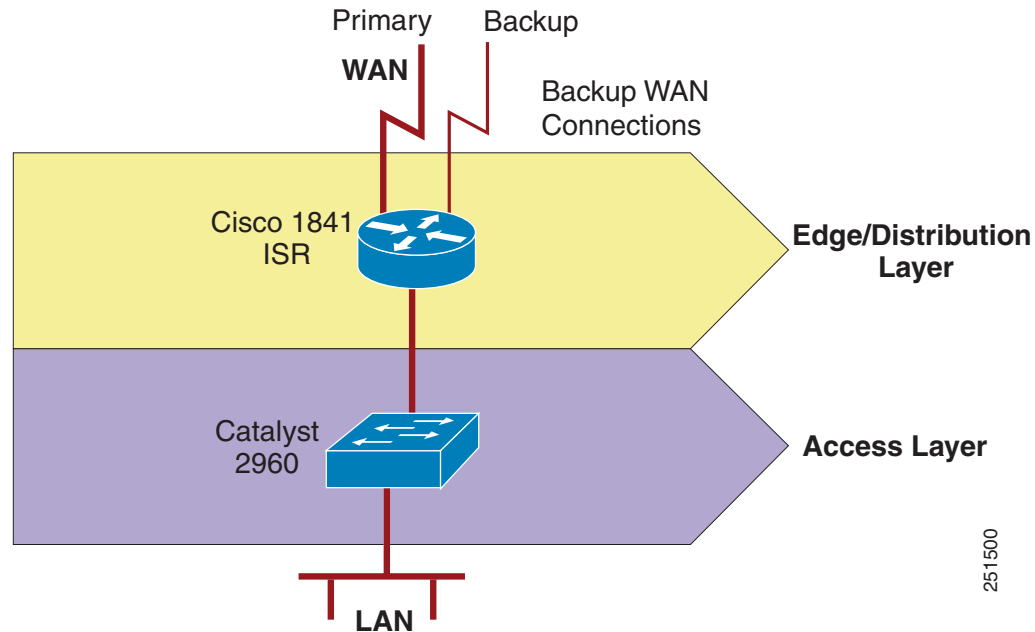
The benefits of a network design that provides high availability, rapid recovery and disaster recovery include the following:

- **Availability:** Network services are available to users when needed and as expected.
- **Minimal time to repair:** There are minimal disruptions when outages or failures occur.
- **Transparent maintenance:** Planned maintenance may be performed with minimal downtime.

The various mechanisms and features used in the different layers of the hierarchical network design to achieve high availability and rapid recovery are shown in Figure 35 and described in the following sections:

- [Backup WAN Link, page 48](#)

Figure 35 High Availability and Rapid Recovery Components



Both switch and router configuration files should be stored on an external storage device to enable disaster recovery. The Basic Small Branch Network used two different methods of storing copies of configuration files:

- Backup to centrally located TFTP server
- Password protected USB flash drive

For more information about backup and restore of configuration files to/from TFTP server, visit:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_tech_note09186a008020260d.shtml

The TFTP backup and recovery method provides fast and convenient access to the configuration files if they are needed for disaster recovery. However, because a centrally located server may not be accessible in all circumstances, locally stored USB flash token is also provided in the Basic Small Branch Network. Aladdin Knowledge Systems USB eToken, shown in Figure 36, was selected for this purpose. It requires authentication to access the configuration files encrypted and stored on the device. The eToken itself should be stored in a secure, fire- and temperature-resistant container at the branch office.

Figure 36 *Aladdin Knowledge Systems USB eToken and Cisco ISR*



To learn more about the Aladdin eToken, visit:

http://www.cisco.com/en/US/prod/collateral/modules/ps6247/product_data_sheet0900aecd80232473.html

Backup WAN Link



Note

The following section applies only to the Cisco 1841 ISR configuration.

Any of the WAN connectivity options that are described in “[WAN Services](#)” [section on page 25](#) can be used as a backup link mechanism. In practice, however, PSTN and Internet based connections are primarily used for this purpose. The main considerations when selecting the backup link are:

- Service provider: The backup link should go through a different service provider network than the primary link. There should be no or minimal sharing of back-end infrastructure by the providers.
- Service availability: Selection of backup link service must take into account local availability.
- Availability and recovery requirements: The properties and type of service expected for the backup connection.
- Cost: The backup link cost must be evaluated based on how well it meets the availability requirements.

Table 7 lists advantages and disadvantages of the most commonly used backup connections for a branch office.

Table 7 Common WAN Backup Link Options for a Small Branch Office

Service Type	Advantages	Disadvantages	Appropriate for Branches
ISDN (PRI or BRI)	- Concurrent data and voice transmission - Symmetric and dedicated bandwidth - Works over telephone wires	- Call setup - Limited bandwidth	- Telephone wires are the only connection option, and the office is too far from POP for xDSL link. - Voice is the primary traffic (use PRI). - Diversify service provider for backup.
xDSL	- Concurrent data and voice transmission - Dedicated bandwidth - Works over telephone wires - Relatively high bandwidth	- Quality dependent on wiring and distance to POP - Asymmetric bandwidth	Appropriate for most branch offices.
Cable	High bandwidth	- Asymmetric bandwidth - Shared bandwidth - Less secure	Require high bandwidth.
3G	- Easy installation - Small antenna - No cabling	- Limited bandwidth - Limited availability - Unreliable link	- Locations without wiring. - Diversify service providers for backup.
Satellite	Global coverage	- Link delay - Unreliable link - Small antenna	- Remote locations. - Diversify service provider for backup.

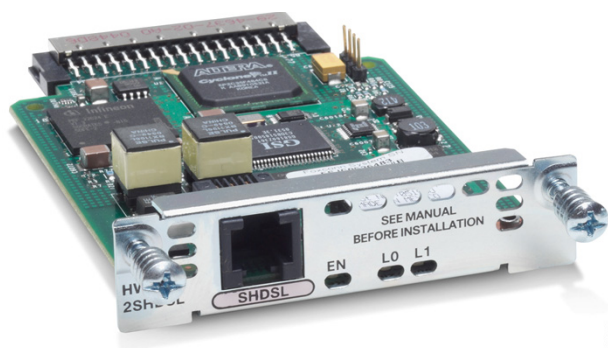
In addition to these general considerations, a backup link must meet the business criteria outlined in the “[Small Branch Design Considerations](#)” section on page 4. At present, the Basic Small Branch Network has been validated only with SHDSL as a backup WAN link. In future updates to this guide, some of the other options listed in Table 7 will be validated and documented.

All WAN deployments described in the “WAN Services” section on page 25 provide a backup link to the central site. The traffic is encrypted and directed over the Internet as shown in Figure 47. The backup link connects the branch to the nearest location where the provider makes access to the Internet service available. The link can be set to standby mode and used only for backup when the primary WAN link fails, or it can stay active and provide access to the Internet using a split tunneling mechanism. Both of these options were validated in the design.

For the Basic Small Branch Network, the following connection option was selected for backup:

- A single broadband G.SHDSL link connected to the Cisco HWIC-2SHDSL interface is shown in Figure 37

Figure 37 2-Port Symmetric High-Speed DSL (SHDSL) WAN Interface Card (HWIC-2SHDSL)



To learn more about the Cisco HWIC-2SHDSL interface card, visit:

http://www.cisco.com/en/US/prod/collateral/modules/ps5949/ps7175/product_data_sheet0900aecd80581fa0.html

Physical connectivity for the xDSL line consists of one or multiple telephone wires terminated at a DSL access multiplexer (DSLAM) in the provider’s nearest point of presence (POP). The Cisco HWIC-2SHDSL comes with a cable that directly connects its single RJ-45 port to two telephone lines terminated at one of the supported DSLAMs. Table 8 identifies the WAN backup link, bandwidth, physical connection for the link, and Cisco ISR interface that provides access to the Internet provider’s network.

Table 8 WAN Backup Line Option

WAN Backup Line Type	Bandwidth	Physical Connection	ISR Interface or Module
SHDSL with M-Pair	2.3 Mb/s	Two twisted-pair telephone wires	HWIC-2SHDSL

- xDSL Connection

Digital subscriber line (DSL) technology is a popular option for connecting home office workers and small branch offices to the enterprise network. In a large branch office, it is used mainly as a backup link. DSL creates an always-on connection that uses existing telephone wires to transport high-bandwidth data and to provide IP-based services. A DSL modem converts digital signals to and from analog signals. At the telephone company POP, a DSLAM is used to redigitize the signal and forward it to the Internet service provider. There are various DSL standards, all under the general name xDSL, for various x. The Basic Small Branch Network office used single-pair high-speed DSL (G.SHDSL).

The universal choice of Layer-2 encapsulation protocol for use on xDSL lines is asynchronous transfer mode (ATM). ATM adaptation layer (AAL) is a mechanism for segmenting upper-layer information into ATM cells at the transmitter and reassembling them at the receiver. AAL5 provides support for segmenting and reassembling routed/switched protocols over ATM permanent virtual circuits (PVCs) using Logical Link Control Layer (LLC)/Subnet Access Protocol (SNAP) or virtual channel multiplexing (VCMUX). LLC/SNAP adds an extra header that allows multiplexing of multiple protocols over the same PVC circuit. VCMUX allows multiple virtual circuits (VCs) on the xDSL link and maps each protocol to a different VC. For simplicity, AAL5+SNAP encapsulation was chosen for the Basic Small Branch Network.

ATM M-Pair allows bundling of several xDSL lines to form a single logical link of higher combined bandwidth. Two telephone lines were bundled together in the Basic Small Branch Network to create a bandwidth of 2.3 Mb/s.

In summary, the Basic Small Branch Network used the following xDSL configuration:

- G.SHDSL with 2-line M-Pair and AAL5+SNAP encapsulation

IP Addressing and IP Routing

Cisco offers a broad portfolio of IP routing and addressing technologies. Only some of these technologies are relevant to branch offices. To meet the design criteria in the “[Small Branch Design Considerations](#)” section on page 4, the Basic Small Branch Network was deployed with the following IP routing and addressing services enabled in the Cisco IOS software on the routers:

- [Routing Protocols](#), page 53
- [Multicast](#), page 55
- [DHCP](#), page 55
- [NAT and PAT](#), page 55

When assigning IP addresses to the various devices in the branch office, it is important to follow the IP addressing scheme and conventions set for the entire enterprise network. Today, enterprises use classless IP addressing, classless IP routing protocols, and route summarization. The Basic Small Branch Network uses a private addressing scheme allocated from the 10.0.0.0/22 address pool that has 1022 available hosts. The design assumes that a single user will need two IP addresses: one for the PC and another for the IP Phone. The other addresses are used for server and network devices, or are left unallocated.



Note

The Voice VLAN applies only to the Cisco 1861 ISR configuration.

The address pool is divided among VLANs as follows:

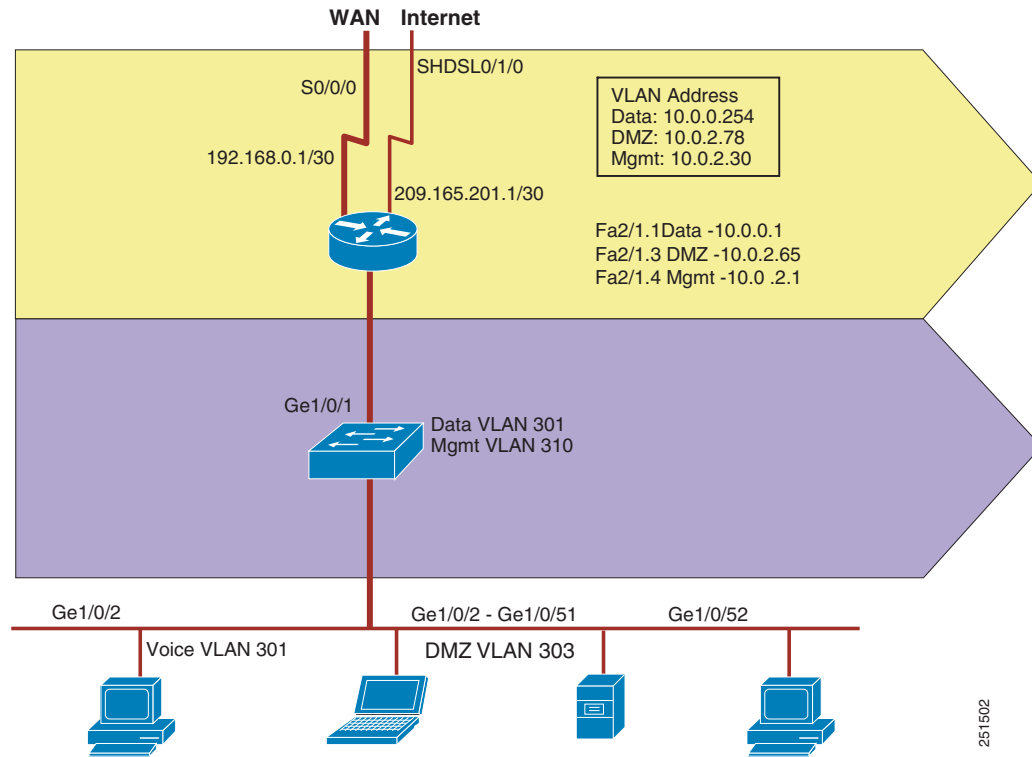
- Voice VLAN: 254 addresses
- Data VLAN: 254 addresses
- DMZ VLAN: 14 addresses
- Management VLAN: 30 addresses
- Black hole VLAN: 30 addresses

[Table 9](#) shows the address assignment, and [Figure 38](#) and [Figure 40](#) show the corresponding topologies. The addressing scheme is only an example. Each enterprise should follow its own addressing scheme.

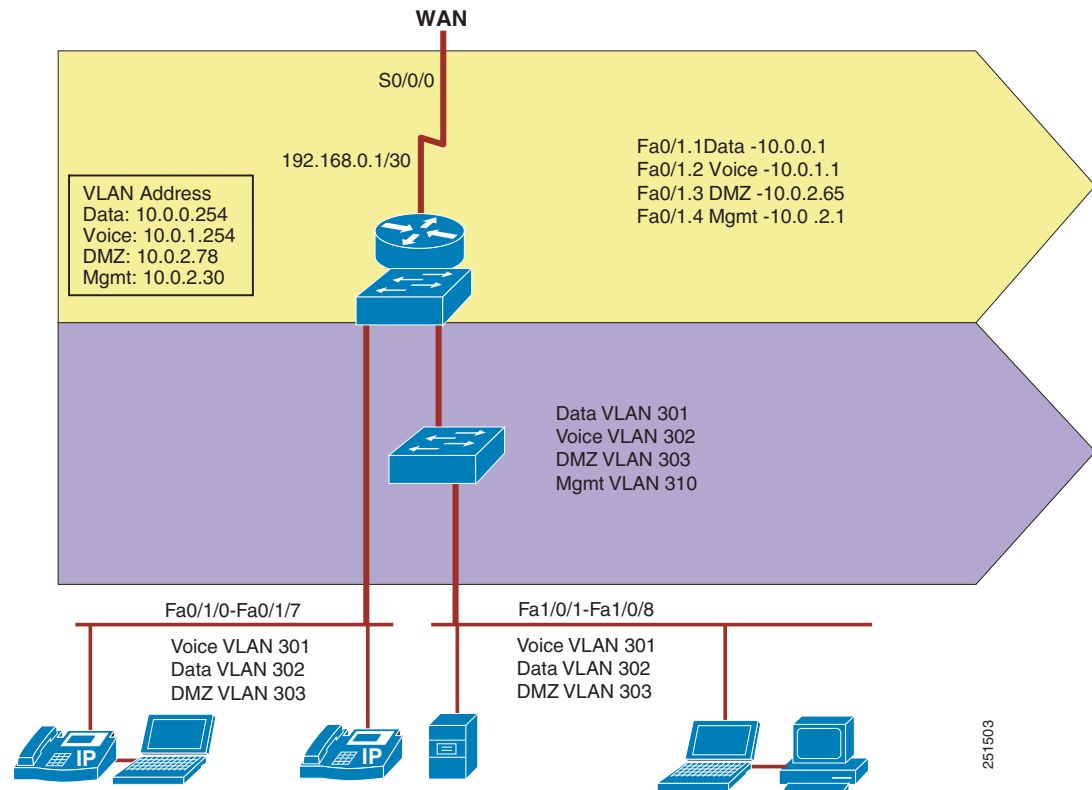
Table 9 Sample Address Assignment Scheme for the Basic Small Branch Network

Component	Network
Data VLAN	10.0.0.0/24
Voice VLAN	10.0.1.0/24
Management VLAN	10.0.2.0/27
Black Hole VLAN	10.0.2.32/27
DMZ VLAN	10.0.2.64/28

Figure 38 Sample Address Assignment for the Basic Small Branch Network



251502

Figure 39 Sample Address Assignment for the Basic Small Branch Network

Routing Protocols

Several routing protocols are relevant to the branch office. Although there are design differences among these routing protocols, all have a common goal of stability, availability, fast convergence, and high performance. However, no one protocol is best suited for all situations, and trade-offs must be considered when deciding on the appropriate one. The following are the most common routing protocols:

- **Static routing:** Manually defined routes as next hops to various destinations. Static routes are generally used in very small networks or when the routing is managed by the service provider. In a branch, a static route is typically used to forward traffic to the Internet service provider network.

For more information about static routes, visit:

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800ef7b2.shtml

- **Routing Information Protocol version 2 (RIPv2):** Distance vector protocol now considered a legacy. It is should be used only in small legacy networks that have little need to grow.

For more information about RIP, visit:

http://www.cisco.com/en/US/tech/tk365/tk554/tsd_technology_support_sub-protocol_home.html

- **Enhanced Interior Gateway Routing Protocol (EIGRP):** Enhanced distance vector protocol proprietary to Cisco. Unlike traditional distance vector protocols, EIGRP does not age out routing entries or uses periodic updates. The Distributed Update Algorithm (DUAL) algorithm is used to determine the best path to a destination network. The EIGRP protocol maintains a topology table that includes both the best path and any loop-free backup paths. When a route becomes unavailable,

the DUAL algorithm finds the best backup path to the destination. The protocol uses bandwidth and delay to select the preferred path, and can optionally include link reliability and jitter. EIGRP works best in small to medium-sized networks that have a flat design and use only Cisco routers.

For more information about EIGRP, visit:

http://www.cisco.com/en/US/tech/tk365/tk207/tsd_technology_support_sub-protocol_home.html

- Open Shortest Path First (OSPF): Link state protocol standardized by EITF. OSPF floods link state information to its neighbors and builds a complete view of the network topology. The Shortest Path First (SPF) algorithm is used to determine the best path to a destination. The protocol uses bandwidth to determine the best path, or can be optionally forced to use a manually defined cost for a path. OSPF works best in networks that are large, have a hierarchical design, have a mixture of Cisco and non-Cisco routers, are expected to grow to a large scale, or require fast convergence time.

For more information about OSPF, visit:

http://www.cisco.com/en/US/tech/tk365/tk480/tsd_technology_support_sub-protocol_home.html

Choosing the appropriate routing protocol in most cases depends on the routing protocol currently used in the enterprise network. Therefore, to ensure its relevance and applicability, the Basic Small Branch Network was validated with all of the routing protocols listed.



Note

The following section applies only to the Cisco 1841 ISR configuration.

In all WAN deployments, with the exception of Layer 3 Virtual Private Network (L3VPN), the enterprise manages routing. RIPv2, EIGRP, or OSPF is used to route traffic on the primary link. Both the primary and backup links have a default static route to either the PE or the ISP router. With a standby mode backup interface configuration, the backup default route is automatically inserted into the routing table only after the backup interface becomes active. With an active mode backup interface configuration, the primary default route was assigned a lower cost than the backup default route. The primary default route became active and started directing Internet traffic to the central site only after the backup link failed, and its default route was removed from the routing table.

VPN access by the Basic Small Branch Network is accomplished by the following:

- Split Tunneling

The Basic Small Branch Network provides direct access to the Internet through split tunneling. To access the Internet, NAT and PAT are used to map the branch network private addresses to public addresses. See the “NAT and PAT” section on page 55. Split tunneling is accomplished by running a separate routing process for the Internet-bound traffic. There are four options for split tunneling in the Basic Small Branch Network, depending on the type of VPN used for the primary link and whether the backup interface is in active or standby mode. The “Routing Protocol Implementation” section on page 119 provides detailed configurations. The following are the four different options:

- Active/Standby Primary/Backup WAN links with DMVPN
- Active/Standby Primary/Backup WAN links with GETVPN
- Active/Active Primary/Backup WAN links with DMVPN
- Active/Active Primary/Backup WAN links with GETVPN

- Remote User Access

In the Basic Small Branch Network, remote office workers have direct access to the DMZ VLAN over SSL VPN. The users connect to the SSL VPN gateway that is running in the branch office.

Multicast

IP multicast was enabled in the Basic Small Branch Network for applications that take advantage of multicast technologies, such as video conferencing, corporate communications, distance learning, and distribution of software. Cisco Protocol Independent Multicast (PIM) was used to forward multicast traffic. The protocol leverages the router's unicast routing table populated by IGP protocols to maintain a multicast routing table that is used strictly for multicast traffic. PIM does not send routing updates, and it relies on IGP protocols to keep routing information up-to-date.

There are several modes of operation for PIM. In dense mode, the router floods multicast traffic to all interfaces except the one through which the multicast packet arrived. In sparse mode, multicast receivers request multicast traffic to be forwarded to their network segment. This information is propagated between the PIM-enabled network nodes. Sparse-dense mode allows an interface to be configured in both modes in order for different multicast groups to leverage either propagation mechanism.

To learn more about multicast, visit:

http://www.cisco.com/en/US/tech/tk828/tech_brief09186a00800a4415.html

DHCP

Dynamic Host Control Protocol (DHCP) was enabled in the Basic Small Branch Network to automatically assign and manage end device IP addresses from specified address pools within the router.

When a DHCP-enabled end device is connected to the network, the end device first sends out a DHCP discovery request. Then, any available DHCP server offers a lease for an IP address to the end device. However, before the IP address can be assigned, the DHCP server must first check that no other device is currently using this same address. To perform this check, the DHCP server pings the address and waits for the response. When the end device receives a lease offer, it then returns a formal request for the offered IP address to the originating DHCP server. The server confirms that the IP address has been exclusively allocated to the end device.

Any servers running in the branch should use static addressing. Only PCs and IP Phones should rely on DHCP for address assignment. There is a special consideration for IP Phones. They must be registered with Cisco Unified Communications Manager (Cisco Unified CM). If the active router fails, a lease renewal would force the phones to reregister with the Cisco Unified CM or Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) agent, which would make the phones unavailable for the period of reregistration.

To learn more about Cisco IOS DHCP server, visit:

http://cco.cisco.com/en/US/docs/ios/12_0t/12_0t1/feature/guide/Easyip2.html

NAT and PAT



Note

The following section applies only to the Cisco 1841 ISR configuration.

To access the Internet directly from the branch office, Network Address Translation (NAT) or Port Address Translation (PAT) is needed to map the private addresses of the branch network to valid public addresses. When a packet comes to the router, NAT rewrites the source address in the IP header. The router tracks this translation. When return traffic comes back, the destination address will be rewritten to its original value. PAT adds the ability to rewrite port numbers, thereby increasing the number of times

that a single public address can be used for translation. NAT and PAT were enabled to allow multiple hosts from the private branch network to access the Internet by using a single shared public IP address and various port numbers.

To learn more about NAT and PAT (also referred to as *NAT Overloading*), visit:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml

Quality of Service

- [Classification and Marking, page 60](#)
- [Policing and Markdown, page 61](#)
- [Scheduling, page 61](#)
- [Shaping, page 62](#)
- [Scavenger Class QoS, page 62](#)
- [Security Services, page 63](#)

An enterprise branch must support a variety of user applications, and some applications are more sensitive than others to packet delay, loss, and jitter that exceed tolerable levels when multiple users share limited network resources. Business-critical applications tend to be sensitive to delays and packet loss, real-time applications have strict delay and jitter requirements, and other types of applications may impose additional requirements. QoS is a set of tools and techniques for managing network resources in order to provide different priorities to different applications or to guarantee them a certain level of performance.

For more information about QoS and the various tools available in Cisco IOS software see the *Enterprise QoS Solution Reference Network Design Guide* at:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html



Note

The following sections apply only to the Cisco 1861 ISR configuration.

QoS policies vary from one enterprise to another, as each policy reflects particular business and organizational objectives. To meet the business criteria outlined in the “[Small Branch Design Considerations](#)” [section on page 4](#), the Cisco 1861 Basic Small Branch Network adopted a hierarchical QoS model that is configured to support five classes of traffic flows. The five-class model specifically includes real-time call signaling, critical data, best effort, and scavenger classes, as shown in [Table 10](#). The designated classification conforms to the Cisco QoS Baseline and RFC 3246.

Table 10 QoS Five-Class Model

Application	Layer 3 Classification			Layer 2 CoS/MPLS EXP
	IPP	PHB ¹	DSCP	
Real-time	5, 4	EF, AF41, AF42	34, 36, 46	5, 4
Call signaling	3	CS3	24, 26	3
Critical data	2, 3	AF21, AF22, AF31	18, 20, 25	2, 3

Table 10 **QoS Five-Class Model (continued)**

Application	Layer 3 Classification			Layer 2 CoS/MPLS EXP
Scavenger	1	CS1	8	1
Best effort	0, 1	0, AF11, AF12	0, 10, 12	0, 1

1. PHB = per hop behavior.

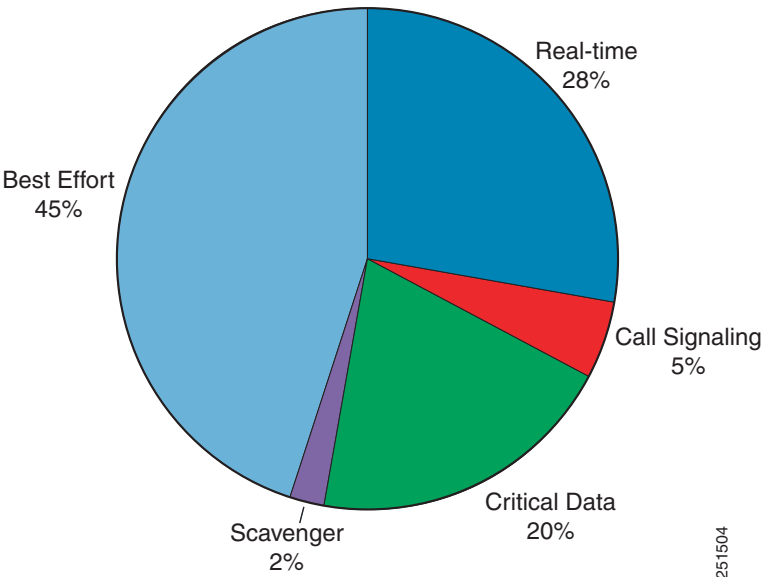
Each class of traffic carries a specific service level requirement. For the five classes selected, the requirements are as follows:

- Real-time
 - Loss should be no more than 1 percent.
 - One-way latency (mouth-to-ear) should be no more than 150 ms.
 - Average one-way jitter should be targeted under 30 ms.
 - Overprovision interactive video queues by 20 percent to accommodate bursts.
- Call Signaling
 - Voice control traffic requires 150 bps (plus Layer 2 overhead) per phone of guaranteed bandwidth. A higher rate may be required, depending on the call signaling protocol(s) in use.
- Critical Data
 - Mission-critical data traffic must have an adequate bandwidth guarantee for the interactive foreground operations that it supports.
- Best Effort
 - Adequate bandwidth should be assigned to the best-effort class as a whole, because the majority of applications will default to this class; reserve at least 25 percent for best-effort traffic.
- Scavenger
 - Scavenger traffic should be assigned the lowest configurable queuing service; for instance, in Cisco IOS this would mean assigning a Class-Based Weighted Fair Queuing (CBWFQ) of 1 percent to the scavenger class.

Figure 40 shows allocation of bandwidth to the five QoS classes. The Five-Class QoS Model allocates bandwidth to the general traffic categories as follows:

- Real-time traffic (voice and interactive video): 28 percent
- Call signaling: 5 percent
- Scavenger: 2 percent
- Best effort traffic: 45 percent
- Critical data traffic: 20 percent

Figure 40 Bandwidth Allocation for Five-Class QoS Model



There are various ways to enable QoS in an enterprise branch network. The Five-Class QoS policy is implemented in two logically different places in the network. A part of the policy is implemented at the access layer, and another part is implemented at the WAN edge layer. [Figure 41](#) and [Figure 42](#) shows summaries of QoS features that are part of the Basic Small Branch Network and their different implementation points. This design conforms to the Differentiated Services (DiffServ) architecture, as defined in RFC 2475.

Figure 41 **WAN Router**

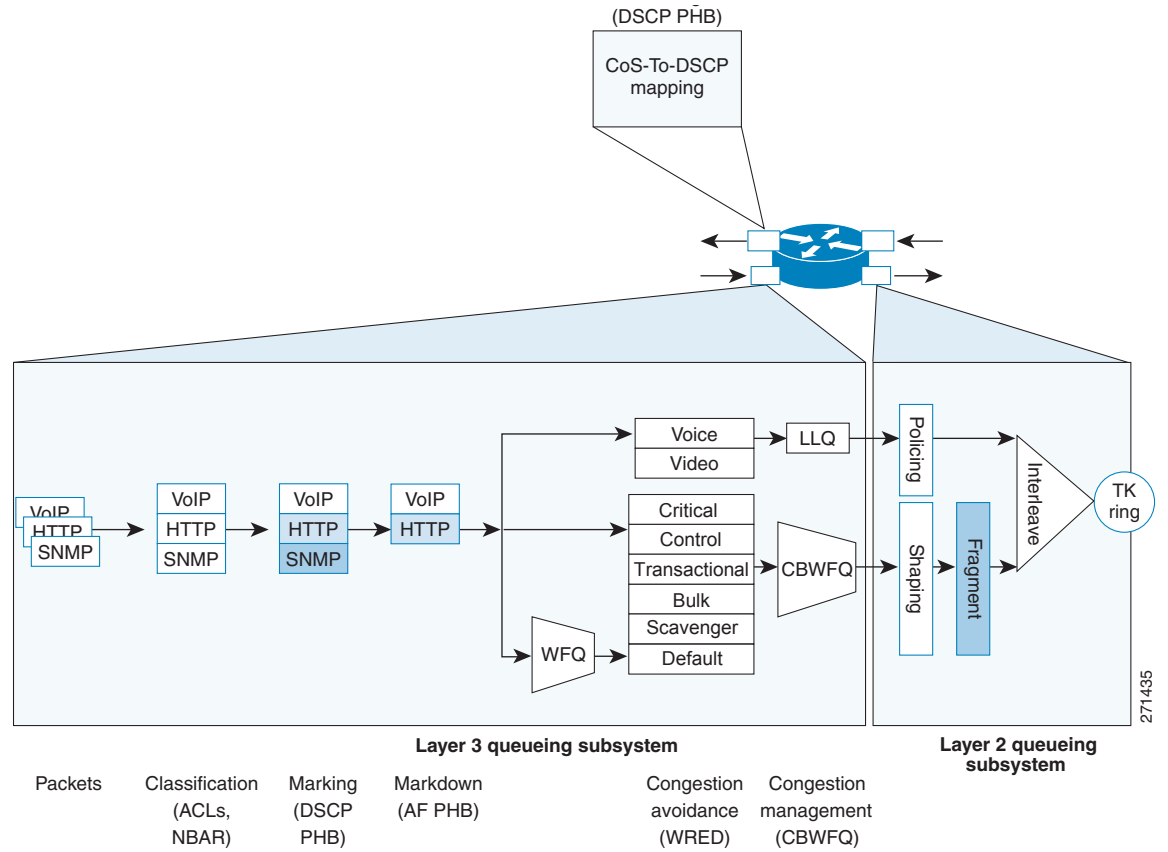
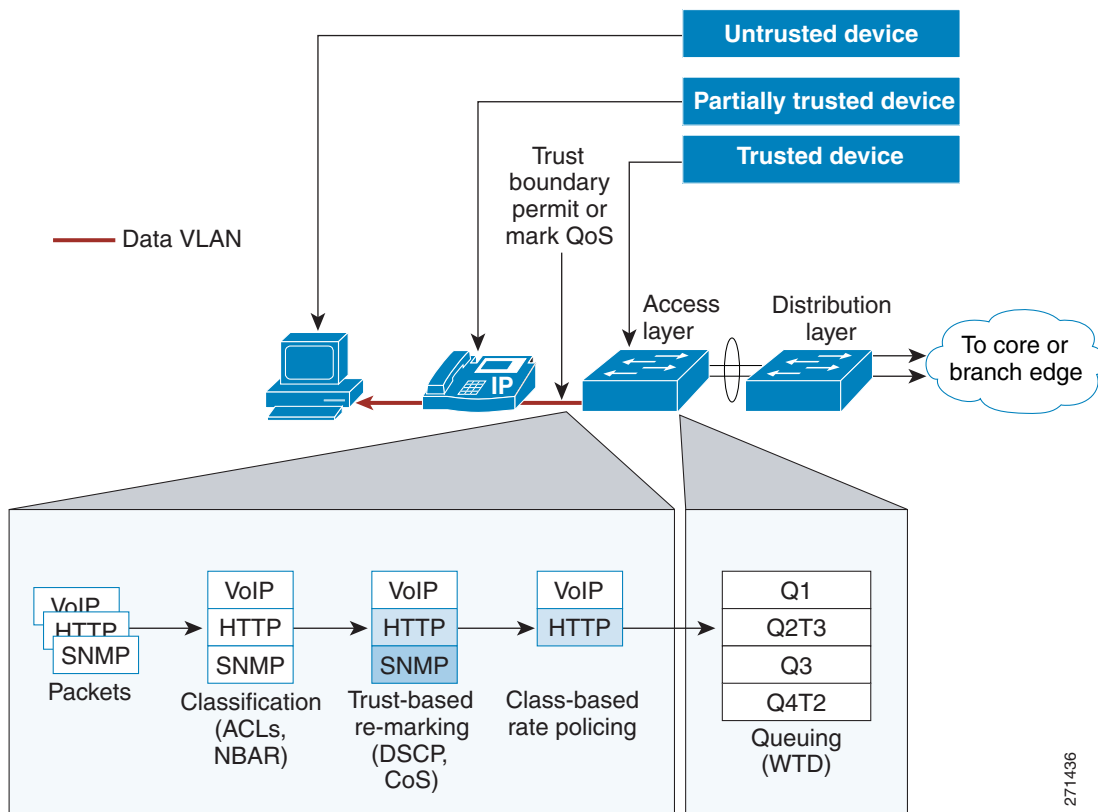


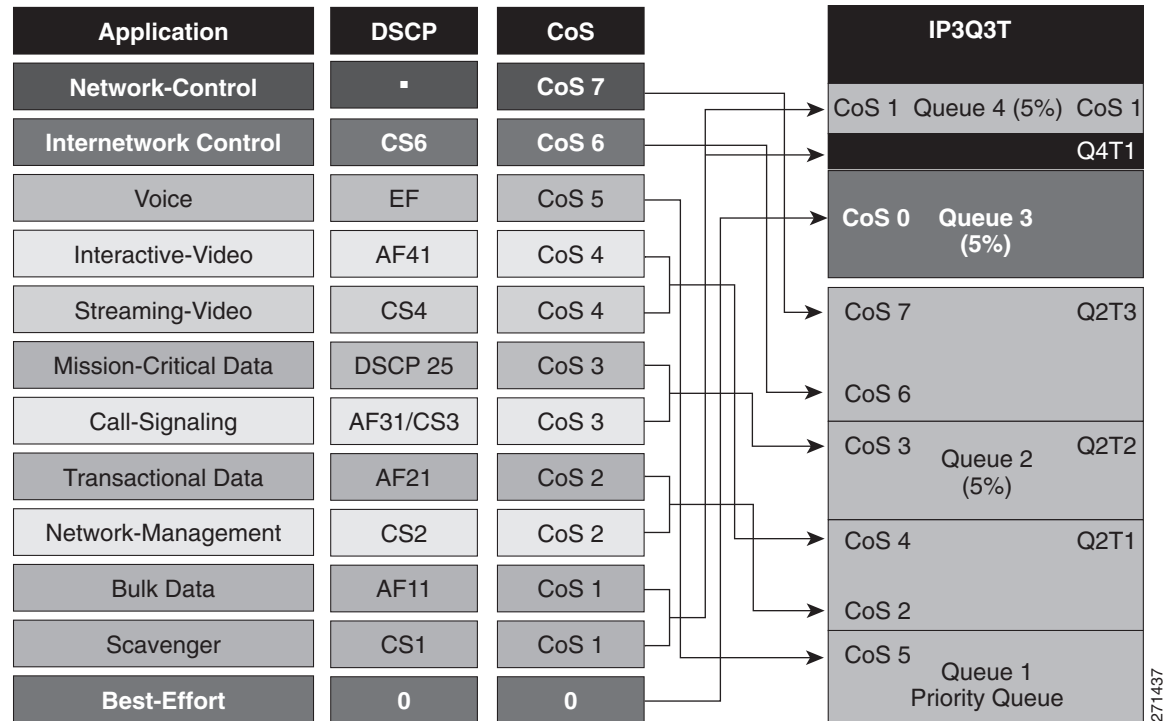
Figure 42 LAN Switch

271436

Regardless of the implementation point, the design incorporated a set of common QoS design principles. These principles are described in the following sections.

Classification and Marking

Classification identifies packets belonging to a certain traffic class, based on one or more TCP/IP header fields as defined in the Access Control List (ACL), or in application signatures via Network Based Application Recognition (NBAR). Marking tags the classified traffic by modifying either the 802.1Q/p class of service (CoS) Ethernet header field for incoming traffic or the DSCP per-hop behavior (PHB) header bits for outgoing traffic. Applications are classified and marked as close to their sources as technically and administratively feasible. Access layer switches remark all the packets coming from PC endpoints, servers, and so on, with appropriate CoS/DSCP values. Voice and signaling packets coming out of Cisco IP Phones are trusted, but all the packets coming from PCs attached to the IP Phones are re-marked. [Figure 43](#) shows assignment of different traffic flows to corresponding DSCP PHB and 802.1Q/p CoS classes. In addition, the assignment of each class to the corresponding Catalyst 3560 queue is shown.

Figure 43 Traffic Flow to QoS Class Mapping

Policing and Markdown

Policing determines whether packets are conforming to administratively defined traffic rates, and marks, re-marks, or drops nonconforming traffic flows. Excess traffic is marked down according to the Assured Forwarding PHB Group (RFC 2597) rules. Traffic flows are policed and marked down as close to their sources as possible. Traffic leaving access layer switches was rate limited. Policing is enabled on the outgoing WAN interface.

Scheduling

Scheduling determines how a frame or packet exits a device. The Weighted Random Early Detection (WRED) algorithm provides for congestion avoidance on network interfaces by providing buffer management and allowing TCP traffic to throttle back before buffers are exhausted. This helps avoid tail drops and global synchronization issues, thereby maximizing network utilization and TCP-based application performance.

Queuing techniques such as weighted fair queuing (WFQ), CBWFQ, and low latency queuing (LLQ) are necessary to ensure that critical applications are forwarded even during network congestion. Real-time applications such as voice or video that need to be forwarded with the least latency and jitter use LLQ. Non-delay-sensitive traffic can use CBWFQ. Best-effort data has several queues using WFQ.

Queuing comes into effect automatically only when the amount of traffic exceeds the available bandwidth.

Shaping

Shaping delays excess traffic that is above an administratively defined rate. It uses a buffer to hold packets when the data rate is higher than expected. Shaping was performed on the WAN interface.

Scavenger Class QoS

QoS can also provide network security by using scavenger class QoS. The scavenger class QoS strategy identifies known worms and attacks. Traffic patterns from that end user that are considered “unusual” or as “normal traffic but at an unusually high rate” are marked as scavenger class (CS1) in the DSCP field and allowed to pass through the switch. Through the use of the scavenger class, QoS can be used as a security mechanism to limit the arrival rate of any traffic that is destined for the firewall or Cisco IOS IPS configurations. The Basic Small Branch Network also uses scavenger class QoS for excess traffic on the data VLAN.

Automatic QoS

**Note**

The following section applies only to the Cisco 1841 ISR configuration

To address customer demand for simplification of QoS deployment, Cisco has developed the Automatic QoS (AutoQoS) features. AutoQoS is an intelligent macro that allows an administrator to enter one or two simple AutoQoS commands to enable all the appropriate features for the recommended QoS settings for an application on a specific interface.

For Cisco Catalyst switches, AutoQoS automatically performs the following tasks:

- Enforces a trust boundary at Cisco IP Phones.
- Enforces a trust boundary on Catalyst switch access ports and uplinks/downlinks.
- Enables Catalyst strict priority queuing for voice and weighted round robin queuing for data traffic.
- Modifies queue admission criteria (CoS-to-queue mappings).
- Modifies queue sizes as well as queue weights where required.
- Modifies CoS-to-DSCP and IP Precedence-to-DSCP mappings.

For Cisco IOS routers, AutoQoS is supported on Frame Relay (FR), Asynchronous Transfer Mode (ATM), High-Level Data Link Control (HDLC), Point-to-Point Protocol (PPP), and FR-to-ATM links.

For Cisco IOS routers, AutoQoS automatically performs the following tasks:

- Classifies and marks VoIP bearer traffic (to DSCP EF) and Call-Signaling traffic (to DSCP CS3).
 - Applies scheduling
 - Low Latency Queuing (LLQ) for voice
 - Class-Based Weighted Fair Queuing (CBWFQ) for Call-Signaling
 - Fair Queuing (FQ) for all other traffic
- Enables Frame Relay Traffic Shaping (FRTS) with optimal parameters, if required.
- Enables Link Fragmentation and Interleaving (LFI), either MLP LFI or FRF.12, on slow (768 kbps) links, if required.
- Enables IP RTP header compression (cRTP), if required.
- Provides Remote Monitoring (RMON) alerts of dropped VoIP packets.

The AutoQoS Enterprise feature consists of two configuration phases, completed in the following order:

- Auto Discovery (data collection)—Uses NBAR-based protocol discovery to detect the applications on the network and performs statistical analysis on the network traffic.
- AutoQoS template generation and installation—Generates templates from the data collected during the Auto Discovery phase and installs the templates on the interface. These templates are then used as the basis for creating the class maps and policy maps for your network.

Security Services

Security services help to protect the branch network from unauthorized, malicious, or inadvertent use of network resources. The challenge in designing the network is to find a balance between the need to keep networks open to support critical business requirements and the need to protect business-sensitive information. The Basic Small Branch Network strikes this balance by using technology and best practices that provide protection against the most common security threats.

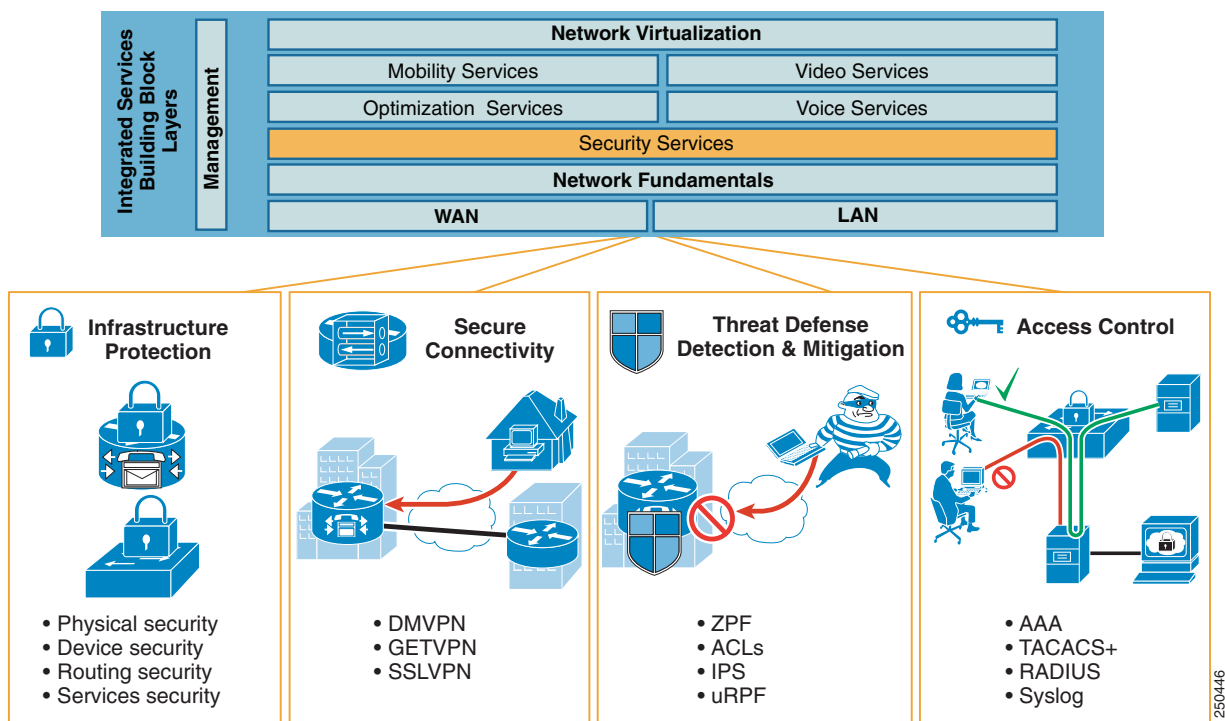
Cisco offers a large number of products, features, and recommendations for securing a network. This design blueprint focuses on security guidelines and security features for services that are integrated into the branch office router and branch office switch. For comprehensive coverage of the subject, see the *Enterprise Branch Security Design Guide* at:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/E_B_SDC1.html

Providing effective security starts with establishment of a security policy for the branch network. A security policy provides a set of rules by which people who have access to the network resources must abide. RFC 2196 Site Security Handbook provides a good starting point for development of a branch office security policy. In addition, SANS Institute (www.sans.org) provides guidelines for developing comprehensive security policies for enterprises of various sizes.

Security services for a large branch office network are described in the following sections and shown in Figure 44:

- [Infrastructure Protection, page 64](#)
- [Access Control, page 66](#)
- [Secure Connectivity, page 68](#)
- [Threat Protection, Detection, and Mitigation, page 76](#)

Figure 44 Security Services Building Blocks

In addition to following the guidelines and implementing security features recommended in this guide, it is important to emphasize that providing security for the branch network is an ongoing activity. Security threats evolve, and vulnerabilities are uncovered almost daily. Therefore, it is critical for the branch network to undergo continuous monitoring, periodic security assessment, and policy review.

While technology can create high enough barriers to prevent security breaches, the most costly security violations tend to be caused by either low-tech methods or unauthorized employees. Therefore, it is also critical to provide physical security and to ensure that security procedures are enforced at every level in the enterprise.

Infrastructure Protection

Infrastructure protection provides proactive measures to protect the branch routers and switches from direct attacks and indirect misuse. Infrastructure protection assists in maintaining network service continuity and availability. To protect network devices, the following methods are used in the Basic Small Branch Network:

- **Physical security:** Place routers and switches in a locked, temperature- and humidity-controlled room or cabinet accessible only by authorized administrators.
- **Device security:** Harden network devices.
 - **Securing unused ports:** Any ports not in use are disabled, autonegotiated trunking is turned off, and the ports are placed into the black hole VLAN.
 - **Enabling Secure Shell (SSH):** SSH is enabled and Telnet is disabled to prevent snooping and unauthorized access by unwanted parties. SSH is configured with five login retries.
 - **Enabling secure web access:** HTTPS access should be used for management applications.

- Enabling VTY, console, and AUX timeouts, and ACLs: Set all VTY, console, and AUX ports with timeouts to automatically drop any idle sessions after 300 seconds. ACLs are applied to restrict access to the network devices and permit only specific protocols for administrative and monitoring purposes.
- Providing banner message: It is a security best practice to provide a banner to inform unauthorized users that access to the device is restricted.
- Routing protocol security:
 - Configure protocol authentication: MD5 algorithm is used to authenticate routing protocol packets. In addition, RIPv2 has all interfaces, except for the primary, set to passive mode.
- Network services security:
 - Turning off unnecessary services: Turning off unnecessary services means disabling any known potentially hazardous interface features and any global services not specifically required in the network. [Table 11](#) lists services available on the branch router that should be disabled if not used.

Table 11 Router Services That Should Be Disabled If Unused

Feature	Description	Default	Action
Cisco Discovery Protocol (CDP)	Layer 2 device discovery protocol	Enabled	Disable
TCP small servers	TCP network services	Disabled	
UDP small servers	UDP network services	Disabled	
Finger	User lookup service	Disabled	
Identification service	Device identification service	Disabled	
BOOTP	Legacy service for obtaining IP addresses	Enabled	Disable
Autoloading	Autoloading of configuration from TFTP	Disabled	
Classless routing	Forwarding packets with no specific route to the best supernet route	Enabled	Disable unless required
HTTP server	Used for web-based configuration	Enabled	Disable and use HTTPS
HTTPS server	Used for web-based configuration	Enabled	Disable if not used
FTP server	Used to copy configuration files	Disabled	
DNS server	Name resolution	Enabled	Disable or enable explicit server if needed
PAD	Packet assembler/disassembler	Disabled	
IP source routing	Packet-specified routing	Enabled	Disable on all interfaces

Table 11 Router Services That Should Be Disabled If Unused (continued)

Feature	Description	Default	Action
Proxy ARP	Proxy for Layer 2 address resolution	Enabled	Disable on all interfaces
IP redirects	ICMP ¹ redirect message	Enabled	Disable on WAN interfaces
ICMP unreachable	Incorrect IP address notification	Enabled	Disable on WAN interfaces
Directed broadcast	Packet specified broadcast	Enabled	Disable on all interfaces
ICMP mask reply messages	Replies to subnet mask queries	Disabled	Disable on WAN interfaces
MOP	Maintenance Operation Protocol for loading Cisco IOS images	Disabled	

1. ICMP = Internet Control Message Protocol.

To simplify the steps for providing network device protection, the Basic Small Branch Network used the AutoSecure feature of Cisco IOS software. It is a single interactive command that disables all nonessential system processes and services as previously described. In addition, it enables several services that improve security, including:

- Tuning of scheduler interval and allocation
- TCP syn wait time
- TCP keepalive messages
- ICMP unreachable messages
- Enables Cisco Express Forwarding (CEF)
- Provides antispoofing
- Blocks all IANA-reserved address blocks
- Blocks all private address blocks

To learn more about AutoSecure, visit:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/cas11_ds.htm

Access Control

Access control is a mechanism for verifying user identity, restricting access to network resources, and auditing usage. Three independent security processes—authentication, authorization, and accounting—are used for this purpose. The processes perform the following functions:

- Provide a method for identifying users, verifying their identity, and granting/denying access to the network resources through mechanisms such as login and password or challenge and response.
- Provide a method for controlling access to network resources by authenticated users through mechanisms such as user groups, various access levels, privileges, or explicit user/group resource assignment (and vice versa).

- Provide a method for auditing the network to ensure compliance with security policies or to monitor attempts of unauthorized use.

Cisco offers several mechanisms to perform the authentication, authorization, and accounting processes independently as well as an integrated architectural framework that consistently enforces security policies across the entire network. The Basic Small Branch Network used a mixture of independent mechanisms and an integrated framework to reinforce and expand access control coverage.

Authentication Authorization Accounting (AAA) service is used as the integrated framework to perform the eponymous identity and access control processes.

When AAA is activated, the network device on which it is running verifies security information and reports user activity to the RADIUS or TACACS+ security server on the network. The Basic Small Branch Network was validated with both RADIUS and TACACS+. The two servers provide the following functions:

- **RADIUS:** Distributed client/server system implemented through AAA that secures networks against unauthorized access. RADIUS clients run on routers and switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

To learn more about RADIUS, visit:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrad.html

- **TACACS+:** Security application implemented through AAA that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. TACACS+ provides for separate and modular authentication, authorization, and accounting facilities.

To learn more about TACACS+, visit:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scftplus.html

Authentication

Authentication identifies the user through a login and verifies the user's identity through a password (or challenge/response in case of a software process). Authentication is the first gate that must be crossed to gain access to the system. If the login is found, the user is identified. If the password matches, then the user's identity is verified. If the login is not found or the password does not match, then the user is denied access. The following measures were taken to provide authentication in the Basic Small Branch Network:

- **Password management:** Password management ensures that only approved users can access a device or services within the network. Strong passwords that are at least 8 characters, combining letters, numbers, and symbols and avoiding dictionary words, numbers, or dates are recommended. Passwords should be changed frequently. The Basic Small Branch Network uses Type 5 encryption for storing administrative passwords in the configuration file as well as the Cisco IOS password encryption feature. In addition, all devices mandate a minimum of an 8-character password length.
- **VTY, console, and AUX passwords:** All access mechanisms on all devices are guarded by administrative passwords.
- **AAA authentication:** A list of authentication methods that are applied to the various interfaces is created. The method list defines the types of authentication to be performed and the sequence in which they will be performed. All authentication methods, except for local, line password, and enable authentication, are defined through AAA.

Authorization

In the simplest terms, authorization defines the network resources accessible to an authenticated user. There are two orthogonal methods for implementing authorization. Either the user is associated with all resources accessible to that user, or a resource is associated with all users that have access to that resource. A user can have different privilege levels for a resource (for example, list, read, write, execute). To simplify management and speed up the authorization process, users are assigned to groups (for example, administrator). Group membership defines which resources can be accessed by the user. Temporal authorization provides a mechanism to grant count- or time-based access to specified resources. The following measures were taken to provide authorization in the Basic Small Branch Network:

- AAA authorization: Assembles a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user, and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database is located on a server at the central site. As with authentication, a named list of authorization methods is created and is applied to various interfaces.

Accounting

As the name implies, accounting tracks access by users to various resources. Accounting is used to audit the network to ensure full compliance with security policies or to identify security breaches. The following measures were taken to provide accounting in the Basic Small Branch Network:

- Enabling logging: Access control of Simple Network Management Protocol (SNMP) and syslog on the router and switches is configured to ensure that there is a tracking mechanism when any unusual activity occurs. For more information about logging see the “[Management Services](#)” section on [page 78](#).
- AAA accounting: Provides a method for collecting and sending security server information used for auditing, and reporting, such as user identities, start and stop times, executed commands, and packet and byte counts. As with authentication and authorization, a named list of accounting methods is created and applied to various interfaces.

For more information about AAA, visit:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfaaa.html

Secure Connectivity

Secure connectivity protects against information theft or alteration of end-user data on public shared transport mediums. A Virtual Private Network (VPN) provides the means for securely and privately transmitting data over such a medium. There are two types of VPNs: provider-provisioned and enterprise-provisioned. The Frame Relay, Layer 3 VPN (L3VPN), and Layer 2 VPN (L2VPN) services described in the “[WAN Services](#)” section on [page 25](#) are examples of provider-provisioned VPNs. This section focuses on WAN-based VPN technologies in the context of a branch office. [Figure 45](#) and [Figure 46](#) show the Cisco 1841 and 1861 ISRs, respectively.

Figure 45 The Basic Small Branch Network Private WAN Deployment Using the Cisco 1841 ISR

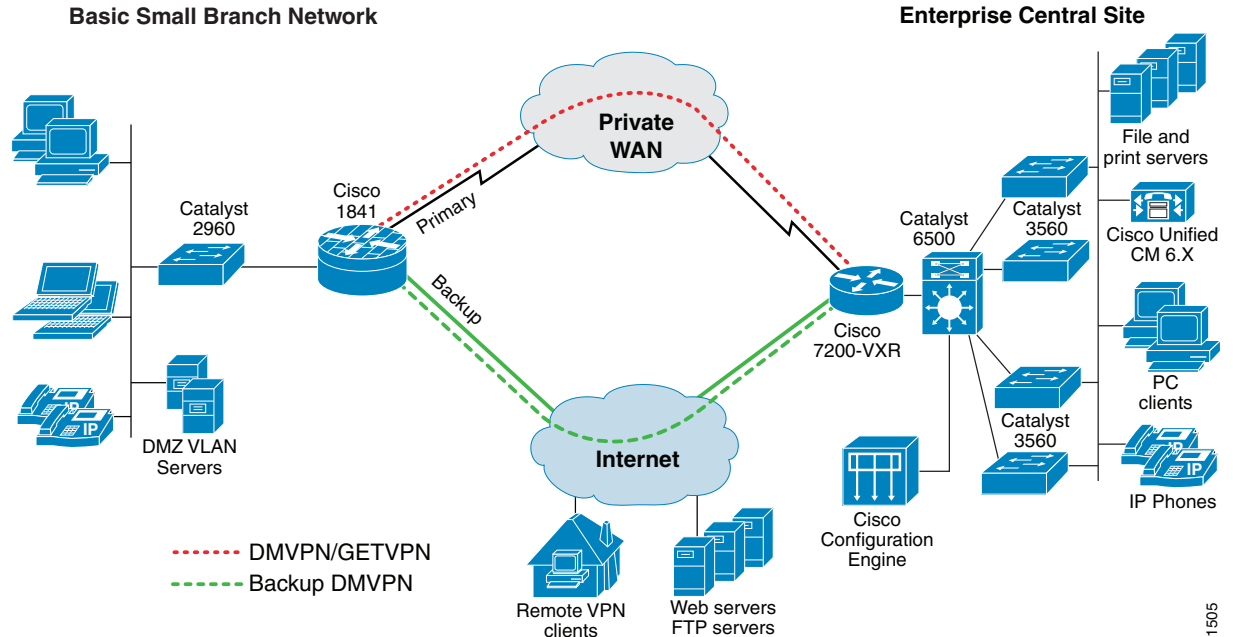
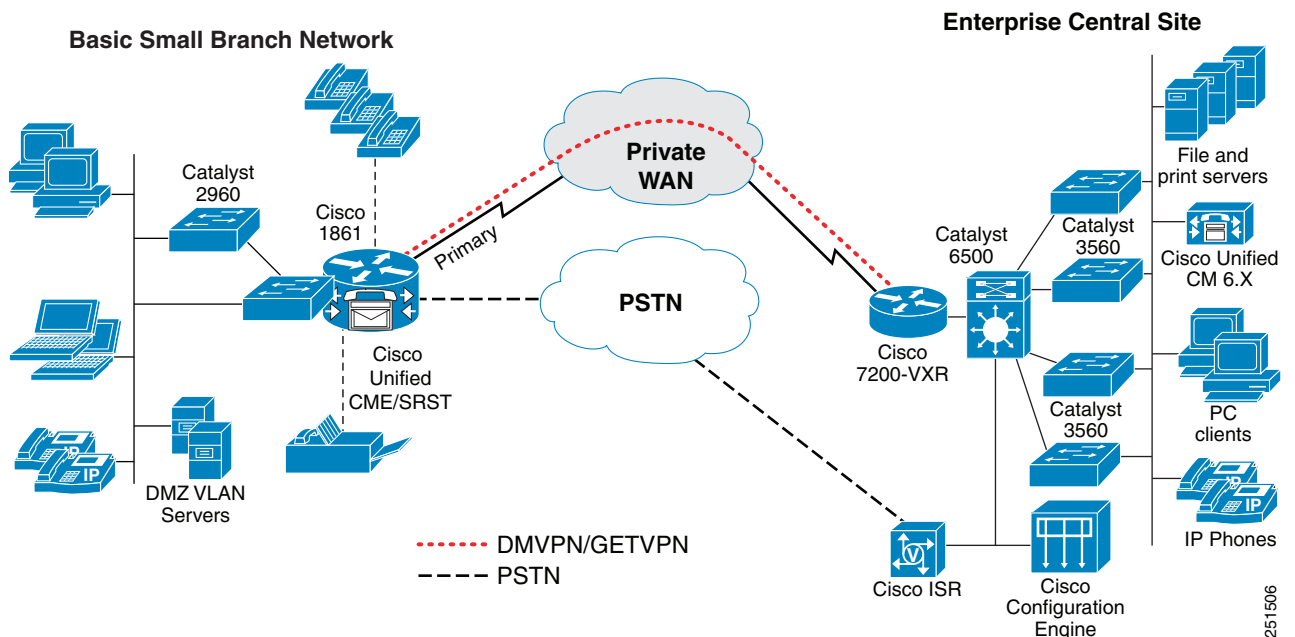


Figure 46 The Basic Small Branch Network Private WAN Deployment Using the 1861 ISR



IP-based WAN VPNs routed over the Internet have in recent years become an attractive alternative to traditional Layer 2 WAN deployments. IP VPNs offer low cost, secure, flexible, and scalable site-to-site connectivity. There are a number of WAN VPN options, and selecting the appropriate one involves many considerations. For a branch office the most important of these considerations are:

- WAN topology: Support for full-mesh or partial-mesh WAN designs.
- Scalability: Number of branch offices in the network and plans for future expansion.

- Availability: Local availability of WAN services that can support VPN deployments.
- Multicast: Requirement to support multicast traffic.
- Security: Type of encryption, key exchange, and authentication required, if any.
- Multiprotocol: Support for non-IP protocols.
- Quality of Service: End-to-end QoS requirements.
- Dynamic routing: Required support for dynamic routing protocols.
- High availability: Degree of resiliency required of a VPN.

To provide traffic separation on a public network, VPN uses a tunneling mechanism such as generic routing encapsulation (GRE), IPsec, Point-to-Point Tunneling Protocol (PPTP), or Layer 2 Tunneling Protocol version 3 (L2TPv3). Direct IPsec and GRE are the most typically deployed tunneling protocols for branch office VPNs. A tunneling protocol combined (or supported natively) with authentication and encryption mechanism, forms the basis of enterprise-provisioned VPNs. [Table 12](#) provides an overview of the most commonly used IP-based WAN VPNs in a branch office. SSL-based VPNs are typically used for traffic that traverses the Internet. In the Basic Small Branch Network, SSL VPN is used to connect home users to the branch network.

Table 12 *Typical VPNs Provisioned in a Small Branch Office*

VPN Type	Advantages	Disadvantages	Appropriate for Branch
IPSec with direct encapsulation	• Multivendor interoperability	• Limited support for mesh topology • No dynamic routing • No multicast • IP only • No QoS	• When interoperability with non-Cisco products is required
IPsec with VTI ¹ encapsulation	• QoS • Multicast • Dynamic routing • Lower overhead than GRE • Ease of use	• Limited interoperability • IP only	• Small number of sites.
IPSec with GRE encapsulation	• Non-IP protocols • Multicast • QoS • Dynamic routing	• Limited support for mesh topology • Overlay routing	• When non-IP protocols are required.
Easy VPN	• Simple configuration	• No mesh topology • No dynamic routing • No multicast • IP-only	• Ease of management and simplicity of configuration are a priority.

Table 12 *Typical VPNs Provisioned in a Small Branch Office (continued)*

VPN Type	Advantages	Disadvantages	Appropriate for Branch
DMVPN ²	• Multicast • Simpler configuration than IPsec+GRE • Small scale on-demand meshing • Easier to scale	• Limited support for meshed topology • IP-only • Overlay routing • No spoke-to-spoke QoS	• Internet-based primary WAN links. • Backup WAN link.
GETVPN	• Tunnel-less VPN • Full-mesh connectivity • Routing • Efficient multicast • Advanced QoS • Scalable	• Public WAN deployments • IP only	• Appropriate for most branch offices. • MPLS/IP WANs. • Traditional Layer 2 WANs that need added security.
SSLVPN	• Clientless solution • Ease of use	• Limited support for application-level protocols • Lower performance than IPsec alternatives	• Remote users connecting to the branch.

1. VTI = Virtual Tunnel Interface.

2. DMVPN = Dynamic Multipoint Virtual Private Network.

In addition to these general considerations, a VPN solution must meet the business criteria outlined in the [“Small Branch Design Considerations”](#) section on page 4. Those requirements specify support for multicast and dynamic routing protocols. Because IPsec with direct encapsulation, IPsec with VTI, and Easy VPN do not support multicast and dynamic routing, they were excluded from branch office considerations. Moreover, IPsec with GRE encapsulation is a less general case of Dynamic Multipoint Virtual Private Network (DMVPN). Therefore, the only VPN solutions evaluated for the Basic Small Branch Network are DMVPN, Group Encrypted Transport Virtual Private Network (GETVPN) and SSL VPN.

GETVPN is appropriate for the primary WAN link, and DMVPN is appropriate for the Internet backup link for all WAN deployment scenarios described in the [“WAN Services”](#) section on page 25. However, existing hub-and-spoke WAN designs may already have DMVPN deployed. Therefore, DMVPN was validated on the primary link for leased line, Frame Relay, and VPWS WAN services. It should be noted that leased-line, Frame Relay, and Virtual Private Wire Service (VPWS) offer a degree of data privacy by providing traffic isolation. However, it is common to add a VPN to improve overall security and to enable enterprises to meet regulatory requirements such as Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act, and Payment Card Industry (PCI) security standards. In summary, the following VPN deployment scenarios were tested for the Basic Small Branch Network:

- GETVPN on the primary link, DMVPN on the backup link, and SSL VPN for remote user access
- DMVPN on the primary link, DMVPN on the backup link, and SSL VPN for remote user access

**Note**

The backup link scenario described in the following section applies only to the Cisco 1841 ISR configuration.

Each VPN technology is described in more detail later in this section.

The foundation of a secure VPN is based on three independent security measures: data confidentiality, data integrity, and authentication. Each VPN solution listed in [Table 12](#) uses a different combination of technologies to provide these security measures. The following technologies are used in the Basic Small Branch Network:

- **Data Confidentiality:** Protects data from unauthorized interception. There are two general mechanisms for providing confidentiality:
 - **Encryption:** Reorders bits of the original message, making it incomprehensible to people not authorized to view the information. There are numerous encryption algorithms of various strengths. The following were used in the Basic Small Branch Network:

Triple Data Encryption Standard (3DES): Symmetric encryption mechanism that uses three different keys to encrypt a message. 3DES was used with both DMVPN and GETVPN.

Advanced Encryption Standard (AES)-256: Symmetric encryption mechanism that uses 256-bit key for encryption. AES-256 was used with both DMVPN and GETVPN.
 - **Tunneling:** Encapsulates original packet in a new packet and sends the composite packet over the network. The following mechanisms are used to provide tunneling:

Generic Routing Encapsulation (GRE): Encapsulates an original IP packet in a new IP packet whose source and destination become the two virtual endpoints of the GRE tunnel. The traffic in a GRE tunnel is not encrypted. However, GRE offers several advantages such as ability to carry both IP and non-IP traffic and the ability to support multicast. Therefore, GRE is typically placed inside an IPsec tunnel for greater security. This is the mechanism used by DMVPN.

IP Security (IPsec): IPsec is a framework for various security features. There are two main protocols within IPsec: tunnel mode protocol (also known as Authentication Header [AH]), and transport mode protocol (also known as Encapsulating Security Payload [ESP]). HA provides unencrypted tunneling and therefore was not used in the Basic Small Branch. ESP tunneling provides both encryption and authentication. In addition, ESP encrypts the original IP header. Standalone ESP is the mechanism used by GETVPN.
- **Data Integrity:** Guarantees that no tampering or alteration of the data occurs while it travels between the source and destination. The following algorithms are used for both DMVPN and GETVPN:
 - **Message Digest 5 (MD5):** A 128-bit hash algorithm. A hashing key is produced on the original message, appended to the end, and then encrypted. The recipient recomputes the hash to detect any alterations.
 - **Secure Hash Algorithm 1 (SHA-1):** A 160-bit hash algorithm. SHA-1 works on the same principle as MD5.
- **Authentication:** Verifies the identity of both endpoints that are communicating. VPN can use a variety of methods to perform authentication, such as login and password, smart cards, or biometrics. Most typically, digital certificates are used. The services-ready method used the following VPN authentication method:
 - **Preshared Key (PSK):** A secret key that is shared between the endpoints using a secure channel. A PSK is entered into each peer manually, and is used to authenticate the peer. In the Basic Small Branch Network, the secure channel for key exchange is provided by the following mechanism:

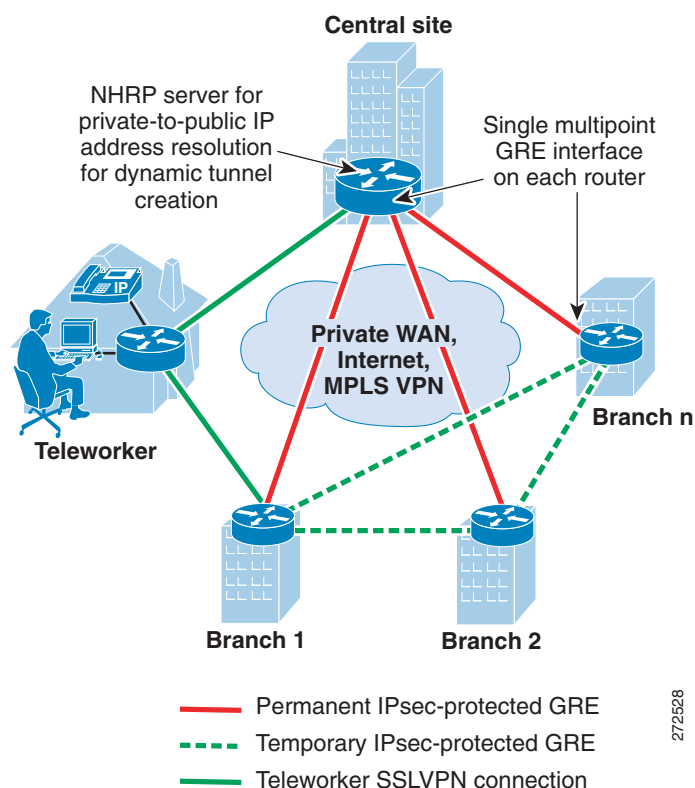
Diffie-Hellman Group 2 (DH2): 3DES and MD5 encryption and hashing algorithm with 1024-bit key

A secure communication channel between two endpoints is also referred to as a *security association* (SA). It is a security best practice to provide a lifetime limit for the SA. Typically, the lifetime is short enough to prevent attackers from gathering enough data to break the encryption ciphers. The lifetime data volume thus depends on effective bandwidth and the encryption algorithm. It is also important to frequently change encryption keys when using the preshared key infrastructure. For the Basic Small Branch Network, both lifetimes are provided in [Table 13](#).

In addition to security measures, VPNs differ in the way they manage keys, provide point-to-point or multipoint communication, and allow for dynamic creation of VPN tunnels. The three VPNs used in the Basic Small Branch Network offer the following functions:

- DMVPN is IPsec- and GRE-based VPN. It enables dynamic spoke-to-spoke tunnel creation in a traditional hub-and-spoke WAN design. DMVPN leverages multipoint GRE (mGRE) to establish multiple tunnel endpoints and to create an overlay non-broadcast multi-access (NBMA) network. While a traditional hub and spoke GRE configuration would require a separate tunnel between endpoints, mGRE allows multiple endpoints to have a single tunnel interface in the same subnet. Next Hop Resolution Protocol (NHRP) is used to provide tunnel-to-physical address lookup, facilitating dynamic configuration of GRE tunnels between endpoints. NHRP operates in a client/server configuration. NHRP Server typically runs on the hub, and each spoke router (NHRP Client) registers its tunnel-to-physical address mapping with the server. When a spoke wants to communicate on the NBMA mGRE subnet, it first sends a request to the NHRP Server to map a tunnel endpoint to a physical address. When the physical address is known, a GRE tunnel is established, and a regular routing process determines the path to the endpoint. [Figure 47](#) shows DMVPN hub-and-spoke and spoke-to-spoke architecture.

Figure 47 DMVPN mGRE architecture

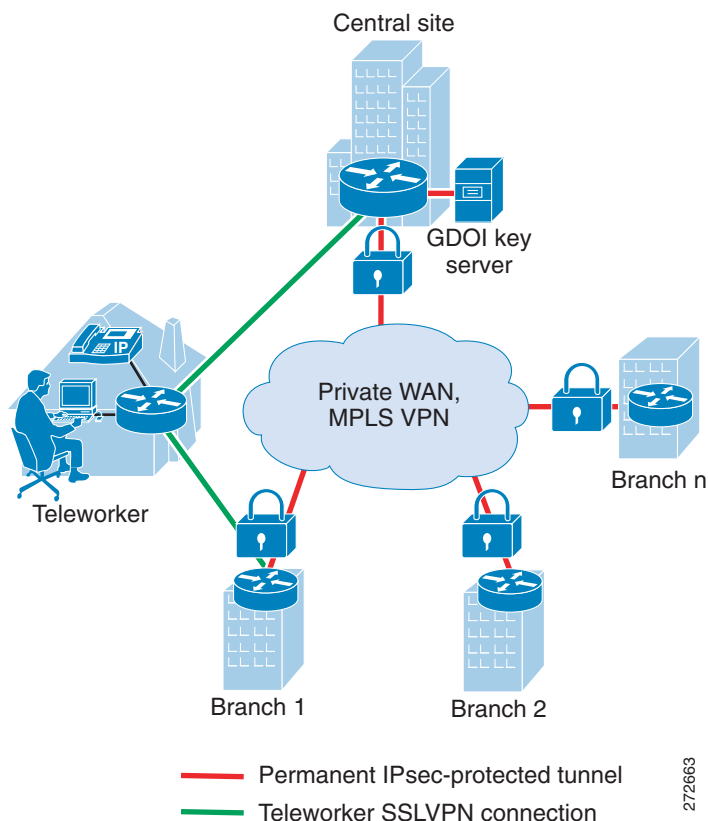


To learn more about DMVPN visit:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftgreips.html

- Group Encrypted Transport VPN (GETVPN) combines IPsec and Group Domain of Interpretation (GDOI) key server to encrypt traffic on a private WAN. Traditional VPN gateways directly authenticate each other and set up IPsec sessions that are private to the pair. This approach does not scale well when the network provides any-to-any connectivity or has large number of VPN gateways. GDOI server facilitates management and distribution of digital certificates or pre-shared cryptography keys. It authenticates group members and distributes keys and policies. GETVPN is a tunnelless VPN and therefore should be used in private WANs such as MPLS or traditional Layer 2 WANs. GETVPN can be used in conjunction with DMVPN or IPsec/GRE to simplify key management for a public WAN VPN. GETVPN uses IPsec ESP to provide confidentiality, integrity, and replay protection for packets flowing between VPN gateways. Figure 48 shows any-to-any GETVPN connectivity.

Figure 48 Any-to-Any GETVPN connectivity



To learn more about GETVPN, visit:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htgetvpn.html

- Secure Socket Layer Virtual Private Network (SSL VPN): Leverages Secure Socket Layer (SSL) and its successor Transport Layer Security (TLS) to provide remote-access VPN capability, using the SSL/TLS function that is already built into a modern web browser. SSL VPN allows users from any Internet-enabled location to launch a web browser to establish remote-access VPN connections. Encryption is a component of the SSL/TLS framework; AAA is used to authenticate the remote users.

To learn more about SSL VPN, visit:

<http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/webvpn.html>

Table 13 summarizes all the security mechanisms used for GETVPN and DMVPN in the Basic Small Branch Network.

Table 13 Security Mechanisms for DMVPN and GETVPN

Mechanism	DMVPN	GETVPN
Peer authentication	Preshared key	Preshared key
Encryption	3DES, AES-256	3DES, AES-256
Integrity algorithm	SHA-1, MD5	SHA-1, MD5
Key exchange	DH2	DH2
Tunneling	GRE inside IPsec ESP	IPsec ESP
SA lifetime ¹	86400 seconds	86400 seconds
	28800 seconds	28800 seconds
	3600 seconds	3600 seconds
Rekey lifetime	300 seconds	300 seconds

1. The SA lifetime value depends on the aggregate amount of data that passes through VPN gateways. This will vary from enterprise to enterprise. To determine appropriate SA value follow instructions provided at:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/white_paper_c11-471053.html



Note

The following section applies only to the Cisco 1841 ISR configuration.

Encryption is a CPU-intensive process. The Basic Small Branch Network uses the VPN and SSL advanced integration module to support the required up to 25 users in the branch. The Cisco VPN and SSL service module provides up to 40 percent better performance for IPsec VPN over the router built-in IPsec encryption, and up to twice the performance for SSL VPN encryption. The AIM supports both SSL encryption and VPN IPsec encryption with either Data Encryption Standard (DES) or Advanced Encryption Standard (AES) in its hardware. For the Cisco 1841 ISRs, use the AIM-VPN/SSL-1 module, shown in Figure 49.

Figure 49 AIM-VPN/SSL Module



Threat Protection, Detection, and Mitigation

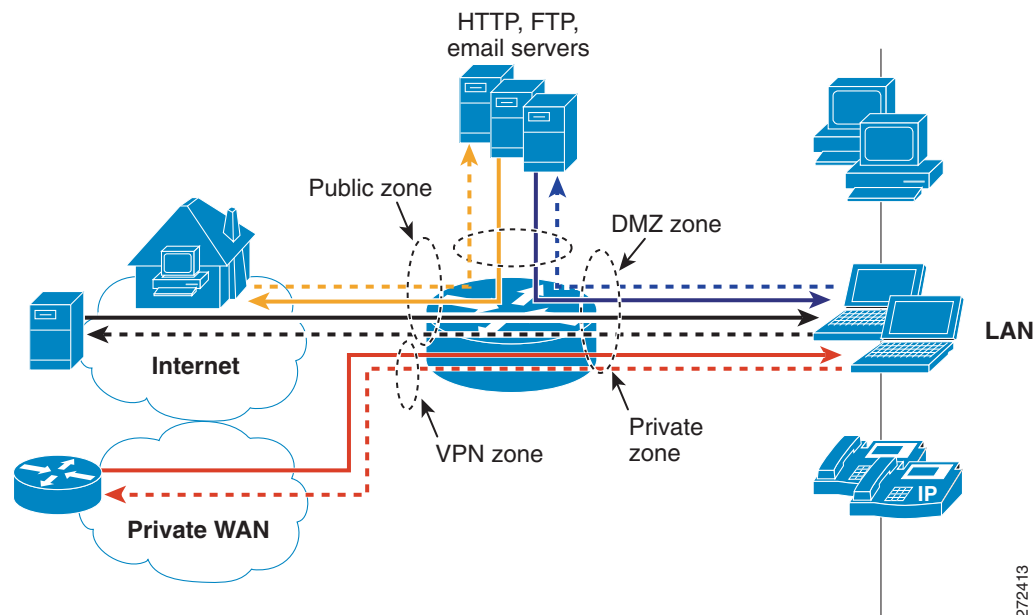
Threat protection, detection, and mitigation are security mechanisms for protecting the branch network from security policy violations and from malicious attacks on the network infrastructure. In the context of this document, threats are security breaches in which the primary goal is information theft or tampering. Reconnaissance and unauthorized access fall into this category. Attacks are intentional or unintentional activity to disrupt the operation of the network. Denial of service and malicious code fall into this category. Prevention proactively blocks both threats and attacks. Detection identifies threats and attacks that are currently in progress. Mitigation stops current threats and attacks, and prevents recurrence. Attackers can be either individuals external to the enterprise or someone within the organization. Internal attackers are much more difficult to spot and block because they have more information and more options for launching an attack. In addition, both types of attackers can use low-tech methods, such as social engineering, to gain unauthorized access. It is therefore critical to have a solid security policy for the branch office and to educate all users to follow the established security measures. Security policy was described in the “[Security Services](#)” section on page 63.

Basic Small Branch Network uses the following security mechanisms to prevent external attacks:

- **Zone-based Policy Firewall (ZPF):** Prevents external threats and attacks. Firewalls provide stateful security and application inspection for each protocol entering or leaving a branch network. A stateful inspection firewall uses a combination of access control with application inspection to ensure that only approved responses get through the firewall. ZPF assigns the router interfaces to various zones and applies inspection policies to traffic flowing between the various zones. Inter-zone policies offer considerable flexibility and granularity, enabling different inspection policies for different host groups connected to the same router interface. An interface can be easily added or removed from a zone. Four security zones were defined for the Basic Small Branch Network: demilitarized zone (DMZ), Public zone, VPN zone, and Private zone as shown in [Figure 50](#). The following traffic is inspected and permitted to pass:
 - From Private zone to Private zone, all traffic passes without any inspection.
 - From Private zone to Public zone HTTP, FTP, DNS, HTTPS, SSH, and ICMP traffic is inspected and allowed, but the rest of the traffic is blocked.
 - From Public zone to Private zone, no traffic is allowed.
 - From Public zone to DMZ zone, only HTTP, HTTPS, and DNS are allowed.
 - From Private zone to VPN zone, all traffic passes with inspection.
 - From VPN zone to Private zone, all traffic passes with inspection.

To learn more about Zone-based Policy Firewall, visit:

http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml

Figure 50 Security Zones

- **Unicast Reverse Path Forwarding (uRPF):** Leverages routing tables to validate source addresses that are expected to be seen on an interface. Packets are forwarded only if they match the router's best path to the source. This ensures that packets coming into an interface are from valid hosts that have a corresponding entry in the routing table. Packets with source addresses that cannot be reached via the input interface are dropped.

To learn more about uRPF, visit:

<http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html>

The following security mechanisms are used to prevent internal threats and to control access to network resources in the Basic Small Branch Network:

- **Standard and extended access control lists (ACLs):** Control whether a router permits or denies packets to pass, based on criteria in the packet header. Standard ACLs filter packets based on source IP address only. Extended ACLs filter packets on source and destination IP addresses, port numbers, and protocol type. ACLs are used extensively within the Basic Small Branch Network to permit or deny access between the different firewall zones.
- **Layer 2 security:** Prevents various attacks or access violations that could be launched through the branch switches
 - **802.1x:** Client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. The authentication is provided by a RADIUS server.
 - **Port Security:** Switch port limits the number of MAC addresses that are able to connect to a switch, and ensures that only approved MAC addresses are able to access the switch. It prevents MAC address flooding and ensures that only approved users can log on to the network.
 - **DHCP Snooping:** Switch port forwards DHCP requests only from trusted access ports and drops all other types of DHCP traffic. DHCP snooping eliminates rogue devices from behaving as the DHCP server.

- Dynamic Address Resolution Protocol (ARP) Inspection (DAI): Maintains a binding table containing IP and MAC address associations dynamically populated using DHCP snooping. This feature ensures the integrity of user and default gateway information so that traffic cannot be captured. This feature mitigates ARP spoofing and ARP poisoning attacks.
- IP Source Guard: When a client receives a valid IP address from the DHCP server, or when a static IP source binding is configured by the user, a per-port and VLAN access control list (PVACL) is installed on the port. This process restricts the client IP traffic to the source IP addresses configured in the binding; any IP traffic with a source IP address except that in the IP source binding is filtered out. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address.
- Bridge Protocol Data Unit (BPDU) Guard: Prevents loops if another switch is attached to a PortFast port. When BPDU Guard is enabled on an interface, the interface is shut down if a BPDU is received on the interface. To assume the root bridge function, a device would be attached to the port and would run STP with a lower bridge priority than that of the current root bridge. If another device assumes the root bridge function in this way, it renders the network suboptimal. This is a simple form of a denial-of-service (DoS) attack on the network.

To detect and mitigate various external and internal attacks, the Basic Small Branch Network uses the following mechanisms:

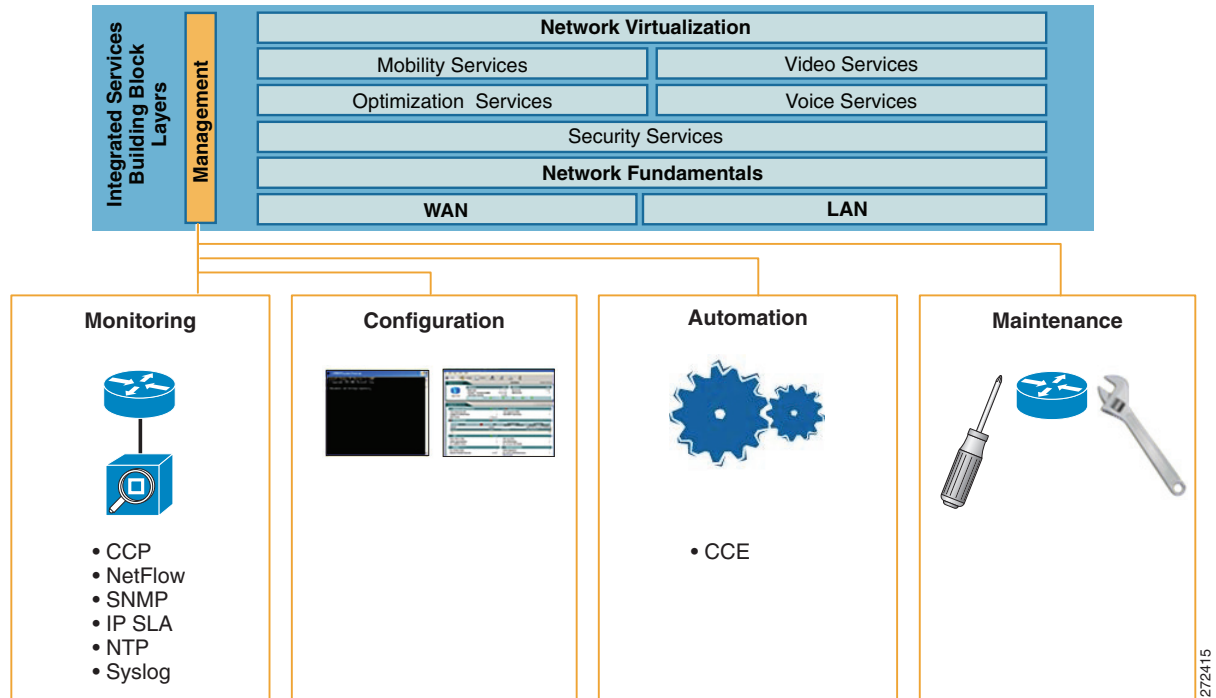
- Cisco Intrusion Prevention System (IPS): Monitors packets and sessions as they flow through the branch, and scans each packet to match any of the IPS signatures. When IPS detects suspicious activity, it can shunt the offending packets before network security can be compromised. When an IPS signature is matched, one or more of the following actions are taken:
 - An alarm is sent to a syslog server or a centralized management interface.
 - The packet is dropped.
 - The connection is reset.

The Basic Small Branch Network is configured to take different actions depending on which attack signature is matched. An advanced signature set was used to identify various attacks. IPS is configured on all outside and inside interfaces. Traffic, regardless of whether it is a WAN link to the public or an internal LAN link, is inspected. See the “[System Testing](#)” chapter or page for the various attacks that were validated for the Basic Small Branch Network.

- Network Based Application Recognition (NBAR): Recognizes certain type of attacks and drops packets involved in a denial-of-service attacks such as SQL Slammer, and worms such as CODE RED and NIMDA.

Management Services

Management services include activities related to configuration, monitoring, automation, and maintenance of a branch office network, as shown in [Figure 51](#).

Figure 51 **Management Services for a Branch Network**

Cisco offers numerous tools for performing network management in the branch office. At this time, only a subset of those tools has been validated for the Basic Small Branch Network. The primary focus was on monitoring the branch router. Future updates to this guide will address configuration management, automation, and maintenance for all the branch network devices.

Monitoring services for the Basic Small Branch Network are described in the following sections:

- [Cisco Configuration Professional, page 79](#)
- [Simple Network Management Protocol, page 80](#)
- [Syslog, page 81](#)
- [NetFlow, page 81](#)
- [Network Based Application Recognition, page 81](#)
- [IP Service Level Agreement, page 82](#)
- [Network Time Protocol, page 82](#)
- [Cisco Configuration Engine, page 82](#)

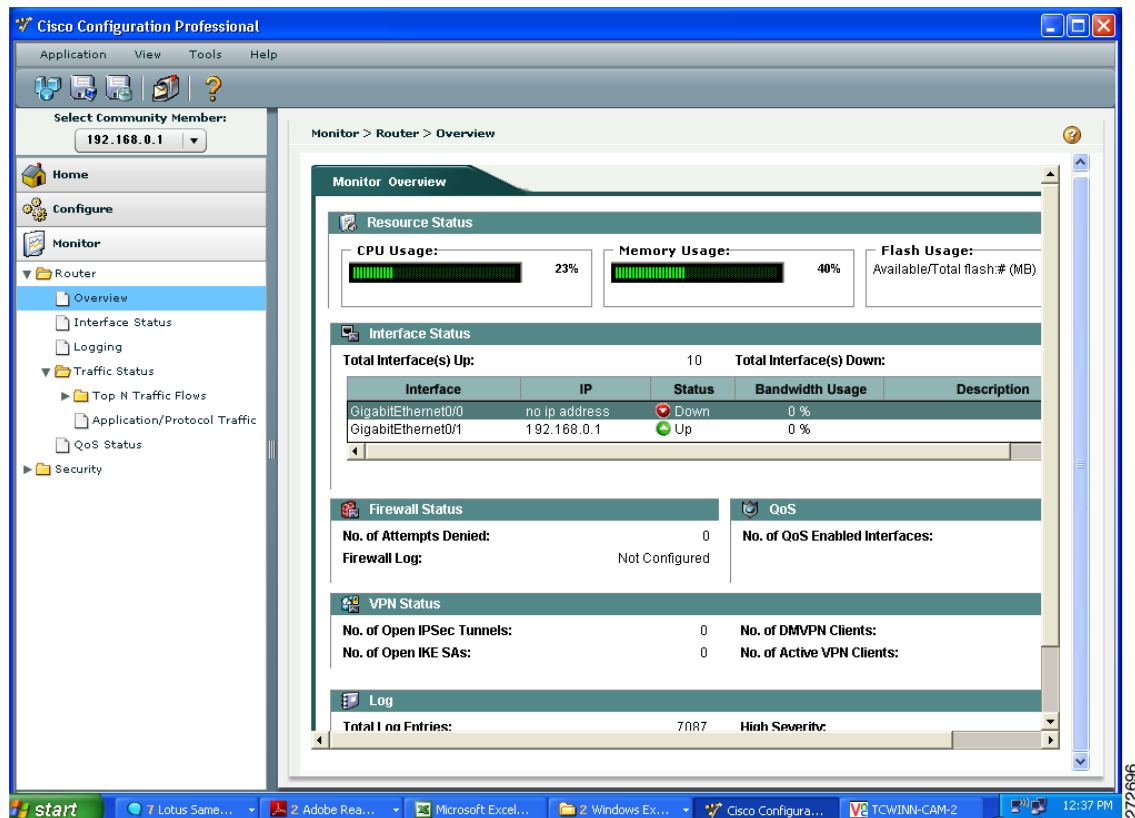
Configuration management in the Basic Small Branch Network was done primarily through the command line. However, several services have a web-based graphical interface that was used to configure those services. Configuration of all networking devices is extensively documented in the “[System Implementation](#)” chapter.

Cisco Configuration Professional

Cisco Configuration Professional, shown in [Figure 52](#), is a web-based device management tool embedded within the Cisco IOS software. Cisco Configuration Professional simplifies router, security, Unified Communications, wireless WAN, and basic LAN configuration through intelligent wizards. It

enables faster configuration and monitoring of the branch router without requiring knowledge of the Cisco IOS command-line interface (CLI). In the Basic Small Branch Network, Cisco Configuration Professional was used for monitoring only.

Figure 52 *Cisco Configuration Professional*



In monitor mode, Cisco Configuration Professional provides an overview of router status and performance metrics such as the Cisco IOS release number, interface status (up or down), and CPU and memory usage. The monitor mode also allows users to view the number of network access attempts that were denied by Cisco IOS Firewall, and provides easy access to the firewall log. Additionally, VPN status, such as the number of active IPsec tunnels, can be monitored.

For more information about Cisco Configuration Professional, visit:

http://www.cisco.com/en/US/prod/collateral/routers/ps9422/data_sheet_c78_462210.html

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) provides a standardized framework and a common language for the monitoring and management of devices in a network. In the Basic Small Branch Network, SNMP version 3 traps were enabled to log various events on the routers and switches.

To learn more about configuring SNMP visit:

http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html

Syslog

Syslog is a protocol for sending logging messages on a network. Various devices log status, events, alerts, and errors, using syslog components that forward the log messages to a syslog service. A syslog service simply accepts messages and stores them in files or prints them to a console. Syslog was used extensively in the Basic Small Branch Network for security accounting and for monitoring the status of various devices.

To learn more about Cisco IOS software syslog messages, visit:

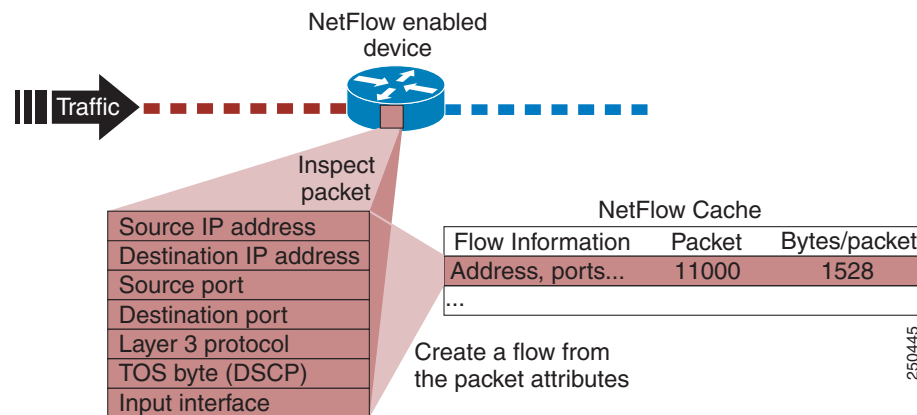
http://www.cisco.com/en/US/docs/ios/12_3/sem1/system/messages/123semv1.html

http://www.cisco.com/en/US/docs/ios/12_3/sem2/system/messages/123semv2.html

NetFlow

NetFlow version 9 technology is used to monitor and measure specific traffic flows and to provide an aggregate view of all network activity. With NetFlow, network administrators can view detailed time and application-specific usage of the network. This information is essential for network planning, security analysis, application optimization and delivery, and traffic engineering. A typical NetFlow record includes source and destination IP addresses, TCP/UDP port numbers, type of service (ToS), packet and byte counts, time stamps, input and output interfaces as shown in Figure 53, TCP flags and routing information. NetFlow data is exported from the router to a centrally located NetFlow collection server for analysis. This typically consumes 1 to 5 percent of bandwidth. The Basic Small Branch Network used Netflow version 9.

Figure 53 Data Captured by NetFlow



For more information about NetFlow and third-party NetFlow data analysis tools, visit:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.html

Network Based Application Recognition

Network Based Application Recognition (NBAR) is a Cisco IOS classification engine that can recognize a wide variety of applications, including web-based applications and client-server applications that dynamically assign TCP or User Datagram Protocol (UDP) ports. After the application is recognized, the network can invoke specific services for the application. In the Basic Small Branch Network, NBAR

was used to support QoS features described in “Quality of Service” section on page 56. NBAR identifies and stops command worms, such as SQL Slammer, NIMDA, and Arctic, from propagating through the network.

To learn more about NBR, visit:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6558/ps6612/ps6653/prod_qas09186a00800a3ded_ps6616_Products_Q_and_A_Item.html

IP Service Level Agreement

The IP service level agreement (IP SLA) feature of Cisco IOS software is used to verify service guarantees, to increase network reliability by validating network performance, and to proactively identify network issues. In the Basic Small Branch Network, IP SLAs were used to measure:

- End-to-end response time (delay) between the branch router and the central location router
- Packet delay variability (jitter) for traffic flowing between the branch and the central location

Both IP SLA metrics are critical to ensure high-quality voice services. To learn more about IP SLAs visit:

http://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_white_paper0900aecd8017f8c9_ps6602_Products_White_Paper.html

Network Time Protocol

Network Time Protocol (NTP) is used to synchronize clocks among network devices. This synchronization allows events to be correlated when system logs are created and when other time-specific events occur. All devices in the Basic Small Branch Network used NTP to synchronize their clocks. The NTP server was hosted at the central site.

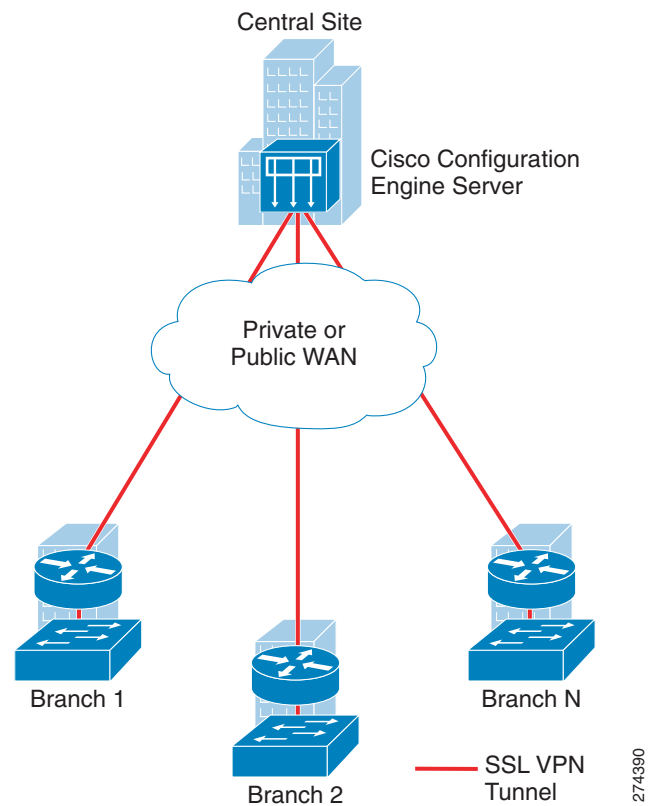
To learn more about NTP, visit:

http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Cisco Configuration Engine

The Cisco Configuration Engine (CCE) automates installation and provisioning of Cisco devices during their initial deployment and in subsequent reconfigurations. It securely distributes software images and device configuration files to one or multiple devices on a local LAN or over the WAN. In the Basic Small Branch Network, a centrally hosted CCE server was used to distribute Cisco IOS images and device configuration files to the branch routers and switches. During the initial deployment, the primary benefit of the CCE is consistent Cisco IOS image and configuration distribution across multiple branch networks. Once the network becomes operational, the CCE provides a simple, secure, and fast way to reconfigure all branch devices without the assistance of an on-site technician. Moreover, the ability to configure multiple devices from a single toolkit is less error-prone than individual configuration of each device. Figure 54 shows the deployment of CCE in the Basic Small Branch Network.

Figure 54 *Deployment of CCE in the Basic Small Branch Network.*



Each device that is to be provisioned with the CCE is assigned a unique Cisco Network Services (CNS) identifier and pre-loaded with a bootstrap configuration. Prior to powering up of the device, the CNS ID must be registered with the centrally hosted CCE server. After the device is powered up, it contacts the CCE server and requests to be provisioned. The CCE server uploads and activates the appropriate Cisco IOS image and configures the device for operation. This provisioning can be further simplified by configuring a centrally hosted DHCP server to provide the bootstrap configuration through the DHCP option 150.

The Basic Small Branch Network is accompanied by several CCE toolkits that can be used to configure the network. Because this document covers several hardware components and networking services that are functional alternatives of one another, the following five sample CCE toolkits, covering different combinations of technologies, are provided:

- Cisco 1861 Configuration
 - Fast Ethernet WAN interface, OSPF routing, DMVPN, and Cisco Unified CME with SCCP IP Phones and H.323 trunking to the central site.
 - A T1 WAN interface bundle with PPP encapsulation, EIGRP routing, GETVPN, and Cisco Unified CME with SIP IP Phones and SIP trunking to central site.
 - A T1 WAN interface bundle with Frame Relay encapsulation, EIGRP routing, DMVPN, and Cisco Unified SRST with SCCP IP Phones and H.323 trunking to central site.
 - One-half T1 WAN interface with Frame Relay encapsulation, OSPF routing, GETVPN, and Cisco Unified SRST with SIP IP Phones and SIP trunking to central site.
- Cisco 1841 Configuration

- Fast Ethernet WAN interface, active primary and standby backup WAN links, OSPF routing, DMVPN over primary and backup WAN links.
- A T1 WAN interface bundle with PPP encapsulation, active primary and standby backup WAN links, EIGRP routing, GETVPN over primary and DMVPN over backup WAN links.
- A T1 WAN interface bundle with Frame Relay encapsulation, simultaneously active primary and backup WAN links, EIGRP routing, DMVPN over primary and backup WAN links.
- One-half T1 WAN interface with Frame Relay encapsulation, simultaneously active primary and backup WAN links, OSPF routing, GETVPN over primary and DMVPN over backup WAN links.
- Access Switches
 - A 24-port access switch with Data, DMZ, and Voice VLANs on access ports.
 - A 8-port access switch with Data, DMZ, and Voice VLANs on access ports.

The sample CCE toolkits are intended to provide:

- Full and validated router and switch configurations for the Basic Small Branch Network
- Alternative configurations of the various technologies of the Basic Small Branch Network
- Starting points for customization of the Basic Small Branch Network configuration

The Basic Small Branch Network used CCE version 3.0 to deploy the branch router and switch Cisco IOS images and configurations. To learn more about CCE, visit:

http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps4617/data_sheet_c78-502925.html

Voice Services



Note

The following section applies only to the Cisco 1861 ISR configuration.

The availability of higher bandwidth and more reliable QoS guarantees enable enterprises to combine voice and data on the same converged IP network. IP-based voice services offer new, business-relevant functionality and are more cost effective than traditional telephone services.

Today, branch offices have two fundamental options for converged telephony:

- Voice over IP (VoIP): Traditional telephony devices such as analog phones, faxes, PBXs, and public switched telephone network (PSTN) attached to an IP network. A voice-enabled router digitizes and packetizes the voice and signaling traffic from the traditional devices and transports the traffic over the IP network.
- IP Telephony: IP-based telephony devices connected to an IP network that natively digitize and packetize voice and signaling traffic. A voice-enabled router transports the traffic over the IP network.

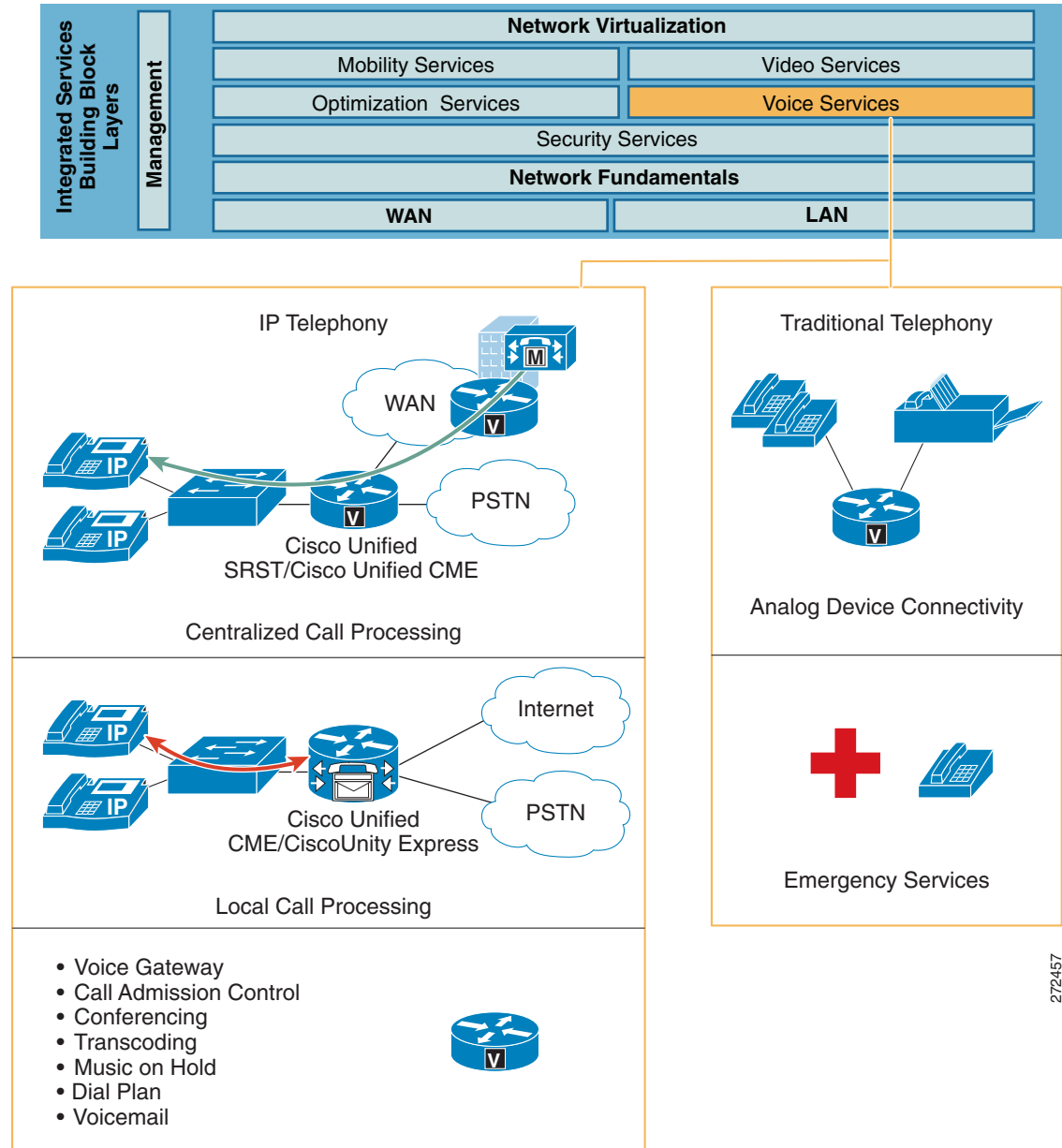
IP telephony was the primary focus of the Basic Small Branch Network. However, a small number of analog phones and fax machines were connected to the network and used for VoIP as well as traditional PSTN connectivity.

Voice services for a large branch office network are described in the following sections and shown in Figure 55:

- [Voice Quality Considerations, page 85](#)
- [WAN Capacity Considerations, page 87](#)

- [IP Telephony, page 90](#)
- [Traditional Telephony, page 99](#)

Figure 55 Voice Services



Voice Quality Considerations

The following fundamental packet propagation criteria must be satisfied in order to provide high-quality voice service:

- **Delay:** Delay is defined as the finite amount of time necessary for a packet to reach the receiving endpoint after being transmitted from the sending endpoint. For voice, this delay is defined as the amount of time it takes for sound to leave the mouth of the speaker and be heard in the ear of the listener. The ITU G.114 and Cisco recommend a maximum one-way, mouth-to-ear delay of 150 ms for high-quality voice.
- **Delay Variability (jitter):** Jitter is the difference in the end-to-end delay between packets. Cisco recommends a maximum jitter of less than 30 ms for high-quality voice.
- **Packet loss:** Packet loss is a relative ratio of packets successfully sent and received to the total number of packets transmitted. The amount of packet loss that can be tolerated is user-dependent; however, on average, packet loss should be kept to less than 1 percent to ensure high-quality voice service.

Table 14 summarizes packet propagation criteria that must be met to support high-quality voice.

Table 14 *Not-to-Exceed Packet Propagation Criteria for High-Quality Voice Service*

Propagation Factor	Not-to-exceed Value
Delay (Latency)	150 ms
Delay variability (Jitter)	30 ms
Packet Loss (Packet Drops)	1 percent

For more information about controlling voice quality, visit:

http://www.cisco.com/en/US/netsol/ns341/ns396/ns172/ns103/networking_solutions_white_paper09186a00801b1c5a.shtml

Another factor affecting voice quality is the codec used to digitize the voice signal. Cisco voice devices typically use the following two codecs:

- **G.711:** Provides encoding that does not perform any compression and requires 64 kb/s of bandwidth (not including overhead) for a single voice call. The mean opinion score (MOS), a metric used to measure voice quality, for G.711 is 4.1.
- **G.729a:** Provides encoding with compression and requires 8 kb/s of bandwidth (not including overhead) for a single voice call. Compression reduces the amount of required bandwidth, but affects the quality of the transmitted voice signal. However, the MOS score for G.729a is 3.9, which is a barely perceptible difference in comparison to G.711, and therefore the codec provides an acceptable tradeoff for the significant reduction in consumed bandwidth.

The selection of the appropriate codec depends on the desired level of voice quality, the amount of available bandwidth, and the number of concurrent voice calls that must be supported. In the Basic Small Branch Network, the G.729a codec is used for voice calls that will traverse the WAN links because it will provide bandwidth savings on these lower-speed links. The G.711 codec is used for LAN calls. To compensate for the quality factors described previously, it is critical that QoS be enabled in the branch network. The “[Quality of Service](#)” section on page 56 provides detailed information on QoS implemented in the Basic Small Branch Network. All real-time traffic was given 28 percent of the available bandwidth and was assigned for low latency queuing (LLQ). Call signaling was assigned 5 percent of the available bandwidth.

Traffic shaping is required for multiple-access, nonbroadcast media such as Frame Relay, where the physical access speed varies between two endpoints and several branch sites are typically aggregated to a single router interface at the central site. Shaping at the branch router alleviates potential congestion when the central site oversubscribes bandwidth or when the branch WAN link allows bursting beyond the Frame Relay committed information rate (CIR). The Basic Small Branch Network used traffic shaping to limit the traffic sent out on the WAN interfaces to a rate lower than the line rate. The specific

settings for traffic shaping vary from implementation to implementation and depend on the central site router provisioning and the Frame Relay configuration. IP SLAs described in the [“Management Services” section on page 78](#) ensured that the desired delay and jitter were maintained on the WAN link.

WAN Capacity Considerations

Three types of calls must be considered when provisioning the branch office for voice: PSTN (traditional), LAN (private exchange), and WAN (toll-bypass) calls. PSTN calls are needed for external communication, LAN calls are for intraoffice communication, and WAN calls enable communication with the rest of the enterprise. Knowing the number of PSTN calls and WAN calls helps to determine the number of voice lines and WAN bandwidth needed for the branch office. Traditionally, basic oversubscription ratios or Erlang traffic models have been used to determine the number of voice lines required for PSTN and WAN calling. Basic oversubscription ratios are typically based on call records collected from other existing offices of similar size and function, and applied to the new office. They equate the number of users to the number of PSTN and WAN calls required for calling. The business criteria outlined in the [Small Branch Design Considerations, page 4](#) specified the following oversubscription ratios:

- 5:1 user-to-active call ratio
- 4:1 WAN-to-LAN call ratio
- 4:1 WAN-to-PSTN call ratio

[Table 15](#) lists the requirements of the number of active calls for sample office sizes.

Table 15 *Active Calls for Typical 8- and 15-User Branch Offices, Using Oversubscription Ratios*

Active Calls	8-User Branch	15-User Branch
WAN	1	2
PSTN	1	2
LAN	1	2
Total calls	3	6

Alternatively, an Erlang traffic model can provide a more accurate method for determining the number of external voice lines (PSTN and WAN) required for a branch office. There are several variants of the Erlang model, depending on the intended telephone use in the branch office. The following example uses the Extended Erlang B to determine the number of voice lines required for the Basic Small Branch Network.

The Extended Erlang B traffic model takes into account the additional traffic load caused by blocked callers that immediately try to call again if their calls are blocked. The four variables involved are recall factor, busy hour traffic (BHT), blocking, and lines:

- Recall factor: Percentage of calls that immediately retry if their calls are blocked.
- Busy hour traffic (BHT): Number of hours (in Erlangs) of call traffic during the busiest hour of operation of a telephone system.
- Blocking: Failure rate of calls because of an insufficient number of available lines. For example, 0.03 means three calls blocked per 100 calls attempted.
- Lines: Total number of external lines needed.

**Note**

An *Erlang* is a unit of measurement of voice traffic. Strictly speaking, an Erlang represents the continuous use of one voice path or line. In practice, it is used to describe the total traffic volume in one hour.

If an average user calls for 12 minutes during the busy hour, external calls account for 10 minutes of those calls (or 10 min/60 min/hr = 0.17 Erlang), half of blocked calls immediately retry, blocked calls are no more than 3 percent of total calls, there is a 4:1 WAN-to-LAN call ratio, and there is a 4:1 WAN-to-PSTN call ratio, the Extended Erlang B calculator at <http://www.erlang.com/calculator/exeb/> suggests the total number of external lines for 8- and 15-user branch office as shown in Table 16.

Table 16 **Active Calls for Typical 15-, 30-, and 50-User Branch Offices, Using Extended Erlang B Traffic Model**

Active Calls	8-User Branch	15-User Branch
Busy Hour Traffic (Erlangs)	1.5	3
WAN	4	5
PSTN	1	2
LAN	1	2
Total calls	6	9

The critical assumption in the Extended Erlang B model is the amount of BHT per user (0.17 Erlang in the preceding example), which varies between enterprises, and even between branch offices within an enterprise. Therefore, Table 16 is provided only as an example. The Basic Small Branch Network used active call counts derived from the oversubscription ratios shown in Table 15.

Real-time Transport Protocol (RTP) is the primary protocol for transporting real-time traffic such as voice or interactive video. The minimum amount of bandwidth required to place a given number of calls over the WAN can be derived from the number of RTP streams. The size of each RTP stream depends on the WAN type, the associated encapsulations (Frame Relay, PPP, MLPP, Ethernet, IPsec, GRE), and the voice sampling rate. Figure 56 shows packet size for a G.729a RTP packet with DMVPN encapsulation. Figure 57 shows the packet size for G.729a RTP packet with GETVPN encapsulations.

Figure 56 **RTP Packet for G.729a Codec with DMVPN Encapsulation**

ESP Auth	ESP Pad	Voice Payload	RTP	UDP	IP	GRE	GRE IP	ESP IV	ESP	IPSecIP	Link Header
12	2-257	20	12	8	20	4	20	8	8	20	x
Bytes											

272664

Figure 57 **RTP Packet for G.729a Codes with GETVPN Encapsulation**

ESP Auth	ESP Pad	Voice Payload	RTP	UDP	IP	ESP IV	ESP	IP	Link Header
12	2-257	20	12	8	20	8	8	20	x
Bytes									

272665

An RTP packet contains 40 bytes of RTP and UDP header information. Because most information in these headers is identical (for example, the same source/destination IP address/UDP port numbers and the same RTP payload type), compressed RTP (cRTP) can be used to eliminate redundant header information in each frame. Using cRTP reduces the 40-byte header to only 2 or 4 bytes, allowing more calls to be placed over the same link speed. Table 17 shows sample bandwidth requirements for RTP and cRTP streams with the various Basic Small Branch Network WAN encapsulations. The Cisco Voice Codec Bandwidth Calculator that was used to calculate the necessary bandwidth requirements is available at:

<http://tools.cisco.com/Support/VBC/do/CodecCalc1.do>,

Although cRTP reduces the amount of required bandwidth, it is a CPU intensive process that may impact the overall performance of the router. Therefore, cRTP is appropriate only when voice traffic represents more than 33 percent of the load on the link, when the link uses a low bit-rate codec (such as G.729), and when no other real-time application (such as video conferencing) is using the same link.

Table 17 Bandwidth Requirement for a Single Call with Various WAN Encapsulation Methods

	Frame Relay, PPP, MLPP		Ethernet	
	RTP (kbps)	cRTP (kb/s)	RTP (kb/s)	cRTP (kb/s)
DMVPN	56	40	60	N/A
GETVPN	46	30	50	N/A

The Basic Small Branch Network used cRTP to minimize bandwidth consumption only on the fractional T1 connection; other WAN connection types used RTP. However, it should be noted that the fractional T1 link does not require cRTP to support up to 15 users with the oversubscription ratios provided previously. In the Basic Small Branch Network, cRTP was validated for completeness and demonstration purposes only.

The QoS model allocates 28 percent of bandwidth to real-time traffic. Table 18 shows the amount of bandwidth required for voice communication and the total bandwidth that is required to support branch offices of 8 and 15 users with various WAN encapsulation methods. The total number of active voice calls is derived from the oversubscription ratios shown in Table 15. In general, each call has two streams for audio traffic; one stream from caller to callee, and another stream in the reverse direction.

Table 18 Bandwidth Requirements for Voice Traffic and Total Bandwidth for a Basic Small Branch Network with 8- and 15-User Counts

	Frame Relay, PPP, MLPPP				Ethernet	
	RTP Voice (Mbps)	RTP Total (Mb/s)	cRTP Voice (Mp/s)	cRTP Total (Mb/s)	RTP Voice (Mb/s)	RTP Total (Mb/s)
8-User Basic Small Network (1 simultaneous WAN call)						
DMVPN	0.05	0.17	0.04	0.12	0.06	0.18
GETVPN	0.04	0.14	0.03	0.09	0.05	0.09
15-User Basic Small Network (2 simultaneous WAN calls)						
DMVPN	0.11	0.33	0.08	0.24	0.12	0.36
GETVPN	0.09	0.27	0.06	0.18	0.1	0.3

Table 18 shows that the following user counts are appropriate for the various WAN connection options of the Basic Small Branch Network:

- T1 line: Up to 15 users with RTP
- ½ T1 line: Up to 15 users with RTP
- Fast Ethernet shaped to 1.5 Mb/s: Up to 15 users with RTP

Besides considering provisioning of bandwidth for voice bearer traffic, you should consider bandwidth requirements for call control traffic. For centralized call control described below, the following calculations can be used to determine the amount of required bandwidth in a VPN network:

- SCCP Phone Traffic with VPN:
Bandwidth (bps) = 415 * (number of IP Phones and gateways in the branch)
- SIP Phone Traffic with VPN:
Bandwidth (bps) = 619 * (number of IP Phones and gateways in the branch)

A 15-user Basic Small Branch Network requires less than 6 kb/s for SCCP phone traffic, and 9 kb/s for SIP phone traffic, which is well below the 5 percent maximum assumed in the preceding calculations.

For the local call control described below the following calculation can be used to determine the amount of required bandwidth in a VPN network:

$$\text{Bandwidth (b/s)} = 116 * (\text{number of telephone lines})$$

A 15-user Basic Small Branch Network requires less than 2 kb/s for H.323 or SIP control traffic, which is also well below the 5 percent maximum assumed in the above calculations.

To learn more about voice communication in a VPN network see the *Voice and Video Enabled IPsec VPN (V3PN) Design Guide* at:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PN_SRND/V3PN_SRND.html

IP Telephony

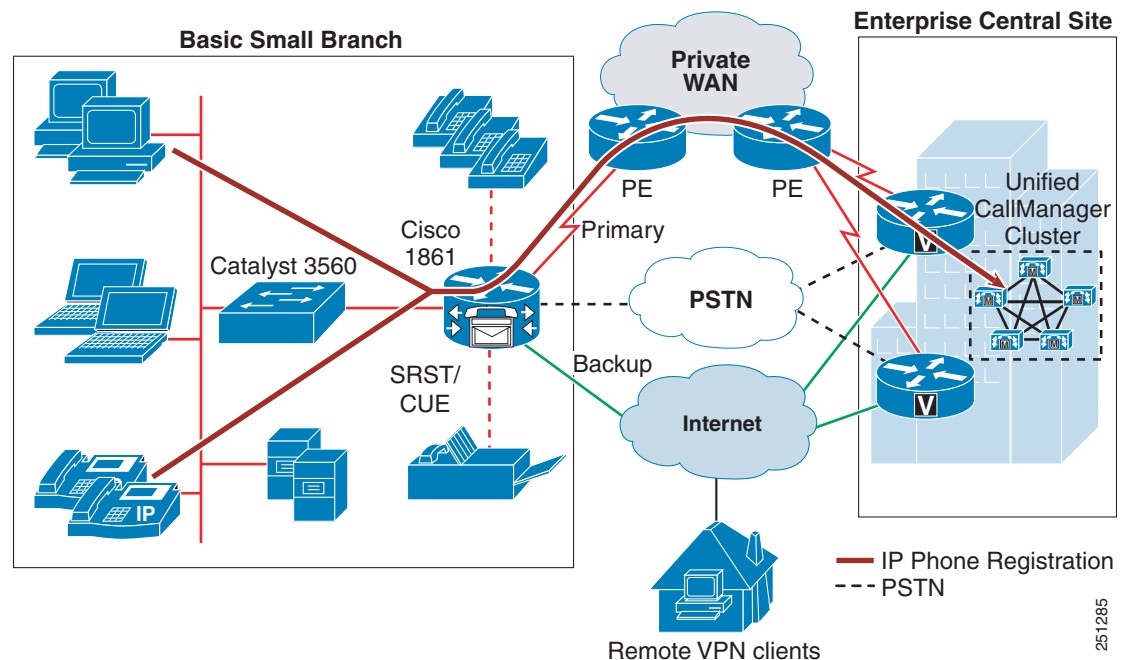
- [Centralized Call Control, page 91](#)
- [Local Call Control, page 92](#)
- [Selecting a Call Control Model, page 93](#)
- [IP Phones, page 93](#)
- [Voice Gateway, page 94](#)
- [Call Admission Control, page 96](#)
- [Conferencing and Transcoding, page 98](#)
- [Music on Hold, page 98](#)
- [Dial Plan, page 98](#)
- [Voice Mail and Auto Attendant Services, page 99](#)

The call control agent is a component of IP telephony that is responsible for overall coordination of all audiovisual communication. The agent has three typical deployment models: single site, multisite centralized, and multisite distributed call control (local). The Basic Small Branch Network assumes the presence of an enterprise central site; therefore, only the multisite centralized and distributed call control models were evaluated.

Centralized Call Control

The centralized call control model consists of a centrally located Cisco Unified Communications Manager (Cisco Unified CM) cluster that provides services for many branch offices and uses the WAN to transport voice traffic between the sites. The WAN also carries call signaling traffic between the central site and the branches. The Centralized Call Processing Model shown in Figure 58 depicts the centralized call control deployment with a Cisco Unified CM cluster as the call control agent at the central site and with a WAN connection to the Basic Small Branch Network. The branch relies on the centralized Cisco Unified CM cluster to handle its call control. Applications such as voice mail and music on hold (MOH) are provided in the branch to reduce the amount of traffic traversing the WAN.

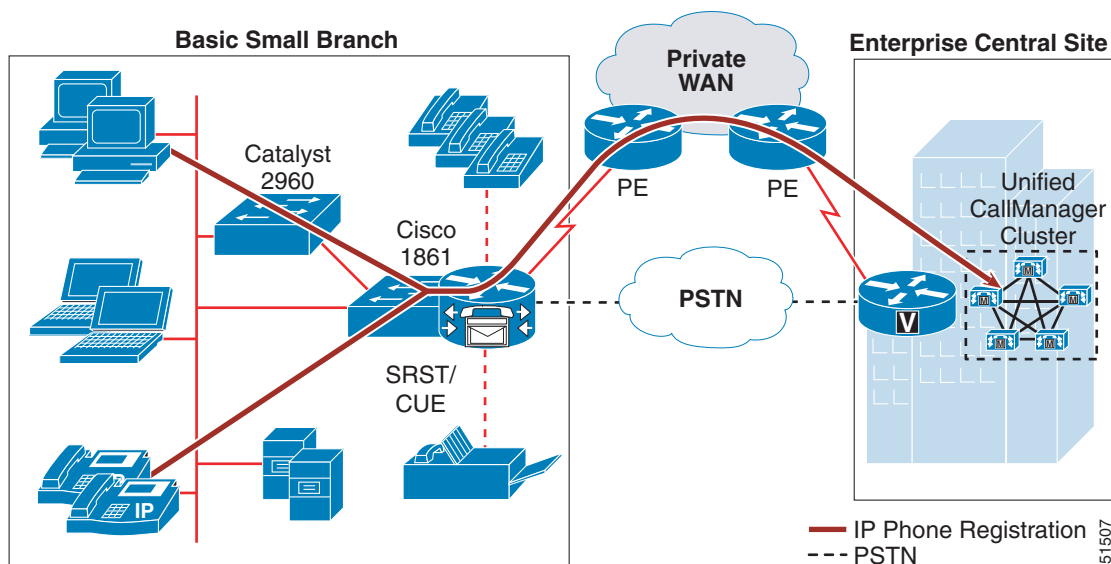
Figure 58 *Centralized Call Control Model*



Under normal operations shown on the left in Figure 58, the branch office connects to the central site via a WAN, which carries data traffic, voice traffic, and call signaling. IP Phones at the branch exchange call signaling information with the Cisco Unified CM cluster at the central site. The voice gateway in the router forwards both types of traffic (call signaling and voice) transparently and has no “knowledge” of the IP Phones in the branch.

If the WAN link to the branch office fails, or if some other event causes loss of connectivity to the Cisco Unified CM cluster, the branch IP Phones reregister with the branch router that is running Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) agent, as shown in Figure 59. The Cisco Unified SRST queries the IP Phones for their configuration and uses this information to build its own configuration automatically. The branch IP Phones can then make and receive calls either internally or through the PSTN. The phone displays the message “Unified CM fallback mode,” and some advanced Cisco Unified CM features are unavailable and are dimmed on the phone display. When WAN connectivity to the central site is reestablished, the branch IP Phones automatically reregister with the Cisco Unified CM cluster and resume normal operation. The branch Cisco Unified SRST router deletes its information about the IP Phones and reverts to its standard gateway configuration.

Figure 59 Cisco Unified SRST Mode for Centralized Call Control Model



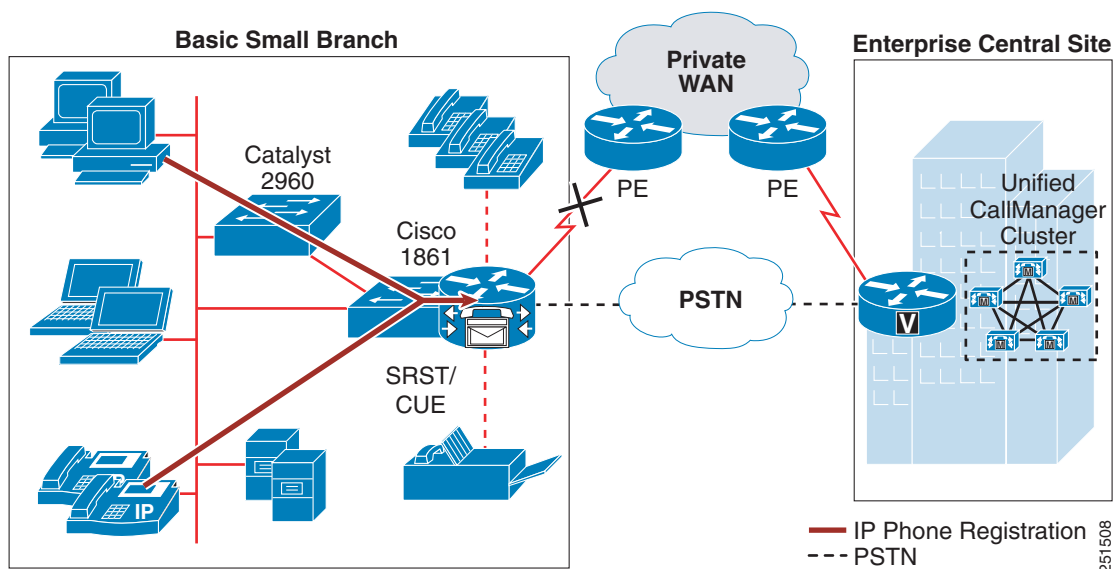
To learn more about Cisco Unified CM, visit:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/6x/uc6_1.html

Local Call Control

In the local call control model, each branch has its own Cisco Unified Communications Manager Express (Cisco Unified CME) connected to a WAN that carries voice traffic between the enterprise branches and central site. The PSTN serves as a backup connection between the sites if the WAN connection fails or has no more bandwidth available for additional calls. All call functionality is provided locally through Cisco Unified CME, and all IP Phones are registered locally, as shown in Figure 60. Applications such as voice mail and music on hold are provided in the branch router.

Figure 60 Distributed Call Control Model



The local call control model eliminates dependency on out-of-the-branch control elements that would otherwise have to be accessed over the WAN. Thus, a WAN link failure has no effects on functionality provided by the IP telephony network; the network changes only the path over which the external WAN calls are routed.

To learn more about Cisco Unified CME, visit:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/srnd/design/guide/cmesrnd.html

Selecting a Call Control Model

Although the local call control model has better availability properties than the centralized model, this advantage comes at an expense of additional functionality and ease management. Selecting the appropriate model involves numerous considerations. Table 19 describes the general trade-offs between the two models.

Table 19 Trade-offs Between Centralized and Local Call Control Models

Factor	Centralized Model	Local Model
WAN link characteristics	Needs more bandwidth and is more sensitive to link delay	Needs less bandwidth and is less sensitive to link delay
High availability	Impacted by WAN link failure	No WAN dependencies
Feature set	More features	Fewer features
Scalability	Scales better	Scales poorly
Management	Centralized	Per-branch office

When deciding between the two deployment models, you must consider the overall enterprise voice deployment and any existing voice systems already in use. The Basic Small Branch Network was validated with both centralized call control using Cisco Unified CM with Cisco Unified SRST and with local call control using Cisco Unified CME.

IP Phones

Cisco IP Phones described in the “[Selecting Network Components](#)” section on page 19 can operate in either Skinny Call Control Protocol (SCCP) or Session Initiation Protocol (SIP) mode. The main trade-off between SCCP and SIP is in the functionality supported and third-party interoperability. SCCP is a Cisco proprietary protocol with a large number of Cisco voice products supporting its various features. SIP, on the other hand, is based on an open standard and has been adapted by a larger number of VoIP vendors. The Basic Small Branch Network has been tested with both SIP and SCCP phones, with both the centralized call control model and the local call control model.

In addition to the IP Phones described previously, the Basic Small Branch Network also uses Cisco IP Communicator, a software-based application that runs on a PC. The Cisco IP Communicator, shown in [Figure 61](#), only uses SCCP for call signaling.

Figure 61 Cisco IP Communicator

To learn more about the Cisco IP Communicator product, visit:

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps5475/product_data_sheet0900aecd8064efe0.html

Voice Gateway

Both VoIP and IP telephony networks require a gateway to convert voice and signaling information between the traditional PSTN system and an IP-based system. The gateway must interpret PSTN analog or digital signaling to provide connectivity. A Cisco IOS voice gateway provides a full range of signaling options. Analog signaling and Basic Rate Interface (BRI)-based digital signaling provide PSTN connectivity for branch offices with a relatively small number of users. [Table 20](#) displays the various Cisco IOS analog signaling options that pertain to the Basic Small Branch Network.

Table 20 Cisco IOS Software Support for Analog Digital Signaling Protocols

Signaling	Description	Typical Use
Analog DID	Analog Direct Inward Dial	Used to connect to an analog PSTN line that has DID service for incoming calls on it.
CAMA	Centralized Automatic Message Accounting	Used to connect the PSTN for emergency services (911 calls) in North America.
FXO	Foreign Exchange Office	Generally, used to connect to an analog PSTN line. It can be connected to any interface where a standard analog phone is currently connected.

The Basic Small Branch Network used two FXO ports provided on the Cisco 1861 ISR to connect the branch network to the PSTN. The FXO ports are connected with regular telephone lines to an FXS interface provided by the local telephone company and run to the nearest central office (CO) in the area. FXO ports, like all other analog interfaces, carry one call per port, so that each FXO port connects to

one line from the PSTN and carries a single call at a time. A second call is given a busy tone if it tries to use the same port or line. In future updates to this guide, some of the other options listed in [Table 20](#) will be validated and documented.

Digital signal processor (DSP) technology provides voice compression, echo cancellation, tone generation, and voice packetization functions for servicing voice interfaces and converting voice signals for transport over IP networks. The number of required DSP modules depends on the amount and type of voice traffic in the branch. The Cisco 1861 ISR is packaged with a single-packet voice DSP module, PVDM-32.

Besides physical connectivity and signal conversion, you must consider other PSTN services when configuring the voice gateway. The FXO signaling mechanism that was selected for the Basic Small Branch Network supports the following PSTN services:

- Traditional fax services continue to be a widely used mechanism for document delivery. Physical integration of fax into the Basic Small Branch Network is described in the [“Analog Device Connectivity” section on page 99](#). In addition to physical connectivity of fax machines, the voice gateway must support a mechanism for interoperability of analog fax with IP telephony networks.

In its original form, fax data is digital and is contained in High-Level Data Link Control (HDLC) frames. However, to transmit across a traditional PSTN, these digital HDLC frames are modulated onto an analog carrier. While this analog carrier is necessary for effective faxing in PSTN environments, it is not ideal for the type of digital transport used by IP packet networks. Therefore, specific transport methods have been devised for successful transport of fax transmissions over an IP infrastructure.

The two main methods for transporting fax over IP are pass-through and relay. Pass-through is the simplest method. It works by sampling and digitizing the analog fax signal just as a voice codec does for human speech. While there are a number of codecs available, pass-through always uses the G.711 codec for carrying fax information because it offers the least distortion of the analog fax signals. Fax pass-through works only with the call control protocols of H.323 and SIP. Because fax pass-through utilizes the call control protocol for its switchover, this is the only pass-through solution that can work with third-party devices.

Relay is the other main method for transporting fax over IP. Relay strips off the analog carrier from the fax signal, in a process known as *demodulation*, to expose the fax HDLC data frames. The pertinent information in these HDLC frames is then removed and efficiently packaged in a fax relay protocol to be transported to the gateway on the other side. After it is received on the other side, the fax information is pulled from the relay protocol, reconstructed into fax HDLC frames, and modulated on to an analog carrier for transmission to a fax machine.

Cisco supports two versions of Fax Relay, T.38 and Cisco Fax Relay. An ITU standard, T.38 allows Cisco gateways to interoperate with third-party devices that also support the T.38 specification. In most scenarios, T.38 Fax Relay uses the call control protocol to switch from voice mode to T.38 fax relay mode. Fax Relay mode, and more specifically T.38, is the preferred method for transporting fax traffic. The Basic Small Branch Network used both T.38-based fax relay and fax pass-through.

Two VoIP-enabled endpoints must use a common protocol stack to perform speech coding, call setup, signaling, data transport, and other functions related to voice communication. To ensure its relevance and applicability, The Basic Small Branch Network was validated with the following VoIP protocol stacks:

- H.323: Defines a suite of protocols, algorithms, and hardware specifications for audiovisual communication over IP-based network. The suite provides a complete protocol stack and defines precisely what is allowed and what is forbidden. H.323 includes speech coding algorithms such as G.711; RTP-based data transport; RTCP for controlling data channels; H.225 protocol for registration, admission, and status control; Q.931 call signaling protocol; and H.245 call control protocol.

- **Session Initiation Protocol (SIP):** Defines a protocol for setting up audiovisual connections over an IP network. Unlike H.323, which provides a complete protocol stack, SIP is a single, extensible module that has been designed to interwork with existing network-based applications. It is a text-based protocol modeled on HTTP.
- **Skinn Client Control Protocol (SCCP):** Lightweight protocol used to set up calls between Cisco IP Phones and a voice gateway proxy (for example, Cisco Unified CME). The proxy communicates with the H.323 gateway, using H.225 and H.245 signaling, and the IP Phone using the SCCP protocol. The IP Phone requires less processing overhead because most of the H.323 processing resides in the proxy.

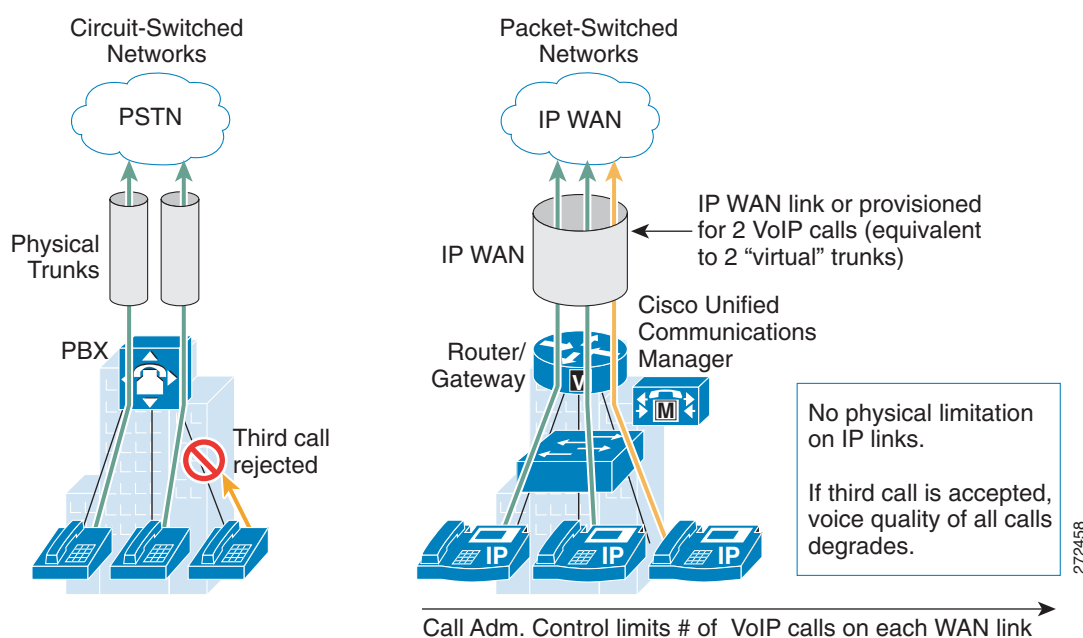
The choice between H.323 and SIP depends on the enterprise and is often based on feature requirements as well as interoperability with existing systems (for example, PBX, voicemail). In the Basic Small Branch Network, the following four combinations of call control agent, IP Phone protocol, and gateway-to-gateway protocol were validated:

- Cisco Unified CME with SCCP endpoints and H.323 trunk
- Cisco Unified CME with SIP endpoints and SIP trunk
- Cisco Unified SRST with SCCP endpoints and H.323 trunk
- Cisco Unified SRST with SIP endpoints and SIP trunk

Call Admission Control

Call Admission Control (CAC) maintains high voice quality over an IP WAN by limiting the number of calls that are admitted. Traditional telephony circuits, in which physical channels limit the number of calls allowed to connect to the PSTN, do not have this requirement. When VoIP calls traverse an IP WAN, calls are packet streams and there are no physical limitations that control the number of calls admitted to the WAN link. An IP WAN link can easily be oversubscribed, and the voice quality of all connected calls can be degraded, as shown in [Figure 62](#).

Figure 62 Traditional Versus VoIP Call Admission Control

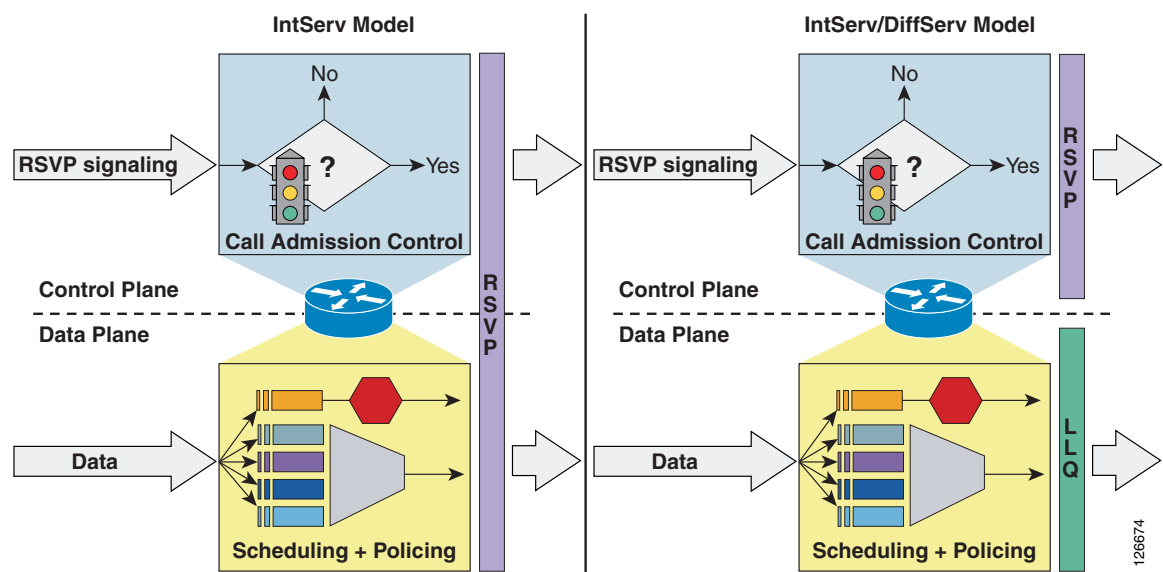


272458

Resource Reservation Protocol (RSVP) is a mechanism for dynamically setting up end-to-end QoS across a heterogeneous network. A resource reservation is created by exchanging signaling messages between the source and destination devices that are processed by intermediate routers along the path. The signaling messages “reserve” bandwidth at the intermediate routers for each unidirectional data flow. RSVP can propagate RSVP requests across routers that do not support the protocol. There are two operational models for RSVP, as described below and shown in Figure 63.

- **IntServ:** Controls resource reservation at both control and data planes. In the control plane, RSVP admits or denies the reservation request. In the data plane, it classifies the data packets, polices them based on the traffic description contained in the RSVP messages, and queues them in the appropriate queue.
- **IntServ/DiffServ:** Controls resource reservation at the control plane only. This means that the CAC function is separate from the scheduling and policing functions, which can be performed by the low latency queuing (LLQ) algorithm according to predefined class maps, policy maps, and service policies. With the IntServ/DiffServ model, it is therefore possible to add RSVP CAC to a network that is already using a differentiated services approach to QoS. RSVP admits or rejects calls, based on a preconfigured bandwidth amount, but the actual scheduling is based on the preexisting LLQ criteria such as the DSCP value of each packet.

Figure 63 *RSVP Operational Models: IntServ and IntServ/DiffServ*



The Basic Small Branch Network used the IntServ/DiffServ RSVP mechanism to control the number of calls placed on the network, but relied on the established QoS policy explained in the [“Quality of Service” section on page 56](#) to control actual packet scheduling. This model is appropriate for the Basic Small Branch Network because all LLQ-destined traffic is controlled by RSVP.

At present, RSVP is supported only in the centralized call control model with Cisco Unified SRST. To simulate the function of RSVP for the local call control model with Cisco Unified CME, a simple maximum call limit was placed on the WAN voice gateway.

Conferencing and Transcoding

Conferencing joins multiple participants into a single call. The number of media streams connected to a conference corresponds to the number of participants. A conference bridge mixes the streams together and creates a unique output stream for each connected participant. The output stream for a given participant is the composite of the streams from all connected participants minus their own input stream. The conference bridge is controlled by Cisco Unified CM or Cisco Unified CME. A conference bridge is allocated from the onboard DSPs. The Basic Small Branch Network was designed to support up to two simultaneous conferencing sessions. Cisco Unified CME provides conferencing locally through the branch router, while the centralized call control model leverages the conferencing functionality of the Cisco Unified CM in the central site.

Transcoding converts an input stream from one codec into an output stream that uses a different codec. It may also connect two streams that utilize the same codec but with a different sampling rate. Transcoding is typically used to convert between a G.711 voice stream and the low bit-rate compressed voice stream G.729a. The Basic Small Branch Network used transcoding to support endpoints that are configured for G.711 only. This condition exists when G.729a is used in the system but there are devices that do not support this codec, or there is a device with G.729a support that may be configured to not use G.729a. The Basic Small Branch Network was designed to support up to two simultaneous transcoding sessions.

The G.711 codec was used for LAN calls to maximize call quality and the G.729a codec was used for calls that traverse a WAN to maximize bandwidth efficiency. The G.729a codec is supported on all Cisco Unified IP Phone models and therefore G.711 to G.729a transcoding is not required.

Music on Hold

Music on hold (MOH) provides music to callers when their call is placed on hold, transferred, parked, or added to an ad-hoc conference. The integrated MOH feature allows both internal and external users to place users on hold with music streamed from a streaming source. There are two types of MOH transport mechanism: unicast and multicast. The Basic Small Branch Network used unicast to transport MOH data in the local call control mode (Cisco Unified CME). In the case of centralized call processing, multicast is used to transport MOH data. Multicast MOH consists of streams that are sent from the MOH source to a multicast group IP address, to which endpoints requesting an MOH audio stream can join. A multicast MOH stream is a point-to-multipoint, one-way audio RTP stream between the MOH source and the multicast group IP address. Multicast MOH conserves system resources and bandwidth because it enables multiple users to use the same audio source stream.

In the case of SCCP phones, the multicast was enabled on the branch router. In the case of SIP phones, multicast was configured at the central Cisco Unified CM, and the branch router simply forwarded the traffic as it would any other multicast application.

In the Basic Small Branch Network, the MOH source was an audio file stored on the branch router, except for the centralized deployment option with SIP phones.

Dial Plan

The dial plan is one of the key elements of an IP telephony system, and is an integral part of all call control agents. Generally, the dial plan is responsible for instructing the call control agent on how to route calls. Specifically, the dial plan in the Basic Small Branch Network performs the following functions:

- Endpoint addressing: Reachability of internal destinations is provided by assigning directory numbers (DNs) to all endpoints (such as IP Phones, fax machines, and analog phones) and applications (such as voice mail systems, auto attendants, and conferencing systems).

- Path selection: A secondary path can be used when the primary path is not available. The secondary path is made by rerouting over the PSTN during an IP WAN failure.



Note Cisco Unified CME does not support path selection.

- Digit manipulation: In some cases, it is necessary to manipulate the dialed string before routing the call; for example, when rerouting over the PSTN, a call originally dialed using the access code, or when expanding an abbreviated code (such as 0 for the operator) to an extension.

Additional functions are possible and will be validated in the future update to this guide:

- Calling privileges: Different groups of devices can be assigned to different classes of service by granting or denying access to certain destinations. For example, lobby phones might be allowed to reach only internal and local PSTN destinations, but executive phones could have unrestricted PSTN access.
- Call coverage: Special groups of devices can be created to handle incoming calls for a certain service according to different rules (top-down, circular hunt, longest idle, or broadcast).

The automated alternate routing (AAR) feature enables Cisco Unified CM to establish an alternate path for the voice data when the preferred path between two endpoints within the same cluster runs out of available bandwidth, as determined by the locations mechanism for call admission control. If a phone in one branch calls a phone in another branch, and the available bandwidth for the WAN link between the branches is insufficient, then AAR reroutes the call through the PSTN.

Voice Mail and Auto Attendant Services

All voice mail in the Basic Small Branch Network is stored locally in the branch for both centralized and distributed call control models. Cisco Unity Express provides cost-effective voice and integrated messaging and automated attendant for enterprise branch offices with up to 240 users. The Cisco 1861 ISR comes packaged with a Cisco Unity Express Advanced Integration Module (AIM) that can support up to 15 users.

Traditional Telephony

In the Basic Small Branch Network, traditional telephony is used to provide traditional fax services, emergency response, and call backup options as described in the following sections.

Analog Device Connectivity

There are various reasons to continue using some forms of traditional telephony in a branch office. For example, fax services continue to be widely used, and analog phones connected directly to a voice gateway can provide a backup of last resort. The Basic Small Branch Network used the four FXS ports provided by the Cisco 1861 ISR for connecting traditional voice devices into the network.

The ports were used for connecting a mixture of analog phones and faxes.

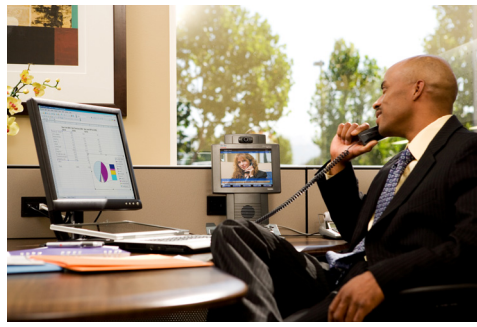
Emergency Services

Emergency services are of great importance in a proper deployment of a voice system. The Basic Small Branch Network was validated with the 911 emergency network as deployed in Canada and the United States. The design and implementation described are adaptable to other locales. Please consult with your local telephony network provider for appropriate implementation of emergency call functionality.

In general, a local exchange carrier has a dedicated network for the 911 service. In the Basic Small Branch Network, each of the FXO telephone lines connected the branch to the 911 service that was managed by Public Safety Answering Point (PSAP) through telephone company central office (CO).

To learn more about Emergency Services see:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/6x/e911.html



System Implementation

Revised: March 25, 2009

This section describes the information you need to configure the Cisco 1800 Series Integrated Services Router (ISR) branch routers and a Catalyst 2960 switch used in the Basic Small Branch Network.



Note

Use the [Command Lookup Tool \(registered customers only\)](#) for more information on the commands used in this document.

The full configuration of the Cisco 1800 Series ISR that was used for validating the features described in this guide is provided in the [Basic Small Branch Network Toolkit](#).

Contents

- [Network Topology, page 101](#)
- [WAN Services Implementation, page 105](#)
- [LAN Services Implementation, page 108](#)
- [Network Fundamental Services Implementation, page 118](#)
- [Security Services Implementation, page 136](#)
- [Voice Services Implementation, page 181](#)
- [Caveats, page 230](#)

Network Topology

[Figure 64](#) shows the components of the Basic Small Branch Network test bed. The topology includes the following components:

Enterprise Headquarters

- Web servers
- File servers
- Print servers
- PC clients

- Cisco 7200 Series VXR routers
- Cisco Secure ACS
- Catalyst 2960 and Catalyst 6500 switches
- IP Phones
- Cisco Unified Communications Manager (Cisco Unified CM)
- Cisco Wide Area Application Engine (Cisco WAE) 512
- Cisco Configuration Engine

Enterprise Branch

- Cisco 1861 and Cisco 1841 ISRs
- Cisco Catalyst 2960 switches
- Cisco Unified IP Phones 7942G, 7945G, 7961G, 7962G, 7965G, 7971G, and 7985G
- Cisco Unified IP Conference Station 7936
- PC clients
- Demilitarized zone (DMZ) servers
- Analog telephones and faxes

Figure 64 Basic Small Branch Network Test Bed

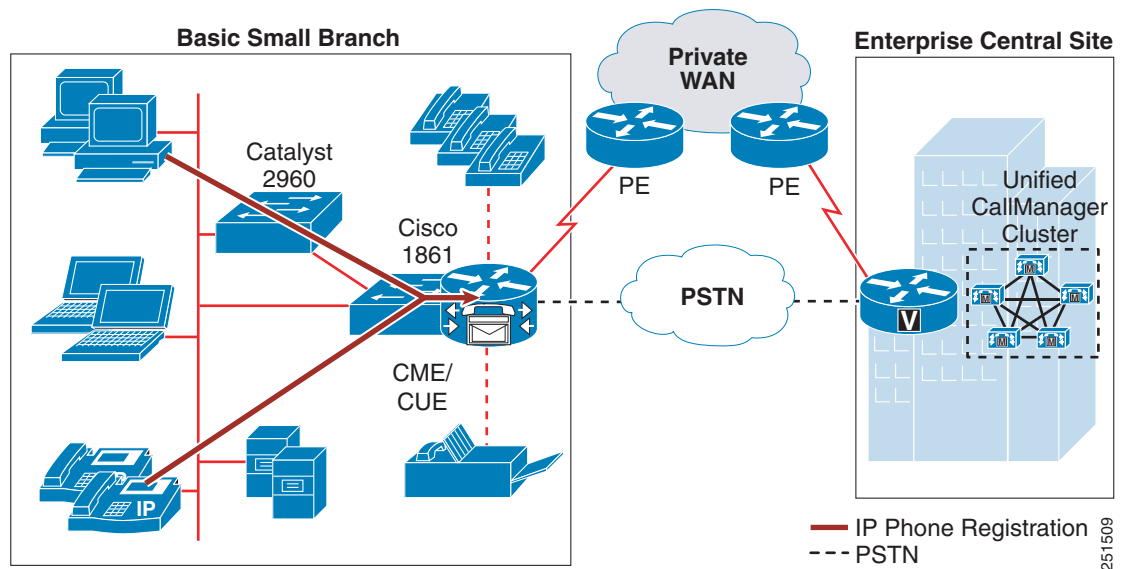


Figure 65 shows the detailed topology, interface assignment, and IP addressing scheme for the Cisco 1861 ISR.

Figure 65 Basic Small Branch Network Topology Using the Cisco 1861 ISR

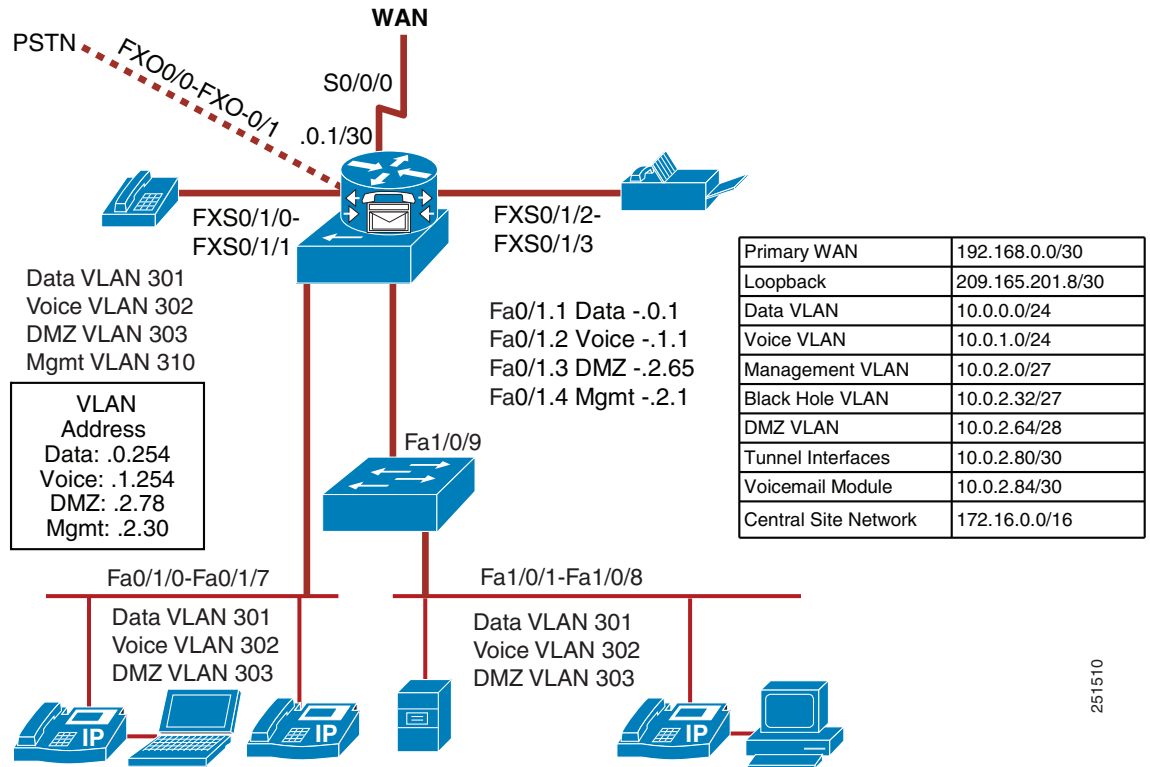


Figure 66 shows the detailed topology, interface assignment, and IP addressing scheme for the Cisco 1841 ISR.

251510

Figure 66 Basic Small Branch Network Topology Using the Cisco 1841 ISR

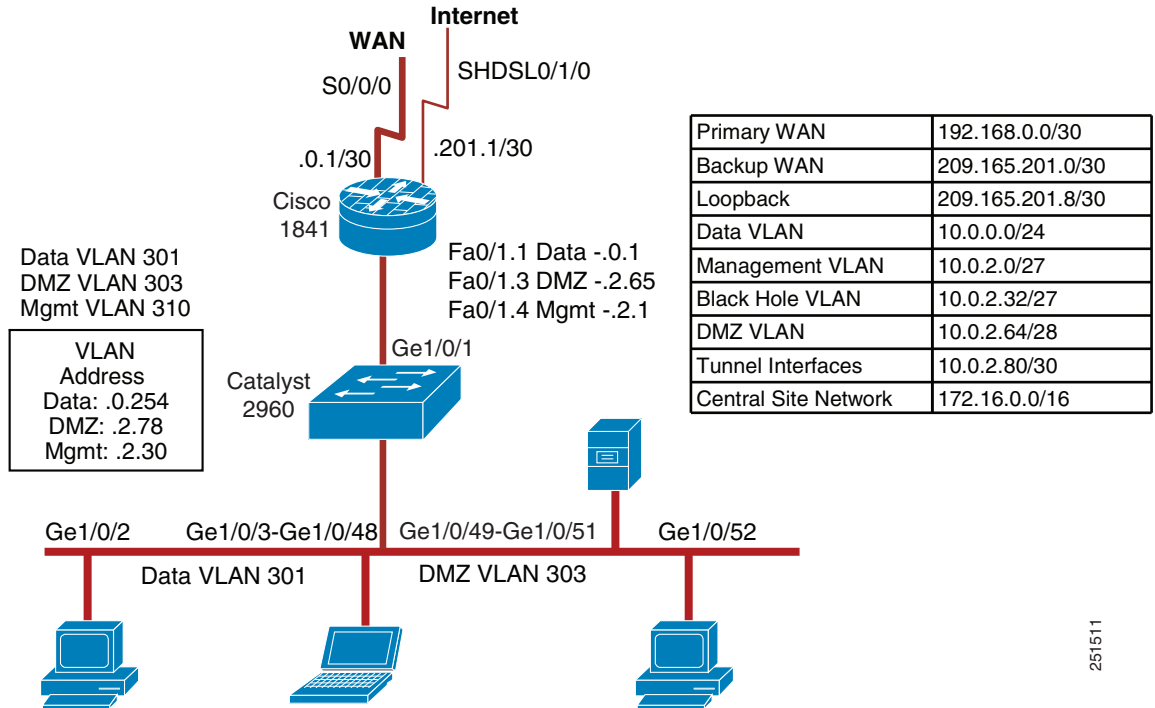


Figure 67 shows the high-speed WAN interface card (HWIC) on a Cisco 1861 router. WAN connectivity is provided by the 1-port high-speed interface card (HWIC-1T1/E1). A Cisco 1841 router, shown in Figure 68, was filled with a 1-port high-speed HWIC-1T interface card that does not provide an integrated CSU/DSU and HWIC-2SHDSL for backup WAN connectivity. In addition, the Cisco 1841 had an internal VPN module (AIM-VPN) that was placed into internal slot 0.

Figure 67 Interface Card and Service Module Configuration on a Cisco 1861 Router

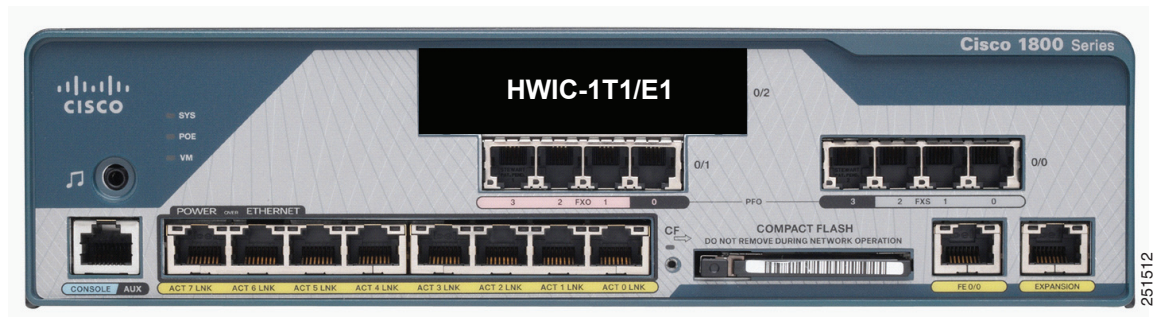
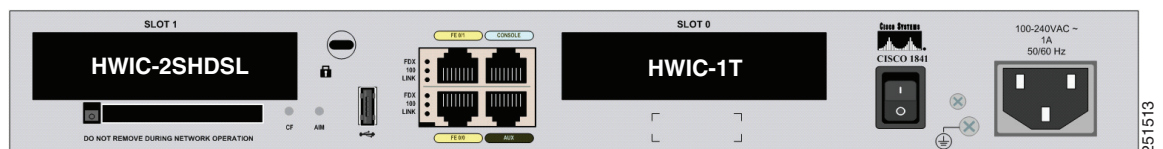


Figure 68 Interface Card and Service Module Configuration On a Cisco 1841 Router



WAN Services Implementation

The following three configurations were tested for connecting WAN access lines to the nearest provider edge (PE) device of the service provider network:

- [Single-Port DS-1 Interface with Frame Relay Encapsulation, page 105](#)
- [Single-Port DS-1 Interface with Point-to-Point Encapsulation, page 106](#)
- [Onboard Fast Ethernet Interface, page 107](#)

Single-Port DS-1 Interface with Frame Relay Encapsulation

A one-port T1/E1 high-speed WAN interface card was used for this configuration. Traditional Frame Relay (FR) shaping was applied on the interface. Alternatively, QoS-based shaping as defined in the *FIVE-CLASS-V3PN-EDGE-SHAPE* service policy can be used.

```
Router(config)# interface Serial0/0/0 ! Enters serial interface configuration mode
Router(config-if)# no ip address ! Disable IP processing on the serial interface
Router(config-if)# ip nbar protocol-discovery ! Enables NBAR to discover default protocols
and gather statistics
Router(config-if)# load-interval 30 ! Specifies interval for computing load statistics
Router(config-if)# dsu bandwidth 1550 ! Specifies maximum allowed bandwidth in Kbps for the
interface
Router(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth
available for QoS reservations
Router(config-if)# encapsulation frame-relay IETF ! Enables Frame Relay IETF standard
Router(config-if)# interface Serial0/0/0.1 point-to-point ! Defines point-to-point Frame
Relay sub-interface for the primary link
Router(config-subif)# ip address 192.168.0.1 255.255.255.252 ! Specifies an IP address for
the sub-interface
Router(config-subif)# ip access-group BLOCK-TFTP in ! Applies ACL named "BLOCK-TFTP" on
incoming traffic
Router(config-subif)# ip access-group BLOCK-TFTP out ! Applies ACL named "BLOCK-TFTP" on
outgoing traffic
Router(config-subif)# ip nbar protocol-discovery ! Enables NBAR to discover default
protocols and gather statistics
Router(config-subif)# ip flow ingress ! Enables NetFlow accounting for incoming packets
Router(config-subif)# ip flow egress ! Enables NetFlow accounting for outgoing packets
Router(config-subif)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
Router(config-subif)# no ip mroute-cache ! Disables fast-switching of multicast packets
Router(config-subif)# snmp trap link-status ! Generates SNMP trap when link-status changes
Router(config-subif)# frame-relay interface-dlci 230 ! Defines Frame Relay DLCI for the
sub-interface
Router(config-fr-dlci)# class FR-SHAPING ! Assigns Frame Relay configuration map
"FR-SHAPING" for traffic shaping. The map-class is defined in QoS section
Router(config-fr-dlci)# exit
```

Apply the following command on the Serial0/0/0.1 subinterface after defining the *Public* security zone as shown in the Security section.

```
Router(config-subif)# zone-member security Public ! Adds sub-interface to firewall zone
called Public
```

Apply the following command on the Serial0/0/0 interface after defining the *VPN-MAP* crypto map as shown in the Security section if using GETVPN.

```
Router(config-fr-dlci)# crypto map VPN-MAP ! Applies crypto map "VPN-MAP" to the Frame
Relay DLCI
```

Verification of Single-Port DS-1 Interface with Frame Relay Encapsulation

To verify your Frame Relay single-port DS-1 interface configuration, enter and verify the output of the following command:

```
Router# show frame-relay pvc 230
```

```
PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)
```

```
DLCI = 230, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.1
```

```

input pkts 12487          output pkts 12470          in bytes 2441416
out bytes 2441892        dropped pkts 0          in pkts dropped 0
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0          in BECN pkts 0          out FECN pkts 0
out BECN pkts 0         in DE pkts 0           out DE pkts 0
out bcast pkts 12443    out bcast bytes 2438648
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 4d03h, last time pvc status changed 4d03h
cir 56000    bc 7000    be 0          byte limit 875    interval 125
mincir 28000  byte increment 875    Adaptive Shaping none
pkts 12235    bytes 2398060  pkts delayed 0          bytes delayed 0
shaping inactive
traffic shaping drops 0
Queueing strategy: fifo
Output queue 0/40, 0 drop, 0 dequeued
Router#
```

Single-Port DS-1 Interface with Point-to-Point Encapsulation

The following configuration for the HWIC-1T T1/E1 interface card uses the PPP Layer 2 encapsulation method.

```

Router(config)# interface Serial0/0/0 ! Enters serial interface configuration mode
Router(config-if)# no ip address ! Disable IP processing on the serial interface
Router(config-if)# ip nbar protocol-discovery ! Enables NBAR to discover default protocols
and gather statistics
Router(config-if)# load-interval 30 ! Specifies interval for computing load statistics
Router(config-if)# dsu bandwidth 1550 ! Specifies maximum allowed bandwidth in Kbps for
the interface
Router(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth
available for QoS reservations
Router(config-if)# encapsulation PPP ! Sets Layer 2 encapsulation to PPP
Router(config-if)# ip address 192.168.0.1 255.255.255.252 ! Specifies an IP address for
the sub-interface
Router(config-if)# ip access-group BLOCK-TFTP in ! Applies ACL named "BLOCK-TFTP" on
incoming traffic
Router(config-if)# ip access-group BLOCK-TFTP out ! Applies ACL named "BLOCK-TFTP" on
outgoing traffic
Router(config-if)# ip nbar protocol-discovery ! Enables NBAR to discover default protocols
and gather statistics
Router(config-if)# ip flow ingress ! Enables NetFlow accounting for incoming packets
Router(config-if)# ip flow egress ! Enables NetFlow accounting for outgoing packets
Router(config-if)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
Router(config-if)# no ip mroute-cache ! Disables fast-switching of multicast packets
Router(config-if)# snmp trap link-status ! Generates SNMP trap when link-status changes
```

Apply the following command on the Serial0/0/0 interface after defining the *FIVE-CLASS-V3PN-EDGE-SHAPE* class as shown in the Security section.


```
Router(config-if)# service-policy output FIVE-CLASS-V3PN-EDGE-SHAPE ! Applies QoS policy
to the interface in outgoing direction to provide preferential treatment for traffic
```

Apply the following command on the Serial0/0/0 interface after defining the *Public* security zone in the Security section.

```
Router(config-if)# zone-member security Public ! Adds interface to firewall zone called
Public
```

Apply the following command on the Serial0/0/0 interface after defining the *VPN-MAP* crypto map in the Security section if using GETVPN.

```
Router(config-if)# crypto map VPN-MAP ! Applies crypto map "VPN-MAP" to the interface.
```

Onboard Fast Ethernet Interface

The onboard Fast Ethernet port was used for WAN connection with Ethernet encapsulation.

```
Branch(config)# interface FastEthernet0/0 ! Enters the Fast Ethernet interface
configuration mode
Branch(config-if)# ip address 192.168.0.1 255.255.255.252 ! Specifies an IP address for
interface
Branch(config-if)# ip access-group BLOCK-TFTP in ! Applies ACL named "BLOCK-TFTP" on
incoming traffic
Branch(config-if)# ip access-group BLOCK-TFTP out ! Applies ACL named "BLOCK-TFTP" on
outgoing traffic
Branch(config-subif)# ip nbar protocol-discovery ! Enables NBAR to discover default
protocols and gather statistics
Branch(config-if)# ip flow ingress ! Enables NetFlow accounting for incoming traffic
Branch(config-if)# ip flow egress ! Enables NetFlow accounting for outgoing traffic
Branch(config-if)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
Branch(config-if)# no ip mroute-cache ! Disables fast-switching of multicast packets
Branch(config-if)# load-interval 30 ! Specifies interval for computing load statistics
Branch(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth
available for QoS reservations
Branch(config-if)# media-type sfp ! Sets the Ethernet connector to SFP module
Branch(config-if)# no shutdown
Branch(config-if)# end
```

Apply the following command on the Fast Ethernet interface after defining the *FIVE-CLASS-V3PN-EDGE-SHAPE* class as shown in the Security section.

```
Router(config-if)# service-policy output FIVE-CLASS-V3PN-EDGE-SHAPE ! Applies QoS policy
to the interface in outgoing direction to provide preferential treatment for traffic
```

Apply the following command on the Fast Ethernet interface after defining the *Public* security zone as shown in the Security section.

```
Router(config-if)# zone-member security Public ! Adds interface to firewall zone called
Public
```

Apply the following command on the Fast Ethernet interface after defining the *VPN-MAP* crypto map as shown in the Security section if using GETVPN.

```
Router(config-if)# crypto map VPN-MAP ! Applies crypto map "VPN-MAP" to the interface
```

LAN Services Implementation

The main design consideration in the small branch office LAN design are security and manageability. A simplified multilayered LAN architecture addresses these criteria and makes it easier to troubleshoot network issues.

The simplified multilayered branch LAN architecture can be divided into the following layers:

- [Edge and Distribution Layer](#): Provides WAN connectivity, routing, addressing, high availability, quality of service (QoS), security, management services, and an exit point to the rest of the network.
- [Access Layer](#): Provides connectivity and Power-over-Ethernet (PoE) to end user devices. Layer 2 security, authentication, private VLANs, trunking, and QoS are addressed at this layer.

Edge and Distribution Layer

One of the onboard Fast Ethernet ports was connected to the access layer switch. The following VLAN configurations were applied to create VLANs across the branch network:

- [Data VLAN, page 108](#)
- [Voice VLAN, page 109](#)
- [DMZ VLAN, page 109](#)
- [Management VLAN, page 110](#)

Enable the LAN facing the Fast Ethernet interface.

```
Branch(config)# interface FastEthernet0/1 ! Enters Fast Ethernet sub-interface 2
configuration mode
Branch(config-subif)# no shutdown
```

Data VLAN

```
Branch(config)# interface FastEthernet0/1.1 ! Enters Fast Ethernet sub-interface 1
configuration mode
Branch(config-subif)# description Data-VLAN
Branch(config-subif)# encapsulation dot1q 301 ! Defines IEEE 802.1Q VLAN encapsulation
type
Branch(config-subif)# ip address 10.0.0.1 255.255.255.0 ! Assigns IP address to the
interface
Branch(config-subif)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
```

Apply the following command on the Fast Ethernet subinterface after defining the *INPUT-POLICY* class as shown in the Security section.

```
Branch(config-subif)# service-policy input INPUT-POLICY ! Executes a policy "INPUT-POLICY"
on incoming traffic
```

Apply the following command on the Fast Ethernet subinterface after defining the *Private* security zone as shown in the Security section.

```
Branch(config-subif)# zone-member security Private ! Adds the subinterface to firewall
zone called Private
```

Apply the following command on the Fast Ethernet subinterface after defining the *IPS-ADVSET* ACL as shown in the Security section.

```
Branch(config-subif)# ip ips IPS-ADVSET out ! Enables IPS signature matching for traffic
flowing in outward direction
```

```
Branch(config-subif)# ip ips IPS-ADVSET in ! Enables IPS signature matching for traffic
flowing in inward direction
```

Voice VLAN



Note

The following section applies only to the Cisco 1861 ISR configuration.

```
Branch(config)# interface FastEthernet0/1.2 ! Enters Fast Ethernet sub-interface 2
configuration mode
Branch(config-subif)# description Voice-VLAN
Branch(config-subif)# encapsulation dot1Q 302 ! Defines IEEE 802.1Q VLAN encapsulation
type
Branch(config-subif)# ip address 10.0.1.1 255.255.255.0 ! Assigns IP address to the
interface
Branch(config-subif)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
```

Apply the following command on the Fast Ethernet subinterface after defining the *INPUT-POLICY* class as shown in the Security section.

```
Branch(config-subif)# service-policy input INPUT-POLICY ! Executes a policy "INPUT-POLICY"
on incoming traffic
```

Apply the following command on the Fast Ethernet subinterface after defining the *Private* security zone as shown in the Security section.

```
Branch(config-subif)# zone-member security Private ! Adds the subinterface to firewall
zone called Private
```

DMZ VLAN

```
Branch(config-subif)# interface FastEthernet0/1.3 ! Enters Fast Ethernet sub-interface 3
configuration mode
Branch(config-subif)# description DMZ-VLAN
Branch(config-subif)# encapsulation dot1Q 303 ! Defines IEEE 802.1Q VLAN encapsulation
type
Branch(config-subif)# ip address 10.0.2.65 255.255.255.240 ! Assigns IP address to the
interface
Branch(config-subif)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
```

Apply the following command on the Fast Ethernet subinterface after defining the *INPUT-POLICY* class as shown in the Security section.

```
Branch(config-subif)# service-policy input INPUT-POLICY ! Executes a policy "INPUT-POLICY"
on incoming traffic
```

Apply the following command on the Fast Ethernet subinterface after defining the *DMZ* security zone as shown in the Security section.

```
Branch(config-subif)# zone-member security DMZ ! Adds the subinterface to firewall zone
called DMZ
```

Apply the following command on the Fast Ethernet subinterface after defining the *IPS-ADVSET* ACL as shown in the Security section.

```
Branch(config-subif)# ip ips IPS-ADVSET out ! Enables IPS signature matching for traffic
flowing in outward direction
Branch(config-subif)# ip ips IPS-ADVSET in ! Enables IPS signature matching for traffic
flowing in inward direction
```

Management VLAN

```
Branch(config-subif)# interface FastEthernet0/1.4 ! Enters Fast Ethernet sub-interface 4
configuration mode
Branch(config-subif)# description Management-VLAN
Branch(config-subif)# encapsulation dot1Q 310 ! Defines IEEE 802.1Q VLAN encapsulation
type
Branch(config-subif)# ip address 10.0.2.1 255.255.255.224 ! Assigns IP address to the
interface
Branch(config-subif)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
```

Apply the following command on the Fast Ethernet subinterface after defining the *INPUT-POLICY* class as shown in the Security section.

```
Branch(config-subif)# service-policy input INPUT-POLICY ! Executes a policy "INPUT-POLICY"
on incoming traffic
```

Apply the following command on the Fast Ethernet subinterface after defining the *Private* security zone as shown in the Security section.

```
Branch(config-subif)# zone-member security Private ! Adds the subinterface to firewall
zone called Private
```

Access Layer

- [VLAN Trunking Protocol Implementation, page 110](#)
- [Spanning Tree Implementation, page 112](#)
- [DOT1X Services, page 113](#)
- [QoS Implementation, page 114](#)
- [Assigning QoS to Switch Port, page 117](#)

VLAN Trunking Protocol Implementation

VLAN Trunking Protocol (VTP) is a client server protocol that reduces the overhead of network administration by propagating the VLAN information from the server to all the clients in a single VTP domain.

In the Basic Medium Branch Network, the Catalyst 2960 series switch at the distribution layer was configured as a VTP server. This provides an additional level of resiliency and simplifies management.

```
Switch-Access(config)# vtp domain VTP-BRANCH ! Creates VTP domain with name "VTP-BRANCH"
Switch-Access(config)# vtp mode server ! Sets the distribution switch to server VTP mode
```



Note

Always check the revision number of a new switch before bringing adding it to the network, regardless of whether the switch is going to operate in VTP client mode or operate in VTP server mode. To reset the revision number, do one of the following:

- Reboot the switch
or
- Temporarily change the domain name of the new switch and then change it back to its valid domain name.

VTP Verification

To verify your VTP configuration, enter the **show vtp status** command to display the VTP management status and other counters.

```
Switch# show vtp status
VTP Version                : 2
Configuration Revision      : 91
Maximum VLANs supported locally : 1005
Number of existing VLANs    : 5
VTP Operating Mode          : Server
VTP Domain Name             : VTP-BRANCH
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x01 0x71 0x91 0x17 0x8C 0x59 0xE5 0x39
Configuration last modified by 10.0.1.254 at 7-29-08 17:23:15
Local updater ID is 10.0.1.254 on interface Vl10 (lowest numbered VLAN interface found)
Switch#
```

VLAN Implementation

VLAN is a logical segmentation of LAN into multiple-broadcast domain that allows a group of hosts to communicate as if they were on a single LAN even if they are not physically collocated. A Layer 3 device is required for communication between VLANs.

Five VLANs were defined: DATA, VOICE, DMZ, MANAGEMENT, and BLACKHOLE.

```
Switch-Access(config)# vlan 301 ! Creates Data VLAN to vlan database
Switch-Access(config-vlan)# name DATA
Switch-Access(config-vlan)# exit
Switch-Access(config)# vlan 302 ! Creates Voice VLAN to vlan database
Switch-Access(config-vlan)# name VOICE
Switch-Access(config-vlan)# exit
Switch-Access(config) # vlan 303 ! Creates DMZ VLAN to vlan database
Switch-Access(config-vlan)# name DMZ
Switch-Access(config-vlan)# exit
Switch-Access(config)# vlan 310 ! Creates management VLAN to vlan database
Switch-Access(config-vlan)# name MANAGEMENT
Switch-Access(config-vlan)# exit
Switch-Access(config-vlan)# vlan 333 ! Creates black hole VLAN to vlan database
Switch-Access(config-vlan)# name BLACKHOLE
Switch-Access(config-vlan)# exit
Switch-Access(config)# interface Vlan301 ! Enters Data VLAN configuration mode
Switch-Access(config-if)# ip address 10.0.0.254 255.255.255.0 ! Specifies the IP address
for the SVI interface
Switch-Access(config-if)# interface Vlan302 ! Enters Voice VLAN configuration mode
Switch-Access(config-if)# ip address 10.0.1.0 254 255.255.255.0 ! Specifies the IP address
for the SVI interface
Switch-Access(config-if)# interface Vlan303 ! Enters switch virtual interface (SVI)
configuration
Switch-Access(config-if)# ip address 10.0.2.78 255.255.255.240 ! Specifies the IP address
for the SVI interface
Switch-Access(config-if)# interface Vlan310 ! Enters Management VLAN interface
configuration mode
Switch-Access(config-if)# ip address 10.0.2.30 255.255.255.224 ! Specifies the IP address
for the SVI interface
```

The following configuration was applied to all access ports connected to an IP Phone.



Note

The following example uses a 24-port Catalyst 2960. Modify the port types and ranges accordingly if an 8-port Catalyst 2960 series switch is used.

```
Switch-Access(config)# interface range g1/0/2 - 24 ! Enters configuration for range of
gigabit Ethernet ports
Switch-Access(config-if-range)# switchport mode access ! Sets the port to access mode
Switch-Access(config-if-range)# switch access vlan 301 ! Assigns the port to Data VLAN
Switch-Access(config-if-range)# switchport voice vlan 302 ! Assigns the port to Voice VLAN
Switch-Access(config-if-range)# spanning-tree portfast ! Sets the switch port to
forwarding state ignoring listening/learning state
Switch-Access(config-if-range)# srr-queue bandwidth share 1 70 25 5 ! Enables bandwidth
sharing for all output queues. Queue 1 is strict priority queue, queue 2 gets 70% of
bandwidth, queue 3 25% of bandwidth, and queue 4 5% of the bandwidth
Switch-Access(config-if-range)# srr-queue bandwidth shape 3 0 0 0 ! Specifies queue 2,3,4
to operate in shared mode.
Switch-Access(config-if-range)# priority-queue out ! Egress expedite queue is enabled.
This command will force SRR to ignore weight of queue 1 while calculating the bandwidth
ratio. This queue will be emptied before servicing other queues.
Switch-Access(config-if-range)# mls qos trust device cisco-phone ! Specifies the port to
trust the CoS/DSCP value if the CDP neighbor is Cisco IP Phone
Switch-Access(config-if-range)# load-interval 30 ! Specifies interval for computing load
statistics
```

The following configuration was applied to all access ports connected to a DMZ server.

```
Switch-Access(config)# interface range g1/0/25 - 28 ! Enters configuration for range of
gigabit Ethernet ports
Switch-Access(config-if-range)# switchport mode access ! Sets the port to access mode
Switch-Access(config-if-range)# switch access vlan 303 ! Assigns the port to DMZ VLAN
Switch-Access(config-if-range)# spanning-tree portfast ! Sets the switch port to
forwarding state ignoring listening/learning state
Switch-Access(config-if-range)# srr-queue bandwidth share 1 70 25 5 ! Enables bandwidth
sharing for all output queues. Queue 1 is strict priority queue, queue 2 gets 70% of
bandwidth, queue 3 25% of bandwidth, and queue 4 5% of the bandwidth
Switch-Access(config-if-range)# srr-queue bandwidth shape 3 0 0 0 ! Specifies queue 2,3,4
to operate in shared mode.
Switch-Access(config-if-range)# priority-queue out ! Egress expedite queue is enabled.
This command will force SRR to ignore weight of queue 1 while calculating the bandwidth
ratio. This queue will be emptied before servicing other queues.
Switch-Access(config-if-range)# load-interval 30 ! Specifies interval for computing load
statistics
```

Spanning Tree Implementation

```
Switch-Access(config)# spanning-tree mode pvst ! Enables Per-VLAN spanning-tree protocol
```

Spanning Tree Verification

To verify your Spanning Tree configuration, enter the **show spanning-tree summary** command to display the Spanning Tree mode enabled in the switch.

```
Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID          is enabled
Portfast Default            is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
```

```

Loopguard Default          is disabled
EtherChannel misconfig guard is enabled
UplinkFast                 is disabled
BackboneFast               is disabled
Configured Pathcost method used is short
    <Removed>

```

Uplink to Router Implementation

```

Switch-Access(config)# interface g1/0/1 ! Enters gigabit Ethernet interface configuration
mode
Switch-Access(config-if)# description trunk to router
Switch-Access(config-if)# switchport trunk encapsulation dot1q ! Tags outgoing frames with
IEEE 802.1Q trunk encapsulation format
Switch-Access(config-if)# switchport trunk allowed vlan 301-303,310 ! Defines list of
allowed VLANs that can send traffic on the trunk.
Switch-Access(config-if)# switchport mode trunk ! Enables the Ethernet port as VLAN trunk
Switch-Access(config-if)# load-interval 30 ! Specifies interval for computing load
statistics

```

DOT1X Services

```

Switch-Access(config)# aaa new-model ! Enables Authentication, Authorization and
Accounting services
Switch-Access(config)# aaa authentication dot1x default group radius ! Specifies default
dot1x authentication to use RADIUS server database
Switch-Access(config)# aaa session-id common ! Specifies to use the same session identifier
for all invocations of accounting services
Switch-Access(config)# dot1x system-auth-control ! Enables IEEE 802.1x authentication
globally on the switch
Switch-Access(config)# radius-server host 172.16.0.80 ! Specifies RADIUS server IP address
Switch-Access(config)# radius-server key KEY-BR ! Specifies RADIUS server key as "KEY-BR"
for encrypting all communication with the RADIUS server
Switch-Access(config)# int range g1/0/2 - 52 ! Enters configuration for the range of Gigabit
Ethernet ports
Switch-Access(config-if-range)# dot1x port-control auto ! Enables dot1x authentication on
the port
Switch-Access(config-if-range)# dot1x timeout server-timeout 60 ! Specifies time to wait
for a response from RADIUS server before retransmitting

```

DOT1X Services Verification

To verify your DOT1X services configuration, enter the following command:

```

Switch-Access# show dot1x interface g1/0/2
Supplicant MAC <Not Applicable>
  AuthSM State      = N/A
  BendSM State      = N/A
PortStatus          = N/A
MaxReq              = 2
MaxAuthReq          = 2
HostMode            = Single
PortControl         = Auto
QuietPeriod         = 60 Seconds
Re-authentication   = Disabled
ReAuthPeriod        = 3600 Seconds
ServerTimeout       = 60 Seconds
SuppTimeout         = 30 Seconds
TxPeriod            = 30 Seconds
Guest-Vlan          = 0

```

QoS Implementation



Note

The following section applies only to the internal switch of the Cisco 1861 ISR configuration.

The mapping for the CoS to DSCP values is shown in [Figure 43](#) in the “Quality of Service” section on [page 56](#).

```
Switch-Access(config)# mls qos ! Enables QoS on the switch
Switch-Access(config)# mls qos map policed-dscp 0 10 18 24 25 34 to 8 ! Defines
Policed-DSCP map which is used to mark down the packets with specified values to DSCP 8.
Switch-Access(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56 ! Defines CoS-DSCP map
for preferential treatment
Switch-Access(config)# mls qos srr-queue output cos-map queue 1 threshold 3 5 ! Maps the
CoS 5 to egress queue 1 with threshold 3
Switch-Access(config)# mls qos srr-queue output cos-map queue 2 threshold 1 2 4 ! Maps the
CoS 2 and CoS 4 to egress queue 2 with threshold 1
Switch-Access(config)# mls qos srr-queue output cos-map queue 2 threshold 2 3 ! Maps the
CoS 3 to egress queue 2 with threshold 2
Switch-Access(config)# mls qos srr-queue output cos-map queue 2 threshold 3 6 7 ! Maps the
CoS 6 and CoS 7 to egress queue 2 with threshold 3
Switch-Access(config)# mls qos srr-queue output cos-map queue 3 threshold 3 0 ! Maps the
CoS 0 to egress queue 3 with threshold 3
Switch-Access(config)# mls qos srr-queue output cos-map queue 4 threshold 3 1 ! Maps the
CoS 1 to egress queue 4 with threshold 3
Switch-Access(config)# mls qos srr-queue output dscp-map queue 1 threshold 3 46 ! Maps
the DSCP value 46 to egress queue 1 with threshold 3
Switch-Access(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22
25 32 34 36 ! Maps the DSCP values 16, 18, 20, 22, 25, 32, 34 and 36 to egress queue 2 with
threshold 1
Switch-Access(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 38 ! Maps the
DSCP value 38 to egress queue 2 with threshold 1
Switch-Access(config)# mls qos srr-queue output dscp-map queue 2 threshold 2 24 26 36 !
Maps the DSCP values 24, 26, and 36 to egress queue 2 with threshold 2
Switch-Access(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 48 56 36 !
Maps the DSCP values 36, 48, and 56 to egress queue 2 with threshold 3
Switch-Access(config)# mls qos srr-queue output dscp-map queue 3 threshold 3 0 36 ! Maps
the DSCP values 0 and 36 to egress queue 3 with threshold 3
Switch-Access(config)# mls qos srr-queue output dscp-map queue 4 threshold 1 8 36 ! Maps
the DSCP values 8 and 36 to egress queue 4 with threshold 1
Switch-Access(config)# mls qos srr-queue output dscp-map queue 4 threshold 3 10 12 14 36 !
Maps the DSCP values 10, 12, 14, and 36 to egress queue 4 with threshold 3
Switch-Access(config)# mls qos queue-set output 1 threshold 2 70 80 100 100 ! Defines the
weighed tail-drop thresholds for queue 2 to 70% for threshold 1 and 80% for threshold 2
Switch-Access(config)# mls qos queue-set output 1 threshold 4 40 100 100 100 ! Defines the
weighed tail-drop thresholds for queue 4 to 40% for threshold 1 and 100% for threshold 2
Switch-Access(config)# ip access-list extended DVLAN-BULK-DATA ! Defines ACL to match Bulk
Data
Switch-Access(config-ext-nacl)# permit tcp any any eq 220 ! Match Internet Mail Access
Protocol v3 (IMAPv3)
Switch-Access(config-ext-nacl)# permit tcp any any eq 143 ! Match Internet Message Access
Protocol (IMAP)
Switch-Access(config-ext-nacl)# permit tcp any any eq smtp ! Match Simple Mail Transfer
Protocol
Switch-Access(config-ext-nacl)# ip access-list extended DVLAN-MISSION-CRITICAL-DATA !
Defines ACL to match Business Critical Data
Switch-Access(config-ext-nacl)# permit tcp any any eq www ! Match HTTP traffic for port 80
Switch-Access(config-ext-nacl)# permit tcp any any range 3200 3203 ! Match SAP traffic
Switch-Access(config-ext-nacl)# permit tcp any any eq 3600 ! Match SAP traffic
Switch-Access(config-ext-nacl)# permit tcp any any range 2000 2002 ! Match SCCP traffic
Switch-Access(config-ext-nacl)# permit udp any any eq isakmp ! Match Internet Security
Association and Key Management Protocol
```



```

Switch-Access(config-ext-nacl)# permit tcp any eq www any ! Match HTTP traffic coming from
source port 80
Switch-Access(config-ext-nacl)# ip access-list extended DVLAN-PC-VIDEO ! Defines ACL to
match Video traffic
Switch-Access(config-ext-nacl)# permit udp any any range 16384 32767 ! Match traffic in
the given port range
Switch-Access(config-ext-nacl)# ip access-list extended DVLAN-TRANSACTIONAL-DATA ! Defines
ACL to match Transactional Data
Switch-Access(config-ext-nacl)# permit tcp any any eq 1352 ! Match Lotus Notes traffic
Switch-Access(config-ext-nacl)# permit udp any any eq domain ! Match DNS traffic
Switch-Access(config-ext-nacl)# permit udp any any eq netbios-dgm ! Match NetBios traffic
Switch-Access(config-ext-nacl)# permit udp any any eq netbios-ns ! Match NetBios traffic
Switch-Access(config-ext-nacl)# permit udp any any eq netbios-ss ! Match NetBios traffic
Switch-Access(config-ext-nacl)# ip access-list extended VVLAN-ANY ! Defines ACL to match
Voice VLAN traffic
Switch-Access(config-ext-nacl)# permit ip 10.0.1.0 0.0.0.255 any
Switch-Access(config-ext-nacl)# ip access-list extended VVLAN-CALL-SIGNALING ! Defines ACL
to match voice signaling traffic
Switch-Access(config-ext-nacl)# permit udp 10.0.1.0 0.0.0.255 any
Switch-Access(config-ext-nacl)# permit tcp 10.0.1.0 0.0.0.255 any range 2000 2002
Switch-Access(config-ext-nacl)# ip access-list extended VVLAN-VOICE ! Defines ACL to match
voice traffic
Switch-Access(config-ext-nacl)# permit udp 10.0.1.0 0.0.0.255 any
Switch-Access(config-ext-nacl)# permit udp 10.0.1.0 0.0.0.255 any range 16384 32767
Switch-Access(config-ext-nacl)# class-map match-all DVLAN-TRANSACTIONAL-DATA ! Defines
class-map for Transactional Data
Switch-Access(config-cmap)# match access-group name DVLAN-TRANSACTIONAL-DATA ! Matches
traffic specified in DVLAN-TRANSACTIONAL-DATA ACL
Switch-Access(config-cmap)# class-map match-all DVLAN-PC-VIDEO ! Defines class-map for
Video traffic
Switch-Access(config-cmap)# match access-group name DVLAN-PC-VIDEO ! Matches traffic
specified in DVLAN-PC-VIDEO ACL
Switch-Access(config-cmap)# class-map match-all VVLAN-CALL-SIGNALING ! Defines class-map
for Voice signalling
Switch-Access(config-cmap)# match access-group name VVLAN-CALL-SIGNALING ! Matches traffic
specified in VVLAN-CALL-SIGNALING ACL
Switch-Access(config-cmap)# class-map match-all DVLAN-MISSION-CRITICAL-DATA ! Defines
class-map for Business critical traffic
Switch-Access(config-cmap)# match access-group name DVLAN-MISSION-CRITICAL-DATA ! Matches
traffic specified in DVLAN-MISSION_CRITICAL_DATA ACL
Switch-Access(config-cmap)# class-map match-all VVLAN-VOICE ! Defines class-map for voice
traffic
Switch-Access(config-cmap)# match access-group name VVLAN-VOICE ! Matches traffic
specified in VVLAN-VOICE ACL
Switch-Access(config-cmap)# class-map match-all VVLAN-ANY ! Defines class-map for voice
vlan traffic
Switch-Access(config-cmap)# match access-group name VVLAN-ANY ! Matches traffic specified
in VVLAN-ANY ACL
Switch-Access(config-cmap)# class-map match-all DVLAN-BULK-DATA ! Defines class-map for
Bulk traffic
Switch-Access(config-cmap)# match access-group name DVLAN-BULK-DATA ! Matches traffic
specified in DVLAN-BULK_DATA ACL
Switch-Access(config-cmap)# policy-map IPPHONE+PC-ADVANCED ! Defines Policy-map
Switch-Access(config-pmap)# class VVLAN-VOICE ! Matches traffic classified by VVLAN-VOICE
class-map
Switch-Access(config-pmap-c)# set dscp ef ! Set DSCP value to EF
Switch-Access(config-pmap-c)# police 6144000 61440 exceed-action drop ! Incoming traffic
will be policed to 6.2 Mbps with a 62 KB burst size and if the rate is exceeded packet
will be dropped
Switch-Access(config-pmap-c)# class VVLAN-CALL-SIGNALING ! Matches traffic classified by
VVLAN-VOICE class-map
Switch-Access(config-pmap-c)# set dscp cs3 ! Set DSCP value to CS3

```

```

Switch-Access(config-pmap-c)# police 1024000 10240 exceed-action policed-dscp-transmit !
Incoming traffic will be policed to 10.2 Mbps with a 10.2 KB burst size and if the rate is
exceeded packet will be marked down to Scavenger class (CS1)
Switch-Access(config-pmap-c)# class VVLAN-ANY ! Matches traffic classified by class-map
Switch-Access(config-pmap-c)# set dscp default ! Set DSCP value to 0
Switch-Access(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit !
Incoming traffic will be policed to 32 kbps with a 8 KB burst size and if the rate is
exceeded packet will be marked down to Scavenger class (CS1)
Switch-Access(config-pmap-c)# class DVLAN-PC-VIDEO ! Matches traffic classified by
class-map
Switch-Access(config-pmap-c)# set dscp af41 ! Set DSCP value to 0
Switch-Access(config-pmap-c)# police 1984000 19840 exceed-action policed-dscp-transmit !
Incoming traffic will be policed to 10.2 Mbps with a 10.2 KB burst size and if the rate is
exceeded packet will be marked down to Scavenger class (CS1)
Switch-Access(config-pmap-c)# class DVLAN-MISSION-CRITICAL-DATA ! Matches traffic
classified by class-map
Switch-Access(config-pmap-c)# set dscp 25 ! Set DSCP value to 25
Switch-Access(config-pmap-c)# police 12500000 125000 exceed-action policed-dscp-transmit !
Incoming traffic will be policed to 12.5 Mbps with a 125 KB burst size and if the rate is
exceeded packet will be marked down to Scavenger class (CS1)
Switch-Access(config-pmap-c)# class DVLAN-TRANSACTIONAL-DATA ! Matches traffic classified
by class-map
Switch-Access(config-pmap-c)# police 10000000 100000 exceed-action policed-dscp-transmit !
Incoming traffic will be policed to 10 Mbps with a 100 KB burst size and if the rate is
exceeded packet will be marked down to Scavenger class (CS1)
Switch-Access(config-pmap-c)# set dscp af21 ! Set DSCP value to AF21
Switch-Access(config-pmap-c)# class DVLAN-BULK-DATA ! Matches traffic classified by
class-map
Switch-Access(config-pmap-c)# set dscp af11 ! Set DSCP value to AF11
Switch-Access(config-pmap-c)# police 5000000 50000 exceed-action policed-dscp-transmit !
Incoming traffic will be policed to 5 Mbps with a 50 KB burst size and if the rate is
exceeded packet will be marked down to Scavenger class (CS1)
Switch-Access(config-pmap-c)# class class-default ! Defines default class
Switch-Access(config-pmap-c)# set dscp default ! Set DSCP value to 0
Switch-Access(config-pmap-c)# police 12500000 125000 exceed-action policed-dscp-transmit
! Incoming traffic will be policed to 12.5 Mbps with a 125 KB burst size and if the rate
is exceeded packet will be marked down to Scavenger class (CS1)

```

QoS Verification

To verify your QoS configuration, enter the **show mls qos** command to display whether QoS is enabled in the switch.

```

Switch-Access# show mls qos
QoS is enabled
QoS ip packet dscp rewrite is enabled

Switch-Access# show mls qos maps policed-dscp
Policed-dscp map:
  d1 :  d2 0  1  2  3  4  5  6  7  8  9
-----
  0 :    08 01 02 03 04 05 06 07 08 09
  1 :    08 11 12 13 14 15 16 17 08 19
  2 :    20 21 22 23 08 08 26 27 28 29
  3 :    30 31 32 33 08 35 36 37 38 39
  4 :    40 41 42 43 44 45 46 47 48 49
  5 :    50 51 52 53 54 55 56 57 58 59
  6 :    60 61 62 63

Switch-Access# show mls qos maps cos-dscp
Cos-dscp map:
  cos:   0  1  2  3  4  5  6  7

```

```
-----
dscp:   0   8 16 24 32 46 48 56
```

Assigning QoS to Switch Port



Note

The following section applies only to the internal switch of the Cisco 1861 ISR configuration.

```
Switch-Access(config)# interface range f1/0/1 - 8 ! Enters configuration for the range of
Gigabit Ethernet ports
Switch-Access(config-if-range)# service-policy input IPPHONE+PC-ADVANCED ! Applies QoS
policy IPPHONE+PC-ADVANCED to the interface in input direction.
ignoring listening/learning state
```

Verification of Assigning QoS to Switch Port

To verify that QoS is being assigned to the switch port, enter the **show policy-map interface** to display the QoS policy and the related counters.

```
Switch-Access# show policy-map interface f1/0/1
GigabitEthernet1/0/3

Service-policy input: IPPHONE+PC-ADVANCED

Class-map: VVLAN-VOICE (match-all)
  0 packets, 0 bytes
    offered rate 0 bps, drop rate 0 bps
  Match: access-group name VVLAN-VOICE

Class-map: VVLAN-CALL-SIGNALING (match-all)
  0 packets, 0 bytes
    offered rate 0 bps, drop rate 0 bps
  Match: access-group name VVLAN-CALL-SIGNALING

Class-map: VVLAN-ANY (match-all)
  0 packets, 0 bytes
    offered rate 0 bps, drop rate 0 bps
  Match: access-group name VVLAN-ANY

Class-map: DVLAN-PC-VIDEO (match-all)
  0 packets, 0 bytes
    offered rate 0 bps, drop rate 0 bps
  Match: access-group name DVLAN-PC-VIDEO

Class-map: DVLAN-MISSION-CRITICAL-DATA (match-all)
  0 packets, 0 bytes
    offered rate 0 bps, drop rate 0 bps
  Match: access-group name DVLAN-MISSION-CRITICAL-DATA

Class-map: DVLAN-TRANSACTIONAL-DATA (match-all)
  0 packets, 0 bytes
    offered rate 0 bps, drop rate 0 bps
  Match: access-group name DVLAN-TRANSACTIONAL-DATA

Class-map: DVLAN-BULK-DATA (match-all)
  0 packets, 0 bytes
    offered rate 0 bps, drop rate 0 bps
  Match: access-group name DVLAN-BULK-DATA

Class-map: class-default (match-any)
  0 packets, 0 bytes
```

```

offered rate 0 bps, drop rate 0 bps
Match: any
    0 packets, 0 bytes
    rate 0 bps

```

Network Fundamental Services Implementation

- [High Availability, page 118](#)
- [IP Addressing and IP Routing, page 119](#)

High Availability

- [Redundant WAN Link, page 118](#)

Redundant WAN Link



Note

The following section is relevant only to the Cisco 1841 ISR configuration.

Backup for any of the three access links is provided by using a Systematic High-Speed Digital Subscriber Line (SHDSL) with M-Pair bonding over ATM interface. The backup interface is connected to the closest PE device of the service provider network.

```

Router(config)# controller SHDSL 0/1/0 ! Enters controller configuration mode
Router(config-controller)# dsl-group 0 pairs 0, 1 m-pair ! Creates an M-Pair bundle
pairing links 0-1
Router(config-controller-dsl-group)# shdsl annex A-B ! Specifies annex A/B of G.991.2
standard to be used on the controller
Router(config-controller-dsl-group)# shdsl rate auto ! Sets the controller rate
negotiation in auto mode
Router(config-controller-dsl-group)# end

Router(config)# interface ATM0/1/0 ! Enters ATM interface configuration mode
Router(config-if)# bandwidth 2304 ! Sets the maximum allowed bandwidth in Kbps
Router(config-if)# load-interval 30 ! Specifies interval for computing load statistics
Router(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth
available for QoS reservations
Router(config-if)# exit

Router(config)# interface ATM0/1/0.1 point-to-point ! Creates ATM point-to-point
sub-interface and specifies its parameters
Router(config-subif)# ip address 209.165.201.1 255.255.255.252 ! Assigns IP address to the
interface
Router(config-subif)# pvc 10/10 ! Creates a PVC and specifies its parameters
Router(config-if-atm-vc)# protocol ip 209.165.201.2 broadcast ! Enables broadcast
capability to perform reverse-arp on the ISP router
Router(config-if-atm-vc)# vbr-rt 2304 2304 ! Assigns VBR class of service and defines peak
and average cell rate
Router(config-if-atm-vc)# oam-pvc manage ! Enables end-to-end F5 OAM loopback cell
transmission and OAM management
Router(config-if-atm-vc)# encapsulation aal5snap ppp Virtual-Template10 ! Configures PPPoA
AAL5+SNAP point-to-point encapsulation and associates it with Virtual-Template

Router(config)# interface Virtual-Template10 ! Enters Virtual Template configuration
Router(config-if)# bandwidth 2304 ! Sets the maximum allowed bandwidth in Kbps

```

```

Router(config-if)# ip unnumbered ATM0/1/0.1 ! Reuses the IP address of the ATM
sub-interface
Router(config-if)# ip nbar protocol-discovery ! Enables NBAR to discover default protocols
and gather statistics
Router(config-if)# ip flow ingress ! Enables NetFlow accounting for incoming traffic
Router(config-if)# ip flow egress ! Enables NetFlow accounting for outgoing traffic
Router(config-if)# load-interval 30 ! Specifies interval for computing load statistics
Router(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth
available for QoS reservations
Router(config-if)# end

```

Apply the following command on the Virtual Template interface after defining the *FIVE-CLASS-V3PN-EDGE-SHAPE* class as shown in the Security section.

```

Router(config-if)# service-policy output FIVE-CLASS-V3PN-EDGE-SHAPE ! Applies QoS policy
to the interface in outgoing direction to provide preferential treatment for traffic

```

Apply the following command on the Virtual Template interface after defining the *Public* security zone as shown in the Security section.

```

Router(config-if)# zone-member security Public ! Adds interface to firewall zone called
Public

```

Apply the following command on the Virtual Template interface after defining the *VPN-MAP* crypto map as shown in the Security section if using GETVPN.

```

Router(config-if)# crypto map VPN-MAP ! Applies crypto map "VPN-MAP" to the interface

```

Redundant WAN Link Verification

To verify the redundant WAN link configuration, enter the **show backup** command to display the backup interface and its status for each primary interface.

```

Router# show backup
Primary Interface   Secondary Interface   Status
-----
Serial0/0/0        ATM0/2/IMA0          normal operation

```

IP Addressing and IP Routing

- [Routing Protocol Implementation, page 119](#)
- [Multicast Implementation, page 127](#)
- [DHCP Implementation, page 127](#)
- [NAT Implementation, page 128](#)
- [Quality of Service Implementation, page 129](#)

Routing Protocol Implementation

A branch office router is likely to use a single routing protocol. However, because a network may use EIGRP, OSPF, RIPv2, BGP or static routing, all of these protocols were independently validated. The following configurations are for each of the protocols. [Table 21](#) summarizes the subnets in the Basic Small Branch Network.

Table 21 Subnet Assignment

Network	Address	Type
Primary WAN	192.168.0.0/30	Private
Backup WAN	209.165.201.0/30	Public
Loopback	209.165.201.8/30	Public
Data VLAN	10.0.0.0/24	Private
Voice VLAN	10.0.1.0/24	Private
Management VLAN	10.0.2.0/27	Private
Black Hole VLAN	10.0.2.32/27	Private
DMZ VLAN	10.0.2.64/28	Private
Tunnel Interfaces	10.0.2.80/30	Private
Voice Mail Module	10.0.2.84/30	Private
Cisco WAAS Module	10.0.2.88/30	Private
Central Site Network	172.16.0.0/16	Private

**Note**

The following sections apply only to the Cisco 1841 ISR configuration.

The Basic Small Branch Network provides direct access to the Internet through split tunneling. Various combinations of WAN services and VPN technologies lead to several different options for implementing the split tunnel mechanism. In WAN implementations where the network service provider is responsible for routing (for example, Layer 3 VPN [L3VPN]), split tunneling can be provided on the primary link and the backup link can be set to standby state. The implementation options vary slightly for GETVPN and DMVPN. In WAN implementations where the enterprise is responsible for routing, split tunneling can be provided on the backup link by maintaining it in an active state. Again, there is a slight variation between GETVPN and DMVPN implementations.

Active/Standby Primary/Backup WAN Links with DMVPN Implementation

The secondary WAN interface must be configured as the backup interface for the primary WAN link.

```
Router(config)# interface Serial0/0/0 ! Enters multilink interface configuration mode
Router(config-if)# backup interface ATM0/1/0 ! Specifies backup interface
Router(config-if)# exit
```

A loopback interface with a public address is used as the source interface for the DMVPN tunnel.

```
Router(config)# interface Loopback0 ! Enters loopback interface configuration mode
Router(config-if)# ip address 209.165.201.9 255.255.255.252 ! Specifies loopback subnet
Router(config-if)# exit
```

The “[DMVPN Implementation](#)” section on page 145 provides configuration for the tunnel interface. After the tunnel interface is defined, two routing processes are configured: one for the enterprise network, and another for the public network. The following sections provide implementations in which OSPF, EIGRP, and RIPv2 provide routing for enterprise traffic in which BGP is responsible for routing public traffic.

Enterprise Routing With OSPF

Enterprise networks are learned through the tunnel interface.

```
Router(config)# router ospf 1 ! Enables private network OSPF routing process
Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface
Router(config-router)# router-id 10.0.0.1 ! Specifies the OSPF router ID
Router(config-router)# network 10.0.0.0 0.0.0.255 area 0 ! Advertis Data VLAN subnet in
backbone area
Router(config-router)# network 10.0.1.0 0.0.0.255 area 0 ! Advertis Voice VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.0 0.0.0.31 area 0 ! Advertis Management VLAN
subnet in backbone area
Router(config-router)# network 10.0.2.64 0.0.0.15 area 0 ! Advertis DMZ VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.80 0.0.0.3 area 0 ! Advertis Tunnel subnet in
backbone area
Router(config-router)# network 10.0.2.88 0.0.0.3 area 0 ! Advertis WAAS subnet in
backbone area
Router(config-router)# exit
```

Enterprise Routing with EIGRP

Enterprise networks are learned through the tunnel interface.

```
Router(config)# router eigrp 1 ! Enables private network EIGRP routing process
Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface
Router(config-router)# no auto-summary ! Disable automatic route summarization
Router(config-router)# network 10.0.0.0 0.0.0.255 ! Advertis Data VLAN subnet
Router(config-router)# network 10.0.1.0 0.0.0.255 ! Advertis Voice VLAN subnet
Router(config-router)# network 10.0.2.0 0.0.0.31 ! Advertis Management VLAN subnet
Router(config-router)# network 10.0.2.64 0.0.0.15 ! Advertis DMZ VLAN subnet
Router(config-router)# network 10.0.2.80 0.0.0.3 ! Advertis Tunnel subnet
Router(config-router)# network 10.0.2.88 0.0.0.3 ! Advertis WAAS subnet
Router(config-router)# exit
```

Enterprise Routing with RIPv2

Enterprise networks are learned through the tunnel interface.

```
Router(config)# router rip ! Enables private network RIP routing process
Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface
Router(config-router)# no auto-summary ! Disable automatic route summarization
Router(config-router)# version 2 ! Enable RIP version 2
Router(config-router)# network 10.0.0.0 ! Advertis all branch subnets
Router(config-router)# exit
```

Service Provider Routing with BGP

The BGP routing process is responsible for establishing the tunnel link by advertising the loopback network. In default BGP configuration, the router learns public routes advertised by the PE or ISP router. A large routing table would slow down the destination network lookup process. In general, network service providers should not advertise Internet routes to the branch network, but in case this happens, an access list is defined to exclude public routes.

```
Router(config)# access-list 20 permit 209.165.201.8 0.0.0.3 ! Permits Loopback network and
blocks all others
Router(config)# router bgp 1 ! Enables public and loopback network BGP routing process
```

```

Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface
Router(config-router)# neighbor 192.168.0.2 remote-as 65015 ! Neighbor router IP for
primary link that is in autonomous system 65015
Router(config-router)# neighbor 209.165.201.2 remote-as 65016 ! Neighbor router IP for
backup link that is in autonomous system 65016
Router(config-router)# network 192.168.0.0 mask 255.255.255.252 ! Advertises primary WAN
link subnet
Router(config-router)# network 209.165.201.0 mask 255.255.255.252 ! Advertises backup WAN
link subnet
Router(config-router)# network 209.165.201.8 mask 255.255.255.252 ! Advertises Loopback
subnet
Router(config-router)# distribute-list 20 in ! Block all routing updates except for
Loopback network
Router(config-router)# exit

```

Finally, static routes are defined to direct traffic to the public network. When the primary link is active, it is used as the default route for all traffic. When the backup link is active, it is used as the default for all traffic.

```

Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.0.2 ! Sets the primary WAN link as
default for all traffic
Router(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.2 ! Sets the backup WAN link as
default for all traffic

```

Active/Standby Primary/Backup WAN Links with GETVPN on Primary Link and DMVPN on Backup Link Implementation

Because GETVPN is a tunnel-less protocol, it is used only on the primary WAN link. Because DMVPN is used for the backup link, the tunnel interface is needed only when the primary link fails. All enterprise network information is advertised over the primary link. Since this link also routes public traffic, it may insert public routes into the routing table. To prevent this situation, the following ACL is defined to allow only enterprise networks in the routing table.

```

Router(config)# access-list 10 permit 172.16.0.0 0.0.255.255 ! Permits all Enterprise
networks

```

Enterprise Routing with OSPF

Enterprise networks are learned through the primary WAN interface.

```

Router(config)# router ospf 1 ! Enables private network OSPF routing process
Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface
Router(config-router)# router-id 10.0.0.1 ! Specifies the OSPF router ID
Router(config-router)# network 10.0.0.0 0.0.0.255 area 0 ! Advertises Data VLAN subnet in
backbone area
Router(config-router)# network 10.0.1.0 0.0.0.255 area 0 ! Advertises Voice VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.0 0.0.0.31 area 0 ! Advertises Management VLAN
subnet in backbone area
Router(config-router)# network 10.0.2.64 0.0.0.15 area 0 ! Advertises DMZ VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.80 0.0.0.3 area 0 ! Advertises Tunnel subnet in
backbone area
Router(config-router)# network 10.0.2.88 0.0.0.3 area 0 ! Advertises WAAS subnet in
backbone area
Router(config-router)# network 192.168.0.0 0.0.0.3 area 0 ! Advertises primary WAN link
subnet in the backbone area
Router(config-router)# distribute-list 10 in ! Block all Internet routing updates
Router(config-router)# exit

```


Enterprise Routing with EIGRP

Enterprise networks are learned through the primary WAN interface.

```
Router(config)# router eigrp 1 ! Enables private network EIGRP routing process
Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface
Router(config-router)# no auto-summary ! Disable automatic route summarization
Router(config-router)# network 10.0.0.0 0.0.0.255 ! Advertises Data VLAN subnet
Router(config-router)# network 10.0.1.0 0.0.0.255 ! Advertises Voice VLAN subnet
Router(config-router)# network 10.0.2.0 0.0.0.31 ! Advertises Management VLAN subnet
Router(config-router)# network 10.0.2.64 0.0.0.15 ! Advertises DMZ VLAN subnet
Router(config-router)# network 10.0.2.80 0.0.0.3 ! Advertises Tunnel subnet
Router(config-router)# network 10.0.2.88 0.0.0.3 ! Advertises WAAS subnet
Router(config-router)# network 192.168.0.0 0.0.0.3 ! Advertises primary WAN link subnet
Router(config-router)# distribute-list 10 in ! Block all Internet routing updates
Router(config-router)# exit
```

Enterprise Routing with RIPv2

Enterprise networks are learned through the primary WAN interface.

```
Router(config)# router rip ! Enables private network RIP routing process
Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface
Router(config-router)# no auto-summary ! Disable automatic route summarization
Router(config-router)# version 2 ! Enable RIP version 2
Router(config-router)# network 10.0.0.0 ! Advertises all branch subnets
Router(config-router)# network 192.168.0.0 ! Advertises primary WAN link subnet
Router(config-router)# distribute-list 10 in ! Block all Internet routing updates
Router(config-router)# exit
```

Service Provider Routing with BGP

The BGP routing process is responsible for establishing the tunnel link by advertising the loopback network. In the default BGP configuration, the router learns public routes that are advertised by the ISP router. A large routing table would slow down the destination network lookup process. In general, network service providers should not advertise Internet routes to the branch network; an access list should be defined to exclude public routes.

```
Router(config)# access-list 20 permit 209.165.201.8 0.0.0.3 ! Permits Loopback network and
blocks all others

Router(config)# router bgp 1 ! Enables public and loopback network BGP routing process
Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface
Router(config-router)# neighbor 209.165.201.2 remote-as 65016! Neighbor router IP for
backup link that is in autonomous system 65016
Router(config-router)# network 209.165.201.0 mask 255.255.255.252 ! Advertises backup WAN
link subnet
Router(config-router)# network 209.165.201.8 mask 255.255.255.252 ! Advertises Loopback
subnet
Router(config-router)# distribute-list 20 in ! Block all routing updates except for
Loopback network
Router(config-router)# exit
```

Finally, static routes are defined to direct traffic to the public network. When the primary link is active, it is used as the default for all traffic. When the backup link is active, it is used as the default for all traffic.

```
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.0.2 ! Sets the primary WAN link as
default for all traffic
Router(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.2 ! Sets the backup WAN link as
default for all traffic
```

Active/Active Primary/Backup WAN Link with DMVPN Implementation

The primary function of the backup interface in the Basic Small Branch Network is to provide an alternate path in case the primary link fails. When the primary WAN interface is operational, the backup interface is in standby mode. However, for purposes of split tunneling, the interface can be kept in active state and provide access to the Internet, because it is a direct connection.

Again, there are two routing processes, one for enterprise traffic and another for public traffic. The routing is similar to the Active/Standby configuration for DMVPN because BGP likely selects the primary interface as the lowest-cost path to the central site network. It automatically switches over the tunnel interface to the backup link when the primary fails. To prevent situations where the Internet has a lower cost path to the central site, static routes with different costs are defined for the central site loopback interface. The only other difference in configuration is the default route configuration. Non-enterprise traffic must be directed out over the backup link.

Enterprise Routing with OSPF

Enterprise networks are learned through the tunnel interface.

```
Router(config)# router ospf 1 ! Enables private network OSPF routing process
Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface
Router(config-router)# router-id 10.0.0.1 ! Specifies the OSPF router ID
Router(config-router)# network 10.0.0.0 0.0.0.255 area 0 ! Advertises Data VLAN subnet in
backbone area
Router(config-router)# network 10.0.1.0 0.0.0.255 area 0 ! Advertises Voice VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.0 0.0.0.31 area 0 ! Advertises Management VLAN
subnet in backbone area
Router(config-router)# network 10.0.2.64 0.0.0.15 area 0 ! Advertises DMZ VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.80 0.0.0.3 area 0 ! Advertises Tunnel subnet in
backbone area
Router(config-router)# network 10.0.2.88 0.0.0.3 area 0 ! Advertises WAAS subnet in
backbone area
Router(config-router)# exit
```

Enterprise Routing with EIGRP

Enterprise networks are learned through the tunnel interface.

```
Router(config)# router eigrp 1 ! Enables private network EIGRP routing process
Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface
Router(config-router)# no auto-summary ! Disable automatic route summarization
Router(config-router)# network 10.0.0.0 0.0.0.255 ! Advertises Data VLAN subnet
Router(config-router)# network 10.0.1.0 0.0.0.255 ! Advertises Voice VLAN subnet
Router(config-router)# network 10.0.2.0 0.0.0.31 ! Advertises Management VLAN subnet
Router(config-router)# network 10.0.2.64 0.0.0.15 ! Advertises DMZ VLAN subnet
Router(config-router)# network 10.0.2.80 0.0.0.3 ! Advertises Tunnel subnet
Router(config-router)# network 10.0.2.88 0.0.0.3 ! Advertises WAAS subnet
Router(config-router)# exit
```

Enterprise Routing with RIPv2

Enterprise networks are learned through the Tunnel interface.

```
Router(config)# router rip ! Enables private network RIP routing process
Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface
Router(config-router)# no auto-summary ! Disable automatic route summarization
```

```
Router(config-router)# version 2 ! Enable RIP version 2
Router(config-router)# network 10.0.0.0 ! Advertises all branch subnets
Router(config-router)# exit
```

Service Provider Routing with BGP

The BGP routing process is responsible for establishing the tunnel link by advertising the loopback network. In the default BGP configuration, the router learns public routes that are advertised by the PE or ISP router. A large routing table would slow down the destination network lookup process. In general, network service providers should not advertise Internet routes to the branch network; an access list should be defined to exclude public routes.

```
Router(config)# access-list 20 permit 209.165.201.8 0.0.0.3 ! Permits Loopback network and blocks all others
```

```
Router(config)# router bgp 1 ! Enables public and loopback network BGP routing process
Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing advertisements on the LAN interface
Router(config-router)# neighbor 192.168.0.2 remote-as 65015 ! Neighbor router IP for primary link that is in autonomous system 65015
Router(config-router)# neighbor 209.165.201.2 remote-as 65016 ! Neighbor router IP for backup link that is in autonomous system 65016
Router(config-router)# network 192.168.0.0 mask 255.255.255.252 ! Advertises primary WAN link subnet
Router(config-router)# network 209.165.201.0 mask 255.255.255.252 ! Advertises backup WAN link subnet
Router(config-router)# network 209.165.201.8 mask 255.255.255.252 ! Advertises Loopback subnet
Router(config-router)# distribute-list 20 in ! Block all routing updates except for Loopback network
Router(config-router)# exit
```

Finally, static routes are defined to direct traffic to the public network. When the primary link is active, it is used as the default for all traffic. When the backup link is active, it is used as the default for all traffic. In addition, static routes ensure that the central site loopback interface is routed over the primary link when it is in an active state.

```
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.0.2 250 ! Sets the primary WAN link as default for all traffic with higher cost than the backup WAN link
Router(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.2 ! Sets the backup WAN link as default for all traffic with lower cost than the primary link
Router(config)# ip route 209.165.201.10 255.255.255.255 192.168.0.2 ! Sets the primary WAN link as the preferred interface for reaching the central site Loopback interface
Router(config)# ip route 209.165.201.10 255.255.255.255 209.165.201.2 250 ! Sets the backup WAN link as the preferred interface for reaching the central site Loopback interface
```

Active/Active Primary/Backup WAN Links with GETVPN on Primary Link and DMVPN on Backup Link Implementation

As in the Active/Standby configuration with DMVPN, this implementation differs from the Active/Standby GETVPN and DMVPN implementation in the assignment of static routes for loopback network and public traffic.

```
Router(config)# access-list 10 permit 172.16.0.0 0.0.255.255 ! Permits all Enterprise networks
```

Enterprise Routing with OSPF

Enterprise networks are learned through the primary WAN interface.

```
Router(config)# router ospf 1 ! Enables private network OSPF routing process
```

```

Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface
Router(config-router)# router-id 10.0.0.1 ! Specifies the OSPF router ID
Router(config-router)# network 10.0.0.0 0.0.0.255 area 0 ! Advertises Data VLAN subnet in
backbone area
Router(config-router)# network 10.0.1.0 0.0.0.255 area 0 ! Advertises Voice VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.0 0.0.0.31 area 0 ! Advertises Management VLAN
subnet in backbone area
Router(config-router)# network 10.0.2.64 0.0.0.15 area 0 ! Advertises DMZ VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.80 0.0.0.3 area 0 ! Advertises Tunnel subnet in
backbone area
Router(config-router)# network 10.0.2.88 0.0.0.3 area 0 ! Advertises WAAS subnet in
backbone area
Router(config-router)# network 192.168.0.0 0.0.0.3 area 0 ! Advertises primary WAN link
subnet in the backbone area
Router(config-router)# distribute-list 10 in ! Block all Internet routing updates
Router(config-router)# exit

```

Enterprise Routing with EIGRP

Enterprise networks are learned through the primary WAN interface.

```

Router(config)# router eigrp 1 ! Enables private network EIGRP routing process
Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface
Router(config-router)# no auto-summary ! Disable automatic route summarization
Router(config-router)# network 10.0.0.0 0.0.0.255 ! Advertises Data VLAN subnet
Router(config-router)# network 10.0.1.0 0.0.0.255 ! Advertises Voice VLAN subnet
Router(config-router)# network 10.0.2.0 0.0.0.31 ! Advertises Management VLAN subnet
Router(config-router)# network 10.0.2.64 0.0.0.15 ! Advertises DMZ VLAN subnet
Router(config-router)# network 10.0.2.80 0.0.0.3 ! Advertises Tunnel subnet
Router(config-router)# network 10.0.2.88 0.0.0.3 ! Advertises WAAS subnet
Router(config-router)# network 192.168.0.0 0.0.0.3 ! Advertises primary WAN link subnet
Router(config-router)# distribute-list 10 in ! Block all Internet routing updates
Router(config-router)# exit

```

Enterprise Routing with RIPv2

Enterprise networks are learned through the primary WAN interface.

```

Router(config)# router rip ! Enables private network RIP routing process
Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface
Router(config-router)# no auto-summary ! Disable automatic route summarization
Router(config-router)# version 2 ! Enable RIP version 2
Router(config-router)# network 10.0.0.0 ! Advertises all branch subnets
Router(config-router)# network 192.168.0.0 ! Advertises primary WAN link subnet
Router(config-router)# distribute-list 10 in ! Block all Internet routing updates
Router(config-router)# exit

```

Service Provider Routing with BGP

The BGP routing process is responsible for establishing the tunnel link by advertising the loopback network. In the default BGP configuration, the router learns public routes advertised by the ISP router. In general, network service providers should not advertise Internet routes to the branch network; an access list should be defined to exclude public routes.

```

Router(config)# access-list 20 permit 209.165.201.8 0.0.0.3 ! Permits Loopback network and
blocks all others

Router(config)# router bgp 1 ! Enables public and loopback network BGP routing process
Router(config-router)# passive interface FastEthernet 0/1 ! Disables routing
advertisements on the LAN interface

```

```

Router(config-router)# neighbor 209.165.201.2 remote-as 65016 ! Neighbor router IP for
backup link that is in autonomous system 65016
Router(config-router)# network 209.165.201.0 mask 255.255.255.252 ! Advertises backup WAN
link subnet
Router(config-router)# network 209.165.201.8 mask 255.255.255.252 ! Advertises Loopback
subnet
Router(config-router)# distribute-list 20 in ! Block all routing updates except for
Loopback network
Router(config-router)# exit

```

There is a possibility that the tunnel link has a lower cost to the central site than the primary WAN link. To prevent traffic from being sent over the tunnel link when the WAN link is available, the tunnel interface is defined as backup for the primary WAN interface.

```

Router(config)# interface Serial0/0/0 ! Enters multilink interface configuration mode
Router(config-if)# backup interface Tunnel1 ! Specifies backup interface
Router(config-if)# exit

```

Finally, static routes are defined to direct traffic to the public network. When the primary link is active, it is used as the default for all route traffic. When the backup link is active, it is used as the default route for all traffic.

```

Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.0.2 250 ! Sets the primary WAN link as
default for all traffic with higher cost than backup WAN link
Router(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.2 ! Sets the backup WAN link as
default for all traffic with lower cost than primary WAN link

```

Multicast Implementation

Previous sections have shown how to apply multicast on each interface.

```

Router(config)# ip multicast-routing ! Enables multicast routing

```

Multicast Verification

To verify your multicast configuration, enter the following command:

```

Router# show ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      S - State Refresh Capable
Neighbor      Interface      Uptime/Expires    Ver   DR
Address                               00:00:16/00:01:27 v2    Prio/Mode
192.168.0.1    Serial0/0/0
Router#

```

DHCP Implementation

Addresses were dynamically assigned for the data and voice VLAN devices. The DMZ server used static addressing. The DHCP server should be implemented on the router that is configured as active for voice traffic.

```

Router(config)# ip dhcp excluded-address 10.0.1.1 10.0.1.10 ! Specifies the addresses to
be excluded from DHCP
Router(config)# ip dhcp excluded-address 10.0.1.245 10.0.1.254 ! Specifies the addresses
to be excluded from DHCP
Router(config)# ip dhcp pool IP-PHONES ! Specifies DHCP pool for IP Phones
Router(dhcp-config)# network 10.0.1.0 255.255.255.0 ! Specifies the DHCP address range
Router(dhcp-config)# default-router 10.0.1.3 ! Specifies the default HSRP gateway
Router(dhcp-config)# option 150 ip 10.0.0.2 ! Specifies the default TFTP server

```

```

Router(dhcp-config)# lease 30 ! Sets the lease expiration to 1 month
Router(dhcp-config)# exit
Router(config)# ip dhcp excluded-address 10.0.0.1 10.0.0.30! Specifies the addresses to be
excluded from DHCP
Router(config)# ip dhcp excluded-address 10.0.0.245 10.0.0.254! Specifies the addresses to
be excluded from DHCP
Router(config)# ip dhcp pool PCS ! Specifies the DHCP pool for PCs
Router(dhcp-config)# network 10.0.0.0 255.255.255.0 ! Specifies the DHCP address range
Router(dhcp-config)# default-router 10.0.0.3 ! Specifies the default HSRP gateway
Router(dhcp-config)# exit
Router(config)# service dhcp ! Starts the DHCP server

```

DHCP Verification

To verify your DHCP configuration, enter the **show ip dhcp binding** command to display the IP address details leased by the DHCP server.

```

Router# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/          Lease expiration      Type
                   Hardware address/
                   User name
10.0.1.26           0100.1e4a.a8e5.e1   Infinite              Automatic
10.0.1.29           0100.5060.0387.20   Infinite              Automatic
Router#

```

NAT Implementation



Note

The following section applies only to the Cisco 1841 ISR configuration.

```

Router(config)# ip access-list standard NAT-BRANCH ! Defines extended ACL for translation
Router(config-ext-nacl)# permit 10.0.0.0 0.0.0.255
Router(config-ext-nacl)# exit
Router(config)# ip nat translation tcp-timeout 300 ! Specifies timeout value for TCP ports
Router(config)# ip nat inside source list NAT-BRANCH interface ATM0/2/IMA0.1 overload !
Enables NAT for traffic that matches the ACL (Inside local) and translates the source
address to specified interface address (Inside global) on the backup interface
Router(config)# interface FastEthernet0/1.1 ! Enters gigabit Ethernet configuration mode
Router(config-subif)# ip nat inside ! Specifies the interface as connected to inside
network
Router(config-subif)# exit
Router(config)# interface ATM0/2/IMA0.1 ! Enters backup interface configuration mode
Router(config-if)# ip nat outside ! Specifies the interface as connected to outside
network
Router(config-if)# exit

```

NAT Verification

To verify your NAT configuration, enter the following command:

```

Router# show ip nat translations
Pro Inside global      Inside local          Outside local          Outside global
tcp 22
10.0.0.15: 2140        10.0.0.15: 2140       201.165.201.1:2000    201.165.201.1:2000
Router#

```

Quality of Service Implementation

Quality of service (QoS) identifies business-critical traffic and ensures that appropriate bandwidth and network resources are allocated according to a classification scheme. QoS includes classification of different traffic types, marking specific fields in Layer 2 or Layer 3 headers, prioritizing the traffic based on the marked field, and dropping unwanted traffic.

Five-Class QoS was configured to match traffic, based on the NBAR protocol classification or using Layer 2 or Layer 3 header information. A different level of service is provided for the matched traffic. The QoS scheme also checks for any unwanted traffic and drops it if matches are found in the incoming traffic from the LAN. A parent policy-map is configured to shape the outgoing traffic to a specified rate (as per the service provider), and a child policy-map is applied to the shaping queue.

```
Router(config)# ip access-list extended ACL-FTP ! Defines extended ACL to identify traffic
from a local FTP server
Router(config-ext-nacl)# permit ip host 10.0.0.4 any
Router(config-ext-nacl)# exit ! Defines two extended access lists (101 and 102) to
classify PCs running enterprise applications
Router(config)# access-list 101 permit ip host 10.0.0.5 host 172.16.0.30
Router(config)# access-list 101 permit ip host 10.0.0.6 host 172.16.0.30
Router(config)# access-list 102 permit ip host 10.0.0.7 any
Router(config)# access-list 102 permit ip host 10.0.0.8 any
Router(config)# access-list 102 permit ip host 10.0.0.9 any
Router(config)# access-list 102 permit ip host 10.0.0.10 any
Router(config)# ip nbar port-map custom-02 udp 1434 ! Customizes NBAR protocol to match
UDP port 1434 used by the SQL Slammer and Sapphire worms
Router(config)# ip nbar port-map custom-03 tcp 5554 9996 ! Customizes NBAR protocol to
match TCP ports 5554 and 9996 used by the Sasser worm
Router(config)# ip nbar port-map custom-04 tcp 445 ! Customize NBAR protocol to match TCP
port 445 used by Microsoft SMB protocol for file sharing
Router(config)# class-map match-all SQL-SLAMMER ! Defines Class map for Sql-Slammer
traffic
Router(config-cmap)# match protocol custom-02 ! Matches traffic with port number in
custom-02
Router(config-cmap)# match packet length min 404 max 404 ! Matches traffic with packet
length 404 bytes
Router(config-cmap)# exit
Router(config)# class-map match-any WORMS ! Defines class map for unwanted traffic
Router(config-cmap)# match protocol http url "*.ida*" ! Matches HTTP traffic with the
specific string in the URL
Router(config-cmap)# match protocol http url "**cmd.exe*" ! Matches HTTP traffic with the
specific string in the URL
Router(config-cmap)# match protocol http url "**root.exe*" ! Matches HTTP traffic with the
specific string in the URL
Router(config-cmap)# match protocol http url "**readme.eml*" ! Matches HTTP traffic with
the specific string in the URL
Router(config-cmap)# match class-map SQL-SLAMMER ! Matches SQL-Slammer worm signature
Router(config-cmap)# match protocol custom-03 ! Matches Sasser worm signature
Router(config-cmap)# exit
Router(config)# class-map match-any VOICE ! Defines class map for Voice traffic
Router(config-cmap)# match ip dscp ef ! Matches traffic with DSCP set to EF
Router(config-cmap)# exit
Router(config)# class-map match-all INTERACTIVE-VIDEO ! Defines class map for interactive
video traffic
Router(config-cmap)# match ip dscp af41 af42 ! Matches traffic with DSCP set to AF41 or
AF42
Router(config-cmap)# exit
Router(config)# class-map match-all SCAVENGER ! Defines class map for Scavenger traffic
Router(config-cmap)# match ip dscp cs1 ! Matches traffic with DSCP set to cs1
Router(config-cmap)# exit
Router(config)# class-map match-any MISSION-CRITICAL ! Defines classmap for mission
critical traffic
```



```

Router(config-cmap)# match ip dscp cs3 ! Matches traffic with DSCP set to CS3
Router(config-cmap)# match ip dscp af31 ! Matches traffic with DSCP set to AF31
Router(config-cmap)# match access-group 101 ! Matches ip traffic in ACL 101
Router(config-cmap)# match ip dscp 25 ! Matches traffic with DSCP set to 25
Router(config-cmap)# match protocol http ! Matches HTTP traffic
Router(config-cmap)# exit
Router(config)# class-map match-any INTERNETWORK-CONTROL ! Defines class map for routing
control traffic
Router(config-cmap)# match ip dscp cs6 ! Matches traffic with DSCP set to CS6
Router(config-cmap)# exit
Router(config)# class-map match-any TRANSACTIONAL-DATA ! Defines class map for
transactional data traffic
Router(config-cmap)# match ip dscp af21 af22 ! Matches traffic with DSCP set to AF21 or
AF22
Router(config-cmap)# match access-group 102 ! Matches ip traffic in ACL
Router(config-cmap)# match protocol custom-04 ! Matches traffic with port number mentioned
in custom-04
Router(config-cmap)# exit
Router(config)# class-map match-any BULK-DATA ! Defines Class map for bulk traffic
Router(config-cmap)# match ip dscp af11 af12 ! Matches traffic with DSCP set to AF11 or
AF12
Router(config-cmap)# match protocol ftp ! Matches FTP traffic
Router(config-cmap)# match access-group name ACL-FTP ! Matches ip traffic in ACL-FTP ACL
Router(config-cmap)# exit

Router(config)# policy-map FIVE-CLASS-V3PN-EDGE ! Defines child policy map
Router(config-pmap)# class VOICE ! Matches traffic classified by VOICE class-map
Router(config-pmap-c)# priority % 18 ! Specifies guaranteed bandwidth of 14% of interface
bandwidth
Router(config-pmap-c)# class INTERACTIVE-VIDEO ! Matches traffic classified by
INTERACTIVE-VIDEO class-map
Router(config-pmap-c)# priority % 10 ! Specifies guaranteed bandwidth of 6% of interface
bandwidth
Router(config-pmap-c)# class MISSION-CRITICAL ! Matches traffic classified
byMISSION-CRITICAL class-map
Router(config-pmap-c)# bandwidth % 25 ! Specifies a minimum bandwidth of 25% of interface
bandwidth
Router(config-pmap-c)# random-detect ! Specifies to drop TCP packet randomly to avoid tail
drop
Router(config-pmap-c)# class INTERNETWORK-CONTROL ! Matches traffic classified by
INTERNETWORK-CONTROL class-map
Router(config-pmap-c)# bandwidth % 3 ! Specifies a minimum bandwidth of 3% of interface
bandwidth
Router(config-pmap-c)# class TRANSACTIONAL-DATA ! Matches traffic classified by
TRANSACTIONAL-DATA class-map
Router(config-pmap-c)# bandwidth % 12 ! Specifies a minimum bandwidth of 18% of interface
bandwidth
Router(config-pmap-c)# random-detect ! Specifies to drop TCP packet randomly to avoid tail
drop
Router(config-pmap-c)# class BULK-DATA ! Matches traffic classified by BULK-DATA class map
Router(config-pmap-c)# bandwidth % 5 ! Specifies a minimum bandwidth of 5% of interface
bandwidth
Router(config-pmap-c)# class SCAVENGER ! Matches traffic classified by SCAVENGER class map
Router(config-pmap-c)# bandwidth % 2 ! Specifies a minimum bandwidth of 2% of interface
bandwidth
Router(config-pmap-c)# class class-default ! Defines default class
Router(config-pmap-c)# bandwidth % 25 ! Specifies a minimum bandwidth of 25% of interface
bandwidth
Router(config-pmap-c)# random-detect ! Specifies to drop TCP packet randomly to avoid tail
drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit

```


After creating the following two policy maps, apply them on WAN interfaces as described in the DS-3, DS-1, and Fast Ethernet interface configuration section.

```
Router(config)# policy-map FIVE-CLASS-V3PN-EDGE-SHAPE ! Defines parent policy map for
Primary interface
Router(config-pmap)# class class-default ! Matches all traffic
Router(config-pmap-c)# shape average 6912000 ! Outgoing traffic was shaped at a rate of
6.9 Mbps
Router(config-pmap-c)# service-policy FIVE-CLASS-V3PN-EDGE ! Attaches traffic policy to
shaping queue.
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map FIVE-CLASS-V3PN-EDGE-BACKUP ! Defines parent policy map for
Backup interface
Router(config-pmap)# class class-default ! Matches all traffic
Router(config-pmap-c)# shape average 4608000 ! Outgoing traffic was shaped at a rate of
4.6 Mbps
Router(config-pmap-c)# service-policy FIVE-CLASS-V3PN-EDGE ! Attaches traffic policy to
shaping queue.
Router(config-pmap-c)# exit
Router(config)# map-class frame-relay FR-SHAPING ! Defines a map-class for Frame Relay
traffic shaping
Router(config-map-class)# frame-relay cir 24000000 ! Sets average rate to 24 Mbps
Router(config-map-class)# frame-relay bc 120000 ! Sets committed burst size to 120 Kb
Router(config-map-class)# frame-relay mincir 24000000 ! Sets the minimum guaranteed rate
it should drop in case of congestion to 24 Mbps
Router(config-map-class)# frame-relay adaptive-shaping becn ! Enables to adjust the
shaping rate in response to backward congestion notification
Router(config-map-class)# service-policy output FIVE-CLASS-V3PN-EDGE-SHAPE ! Attaches
traffic policy to Frame Relay shaping queue.
Router(config-map-class)# exit
Router(config)# policy-map INPUT-POLICY ! Defines Policy map for LAN interface
Router(config-pmap)# class WORMS ! Matches HTTP traffic with Virus
Router(config-pmap-c)# drop ! Drop the traffic
Router(config-pmap-c)# class class-default ! Matches all traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)#
```

Quality of Service Verification

To verify your QoS configuration, enter the **show policy-map interface** command to display the QoS policy and related traffic counters on each interface.

```
Router# show policy-map interface
FastEthernet0/1.1

Service-policy input: INPUT-POLICY

Class-map: WORMS (match-any)
  9 packets, 594 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: protocol http url "*.ida*"
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol http url "*cmd.exe*"
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol http url "*root.exe*"
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol http url "*readme.eml*"
    0 packets, 0 bytes
```

```

        30 second rate 0 bps
    Match: class-map match-all SQL-SLAMMER
        0 packets, 0 bytes
        30 second rate 0 bps
    Match: protocol custom-02
    Match: packet length min 404 max 404
    Match: protocol custom-03
        9 packets, 594 bytes
        30 second rate 0 bps
    drop

Class-map: class-default (match-any)
  103593411 packets, 6980776240 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: any
  QoS Set
    dscp cos
    Packets marked 103593416
FastEthernet0/1.2

```

Service-policy input: INPUT-POLICY

```

Class-map: WORMS (match-any)
  0 packets, 0 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: protocol http url "*.ida*"
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol http url "*cmd.exe*"
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol http url "*root.exe*"
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol http url "*readme.eml*"
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: class-map match-all SQL-SLAMMER
    0 packets, 0 bytes
    30 second rate 0 bps
    Match: protocol custom-02
    Match: packet length min 404 max 404
  Match: protocol custom-03
    0 packets, 0 bytes
    30 second rate 0 bps
  drop

Class-map: class-default (match-any)
  3350613 packets, 212885188 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: any
  QoS Set
    dscp cos
    Packets marked 3350613
FastEthernet0/1.3

```

Service-policy input: INPUT-POLICY

```

Class-map: WORMS (match-any)
  0 packets, 0 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: protocol http url "*.ida*"
    0 packets, 0 bytes
    30 second rate 0 bps

```

```

Match: protocol http url "*cmd.exe*"
      0 packets, 0 bytes
      30 second rate 0 bps
Match: protocol http url "*root.exe*"
      0 packets, 0 bytes
      30 second rate 0 bps
Match: protocol http url "*readme.eml*"
      0 packets, 0 bytes
      30 second rate 0 bps
Match: class-map match-all SQL-SLAMMER
      0 packets, 0 bytes
      30 second rate 0 bps
Match: protocol custom-02
Match: packet length min 404 max 404
Match: protocol custom-03
      0 packets, 0 bytes
      30 second rate 0 bps
drop

Class-map: class-default (match-any)
      3266743 packets, 201900728 bytes
      30 second offered rate 0 bps, drop rate 0 bps
Match: any
QoS Set
  dscp cos
    Packets marked 3266743
FastEthernet0/0/0

```

Service-policy output: FIVE-CLASS-V3PN-EDGE-SHAPE

```

Class-map: class-default (match-any)
      86921887 packets, 11420188514 bytes
      30 second offered rate 1000 bps, drop rate 0 bps
Match: any
Traffic Shaping
      Target/Average      Byte      Sustain      Excess      Interval      Increment
      Rate                Limit      bits/int    bits/int    (ms)          (bytes)
      6912000/6912000      43200     172800      172800      25            21600

Adapt Queue      Packets      Bytes      Packets      Bytes      Shaping
Active Depth     Delayed      Delayed     Active
-      0      85141012    2709383642  0      0      no

```

Service-policy : FIVE-CLASS-V3PN-EDGE

```

Class-map: VOICE (match-any)
      1781 packets, 206488 bytes
      30 second offered rate 0 bps, drop rate 0 bps
Match: ip dscp ef (46)
      0 packets, 0 bytes
      30 second rate 0 bps
Queueing
  Strict Priority
  Output Queue: Conversation 136
  Bandwidth 14 ( %)
  Bandwidth 967 (kbps) Burst 24175 (Bytes)
  (pkts matched/bytes matched) 0/0
  (total drops/bytes drops) 0/0

Class-map: INTERACTIVE-VIDEO (match-all)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
Match: ip dscp af41 (34) af42 (36)
Queueing

```

```

Strict Priority
Output Queue: Conversation 136
Bandwidth 6 ( %)
Bandwidth 414 (kbps) Burst 10350 (Bytes)
(pkts matched/bytes matched) 0/0
(total drops/bytes drops) 0/0

Class-map: MISSION-CRITICAL (match-any)
  1181375 packets, 148873894 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: ip dscp cs3 (24)
    1181375 packets, 148873894 bytes
    30 second rate 0 bps
  Match: ip dscp af31 (26)
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: access-group 101
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: ip dscp 25
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol http
    0 packets, 0 bytes
    30 second rate 0 bps
Queueing
  Output Queue: Conversation 137
  Bandwidth 25 ( %)
  Bandwidth 1728 (kbps)
  (pkts matched/bytes matched) 0/0
(depth/total drops/no-buffer drops) 0/0/0
  exponential weight: 9
  mean queue depth: 0

```

class	Transmitted pkts/bytes	Random drop pkts/bytes	Tail drop pkts/bytes	Minimum thresh	Maximum thresh	Mark prob
0	0/0	0/0	0/0	20	40	1/10
1	0/0	0/0	0/0	22	40	1/10
2	0/0	0/0	0/0	24	40	1/10
3	1181305/148866418	0/0	0/0	26	40	1/10
4	0/0	0/0	0/0	28	40	1/10
5	0/0	0/0	0/0	30	40	1/10
6	0/0	0/0	0/0	32	40	1/10
7	0/0	0/0	0/0	34	40	1/10
rsvp	0/0	0/0	0/0	36	40	1/10

```

Class-map: INTERNETWORK-CONTROL (match-any)
  1245619 packets, 176240010 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: ip dscp cs6 (48)
    1245619 packets, 176240010 bytes
    30 second rate 0 bps
Queueing
  Output Queue: Conversation 138
  Bandwidth 3 ( %)
  Bandwidth 207 (kbps)Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
(depth/total drops/no-buffer drops) 0/0/0

Class-map: TRANSACTIONAL-DATA (match-any)
  8833287 packets, 1254893912 bytes
  30 second offered rate 1000 bps, drop rate 0 bps
  Match: ip dscp af21 (18) af22 (20)

```

```

8833286 packets, 1254893912 bytes
30 second rate 1000 bps
Match: access-group 102
0 packets, 0 bytes
30 second rate 0 bps
Match: protocol custom-04
0 packets, 0 bytes
30 second rate 0 bps
Queueing
Output Queue: Conversation 139
Bandwidth 18 ( %)
Bandwidth 1244 (kbps)
(pkts matched/bytes matched) 0/0
(depth/total drops/no-buffer drops) 0/0/0
exponential weight: 9
mean queue depth: 0

```

class	Transmitted pkts/bytes	Random drop pkts/bytes	Tail drop pkts/bytes	Minimum thresh	Maximum thresh	Mark prob
0	0/0	0/0	0/0	20	40	1/10
1	0/0	0/0	0/0	22	40	1/10
2	8833254/1254889504	0/0	0/0	24	40	1/10
3	0/0	0/0	0/0	26	40	1/10
4	0/0	0/0	0/0	28	40	1/10
5	0/0	0/0	0/0	30	40	1/10
6	0/0	0/0	0/0	32	40	1/10
7	0/0	0/0	0/0	34	40	1/10
rsvp	0/0	0/0	0/0	36	40	1/10

```

Class-map: BULK-DATA (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: ip dscp af11 (10) af12 (12)
0 packets, 0 bytes
30 second rate 0 bps
Match: protocol ftp
0 packets, 0 bytes
30 second rate 0 bps
Match: access-group name aclftp
0 packets, 0 bytes
30 second rate 0 bps
Queueing
Output Queue: Conversation 140
Bandwidth 5 ( %)
Bandwidth 345 (kbps)Max Threshold 64 (packets)
(pkts matched/bytes matched) 0/0
(depth/total drops/no-buffer drops) 0/0/0

```

```

Class-map: SCAVENGER (match-all)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: ip dscp cs1 (8)
Queueing
Output Queue: Conversation 141
Bandwidth 2 ( %)
Bandwidth 138 (kbps)Max Threshold 64 (packets)
(pkts matched/bytes matched) 0/0
(depth/total drops/no-buffer drops) 0/0/0

```

```

Class-map: class-default (match-any)
75659826 packets, 9839974210 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any

```

```

Queueing
  Output Queue: Conversation 142
  Bandwidth 25 ( %)
  Bandwidth 1728 (kbps)
  (pkts matched/bytes matched) 0/0
(depth/total drops/no-buffer drops) 0/0/0
  exponential weight: 9
  mean queue depth: 0

class      Transmitted      Random drop      Tail drop      Minimum Maximum      Mark
          pkts/bytes      pkts/bytes      pkts/bytes      thresh  thresh  prob
0 73879122/9719111088      0/0              0/0              20      40  1/10
1          0/0              0/0              0/0              22      40  1/10
2          18/14796          0/0              0/0              24      40  1/10
3          0/0              0/0              0/0              26      40  1/10
4          0/0              0/0              0/0              28      40  1/10
5          0/0              0/0              0/0              30      40  1/10
6          0/0              0/0              0/0              32      40  1/10
7          0/0              0/0              0/0              34      40  1/10
rsvp       0/0              0/0              0/0              36      40  1/10

Virtual-Template10

Service-policy output: FIVE-CLASS-V3PN-EDGE-BACKUP

Service policy content is displayed for cloned interfaces only such as vaccess and
sessions

```

Security Services Implementation

- [Infrastructure Protection Implementation, page 136](#)
- [Access Control Implementation, page 143](#)
- [Secure Connectivity Implementation, page 143](#)
- [Threat Defense Detection and Mitigation Implementation, page 150](#)

Infrastructure Protection Implementation

- [Securing Unused Ports, page 136](#)
- [Turning Off Unused Services, page 137](#)
- [Routing Protocol Security, page 141](#)
- [Additional Services Measures, page 142](#)

Securing Unused Ports

The following is an example of securing an unused port. The example applies to the access layer switch.

```

Switch(config)# interface g1/0/4 ! Enters configuration mode for the specified port
Switch(config-if)# switchport mode access !Assign the port to access mode
Switch(config-if)# switchport access vlan 333 ! Assign the unused port to Black Hole VLAN
Switch(config-if)# exit

```

Turning Off Unused Services

To improve the overall security of the network, the Cisco IOS devices must be secured from infrastructure attack. As a security best practice, disable any unused services because these unused services are only rarely used for legitimate purposes and can be used to launch a denial of service (DoS) attack. The following example disables the unused services.

```
Router(config)# no service pad ! Disable PAD service
Router(config)# no service udp-small-servers ! Disable UDP small server
Router(config)# no service tcp-small-servers ! Disable TCP small server
Router(config)# no ip bootp server ! Disable BOOTP server
Router(config)# no cdp run ! Disable Cisco Discover Protocol service
Router(config)# no ip source-route ! Disable source routing
Router(config)# no ip classless ! Disable forwarding of packets for unrecognized subnets
Router(config)# no ip http server ! Disable HTTP server
Router(config)# no ip http secure-server ! Disable HTTPS server
Router(config)# no ip domain-lookup ! Disable DNS server
Router(config) # interface Serial0/0/0 ! Enters interface configuration mode
Router(config-if)# no cdp enable ! Disable Cisco discovery protocol on the interface
Router(config-if)# no ip redirects ! Disable ICMP redirect message
Router(config-if)# no ip proxy-arp ! Disable Proxy ARP
Router(config-if)# no ip unreachable ! Disable ICMP unreachable error message
Router(config-if)# no ip directed-broadcast ! Disable directed broadcasts
Router(config-if)# no ip mask-reply ! Disable ICMP mask reply messages
```

The unused services can also be disabled by running Cisco AutoSecure.

```
Router# auto secure
    --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***
```

AutoSecure will modify the configuration of your device. All configuration changes will be shown. For a detailed explanation of how the configuration changes enhance security and any possible side effects, please refer to Cisco.com for AutoSecure documentation.

At any prompt you may enter '?' for help.

Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

```
Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: 3
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	NVRAM	up	up
FastEthernet0/1.1	10.0.0.1	YES	NVRAM	up	up
FastEthernet0/1.2	10.0.1.1	YES	NVRAM	up	up
FastEthernet0/1.3	10.0.2.65	YES	NVRAM	up	up
FastEthernet0/1.4	10.0.2.1	YES	NVRAM	up	up
Serial0/1/0	unassigned	YES	NVRAM	up	up
ATM0/1/0	unassigned	YES	NVRAM	standby mode	down
ATM0/2/0.1	209.165.201.1	YES	NVRAM	standby mode	down
In1/0	10.0.2.85	YES	NVRAM	up	up
Virtual-Access1	unassigned	YES	unset	up	up
Virtual-Access2	unassigned	YES	unset	down	down
Virtual-Template10	209.165.201.1	YES	TFTP	down	down

```

Loopback0          209.165.201.9    YES NVRAM  up          up
Tunnell            10.0.2.81      YES NVRAM  up          up
Enter the interface name that is facing the internet: Serial0/0/0
Enter the interface name that is facing the internet: ATM0/1/0
Enter the interface name that is facing the internet: Loopback0
Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Is SNMP used to manage the router? [yes/no]: no
Disabling SNMP

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
  This system is the property of So-&-So-Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.

Enter the security banner {Put the banner between
k and k, where k is any character}:
k Unauthorised access to this device is prohibited k
Enable secret is either not configured or
  is the same as enable password
Enter the new enable secret:
Confirm the enable secret :
Enter the new enable password:
Confirm the enable password:
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 5

Maximum Login failures with the device: 5

Maximum time period for crossing the failed login attempts: 5

Configure SSH server? [yes]: yes
Enter hostname: Branch

```


Enter the domain-name: **example.com**

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

```
no ip redirects
no ip proxy-arp
no ip unreachable
no ip directed-broadcast
no ip mask-reply
```

Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected
to internet

Configure CBAC Firewall feature? [yes/no]: **no**
Tcp intercept feature is used prevent tcp syn attack
on the servers in the network. Create autosec_tcp_intercept_list
to form the list of servers to which the tcp traffic is to
be observed

Enable tcp intercept feature? [yes/no]: **no**

This is the configuration generated:

```
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
no snmp-server
banner motd ^C Unauthorised access to this device is prohibited ^C
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$2gLN$RpNwkFyfJdCjXkMDxY3PI1
enable password 7 011F07065802150C2E
aaa new-model
aaa authentication login local_auth local
line con 0
  login authentication local_auth
  exec-timeout 5 0
  transport output telnet
line aux 0
  login authentication local_auth
  exec-timeout 10 0
  transport output telnet
```

```

line vty 0 4
  login authentication local_auth
  transport input telnet
line tty 1
  login authentication local_auth
  exec-timeout 15 0
line tty 66
  login authentication local_auth
  exec-timeout 15 0
line tty 130
  login authentication local_auth
  exec-timeout 15 0
login block-for 5 attempts 5 within 5
ip domain-name example.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
  transport input ssh telnet
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/0
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
  no mop enabled
interface FastEthernet0/1
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
  no mop enabled
interface FastEthernet0/1.1
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
interface FastEthernet0/1.2
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
interface FastEthernet0/1.3
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
interface Serial0/0/0

```

```

no ip redirects
no ip proxy-arp
no ip unreachable
no ip directed-broadcast
no ip mask-reply
interface ATM0/1/0
no ip redirects
no ip proxy-arp
no ip unreachable
no ip directed-broadcast
no ip mask-reply
interface ATM0/1/0.1
no ip redirects
no ip proxy-arp
no ip unreachable
no ip directed-broadcast
no ip mask-reply
ip cef
access-list 100 permit udp any any eq bootpc
interface ATM0/1/0.1
ip verify unicast source reachable-via rx allow-default 100
!
end

```

Apply this configuration to running-config? [yes]: **yes**

Applying the config generated to running-config
The name for the keys will be: Router.example.com

```

percent The key modulus size is 1024 bits
percent Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```

```

Router#
092165: Sep 23 03:03:32.096 PDT: percentAUTOSEC-1-MODIFIED: AutoSecure configuration has
been Modified on this device
Router#

```

Routing Protocol Security

Apply an authentication mechanism to all the WAN interfaces.

OSPF

```

Router(config)# interface Tunnel 1 ! Enters tunnel interface configuration mode
Router(config-line)# ip ospf authentication message-digest ! Enables MD5 routing protocol
authentication
Router(config-line)# ip ospf message-digest-key 100 md5 c1$k0$ys ! Sets key and password
for MD5
Router(config)# exit
Router(config)# interface Serial0/0/0 ! Enters serial interface configuration mode
Router(config-line)# ip ospf authentication message-digest ! Enables MD5 routing protocol
authentication
Router(config-line)# ip ospf message-digest-key 100 md5 c1$k0$ys ! Sets key and password
for MD5
Router(config)# exit

```

EIGRP

```

Router(config)# key chain EIGRP-KEY ! Creates chain of keys
Router(config-keychain)# key 1 ! Creates a key
Router(config-keychain-key)# key-string c1$k0SyS ! Sets the key value
Router(config-keychain-key)# exit
Router(config-keychain)# exit

Router(config)# interface Tunnel 1 ! Enters tunnel interface configuration mode
Router(config-line)# ip authentication mode eigrp 100 md5 ! Enables MD5 routing protocol
authentication
Router(config-line)# ip authentication key-chain eigrp 100 EIGRP-KEY ! Sets key and
password for MD5
Router(config)# exit
Router(config)# interface Serial0/0/0 ! Enters serial interface configuration mode
Router(config-line)# ip authentication mode eigrp 100 md5 ! Enables MD5 routing protocol
authentication
Router(config-line)# ip authentication key-chain eigrp 100 EIGRP-KEY ! Sets key and
password for MD5
Router(config)# exit

```

RIPv2

```

Router(config)# key chain RIP-KEY ! Creates chain of keys
Router(config-keychain)# key 1 ! Creates a key
Router(config-keychain-key)# key-string c1$k0SyS ! Sets the key value
Router(config-keychain-key)# exit
Router(config-keychain)# exit

Router(config)# interface Tunnel 1 ! Enters tunnel interface configuration mode
Router(config-line)# ip rip authentication mode md5 ! Enables MD5 routing protocol
authentication
Router(config-line)# ip rip authentication key-chain RIP-KEY ! Sets key and password for
MD5
Router(config)# exit
Router(config)# interface Serial0/0/0 ! Enters serial interface configuration mode
Router(config-line)# ip rip authentication mode md5 ! Enables MD5 routing protocol
authentication
Router(config-line)# ip rip authentication key-chain RIP-KEY ! Sets key and password for
MD5
Router(config)# exit

```

Additional Services Measures

```

Router(config)# line vty 0 4 ! Specifies VTY line specific parameters
Router(config-line)# transport input ssh ! Allows only SSH connection
Router(config)# exit
Router(config)# ip http secure-server ! Enables HTTPS service
Router(config)# ip http authentication aaa login-authentication default ! Specifies to use
AAA database for HTTP login

```

Verification of Additional Services Measures

To verify your additional services configuration, enter the following command.

```

Router# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3

```

Access Control Implementation

Authentication, Authorization, and Accounting (AAA) is an architectural framework for consistently configuring a set of independent security functions. It provides a modular way of performing authentication, authorization, and accounting using a protocol such as RADIUS or TACACS.

In the branch architecture, AAA is the primary method for access control, using RADIUS as the protocol for communication between network devices and the AAA server.

```
Router(config)# aaa new-model ! Enables Authentication, Authorization and Accounting
services
Router(config)# aaa group server radius AAA-BRANCH ! Specifies the RADIUS server group
Router(config-sg-radius)# server 172.16.0.80 auth-port 1645 acct-port 1646 ! Specifies the
RADIUS server ip address
Router(config-sg-radius)# aaa authentication login default group radius local ! Specifies
default login authentication to use RADIUS server database
Router(config-sg-radius)# aaa authentication login VPN-AUTH-LIST group radius local !
Specifies SSL VPN login authentication to use RADIUS server database
Router(config)# aaa session-id common ! Specifies the use of the same session identifier
for all invocations of accounting services
Router(config)# radius-server key BRANCH-KEY ! Specifies RADIUS server key
```

Password Management

```
Router(config)# security passwords min-length 8 ! Sets minimum length of passwords to 8
characters
Router(config)# service password-encryption ! Enables Cisco IOS to encrypt all password in
configuration file
Router(config)# enable password level 7 C1$k0SyS ! Enables configuration password with
privilege level 7
Router(config)# enable secret level 5 C1$k0SyS ! Enables configuration password stored
with MD5 encryption with privilege level 5
Router(config)# security authentication failure rate 10 log ! Allows up to 10 unsuccessful
login attempts with a syslog entry for attempts that exceed the threshold
Router(config)# username admin password C1$k0SyS ! Sets login password
```

```
Switch-Access(config)# service password-encryption ! Enables Cisco IOS to encrypt all
password in configuration file
Switch-Access(config)# enable secret level 5 C1$k0SyS ! Enables configuration password
stored with MD5 encryption with privilege level 5
```

Secure Connectivity Implementation

- [GETVPN Key Server, page 144](#)
- [DMVPN Implementation, page 145](#)
- [SSL VPN Implementation, page 147](#)

Group Encrypted Transport Virtual Private Networks (GETVPN) eliminates the need for tunnels across the WAN. By removing the need for point-to-point tunnels, meshed networks can scale better while maintaining network-intelligence features that are critical to voice and video quality, such as QoS, routing, and multicast. GETVPN offers a new standards-based IPsec security model that is based on the concept of “trusted” group members. Trusted member routers use a common security methodology that is independent of any point-to-point IPsec tunnel relationship.

GET-based networks can be used in a variety of WAN environments, including IP and Multiprotocol Label Switching (MPLS). MPLS VPNs that use this encryption technology are highly scalable, manageable, and cost-effective, and they meet government-mandated encryption requirements. The flexible nature of GET allows security-conscious enterprises either to manage their own network security over a service provider WAN service or to offload encryption services to their providers. GET simplifies securing large Layer 2 or MPLS networks that require partial or full-mesh connectivity.

In the Basic Small Branch Foundation, GETVPN encryption was used on the primary WAN link.

```
Router(config)# crypto isakmp policy 1 ! Identifies the policy to create and enters isakmp
configuration mode
Router(config-isakmp)# encryption 3des ! Specifies the 3-DES encryption algorithm
Router(config-isakmp)# authentication pre-share ! Specifies authentication with preshared
keys
Router(config-isakmp)# hash md5 ! Specifies hash algorithm as MD5
Router(config-isakmp)# group 2 ! Specifies the 1024-bit Diffie-Hellman group
Router(config-isakmp)# lifetime 28800 ! Specifies the lifetime of IKE security association
Router(config-isakmp)# crypto isakmp key VPN-KEY address 209.165.201.10 ! Specifies static
key for the ISAKMP negotiation with peer device using remote peer Loopback address
Router(config)# crypto isakmp keepalive 30 ! Enables keepalives between peers with
specified interval
Router(config)# crypto gdoi group GET-GROUP ! Enters GDOI group configuration mode.
Router(config-gdoi-group)# identity number 1357924680 ! Sets GDOI group number
Router(config-gdoi-group)# server address ipv4 209.165.201.10 ! Specifies GDOI key server
address
Router(config-gdoi-group)# crypto map VPN-MAP local-address Loopback0 ! Specifies the
interface to be used by the crypto map for the IPSEC traffic
Router(config)# crypto map VPN-MAP 1 gdoi ! Enters crypto map configuration mode and
creates or modifies a crypto map entry.
Router(config-crypto-map)# set group GET-GROUP ! Associates the GDOI group to the crypto
map.
Router(config-crypto-map)# qos pre-classify ! Enables QoS on VPN tunnel interface
Router(config-crypto-map)# exit
```

Apply the *VPN-MAP* on all WAN interfaces and subinterfaces.

```
Router(config-fr-dlci)# crypto map VPN-MAP
```

or

```
Router(config-if)# crypto map VPN-MAP
```

GETVPN Key Server

The key server was configured at the central location.

```
KEY-SERVER(config)# crypto isakmp policy 1 ! Defines an IKE policy
KEY-SERVER(config-isakmp)# encryption 3des ! Specifies 3-DES encryption algorithm
KEY-SERVER(config-isakmp)# authentication pre-share ! Specifies authentication with
preshared keys
KEY-SERVER(config-isakmp)# group 2 ! Specifies the 1024-bit Diffie-Hellman group
KEY-SERVER(config-isakmp)# lifetime 28800 ! Specifies the lifetime of IKE security
association
KEY-SERVER(config)# crypto ipsec transform-set GET-GROUP esp-aes 256 esp-sha-hmac
! Defines a IPsec transform set with ESP encapsulation and AES 256 bit encryption
KEY-SERVER(cfg-crypto-trans)# crypto ipsec profile GET-VPN ! Defines a profile and enters
IPSEC configuration mode
KEY-SERVER(ipsec-profile)# set security-association lifetime seconds 86400 ! Specifies
security association lifetime
KEY-SERVER(ipsec-profile)# set transform-set GET-GROUP ! Specifies which transform sets
can be used with the crypto map entry.
KEY-SERVER(ipsec-profile)# crypto gdoi group GET-GROUP ! Identifies a GDOI group and
enters GDOI group configuration mode
```

```

KEY-SERVER(config-gdoi-group)# identity number 1357924680 ! Sets GDOI group number
KEY-SERVER(config-gdoi-group)# server local ! Specified GDOI key server as local and
enters its configuration
KEY-SERVER(gdoi-local-server)# rekey address ipv4 REKEY-ADDRESS ! Defines destination
information for rekey messages as defined in the REKEY-ADDRESS ACL
KEY-SERVER(gdoi-local-server)# rekey lifetime seconds 300 ! Limits the number of seconds
that any one encryption key should be used
KEY-SERVER(gdoi-local-server)# rekey retransmit 10 number 2 ! Specifies the number of
times the rekey message is retransmitted
KEY-SERVER(gdoi-local-server)# rekey authentication mypubkey rsa REKEY-RSA ! Specifies the
keys to be used for a rekey to GDOI group members
KEY-SERVER(gdoi-local-server)# sa ipsec 1 ! Specifies the IPsec SA policy information to
be used for a GDOI group and enters GDOI SA IPsec configuration mode
KEY-SERVER(gdoi-sa-ipsec)# profile GET-VPN ! Defines the IPsec SA policy for a GDOI group
KEY-SERVER(gdoi-sa-ipsec)# match address ipv4 SA-ACL ! Specifies an IP extended access
list for a GDOI registration.
KEY-SERVER(gdoi-sa-ipsec)# replay counter window-size 64 ! Specifies the window-size for
the replay counter
KEY-SERVER(config)# ip access-list extended REKEY-ADDRESS ! Defines an extended
access-list and enters acl mode
KEY-SERVER(config-ext-nacl)# permit udp host host 209.165.201.10 eq 848 host 239.1.100.1
eq 248 ! Permits packets from a specific address to register with the Key-Server at its
multicast address
KEY-SERVER(config)# ip access-list extended SA-ACL ! Defines an extended access-list and
enters acl mode
KEY-SERVER(config-ext-nacl)# permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.255.255
! Permits traffic from branch subnets to central site subnets and vice versa
KEY-SERVER(config-ext-nacl)# permit ip 10.0.1.0 0.0.0.255 172.16.0.0 0.0.255.255
KEY-SERVER(config-ext-nacl)# permit ip 10.0.2.0 0.0.0.31 172.16.0.0 0.0.255.255
KEY-SERVER(config-ext-nacl)# permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255
KEY-SERVER(config-ext-nacl)# permit ip 172.16.0.0 0.0.255.255 10.0.1.0 0.0.0.255
KEY-SERVER(config-ext-nacl)# permit ip 172.16.0.0 0.0.255.255 10.0.2.0 0.0.0.31

```

DMVPN Implementation

Dynamic Multipoint Virtual Private Network (DMVPN) is useful for building scalable IPsec VPNs. DMVPN uses a centralized architecture to provide easier implementation and management for deployment that requires granular access control for diverse users including teleworkers and mobile workers.

Cisco DMVPN allows branch locations to communicate directly with each other over the public WAN or Internet, such as when using Voice over IP (VoIP) between two branch offices, but does not require a permanent VPN connection between sites. In the Basic Small Branch Network, DMVPN was tested on both the primary WAN link and the backup WAN link depending on whether the tunnel interface is active.

```

Router(config)# crypto isakmp policy 1 ! Defines IKE policy
Router(config-isakmp)# encr 3des ! Specifies the encryption mode as 3DES
Router(config-isakmp)# hash md5 ! Specifies hash algorithm as MD5
Router(config-isakmp)# authentication pre-share ! Specifies authentication with pre-shared
keys
Router(config-isakmp)# group 2 ! Specifies 1024-bit Diffie-Hellman group
Router(config-isakmp)# lifetime 28800 ! Specifies the lifetime of IKE security association
Router(config)# crypto isakmp key VPN-KEY address 209.165.201.10 ! Defines the preshared
key to be used for authentication
Router(config)# crypto isakmp keepalive 30 ! Enables keepalives between peers with
specified interval
Router(config)# crypto ipsec transform-set DM-GROUP esp-3des esp-md5-hmac
! Specifies IPsec transform set with ESP encapsulation and AES 256 bit encryption
Router(cfg-crypto-trans)# exit
Router(config)# crypto ipsec profile DM-VPN ! Defines IPsec Profile

```

```

Router(ipsec-profile)# set security-association lifetime seconds 86400 ! Specifies the
amount of time for SA to be active
Router(ipsec-profile)# set transform-set DM-GROUP ! Specifies the IPSec transform set for
encrypting traffic
Router(ipsec-profile)# exit
Router(config)# interface Tunnel 1 ! Enters tunnel interface configuration mode
Router(config-if)# ip address 10.0.2.81 255.255.255.252 ! Specifies tunnel interface IP
address
Router(config-if)# ip mtu 1416 ! Sets the MTU size to 1416 bytes
Router(config-if)# tunnel source Loopback 0 ! Specifies the source address to be used for
tunnel packets
Router(config-if)# ip nbar protocol-discovery ! Enables NBAR protocol discovery
Router(config-if)# ip flow ingress ! Enables Netflow accounting on incoming traffic
Router(config-if)# ip flow egress ! Enables Netflow accounting on outgoing traffic
Router(config-if)# ip nhrp authentication KEY-BR ! Specifies authentication string
Router(config-if)# ip nhrp map 172.16.0.10 209.165.201.10 ! Specifies central site Tunnel
address to Tunnel source mapping
Router(config-if)# ip nhrp map multicast 209.165.201.10 ! Enables Broadcast/Multicast
support for Tunnel source address
Router(config-if)# ip nhrp network-id 100000 ! Specifies network identifier for this NBMA
network
Router(config-if)# ip nhrp holdtime 300 ! Specifies the time the NHRP address will be
advertised as valid
Router(config-if)# ip nhrp nhs 172.16.0.10 ! Specifies next hop server as the Tunnel
interface
Router(config-if)# load-interval 30 ! Specifies the interval for computing load statistics
Router(config-if)# qos pre-classify ! Enables QoS on VPN tunnel interface
Router(config-if)# tunnel mode gre multipoint ! Specifies the tunnel mode as multipoint
GRE
Router(config-if)# tunnel key 100000 ! Specifies the tunnel key
Router(config-if)# tunnel protection ipsec profile DM-VPN ! Associate IPSec profile with
tunnel interface

```

Apply the following command on the Tunnel interface after defining VPN security zone.

```

Router(config-if)# zone-member security VPN ! Adds this interface to firewall zone called
VPN

```

DMVPN Verification

To verify your DMVPN configuration, enter the following commands:

```

Router# show crypto ipsec sa

interface: Tunnel1
  Crypto map tag: Tunnel1-head-0, local addr 209.165.201.9

  protected vrf: (none)
  local ident (addr/mask/prot/port): (209.165.201.9/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (209.165.201.10/255.255.255.255/47/0)
  current_peer 209.165.201.10 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 13642629, #pkts encrypt: 13642629, #pkts digest: 13642629
    #pkts decaps: 16147685, #pkts decrypt: 16147685, #pkts verify: 16147685
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 5522

  local crypto endpt.: 209.165.201.9, remote crypto endpt.: 209.165.201.10
  path mtu 1514, ip mtu 1514, ip mtu idb Loopback0
  current outbound spi: 0x6523EA4E(1696852558)

inbound esp sas:

```



```

spi: 0x2DD40AB3(768871091)
  transform: esp-3des esp-md5-hmac ,
  in use settings ={Tunnel, }
  conn id: 11125, flow_id: AIM-VPN/SSL-3:125, crypto map: Tunnell1-head-0
  sa timing: remaining key lifetime (k/sec): (4435361/55246)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
  spi: 0x6523EA4E(1696852558)
  transform: esp-3des esp-md5-hmac ,
  in use settings ={Tunnel, }
  conn id: 11126, flow_id: AIM-VPN/SSL-3:126, crypto map: Tunnell1-head-0
  sa timing: remaining key lifetime (k/sec): (4419430/55246)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcg sas:

```

```

Router# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
209.165.201.9      209.165.201.10  QM_IDLE          21440      0 ACTIVE

```

SSL VPN Implementation

Secure Socket Layer Virtual Private Network (SSL VPN) is used to connect remote office users directly to the branch and provide them access to resources in the DMZ VLAN. They are also able to place calls using PC soft phones.

```

Router(config)#crypto pki trustpoint SSLVPN ! Defines a PKI certificate trust point
Router(ca-trustpoint)# enrollment selfsigned ! Specifies this router as self-signed root
certificate authority
Router(ca-trustpoint)# serial-number ! Specifies that the routers serial number should be
in the certificate request
Router(ca-trustpoint)# revocation-check none ! Disable certificate status check
Router(ca-trustpoint)# rsakeypair CERT-KEY ! Specified RSA key pair
Router(ca-trustpoint)# exit
Router(config)#crypto pki certificate chain SSLVPN ! Enters certificate configuration mode
Router(config-cert-chain)# certificate self-signed 01 ! Manually enters self-signed
certificate

```

There can be only one self-signed PKI certificate per router. AutoSecure, described in the Infrastructure Protection Implementation section, creates a self-signed certificate for the router while configuring SSH access. If AutoSecure was enabled on the router, then the next step is not necessary. However, if AutoSecure was not enabled, the above command will request a self-signed PKI certificate. To learn about creating self-signed certificates, visit:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6657/white_paper_c07-372106.html

Enter the certificate in hexadecimal representation....

```

Router(config-pubkey)# 308201F2 3082019C A0030201 02020101 300D0609 2A864886 F70D0101
04050030
Router(config-pubkey)# 42314030 12060355 0405130B 46545831 31343841 36433030 2A06092A
864886F7
Router(config-pubkey)# 0D010902 161D4B69 76752D33 3832352D 42722D31 2E796F75 72646F6D
61696E2E
Router(config-pubkey)# 636F6D30 1E170D30 38303231 33323232 3131345A 170D3230 30313031
30303030
Router(config-pubkey)# 30305A30 42314030 12060355 0405130B 46545831 31343841 36433030
2A06092A
Router(config-pubkey)# 864886F7 0D010902 161D4B69 76752D33 3832352D 42722D31 2E796F75
72646F6D
Router(config-pubkey)# 61696E2E 636F6D30 5C300D06 092A8648 86F70D01 01010500 034B0030
48024100
Router(config-pubkey)# A699E60C 8EBCF9EA B3142412 FDEE1150 BF25E671 0FBF5E3E 323ABFEB
FFC9790D
Router(config-pubkey)# D5D10D76 7639A04A DDD45FA3 F82E6EFE 2F14C046 E05C0488 433CD054
44E97E61
Router(config-pubkey)# 02030100 01A37D30 7B300F06 03551D13 0101FF04 05300301 01FF3028
0603551D
Router(config-pubkey)# 11042130 1F821D4B 6976752D 33383235 2D42722D 312E796F 7572646F
6D61696E
Router(config-pubkey)# 2E636F6D 301F0603 551D2304 18301680 14E94478 E4EE44CD 8277D8E9
B12EBC6D
Router(config-pubkey)# ABC165DC D8301D06 03551D0E 04160414 E94478E4 EE44CD82 77D8E9B1
2EBC6D
Router(config-pubkey)# C165DCD8 300D0609 2A864886 F70D0101 04050003 41001086 6FDC6C2E
735E9A99
Router(config-pubkey)# 764F874B 03F10F55 31414E96 A0901C04 D172E2B1 AF990499 5404A7B8
94543832
Router(config-pubkey)# 5B5C0389 C543C76F 49E70F1D CCBCEC3 A9B346CF D561
Router(config-pubkey)# quit
Router(config-cert-chain)# exit

```

Add the following rules to the firewall access control list (ACL) definitions.

```

Router(config)# ip access-list extended publicSelfInRule20Acl ! Enters Public to IOS zone
ACL definition
Router(config-ext-nacl)# permit tcp any host 209.165.201.15 ! Public address of SSLVPN
gateway 1
Router(config-ext-nacl)# permit tcp any host 209.165.201.17 ! Public address of SSLVPN
gateway 2
Router(config-ext-nacl)# permit tcp any host 209.165.201.20 eq www ! Public address of DMZ
server
Router(config-ext-nacl)# permit tcp any host 209.165.201.21 eq www ! Public address of DMZ
server
Router(config-ext-nacl)# permit tcp any host 209.165.201.22 eq www ! Public address of DMZ
server
Router(config-ext-nacl)# permit ip 192.168.0.0 0.0.0.252 ! Central site network
Router(config-ext-nacl)# permit ip 209.165.201.0 0.0.0.252 ! Central site network
Router(config-ext-nacl)# exit
Router(config)#

```

```

Router(config)# ip access-list extended publicDMZInRule20Acl ! Enters Public to DMZ zone
ACL definition
Router(config-ext-nacl)# permit tcp any host 209.165.201.16 ! Public address of SSLVPN
gateway 1
Router(config-ext-nacl)# permit tcp any host 209.165.201.17 ! Public address of SSLVPN
gateway 2
Router(config-ext-nacl)# permit tcp any host 209.165.201.20 eq www ! Public address of DMZ
server
Router(config-ext-nacl)# permit tcp any host 209.165.201.21 eq www ! Public address of DMZ
server

```

```

Router(config-ext-nacl)# permit tcp any host 209.165.201.22 eq www ! Public address of DMZ
server
Router(config-ext-nacl)# exit

Router(config)# ip local pool SSLVPN-Address-Pool 10.0.0.70 10.0.2.79 ! Defines pool of
addresses for VPN clients

Router(config)# webvpn gateway SSLVPN-GATEWAY-1 ! Enters webvpn gateway configuration mode
Router(config-webvpn-gateway)# ip address 209.165.201.15 port 443 ! Assigns public IP for
the gateway
Router(config-webvpn-gateway)# http-redirect port 80 ! Configures HTTP traffic to be
carried as HTTPS
Router(config-webvpn-gateway)# ssl trustpoint SSLVPN ! Assigns PKI certificate trust point
Router(config-webvpn-gateway)# inservice ! Starts the SSLVPN process
Router(config-webvpn-gateway)# exit

Router(config)# webvpn gateway SSLVPN-GATEWAY-2
Router(config-webvpn-gateway)# ip address 209.165.201.17 port 443 ! Assigns public IP for
the gateway
Router(config-webvpn-gateway)# http-redirect port 80 ! Configures HTTP traffic to be
carried as HTTPS
Router(config-webvpn-gateway)# ssl trustpoint SSLVPN ! Assigns PKI certificate trust point
Router(config-webvpn-gateway)# inservice ! Starts the SSLVPN process
Router(config-webvpn-gateway)# exit

Router(config)# webvpn install svc flash:sslclient-win-1.1.4.176.pkg ! Installs Cisco
AnyConnect VPN package

Router(config-webvpn-context)# webvpn context SSLVPN-GW-WEB ! Enters webvpn context
configuration mode
Router(config-webvpn-context)# secondary-color white ! Configures login portal
Router(config-webvpn-context)# title-color #FF9900 ! Configures login portal
Router(config-webvpn-context)# text-color black ! Configures login portal
Router(config-webvpn-context)# ssl encryption rc4-md5 ! Configures RC4-MD5 SSL encryption
Router(config-webvpn-context)# ssl authenticate verify all ! Performs user authentication
Router(config-webvpn-context)# url-list "WEB-SERVERS" ! Configures list of URLs in DMZ
that the user can access
Router(config-webvpn-url)# heading "Web Servers" ! Configures display properties for web
servers
Router(config-webvpn-url)# url-text "Server1" url-value "http://10.0.2.65/index.html"
Router(config-webvpn-url)# url-text "Server2" url-value "http://10.0.2.66/index.html"
Router(config-webvpn-url)# url-text "Server3" url-value "http://10.0.2.67/index.html"

Router(config-webvpn-url)# policy group SSLVPN-POLICY-WEB ! Defines policy for DMZ web
servers
Router(config-webvpn-group)# url-list "WEB-SERVERS" ! Associates policy with URL list
Router(config-webvpn-group)# functions svc-enabled ! Enables use of tunnel mode
Router(config-webvpn-group)# mask-urls ! Obfuscates sensitive URLs
Router(config-webvpn-group)# svc address-pool "SSLVPN-Address-Pool" ! Assigns local
addresses
Router(config-webvpn-group)# svc keep-client-installed ! Maintains Cisco AnyConnect VPN
client software installations on the connecting PCs
Router(config-webvpn-group)# default-group-policy SSLVPN-POLICY-WEB ! Associates SSLVPN
context with this group policy
Router(config-webvpn-context)# aaa authentication list VPN-AUTH-LIST ! Configures AAA for
SSLVPN users
Router(config-webvpn-context)# gateway SSLVPN-GATEWAY-1 ! Assigns gateway to this SSLVPN
context
Router(config-webvpn-context)# inservice ! Starts the SSLVPN policy
Router(config-webvpn-context)# exit

```

The following example illustrates a second SSL VPN context.

```

Router(config-webvpn)# webvpn context SSLVPN-GW-APP ! Enters webvpn context configuration
mode
Router(config-webvpn-context)# ssl encryption rc4-md5 ! Configures RC4-MD5 SSL encryption
Router(config-webvpn-context)# ssl authenticate verify all ! Performs user authentication
Router(config-webvpn-context)# url-list "APP-SERVERS" ! Associates policy with URL list
Router(config-webvpn-url)# heading "Application Servers" ! Configures display properties
for application servers
Router(config-webvpn-url)# url-text "Server1" url-value "http://10.0.2.65/index.html"
Router(config-webvpn-url)# url-text "Server2" url-value "http://10.0.2.66/index.html"
Router(config-webvpn-url)# url-text "Server3" url-value "http://10.0.2.67/index.html"
Router(config-webvpn-url)# policy group SSLVPN-POLICY-APP
Router(config-webvpn-group)# url-list "APP-SERVERS" ! Associates policy with URL list
Router(config-webvpn-group)# default-group-policy SSLVPN-POLICY-APP ! Associates SSLVPN
context with this group policy
Router(config-webvpn-context)# aaa authentication list VPN-AUTH-LIST ! Configures AAA for
sslvpn users
Router(config-webvpn-context)# gateway SSLVPN-GATEWAY-2 ! Assigns gateway to this SSLVPN
context
Router(config-webvpn-context)# inservice ! Starts the SSLVPN policy
Router(config-webvpn-context)# exit
Router(config)#

```

Threat Defense Detection and Mitigation Implementation

- [Zone-based Policy Firewall Implementation, page 150](#)
- [Cisco IOS IPS Implementation, page 162](#)
- [Layer 2 Security, page 164](#)

Zone-based Policy Firewall Implementation

Zone-based Policy Firewall (ZPF) offers assignment of traffic into secure zones for multiple-interface routers. It changes the firewall configuration from interface-based classic Context-Based Access Control (CBAC) model to a more flexible zone-based configuration.

Interfaces are assigned to different zones, and inspection policies are applied to traffic moving between zones. As the inspection policies are zone based rather than interface based, different policies can be applied to traffic from and to the same interface.

There are four zones in the Basic Small Branch Network: Private (LAN), Public (WAN), VPN, and DMZ. Inspection policies were applied for the following zone pairs:

- Traffic originated from Private to Public
- Traffic originated from Private to DMZ
- Traffic originated from Public to Private
- Traffic originated from Public to DMZ
- Traffic originated from router to Private
- Traffic originated from Private to router
- Traffic originated from Private to VPN
- Traffic originated from VPN to Private

```

Router(config)# parameter-map type inspect publicPrivateOutParamMap ! Defines a
parameter-map for traffic from Public to Private zone
Router(config-profile)# max-incomplete low 6000 ! Specifies minimum number of half-open
session before IOS stops removing sessions

```

```

Router(config-profile)# max-incomplete high 10000 ! Specifies maximum number of half-open
session after which IOS starts removing sessions
Router(config-profile)# one-minute low 18000 ! Specifies minimum number of half-open
session in one minute before IOS stops removing sessions
Router(config-profile)# one-minute high 20000 ! Specifies maximum number of half-open
session in one minute after which IOS starts removing sessions
Router(config-profile)# udp idle-time 10 ! Specifies maximum length of time for which UDP
inspect information is maintained
Router(config-profile)# icmp idle-time 5 ! Specifies maximum length of time for which ICMP
inspect information is maintained
Router(config-profile)# tcp max-incomplete host 7000 block-time 0 ! Specifies the maximum
number of half-open TCP sessions to the same destination before IOS starts removing
sessions
Router(config-profile)# exit
Router(config)# ip access-list extended privatePublicOutRule10Acl ! Defines ACL for
traffic from IOS to Private zone
Router(config-ext-nacl)# permit 10.0.0.0 0.0.0.255 ! Permits all data VLAN traffic
Router(config-ext-nacl)# permit 10.0.1.0 0.0.0.255 ! Permits all voice VLAN traffic
Router(config-ext-nacl)# exit

Router(config)# ip access-list extended publicPrivateOutRule10Acl ! Defines ACL for
traffic from Public zone to Private zone
Router(config-ext-nacl)# permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255 ! Permits
central site traffic to Data VLAN
Router(config-ext-nacl)# permit ip 172.16.0.0 0.0.255.255 10.0.1.0 0.0.0.255 ! Permits
central site traffic to Voice VLAN
Router(config-ext-nacl)# permit ip 172.16.0.0 0.0.255.255 10.0.2.0 0.0.0.31 ! Permits
central site traffic to Management VLAN
Router(config-ext-nacl)# permit ip host 239.1.100.1 any ! Permits key server multicast
address
Router(config-ext-nacl)# permit ip host 209.165.201.10 any ! Permits key server
Router(config-ext-nacl)# exit
Router(config)# class-map type inspect match-all FROM-SELF-CMAP ! Defines class map for
traffic from IOS to Private zone
Router(config-cmap)# match access-group name selfPrivateRule10 ! Matches traffic in
specified ACL
Router(config-cmap)# exit
Router(config)# class-map type inspect match-any TO-SELF-CMAP ! Defines class map for
traffic from Private
Router(config-cmap)# match access-group name selfPrivateRule10 ! Matches traffic in
specified ACL
Router(config-cmap)# exit
Router(config)# class-map type inspect match-any privateDMZOutRule10Protocols ! Defines
class map for protocols from Private to DMZ zone
Router(config-cmap)# match protocol http ! Matches HTTP traffic
Router(config-cmap)# match protocol https ! Matches Secure HTTP traffic
Router(config-cmap)# match protocol dns ! Matches DNS traffic
Router(config-cmap)# match protocol ssh ! Matches Secure Shell traffic
Router(config-cmap)# exit
Router(config)# class-map type inspect match-any privatePublicOutRule10 ! Defines class
map for traffic from Private to Public zone
Router(config-cmap)# match access-group name publicPrivateOutRule10Acl ! Matches traffic
in specified ACL
Router(config-cmap)# exit
Router(config)# class-map type inspect match-any SELF-SERVICE-CMAP ! Defines class map for
protocols originating from IOS
Router(config-cmap)# match protocol tcp ! Matches TCP traffic
Router(config-cmap)# match protocol udp ! Matches UDP traffic
Router(config-cmap)# match protocol icmp ! Matches ICMP traffic
Router(config-cmap)# match protocol h323 ! Matches H323 traffic
Router(config-cmap)# match protocol echo ! Matches ICMP echo traffic
Router(config-cmap)# exit
Router(config-cmap)# class-map type inspect match-any publicDMZOutRule10Protocols
! Defines class map for protocols from Public to DMZ zone

```

```

Router(config-cmap)# match protocol http ! Matches HTTP traffic
Router(config-cmap)# match protocol https ! Matches Secure HTTP traffic
Router(config-cmap)# match protocol dns ! Matches DNS traffic
Router(config-cmap)# match protocol ssh ! Matches Secure Shell traffic
Router(config-cmap)# exit

Router(config)# policy-map type inspect publicDMZOutFwPolicy ! Defines inspect policy for
Public to DMZ zone
Router(config-pmap)# class type inspect publicDMZOutRule10Protocols ! Matches traffic
classified by specified class-map
Router(config-pmap-c)# inspect publicPrivateOutParamMap ! Enables packet inspection
according to the Public to Private zone parameter map definition
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop log ! Drops the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect privateSelfOutFwPolicy ! Defines inspect policy
for Private to IOS zone
Router(config-pmap)# class type inspect SELF-SERVICE-MAP ! Matches traffic classified to
IOS parameter map definition
Router(config-pmap-c)# pass ! Passes the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop ! Drops the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect selfPrivateOutFwPolicy ! Defines inspect policy
for IOS to Private zone
Router(config-pmap)# class type inspect SELF-SERVICE-MAP ! Matches from IOS parameter map
definition
Router(config-pmap-c)# pass ! Passes the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop ! Drops the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect privatePublicOutFwPolicy ! Defines inspect policy
for Private to Public zone
Router(config-pmap)# class type inspect privatePublicOutRule10 ! Matches traffic
classified by specified class-map
Router(config-pmap-c)# inspect publicPrivateOutParamMap ! Enables packet inspection
according to the Public to Private zone parameter map definition percent. No specific
protocol configured in class privatePublicOutRule10 for inspection. All protocols will be
inspected
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop ! Drops the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect privateDMZOutFwPolicy ! Defines inspect policy for
Private to DMZ zone
Router(config-pmap)# class type inspect privateDMZOutRule10Protocols ! Matches traffic
classified by specified class-map
Router(config-pmap-c)# inspect publicPrivateOutParamMap ! Enables packet inspection
according to the Public to Private zone parameter map definition
Router(config-pmap-c)# exit
Router(config-pmap-c)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop log ! Drops the traffic
Router(config-pmap-c)# exit

```

```
Router(config-pmap)# exit
```

```
Router(config)# zone security Public ! Define Security Zone named Public
Router(config-sec-zone)# description Public Internet Connection
Router(config-sec-zone)# exit
```

Apply *Public* security zone on the WAN interface or subinterface as described in WAN interface configuration sections.

```
Router(config)# zone security Private ! Define Security Zone named Private
Router(config-sec-zone)# description Customer Private Network
Router(config-sec-zone)# exit
Router(config)# zone security DMZ ! Define Security Zone named DMZ
Router(config-sec-zone)# description Customer DMZ Network
Router(config-sec-zone)# exit
```

Apply *Private* and *DMZ* security zones on the LAN interface or subinterface as described in VLAN interface configuration sections.

```
Router(config)# zone-pair security privatePublicOut source Private destination Public !
Define zone-pair for Private to Public traffic
Router(config-sec-zone-pair)# description Outbound Firewall Policy from Private to Public
Router(config-sec-zone-pair)# service-policy type inspect privatePublicOutFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit
```

```
Router(config)# zone-pair security publicDMZOut source Public destination DMZ ! Define
zone-pair for Public to DMZ traffic
Router(config-sec-zone-pair)# description Outbound Firewall Policy from Public to DMZ
Router(config-sec-zone-pair)# service-policy type inspect publicDMZOutFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit
```

```
Router(config)# zone-pair security privateDMZOut source Private destination DMZ ! Define
zone-pair for Private to DMZ traffic
Router(config-sec-zone-pair)# description Outbound Firewall Policy from Private to DMZ
```

```
Router(config-sec-zone-pair)# service-policy type inspect privateDMZOutFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit
```

```
Router(config)# zone-pair security privateSelf source Private destination self ! Define
zone-pair for Private to IOS traffic
Router(config-sec-zone-pair)# service-policy type inspect privateSelfOutFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit
```

```
Router(config)# zone-pair security selfPrivate source self destination Private ! Define
zone-pair for IOS to Private traffic
Router(config-sec-zone-pair)# service-policy type inspect selfPrivateOutFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit
```

Zone-based Policy Firewall Verification

To verify your zone-based firewall configuration, enter the following commands:

```
Router# show policy-map type inspect zone-pair
Zone-pair: publicPrivateOut

Service-policy inspect : publicPrivateOutFwPolicy

Class-map: publicPrivateOutRule10 (match-any)
  Match: access-group name publicPrivateOutRule10Acl
```

```

0 packets, 0 bytes
30 second rate 0 bps
Match: class-map match-any publicPrivateOutRule10Protocols
160728 packets, 5222722 bytes
30 second rate 0 bps
Match: protocol http
0 packets, 0 bytes
30 second rate 0 bps
Match: protocol https
23 packets, 1196 bytes
30 second rate 0 bps
Match: protocol dns
0 packets, 0 bytes
30 second rate 0 bps
Match: protocol ssh
0 packets, 0 bytes
30 second rate 0 bps
Match: protocol icmp
81876 packets, 2947880 bytes
30 second rate 0 bps
Match: protocol ftp
0 packets, 0 bytes
30 second rate 0 bps
Match: protocol tcp
78575 packets, 2251480 bytes
30 second rate 0 bps
Match: protocol udp
246 packets, 22166 bytes
30 second rate 0 bps
Match: protocol bgp
0 packets, 0 bytes
30 second rate 0 bps
Match: protocol smtp
0 packets, 0 bytes
30 second rate 0 bps
Inspect
Packet inspection statistics [process switch:fast switch]
tcp packets: [77702:1346327]
udp packets: [2:0]
icmp packets: [18235:7]

Session creations since subsystem startup or last reset 95910
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [14:101:1]
Last session created 08:55:49
Last statistic reset never
Last session creation rate 0
Maxever session creation rate 15120
Last half-open session total 0

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
Zone-pair: publicDMZOut

Service-policy inspect : publicDMZOutFwPolicy

Class-map: publicDMZOutRule10Protocols (match-any)
Match: protocol http
0 packets, 0 bytes
30 second rate 0 bps
Match: protocol https
0 packets, 0 bytes

```



```

    30 second rate 0 bps
Match: protocol dns
    0 packets, 0 bytes
    30 second rate 0 bps
Match: protocol ssh
    0 packets, 0 bytes
    30 second rate 0 bps
Match: protocol bgp
    0 packets, 0 bytes
    30 second rate 0 bps
Match: protocol icmp
    0 packets, 0 bytes
    30 second rate 0 bps
Match: access-group name DMZPublicOutRuleAcl20
    0 packets, 0 bytes
    30 second rate 0 bps
Inspect
    Session creations since subsystem startup or last reset 0
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [0:0:0]
    Last session created never
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 0
    Last half-open session total 0

Class-map: class-default (match-any)
    Match: any
    Drop
        0 packets, 0 bytes
Zone-pair: privateDMZOut

Service-policy inspect : privateDMZOutFwPolicy

Class-map: privateDMZOutRule10Protocols (match-any)
    Match: protocol http
        0 packets, 0 bytes
        30 second rate 0 bps
    Match: protocol https
        0 packets, 0 bytes
        30 second rate 0 bps
    Match: protocol dns
        0 packets, 0 bytes
        30 second rate 0 bps
    Match: protocol ssh
        0 packets, 0 bytes
        30 second rate 0 bps
    Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 0
        Last half-open session total 0

Class-map: class-default (match-any)
    Match: any
    Drop
        0 packets, 0 bytes
Zone-pair: vpnPrivateIn

Service-policy inspect : vpnPrivateInFwPolicy

```

```

Class-map: vpnPrivateInRule10 (match-any)
  Match: access-group name vpnPrivateInRule10Acl
    4314 packets, 109136 bytes
    30 second rate 0 bps
  Inspect
    Packet inspection statistics [process switch:fast switch]
    tcp packets: [229:3495]
    udp packets: [10:6177032]
    icmp packets: [0:31]

    Session creations since subsystem startup or last reset 271
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [2:11:1]
    Last session created 5d08h
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 10
    Last half-open session total 0

Class-map: class-default (match-any)
  Match: any
  Drop
    0 packets, 0 bytes
Zone-pair: vpnPrivateOut

Service-policy inspect : vpnPrivateOutFwPolicy

Class-map: vpnPrivateOutRule10 (match-any)
  Match: access-group name vpnPrivateOutRule10Acl
    6356447 packets, 231662957 bytes
    30 second rate 0 bps
  Inspect
    Packet inspection statistics [process switch:fast switch]
    tcp packets: [9061:117338799]
    udp packets: [1761:2253]
    icmp packets: [0:6176836]
    ftp packets: [0:11]
    tftp packets: [160:6]
    tftp-data packets: [1600:1756]
    skinny packets: [2867:62498341]

    Session creations since subsystem startup or last reset 6356113
    Current session counts (estab/half-open/terminating) [5:0:0]
    Maxever session counts (estab/half-open/terminating) [193:22:97]
    Last session created 00:00:48
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 22400
    Last half-open session total 0

Class-map: class-default (match-any)
  Match: any
  Drop
    0 packets, 0 bytes
Zone-pair: publicSelfOut

Service-policy inspect : publicSelfOutFwPolicy

Class-map: publicSelfOutRule20 (match-any)
  Match: access-group name publicSelfOutRule20Acl
    255 packets, 39396 bytes
    30 second rate 0 bps
  Match: protocol tcp

```

```

17229 packets, 735614 bytes
30 second rate 0 bps
Match: protocol udp
89136 packets, 6774336 bytes
30 second rate 0 bps
Match: protocol icmp
5 packets, 400 bytes
30 second rate 0 bps
Inspect
Packet inspection statistics [process switch:fast switch]
tcp packets: [457182:0]
udp packets: [179870:0]
icmp packets: [43:0]

Session creations since subsystem startup or last reset 89587
Current session counts (estab/half-open/terminating) [1:0:0]
Maxever session counts (estab/half-open/terminating) [4:4:1]
Last session created 00:00:45
Last statistic reset never
Last session creation rate 1
Maxever session creation rate 6
Last half-open session total 0

Class-map: CRYPTO-CMAP (match-all)
Match: access-group 123
Pass
81354612 packets, 8078747532 bytes

Class-map: class-default (match-any)
Match: any
Drop (default action)
0 packets, 0 bytes
Zone-pair: publicSelfIn

Service-policy inspect : publicSelfInFwPolicy

Class-map: publicSelfInRule20 (match-any)
Match: access-group name publicSelfInRule20Acl
279 packets, 35460 bytes
30 second rate 0 bps
Match: protocol tcp
0 packets, 0 bytes
30 second rate 0 bps
Match: protocol udp
0 packets, 0 bytes
30 second rate 0 bps
Match: protocol icmp
0 packets, 0 bytes
30 second rate 0 bps
Inspect
Packet inspection statistics [process switch:fast switch]
udp packets: [919:0]
icmp packets: [111:0]

Session creations since subsystem startup or last reset 279
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [1:2:0]
Last session created 21:40:08
Last statistic reset never
Last session creation rate 0
Maxever session creation rate 74
Last half-open session total 0

Class-map: CRYPTO-CMAP (match-all)

```

```

Match: access-group 123
Pass
    0 packets, 0 bytes

Class-map: class-default (match-any)
Match: any
Drop (default action)
    0 packets, 0 bytes
Zone-pair: DMZPublicOut

Service-policy inspect : publicDMZOutFwPolicy

Class-map: publicDMZOutRule10Protocols (match-any)
Match: protocol http
    0 packets, 0 bytes
    30 second rate 0 bps
Match: protocol https
    0 packets, 0 bytes
    30 second rate 0 bps
Match: protocol dns
    0 packets, 0 bytes
    30 second rate 0 bps
Match: protocol ssh
    0 packets, 0 bytes
    30 second rate 0 bps
Match: protocol bgp
    0 packets, 0 bytes
    30 second rate 0 bps
Match: protocol icmp
    0 packets, 0 bytes
    30 second rate 0 bps
Match: access-group name DMZPublicOutRuleAcl20
    0 packets, 0 bytes
    30 second rate 0 bps
Inspect
    Session creations since subsystem startup or last reset 0
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [0:0:0]
    Last session created never
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 0
    Last half-open session total 0

Class-map: class-default (match-any)
Match: any
Drop
    0 packets, 0 bytes

Zone-pair: selfprivate

Service-policy inspect : selfFwPolicy

Class-map: SELF-CMAP (match-any)
Match: access-group name SELF-ACL
    24257448 packets, 1807595033 bytes
    30 second rate 1000 bps
Pass
    24257448 packets, 1807595033 bytes

Class-map: class-default (match-any)
Match: any
Drop
    0 packets, 0 bytes

```

```

Zone-pair: vpnself

Service-policy inspect : selfFwPolicy

Class-map: SELF-CMAP (match-any)
  Match: access-group name SELF-ACL
    545089 packets, 17426918 bytes
    30 second rate 0 bps
  Pass
    545089 packets, 17426918 bytes

Class-map: class-default (match-any)
  Match: any
  Drop
    0 packets, 0 bytes
Zone-pair: selfvpn

Service-policy inspect : selfFwPolicy

Class-map: SELF-CMAP (match-any)
  Match: access-group name SELF-ACL
    1088484 packets, 28319861 bytes
    30 second rate 0 bps
  Pass
    1088484 packets, 28319861 bytes

Class-map: class-default (match-any)
  Match: any
  Drop
    0 packets, 0 bytes
Router#

```

DMVPN uses Virtual Tunnel Interface (VTI) for IPsec VPN connectivity. When the DMVPN interface is assigned to a security zone, traffic routing to and from other interfaces in the router are subjected to zone-to-zone firewall policy.

If the DMVPN interface is assigned to the same security zone as another interface (for example, Fast Ethernet 0/0), traffic moving between hosts on the DMVPN and hosts connected to Fast Ethernet 0/0 will pass freely with no policy application.

In the Basic Small Branch Network, the tunnel interface is assigned to the VPN security zone. Additional inspection policies were applied.

```

Router(config)# ip access-list extended publicSelfInRule20Acl ! Defines ACL for Public to
IOS zone traffic
Router(config-ext-nacl)# permit udp any eq isakmp host 209.165.201.9 eq isakmp ! Matches
ISAKMP traffic
Router(config-ext-nacl)# exit

Router(config)# ip access-list extended publicSelfOutRule20Acl ! Defines ACL for IOS to
Public zone traffic
Router(config-ext-nacl)# permit udp host 22.0.14.253 eq isakmp any eq isakmp ! Matches
ISAKMP traffic
Router(config-ext-nacl)# permit ip 192.168.0.0 0.0.0.252 ! Central site network
Router(config-ext-nacl)# permit ip 209.165.201.0 0.0.0.252 ! Central site network
Router(config-ext-nacl)# exit

Router(config)# ip access-list extended vpnPrivateInRule10Acl ! Defines ACL for VPN to
Private zone traffic
Router(config-ext-nacl)# permit ip any any ! Matches all traffic
Router(config-ext-nacl)# exit

Router(config)# ip access-list extended vpnPrivateOutRule10Acl ! Defines ACL for Private
to VPN zone traffic

```

```

Router(config-ext-nacl)# permit ip any any ! Matches all traffic
Router(config-ext-nacl)# exit

Router(config)# ip access-list extended NON-TCP-ACL ! Defines ACL for WAAS GRE tunnel
Router(config-ext-nacl)# permit gre host 10.0.2.90 host 10.0.2.89
Router(config-ext-nacl)# exit

Router(config)# ip access-list extended DMZPublicOutRuleAcl20 ! Defines ACL for DMZ to
Public zone traffic
Router(config-ext-nacl)# permit tcp host 10.0.2.70 eq www any ! DMZ server
Router(config-ext-nacl)# permit tcp host 10.0.2.71 eq www any ! DMZ server
Router(config-ext-nacl)# permit tcp host 10.0.2.72 eq www any ! DMZ server

Router(config-ext-nacl)# exit

Router(config)# access-list 123 permit esp any any ! Matches IPSec ESP traffic
Router(config)# ip access-list extended SELF-ACL ! Defines ACL for IOS traffic
Router(config-ext-nacl)# permit tcp any any ! Matches TCP
Router(config-ext-nacl)# permit gre any any ! Matches GRE
Router(config-ext-nacl)# permit ip any any ! Matches IP
Router(config-ext-nacl)# exit

Router(config)# class-map type inspect match-any vpnPrivateInRule10 ! Defines class-map
for VPN to Private zone traffic
Router(config-cmap)# match access-group name vpnPrivateInRule10Acl ! Matches traffic
specified in ACL
Router(config-cmap)# exit

Router(config)# class-map type inspect match-all CRYPTO-MAP ! Defines class-map for
matching VPN traffic
Router(config-cmap)# match access-group 123 ! Matches traffic specified in ACL
Router(config-cmap)# exit

Router(config)# class-map type inspect match-any publicSelfInRule20 ! Defines class-map
for matching Public to IOS zone traffic
Router(config-cmap)# match access-group name publicSelfInRule20Acl ! Matches traffic
specified in ACL
Router(config-cmap)# match protocol tcp ! Matches TCP traffic
Router(config-cmap)# match protocol udp ! Matches UDP traffic
Router(config-cmap)# match protocol icmp ! Matches ICMP traffic
Router(config-cmap)# exit

Router(config)# class-map type inspect match-any vpnPrivateOutRule10 ! Defines class-map
for Private to VPN zone traffic
Router(config-cmap)# match access-group name vpnPrivateOutRule10Acl ! Matches traffic
specified in ACL
Router(config-cmap)# exit

Router(config)# class-map type inspect match-any publicSelfOutRule20 ! Defines class-map
for matching IOS to Public zone traffic
Router(config-cmap)# match access-group name publicSelfOutRule20Acl ! Matches traffic
specified in ACL
Router(config-cmap)# match protocol tcp ! Matches TCP traffic
Router(config-cmap)# match protocol udp ! Matches UDP traffic
Router(config-cmap)# match protocol icmp ! Matches ICMP traffic
Router(config-cmap)# exit

Router(config)# class-map type inspect match-any publicDMZOutRule10Protocols
! Defines class-map for matching DMZ to Public zone traffic
Router(config-cmap)# match protocol http ! Matches HTTP traffic
Router(config-cmap)# match protocol https ! Matches Secure HTTP traffic
Router(config-cmap)# match protocol dns ! Matches DNS traffic
Router(config-cmap)# match protocol ssh ! Matches Secure Shell traffic
Router(config-cmap)# match protocol bgp ! Matches BGP traffic

```

```

Router(config-cmap)# match protocol icmp ! Matches ICMP traffic
Router(config-cmap)# match access-group name DMZPublicOutRuleAcl20 ! Matches traffic
specified in ACL
Router(config-cmap)# exit

Router(config)# policy-map type inspect publicSelfInFwPolicy ! Defines inspect policy for
Public to IOS zone
Router(config-pmap)# class type inspect publicSelfInRule20 ! Matches traffic classified by
specified class-map
Router(config-pmap-c)# inspect ! Enables packet inspection
Router(config-pmap-c)# exit
Router(config-pmap)# class type inspect CRYPTO-CMAP ! Matches traffic classified by
specified class-map
Router(config-pmap-c)# pass ! Passes traffic
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop log ! Drops traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect publicDMZOutFwPolicy ! Defines policy for DMZ to
Public zone
Router(config-pmap)# class type inspect publicDMZOutRule10Protocols ! Matches
traffic classified by specified class-map
Router(config-pmap-c)# inspect publicPrivateOutParamMap ! Enables inspection for Public to
Private zone traffic
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop log ! Drops traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect vpnPrivateInFwPolicy ! Defines policy for VPN to
Private zone traffic
Router(config-pmap)# class type inspect vpnPrivateInRule10 ! Matches
traffic classified by specified class-map
Router(config-pmap-c)# inspect ! Enables packet inspection percent. No specific protocol
configured in class vpnPrivateInRule10 for inspection. All protocols will be inspected
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop log ! Drops traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect publicSelfOutFwPolicy ! Defines policy for IOS to
Public zone traffic
Router(config-pmap)# class type inspect publicSelfOutRule20 ! Matches traffic classified
by specified class-map
Router(config-pmap-c)# inspect ! Enables packet inspection
Router(config-pmap-c)# exit
Router(config-pmap)# class type inspect CRYPTO-CMAP ! Matches traffic classified by
specified class-map
Router(config-pmap-c)# pass ! Pass the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop log ! Drops the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect vpnPrivateOutFwPolicy ! Defines policy for Private
to VPN zone traffic
Router(config-pmap)# class type inspect vpnPrivateOutRule10 ! Matches traffic classified
by specified class-map
Router(config-pmap-c)# inspect ! Enables packet inspection
percentNo specific protocol configured in class vpnPrivateOutRule10 for inspection. All
protocols will be inspected

```

```

Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop log ! Drops traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# zone security VPN ! Define VPN Zone name
Router(config-sec-zone)# description customer VPN Network
Router(config-sec-zone)# exit

Router(config)# zone-pair security vpnPrivateIn source VPN destination Private ! Define
zone-pair for VPN to Private zone traffic
Router(config-sec-zone-pair)# service-policy type inspect vpnPrivateInFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security vpnPrivateOut source Private destination VPN ! Define
zone-pair for Private to VPN zone traffic
Router(config-sec-zone-pair)# service-policy type inspect vpnPrivateOutFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security publicSelfOut source self destination Public ! Define
zone-pair for IOS to Public zone traffic
Router(config-sec-zone-pair)# service-policy type inspect publicSelfOutFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security publicSelfIn source Public destination self ! Define
zone-pair for Public to IOS zone traffic
Router(config-sec-zone-pair)# service-policy type inspect publicSelfInFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security DMZPublicOut source DMZ destination Public ! Define
zone-pair to for DMZ to Public zone traffic
Router(config-sec-zone-pair)# service-policy type inspect publicDMZOutFwPolicy
Router(config-sec-zone-pair)# exit

Router(config)# interface Tunnel 1 ! Enters Tunnel interface configuration mode
Router(config-if)# zone-member security VPN ! Assign a zone to the interface
Router(config-if)# exit

```

Cisco IOS IPS Implementation

The Cisco IOS IPS acts as an inline intrusion detection sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When Cisco IOS IPS detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages or Security Device Event Exchange (SDEE).

In the Basic Small Branch Foundation, IPS inspection was enabled on the DATA VLAN in both directions. All types of traffic were inspected using advanced signature set stored in the flash memory.

```

Router# mkdir flash:ips5 ! Creates the folder in flash for saving the signature files
Router(config)# config t
Router(config)# ip ips config location flash:/ips5/ retries 1 ! Specifies the location to
save the signature file
Router(config)# ip ips deny-action ips-interface ! Changes the default behavior of the ACL
filters that are created for the deny actions.
Router(config)# ip ips notify SDEE ! Enables SDEE event notification on a router
Router(config)# ip ips name IPS-ADVSET ! Defines an IOS IPS rule

```



```

Router(config)# ip ips signature-category ! Allows the fine tuning of signature parameters
on the basis of signature category
Router (config-ips-category)# category all ! Specifies the signature category to be used
for multiple signature actions or conditions
Router(config-ips-category-action)# retired true ! Retires all the signatures in the "all"
category
Router(config-ips-category-action)# category ios_ips advanced ! Enables advanced signature
set
Router (config-ips-category-action)# retired false ! Enables the signatures in the IOS_IPS
category
Router(config-ips-category-action)# end
Router(config)# copy tftp://<ipaddr>/IOS-S341-CLI.pkg idconf ! Loads the signature package
(IOS-S341-CLI.pkg) to the specified location in ip ips config location

```

Cisco IOS IPS Verification

To verify your Cisco IOS IPS configuration, enter the following command:

```

Router# show ip ips statistics
Interfaces configured for ips 2
Session creations since subsystem startup or last reset 0
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [0:0:0]
Last session created never
Last statistic reset never
TCP reassembly statistics
    received 0 packets out-of-order; dropped 0
    peak memory usage 0 KB; current usage: 0 KB
    peak queue length 0

```

Access Control List Implementation

Access control list (ACL) configuration is a basic filtering process that can be used to control access network based on source or source/destination combination.

In Basic Small Branch Network, ACLs entries are used to block TFTP traffic between certain endpoints. This is only an illustrative example.

```

Router(config)# ip access-list extended BLOCK-TFTP ! Specifies an Extended named ACL
Router(config-ext-nacl)# deny udp 172.16.10.0 0.0.0.255 eq tftp 10.0.0.0 0.0.0.255 eq tftp
! Deny TFTP traffic from specific source to specific destination
Router(config-ext-nacl)# deny udp 172.16.20.0 0.0.0.255 eq tftp 10.0.0.0 0.0.0.255 eq tftp
Router(config-ext-nacl)# deny udp 172.16.30.0 0.0.0.255 eq tftp 10.0.0.0 0.0.0.255 eq tftp

```

uRPF Implementation

The uRPF feature is automatically implemented when using AutoSecure. For the sake of completeness, the full configuration is provided.

```

Router(config)# access-list 103 permit udp any any eq bootpc ! Specifies ACL that permits
bootpc traffic

```

Each WAN interface was configured to support uRPF filtering.

```

Router(config)# interface Serial0/0/0 ! Enters Multilink interface configuration mode
Router(config-if)# ip verify unicast source reachable-via rx allow-default 103 ! Enables
uRPF filtering
Router(config-if)# exit

```

```
Router(config)# interface ATM0/1/0.1 point-to-point ! Enters backup interface
configuration mode
Router(config-if)# ip verify unicast source reachable-via rx allow-default 103 ! Enables
uRPF filtering
Router(config-if)# exit
```

Layer 2 Security



Note

The following examples use a 24-port Catalyst 2960. Modify the port types and ranges accordingly if an 8-port Catalyst 2960 series switch is used.

- [Port Security Implementation, page 164](#)
- [Dynamic ARP Inspection Implementation, page 165](#)
- [IP Source Guard Implementation, page 165](#)
- [DHCP Snooping Implementation, page 166](#)
- [BPDU Guard Implementation, page 166](#)

Port Security Implementation

Following port security configuration was applied to the access layer switch.

```
Switch-Access(config)# interface range g1/0/2 - 28 ! Enters configuration for range of
Gigabit Ethernet
Switch-Access(config-if-range)# switchport port-security ! Enables port security in this
port
Switch-Access(config-if-range)# switchport port-security maximum 2 ! Specifies to allow
traffic from maximum 2 mac-address as source address
Switch-Access(config-if-range)# switchport port-security aging type inactivity ! Specifies
to age out the dynamically learned mac address if no traffic for specified period
Switch-Access(config-if-range)# switchport port-security aging time 2 ! Specifies to age
out the dynamically learned mac-address after 2 minutes
Switch-Access(config-if-range)# switchport port-security violation restrict ! Specifies
the port to drop packet from non secure mac address and send a trap
```

Port Security Verification

To verify your port security configuration, enter the following command:

```
Switch-Access# show port-security interface g1/0/2
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode                : Restrict
Aging Time                   : 2 mins
Aging Type                   : Inactivity
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 2
Total MAC Addresses          : 0
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 0
Last Source Address:Vlan     : 0000.0000.0000:0
Security Violation Count     : 0
Switch-Access#
```

Dynamic ARP Inspection Implementation

Following command demonstrates how to apply dynamic Address Resolution Protocol (ARP) inspection excluding specified hosts.

```
Switch-Access(config)# arp access-list STATIC-HOSTS ! Defines ARP access-list for hosts
that will be allowed to ARP packets
Switch-Access(config-arp-nacl)# permit ip host 10.0.0.5 mac any
Switch-Access(config-arp-nacl)# permit ip host 10.0.0.6 mac any
Switch-Access(config-arp-nacl)# permit ip host 10.0.0.7 mac any
Switch-Access(config-arp-nacl)# permit ip host 10.0.0.8 mac any
Switch-Access(config-arp-nacl)# permit ip host 10.0.0.9 mac any
Switch-Access(config-arp-nacl)# permit ip host 10.0.0.10 mac any
Switch-Access(config-arp-nacl)# exit
Switch-Access(config)# ip arp inspection vlan 301-302 ! Enables ARP inspection on
specified VLANs
Switch-Access(config)# ip arp inspection validate dst-mac ! Specifies to perform a check
destination-MAC and Target MAC to be same on ARP packet
Switch-Access(config)# ip arp inspection log-buffer entries 100 ! Enable the dynamic ARP
inspection log buffer to hold 100 entries
Switch-Access(config)# ip arp inspection log-buffer logs 1 interval 100 ! Enables every
log entry to generate a system message every 100 seconds
Switch-Access(config)# ip arp inspection filter STATIC-HOSTS vlan 301-303 ! Applies ARP
ACL to specified VLANs
Switch-Access(config)# errdisable recovery cause arp-inspection ! Enable error recovery
for Dynamic ARP inspection error-disabled state.
Switch-Access(config)# interface Port-Channel1 ! Enters EtherChannel configuration mode
Switch-Access(config-if)# ip arp inspection trust ! Disables ARP inspection
Switch-Access(config)# interface range g1/0/1 ! Enters gigabit Ethernet configuration mode
Switch-Access(config-if)# ip arp inspection trust ! Disables ARP inspection
```

Dynamic ARP Inspection Verification

To verify your dynamic ARP inspection configuration, enter the following command:

```
Switch-Access# show ip arp inspection vlan 301
```

```
Source Mac Validation      : Disabled
Destination Mac Validation : Enabled
IP Address Validation      : Disabled
```

Vlan	Configuration	Operation	ACL Match	Static ACL
301	Enabled	Active	static-host	No

Vlan	ACL Logging	DHCP Logging
301	Deny	Deny

```
Switch-Access#
```

IP Source Guard Implementation

The following source guard configuration was applied to both the distribution and access layer switches.

```
Switch-Access(config)# ip source binding 0030.94C2.9A40 vlan 303 10.0.2.65 interface
g1/0/49
! Specifies MAC to IP binding for statically assigned DMZ server address
Switch-Access(config)# ip source binding 0030.94C2.9A41 vlan 303 10.0.2.66 interface
g1/0/50
! Specifies MAC to IP binding for statically assigned DMZ server address
```

```
Switch-Access(config)# ip source binding 0030.94C2.9A42 vlan 303 10.0.2.67 interface
g1/0/51
! Specifies MAC to IP binding for statically assigned DMZ server address
Switch-Access(config)# ip source binding 0030.94C2.9A43 vlan 303 10.0.2.68 interface
g1/0/52
! Specifies MAC to IP binding for statically assigned DMZ server address

Switch-Access(config)# interface range g1/0/2 - 28 ! Enters gigabit Ethernet configuration
mode
Switch-Access(config-if-range)# ip verify source port-security ! Specifies to check the
binding table and allow traffic only if it matches an entry
```

DHCP Snooping Implementation

```
Switch-Access(config)# ip dhcp snooping ! Enables DHCP snooping globally on the switch
Switch-Access(config)# ip dhcp snooping vlan 301-302 ! Enables DHCP snooping for specified
VLANs
Switch-Access(config)# interface range g1/0/1 ! Enters gigabit Ethernet configuration mode
Switch-Access(config-if)# ip dhcp snooping trust ! Disables DHCP snooping
```

DHCP Snooping Verification

To verify your Dynamic Host Configuration Protocol (DHCP) snooping configuration, enter the following command.

```
Switch-Access# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
301-303
Insertion of option 82 is enabled
```

BPDU Guard Implementation

The following is an example for configuring port security on all trunk ports.

```
Switch-Access(config-if)# interface g1/0/1 ! Enters gigabit Ethernet configuration mode
Switch-Access(config-if)# spanning-tree bpduguard disable ! Disables BPDU guard
Switch-Access(config)# interface range g1/0/2 - 28 ! Enters gigabit Ethernet configuration
mode
Switch-Access(config-if)# spanning-tree bpduguard enable ! Enables BPDU guard
```

Management Services Implementation

- [NetFlow Implementation, page 167](#)
- [SNMP Implementation, page 167](#)
- [NTP Implementation, page 168](#)
- [IP SLA Implementation, page 169](#)
- [Syslog Implementation, page 170](#)
- [Cisco Configuration Professional Implementation, page 170](#)
- [Cisco Configuration Engine Implementation, page 175](#)

NetFlow Implementation

Cisco IOS NetFlow efficiently collects and measure data as it enters specific router interface. This data can be used for network traffic accounting and network planning.

NetFlow can be configured to collect data for top flows, and the data can be used for further analysis.

```
Router(config)# ip flow-top-talkers ! Enabled NetFlow to capture traffic statistics for
top flows
Router(config-flow-top-talkers)# top 5 ! Specifies the maximum number of top talkers
Router(config-flow-top-talkers)# sort-by packets ! Specifies to sort top talkers by number
of bytes
Router(config-flow-top-talkers)# cache-timeout 100 ! Specifies the time up to which top
talkers statistics collected
Router(config-flow-top-talkers)# exit
Router(config)# exit
```

NetFlow Verification

To verify your NetFlow configuration, enter the following command:

```
Router# show ip flow top-talkers
```

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Mu1	10.0.0.22	Local	10.0.0.8	2F	0000	0000	28
Mu1	10.0.0.27	Local	10.0.0.10	32	AAB6	2992	28
Tu1	172.16.0.10	Null	224.0.0.10	58	0000	0000	27

3 of 5 top talkers shown. 3 flows processed.

```
Router#
```

SNMP Implementation

Simple Network Management Protocol (SNMP) is an application layer protocol which facilitates the exchange of management information between a network device and an SNMP server. This information can be used for network management and troubleshooting.

SNMP is enabled to send traps for specific events that will be used for troubleshooting. Two SNMP communities with different privileges were configured.

```
Router(config)# ip access-list standard Full ! List of clients with full access to SNMP
agent
Router(config-std-nacl)# permit host 172.16.4.5
Router(config-std-nacl)# exit
Router(config)# ip access-list standard Browse ! List of clients with browse access to
SNMP agent
Router(config-std-nacl)# permit host 10.0.0.6
Router(config-std-nacl)# exit
Router(config)# snmp-server community RW-ACCESS rw Full ! Enables SNMP community with
Read/Write access to server
Router(config)# snmp-server community RO-ACCESS ro Browse ! Enables SNMP community with
Read-Only access to server
Router(config)# snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart ! Enables notification for various router events
Router(config)# snmp-server enable traps eigrp ! Enables EIGRP notification
Router(config)# snmp-server enable traps flash insertion removal ! Enables Flash
Insertion/Removal notification
Router(config)# snmp-server enable traps envmon ! Enables Environmental monitor
notification
Router(config)# snmp-server enable traps bgp ! Enables BGP protocol notification
```

```

Router(config)# snmp-server enable traps memory bufferpeak ! Enables Memory buffer peak
notification
Router(config)# snmp-server enable traps hsrp ! Enables HSRP notification
Router(config)# snmp-server enable traps ospf state-change ! Enables OSPF protocol
state-change notification
Router(config)# snmp-server enable traps ospf errors ! Enables OSPF error notification
Router(config)# snmp-server enable traps ospf retransmit ! Enables OSPF LSA retransmit
notification
Router(config)# snmp-server enable traps ospf lsa ! Enables OSPF LSA notification
Router(config)# snmp-server enable traps ospf cisco-specific state-change
nssa-trans-change
! Enables OSPF NSSA state change notification
Router(config)# snmp-server enable traps ospf cisco-specific state-change shamlink
interface-old ! Enables OSPF replaced interface shamlink notification
Router(config)# snmp-server enable traps ospf cisco-specific state-change shamlink
neighbor ! Enables OSPF neighbor shamlink transition notification
Router(config)# snmp-server enable traps ospf cisco-specific errors ! Enables OSPF
nonvirtual interface mismatch error notification
Router(config)# snmp-server enable traps ospf cisco-specific retransmit ! Enables OSPF
retransmit error notification
Router(config)# snmp-server enable traps ospf cisco-specific lsa ! Enables OSPF LSA
notification
Router(config)# snmp-server enable traps cpu threshold ! Enables CPU threshold violation
notification
Router(config)#

```

NTP Implementation

Network Time Protocol (NTP) is used to synchronize the time in local devices to a radio clock or atomic clock attached to the time server. Synchronized time in all the network devices is helpful for troubleshooting and understanding logging messages.

```

Router(config)# ntp authenticate ! Enables NTP authentication
Router(config)# ntp authentication-key 1234 md5 NTP-KEY ! Specifies authentication key and
Password
Router(config)# ntp trusted-key 1234 ! Specifies the key number to be used for
authentication
Router(config)# ntp server 172.16.0.60 key 1234 ! Specifies central site NTP server
address and key

```

```

Switch-Dist (config)# ntp authenticate ! Enables NTP authentication
Switch-Dist (config)# ntp authentication-key 1234 md5 NTP-KEY ! Specifies authentication
key and Password
Switch-Dist (config)# ntp trusted-key 1234 ! Specifies the key number to be used for
authentication
Switch-Dist (config)# ntp server 172.16.0.60 key 1234 ! Specifies central site NTP server
address and key

```

```

Switch-Access (config)# ntp authenticate ! Enables NTP authentication
Switch-Access (config)# ntp authentication-key 1234 md5 NTP-KEY ! Specifies authentication
key and Password
Switch-Access (config)# ntp trusted-key 1234 ! Specifies the key number to be used for
authentication
Switch-Access (config)# ntp server 172.16.0.60 key 1234 ! Specifies central site NTP
server address and key

```

Set time zone and daylight saving for a specific time zone. The following example uses U.S. Pacific Standard Time zone.

```

Router(config)# clock timezone pst -8 ! Sets the time zone
Router(config)# clock summer-time pdt recurring ! Sets daylight savings time
Switch-Dist(config)# clock timezone pst -8 ! Sets the time zone

```

```
Switch-Dist(config)# clock summer-time pdt recurring ! Sets daylight savings time

Switch-Access(config)# clock timezone pst -8 ! Sets the time zone
Switch-Access(config)# clock summer-time pdt recurring ! Sets daylight savings time
```

NTP Verification

To verify your NTP configuration, enter the following command:

```
Router# show ntp status
Clock is synchronized, stratum 4, reference is 10.66.66.11
nominal freq is 250.0000 Hz, actual freq is 249.9966 Hz, precision is 2**18
reference time is CC70BD86.5EFBE4E6 (02:16:54.371 PDT Tue Sep 9 2008)
clock offset is -0.0255 msec, root delay is 0.79 msec
root dispersion is 0.11 msec, peer dispersion is 0.05 msec
Router#
```

IP SLA Implementation

An IP Service Level Agreement (SLA) is a management tool running on Cisco IOS software that can be used to analyze IP service levels for IP applications and services in order to increase the network productivity and to reduce the frequency of network outages.

In the Basic Small Branch Network architecture, the User Datagram Protocol (UDP)-echo operation is used to test end-to-end connectivity and response time, and UDP jitter is used to measure packet variability.

```
Router(config)# ip sla 10 ! Configures IP SLA operation with specified ID
Router(config-ip-sla)# udp-echo 209.165.201.10 65535 source-ip 209.165.201.9 source-port
65000 ! Performs UDP echo operation between two Loopback Interfaces
Router(config-ip-sla-udp)# frequency 30 ! Sets the rate at which a specified IP SLA
operation repeats
Router(config)# ip sla 20 ! Configures IP SLA operation with specified ID
Router(config-ip-sla-udp)# udp-jitter 209.165.201.10 65535 source-ip 209.165.201.9
source-port 65000 ! Performs UDP jitter operation between two Loopback Interfaces
Router(config-ip-sla-jitter)# frequency 30 ! Sets the rate at which a specified IP SLA
operation repeats

Router(config-ip-sla-udp)# exit
Router(config)# ip sla schedule 10 start-time now life forever ! Starts the IP SLA
operation now and runs it indefinitely
Router(config)# ip sla schedule 20 start-time now life forever ! Starts the IP SLA
operation now and runs it indefinitely
```

IP SLA Verification

To verify your IP SLA configuration, enter the following command:

```
Router# show ip sla statistics

Round Trip Time (RTT) for      Index 10
      Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: *22:45:46.259 pst Mon Feb 2 2009
Latest operation return code: No connection
Number of successes: 0
Number of failures: 3
Operation time to live: Forever
```

```

Round Trip Time (RTT) for          Index 20
    Latest RTT: 0 milliseconds
Latest operation start time: *20:22:59.119 pst Mon Feb 2 2009
Latest operation return code: Socket bind error
RTT Values:
    Number Of RTT: 0                RTT Min/Avg/Max: 0/0/0 milliseconds
Latency one-way time:
    Number of Latency one-way Samples: 0
    Source to Destination Latency one way Min/Avg/Max: 0/0/0 milliseconds
    Destination to Source Latency one way Min/Avg/Max: 0/0/0 milliseconds
Jitter Time:
    Number of SD Jitter Samples: 0
    Number of DS Jitter Samples: 0
    Source to Destination Jitter Min/Avg/Max: 0/0/0 milliseconds
    Destination to Source Jitter Min/Avg/Max: 0/0/0 milliseconds
Packet Loss Values:
    Loss Source to Destination: 0      Loss Destination to Source: 0
    Out Of Sequence: 0                Tail Drop: 0
    Packet Late Arrival: 0            Packet Skipped: 0
Voice Score Values:
    Calculated Planning Impairment Factor (ICPIF): 0
    Mean Opinion Score (MOS): 0
Number of successes: 0
Number of failures: 4
Operation time to live: Forever

```

Syslog Implementation

Apply following commands to enable syslog logging.

```

Router(config)# service timestamps log datetime msec localtime show-timezone ! Instructs
the system to timestamp syslog messages
Router(config)# logging 172.16.0.90 ! Identifies syslog server
Router(config)# logging trap notifications ! Log notice messages and above
Router(config)# logging facility local2 ! Specifies the facility level used by the syslog
messages
Router(config)# logging buffered 4096 ! Sets size of internal log buffer

Switch-Access(config)# service timestamps log datetime msec localtime show-timezone !
Instructs the system to timestamp syslog messages
Switch-Access (config)# logging 172.16.0.90 ! Identifies syslog server
Switch-Access (config)# logging trap notifications ! Log notice messages and above
Switch-Access (config)# logging facility local2 ! Specifies the facility level used by the
syslog messages
Switch-Access (config)# logging buffered 4096 ! Sets size of internal log buffer

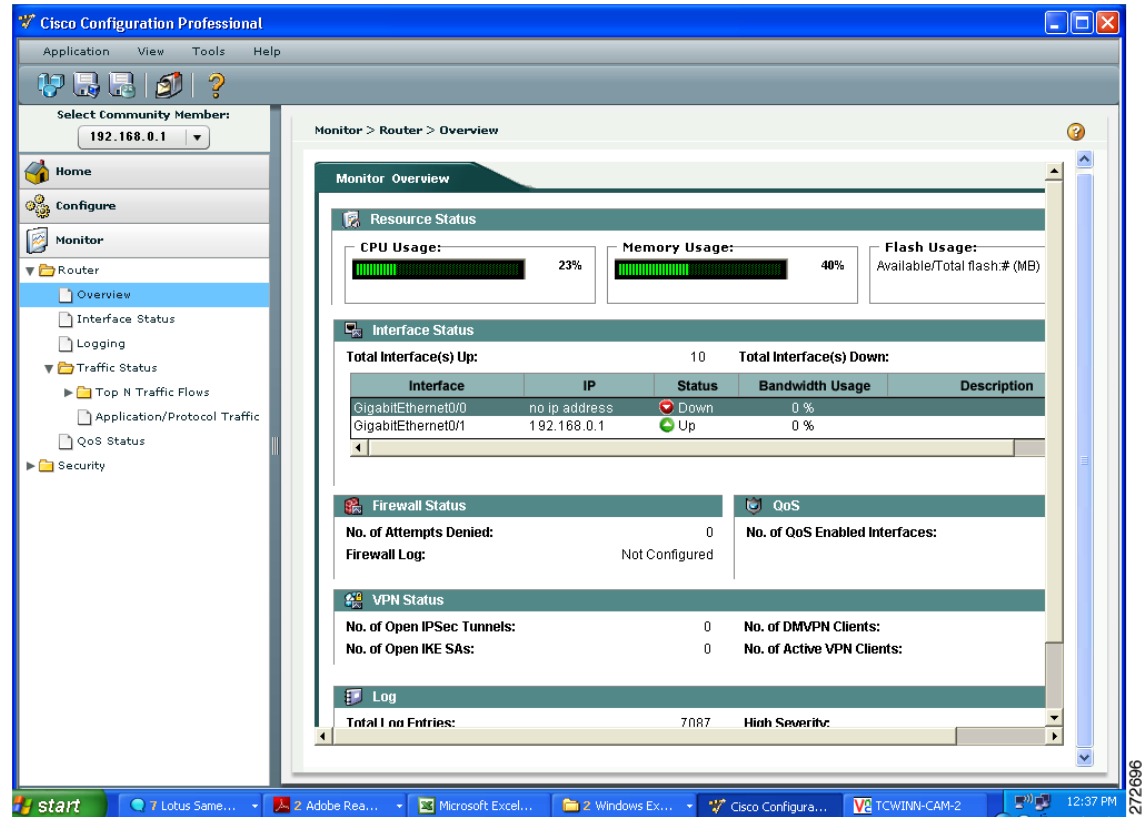
Switch-Dist(config)# service timestamps log datetime msec localtime show-timezone !
Instructs the system to timestamp syslog messages
Switch-Dist (config)# logging 172.16.0.90 ! Identifies syslog server
Switch-Dist (config)# logging trap notifications ! Log notice messages and above

```

Cisco Configuration Professional Implementation

Monitoring of the Basic Small Branch Network was done with the Cisco Configuration Professional in monitor mode. Cisco Configuration Professional provides an overview of router status and performance metrics without having to use the Cisco IOS command-line interface. [Figure 69](#) shows the monitor overview, which includes information such as CPU and memory usage, interface status, firewall status, and VPN status.

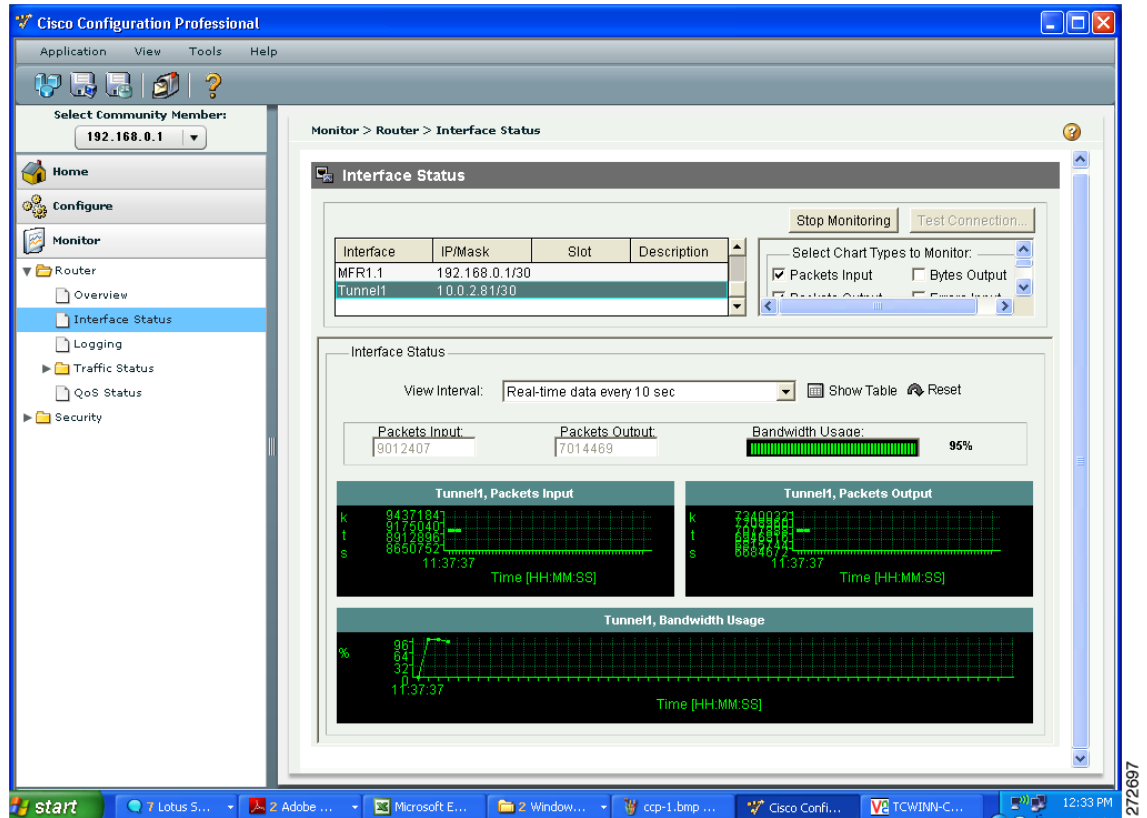
Figure 69 Cisco Configuration Professional Monitor Overview



272696

Figure 70 shows the interface status for the Fast Ethernet interface, which includes packets in and out, and bandwidth usage.

Figure 70 Cisco Configuration Professional Fast Ethernet Interface Status



272697

Figure 71 shows the interface status for the tunnel interface.

Figure 71 Cisco Configuration Professional Tunnel Interface Status

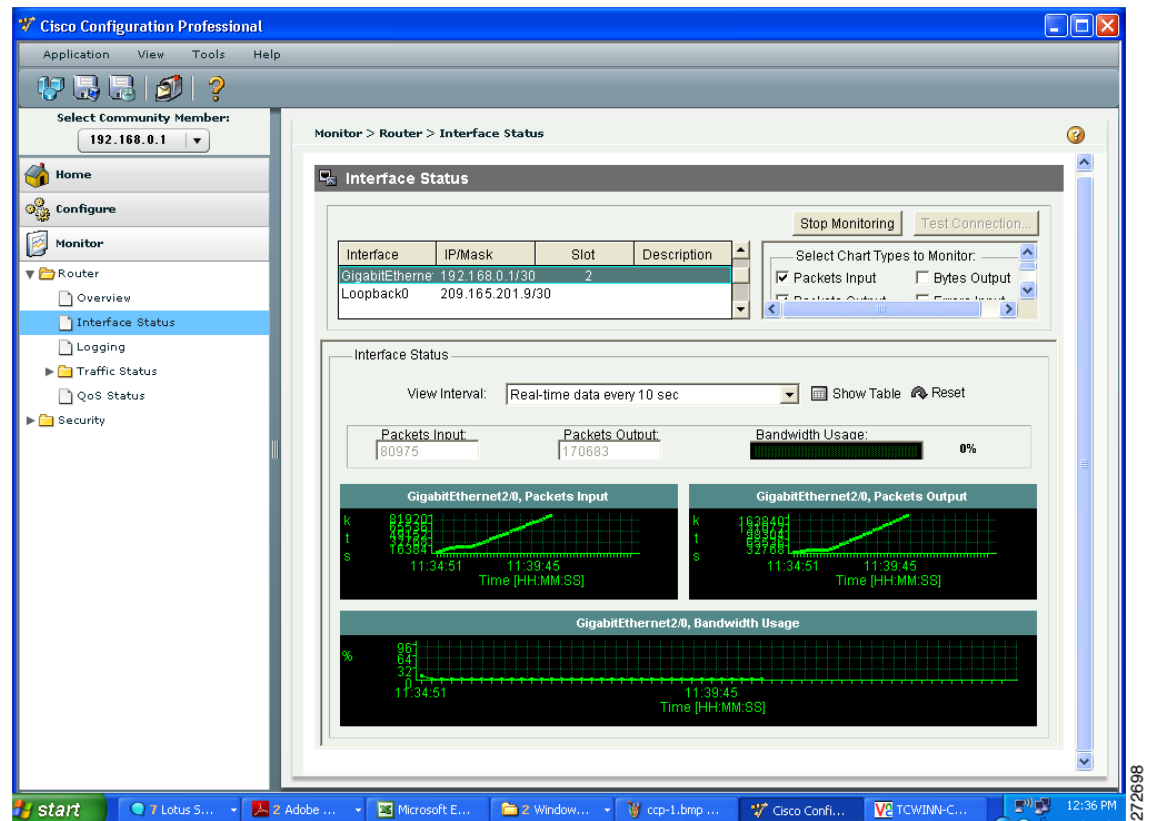


Figure 72 shows the VPN status for the DMVPN tunnel, which includes encapsulation and decapsulation packets and send and receive error packets.

Figure 72 Cisco Configuration Professional VPN Status

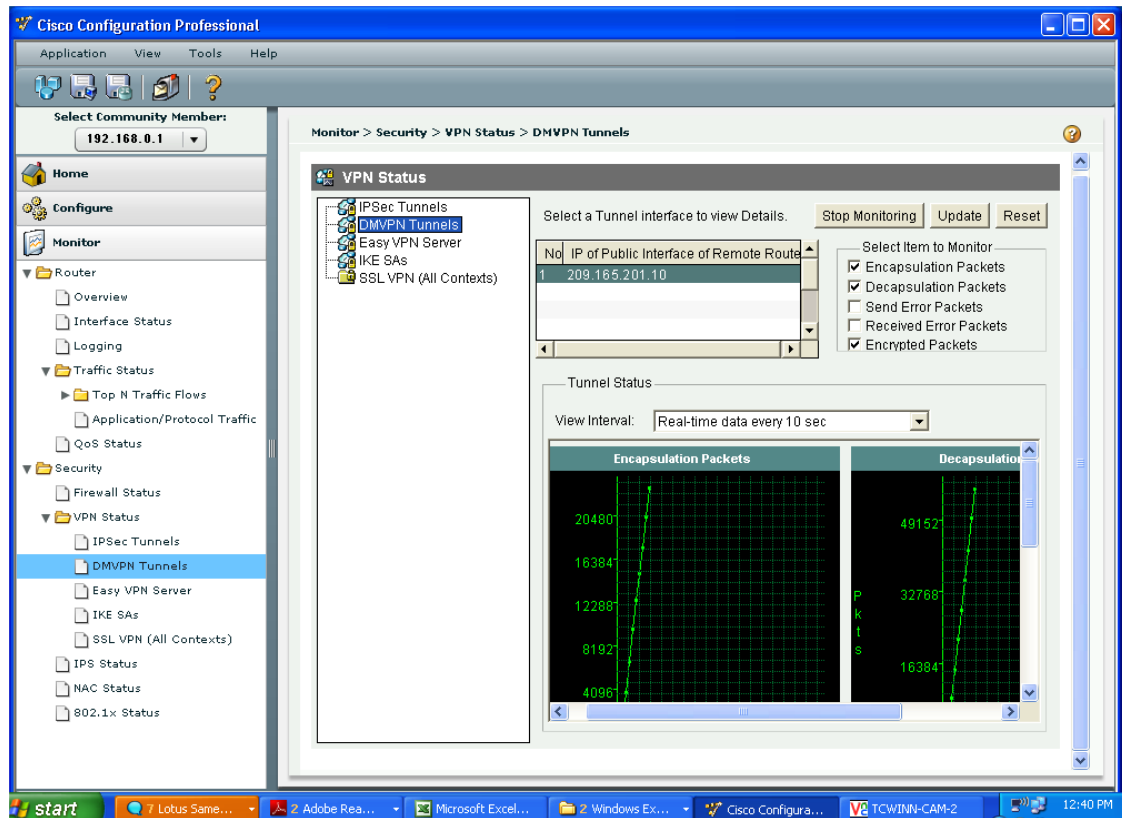
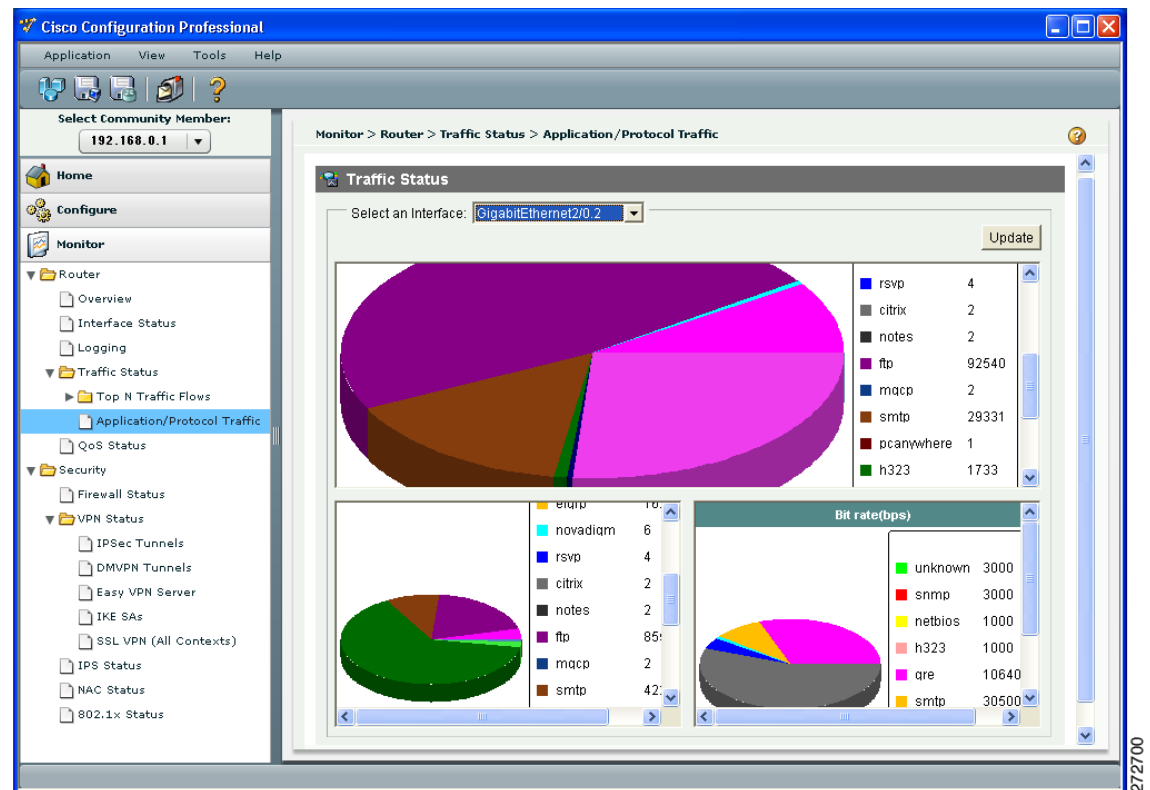


Figure 73 shows the interface traffic analysis.

Figure 73 Cisco Configuration Professional Traffic Analysis



Cisco Configuration Engine Implementation

There are several steps required to enable deployment with the Cisco Configuration Engine. First, *bootstrap configuration* must be applied to each device. The bootstrap configuration is either preloaded or obtained from a centrally hosted DHCP server through option 150. In the Basic Small Branch Network, both routers and all switches were preloaded with the following bootstrap configuration.

```
Router(config)# cns trusted-server all-agents cce.example.com ! Specifies trusted server for CNS agent
Router(config)# cns id hardware-serial ! Identifies this devices by its serial number to CCE
Router(config)# cns id hardware-serial event ! Identifies this devices by its serial number to CCE event logging component
Router(config)# cns event cce.example.com ! Enables event agent
Router(config)# cns config initial cce.example.com 80 ! Initiates an initial configuration on CCE server port 80
Router(config)# cns config partial cce.example.com 80 ! Initiates an incremental configuration on CCE server port 80
Router(config)# cns exec 80 ! Enables CNS agent

Switch-Access(config)# cns trusted-server all-agents cce.example.com ! Specifies trusted server for CNS agent
Switch-Access(config)# cns id hardware-serial ! Identifies this devices by its serial number to CCE
Switch-Access(config)# cns id hardware-serial event ! Identifies this devices by its serial number to CCE event logging component
```

```

Switch-Access(config)# cns event cce.example.com ! Enables event agent
Switch-Access(config)# cns config initial cce.example.com 80 ! Initiates an initial
configuration on CCE server port 80
Switch-Access(config)# cns config partial cce.example.com 80 ! Initiates an incremental
configuration on CCE server port 80
Switch-Access(config)# cns exec 80 ! Enables CNS agent

Switch-Dist(config)# cns trusted-server all-agents cce.example.com ! Specifies trusted
server for CNS agent
Switch-Dist(config)# cns id hardware-serial ! Identifies this devices by its serial number
to CCE
Switch-Dist(config)# cns id hardware-serial event ! Identifies this devices by its serial
number to CCE event logging component
Switch-Dist(config)# cns event cce.example.com ! Enables event agent
Switch-Dist(config)# cns config initial cce.example.com 80 ! Initiates an initial
configuration on CCE server port 80
Switch-Dist(config)# cns config partial cce.example.com 80 ! Initiates an incremental
configuration on CCE server port 80
Switch-Dist(config)# cns exec 80 ! Enables CNS agent

```

Secondly, the device CNS ID must be entered into the CCE server prior to powering on of branch devices. Each device CNS is associated with Cisco IOS image to be loaded onto the device and a configuration template. The Basic Small Branch Network provides following 6 CCE templates:

- **Configuration for zero-touch deployment with Cisco Configuration Engine**
 - Bootstrap Configuration for routers and switches
- **Cisco 1861 Configuration**
 - Fast Ethernet WAN interface, OSPF routing, DMVPN, and Cisco Unified CME with SCCP IP Phones and H.323 trunking to the central site.
 - A T1 WAN interface bundle with PPP encapsulation, EIGRP routing, GETVPN, and Cisco Unified CME with SIP IP Phones and SIP trunking to central site.
 - A T1 WAN interface bundle with Frame Relay encapsulation, EIGRP routing, DMVPN, and Cisco Unified SRST with SCCP IP Phones and H.323 trunking to central site.
 - One-half T1 WAN interface with Frame Relay encapsulation, OSPF routing, GETVPN, and Cisco Unified SRST with SIP IP Phones and SIP trunking to central site.
- **Cisco 1841 Configuration**
 - Fast Ethernet WAN interface, active primary and standby backup WAN links, OSPF routing, DMVPN over primary and backup WAN links.
 - A T1 WAN interface bundle with PPP encapsulation, active primary and standby backup WAN links, EIGRP routing, GETVPN over primary and DMVPN over backup WAN links.
 - A T1 WAN interface bundle with Frame Relay encapsulation, simultaneously active primary and backup WAN links, EIGRP routing, DMVPN over primary and backup WAN links.
 - One-half T1 WAN interface with Frame Relay encapsulation, simultaneously active primary and backup WAN links, OSPF routing, GETVPN over primary and DMVPN over backup WAN links.
- **Access Switches**
 - A 24-port access switch with Data, DMZ, and Voice VLANs on access ports.
 - A 8-port access switch with Data, DMZ, and Voice VLANs on access ports.

Downloading and Using the Configuration Templates

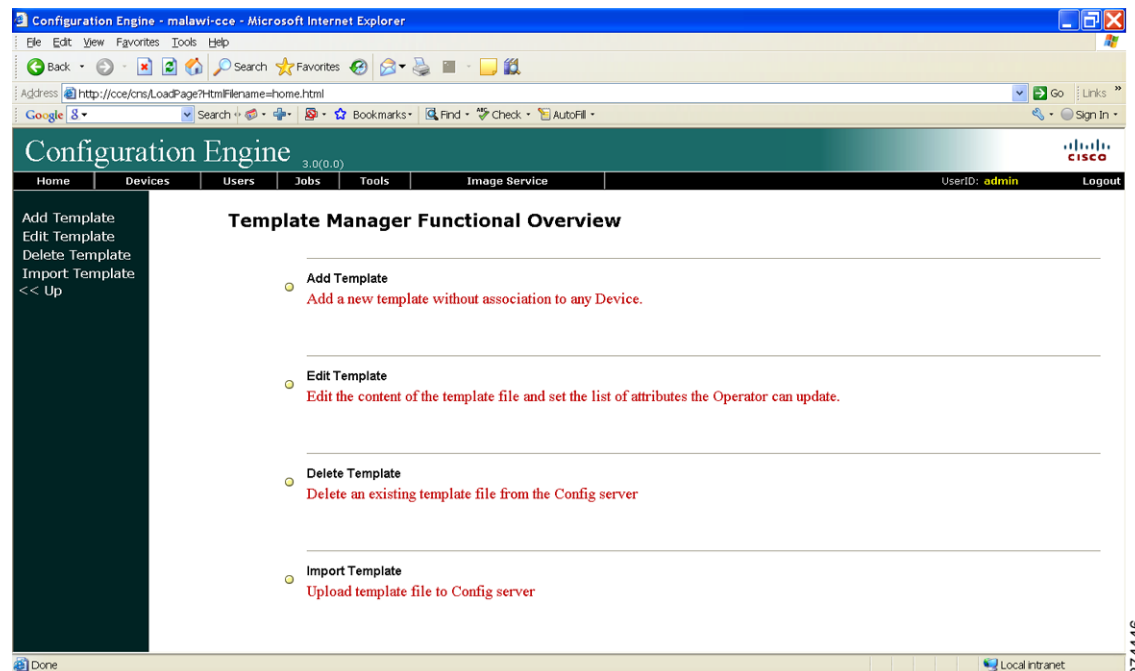
Download the templates from the following location:

- [Configuration Toolkit for Basic Small Branch Network](#)

To use the configuration templates for manual configurations, download them to a TFTP server that is accessible from the routers and switches. To use the configuration templates with Cisco Configuration Engine (CCE) 3.0, complete the following steps:

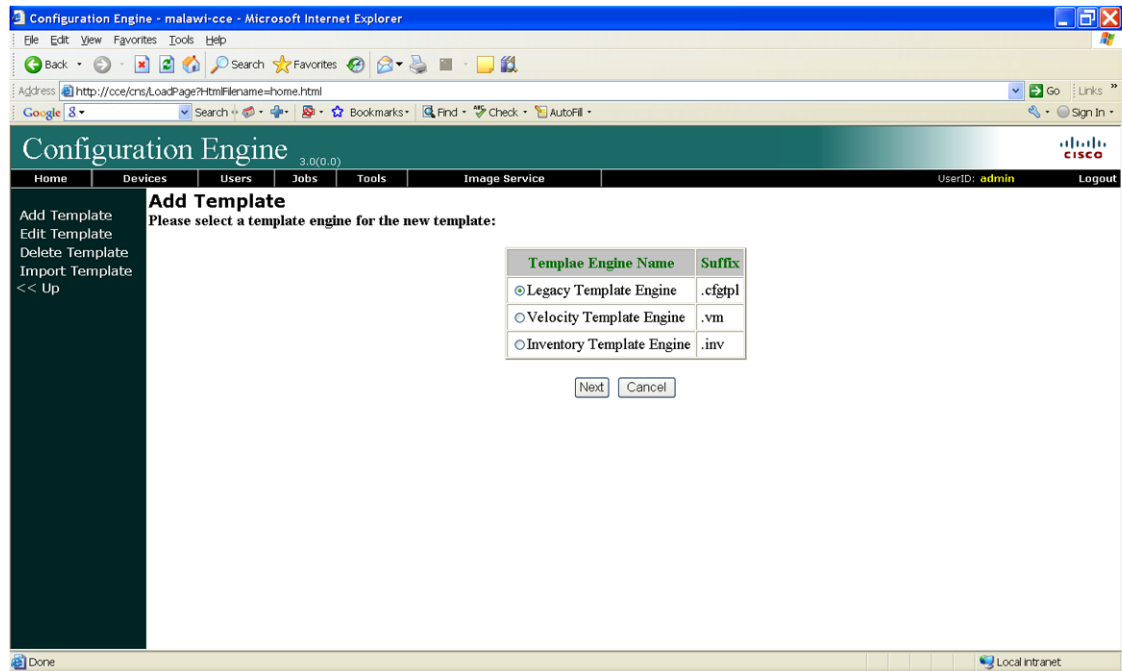
-
- Step 1** Log in to CCE and navigate to **Tools > Template Manager**.
- Step 2** In the Template Manager window, shown in [Figure 74](#), click **Add Template**. The Template Engine window appears.

Figure 74 CCE Template Manager

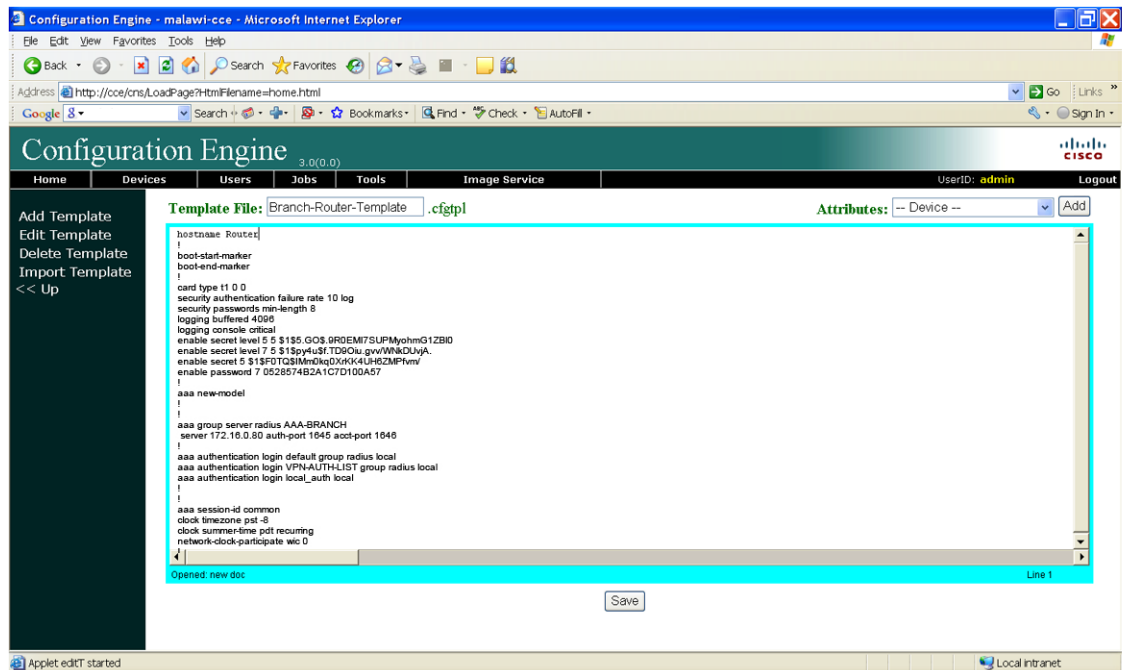


- Step 3** In the Template Engine window, shown in [Figure 75](#), choose the best template engine for your specific environment, and then click **Next**. The CCE Configuration Editor window appears.

274446

Figure 75 CCE Template Engine

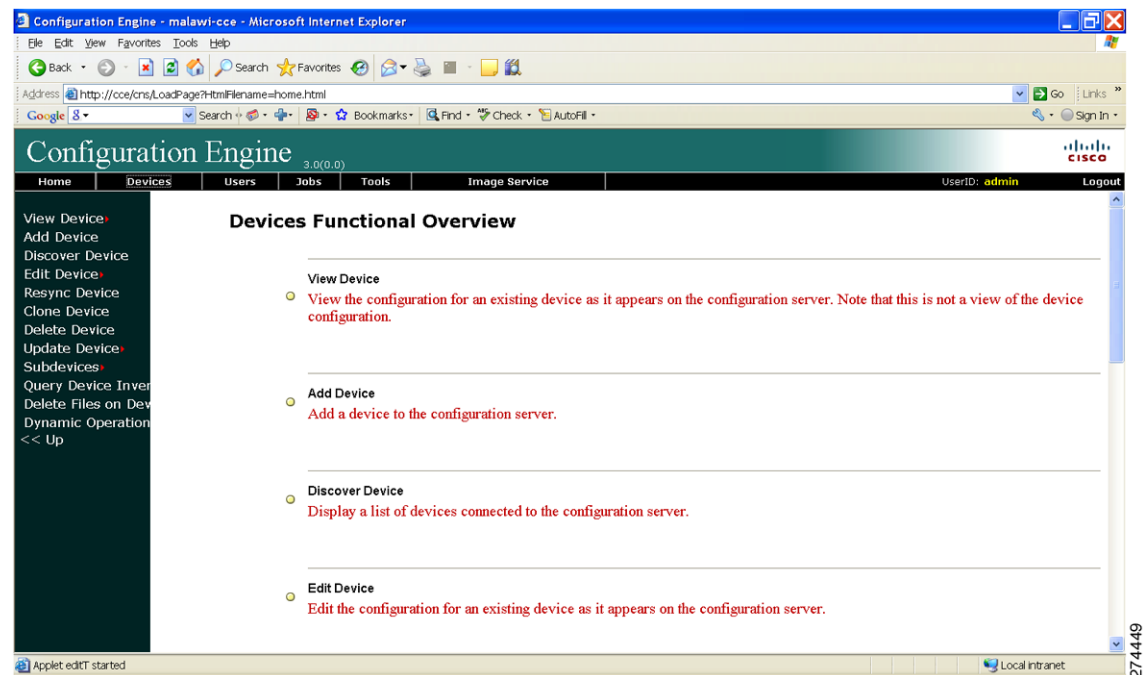
- Step 4** From the list of configuration templates, copy the configuration template that best meets your needs from one of the above listed configuration templates and paste it into the CCE Configuration Editor, shown in Figure 76.

Figure 76 CCE Configuration Editor

- Step 5** Customize the configuration to meet the needs of your specific environment. After editing the configuration, name and save the configuration.

Step 6 Navigate to the Device Manager window, shown in [Figure 77](#), and click **Add Device**.

Figure 77 CCE Device Manager



Step 7 In the Create Device Editor window, shown in [Figure 78](#), assign a Device Name, a Unique ID that corresponds to the configuration name specified in [Step 5](#), and a Device Type. Click **Next**. The Device Group Selector window appears.

Figure 78 CCE Create Device Editor

- Step 8** Choose group membership as shown in Figure 79. CCE supports management of devices as groups. See the CCE documentation for details on how to manage devices as a group. Click **Next**. The Device Group Selector window appears.

Figure 79 CCE Device Group Selector

- Step 9** In the Device Identification Assignment window, shown in [Figure 80](#), enter the Event ID, Config ID, and Image ID (CCE supports the ability to distribute Cisco IOS software images; see the CCE documentation for additional information) for the Device Type. Click **Finish**.

**Note**

These IDs must match the identification provided in the device Bootstrap Configuration.

Figure 80 CCE Device Identification Assignment

- Step 10** Repeat this procedure for all routers and switches.

Voice Services Implementation

**Note**

The following sections apply only to the Cisco 1861 ISR configuration.

- [FXO and FXS Port Implementation, page 182](#)
- [Cisco Unified CME with SCCP Endpoints Implementation, page 183](#)
- [Cisco Unified CME with SIP Endpoints Implementation, page 200](#)
- [Cisco Unified SRST with SCCP Endpoints Implementation, page 206](#)
- [Cisco Unified SRST with SIP Endpoints Implementation, page 218](#)

This section describes the implementation of two scenarios for voice services:

- Distributed infrastructure and branch endpoints are controlled by Cisco Unified Communications Manager Express (Cisco Unified CME). Local branch voice mail is provided through Cisco Unity Express access.

- Centralized call control with Cisco Unified Communications Manager (Cisco Unified CM). Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) is configured in case of WAN failure.

The following high-level steps must be performed for each telephony service:

1. Configure voice connectivity.
2. Perform telephony service setup.
3. Install IP Phones.
4. Configure voice gateway.
5. Configure dial plan.
6. Set up transcoding and conferencing.
7. Implement Music on Hold.
8. Integrate voice mail.
9. Configure emergency services.

FXO and FXS Port Implementation

FXO ports were used to connect the router to the public switched telephone network (PSTN).

```
Router(config)# voice-port0/1/0 ! Enters voice port configuration mode
Router(config-voiceport)# station-id name ANALOG-1 ! Assigns a name for the voice port
Router(config-voiceport)# exit
```

```
Router(config)# voice-port0/1/1 ! Enters voice port configuration mode
Router(config-voiceport)# station-id name ANALOG-2 ! Assigns a name for the voice port
Router(config-voiceport)# exit
```

```
Router(config)# voice-port0/1/2 ! Enters voice port configuration mode
Router(config-voiceport)# station-id name ANALOG-3 ! Assigns a name for the voice port
Router(config-voiceport)# exit
```

```
Router(config)# voice-port0/1/3 ! Enters voice port configuration mode
Router(config-voiceport)# station-id name ANALOG-4 ! Assigns a name for the voice port
Router(config-voiceport)# exit
```

The following configuration applies to analog Foreign Exchange Service (FXS) ports.

```
Router(config)# voice-port0/0/0 ! Enters voice port configuration mode
Router(config-voiceport)# station-id name ANALOG-1 ! Assigns a name for the voice port
Router(config-voiceport)# exit
```

```
Router(config)# voice-port0/0/1 ! Enters voice port configuration mode
Router(config-voiceport)# station-id name ANALOG-2 ! Assigns a name for the voice port
Router(config-voiceport)# exit
```

```
Router(config)# voice-port0/0/2 ! Enters voice port configuration mode
Router(config-voiceport)# station-id name ANALOG-3 ! Assigns a name for the voice port
Router(config-voiceport)# exit
```

```
Router(config)# voice-port0/0/3 ! Enters voice port configuration mode
Router(config-voiceport)# station-id name ANALOG-4 ! Assigns a name for the voice port
Router(config-voiceport)# exit
```

In the Basic Small Branch network T1, the serial interface utilizes compressed RTP to place calls over the WAN. There are several ways to configure cRTP. In the following implantation, cRTP is configured on the QoS class map:

```
Router(config)# policy-map FIVE-CLASS-V3PN-EDGE ! Defines child policy map
Router(config-pmap)# class VOICE ! Matches traffic classified by VOICE class-map
Router(config-pmap-c)# compress header ip rtp ! Enables cRTP compression
Router(config-pmap-c)# exit
```

The Basic Small Branch Networks has been tested with both SIP- and SCCP-enabled phones. Each phone type requires a different configuration. To implement SCCP-based phones, follow the SCCP instructions in the “[Cisco Unified CME with SCCP Endpoints Implementation](#)” section on page 183. To implement SIP-based phones, follow SIP instructions in the “[Cisco Unified CME with SIP Endpoints Implementation](#)” section on page 200.

To implement the various voice services described in the following sections, several resources are necessary at the central site. [Table 22](#) lists these resources and the associated IP addresses that are used in the implementation instructions.

Table 22 *Central Site Resources Required for Voice Implementation*

Resource	IP Address
NTP Server	172.16.0.60
Cisco Call Manager	172.16.200.10
Message Wait Indicator Server	172.16.0.110
Music on Hold Multicast Group	239.1.1.1

Cisco Unified CME with SCCP Endpoints Implementation

- [Cisco Unified CME with SCCP Endpoints: Telephony Service Setup](#), page 183
- [Cisco Unified CME with SCCP Endpoints: IP Phone Installation and Configuration](#), page 185
- [Cisco Unified CME with SCCP Endpoints: H.323 Voice Gateway Implementation](#), page 187
- [Cisco Unified CME with SCCP Endpoints: Dial Plan Implementation](#), page 187
- [Cisco Unified CME with SCCP Endpoints: CAC Implementation](#), page 188
- [Cisco Unified CME with SCCP Endpoints: Transcoding and Conferencing Implementation](#), page 189
- [Cisco Unified CME with SCCP Endpoints: Music on Hold Implementation](#), page 190
- [Cisco Unified CME with SCCP Endpoints: Voice Mail and Auto Attendant Integration](#), page 191
- [Cisco Unified CME with SCCP Endpoints: Emergency Services Implementation](#), page 197
- [Cisco Unified CME with SCCP Endpoints Verification](#), page 198

Cisco Unified CME with SCCP Endpoints: Telephony Service Setup

The Cisco IOS software provides an automated mechanism for configuring IP telephony services.

```
Router(config)# telephony-service setup ! Enters into Unified CME start setup mode

--- Cisco IOS Telephony Services Setup ---
```

Do you want to setup DHCP service for your IP Phones? [yes/no]: **no**

Do you want to start telephony-service setup? [yes/no]: **yes**

Configuring Cisco IOS Telephony Services :

Enter the IP source address for Cisco IOS Telephony Services :**10.0.1.2**

Enter the Skinny Port for Cisco IOS Telephony Services : [2000]:

How many IP Phones do you want to configure : [0]: **30 ! User configurable number of phones up to maximum of 96 on 2800 ISRs**

Do you want dual-line extensions assigned to phones? [yes/no]: **yes**

What Language do you want on IP Phones :

- 0 English
- 1 French
- 2 German
- 3 Russian
- 4 Spanish
- 5 Italian
- 6 Dutch
- 7 Norwegian
- 8 Portuguese
- 9 Danish
- 10 Swedish
- 11 Japanese

[0]: **! Maintains default English language**

Which Call Progress tone set do you want on IP Phones :

- 0 United States
- 1 France
- 2 Germany
- 3 Russia
- 4 Spain
- 5 Italy
- 6 Netherlands
- 7 Norway
- 8 Portugal
- 9 UK
- 10 Denmark
- 11 Switzerland
- 12 Sweden
- 13 Austria
- 14 Canada
- 15 Japan

[0]: **! Maintains default United States call progress tone**

What is the first extension number you want to configure : **5001**

Do you have Direct-Inward-Dial service for all your phones? [yes/no]: **yes**

Enter the full E.164 number for the first phone :**4085555001 ! Assigns DID number**

Do you want to forward calls to a voice message service? [yes/no]: **yes**

Enter extension or pilot number of the voice message service:**5444**

Call forward No Answer Timeout : [18]: **! Maintains default value of 18 seconds.**

Possible values are from 5 to 60000 seconds

Do you wish to change any of the above information? [yes/no]: **no**

CNF-FILES: Clock is not set or synchronized,
retaining old versionStamps

---- Setup completed config ---

Router(config)#

*Sep 10 05:37:10.207: percentLINK-3-UPDOWN: Interface ephone_dsp DN 1.2, changed state to up

*Sep 10 05:37:10.207: percentLINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to up

```
*Sep 10 05:37:10.207: percentLINK-3-UPDOWN: Interface ephone_dsp DN 2.2, changed state to up
*Sep 10 05:37:10.207: percentLINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed state to up
*Sep 10 05:37:10.207: percentLINK-3-UPDOWN: Interface ephone_dsp DN 3.2, changed state to up
*Sep 10 05:37:10.207: percentLINK-3-UPDOWN: Interface ephone_dsp DN 4.1, changed state to up
*Sep 10 05:37:10.207: percentLINK-3-UPDOWN: Interface ephone_dsp DN 4.2, changed state to up
```

Cisco Unified CME with SCCP Endpoints: IP Phone Installation and Configuration

In the Basic Small Branch Network, IP Phones are installed by simply connecting them to ports on the access layer switches. Because all the ports offer Power-over-Ethernet, no additional power cables are necessary. After they are installed, the phones are configured with the default configuration that was generated during the telephony setup in the previous section. However, if the IP Phone firmware needs to be upgraded in the future, enter the following commands.



Note

The following configuration is not required with the Cisco IOS software image used for the Basic Small Branch Network validation.

```
Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telephony)# load 7960-7940 P00308000900 ! Loads telephony SCCP firmware files for 7960 to 7940 phones
Router(config-telephony)# load 7942 SCCP42.8-3-2S ! Loads telephony SCCP firmware files for 7942 phones
Router(config-telephony)# load 7962 SCCP62.8-3-2S ! Loads telephony SCCP firmware files for 7962 phones
Router(config-telephony)# load 7965 SCCP65.8-3-2S ! Loads telephony SCCP firmware files for 7965 phones
Router(config-telephony)# load 7971 SCCP71.8-3-2S ! Loads telephony SCCP firmware files for 7971 phones
Router(config-telephony)# load 7985 cmterm_7985.4-1-6-0 ! Loads telephony SCCP firmware for 7985 video phone
```

Apply the following command after defining the new ephone type.

```
Router(config-telephony)# load 7937 cmterm_7937.1-2-1-0 ! Loads telephony SCCP firmware files for 7937 conference station
```

```
Router(config-telephony)# create cnf-files ! Builds XML configuration file for SCCP phones
Router(config-telephony)# exit
```

This guide provides Cisco IOS software commands for setting up IP Phones. Alternatively, a graphical user interface (GUI) allows the configuration of directory numbers through a web interface. To set up the web configuration tool, use the following instructions to enable the services on the router:

```
Router(config)# ip http server ! Enables HTTP server
Router(config)# ip http path flash: ! Specifies location of HTTP files in IOS
Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telephony)# web admin system name admin password c1$k0SyS ! Defines username and password for system administrator
Router(config-telephony)# dn-webedit ! Enables ability to configure directory numbers
Router(config-telephony)# time-webedit ! Enables ability to configure phone time
Router(config-telephony)# exit
```

```
Router(config)# telephony-service ! Enters telephony configuration mode
```

```

Router(config-telephony)# max-ephones 50 ! Sets the maximum number of phones that can
register with Cisco CME
Router(config-telephony)# max-dn 100 ! Sets the maximum number of directory numbers (two
for each phone)
Router(config-telephony)# ip source-address 10.0.1.2 port 2000 secondary 10.0.1.1 ! Sets
IP address used for phone registration and secondary router for backup
Router(config-telephony)# time-zone 5 ! Sets time zone to Pacific Standard/Daylight Time
Router(config-telephony)# no auto-reg-ephone ! Disables registration of unconfigured
phones
Router(config-telephony)# voicemail 5444 ! Defines number for speed dialing voicemail from
phone
Router(config-telephony)# system message Your current options ! Message displayed on IP
Phones
Router(config-telephony)# secondary-dialtone 9 ! Provides dial tone for PSTN calls
Router(config-telephony)# transfer-system full-blind ! Transfers calls without consultation
Router(config-telephony)# transfer-pattern 9..... ! Allows transfers for all calls
originating from PSTN
Router(config-telephony)# transfer-pattern 4..... ! Allows transfers for all calls
originating in area code starting with "4"
Router(config-telephony)# call-forward pattern .T ! Allows call forwarding for all calls
Router(config-telephony)# exit

Router(config)# ephone-template 1 ! Defines ephone configuration template tag
Router(config-ephone-template)# softkeys hold Join Newcall Resume Select ! Softkey display
when the connected party is on hold
Router(config-ephone-template)# softkeys idle ConfList Join Newcall Pickup Redial !
Softkey display when the phone is idle
Router(config-ephone-template)# softkeys seized Redial Endcall Cfwdall Pickup Callback
Meetme ! Softkey display when caller is attempting to call but has not been connected yet
Router(config-ephone-template)# softkeys connected Trnsfer Hold Confrn Endcall ! Softkey
display when connection to remote point has been established
Router(config-ephone-template)# exit

```

Apply the following configuration to all IP Phones 1 to 50. Set the unique DN number and assign the desired extension to each phone.

```

Router(config)# ephone-dn 1 dual-line ! Enters directory number configuration mode
Router(config-ephone-dn)# number 5001 ! Configures phone (or extension) number for this
directory number
Router(config-ephone-dn)# call-forward busy 5444 ! Forwards call for a busy extension to
voicemail
Router(config-ephone-dn)# call-forward noan 5444 timeout 10 ! Forwards call for an
extension that does not answer to voicemail after 10 seconds of ringing
Router(config-ephone-dn)# exit

Router(config)# ephone 1 ! Enters phone configuration mode
Router(config-ephone)# ephone-template 1 ! Associates phone with configuration template
Router(config-ephone)# button 1:1 ! Associates phone with directory number 1:2, 1:3, etc.
Router(config-ephone)# exit

```

To configure soft phone, use the following example.

```

Router(config)# ephone 120 ! Enters phone configuration mode
Router(config-ephone)# type CIPC ! Specifies that this is softphone
Router(config-ephone)# ephone-template 1 ! Associates phone with configuration template
Router(config-ephone)# button 1:120 ! Associates phone with directory number 1:2, 1:3,
etc.
Router(config-ephone)# exit

```

In Cisco IOS 12.4(20)T and later, apply the following configuration to define a conference station.

```

Router(config)# ephone-type 7937 ! Enters ephone-type template configuration mode
Router(config-ephone-type)# device-id 431 ! Specifies 7937 conference station device id
Router(config-ephone-type)# device-type 7937 ! Specifies device type

```



```

Router(config-ephone-type)# device-name 7936 Conference Station ! Assigns name to the
device type
Router(config-ephone-type)# num-buttons 1 ! Number of line buttons supported
Router(config-ephone-type)# num-presentations 6 ! Number of call presentations lines
Router(config-ephone-type)# exit

Router(config)# ephone-dn 110 dual-line ! Enters directory number configuration
Router(config-ephone-dn)# number 5110 ! Configures extension (or phone) number for this
directory number
Router(config-ephone-dn)# name Engineering Conference Room ! Associates a name with this
directory number
Router(config-ephone-dn)# exit

Router(config)# ephone 110! Enters phone configuration mode
Router(config-ephone)# button 1:110 ! Associates phone with directory number
Router(config-ephone)# exit

```

Generate the configuration file.

```

Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telephony)# create cnf-files ! Builds XML configuration file for SCCP phones
Router(config-telephony)# reset all ! Reloads the phone configuration
Router(config-telephony)# exit

```

Cisco Unified CME with SCCP Endpoints: H.323 Voice Gateway Implementation

The following configuration enables VoIP on the network and sets up H.323 dial peers between the branch gateway and the destination telephone networks.

```

Router(config)# voice service voip ! Enters voice service configuration mode
Router(config-voi-srv)# allow-connections h323 to h323 ! Enables calls h323 endpoint to
h323 endpoint
Router(config-voi-srv)# allow-connections h323 to SIP ! Enables calls from h323 endpoint
to SIP endpoint
Router(config-voi-srv)# exit

```

Cisco Unified CME with SCCP Endpoints: Dial Plan Implementation

Ten dial peers were defined for the Basic Small Branch Network: central site, local calls, two 911 emergency services dial peers, voice mail, auto attendant, long distance, international calling, and fax pass-through or fax relay. Voice mail and emergency services dial peers are described in the “Cisco Unified CME with SIP Endpoints: Voice Mail and Auto Attendant Integration” section on page 205.

```

Router(config)# dial-peer voice 1 voip ! Enters dial peer to central site configuration
mode
Router(config-dial-peer)# dtmf-relay h245-alphanumeric ! Specifies H.245 alphanumeric
method for relaying dual tone multifrequency tones
Router(config-dial-peer)# destination-pattern 408..... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-peer)# exit

Router(config)# dial-peer voice 2 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# destination-pattern 9..... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

```

```

Router(config)# dial-peer voice 3 pots ! Enters dial peer for long distance calls
configuration mode
Router(config-dial-peer)# destination-pattern 91..... ! Specifies area code prefix
for central site dial peer
Router(config-dial-peer)# prefix 1 ! Prefix that the system adds automatically to the dial
string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 4 pots ! Enters dial peer for international calls
configuration mode
Router(config-dial-peer)# destination-pattern 9011T ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 011 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

```

When calls over the WAN exceed the maximum allocated bandwidth, they are redirected to PSTN.

```

Router(config)# dial-peer voice 15 pots ! Enters dial peer for PSTN bypass configuration
mode
Router(config-dial-peer)# destination-pattern 408..... ! Specifies destination pattern
Router(config-dial-peer)# port 0/0/23 ! Specifies outgoing/incoming interface for calls
Router(config-dial-peer)# preference 1 ! Sets the dial peer preference order
Router(config-dial-peer)# prefix 408 ! Prefix that the system adds automatically to the
dial string

```

If you are using fax pass-through, apply the following configuration.

```

Router(config)# dial-peer voice 6 voip ! Enters dial peer for fax passthrough
configuration mode
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-dial-peer)# fax protocol pass-through g711ulaw ! Configures fax passthrough
with G.711 codec
Router(config-peer)# exit

```

If you are using fax relay, apply the following configuration.

```

Router(config)# dial-peer voice 7 voip ! Enters dial peer for fax relay configuration mode
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-dial-peer)# fax-relay ecm disable ! Disables fax relay ECM
Router(config-dial-peer)# fax rate 9600 ! Selects fax transmission rate
Router(config-dial-peer)# fax protocol t38 ! Sets the T.38 fax relay protocol
Router(config-dial-peer)# codec g711ulaw ! Configures fax relay with G.711 codec
Router(config-peer)# exit

```

Cisco Unified CME with SCCP Endpoints: CAC Implementation

RSVP is not supported with Cisco Unified CME. A limited workaround is possible by setting a limit on the number of voice calls that can be placed over the WAN.

```
Router(config)# dial-peer voice 1 voip ! Enters dial peer to central site configuration mode
Router(config-dial-peer)# max-con 36 ! Sets the maximum number of WAN based calls to 36
Router(config-dial-peer)# exit
```

Cisco Unified CME with SCCP Endpoints: Transcoding and Conferencing Implementation

Transcoding compresses and decompresses voice streams to match endpoint-device capabilities. Transcoding is required when an incoming voice stream is digitized and compressed (by means of a codec) to save bandwidth and the local device does not support that type of compression.

```
Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telephony)# sdspfarm units 4 ! Specifies number of DSP farms that can register with SCCP server
Router(config-telephony)# sdspfarm transcode sessions 5 ! Specifies maximum number of simultaneous transcoding sessions
Router(config-telephony)# sdspfarm tag 2 CONFERENCE ! Creates DSP farm profile
Router(config-telephony)# sdspfarm tag 3 TRANSCODE ! Creates DSP farm profile
Router(config-telephony)# conference hardware ! Configures CME for multiparty conferencing
Router(config-telephony)# exit

Router(config)# voice-card 0 ! Enters DSP farm configuration mode
Router(config-voicecard)# dsp services dspfarm ! Enables DSP services
Router(config-voicecard)# exit
Router(config)# sccp local FastEthernet0/1.2 ! Sets the interface for conferencing and transcoding to register with CME
Router(config)# sccp ccm 10.0.1.1 identifier 1 version 5.0.1 ! Associates conferencing and transcoding with CME
Router(config)# sccp ! Enables SCCP globally
Router(config)# sccp ccm group 1 ! Creates SCCP group and enters SCCP configuration mode
Router(config-sccp-ccm)# associate ccm 1 priority 1 ! Associates SCCP group 1 with CME
Router(config-sccp-ccm)# associate profile 2 register CONFERENCE ! Associates DSP farm profile with with a SCCP group
Router(config-sccp-ccm)# associate profile 3 register TRANSCODE ! Associates DSP farm profile with with a SCCP group
Router(config-sccp-ccm)# exit

Router(config)# dspfarm profile 2 transcode ! Enters DSP farm profile configuration mode
Router(config-dspfarm-profile)# codec g711ulaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g711alaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729ar8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729abr8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729r8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec pass-through ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# maximum sessions 5 ! Specifies maximum number of simultaneous sessions supported by this profile
Router(config-dspfarm-profile)# associate application sccp ! Associates SCCP with this DSP farm profile
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit

Router(config)# dspfarm profile 3 conference ! Enters DSP farm profile configuration mode
Router(config-dspfarm-profile)# codec g711ulaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g711alaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729ar8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729abr8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729r8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729br8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# maximum sessions 3 ! Specifies maximum number of simultaneous sessions supported by this profile
```

```

Router(config-dspfarm-profile)# associate application sccp ! Associates SCCP with this DSP
farm profile
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit

Router(config)# ephone-dn 241 dual-line ! Enters directory number configuration mode
Router(config-ephone-dn)# number 5555 ! Associates telephone extension with this directory
number
Router(config-ephone-dn)# conference ad-hoc ! Configures ad-hoc conferencing
Router(config-ephone-dn)# no huntstop ! Continues call hunting if line is unavailable
Router(config-ephone-dn)# exit

Router(config)# ephone-dn 242 dual-line ! Enters directory number configuration mode
Router(config-ephone-dn)# number 5555 ! Associates telephone extension with this directory
number
Router(config-ephone-dn)# conference ad-hoc ! Configures ad-hoc conferencing
Router(config-ephone-dn)# no huntstop ! Continues call hunting if line is unavailable
Router(config-ephone-dn)# preference 1 ! Sets dial peer preference order
Router(config-ephone-dn)# exit

Router(config)# ephone-dn 243 dual-line ! Enters directory number configuration mode
Router(config-ephone-dn)# number 5555 ! Associates telephone extension with this directory
number
Router(config-ephone-dn)# conference ad-hoc ! Configures ad-hoc conferencing
Router(config-ephone-dn)# huntstop ! Stop hunting for lines, all conferencing lines are
occupied
Router(config-ephone-dn)# preference 2 ! Sets dial peer preference order
Router(config-ephone-dn)# exit

Router(config)# ephone-dn 244 dual-line ! Enters directory number configuration mode
Router(config-ephone-dn)# number 5666 ! Associates telephone extension with this directory
number
Router(config-ephone-dn)# conference meetme ! Configures meet me conferencing
Router(config-ephone-dn)# no huntstop ! Continues call hunting if line is unavailable
Router(config-ephone-dn)# exit

Router(config)# ephone-dn 245 dual-line ! Enters directory number configuration mode
Router(config-ephone-dn)# number 5666 ! Associates telephone extension with this directory
number
Router(config-ephone-dn)# conference meetme ! Configures meet me conferencing
Router(config-ephone-dn)# no huntstop ! Continues call hunting if line is unavailable
Router(config-ephone-dn)# preference 1 ! Sets dial peer preference order
Router(config-ephone-dn)# exit

Router(config)# ephone-dn 246 dual-line ! Enters directory number configuration mode
Router(config-ephone-dn)# number 5666 ! Associates telephone extension with this directory
number
Router(config-ephone-dn)# conference meetme ! Configures meet me conferencing
Router(config-ephone-dn)# huntstop ! Stop hunting for lines, all conferencing lines are
occupied
Router(config-ephone-dn)# preference 2 ! Sets dial peer preference order
Router(config-ephone-dn)# exit

```

Cisco Unified CME with SCCP Endpoints: Music on Hold Implementation

Music on Hold (MOH) is an audio stream that is played to PSTN and VoIP G.711 or G.729 callers who are placed on hold by phones in a Cisco Unified Communications Manager Express (Cisco Unified CME) system. This audio stream is intended to reassure callers that they are still connected to their calls.

```

Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telephony)# moh music-on-hold.au ! Specifies music on hold file

```

```
Router(config-telephony)# exit
```

Cisco Unified CME with SCCP Endpoints: Voice Mail and Auto Attendant Integration

Voice mail is provided by the Cisco Unity Express service module either in the Advanced Integration Module (AIM) form factor or the Network Module (NME) form factor. The AIM module requires the following configuration.

```
Router(config)# interface Service-Engine 0/1 ! Enters Cisco Unity Express configuration mode
Router(config-if)# ip address 10.0.2.86 255.255.255.252 ! Assigns ip address to the service engine router interface
Router(config-if)# service-module ip address 10.0.2.85 255.255.255.252 ! Assigns IP address to service module internal interface
Router(config-if)# service-module ip default-gateway 10.0.2.86 ! Assigns default gateway for the service module
Router(config-if)# zone-member security Private ! Assigns Cisco Unity Express to private security zone
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# ip route 10.0.2.884 255.255.255.252 Service-Engine 0/1 ! Adds a static route entry to direct traffic to the module
```

Cisco Unity Express uses SIP as its signaling protocol and requires a SIP dial peer.

```
Router(config)# dial-peer voice 7 voip ! Enters dial peer for voicemail configuration mode
Router(config-dial-peer)# destination-pattern 5444 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.1.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit
```

```
Router(config)# dial-peer voice 9 voip ! Enters dial peer for Auto Attendant configuration mode
Router(config-dial-peer)# destination-pattern 5000 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.2.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2 ! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify ! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit
```

The following configuration turns on the message wait indicator.

```
Router(config)# ephone-dn 19 ! Enters directory number configuration mode
Router(config-ephone-dn)# number 8000.... ! Phone number for placing MWI notification call
Router(config-ephone-dn)# mwi on ! When call placed to this DN turn MWI on

Router(config-ephone-dn)# ephone-dn 20 ! Enters directory number configuration mode
Router(config-ephone-dn)# number 8001.... ! Phone number for placing MWI notification call
Router(config-ephone-dn)# mwi off ! When call placed to this DN turn MWI off
```

Additional Cisco Unified CME configuration is performed through a Web-based user interface as shown in Figure 81 through Figure 86. Figure 81 shows the login prompt window.

Figure 81 Cisco Unified CME Login Prompt

Cisco Unity Express Initialization Wizard - Microsoft Internet Explorer

Address: <http://10.0.2.85/Web/ivw/InitWizard.do?vizAction=INIT>

Cisco Unified Communications Express
 > Discover all that is possible on the Internet.

Cisco Unity Express Initialization Wizard

Steps

1. CallManager Express Login
2. Import CCME Users
3. Defaults
4. Call Handling
5. Commit

CallManager Express Login

Enter the details of the CallManager Express that Cisco Unity Express will connect to. The user name and password will be used to authenticate while retrieving information from the CallManager Express.

Hostname *:

Web User Name *:

Web Password *:

XML User Name:

XML Password:

* indicates a mandatory field

Back Next Finish Cancel Help

Done Local intranet

250781

Figure 82 shows the Cisco Unified CME import users window.

Figure 82 Importing Cisco Unified CME Users

The screenshot shows the Cisco Unity Express Initialization Wizard in a Microsoft Internet Explorer browser window. The address bar shows the URL: http://10.0.2.85/Web/ww/InkWizard.do. The page title is "Cisco Unity Express Initialization Wizard". The Cisco logo is in the top right corner. The main heading is "Cisco Unified Communications Express" with the tagline "> Discover all that is possible on the Internet."

The wizard is in the "Import CCME Users" step. A sidebar on the left lists the steps: 1. CallManager Express Login, 2. Import CCME Users (selected), 3. Defaults, 4. Call Handling, and 5. Commit. The main content area shows a table with 3 results. The table has columns: User ID, Extension(s), Primary Extension, Mailbox, Administrator, and Set CFNA/CFB. The rows are: cisco (5001), cisco3 (5002), and cisco4 (5003). All rows have checkboxes for Mailbox, Administrator, and Set CFNA/CFB, all of which are checked. At the bottom right of the table area are buttons: Back, Next, Finish, Cancel, and Help.

☐	User ID	Extension(s)	Primary Extension	☐ Mailbox	☐ Administrator	☐ Set CFNA/CFB
☒	cisco	5001	5001	☒	☐	☒
☒	cisco3	5002	5002	☒	☐	☒
☒	cisco4	5003	5003	☒	☐	☒

250782

Figure 83 shows the Cisco Unified CME defaults window.

Figure 83 **Configuring Mailbox Defaults**

Cisco Unity Express Initialization Wizard - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address: http://10.0.2.85/Web/UnityWizard.do

Cisco Unified Communications Express
Discover all that is possible on the Internet.

Cisco Unity Express Initialization Wizard

Steps

1. CallManager Express Login
2. Import CCME Users
- 3. Defaults**
4. Call Handling
5. Commit

Defaults

Enter the defaults. These defaults are used while creating the users and mailboxes. The password is used for Web logins and PIN is used for telephone logins. Users will be prompted to change their password/PIN upon next login.

System Default Language: English (United States)

Password & PIN options

☐ Generate random password ☒ Blank password
☐ Generate random PIN ☒ Blank PIN

Mailbox Defaults

Mailbox Size *: 775 seconds

Maximum Caller Message Size *: 240 seconds

Message Expiry Time *: 30 days

* indicates a mandatory field

Back Next Finish Cancel Help

Done Local intranet

250783

Figure 84 shows the call handling configuration window.

Figure 84 **Configuring Call Handling**

The screenshot shows the Cisco Unity Express Initialization Wizard in a Microsoft Internet Explorer browser window. The address bar shows the URL: `http://10.0.2.85/Web/ww/InitWizard.do`. The page title is "Cisco Unity Express Initialization Wizard". The Cisco logo is in the top right corner.

The wizard is currently on the "Call Handling" step, which is highlighted in the left-hand "Steps" menu. The "Steps" menu includes:

1. CallManager Express Login
2. Import CCME Users
3. Defaults
- 4. Call Handling**
5. Commit

The main content area of the "Call Handling" step contains the following instructions and fields:

Enter the Call in Numbers for Voice Mail, Auto Attendant and the Administration via telephone (AVT) system.

Voice Mail Number *:	5444
Voice Mail Operator Extension:	
Auto Attendant Access Number:	5000
Auto Attendant Operator Extension:	0
Administration via Telephone Number:	
SIP MWI Notification Mechanism:	Outcalling
MWI ON Number (Outcalling mechanism):	8000...
MWI OFF Number (Outcalling mechanism):	8001...

* indicates a mandatory field

At the bottom right of the form are the navigation buttons: Back, Next, Finish, Cancel, and Help.

The status bar at the bottom of the browser window shows "Done" and "Local intranet".

250784

Figure 85 shows the Cisco Unified CME configuration verification window.

Figure 85 **Verifying Configuration**

Cisco Unity Express Initialization Wizard - Microsoft Internet Explorer

Address: <http://10.0.2.85/Web/ww/InitWizard.do>

Cisco Unified Communications Express
 > Discover all that is possible on the Internet.

Cisco Unity Express Initialization Wizard

Steps

1. CallManager Express Login
2. Import CCME Users
3. Defaults
4. Call Handling
5. **Commit**

Commit

You have chosen to set/add:

Maximum Caller Message Size:	240
Message Expiry Time:	30
Voice Mail Number:	5444
Auto Attendant Access Number:	
Voice Mail Operator Extension:	
Auto Attendant Operator Extension:	0
Administration via Telephone Number:	
SIP MWI Notification Mechanism:	Outcalling
MWI On Number:	8000....
MWI Off Number:	8001....

Click on Finish to commit the initialization. **Note:** This operation is not reversible.

☐ Finally, save to startup configuration (will take a few minutes more).

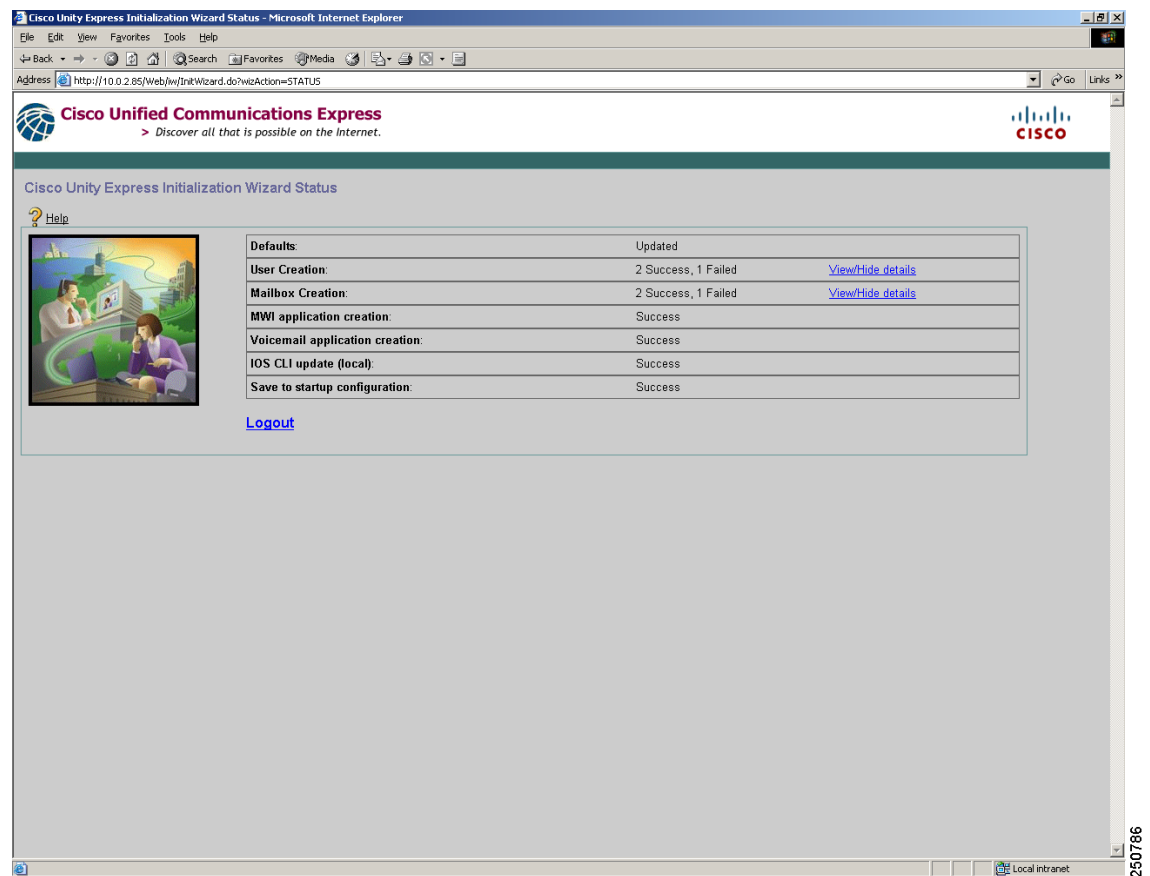
Back Next Finish Cancel Help

Done Local intranet

250785

Figure 86 shows the Cisco Unified CME configuration status window.

Figure 86 *Reviewing Configuration Status*



Cisco Unified CME with SCCP Endpoints: Emergency Services Implementation

The following is the implementation of emergency number calling for North America. The PRI trunk is used for placing emergency calls.

```
Router(config)# dial-peer voice 10 pots ! Enters dial peer for emergency calls
configuration mode
Router(config-dial-peer)# destination-pattern 911 ! Specifies North America emergency
number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

```
Router(config)# dial-peer voice 11 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# destination-pattern 9911 ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 911 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

Cisco Unified CME with SCCP Endpoints Verification

Router(config)# **show ephone phone-load**

DeviceName	CurrentPhoneload	PreviousPhoneload	LastReset
SEP796000060053	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060052	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060051	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060050	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060049	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060059	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060058	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060057	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060056	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060055	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060054	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060063	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060062	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060061	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060060	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060042	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060041	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060040	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060043	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060044	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060045	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060046	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060047	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060048	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized
SEP796000060086	SCCP41.8-3-2S	SCCP41.8-3-2S	Initialized

Router# **show telephony-service ephone-template**

```

ephone-template 1
softkeys hold Join Newcall Resume Select
softkeys idle ConfList Join Newcall Pickup Redial RmLstC
softkeys seized Redial Endcall Cfdall Pickup Callback Meetme
softkeys connected Trnsfer Hold Confrn Endcall
conference drop-mode never
conference add-mode all
conference admin: No
max-calls-per-button 8
busy-trigger-per-button 0
privacy default
Always send media packets to this router: No
Preferred codec: g711ulaw
keepalive 30 auxiliary 30
User Locale: US
Network Locale: US

```

Router# **show ephone**

```

ephone-1[0] Mac:001C.58FB.7640 TCP socket:[7] activeLine:0 REGISTERED in SCCP ver 12/9
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:12
IP:10.0.1.11 53063 7965 keepalive 126205 max_line 6
button 1: dn 1 number 5001 CH1 IDLE CH2 IDLE
Preferred Codec: g722-64

```

```

ephone-2[1] Mac:001E.4AF1.38D4 TCP socket:[-1] activeLine:0 UNREGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:7
IP:0.0.0.0 0 Unknown 0 keepalive 0 max_line 0

```

Preferred Codec: g711ulaw

ephone-3[2] Mac:001C.58F9.BD38 TCP socket:[2] activeLine:0 REGISTERED in SCCP ver 12/9
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:12
IP: 10.0.1.12 51579 7962 keepalive 126880 max_line 6
button 1: dn 2 number 5002 CH1 IDLE CH2 IDLE
Preferred Codec: g711ulaw

```
Router# show telephony-service ephone
Number of Configured ephones 180 (Registered 180)
ephone 1
Device Security Mode: Non-Secure
mac-address 001C.58FB.7640
type 7965
button 1:1
keepalive 30 auxiliary 30
max-calls-per-button 8
busy-trigger-per-button 0
ephone-template 1
Always send media packets to this router: No
Preferred codec: g711ulaw
conference drop-mode never
conference add-mode all
conference admin: No
privacy: Yes
privacy button: No
user-locale US
network-locale US
```

```
Router# show telephony-service
CONFIG (Version=4.1(0))
=====
Version 4.1(0)
Cisco Unified Communications Manager Express
For on-line documentation please see:
www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/ip_ks/index.htm

ip source-address 192.168.0.1 port 2000
max-ephones 120
max-dn 50
max-conferences 3
dspfarm units 4
dspfarm transcode sessions 3
conference software
hunt-group report delay 1 hours
hunt-group logout DND
max-redirect 5
cnf-file location: system:
cnf-file option: PER-PHONE-TYPE
network-locale[0] US (This is the default network locale for this box)
network-locale[1] US
network-locale[2] US
network-locale[3] US
network-locale[4] US
user-locale[0] US (This is the default user locale for this box)
user-locale[1] US
user-locale[2] US
user-locale[3] US
user-locale[4] US
srst mode auto-provision is OFF
srst ephone template is 0
srst dn template is 0
```

```

srst dn line mode is single
time-format 12
date-format mm-dd-yy
timezone 0 Greenwich Standard Time
no transfer-pattern is configured, transfer is restricted to local SCCP phones only.
keepalive 30 auxiliary 30
timeout interdigit 10
timeout busy 10
timeout ringing 180
timeout ringin-callerid 8
timeout night-service-bell 12
caller-id name-only: enable
web admin system name Admin
web admin customer name Customer
edit DN through Web: disabled.
edit TIME through web: disabled.
Log (table parameters):
    max-size: 150
    retain-timer: 15
transfer-system full-consult
local directory service: enabled.
Extension-assigner tag-type ephone-tag.

```

Cisco Unified CME with SIP Endpoints Implementation

- [Cisco Unified CME with SIP Endpoints: Telephony Service Setup, page 200](#)
- [Cisco Unified CME with SIP Endpoints: IP Phone Installation and Configuration, page 201](#)
- [Cisco Unified CME with SIP Endpoints: SIP Voice Gateway Implementation, page 202](#)
- [Cisco Unified CME with SIP Endpoints: Dial Plan Implementation, page 202](#)
- [Cisco Unified CME with SIP Endpoints: CAC Implementation, page 204](#)
- [Cisco Unified CME with SIP Endpoints: Transcoding Implementation, page 204](#)
- [Cisco Unified CME with SIP Endpoints: Music on Hold Implementation, page 204](#)
- [Cisco Unified CME with SIP Endpoints: Voice Mail and Auto Attendant Integration, page 205](#)
- [Cisco Unified CME with SIP Endpoints: Emergency Services Implementation, page 206](#)

Cisco Unified CME with SIP Endpoints: Telephony Service Setup

Configure the SIP gateway at the branch router.

```

Router(config)# voice service voip ! Enters voice service configuration mode
Router(config-voi-srv)# allow-connections SIP to SIP ! Enables calls from SIP endpoint to
SIP endpoint
Router(config-voi-srv)# sip ! Enters SIP configuration mode
Router(config-voi-sip)# registrar server expires max 120 min 60 ! Sets the SIP Phone
keepalive. The phone will check every 2 minutes whether it is registered with Cisco CME in
case the router lost its registration information during reboot
Router(config-voi-sip)# bind control source-interface FastEthernet0/1.2 ! Specifies SIP to
Voice VLAN binding
Router(config-voi-sip)# bind media source-interface FastEthernet0/1.2 ! Specifies SIP to
Voice VLAN binding
Router(config-voi-sip)# exit
Router(config-voi-srv)# exit

```

Cisco Unified CME with SIP Endpoints: IP Phone Installation and Configuration

In the Basic Small Branch Network, IP Phones are installed by simply connecting them to ports on the access layer switches. Because all the ports offer Power over Ethernet, no additional power cables are necessary. Once installed, phones are configured with the default configuration generated during the Cisco Unified CME installation. However, if IP Phone firmware needs to be upgraded in the future, issue the following commands.



Note

The following configuration is not required with the Cisco IOS software image used for the Basic Small Branch Network validation.

```
Router(config)# voice register global ! Enters voice register configuration mode
Router(config-register-global)# mode cme ! Enables CME mode in the register
Router(config-register-global)# load 7960-7940 POS3-08-3-00 ! Loads SIP firmware files for
7960-7940 phones
Router(config-register-global)# load 7961 SIP61.8-3-2S ! Loads SIP firmware files for 7961
phone
Router(config-register-global)# load 7962 SIP62.8-3-2S ! Loads SIP firmware files for 7962
phone
Router(config-register-global)# load 7965 SIP65.8-3-2S ! Loads SIP firmware files for 7965
phone
Router(config-register-global)# load 7971 SIP71.8-3-2S ! Loads SIP firmware files for 7971
phone

Router(config-register-global)# create profile ! Generates provisioning file
Router(config-register-global)# exit
```

To configure Cisco Unified CME with SIP endpoints from the command line, apply the following configuration.

```
Router(config)# voice register global ! Enters voice configuration mode
Router(config-register-global)# mode cme ! Enables CME mode in the register
Router(config-register-global)# max-pool 50 ! Sets the maximum number of SIP Phones
Router(config-register-global)# max-dn 100 ! Sets the maximum number of directory numbers
(two for each phone)
Router(config-register-global)# source-address 10.0.1.2 port 2000 ! Sets IP address used
for phone registration
Router(config-register-global)# dst auto-adjust ! Enables automatic adjustment of Daylight
Savings Time
Router(config-register-global)# timezone 5 ! Sets time zone to Pacific Standard/Daylight
Time
Router(config-register-global)# voicemail 5444 ! Defines number for speed dialing
voicemail from phone
Router(config-register-global)# ntp-server 172.16.0.60 ! Synchronizes clock on the phones
with the specified NTP server
Router(config-register-global)# exit
Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telphony)# secondary-dialtone 9 ! Provides dial tone for PSTN calls
Router(config-telphony)# exit
```

Apply the following configuration to all IP Phones 1 to 50. Set a unique DN number and assign the desired extension to each phone.

```
Router(config)# voice register dn 1 ! Enters directory configuration mode
Router(config-register-dn)# number 5001! Configures extension number for this directory
number
Router(config-register-dn)# call-forward b2bua busy 5444 ! Forwards calls for a busy
extension to voicemail
Router(config-register-dn)# call-forward b2bua noan 5444 timeout 10 ! Forwards calls for a
no answer extension to voicemail after 10 seconds of running
```

```
Router(config-register-dn)# call-forward b2bua mailbox 5444 ! Designates a mailbox at the
end of call forwarding
Router(config-register-dn)# mwi ! Configures Voicemail indicator
Router(config-register-dn)# exit
```

```
Router(config)# voice register pool 1 ! Enters voice register pool configuration mode
Router(config-register-pool)# id mac 00E1.CB13.0395 ! Explicitly identifies the phone
Router(config-register-pool)# type 7960 ! Defines phone type for the SIP phone being
configured. Other types are 7942, 7945, 7961, 7962, 7965, 7971
Router(config-register-pool)# number 1 dn 1 ! Associates phone 1 with directory number 1
Router(config-register-pool)# exit
```

Generate a configuration file.

```
Router(config)# voice register global ! Enters voice register configuration mode
Router(config-register-global)# create profile ! Generates provisioning file
Router(config-register-global)# reset ! Reboots the SIP phone
Router(config-register-global)# exit
```

Cisco Unified CME with SIP Endpoints: SIP Voice Gateway Implementation

The SIP voice gateway is responsible for connecting the branch VoIP network to the PSTN and to the central site telephony network. The following configuration enables VoIP on the network and sets up SIP dial peers between the branch gateway and the destination telephone networks. IP Phones are configured for SIP signaling.

```
Router(config)# voice service voip ! Enters voice service configuration mode
Router(config-voi-srv)# allow-connections SIP to h323 ! Enables calls from SIP endpoint
to h323 endpoint
Router(config-voi-srv)# allow-connections SIP to SIP ! Enables calls between SIP endpoints
```

Cisco Unified CME with SIP Endpoints: Dial Plan Implementation

Ten dial peers were defined for the Basic Small Branch Network: central site, local calls, two 911 emergency services dial peers, voicemail, Auto Attendant, long distance, international calling, and fax pass-through or fax relay. Voice mail, Auto Attendant, and emergency services dial peers are described in the “Cisco Unified CME with SIP Endpoints: Voice Mail and Auto Attendant Integration” section on page 205 and “Cisco Unified CME with SIP Endpoints: Emergency Services Implementation” section on page 206.

To provide automatic dialing without pressing the dial button, apply the following dial plan configuration.

```
Router(config)# voice register dialplan 1 ! Enters dial plan configuration mode
Router(config-register-dialplan)# type 7940-7960-others ! Specifies all phones
Router(config-register-dialplan)# pattern 1 9..... ! Matches outbound PSTN traffic
Router(config-register-dialplan)# pattern 1 4..... ! Matches central site traffic
Router(config-register-dialplan)# exit
```

```
Router(config)# voice register pool 1 ! Enters register configuration mode
Router(config-register-pool)# dialplan 1 ! Assigns dial plan to phones
Router(config-register-pool)# exit ! Assigns dial plan to phones
```

```
Router(config)# dial-peer voice 1 voip ! Enters dial peer to central site configuration
mode
Router(config-dial-peer)# session protocol sipv2 ! Enables SIP for voicemail communication
Router(config-dial-peer)# dtmf-relay rtp-nte ! Specifies Network Time Protocol method for
relaying pressed digit tones
Router(config-dial-peer)# destination-pattern 408..... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
```



```

Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit

Router(config)# dial-peer voice 2 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# destination-pattern 9..... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 3 pots ! Enters dial peer for long distance calls
configuration mode
Router(config-dial-peer)# destination-pattern 91..... ! Specifies area code prefix
for central site dial peer
Router(config-dial-peer)# prefix 1 ! Prefix that the system adds automatically to the dial
string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 4 pots ! Enters dial peer for international calls
configuration mode
Router(config-dial-peer)# destination-pattern 9011T ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 011 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

```

When calls over the WAN exceed the maximum allocated bandwidth, they are redirected to PSTN.

```

Router(config)# dial-peer voice 15 pots ! Enters dial peer for PSTN bypass configuration
mode
Router(config-dial-peer)# destination-pattern 408..... ! Specifies destination pattern
Router(config-dial-peer)# port 0/0/23 ! Specifies outgoing/incoming interface for calls
Router(config-dial-peer)# preference 1 ! Sets the dial peer preference order
Router(config-dial-peer)# prefix 408 ! Prefix that the system adds automatically to the
dial string

```

If you are using fax pass-through, apply the following configuration.

```

Router(config)# dial-peer voice 6 voip ! Enters dial peer for fax passthrough
configuration mode
Router(config-dial-peer)# session protocol sipv2 ! Enables SIP for voicemail communication
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-dial-peer)# fax protocol pass-through g711ulaw ! Configures fax passthrough
with G.711 codec
Router(config-peer)# exit

```

If you are using fax relay, apply the following configuration.

```

Router(config)# dial-peer voice 7 voip ! Enters dial peer for fax relay configuration mode
Router(config-dial-peer)# session protocol sipv2 ! Enables SIP for voicemail communication
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-dial-peer)# fax-relay ecm disable ! Disables fax relay ECM
Router(config-dial-peer)# fax rate 9600 ! Selects fax transmission rate
Router(config-dial-peer)# fax protocol t38 ! Sets the T.38 fax relay protocol

```

```
Router(config-dial-peer)# codec g711ulaw ! Configures fax relay with G.711 codec
Router(config-peer)# exit
```

Cisco Unified CME with SIP Endpoints: CAC Implementation

Resource Reservation Protocol (RSVP) is not supported with Cisco Unified CME. A limited workaround is possible by setting a limit on the number of voice calls that can be placed over the WAN.

```
Router(config)# dial-peer voice 1 voip ! Enters dial peer to central site configuration mode
Router(config-dial-peer)# max-con 36 ! Sets the maximum number of WAN based calls to 36
Router(config-dial-peer)# exit
```

Cisco Unified CME with SIP Endpoints: Transcoding Implementation

Transcoding compresses and decompresses voice streams to match end device capabilities. Transcoding is required when an incoming voice stream is digitized and compressed (by means of a codec) to save bandwidth and the local device does not support that type of compression. Conferencing is not supported with SIP and Cisco Unified CME.

```
Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telephony)# max-ephones 50 ! Sets the maximum number of phones that can register with Cisco CME
Router(config-telephony)# max-dn 100 ! Sets the maximum number of directory numbers (two for each phone)
Router(config-telephony)# sdspfarm units 4 ! Specifies number of DSP farms that can register with SCCP server
Router(config-telephony)# sdspfarm transcode sessions 5 ! Specifies maximum number of simultaneous transcoding sessions
Router(config-telephony)# sdspfarm tag 3 TRANSCODE ! Creates DSP farm profile
Router(config-telephony)# exit

Router(config)# voice-card 0 ! Enters DSP farm configuration mode
Router(config-voicecard)# dsp services dspfarm ! Enables DSP services
Router(config-voicecard)# exit

Router(config)# dspfarm profile 3 ! Enters DSP farm profile configuration mode
Router(config-dspfarm-profile)# codec g711ulaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g711alaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729ar8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729abr8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729r8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec pass-through ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# maximum sessions 5 ! Specifies maximum number of simultaneous sessions supported by this profile
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit
```

Cisco Unified CME with SIP Endpoints: Music on Hold Implementation

MOH is an audio stream that is played to PSTN and VoIP G.711 or G.729 callers who are placed on hold by phones in a Cisco Unified CME system. This audio stream is intended to reassure callers that they are still connected to their calls.

```
Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telephony)# moh music-on-hold.au ! Specifies music on hold file
Router(config-telephony)# exit
```

Cisco Unified CME with SIP Endpoints: Voice Mail and Auto Attendant Integration

Voice mail is provided by the Cisco Unity Express service module either in the Advanced Integration Module (AIM) form factor or the Network Module (NME) form factor. The AIM module requires the following configuration.

```
Router(config)# interface Service-Engine 0/1 ! Enters Cisco Unity Express configuration mode
Router(config-if)# ip address 10.0.2.86 255.255.255.252 ! Assigns ip address to the service engine router interface
Router(config-if)# service-module ip address 10.0.2.85 255.255.255.252 ! Assigns IP address to service module internal interface
Router(config-if)# service-module ip default-gateway 10.0.2.86 ! Assigns default gateway for the service module
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# ip route 10.0.2.84 255.255.255.252 Service-Engine 0/1 ! Adds a static route entry to direct traffic to the module
```

Configure a dial peer for voice mail, because Cisco Unity Express uses SIP as its signaling protocol.

```
Router(config)# dial-peer voice 8 voip ! Enters dial peer for voicemail configuration mode
Router(config-dial-peer)# destination-pattern 5444 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.2.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify ! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit
```

```
Router(config)# dial-peer voice 9 voip ! Enters dial peer for autoattendant configuration mode
Router(config-dial-peer)# destination-pattern 5000 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.2.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit
```

```
Router(config)# sip-ua ! Enters SIP user agent configuration mode
Router(config-sip-ua)# mwi-server ipv4:172.16.0.110 expires 3600 port 5060 transport udp ! Sets Cisco Unified Manager address for providing message wait indicator
Router(config-voi-sip)# exit
```

```
Router# service-module Service-Engine 0/1 session ! Sessions into the CUE service module
```

```
CUE(config)# ccn application voicemail ! Enters voicemail configuration mode
CUE(config-application)# description "Cisco Voicemail" ! Sets user friendly name for voicemail application
CUE(config-application)# maxsessions 4 ! Sets maximum number of users concurrently listening to voicemail
CUE(config-application)# exit
```

```
CUE(config)# ccn trigger sip phonenummer 5444 ! Assigns number that will trigger voicemail
CUE(config-trigger)# application voicemail ! Assigns voicemail to the call trigger
CUE(config-trigger)# enabled ! Turns the trigger on
CUE(config-trigger)# maxsessions 4 ! Sets maximum number of users concurrently listening to voicemail
CUE(config-trigger)# exit
CUE(config)# exit
```

Create user mailboxes. Repeat the following steps for all users.

```
CUE# username John create ! Creates mailbox for user John
CUE# configure terminal
CUE(config)# username John phonenumber 5001 ! Assigns mailbox for John to extension
CUE(config)# exit

CUE# configure terminal
CUE(config)# voice mailbox owner John ! Enters configuration mode for voicemail mailbox
CUE(config-mailbox)# description "John's Mailbox" ! Sets user friendly description
CUE(config-mailbox)# enable ! Turns the mailbox on
CUE(config-mailbox)# expiration time 14 ! Sets expiration time for voicemail to two weeks
CUE(config-mailbox)# mailboxsize 600 ! Sets voicemail box size to 10 minutes of messages
CUE(config-mailbox)# messagesize 120 ! Sets maximum message size to 2 minutes
CUE(config-mailbox)# exit
```

Cisco Unified CME with SIP Endpoints: Emergency Services Implementation

The following is the implementation of emergency number calling for North America. The PRI trunk is used for placing emergency calls.

```
Router(config)# dial-peer voice 10 pots ! Enters dial peer for emergency calls
configuration mode
Router(config-dial-peer)# destination-pattern 911 ! Specifies North America emergency
number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 11 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# destination-pattern 9911 ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 911 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

Cisco Unified SRST with SCCP Endpoints Implementation

- [Cisco Unified SRST with SCCP Endpoints: Telephony Service Setup, page 207](#)
- [Cisco Unified SRST with SCCP Endpoints: IP Phone Installation and Configuration, page 208](#)
- [Cisco Unified SRST with SCCP Endpoints: H.323 Voice Gateway Implementation, page 209](#)
- [Cisco Unified SRST with SCCP Endpoints: Dial Plan Implementation, page 211](#)
- [Cisco Unified SRST with SCCP Endpoints: RSVP Implementation, page 213](#)
- [Cisco Unified SRST with SCCP Endpoints: Transcoding and Conferencing Implementation, page 214](#)
- [Cisco Unified SRST with SCCP Endpoints: Music on Hold Implementation, page 216](#)
- [Cisco Unified SRST with SCCP Endpoints: Voice Mail and Auto Attendant Integration, page 216](#)
- [Cisco Unified SRST with SCCP Endpoints: Emergency Services Implementation, page 217](#)

Cisco Unified SRST provides Cisco Unified CM with fallback support for Cisco IP Phones that are attached to a Cisco router on a branch network. Cisco Unified SRST enables routers to provide call-handling support for Cisco IP Phones when they lose connection to a remote primary, secondary, or tertiary Cisco Unified CM, or when WAN connection is operationally down.

Cisco Unified SRST with SCCP Endpoints: Telephony Service Setup

Configure Cisco Unified SRST at the central site Cisco Unified CM as shown in Figure 87. The Cisco Unified SRST reference name is used in configuring the Cisco Unified SRST device pool as shown in Figure 88.

Figure 87 Cisco Unified SRST Configuration in Cisco Unified CM

SOLUTIONS-UNITY
SRST Reference Configuration - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print

https://172.16.200.10/ccmadmin/srstSave.do

Cisco Unified CallManager Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified CMAdmin

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help

SRST Reference Configuration Related Links

Save Delete Copy Reset Add New

Status
Update successful

SRST Reference Information

Name* BRANCH-SRST

Port* 2000

IP Address* 10.0.1.2

SIP Network/IP Address 10.0.1.2

SIP Port* 5060

SRST Certificate Provider Port* 2445

☐ Is SRST Secure?

Save Delete Copy Reset Add New

***** - indicates required item.

251035

Figure 88 Cisco Unified SRST Device Pool Configuration in Cisco Unified CM

Configure the Cisco Unified SRST fallback mode at the branch router.

```
Router(config)# call-manager-fallback ! Enters call manager fallback configuration mode
Router(config-cm-fallback)# ip source-address 10.0.1.2 port 2000 ! Sets IP address for
phone registration
Router(config-cm-fallback)# max-dn 480 dual-line ! Sets the maximum number of directory
numbers and configures dual channel
Router(config-cm-fallback)# max-ephones 50 ! Sets the maximum number of IP Phones
Router(config-cm-fallback)# exit
```

Cisco Unified SRST with SCCP Endpoints: IP Phone Installation and Configuration

In the Basic Small Branch Network, IP Phones are installed by simply connecting them to ports on the access layer switches. Because all the ports offer Power over Ethernet, no additional power cables are necessary. After installation, the phones are configured with a default configuration generated during the telephony setup in the previous section.

```
Router(config)# clock timezone PST -8 ! Sets the timezone for display on IP Phones
Router(config)# call-manager-fallback ! Enters call manager fallback configuration mode
Router(config-cm-fallback)# user-locale US ! Sets the language for display on IP Phones
Router(config-cm-fallback)# system message primary Your current options ! Sets message for
display on IP Phones
Router(config-cm-fallback)# secondary-dialtone 9 ! Provides dial tone for PSTN calls
Router(config-cm-fallback)# call-forward busy 5444 ! Forwards busy calls to voicemail
Router(config-cm-fallback)# call-forward noan 5444 timeout 10 ! Forwards busy calls to
voicemail after 10 minutes of ringing
```

```

Router(config-cm-fallback)# dialplan-pattern 1 408555.... extension-length 4 ! Creates
dialplan pattern that expands extension numbers to full E.164 numbers
Router(config-cm-fallback)# transfer-system full-blind ! Transfers calls without
consultation
Router(config-cm-fallback)# transfer-pattern 9..... ! Allows transfers for all calls
originating from PSTN
Router(config-cm-fallback)# transfer-pattern 4..... ! Allows transfers for all calls
originating in area code starting with "4"
Router(config-cm-fallback)# transfer-system full-consult ! Consults call before transfer
on second line
Router(config-cm-fallback)# call-forward pattern .T ! Allows call forwarding for all calls

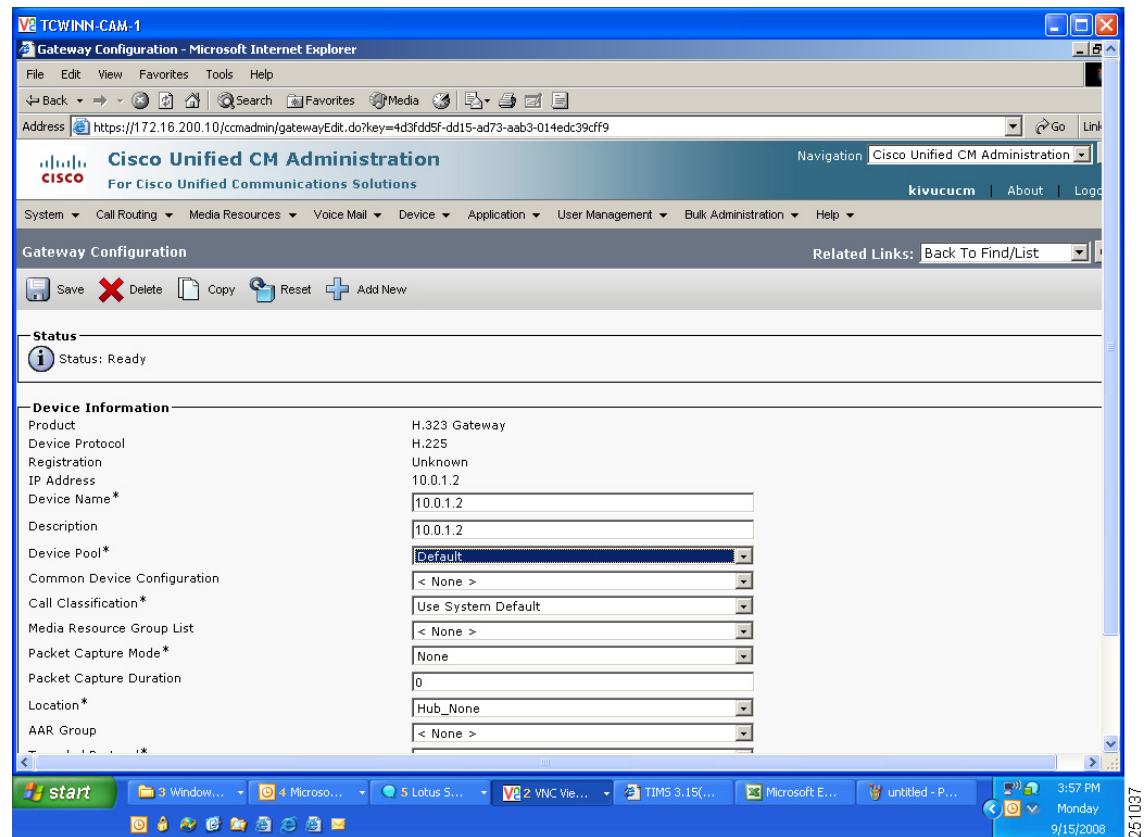
Router(config-cm-fallback)# exit

```

Cisco Unified SRST with SCCP Endpoints: H.323 Voice Gateway Implementation

The following configuration enables VoIP on the network and sets up H.323 dial peers between the branch gateway and the destination telephone network, as shown in [Figure 89](#), [Figure 90](#), and [Figure 91](#).

Figure 89 H.323 Gateway Cisco Unified CM Configuration



251037

Figure 90 *H.323 Gateway Cisco Unified CM Configuration 2?*

TCWINN-CAM-1
Gateway Configuration - Microsoft Internet Explorer

Address: <https://172.16.200.10/ccmadmin/gatewayEdit.do?key=4d3fdd5f-dd15-ad73-aab3-014edc39cff9>

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | kivucum | About | Log

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Administration | Help

Gateway Configuration Related Links: Back To Find/List

Save Delete Copy Reset Add New

AAR Group: < None >

Tunneled Protocol*: None

Signaling Port*: 1720

☐ Media Termination Point Required

☒ Retry Video Call As Audio

☐ Wait for Far End H.245 Terminal Capability Set

☐ Path Replacement Support

☐ Transmit UTF-8 for Calling Party Name

☐ SRTP Allowed - When this flag is checked, IPSec needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

Multilevel Precedence and Preemption (MLPP) Information

MLPP Domain: < None >

MLPP Indication: Not available on this device

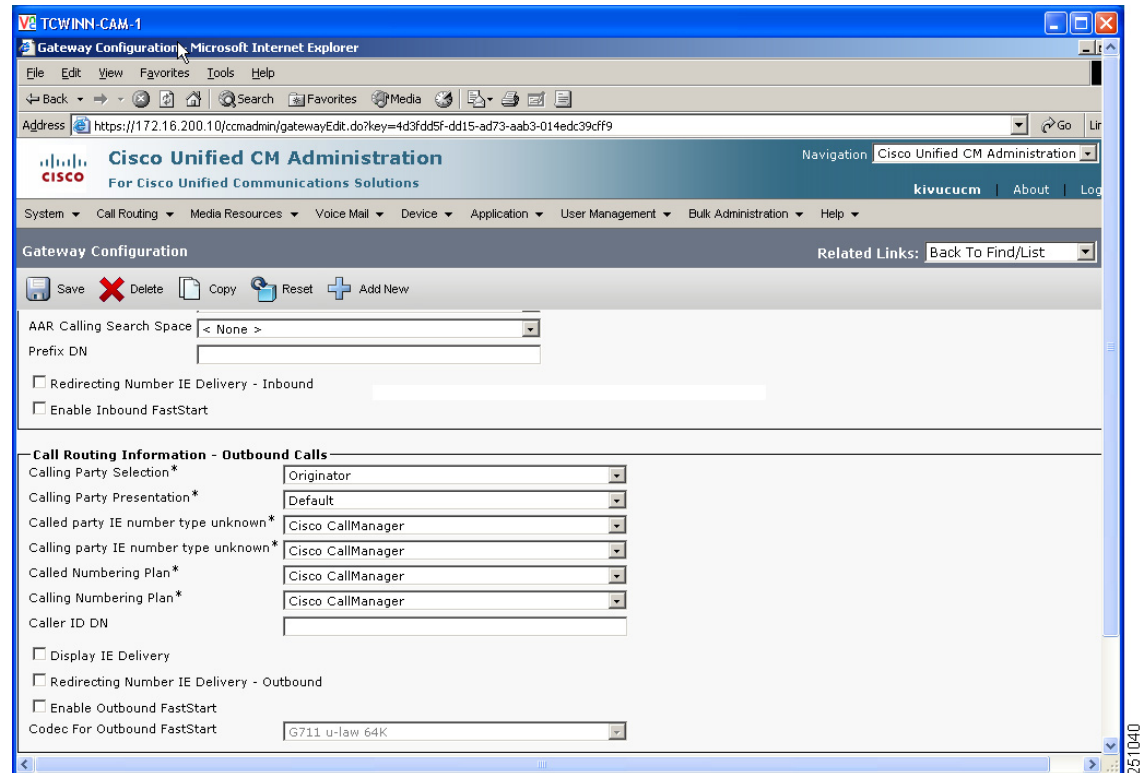
MLPP Preemption: Not available on this device

Call Routing Information - Inbound Calls

Significant Digits*: All

Calling Search Space: BRANCH

251038

Figure 91 H.323 Gateway Cisco Unified CM Configuration for Cisco Unified SRST Mode

Cisco Unified SRST with SCCP Endpoints: Dial Plan Implementation

Twelve dial peers were defined for the Basic Small Branch Network:

- Central site WAN
- Central site PSTN
- Local calls
- Four 911 emergency services dial peers
- Voice mail
- Auto Attendant
- Long distance
- International calling
- Fax pass through or fax relay

Voice mail and emergency services dial peers are described in the “Cisco Unified SRST with SCCP Endpoints: Voice Mail and Auto Attendant Integration” section on page 216 and the “Cisco Unified SRST with SCCP Endpoints: Emergency Services Implementation” section on page 217.

```
Router(config)# dial-peer voice 1 pots ! Enters dial peer for central site calls
Router(config-dial-peer)# destination-pattern 5.... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 1408555 ! Prefix that the system adds automatically to
the dial string
```

```
Router(config-dial-peer)# incoming called-number .T ! Associates dial peer with any
incoming number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

When calls over the WAN exceed the maximum allocated bandwidth, they are redirected to PSTN.

```
Router(config)# dial-peer voice 15 pots ! Enters dial peer for PSTN bypass configuration
mode
Router(config-dial-peer)# destination-pattern 408..... ! Specifies destination pattern
Router(config-dial-peer)# port 0/0/23 ! Specifies outgoing/incoming interface for calls
Router(config-dial-peer)# preference 1 ! Sets the dial peer preference order
Router(config-dial-peer)# prefix 408 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# exit
```

```
Router(config)# dial-peer voice 2 voip ! Enters dial peer to central site configuration
mode
Router(config-dial-peer)# dtmf-relay h245-alphanumeric ! Specifies H.245 method for
relaying pressed digit tones
Router(config-dial-peer)# destination-pattern 408..... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-peer)# exit
```

```
Router(config)# dial-peer voice 3 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# destination-pattern 9..... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

```
Router(config)# dial-peer voice 4 pots ! Enters dial peer for long distance calls
configuration mode
Router(config-dial-peer)# destination-pattern 91..... ! Specifies area code prefix
for central site dial peer
Router(config-dial-peer)# prefix 1 ! Prefix that the system adds automatically to the dial
string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

```
Router(config)# dial-peer voice 5 pots ! Enters dial peer for international calls
configuration mode
Router(config-dial-peer)# destination-pattern 9011T ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 011 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

If using fax pass-through, apply the following configuration.

```
Router(config)# dial-peer voice 6 voip ! Enters dial peer for fax passthrough
configuration mode
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
```

```
Router(config-dial-peer)# fax protocol pass-through g711ulaw ! Configures fax passthrough
with G.711 codec
Router(config-peer)# exit
```

If using fax relay, apply the following configuration.

```
Router(config)# dial-peer voice 7 voip ! Enters dial peer for fax relay configuration mode
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-dial-peer)# fax-relay ecm disable ! Disables fax relay ECM
Router(config-dial-peer)# fax rate 9600 ! Selects fax transmission rate
Router(config-dial-peer)# fax protocol t38 ! Sets the T.38 fax relay protocol
Router(config-dial-peer)# codec g711ulaw ! Configures fax relay with G.711 codec
Router(config-peer)# exit
```

Cisco Unified SRST with SCCP Endpoints: RSVP Implementation

The following implementation applies to Cisco Unified SRST branch voice deployments. Use the following commands on the tunnel interface for DMVPN, WAN primary, and on the WAN interface for GETVPN.



Note

On the four T1 WAN links, the maximum bandwidth that can be managed by RSVP is 4550 kbps.

```
Router(config)# interface Tunnel 1 ! Enters tunnel interface configuration mode
Router(config-if)# ip rsvp bandwidth 8112 ! Sets maximum allowed bandwidth for voice (see
Table 20) plus video (512 kb/s)
Router(config-if)# ip rsvp data-packet classification none ! Turns off per-packet data
processing
Router(config-if)# ip rsvp resource-provider none ! Specifies no resource provider for the
traffic flows
Router(config-if)# ip rsvp policy local identity RSVP-VOICE ! Creates RSVP policy for
voice
Router(config-rsvp-local-policy)# maximum bandwidth group 7600 ! Sets maximum bandwidth for
voice
Router(config-rsvp-local-policy)# forward all ! Forwards all traffic for this policy
Router(config-rsvp-local-policy)# exit
Router(config-if)# ip rsvp policy local identity RSVP-VIDEO ! Creates RSVP policy for
video
Router(config-rsvp-local-policy)# maximum bandwidth group 512 ! Sets maximum bandwidth for
video
Router(config-rsvp-local-policy)# forward all ! Forwards all traffic for this policy
Router(config-rsvp-local-policy)# exit
Router(config-if)# ip rsvp policy local default ! Default policy for traffic that does not
matchin above identifiers
Router(config-if)# exit
```

```
Router(config)# ip rsvp policy identity RSVP-VIDEO policy-locator .*VideoStream.* !
Creates a policy for matching video traffic
Router(config)# ip rsvp policy identity RSVP-VOICE policy-locator .*AudioStream.* !
Creates a policy for matching voice traffic
Router(config)# ip rsvp policy preempt ! Enables preempting of lower reservation by higher
reservation
```

The RSVP policy must be applied on the voice VLAN interface.

```
Branch(config)# interface FastEthernet0/1.2 ! Enters gigabit Ethernet sub-interface 2
configuration mode
Router(config-if)# ip rsvp bandwidth ! Enables RSVP on the interface
```

```
Router(config-if)# exit
```

Cisco Unified SRST with SCCP Endpoints: Transcoding and Conferencing Implementation

Transcoding compresses and decompresses voice streams to match end device capabilities. Transcoding is required when an incoming voice stream is digitized and compressed (by means of a codec) to save bandwidth and the local device does not support that type of compression.

```
Router(config)# call-manager-fallback ! Enters call manager fallback configuration mode
Router(config-cm-fallback)# max-conferences 3 ! Specifies the maximum number of
simultaneous conferences
Router(config-cm-fallback)# exit

Router(config)# voice-card 0 ! Enters DSP farm configuration mode
Router(config-voicecard)# dsp services dspfarm ! Enables DSP services
Router(config-voicecard)# exit
Router(config)# sccp local GigabitEthernet0/1.2 ! Sets the interface for conferencing and
transcoding to register with CME
Router(config)# sccp ccm 10.0.1.2 identifier 1 version 5.0.1 ! Associates conferencing and
transcoding with CME
Router(config)# sccp ! Enables SCCP globally
Router(config)# sccp ccm group 1 ! Creates SCCP group and enters SCCP configuration mode
Router(config-sccp-ccm)# associate ccm 1 priority 1 ! Associates SCCP group 1 with CME
Router(config-sccp-ccm)# associate profile 3 register CONFERENCE ! Associates DSP farm
profile with with a SCCP group
Router(config-sccp-ccm)# associate profile 2 register TRANSCODE ! Associates DSP farm
profile with with a SCCP group
Router(config-sccp-ccm)# exit

Router(config)# dspfarm profile 2 transcode ! Enters DSP farm profile configuration mode
Router(config-dspfarm-profile)# codec g711ulaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g711alaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729ar8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729abr8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729r8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec pass-through ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# maximum sessions 5 ! Specifies maximum number of
simultaneous sessions supported by this profile
Router(config-dspfarm-profile)# associate application sccp ! Associates SCCP with this DSP
farm profile
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit

Router(config)# dspfarm profile 3 conference ! Enters DSP farm profile configuration mode
Router(config-dspfarm-profile)# codec g711ulaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g711alaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729ar8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729abr8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729r8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729br8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# maximum sessions 3 ! Specifies maximum number of
simultaneous sessions supported by this profile
Router(config-dspfarm-profile)# associate application sccp ! Associates SCCP with this DSP
farm profile
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit
```

Transcoding and conferencing are configured on the remote Cisco Unified CM as shown in [Figure 92](#) and [Figure 93](#).

Figure 92 **Transcoding Configuration for Cisco Unified SRST Mode**

The screenshot shows a web browser window titled "TCWJINN-CAM-1" displaying the "Transcoder Configuration" page in Microsoft Internet Explorer. The address bar shows the URL: `https://172.16.200.10/ccmadmin/transcoderEdit.do?key=7793fc30-a7f5-3ef1-642b-13590da6fff9`. The page header includes the Cisco logo and "Cisco Unified CM Administration For Cisco Unified Communications Solutions". A navigation menu contains: System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The main section is titled "Transcoder Configuration" and includes buttons for Save, Delete, Copy, Reset, and Add New. Below this is the "Transcoder Information" section, which displays the following details:

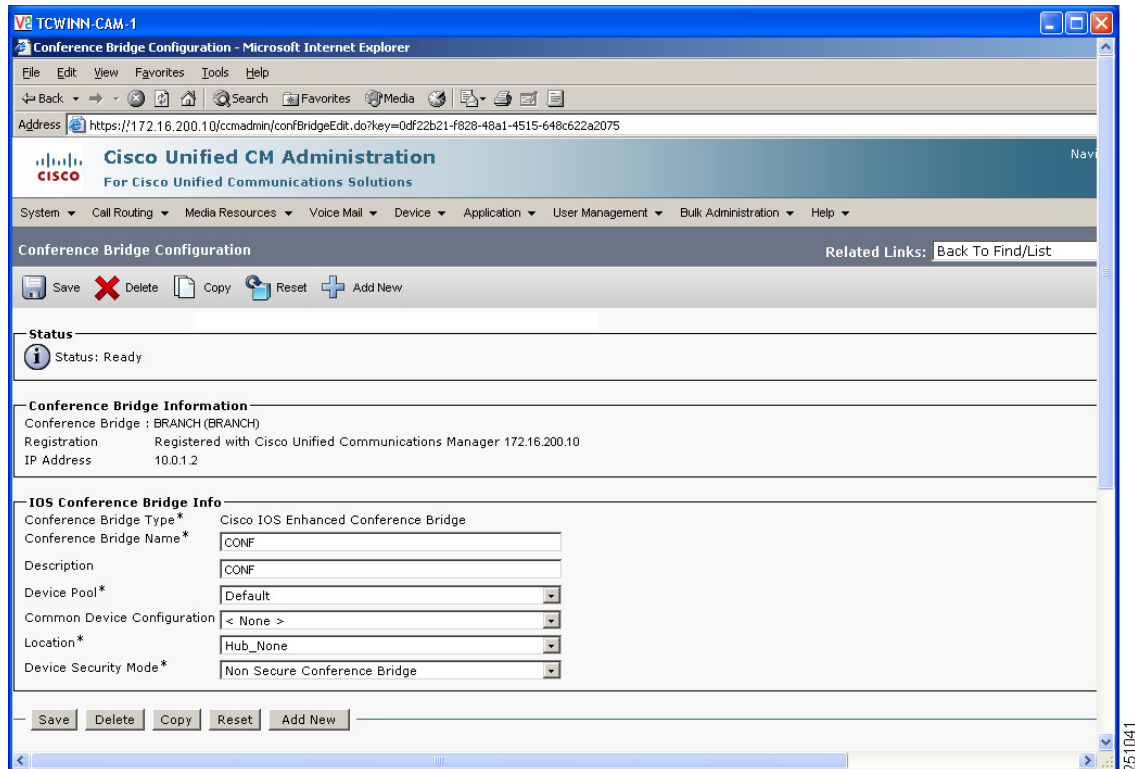
- Transcoder:** BRANCH (BRANCH)
- Registration:** Registered with Cisco Unified Communications Manager 172.16.200.10
- IP Address:** 10.0.1.2

The "IOS Transcoder Info" section contains the following fields:

- Transcoder Type*:** Cisco IOS Enhanced Media Termination Point
- Description:** XCODE
- Device Name*:** XCODE
- Device Pool*:** Default (with a "View Details" link)
- Common Device Configuration:** < None > (with a "View Details" link)
- Special Load Information:** (with a note: "Leave blank to use default")

At the bottom of the form are buttons for Save, Delete, Copy, Reset, and Add New. A note at the bottom left states: "i *- indicates required item."

251041

Figure 93 Conferencing Configuration for Cisco Unified SRST Mode

Cisco Unified SRST with SCCP Endpoints: Music on Hold Implementation

Music on hold (MOH) is an audio stream that is played to PSTN and VoIP G.711 or G.729 callers who are placed on hold by phones in a Cisco Unified CME system. This audio stream is intended to reassure callers that they are still connected to their calls.

```
Router(config)# call-manager-fallback ! Enters call manager fallback configuration mode
Router(config-cm-fallback)# moh music-on-hold.au ! Specifies music on hold file
Router(config-cm-fallback)# multicast moh 239.1.1.1 port 16384 ! Uses multicast for MoH
Router(config-cm-fallback)# exit
```

Cisco Unified SRST with SCCP Endpoints: Voice Mail and Auto Attendant Integration

Voice mail is provided by the Cisco Unity Express service module either in the Advanced Integration Module (AIM) form factor or the Network Module (NME) form factor. The AIM module requires the following configuration.

```
Router(config)# interface service-engine 0/1 ! Enters Cisco Unity Express configuration mode
Router(config-if)# ip address 10.0.2.86 255.255.255.252 ! Assigns ip address to the service engine router interface
Router(config-if)# service-module ip address 10.0.2.85 255.255.255.252 ! Assigns IP address to service module internal interface
Router(config-if)# service-module ip default-gateway 10.0.2.86 ! Assigns default gateway for the service module
Router(config-if)# zone-member security Private ! Assigns Cisco Unity Express to private security zone
Router(config-if)# no shutdown
Router(config-if)# exit
```

```
Router(config)# ip route 10.0.2.84 255.255.255.252 Service-Engine 0/1 ! Adds a static
route entry to direct traffic to the module
```

Configure a dial peer for voice mail because Cisco Unity Express uses SIP as its signaling protocol.

```
Router(config)# dial-peer voice 8 voip ! Enters dial peer for voicemail configuration mode
Router(config-dial-peer)# destination-pattern 5444 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.2.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit
```

```
Router(config)# dial-peer voice 9 voip ! Enters dial peer for autoattendant configuration
mode
Router(config-dial-peer)# destination-pattern 5000 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.2.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit
```

The local Cisco Unity Express software must be registered with the Cisco Unified CM software at the central site. The following reference provides implementation details:

http://cisco.com/en/US/products/sw/voicesw/ps5520/products_configuration_example09186a0080289ef0.shtml

Additional Cisco Unity Express configuration is performed through a web-based user interface, as shown in Figure 81 through Figure 86.

Cisco Unified SRST with SCCP Endpoints: Emergency Services Implementation

The following provides implementation of emergency number calling for North America. The PRI trunk is used to place emergency calls. Each 911 call is selectively routed to the closest Public Safety Answering Point (PSAP), based on the caller's location. In addition, the caller's phone number and address automatically display on a terminal at the PSAP. The PSAP can quickly dispatch emergency help, even if the caller is unable to communicate the caller's location. Also, if the caller disconnects prematurely, the PSAP has the information it needs to contact the 911 caller.

```
Router(config)# voice emergency response location 1 ! Enters emergency response
configuration mode
Router(cfg-emrgncy-resp-location)# elin 1 4085555150 ! Specifies ELIN number provided by
PSAP
Router(cfg-emrgncy-resp-location)# name Bldg 22, Floor 2 ! Internal location name
Router(cfg-emrgncy-resp-location)# subnet 1 10.0.1.0 255.255.255.0 ! Assigns Voice VLAN
subnet as origination of the emergency call
Router(cfg-emrgncy-resp-location)# subnet 2 10.0.4.0 255.255.255.0 ! Assigns backup Voice
VLAN subnet as origination of the emergency call
Router(cfg-emrgncy-resp-location)# exit

Router(config)# dial-peer voice 10 pots ! Enters dial peer for emergency calls
configuration mode
Router(config-dial-peer)# emergency response zone ! Replaces local extension with ELIN
number
Router(config-dial-peer)# destination-pattern 911 ! Specifies North America emergency
number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
```



```

Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 11 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# emergency response zone ! Replaces local extension with ELIN
number
Router(config-dial-peer)# destination-pattern 9911 ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 911 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 12 pots ! Enters dial peer for ELIN callback configuration
mode
Router(config-dial-peer)# incoming called-number 4085555150 ! Specifies ELIN number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# emergency response callback ! Identifies the ELIN dial peer
Router(config-peer)# exit

Router(config)# dial-peer voice 13 pots ! Enters dial peer for ELIN callback configuration
mode
Router(config-dial-peer)# incoming called-number 4085555150 ! Specifies ELIN number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# emergency response callback ! Identifies the ELIN dial peer
Router(config-peer)# exit

```

Cisco Unified SRST with SIP Endpoints Implementation

- [Cisco Unified SRST with SIP Endpoints: Telephony Service Setup, page 218](#)
- [Cisco Unified SRST with SIP Endpoints: Cisco Unified SRST Fallback Mode at the Branch Router, page 220](#)
- [Cisco Unified SRST with SIP Endpoints: IP Phone Installation and Configuration, page 221](#)
- [Cisco Unified SRST with SIP Endpoints: SIP Voice Gateway Implementation, page 221](#)
- [Cisco Unified SRST with SIP Endpoints: Dial Plan Implementation, page 223](#)
- [Cisco Unified SRST with SIP Endpoints: RSVP Implementation, page 225](#)
- [Cisco Unified SRST with SIP Endpoints: Transcoding and Conferencing Implementation, page 225](#)
- [Cisco Unified SRST with SIP Endpoints: Music on Hold Implementation, page 228](#)
- [Cisco Unified SRST with SIP Endpoints: Voice Mail and Auto Attendant Integration, page 228](#)
- [Cisco Unified SRST with SIP Endpoints: Emergency Services Implementation, page 229](#)

Cisco Unified SRST provides Cisco Unified CM with fallback support for Cisco IP Phones that are attached to a Cisco router on a branch network. Cisco Unified SRST enables routers to provide call-handling support for Cisco IP Phones when they lose connection to a remote primary, secondary, or tertiary Cisco Unified CM, or when WAN connection is operationally down.

Cisco Unified SRST with SIP Endpoints: Telephony Service Setup

Configure the Cisco Unified SRST at Cisco Unified CM of the central site, as shown in [Figure 94](#). The Cisco Unified SRST reference name is used in configuring Cisco Unified SRST device pools as shown in [Figure 95](#).

Figure 94 Cisco Unified SRST Configuration in Cisco Unified CM

SOLUTIONS-UNITY
SRST Reference Configuration - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Search Favorites Media Print

https://172.16.200.10/ccmadmin/srstSave.do

Cisco Unified CallManager Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified CMAdmin

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help

SRST Reference Configuration Related Link

Save Delete Copy Reset Add New

Status
Update successful

SRST Reference Information

Name*	BRANCH-SRST
Port*	2000
IP Address*	10.0.1.2
SIP Network/IP Address	10.0.1.2
SIP Port*	5060
SRST Certificate Provider Port*	2445
☐ Is SRST Secure?	

Save Delete Copy Reset Add New

* - indicates required item.

251042

Figure 95 Cisco Unified SRST Device Pool Configuration in Cisco Unified CM

Device Pool Configuration - Microsoft Internet Explorer

Address: <https://172.16.200.10/ccmadmin/devicePoolEdit.do?key=5286511a-eedd-d12b-f518-110d5ed8952>

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Administration | Help

Device Pool Configuration Related Links: Back To Find/List | Go

Save Delete Copy Reset Add New

Status
Status: Ready

Device Pool Information
Device Pool: BRANCH-POOL (7 members)**

Device Pool Settings
 Device Pool Name*: BRANCH-POOL
 Cisco Unified Communications Manager Group*: Default
 Calling Search Space for Auto-registration: < None >
 Reverted Call Focus Priority: Default

Roaming Sensitive Settings
 Date/Time Group*: CMLocal
 Region*: BRANCH
 Media Resource Group List: BRANCH
 Location: Branch
 Network Locale: United States
 SRST Reference*: BRANCH-SRST
 Connection Monitor Duration**:
 Single Button Barge*: Default
 Join Across Lines*: Default
 Physical Location: < None >
 Device Mobility Group: < None >

Device Mobility Related Information****
 Device Mobility Calling Search Space: < None >
 AAR Calling Search Space: < None >
 AAR Group: < None >

Save Delete Copy Reset Add New

*: indicates required item.

Done Local intranet

Cisco Unified SRST with SIP Endpoints: Cisco Unified SRST Fallback Mode at the Branch Router

```

Router(config)# voice register global ! Enters voice configuration mode
Router(config-register-global)# max-pool 50 ! Sets the maximum number of SIP Phones
Router(config-register-global)# max-dn 100 ! Sets the maximum number of directory numbers
(two for each phone)
Router(config-register-global)# system message Your current options ! Sets message for
display on IP Phones
Router(config-register-global)# dialplan-pattern 1 4085555... extension-length 4 ! Creates
dialplan pattern that expands extension numbers to full E.164 numbers
Router(config-register-global)# exit

Router(config)# voice register pool 1 ! Enters voice register pool configuration mode
Router(config-register-pool)# id network 10.0.1.0 255.255.255.0 ! Identifies Voice VLAN
with SIP Phones
Router(config-register-pool)# proxy 172.16.0.20 preference 1 monitor probe icmp-ping !
Defines remote proxy dial peer and method to monitor the state of the peer
Router(config-register-pool)# call-forward b2bua busy 5444 ! Forwards busy calls to
voicemail
Router(config-register-pool)# call-forward b2bua noan 5444 timeout 10 ! Forwards busy
calls to voicemail after 10 minutes of ringing
Router(config-register-pool)# codec g711ulaw ! Sets the codec for local calls
Router(config-register-pool)# exit

```

Cisco Unified SRST with SIP Endpoints: IP Phone Installation and Configuration

In Cisco Unified SRST mode, the Cisco Unified CM controls IP Phone firmware installation and configuration.

Cisco Unified SRST with SIP Endpoints: SIP Voice Gateway Implementation

The following configuration enables VoIP on the network and sets up SIP dial peers between the branch gateway and the destination telephone networks, as shown in [Figure 96](#), [Figure 97](#), and [Figure 98](#).

Figure 96 *SIP Trunk Cisco Unified CM Configuration (1 of 3)*

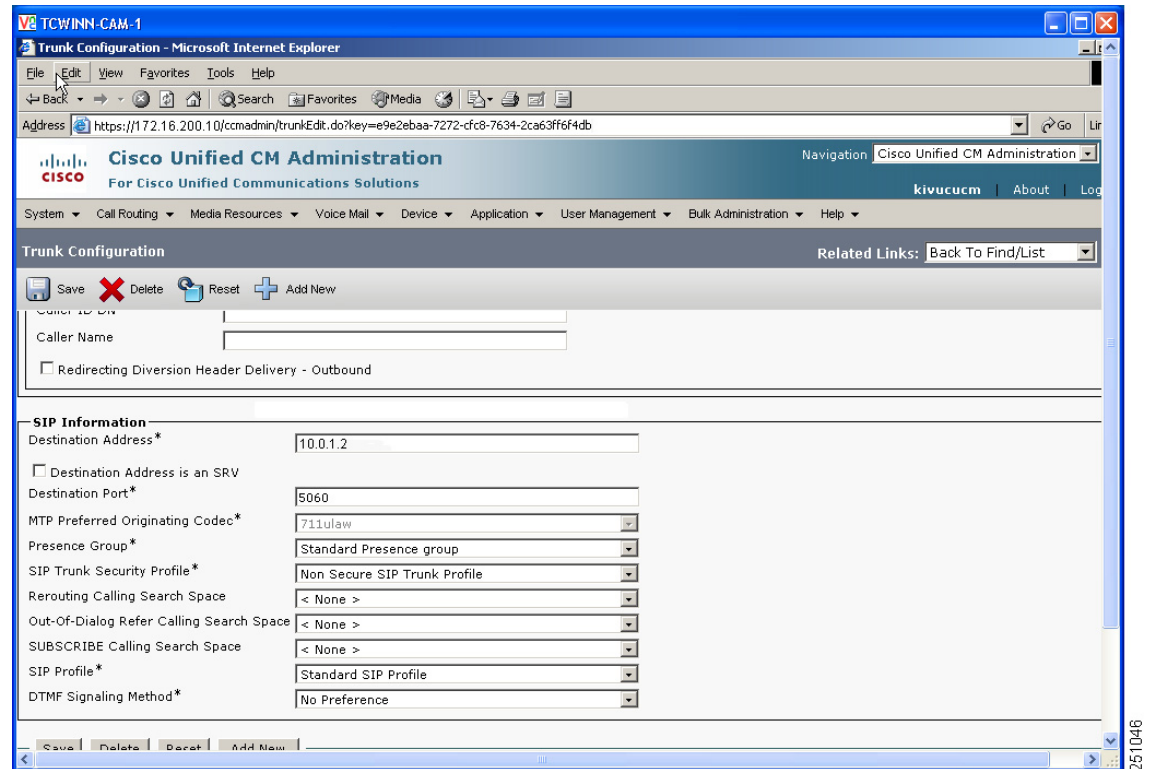
The screenshot shows the Cisco Unified CM Administration web interface in a Microsoft Internet Explorer browser window. The page title is "Trunk Configuration - Microsoft Internet Explorer". The address bar shows the URL: <https://172.16.200.10/ccadmin/trunkEdit.do?key=e9e2ebaa-7272-cfc8-7634-2ca63ff6f4db>. The page header includes the Cisco logo and "Cisco Unified CM Administration For Cisco Unified Communications Solutions". The navigation menu includes System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The main content area is titled "Trunk Configuration" and shows the "SIP Trunk" configuration form. The form includes the following fields and values:

- Product: SIP Trunk
- Device Protocol: SIP
- Device Name*: 10.0.1.2
- Description: (empty)
- Device Pool*: Default
- Common Device Configuration: < None >
- Call Classification*: Use System Default
- Media Resource Group List: < None >
- Location*: Hub_None
- AAR Group: < None >
- Packet Capture Mode*: None
- Packet Capture Duration: 0
- ☐ Media Termination Point Required
- ☒ Retrv Viden Call as Audin

At the bottom right of the browser window, the text "251044" is visible.

Figure 97 SIP Trunk Cisco Unified CM Configuration (2 of 3)

The screenshot shows the Cisco Unified CM Administration web interface in Microsoft Internet Explorer. The browser address bar displays the URL: <https://172.16.200.10/ccmadmin/trunkEdit.do?key=e9e2ebaa-7272-cfc8-7634-2ca63ff6f4db>. The page title is 'Trunk Configuration - Microsoft Internet Explorer'. The Cisco logo and 'Cisco Unified CM Administration' text are visible at the top. A navigation menu includes 'System', 'Call Routing', 'Media Resources', 'Voice Mail', 'Device', 'Application', 'User Management', and 'Bulk Administration'. The 'Bulk Administration' menu is expanded, showing 'SIP' as a sub-option. The main content area is titled 'Trunk Configuration' and includes a 'Related Links' section with a 'Back To Find/List' link. Below this, there are three main sections: 'Multilevel Precedence and Preemption (MLPP) Information', 'Call Routing Information', and 'Outbound Calls'. The 'Call Routing Information' section is expanded, showing 'Inbound Calls' and 'Outbound Calls' settings. The 'Inbound Calls' section includes fields for 'Significant Digits*' (set to 'All'), 'Connected Line ID Presentation*' (set to 'Default'), 'Connected Name Presentation*' (set to 'Default'), 'Calling Search Space' (set to 'BRANCH'), 'AAR Calling Search Space' (set to '< None >'), and 'Prefix DN'. There is also a checkbox for 'Redirecting Diversion Header Delivery - Inbound'. The 'Outbound Calls' section includes fields for 'Calling Party Selection*' (set to 'Originator'), 'Calling Line ID Presentation*' (set to 'Default'), and 'Calling Name Presentation*' (set to 'Default').

Figure 98 SIP Trunk Cisco Unified CM Configuration (3 of 3)

Cisco Unified SRST with SIP Endpoints: Dial Plan Implementation

Twelve dial peers were defined for the Basic Small Branch Network: central site WAN, central site PSTN, local calls, four 911 emergency services dial peers, voice mail, auto attendant, long distance, international calling and fax pass-through or fax relay. Voice mail, auto attendant and emergency services dial peers are described in the [“Cisco Unified SRST with SIP Endpoints: Voice Mail and Auto Attendant Integration”](#) section on page 228 and in the [“Cisco Unified SRST with SIP Endpoints: Emergency Services Implementation”](#) section on page 229.

```
Router(config)# dial-peer voice 1 pots ! Enters dial peer for central site calls
Router(config-dial-peer)# destination-pattern 5.... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 1408555 ! Prefix that the system adds automatically to
the dial string
Router(config-dial-peer)# incoming called-number .T ! Associates dial peer with any
incoming number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

```
Router(config)# dial-peer voice 2 voip ! Enters dial peer to central site configuration
mode
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# dtmf-relay rtp-nte ! Specifies Network Time Protocol method for
relaying pressed digit tones
Router(config-dial-peer)# destination-pattern 408..... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
```

```

Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit

Router(config)# dial-peer voice 3 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# destination-pattern 9..... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 4 pots ! Enters dial peer for long distance calls
configuration mode
Router(config-dial-peer)# destination-pattern 91..... ! Specifies area code prefix
for central site dial peer
Router(config-dial-peer)# prefix 1 ! Prefix that the system adds automatically to the dial
string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 5 pots ! Enters dial peer for international calls
configuration mode
Router(config-dial-peer)# destination-pattern 9011T ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 011 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

```

When calls over the WAN exceed the maximum allocated bandwidth, they are redirected to PSTN.

```

Router(config)# dial-peer voice 15 pots ! Enters dial peer for PSTN bypass configuration
mode
Router(config-dial-peer)# destination-pattern 408..... ! Specifies destination pattern
Router(config-dial-peer)# port 0/0/23 ! Specifies outgoing/incoming interface for calls
Router(config-dial-peer)# preference 1 ! Sets the dial peer preference order
Router(config-dial-peer)# prefix 408 ! Prefix that the system adds automatically to the
dial string

```

If using fax pass-through, apply the following configuration.

```

Router(config)# dial-peer voice 6 voip ! Enters dial peer for fax passthrough
configuration mode
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-dial-peer)# fax protocol pass-through g711ulaw ! Configures fax passthrough
with G.711 codec
Router(config-peer)# exit

```

If using fax relay, apply the following configuration.

```

Router(config)# dial-peer voice 7 voip ! Enters dial peer for fax relay configuration mode
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-dial-peer)# fax-relay ecm disable ! Disables fax relay ECM
Router(config-dial-peer)# fax rate 9600 ! Selects fax transmission rate
Router(config-dial-peer)# fax protocol t38 ! Sets the T.38 fax relay protocol

```

```
Router(config-dial-peer)# codec g711ulaw ! Configures fax relay with G.711 codec
Router(config-peer)# exit
```

Cisco Unified SRST with SIP Endpoints: RSVP Implementation

The following implementation applies to Cisco Unified SRST branch voice deployments. Apply the following commands on the tunnel interface for DMVPN, WAN primary, and for the WAN interface for GETVPN.

```
Router(config)# interface Tunnel 1 ! Enters tunnel interface configuration mode
Router(config-if)# ip rsvp bandwidth 8112 ! Sets maximum allowed bandwidth for voice (see
Table 18) plus video (512 Mbps)
Router(config-if)# ip rsvp data-packet classification none ! Turns off per-packet data
processing
Router(config-if)# ip rsvp resource-provider none ! Specifies no resource provider for the
traffic flows
Router(config-if)# ip rsvp policy local identity RSVP-VOICE ! Creates RSVP policy for
voice
Router(config-rsvp-local-policy)# maximum bandwidth group 7600 ! Sets maximum bandwidth for
voice
Router(config-rsvp-local-policy)# forward all ! Forwards all traffic for this policy
Router(config-rsvp-local-policy)# exit
Router(config-if)# ip rsvp policy local identity RSVP-VIDEO ! Creates RSVP policy for
video
Router(config-rsvp-local-policy)# maximum bandwidth group 512 ! Sets maximum bandwidth for
video
Router(config-rsvp-local-policy)# forward all ! Forwards all traffic for this policy
Router(config-rsvp-local-policy)# exit
Router(config-if)# ip rsvp policy local default ! Default policy for traffic that does not
matching above identifiers
Router(config-if)# exit

Router(config)# ip rsvp policy identity RSVP-VIDEO policy-locator .*VideoStream.* !
Creates a policy for matching video traffic
Router(config)# ip rsvp policy identity RSVP-VOICE policy-locator .*AudioStream.* !
Creates a policy for matching voice traffic
Router(config)# ip rsvp policy preempt ! Enables preempting of lower reservation by higher
reservation
```

The RSVP policy must be applied on the voice VLAN interface.

```
Branch(config)# interface FastEthernet0/1.2 ! Enters gigabit Ethernet sub-interface 2
configuration mode
Router(config-if)# ip rsvp bandwidth ! Enables RSVP on the interface
Router(config-if)# exit
```

Cisco Unified SRST with SIP Endpoints: Transcoding and Conferencing Implementation

Transcoding compresses and decompresses voice streams to match end device capabilities. Transcoding is required when an incoming voice stream is digitized and compressed (by means of a codec) to save bandwidth and the local device does not support that type of compression. Transcoding and conferencing are configured on the Cisco Call Manager of the central site, as shown in [Figure 99](#) and [Figure 100](#).

```
Router(config)# voice-card 0 ! Enters DSP farm configuration mode
Router(config-voicecard)# dsp services dspfarm ! Enables DSP services
Router(config-voicecard)# exit
Router(config)# sccp local FastEthernet0/1.2 ! Sets the interface for conferencing and
transcoding to register with CME
Router(config)# sccp ccm 10.0.1.2 identifier 1 version 5.0.1 ! Associates conferencing
and transcoding with CME
```

```

Router(config)# sccp ! Enables SCCP globally
Router(config)# sccp ccm group 1 ! Creates SCCP group and enters SCCP configuration mode
Router(config-sccp-ccm)# associate ccm 1 priority 1 ! Associates SCCP group 1 with CME
Router(config-sccp-ccm)# associate ccm 2 priority 2 ! Associates SCCP group 2 with CME
Router(config-sccp-ccm)# associate profile 3 register CONFERENCE ! Associates DSP farm
profile with with a SCCP group
Router(config-sccp-ccm)# associate profile 2 register TRANSCODE! Associates DSP farm
profile with with a SCCP group
Router(config-sccp-ccm)# exit

Router(config)# dspfarm profile 2 transcode ! Enters DSP farm profile configuration mode
Router(config-dspfarm-profile)# codec g711ulaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g711alaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729ar8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729abr8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729r8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec pass-through ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# maximum sessions 5 ! Specifies maximum number of
simultaneous sessions supported by this profile
Router(config-dspfarm-profile)# associate application sccp ! Associates SCCP with this DSP
farm profile
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit

Router(config)# dspfarm profile 3 conference ! Enters DSP farm profile configuration mode
Router(config-dspfarm-profile)# codec g711ulaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g711alaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729ar8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729abr8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729r8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729br8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# maximum sessions 3 ! Specifies maximum number of
simultaneous sessions supported by this profile
Router(config-dspfarm-profile)# associate application sccp ! Associates SCCP with this DSP
farm profile
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit

```


Figure 99 **Transcoding Configuration for Cisco Unified SRST Mode**

The screenshot shows a web browser window titled "TCWJINN-CAM-1" displaying the "Transcoder Configuration" page in Microsoft Internet Explorer. The address bar shows the URL: `https://172.16.200.10/ccmadmin/transcoderEdit.do?key=7793fc30-a7f5-3ef1-642b-13590da6fff9`. The page header includes the Cisco logo and "Cisco Unified CM Administration For Cisco Unified Communications Solutions". A navigation menu is visible with options: System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The main content area is titled "Transcoder Configuration" and includes a toolbar with Save, Delete, Copy, Reset, and Add New buttons. Below this, the "Transcoder Information" section shows the transcoder name as "BRANCH (BRANCH)", its registration as "Registered with Cisco Unified Communications Manager 172.16.200.10", and its IP address as "10.0.1.2". The "IOS Transcoder Info" section contains fields for Transcoder Type* (Cisco IOS Enhanced Media Termination Point), Description (XCODE), Device Name* (XCODE), Device Pool* (Default), Common Device Configuration (< None >), and Special Load Information. There are "View Details" links next to the Device Pool and Common Device Configuration fields. At the bottom of the form, there are Save, Delete, Copy, Reset, and Add New buttons, and a note indicating that an asterisk (*) denotes a required item.

TCWJINN-CAM-1

Transcoder Configuration - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Search Favorites Media Print

Address `https://172.16.200.10/ccmadmin/transcoderEdit.do?key=7793fc30-a7f5-3ef1-642b-13590da6fff9`

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help

Transcoder Configuration

Save Delete Copy Reset Add New

Transcoder Information

Transcoder: BRANCH (BRANCH)

Registration Registered with Cisco Unified Communications Manager 172.16.200.10

IP Address 10.0.1.2

IOS Transcoder Info

Transcoder Type* Cisco IOS Enhanced Media Termination Point

Description XCODE

Device Name* XCODE

Device Pool* Default [View Details](#)

Common Device Configuration < None > [View Details](#)

Special Load Information Leave blank to use default

Save Delete Copy Reset Add New

***** - indicates required item.

251047

Figure 100 Conferencing Configuration for Cisco Unified SRST Mode

The screenshot shows the Cisco Unified CM Administration web interface in Microsoft Internet Explorer. The address bar displays the URL: <https://172.16.200.10/ccmadmin/confBridgeEdit.do?key=0df22b21-f828-48a1-4515-648c622a2075>. The page title is "Conference Bridge Configuration - Microsoft Internet Explorer".

The navigation menu includes: System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The "Conference Bridge Configuration" section is active, with a "Related Links" section containing "Back To Find/List".

The "Status" section shows "Status: Ready". The "Conference Bridge Information" section displays the following details:

- Conference Bridge: BRANCH (BRANCH)
- Registration: Registered with Cisco Unified Communications Manager 172.16.200.10
- IP Address: 10.0.1.2

The "IOS Conference Bridge Info" section contains the following configuration fields:

- Conference Bridge Type*: Cisco IOS Enhanced Conference Bridge
- Conference Bridge Name*: CONF
- Description: CONF
- Device Pool*: Default
- Common Device Configuration: < None >
- Location*: Hub_None
- Device Security Mode*: Non Secure Conference Bridge

At the bottom of the configuration section, there are buttons for Save, Delete, Copy, Reset, and Add New.

Cisco Unified SRST with SIP Endpoints: Music on Hold Implementation

Music on hold (MOH) is implemented at the Unified Call Manager at the central site. Please see the following instructions to implement MOH in Cisco Unified CM:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_1_1/ccmfeat/fsmoh.html

Cisco Unified SRST with SIP Endpoints: Voice Mail and Auto Attendant Integration

Voice mail is provided by the Cisco Unity Express service module either in the Advanced Integration Module (AIM) form factor or the Network Module (NME) form factor. The AIM module requires the following configuration.

```
Router(config)# interface Service-Engine 0/1 ! Enters Cisco Unity Express configuration mode
Router(config-if)# ip address 10.0.2.86 255.255.255.252 ! Assigns IP address to the service engine router interface
Router(config-if)# service-module ip address 10.0.2.85 255.255.255.252 ! Assigns IP address to service module internal interface
Router(config-if)# service-module ip default-gateway 10.0.2.86 ! Assigns default gateway for the service module
Router(config-if)# zone-member security Private ! Assigns Cisco Unity Express to private security zone
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# ip route 10.0.2.84 255.255.255.252 Service-Engine 0/1 ! Adds a static route entry to direct traffic to the module
```

Configure a dial peer for voice mail, because Cisco Unity Express uses SIP as its signaling protocol.

```
Router(config)# dial-peer voice 8 voip ! Enters dial peer for voicemail configuration mode
Router(config-dial-peer)# destination-pattern 5444 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.2.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit
```

```
Router(config)# dial-peer voice 9 voip ! Enters dial peer for autoattendant configuration mode
Router(config-dial-peer)# destination-pattern 5000 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.2.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit
```

The local Cisco Unity Express software must be registered with Cisco Unified CM software at the central site. The following reference provides implementation details:

http://cisco.com/en/US/products/sw/voicesw/ps5520/products_configuration_example09186a0080289ef0.shtml

Additional Cisco Unity Express configuration is performed through a web-based user interface, as shown in [Figure 81](#) through [Figure 86](#).

Cisco Unified SRST with SIP Endpoints: Emergency Services Implementation

The following example implements emergency number calling for North America. The PRI trunk is used for placing emergency calls. Each 911 call is selectively routed to the closest PSAP based on the caller's location. In addition, the caller's phone number and address automatically display on a terminal at the PSAP. The PSAP can quickly dispatch emergency help, even if the caller is unable to communicate the caller's location. Also, if the caller disconnects prematurely, the PSAP has the information it needs to contact the 911 caller.

```
Router(config)# voice emergency response location 1 ! Enters emergency response configuration mode
Router(cfg-emrgncy-resp-location)# elin 1 4085555150 ! Specifies ELIN number provided by PSAP
Router(cfg-emrgncy-resp-location)# subnet 1 10.0.1.0 255.255.255.0 ! Assigns Voice VLAN subnet as origination of the emergency call
Router(cfg-emrgncy-resp-location)# subnet 2 10.0.4.0 255.255.255.0 ! Assigns backup Voice VLAN subnet as origination of the emergency call

Router(cfg-emrgncy-resp-location)# exit

Router(config)# dial-peer voice 10 pots ! Enters dial peer for emergency calls configuration mode
Router(config-dial-peer)# emergency response zone ! Replaces local extension with ELIN number
Router(config-dial-peer)# destination-pattern 911 ! Specifies North America emergency number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

```

Router(config)# dial-peer voice 11 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# emergency response zone ! Replaces local extension with ELIN
number
Router(config-dial-peer)# destination-pattern 9911 ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 911 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

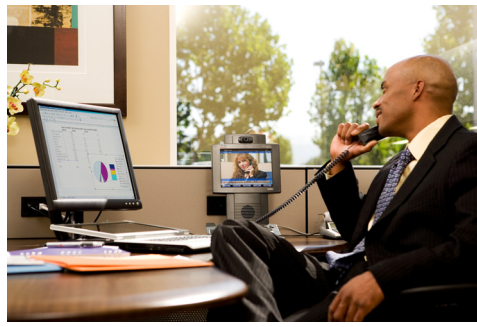
Router(config)# dial-peer voice 12 pots ! Enters dial peer for ELIN callback configuration
mode
Router(config-dial-peer)# incoming called-number 4085555150 ! Specifies ELIN number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# emergency response callback ! Identifies the ELIN dial peer
Router(config-peer)# exit

Router(config)# dial-peer voice 13 pots ! Enters dial peer for ELIN callback configuration
mode
Router(config-dial-peer)# incoming called-number 4085555150 ! Specifies ELIN number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# emergency response callback ! Identifies the ELIN dial peer
Router(config-peer)# exit

```

Caveats

- Zone-based firewall does not support inspection of SIP and SCCP in releases earlier than Cisco IOS Release 12.4(20)T. See DDTS CSCsm79679.
- Zone-based firewall does not support stateful switchover.
- Message waiting indicator (MWI) does not work during router failover.
- Cisco Unified CME does not work with HSRP.
- Cisco web Cache Communication Protocol (Cisco WCCP) version 2 is not Virtual Routing and Forwarding (VRF) aware and does not work if multiple VRF interfaces (VRF-lite) are configured on the customer edge (CE) router.
- Call preservation is not supported during HSRP. Only local IP Phone calls may be preserved.
- Traffic shaping is not supported over virtual access interfaces with PPP over ATM. See DDTS CSCsm77478.
- VRF-aware IP SLA is not supported in releases earlier than Cisco IOS Release 12.4(20)T.
- Bidirectional Forwarding Detection (BFD) is supported only on Fast Ethernet interfaces. Support for additional WAN encapsulations such as Frame Relay and PPP is planned for future releases.
- GETVPN is not VRF aware in releases earlier than Cisco IOS Release 12.4(20)T.
- When registered to Cisco Unified CME, the Cisco Unified IP Conference Station 7936 running firmware version 1.1 continues to display message prompts such as “hold” and “enter number” after the call has ended. See DDTS CSCsm61235.



Configuration Verification

Revised: March 25, 2009

This chapter describes the **show** commands that you can use to display and verify your configuration.



Note

For more information see the following command references:

[Cisco IOS Debug Command Reference](#)
[Cisco IOS IP Addressing Services Command Reference](#)
[Cisco IOS IP Application Services Command Reference](#)
[Cisco IOS IP Multicast Command Reference](#)
[Cisco IOS IP Routing Protocols Command Reference](#)
[Cisco IOS LAN Switching Command Reference](#)
[Cisco IOS NetFlow Command Reference](#)
[Cisco IOS Quality of Service Solutions Command Reference](#)
[Cisco IOS Security Command Reference](#)
[Cisco IOS Voice Command Reference](#)
[Cisco IOS Master Command List, Release 12.4T](#)

Use the [Command Lookup Tool](#) (registered customers only) for more information on the commands used in this document.

Contents

- [General Configuration Verification, page 232](#)
- [QoS Verification, page 233](#)
- [Routing Verification, page 233](#)
- [Security Verification, page 234](#)
- [Voice Verification, page 235](#)
- [Cisco Unity Express Verification, page 237](#)
- [Cisco Wide Area Application Services Verification, page 237](#)

General Configuration Verification

- **show adjacency summary**
This command displays a summary of Cisco Express Forwarding (CEF) adjacency information.
- **show clock**
This command displays the time and date from the system software clock.
- **show interfaces status**
This command displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
- **show interfaces summary**
This command displays a summary of statistics for one interface or for all interfaces that are configured on a networking device.
- **show ip cache flow**
This command displays a summary of the NetFlow accounting statistics.
- **show ip flow export**
This command displays the status and the statistics for NetFlow accounting data export, including the main cache and all other enabled caches.
- **show ip wccp**
This command displays global statistics related to Cisco Web Cache Communication Protocol (Cisco WCCP).
- **show logging**
This command displays the state of system logging (syslog) and the contents of the standard system logging buffer.
- **show memory dead**
This command displays statistics on memory allocated by processes that have terminated.
- **show memory debug leaks**
This command displays detected memory leaks.
- **show memory free**
This command displays statistics about free memory when Cisco IOS software or Cisco IOS Software Modularity images are running.
- **show mls qos interface policers**
This command displays all the policers configured on the interface, their settings, and the number of policers unassigned.
- **show ntp status**
This command displays statistics for the Network Time Protocol (NTP) server.
- **show processes cpu**
This command displays detailed CPU utilization statistics (CPU use per process) when Cisco IOS software or Cisco IOS Software Modularity images are running.

- **show processes memory**

This command shows the amount of memory used by each system process in Cisco IOS software or Cisco IOS Software Modularity images.

- **show spanning-tree**

This command displays Spanning Tree information for the specified Spanning Tree instances.

QoS Verification

- **show class-map**

This command displays all class maps and their matching criteria.

- **show ip nbar protocol-discovery**

This command displays the statistics gathered by the Network Based Application Recognition (NBAR) protocol discovery feature.

- **show mls qos**

This command displays multilayer switching (MLS) quality of service (QoS) information.

- **show mls qos *interface***

This command displays QoS information for the specified interface.

- **show mls qos maps**

This command displays information about the QoS mapping.

- **show policy-map**

This command displays the configurations of all classes for a specified service policy map or all classes for all existing policy maps.

- **show policy-map interface**

This command displays the statistics and the configurations of the input and output policies that are attached to an interface.

Routing Verification

- **show bfd neighbors**

This command displays a line-by-line listing of existing Bidirectional Forwarding Detection (BFD) adjacencies.

- **show ip bgp**

This command displays entries in the Border Gateway Protocol (BGP) routing table.

- **show ip bgp neighbors**

This command displays information about BGP and TCP connections to neighbors.

- **show ip bgp summary**

This command displays the status of all BGP connections.

- **show ip dhcp binding**

This command displays address bindings on the Cisco IOS DHCP server.

- **show ip dhcp server statistics**

This command displays Cisco IOS DHCP server statistics.

- **show ip eigrp neighbors**

This command displays neighbors discovered by Enhanced Interior Gateway Routing Protocol (EIGRP).

- **show ip mroute active**

This command displays the contents of the multicast routing (mroute) table. Displays the rate that active sources are sending to multicast groups, in kilobits per second.

- **show ip mroute count**

This command displays the contents of the multicast routing (mroute) table. Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bytes per second.

- **show ip nat translations**

This command displays active Network Address Translations (NATs).

- **show ip nat statistics**

This command displays NAT statistics.

- **show ip ospf neighbors**

This command displays Open Shortest Path First (OSPF)—neighbor information on a per-interface basis.

- **show ip route**

This command displays the current state of the routing table.

Security Verification

- **show crypto engine accelerator statistics**

This command displays a summary of the configuration information for the crypto accelerator.

- **show crypto engine connections active**

This command displays a summary of the configuration information for the crypto engine connections.

- **show crypto gdoi**

This command displays information about a Group Domain of Interpretation (GDOI) configuration.

- **show crypto gdoi ipsec sa**

This command displays information about the IPsec security association (SA) for all group members.

- **show crypto ipsec sa**

This command displays the settings used by current SAs.

- **show crypto isakmp sa**

This command displays current Internet Key Exchange (IKE) SAs.

- **show crypto session**

This command displays status information for active crypto sessions.

- **show ip ips interfaces**
This command displays the Cisco IOS Intrusion Prevention System (IPS) interface configuration.
- **show ip ips sessions**
This command displays the Cisco IOS IPS session-related information.
- **show ip ips signatures**
This command displays the Cisco IOS IPS signature information, such as which signatures are disabled and marked for deletion.
- **show ip ips statistics**
This command displays the Cisco IOS IPS information such as the number of packets audited and the number of alarms sent.
- **show policy-map type inspect**
This command displays a specified policy map.
- **show policy-map type inspect zone-pair**
This command displays the runtime inspect type policy map statistics and other information such as sessions existing on a specified zone pair.
- **show standby**
This command displays Hot Standby Router Protocol (HSRP) information.
- **show webvpn gateway**
This command displays the status of a Secure Socket Layer (SSL) Virtual Private Network (VPN) gateway.
- **show webvpn context**
This command displays the operational status and configuration parameters for SSL VPN context configurations.
- **show webvpn session context**
This command displays a list of active SSL VPN user sessions for only the named context.
- **show webvpn session user**
This command displays detailed information about the named SSL VPN user session.
- **show webvpn stats**
This command displays SSL VPN application and network statistics.
- **show zone-pair security**
This command displays the source zone, destination zone, and policy attached to the zone pair.
- **show zone security**
This command displays information about the security zone, including the name and description.

Voice Verification

- **show call active voice brief**
This command displays a truncated version of call information for voice calls in progress.

- **show call-manager-fallback all**

This command displays the Cisco Unified Communications Manager fallback configuration and statistics.

- **show dial-peer voice summary**

This command displays a short summary of information for each voice dial peer.

- **show dspfarm**

This command displays digital signal processor (DSP) farm-service information such as operational status and DSP resource allocation for transcoding and conferencing.

- **show dspfarm dsp all**

This command displays DSP-farm DSP global information.

- **show ephone offhook**

This command displays information and packet counts for the phones that are currently off hook.

- **show ephone registered**

This command displays the status of registered phones.

- **show ephone summary**

This command displays brief information about Cisco IP Phones.

- **show rtpspi call**

This command displays Real-time Transport Protocol (RTP) service provider interface active call details.

- **show sccp all**

This command displays all Skinny Client Control Protocol (SCCP) global information, such as administrative and operational status.

- **show sccp connections summary**

This command displays a summary of the number of sessions and connections based on the service type under the SCCP application.

- **show sip-ua status registrar**

This command displays status for the SIP user agent (UA) registrar clients.

- **show telephony-service all**

This command displays detailed configuration for phones, voice ports, and dial peers in a Cisco Unified Communications Manager Express (Cisco Unified CME) system.

- **show voice call status**

This command displays the status of active calls.

- **show voice call summary**

This command displays the current settings and state of voice ports on the Cisco router, regardless of port activity.

- **show voice dsp**

This command displays the current status or selective statistics of DSP voice channels.

- **show voice port summary**

This command displays a summary of configuration information for all voice ports.

- **show voice register all**

This command displays all Session Initiation Protocol (SIP) Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) and Cisco Unified CME configurations and register information.

- **show voip rtp connections**

This command displays (RTP) named event packets.

Cisco Unity Express Verification

- **show ccn application**

This command displays the currently configured applications.

- **show ccn engine**

This command display details of the configured Cisco Unity Express software engine.

- **show ccn subsystem jtapi**

This command display the JTAPI subsystem parameters.

- **show ccn subsystem sip**

This command display the SIP subsystem parameters.

- **show system language installed**

This command displays the languages that are available for use.

- **show voicemail configuration**

This command displays the configured From address for outgoing e-mail.

- **show voicemail detail**

This command displays the details for a general delivery mailbox or a subscriber with the name value.

- **show voicemail limits**

This command displays default values for all mailboxes.

- **show voicemail mailboxes**

This command displays all configured mailboxes and their current storage status.

- **show voicemail messages future**

This command displays all messages scheduled for future delivery.

- **show voicemail users**

This command lists all the local voice-mail subscribers.

Cisco Wide Area Application Services Verification

- **show cifs auto-discovery**

This command displays Common Internet File System (CIFS) autodiscovery status and run-time data.

- **show cifs cache**
This command displays CIFS cache information.
- **show cifs connectivity peers**
This command displays run-time information on edge-core connectivity and a list of connected cores.
- **show cifs sessions count**
This command displays run-time information on active CIFS sessions and the number of pending CIFS requests.
- **show cifs sessions list**
This command displays run-time information on active CIFS sessions and a list of connected CIFS sessions.
- **show device-mode**
This command displays the configured or current device mode of a Cisco Wide Area Application Services (WAAS) device.
- **show disks details**
This command displays detailed SMART disk monitoring information for Cisco WAAS device disks.
- **show egress-methods**
This command displays the egress method that is configured and that is being used on a particular Cisco WAE.
- **show policy-engine status**
This command displays high-level information about a Cisco Wide Area Application Engine (Cisco WAE): Cisco WAE's policy engine.
- **show policy-engine application classifier**
This command displays information about the specified application classifier.
- **show statistics cifs**
This command displays the CIFS statistics information.
- **show statistics dre**
This command displays data redundancy elimination (DRE) general statistics for a Cisco WAE.
- **show statistics tfo**
This command displays TFO statistics for a Cisco WAE.
- **show tfo auto-discovery**
This command displays TFO auto discovery statistics for a Cisco WAE.
- **show tfo status**
This command displays global Traffic Flow Optimization (TFO) status information for a Cisco WAE.
- **show tfo connections**
This command displays Traffic Flow Optimization (TFO) connection information for a Cisco WAE.
- **show tfo connections summary**
This command displays a summary list of TFO connections for a Cisco WAE.

- **show wccp**

This command displays Cisco Web Cache Communication Protocol (Cisco WCCP) information for a Cisco WAE.

- **show wccp gre**

This command displays Cisco WCCP generic routing encapsulation (GRE) packet-related information

- **show wccp routers**

This command displays routers seen and not seen by this Cisco WAE.

- **show wccp status**

This command displays the version of Cisco WCCP that is enabled and running.

Additional Command Reference Documentation

See the following command references for more information:

- [Cisco IOS Configuration Fundamentals Command Reference](#)
- [Cisco IOS IP Addressing Services Command Reference](#)
- [Cisco IOS IP Application Services Command Reference](#)
- [Cisco IOS IP Multicast Command Reference](#)
- [Cisco IOS IP Routing Protocols Command Reference](#)
- [Cisco IOS LAN Switching Command Reference](#)
- [Cisco IOS NetFlow Command Reference](#)
- [Cisco IOS Quality of Service Solutions Command Reference](#)
- [Cisco IOS Security Command Reference](#)

The [Output Interpreter Tool \(registered customers only\)](#) (OIT) supports certain **show** commands. Use the OIT to view an analysis of the **show** command output.



Troubleshooting

Revised: March 25, 2009

This chapter describes the **debug** commands you can use to troubleshoot your configuration.

The OIT [Output Interpreter Tool](#) (registered customers only) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.



Note

See the [Important Information on Debug Commands](#) before you use **debug** commands.

See the [Cisco IOS Debug Command Reference](#) for more information.

Contents

- [Baseline Troubleshooting Commands, page 241](#)
- [Voice Troubleshooting Commands, page 242](#)
- [Cisco WAAS Troubleshooting Commands, page 242](#)

Baseline Troubleshooting Commands

- **debug aaa authentication**
- **debug bgp all events**
- **debug crypto gdoi**
- **debug crypto isakmp**
- **debug frame-relay events**
- **debug frame-relay lmi**
- **debug frame-relay packet**
- **debug h225 events**
- **debug ip inspect detailed**
- **debug ip inspect policy detailed**
- **debug ip ips category**

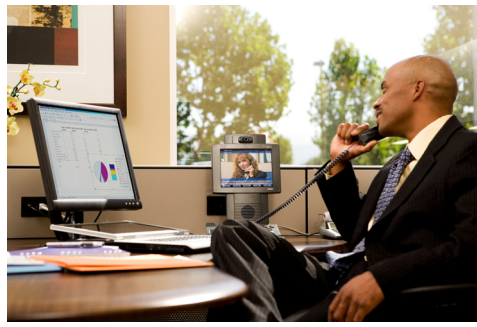
- **debug ip ips detailed**
- **debug ip ips function-trace**
- **debug ip ips idconf**
- **debug ppp multilink data**
- **debug ppp multilink events**
- **debug radius authentication**
- **debug qos cce**
- **debug qos events**
- **debug qos stats**

Voice Troubleshooting Commands

- **debug ephone detail**
- **debug sccp errors**
- **debug sccp events**
- **debug sccp keepalive**
- **debug sccp packets**
- **debug voice ccapi inout**
- **debug voice confmsp**
- **debug voice dsmp**
- **debug voice xcodemsp**
- **debug voip dialpeer**

Cisco WAAS Troubleshooting Commands

- **debug wccp events**
- **debug wccp error**



System Testing

Revised: March 25, 2009

This chapter describes the tests performed on the Basic Small Branch Network.

Contents

- [Test Result Summary, page 243](#)
- [Traffic Profile, page 247](#)
- [Test Setups, page 247](#)
- [Test Cases, page 251](#)

Test Result Summary

Table 23 lists the test cases and their results.

Table 23 **Test Cases and Results**

Test Case	Result
Fast Ethernet Primary WAN Connection for Cisco 1800 Series Small Branch	Passed
PPP Primary WAN Connections for Cisco 1800 Series Small Branch	Passed
Frame Relay Primary WAN Connections for Cisco 1800 Series Small Branch	Passed
SHDSL Secondary WAN Connection for Cisco 1800 Series Small Branch	Passed
Layer 2 Access Layer Switch	Passed
L2 Security–802.1x Authentication on the Access Layer Switch	Passed
L2 Security–DHCP Snooping and Dynamic ARP Inspection on the Access Switch	Passed
L2 Security–Port Security on the Access Layer Switch	Passed
L2 Security–IP Source Guard on the Access Layer Switch	Passed
L2 Security–BPDU Guard on the Access Layer Switch	Passed
QoS on the LAN	Passed
WAN Edge QoS–5 Class QoS Model	Passed

Table 23 **Test Cases and Results**

Test Case	Result
LLQ for Voice and Interactive Video Traffic	Passed
CBWFQ and WRED for Data Traffic	Passed
Traffic Shaping on Different WAN Links	Passed
DSCP/CoS Marking Incoming/Returning Traffic from WAN to LAN	Passed
Modification and Deletion of ACLs Defined with Class Map match access-group Command	Passed
Unconfigure and Reconfigure QoS	Passed
Unconfigure QoS, Reload Router, and Reconfigure QoS	Passed
OSPF Routing as IGP Between Branch and Headquarters Network	Passed
EIGRP Routing as IGP Between the Branch Router and the Headquarters Router	Passed
Traffic Measurement Using NetFlow When QoS is Enabled on the Branch Router	Passed
NBAR Classification with QoS	Passed
Modify Match Protocol Statements and Bandwidth Percentage	Passed
100 ACLs	Passed
NTP in the Branch Router	Passed
Branch Router as a DHCP Server	Passed
IP SLA VoIP UDP Jitter Codec G.711 u-law (Branch to HQ)	Passed
IP SLA VoIP UDP Jitter Codec G.729A u-law (Branch to HQ)	Passed
IP SLA ICMP Echo (Branch to HQ)	Passed
IPsec Site-to-Site VPN Using DMVPN	Passed
IPsec Using GETVPN	Passed
GETVPN Unicast Rekeying	Passed
GETVPN Multicast Rekeying	Passed
IPsec DMVPN with Prefragmentation	Passed
IPsec DMVPN and IGP	Passed
DMVPN Backup for MPLS Network (Branch to HQ)	Passed
DMVPN Backup for MPLS Network (Branch to Branch)	Passed
DMVPN Backup for MPLS Network Using BFD (Branch to HQ)	Passed
DMVPN Backup for MPLS Network Using BFD (Branch to Branch)	Passed
DMVPN Backup for MPLS Network Using BFD IGP as OSPF (Branch to Branch)	Passed
DMVPN Backup for MPLS Network Using EBGp (Branch to HQ)	Passed
DMVPN with QoS	Passed
GETVPN with QoS	Passed
DMVPN with QoS and NBAR	Passed
GETVPN with QoS and NBAR	Passed
DMVPN/GETVPN with QoS, NBAR, and NetFlow	Passed
Zone-based Policy Firewall Configuration on the Branch Router	Passed

Table 23 **Test Cases and Results**

Test Case	Result
NAT and PAT Configuration on the Branch Router	Passed
NAT, QoS, and NetFlow on the Branch	Passed
ZPF, QoS, and NetFlow on the Branch	Passed
ZPF, QoS, NBAR, and NetFlow on the Branch	Passed
ZPF, QoS, NBAR, NAT, and NetFlow on the Branch	Passed
ZPF with DMVPN	Passed
ZPF with GETVPN	Passed
IPsec, ZPF, QoS, NBAR, NAT, and NetFlow on the Branch	Passed
DDOS Prevention Using Cisco IOS IPS	Passed
Cisco IOS IPS with Background Data Traffic	Passed
ZPF with NAT and Cisco IOS IPS	Passed
IPsec, ZPF, QoS, NBAR, NAT, Cisco IOS IPS, and NetFlow on the Branch	Passed
Remote Users Using WebVPN (SSL VPN)	Passed
Remote Users Using WebVPN (SSL VPN) Full Tunnel	Passed
Complete Baseline Test	Passed
EIGRP Subsecond Convergence During Primary WAN Failure	Passed
OSPF Subsecond Convergence During Primary WAN Failure	Passed
IPsec over Backup SHDSL WAN Link	Passed
ZPF, NAT, and IPsec over Backup SHDSL WAN Link	Passed
IPsec, ZPF, QoS, NBAR, and NetFlow on Both Primary and Secondary Link, and NAT on the Secondary Link	Passed
Multicast with Security and QoS Features	Passed
Enable SNMP on the UUTs for Management and Monitoring	Passed
Enable SYSLOG on the UUT for Management and Monitoring	Passed
Using Cisco CCP for Configuration and Monitoring of the UUTs	Passed
SCCP Phone Registration to Cisco Unified CME	Passed
SIP Phone Registration to Cisco Unified CME	Passed
SCCP Local Calls	Passed
SIP Local Calls	Passed
PSTN Calls	Passed
Branch to Headquarters Calls over the WAN with a SIP Trunk	Passed
Branch to Headquarters Calls over the WAN with an H.323 trunk	Passed
Supplementary Services with Cisco Unified CME	Passed
Supplementary Services Between Phones in the Branch, Headquarters, and PSTN	Passed
Call Conference in the Branch Cisco Unified CME	Passed
Call Forward to Voice Mail	Passed

Table 23 **Test Cases and Results**

Test Case	Result
Video Call Between Branch and Headquarters	Passed
T.38 Fax Between Branch and Headquarters	Passed
IP SLA VoIP UDP Jitter Codec g711ulaw (Branch to HQ)	Passed
Remote Phones on the Cisco Unified CME	Passed
Cisco Unified CME with WAN Failure Scenario to Headquarters	Passed
Cisco Unified CME with IPsec over the WAN	Passed
Cisco Unified CME with QoS and NBAR	Passed
Cisco Unified CME with ZPF	Passed
Cisco Unified CME Remote Phones with ZPF	Passed
Cisco Unified CME Failover with Secondary Cisco Unified CME	Passed
Baseline Features Plus Cisco Unified CME	Passed
SCCP Phone Registration to Cisco Unified CM	Passed
SIP Phone Registration to Cisco Unified CM	Passed
SIP Local Calls	Passed
SCCP Local Calls	Passed
PSTN Calls with SIP Gateway	Passed
PSTN Calls with H.323 Gateway	Passed
Branch to Headquarters Calls over the WAN	Passed
Supplementary Services Between Phones in Branch, Headquarters, and PSTN	Passed
Call Conference in the Branch	Passed
Call Forward to Voice Mail	Passed
Phone Registration During Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST)	Passed
Local and PSTN Calls in Cisco Unified SRST Mode	Passed
Supplementary Services in Cisco Unified SRST Mode	Passed
Call Forward to Voice Mail in Cisco Unified SRST Mode	Passed
Call Conference in Cisco Unified SRST Mode	Passed
Branch to Headquarters Calls with IPsec over the WAN	Passed
Branch to Headquarters Voice and Video Calls with QoS and NBAR	Passed
Branch to Headquarters Voice and Video calls with ZPF	Passed
High Availability in Cisco Unified SRST mode	Passed
Baseline Features Plus Cisco Unified Communications Manager	Passed
RSVP Agent in SRST Router–HQ to Branch Call with Phones Registered to Cisco Unified CM	Passed
RSVP Agent with Application ID in SRST Router–HQ to Branch Call with Phones Registered to Cisco Unified CM	Passed
RSVP Agent–HQ to Branch Call with H.323 Trunk	Passed

Table 23 **Test Cases and Results**

Test Case	Result
Baseline Performance Test	Passed
Baseline Plus Voice Performance Test with Cisco Unified CME	Passed
Baseline Plus Voice Performance Test with Cisco Unified CM and Cisco Unified SRST	Passed

Traffic Profile

The following traffic profile was used to represent typical traffic in a large enterprise branch network.

HTTP Traffic—75 percent

- 16 KB object size representing large HTML files containing images (10 URLs)
- 4 KB object size representing transactional data (10 URLs)

FTP Traffic—10 percent

- 1 MB file size

SMTP Traffic—10 percent

- 4 KB fixed object size

DNZ Traffic—5 percent

- 89 byte object size

Test Setups

The test cases described in this section use the test setups shown in [Figure 101](#) through [Figure 106](#), in addition to test setups shown in the other figures referenced in the specific test case.

Figure 101 Cisco 1861 ISR Private WAN, Cisco Unified CME Mode

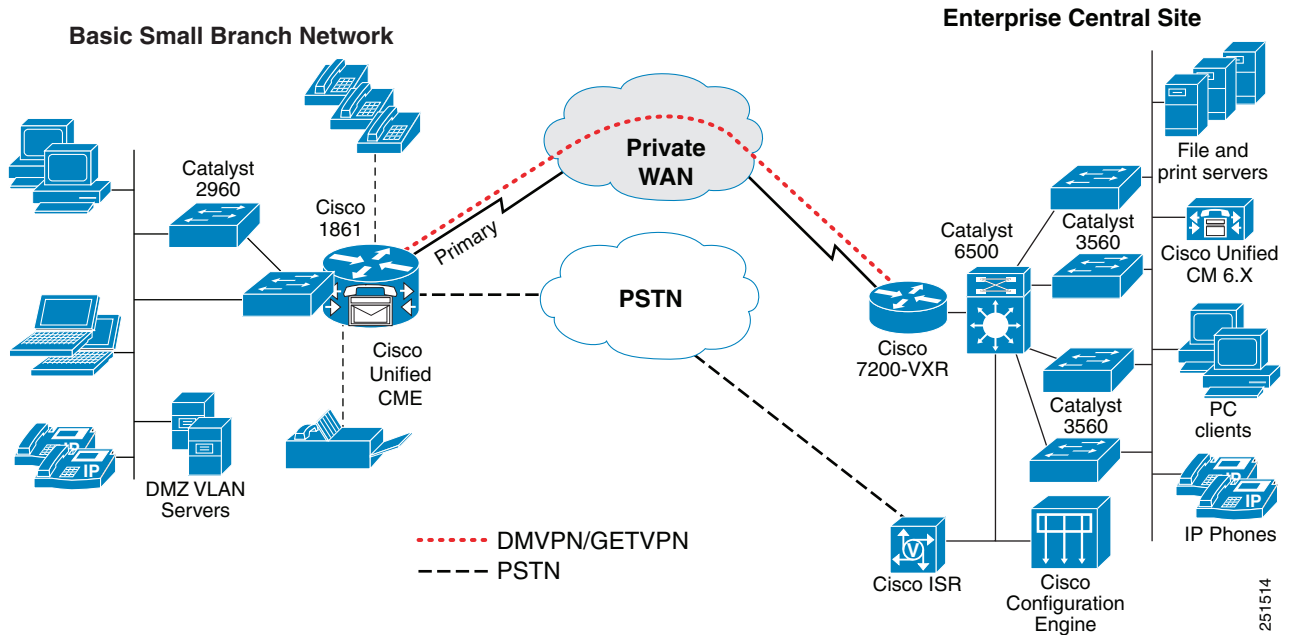


Figure 102 Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode

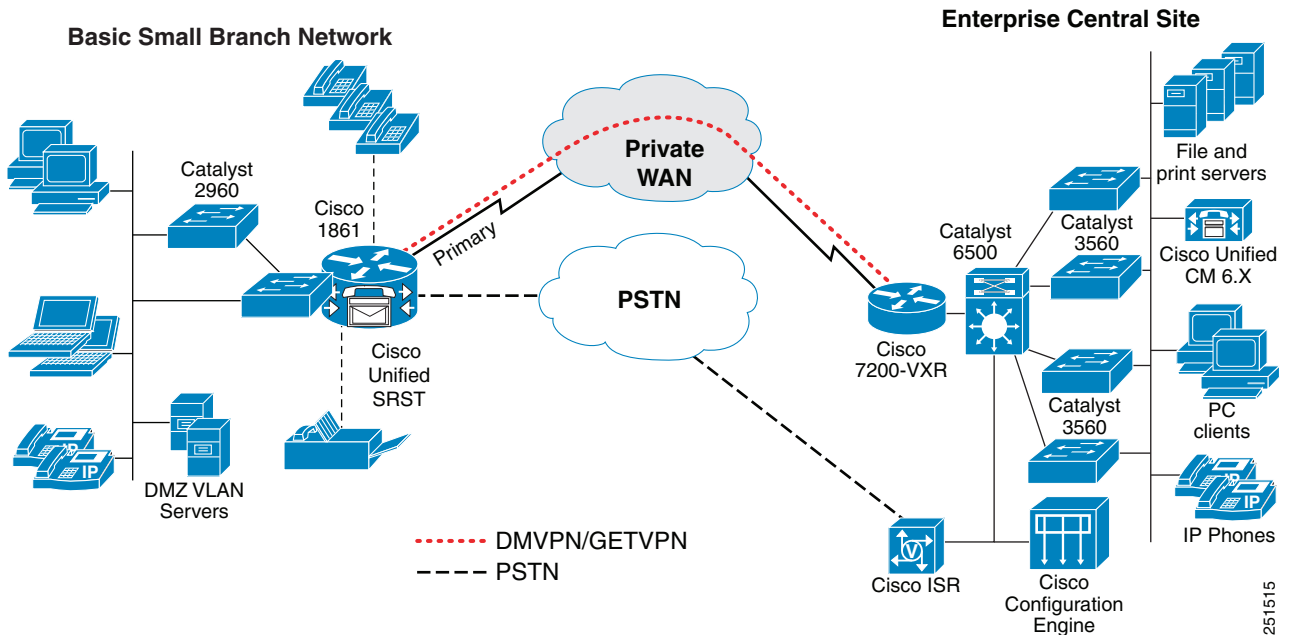


Figure 103 Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode

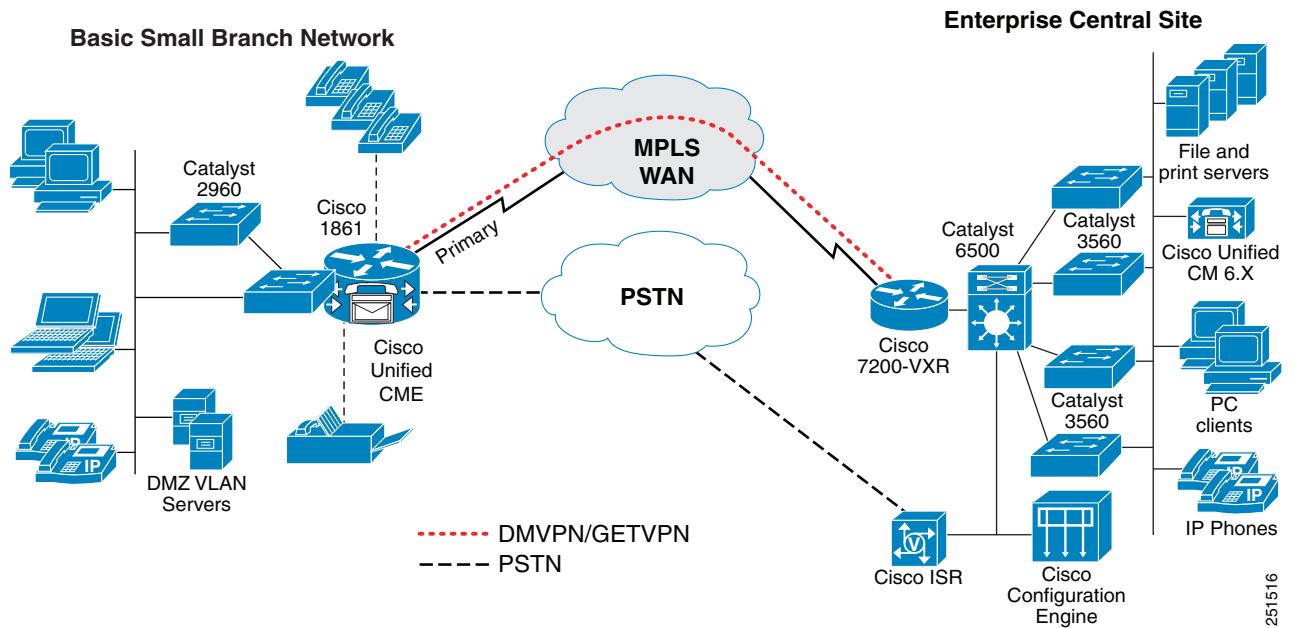


Figure 104 Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode

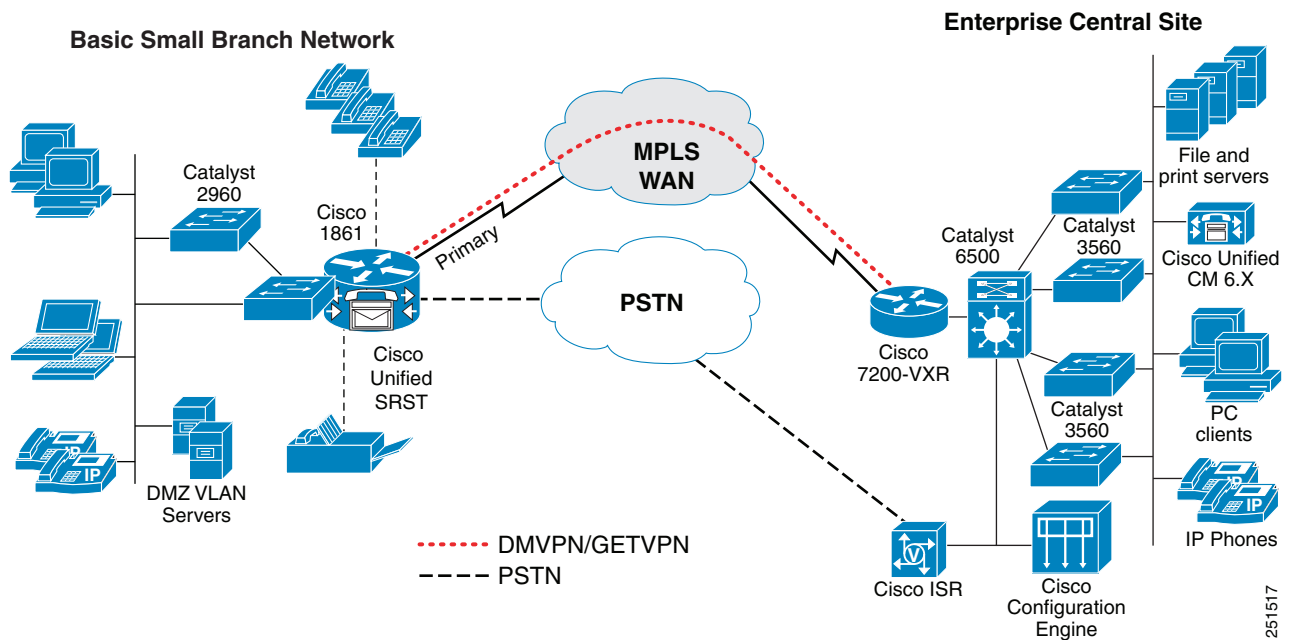


Figure 105 Private WAN, Cisco 1841 ISR

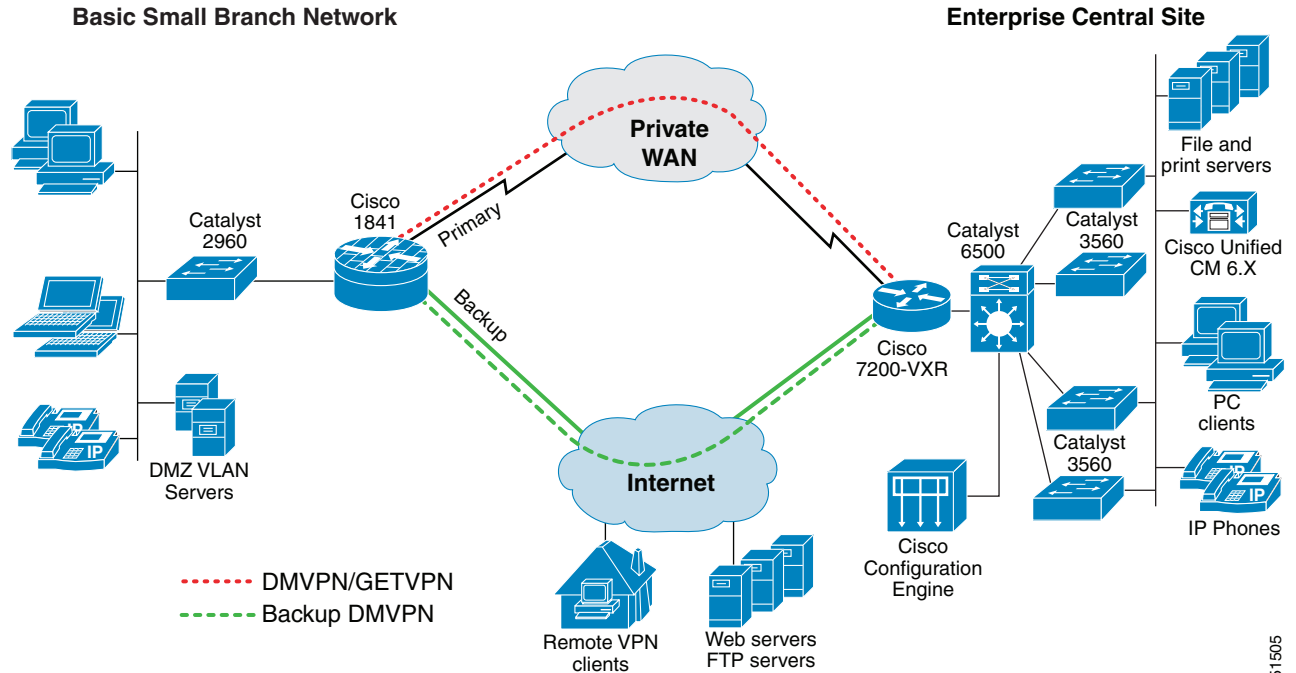
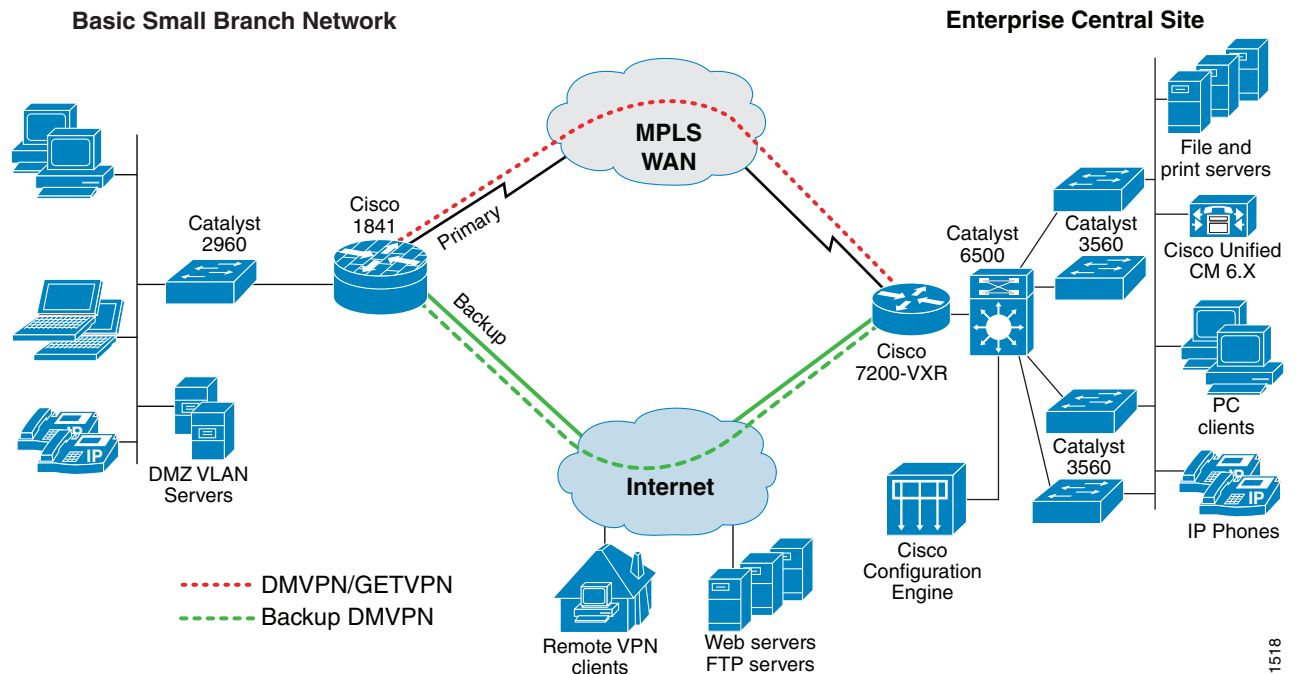


Figure 106 MPLS WAN, Cisco 1841 ISR



Test Cases

This section contains the following test cases:

- [WAN Connectivity Test Cases, page 252](#)
- [Network Services Test Cases, page 254](#)
- [High Availability Test Cases, page 313](#)
- [Network Management Test Cases, page 325](#)
- [Cisco Unified CME Test Cases, page 327](#)
- [Cisco Unified SRST Test Cases, page 343](#)
- [Performance Test Cases, page 360](#)

WAN Connectivity Test Cases

Fast Ethernet Primary WAN Connection for Cisco 1800 Series Small Branch

Description	Set up a Fast Ethernet private WAN connection between the branch Cisco ISR and the headend router
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Connect the Cisco 1800 FE port to the GE port on the headend router using category 5 UTP copper wire. 2. Configure the IP address and both routers. 3. Make sure that the IP addresses belong to the same segment and have the same subnet mask. 4. Ping both routers. 5. Send 100-Mb/s bidirectional HTTP and FTP traffic (50 Mb/s in each direction), with 75% HTTP and 25% FTP. 6. Measure the branch Cisco ISR CPU utilization.
Pass/Fail Criteria	The FE link and line protocol should come up on both routers. The ping should be 100% successful. 100-Mb/s throughput should be achieved, and the branch Cisco ISR CPU should be less than 75%.
Result	Passed

PPP Primary WAN Connections for Cisco 1800 Series Small Branch

Description	Set up a DS1 (T1) private WAN connection between the branch Cisco ISR and headend router
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR

Procedure	1. Install an HWIC-1T card into the branch Integrated Services Router (ISR). 2. Configure the card as T1 on both branch and headend routers. 3. Connect the card using a T1 serial cable. 4. Configure the IP address on both routers. 5. Make sure that the IP addresses belong to the same segment and have the same subnet mask. 6. Configure PPP encapsulation. 7. Ping both routers. 8. Send T1 line rate HTTP and FTP bidirectional traffic, with 75% HTTP and 25% FTP, and measure the branch Cisco ISR CPU utilization.
Pass/Fail Criteria	The T1 link and line protocol should come up on both routers. The ping should be 100% successful. T1 line rate should be achieved, and branch Cisco ISR CPU should be less than 75%.
Result	Passed

Frame Relay Primary WAN Connections for Cisco 1800 Series Small Branch

Description	Set up a DS1 (T1) private WAN connection between the branch Cisco ISR and headend router
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Install an HWIC-1T card into the branch Integrated Services Router (ISR). 2. Configure the card as T1 on both branch and headend routers. 3. Connect the card using a T1 serial cable. 4. Configure the IP address on both routers. 5. Make sure that the IP addresses belong to the same segment and have the same subnet mask. 6. Configure PPP encapsulation. 7. Ping both routers. 8. Send T1 line rate HTTP and FTP bidirectional traffic, with 75% HTTP and 25% FTP, and measure the branch Cisco ISR CPU utilization.
Pass/Fail Criteria	The T1 link and line protocol should come up on both routers. The ping should be 100% successful. T1 line rate should be achieved, and branch Cisco ISR CPU should be less than 75%.
Result	Passed

SHDSL Secondary WAN Connection for Cisco 1800 Series Small Branch

Description	Set up an SHDSL WAN connection between the branch Cisco ISR and the DSLAM
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Install an HWIC-2SHDSL card into one of the HWIC slots on the Cisco 1841 ISR. 2. Connect to the ISP DSLAM. 3. Configure a single port to achieve a bandwidth of 2304 kb/s. 4. Configure a PVC with AAL5SNAP encapsulation. 5. Configure the IP address on the ATM interface. Verify the connection by pinging the DSLAM IP address. 6. Send line rate bidirectional HTTP and FTP traffic over the interface.
Pass/Fail Criteria	The ATM link and line protocol should come up. The ping should be 100% successful. Close to line rate should be achieved for HTTP and FTP traffic, and the router CPU should be less than 75%.
Result	Passed

Network Services Test Cases

Layer 2 Access Layer Switch

Description	Set up Catalyst 2960 switches as access layer switches
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Configure Catalyst 2960 switches in Layer 2 mode. 2. Define VLANs for voice, data, management, and DMZ. 3. Enable RSPT for subsecond switchover in case of master switch failure. 4. Do not enable Layer 3 routing on the access layer switches.
Pass/Fail Criteria	Layer 2 voice, data, management, and DMZ VLANs should come up. During master switch failure, Layer 2 convergence should happen within a second.
Result	Passed

L2 Security–802.1x Authentication on the Access Layer Switch

Description	Set up to verify 802.1x authentication on one of the access switches
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Configure DHCP snooping on the switch. 2. Configure the trunk port connecting the access switch and the router as the trusted port. Configure all other ports as non-trusted ports. 3. Configure the router as the DHCP server. 4. Add a Windows DHCP server and connect it to one of the non-trusted ports of the switch. 5. Configure DAI for VLAN (x,y). 6. Assign all the switch ports to either x or y VLAN. 7. Configure the DHCP scope in the DHCP servers to assign IP addresses to x and y VLANs. 8. Connect phones and PCs to the switch ports. 9. Place all IP Phones in VLAN x and PCs in VLAN y.
Pass/Fail Criteria	The IP Phones and PCs should obtain IP addresses from the DHCP server on the router and not from the Windows DHCP server, because the Windows server is connected to a non-trusted port. DAI should build dynamic entries (ACLs) with IP addresses (obtained through DHCP) and corresponding MAC addresses for the phones and PCs. If a laptop with a statically configured IP address (in the y VLAN) is connected to a switch port associated to the y VLAN, the DAI should prevent the laptop from obtaining network connectivity; that is, it builds a deny ACL for this laptop.
Result	Passed

L2 Security–DHCP Snooping and Dynamic ARP Inspection on the Access Switch

Description	Set up to verify DHCP snooping and Dynamic ARP inspection on one of the access switches
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR

Procedure	1. Configure 802.1x port authentication on several of the switch ports along with DHCP snooping and DAI. 2. Configure AAA on the switch. 3. Configure the IP address of the RADIUS server. 4. Set up the EtherSwitch module as a NAS by providing its IP address in the Cisco Secure ACS server located in HQ. 5. Install a self-signed certificate on the ACS server. 6. Configure EAP-PEAP MSCHAPV2 authentication on the ACS server. 7. Download the ACS certificate onto one of the PCs that is running Windows XP and that is located in the branch office. 8. Install the certificate on the PC. 9. Configure the PC for EAP-PEAP MSCHAPV2 authentication. 10. Connect the IP Phone to the switch port on which 802.1x authentication is enabled. 11. Connect the PC to the switch port of the IP Phone. 12. Connect another PC that does not have the ACS certificate installed to another switch port on which 802.1x port authentication is enabled.
Pass/Fail Criteria	The traffic should be distributed 2:1 between the primary and secondary router. The standby router should take over control after the primary router is power cycled. When power returns to the primary router, it should take over control from the standby router after waiting for the preemption time to expire.
Result	Passed

L2 Security—Port Security on the Access Layer Switch

Description	Set up to verify port security on one of the access switches
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Configure the port security feature on one of the switch ports of the access switch to allow only one MAC address. 2. Configure the port security aging timer to be 2 seconds, and configure the port security violation policy to Restrict. 3. Connect a laptop to the switch port. 4. After the laptop gets an IP address through DHCP, disconnect the laptop and connect a different laptop to the same switch port.

Pass/Fail Criteria	When the laptop is connected to the switch port, it should get an IP address through DHCP. The switch should populate the laptop's MAC address and port information into a port security table. When another laptop with a different MAC address is connected to the same port, a port security violation error should be displayed on the console of the switch, and the new laptop should not be provided with an IP address.
Result	Passed

L2 Security—IP Source Guard on the Access Layer Switch

Description	Set up to verify IP source guard on one of the access switches
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Configure IP source guard on the switch ports. 2. Connect a traffic generator to the switch port on which the IP source guard is configured, and send line rate traffic to HQ. 3. Obtain the IP address of the traffic generator, using DHCP before sending the traffic. 4. After sending traffic for about 15 minutes, change the source MAC address of the traffic generator connected to the switch port, and observe the behavior.
Pass/Fail Criteria	The traffic from the traffic generator should be successfully allowed from the switch port and should reach the traffic generator at HQ. The IP source guard feature validates the source MAC address of the host that is connected to the switch port on which the IP source guard is enabled. It associates the host MAC address to the IP address obtained through DHCP. Once the traffic generator MAC address is changed, traffic should be dropped and not be allowed to pass from the switch port.
Result	Passed

L2 Security—BPDU Guard on the Access Layer Switch

Description	Set up to verify BPDU guard on one of the access switches
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR

Procedure	1. Configure Spanning Tree PortFast with the BPDU guard on the switch port that is connected to PC and phones. 2. Remove the PC or phone from one of the ports where BPDU guard is enabled, and connect another switch.

Pass/Fail Criteria	The phones and PC ports should be operational and able to send traffic normally after enabling BPDU guard. The port shut down after connecting the switch.

Result	Passed

QoS on the LAN

Description	Enable conditionally trusted IP Phone and PC and scavenger-class traffic (Advanced) Model Configuration on the Catalyst 2960 switches

Test Setup	Figure 43 on page 61, Traffic Flow to QoS Class Mapping Figure 42 on page 60, LAN Switch

Procedure

1. Enable QoS on the access layer switch. Re-mark all the packets coming from PC endpoints, servers, and so on, with appropriate CoS or DSCP values. Trust the voice and signaling packets coming out of Cisco IP Phones, but re-mark all the packets coming from PCs attached to the IP Phones. Use Ethereal to verify proper packet marking.
2. Enable MLS QoS on the Catalyst switches.
3. Configure CoS to DSCP mapping to map CoS 5 to DSCP EF.
4. Re-mark excess data VLAN traffic marked 0, AF11, AF21, CS3, DSCP 25, and AF41 to scavenger class (CS1).
5. Define class maps for real-time traffic, voice signaling, mission-critical data, and default (best effort).
6. Define policy maps and mark voice traffic to DSCP 46 (EF), voice signaling traffic to DSCP 24 (CS3), interactive video to DSCP 34 (AF41), mission-critical traffic to DSCP 25 (CS3), transactional data traffic to DSCP 18 (AF21), bulk data to DSCP 10 (AF11), and default to DSCP 0.
7. Configure policing (rate limiting) for each class.
8. Configure Catalyst switch egress queue in 1P3Q3T mode, that is, set up Q1 as the priority queue to carry all voice traffic, and set up the rest of the three queues in shared-bandwidth mode. Assign Q2 for mission-critical data traffic, Q3 for best-effort traffic, and Q4 for scavenger and bulk traffic. Configure shared weights of 70, 25, and 5 for Q2, Q3, and Q4, respectively.
9. Configure Weighted Tail Drop (WTD) thresholds per queue as shown in [Figure 43](#). For Q2 set the first threshold to 70% and the second threshold to 80%. For Q4, set the first threshold to 40% and the second threshold to 100%.
10. Verify, using the following **show** commands:
 - show mls qos**
 - show mls qos map**
 - show mls qos interface**
 - show mls qos interface policers**
 - show class-map**
 - show policy-map**
 - show policy interface**

Pass/Fail Criteria

Voice and data packets should be properly marked by the switches.

Excess traffic should be re-marked to scavenger class and dropped if the scavenger class limit is also exceeded.

Queuing should be engaged only during congestion.

Each traffic type should be properly queued based on the queue assignments.

Result

Passed

WAN Edge QoS—5 Class QoS Model

Description	Enable 5-class hierarchical QoS on the primary WAN interface
Test Setup	<pre> class-map match-all REALTIME match ip dscp ef af41 af42 ! VoIP and Interactive Video class-map match-any CALL-SIGNALING match ip dscp cs3 ! Old Call Signaling match ip dscp af31 ! New Call Signaling class-map match-all CRITICAL-DATA match ip dscp af21 af22 af31 cs6 ! Critical Data class-map match-all SCAVENGER match ip dscp cs1 ! Scavenger !</pre>
Procedure	1. Configure class maps for real-time, voice signaling, mission-critical data, scavenger data, and best-effort data. 2. Match voice, based on a DSCP value of 46, and also based on IP address/port number using ACLs. Port numbers range from 16384 to 32768. 3. Match voice signaling, based on a DSCP of CS3, and also based on IP address/port number using ACLs. Use port number range 2000 to 2002 for SCCP, 1720 for H.323, and 5060 to 5062 for SIP. 4. Match interactive video-based on a DSCP value of 34, and also based on IP address/port number using ACLs. Use port number range 16384 to 32768. 5. Match mission-critical data traffic-based on a DSCP value of 25, and also based on IP address/port number using ACLs. 6. Match transactional data traffic, based on a DSCP value of 18, and also based on IP address/port number using ACLs. 7. Match internetwork control traffic, based on a DSCP value of 48, and also based on IP address/port number using ACLs. 8. Match bulk/scavenger traffic, based on a DSCP value of 8, and also based on IP address/port number using ACLs. 9. Match best-effort traffic, based on a DSCP value of 0, and also based on IP address/port number using ACLs. 10. Verify whether packets are matched to the correct class map, using the show policy-map interface command.
Pass/Fail Criteria	Incoming traffic from the LAN interface of the router should be properly classified, based on the DSCP/CoS values present in the packet.
Result	Passed

LLQ for Voice and Interactive Video Traffic

Description	Enable LLQ for RTP traffic, which includes voice and video
Test Setup	<pre>policy-map FIVE-CLASS-V3PN-EDGE class REALTIME priority percent 28 ! VoIP and Interactive Video get 28% LLQ</pre>
Procedure	1. Configure strict priority queuing for voice and video traffic not exceeding 33% of the configured bandwidth. 2. Drop excess RTP traffic during link congestion. 3. Make voice and video calls, and also send background HTTP traffic. 4. Verify using show ip policy-map interface command.
Pass/Fail Criteria	RTP and data packets should be Cisco Express Forwarding switched. Voice traffic and video traffic should always be given priority, even during congestion, and they should not be dropped, provided they do not exceed their allocated bandwidth.
Result	Passed

CBWFQ and WRED for Data Traffic

Description	Configure CBWFQ for various types of data traffic, allocate bandwidth for each category, and configure WRED for congestion management
Test Setup	<pre>class CALL-SIGNALING bandwidth percent 5 ! Call signaling class MISSION-CRITICAL bandwidth percent 20 ! Mission-Critical-Data provisioning queue-limit 18 ! Optional: Anti-Replay tuning class SCAVENGER bandwidth percent 1 ! Scavenger class is throttled queue-limit 1 ! Optional: Anti-Replay tuning class class-default bandwidth percent 45 ! Best Effort needs BW guarantee queue-limit 16 ! Optional: Anti-Replay Tuning</pre>

Procedure

1. Allocate A% of bandwidth for mission-critical traffic, B% of bandwidth for transactional data traffic, C% for internetwork control traffic, D% for bulk/scavenger traffic, and the remaining bandwidth for best-effort traffic.
2. Configure DSCP-based WRED for mission-critical, transactional, and best-effort traffic. Retain default thresholds, and drop probabilities for WRED.
3. Send voice, video, and data traffic, and oversubscribe the bandwidth with data traffic.

The following data traffic types are mandatory:

- HTTP
- HTTPS
- FTP
- ICMP
- DNS

The following data traffic types are optional and based on availability of tools:

- CIFS
- SMTP
- POP3
- Citrix

Pass/Fail Criteria

Voice traffic and video traffic should always be given priority, even during congestion, and they should not be dropped, provided they do not exceed their allocated bandwidth. Excess data traffic not conforming to the allocated bandwidth should be dropped based on WRED and DSCP. WRED should minimize tail drops for high-priority traffic.

Result

Passed

Traffic Shaping on Different WAN Links**Description**

Enable traffic shaping on the WAN interface as part of the hierarchical QoS configuration

Test Setup

[Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode](#), or

[Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode](#), or

[Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode](#), or

[Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode](#)

Procedure	1. Configure traffic shaping on the WAN links to shape the egress traffic to 95% of the available bandwidth. 2. Send voice and data traffic to oversubscribe bandwidth.
Pass/Fail Criteria	The egress traffic should be shaped to an average of 95% of the total available bandwidth.
Result	Passed

DSCP/CoS Marking Incoming/Returning Traffic from WAN to LAN

Description	Re-mark ingress traffic to the router coming from the WAN and going to the LAN
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure DSCP to CoS mapping for the various ingress traffic types from the WAN. The marking should match the DSCP value of similar or the same type of traffic egressing the WAN interface. 2. Verify using the show policy-map interface command and using the Ethereal packet sniffer on the LAN.
Pass/Fail Criteria	The ingress traffic should be properly marked.
Result	Passed

Modification and Deletion of ACLs Defined with Class Map match access-group Command

Description	Modify or delete ACLs defined under class-map configuration mode using match access-group statements
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode

Procedure	1. Change ACLs' source and destination IP addresses. 2. Change ACLs' source and destination ports. 3. Delete ACLs. 4. Save configuration. 5. Run traffic while making the changes.
Pass/Fail Criteria	The ACL changes or deletions should not have no adverse impact on the router such as tracebacks, memory leaks, or a crash. The changes should be properly handled and applied to the traffic stream.

Result Passed

Unconfigure and Reconfigure QoS

Description	Remove QoS configuration, and reapply QoS configuration
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Remove QoS configuration. 2. Reapply QoS configuration.
Pass/Fail Criteria	There should be no adverse impact on the router such as tracebacks, memory leaks, or a crash.
Result	Passed

Unconfigure QoS, Reload Router, and Reconfigure QoS

Description	Remove QoS configuration, and reapply QoS configuration after router reload
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Remove the entire hierarchical QoS configuration from the branch router. 2. Reload the router. 3. Reapply the configuration to the branch router while running traffic.
Pass/Fail Criteria	There should be no adverse impact on the router such as tracebacks, memory leaks, or a crash.
Result	Passed

OSPF Routing as IGP Between Branch and Headquarters Network

Description	Enable OSPF between the branch router and headend router, and advertise each other's LAN addresses
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Configure OSPF routing between the branch router and the headend router. 2. Advertise all the LAN addresses attached to the branch and the LAN addresses attached to the headend so that the headend router can see the branch network and vice versa. 3. Redistribute connected and static routes in the branch and headend into OSPF. 4. Verify by OSPF adjacency, using the show ip ospf neighbors command. 5. Verify by pinging from the branch LAN to the headend LAN and vice versa.
Pass/Fail Criteria	OSPF adjacency should be established between the branch router and the headend router.
Result	Passed

EIGRP Routing as IGP Between the Branch Router and the Headquarters Router

Description	Enable EIGRP between the branch router and headend router and advertise each other's LAN addresses
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Configure EIGRP routing between the branch router and the headend router. 2. Advertise all the LAN addresses attached to the branch and the headend so that the headend router can see the branch network and vice versa. 3. Redistribute connected and static routes in the branch and headend into EIGRP. 4. Verify by EIGRP adjacency, using the show ip eigrp neighbors command. 5. Verify by pinging from the branch LAN to the headend LAN and vice versa.
Pass/Fail Criteria	EIGRP adjacency should be established between the branch router and the headend router. Ping should be 100% successful.
Result	Passed

Traffic Measurement Using NetFlow When QoS is Enabled on the Branch Router

Description	Enable NetFlow on the branch router
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Configure NetFlow version 5 or version 9 for both ingress and egress traffic on the WAN and LAN interfaces of the branch router. 2. Send bidirectional HTTP, FTP, and voice traffic between the branch and the headend router. 3. Collect protocol distribution charts, interface statistics, and QoS statistics. 4. Export the statistics to a network analysis module (NAM) located at the enterprise headquarters.
Pass/Fail Criteria	NetFlow should collect the statistics and export it to the NAM. The collected statistics should be within performance requirements.
Result	Passed

NBAR Classification with QoS

Description

Enable NBAR protocol discovery and classification. With the help of QoS, provide bandwidth guarantees for certain traffic flows, and drop certain distributed denial of service (DDoS) traffic such as SQL slammer and worms such as CODE RED, NIMDA, and so on.

Test Setup

```
ip nbar port-map custom-02 udp 1434 ! SQL Slammer custom PDL
ip nbar port-map custom-03 tcp 5554 9996 ! Sasser custom PDL
class-map match-all SQL-SLAMMER
match protocol custom-02 ! Matches the SQL Slammer PDL
match packet length min 404 max 404 ! Matches the packet length
(376+28)
!
class-map match-any WORMS
match protocol http url "*.ida*" ! CodeRed
match protocol http url "*cmd.exe*" ! CodeRed
match protocol http url "*root.exe*" ! CodeRed
match protocol http url "*readme.eml*" ! NIMDA
match class-map SQL-SLAMMER ! SQL Slammer class-map
match protocol custom-03 ! Sasser custom PDL
!
policy-map WORM-DROP
class WORMS
drop ! Drops all known worms
!
interface GigabitEthernet0/0.1
description DATA VLAN SUBNET
encapsulation dot1Q 301
ip address 10.0.0.1 255.255.255.0
service-policy input WORM-DROP ! Drops known worms (DVLAN only)
!
```

Procedure

1. Configure NBAR protocol discovery on the interfaces, and match protocol statements in the QoS policy map.
 - Mark HTTP traffic to a certain URL, such as <http://example.com> as mission critical.
 - Mark all other HTTP traffic as best effort.
 - Limit bulk traffic such as FTP.
 - Mark all voice traffic as critical.
2. Provide bandwidth guarantees by specifying bandwidth percentage in the QoS policy map configuration for different classes of traffic.
 - For mission-critical traffic, provide X% bandwidth.
 - For voice traffic, provide Y% bandwidth.
 - For transactional traffic, provide Z% bandwidth.
 - For all other traffic, provide the remaining bandwidth.
3. Measure the various traffic flows, using NBAR.
4. Send HTTP, FTP, and voice traffic.

Pass/Fail Criteria NBAR should properly classify the different protocols and provide bandwidth guarantees based on the policy map configuration. NBAR should provide the percentage breakdown of various protocols traversing the LAN and WAN links. NBAR should drop worm packets.

Result Passed

Modify Match Protocol Statements and Bandwidth Percentage

Description Modify “match protocol” statements and bandwidth percentage in the policy map configuration

Test Setup [Figure 105 on page 250, Private WAN, Cisco 1841 ISR](#)
[Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR](#)

Procedure Modify the match protocol statements in the NBAR configuration by adding more protocols, changing the existing HTTP URL, and modifying the percentage bandwidth allocated for each traffic class over a live network

Pass/Fail Criteria Changes should not cause any abnormal behavior in the branch router such as tracebacks, memory leaks, or crashes. Changes should be applied to traffic.

Result Passed

100 ACLs

Description Configure about 100 ACLs on the branch router

Test Setup [Figure 105 on page 250, Private WAN, Cisco 1841 ISR](#)
[Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR](#)

Procedure

1. Configure about 100 ACLs, either dummy ACLs or ACLs matching certain hosts or networks.
2. At the end of the list configure a **permit ip any any** statement.
3. Configure the ACL on the primary and secondary WAN interface.
4. Send data traffic.

Pass/Fail Criteria If a packet does not match any of the statements in the list, the packet should match the **permit ip any any** statement at the end of the list and be allowed to pass through. If the packet matches any statement in the last, appropriate action such as permit or deny should be taken, depending on what is configured in the ACL statement.

Result Passed

NTP in the Branch Router

Description	NTP in the branch router
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure NTP in the branch to source the clock from an NTP server in the network. The NTP server could be local to the branch, or it could be located in either the headquarters or the service provider premises. 2. Configure Message Digest 5 (MD5) authentication for NTP. 3. Verify, using the show ntp status command.
Pass/Fail Criteria	NTP should be sourced from the NTP server after successful authentication.
Result	Passed

Branch Router as a DHCP Server

Description	Branch router as a DHCP server
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Configure a DHCP server on the branch router to provide IP addresses for DHCP clients such as IP Phones and PCs. 2. Verify, using the show ip dhcp binding and show ip dhcp server statistics commands.
Pass/Fail Criteria	The DHCP server on the router should be able to provide IP addresses to the clients using DHCP.
Result	Passed

IP SLA VoIP UDP Jitter Codec G.711 u-law (Branch to HQ)

Description	Set up for verification of the service level agreement (SLA) for VoIP UDP jitter SLA																		
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode																		
Procedure	1. Enable the IP SLA responder on the HQ router. 2. Configure a basic type of VoIP UDP jitter operation on the branch router. 3. Configure any available options, such as codec G.711 u-law for a VoIP UDP jitter SLAs operation type. 4. Configure any threshold conditions, if required. 5. Schedule the operation to run, and then allow the operation to run for enough time to gather statistics. 6. Display and interpret the results of the operation, using Cisco IOS CLI or using an NMS system using SNMP.																		
Pass/Fail Criteria	To view and interpret the results of an IP SLA operation, use the show ip sla monitor statistics command, and check that the boundaries are within limits. For example, <table><tr><th>ICPIF Range</th><th>MOS</th><th>Quality</th></tr><tr><td>0–3</td><td>5</td><td>Best</td></tr><tr><td>4–13</td><td>4</td><td>High</td></tr><tr><td>14–23</td><td>3</td><td>Medium</td></tr><tr><td>24–33</td><td>2</td><td>Low</td></tr><tr><td>34–43</td><td>1</td><td>Poor</td></tr></table>	ICPIF Range	MOS	Quality	0–3	5	Best	4–13	4	High	14–23	3	Medium	24–33	2	Low	34–43	1	Poor
ICPIF Range	MOS	Quality																	
0–3	5	Best																	
4–13	4	High																	
14–23	3	Medium																	
24–33	2	Low																	
34–43	1	Poor																	
Result	Passed																		

IP SLA VoIP UDP Jitter Codec G.729A u-law (Branch to HQ)

Description	Set up verification of the service level agreement (SLA) for VoIP UDP jitter SLA																		
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode																		
Procedure	1. Enable the IP SLA responder on the HQ router. 2. Configure a basic type of VoIP UDP jitter operation on the branch router. 3. Configure any available options, such as codec G.729A u-law for a VoIP UDP jitter SLA operation type. 4. Configure any threshold conditions, if required. 5. Schedule the operation to run, and then allow the operation to run for enough time to gather statistics. 6. Display and interpret the results of the operation, using Cisco IOS CLI or using an NMS system using SNMP.																		
Pass/Fail Criteria	To view and interpret the results of an IP SLA operation, use the show ip sla monitor statistics command and check that the boundaries are within limits. For example, <table><tr><th>ICPIF Range</th><th>MOS</th><th>Quality</th></tr><tr><td>0–3</td><td>5</td><td>Best</td></tr><tr><td>4–13</td><td>4</td><td>High</td></tr><tr><td>14–23</td><td>3</td><td>Medium</td></tr><tr><td>24–33</td><td>2</td><td>Low</td></tr><tr><td>34–43</td><td>1</td><td>Poor</td></tr></table>	ICPIF Range	MOS	Quality	0–3	5	Best	4–13	4	High	14–23	3	Medium	24–33	2	Low	34–43	1	Poor
ICPIF Range	MOS	Quality																	
0–3	5	Best																	
4–13	4	High																	
14–23	3	Medium																	
24–33	2	Low																	
34–43	1	Poor																	
Result	Passed																		

IP SLA ICMP Echo (Branch to HQ)

Description	Set up verification of the service level agreement (SLA) for ICMP echo
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Enable the IP SLA responder on the HQ router. 2. Configure ICMP echo operation type on the branch router. 3. Configure any options available for SLAs operation type. 4. Configure any threshold conditions, if required. 5. Schedule the operation to run, and then allow the operation run for enough time to gather statistics. 6. Display and interpret the results of the operation, using Cisco IOS CLI or using an NMS system using SNMP. For example <pre> ip sla monitor 6 type echo protocol ipIcmpEcho 192.168.0.2 source-ipaddr 192.168.0.1 frequency 300! ip sla monitor schedule 6 life forever start-time now </pre>
Pass/Fail Criteria	To view and interpret the results of an IP SLA operation, use the show ip sla monitor 6 command to verify details, and report any significant delay issues.
Result	Passed

IPsec Site-to-Site VPN Using DMVPN

Description	Setup an IPsec site-to-site VPN between the branch router and the headend router, using DMVPN.
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR

Procedure	1. Install the AIM-VPN/SSL-3 module on the motherboard of the branch router. 2. Configure the headend router as a DMVPN hub and Next Hop Resolution Protocol (NHRP) server with multipoint GRE. 3. Configure the branch router as a spoke with multipoint GRE. 4. Configure ISAKMP policy preshared authentication with 3-DES encryption for the keys. 5. Configure ISAKMP SA lifetime to be 3600. 6. Configure transform set with 3-DES, ESP-SHA, DH Group 2 and preshared keys. 7. Configure IPsec SA lifetime to be 86400. 8. Configure tunnel protection for the DMVPN tunnel interface. 9. Add the DMVPN tunnel interface network address to the IGP configuration. 10. Verify IPsec connectivity, using the following show commands: • show crypto isakmp sa • show crypto ipsec sa • show crypto engine connections active 11. Send a sweep ping from a host connected to the branch data VLAN to a host connected to the headquarters data VLAN. 12. Verify whether the ping traffic gets encrypted; use the show crypto engine accelerator statistics command.
Pass/Fail Criteria	ISAKMP and IPsec sessions should be established. The DMVPN tunnel line protocol should come up. Routing tables at both the branch and headquarters routers should be updated. Ping should be 100% successful. Ping traffic should be encrypted.
Result	Passed
IPsec Using GETVPN	
Description	Set up an IPsec VPN between the branch router and the headend router, using GETVPN
Test Setup	Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR

Procedure	1. Install the AIM-VPN/SSL-3 module on the motherboard of the branch router. 2. Set up a GDOI key server for GETVPN in headquarters. The key server can be a Cisco 1800 series ISR platform. 3. Configure the key server to send unicast rekeys. 4. Configure the network segments associated with branch and headquarters LANs for encryption, using an ACL. Associate the ACL to the GDOI SA. 5. Configure AES 256-bit encryption for IPsec. 6. Configure a rekey timeout of 10800 seconds. 7. Configure antireplay protection. 8. Configure the branch routers and the headend routers as group members. 9. Configure the GDOI crypto map on the primary WAN interface of the branch router and the headend router. 10. Configure the TCP maximum segment size (MSS) to 1360 bytes on the router interfaces. 11. Register the group members to the key server. 12. Send a sweep ping from a host connected to the branch data VLAN to a host connected to the headquarters data VLAN. 13. Verify whether the ping traffic gets encrypted; use the show crypto engine accelerator statistics command. 14. Verify GETVPN, using the following show commands: • show crypto isakmp sa • show crypto ipsec sa • show crypto engine connections active
Pass/Fail Criteria	Group members should be registered to the key server. The key server should successfully push the IPsec SA ACL and rekey the ACL to the group members. The routing tables at both the branch and head quarters routers should be updated. Ping should be 100% successful. Ping traffic should be encrypted.
Result	Passed

GETVPN Unicast Rekeying

Description	GETVPN unicast rekeying
Test Setup	Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Set up a GDOI key server for GETVPN in the headquarters. The key server can be a Cisco 1800 series ISR platform. 2. Configure the key server to send unicast rekeys. 3. Configure the network segments associated with the branch and headquarters LANs for encryption, using an ACL. Associate the ACL to the GDOI SA. 4. Configure AES 256-bit encryption for IPsec. 5. Configure a rekey timeout of 10800 seconds. 6. Configure the branch router(s) and the headend router (s) as group members. 7. Configure the GDOI crypto map on the primary WAN interface of the branch router and headend router. 8. Register the group members to the key server. 9. Verify rekeying functionality. 10. Use the show crypto isakmp sa command to verify.
Pass/Fail Criteria	Group members should be registered to the key server. The key server should be able to successfully push the ACL for unicast rekeying to the group members. After the rekey timeout, the key server should send new keys to the group members. For some time, both old keys and new keys should be present in group members. The new key should take over after a certain amount of time, usually within a minute.
Result	Passed

GETVPN Multicast Rekeying

Description	GETVPN multicast rekeying
Test Setup	Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Set up a GDOI key server for GETVPN in the headquarters. The key server can be a Cisco 1800 series ISR platform. 2. Configure the key server to send multicast rekeys, with unicast rekeys as a backup mechanism. 3. Define an ACL for multicast rekeying in the key server, and use the 239.x.x.x multicast group for rekeying. 4. Configure PIM sparse mode (PIM-SM) on the key server and all the group members. 5. Configure the headend router as the rendezvous point (RP). 6. Configure the network segments associated with the branch and headquarters LANs for encryption, using an ACL. Associate the ACL to the GDOI SA. 7. Configure AES 256-bit encryption for IPsec. 8. Configure a rekey timeout of 10800 seconds. 9. Configure the branch router(s) and the headend router(s) as group members. 10. Configure the GDOI crypto map on the primary WAN interface of the branch router and the headend router. 11. Register the group members to the key server. 12. Verify rekeying functionality. 13. Use the show crypto isakmp sa command to verify.
Pass/Fail Criteria	Group members should be registered to the key server. The key server should be able to successfully push the ACL for multicast rekeying to the group members. Group members should register to the 239.x.x.x multicast group successfully. After the rekey timeout, the key server should send new keys to the multicast group. For some time, both old keys and new keys should be present in group members, and the new key should take over after a certain amount of time, usually within a minute.
Result	Passed

IPsec DMVPN with Prefragmentation

Description	IPsec DMVPN with prefragmentation
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Configure IPsec VPN between the branch and headquarters with a tunnel MTU of 1000 bytes. 2. Enable prefragmentation. 3. Send voice and data traffic through the IPsec VPN tunnel.
Pass/Fail Criteria	The IPsec packets that are larger than 1000 bytes should be fragmented.
Result	Passed

IPsec DMVPN and IGP

Description	IPsec DMVPN and IGP
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Bring down the IPsec tunnel between the branch and the headquarters router. 2. Verify whether the routing table is updated at both the branch and headquarters routers. 3. After 3 minutes, bring up the IPsec tunnel between the branch and headquarters routers. 4. Verify whether the routing table is updated at both the branch and headquarters routers.
Pass/Fail Criteria	When the IPsec tunnel goes down, the routing tables at both the branch and headquarters are updated. At the branch, the headquarters becomes unreachable, and the routes should be removed from the routing table. Similarly, at the headquarters, the branch becomes unreachable, and routes should be removed from the routing table. When the tunnel comes back up, the routes at both the branch and headquarters should reappear.
Result	Passed

DMVPN Backup for MPLS Network (Branch to HQ)

Description	DMVPN backup on small branch using static floating route (Spoke-to-HQ)
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. On the small branch Cisco 1841 router, configure the serial interface on the branch that connects to the Internet Cloud router for frame-relay. 2. Configure the static route in the branch router to reach to HQ with higher administrative distance (for example, 240). 3. Redistribute the static route into the IGP on the branch router. 4. Make sure that the entire traffic flow is going through the MPLS network when the branch WAN is up and running. 5. Shut down the WAN and verify that the IP traffic flows to HQ using the Internet Cloud.
Pass/Fail Criteria	Verify that you can reach HQ from the branch when the primary WAN is down.
Result	Passed

DMVPN Backup for MPLS Network (Branch to Branch)

Description	DMVPN backup on small branch using static floating route (Spoke-to-Spoke)
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. On the small branch Cisco 1841 router, configure the serial interface on the branch that connects to the Internet Cloud router for frame-relay. 2. Configure the static route in the branch router to reach to HQ with higher administrative distance (for example, 240). 3. Redistribute the static route into the IGP on the branch router. 4. Make sure that the entire traffic is going through the MPLS network when the branch WAN is up and running. 5. Shut down the WAN and verify that IP traffic flows to HQ through the Internet Cloud. 6. Verify that from small branch running DMVPN that you can reach the small branch when the WAN link is down. 7. Check the DMVPN hub for the NHRP database for all the spoke addresses (registered branch address). 8. Verify that a dynamic tunnel has been created between the small branch and the small branch.

Pass/Fail Criteria Verify that you can reach HQ and the small branch from the small branch when the primary WAN is down.

Result Passed

DMVPN Backup for MPLS Network Using BFD (Branch to HQ)

Description DMVPN backup with BFD using EIGRP as IGP (Branch to HQ)

Test Setup [Figure 105 on page 250, Private WAN, Cisco 1841 ISR](#)
[Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR](#)

- Procedure**
1. Configure the primary WAN interface and secondary WAN interface on the branch router.
 2. Configure the secondary WAN interface as a Frame Relay interface that accesses the Internet.
 3. Configure DMVPN on the branch router.
 4. Configure the secondary WAN to be a higher cost route than the primary WAN so that primary WAN is always the preferred route.
 5. Configure BFD on the primary WAN interface of the branch router and the primary WAN interface of the head-end router with a BFD interval of 50 ms, min_rx of 50 ms, and a BFD multiplier of 5.
 6. Configure BFD on the secondary WAN interface.
 7. Enable BFD for all interfaces in the EIGRP routing process.
 8. Verify whether BFD is up and running by issuing **show bfd neighbor** command
 9. Send HTTP and voice traffic between the branch and HQ.
 10. Bring down the primary WAN interface by either disconnecting the cable or shutting down the link on the head-end side.
 11. After about three minutes, bring up the primary WAN interface.

Pass/Fail Criteria Verify that, when the primary WAN fails, EIGRP reconvergence occurs within a second because of BFD.

Verify that all the traffic is routed through the secondary WAN interface.

Verify that voice and HTTP sessions are maintained during reconvergence.

Verify that, when the primary WAN comes up after three minutes, the traffic is routed over the primary WAN interface.

Result Passed

DMVPN Backup for MPLS Network Using BFD (Branch to Branch)

Description	DMVPN backup with BFD using EIGRP as IGP (Branch to Branch)
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Configure the primary WAN interface and secondary WAN interface on the branch router. 2. Configure the secondary WAN interface as a Frame Relay interface that assesses the Internet. 3. Configure DMVPN on the branch router. 4. Configure the secondary WAN to be a higher cost route than the primary WAN so that primary WAN is always the preferred route. 5. Configure BFD on the primary WAN interface of the branch router and the primary WAN interface of the head-end router with BFD interval of 50 ms, min_rx of 50 ms, and a BFD multiplier of 5. 6. Configure BFD on the secondary WAN interface. 7. Enable BFD for all interfaces in the EIGRP routing process. 8. Verify whether BFD is up and running by issuing show bfd neighbor command. 9. Send HTTP and voice traffic between the branch and HQ. 10. Bring down the primary WAN interface by either disconnecting the cable or shutting down the link on the head-end side. 11. After about three minutes, bring up the primary WAN interface.
Pass/Fail Criteria	Verify that, when the primary WAN fails, EIGRP reconvergence occurs within a second because of BFD. Verify that all the traffic is routed through the secondary WAN interface. Verify that voice and HTTP sessions are maintained during reconvergence. Verify that, when the primary WAN comes up after three minutes, the traffic is routed over the primary WAN interface.
Result	Passed

DMVPN Backup for MPLS Network Using BFD IGP as OSPF (Branch to Branch)

Description	DMVPN backup with BFD using OSPF as IGP (Branch to Branch)
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR

Procedure	1. Configure the primary WAN interface and secondary WAN interface on the branch router. 2. Configure the secondary WAN interface as a Frame Relay interface that assesses the Internet. 3. Configure DMVPN on the branch router. 4. Configure the secondary WAN to be a higher cost route than the primary WAN so that primary WAN is always the preferred route. 5. Configure BFD on the primary WAN interface of the branch router and the primary WAN interface of the head-end router with BFD interval of 50 ms, min_rx of 50 ms, and a BFD multiplier of 5. 6. Configure BFD on the secondary WAN interface. 7. Enable BFD for all interfaces in the EIGRP routing process. 8. Verify whether BFD is up and running by issuing show bfd neighbor command. 9. Send HTTP and voice traffic between the branch and HQ. 10. Bring down the primary WAN interface by either disconnecting the cable or shutting down the link on the head-end side. 11. After about three minutes, bring up the primary WAN interface.
Pass/Fail Criteria	Verify that, when the primary WAN fails, EIGRP reconvergence occurs within a second because of BFD. Verify that all the traffic is routed through the secondary WAN interface. Verify that voice and HTTP sessions are maintained during reconvergence. Verify that, when the primary WAN comes up after three minutes, the traffic is routed over the primary WAN interface.
Result	Passed

DMVPN Backup for MPLS Network Using EBGp (Branch to HQ)

Description	DMVPN backup for MPLS using EBGp
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR

Procedure	1. Configure the primary WAN interface and backup WAN interface on the branch router. 2. Configure the secondary WAN interface as a Frame Relay interface that assesses the Internet. 3. Configure DMVPN on the branch router. 4. Configure EBGp peers with the Internet router on the branch router. Under normal conditions, when the primary WAN is up and running, the backup DMVPN is dormant. 5. Shut down the primary WAN interface. The backup interface should come up and the EBGp peers become activated. Finally, the DMVPN should come up. 6. Send 2 Mb/s of traffic from the backup interface (DMVPN is up) and check the QoS status and various queues. 7. Send HTTP and Voice traffic between the branch and HQ 8. After about three minutes, bring up the primary WAN interface
Pass/Fail Criteria	Verify that, when the primary WAN fails, the backup DMVPN comes up. Verify that voice and HTTP sessions pass through. Check for appropriate QoS Queues. When the primary comes up after three minutes, verify that the traffic is routed over the primary WAN interface.
Result	Passed
DMVPN with QoS	
Description	DMVPN with QoS
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure the 5-class QoS model as explained in the QoS test cases. 2. Configure DMVPN with the qos pre-classify command to classify IPsec packets before encryption. 3. Send voice and data traffic, and verify whether traffic going through the DMVPN tunnel gets the correct QoS treatment, such as voice put in strict priority queue with proper bandwidth percentages applied.

Pass/Fail Criteria	The IPsec packets should get the correct QoS treatment.
Result	Passed
GETVPN with QoS	
Description	GETVPN with QoS
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure the 5-class QoS model as explained in the QoS test cases. 2. Configure GETVPN with the qos pre-classify command to classify IPsec packets before encryption. 3. Send voice traffic and data traffic, and verify whether traffic going through the GETVPN gets the correct QoS treatment, such as voice put in strict priority queue with proper bandwidth percentages applied.
Pass/Fail Criteria	The IPsec packets should get the correct QoS treatment.
Result	Passed
DMVPN with QoS and NBAR	
Description	DMVPN with QoS and NBAR
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode

Procedure	1. Configure the 5-class QoS model as explained in the QoS test cases. 2. Configure NBAR with the custom ip nbar port-map and ip nbar protocol-discovery commands as in the NBAR test case. 3. Configure DMVPN with the qos pre-classify command to classify IPsec packets before encryption. 4. Send voice and data (HTTP, FTP, and ICMP) traffic, and verify whether traffic going through the DMVPN tunnel gets the correct NBAR and QoS treatment, such as voice put in the strict priority queue with the proper bandwidth percentages applied.
Pass/Fail Criteria	QoS and NBAR classification and bandwidth guarantees should be given to the voice and data traffic egressing the WAN interface before encryption.
Result	Passed

GETVPN with QoS and NBAR

Description	GETVPN with QoS and NBAR
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure the 5-class QoS model as explained in the QoS test cases. 2. Configure NBAR with the custom ip nbar port-map and ip nbar protocol-discovery commands as in the NBAR test case. 3. Configure GETVPN with the qos pre-classify command to classify IPsec packets before encryption. 4. Send voice and data (HTTP, FTP, and ICMP) traffic and verify whether traffic going through the IPsec tunnel gets the correct NBAR and QoS treatment, such as voice put in the strict priority queue with the proper bandwidth percentages applied.
Pass/Fail Criteria	QoS and NBAR classification and bandwidth guarantees should be given to the voice and data traffic egressing the WAN interface before encryption.
Result	Passed

DMVPN/GETVPN with QoS, NBAR, and NetFlow

Description	DMVPN/GETVPN with QoS, NBAR and NetFlow
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure the 5-class QoS model as explained in the QoS test cases. 2. Configure NBAR with custom ip nbar port-map and ip nbar protocol-discovery commands as in the NBAR test case. 3. Configure NetFlow version 5 or version 9 for both ingress and egress traffic on the WAN and LAN interfaces of the branch router. 4. Configure IPsec with the qos pre-classify command to classify IPsec packets before encryption. 5. Send voice and data (HTTP, FTP, and ICMP) traffic, and verify whether traffic going through the IPsec tunnel gets the correct NBAR and QoS treatment, such as voice put in the strict priority queue with the proper bandwidth percentages applied. 6. Collect protocol distribution charts, interface statistics, and QoS statistics. Export the statistics to a NAM at the enterprise headquarters.
Pass/Fail Criteria	QoS and NBAR classification and bandwidth guarantees should be given to the voice and data traffic egressing the WAN interface before encryption NetFlow should collect the statistics and export them to the NAM, and the collected statistics should be within performance requirements.
Result	Passed

Zone-based Policy Firewall Configuration on the Branch Router

Description	Configure Zone-based Policy Firewall (ZPF) with three zones: Public, Private, and DMZ
Test Setup	<pre> class-map type inspect match-any publicPrivateOutRule10Protocols match protocol http match protocol https match protocol dns match protocol ssh match protocol icmp match protocol ftp exit class-map type inspect match-any publicDMZOutRule10Protocols match protocol http match protocol https match protocol dns exit class-map type inspect match-all publicPrivateOutRule10 match access-group name publicPrivateOutRule10Acl match class-map publicPrivateOutRule10Protocols exit ip access-list extended publicPrivateOutRule10Acl permit ip 172.16.0.0 0.0.0.255 any exit policy-map type inspect publicPrivateOutFwPolicy class type inspect publicPrivateOutRule10 inspect publicPrivateOutParamMap class class-default drop log exit policy-map type inspect publicDMZOutFwPolicy class type inspect publicDMZOutRule10Protocols inspect publicPrivateOutParamMap class class-default drop log exit parameter-map type inspect publicPrivateOutParamMap alert on audit-trail on dns-timeout 5 icmp idle-time 10 max-incomplete low 2000 max-incomplete high 3000 one-minute low 2000 one-minute high 3000 tcp finwait-time 5 tcp idle-time 3600 tcp max-incomplete host 50 block-time 0 tcp synwait-time 30 udp idle-time 30 </pre>

**Test Setup
(continued)**

```

zone security Public
description Public Internet Connection
exit

zone security Private
description Customer Private Network
exit

interface Serial0/1/0:0.500
zone-member security Public
exit

interface Serial0/1/1:0.500
zone-member security Private
exit

interface FastEthernet0/0
zone-member security Private
exit

zone-pair security publicPrivateOut source Private destination
Public
description Outbound Firewall Policy from Private to Public
service-policy type inspect publicPrivateOutFwPolicy
exit
zone-pair security publicDMZOut source Public destination DMZ
description Outbound Firewall Policy from Public to DMZ
service-policy type inspect publicDMZOutFwPolicy
exit

```

Procedure

1. Create the firewall policy.
Referring to the test setup, the steps for creating zone-based policy firewall are outlined below.
2. Create the class maps to classify network traffic.
3. Create the policy map (firewall policy).
4. Create the Inspect Parameter-Map.
5. Create the security zones: Public, Private, and DMZ.
6. Assign the interfaces to the security zones (zone membership).
7. Assign the primary WAN interfaces to the Private zone.
8. Assign the voice and data VLANs to the Private zone.
9. Assign the DMZ VLAN to the DMZ zone.
10. Assign secondary WAN interface to Public zone.
11. Create the zone pairs in the test setup, and assign a policy map (firewall policy).
12. Send various kinds of traffic, such as HTTP, HTTPS, DNS, FTP, and ICMP, between the zones.

Pass/Fail Criteria	From Private zone to Private zone all traffic should be passed without any inspection. From Private zone to Public zone, HTTP, FTP, DNS, HTTPS, SSH, and ICMP traffic should be inspected and allowed, and the rest of the traffic should be blocked. From Public zone to Private zone, no traffic should be allowed. From Public zone to DMZ zone, only HTTP, FTP, and DNS should be allowed.
Result	Passed

NAT and PAT Configuration on the Branch Router

Description	Configure NAT and PAT for traffic going out to the Internet
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Configure static NAT translations for certain hosts on the data VLAN, using an address pool. 2. For the rest of the hosts, configure PAT by using the overload command in the NAT configuration. 3. Configure the secondary WAN interface as the interface connecting to the Internet through the ISP. 4. Configure the LAN as NAT inside, and configure the secondary WAN interface as NAT outside. 5. Send HTTP, HTTPS, ICMP, DNS, and SSH traffic from clients on the LAN to the Internet. 6. Verify translations and statistics using the show ip nat translations and show ip nat statistics commands.
Pass/Fail Criteria	The inside address should be translated to the outside global address when the traffic from the LAN is going out to the Internet. The return traffic from the Internet to the LAN should always be directed to the outside global address of the inside hosts.
Result	Passed

NAT, QoS, and NetFlow on the Branch

Description	Configure NAT and QoS on the branch
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR

Procedure

1. Configure static NAT translations for certain hosts on the data VLAN using an address pool and for the rest of the hosts configure PAT by using the **overload** command in the NAT configuration.
2. Configure the secondary WAN interface as the interface connecting to the Internet through the ISP.
3. Configure 5-class H-QoS on the secondary WAN interface.
4. Mark all the traffic going out to the Internet as best-effort traffic.
5. Configure traffic shaping to 95% of the available WAN bandwidth.
6. Configure NetFlow on the secondary WAN interface for ingress and egress traffic.
7. Collect traffic statistics and distribution charts, and export the statistics to a NAM, using either v5 or v9 NetFlow.
8. Send HTTP, HTTPS, ICMP, DNS and SSH traffic from clients on the LAN to the Internet.
9. Verify translations and statistics, using the **show ip nat translations** and **show ip nat statistics** commands.
10. Verify QoS, using the **show policy-map interface** command.
11. Verify NetFlow, using the **show ip flow** command.

Pass/Fail Criteria

The inside address should be translated to the outside global address when the traffic from the LAN is going out to the Internet. The return traffic from the Internet to the LAN should always be directed to the outside global address of the inside hosts.

All the Internet traffic should be marked as best effort.

Traffic should be shaped to 95% of the WAN bandwidth.

The NetFlow statistics collected should be within performance requirements.

Result

Passed

ZPF, QoS, and NetFlow on the Branch**Description**

Configure ZPF, QoS, and NetFlow on the branch router

Test Setup

[Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode,](#)

[Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode,](#)

[Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode,](#)

[Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode](#)

Procedure

1. Configure ZPF as explained in the [Zone-based Policy Firewall Configuration on the Branch Router](#) test case procedure.
2. Configure the secondary WAN interface as the interface connecting to the Internet through the ISP.
3. Assign the primary WAN interface to the Private zone.
4. Assign the secondary WAN interface to the Public zone.
5. Assign the voice VLAN and data VLAN interfaces to the Private zone.
6. Configure 5-class hierarchical QoS on both the primary and secondary WAN interfaces.
7. Mark all the traffic going out to the Internet as best-effort traffic.
8. Configure traffic shaping to 95% of the available WAN bandwidth.
9. Configure NetFlow on the WAN and LAN interfaces for ingress and egress traffic.
10. Collect traffic statistics and distribution charts, and export the statistics to a NAM, using NetFlow version 5 or version 9.
11. Send HTTP, HTTPS, ICMP, DNS, and SSH traffic from clients on the LAN to the Internet.
12. Send bidirectional HTTP, HTTPS, and FTP traffic between the branch and headquarters.
13. Ping one of the clients on the LAN from the ISP.
14. Verify translations and statistics, using the **show ip nat translations** and **show ip nat statistics** command.
15. Verify QoS, using the **show policy-map interface** command.
16. Verify NetFlow, using the **show ip flow** command.

Pass/Fail Criteria

Traffic from the branch to headquarters should not be inspected.

Traffic from the branch to the Internet should be inspected.

QoS should be applied to the traffic, and ZPF should have no adverse effect on the QoS.

All the Internet traffic should be marked as best effort.

Traffic should be shaped to 95% of the WAN bandwidth.

The NetFlow statistics collected should be within performance requirements.

The ping should fail.

Result

Passed

ZPF, QoS, NBAR, and NetFlow on the Branch

Description	Configure ZPF, QoS, NBAR, and NetFlow on the branch router
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure ZPF as explained in the Zone-based Policy Firewall Configuration on the Branch Router test case procedure. 2. Configure the secondary WAN interface as the interface connecting to the Internet through the ISP. 3. Assign the primary WAN interface to the Private zone. 4. Assign the secondary WAN interface to the Public zone. 5. Assign the voice VLAN and data VLAN interfaces to the Private zone. 6. Configure 5-class hierarchical QoS on both primary and secondary WAN interfaces. 7. Mark all the traffic going out to the Internet as best-effort traffic. 8. Configure traffic shaping to 95% of the available WAN bandwidth. 9. Configure NBAR as in the NBAR Classification with QoS test case. 10. Configure NetFlow on the WAN and LAN interfaces for ingress and egress traffic. 11. Collect traffic statistics and distribution charts, and export the statistics to a NAM, using NetFlow version 5 or version 9. 12. Send HTTP, HTTPS, ICMP, DNS, and SSH traffic from clients on the LAN to the Internet. 13. Send bidirectional HTTP, HTTPS, and FTP traffic between the branch and headquarters. 14. Ping one of the clients on the LAN from the ISP. 15. Verify translations and statistics using the show ip nat translations and show ip nat statistics commands. 16. Verify QoS, using the show policy-map interface command. 17. Verify NetFlow, using the show ip flow command.

Pass/Fail Criteria	Traffic from the branch to headquarters should not be inspected. Traffic from the branch to the Internet should be inspected. QoS should be applied to the traffic, and ZPF should have no adverse effect on the QoS. All the Internet traffic should be marked as best effort. Traffic should be shaped to 95% of the WAN bandwidth. NBAR should provide bandwidth guarantees to different flows and should detect and stop worms such as NIMDA and CODE RED. The NetFlow statistics collected should be within performance requirements. The ping should fail.
Result	Passed

ZPF, QoS, NBAR, NAT, and NetFlow on the Branch

Description	Configure ZPF, QoS, NBAR, and NetFlow on the branch router
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Configure ZPF as explained in the [Zone-based Policy Firewall Configuration on the Branch Router](#) test case procedure.
2. Configure the secondary WAN interface as the interface connecting to the Internet through the ISP.
3. Assign the primary WAN interface to the Private zone.
4. Assign the secondary WAN interface to the Public zone.
5. Assign the voice VLAN and data VLAN interfaces to the Private zone.
6. Configure static NAT translations for certain hosts on the data VLAN using an address pool. For the rest of the hosts, configure PAT by using the **overload** keyword in the **ip nat inside source** command in the NAT configuration.
7. Configure the data VLAN as NAT inside, and configure the secondary WAN interface as NAT outside.
8. Configure 5-class hierarchical QoS on both primary and secondary WAN interfaces.
9. Mark all the traffic going out to the Internet as best-effort traffic.
10. Configure traffic shaping to 95% of the available WAN bandwidth.
11. Configure NBAR as in the [NBAR Classification with QoS](#) test case.
12. Configure NetFlow on the WAN and LAN interfaces for ingress and egress traffic.
13. Collect traffic statistics and distribution charts, and export the statistics to a NAM, using NetFlow version 5 or version 9.
14. Send HTTP, HTTPS, ICMP, DNS, and SSH traffic from clients on the LAN to the Internet.
15. Send bidirectional HTTP, HTTPS, and FTP traffic between the branch and headquarters.
16. Ping one of the clients on the LAN from the ISP.
17. Verify translations and statistics, using the **show ip nat translations** and **show ip nat statistics** commands.
18. Verify QoS, using the **show policy-map interface** command.
19. Verify NetFlow, using the **show ip flow** command.

Pass/Fail Criteria	Traffic from the branch to headquarters should not be inspected. Traffic from the branch to the Internet should be inspected. Inside addresses should be translated to outside global addresses when the traffic from the LAN is going out to the Internet. The return traffic from the Internet to the LAN should always be directed to the outside global address of the inside hosts. QoS should be applied to the traffic, and ZPF should not have any adverse effect on the QoS. All the Internet traffic should be marked as best effort. Traffic should be shaped to 95% of the WAN bandwidth. NBAR should provide bandwidth guarantees to different flows and should detect and stop worms such as NIMDA and CODE RED. The NetFlow statistics collected should be within performance requirements. The ping should fail.

Result	Passed

ZPF with DMVPN

Description	Configure ZPF with DMVPN on the primary WAN interface connecting the branch and headquarters
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode

Procedure	1. Configure ZPF as explained in the Zone-based Policy Firewall Configuration on the Branch Router test case procedure. 2. Configure the secondary WAN interface as the interface connecting to the Internet through the ISP. 3. Assign the primary WAN interface to the Private zone. 4. Assign the DMVPN tunnel interface over the primary WAN to the Private zone. 5. Assign the voice VLAN and data VLAN interfaces to the Private zone. 6. Assign the secondary WAN interface to the Public zone. 7. Configure firewall policy for the Private zone to the Public zone, the Private zone to the DMZ zone, and the Public zone to the DMZ zone. 8. Send bidirectional HTTP, HTTPS, and FTP traffic between the branch and headquarters.
Pass/Fail Criteria	ZPF should have no adverse impact on DMVPN. Traffic between the branch and headquarters over the primary WAN interface should be encrypted.
Result	Passed

ZPF with GETVPN

Description	Configure ZPF with GETVPN connecting the branch and headquarters
Test Setup	Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure ZPF as explained in the Zone-based Policy Firewall Configuration on the Branch Router test case procedure. 2. Assign the primary WAN interface to the Public zone. 3. Assign the voice VLAN and data VLAN interfaces to the Private zone. 4. Configure GETVPN as in the IPsec Using GETVPN test case procedure. 5. Send bidirectional HTTP, HTTPS, and FTP traffic between the branch and headquarters.
Pass/Fail Criteria	Traffic between the branch and headquarters should be encrypted. ZPF should have no effect on the traffic between the branch and headquarters.
Result	Passed

IPsec, ZPF, QoS, NBAR, NAT, and NetFlow on the Branch

Description	Configure ZPF, QoS, NBAR, and NetFlow on the branch router
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Configure IPsec VPN, using either DMVPN or GETVPN on the primary WAN interface.
2. Configure ZPF as explained in the [Zone-based Policy Firewall Configuration on the Branch Router](#) test case procedure.
3. Configure the secondary WAN interface as the interface connecting to the Internet through the ISP.
4. Assign the primary WAN interface to the Private zone.
5. Assign the secondary WAN interface to the Public zone.
6. Assign the voice VLAN and data VLAN interfaces to the Private zone.
7. Configure static NAT translations for certain hosts on the data VLAN, using an address pool. For the rest of the hosts, configure PAT by using the **overload** command in the NAT configuration.
8. Configure the data VLAN as NAT inside, and configure the secondary WAN interface as NAT outside.
9. Configure 5-class hierarchical QoS on both the primary and secondary WAN interfaces.
10. Mark all the traffic going out to the Internet as best-effort traffic.
11. Configure traffic shaping to 95% of the available WAN bandwidth.
12. Configure NBAR as in the [NBAR Classification with QoS](#) test case.
13. Configure NetFlow on the WAN and LAN interfaces for ingress and egress traffic.
14. Collect traffic statistics and distribution charts, and export the statistics to a NAM using NetFlow version 5 or version 9.
15. Send HTTP, HTTPS, ICMP, DNS, and SSH traffic from clients on the LAN to the Internet.
16. Send bidirectional HTTP, HTTPS, and FTP traffic between the branch and headquarters.
17. Ping one of the clients on the LAN from the ISP.
18. Verify translations and statistics, using the **show ip nat translations** and **show ip nat statistics** commands.
19. Verify QoS, using the **show policy-map interface** command.
20. Verify NetFlow, using the **show ip flow** command.

Pass/Fail Criteria

Traffic from the branch to headquarters should be encrypted.

Traffic from the branch to headquarters should not be inspected.

Traffic from the branch to the Internet should be inspected.

Inside addresses should be translated to outside global addresses when the traffic from the LAN is going out to the Internet. The return traffic from the Internet to the LAN should always be directed to the outside global address of the inside hosts.

QoS should be applied to the traffic, and ZPF should not have any adverse effect on the QoS.

All the Internet traffic should be marked as best-effort.

Traffic should be shaped to 95% of the WAN bandwidth.

NBAR should provide bandwidth guarantees to different flows and should detect and stop worms such as NIMDA and CODE RED.

The NetFlow statistics collected should be within performance requirements.

The ping should fail.

Result

Passed

DDOS Prevention Using Cisco IOS IPS

Description Configure Cisco IOS IPS with IDCONF v5.0 in the branch router to prevent denial-of-service attacks

Test Setup

```

ip ips config location flash:/ips5/ retries 1
ip ips name IPS-ADVSET
!
ip ips signature-category
  category all
  retired true
  category ios_ips advanced
  retired false
!
crypto key pubkey-chain rsa
  named-key realm 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
!
interface GigabitEthernet0/1.2
  description Data-VLAN
  encapsulation dot1Q 301
  ip address 10.0.0.1 255.255.255.0
  ip ips IPS-ADVSET in
  ip ips IPS-ADVSET out
!

```

Procedure	1. Download the latest IPS signature pack from: http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup to the router flash. 2. Configure Cisco IOS IPS with IDCONF v5.0 on the router. 3. Enable the advanced category signature set. 4. Configure Cisco IOS IPS for both directions of traffic on the data VLAN and WAN interfaces. 5. Enable syslog on the router and log the syslog messages to a syslog server located in the branch. 6. Launch DDOS attacks from a PC attached to the branch router data VLAN to a server at the headquarters. 7. Verify whether the attacks are detected by Cisco IOS IPS and whether the alert messages are logged to the syslog server.
Pass/Fail Criteria	The attacks should be detected by Cisco IOS IPS, and appropriate signatures should be triggered. Actions such as warning, dropping the packets, or dropping the session should be taken based on a particular signature configuration. The alert messages related to the attack should be logged to a syslog server.
Result	Passed

Cisco IOS IPS with Background Data Traffic

Description	Configure Cisco IOS IPS with IDCONF v5.0 in the branch router to prevent denial-of-service attacks
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode

Procedure	1. Download the latest IPS signature pack from: http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup to the router flash. 2. Configure Cisco IOS IPS with IDCONF v5.0 on the router. 3. Enable advanced category signature set. 4. Configure Cisco IOS IPS for both directions of traffic on the data VLAN and WAN interfaces. 5. Enable syslog on the router, and log the syslog messages to a syslog server located in the branch. 6. Send HTTP, HTTPS, and FTP traffic between the branch and headquarters. 7. Launch DDOS attacks from a PC attached to the branch router data VLAN to a server at the headquarters. 8. Verify whether the attacks are detected by Cisco IOS IPS and whether the alert messages, logged to the syslog server.
Pass/Fail Criteria	The attacks should be detected by Cisco IOS IPS, and appropriate signatures should be triggered. Actions such as warning, dropping the packets, or dropping the session should be taken based on a particular signature configuration. The alert messages related to the attack should be logged to a syslog server.
Result	Passed

ZPF with NAT and Cisco IOS IPS

Description	Configure ZPF with NAT and Cisco IOS IPS on the branch router
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR

Procedure

1. Configure ZPF as explained in the [Zone-based Policy Firewall Configuration on the Branch Router](#) test case procedure
2. Configure the secondary WAN interface as the interface connecting to the Internet through the ISP.
3. Assign the primary WAN interface to the Private zone.
4. Assign the secondary WAN interface to the Public zone.
5. Assign the voice VLAN and data VLAN interfaces to the Private zone.
6. Configure static NAT translations for certain hosts on the data VLAN, using an address pool. For the rest of the hosts, configure PAT by using the **overload** command in the NAT configuration.
7. Configure the data VLAN as NAT inside, and configure the secondary WAN interface as NAT outside.
8. Download the latest Cisco IOS IPS signature pack from: <http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup> to the router flash.
9. Configure Cisco IOS IPS with IDCONF v5.0 on the router.
10. Enable advanced category signature set.
11. Configure Cisco IOS IPS for both directions of traffic on the data and DMZ VLAN and WAN interfaces.
12. Enable syslog on the router, and log the syslog messages to a syslog server located at the branch.
13. Send HTTP, HTTPS, and FTP traffic between the branch and headquarters.
14. Send HTTP, FTP, and DNS traffic between the branch and the Internet.
15. Launch DDOS attacks from a PC attached to the branch router data VLAN to a server located at the headquarters.
16. Launch threats from a host in the Internet to the DMZ servers.
17. Verify whether the attacks are detected by Cisco IOS IPS and whether the alert messages are logged to the syslog server.

Pass/Fail Criteria	Traffic from the branch to headquarters should not be inspected. Traffic from the branch to Internet should be inspected. Inside addresses should be translated to outside global addresses when the traffic from the LAN is going out to the Internet. The return traffic from the Internet to the LAN should always be directed to the outside global address of the inside hosts. The attacks should be detected by Cisco IOS IPS, and appropriate signatures should be triggered. Actions such as warning, dropping the packets or dropping the session, or blocking the host should be taken based on a particular signature configuration. The alert messages related to the attack should be logged to a syslog server.
Result	Passed

IPsec, ZPF, QoS, NBAR, NAT, Cisco IOS IPS, and NetFlow on the Branch

Description	Configure ZPF, QoS, NBAR, NAT, Cisco IOS IPS, and NetFlow on the branch router
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Configure IPsec VPN using either DMVPN or GETVPN on the primary WAN interface. 2. Configure ZPF as explained in the Zone-based Policy Firewall Configuration on the Branch Router test case procedure. 3. Configure the secondary WAN interface as the interface connecting to the Internet through the ISP. 4. Assign the primary WAN interface to the Private zone. 5. Assign the secondary WAN interface to the Public zone. 6. Assign the voice VLAN and data VLAN interfaces to the Private zone. 7. Configure static NAT translations for certain hosts on the data VLAN, using an address pool. For the rest of the hosts, configure PAT by using the overload command in the NAT configuration. 8. Configure the data VLAN as NAT inside, and configure the secondary WAN interface as NAT outside. 9. Configure Cisco IOS IPS with IDCONF v5.0 on the router. 10. Enable advanced category signature set. 11. Configure Cisco IOS IPS for both directions of traffic on the data and DMZ VLAN and WAN interfaces.

- Procedure (continued)**
12. Enable syslog on the router and log the syslog messages to a syslog server at the branch.
 13. Configure 5-class hierarchical QoS on both primary and secondary WAN interfaces.
 14. Mark all the traffic going out to the Internet as best-effort traffic.
 15. Configure traffic shaping to 95% of the available WAN bandwidth.
 16. Configure NBAR as in the [NBAR Classification with QoS](#) test case.
 17. Configure NetFlow on the WAN and LAN interfaces for ingress and egress traffic.
 18. Collect traffic statistics and distribution charts, and export the statistics to a NAM, using NetFlow version 5 or version 9.
 19. Send HTTP, HTTPS, ICMP, DNS, and SSH traffic from clients on the LAN to the Internet.
 20. Send bidirectional HTTP, HTTPS, and FTP traffic between the branch and headquarters.
 21. Ping one of the clients on the LAN from the ISP.
 22. Launch DDOS attacks from a PC attached the branch router data VLAN to a server located at the headquarters.
 23. Launch threats from a host in the Internet to the DMZ servers.
 24. Verify translations and statistics, using the **show ip nat translations** and **show ip nat statistics** commands.
 25. Verify whether the attacks are detected by Cisco IOS IPS and whether the alert messages are logged to the syslog server.
 26. Verify QoS, using the **show policy-map interface** command.
 27. Verify NetFlow, using **show ip flow** command.

Pass/Fail Criteria

All traffic should be Cisco Express Forwarding switched.

Traffic from the branch to headquarters should be encrypted.

Traffic from the branch to headquarters should not be inspected.

Traffic from the branch to the Internet should be inspected.

Inside addresses should be translated to the outside global address when the traffic from the LAN is going out to the Internet. The return traffic from the Internet to the LAN should always be directed to the outside global address of the inside hosts.

QoS should be applied to the traffic, and ZPF should not have any adverse effect on the QoS.

All the Internet traffic should be marked as best-effort.

Traffic should be shaped to 95% of the WAN bandwidth.

The attacks should be detected by Cisco IOS IPS, and appropriate signatures should be triggered.

Actions such as warning, dropping the packets or dropping the session, blocking host should be taken based on a particular signature configuration.

The alert messages related to the attack should be logged to a syslog server.

NBAR should provide bandwidth guarantees to different flows and should detect and stop worms such as NIMDA and CODE RED.

NetFlow statistics collected should be within performance requirements.

The ping should fail.

Result

Passed

Remote Users Using WebVPN (SSL VPN)

Description

Configure WebVPN in clientless mode

Test Setup

```
gateway gw-1
  ip address 209.165.201.17 port 443
  ssl trustpoint SSLVPN
  inservice
webvpn context con-1
url-list "u1"
  heading "u1-h1"
  url-text "Intranet" url-value "http://example.com"
  url-text "Intranet2" url-value "example.com"
!
policy group p1
  url-list "u1"
default-group-policy p1
gateway gw-1 domain one
  inservice

webvpn context cifs
  title "CIFS CONTEXT"
  ssl encryption
  ssl authenticate verify all
!
nbns-list cifs
  nbns-server 10.0.0.2 master
!
policy group cifs
  nbns-list "cifs"
  functions file-access
  functions file-browse
  functions file-entry
!
policy group cifs'
default-group-policy cifs
gateway gw-1 domain cifs
  inservice
```


Procedure

1. Configure AAA RADIUS authentication.
2. Configure a trust point with a persistent self-signed certificate.
3. Configure the WebVPN gateway with an IP address, and associate the trust point to the gateway. Enable the WebVPN service.
4. Configure the WebVPN context, and define the URL list and the port list in the context.
5. Configure WebVPN for clientless access with support for intranet web-based applications and Windows File Sharing Common Internet File System (CIFS).
6. Configure the WebVPN policy, and associate the context and gateway to the policy. Enable WebVPN policy.
7. Connect from a remote user from the Internet, using a web browser (Microsoft Internet Explorer 6.0) to the WebVPN gateway.
8. Access web-based applications and shared drives on the intranet.
9. Use either the Cisco IOS CLI or CCP 1.1 to configure WebVPN.
10. Verify WebVPN functionality, by using the following **show** commands or by monitoring through CCP 1.1:
 - **show webvpn gateway**
 - **show webvpn context**
 - **show webvpn session context**
 - **show webvpn session user**
 - **show webvpn stats**

Pass/Fail Criteria

All traffic should be Cisco Express Forwarding switched.

The remote user should be able to connect to the WebVPN gateway by just using only a web browser, without running any Java applet or application.

The remote user should be able to access branch intranet web-based applications and Windows shared drives.

All the SSL VPN traffic should be accelerated by the hardware encryption engine AIM-VPN/SSL-3 module.

Result

Passed

Remote Users Using WebVPN (SSL VPN) Full Tunnel

Description	Configure WebVPN in SVC or full tunnel access mode
Test Setup	<pre> ip local pool svc 10.0.0.21 10.0.0.30 ! webvpn gateway ssl-vpn ip address 209.165.201.17 port 443 ssl trustpoint golden-tp inservice ! webvpn context Default_context ssl trustpoint ssl authenticate verify all inservice ! webvpn context sslvpn ssl trustpoint ssl authenticate verify all inservice ! policy group default functions svc-enabled svc address-pool "svc" svc keep-client-installed svc split include 10.0.0.0 255.255.255.0 default-group-policy default gateway ssl-vpn inservice </pre>

Procedure

Note Tunneling Client (also known as Thick Client or Full Tunneling): A larger client (generally around 500K max) is delivered to the end user. The applications that can be accessed are very similar to those available via IPsec VPN. This client is delivered via a web page (the device to which the user is connecting) and never needs to be manually distributed or installed.

The Cisco SSL VPN client (SVC) client configuration requires:

- Configuration of an address pool (very similar to IPsec VPN).
 - The address pool to be called in the policy group.
 - Turning on SVC with tunnel mode enabled.
1. Configure AAA RADIUS authentication.
 2. Configure an IP address pool for SVC.
 3. Configure a trust point with persistent self-signed certificate.
 4. Configure the WebVPN gateway with an IP address, and associate the trust point to the gateway. Enable the WebVPN service.
 5. Configure the WebVPN context.
 6. Configure the WebVPN policy, and associate the context and gateway to the policy. Enable WebVPN policy.
 7. Associate the address pool in the WebVPN policy.
 8. Turn on SVC with tunnel mode enabled.
 9. From the remote PC, download the SVC client software and connect.
 10. Access web-based applications and shared drives in the intranet.
 11. Use either the Cisco IOS CLI or CCP 1.1 to configure WebVPN.
 12. Verify WebVPN functionality, using the following **show** commands or by monitoring through CCP 1.1:
 - **show webvpn gateway**
 - **show webvpn context**
 - **show webvpn session context**
 - **show webvpn session user**
 - **show webvpn stats**

Pass/Fail Criteria

All traffic should be Cisco Express Forwarding switched.

The remote user should be able to connect to the WebVPN gateway, using the SVC client application.

The remote user should be able to access branch intranet web-based applications and Windows shared drives.

All the SSL VPN traffic should be accelerated by the hardware encryption engine AIM-VPN/SSL-3 module.

Result

Passed

Complete Baseline Test

Description

Enable all the baseline services in the branch and headend routers. The baseline features include BGP routing, OSPF/EIGRP routing, IPsec using DMVPN or GETVPN, ZPF, NAT, IPS, QoS, NBAR, ACL, NetFlow, DHCP, AAA RADIUS server, NTP, syslog, SNMP, WebVPN, PIM-v2, and IGMP v2.

Configure L2 switching on the access layer switches.

Enable QoS on the L2 access switches.

Test Setup

[Figure 105 on page 250, Private WAN, Cisco 1841 ISR](#)

[Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR](#)

Procedure

1. Configure L2 switching with RSTP on the Catalyst 2960 switches. Verify, using the **show spanning tree** command.
2. Configure voice, data, and DMZ VLANs.
3. Configure Catalyst QoS on the Catalyst 2960 switch.
4. Configure BGP routing. Verify whether the default route is injected into the branch router, using the **show ip route** and **show ip bgp summary** commands.
5. Configure OSPF/EIGRP routing as the IGP. Verify the neighbor relationship between headquarters and branch routers, using the **show ip ospf neighbors** or **show ip eigrp neighbors** command. Verify the routes using the **show ip route** command.
6. Configure IPsec (DMVPN/GETVPN) over the primary and secondary WAN interfaces. Verify, using the **show crypto engine connections active** and **show crypto session** commands.
7. Configure ZPF with voice VLAN, data VLAN, and primary WAN in the Private zone, DMZ VLAN in the DMZ zone, secondary WAN in the Public zone, and IPsec tunnel in the VPN zone. Verify, using the **show policy-map type inspect** command.
8. Configure the 5-class QoS model with the **qos pre-classify** command. Verify, using the **show policy-map interface** command.
9. Configure NBAR to provide bandwidth guarantees to different protocols such as HTTP, HTTPS, FTP, DNS, SSH, and ICMP. Verify, using the **show ip nbar protocol-discovery** command.
10. Configure NAT to translate the addresses of hosts in the data VLAN when accessing the Internet through the secondary WAN interface. Verify, using the **show ip nat translations** command.
11. Configure IPS to prevent DDOS attacks, slackware, malware, worms, and so on, against the branch/headquarters clients and servers. Send alert messages to a syslog server.

- Procedure (continued)**
12. Configure NetFlow on all the interfaces, and export the statistics to a NAM in headquarters. Verify NetFlow statistics, using the **show ip flow** command.
 13. Configure NTP in the branch router, and authenticate the NTP server using MD5 authentication. Verify, using the **show ntp status** command.
 14. Configure the DHCP server on the branch router to provide dynamic IP addresses to clients in the voice, data, and DMZ VLANs. Verify, using the **show ip dhcp bindings** command.
 15. Configure AAA to authenticate and authorize users using a RADIUS server located in the headquarters.
 16. Configure SNMP to collect traps.
 17. Configure WebVPN in clientless mode, and have at least five remote users access the branch web-based applications and Windows File Sharing from the Internet.
 18. Configure an IPTV server in the headquarters to stream 300 kb/s video using multicast. Set up the headquarters router as an RP, and configure PIM-SM on branch and headend routers.
 19. Send HTTP, HTTPS, DNS, SSH, ICMP, and CIFS traffic between the branch and headquarters.
 20. Send HTTP, FTP, DNS, and SSH traffic between the branch and the Internet.
 21. Send HTTP traffic between the Internet and the DMZ.
 22. Join four clients to the multicast group to receive IPTV video streams.
 23. Launch threats from hosts on the branch LAN to servers on the headquarters.

Pass/Fail Criteria

All traffic should be Cisco Express Forwarding switched.

The Catalyst switch should properly mark the traffic and put it in appropriate queues.

Traffic from the branch to headquarters should be encrypted.

Traffic from the branch to headquarters should not be inspected.

Traffic from the branch to the Internet should be inspected.

Inside addresses should be translated to outside global addresses when the traffic from the LAN is going out to the Internet. The return traffic from the Internet to the LAN should always be directed to the outside global address of the inside hosts.

QoS should be applied to the traffic, and ZPF should not have any adverse effect on the QoS.

All Internet traffic should be marked as best effort.

Traffic should be shaped to 95% of the WAN bandwidth.

The attacks should be detected by Cisco IOS IPS, and appropriate signatures should be triggered.

Actions such as warning, dropping the packets or dropping the session, or blocking the host should be taken based on a particular signature configuration.

The alert messages related to the attack should be logged to a syslog server.

NBAR should provide bandwidth guarantees to different flows and should detect and stop worms such as NIMDA and CODE RED.

Remote users should be able to access the branch intranet web-based applications and shared Windows network drives. The WebVPN traffic should be accelerated by the AIM-VPN/SSL-3 module.

The NetFlow statistics should be collected and exported, and they should be within performance requirements.

The router should be able to source the clock from the NTP server after successful authentication.

The DHCP server on the router should provide IP addresses to the clients on the LAN.

AAA should be able to authenticate users using a RADIUS server.

Result

Passed

High Availability Test Cases

EIGRP Subsecond Convergence During Primary WAN Failure

Description	Enable BFD for EIGRP subsecond convergence during primary WAN failure
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Set up a primary WAN interface and a secondary WAN interface on the branch router. 2. Set up a secondary WAN interface to be an SHDSL interface. 3. Configure the secondary WAN to be a higher cost route than the primary WAN so that the primary WAN is always preferred. 4. Configure BFD on the primary WAN interface of the branch router. Configure the primary WAN interface of the headend router with a BFD interval of 50 ms, a min_rx of 50 ms, and a BFD multiplier of 5. 5. Configure BFD on the secondary WAN interface. 6. Enable BFD for all interfaces in the EIGRP routing process. 7. Verify whether BFD is up by entering the show bfd neighbor command. 8. Send HTTP and voice traffic between the branch and headquarters. 9. Bring down the primary WAN interface by either pulling out the cable or shutting down the link on the headend side. 10. After about 3 minutes, bring up the primary WAN interface.
Pass/Fail Criteria	When the primary WAN fails, EIGRP reconvergence should occur within a second because of BFD, and all the traffic should be routed through the secondary WAN interface. Voice and HTTP sessions should be maintained during reconvergence. When the primary WAN comes up after 3 minutes, the traffic should be routed over the primary WAN interface.
Result	Passed on Gigabit Ethernet interfaces. BFD is supported only on Gigabit Ethernet interfaces. Support for additional WAN encapsulations such as Frame Relay and PPP is planned for future releases.

OSPF Subsecond Convergence During Primary WAN Failure

Description	Enable BFD for OSPF subsecond convergence during primary WAN failure
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR

Procedure	1. Set up a primary WAN interface and a secondary WAN interface on the branch router. 2. Set up a secondary WAN interface to be an SHDSL interface. 3. Configure the secondary WAN to be a higher cost route than the primary WAN, using the OSPF ip ospf cost command, so that the primary WAN is always preferred. 4. Configure BFD on the primary WAN interface of the branch router and the primary WAN interface of the headend router with a BFD interval of 50 ms, a min_rx of 50 ms, and a BFD multiplier of 5. 5. Configure BFD on the secondary WAN interface. 6. Enable BFD for all interfaces in the OSPF routing process. 7. Verify whether BFD is up by entering the show bfd neighbor command. 8. Send HTTP and voice traffic between the branch and headquarters. 9. Bring down the primary WAN interface by either pulling out the cable or shutting down the link on the headend side. 10. After about 3 minutes bring up the primary WAN interface.
Pass/Fail Criteria	When the primary WAN fails, OSPF reconvergence should occur within a second because of BFD, and all the traffic should be routed through the secondary WAN interface. Voice and HTTP sessions should be maintained during reconvergence. When the primary WAN comes up after 3 minutes, the traffic should be routed over the primary WAN interface.
Result	Passed on Fast Ethernet interfaces BFD is supported only on Fast Ethernet interfaces. Support for additional WAN encapsulations such as Frame Relay and PPP is planned for future releases.

IPsec over Backup SHDSL WAN Link

Description	Encryption over backup link between the branch and headquarters
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR

Procedure	1. Set up a primary WAN interface and a secondary WAN interface on the branch router. 2. Set up the secondary WAN interface to be an SHDSL interface. 3. Configure the secondary WAN to be a higher cost route than the primary WAN, using the OSPF ip ospf cost command, so that the primary WAN is always preferred. 4. Configure BFD on the primary WAN interface of the branch router and the primary WAN interface of the headend router with a BFD interval of 50 ms, a min_rx of 50 ms, and a BFD multiplier of 5. 5. Configure BFD on the secondary WAN interface. 6. Enable BFD for all interfaces in the OSPF routing process. 7. Verify whether BFD is up by entering the show bfd neighbor command. 8. Configure one of the IPsec types, that is, IPsec DMVPN or GETVPN, on both the primary and secondary WAN interfaces between the branch and headquarters. 9. Send HTTP, FTP, and ICMP traffic between the branch and headquarters. 10. Bring down the primary WAN interface by either pulling out the cable or shutting down the link on the headend side. 11. After about 3 minutes bring up the primary WAN interface.
Pass/Fail Criteria	When the primary WAN fails, OSPF reconvergence should occur within a second because of BFD. All the traffic should be sent through the IPsec tunnel over the secondary WAN interface. HTTP, FTP, and ICMP sessions should be maintained during the switchover and switchback. When the primary WAN comes up after 3 minutes, the traffic should be routed over the primary WAN interface IPsec tunnel. No router tracebacks, memory leaks, or crashes should be observed. All the traffic should be Cisco Express Forwarding switched.
Result	Passed on Fast Ethernet interfaces. BFD is supported only on Fast Ethernet interfaces. Support for additional WAN encapsulations such as Frame Relay and PPP is planned for future releases.

ZPF, NAT, and IPsec over Backup SHDSL WAN Link

Description	ZPF, NAT, and IPsec over backup SHDSL WAN link
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR

Procedure

1. Set up a primary WAN interface and a secondary WAN interface on the branch router.
2. Set up a secondary WAN interface to be an SHDSL interface.
3. Configure the secondary WAN to be a higher cost route than the primary WAN, using the OSPF **ip ospf cost** command, so that the primary WAN is always preferred.
4. Configure BFD on the primary WAN interface of the branch router and the primary WAN interface of the headend router with a BFD interval of 50 ms, a min_rx of 50 ms, and a BFD multiplier of 5.
5. Configure BFD on the secondary WAN interface.
6. Enable BFD for all interfaces in the OSPF routing process.
7. Verify whether BFD is up by entering the **show bfd neighbor** command.
8. Configure one of the IPsec types, that is, IPsec DMVPN or GETVPN, on both the primary and secondary WAN interfaces between the branch and headquarters.
9. Configure ZPF as explained in the [Zone-based Policy Firewall Configuration on the Branch Router](#) test case procedure.
10. Configure the secondary WAN interface as the interface connecting to the Internet through the ISP.
11. Assign the primary WAN interface to the Private zone.
12. Assign the secondary WAN interface to the Public zone.
13. Assign the voice VLAN and data VLAN interfaces to the Private zone.
14. If you are using DMVPN, assign the tunnel interface to the VPN zone.
15. Define a firewall policy between the VPN zone and the Public zone.
16. Define a firewall policy between the VPN zone and the Private zone.
17. Configure static NAT translations for certain hosts on the data VLAN using an address pool. For the rest of the hosts, configure PAT by using the **overload** command in the NAT configuration.
18. Configure the data VLAN as NAT inside, and configure the secondary WAN interface as NAT outside.
19. Send HTTP, FTP, and ICMP traffic between the branch and headquarters.
20. Send HTTP, FTP, DNS, and ICMP traffic between PCs on the branch data VLAN to the Internet.
21. Verify translations and statistics, using the **show ip nat translations** and **show ip nat statistics** commands.
22. Bring down the primary WAN interface by either pulling the cable out or shutting down the link on the headend side.
23. After about 3 minutes bring up the primary WAN interface.

Pass/Fail Criteria

When the primary WAN fails, OSPF reconvergence should occur within a second because of BFD.

ZPF should inspect all traffic going out of the secondary WAN interface.

All the traffic between the branch and headquarters should be sent through the IPsec tunnel over the secondary WAN interface.

Inside addresses should be translated to outside global addresses when the traffic from the LAN is going out to the Internet. The return traffic from the Internet to the LAN should always be directed to the outside global addresses of the inside hosts.

HTTP, FTP, and ICMP sessions should be maintained during the switchover and switchback.

When the primary comes up after 3 minutes, the traffic should be routed over the primary WAN interface IPsec tunnel.

No router tracebacks, memory leaks, or crashes should be observed.

All the traffic should be Cisco Express Forwarding switched.

Result

Passed on Gigabit Ethernet interfaces.

BFD is supported only on Gigabit Ethernet interfaces. Support for additional WAN encapsulations such as Frame Relay and PPP is planned for future releases.

IPsec, ZPF, QoS, NBAR, and NetFlow on Both Primary and Secondary Link, and NAT on the Secondary Link**Description**

ZPF, NAT, and IPsec over backup SHDSL WAN link

Test Setup

[Figure 105 on page 250, Private WAN, Cisco 1841 ISR](#)

[Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR](#)

Procedure

1. Set up a primary WAN interface and a secondary WAN interface on the branch router.
2. Set up the secondary WAN interface to be an SHDSL interface.
3. Configure the secondary WAN to be a higher cost route than the primary WAN, using the OSPF **ip ospf cost** command, so that the primary WAN is always preferred.
4. Configure BFD on the primary WAN interface of the branch router and the primary WAN interface of the headend router with a BFD interval of 50 ms, a min_rx of 50 ms and a BFD multiplier of 5.
5. Configure BFD on the secondary WAN interface.
6. Enable BFD for all interfaces in the OSPF routing process.
7. Verify whether BFD is up by entering the **show bfd neighbor** command.
8. Configure one of the IPsec types, that is, DMVPN or GETVPN, on both the primary and secondary WAN interfaces between the branch and headquarters.
9. Configure ZPF as explained in the [Zone-based Policy Firewall Configuration on the Branch Router](#) test case procedure.
10. Configure the secondary WAN interface as the interface connecting to the Internet through the ISP.
11. Assign the primary WAN interface to the Private zone.
12. Assign the secondary WAN interface to the Public zone.
13. Assign the voice VLAN and data VLAN interfaces to the Private zone.
14. If you are using DMVPN, assign the tunnel interface to the VPN zone.
15. Define a firewall policy between the VPN zone and the Public zone.
16. Define a firewall policy between the VPN zone and the Private zone.
17. Configure static NAT translations for certain hosts on the data VLAN, using an address pool. For the rest of the hosts, configure PAT by using the **overload** command in the NAT configuration.
18. Configure the data VLAN as NAT inside, and configure the secondary WAN interface as NAT outside.
19. Configure Cisco IOS IPS with IDCONF v5.0 on the router.
20. Enable advanced category signature set.
21. Configure Cisco IOS IPS for both directions of traffic on the data and DMZ VLAN and WAN interfaces.
22. Enable syslog on the router, and log the syslog messages to a syslog server located in the branch.
23. Configure 5-class hierarchical QoS on both the primary and secondary WAN interfaces.
24. Mark all the traffic going out to the Internet as best-effort traffic.
25. Configure traffic shaping to 95% of the available WAN bandwidth.
26. Configure NBAR as in the [NBAR Classification with QoS](#) test case.

**Procedure
(continued)**

27. Configure NetFlow on the WAN and LAN interfaces for ingress and egress traffic.
28. Collect traffic statistics and distribution charts, and export the statistics to a NAM, using NetFlow version 5 or version 9.
29. Send HTTP, FTP, and ICMP traffic between the branch and headquarters.
30. Send HTTP, FTP, DNS, and ICMP traffic between PCs on the branch, and configure NetFlow on the WAN and LAN interfaces for ingress and egress traffic.
31. Verify translations and statistics, using the **show ip nat translations** and **show ip nat statistics** commands.
32. Launch DDOS attacks from a PC attached to the branch router data VLAN to a server located in the headquarters.
33. Launch threats from a host in the Internet to the DMZ servers.
34. Verify translations and statistics, using the **show ip nat translations** and **show ip nat statistics** commands.
35. Verify whether the attacks are detected by Cisco IOS IPS and the alert messages logged to the syslog server.
36. Verify QoS, using the **show policy-map interface** command.
37. Verify NetFlow, using the **show ip flow** command.
38. Bring down the primary WAN interface by either pulling out the cable or shutting down the link on the headend side.
39. After about 3 minutes bring up the primary WAN interface.

Pass/Fail Criteria

When the primary WAN fails, OSPF reconvergence should occur within a second because of BFD.

ZPF should inspect all traffic going out the secondary WAN interface.

All the traffic between the branch and headquarters should be sent through the IPsec tunnel over the secondary WAN interface.

Inside addresses should be translated to outside global addresses when the traffic from the LAN is going out to the Internet. The return traffic from the Internet to the LAN should always be directed to the outside global address of the inside hosts.

HTTP, FTP, and ICMP sessions should be maintained during the switchover and switchback.

QoS should be applied to the traffic, and ZPF should not have any adverse effect on the QoS.

All the Internet traffic should be marked as best effort.

Traffic should be shaped to 95% of the WAN bandwidth.

Since the secondary WAN link bandwidth is less than the primary WAN bandwidth, only conforming high-priority traffic, such as voice traffic or mission-critical traffic, should be carried over the secondary WAN link. The rest should be dropped.

The attacks should be detected by Cisco IOS IPS, and appropriate signatures should be triggered.

Actions such as warning, dropping the packets or dropping the session, or blocking the host should be taken based on a particular signature configuration.

The alert messages related to the attack should be logged to a syslog server.

NBAR should provide bandwidth guarantees to different flows and should detect and stop worms such as NIMDA and CODE RED.

NetFlow statistics collected should be within performance requirements.

When the primary comes up after 3 minutes, the traffic should be routed over the primary WAN interface IPsec tunnel.

No router tracebacks, memory leaks, or crashes should be observed.

All the traffic should be Cisco Express Forwarding switched.

Result

Passed on Gigabit Ethernet interfaces.

BFD is supported only on Gigabit Ethernet interfaces. Support for additional WAN encapsulations such as Frame Relay and PPP is planned for future releases.

Multicast with Security and QoS Features

Description	Configure multicast PIM-v2 sparse mode on the branch and headend routers to send/receive multicast traffic
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Set up a primary WAN interface and a secondary WAN interface on the branch router.
2. Set up the secondary WAN interface to be an SHDSL interface.
3. Configure secondary WAN to be a higher cost route than the primary WAN, using the OSPF **ip ospf cost** command, so that the primary WAN is always preferred.
4. Configure BFD on the primary WAN interface of the branch router and the primary WAN interface of the headend router with a BFD interval of 50 ms, a min_rx of 50 ms, and a BFD multiplier of 5.
5. Configure BFD on the secondary WAN interface.
6. Enable BFD for all interfaces in the OSPF routing process.
7. Verify whether BFD is up by entering the **show bfd neighbor** command.
8. Configure an IPTV server on the headend to stream a 300-kb/s stream to a multicast group 239.10.x.x.
9. Configure the headend router as an RP, and configure PIM-SM on both the headend and branch routers.
10. Configure IGMP v2 on the access switches.
11. Configure one of the IPsec types, that is, DMVPN or GETVPN, on both the primary and secondary WAN interface between the branch and headquarters.
12. Configure ZPF as explained in the [Zone-based Policy Firewall Configuration on the Branch Router](#) test case procedure.
13. Configure the secondary WAN interface as the interface connecting to the Internet through the ISP.
14. Assign the primary WAN interface to the Private zone.
15. Assign the secondary WAN interface to the Public zone.
16. Assign the voice VLAN and data VLAN interfaces to the Private zone.
17. If you are using DMVPN, assign the tunnel interface to the VPN zone.
18. Define a firewall policy between the VPN zone and the Public zone.
19. Define a firewall policy between the VPN zone and the Private zone.
20. Configure static NAT translations for certain hosts on the data VLAN, using an address pool. For the rest of the hosts, configure PAT by using the **overload** command in the NAT configuration.
21. Configure the data VLAN as NAT inside, and configure the secondary WAN interface as NAT outside.
22. Configure Cisco IOS IPS with IDCONF v5.0 on the router.
23. Enable advanced category signature set.
24. Configure Cisco IOS IPS for both directions of traffic on the data and DMZ VLAN and WAN interfaces.
25. Enable syslog on the router, and log the syslog messages to a syslog server located in the branch.

**Procedure
(continued)**

26. Configure 5-class hierarchical QoS on both the primary and secondary WAN interfaces.
27. Mark all the traffic going out to the Internet as best-effort traffic.
28. Configure traffic shaping to 95% of the available WAN bandwidth.
29. Configure NBAR as in the [NBAR Classification with QoS](#) test case.
30. Configure NetFlow on the WAN and LAN interfaces for ingress and egress traffic.
31. Collect traffic statistics and distribution charts, and export the statistics to a NAM, using NetFlow version 5 or version 9.
32. Send HTTP, FTP, and ICMP traffic between the branch and headquarters.
33. Send HTTP, FTP, DNS, and ICMP traffic between PCs on the branch data VLAN to the Internet.
34. Four clients in the branch join the multicast group 239.10.x.x to view the IPTV video stream.
35. Verify translations and statistics, using the **show ip nat translations** and **show ip nat statistics** commands.
36. Launch DDOS attacks from a PC attached the branch router data VLAN to a server located in the headquarters.
37. Launch threats from a host in the Internet to the DMZ servers.
38. Verify translations and statistics, using the **show ip nat translations** and **show ip nat statistics** commands.
39. Verify whether the attacks are detected by Cisco IOS IPS and whether the alert messages are logged to the syslog server.
40. Verify QoS, using the **show policy-map interface** command.
41. Verify NetFlow, using the **show ip flow** command.
42. Verify multicast traffic, using the **show ip mroute active** and **show ip mroute count** commands.
43. Bring down the primary WAN interface by either pulling out the cable or shutting down the link on the headend side.
44. After about 3 minutes, bring up the primary WAN interface.

Note IPTV clients leave the group after 5 minutes.

Pass/Fail Criteria

When the primary WAN fails, OSPF reconvergence should occur within a second because of BFD.

ZPF should inspect all traffic going out of the secondary WAN interface.

All the traffic between the branch and headquarters should be sent through the IPsec tunnel over the secondary WAN interface.

Inside addresses should be translated to outside global addresses when the traffic from the LAN is going out to the Internet. The return traffic from the Internet to the LAN should always be directed to the outside global address of the inside hosts.

HTTP, FTP, and ICMP sessions should be maintained during the switchover and switchback.

QoS should be applied to the traffic, and ZPF should not have any adverse effect on the QoS.

All the Internet traffic should be marked as best-effort.

Traffic should be shaped to 95% of the WAN bandwidth.

Since the secondary WAN link bandwidth is less than the primary WAN bandwidth, only conforming high-priority traffic, such as voice traffic or mission-critical traffic, should be carried over the secondary WAN link. The rest should be dropped.

The attacks should be detected by Cisco IOS IPS, and appropriate signatures should be triggered.

Actions such as warning, dropping the packets or dropping the session, or blocking the host should be taken based on a particular signature configuration.

The alert messages related to the attack should be logged to a syslog server.

NBAR should provide bandwidth guarantees to different flows and should detect and stop worms such as NIMDA and CODE RED.

The multicast join should be successful, and IPTV clients should be able to view the IPTV video stream.

Even when multiple clients join the multicast group, only one stream should be coming from the headend to the branch.

The multicast clients should continue to receive the video stream during primary WAN link failure.

NetFlow statistics collected should be within performance requirements.

When the primary comes up after 3 minutes, the traffic should be routed over the primary WAN interface IPsec tunnel.

No router tracebacks, memory leaks, or crashes should be observed.

The multicast stream should cease from the headend to the branch when all the clients leave the multicast group.

All the traffic should be Cisco Express Forwarding switched.

Result	Passed on Gigabit Ethernet interfaces. BFD is supported only on Gigabit Ethernet interfaces. Support for additional WAN encapsulations such as Frame Relay and PPP is planned for future releases.

Network Management Test Cases

Enable SNMP on the UUTs for Management and Monitoring

Description	Network management using SNMP
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	Enable SNMP on the Units Under Test (UUTs) as follows: 1. Define read-only and read-write community strings, using the snmp-server community command. 2. Enable SNMP traps, using the snmp-server enable traps command. 3. Enable traps related to link status in the interface, using the snmp trap link-status command, After enabling the UUTs for SNMP read-only and read-write access, poll an OID using the snmpget command on a UNIX box (for example, poll for the iftable to get a list of the interfaces on the router).
Pass/Fail Criteria	If an SNMP trap-listener is configured, you should be able to see the traps sent by the UUT. You can simulate a link flap by entering a shutdown command, and then entering a no shutdown command. Configure the address of the management station, using the snmp-server host command.
Result	Passed

Enable SYSLOG on the UUT for Management and Monitoring

Description	Syslog for management and monitoring
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Enable syslog on the UUTs, using the logging command in global configuration mode, and redirect it to a syslog server. 2. Enable syslog using the logging host and logging facility local5 commands accordingly.
Pass/Fail Criteria	Syslog messages from the router should be sent to the syslog server; messages can be verified by comparing time stamps.
Result	Passed

Using Cisco CCP for Configuration and Monitoring of the UUTs

Description	Using CCP for router configuration and management
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode, Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR
Procedure	1. Enter the ip http server command on the UUT. CCP can reside on the flash memory or on the PC connected to the network. 2. Use the CCP GUI to configure and monitor the UUT. You can use the CCP GUI to configure most features, including firewall and VPN.

Pass/Fail Criteria	Log on to the UUTs using CCP, and use the GUI to configure and monitor the UUT and interfaces.
Result	Passed

Cisco Unified CME Test Cases

SCCP Phone Registration to Cisco Unified CME

Description	Register SCCP phones to the Cisco Unified CME
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode
Procedure	1. Configure Cisco Unified CME on the branch router with the Cisco Unified CME address belonging to the voice VLAN segment. 2. For the Cisco 1861 branch, configure the maximum ephones to be 15 phones. 3. Configure dual lines and auto-registration for each of the phones. 4. Configure a TFTP server on the branch router for the phones to download the firmware. 5. Configure a DHCP server on the branch router to provide IP addresses for Cisco IP Phone endpoints. 6. Register SCCP phones to Cisco Unified CME. Register multiple phone types such as 7960, 7962, 7965, 7971, 7975, 7985, and 7936 phones. 7. Verify the configuration, using the show telephony-service and show ephone registered commands.
Pass/Fail Criteria	All the phones should successfully register to the Cisco Unified CME.
Result	Passed

SIP Phone Registration to Cisco Unified CME

Description	Register SIP phones to Cisco Unified CME
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode

Procedure	1. Configure Cisco Unified CME on the branch router with the Cisco Unified CME address belonging to the voice VLAN segment. 2. For the Cisco 1861 branch, configure the maximum ephones to be 15 phones. 3. Configure dual lines and auto-registration for each of the phones. 4. Configure a TFTP server on the branch router for the phones to download the firmware. 5. Configure a DHCP server on the branch router to provide IP addresses for the Cisco IP Phone endpoints. 6. Register SIP phones to Cisco Unified CME. Register multiple phone types such as 7960, 7962, 7965, 7971, 7975, 7985, and 7936 phones. 7. Verify the configuration, using the show voice register command.

Pass/Fail Criteria	All the phones should successfully register to the Cisco Unified CME.

Result	Passed

SCCP Local Calls

Description	Make calls between the SCCP phones registered to the Cisco Unified CME
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode , or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode
Procedure	1. Make a call between two phones registered to the Cisco Unified CME. 2. Verify ringback tone when the phone is ringing. 3. Verify the voice path, and pass DTMF digits between the phones.

Pass/Fail Criteria	Voice call should be successful with 100% path confirmation. DTMF digit passing should be successful.

Result	Passed

SIP Local Calls

Description	Make calls between the SIP phones registered to the Cisco Unified CME
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode

Procedure	1. Make a call between two phones registered to the Cisco Unified CME. 2. Verify the ringback tone when the phone is ringing. 3. Verify the voice path, and pass DTMF digits between the phones.
Pass/Fail Criteria	The voice call should be successful with 100% path confirmation. DTMF digit passing should be successful.
Result	Passed

PSTN Calls

Description	Make calls between the IP Phones registered to Cisco Unified CME to PSTN
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode , or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode
Procedure	1. Configure a PRI trunk to the PSTN on the branch router. 2. Configure voice translation rules to translate incoming calls from the PSTN. 3. Make a call from a PSTN phone to the branch IP Phone. 4. Verify the ringback tone when the phone is ringing. 5. Verify the voice path, and pass DTMF digits. 6. Verify for both SCCP and SIP phones.
Pass/Fail Criteria	Voice call should be successful with 100% path confirmation. DTMF digit passing should be successful.
Result	Passed

Branch to Headquarters Calls over the WAN with a SIP Trunk

Description	Make calls between the IP Phones registered to Cisco Unified CME in the branch and IP Phones registered to Cisco Unified CM in the headquarters
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode , or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode

Procedure	1. Configure a SIP trunk over the WAN interface between Cisco Unified CME and Cisco Unified CM. 2. Configure voice class with G.729 and G.711 as the codec options, with the first choice being G.729, and the second choice being G.711. 3. Configure RFC 2833 for DTMF relay. 4. Associate the voice class to the SIP trunk dial peer. 5. Make a call from an IP Phone in the branch to the IP Phone in the headquarters. 6. Verify the ringback tone when the phone is ringing. 7. Verify the voice path, and pass DTMF digits. 8. Verify for both SCCP and SIP phones.
Pass/Fail Criteria	Voice call should be successful with 100% path confirmation. DTMF digit passing should be successful.
Result	Passed

Branch to Headquarters Calls over the WAN with an H.323 trunk

Description	Make calls between the IP Phones registered to Cisco Unified CME in the branch and IP Phones registered to Cisco Unified CM in the headquarters
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode
Procedure	1. Configure an H.323 trunk over the WAN interface between Cisco Unified CME and Cisco Unified CM. 2. Configure voice class with G.729 and G.711 as the codec options, with the first choice being G.729, and the second choice being G.711. 3. Configure RFC 2833 DTMF relay. 4. Associate the voice class to the H.323 dial peer. 5. Make a call from an IP Phone in the branch to the IP Phone in the headquarters. 6. Verify the ringback tone when the phone is ringing. 7. Verify the voice path, and pass DTMF digits. 8. Verify for both SCCP and SIP Phones.
Pass/Fail Criteria	Voice call should be successful with 100% path confirmation. DTMF digit passing should be successful.
Result	Passed

Supplementary Services with Cisco Unified CME

Description	Test the various supplementary features in Cisco Unified CME with all the phones local to the branch
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode
Procedure	1. Configure transfer system full-consult on the Cisco Unified CME. 2. Configure music on hold (MOH) to source from a file in flash memory. 3. Verify call transfer full consult between phones A, B, and C, with C being the transferrer; that is, make a call from phone A to phone B, and transfer the call to phone C. 4. Verify MOH on phone A during call transfer. 5. Configure transfer system full-blind on the Cisco Unified CME. 6. Verify call transfer full-blind between phones A, B, and C with C being the transferrer, that is, make a call from phone A to phone B, and transfer the call to phone C. 7. Verify MOH on phone A during call transfer. 8. Configure call forward functionality by configuring forward-to numbers under the ephone-dns. 9. Verify call forward no answer to another ephone extension. 10. Verify call forward all to another ephone extension.
Pass/Fail Criteria	Voice call should be successful with 100% path confirmation. Call transfer full-consult should be successful. Call transfer full-blind should be successful. Call forward no answer should be successful. Call forward all should be successful. MOH should be heard.
Result	Passed

Supplementary Services Between Phones in the Branch, Headquarters, and PSTN

Description	Test the various supplementary features between phones in the branch registered to Cisco Unified CME, phones registered to Cisco Unified CM, and PSTN phones
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode
Procedure	1. Configure transfer system full-consult on the Cisco Unified CME. 2. Configure MOH to source from a file in flash memory. 3. Configure multicast MOH. 4. Verify call transfer full-consult between phones A, B, and C with C being the transferrer; that is, make a call from phone A to phone B, and transfer the call to phone C. Phone A is located in headquarters, Phone B is located in the branch, and Phone C is in the PSTN. 5. Verify MOH on phone A during call transfer. 6. Configure transfer system full-blind on the Cisco Unified CME. 7. Verify call transfer full-blind between phones A, B, and C with C being the transferrer; that is, make a call from phone A to phone B, and transfer the call to phone C. 8. Verify MOH on phone A during call transfer. 9. Configure call forward functionality for Cisco Unified CME phones by configuring forward-to numbers under the ephone-dns. 10. Verify call forward no answer to another ephone extension. 11. Verify call forward all to another ephone extension.
Pass/Fail Criteria	Voice call should be successful with 100% path confirmation. Call transfer full-consult should be successful. Call transfer full-blind should be successful. Call forward no answer should be successful. Call forward all should be successful. MOH should be heard.
Result	Passed

Call Conference in the Branch Cisco Unified CME

Description	Test a three-party conference with the branch IP Phone as the conference initiator
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode
Procedure	1. Make a three-party conference between a branch phone, a headquarters phone, and a PSTN phone, with the branch phone as the conference initiator.
Pass/Fail Criteria	Conference call should be successful.
Result	Passed

Call Forward to Voice Mail

Description	Test call forward to Cisco Unity Express with transcoding on the Cisco Unified CME
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode
Procedure	1. Configure call forward on no answer or busy to voice mail on the ephone DN of the IP Phones on the branch. 2. Set up Cisco Unity Express as the voice mail system. 3. Configure DSP farm on the branch router for Cisco Unified CME transcoding to transcode G.729 codec to G.711-ulaw codec. 4. Make a call from the headquarters phone to the branch phone that uses the G.729 codec. 5. Make a branch phone busy. 6. Verify whether the call was forwarded to voice mail. 7. Verify whether the MWI appears on the branch phone. 8. Retrieve the voice mail from Cisco Unity Express by dialing the voice mail from the branch phone. 9. Verify whether the MWI disappears once the message is heard.

Pass/Fail Criteria	The call should be forwarded to voice mail. Cisco Unified CME transcoding resources should be invoked when the call is forwarded to voice mail, because Cisco Unity Express supports only the G.711u-law codec. The MWI light should appear when the message is left in Cisco Unity Express and should disappear once the message is retrieved.
Result	Passed

Video Call Between Branch and Headquarters

Description	Test a video call between the branch and headquarters using either Cisco Unified Video Advantage or the Cisco Unified IP Phone 7985G.
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode
Procedure	1. Make a video call between the branch phone and the headquarters phone using either Cisco Unified Video Advantage or the Cisco Unified IP Phone 7985G with H.263 for the video and G.711u-law codec for the voice. 2. Test Hold and Resume on the Cisco Unified CME phone. 3. Test mute. 4. Verify the voice and video path.
Pass/Fail Criteria	The voice and video path confirmation should be 100%. When the Cisco Unified CME phone puts the call on hold, the headquarters phone should hear MOH. When the Cisco Unified CME phone mutes the call, the headquarters phone should not hear anything, and the video should freeze.
Result	Passed

T.38 Fax Between Branch and Headquarters

Description	Test T.38 fax between the branch and headquarters
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode

Procedure	1. Configure T.38 fax on the branch router and T.38 fax the Cisco Unified CM. 2. Using a fax machine in the branch, send a multipage fax to a fax machine in the headquarters.
Pass/Fail Criteria	The fax should be received properly on the headquarters fax machine.
Result	Passed

IP SLA VoIP UDP Jitter Codec g711ulaw (Branch to HQ)

Description	VoIP UDP Jitter IP SLA codec g711ulaw																		
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode																		
Procedure	1. Enable the IP SLA responder on the HQ router. 2. Configure the basic VoIP UDP Jitter operation type on the branch router. 3. Configure any options available, such as codec g711ulaw, for the VoIP UDP Jitter SLAs operation type. 4. Configure the threshold conditions, if required. 5. Schedule the operation to run and let the operation run for enough of a period of time to gather statistics. 6. Display and interpret the results of the operation using either the Cisco IOS CLI or an NMS system with SNMP.																		
Pass/Fail Criteria	To view and interpret the operational results of an IP SLA, use the show ip sla monitor statistics command to check the boundaries the limits, for example: <table><tr><th>ICPIF Range</th><th>MOS</th><th>Quality</th></tr><tr><td>0–3</td><td>5</td><td>Best</td></tr><tr><td>4–13</td><td>4</td><td>High</td></tr><tr><td>14–23</td><td>3</td><td>Medium</td></tr><tr><td>24–33</td><td>2</td><td>Low</td></tr><tr><td>34–43</td><td>1</td><td>Poor</td></tr></table>	ICPIF Range	MOS	Quality	0–3	5	Best	4–13	4	High	14–23	3	Medium	24–33	2	Low	34–43	1	Poor
ICPIF Range	MOS	Quality																	
0–3	5	Best																	
4–13	4	High																	
14–23	3	Medium																	
24–33	2	Low																	
34–43	1	Poor																	
Result	Passed																		

Remote Phones on the Cisco Unified CME

Description	Test remote phone support in the Cisco Unified CME
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode
Procedure	1. Register a remote phone to the Cisco Unified CME through the Internet; that is, the remote phone is located in the remote teleworker's home office. 2. Configure the G.729 codec for remote phones. 3. Configure the media termination point (MTP) option on the Cisco Unified CME to terminate and originate RTP packets from and to the remote phone. 4. Configure DSP farm assist for the remote phone to transcode G.729 calls to G.711 calls. 5. Make a call from the remote phone to a branch IP Phone. 6. Verify the ringback tone when the phone is ringing. 7. Verify the voice path and also pass DTMF digits.
Pass/Fail Criteria	The ringback tone should be heard. The voice path confirmation should be 100%. DTMF digit passing should be successful.
Result	Passed

Cisco Unified CME with WAN Failure Scenario to Headquarters

Description	Test the Cisco Unified CME functionality to the headquarters during WAN failure
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode
Procedure	1. Make a call between a branch IP Phone and a headquarters IP Phone. 2. Make a call between a branch IP Phone and a PSTN phone. 3. Make a call between two branch IP Phones. 4. Bring down the WAN interface of the router.

Pass/Fail Criteria During WAN failure the call between the branch IP Phone and the headquarters IP Phone should be dropped; however, the call between the IP Phone and the PSTN phone and the call between the two IP Phones in the branch should be sustained.

Result Passed

Cisco Unified CME with IPsec over the WAN

Description Test Cisco Unified CME functionality with IPsec over the WAN

Test Setup [Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode](#), or
[Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode](#)

- Procedure**
1. Configure IPsec over the WAN, and test with all types of IPsec.
 2. Make a video call from a branch IP Phone to a headquarters IP Phone.
 3. Verify ringback.
 4. Verify whether signaling, voice, and video packets are encrypted and decrypted properly.
 5. Verify voice and video path, and pass DTMF digits.

Pass/Fail Criteria Signaling, voice, and video packets should be encrypted and decrypted properly.

The ringback tone should be heard when the remote phone rings.

The voice and video path confirmation should be 100%.

DTMF digit passing should be successful.

Result Passed

Cisco Unified CME with QoS and NBAR

Description Test Cisco Unified CME functionality with QoS and NBAR applied to signaling and RTP packets

Test Setup [Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode](#), or
[Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode](#)

Procedure

1. Configure the 5-class QoS model over the primary WAN interface.
2. Configure LLQ for voice and video traffic and allocate X% and Y% of the bandwidth for voice and video, but make sure not to exceed 33% of the total bandwidth.
3. Configure 1P3Q3T on the Catalyst switch, and trust the COS value coming from the Cisco IP Phones.
4. Configure a DSCP value of CS3 on the SIP/H.323 dial peer to give priority to signaling traffic.
5. Make voice and video calls from branch IP Phones to headquarters IP Phones.
6. Verify whether the IP Phone marks the voice traffic with a DSCP value of EF.
7. Verify whether the Catalyst switch marks the video packets with a DSCP value of AF41.
8. Verify whether call signaling, voice, and video traffic are classified properly and put in priority queue.
9. Send more voice and video traffic to exceed the allocated bandwidth, and verify whether voice and video traffic is dropped.

Pass/Fail Criteria

The IP Phone should mark the voice traffic with DSCP value of EF.

The IP Phone should mark SCCP signaling traffic with DSCP value of CS3.

The Catalyst switch should trust the COS value marked by IP Phone.

Catalyst switch should remark the video traffic to AF41.

QoS on the router should properly classify signaling, voice, and video packets, based on their DSCP value.

Voice and video should get strict priority queuing treatment; that is, adhering voice and video traffic should be sent out first, and exceeding voice and video traffic should be dropped.

Result

Passed

Cisco Unified CME with ZPF**Description**

Test Cisco Unified CME functionality with ZPF

Test Setup

[Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode](#), or

[Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode](#)

Procedure	1. Configure ZPF, with data and voice VLANs in the Private zone and with WAN interface in the Public zone. 2. Configure a policy to inspect router-generated SIP, H.323, and RTP traffic from system-defined self-zone to Public zone, and vice versa. 3. Configure access lists to allow calls originated in headquarters through the firewall. 4. Make a voice call from a branch IP Phone to a headquarters IP Phone. 5. Verify the ringback tone. 6. Verify the voice path and pass DTMF digits.
Pass/Fail Criteria	ZPF should inspect call signaling and RTP packets and open holes for the return traffic. The ringback tone should be heard. The voice path confirmation should be 100%. DTMF digit passing should be successful.
Result	Passed

Cisco Unified CME Remote Phones with ZPF

Description	Test Cisco Unified CME remote phone support with ZPF
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode

Procedure	1. Configure ZPF, with data and voice VLANs in the Private zone and WAN interface in the Public zone. 2. Configure a policy to inspect router generated SIP, H.323, and RTP traffic from system-defined self-zone to Public zone, and vice versa. 3. Configure a policy to inspect SCCP traffic for the remote phone. 4. Configure an access list to allow incoming SCCP and RTP traffic from a remote phone to the Cisco Unified CME. 5. Configure MTP on the Cisco Unified CME. 6. Configure DSP farm assist for the remote phone. 7. Configure an access list to allow calls originated in headquarters through the firewall. 8. Make a voice call from a remote IP Phone to a branch IP Phone. 9. Verify the ringback tone. 10. Verify the voice path and pass DTMF digits. 11. When the call is verified, transfer the call, using full-consult transfer, to a headquarters, with the branch phone being the transferrer. Commit the transfer. 12. Verify whether the transfer completes. 13. Verify whether the voice path between the remote phone and the headquarters phone is set up. 14. Verify DTMF digit passing.
Pass/Fail Criteria	ZPF should open holes for SCCP traffic for remote phone registration. ZPF should inspect call signaling and RTP packets and open holes for the return traffic. The ringback tone should be heard. The voice path confirmation should be 100%. DTMF digit passing should be successful. Transfer should be successful.
Result	Passed

Cisco Unified CME Failover with Secondary Cisco Unified CME

Description	Test Cisco Unified CME failover to a secondary Cisco Unified CME
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode

Procedure

1. Set up Cisco Unified CMEs on two branch routers; make one of the routers the primary Cisco Unified CME, and make the other the secondary.
2. Register all the phones to the primary Cisco Unified CME.
3. Verify in the phone network configuration whether both Cisco Unified CMEs exist.
4. Make a call between the branch IP Phone and the headquarters IP Phone.
5. Make a call between the branch IP Phone and another branch IP Phone.
6. Bring down the primary Cisco Unified CME by reloading that router.
7. Verify whether all the phones register to the secondary Cisco Unified CME.
8. Verify the status of active calls.
9. Verify MWI status of phones with active voice mail.
10. Verify whether the phones fall back to the primary Cisco Unified CME when it comes back up.

Pass/Fail Criteria

When the primary Cisco Unified CME fails, all the phones with no active calls should immediately register to the secondary Cisco Unified CME.

For phones with active calls over the WAN to headquarters or the PSTN, those calls should be dropped. The phones should immediately register to the secondary Cisco Unified CME.

For phones with active calls local to the branch, those calls should be sustained. When those calls complete, those phones should register to the secondary Cisco Unified CME.

Phones with active voice mail should lose their MWI.

When the primary Cisco Unified CME comes up, all the phones should register to primary Cisco Unified CME.

Result

Passed

Baseline Features Plus Cisco Unified CME**Description**

Test baseline features plus Cisco Unified CME

Test Setup

[Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode](#), or

[Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode](#)

Procedure

1. Enable all baseline features as described in the [Complete Baseline Test](#) test case.
2. Configure a primary Cisco Unified CME and a secondary Unified CME.
3. Register all the phones to the primary Cisco Unified CME.
4. Make voice and video calls between branch IP Phones and headquarters IP Phones.
 - a. Verify the ringback tone, verify the voice and video path, and pass DTMF digits.
5. Make voice calls between branch IP Phones and PSTN phones.
 - a. Verify the ringback tone, verify the voice path, and pass DTMF digits.
6. Make voice calls between branch IP Phones.
 - a. Verify the ringback tone, verify the voice path, and pass DTMF digits.
7. Make a 4-party conference call with a branch IP Phone, a branch FXS phone, a headquarters IP Phone, and a PSTN phone as the conference participants.
 - a. Verify that when the conference initiator leaves the conference, all the parties are dropped.
8. Make a call from a headquarters IP Phone to a branch IP Phone, which is busy.
 - a. Verify whether the headquarters IP Phone is able to leave voice mail.
 - b. Verify whether Cisco Unified CME transcoding is invoked.
 - c. Verify whether the branch phone receives an MWI.
9. Retrieve voice mail from branch IP Phones.
 - a. Verify whether MWI changes status once the voice mail messages are retrieved.
10. Make a call from a remote Cisco Unified CME phone to a branch IP Phone.
 - a. Verify the ringback tone, verify the voice path, and pass DTMF digits.
11. Verify supplementary services.

Pass/Fail Criteria	The voice and video path confirmation should be 100%. Cisco Unified CME transcoding gets invoked for call transfers to voice mail, with the calling party being in headquarters. DSP farm assist gets invoked for remote phones. The MWI light should turn on when voice mail messages are left and should turn off when the voice mail messages are retrieved. The conference call should be successful. Supplementary services such as call transfer and call forward should be successful.
Result	Passed

Cisco Unified SRST Test Cases

SCCP Phone Registration to Cisco Unified CM

Description	Register IP Phones in the branch to the Cisco Unified CM located in the headquarters using SCCP
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. For the Cisco 1861 branch, register 15 phones to Cisco Unified CM. 2. Use Cisco Unified CM bulk registration utility to register all the phones. 3. Configure regions in Cisco Unified CM for each branch. 4. Configure dual lines for each phone. 5. Configure the TFTP server as the Cisco Unified CM in the branch router that is used to download the firmware. 6. Configure a DHCP server on the branch router to provide IP addresses to IP Phone endpoints. 7. Register SCCP phones to Cisco Unified CM. Register multiple phone types such as 7960, 7962, 7965, 7971, 7975, 7985, and 7936 phones.
Pass/Fail Criteria	All the phones should successfully register to the Cisco Unified CM.
Result	Passed

SIP Phone Registration to Cisco Unified CM

Description	Register IP Phones in the branch to the Cisco Unified Communications Manager, located in the headquarters using SIP
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. For the Cisco 1861 branch, register 15 phones to Cisco Unified CM. 2. Use the Cisco Unified CM bulk registration utility to register all the phones. 3. Configure regions in the Cisco Unified CM for each branch. 4. Configure dual lines for each of the phones. 5. Configure a TFTP server as the Cisco Unified Communications Manager in the branch router for the phones to download the firmware. 6. Configure a DHCP server on the branch router to provide IP addresses to IP Phone endpoints. 7. Register SIP phones to Cisco Unified CM. Register multiple phone types such as 7960, 7962, 7965, 7971, 7975, 7985, and 7936 phones.
Pass/Fail Criteria	All the phones should successfully register to the Cisco Unified CM.
Result	Passed

SIP Local Calls

Description	Make calls between the SIP phones registered to the Cisco Unified CM
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Make a call between two phones registered to the Cisco Unified CM. 2. Verify the ringback tone when the phone is ringing. 3. Verify the voice path, and pass DTMF digits between the phones.
Pass/Fail Criteria	The voice calls should be successful with 100% path confirmation. DTMF digit passing should be successful.
Result	Passed

SCCP Local Calls

Description	Make calls between the SCCP phones registered to the Cisco Unified CM.
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Make a call between two phones registered to the Cisco Unified CM. 2. Verify the ringback tone when the phone is ringing. 3. Verify the voice path, and pass DTMF digits between the phones.
Pass/Fail Criteria	The voice call should be successful with 100% path confirmation. DTMF digit passing should be successful.
Result	Passed

PSTN Calls with SIP Gateway

Description	Make calls between the IP Phones registered to Cisco Unified CM and PSTN phones
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure a PRI trunk to the PSTN on the branch router. 2. Configure voice translation rules to translate incoming calls from the PSTN. 3. Configure a SIP trunk between the branch router and Cisco Unified CM. 4. Register the branch router as a SIP gateway in Cisco Unified CM. 5. Configure an autoattendant in Cisco Unified CM that includes route lists, route groups, and route pattern. 6. Make a call from a PSTN phone to the branch IP Phone. 7. Verify the ringback tone when the phone is ringing. 8. Verify the voice path, and pass DTMF digits.
Pass/Fail Criteria	The voice call should be successful with 100% path confirmation. DTMF digit passing should be successful.
Result	Passed

PSTN Calls with H.323 Gateway

Description	Make calls between the IP Phones registered to Cisco Unified CM to PSTN
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure a PRI trunk to the PSTN on the branch router. 2. Configure voice translation rules to translate incoming calls from the PSTN. 3. Configure an H.323 trunk between the branch router and Cisco Unified CM. 4. Register the branch router as an H.323 gateway in Cisco Unified CM. 5. Configure a autoattendant in Cisco Unified CM that includes route lists, route groups, and route pattern. 6. Make a call from a PSTN phone to the branch IP Phone. 7. Verify the ringback tone when the phone is ringing. 8. Verify the voice path, and pass DTMF digits.
Pass/Fail Criteria	The voice call should be successful with 100% path confirmation. DTMF digit passing should be successful.
Result	Passed

Branch to Headquarters Calls over the WAN

Description	Make calls between the branch IP Phones registered to Cisco Unified CM and IP Phones registered to Cisco Unified CM in the headquarters
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Make a call from an IP Phone in the branch to the IP Phone in the headquarters. 2. Verify the ringback tone when the phone is ringing. 3. Verify the voice path, and pass DTMF digits. 4. Verify for both SCCP and SIP Phones.

Pass/Fail Criteria The voice call should be successful with 100% path confirmation.
DTMF digit passing should be successful.

Result Passed

Supplementary Services Between Phones in Branch, Headquarters, and PSTN

Description Test the various supplementary features between phones in the branch registered to Cisco Unified CM, phones in headquarters registered to Cisco Unified CM, and PSTN phones

Test Setup [Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode](#), or
[Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode](#)

- Procedure**
1. Configure the branch router as a SIP gateway.
 2. Configure multicast MOH on Cisco Unified CM.
 3. Enable PIM-SM on the branch router and headend router, with the headend router as the RP.
 4. Verify call transfer full-consult between phones A (located in headquarters), B (located in the branch), and C (on the PSTN) with C being the transferrer; that is, make a call from phone A to phone B, and transfer the call to phone C.
 5. Verify MOH on phone A during call transfer.
 6. Configure call forward functionality for IP Phones by configuring forward-to numbers in the phone configuration in Cisco Unified CM.
 7. Verify call forward no answer to another IP Phone extension.
 8. Verify call forward all to another IP Phone extension.

Pass/Fail Criteria The voice call should be successful with 100% path confirmation.
Call transfer full-consult should be successful.
Call forward no answer should be successful.
Call forward all should be successful.
MOH should be heard.

Result Passed

Call Conference in the Branch

Description	Test a three-party conference with the branch IP Phone as the conference initiator
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure DSP farm conferencing on the branch router to utilize the DSP resources in the branch router for conferencing. 2. Configure a media resources group for conference in the Cisco Unified CM. 3. Add the branch router DSP farm resource to the media resource group. 4. Register the DSP farm to the Cisco Unified CM. 5. Make a three-party conference between a branch phone, headquarters phone, and a PSTN phone, with the branch phone as the conference initiator. 6. Verify whether DSP farm conferencing resources is utilized, using the show dspfarm and show sccp connections commands.
Pass/Fail Criteria	Conference call should be successful. The DSP farm resources on the branch router should be utilized for conferencing. When the conference initiator drops the call, all the parties should drop out of the conference.
Result	Passed

Call Forward to Voice Mail

Description	Test call forward to Cisco Unity Express with DSP farm transcoding
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode

Procedure	1. Set up Cisco Unity Express on the branch router and register Cisco Unity Express to Cisco Unified CM using JTAPI. 2. Configure CTI ports on Cisco Unified CM. 3. Configure call forward on no answer or busy to voice mail in the device, phone configuration in Cisco Unified CM. 4. Configure DSP farm transcoding on the branch router to transcode G.729 codec to G.711ulaw codec. 5. Configure a media resource group for transcoder in Cisco Unified CM, and add the branch DSP farm transcoding resource to the media resource group. 6. Make a call from the headquarters phone to the branch phone using the G.729 codec. 7. Make the branch phone busy. 8. Verify whether the call was forwarded to voice mail. 9. Verify whether MWI appears on the branch phone when the voice mail is left. 10. Retrieve the voice mail from the Cisco Unity Express by dialing the voice mail from the branch phone. 11. Verify whether the MWI disappears when the message is heard.
Pass/Fail Criteria	The call should be forwarded to voice mail. The DSP farm transcoding resources should be invoked when the call is forwarded to voice mail, since Cisco Unity Express supports only the G.711u-law codec. The MWI light should appear when the message is left in Cisco Unity Express and should disappear when the message is retrieved.
Result	Passed

Phone Registration During Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST)

Description	Test IP Phone registrations during Cisco Unified SRST mode
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode

Procedure	1. Initially register all the branch phones to Cisco Unified CM. 2. Configure Cisco Unified SRST in the branch router. 3. Configure Cisco Unified SRST in Cisco Unified CM as the branch router. 4. Make calls between branch phones and headquarters phones, local calls, and calls from the branch to the PSTN. 5. Bring down the WAN interface or bring down Cisco Unified CM by shutting it down. 6. Verify the state of active calls during WAN/Cisco Unified CM failure. 7. Verify whether all the phones register to Cisco Unified SRST. 8. Bring up the Cisco Unified CM after about 10 minutes, and verify whether all the phones register to Cisco Unified Communications Manager.
Pass/Fail Criteria	Phones with no active calls should immediately register to Cisco Unified SRST. Phones with active calls to headquarters should drop the call and register to Cisco Unified SRST. Local calls and calls to the PSTN should be sustained. When the call completes, those phones should register to Cisco Unified SRST. All the phones should immediately register to Cisco Unified CM when it comes up.
Result	Passed

Local and PSTN Calls in Cisco Unified SRST Mode

Description	Test local and PSTN calls in Cisco Unified SRST mode
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure MOH to source audio files from flash memory. 2. Make locals calls, and make calls to the PSTN. 3. Verify the ringback tone. 4. Verify the voice path, and pass DTMF digits. 5. Place local calls on hold for 30 seconds, and then resume the call. 6. Place PSTN calls on hold for 30 seconds, and then resume the call.

Pass/Fail Criteria	The ringback tone should be heard. The voice path confirmation should be 100%. DTMF digit passing should be successful. Local call hold/resume should be successful. PSTN call hold/resume should be successful. Locals call should hear tone on hold. PSTN callers should hear music on hold.
Result	Passed

Supplementary Services in Cisco Unified SRST Mode

Description	Test supplementary services such as call transfers and call forwards in Cisco Unified SRST mode
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure transfer system full-consult on the Cisco Unified SRST. 2. Configure MOH to source from a file in flash memory. 3. Configure Multicast MOH. 4. Verify call transfer full-consult between phones A, B, and C with C being the transferrer; that is, make a call from phone A to phone B, and transfer the call to phone C. Phone C and phone B are located in the branch, and phone A is in the PSTN. 5. Make a call from phone A to phone B, and transfer the call to phone C. 6. Verify MOH on phone A during call transfer. 7. Configure transfer system full-blind on the Cisco Unified SRST. 8. Verify call transfer full-blind between phones A, B, and C, with C being the transferer; that is, make a call from phone A to phone C, and transfer the call to phone B. 9. Verify MOH on phone A during call transfer. 10. Configure call forward functionality for the Cisco Unified SRST phones. 11. Verify call forward no answer to another ephone extension. 12. Verify call forward all to another ephone extension.

Pass/Fail Criteria	The voice call should be successful with 100% path confirmation. Call transfer full-consult should be successful. Call forward no answer should be successful. Call forward all should be successful. MOH should be heard.
Result	Passed

Call Forward to Voice Mail in Cisco Unified SRST Mode

Description	Test call forward to Cisco Unity Express with transcoding on the Cisco Unified CME
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode, or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode
Procedure	1. Configure call forward on no answer or busy to voice mail in Cisco Unified Communications Manager phone configuration. 2. Go to Cisco Unified SRST mode. 3. Set up Cisco Unity Express as the voice mail system. 4. Make a call from the PSTN phone to a busy branch phone. 5. Verify whether the call was forwarded to voice mail. 6. Verify whether MWI appears on the branch phone. 7. Retrieve the voice mail from Cisco Unity Express by dialing the voice mail from the branch phone. 8. Verify whether the MWI disappears when the message is heard.
Pass/Fail Criteria	The call should be forwarded to voice mail. The MWI light should appear when the message is left in Cisco Unity Express and should disappear when the message is retrieved.
Result	Passed

Call Conference in Cisco Unified SRST Mode

Description	Test a three-party conference with the branch IP Phone as the conference initiator
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Make a three-party conference call between two branch phones and a PSTN phone, with one of the branch phones as the conference initiator.
Pass/Fail Criteria	The conference call should be successful.
Result	Passed

Branch to Headquarters Calls with IPsec over the WAN

Description	Test branch to headquarters calls with IPsec over the WAN
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure IPsec over the WAN, and test with all types of IPsec. 2. Register the branch phones to the Cisco Unified Communications Manager. 3. Make a video call from a branch IP Phone to a headquarters IP Phone. 4. Verify the ringback tone. 5. Verify whether signaling, voice, and video packets are encrypted and decrypted properly. 6. Verify voice and video path, and pass DTMF digits.
Pass/Fail Criteria	Signaling, voice, and video packets should be encrypted and decrypted properly. The ringback tone should be heard when the remote phone rings. The voice and video path confirmation should be 100%. DTMF digit passing should be successful.
Result	Passed

Branch to Headquarters Voice and Video Calls with QoS and NBAR

Description	Test branch to headquarters voice and video calls with QoS and NBAR applied to signaling and RTP packets
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure the 5-class QoS Model over the primary WAN interface. 2. Configure LLQ for voice and video traffic, and allocate X% and Y% of the bandwidth for voice and video, but make sure not to exceed 33% of the total bandwidth. 3. Configure 1P3Q3T on the Catalyst switch, and trust the CoS value coming from the Cisco IP Phones. 4. Configure a DSCP value of CS3 on the SIP/H.323 dial peer to give priority to signaling traffic. 5. Register the branch phones to the Cisco Unified Communications Manager. 6. Make voice and video calls from branch IP Phones to headquarters IP Phones. 7. Verify whether the IP Phone marks the voice traffic with a DSCP value of EF. 8. Verify whether the Catalyst switch marks the video packets with a DSCP value of AF41. 9. Verify whether call signaling, voice, and video traffic is classified properly and put in priority queue. 10. Send more voice and video traffic to exceed the allocated bandwidth, and verify whether voice and video traffic is dropped.
Pass/Fail Criteria	The IP Phone should mark the voice traffic with a DSCP value of EF. The IP Phone should mark SCCP signaling traffic with a DSCP value of CS3. The Catalyst switch should trust the COS value marked by the IP Phone. The Catalyst switch should re-mark the video traffic to AF41. QoS on the router should properly classify signaling, voice, and video packets, based on their DSCP values. Voice and video traffic should receive strict priority queuing treatment; that is, adhering voice and video traffic should be sent out first, and exceeding voice and video traffic should be dropped.
Result	Passed

Branch to Headquarters Voice and Video calls with ZPF

Description	Test Cisco Unified CME functionality with ZPF
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode
Procedure	1. Configure ZPF with data and voice VLANs in the Private zone and WAN interface in the Public zone. 2. In the Private-Public zone policy, add statements to inspect SCCP and SIP signaling the traffic from the phones, and add access lists to all incoming calls to the branch from headquarters. 3. Make a voice call from a branch IP Phone to a headquarters IP Phone. 4. Verify the ringback tone. 5. Verify the voice path, and pass DTMF digits.
Pass/Fail Criteria	ZPF should inspect call signaling and dynamically open holes for RTP packets. The ringback tone should be heard. The voice path confirmation should be 100%. DTMF digit passing should be successful.
Result	Passed

High Availability in Cisco Unified SRST mode

Description	Test high availability in Cisco Unified SRST mode using HSRP
Test Setup	Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode, or Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Configure two branch routers with HSRP, with one as the primary router and the other as the secondary router.
2. Configure the Cisco Unified SRST address as the HSRP virtual address on both the branch routers.
3. Configure Cisco Unified SRST in Cisco Unified Communications Manager with the HSRP virtual address.
4. Initially register all the phones to Cisco Unified Communications Manager.
5. Make local calls in the branch.
6. Bring down Cisco Unified Communications Manager.
7. Verify that the phones register to Cisco Unified SRST except the one phone with active calls.
8. Bring down the primary branch routers after 10 minutes.
9. Verify that all the phones register to the secondary Cisco Unified SRST router.
10. Tear down active calls, and verify whether those phones register to the secondary Cisco Unified SRST router.
11. Bring up the primary branch router after 5 minutes.
12. Verify whether all the phones register back to the primary Cisco Unified SRST router when it comes up.
13. Bring up the Cisco Unified Communications Manager after 30 minutes.
14. Verify whether all the phones register to Cisco Unified Communications Manager when it comes up.

Pass/Fail Criteria

The phones should successfully register to Cisco Unified Communications Manager.

The phones should successfully register to the primary Cisco Unified SRST router when Cisco Unified Communications Manager goes down.

The phones should successfully register to the secondary Cisco Unified SRST router when the primary Cisco Unified SRST goes down.

The phones should switch back to the primary Cisco Unified SRST router when it comes up.

The phones should switch back to Cisco Unified Communications Manager when it comes up.

Result

Passed

Baseline Features Plus Cisco Unified Communications Manager

Description	Test baseline features plus Cisco Unified Communications Manager
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode , or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode
Procedure	1. Enable all baseline features as described in the Complete Baseline Test test case. 2. Register all the phones to the primary Cisco Unified Communications Manager. 3. Register all DSP farm transcoding and conferencing resources to Cisco Unified Communications Manager. 4. Make voice and video calls between branch IP Phones and headquarters IP Phones. a. Verify the ringback tone, verify the voice/video path, and pass DTMF digits. 5. Make voice calls between branch IP Phones and PSTN phones. a. Verify the ringback tone, verify the voice path, and pass DTMF digits. 6. Make voice calls between branch IP Phones. a. Verify the ringback tone, verify the voice path, and pass DTMF digits. 7. Make a four-party conference call with a branch IP Phone, a branch FXS phone, a headquarters IP Phone and a PSTN phone as the conference participants. a. Verify that when the conference initiator leaves the conference, all the parties are dropped. b. Verify whether DSP farm conferencing resources are utilized. 8. Make a call from a headquarters IP Phone to a branch IP Phone that is busy. a. Verify whether the headquarters IP Phone is able to leave voice mail. b. Verify whether DSP farm transcoding gets invoked. c. Verify whether the branch phone receives an MWI. 9. Retrieve the voice mail messages from the branch IP Phones. a. Verify that MWI changes status when the voice mail messages are retrieved. 10. Verify supplementary services.

Pass/Fail Criteria

Voice and video path confirmation should be 100%.

DSP farm transcoding is invoked for call transfers to voice mail when the calling party is in headquarters.

The MWI light should turn on when voice mail messages are left and should turn off when the voice mail messages are retrieved.

Conference call should be successful.

Supplementary services such as call transfers and call forwards should be successful.

Result Passed

RSVP Agent in SRST Router–HQ to Branch Call with Phones Registered to Cisco Unified CM

Description Test calls between the IP Phones in the HQ to phones registered in the branch in centralized call control deployment scenario with RSVP agent enabled in HQ and WAN router

Test Setup [Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode](#) or [Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode](#)

Procedure

1. Enable SCCP and configure transcoder/MTP profile with RSVP and coded pass-through in SRST branch router and WAN router in HQ.
2. Register both the transcoder and MTP to Cisco Unified CM.
3. Configure HQ and branch phones in different locations.
4. Configure RSVP policy as mandatory for voice and video calls in Cisco Unified CM.
5. Make a voice call from the HQ phone to a branch phone.
6. Make a video call from the HQ phone to a branch phone.
7. Make multiple voice calls from the HQ to the branch, so that the voice bandwidth is consumed.
8. Make a new voice call.

Pass/Fail Criteria

Verify that an RSVP reservation is made and that both voice and video calls are successful.

Verify the voice path and pass DTMF.

Verify that both SCCP and SIP Phones work properly.

Verify RSVP reservation fails and the call is not successful when the bandwidth is consumed.

Result Passed

RSVP Agent with Application ID in SRST Router–HQ to Branch Call with Phones Registered to Cisco Unified CM

Description	Make calls between the IP Phones registered to Cisco Unified CM in the HQ and IP Phones registered to Cisco Unified CME in the branch with RSVP agent configured
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode
Procedure	1. Enable SCCP and configure transcoder/MTP profile with RSVP and coded pass-through in SRST branch router and WAN router in HQ. 2. Configure the RSVP application ID for voice and video calls and specify the bandwidth to be 384 for video. 3. Register both the transcoder and MTP to Cisco Unified CM. 4. Configure HQ and branch phones in different locations. 5. Configure RSVP policy as mandatory for voice and video calls in Cisco Unified CM. 6. Make a voice call from the HQ phone to a branch phone. 7. Make a video call from the HQ phone to a branch phone.
Pass/Fail Criteria	Verify that an RSVP reservation is made and that both voice and video calls are successful. Verify that the second video call fails because the bandwidth is configured in application ID for video. Verify the voice path and pass DTMF. Verify that both SCCP and SIP phones work properly. Verify that RSVP reservation fails and that the call is not successful when the bandwidth is consumed.
Result	Passed

RSVP Agent–HQ to Branch Call with H.323 Trunk

Description	Make calls between the IP Phones in HQ to phones registered in the branch in centralized call control deployment scenario with RSVP agent enabled and with application ID in HQ and WAN router
Test Setup	Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode or Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode

Procedure	1. Configure H.323 trunk over the WAN interface between Cisco Unified CME and Cisco Unified CM 2. Enable SCCP and configure transcoder/MTP profile with RSVP and coded pass-through in SRST branch router and WAN router in HQ. 3. Register both the transcoder and MTP to Cisco Unified CM. 4. Configure RSVP policy as mandatory for voice and video calls in Cisco Unified CM. 5. Configure voice class with G.729 and G.711 as the codec options, with the first choice being G.729 and second choice being G.711. 6. Associate the voice class to the H.323 dial peer. 7. Make a voice call from the HQ phone to a branch phone. 8. Make a video call from the HQ phone to a branch phone. 9. Make multiple voice calls from the HQ to the branch so that the voice bandwidth is consumed, and then make a new voice call.
Pass/Fail Criteria	Verify that an RSVP reservation is made and that both voice and video calls are successful. Verify the voice path and pass DTMF. Verify that both SCCP and SIP phones work properly. Verify that the RSVP reservation fails and the call is not successful when the bandwidth is consumed.
Result	Passed

Performance Test Cases

Baseline Performance Test

Description	Enable all the baseline services in the branch and headend routers. The baseline features include BGP routing, OSPF/EIGRP routing, IPsec using DMVPN or GETVPN, ZPF, NAT, IPS, QoS, NBAR, ACL, NetFlow, DHCP, AAA RADIUS server, NTP, syslog, SNMP, PIM-v2, and IGMP v2. Configure L2 switching on the access layer switches.
Test Setup	Figure 105 on page 250, Private WAN, Cisco 1841 ISR Figure 106 on page 250, MPLS WAN, Cisco 1841 ISR

Procedure

1. Before the start of the test, measure the CPU utilization and memory utilization of the router.
2. Use the following traffic profile.
 - HTTP: 75% of the traffic
 - FTP: 10% of the traffic
 - SMTP: 10% of the traffic
 - DNS: 5% of the traffic

For HTTP, use two different object sizes:

- 16-KB object size for large HTML files (10 URLs)
- 4-KB object size for transactional type data

For FTP, use a 1-MB file size.

For SMTP, use a 4-KB fixed object size.

For DNS, use 89 bytes.

3. Start the traffic to achieve line rate on the primary WAN interface.
4. Record the router performance metrics such as CPU, processor and I/O memory utilization, and LAN/WAN throughput.
5. Do not generate any threats to the router during the performance test.
6. Start adding the features incrementally and measure performance. Take at least five measurements, 3 minutes apart, before turning on the next feature.
7. When all the features are added, check whether the router CPU utilization is less than or equal to 75% with line rate traffic. If it is greater than the 75%, tune the traffic to reach 75% CPU utilization, with a tolerance of +/- 2%.
8. At 75% CPU utilization, take performance readings of the router every 3 minutes for a duration of 1 hour.
9. Stop all traffic at the end of the hour. Wait for about 30 minutes, and take router memory readings. Use the **show memory debug leaks** command to determine whether there were any memory leaks during the test.
10. Collect the following performance readings:
 - Router CPU utilization at 5 seconds, 1 minute, and 5 minutes, using the **show proc cpu** command
 - Router memory, using the **show mem free** and **show proc mem** commands
 - Interface statistics, using the **show interface summary** command
 - Cisco Express Forwarding switching statistics, using the **show interfaces stats** command

- Procedure (continued)** 11. Also record the following feature-specific measurements:
- QoS: **show policy-map interface** command
 - IPsec: **show crypto engine connections active** command
 - ZPF: **show policy-map type inspect** command
 - NAT: **show ip nat statistics** command
 - NetFlow: **show ip cache flow** command
 - Multicast: **show ip mroute count** command
 - NBAR: **show ip nbar protocol-discovery** command
 - IPS: **show ip ips statistics** command

Pass/Fail Criteria

There are no router tracebacks.

There are no router memory leaks.

There are no router crashes.

Most of the traffic should be Cisco Express Forwarding switched.

Result Passed

Baseline Plus Voice Performance Test with Cisco Unified CME

Description

Enable all the baseline services in the branch and headend routers. The baseline features include BGP routing, OSPF/EIGRP routing, IPsec using DMVPN or GETVPN, ZPF, NAT, IPS, QoS, NBAR, ACL, NetFlow, DHCP, AAA RADIUS server, NTP, syslog, SNMP, PIM-v2, and IGMP v2.

Configure L2 switching on the access layer switches.

Enable QoS on the L2 access switches.

Enable Cisco Unified CME on the branch router.

Measure the performance of the branch router in terms of CPU utilization, throughput of WAN and LAN interfaces, and processor and IO memory consumption.

Test Setup

[Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode](#), or

[Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode](#), or

[Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode](#), or

[Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode](#)

Procedure

1. Before the start of the test, measure the CPU utilization and memory utilization of the router.
2. Register 15 phones to Cisco Unified CME on the Cisco 1861 platform.
3. Configure dual lines for all the phones.
4. Use the following voice traffic profiles:
 - For T1 or 1.5-Mb/s bandwidth:
 - On the Cisco 1861 platform:
 - 3 voice calls over the WAN with G.729r8 codec
 - 1 384-KB video call over the WAN
 - 1 transcoding sessions
 - 1 three-party conference
 - 5 local calls
 - Call duration of voice and video calls is 180 seconds with intercall delay of 10 seconds.
 - Call duration for conferences is 10 minutes.

Procedure (continued)

5. Use the following data traffic profile:

- HTTP: 75% of the traffic
- FTP: 10% of the traffic
- SMTP: 10% of the traffic
- DNS: 5% of the traffic

For HTTP, use two different object sizes:

- 16-KB object size for large HTML files (10 URLs)
- 4-KB object size for transactional type data (10 URLs)

For FTP, use a 1-MB file size.

For SMTP, use 4-KB fixed object size.

For DNS, use 89 bytes.

6. Start all the voice and video calls. When the calls have stabilized, take a couple of CPU measurements 3 minutes apart. Stop all the voice and video traffic.
7. Start the data traffic and take a CPU utilization measurement after stabilization. The CPU utilization measurement should be very close to 75% as measured in the baseline performance test.
8. Adjust the data traffic throughput to accommodate all the voice and video traffic, while maintaining 75% CPU utilization. When the router has stabilized, take performance readings for about 1 hour, and stop all the traffic. Wait for about 30 minutes to record the memory readings.
9. In addition to the metrics mentioned in the [Baseline Performance Test](#), collect the following metrics:
- Calls-per-second rate
 - Voice and video call completion rate
 - Throughput in bits per second

Pass/Fail Criteria

There are no router tracebacks.

There are no router memory leaks.

There are no router crashes.

Most of the traffic should be Cisco Express Forwarding switched.

Result

Passed

Baseline Plus Voice Performance Test with Cisco Unified CM and Cisco Unified SRST**Description**

Enable all the baseline services in the branch and headend routers. The baseline features include BGP routing, OSPF/EIGRP routing, IPsec using DMVPN or GETVPN, ZPF, NAT, IPS, QoS, NBAR, ACL, NetFlow, DHCP, AAA Radius server, NTP, syslog, SNMP, PIM-v2, and IGMP v2.

Configure L2 switching on the access layer switches.

Enable QoS on the L2 access switches.

Enable Cisco Unified SRST on the branch router.

Measure the performance of the branch router in terms of CPU utilization, throughput of WAN and LAN interfaces, and processor and IO memory consumption.

Test Setup

[Figure 101 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified CME Mode](#), or

[Figure 102 on page 248, Cisco 1861 ISR Private WAN, Cisco Unified SRST Mode](#), or

[Figure 103 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified CME Mode](#), or

[Figure 104 on page 249, Cisco 1861 ISR MPLS WAN, Cisco Unified SRST Mode](#)

Procedure

1. Before the start of the test, measure the CPU utilization and memory utilization of the router.
2. Register 15 phones to Cisco Unified CM for the Cisco 1861 branch.
3. Configure dual lines for all the phones.
4. Use the following voice traffic profiles.
 - For T1 or 1.5-Mb/s bandwidth:
 - On the Cisco 1861 platform:
 - 3 voice calls over the WAN with G.729r8 codec
 - 1 384-KB video call over the WAN
 - 1 transcoding sessions
 - 1 three-party conference
 - 5 local calls
 - Call duration of voice and video calls is 180 seconds with intercall delay of 10 seconds.

Procedure (continued)

- Call duration for conferences is 10 minutes.

5. Use the following data traffic profile:

- HTTP: 75% of the traffic
- FTP: 10% of the traffic
- SMTP: 10% of the traffic
- DNS: 5% of the traffic

For HTTP, use two different object sizes:

- 16-KB object size for large HTML files (10 URLs)
- 4-KB object size for transactional type data (10 URLs)

For FTP, use a 1-MB file size.

For SMTP, use 4-KB fixed object size.

For DNS, use 89 bytes.

6. Start all the voice and video calls. When the calls have stabilized, take a couple of CPU utilization measurements 3 minutes apart. Stop all the voice and video traffic.
7. Start the data traffic, and take CPU utilization measurement after stabilization. The CPU utilization measurement should be very close to 75% as measured in the baseline performance test.
8. Adjust the data traffic throughput to accommodate all the voice and video traffic, while maintaining 75% CPU utilization. When the router has stabilized, take performance readings for about 1 hour and stop all the traffic. Wait for about 30 minutes to record the memory readings.
9. In addition to the metrics mentioned in the [Baseline Performance Test](#), collect the following metrics:
 - Calls per second rate
 - Voice and video call completion rate
 - Throughput in bits per second

Pass/Fail Criteria

There are no router tracebacks.

There are no router memory leaks.

There are no router crashes.

Most of the traffic should be Cisco Express Forwarding switched.

Result

Passed