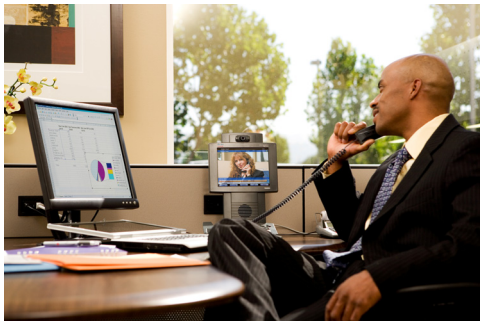


System Testing

Revised: December 21, 2009

This chapter describes the tests performed on the Streamlined Medium Branch Network.

Contents

- Test Result Summary, page 1
- Traffic Profile, page 5
- Test Setups, page 5
- Test Cases, page 7

Test Result Summary

Table 1 lists the test cases and their results.

Table 1 Test Cases and Results

Test Case	Result
Gigabit Ethernet Primary WAN Connection for Cisco 2900 Series Large Branch	Passed
MLPPP Primary WAN Connection for Cisco 2900 Series Large Branch	Passed
MLFR Primary WAN Connection for Cisco 2900 Series Large Branch	Passed
SHDSL IMA Secondary WAN Connection for Cisco 2900 Series Large Branch	Passed
Interface Removal and Addition to SHDSL IMA Interface	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

Table 1 Test Cases and Results

Test Case	Result
WAN Edge QoS–8 Class QoS Model	Passed
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
BGP Routing on the Branch	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 Metwork 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

Table 1 Test Cases and Results

Test Case	Result
DMVPN/GETVPN with QoS, NBAR, and NetFlow	Passed
Zone-based Policy Firewall Configuration on the Branch Router	Passed
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
EtherChannel Link Between Access Layer Switches	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 NefFlow on Both Primary and Secondary Link, and NAT on the Secondary Link	Passed
Multicast with Security and QoS Features	Passed
Box-to-Box Redundancy with HSRP	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
Cisco WCCP Redirection	Passed
Cisco WAE Automatic Discovery to Identify WAE Appliances	Passed
Cisco WAE Optimization Feature (TFO)	Passed
Cisco WAAS, Cisco IOS Zone-based Firewall, and Cisco IOS IPS Interoperability	Passed
Cisco WAAS with NBAR	Passed
Cisco WAAS with CIFS	Passed
Cisco WAE with Data Redundancy Elimination	Passed

Table 1 Test Cases and Results

Test Case	Result
Negative Test Case for DRE	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
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

Table 1 Test Cases and Results

Test Case	Result
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
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
Baseline Plus Voice Plus Cisco WAAS Performance Test	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 1 through Figure 4, in addition to test setups shown in the other figures referenced in the specific test case.

Figure 1 Private WAN, Cisco Unified CME Mode

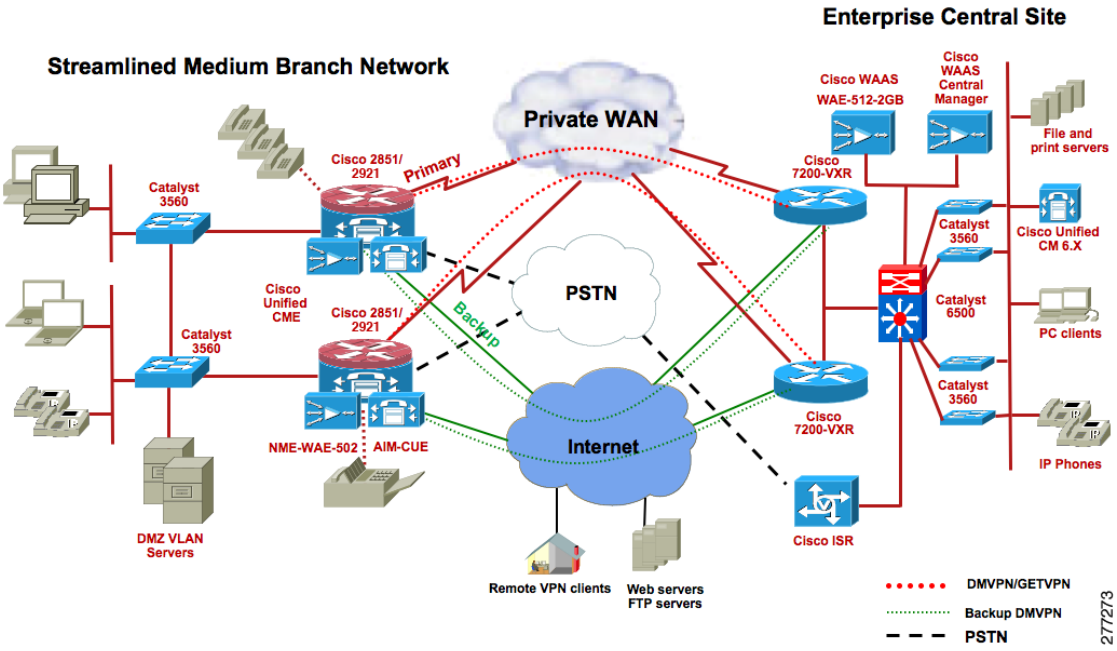


Figure 2 Private WAN, Cisco Unified SRST Mode

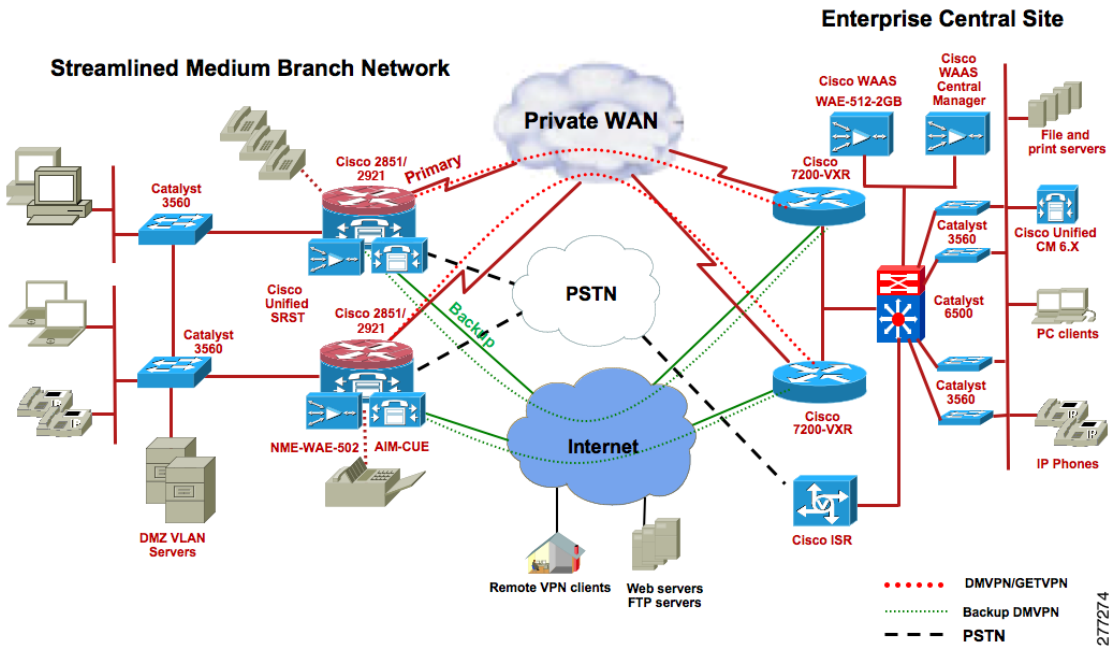


Figure 3 MPLS WAN, Cisco Unified CME Mode

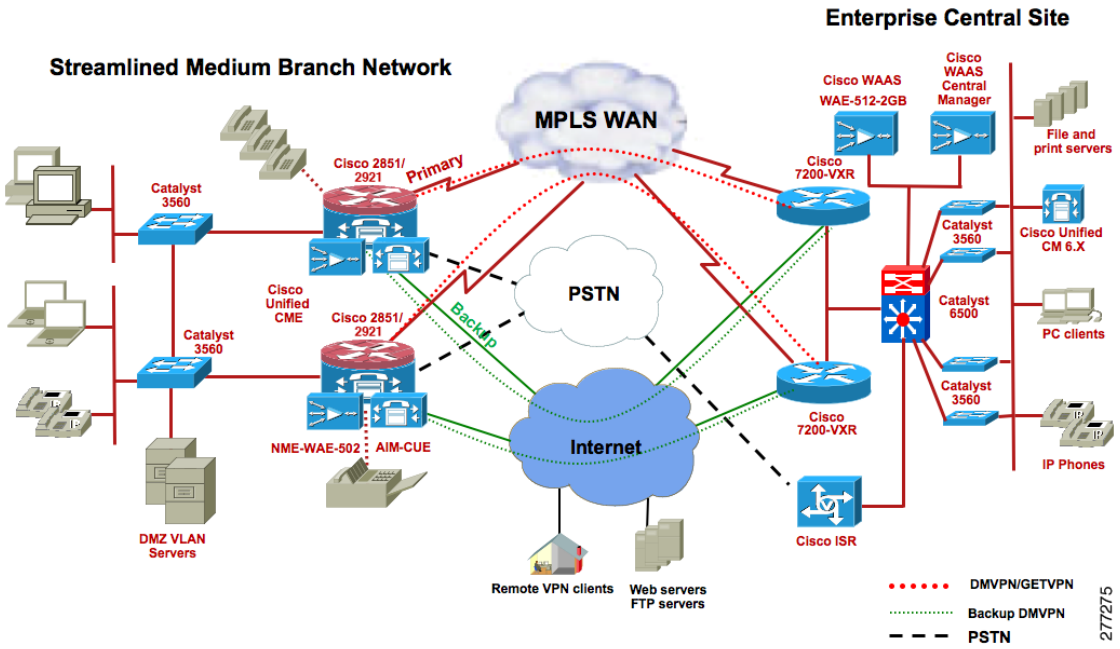
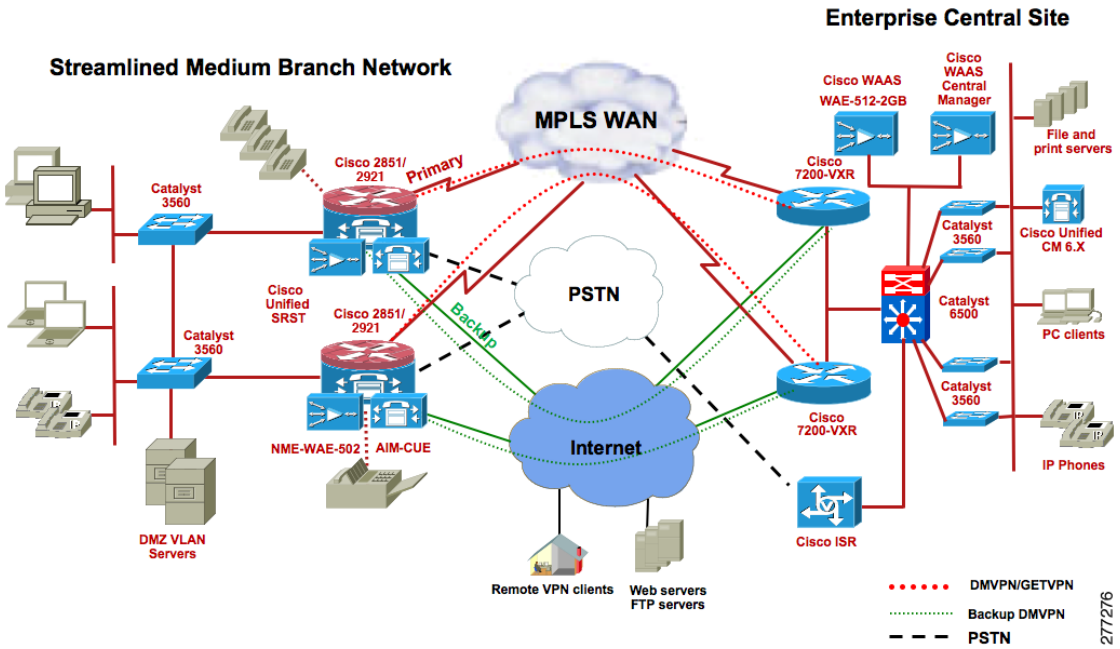


Figure 4 MPLS WAN, Cisco Unified SRST Mode



Test Cases

This section contains the following test cases:

- WAN Connectivity Test Cases, page 8
- Network Services Test Cases, page 11
- High Availability Test Cases, page 71
- Network Management Test Cases, page 86
- WAN Optimization Test Cases, page 87
- Cisco Unified CME Test Cases, page 91
- Cisco Unified SRST Test Cases, page 106
- Performance Test Cases, page 123

WAN Connectivity Test Cases

Gigabit Ethernet Primary WAN Connection for Cisco 2900 Series Large Branch

Description Set up a Gigabit Ethernet private WAN connection between the branch Cisco ISR and the headend router

Test Setup Figure 1 on page 6, Private WAN, Cisco Unified CME Mode

Procedure

1. Connect the Cisco 2900 GE port to the GE port on the headend router using multimode fiber.
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 GE 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

MLPPP Primary WAN Connection for Cisco 2900 Series Large Branch

Description Set up an MLPPP primary WAN connection between the branch Cisco ISR and the headend router

Test Setup Figure 1 on page 6, Private WAN, Cisco Unified CME Mode

Procedure

1. Install an HWIC-4T card into one of the HWIC slots on the branch Cisco ISR.
2. Connect the card to the headend using Smart Serial cables. If you are using an HWIC-4T, configure the four serial ports with a clock rate of 2048000 Hz.
3. Enable PPP encapsulation. Bundle all the four serial interfaces into an MLPPP link.
4. Configure an IP address on the multilink interface of each router, make sure that the IP addresses belong to the same segment and have the same subnet mask.
5. Ping both routers.
6. Send 90 percent of line rate of bidirectional HTTP and FTP traffic, with 75% HTTP and 25% FTP. Measure branch Cisco ISR CPU.

Pass/Fail Criteria

The MLPPP link and line protocol should come up on both branch and headend routers. The ping should be 100% successful. The required throughput should be achieved, and the branch Cisco ISR CPU should be less than 75%.

Result

Passed

MLFR Primary WAN Connection for Cisco 2900 Series Large Branch

Description

Set up an MLFR primary WAN connection between the branch Cisco ISR and the headend router

Test Setup

Figure 1 on page 6, Private WAN, Cisco Unified CME Mode

Procedure

1. Install an HWIC-4T card into one of the HWIC slots on the branch Cisco ISR.
2. Connect to the headend using Smart Serial cables.
3. If you are using an HWIC-4T, configure the four serial ports with a clock rate of 2048000 Hz.
4. Enable Frame Relay encapsulation.
5. Configure four Frame Relay point-to-point subinterfaces with DLCIs, and bundle all four serial interfaces into an MLFR link.
6. Configure an IP address on the multilink interface of each router. Make sure that the IP addresses belong to the same segment and have the same subnet mask.
7. Ping both routers.
8. Send 90 percetn of line rate of bidirectional HTTP and FTP traffic, with 75% HTTP and 25% FTP. Measure branch Cisco ISR CPU.

Pass/Fail Criteria The MLFR link and line protocol should come up on both branch and headend routers. The ping should be 100% successful. The required throughput should be achieved, and the branch Cisco ISR CPU should be less than 75%.

Result Passed

SHDSL IMA Secondary WAN Connection for Cisco 2900 Series Large Branch

Description Set up an SHDSL IMA WAN connection between the branch Cisco ISR and the DSLAM

Test Setup Figure 1 on page 6, Private WAN, Cisco Unified CME Mode

Procedure

1. Install an HWIC-4SHDSL card into one of the HWIC slots on the branch Cisco ISR.
2. Connect to the ISP DSLAM.
3. Configure IMA with two ports to achieve a bandwidth of 4608 kb/s.
4. Configure a PVC with AAL5SNAP encapsulation.
5. Configure the IP address on the ATM IMA 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

Interface Removal and Addition to SHDSL IMA Interface

Description Set up an SHDSL IMA WAN connection between the branch Cisco ISR and the ISP router (or DSLAM). Remove interfaces from the IMA group, and add the interfaces back to the IMA group while the traffic is traversing the IMA link.

Test Setup Figure 1 on page 6, Private WAN, Cisco Unified CME Mode

Procedure

1. Install an HWIC-4SHDSL card into one of the HWIC slots on the branch Cisco ISR.
2. Connect to the ISP DSLAM or router.
3. Configure IMA with two ports to achieve a bandwidth of 4608 kb/s.
4. Configure a PVC with a AAL5SNAP encapsulation.
5. Configure the IP address on the ATM IMA interface. address belongs Verify the connection by pinging the DSLAM IP address.
6. Send line rate bidirectional HTTP and FTP traffic over the interface.
7. Shut down one of the ports of the IMA group.
8. After 2 minutes, restart the port.

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%.

The IMA link should not go down when one of the ports of the IMA group goes down, and all the traffic should be carried over just one port. When the port is brought back up using the **no shutdown** command, the traffic should be carried over both the links equally.

Result

Passed

Network Services Test Cases

Layer 2 Access Layer Switch

Description

Set up Catalyst 3560 switches as access layer switches

Test Setup

Figure 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Configure Catalyst 3560 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 Widows 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 3560 switches

Test Setup

Figure 33 on page 48, Traffic Flow to QoS Class Mapping

Figure 32 on page 47, 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 voice VLAN, voice signaling, interactive video, transactional data, mission-critical data, bulk 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 Q2 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 33. 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–8 Class QoS Model

Description

Enable 8-class hierarchical QoS on the primary WAN interface

Test Setup

```
class-map match-all VOICE
match ip dscp ef ! VoIP
class-map match-all INTERACTIVE-VIDEO
match ip dscp af41 af42 ! 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-any INTERNETWORK-CONTROL
match ip dscp cs6 ! IP Routing
match access-group name IKE ! References ISAKMP ACL
class-map match-all TRANSACTIONAL-DATA
match ip dscp af21 af22 ! Transactional Data
class-map match-all BULK-DATA
match ip dscp af11 af12 ! Bulk Data
class-map match-all SCAVENGER
match ip dscp cs1 ! Scavenger
!
```

Procedure

1. Configure class maps for voice, voice signaling, interactive video, mission-critical data, transactional data, internetwork control, bulk/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

```
policy-map EIGHT-CLASS-V3PN-EDGE
class VOICE
priority percent 18 ! VoIP gets 18% LLQ
class INTERACTIVE-VIDEO
priority percent 15 ! IP/VC gets 15% LLQ
```

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

```
class INTERNETWORK-CONTROL
bandwidth percent 5 ! Control Plane provisioning
class MISSION-CRITICAL
bandwidth percent 22 ! Mission-Critical-Data provisioning
queue-limit 18 ! Optional: Anti-Replay tuning
class TRANSACTIONAL-DATA
bandwidth percent 10 ! Transactional-Data provisioning
queue-limit 18 ! Optional: Anti-Replay tuning
class BULK-DATA
bandwidth percent 4 ! Bulk-Data provisioning
queue-limit 3
class SCAVENGER
bandwidth percent 1 ! Scavenger class is throttled
queue-limit 1 ! Optional: Anti-Replay tuning
class class-default
bandwidth percent 25 ! Best Effort needs BW guarantee
queue-limit 16 ! Optional: Anti-Replay Tuning
```

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, 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

BGP Routing on the Branch

Description Configure BGP routing to the ISP

Test Setup Figure 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Configure External BGP (eBGP) on the branch router on the secondary WAN interface.
2. Inject a default route and a limited set of required routes, using a route filter, into the branch Interior Gateway Protocol (IGP) from the ISP.
3. Disable synchronization in the BGP configuration.
4. Advertise only the outside address of the branch to the ISP.
5. Do not advertise any inside addresses (LAN) of the branch router to the ISP.
6. Verify by pinging the headend router.

Pass/Fail Criteria BGP should come up between the branch and the ISP. The default route and all other routes injected from the ISP should be visible in the branch router's Routing Information Base (RIB).

Ping should be successful between the branch and headend router.

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode
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 PDLM
ip nbar port-map custom-03 tcp 5554 9996 ! Sasser custom PDLM
class-map match-all SQL-SLAMMER
match protocol custom-02 ! Matches the SQL Slammer PDLM
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 PDLM
!
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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 1 on page 6, Private WAN, Cisco Unified CME 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,

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 1 on page 6, Private WAN, Cisco Unified CME 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,

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 1 on page 6, Private WAN, Cisco Unified CME 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

```
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
```

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Configure the headend router as a DMVPN hub and Next Hop Resolution Protocol (NHRP) server with multipoint GRE.
2. Configure the branch router as a spoke with multipoint GRE.
3. Configure ISAKMP policy preshared authentication with 3-DES encryption for the keys.
4. Configure ISAKMP SA lifetime to be 3600.
5. Configure transform set with 3-DES, ESP-SHA, DH Group 2 and preshared keys.
6. Configure IPsec SA lifetime to be 86400.
7. Configure tunnel protection for the DMVPN tunnel interface.
8. Add the DMVPN tunnel interface network address to the IGP configuration.
9. Verify IPsec connectivity, using the following **show** commands:
   - **show crypto isakmp sa**
   - **show crypto ipsec sa**
   - **show crypto engine connections active**
10. Send a sweep ping from a host connected to the branch data VLAN to a host connected to the headquarters data VLAN.
11. 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 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Set up a GDOI key server for GETVPN in headquarters. The key server can be a Cisco 2900 series ISR platform.
2. Configure the key server to send unicast rekeys.
3. Configure the network segments associated with 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 antireplay protection.
7. Configure the branch routers and the headend routers as group members.
8. Configure the GDOI crypto map on the primary WAN interface of the branch router and the headend router.
9. Configure the TCP maximum segment size (MSS) to 1360 bytes on the router interfaces.
10. Register the group members to the key server.
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.
13. 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 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Set up a GDOI key server for GETVPN in the headquarters. The key server can be a Cisco 2900 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 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Set up a GDOI key server for GETVPN in the headquarters. The key server can be a Cisco 2900 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 medium branch using static floating route (Spoke-to-HQ)

Test Setup

Figure 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. On the medium branch Cisco 2951 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 medium branch using static floating route (Spoke-to-Spoke)

Test Setup

Figure 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. On the medium branch Cisco 2951 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 medium 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 medium branch and the small branch.

Pass/Fail Criteria Verify that you can reach HQ and the small branch from the medium branch when the primary WAN is down.

Result Passed

DMVPN Backup for MPLS Metwork Using BFD (Branch to HQ)

Description DMVPN backup with BFD using EIGRP as IGP (Branch to HQ)

Test Setup Figure 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Configure the 8-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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Configure the 8-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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Configure the 8-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 1 on page 6, Private WAN, Cisco Unified CME Mode or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Configure the 8-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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Configure the 8-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

```
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
```

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

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 8-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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, 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 8-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 1 on page 6, Private WAN, Cisco Unified CME Mode, or Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or Figure 4 on page 7, 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 8-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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, 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 8-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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, 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 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, 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 8-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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, 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** 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, 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 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 8-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 1.1to 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.

Result

Passed

Remote Users Using WebVPN (SSL VPN) Full Tunnel

Description Configure WebVPN in SVC or full tunnel access mode

Test Setup

```
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
```

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.

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Configure L2 switching with RSTP on the Catalyst 3560 switches. Verify, using the **show spanning tree** command.
2. Configure voice, data, and DMZ VLANs.
3. Configure Catalyst QoS on the Catalyst 3560 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 8-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.

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

EtherChannel Link Between Access Layer Switches

Description

Set up an EtherChannel connection between access layer switches

Test Setup

Connect two ports between access layer switches

Procedure

1. Bundle two Gigabit Ethernet uplinks on the Catalyst 3560 switches into an LACP EtherChannel, and connect each of the ports to the other access switch.
2. Send LAN traffic between the access switches.
3. Bring down one of the links in the EtherChannel bundle; after about 30 seconds, bring up the link again.

Pass/Fail Criteria

The two Gigabit Ethernet bundle EtherChannel link should behave as one 2-Gigabit Ethernet link. The LAN traffic between the access switches should be load balanced between the two Gigabit Ethernet links in the EtherChannel. When one of the Gigabit Ethernet links goes down, the EtherChannel should stay up, and there should be no impact on the LAN traffic. All the traffic should now be carried by just one Gigabit Ethernet link. When the other Gigabit Ethernet link comes up, load balancing should resume.

Result

Passed

EIGRP Subsecond Convergence During Primary WAN Failure

Description

Enable BFD for EIGRP subsecond convergence during primary WAN failure

Test Setup

Figure 1 on page 6, Private WAN, Cisco Unified CME Mode or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode or
Figure 4 on page 7, 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 a secondary WAN interface to be an SHDSL IMA 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, 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 a secondary WAN interface to be an SHDSL IMA 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 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 over Backup SHDSL WAN Link

Description

Encryption over backup link between the branch and headquarters

Test Setup

Figure 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, 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 IMA 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 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.

ZPF, NAT, and IPsec over Backup SHDSL WAN Link

Description	ZPF, NAT, and IPsec over backup SHDSL WAN link
Test Setup	Figure 1 on page 6, Private WAN, Cisco Unified CME Mode, or Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or Figure 4 on page 7, 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 a secondary WAN interface to be an SHDSL IMA 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 NefFlow 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or Figure 4 on page 7, 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 IMA 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 8-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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, 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 IMA 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 8-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.

Box-to-Box Redundancy with HSRP

Description Configure HSRP to provide box-to-box redundancy so that if the primary router fails, the standby router takes over and routes all the traffic

Test Setup Figure 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Configure HSRP on both routers in the branch.
2. Configure one of the router as a primary router by setting the standby priority to be higher; for example, 140.
3. Configure the remaining router as the secondary router with a standby priority of 110.
4. Configure preemption delay of 60 seconds.
5. Configure separate HSRP addresses for voice, data, and DMZ VLANs.
6. Track the LAN and WAN interfaces of the primary router.
7. Configure the default gateway as the HSRP address on the PC clients and servers in the LAN.
8. Send HTTP, FTP, and ICMP traffic from the branch to headquarters.
9. Power-cycle the primary router.
10. Verify HSRP, using the **show standby** command.

Pass/Fail Criteria The standby router should take over when the power is cycled on the primary router.

All the traffic should be routed through the standby router.

The existing sessions for HTTP and FTP traffic should be torn down and new sessions should be set up through the standby router.

When the primary router comes back, it should take over from the standby after waiting for preemption time to expire.

Result Passed

Network Management Test Cases

Enable SNMP on the UUTs for Management and Monitoring

Description Network management using SNMP

Test Setup Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode

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 2 on page 6, Private WAN, Cisco Unified SRST Mode

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 2 on page 6, Private WAN, Cisco Unified SRST Mode

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

WAN Optimization Test Cases

Cisco WCCP Redirection

Description Cisco WCCP redirection of TCP traffic to NME

Test Setup Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode

Procedure

1. Enable Cisco WCCP redirection on the UUT for redirecting TCP flows to the Cisco WAE module using these commands:

   ip wccp version 2

   ip wccp 61

   ip wccp 62
2. On the WAN interface, enter the **ip wccp redirect-out** command to redirect all the TCP traffic exiting the WAN interface to the Cisco WAE module in the UUT. Enable Cisco WCCP on the Cisco WAE, using the **wccp version 2** and **wccp router-list** commands.
3. Use the s**how wccp** command to verify the status on the NME, and use the **show ip wccp status** command on the router.

Pass/Fail Criteria Use the **show ip wccp** command to verify Cisco WCCP redirection.

Result Passed

Cisco WAE Automatic Discovery to Identify WAE Appliances

Description Verify automatic Cisco WAE appliance discovery with TCP traffic

Test Setup Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode

Procedure

1. Enable Cisco WCCP on the router and on the NME as mentioned in the Cisco WCCP Redirection test case.
2. Enable Cisco WCCP redirection on the UUT to redirect TCP traffic to the NM.
3. Initiate a Telnet session or TCP-based service from the branch to the headquarters. This service should be able to start the autodiscovery of the Cisco WAE appliances.

Pass/Fail Criteria Cisco WAE devices in the branch network should be able to automatically discover the Cisco WAE appliance in the headquarters when the TCP traffic flows are redirected to the NM, using TCP options.

Result Passed

Cisco WAE Optimization Feature (TFO)

Description Verify that the TFO feature is working for TCP traffic between the branch and headquarters with and without introducing delay

Test Setup Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode

Procedure

1. Set up Cisco WCCP redirection and enable the TFO feature on the Cisco WAE module on the UUT as mentioned in the previous WAN Optimization test cases.
2. Send stateful TCP traffic from the branch to headquarters, and monitor whether the traffic is being optimized.
3. Use the **show statistics tfo** command to check the statistics on the NME-WAE.
4. Enable delay, using the PMOD router on the headquarters network, and run the traffic again. Measure the flow optimization, and compare the two statistics (with and without delay).

Pass/Fail Criteria TCP traffic should be redirected to the Cisco WAE module and optimized successfully. Use **show** commands on the Cisco WAE module to verify the optimization.

Result Passed

Cisco WAAS, Cisco IOS Zone-based Firewall, and Cisco IOS IPS Interoperability

Description Cisco WAAS with security feature interoperability

Test Setup Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode

Procedure

1. Configure Cisco WCCP redirection so that the TCP flows are redirected to the Cisco WAE module on the UUT as mentioned in the previous test cases.
2. Configure zone-based firewall as described in the previous test cases.
3. Configure Cisco IOS Intrusion Prevention as described in the previous test cases.
4. Send stateful TCP traffic from the branch network on the UUT to the headquarters data network.
5. Monitor the traffic, using **show** commands.

Pass/Fail Criteria

Verify that the TCP traffic is being optimized with all other Cisco IOS features being executed by using **show** commands listed in the "Cisco Wide Area Application Services Verification" section on page 7.

Result

Passed

Cisco WAAS with NBAR

Description

Interoperability between NBAR and Cisco WAAS

Test Setup

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode

Procedure

1. Set up NBAR on the UUT as described in previous test cases. NBAR policies are to mark traffic before it hits the Cisco WAE.
2. Pass TCP/UDP traffic from the branch to the headquarters network.
3. Verify that the NBAR policies are executed on the traffic flows and that Cisco WAAS optimizes the traffic flows.

Pass/Fail Criteria

Traffic from the branch to headquarters should be optimized, and the NBAR functionality should be verified.

Result

Passed

Cisco WAAS with CIFS

Description

Verify the CIFS feature on the Cisco WAAS

Test Setup

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode

Procedure

1. Enable the CIFS feature on the Cisco WAE NM in the UUT and on the appliance in the headquarters.

   Clients on the LAN can safely overcome protocol-specific performance limitations such as latency, data transfer, and bandwidth consumption. With Cisco WAAS acceleration, remote office users receive LAN-like access to centralized file server data, and with disconnected mode of operation, remote users retain continuous ability to read files during periods of prolonged disconnection.
2. Use the CIFS_BM benchmark tool to test CIFS optimization and measure the latency and delay in ms.

Pass/Fail Criteria CIFS caching should produce LAN-like access to file server data with low speed or delayed WAN links.

Result Passed

Cisco WAE with Data Redundancy Elimination

Description Verify the DRE feature on Cisco WAAS

Test Setup Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode

Procedure

1. Enable the DRE feature on the Cisco WAE NM on the UUT in the branch and also on the appliance in the headquarters.
2. Pass TCP traffic from the branch to headquarters like FTP traffic with redundant data so that the directory is built up with hashes on the storage.
3. Use the **show statistics dre** command to check the DRE cache hit and miss.
4. You can also monitor the DRE feature using the Central Manager GUI.

Pass/Fail Criteria The DRE feature is supposed to reduce the amount of traffic traversing the WAN. You can validate the DRE feature by passing similar traffic multiple times and checking the WAN bandwidth usage.

Result Passed

Negative Test Case for DRE

Description Negative test case for DRE, reload the UUT on the branch network

Test Setup Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode

Procedure

1. In the Cisco WAE with Data Redundancy Elimination test case, we verified that the DRE is working, and after sending traffic for a while, verified that the database is built up on both ends. Reload the UUT or reload the NME WAE on the branch network.
2. The database should be flushed and rebuilt on both sides.
3. Verify using **show** commands on both sides.

Pass/Fail Criteria The existing database should be flushed and rebuilt when the UUT is reloaded on the branch or headquarters side.

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or Figure 3 on page 7, 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 2951 branch, configure the maximum ephones to be 100 phones.
3. For the Cisco 2921 branch, configure the maximum ephones to be 60 phones.
4. Configure dual lines and auto-registration for each of the phones.
5. Configure a TFTP server on the branch router for the phones to download the firmware.
6. Configure a DHCP server on the branch router to provide IP addresses for Cisco IP Phone endpoints.
7. Register SCCP phones to Cisco Unified CME. Register multiple phone types such as 7960, 7962, 7965, 7971, 7975, 7985, and 7936 phones.
8. 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or Figure 3 on page 7, 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 2951 branch, configure the maximum ephones to be 100 phones.
3. For the Cisco 2921 branch, configure the maximum ephones to be 60 phones.
4. Configure dual lines and auto-registration for each of the phones.
5. Configure a TFTP server on the branch router for the phones to download the firmware.
6. Configure a DHCP server on the branch router to provide IP addresses for the Cisco IP Phone endpoints.
7. Register SIP phones to Cisco Unified CME. Register multiple phone types such as 7960, 7962, 7965, 7971, 7975, 7985, and 7936 phones.
8. 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or Figure 3 on page 7, 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 successful.

Result Passed

SIP Local Calls

Description Make calls between the SIP phones registered to the Cisco Unified CME

Test Setup Figure 1 on page 6, Private WAN, Cisco Unified CME Mode or Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode

Procedure

1. Configure call forward on no answer or busy to voice mail on the ephone DNs 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or Figure 3 on page 7, 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:

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 1 on page 6, Private WAN, Cisco Unified CME Mode or
Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode

Procedure

1. Configure the 8-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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 3 on page 7, 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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. For the Cisco 2951 branch, register 100 phones to Cisco Unified CM.
2. For the Cisco 2921 branch register 60 phones to Cisco Unified CM.
3. Use Cisco Unified CM bulk registration utility to register all the phones.
4. Configure regions in Cisco Unified CM for each branch.
5. Configure dual lines for each phone.
6. Configure the TFTP server as the Cisco Unified CM in the branch router that is used to download the firmware.
7. Configure a DHCP server on the branch router to provide IP addresses to IP Phone endpoints.
8. 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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. For the Cisco 2951 branch, register 100 phones to Cisco Unified CM.
2. For the Cisco 2921 branch, register 60 phones to Cisco Unified CM.
3. Use the Cisco Unified CM bulk registration utility to register all the phones.
4. Configure regions in the Cisco Unified CM for each branch.
5. Configure dual lines for each of the phones.
6. Configure a TFTP server as the Cisco Unified Communications Manager in the branch router for the phones to download the firmware.
7. Configure a DHCP server on the branch router to provide IP addresses to IP Phone endpoints.
8. 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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or Figure 4 on page 7, 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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or Figure 4 on page 7, 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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or Figure 4 on page 7, 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 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

PSTN Calls with H.323 Gateway

Description Make calls between the IP Phones registered to Cisco Unified CM to PSTN

Test Setup Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or Figure 4 on page 7, 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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or Figure 4 on page 7, 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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 4 on page 7, 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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 4 on page 7, 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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 4 on page 7, 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.71u-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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 4 on page 7, 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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or Figure 4 on page 7, 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%.

DMTF 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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 4 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or Figure 3 on page 7, 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 2 on page 6, Private WAN, Cisco Unified SRST Mode or Figure 4 on page 7, 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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or Figure 4 on page 7, 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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or Figure 4 on page 7, MPLS WAN, Cisco Unified SRST Mode

Procedure

1. Configure the 8-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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 4 on page 7, 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 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 4 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode or

Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode or

Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode or
Figure 3 on page 7, 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or
Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or
Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or
Figure 4 on page 7, 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. 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, 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 100 phones to Cisco Unified CME on the Cisco 2951 platform.
3. Register 60 phones to Cisco Unified CME on the Cisco 2921 platform.
4. Configure dual lines for all the phones.
5. Use the following voice traffic profiles:

- For 4 T1 or 6-Mb/s bandwidth:
  - On the Cisco 2951 platform:

    10 voice calls over the WAN with G.729r8 codec

    1 384-KB video call over the WAN

    2 transcoding sessions

    1 three-party conference

    40 local calls
  - On the Cisco 2921 platform:

    6 voice calls over the WAN with G.729r8 codec

    1 384-KB video call over the WAN

    2 transcoding sessions

    1 three-party conference

    40 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)

6. 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.
7. 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.
8. 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.
9. 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.
10. 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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, 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 100 phones to Cisco Unified CM for the Cisco 2951 branch.
3. Register 60 phones to Cisco Unified CM for the Cisco 2921 branch.
4. Configure dual lines for all the phones.
5. Use the following voice traffic profiles.

- For 4 T1 or 6-Mb/s bandwidth:
  - On the Cisco 2951 platform:

    10 voice calls over the WAN with G.729r8 codec

    1 384-KB video call over the WAN

    2 transcoding sessions

    1 three-party conference

    40 local calls
  - On the Cisco 2921 platform:

    6 voice calls over the WAN with G.729r8 codec

    1 384-KB video call over the WAN

    2 transcoding sessions

    1 three-party conference

    40 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.

6. 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.
7. 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.
8. 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.
9. 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.
10. 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 Plus Cisco WAAS 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.

Enable QoS on the L2 access layer switches.

Enable Cisco Unified SRST on the branch router.

Enable Cisco WCCPv2 and Cisco WCCP 61 and 62 on the branch router.

Set up the Cisco WAAS module to do WAN optimization.

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 1 on page 6, Private WAN, Cisco Unified CME Mode, or

Figure 2 on page 6, Private WAN, Cisco Unified SRST Mode, or

Figure 3 on page 7, MPLS WAN, Cisco Unified CME Mode, or

Figure 4 on page 7, 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. Initially disable WAN optimization.
3. 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.
4. Enable the WAN optimization, and run the baseline performance test again. Measure the CPU utilization. Since Cisco WAAS optimizes the TCP traffic, the CPU utilization may be lower than 75%. Record CPU measurements. Stop the data traffic.
5. 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.
6. 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.
7. In addition to the metrics mentioned in the Baseline Plus Voice Performance Test with Cisco Unified CME, collect the following metrics:
   - TFO statistics in the Cisco WAAS module
   - DRE statistics in the Cisco WAAS module

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. The system throughput achieved should be higher than in the Baseline Plus Voice Performance Test with Cisco Unified CME or the Baseline Plus Voice Performance Test with Cisco Unified CM and Cisco Unified SRST.
Result	Passed