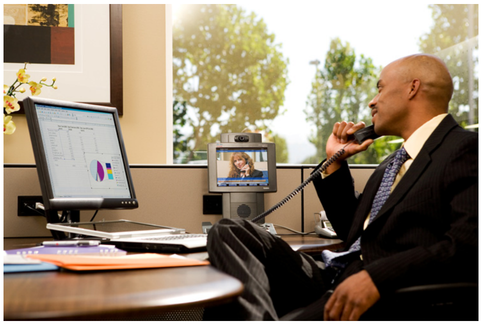

System Implementation

Revised: December 21, 2009

This section describes the information you need to configure the Cisco 3900 Series Integrated Services Routers Generation 2 (ISRs G2) branch routers, Catalyst 3560 switch, and EtherSwitch service module used in the Services Ready Medium Branch Network.

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

The full configuration of the Cisco 3900 Series ISR that was used for validating the features described in this guide is provided in the *Services Ready Medium Branch Network Toolkit*.

Contents

Network Topology

Figure 1 shows the components of the Services Ready Medium Branch Network test bed. The topology includes the following components:

Enterprise Headquarters

- Web servers
- File servers

- Print servers
- PC clients
- Cisco 7200 Series VXR routers
- Cisco Secure ACS
- Catalyst 3560 and Catalyst 6500 switches
- IP Phones
- Cisco Unified Communications Manager (Cisco Unified CM)
- Cisco Wide Area Application Engine (Cisco WAE) 512
- Cisco Configuration Engine server

Enterprise Branch

- Cisco 3925 and Cisco 3945 ISRs
- Cisco 3560 switches and EtherSwitch service module
- Cisco Unified IP Phones 7942G, 7945G, 7961G, 7962G, 7965G, 7971G, and 7985G
- Cisco Unified IP Conference Station 7936
- PC clients
- Demilitarized zone (DMZ) servers
- Analog telephones and faxes

Figure 1 Services Ready Medium Branch Network Test Bed

Figure 2 shows the detailed topology, interface assignment, and IP addressing scheme.

Figure 2 Services Ready Medium Branch Network Topology

Figure 3 shows the high-speed WAN interface cards (HWICs), voice interface cards (VICs), voice WAN interface cards (VWICs), and network modules configuration on a Cisco 3945 router. WAN connectivity is provided by the 4-port high-speed interface card (HWIC-4T). A 1-port T3/E3 network module (NME-1T1/E1) would occupy a network module slot. A Cisco 3925 router, shown in Figure 4 was filled in the same way, except that a Cisco Unity Express Advanced Integration Module (AIM2-CUE) was used instead of the network module (NME-CUE). In the Cisco 3925 configuration, the Cisco Unity Express AIM2-CUE module was placed into internal slot *1*.

Figure 3 Interface Card and Service Module Configuration on a Cisco 3945 Router

Figure 4 Interface Card and Service Module Configuration On a Cisco 3925

The access layer switch configuration in the following sections applies to both switches.

WAN Services Implementation

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

- Single-Port DS-3 Interface with Frame Relay Encapsulation, page 4
- Single-Port DS-3 Interface with Point-to-Point Encapsulation, page 5
- Multiport DS-1 Interface with Multilink Point-to-Point Encapsulation, page 6
- Multiport DS-1 Interface with Multilink Frame Relay Encapsulation, page 8
- Onboard Gigabit Ethernet Interface, page 10

Single-Port DS-3 Interface with Frame Relay Encapsulation

A single-port clear-channel T3/E3 network module was used for this configuration. Traditional Frame Relay (FR) shaping was applied on the interface. Alternatively, QoS-based shaping as defined in the Eight-Class-V3PN-Edge-Shape service policy can be used. This example is shown in the "Multiport DS-1 Interface with Multilink Frame Relay Encapsulation" section on page 8.

```
Router(config)# card type t3 3 ! Declares network module in slot 3 operational in T3 mode
Router(config)# interface Serial3/0 ! Enters serial interface configuration mode
Router(config-if)#  no ip address ! Disable IP processing on the serial interface
Router(config-if)# ip nbar protocol-discovery ! Enables NBAR to discover default protocols
and gather statistics
Router(config-if)# load-interval 30 ! Specifies interval for computing load statistics
Router(config-if)# dsu bandwidth 44210 ! Specifies maximum allowed bandwidth in Kbps for
the interface
Router(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth
available for QoS reservations
Router(config-if)# encapsulation frame-relay IETF ! Enables Frame Relay IETF standard
Router(config-if)# interface Serial3/0.1 point-to-point ! Defines point-to-point Frame
Relay sub-interface for the primary link
Router(config-subif)# ip address 192.168.0.1 255.255.255.252 ! Specifies an IP address for
the sub-interface
Router(config-subif)# ip access-group BLOCK-TFTP in ! Applies ACL named "BLOCK-TFTP" on
incoming traffic
Router(config-subif)# ip access-group BLOCK-TFTP out ! Applies ACL named "BLOCK-TFTP" on
outgoing traffic
Router(config-subif)# ip nbar protocol-discovery ! Enables NBAR to discover default
protocols and gather statistics
```

```
Router(config-subif)# ip flow ingress ! Enables NetFlow accounting for incoming packets
Router(config-subif)# ip flow egress ! Enables NetFlow accounting for outgoing packets
Router(config-subif)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
Router(config-subif)# no ip mroute-cache ! Disables fast-switching of multicast packets
Router(config-subif)# snmp trap link-status ! Generates SNMP trap when link-status changes
Router(config-subif)# frame-relay interface-dlci 230 ! Defines Frame Relay DLCI for the
sub-interface
Router(config-fr-dlci)#  class FR-SHAPING ! Assigns Frame Relay configuration map
"FR-SHAPING" for traffic shaping. The map-class is defined in QoS section
Router(config-fr-dlci)# exit
```

Apply the following command on the Serial3/0.1 subinterface after defining the *Public* security zone as shown in the Security section.

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

Apply the following command on the Serial3 interface after defining the VPN-MAP crypto map as shown in the Security section if using GETVPN.

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

Verification of Single-Port DS-3 Interface with Frame Relay Encapsulation

To verify your Frame Relay single-port DS-3 interface configuration, enter and verify the output of the following command:

```
Router# show frame-relay pvc 230

PVC Statistics for interface Serial3/0 (Frame Relay DTE)

DLCI = 230, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial3/0.1

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

Single-Port DS-3 Interface with Point-to-Point Encapsulation

The following configuration for the T3/E3 network module uses the PPP Layer 2 encapsulation method.

```
Router(config)# card type t3 3 ! Declares network module in slot 3 operational in T3 mode
Router(config)# interface Serial3/0 ! Enters serial interface configuration mode
Router(config-if)# no ip address ! Disable IP processing on the serial interface
Router(config-if)# ip nbar protocol-discovery ! Enables NBAR to discover default protocols
and gather statistics
Router(config-if)# load-interval 30 ! Specifies interval for computing load statistics
Router(config-if)# dsu bandwidth 44210 ! Specifies maximum allowed bandwidth in Kbps for
the interface
Router(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth
available for QoS reservations
Router(config-if)# encapsulation PPP ! Sets Layer 2 encapsulation to PPP
Router(config-if)# ip address 192.168.0.1 255.255.255.252 ! Specifies an IP address for
the sub-interface
Router(config-if)# ip access-group BLOCK-TFTP in ! Applies ACL named "BLOCK-TFTP" on
incoming traffic
Router(config-if)# ip access-group BLOCK-TFTP out ! Applies ACL named "BLOCK-TFTP" on
outgoing traffic
Router(config-if)# ip nbar protocol-discovery ! Enables NBAR to discover default protocols
and gather statistics
Router(config-if)# ip flow ingress ! Enables NetFlow accounting for incoming packets
Router(config-if)# ip flow egress ! Enables NetFlow accounting for outgoing packets
Router(config-if)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
Router(config-if)# no ip mroute-cache ! Disables fast-switching of multicast packets
Router(config-if)# snmp trap link-status ! Generates SNMP trap when link-status changes
```

Apply the following command on the Serial3 interface after defining the *EIGHT-CLASS-V3PN-EDGE-SHAPE* class as shown in the Security section.

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

Apply the following command on the Serial3 interface after defining the *Public* security zone in the Security section.

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

Apply the following command on the Serial3 interface after defining the *VPN-MAP* crypto map in the Security section if using GETVPN

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

Multiport DS-1 Interface with Multilink Point-to-Point Encapsulation

To support the multilink PPP configuration, four interfaces on the HWIC-4T were bundled together to form a single multilink bundle.

```
Router(config)# interface Multilink1 ! Enters multilink interface configuration mode
Router(config-if)# ip address 192.168.0.1 255.255.255.252 ! Specifies an IP address for
interface
Router(config-if)# ip access-group BLOCK-TFTP in ! Applies ACL named “BLOCK-TFTP” on
incoming traffic
Router(config-if)# ip access-group BLOCK-TFTP out ! Applies ACL named “BLOCK-TFTP” on
outgoing traffic
Router(config-if)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
Router(config-if)# no ip mroute-cache ! Disables fast-switching of multicast packets
Router(config-if)# ip nbar protocol-discovery ! Enables NBAR to discover default protocols
and gather statistics
Router(config-if)# load-interval 30 ! Specifies interval for computing load statistics
Router(config-if)# ip flow egress ! Enables NetFlow accounting for outgoing packets
Router(config-if)# ip flow ingress ! Enables NetFlow accounting for incoming packets
Router(config-if)# ppp multilink ! Enables Multilink PPP
Router(config-if)# ppp multilink group 1 ! Assigns interface to the multilink group 1
Router(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth
available for QoS reservations
Router(config-if)# exit

Router(config)# interface Serial0/1/0 ! Enters serial interface configuration mode for
channel group 0
Router(config-if)# no ip address
Router(config-if)# encapsulation ppp ! Configures encapsulation type for interface as PPP
Router(config-if)# ppp multilink ! Enables Multilink PPP
Router(config-if)# ppp multilink group 1 ! Assigns interface to multilink group 1
Router(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth
available for QoS reservations
Router(config-if)# no shutdown
Router(config-if)# interface Serial0/1/1 ! Enters serial interface configuration mode for
channel group 0
Router(config-if)# no ip address
Router(config-if)# encapsulation ppp ! Configures encapsulation type for interface as PPP
Router(config-if)# ppp multilink ! Enables Multilink PPP
Router(config-if)# ppp multilink group 1 ! Assigns interface to multilink group 1
Router(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth
available for QoS reservations
Router(config-if)# no shutdown
Router(config-if)# interface Serial0/1/2 ! Enters serial interface configuration mode for
channel group 0
Router(config-if)# no ip address
Router(config-if)# encapsulation ppp ! Configures encapsulation type for interface as PPP
Router(config-if)# ppp multilink ! Enables Multilink PPP
Router(config-if)# ppp multilink group 1 ! Assigns interface to multilink group 1
Router(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth
available for QoS reservations
Router(config-if)# no shutdown
Router(config-if)# interface Serial0/1/3 ! Enters serial interface configuration mode for
channel group 0
Router(config-if)# no ip address
Router(config-if)# encapsulation ppp ! Configures encapsulation type for interface as PPP
Router(config-if)# ppp multilink ! Enables Multilink PPP
Router(config-if)# ppp multilink group 1 ! Assigns interface to multilink group 1
Router(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth
available for QoS reservations
Router(config-if)# no shutdown
Router(config-if)# exit
```

Apply the following command on the Multilink1 interface after defining the *EIGHT-CLASS-V3PN-EDGE-SHAPE* class as shown in the Security section.

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

Apply the following command on the Multilink1 interface after defining the *Public* security zone as shown in the Security section.

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

Apply the following command on the Multlink1 interface after defining the *VPN-MAP* crypto map as shown in the Security section if using GETVPN.

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

Verification of Multiport DS-1 Interface with Multilink PPP Encapsulation

To verify the multilink interface configuration, enter the **show ppp multilink** command to display the active serial interfaces bundled as part of PPP multilink.

```
Router# show ppp multilink

Multilink1
  Bundle name: BRANCH
  Remote Endpoint Discriminator: [1] ISP-1
  Local Endpoint Discriminator: [1] Router
  Bundle up for 2w2d, total bandwidth 8192, load 1/255
  Receive buffer limit 48000 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    3 lost fragments, 4704524 reordered
    9/800 discarded fragments/bytes, 0 lost received
    0xE543EE received sequence, 0xE83A54 sent sequence
  Member links: 4 active, 0 inactive (max not set, min not set)
    Se0/1/0, since 2w2d
    Se0/1/1, since 2w2d
    Se0/1/2, since 2w2d
    Se0/1/3, since 2w2d
No inactive multilink interfaces
Router#
```

Use the **show interface multilink** command to show the status of multilink.

```
Router1# show interface Multilink 1
Multilink1 is up, line protocol is up
  Hardware is multilink group interface
  Internet address is 192.168.0.1/30
  Backup interface ATM0/2/IMA0, failure delay 0 sec, secondary disable delay 0 sec,
  kickin load not set, kickout load not set
  MTU 1500 bytes, BW 8192 Kbit, DLY 100000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open, multilink Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  DTR is pulsed for 2 seconds on reset
  Last input 00:00:21, output never, output hang never
  Last clearing of "show interface" counters 2w2d
  Input queue: 0/75/178/0 (size/max/drops/flushes); Total output drops: 791
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 1000 bits/sec, 1 packets/sec
     5463859 packets input, 1356700636 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     12 input errors, 0 CRC, 1 frame, 0 overrun, 0 ignored, 8 abort
     5275968 packets output, 3619744669 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
Router#
```

Multiport DS-1 Interface with Multilink Frame Relay Encapsulation

To support the multilink Frame Relay configuration, four interfaces on the HWIC-4T were bundled together to form a single multilink bundle.

```
Router(config)# interface MFR 1 ! Enters Frame Relay multilink interface configuration mode
Router(config-if)# encapsulation frame-relay ! Specifies Frame Relay encapsulation for the
interface
Router(config-if)# ip address 192.168.0.1 255.255.255.252 ! Specifies an IP address for
interface
Router(config-if)# ip access-group BLOCK-TFTP in ! Applies ACL named "BLOCK-TFTP" on
incoming traffic
Router(config-if)# ip access-group BLOCK-TFTP out ! Applies ACL named "BLOCK-TFTP" on
outgoing traffic
Router(config-if)# no ip mroute-cache ! Disables fast-switching of multicast packets
Router(config-if)# ip nbar protocol-discovery ! Enables NBAR to discover default protocols
and gather statistics
Router(config-if)# load-interval 30 ! Specifies interval for computing load statistics
Router(config-if)# ip flow egress ! Enables NetFlow accounting for outgoing packets
Router(config-if)# ip flow ingress ! Enables NetFlow accounting for incoming packets
Router(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth
available for QoS reservations
Router(config-if)# end

Router(config)# interface Serial0/1/0 ! Enters serial interface configuration mode for
channel group 1
Router(config-if)# encapsulation frame-relay MFR 1 ! Assigns the link to MFR bundle with id
1
Router(config-if)# no shutdown
Router(config-if)# interface Serial0/1/1 ! Enters serial interface configuration mode for
channel group 1
Router(config-if)# encapsulation frame-relay MFR 1 ! Assigns the link to MFR bundle with id
1
Router(config-if)# no shutdown
Router(config-if)# interface Serial0/1/2 ! Enters serial interface configuration mode for
channel group 1
Router(config-if)# encapsulation frame-relay MFR 1 ! Assigns the link to MFR bundle with id
1
Router(config-if)# no shutdown
Router(config-if)# interface Serial0/1/3 ! Enters serial interface configuration mode for
channel group 1
Router(config-if)# encapsulation frame-relay MFR 1 ! Assigns the link to MFR bundle with id
1
Router(config-if)# end
```

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

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

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

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

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

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

Onboard Gigabit Ethernet Interface

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

Note When using the Small Form Plugable (SFP) module that provides optical connectivity, the default media type for the interface must be changed to SFP.

```
Branch(config)# interface gigabitEthernet0/0! Enters the gigabit Ethernet interface
configuration mode
Branch(config-if)# ip address 192.168.0.1 255.255.255.252 ! Specifies an IP address for
interface
Branch(config-if)# ip access-group BLOCK-TFTP in ! Applies ACL named "BLOCK-TFTP" on
incoming traffic
Branch(config-if)# ip access-group BLOCK-TFTP out ! Applies ACL named "BLOCK-TFTP" on
outgoing traffic
Branch(config-subif)# ip nbar protocol-discovery ! Enables NBAR to discover default
protocols and gather statistics
Branch(config-if)# ip flow ingress ! Enables NetFlow accounting for incoming traffic
Branch(config-if)# ip flow egress ! Enables NetFlow accounting for outgoing traffic
Branch(config-if)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
Branch(config-if)# no ip mroute-cache ! Disables fast-switching of multicast packets
Branch(config-if)# load-interval 30 ! Specifies interval for computing load statistics
Branch(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth
available for QoS reservations
Branch(config-if)# media-type sfp ! Sets the Ethernet connector to SFP module
Branch(config-if)# no shutdown
Branch(config-if)# end
```

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

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

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

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

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

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

LAN Services Implementation

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

The Multilayered Branch LAN architecture can be divided into the following layers:

- Edge Layer: Provides WAN connectivity, routing, addressing, high availability, quality of service (QoS), security, management services, and an exit point to the rest of the network.
- Distribution Layer: Provides private VLANs and trunking.

- Access Layer: Provides connectivity and Power-over-Ethernet (PoE) to end user devices. Layer 2 security, authentication, private VLANs, and QoS are addressed at this layer.

Edge Layer

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

- Data VLAN, page 11
- Voice VLAN, page 11
- DMZ VLAN, page 12
- Management VLAN, page 12

Enable the LAN facing the Gigabit Ethernet interface.

```
Branch(config)# interface GigabitEthernet0/1 ! Enters gigabit Ethernet sub-interface 2
configuration mode
Branch(config-subif)# no shutdown
```

Data VLAN

```
Branch(config)# interface GigabitEthernet2/0.1 ! Enters internal gigabit Ethernet
sub-interface 1 configuration mode
Branch(config-subif)# description Data-VLAN
Branch(config-subif)# encapsulation dot1Q 301 ! Defines IEEE 802.1Q VLAN encapsulation
type
Branch(config-subif)# ip address 10.0.0.1 255.255.255.0 ! Assigns IP address to the
interface
Branch(config-subif)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
```

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

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

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

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

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

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

Voice VLAN

```
Branch(config)# interface GigabitEthernet2/0.2 ! Enters internal gigabit Ethernet
sub-interface 2 configuration mode
Branch(config-subif)# description Voice-VLAN
Branch(config-subif)# encapsulation dot1Q 302 ! Defines IEEE 802.1Q VLAN encapsulation
type
```

```
Branch(config-subif)# ip address 10.0.1.1 255.255.255.0 ! Assigns IP address to the
interface
Branch(config-subif)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
```

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

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

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

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

DMZ VLAN

```
Branch(config-subif)# interface GigabitEthernet2/0.3 ! Enters internal gigabit Ethernet
sub-interface 3 configuration mode
Branch(config-subif)# description DMZ-VLAN
Branch(config-subif)# encapsulation dot1Q 303 ! Defines IEEE 802.1Q VLAN encapsulation
type
Branch(config-subif)# ip address 10.0.2.65 255.255.255.240 ! Assigns IP address to the
interface
Branch(config-subif)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
```

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

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

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

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

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

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

Management VLAN

```
Branch(config-subif)# interface GigabitEthernet2/0.4 ! Enters internal gigabit Ethernet
sub-interface 4 configuration mode
Branch(config-subif)# description Management-VLAN
Branch(config-subif)# encapsulation dot1Q 310 ! Defines IEEE 802.1Q VLAN encapsulation
type
Branch(config-subif)# ip address 10.0.2.1 255.255.255.224 ! Assigns IP address to the
interface
Branch(config-subif)# ip pim sparse-dense-mode ! Enables multicast in sparse-dense mode
```

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

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

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

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

Distribution Layer

Configuring EtherSwitch Service Module

The EtherSwitch service module is accessible from the router's command line. The Gigabit Ethernet link between the router and the switch requires IP addresses to be configured in order to session into the module.

```
Branch(config)#interface GigabitEthernet 1/0

Branch(config-if)#ip address 10.0.2.93 255.255.255.252 ! Assigns IP address to internal
Gigabit Ethernet link
Branch(config-if)#no shutdown
Branch(config-if)#exit
```

From the console, initiate a session with the EtherSwitch service module.

```
Branch# service-module gigabitEthernet 2/0 session
Trying 10.0.2.93, 2066 ... Open

         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]:
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname Switch-Dist
```

VLAN Trunking Protocol Implementation

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

In the Services Ready Medium Branch Network, the EtherSwitch service module at the distribution layer was configured as the VTP server.

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

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

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

VTP Verification

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

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

VLAN Implementation

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

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

```
Switch-Dist(config)# vlan 301 ! Creates Data VLAN to vlan database
Switch-Dist(config-vlan)# name DATA
Switch-Dist(config-vlan)# exit
Switch-Dist(config)# vlan 302 ! Creates Voice VLAN to vlan database
Switch-Dist(config-vlan)# name VOICE
Switch-Dist(config-vlan)# exit
Switch-Dist(config) # vlan 303 ! Creates DMZ VLAN to vlan database
Switch-Dist(config-vlan)# name DMZ
Switch-Dist(config-vlan)# exit
Switch-Dist(config)# vlan 310 ! Creates management VLAN to vlan database
Switch-Dist(config-vlan)# name MANAGEMENT
Switch-Dist(config-vlan)# exit
Switch-Dist(config-vlan)# vlan 333 ! Creates black hole VLAN to vlan database
Switch-Dist(config-vlan)# name BLACKHOLE
```

```
Switch-Dist(config-vlan)# exit
Switch-Dist(config)# interface Vlan301 ! Enters Data VLAN configuration mode
Switch-Dist(config-if)# ip address 10.0.0.254 255.255.255.0 ! Specifies the IP address for
the SVI interface
Switch-Dist(config-if)# interface Vlan302 ! Enters Voice VLAN configuration mode
Switch-Dist(config-if)# ip address 10.0.1.0 254 255.255.255.0 ! Specifies the IP address
for the SVI interface
Switch-Dist(config-if)# interface Vlan303 ! Enters switch virtual interface (SVI)
configuration
Switch-Dist(config-if)# ip address 10.0.2.78 255.255.255.240 ! Specifies the IP address for
the SVI interface
Switch-Dist(config-if)# interface Vlan310 ! Enters Management VLAN interface configuration
mode
Switch-Dist(config-if)# ip address 10.0.2.30 255.255.255.224 ! Specifies the IP address for
the SVI interface
```

Spanning Tree Implementation

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

Spanning Tree Verification

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

```
Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short
       <Removed>
```

Uplink to Router Implementation

```
Switch-Dist(config)# interface g1/0/2 ! Enters gigabit Ethernet interface configuration
mode for internal link to the router
Switch-Dist(config-if)# description trunk to router
Switch-Dist(config-if)# switchport trunk encapsulation dot1q ! Tags outgoing frames with
IEEE 802.1Q trunk encapsulation format
Switch-Dist(config-if)# switchport trunk allowed vlan 301-303,310 ! Defines list of allowed
VLANs that can send traffic on the trunk.
Switch-Dist(config-if)# switchport mode trunk ! Enables the Ethernet port as VLAN trunk
Switch-Dist(config-if)# load-interval 30 ! Specifies interval for computing load
statistics
```

EtherChannel Implementation

EtherChannel supports the IEEE 802.3ad Link Aggregation Control Protocol (LACP) that has three EtherChannel modes:

- On: The link aggregation is forced to be formed without any LACP negotiation. In other words, the switch will neither send the LACP packet nor process any incoming LACP packet.
- Passive: The switch does not initiate the channel, but does understand incoming LACP packets. The peer (in the active state) initiates negotiation (by sending out an LACP packet) which is received and replied to, eventually forming the aggregation channel with the peer.
- Active: An aggregate link is formed, and it initiates the negotiation. The link aggregate will be formed if the other end is running in LACP active or passive mode. This is the recommended configuration.

EtherChannel was established between access layer Catalyst 3560 switches and the EtherSwitch service module using LACP.

```
Switch-Dist(config)# interface f1/0/1 ! Enters Fast Ethernet port 1 configuration mode
Switch-Dist(config-if)# description EtherChannel link-1 to access switch 1
Switch-Dist(config-if)# switchport trunk encapsulation dot1q ! Tags outgoing frames with
IEEE 802.1Q trunk encapsulation format
Switch-Dist(config-if)# switchport mode trunk ! Enables the Ethernet port as VLAN trunk
Switch-Dist(config-if)# load-interval 30 ! Specifies interval for computing load
statistics
Switch-Dist(config-if)# mls qos trust dscp ! Accept incoming DSCP markings
Switch-Dist(config-if)# channel-group 1 mode active ! Assigns the interface to EtherChannel
group 1 in LACP active mode
Creating a port-channel interface Port-channel 1
Switch-Dist(config-if)# interface f1/0/2 ! Enters Fast Ethernet port 2 configuration
Switch-Dist(config-if)# description EtherChannel link-2 to access switch 1
Switch-Dist(config-if)# switchport trunk encapsulation dot1q ! Tags outgoing frames with
IEEE 802.1Q trunk encapsulation format
Switch-Dist(config-if)# switchport mode trunk ! Enables the Ethernet port as VLAN trunk
Switch-Dist(config-if)# load-interval 30 ! Specifies interval for computing load
statistics
Switch-Dist(config-if)# mls qos trust dscp ! Accept incoming DSCP markings
Switch-Dist(config-if)# channel-group 1 mode active ! Assigns the interface to be
EtherChannal  group 1 in LACP active mode
Switch-Dist(config-if)# interface Port-channel1 ! Enters EtherChannel specific
configuration
Switch-Dist(config-if)# switchport trunk encapsulation dot1q ! Tags outgoing frames with
IEEE 802.1Q trunk encapsulation format
Switch-Dist(config-if)# switchport mode trunk ! Enables the EtherChannel as VLAN trunk
Switch-Dist(config-if)# load-interval 30 ! Specifies interval for computing load
statistics

Switch-Dist(config)# interface f1/0/3 ! Enters fast Ethernet port 1 configuration mode
Switch-Dist(config-if)# description EtherChannel link-1 to access switch 2
Switch-Dist(config-if)# switchport trunk encapsulation dot1q ! Tags outgoing frames with
IEEE 802.1Q trunk encapsulation format
Switch-Dist(config-if)# switchport mode trunk ! Enables the Ethernet port as VLAN trunk
Switch-Dist(config-if)# load-interval 30 ! Specifies interval for computing load
statistics
Switch-Dist(config-if)# mls qos trust dscp ! Accept incoming DSCP markings
Switch-Dist(config-if)# channel-group 2 mode active ! Assigns the interface to EtherChannel
group 2 in LACP active mode
Creating a port-channel interface Port-channel 2
Switch-Dist(config-if)# interface f1/0/4 ! Enters fast Ethernet port 2 configuration
Switch-Dist(config-if)# description EtherChannel link-2 to access switch 2
Switch-Dist(config-if)# switchport trunk encapsulation dot1q ! Tags outgoing frames with
IEEE 802.1Q trunk encapsulation format
Switch-Dist(config-if)# switchport mode trunk ! Enables the Ethernet port as VLAN trunk
Switch-Dist(config-if)# load-interval 30 ! Specifies interval for computing load
statistics
Switch-Dist(config-if)# mls qos trust dscp ! Accept incoming DSCP markings
```

```
Switch-Dist(config-if)# channel-group 2 mode active ! Assigns the interface to be
EtherChannal  group 2 in LACP active mode
Switch-Dist(config-if)# interface Port-channel2 ! Enters EtherChannel specific
configuration
Switch-Dist(config-if)# switchport trunk encapsulation dot1q ! Tags outgoing frames with
IEEE 802.1Q trunk encapsulation format
Switch-Dist(config-if)# switchport mode trunk ! Enables the EtherChannel as VLAN trunk
Switch-Dist(config-if)# load-interval 30 ! Specifies interval for computing load
statistics
```

EtherChannel Verification

To verify your cross-stack EtherChannel configuration, enter the following commands:

```
Switch-Dist# show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Fa1/0/1(P) Fa1/0/2(P)
2      Po2(SU)         LACP      Fa1/0/3(P) Fa1/0/4(P)

Switch# show interface port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 000d.2851.8d8b (bia 000d.2851.8d8b)
  MTU 1500 bytes, BW 2000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 1000Mb/s, link type is auto, media type is unknown
  Media-type configured as  connector
  input flow-control is off, output flow-control is unsupported
  Members in this channel: Fa1/0/1 Fa1/0/2
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:00, output hang never
  Last clearing of "show interface" counters 6w6d
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 2000 bits/sec, 4 packets/sec
  30 second output rate 134000 bits/sec, 110 packets/sec
     136360555 packets input, 2314351511 bytes, 0 no buffer
     Received 18489892 broadcasts (0 multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 18243546 multicast, 0 pause input
     0 input packets with dribble condition detected
     535580165 packets output, 1770503169 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

DOT1X Services

```
Switch-Dist(config)# aaa new-model ! Enables Authentication, Authorization and Accounting
services
Switch-Dist(config)# aaa authentication dot1x default group radius ! Specifies default
dot1x authentication to use RADIUS server database
Switch-Dist(config)# aaa session-id common ! Specifies to use the same session identifier
for all invocations of accounting services
Switch-Dist(config)# dot1x system-auth-control ! Enables IEEE 802.1x authentication
globally on the switch
Switch-Dist(config)# radius-server host 172.16.0.80 ! Specifies RADIUS server IP address
Switch-Dist(config)# radius-server key KEY-BR ! Specifies RADIUS server key as "KEY-BR"
for encrypting all communication with the RADIUS server
Switch-Dist(config)# int range f1/0/5 - 16 ! Enters configuration for range of gigabit
Ethernet ports
Switch-Dist(config-if-range)# dot1x port-control auto ! Enables dot1x authentication on
the port
Switch-Dist(config-if-range)# dot1x timeout server-timeout 60 ! Specifies time to wait for
a response from RADIUS server before retransmitting
```

The mapping for the CoS to DSCP values is shown in Figure 35 in the "Quality of Service" section on page 41.

```
Switch-Dist(config)# mls qos ! Enables QoS on the switch
Switch-Dist(config)# mls qos map policed-dscp 0 10 18 24 25 34 to 8 ! Defines Policed-DSCP
map which is used to mark down the packets with specified values to DSCP 8.
Switch-Dist(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56 ! Defines CoS-DSCP map for
preferential treatment
Switch-Dist(config)# mls qos srr-queue output cos-map queue 1 threshold 3 5 ! Maps the CoS
5 to egress queue 1 with threshold 3
Switch-Dist(config)# mls qos srr-queue output cos-map queue 2 threshold 1 2 4 ! Maps the
CoS 2 and CoS 4to egress queue 2 with threshold 1
Switch-Dist(config)# mls qos srr-queue output cos-map queue 2 threshold 2 3 ! Maps the CoS
3 to egress queue 2 with threshold 2
Switch-Dist(config)# mls qos srr-queue output cos-map queue 2 threshold 3 6 7 ! Maps the
CoS 6 and CoS 7to egress queue 2 with threshold 3
Switch-Dist(config)# mls qos srr-queue output cos-map queue 3 threshold 3 0 ! Maps the CoS
0 to egress queue 3 with threshold 3
Switch-Dist(config)# mls qos srr-queue output cos-map queue 4 threshold 3 1 ! Maps the CoS
1to egress queue 4 with threshold 3
Switch-Dist(config)# mls qos srr-queue output dscp-map queue 1 threshold 3 46 ! Maps the
DSCP value 46 to egress queue 1 with threshold 3
Switch-Dist(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22 25
32 34 36  ! Maps the DSCP values16, 18, 20, 22, 25, 32, 34 and 36 to egress queue 2 with
threshold 1
Switch-Dist(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 38 ! Maps the
DSCP value 38 to egress queue 2 with threshold 1
Switch-Dist(config)# mls qos srr-queue output dscp-map queue 2 threshold 2 24 26 36 ! Maps
the DSCP values 24, 26, and 36 to egress queue 2 with threshold 2
Switch-Dist(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 48 56 36 ! Maps
the DSCP values 36, 48, and 56 to egress queue 2 with threshold 3
Switch-Dist(config)# mls qos srr-queue output dscp-map queue 3 threshold 3 0 36 ! Maps the
DSCP values 0 and 36 to egress queue 3 with threshold 3
Switch-Dist(config)# mls qos srr-queue output dscp-map queue 4 threshold 1 8 36 ! Maps the
DSCP values 8 and 36 to egress queue 4 with threshold 1
Switch-Dist(config)# mls qos srr-queue output dscp-map queue 4 threshold 3 10 12 14 36 !
Maps the DSCP values 10, 12,14, and 36 to egress queue 4 with threshold 3
Switch-Dist(config)# mls qos queue-set output 1 threshold 2 70 80 100 100 ! Defines the
weighed tail-drop thresholds for queue 2 to 70% for threshold 1 and 80% for threshold 2
Switch-Dist(config)# mls qos queue-set output 1 threshold 4 40 100 100 100 ! Defines the
weighed tail-drop thresholds for queue 4 to 40% for threshold 1 and 100% for threshold 2
```

The distribution layer switches are connected only to DMZ servers that should be collocated and physically secured. Therefore, all DSCP marking originating at DMZ servers is trusted.

```
Switch-Dist(config)# int range f1/0/5 - 16 ! Enters configuration for range of gigabit
Ethernet ports
Switch-Dist(config-if-range)# mls qos trust dscp ! Accept incoming DSCP markings
```

Access Layer

- VTP Implementation, page 19
- Spanning Tree Implementation, page 19
- EtherChannel Implementation, page 19
- DOT1X Services, page 21
- QoS Implementation, page 21
- Assigning QoS to Switch Port, page 24

VTP Implementation

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

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

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

Spanning Tree Implementation

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

EtherChannel Implementation

```
Switch-Access(config)# interface g1/0/1 ! Enters port 0 configuration mode
Switch-Access(config-if)# switchport trunk encapsulation dot1q ! Tags outgoing frames with
IEEE 802.1Q trunk encapsulation format
Switch-Access(config-if)# switchport mode trunk ! Enables the Ethernet port as VLAN trunk
Switch-Access(config-if)# load-interval 30 ! Specifies interval for computing load
statistics
Switch-Access(config-if)# channel-group 1 mode active! Assigns the interface to be
EtherChannal EtherChannel group 1 in LACP active mode
Switch-Access(config-if)# interface g1/0/2 ! Enters port 1 configuration mode
Switch-Access(config-if)# switchport trunk encapsulation dot1q ! Tags outgoing frames with
IEEE 802.1Q trunk encapsulation format
Switch-Access(config-if)# switchport mode trunk ! Enables the Ethernet port as VLAN trunk
```

```
Switch-Access(config-if)# load-interval 30 ! Specifies interval for computing load
statistics
Switch-Access(config-if)# channel-group 1 mode active ! Assigns the interface to be
EtherChannal EtherChannel group 1 in LACP active mode
Switch-Access(config-if)# exit
Switch-Access(config)# interface Port-channel1 ! Enters EtherChannel specific
configuration mode
Switch-Access(config-if)# switchport trunk encapsulation dot1q ! Tags outgoing frames with
IEEE 802.1Q trunk encapsulation format
Switch-Access(config-if)# switchport mode trunk ! Enables the EtherChannel as VLAN trunk
Switch-Access(config-if)# load-interval 30 ! Specifies interval for computing load
statistics
Switch-Access(config-if)# exit

Switch-Access(config)# interface g1/0/3 ! Enters port 3 configuration mode
Switch-Access(config-if)# switchport trunk encapsulation dot1q ! Tags outgoing frames with
IEEE 802.1Q trunk encapsulation format
Switch-Access(config-if)# switchport mode trunk ! Enables the Ethernet port as VLAN trunk
Switch-Access(config-if)# load-interval 30 ! Specifies interval for computing load
statistics
Switch-Access(config-if)# channel-group 2 mode active ! Assigns the interface to be
EtherChannal EtherChannel group 2 in LACP active mode
Switch-Access(config-if)# interface g1/0/4 ! Enters port 4 configuration mode
Switch-Access(config-if)# switchport trunk encapsulation dot1q ! Tags outgoing frames with
IEEE 802.1Q trunk encapsulation format
Switch-Access(config-if)# switchport mode trunk ! Enables the Ethernet port as VLAN trunk
Switch-Access(config-if)# load-interval 30 ! Specifies interval for computing load
statistics
Switch-Access(config-if)# channel-group 2 mode active ! Assigns the interface to be
EtherChannal EtherChannel group 2 in LACP active mode
Switch-Access(config-if)# exit
Switch-Access(config)# interface Port-channel2 ! Enters EtherChannel specific
configuration mode
Switch-Access(config-if)# switchport trunk encapsulation dot1q ! Tags outgoing frames with
IEEE 802.1Q trunk encapsulation format
Switch-Access(config-if)# switchport mode trunk ! Enables the EtherChannel as VLAN trunk
Switch-Access(config-if)# load-interval 30 ! Specifies interval for computing load
statistics
Switch-Access(config-if)# exit
```

VLAN Implementation

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

```
Switch-Access(config)# interface range g1/0/5 - 52 ! Enters configuration for range of
gigabit Ethernet ports
Switch-Access(config-if-range)# switchport mode access ! Sets the port to access mode
Switch-Access(config-if-range)# switch access vlan 301 ! Assigns the port to Data VLAN
Switch-Access(config-if-range)# switchport voice vlan 302 ! Assigns the port to Voice VLAN
Switch-Access(config-if-range)# srr-queue bandwidth share 1 70 25 5 ! Enables bandwidth
sharing for all output queues. Queue 1 is strict priority queue, queue 2 gets 70% of
bandwidth, queue 3 25% of bandwidth, and queue 4 5% of the bandwidth
Switch-Access(config-if-range)# srr-queue bandwidth shape 3 0 0 0  ! Specifies queue 2,3,4
to operate in shared mode.
Switch-Access(config-if-range)# priority-queue out ! Egress expedite queue is enabled.
This command will force SRR to ignore weight of queue 1 while calculating the bandwidth
ratio. This queue will be emptied before servicing other queues.
Switch-Access(config-if-range)# mls qos trust device cisco-phone ! Specifies the port to
trust the CoS/DSCP value if the CDP neighbor is Cisco IP Phone
```

```
Switch-Access(config-if-range)# spanning-tree portfast ! Sets the switch port to
forwarding state ignoring listening/learning state
Switch-Access(config-if-range)# load-interval 30 ! Specifies interval for computing load
statistics
```

DOT1X Services

```
Switch-Access(config)# aaa new-model ! Enables Authentication, Authorization and
Accounting services
Switch-Access(config)# aaa authentication dot1x default group radius ! Specifies default
dot1x authentication to use RADIUS server database
Switch-Access(config)# aaa session-id common ! Specifies to use the same session identifier
for all invocations of accounting services
Switch-Access(config)# dot1x system-auth-control ! Enables IEEE 802.1x authentication
globally on the switch
Switch-Access(config)# radius-server host 172.16.0.80 ! Specifies RADIUS server IP address
Switch-Access(config)# radius-server key KEY-BR ! Specifies RADIUS server key as "KEY-BR"
for encrypting all communication with the RADIUS server
Switch-Access(config)# int range g1/0/5 - 52! Enters configuration for the range of Gigabit
Ethernet ports
Switch-Access(config-if-range)# dot1x port-control auto ! Enables dot1x authentication on
the port
Switch-Access(config-if-range)# dot1x timeout server-timeout 60 ! Specifies time to wait
for a response from RADIUS server before retransmitting
```

DOT1X Services Verification

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

```
Switch-Access# show dot1x interface g1/0/5
Supplicant MAC <Not Applicable>
   AuthSM State      = N/A
   BendSM State      = N/A
PortStatus        = N/A
MaxReq            = 2
MaxAuthReq        = 2
HostMode          = Single
PortControl       = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 60 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

QoS Implementation

The mapping for the CoS to DSCP values is shown in Figure 35 in the "Quality of Service" section on page 41.

```
Switch-Access(config)# mls qos ! Enables QoS on the switch
Switch-Access(config)# mls qos map policed-dscp 0 10 18 24 25 34 to 8 ! Defines
Policed-DSCP map which is used to mark down the packets with specified values to DSCP 8.
Switch-Access(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56 ! Defines CoS-DSCP map
for preferential treatment
Switch-Access(config)# mls qos srr-queue output cos-map queue 1 threshold 3 5 ! Maps the
CoS 5 to egress queue 1 with threshold 3
Switch-Access(config)# mls qos srr-queue output cos-map queue 2 threshold 1 2 4 ! Maps the
CoS 2 and CoS 4to egress queue 2 with threshold 1
```

```
Switch-Access(config)# mls qos srr-queue output cos-map queue 2 threshold 2 3 ! Maps the
CoS 3 to egress queue 2 with threshold 2
Switch-Access(config)# mls qos srr-queue output cos-map queue 2 threshold 3 6 7 ! Maps the
CoS 6 and CoS 7to egress queue 2 with threshold 3
Switch-Access(config)# mls qos srr-queue output cos-map queue 3 threshold 3 0 ! Maps the
CoS 0 to egress queue 3 with threshold 3
Switch-Access(config)# mls qos srr-queue output cos-map queue 4 threshold 3 1 ! Maps the
CoS 1to egress queue 4 with threshold 3
Switch-Access(config)# mls qos srr-queue output dscp-map queue 1 threshold 3 46 ! Maps the
DSCP value 46 to egress queue 1 with threshold 3
Switch-Access(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22
25 32 34 36 ! Maps the DSCP values16, 18, 20, 22, 25, 32, 34 and 36 to egress queue 2 with
threshold 1
Switch-Access(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 38 ! Maps the
DSCP value 38 to egress queue 2 with threshold 1
Switch-Access(config)# mls qos srr-queue output dscp-map queue 2 threshold 2 24 26 36 !
Maps the DSCP values 24, 26, and 36 to egress queue 2 with threshold 2
Switch-Access(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 48 56 36 !
Maps the DSCP values 36, 48, and 56 to egress queue 2 with threshold 3
Switch-Access(config)# mls qos srr-queue output dscp-map queue 3 threshold 3 0 36 ! Maps
the DSCP values 0 and 36 to egress queue 3 with threshold 3
Switch-Access(config)# mls qos srr-queue output dscp-map queue 4 threshold 1 8 36 ! Maps
the DSCP values 8 and 36 to egress queue 4 with threshold 1
Switch-Access(config)# mls qos srr-queue output dscp-map queue 4 threshold 3 10 12 14 36
! Maps the DSCP values 10, 12,14, and 36 to egress queue 4 with threshold 3
Switch-Access(config)# mls qos queue-set output 1 threshold 2 70 80 100 100 ! Defines the
weighed tail-drop thresholds for queue 2 to 70% for threshold 1 and 80% for threshold 2
Switch-Access(config)# mls qos queue-set output 1 threshold 4 40 100 100 100 ! Defines the
weighed tail-drop thresholds for queue 4 to 40% for threshold 1 and 100% for threshold 2
Switch-Access(config)# ip access-list extended DVLAN-BULK-DATA ! Defines ACL to match Bulk
Data
Switch-Access(config-ext-nacl)# permit tcp any any eq 220 ! Match Internet Mail Access
Protocol v3 (IMAPv3)
Switch-Access(config-ext-nacl)# permit tcp any any eq 143 ! Match Internet Message Access
Protocol (IMAP)
Switch-Access(config-ext-nacl)# permit tcp any any eq smtp ! Match Simple Mail Transfer
Protocol
Switch-Access(config-ext-nacl)# ip access-list extended DVLAN-MISSION-CRITICAL-DATA !
Defines ACL to match Business Critical Data
Switch-Access(config-ext-nacl)# permit tcp any any eq www ! Match HTTP traffic for port 80
Switch-Access(config-ext-nacl)# permit tcp any any range 3200 3203 ! Match SAP traffic
Switch-Access(config-ext-nacl)# permit tcp any any eq 3600 ! Match SAP traffic
Switch-Access(config-ext-nacl)# permit tcp any any range 2000 2002 ! Match SCCP traffic
Switch-Access(config-ext-nacl)# permit udp any any eq isakmp ! Match Internet Security
Association and Key Management Protocol
Switch-Access(config-ext-nacl)# permit tcp any eq www any ! Match HTTP traffic coming from
source port 80
Switch-Access(config-ext-nacl)# ip access-list extended DVLAN-PC-VIDEO
! Defines ACL to match Video traffic
Switch-Access(config-ext-nacl)# permit udp any any range 16384 32767! Match traffic in the
given port range
Switch-Access(config-ext-nacl)# ip access-list extended DVLAN-TRANSACTIONAL-DATA
! Defines ACL to match Transactional Data
Switch-Access(config-ext-nacl)# permit tcp any any eq 1352 ! Match Lotus Notes traffic
Switch-Access(config-ext-nacl)# permit udp any any eq domain ! Match DNS traffic
Switch-Access(config-ext-nacl)# permit udp any any eq netbios-dgm ! Match NetBios traffic
Switch-Access(config-ext-nacl)# permit udp any any eq netbios-ns ! Match NetBios traffic
Switch-Access(config-ext-nacl)# permit udp any any eq netbios-ss ! Match NetBios traffic
Switch-Access(config-ext-nacl)# ip access-list extended VVLAN-ANY ! Defines ACL to match
Voice VLAN traffic
Switch-Access(config-ext-nacl)# permit ip 10.0.1.0 0.0.0.255 any
Switch-Access(config-ext-nacl)# ip access-list extended VVLAN-CALL-SIGNALING ! Defines ACL
to match voice signaling traffic
Switch-Access(config-ext-nacl)# permit udp 10.0.1.0 0.0.0.255 any
```

```
Switch-Access(config-ext-nacl)# permit tcp 10.0.1.0 0.0.0.255 any range 2000 2002
Switch-Access(config-ext-nacl)# ip access-list extended VVLAN-VOICE ! Defines ACL to match
voice traffic
Switch-Access(config-ext-nacl)# permit udp 10.0.1.0 0.0.0.255 any
Switch-Access(config-ext-nacl)# permit udp 10.0.1.0 0.0.0.255 any range 16384 32767
Switch-Access(config-ext-nacl)# class-map match-all DVLAN-TRANSACTIONAL-DATA ! Defines
class-map for Transactional Data
Switch-Access(config-cmap)# match access-group name DVLAN-TRANSACTIONAL-DATA ! Matches
traffic specified in DVLAN-TRANSACTIONAL-DATA ACL
Switch-Access(config-cmap)# class-map match-all DVLAN-PC-VIDEO ! Defines class-map for
Video traffic
Switch-Access(config-cmap)# match access-group name DVLAN-PC-VIDEO ! Matches traffic
specified in DVLAN-PC-VIDEO ACL
Switch-Access(config-cmap)# class-map match-all VVLAN-CALL-SIGNALING ! Defines class-map
for Voice signalling
Switch-Access(config-cmap)# match access-group name VVLAN-CALL-SIGNALING ! Matches traffic
specified in VVLAN-CAL-SIGNALING ACL
Switch-Access(config-cmap)# class-map match-all DVLAN-MISSION-CRITICAL-DATA
! Defines class-map for Business critical traffic
Switch-Access(config-cmap)# match access-group name DVLAN-MISSION-CRITICAL-DATA
! Matches traffic specified in DVLAN-MISSION_CRITICAL_DATA ACL
Switch-Access(config-cmap)# class-map match-all VVLAN-VOICE ! Defines class-map for voice
traffic
Switch-Access(config-cmap)# match access-group name VVLAN-VOICE ! Matches traffic
specified in VVLAN-VOICE ACL
Switch-Access(config-cmap)# class-map match-all VVLAN-ANY ! Defines class-map for voice
vlan traffic
Switch-Access(config-cmap)# match access-group name VVLAN-ANY ! Matches traffic specified
in VVLAN-ANY ACL
Switch-Access(config-cmap)# class-map match-all DVLAN-BULK-DATA ! Defines class-map for
Bulk traffic
Switch-Access(config-cmap)# match access-group name DVLAN-BULK-DATA ! Matches traffic
specified in DVLAN-BULK_DATA ACL
Switch-Access(config-cmap)# policy-map IPPHONE+PC-ADVANCED ! Defines Policy-map
Switch-Access(config-pmap)# class VVLAN-VOICE ! Matches traffic classified by VVLAN-VOICE
class-map
Switch-Access(config-pmap-c)# set dscp ef ! Set DSCP value to EF
Switch-Access(config-pmap-c)# police 6144000 61440 exceed-action drop ! Incoming traffic
will be policed to 6.2 Mbps with a 62 KB burst size and if the rate is exceeded packet
will be dropped
Switch-Access(config-pmap-c)# class VVLAN-CALL-SIGNALING ! Matches traffic classified by
VVLAN-VOICE class-map
Switch-Access(config-pmap-c)# set dscp cs3 ! Set DSCP value to CS3
Switch-Access(config-pmap-c)# police 1024000 10240 exceed-action policed-dscp-transmit
!Incoming traffic will be policed to 10.2 Mbps with a 10.2 KB burst size and if the rate
is exceeded packet will be marked down to Scavenger class (CS1)
Switch-Access(config-pmap-c)# class VVLAN-ANY ! Matches traffic classified by class-map
Switch-Access(config-pmap-c)# set dscp default ! Set DSCP value to 0
Switch-Access(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit !
Incoming traffic will be policed to 32 kbps with a 8 KB burst size and if the rate is
exceeded packet will be marked down to Scavenger class (CS1)
Switch-Access(config-pmap-c)# class DVLAN-PC-VIDEO ! Matches traffic classified by
class-map
Switch-Access(config-pmap-c)# set dscp af41 ! Set DSCP value to 0
Switch-Access(config-pmap-c)# police 1984000 19840 exceed-action policed-dscp-transmit
!Incoming traffic will be policed to 10.2 Mbps with a 10.2 KB burst size and if the rate
is exceeded packet will be marked down to Scavenger class (CS1)
Switch-Access(config-pmap-c)# class DVLAN-MISSION-CRITICAL-DATA ! Matches traffic
classified by class-map
Switch-Access(config-pmap-c)# set dscp 25 ! Set DSCP value to 25
Switch-Access(config-pmap-c)# police 12500000 125000 exceed-action policed-dscp-transmit
!Incoming traffic will be policed to 12.5 Mbps with a 125 KB burst size and if the rate is
exceeded packet will be marked down to Scavenger class (CS1)
```

```
Switch-Access(config-pmap-c)# class DVLAN-TRANSACTIONAL-DATA ! Matches traffic classified
by class-map
Switch-Access(config-pmap-c)# police 10000000 100000 exceed-action policed-dscp-transmit
!Incoming traffic will be policed to 10 Mbps with a 100 KB burst size and if the rate is
exceeded packet will be marked down to Scavenger class (CS1)
Switch-Access(config-pmap-c)# set dscp af21 ! Set DSCP value to AF21
Switch-Access(config-pmap-c)# class DVLAN-BULK-DATA ! Matches traffic classified by
class-map
Switch-Access(config-pmap-c)# set dscp af11 ! Set DSCP value to AF11
Switch-Access(config-pmap-c)# police 5000000 50000 exceed-action policed-dscp-transmit
!Incoming traffic will be policed to 5 Mbps with a 50 KB burst size and if the rate is
exceeded packet will be marked down to Scavenger class (CS1)
Switch-Access(config-pmap-c)# class class-default ! Defines default class
Switch-Access(config-pmap-c)# set dscp default ! Set DSCP value to 0
Switch-Access(config-pmap-c)# police 12500000 125000 exceed-action policed-dscp-transmit !
Incoming traffic will be policed to 12.5 Mbps with a 125 KB burst size and if the rate is
exceeded packet will be marked down to Scavenger class (CS1)
```

QoS Verification

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

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

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

Switch-Access# show mls qos maps cos-dscp
   Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   0  8 16 24 32 46 48 56
```

Assigning QoS to Switch Port

```
Switch-Access(config)# interface range g1/0/5 - 52 ! Enters configuration for the range of
Gibabit Ethernet ports
Switch-Access(config-if-range)# service-policy input IPPHONE+PC-ADVANCED ! Applies QoS
policy IPPHONE+PC-ADVANCED to the interface in input direction.
ignoring listening/learning state
```

Verification of Assigning QoS to Switch Port

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

```
Switch-Access# show policy-map interface g1/0/3
 GigabitEthernet1/0/3

  Service-policy input: IPPHONE+PC-ADVANCED

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

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

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

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

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

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

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

    Class-map: class-default (match-any)
      0 packets, 0 bytes
       offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
         rate 0 bps
```

Network Fundamental Services Implementation

- Path Redundancy, page 25
- IP Addressing and IP Routing, page 27

Path Redundancy

- Redundant WAN Link, page 26

Redundant WAN Link

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

```
Router(config)# controller SHDSL 0/2/0 ! Enters controller configuration mode
Router(config-controller)# dsl-group 0 pairs 0, 1, 2 ima ! Creates an IMA bundle pairing 
links 0-2
Router(config-controller-dsl-group)# ima group clock-mode itc ! Defines clock mode for the 
IMA group. Sets the transmit clock for at least one link to be different from the other 
links.
Router(config-controller-dsl-group)# shdsl annex A-B ! Specifies annex A/B of G.991.2 
standard to be used on the controller
Router(config-controller-dsl-group)# shdsl rate auto ! Sets the controller rate 
negotiation in auto mode
Router(config-controller-dsl-group)# end

Router(config)# interface ATM0/2/IMA0 ! Enters IMA interface configuration mode
Router(config-if)# bandwidth 4608 ! Sets the maximum allowed bandwidth in Kbps
Router(config-if)# load-interval 30 ! Specifies interval for computing load statistics
Router(config-if)# max-reserved-bandwidth 100 ! Makes 100 % of interface bandwidth 
available for QoS reservations
Router(config-if)# exit

Router(config)# interface ATM0/2/IMA0.1 point-to-point ! Creates IMA point-to-point 
sub-interface and specifies its parameters
Router(config-subif)# ip address 209.165.201.1 255.255.255.252 ! Assigns IP address to the 
interface
Router(config-subif)# pvc 10/10 ! Creates a PVC and specifies its parameters
Router(config-if-atm-vc)# protocol ip 209.165.201.2 broadcast ! Enables broadcast 
capability to perform reverse-arp on the ISP router
Router(config-if-atm-vc)# vbr-rt 2304 2304 ! Assigns VBR class of service and defines peak 
and average cell rate
Router(config-if-atm-vc)# oam-pvc manage ! Enables end-to-end F5 OAM loopback cell 
transmission and OAM management
Router(config-if-atm-vc)# encapsulation aal5mux ppp Virtual-Template10 ! Configures PPPoA 
AAL5+MUX point-to-point encapsulation and associates it with Virtual-Template

Router(config)# interface Virtual-Template10 ! Enters Virtual Template configuration
Router(config-if)# bandwidth 4608 ! Sets the maximum allowed bandwidth in Kbps
Router(config-if)# ip unnumbered ATM0/2/IMA0.1 ! Reuses the IP address of the IMA 
sub-interface
Router(config-if)# ip nbar protocol-discovery ! Enables NBAR to discover default protocols 
and gather statistics
Router(config-if)# ip flow ingress ! Enables NetFlow accounting for incoming traffic
Router(config-if)# ip flow egress ! Enables NetFlow accounting for outgoing traffic
Router(config-if)# load-interval 30 ! Specifies interval for computing load statistics
Router(config-if)# max-reserved-bandwidth 100 ! Makes 100% of interface bandwidth 
available for QoS reservations
Router(config-if)# end
```

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

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

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

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

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

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

Redundant WAN Link Verification

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

```
Router# show backup
Primary Interface   Secondary Interface   Status
-----------------   -------------------   ------
Multilink1          ATM0/2/IMA0           normal operation
```

IP Addressing and IP Routing

Routing Protocol Implementation

A branch office router is likely to use a single routing protocol. However, because a network may use EIGRP, OSPF, RIPv2, BGP or static routing, all of these protocols were independently validated. The following configurations are for each of the protocols. Table 1 summarizes the subnets in the Services Ready Medium Branch Network.

Table 1 Subnet Assignment

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

Table 1 Subnet Assignment (continued)

Network	Address	Type
EtherSwitch Module	10.0.2.92/30	Private
Central Site Network	172.16.0.0/16	Private

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

Active/Standby Primary/Backup WAN Links with DMVPN Implementation

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

```
Router(config)# interface Multilink1 ! Enters multilink interface configuration mode
Router(config-if)# backup interface ATM0/2/IMA0 ! Specifies backup interface
Router(config-if)# exit

A loopback interface with a public address is used as the source interface for the DMVPN
tunnel.
Router(config)# interface Loopback0 ! Enters loopback interface configuration mode
Router(config-if)# ip address 209.165.201.9 255.255.255.252 ! Specifies loopback subnet
Router(config-if)# exit
```

The "DMVPN Implementation" section on page 54 provides configuration for the tunnel interface. After the tunnel interface is defined, two routing processes are configured: one for the enterprise network, and another for the public network. The following sections provide implementations in which OSPF, EIGRP, and RIPv2 provide routing for enterprise traffic in which BGP is responsible for routing public traffic.

Enterprise Routing With OSPF

Enterprise networks are learned through the tunnel interface.

```
Router(config)# router ospf 1 ! Enables private network OSPF routing process
Router(config-router)# passive interface GigabitEthernet 2/0 ! Disables routing
advertisements on the LAN interface
Router(config-router)# router-id 10.0.0.1 ! Specifies the OSPF router ID
Router(config-router)# network 10.0.0.0 0.0.0.255 area 0 ! Advertises Data VLAN subnet in
backbone area
Router(config-router)# network 10.0.1.0 0.0.0.255 area 0 ! Advertises Voice VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.0 0.0.0.31 area 0 ! Advertises Management VLAN
subnet in backbone area
Router(config-router)# network 10.0.2.64 0.0.0.15 area 0 ! Advertises DMZ VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.80 0.0.0.3 area 0 ! Advertises Tunnel subnet in
backbone area
Router(config-router)# network 10.0.2.88 0.0.0.3 area 0 ! Advertises WAAS subnet in
backbone area
Router(config-router)# exit
```

Enterprise Routing with EIGRP

Enterprise networks are learned through the tunnel interface.

```
Router(config)# router eigrp 1 ! Enables private network EIGRP routing process
Router(config-router)# passive interface GigabitEthernet 2/0 ! Disables routing
advertisements on the LAN interface
Router(config-router)# no auto-summary ! Disable automatic route summarization
Router(config-router)# network 10.0.0.0 0.0.0.255 ! Advertises Data VLAN subnet
Router(config-router)# network 10.0.1.0 0.0.0.255 ! Advertises Voice VLAN subnet
Router(config-router)# network 10.0.2.0 0.0.0.31 ! Advertises Management VLAN subnet
Router(config-router)# network 10.0.2.64 0.0.0.15 ! Advertises DMZ VLAN subnet
Router(config-router)# network 10.0.2.80 0.0.0.3 ! Advertises Tunnel subnet
Router(config-router)# network 10.0.2.88 0.0.0.3 ! Advertises WAAS subnet
Router(config-router)# exit
```

Enterprise Routing with RIPv2

Enterprise networks are learned through the tunnel interface.

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

Service Provider Routing with BGP

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

```
Router(config)# access-list 20 permit 209.165.201.8 0.0.0.3 ! Permits Loopback network and
blocks all others
Router(config)# router bgp 1 ! Enables public and loopback network BGP routing process
Router(config-router)# passive interface GigabitEthernet 2/0 ! Disables routing
advertisements on the LAN interface
Router(config-router)# neighbor 192.168.0.2 remote-as 65015! Neighbor router IP for
primary link that is in autonomous system 65015
Router(config-router)# neighbor 209.165.201.2 remote-as 65016! Neighbor router IP for
backup link that is in autonomous system 65016
Router(config-router)# network 192.168.0.0 mask 255.255.255.252 ! Advertises primary WAN
link subnet
Router(config-router)# network 209.165.201.0 mask 255.255.255.252 ! Advertises backup WAN
link subnet
Router(config-router)# network 209.165.201.8 mask 255.255.255.252 ! Advertises Loopback
subnet
Router(config-router)# distribute-list 20 in ! Block all routing updates except for
Loopback network
Router(config-router)#exit
```

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

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

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

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

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

Enterprise Routing with OSPF

Enterprise networks are learned through the primary WAN interface.

```
Router(config)# router ospf 1 ! Enables private network OSPF routing process
Router(config-router)# passive interface GigabitEthernet 2/0 ! Disables routing
advertisements on the LAN interface
Router(config-router)# router-id 10.0.0.1 ! Specifies the OSPF router ID
Router(config-router)# network 10.0.0.0 0.0.0.255 area 0 ! Advertises Data VLAN subnet in
backbone area
Router(config-router)# network 10.0.1.0 0.0.0.255 area 0 ! Advertises Voice VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.0 0.0.0.31 area 0 ! Advertises Management VLAN
subnet in backbone area
Router(config-router)# network 10.0.2.64 0.0.0.15 area 0 ! Advertises DMZ VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.80 0.0.0.3 area 0 ! Advertises Tunnel subnet in
backbone area
Router(config-router)# network 10.0.2.88 0.0.0.3 area 0 ! Advertises WAAS subnet in
backbone area
Router(config-router)# network 192.168.0.0 0.0.0.3 area 0! Advertises primary WAN link
subnet in the backbone area
Router(config-router)# distribute-list 10 in ! Block all Internet routing updates
Router(config-router)# exit
```

Enterprise Routing with EIGRP

Enterprise networks are learned through the primary WAN interface.

```
Router(config)# router eigrp 1 ! Enables private network EIGRP routing process
Router(config-router)# passive interface GigabitEthernet 2/0 ! Disables routing
advertisements on the LAN interface
Router(config-router)# no auto-summary ! Disable automatic route summarization
Router(config-router)# network 10.0.0.0 0.0.0.255 ! Advertises Data VLAN subnet
Router(config-router)# network 10.0.1.0 0.0.0.255 ! Advertises Voice VLAN subnet
Router(config-router)# network 10.0.2.0 0.0.0.31 ! Advertises Management VLAN subnet
Router(config-router)# network 10.0.2.64 0.0.0.15 ! Advertises DMZ VLAN subnet
Router(config-router)# network 10.0.2.80 0.0.0.3 ! Advertises Tunnel subnet
Router(config-router)# network 10.0.2.88 0.0.0.3 ! Advertises WAAS subnet
Router(config-router)# network 192.168.0.0 0.0.0.3 ! Advertises primary WAN link subnet
Router(config-router)# distribute-list 10 in ! Block all Internet routing updates
Router(config-router)# exit
```

Enterprise Routing with RIPv2

Enterprise networks are learned through the primary WAN interface.

```
Router(config)# router rip ! Enables private network RIP routing process
Router(config-router)# passive interface GigabitEthernet 2/0 ! Disables routing
advertisements on the LAN interface
```

```
Router(config-router)# no auto-summary ! Disable automatic route summarization
Router(config-router)# version 2 ! Enable RIP version 2
Router(config-router)# network 10.0.0.0 ! Advertises all branch subnets
Router(config-router)# network 192.168.0.0! Advertises primary WAN link subnet
Router(config-router)# distribute-list 10 in ! Block all Internet routing updates
Router(config-router)# exit
```

Service Provider Routing with BGP

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

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

Router(config)# router bgp 1 ! Enables public and loopback network BGP routing process
Router(config-router)# passive interface GigabitEthernet 2/0 ! Disables routing 
advertisements on the LAN interface
Router(config-router)# neighbor 209.165.201.2 remote-as 65016! Neighbor router IP for 
backup link that is in autonomous system 65016
Router(config-router)# network 209.165.201.0 mask 255.255.255.252 ! Advertises backup WAN 
link subnet
Router(config-router)# network 209.165.201.8 mask 255.255.255.252 ! Advertises Loopback 
subnet
Router(config-router)# distribute-list 20 in ! Block all routing updates except for 
Loopback network
Router(config-router)# exit
```

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

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

Active/Active Primary/Backup WAN Link with DMVPN Implementation

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

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

Enterprise Routing with OSPF

Enterprise networks are learned through the tunnel interface.

```
Router(config)# router ospf 1 ! Enables private network OSPF routing process
Router(config-router)# passive interface GigabitEthernet 2/0 ! Disables routing
advertisements on the LAN interface
Router(config-router)# router-id 10.0.0.1 ! Specifies the OSPF router ID
Router(config-router)# network 10.0.0.0 0.0.0.255 area 0 ! Advertises Data VLAN subnet in
backbone area
Router(config-router)# network 10.0.1.0 0.0.0.255 area 0 ! Advertises Voice VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.0 0.0.0.31 area 0 ! Advertises Management VLAN
subnet in backbone area
Router(config-router)# network 10.0.2.64 0.0.0.15 area 0 ! Advertises DMZ VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.80 0.0.0.3 area 0 ! Advertises Tunnel subnet in
backbone area
Router(config-router)# network 10.0.2.88 0.0.0.3 area 0 ! Advertises WAAS subnet in
backbone area
Router(config-router)# exit
```

Enterprise Routing with EIGRP

Enterprise networks are learned through the tunnel interface.

```
Router(config)# router eigrp 1 ! Enables private network EIGRP routing process
Router(config-router)# passive interface GigabitEthernet 2/0 ! Disables routing
advertisements on the LAN interface
Router(config-router)# no auto-summary ! Disable automatic route summarization
Router(config-router)# network 10.0.0.0 0.0.0.255 ! Advertises Data VLAN subnet
Router(config-router)# network 10.0.1.0 0.0.0.255 ! Advertises Voice VLAN subnet
Router(config-router)# network 10.0.2.0 0.0.0.31 ! Advertises Management VLAN subnet
Router(config-router)# network 10.0.2.64 0.0.0.15 ! Advertises DMZ VLAN subnet
Router(config-router)# network 10.0.2.80 0.0.0.3 ! Advertises Tunnel subnet
Router(config-router)# network 10.0.2.88 0.0.0.3 ! Advertises WAAS subnet
Router(config-router)# exit
```

Enterprise Routing with RIPv2

Enterprise networks are learned through the Tunnel interface.

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

Service Provider Routing with BGP

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

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

Router(config)# router bgp 1 ! Enables public and loopback network BGP routing process
Router(config-router)# passive interface GigabitEthernet 2/0 ! Disables routing
advertisements on the LAN interface
Router(config-router)# neighbor 192.168.0.2 remote-as 65015! Neighbor router IP for
primary link that is in autonomous system 65015
Router(config-router)# neighbor 209.165.201.2 remote-as 65016! Neighbor router IP for
backup link that is in autonomous system 65016
```

```
Router(config-router)# network 192.168.0.0 mask 255.255.255.252 ! Advertises primary WAN
link subnet
Router(config-router)# network 209.165.201.0 mask 255.255.255.252 ! Advertises backup WAN
link subnet
Router(config-router)# network 209.165.201.8 mask 255.255.255.252 ! Advertises Loopback
subnet
Router(config-router)# distribute-list 20 in ! Block all routing updates except for
Loopback network
Router(config-router)#exit
```

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

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

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

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

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

Enterprise Routing with OSPF

Enterprise networks are learned through the primary WAN interface.

```
Router(config)# router ospf 1 ! Enables private network OSPF routing process
Router(config-router)# passive interface GigabitEthernet 2/0 ! Disables routing
advertisements on the LAN interface
Router(config-router)# router-id 10.0.0.1 ! Specifies the OSPF router ID
Router(config-router)# network 10.0.0.0 0.0.0.255 area 0 ! Advertises Data VLAN subnet in
backbone area
Router(config-router)# network 10.0.1.0 0.0.0.255 area 0 ! Advertises Voice VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.0 0.0.0.31 area 0 ! Advertises Management VLAN
subnet in backbone area
Router(config-router)# network 10.0.2.64 0.0.0.15 area 0 ! Advertises DMZ VLAN subnet in
backbone area
Router(config-router)# network 10.0.2.80 0.0.0.3 area 0 ! Advertises Tunnel subnet in
backbone area
Router(config-router)# network 10.0.2.88 0.0.0.3 area 0 ! Advertises WAAS subnet in
backbone area
Router(config-router)# network 192.168.0.0 0.0.0.3 area 0! Advertises primary WAN link
subnet in the backbone area
Router(config-router)# distribute-list 10 in ! Block all Internet routing updates
Router(config-router)# exit
```

Enterprise Routing with EIGRP

Enterprise networks are learned through the primary WAN interface.

```
Router(config)# router eigrp 1 ! Enables private network EIGRP routing process
Router(config-router)# passive interface GigabitEthernet 2/0 ! Disables routing
advertisements on the LAN interface
Router(config-router)# no auto-summary ! Disable automatic route summarization
Router(config-router)# network 10.0.0.0 0.0.0.255 ! Advertises Data VLAN subnet
Router(config-router)# network 10.0.1.0 0.0.0.255 ! Advertises Voice VLAN subnet
Router(config-router)# network 10.0.2.0 0.0.0.31 ! Advertises Management VLAN subnet
Router(config-router)# network 10.0.2.64 0.0.0.15 ! Advertises DMZ VLAN subnet
Router(config-router)# network 10.0.2.80 0.0.0.3 ! Advertises Tunnel subnet
Router(config-router)# network 10.0.2.88 0.0.0.3 ! Advertises WAAS subnet
Router(config-router)# network 192.168.0.0 0.0.0.3 ! Advertises primary WAN link subnet
Router(config-router)# distribute-list 10 in ! Block all Internet routing updates
Router(config-router)# exit
```

Enterprise Routing with RIPv2

Enterprise networks are learned through the primary WAN interface.

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

Service Provider Routing with BGP

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

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

Router(config)# router bgp 1 ! Enables public and loopback network BGP routing process
Router(config-router)# passive interface GigabitEthernet 2/0 ! Disables routing
advertisements on the LAN interface
Router(config-router)# neighbor 209.165.201.2 remote-as 65016! Neighbor router IP for
backup link that is in autonomous system 65016
Router(config-router)# network 209.165.201.0 mask 255.255.255.252 ! Advertises backup WAN
link subnet
Router(config-router)# network 209.165.201.8 mask 255.255.255.252 ! Advertises Loopback
subnet
Router(config-router)# distribute-list 20 in ! Block all routing updates except for
Loopback network
Router(config-router)#exit
```

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

```
Router(config)# interface Multilink1 ! Enters multilink interface configuration mode
Router(config-if)# backup interface Tunnel1 ! Specifies backup interface
Router(config-if)# exit
```

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

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

Multicast Implementation

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

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

Multicast Verification

To verify your multicast configuration, enter the following command:

```
Router# show ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      S - State Refresh Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
192.168.0.1       Multilink1               00:00:16/00:01:27 v2    1 / S P
Router#
```

DHCP Implementation

Addresses were dynamically assigned for the data and voice VLAN devices. The DMZ server used static addressing.

```
Router(config)# ip dhcp excluded-address 10.0.1.1 10.0.1.10 ! Specifies the addresses to
be excluded from DHCP
Router(config)# ip dhcp excluded-address 10.0.1.245 10.0.1.254 ! Specifies the addresses
to be excluded from DHCP
Router(config)# ip dhcp pool IP-PHONES ! Specifies DHCP pool for IP Phones
Router(dhcp-config)# network 10.0.1.0 255.255.255.0 ! Specifies the DHCP address range
Router(dhcp-config)# default-router 10.0.1.3 ! Specifies the default HSRP gateway
Router(dhcp-config)# option 150 ip 10.0.0.2 ! Specifies the default TFTP server
Router(dhcp-config)# lease 30 ! Sets the lease expiration to 1 month
Router(dhcp-config)# exit
Router(config)# ip dhcp excluded-address 10.0.0.1 10.0.0.30! Specifies the addresses to be
excluded from DHCP
Router(config)# ip dhcp excluded-address 10.0.0.245 10.0.0.254! Specifies the addresses to
be excluded from DHCP
Router(config)# ip dhcp pool PCS ! Specifies the DHCP pool for PCs
Router(dhcp-config)# network 10.0.0.0 255.255.255.0 ! Specifies the DHCP address range
Router(dhcp-config)# default-router 10.0.0.3 ! Specifies the default HSRP gateway
Router(dhcp-config)# exit
Router(config)# service dhcp ! Starts the DHCP server
```

DHCP Verification

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

```
Router# show ip dhcp binding
Bindings from all pools not associated with VRF:
```

```
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.0.1.26       0100.1e4a.a8e5.e1       Infinite                Automatic
10.0.1.29       0100.5060.0387.20       Infinite                Automatic
Router#
```

NAT Implementation

```
Router(config)# ip access-list standard NAT-BRANCH ! Defines extended ACL for translation
Router(config-ext-nacl)# permit 10.0.0.0 0.0.0.255
Router(config-ext-nacl)# exit
Router(config)# ip nat translation tcp-timeout 300 ! Specifies timeout value for TCP ports
Router(config)# ip nat inside source list NAT-BRANCH interface ATM0/2/IMA0.1 overload !
Enables NAT for traffic that matches the ACL (Inside local) and translates the source
address to specified interface address (Inside global) on the backup interface
Router(config)# interface GigabitEthernet2/0.1 ! Enters gigabit Ethernet configuration
mode
Router(config-subif)# ip nat inside ! Specifies the interface as connected to inside
network
Router(config-subif)# exit
Router(config)# interface ATM0/2/IMA0.1 ! Enters backup interface configuration mode
Router(config-if)# ip nat outside ! Specifies the interface as connected to outside
network
Router(config-if)# exit
```

NAT Verification

To verify your NAT configuration, enter the following command:

```
Router# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 22

10.0.0.15: 2140     10.0.0.15: 2140    201.165.201.1:2000    201.165.201.1:2000
Router#
```

Quality of Service Implementation

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

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

```
Router(config)# ip access-list extended ACL-FTP ! Defines extended ACL to identify traffic
from a local FTP server
Router(config-ext-nacl)# permit ip host 10.0.0.4 any
Router(config-ext-nacl)#exit
!Defines two extended access lists (101 and 102) to classify PCs running enterprise
applications
Router(config)# access-list 101 permit ip host 10.0.0.5 host 172.16.0.30
Router(config)# access-list 101 permit ip host 10.0.0.6 host 172.16.0.30
Router(config)# access-list 102 permit ip host 10.0.0.7 any
Router(config)# access-list 102 permit ip host 10.0.0.8 any
Router(config)# access-list 102 permit ip host 10.0.0.9 any
Router(config)# access-list 102 permit ip host 10.0.0.10 any
Router(config)# ip nbar port-map custom-02 udp 1434 ! Customizes NBAR protocol to match
UDP port 1434 used by the SQL Slammer and Sapphire worms
Router(config)# ip nbar port-map custom-03 tcp 5554 9996 ! Customizes NBAR protocol to
match TCP ports 5554 and 9996 used by the Sasser worm
Router(config)# ip nbar port-map custom-04 tcp 445 ! Customize NBAR protocol to match TCP
port 445 used by Microsoft SMB protocol for file sharing
Router(config)# class-map match-all SQL-SLAMMER ! Defines Class map for Sql-Slammer
traffic
Router(config-cmap)# match protocol custom-02 ! Matches traffic with port number in
custom-02
Router(config-cmap)# match packet length min 404 max 404 ! Matches traffic with packet
length 404 bytes
Router(config-cmap)# exit
Router(config)# class-map match-any WORMS ! Defines class map for unwanted traffic
Router(config-cmap)# match protocol http url "*.ida*" ! Matches HTTP traffic with the
specific string in the URL
Router(config-cmap)# match protocol http url "*cmd.exe*" ! Matches HTTP traffic with the
specific string in the URL
Router(config-cmap)# match protocol http url "*root.exe*" ! Matches HTTP traffic with the
specific string in the URL
Router(config-cmap)# match protocol http url "*readme.eml*" ! Matches HTTP traffic with
the specific string in the URL
Router(config-cmap)# match class-map SQL-SLAMMER ! Matches SQL-Slammer worm signature
Router(config-cmap)# match protocol custom-03 ! Matches Sasser worm signature
Router(config-cmap)# exit
Router(config)# class-map match-any VOICE ! Defines class map for Voice traffic
Router(config-cmap)# match ip dscp ef ! Matches traffic with DSCP set to EF
Router(config-cmap)# exit
Router(config)# class-map match-all INTERACTIVE-VIDEO ! Defines class map for interactive
video traffic
Router(config-cmap)# match ip dscp af41 af42 ! Matches traffic with DSCP set to AF41 or
AF42
Router(config-cmap)# exit
Router(config)# class-map match-all SCAVENGER ! Defines class map for Scavenger traffic
Router(config-cmap)# match ip dscp cs1 ! Matches traffic with DSCP set to cs1
Router(config-cmap)# exit
Router(config)# class-map match-any MISSION-CRITICAL ! Defines classmap for mission
critical traffic
Router(config-cmap)# match ip dscp cs3 ! Matches traffic with DSCP set to CS3
Router(config-cmap)# match ip dscp af31 ! Matches traffic with DSCP set to AF31
Router(config-cmap)# match access-group 101 ! Matches ip traffic in ACL 101
Router(config-cmap)# match ip dscp 25 ! Matches traffic with DSCP set to 25
Router(config-cmap)# match protocol http ! Matches HTTP traffic
Router(config-cmap)# exit
Router(config)# class-map match-any INTERNETWORK-CONTROL ! Defines class map for routing
control traffic
Router(config-cmap)# match ip dscp cs6 ! Matches traffic with DSCP set to CS6
Router(config-cmap)# exit
Router(config)# class-map match-any TRANSACTIONAL-DATA ! Defines class map for
transactional data traffic
Router(config-cmap)# match ip dscp af21 af22 ! Matches traffic with DSCP set to AF21 or
AF22
Router(config-cmap)# match access-group 102 ! Matches ip traffic in ACL
Router(config-cmap)# match protocol custom-04 ! Matches traffic with port number mentioned
in custom-04
Router(config-cmap)# exit
Router(config)# class-map match-any BULK-DATA ! Defines Class map for bulk traffic
Router(config-cmap)# match ip dscp af11 af12 ! Matches traffic with DSCP set to AF11 or
AF12
```

```
Router(config-cmap)# match protocol ftp ! Matches FTP traffic
Router(config-cmap)# match access-group name ACL-FTP ! Matches ip traffic in ACL-FTP ACL
Router(config-cmap)# exit

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

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

```
Router(config)# policy-map EIGHT-CLASS-V3PN-EDGE-SHAPE ! Defines parent policy map for
Primary interface
Router(config-pmap)# class class-default ! Matches all traffic
Router(config-pmap-c)# shape average 6912000 ! Outgoing traffic was shaped at a rate of
6.9 Mbps
Router(config-pmap-c)# service-policy EIGHT-CLASS-V3PN-EDGE ! Attaches traffic policy to
shaping queue.
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map EIGHT-CLASS-V3PN-EDGE-BACKUP ! Defines parent policy map for
Backup interface
Router(config-pmap)# class class-default ! Matches all traffic
Router(config-pmap-c)# shape average 4608000 ! Outgoing traffic was shaped at a rate of
4.6 Mbps
Router(config-pmap-c)# service-policy EIGHT-CLASS-V3PN-EDGE ! Attaches traffic policy to
shaping queue.
Router(config-pmap-c)# exit
Router(config)# map-class frame-relay FR-SHAPING ! Defines a map-class for Frame Relay
traffic shaping
```

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

Quality of Service Verification

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

```
Router# show policy-map interface
 GigabitEthernet2/0.1

  Service-policy input: INPUT-POLICY

    Class-map: WORMS (match-any)
      9 packets, 594 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: protocol http url "*.ida*"
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol http url "*cmd.exe*"
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol http url "*root.exe*"
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol http url "*readme.eml*"
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: class-map match-all SQL-SLAMMER
        0 packets, 0 bytes
        30 second rate 0 bps
        Match: protocol custom-02
        Match: packet length min 404 max 404
      Match: protocol custom-03
        9 packets, 594 bytes
        30 second rate 0 bps
      drop

    Class-map: class-default (match-any)
      103593411 packets, 6980776240 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      QoS Set
        dscp cos
          Packets marked 103593416
 GigabitEthernet2/0.2

  Service-policy input: INPUT-POLICY
```

```
   Class-map: WORMS (match-any)
     0 packets, 0 bytes
     30 second offered rate 0 bps, drop rate 0 bps
     Match: protocol http url "*.ida*"
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol http url "*cmd.exe*"
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol http url "*root.exe*"
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol http url "*readme.eml*"
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: class-map match-all SQL-SLAMMER
       0 packets, 0 bytes
       30 second rate 0 bps
       Match: protocol custom-02
       Match: packet length min 404 max 404
     Match: protocol custom-03
       0 packets, 0 bytes
       30 second rate 0 bps
     drop

   Class-map: class-default (match-any)
     3350613 packets, 212885188 bytes
     30 second offered rate 0 bps, drop rate 0 bps
     Match: any
     QoS Set
       dscp cos
         Packets marked 3350613
GigabitEthernet2/0.3

 Service-policy input: INPUT-POLICY

   Class-map: WORMS (match-any)
     0 packets, 0 bytes
     30 second offered rate 0 bps, drop rate 0 bps
     Match: protocol http url "*.ida*"
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol http url "*cmd.exe*"
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol http url "*root.exe*"
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol http url "*readme.eml*"
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: class-map match-all SQL-SLAMMER
       0 packets, 0 bytes
       30 second rate 0 bps
       Match: protocol custom-02
       Match: packet length min 404 max 404
     Match: protocol custom-03
       0 packets, 0 bytes
       30 second rate 0 bps
     drop

   Class-map: class-default (match-any)
     3266743 packets, 201900728 bytes
     30 second offered rate 0 bps, drop rate 0 bps
     Match: any
     QoS Set
       dscp cos
         Packets marked 3266743
GigabitEthernet0/0/0

 Service-policy output: EIGHT-CLASS-V3PN-EDGE-SHAPE

   Class-map: class-default (match-any)
     86921887 packets, 11420188514 bytes
     30 second offered rate 1000 bps, drop rate 0 bps
     Match: any
     Traffic Shaping
          Target/Average   Byte   Sustain   Excess    Interval  Increment
            Rate           Limit  bits/int  bits/int  (ms)      (bytes)
         6912000/6912000   43200  172800    172800    25        21600

       Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
       Active Depth                         Delayed   Delayed   Active
       -      0         85141012  2709383642 0         0         no

     Service-policy : EIGHT-CLASS-V3PN-EDGE

       Class-map: VOICE (match-any)
         1781 packets, 206488 bytes
         30 second offered rate 0 bps, drop rate 0 bps
         Match: ip dscp ef (46)
           0 packets, 0 bytes
           30 second rate 0 bps
         Queueing
           Strict Priority
           Output Queue: Conversation 136
           Bandwidth 14 ( %)
           Bandwidth 967 (kbps) Burst 24175 (Bytes)
           (pkts matched/bytes matched) 0/0
           (total drops/bytes drops) 0/0

       Class-map: INTERACTIVE-VIDEO (match-all)
         0 packets, 0 bytes
         30 second offered rate 0 bps, drop rate 0 bps
         Match: ip dscp af41 (34) af42 (36)
         Queueing
           Strict Priority
           Output Queue: Conversation 136
           Bandwidth 6 ( %)
           Bandwidth 414 (kbps) Burst 10350 (Bytes)
           (pkts matched/bytes matched) 0/0
           (total drops/bytes drops) 0/0

       Class-map: MISSION-CRITICAL (match-any)
         1181375 packets, 148873894 bytes
         30 second offered rate 0 bps, drop rate 0 bps
         Match: ip dscp cs3 (24)
           1181375 packets, 148873894 bytes
           30 second rate 0 bps
         Match: ip dscp af31 (26)
           0 packets, 0 bytes
           30 second rate 0 bps
         Match: access-group 101
           0 packets, 0 bytes
           30 second rate 0 bps
         Match: ip dscp 25
           0 packets, 0 bytes
           30 second rate 0 bps
```

```
        Match: protocol http
          0 packets, 0 bytes
          30 second rate 0 bps
        Queueing
          Output Queue: Conversation 137
          Bandwidth 25 ( %)
          Bandwidth 1728 (kbps)
          (pkts matched/bytes matched) 0/0
      (depth/total drops/no-buffer drops) 0/0/0
           exponential weight: 9
           mean queue depth: 0

class    Transmitted       Random drop      Tail drop    Minimum Maximum  Mark
         pkts/bytes        pkts/bytes       pkts/bytes    thresh  thresh  prob
    0       0/0               0/0              0/0           20      40  1/10
    1       0/0               0/0              0/0           22      40  1/10
    2       0/0               0/0              0/0           24      40  1/10
    3 1181305/148866418       0/0              0/0           26      40  1/10
    4       0/0               0/0              0/0           28      40  1/10
    5       0/0               0/0              0/0           30      40  1/10
    6       0/0               0/0              0/0           32      40  1/10
    7       0/0               0/0              0/0           34      40  1/10
 rsvp       0/0               0/0              0/0           36      40  1/10


      Class-map: INTERNETWORK-CONTROL (match-any)
        1245619 packets, 176240010 bytes
        30 second offered rate 0 bps, drop rate 0 bps
        Match: ip dscp cs6 (48)
          1245619 packets, 176240010 bytes
          30 second rate 0 bps
        Queueing
          Output Queue: Conversation 138
          Bandwidth 3 ( %)
          Bandwidth 207 (kbps)Max Threshold 64 (packets)
          (pkts matched/bytes matched) 0/0
      (depth/total drops/no-buffer drops) 0/0/0

      Class-map: TRANSACTIONAL-DATA (match-any)
        8833287 packets, 1254893912 bytes
        30 second offered rate 1000 bps, drop rate 0 bps
        Match: ip dscp af21 (18) af22 (20)
          8833286 packets, 1254893912 bytes
          30 second rate 1000 bps
        Match: access-group 102
          0 packets, 0 bytes
          30 second rate 0 bps
        Match: protocol custom-04
          0 packets, 0 bytes
          30 second rate 0 bps
        Queueing
          Output Queue: Conversation 139
          Bandwidth 18 ( %)
          Bandwidth 1244 (kbps)
          (pkts matched/bytes matched) 0/0
      (depth/total drops/no-buffer drops) 0/0/0
           exponential weight: 9
           mean queue depth: 0

class    Transmitted       Random drop      Tail drop    Minimum Maximum  Mark
         pkts/bytes        pkts/bytes       pkts/bytes    thresh  thresh  prob
    0       0/0               0/0              0/0           20      40  1/10
    1       0/0               0/0              0/0           22      40  1/10
    2 8833254/1254889504      0/0              0/0           24      40  1/10
```

```
     3       0/0                0/0              0/0           26      40  1/10
     4       0/0                0/0              0/0           28      40  1/10
     5       0/0                0/0              0/0           30      40  1/10
     6       0/0                0/0              0/0           32      40  1/10
     7       0/0                0/0              0/0           34      40  1/10
  rsvp       0/0                0/0              0/0           36      40  1/10


       Class-map: BULK-DATA (match-any)
         0 packets, 0 bytes
         30 second offered rate 0 bps, drop rate 0 bps
         Match: ip dscp af11 (10) af12 (12)
           0 packets, 0 bytes
           30 second rate 0 bps
         Match: protocol ftp
           0 packets, 0 bytes
           30 second rate 0 bps
         Match: access-group name aclftp
           0 packets, 0 bytes
           30 second rate 0 bps
         Queueing
           Output Queue: Conversation 140
           Bandwidth 5 ( %)
           Bandwidth 345 (kbps)Max Threshold 64 (packets)
           (pkts matched/bytes matched) 0/0
       (depth/total drops/no-buffer drops) 0/0/0

       Class-map: SCAVENGER (match-all)
         0 packets, 0 bytes
         30 second offered rate 0 bps, drop rate 0 bps
         Match: ip dscp cs1 (8)
         Queueing
           Output Queue: Conversation 141
           Bandwidth 2 ( %)
           Bandwidth 138 (kbps)Max Threshold 64 (packets)
           (pkts matched/bytes matched) 0/0
       (depth/total drops/no-buffer drops) 0/0/0

       Class-map: class-default (match-any)
         75659826 packets, 9839974210 bytes
         30 second offered rate 0 bps, drop rate 0 bps
         Match: any
         Queueing
           Output Queue: Conversation 142
           Bandwidth 25 ( %)
           Bandwidth 1728 (kbps)
           (pkts matched/bytes matched) 0/0
       (depth/total drops/no-buffer drops) 0/0/0
            exponential weight: 9
            mean queue depth: 0

 class    Transmitted      Random drop      Tail drop    Minimum Maximum  Mark
          pkts/bytes       pkts/bytes       pkts/bytes    thresh  thresh  prob
     0 73879122/9719111088      0/0              0/0           20      40  1/10
     1       0/0                0/0              0/0           22      40  1/10
     2      18/14796            0/0              0/0           24      40  1/10
     3       0/0                0/0              0/0           26      40  1/10
     4       0/0                0/0              0/0           28      40  1/10
     5       0/0                0/0              0/0           30      40  1/10
     6       0/0                0/0              0/0           32      40  1/10
     7       0/0                0/0              0/0           34      40  1/10
  rsvp       0/0                0/0              0/0           36      40  1/10

Virtual-Template10
```

```
    Service-policy output: EIGHT-CLASS-V3PN-EDGE-BACKUP

      Service policy content is displayed for cloned interfaces only such as vaccess and
sessions
```

Security Services Implementation

- Infrastructure Protection Implementation, page 44
- Access Control Implementation, page 51
- Secure Connectivity Implementation, page 52
- Threat Defense Detection and Mitigation Implementation, page 59

Infrastructure Protection Implementation

- Securing Unused Ports, page 44
- Turning Off Unused Services, page 44
- Routing Protocol Security, page 50
- Additional Services Measures, page 51

Securing Unused Ports

The following is an example of securing an unused port. The example applies both to the access switch and the distribution layer switch.

```
Switch(config)# interface g1/0/4 ! Enters configuration mode for the specified port
Switch(config-if)# switchport mode access ! Assign the port to access mode
Switch(config-if)# switchport access vlan 333 ! Assign the unused port to Black Hole VLAN
Switch(config-if)# exit
```

Turning Off Unused Services

To improve the overall security of the network, the Cisco IOS devices must be secured from infrastructure attack. As a security best practice, disable any unused services because these unused services are only rarely used for legitimate purposes and can be used to launch a denial of service (DoS) attack. The following example disables the unused services.

```
Router(config)# no service pad ! Disable PAD service
Router(config)# no service udp-small-servers ! Disable UDP small server
Router(config)# no service tcp-small-servers ! Disable TCP small server
Router(config)# no ip bootp server ! Disable BOOTP server
Router(confif)# no cdp run ! Disable Cisco Discover Protocol service
Router(config)# no ip source-route ! Disable source routing
Router(config)# no ip classless ! Disable forwarding of packets for unrecognized subnets
Router(config)# no ip http server ! Disable HTTP server
Router(config)# no ip http secure-server ! Disable HTTPS server
Router(config)# no ip domain-lookup ! Disable DNS server
Router(config) # interface Multilink1 ! Enters interface configuration mode
Router(config-if)# no cdp enable ! Disable Cisco discovery protocol on the interface
Router(config-if)# no ip redirects ! Disable ICMP redirect message
Router(config-if)# no ip proxy-arp ! Disable Proxy ARP
Router(config-if)# no ip unreachables ! Disable ICMP unreachable error message
Router(config-if)# no ip directed-broadcast! Disable directed broadcasts
Router(config-if)# no ip mask-reply! Disable ICMP mask reply messages
```

The unused services can also be disabled by running Cisco AutoSecure.

```
Router# auto secure
                --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: 3
Controller Timeslots D-Channel Configurable modes Status
T1 0/0/0   24        23        pri/channelized    Administratively up
T1 0/0/1   24        23        pri/channelized    Administratively up Administratively up

Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/1         unassigned      YES NVRAM  up                    up
GigabitEthernet2/0.1       10.0.0.1        YES NVRAM  up                    up
GigabitEthernet2/0.2       10.0.1.1        YES NVRAM  up                    up
GigabitEthernet2/0.3       10.0.2.65       YES NVRAM  up                    up
GigabitEthernet2/0.4       10.0.2.1        YES NVRAM  up                    up
Serial0/0/0:0              unassigned      YES unset  down                  down
Serial0/0/0:1              unassigned      YES unset  down                  down
Serial0/0/0:2              unassigned      YES unset  down                  down
Serial0/0/0:3              unassigned      YES unset  down                  down
Serial0/0/0:4              unassigned      YES unset  down                  down
Serial0/0/0:5              unassigned      YES unset  down                  down
Serial0/0/0:6              unassigned      YES unset  down                  down
Serial0/0/0:7              unassigned      YES unset  down                  down
Serial0/0/0:8              unassigned      YES unset  down                  down
Serial0/0/0:9              unassigned      YES unset  down                  down
Serial0/0/0:10             unassigned      YES unset  down                  down
Serial0/0/0:11             unassigned      YES unset  down                  down
Serial0/0/0:12             unassigned      YES unset  down                  down
Serial0/0/0:13             unassigned      YES unset  down                  down
Serial0/0/0:14             unassigned      YES unset  down                  down
Serial0/0/0:15             unassigned      YES unset  down                  down
Serial0/0/0:16             unassigned      YES unset  down                  down
Serial0/0/0:17             unassigned      YES unset  down                  down
Serial0/0/0:18             unassigned      YES unset  down                  down
Serial0/0/0:19             unassigned      YES unset  down                  down
Serial0/0/0:20             unassigned      YES unset  down                  down
Serial0/0/0:21             unassigned      YES unset  down                  down
Serial0/0/0:22             unassigned      YES unset  down                  down
Serial0/0/0:23             unassigned      YES NVRAM  up                    up
Serial0/1/0                unassigned      YES NVRAM  up                    up
```

```
Serial0/1/1                unassigned      YES NVRAM  up                    up
Serial0/1/2                unassigned      YES NVRAM  up                    up
Serial0/1/3                unassigned      YES NVRAM  up                    up
ATM0/2/IMA0                unassigned      YES NVRAM  standby mode          down
ATM0/2/IMA0.1              209.165.201.1   YES NVRAM  standby mode          down
In1/0                      10.0.2.85       YES NVRAM  up                    up
Integrated-Service-Engine1/0 10.0.2.89     YES NVRAM  administratively down down
Multilink1                 192.168.0.1     YES NVRAM  up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Virtual-Access2            unassigned      YES unset  down                  down
Virtual-Template10         209.165.201.1   YES TFTP   down                  down
Loopback0                  209.165.201.9   YES NVRAM  up                    up
Tunnel1                    10.0.2.81       YES NVRAM  up                    up
Enter the interface name that is facing the internet: Multilink1
Enter the interface name that is facing the internet: ATM0/2/IMA0.1
Enter the interface name that is facing the internet: Loopback0
Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Is SNMP used to manage the router? [yes/no]: no
Disabling SNMP

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
  This system is the property of So-&-So-Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.

Enter the security banner {Put the banner between
k and k, where k is any character}:
k Unauthorised access to this device is prohibited k
Enable secret is either not configured or
 is the same as enable password
Enter the new enable secret:
Confirm the enable secret :
Enter the new enable password:
Confirm the enable password:
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
```

```
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 5

Maximum Login failures with the device: 5

Maximum time period for crossing the failed login attempts: 5

Configure SSH server? [yes]: yes
Enter hostname: Branch
Enter the domain-name: example.com

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected
to internet

Configure CBAC Firewall feature? [yes/no]: no
Tcp intercept feature is used prevent tcp syn attack
on the servers in the network. Create autosec_tcp_intercept_list
to form the list of servers to which the tcp traffic is to
be observed


Enable tcp intercept feature? [yes/no]: no

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
no snmp-server
banner motd ^C Unauthorised access to this device is prohibited ^C
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$2gLN$RpNwkFyfJdCjXkMDxY3PI1
enable password 7 011F07065802150C2E
aaa new-model
aaa authentication login local_auth local
line con 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
line tty 1
 login authentication local_auth
 exec-timeout 15 0
line tty 66
 login authentication local_auth
 exec-timeout 15 0
line tty 130
 login authentication local_auth
 exec-timeout 15 0
login block-for 5 attempts 5 within 5
ip domain-name example.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface GigabitEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface GigabitEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface GigabitEthernet2/0.1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface GigabitEthernet2/0.2
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface GigabitEthernet2/0.3
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/1/2
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/1/3
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/0/0:23
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface ATM0/2/IMA0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface ATM0/2/IMA0.1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Integrated-Service-Engine1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
```

```
interface Integrated-Service-Engine2/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
ip cef
access-list 100 permit udp any any eq bootpc
interface ATM0/3/IMA0.1
 ip verify unicast source reachable-via rx allow-default 100
!
end


Apply this configuration to running-config? [yes]: yes

Applying the config generated to running-config
The name for the keys will be: Router.example.com

 percent The key modulus size is 1024 bits
 percent Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Router#
092165: Sep 23 03:03:32.096 PDT:  percentAUTOSEC-1-MODIFIED: AutoSecure configuration has
been Modified on this device
Router#
```

Routing Protocol Security

Apply an authentication mechanism to all the WAN interfaces.

OSPF

```
Router(config)# interface Tunnel 1 ! Enters tunnel interface configuration mode
Router(config-line)# ip ospf authentication message-digest ! Enables MD5 routing protocol
authentication
Router(config-line)# ip ospf message-digest-key 100 md5 c1$k0Sys ! Sets key and password
for MD5
Router(config)# exit
Router(config)# interface Multilink1 ! Enters serial interface configuration mode
Router(config-line)# ip ospf authentication message-digest ! Enables MD5 routing protocol
authentication
Router(config-line)# ip ospf message-digest-key 100 md5 c1$k0Sys ! Sets key and password
for MD5
Router(config)# exit
```

EIGRP

```
Router(config)# key chain EIGRP-KEY ! Creates chain of keys
Router(config-keychain)# key 1 ! Creates a key
Router(config-keychain-key)# key-string c1$k0SyS ! Sets the key value
Router(config-keychain-key)# exit
Router(config-keychain)# exit

Router(config)# interface Tunnel 1 ! Enters tunnel interface configuration mode
Router(config-line)# ip authentication mode eigrp 100 md5 ! Enables MD5 routing protocol
authentication
```

```
Router(config-line)# ip authentication key-chain eigrp 100 EIGRP-KEY ! Sets key and
password for MD5
Router(config)# exit
Router(config)# interface Multilink1 ! Enters serial interface configuration mode
Router(config-line)# ip authentication mode eigrp 100 md5 ! Enables MD5 routing protocol
authentication
Router(config-line)# ip authentication key-chain eigrp 100 EIGRP-KEY ! Sets key and
password for MD5
Router(config)# exit
```

RIPv2

```
Router(config)# key chain RIP-KEY ! Creates chain of keys
Router(config-keychain)# key 1 ! Creates a key
Router(config-keychain-key)# key-string c1$k0SyS ! Sets the key value
Router(config-keychain-key)# exit
Router(config-keychain)# exit

Router(config)# interface Tunnel 1 ! Enters tunnel interface configuration mode
Router(config-line)# ip rip authentication mode md5 ! Enables MD5 routing protocol
authentication
Router(config-line)# ip rip authentication key-chain RIP-KEY ! Sets key and password for
MD5
Router(config)# exit
Router(config)# interface Multilink1 ! Enters serial interface configuration mode
Router(config-line)# ip rip authentication mode md5 ! Enables MD5 routing protocol
authentication
Router(config-line)# ip rip authentication key-chain RIP-KEY ! Sets key and password for
MD5
Router(config)# exit
```

Additional Services Measures

```
Router(config)# line vty 0 4 ! Specifies VTY line specific parameters
Router(config-line)# transport input ssh ! Allows only SSH connection
Router(config)# exit
Router(config)# ip http secure-server ! Enables HTTPS service
Router(config)# ip http authentication aaa login-authentication default ! Specifies to use
AAA database for HTTP login
```

Verification of Additional Services Measures

To verify your additional services configuration, enter the following command.

```
Router# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

Access Control Implementation

Authentication, Authorization, and Accounting (AAA) is an architectural framework for consistently configuring a set of independent security functions. It provides a modular way of performing authentication, authorization, and accounting using a protocol such as RADIUS or TACACS.

In the branch architecture, AAA is the primary method for access control, using RADIUS as the protocol for communication between network devices and the AAA server.

```
Router(config)# aaa new-model ! Enables Authentication, Authorization and Accounting
services
Router(config)# aaa group server radius AAA-BRANCH ! Specifies the RADIUS server group
Router(config-sg-radius)# server 172.16.0.80 auth-port 1645 acct-port 1646 ! Specifies the
RADIUS server ip address
Router(config-sg-radius)# aaa authentication login default group radius local ! Specifies
default login authentication to use RADIUS server database
Router(config-sg-radius)# aaa authentication login VPN-AUTH-LIST group radius local !
Specifies SSL VPN login authentication to use RADIUS server database
Router(config)# aaa session-id common ! Specifies the use of the same session identifier
for all invocations of accounting services
Router(config)# radius-server key BRANCH-KEY ! Specifies RADIUS server key
```

Password Management

```
Router(config)# security passwords min-length 8 ! Sets minimum length of passwords to 8
characters
Router(config)# service password-encryption ! Enables Cisco IOS to encrypt all password in
configuration file
Router(config)# enable password level 7 C1$k0SyS ! Enables configuration password with
privilege level 7
Router(config)# enable secret level 5 C1$k0SyS ! Enables configuration password stored
with MD5 encryption with privilege level 5
Router(config)# security authentication failure rate 10 log ! Allows up to 10 unsuccessful
login attempts with a syslog entry for attempts that exceed the threshold
Router(config)# username admin password C1$k0SyS ! Sets login password


Switch-Dist(config)# service password-encryption ! Enables Cisco IOS to encrypt all
password in configuration file
Switch-Dist(config)# enable secret level 5 C1$k0SyS ! Enables configuration password
stored with MD5 encryption with privilege level 5

Switch-Access(config)# service password-encryption ! Enables Cisco IOS to encrypt all
password in configuration file
Switch-Access(config)# enable secret level 5 C1$k0SyS ! Enables configuration password
stored with MD5 encryption with privilege level 5
```

Secure Connectivity Implementation

Group Encrypted Transport Virtual Private Networks (GETVPN) eliminates the need for tunnels across the WAN. By removing the need for point-to-point tunnels, meshed networks can scale better while maintaining network-intelligence features that are critical to voice and video quality, such as QoS, routing, and multicast. GETVPN offers a new standards-based IPsec security model that is based on the concept of "trusted" group members. Trusted member routers use a common security methodology that is independent of any point-to-point IPsec tunnel relationship.

GET-based networks can be used in a variety of WAN environments, including IP and Multiprotocol Label Switching (MPLS). MPLS VPNs that use this encryption technology are highly scalable, manageable, and cost-effective, and they meet government-mandated encryption requirements. The flexible nature of GET allows security-conscious enterprises either to manage their own network security over a service provider WAN service or to offload encryption services to their providers. GET simplifies securing large Layer 2 or MPLS networks that require partial or full-mesh connectivity.

In the Services Ready Medium Branch Foundation, GETVPN encryption was used on the primary WAN link.

```
Router(config)# crypto isakmp policy  1 ! Identifies the policy to create and enters
isakmp configuration mode
Router(config-isakmp)# encryption 3des ! Specifies the 3-DES encryption algorithm
Router(config-isakmp)# authentication pre-share ! Specifies authentication with preshared
keys
Router(config-isakmp)# hash md5 ! Specifies hash algorithm as MD5
Router(config-isakmp)# group 2 ! Specifies the 1024-bit Diffie-Hellman group
Router(config-isakmp)# lifetime 28800 ! Specifies the lifetime of IKE security association
Router(config-isakmp)# crypto isakmp key VPN-KEY address 209.165.201.10! Specifies static
key for the ISAKMP negotiation with peer device using remote peer Loopback address
Router(config)# crypto isakmp keepalive 30 ! Enables keepalives between peers with
specified interval
Router(config)# crypto gdoi group GET-GROUP ! Enters GDOI group configuration mode.
Router(config-gdoi-group)# identity number 1357924680 ! Sets GDOI group number
Router(config-gdoi-group)# server address ipv4 209.165.201.10! Specifies GDOI key server
address
Router(config-gdoi-group)# crypto map VPN-MAP local-address Loopback0 ! Specifies the
interface to be used by the crypto map for the IPSEC traffic
Router(config)# crypto map VPN-MAP 1 gdoi  ! Enters crypto map configuration mode and
creates or modifies a crypto map entry.
Router(config-crypto-map)# set group GET-GROUP ! Associates the GDOI group to the crypto
map.
Router(config-crypto-map)# qos pre-classify ! Enables QoS on VPN tunnel interface
Router(config-crypto-map)# exit
```

Apply the *VPN-MAP* on all WAN interfaces and subinterfaces.

```
Router(config-fr-dlci)# crypto map VPN-MAP

or

Router(config-if)# crypto map VPN-MAP
```

GETVPN Key Server

The key server was configured at the central location.

```
KEY-SERVER(config)# crypto isakmp policy 1 ! Defines an IKE policy
KEY-SERVER(config-isakmp)# encryption 3des ! Specifies 3-DES encryption algorithm
KEY-SERVER(config-isakmp)# authentication pre-share ! Specifies authentication with
preshared keys
KEY-SERVER(config-isakmp)# group 2 ! Specifies the 1024-bit Diffie-Hellman group
KEY-SERVER(config-isakmp)# lifetime 28800 ! Specifies the lifetime of IKE security
association
KEY-SERVER(config)# crypto ipsec transform-set GET-GROUP esp-aes 256 esp-sha-hmac
! Defines a IPSec transform set with ESP encapsulation and AES 256 bit encryption
KEY-SERVER(cfg-crypto-trans)# crypto ipsec profile GET-VPN ! Defines a profile and enters
IPSEC configuration mode
KEY-SERVER(ipsec-profile)# set security-association lifetime seconds 86400 ! Specifies
security association lifetime
KEY-SERVER(ipsec-profile)# set transform-set GET-GROUP ! Specifies which transform sets
can be used with the crypto map entry.
KEY-SERVER(ipsec-profile)# crypto gdoi group GET-GROUP ! Identifies a GDOI group and
enters GDOI group configuration mode
KEY-SERVER(config-gdoi-group)# identity number 1357924680 ! Sets GDOI group number
```

```
KEY-SERVER(config-gdoi-group)# server local ! Specified GDOI key server as local and
enters its configuration
KEY-SERVER(gdoi-local-server)# rekey address ipv4 REKEY-ADDRESS ! Defines destination
information for rekey messages as defined in the REKEY-ADDRESS ACL
KEY-SERVER(gdoi-local-server)# rekey lifetime seconds 300 ! Limits the number of seconds
that any one encryption key should be used
KEY-SERVER(gdoi-local-server)# rekey retransmit 10 number 2 ! Specifies the number of
times the rekey message is retransmitted
KEY-SERVER(gdoi-local-server)# rekey authentication mypubkey rsa REKEY-RSA ! Specifies the
keys to be used for a rekey to GDOI group members
KEY-SERVER(gdoi-local-server)# sa ipsec 1 ! Specifies the IPsec SA policy information to
be used for a GDOI group and enters GDOI SA IPsec configuration mode
KEY-SERVER(gdoi-sa-ipsec)# profile GET-VPN ! Defines the IPsec SA policy for a GDOI group
KEY-SERVER (gdoi-sa-ipsec)# match address ipv4 SA-ACL ! Specifies an IP extended access
list for a GDOI registration.
KEY-SERVER (gdoi-sa-ipsec)# replay counter window-size 64 ! Specifies the window-size for
the replay counter
KEY-SERVER (config)# ip access-list extended REKEY-ADDRESS ! Defines an extended
access-list and enters acl mode
KEY-SERVER (config-ext-nacl)# permit udp host host 209.165.201.10 eq 848 host 239.1.100.1
eq 248 ! Permits packets from a specific address to register with the Key-Server at its
multicast address
KEY-SERVER (config)# ip access-list extended SA-ACL ! Defines an extended access-list and
enters acl mode
KEY-SERVER(config-ext-nacl)# permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.255.255
! Permits traffic from branch subnets to central site subnets and vice versa
KEY-SERVER(config-ext-nacl)# permit ip 10.0.1.0 0.0.0.255 172.16.0.0 0.0.255.255
KEY-SERVER(config-ext-nacl)# permit ip 10.0.2.0 0.0.0.31 172.16.0.0 0.0.255.255
KEY-SERVER(config-ext-nacl)# permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255
KEY-SERVER(config-ext-nacl)# permit ip 172.16.0.0 0.0.255.255 10.0.1.0 0.0.0.255
KEY-SERVER(config-ext-nacl)# permit ip 172.16.0.0 0.0.255.255 10.0.2.0 0.0.0.31
```

DMVPN Implementation

Dynamic Multipoint Virtual Private Network (DMVPN) is useful for building scalable IPsec VPNs. DMVPN uses a centralized architecture to provide easier implementation and management for deployment that requires granular access control for diverse users including teleworkers and mobile workers.

Cisco DMVPN allows branch locations to communicate directly with each other over the public WAN or Internet, such as when using Voice over IP (VoIP) between two branch offices, but does not require a permanent VPN connection between sites. In the Services Ready Medium Branch Network, DMVPN was tested on both the primary WAN link and the backup WAN link depending on whether the tunnel interface is active.

```
Router(config)# crypto isakmp policy 1 ! Defines IKE policy
Router(config-isakmp)# encr 3des ! Specifies the encryption mode as 3DES
Router(config-isakmp)# hash md5 ! Specifies hash algorithm as MD5
Router(config-isakmp)# authentication pre-share ! Specifies authentication with pre-shared
keys
Router(config-isakmp)# group 2 ! Specifies 1024-bit Diffie-Hellman group
Router(config-isakmp)# lifetime 28800 ! Specifies the lifetime of IKE security association
Router(config)# crypto isakmp key VPN-KEY address 209.165.201.10 ! Defines the preshared
key to be used for authentication
Router(config)# crypto isakmp keepalive 30 ! Enables keepalives between peers with
specified interval
Router(config)# crypto ipsec transform-set DM-GROUP esp-3des esp-md5-hmac
! Specifies IPSec transform set with ESP encapsulation and AES 256 bit encryption
Router(cfg-crypto-trans)# exit
Router(config)# crypto ipsec profile DM-VPN ! Defines IPSec Profile
Router(ipsec-profile)# set security-association lifetime seconds 86400 ! Specifies the
amount of time for SA to be active
```

```
Router(ipsec-profile)# set transform-set DM-GROUP ! Specifies the IPSec transform set for
encrypting traffic
Router(ipsec-profile)# exit
Router(config)# interface Tunnel 1 ! Enters tunnel interface configuration mode
Router(config-if)# ip address 10.0.2.81 255.255.255.252 ! Specifies tunnel interface IP
address
Router(config-if)# ip mtu 1416 ! Sets the MTU size to 1416 bytes
Router(config-if)# tunnel source Loopback 0 ! Specifies the source address to be used for
tunnel packets
Router(config-if)# ip nbar protocol-discovery ! Enables NBAR protocol discovery
Router(config-if)# ip flow ingress ! Enables Netflow accounting on incoming traffic
Router(config-if)# ip flow egress ! Enables Netflow accounting  on outgoing traffic
Router(config-if)# ip nhrp authentication KEY-BR ! Specifies authentication string
Router(config-if)# ip nhrp map 172.16.0.10 209.165.201.10 ! Specifies central site Tunnel
address to Tunnel source mapping
Router(config-if)# ip nhrp map multicast 209.165.201.10 ! Enables Broadcast/Multicast
support for Tunnel source address
Router(config-if)# ip nhrp network-id 100000 ! Specifies network identifier for this NBMA
network
Router(config-if)# ip nhrp holdtime 300 ! Specifies the time the NHRP address will be
advertised as valid
Router(config-if)# ip nhrp nhs 172.16.0.10 ! Specifies next hop server as the Tunnel
interface
Router(config-if)# load-interval 30 ! Specifies the interval for computing load statistics
Router(config-if)# qos pre-classify ! Enables QoS on VPN tunnel interface
Router(config-if)# tunnel mode gre multipoint ! Specifies the tunnel mode as multipoint
GRE
Router(config-if)# tunnel key 100000 ! Specifies the tunnel key
Router(config-if)# tunnel protection ipsec profile DM-VPN ! Associate IPSec profile with
tunnel interface
```

Apply the following command on the Tunnel interface after defining *VPN* security zone.

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

DMVPN Verification

To verify your DMVPN configuration, enter the following commands:

```
Router# show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 10.10.11.137

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.10.11.137/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (80.80.80.214/255.255.255.255/47/0)
   current_peer 80.80.80.214 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 259540, #pkts encrypt: 259540, #pkts digest: 259540
    #pkts decaps: 256812, #pkts decrypt: 256812, #pkts verify: 256812
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.10.11.137, remote crypto endpt.: 80.80.80.214
     path mtu 1514, ip mtu 1514, ip mtu idb Loopback0
     current outbound spi: 0xA4863CF6(2760260854)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x3EF09B6E(1055955822)
```

```
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 39, flow_id: Onboard VPN:39, sibling_flags 80000046, crypto map:
Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4565229/2312)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xA4863CF6(2760260854)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 40, flow_id: Onboard VPN:40, sibling_flags 80000046, crypto map:
Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4564995/2312)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

Router# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
209.165.201.9     209.165.201.10  QM_IDLE          21440    0 ACTIVE
```

SSL VPN Implementation

Secure Socket Layer Virtual Private Network (SSL VPN) is used to connect remote office users directly to the branch and provide them access to resources in the DMZ VLAN. They are also able to place calls using PC soft phones.

```
Router(config)#crypto pki trustpoint SSLVPN ! Defines a PKI certificate trust point
Router(ca-trustpoint)# enrollment selfsigned ! Specifies this router as self-signed root
certificate authority
Router(ca-trustpoint)# serial-number ! Specifies that the routers serial number should be
in the certificate request
Router(ca-trustpoint)# revocation-check none ! Disable certificate status check
Router(ca-trustpoint)# rsakeypair CERT-KEY ! Specified RSA key pair
Router(ca-trustpoint)#exit
Router(config)#crypto pki certificate chain SSLVPN ! Enters certificate configuration mode
Router(config-cert-chain)# certificate self-signed 01 ! Manually enters self-signed
certificate
```

There can be only one self-signed PKI certificate per router. AutoSecure, described in the Infrastructure Protection Implementation section, creates a self-signed certificate for the router while configuring SSH access. If AutoSecure was enabled on the router, then the next step is not necessary. However, if AutoSecure was not enabled, the above command will request a self-signed PKI certificate. To learn about creating self-signed certificates, visit:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6657/white_paper_c07-372106.html

```
Enter the certificate in hexidecimal representation....
```

```
Router(config-pubkey)# 308201F2 3082019C A0030201 02020101 300D0609 2A864886 F70D0101
04050030
Router(config-pubkey)# 42314030 12060355 0405130B 46545831 31343841 36433030 2A06092A
864886F7
Router(config-pubkey)# 0D010902 161D4B69 76752D33 3832352D 42722D31 2E796F75 72646F6D
61696E2E
Router(config-pubkey)# 636F6D30 1E170D30 38303231 33323232 3131345A 170D3230 30313031
30303030
Router(config-pubkey)# 30305A30 42314030 12060355 0405130B 46545831 31343841 36433030
2A06092A
Router(config-pubkey)# 864886F7 0D010902 161D4B69 76752D33 3832352D 42722D31 2E796F75
72646F6D
Router(config-pubkey)# 61696E2E 636F6D30 5C300D06 092A8648 86F70D01 01010500 034B0030
48024100
Router(config-pubkey)# A699E60C 8EBCF9EA B3142412 FDEE1150 BF25E671 0FBF5E3E 323ABFEB
FFC9790D
Router(config-pubkey)# D5D10D76 7639A04A DDD45FA3 F82E6EFE 2F14C046 E05C0488 433CD054
44E97E61
Router(config-pubkey)# 02030100 01A37D30 7B300F06 03551D13 0101FF04 05300301 01FF3028
0603551D
Router(config-pubkey)# 11042130 1F821D4B 6976752D 33383235 2D42722D 312E796F 7572646F
6D61696E
Router(config-pubkey)# 2E636F6D 301F0603 551D2304 18301680 14E94478 E4EE44CD 8277D8E9
B12EBC6D
Router(config-pubkey)# ABC165DC D8301D06 03551D0E 04160414 E94478E4 EE44CD82 77D8E9B1
2EBC6D
Router(config-pubkey)# C165DCD8 300D0609 2A864886 F70D0101 04050003 41001086 6FDC6C2E
735E9A99
Router(config-pubkey)# 764F874B 03F10F55 31414E96 A0901C04 D172E2B1 AF990499 5404A7B8
94543832
Router(config-pubkey)# 5B5C0389 C543C76F 49E70F1D CCBCCEC3 A9B346CF D561
Router(config-pubkey)# quit
Router(config-cert-chain)# exit
```

Add the following rules to the firewall access control list (ACL) definitions.

```
Router(config)# ip access-list extended publicSelfInRule20Acl ! Enters Public to IOS zone
ACL definition
Router(config-ext-nacl)# permit tcp any host 209.165.201.15 ! Public address of SSLVPN
gateway 1
Router(config-ext-nacl)# permit tcp any host 209.165.201.17 ! Public address of SSLVPN
gateway 2
Router(config-ext-nacl)# permit tcp any host 209.165.201.20 eq www ! Public address of DMZ
server
Router(config-ext-nacl)# permit tcp any host 209.165.201.21 eq www ! Public address of DMZ
server
Router(config-ext-nacl)# permit tcp any host 209.165.201.22 eq www ! Public address of DMZ
server
Router(config-ext-nacl)# permit ip 192.168.0.0 0.0.0.252 ! Central site network
Router(config-ext-nacl)# permit ip 209.165.201.0 0.0.0.252 ! Central site network
Router(config-ext-nacl)# exit
Router(config)#

Router(config)# ip access-list extended publicDMZInRule20Acl ! Enters Public to DMZ zone
ACL definition
Router(config-ext-nacl)# permit tcp any host 209.165.201.16 ! Public address of SSLVPN
gateway 1
Router(config-ext-nacl)# permit tcp any host 209.165.201.17 ! Public address of SSLVPN
gateway 2
Router(config-ext-nacl)# permit tcp any host 209.165.201.20 eq www ! Public address of DMZ
server
Router(config-ext-nacl)# permit tcp any host 209.165.201.21 eq www ! Public address of DMZ
server
```

```
Router(config-ext-nacl)# permit tcp any host 209.165.201.22 eq www ! Public address of DMZ
server
Router(config-ext-nacl)# exit

Router(config)# ip local pool SSLVPN-Address-Pool 10.0.0.70 10.0.2.79 ! Defines pool of
addresses for VPN clients

Router(config)# webvpn gateway SSLVPN-GATEWAY-1 ! Enters webvpn gateway configuration mode
Router(config-webvpn-gateway)# ip address 209.165.201.15 port 443 ! Assigns public IP for
the gateway
Router(config-webvpn-gateway)# http-redirect port 80 ! Configures HTTP traffic to be
carried as HTTPS
Router(config-webvpn-gateway)# ssl trustpoint SSLVPN ! Assigns PKI certificate trust point
Router(config-webvpn-gateway)# inservice ! Starts the SSLVPN process
Router(config-webvpn-gateway)# exit

Router(config)# webvpn gateway SSLVPN-GATEWAY-2
Router(config-webvpn-gateway)# ip address 209.165.201.17 port 443 ! Assigns public IP for
the gateway
Router(config-webvpn-gateway)# http-redirect port 80 ! Configures HTTP traffic to be
carried as HTTPS
Router(config-webvpn-gateway)# ssl trustpoint SSLVPN ! Assigns PKI certificate trust point
Router(config-webvpn-gateway)# inservice ! Starts the SSLVPN process
Router(config-webvpn-gateway)# exit

Router(config)# webvpn install svc flash:sslclient-win-1.1.4.176.pkg ! Installs Cisco
AnyConnect VPN package

Router(config-webvpn-context)# webvpn context SSLVPN-GW-WEB ! Enters webvpn context
configuration mode
Router(config-webvpn-context)# secondary-color white ! Configures login portal
Router(config-webvpn-context)# title-color #FF9900 ! Configures login portal
Router(config-webvpn-context)# text-color black ! Configures login portal
Router(config-webvpn-context)# ssl encryption rc4-md5 ! Configures RC4-MD5 SSL encryption
Router(config-webvpn-context)# ssl authenticate verify all ! Performs user authentication
Router(config-webvpn-context)# url-list "WEB-SERVERS" ! Configures list of URLs in DMZ
that the user can access
Router(config-webvpn-url)# heading "Web Servers" ! Configures display properties for web
servers
Router(config-webvpn-url)#url-text "Server1" url-value “http://10.0.2.65/index.html"
Router(config-webvpn-url)# url-text "Server2" url-value “http://10.0.2.66/index.html"
Router(config-webvpn-url)# url-text "Server3" url-value “http://10.0.2.67/index.html"

Router(config-webvpn-url)#policy group SSLVPN-POLICY-WEB ! Defines policy for DMZ web
servers
Router(config-webvpn-group)# url-list "WEB-SERVERS" ! Associates policy with URL list
Router(config-webvpn-group)# functions svc-enabled ! Enables use of tunnel mode
Router(config-webvpn-group)# mask-urls ! Obfuscates sensitive URLs
Router(config-webvpn-group)# svc address-pool "SSLVPN-Address-Pool" ! Assigns local
addresses
Router(config-webvpn-group)# svc keep-client-installed ! Maintains Cisco AnyConnect VPN
client software installations on the connecting PCs
Router(config-webvpn-group)# default-group-policy SSLVPN-POLICY-WEB ! Associates SSLVPN
context with this group policy
Router(config-webvpn-context)# aaa authentication list VPN-AUTH-LIST ! Configures AAA for
SSLVPN users
Router(config-webvpn-context)# gateway SSLVPN-GATEWAY-1 ! Assigns gateway to this SSLVPN
context
Router(config-webvpn-context)# inservice ! Starts the SSLVPN policy
Router(config-webvpn-context)# exit
```

The following example illustrates a second SSL VPN context.

```
Router(config-webvpn)# webvpn context SSLVPN-GW-APP ! Enters webvpn context configuration
mode
Router(config-webvpn-context)# ssl encryption rc4-md5 ! Configures RC4-MD5 SSL encryption
Router(config-webvpn-context)# ssl authenticate verify all ! Performs user authentication
Router(config-webvpn-context)# url-list "APP-SERVERS" ! Associates policy with URL list
Router(config-webvpn-url)#   heading "Application Servers" ! Configures display properties
for application servers
Router(config-webvpn-url)# url-text "Server1" url-value "http://10.0.2.65/index.html"
Router(config-webvpn-url)# url-text "Server2" url-value "http://10.0.2.66/index.html"
Router(config-webvpn-url)# url-text "Server3" url-value "http://10.0.2.67/index.html"
Router(config-webvpn-url)# policy group SSLVPN-POLICY-APP
Router(config-webvpn-group)# url-list "APP-SERVERS" ! Associates policy with URL list
Router(config-webvpn-group)# default-group-policy SSLVPN-POLICY-APP ! Associates SSLVPN
context with this group policy
Router(config-webvpn-context)# aaa authentication list VPN-AUTH-LIST ! Configures AAA for
SSLVPN users
Router(config-webvpn-context)# gateway SSLVPN-GATEWAY-2 ! Assigns gateway to this SSLVPN
context
Router(config-webvpn-context)# inservice ! Starts the SSLVPN policy
Router(config-webvpn-context)# exit
Router(config)#
```

Threat Defense Detection and Mitigation Implementation

Zone-based Policy Firewall Implementation

Zone-based Policy Firewall (ZPF) offers assignment of traffic into secure zones for multiple-interface routers. It changes the firewall configuration from interface-based classic Context-Based Access Control (CBAC) model to a more flexible zone-based configuration.

Interfaces are assigned to different zones, and inspection policies are applied to traffic moving between zones. As the inspection policies are zone based rather than interface based, different policies can be applied to traffic from and to the same interface.

There are four zones in the Services Ready Medium Branch Network: Private (LAN), Public (WAN), VPN, and DMZ. Inspection policies were applied for the following zone pairs:

- Traffic originated from Private to Public
- Traffic originated from Private to DMZ
- Traffic originated from Public to Private
- Traffic originated from Public to DMZ
- Traffic originated from router to Private
- Traffic originated from Private to router
- Traffic originated from Private to VPN
- Traffic originated from VPN to Private

```
Router(config)# parameter-map type inspect publicPrivateOutParamMap ! Defines a
parameter-map for traffic from Public to Private zone
Router(config-profile)# max-incomplete low 6000 ! Specifies minimum number of half-open
session before IOS stops removing sessions
```

```
Router(config-profile)# max-incomplete high 10000 ! Specifies maximum number of half-open
session after which IOS starts removing sessions
Router(config-profile)# one-minute low 18000 ! Specifies minimum number of half-open
session in one minute before IOS stops removing sessions
Router(config-profile)# one-minute high 20000 ! Specifies maximum number of half-open
session in one minute after which IOS starts removing sessions
Router(config-profile)# udp idle-time 10 ! Specifies maximum length of time for which UDP
inspect information is maintained
Router(config-profile)# icmp idle-time 5 ! Specifies maximum length of time for which ICMP
inspect information is maintained
Router(config-profile)# tcp max-incomplete host 7000 block-time 0 ! Specifies the maximum
number of half-open TCP sessions to the same destination before IOS starts removing
sessions
Router(config-profile)# exit
Router(config)# ip access-list extended privatePublicOutRule10Acl ! Defines ACL for
traffic from IOS to Private zone
Router(config-ext-nacl)# permit 10.0.0.0 0.0.0.255 ! Permits all data VLAN traffic
Router(config-ext-nacl)# permit 10.0.1.0 0.0.0.255 ! Permits all voice VLAN traffic
Router(config-ext-nacl)# exit

Router(config)# ip access-list extended publicPrivateOutRule10Acl ! Defines ACL for
traffic from Public zone to Private zone
Router(config-ext-nacl)# permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255 ! Permits
central site traffic to Data VLAN
Router(config-ext-nacl)# permit ip 172.16.0.0 0.0.255.255 10.0.1.0 0.0.0.255 ! Permits
central site traffic to Voice VLAN
Router(config-ext-nacl)# permit ip 172.16.0.0 0.0.255.255 10.0.2.0 0.0.0.31 ! Permits
central site traffic to Managment VLAN
Router(config-ext-nacl)# permit ip host 239.1.100.1 any ! Permits key server multicast
address
Router(config-ext-nacl)# permit ip host 209.165.201.10 any ! Permits key server
Router(config-ext-nacl)# exit
Router(config)# class-map type inspect match-all FROM-SELF-CMAP ! Defines class map for
traffic from IOS to Private zone
Router(config-cmap)# match access-group name selfPrivateRule10 ! Matches traffic in
specified ACL
Router(config-cmap)# exit
Router(config)# class-map type inspect match-any TO-SELF-CMAP ! Defines class map for
traffic from Private
Router(config-cmap)# match access-group name selfPrivateRule10 ! Matches traffic in
specified ACL
Router(config-cmap)# exit
Router(config)# class-map type inspect match-any privateDMZOutRule10Protocols ! Defines
class map for protocols from Private to DMZ zone
Router(config-cmap)# match protocol http ! Matches HTTP traffic
Router(config-cmap)# match protocol https ! Matches Secure HTTP traffic
Router(config-cmap)# match protocol dns ! Matches DNS traffic
Router(config-cmap)# match protocol ssh ! Matches Secure Shell traffic
Router(config-cmap)# exit
Router(config)# class-map type inspect match-any privatePublicOutRule10 ! Defines class
map for traffic from Private to Public zone
Router(config-cmap)# match access-group name publicPrivateOutRule10Acl ! Matches traffic
in specified ACL
Router(config-cmap)# exit
Router(config)# class-map type inspect match-any SELF-SERVICE-CMAP ! Defines class map for
protocols originating from IOS
Router(config-cmap)# match protocol tcp ! Matches TCP traffic
Router(config-cmap)# match protocol udp ! Matches UDP traffic
Router(config-cmap)# match protocol icmp ! Matches ICMP traffic
Router(config-cmap)# match protocol h323 ! Matches H323 traffic
Router(config-cmap)# match protocol echo ! Matches ICMP echo traffic
Router(config-cmap)# exit
Router(config-cmap)# class-map type inspect match-any publicDMZOutRule10Protocols
! Defines class map for protocols from Public to DMZ zone
```

```
Router(config-cmap)# match protocol http ! Matches HTTP traffic
Router(config-cmap)# match protocol https ! Matches Secure HTTP traffic
Router(config-cmap)# match protocol dns ! Matches DNS traffic
Router(config-cmap)# match protocol ssh ! Matches Secure Shell traffic
Router(config-cmap)# exit

Router(config)# policy-map type inspect publicDMZOutFwPolicy ! Defines inspect policy for
Public to DMZ zone
Router(config-pmap)# class type inspect publicDMZOutRule10Protocols ! Matches traffic
classified by specified class-map
Router(config-pmap-c)# inspect publicPrivateOutParamMap ! Enables packet inspection
according to the Public to Private zone parameter map definition
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop log ! Drops the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect privateSelfOutFwPolicy ! Defines inspect policy
for Private to IOS zone
Router(config-pmap)# class type inspect SELF-SERVICE-MAP ! Matches traffic classified to
IOS parameter map definition
Router(config-pmap-c)# pass ! Passes the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop ! Drops the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect selfPrivateOutFwPolicy ! Defines inspect policy
for IOS to Private zone
Router(config-pmap)# class type inspect SELF-SERVICE-MAP ! Matches from IOS parameter map
definition
Router(config-pmap-c)# pass ! Passes the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop ! Drops the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect privatePublicOutFwPolicy ! Defines inspect policy
for Private to Public zone
Router(config-pmap)# class type inspect privatePublicOutRule10 ! Matches traffic
classified by specified class-map
Router(config-pmap-c)# inspect publicPrivateOutParamMap ! Enables packet inspection
according to the Public to Private zone parameter map definition percent. No specific
protocol configured in class privatePublicOutRule10 for inspection. All protocols will be
inspected
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop ! Drops the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect privateDMZOutFwPolicy ! Defines inspect policy for
Private to DMZ zone
Router(config-pmap)# class type inspect privateDMZOutRule10Protocols ! Matches traffic
classified by specified class-map
Router(config-pmap-c)# inspect publicPrivateOutParamMap ! Enables packet inspection
according to the Public to Private zone parameter map definition
Router(config-pmap-c)# exit
Router(config-pmap-c)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop log ! Drops the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# zone security Public ! Define Security Zone named Public
Router(config-sec-zone)# description Public Internet Connection
Router(config-sec-zone)# exit
```

Apply *Public* security zone on the WAN interface or subinterface as described in WAN interface configuration sections.

```
Router(config)# zone security Private ! Define Security Zone named Private
Router(config-sec-zone)# description Customer Private Network
Router(config-sec-zone)# exit
Router(config)# zone security DMZ ! Define Security Zone named DMZ
Router(config-sec-zone)# description Customer DMZ Network
Router(config-sec-zone)# exit
```

Apply *Private* and *DMZ* security zones on the LAN interface or subinterface as described in VLAN interface configuration sections.

```
Router(config)# zone-pair security privatePublicOut source Private destination Public !
Define zone-pair for Private to Public traffic
Router(config-sec-zone-pair)# description Outbound Firewall Policy from Private to Public
Router(config-sec-zone-pair)# service-policy type inspect privatePublicOutFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security publicDMZOut source Public destination DMZ ! Define
zone-pair for Public to DMZ traffic
Router(config-sec-zone-pair)# description Outbound Firewall Policy from Public to DMZ
Router(config-sec-zone-pair)# service-policy type inspect publicDMZOutFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security privateDMZOut source Private destination DMZ ! Define
zone-pair for Private to DMZ traffic
Router(config-sec-zone-pair)# description Outbound Firewall Policy from Private to DMZ

Router(config-sec-zone-pair)# service-policy type inspect privateDMZOutFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security privateSelf source Private destination self ! Define
zone-pair for Private to IOS traffic
Router(config-sec-zone-pair)# service-policy type inspect privateSelfOutFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security selfPrivate source self destination Private ! Define
zone-pair for IOS to Private traffic
Router(config-sec-zone-pair)# service-policy type inspect selfPrivateOutFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit
```

Zone-based Policy Firewall Verification

To verify your zone-based firewall configuration, enter the following commands:

```
Router# show policy-map type inspect zone-pair
 Zone-pair: publicPrivateOut

  Service-policy inspect : publicPrivateOutFwPolicy

    Class-map: publicPrivateOutRule10 (match-any)
```

```
     Match: access-group name publicPrivateOutRule10Acl
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: class-map match-any publicPrivateOutRule10Protocols
       160728 packets, 5222722 bytes
       30 second rate 0 bps
       Match: protocol http
         0 packets, 0 bytes
         30 second rate 0 bps
       Match: protocol https
         23 packets, 1196 bytes
         30 second rate 0 bps
       Match: protocol dns
         0 packets, 0 bytes
         30 second rate 0 bps
       Match: protocol ssh
         0 packets, 0 bytes
         30 second rate 0 bps
       Match: protocol icmp
         81876 packets, 2947880 bytes
         30 second rate 0 bps
       Match: protocol ftp
         0 packets, 0 bytes
         30 second rate 0 bps
       Match: protocol tcp
         78575 packets, 2251480 bytes
         30 second rate 0 bps
       Match: protocol udp
         246 packets, 22166 bytes
         30 second rate 0 bps
       Match: protocol bgp
         0 packets, 0 bytes
         30 second rate 0 bps
       Match: protocol smtp
         0 packets, 0 bytes
         30 second rate 0 bps
     Inspect
       Packet inspection statistics [process switch:fast switch]
       tcp packets: [77702:1346327]
       udp packets: [2:0]
       icmp packets: [18235:7]

       Session creations since subsystem startup or last reset 95910
       Current session counts (estab/half-open/terminating) [0:0:0]
       Maxever session counts (estab/half-open/terminating) [14:101:1]
       Last session created 08:55:49
       Last statistic reset never
       Last session creation rate 0
       Maxever session creation rate 15120
       Last half-open session total 0

   Class-map: class-default (match-any)
     Match: any
     Drop
       0 packets, 0 bytes
Zone-pair: publicDMZOut

 Service-policy inspect : publicDMZOutFwPolicy

   Class-map: publicDMZOutRule10Protocols (match-any)
     Match: protocol http
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol https
```

```
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol dns
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol ssh
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol bgp
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol icmp
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: access-group name DMZPublicOutRuleAcl20
       0 packets, 0 bytes
       30 second rate 0 bps
     Inspect
       Session creations since subsystem startup or last reset 0
       Current session counts (estab/half-open/terminating) [0:0:0]
       Maxever session counts (estab/half-open/terminating) [0:0:0]
       Last session created never
       Last statistic reset never
       Last session creation rate 0
       Maxever session creation rate 0
       Last half-open session total 0

   Class-map: class-default (match-any)
     Match: any
     Drop
       0 packets, 0 bytes
Zone-pair: privateDMZOut

 Service-policy inspect : privateDMZOutFwPolicy

   Class-map: privateDMZOutRule10Protocols (match-any)
     Match: protocol http
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol https
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol dns
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol ssh
       0 packets, 0 bytes
       30 second rate 0 bps
     Inspect
       Session creations since subsystem startup or last reset 0
       Current session counts (estab/half-open/terminating) [0:0:0]
       Maxever session counts (estab/half-open/terminating) [0:0:0]
       Last session created never
       Last statistic reset never
       Last session creation rate 0
       Maxever session creation rate 0
       Last half-open session total 0

   Class-map: class-default (match-any)
     Match: any
     Drop
       0 packets, 0 bytes
Zone-pair: vpnPrivateIn
```

```
 Service-policy inspect : vpnPrivateInFwPolicy

   Class-map: vpnPrivateInRule10 (match-any)
     Match: access-group name vpnPrivateInRule10Acl
       4314 packets, 109136 bytes
       30 second rate 0 bps
     Inspect
       Packet inspection statistics [process switch:fast switch]
       tcp packets: [229:3495]
       udp packets: [10:6177032]
       icmp packets: [0:31]

       Session creations since subsystem startup or last reset 271
       Current session counts (estab/half-open/terminating) [0:0:0]
       Maxever session counts (estab/half-open/terminating) [2:11:1]
       Last session created 5d08h
       Last statistic reset never
       Last session creation rate 0
       Maxever session creation rate 10
       Last half-open session total 0

   Class-map: class-default (match-any)
     Match: any
     Drop
       0 packets, 0 bytes
Zone-pair: vpnPrivateOut

 Service-policy inspect : vpnPrivateOutFwPolicy

   Class-map: vpnPrivateOutRule10 (match-any)
     Match: access-group name vpnPrivateOutRule10Acl
       6356447 packets, 231662957 bytes
       30 second rate 0 bps
     Inspect
       Packet inspection statistics [process switch:fast switch]
       tcp packets: [9061:117338799]
       udp packets: [1761:2253]
       icmp packets: [0:6176836]
       ftp packets: [0:11]
       tftp packets: [160:6]
       tftp-data packets: [1600:1756]
       skinny packets: [2867:62498341]

       Session creations since subsystem startup or last reset 6356113
       Current session counts (estab/half-open/terminating) [5:0:0]
       Maxever session counts (estab/half-open/terminating) [193:22:97]
       Last session created 00:00:48
       Last statistic reset never
       Last session creation rate 0
       Maxever session creation rate 22400
       Last half-open session total 0

   Class-map: class-default (match-any)
     Match: any
     Drop
       0 packets, 0 bytes
Zone-pair: publicSelfOut

 Service-policy inspect : publicSelfOutFwPolicy

   Class-map: publicSelfOutRule20 (match-any)
     Match: access-group name publicSelfOutRule20Acl
       255 packets, 39396 bytes
       30 second rate 0 bps
     Match: protocol tcp
       17229 packets, 735614 bytes
       30 second rate 0 bps
     Match: protocol udp
       89136 packets, 6774336 bytes
       30 second rate 0 bps
     Match: protocol icmp
       5 packets, 400 bytes
       30 second rate 0 bps
     Inspect
       Packet inspection statistics [process switch:fast switch]
       tcp packets: [457182:0]
       udp packets: [179870:0]
       icmp packets: [43:0]

       Session creations since subsystem startup or last reset 89587
       Current session counts (estab/half-open/terminating) [1:0:0]
       Maxever session counts (estab/half-open/terminating) [4:4:1]
       Last session created 00:00:45
       Last statistic reset never
       Last session creation rate 1
       Maxever session creation rate 6
       Last half-open session total 0

   Class-map: CRYPTO-CMAP (match-all)
     Match: access-group 123
     Pass
       81354612 packets, 8078747532 bytes

   Class-map: class-default (match-any)
     Match: any
     Drop (default action)
       0 packets, 0 bytes
Zone-pair: publicSelfIn

 Service-policy inspect : publicSelfInFwPolicy

   Class-map: publicSelfInRule20 (match-any)
     Match: access-group name publicSelfInRule20Acl
       279 packets, 35460 bytes
       30 second rate 0 bps
     Match: protocol tcp
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol udp
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol icmp
       0 packets, 0 bytes
       30 second rate 0 bps
     Inspect
       Packet inspection statistics [process switch:fast switch]
       udp packets: [919:0]
       icmp packets: [111:0]

       Session creations since subsystem startup or last reset 279
       Current session counts (estab/half-open/terminating) [0:0:0]
       Maxever session counts (estab/half-open/terminating) [1:2:0]
       Last session created 21:40:08
       Last statistic reset never
       Last session creation rate 0
       Maxever session creation rate 74
       Last half-open session total 0
   Class-map: CRYPTO-CMAP (match-all)
     Match: access-group 123
     Pass
       0 packets, 0 bytes

   Class-map: class-default (match-any)
     Match: any
     Drop (default action)
       0 packets, 0 bytes
Zone-pair: DMZPublicOut

 Service-policy inspect : publicDMZOutFwPolicy

   Class-map: publicDMZOutRule10Protocols (match-any)
     Match: protocol http
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol https
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol dns
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol ssh
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol bgp
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: protocol icmp
       0 packets, 0 bytes
       30 second rate 0 bps
     Match: access-group name DMZPublicOutRuleAcl20
       0 packets, 0 bytes
       30 second rate 0 bps
     Inspect
       Session creations since subsystem startup or last reset 0
       Current session counts (estab/half-open/terminating) [0:0:0]
       Maxever session counts (estab/half-open/terminating) [0:0:0]
       Last session created never
       Last statistic reset never
       Last session creation rate 0
       Maxever session creation rate 0
       Last half-open session total 0

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

Zone-pair: selfprivate

 Service-policy inspect : selfFwPolicy

   Class-map: SELF-CMAP (match-any)
     Match: access-group name SELF-ACL
       24257448 packets, 1807595033 bytes
       30 second rate 1000 bps
     Pass
       24257448 packets, 1807595033 bytes

   Class-map: class-default (match-any)
     Match: any
     Drop
```

```
        0 packets, 0 bytes
 Zone-pair: vpnself

  Service-policy inspect : selfFwPolicy

    Class-map: SELF-CMAP (match-any)
      Match: access-group name SELF-ACL
        545089 packets, 17426918 bytes
        30 second rate 0 bps
      Pass
        545089 packets, 17426918 bytes

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
 Zone-pair: selfvpn

  Service-policy inspect : selfFwPolicy

    Class-map: SELF-CMAP (match-any)
      Match: access-group name SELF-ACL
        1088484 packets, 28319861 bytes
        30 second rate 0 bps
      Pass
        1088484 packets, 28319861 bytes

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
Router#
```

DMVPN uses Virtual Tunnel Interface (VTI) for IPsec VPN connectivity. When the DMVPN interface is assigned to a security zone, traffic routing to and from other interfaces in the router are subjected to zone-to-zone firewall policy.

If the DMVPN interface is assigned to the same security zone as another interface (for example, Gigabit Ethernet 0/0), traffic moving between hosts on the DMVPN and hosts connected to Gigabit Ethernet 0/0 will pass freely with no policy application.

In the Services Ready Medium Branch Network, the tunnel interface is assigned to the VPN security zone. Additional inspection policies were applied.

```
Router(config)# ip access-list extended publicSelfInRule20Acl ! Defines ACL for Public to IOS zone traffic
Router(config-ext-nacl)# permit udp any eq isakmp host 209.165.201.9 eq isakmp ! Matches ISAKMP traffic
Router(config-ext-nacl)# exit

Router(config)# ip access-list extended publicSelfOutRule20Acl ! Defines ACL for IOS to Public zone traffic
Router(config-ext-nacl)# permit udp host 22.0.14.253 eq isakmp any eq isakmp ! Matches ISAKMP traffic
Router(config-ext-nacl)# permit ip 192.168.0.0 0.0.0.252 ! Central site network
Router(config-ext-nacl)# permit ip 209.165.201.0 0.0.0.252 ! Central site network
Router(config-ext-nacl)# exit

Router(config)# ip access-list extended vpnPrivateInRule10Acl ! Defines ACL for VPN to Private zone traffic
Router(config-ext-nacl)# permit ip any any ! Matches all traffic
Router(config-ext-nacl)# exit
Router(config)# ip access-list extended vpnPrivateOutRule10Acl ! Defines ACL for Private 
to VPN zone traffic
Router(config-ext-nacl)# permit ip any any ! Matches all traffic
Router(config-ext-nacl)# exit

Router(config)# ip access-list extended NON-TCP-ACL ! Defines ACL for WAAS GRE tunnel
Router(config-ext-nacl)# permit gre host 10.0.2.90 host 10.0.2.89
Router(config-ext-nacl)# exit

Router(config)# ip access-list extended DMZPublicOutRuleAcl20 ! Defines ACL for DMZ to 
Public zone traffic
Router(config-ext-nacl)# permit tcp host 10.0.2.70 eq www any ! DMZ server
Router(config-ext-nacl)# permit tcp host 10.0.2.71 eq www any ! DMZ server
Router(config-ext-nacl)# permit tcp host 10.0.2.72 eq www any ! DMZ server

Router(config-ext-nacl)# exit

Router(config)# access-list 123 permit esp any any  ! Matches IPSec ESP traffic
Router(config)# ip access-list extended SELF-ACL ! Defines ACL for IOS traffic
Router(config-ext-nacl)# permit tcp any any ! Matches TCP
Router(config-ext-nacl)# permit gre any any ! Matches GRE
Router(config-ext-nacl)# permit ip any any ! Matches IP
Router(config-ext-nacl)# exit

Router(config)# class-map type inspect match-any vpnPrivateInRule10 ! Defines class-map 
for VPN to Private zone traffic
Router(config-cmap)# match access-group name vpnPrivateInRule10Acl ! Matches traffic 
specified in ACL
Router(config-cmap)# exit

Router(config)# class-map type inspect match-all CRYPTO-MAP ! Defines class-map for 
matching VPN traffic
Router(config-cmap)# match access-group 123 ! Matches traffic specified in ACL
Router(config-cmap)# exit

Router(config)# class-map type inspect match-any publicSelfInRule20 ! Defines class-map 
for matching Public to IOS zone traffic
Router(config-cmap)# match access-group name publicSelfInRule20Acl ! Matches traffic 
specified in ACL
Router(config-cmap)# match protocol tcp ! Matches TCP traffic
Router(config-cmap)# match protocol udp ! Matches UDP traffic
Router(config-cmap)# match protocol icmp ! Matches ICMP traffic
Router(config-cmap)# exit

Router(config)# class-map type inspect match-any vpnPrivateOutRule10 ! Defines class-map 
for Private to VPN zone traffic
Router(config-cmap)# match access-group name vpnPrivateOutRule10Acl ! Matches traffic 
specified in ACL
Router(config-cmap)# exit

Router(config)# class-map type inspect match-any publicSelfOutRule20 ! Defines class-map 
for matching IOS to Public zone traffic
Router(config-cmap)# match access-group name publicSelfOutRule20Acl ! Matches traffic 
specified in ACL
Router(config-cmap)# match protocol tcp ! Matches TCP traffic
Router(config-cmap)# match protocol udp ! Matches UDP traffic
Router(config-cmap)# match protocol icmp ! Matches ICMP traffic
Router(config-cmap)# exit

Router(config)# class-map type inspect match-any publicDMZOutRule10Protocols
! Defines class-map for matching DMZ to Public zone traffic
Router(config-cmap)# match protocol http ! Matches HTTP traffic
Router(config-cmap)# match protocol https ! Matches Secure HTTP traffic
Router(config-cmap)# match protocol dns ! Matches DNS traffic
Router(config-cmap)# match protocol ssh ! Matches Secure Shell traffic
Router(config-cmap)# match protocol bgp ! Matches BGP traffic
Router(config-cmap)# match protocol icmp ! Matches ICMP traffic
Router(config-cmap)# match access-group name DMZPublicOutRuleAcl20 ! Matches traffic
specified in ACL
Router(config-cmap)# exit

Router(config)# policy-map type inspect publicSelfInFwPolicy ! Defines inspect policy for
Public to IOS zone
Router(config-pmap)# class type inspect publicSelfInRule20 ! Matches traffic classified by
specified class-map
Router(config-pmap-c)# inspect ! Enables packet inspection
Router(config-pmap-c)# exit
Router(config-pmap)# class type inspect CRYPTO-CMAP ! Matches traffic classified by
specified class-map
Router(config-pmap-c)# pass ! Passes traffic
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop log ! Drops traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect publicDMZOutFwPolicy ! Defines policy for DMZ to
Public zoneRouter(config-pmap)# class type inspect publicDMZOutRule10Protocols ! Matches
traffic classified by specified class-map
Router(config-pmap-c)# inspect publicPrivateOutParamMap ! Enables inspection for Public to
Private zone traffic
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop log ! Drops traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect vpnPrivateInFwPolicy ! Defines policy for VPN to
Private zone trafficRouter(config-pmap)# class type inspect vpnPrivateInRule10 ! Matches
traffic classified by specified class-map
Router(config-pmap-c)# inspect  ! Enables packet inspection percent. No specific protocol
configured in class vpnPrivateInRule10 for inspection. All protocols will be inspected
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop log ! Drops traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect publicSelfOutFwPolicy ! Defines policy for IOS to
Public zone traffic
Router(config-pmap)# class type inspect publicSelfOutRule20 ! Matches traffic classified
by specified class-map
Router(config-pmap-c)# inspect ! Enables packet inspection
Router(config-pmap-c)# exit
Router(config-pmap)# class type inspect CRYPTO-CMAP ! Matches traffic classified by
specified class-map
Router(config-pmap-c)# pass ! Pass the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop log ! Drops the traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# policy-map type inspect vpnPrivateOutFwPolicy ! Defines policy for Private
to VPN zone traffic
Router(config-pmap)# class type inspect vpnPrivateOutRule10 ! Matches traffic classified
by specified class-map
Router(config-pmap-c)# inspect ! Enables packet inspection
```

```
 percentNo specific protocol configured in class vpnPrivateOutRule10 for inspection. All
protocols will be inspected
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default ! Matches all other traffic
Router(config-pmap-c)# drop log ! Drops traffic
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# zone security VPN ! Define VPN Zone name
Router(config-sec-zone)# description customer VPN Network
Router(config-sec-zone)# exit

Router(config)# zone-pair security vpnPrivateIn source VPN destination Private ! Define
zone-pair for VPN to Private zone traffic
Router(config-sec-zone-pair)# service-policy type inspect vpnPrivateInFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security vpnPrivateOut source Private destination VPN ! Define
zone-pair for Private to VPN zone traffic
Router(config-sec-zone-pair)# service-policy type inspect vpnPrivateOutFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security publicSelfOut source self destination Public ! Define
zone-pair for IOS to Public zone traffic
Router(config-sec-zone-pair)# service-policy type inspect publicSelfOutFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security publicSelfIn source Public destination self ! Define
zone-pair for Public to IOS zone traffic
Router(config-sec-zone-pair)# service-policy type inspect publicSelfInFwPolicy ! Apply
firewall policy for zone-pair
Router(config-sec-zone-pair)# exit

Router(config)# zone-pair security DMZPublicOut source DMZ destination Public ! Define
zone-pair to  for DMZ to Public zone traffic
Router(config-sec-zone-pair)# service-policy type inspect publicDMZOutFwPolicy
Router(config-sec-zone-pair)# exit

Router(config)# interface Tunnel 1 ! Enters Tunnel interface configuration mode
Router(config-if)# zone-member security VPN ! Assign a zone to the interface
Router(config-if)# exit
```

Cisco IOS IPS Implementation

The Cisco IOS IPS acts as an inline intrusion detection sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When Cisco IOS IPS detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages or Security Device Event Exchange (SDEE).

In the Services Ready Medium Branch Foundation, IPS inspection was enabled on the DATA VLAN in both directions. All types of traffic were inspected using advanced signature set stored in the flash memory.

```
Router# mkdir flash:ips5 ! Creates the folder in flash for saving the signature files
Router(config)# config t
Router(config)# ip ips config location flash:/ips5/ retries 1 ! Specifies the location to
save the signature file
Router(config)# ip ips deny-action ips-interface ! Changes the default behavior of the ACL
filters that are created for the deny actions.
```

```
Router(config)# ip ips notify SDEE ! Enables SDEE event notification on a router
Router(config)# ip ips name IPS-ADVSET ! Defines an IOS IPS rule

Router(config)# ip ips signature-category ! Allows the fine tuning of signature parameters
on the basis of signature category
Router (config-ips-category)# category all ! Specifies the signature category to be used
for multiple aignature actions or conditions
Router(config-ips-category-action)# retired true ! Retires all the signatures in the "all"
category
Router(config-ips-category-action)# category ios_ips advanced ! Enables advanced signature
set
Router (config-ips-category-action)# retired false ! Enables the signatures in the IOS_IPS
category
Router(config-ips-category-action)# end
Router(config)# copy tftp://<ipaddr>/IOS-S341-CLI.pkg idconf ! Loads the signature package
(IOS-S341-CLI.pkg) to the specified location in ip ips config location
```

Cisco IOS IPS Verification

To verify your Cisco IOS IPS configuration, enter the following command:

```
Router# show ip ips statistics
Interfaces configured for ips 2
Session creations since subsystem startup or last reset 0
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [0:0:0]
Last session created never
Last statistic reset never
TCP reassembly statistics
  received 0 packets out-of-order; dropped 0
  peak memory usage 0 KB; current usage: 0 KB
  peak queue length 0
```

Access Control List Implementation

Access control list (ACL) configuration is a basic filtering process that can be used to control access network based on source or source/destination combination.

In Services Ready Medium Branch Network, ACLs entries are used to block TFTP traffic between certain endpoints. This is only an illustrative example.

```
Router(config)# ip access-list extended BLOCK-TFTP ! Specifies an Extended named ACL
Router(config-ext-nacl)# deny udp 172.16.10.0 0.0.0.255 eq tftp 10.0.0.0 0.0.0.255 eq tftp
! Deny TFTP traffic from specific source to specific destination
Router(config-ext-nacl)# deny udp 172.16.20.0 0.0.0.255 eq tftp 10.0.0.0 0.0.0.255 eq tftp
Router(config-ext-nacl)# deny udp 172.16.30.0 0.0.0.255 eq tftp 10.0.0.0 0.0.0.255 eq tftp
```

uRPF Implementation

The uRPF feature is automatically implemented when using AutoSecure. For the sake of completeness, the full configuration is provided.

```
Router(config)# access-list 103 permit udp any any eq bootpc ! Specifies ACL that permits
bootpc traffic
```

Each WAN interface was configured to support uRPF filtering.

```
Router(config)# interface Multilink1 ! Enters Multilink interface configuration mode
Router(config-if)# ip verify unicast source reachable-via rx allow-default 103 ! Enables
uRPF filtering
```

```
Router(config-if)# exit

Router(config)# interface ATM0/2/0.1 point-to-point ! Enters backup interface
configuration mode
Router(config-if)# ip verify unicast source reachable-via rx allow-default 103 ! Enables
uRPF filtering
Router(config-if)# exit
```

Layer 2 Security

Port Security Implementation

Following port security configuration was applied to both the distribution and access layer switches.

```
Switch-Dist(config)# interface range f1/0/5 - 16 ! Enters configuration for range of
gigabit Ethernet ports
Switch-Dist(config-if-range)# switchport port-security ! Enables port security in this
port
Switch-Dist(config-if-range)# switchport port-security maximum 2 ! Specifies to allow
traffic from maximum 2 mac-address as source address
Switch-Dist(config-if-range)# switchport port-security aging type inactivity ! Specifies
to age out the dynamically learned mac address if no traffic for specified period
Switch-Dist(config-if-range)# switchport port-security aging time 2 ! Specifies to age out
the dynamically learned mac-address after 2 minutes
Switch-Dist(config-if-range)# switchport port-security violation restrict ! Specifies the
port to drop packet from non secure mac address and send a trap

Switch-Access(config)# interface range g1/0/5 - 52 ! Enters configuration for range of
Gigabit Ethernet
Switch-Access(config-if-range)# switchport port-security ! Enables port security in this
port
Switch-Access(config-if-range)# switchport port-security maximum 2 ! Specifies to allow
traffic from maximum 2 mac-address as source address
Switch-Access(config-if-range)# switchport port-security aging type inactivity ! Specifies
to age out the dynamically learned mac address if no traffic for specified period
Switch-Access(config-if-range)# switchport port-security aging time 2 ! Specifies to age
out the dynamically learned mac-address after 2 minutes
Switch-Access(config-if-range)# switchport port-security violation restrict ! Specifies
the port to drop packet from non secure mac address and send a trap
```

Port Security Verification

To verify your port security configuration, enter the following command:

```
Switch-Access# show port-security interface g1/0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 2 mins
Aging Type                 : Inactivity
```

```
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
Switch-Access#
```

Dynamic ARP Inspection Implementation

Following command demonstrates how to apply dynamic Address Resolution Protocol (ARP) inspection excluding specified hosts.

```
Switch-Dist(config)# arp access-list STATIC-HOSTS ! Defines ARP access-list for hosts that
will be allowed to ARP packets
Switch-Dist(config-arp-nacl)# permit ip host 10.0.0.5  mac any
Switch-Dist(config-arp-nacl)# permit ip host 10.0.0.6 mac any
Switch-Dist(config-arp-nacl)# permit ip host 10.0.0.7  mac any
Switch-Dist(config-arp-nacl)# permit ip host 10.0.0.8  mac any
Switch-Dist(config-arp-nacl)# permit ip host 10.0.0.9  mac any
Switch-Dist(config-arp-nacl)# permit ip host 10.0.0.10  mac any
Switch-Dist(config-arp-nacl)# exit
Switch-Dist(config)# ip arp inspection vlan 301-303 ! Enables ARP inspection on specified
VLANs
Switch-Dist(config)# ip arp inspection validate dst-mac ! Specifies to perform a check
destination-MAC and Target MAC to be same on ARP packet
Switch-Dist(config)# ip arp inspection log-buffer entries 100 ! Enable the dynamic ARP
inspection log buffer to hold 100 entries
Switch-Dist(config)# ip arp inspection log-buffer logs 1 interval 100 ! Enables every log
entry to generate a system message every 100 seconds
Switch-Dist(config)# ip arp inspection filter STATIC-HOSTS vlan  301-303 ! Applies ARP ACL
to specified VLANs
Switch-Dist(config)# errdisable recovery cause arp-inspection ! Enable error recovery for
Dynamic ARP inspection error-disabled state.
Switch-Dist(config)# interface range Port-Channel 1 - 2 ! Enters EtherChannel
configuration mode
Switch-Dist(config-if)# ip arp inspection trust ! Disable ARP inspection
Switch-Dist(config)# interface range f1/0/1 - 4 ! Enters Fast Ethernet configuration mode
Switch-Dist(config-if)# ip arp inspection trust ! Disables ARP inspection
Switch-Dist(config)# interface g1/0/2 ! Enters gigabit Ethernet configuration mode
Switch-Dist(config-if)# ip arp inspection trust ! Disables ARP inspection


Switch-Access(config)# arp access-list STATIC-HOSTS ! Defines ARP access-list for hosts
that will be allowed to ARP packets
Switch-Access(config-arp-nacl)# permit ip host 10.0.0.5  mac any
Switch-Access(config-arp-nacl)# permit ip host 10.0.0.6 mac any
Switch-Access(config-arp-nacl)# permit ip host 10.0.0.7  mac any
Switch-Access(config-arp-nacl)# permit ip host 10.0.0.8  mac any
Switch-Access(config-arp-nacl)# permit ip host 10.0.0.9  mac any
Switch-Access(config-arp-nacl)# permit ip host 10.0.0.10  mac any
Switch-Access(config-arp-nacl)# exit
Switch-Access(config)# ip arp inspection vlan 301-302 ! Enables ARP inspection on
specified VLANs
Switch-Access(config)# ip arp inspection validate dst-mac ! Specifies to perform a check
destination-MAC and Target MAC to be same on ARP packet
Switch-Access(config)# ip arp inspection log-buffer entries 100 ! Enable the dynamic ARP
inspection log buffer to hold 100 entries
Switch-Access(config)# ip arp inspection log-buffer logs 1 interval 100 ! Enables every
log entry to generate a system message every 100 seconds
```

```
Switch-Access(config)# ip arp inspection filter STATIC-HOSTS vlan 301-303 ! Applies ARP
ACL to specified VLANs
Switch-Access(config)# errdisable recovery cause arp-inspection ! Enable error recovery
for Dynamic ARP inspection error-disabled state.
Switch-Access(config)# interface range Port-Channel 1 - 2 ! Enters EtherChannel
configuration mode
Switch-Access(config-if)# ip arp inspection trust ! Disables ARP inspection
Switch-Access(config)# interface range g1/0/1 - 4 ! Enters gigabit Ethernet configuration
mode
Switch-Access(config-if)# ip arp inspection trust ! Disables ARP inspection
```

Dynamic ARP Inspection Verification

To verify your dynamic ARP inspection configuration, enter the following command:

```
Switch-Access# show ip arp inspection vlan 301

Source Mac Validation      : Disabled
Destination Mac Validation : Enabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
  301     Enabled          Active      static-host        No

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
  301     Deny             Deny
Switch-Access#
```

IP Source Guard Implementation

The following source guard configuration was applied to both the distribution and access layer switches.

```
Switch-Dist(config)# ip source binding 0030.94C2.9A40 vlan 303 10.0.2.65 interface f1/0/5
! Specifies MAC to IP binding for statically assigned DMZ server address
Switch-Dist(config)# ip source binding 0030.94C2.9A41 vlan 303 10.0.2.66 interface f1/0/6
! Specifies MAC to IP binding for statically assigned DMZ server address
Switch-Dist(config)# ip source binding 0030.94C2.9A41 vlan 303 10.0.2.66 interface f1/0/7
! Specifies MAC to IP binding for statically assigned DMZ server address
Switch-Dist(config)# ip source binding 0030.94C2.9A41 vlan 303 10.0.2.66 interface f1/0/8
! Specifies MAC to IP binding for statically assigned DMZ server address
Switch-Dist(config)# ip source binding 0030.94C2.9A42 vlan 303 10.0.2.67 interface f1/0/9
! Specifies MAC to IP binding for statically assigned DMZ server address
Switch-Dist(config)# ip source binding 0030.94C2.9A43 vlan 303 10.0.2.68 interface f1/0/10
! Specifies MAC to IP binding for statically assigned DMZ server address
Switch-Dist(config)# ip source binding 0030.94C2.9A44 vlan 303 10.0.2.69 interface f1/0/11
! Specifies MAC to IP binding for statically assigned DMZ server address
Switch-Dist(config)# ip source binding 0030.94C2.9A45 vlan 303 10.0.2.70 interface f1/0/12
! Specifies MAC to IP binding for statically assigned DMZ server address
Switch-Dist(config)# ip source binding 0030.94C2.9A46 vlan 303 10.0.2.71 interface f1/0/13
! Specifies MAC to IP binding for statically assigned DMZ server address
Switch-Dist(config)# ip source binding 0030.94C2.9A47 vlan 303 10.0.2.72 interface f1/0/14
! Specifies MAC to IP binding for statically assigned DMZ server address
Switch-Dist(config)# ip source binding 0030.94C2.9A48 vlan 303 10.0.2.73 interface f1/0/15
! Specifies MAC to IP binding for statically assigned DMZ server address
Switch-Dist(config)# ip source binding 0030.94C2.9A49 vlan 303 10.0.2.74 interface f1/0/16
! Specifies MAC to IP binding for statically assigned DMZ server address
Switch-Access(config)# interface range f1/0/5 - 16 ! Enters Fast Ethernet configuration
mode
Switch-Access(config-if-range)# ip verify source port-security ! Specifies to check the
binding table and allow traffic only if it matches an entry
```

```
Switch-Access(config)# interface range g1/0/5 - 52 ! Enters gigabit Ethernet configuration
mode
Switch-Access(config-if-range)# ip verify source port-security ! Specifies to check the
binding table and allow traffic only if it matches an entry
```

DHCP Snooping Implementation

```
Switch-Dist(config)# ip dhcp snooping ! Enables DHCP snooping globally on the switch
Switch-Dist(config)# ip dhcp snooping vlan 301-303 ! Enables DHCP snooping for specified
VLANs
Switch-Dist (config)# interface range Port-Channel 1 - 2 ! Enters EtherChannel
configuration mode
Switch-Dist(config-if)# ip dhcp snooping trust ! Disable ARP inspection on EtherChannel
Switch-Dist(config)# interface range f1/0/1 - 4 ! Enters Fast Ethernet configuration mode
Switch-Dist(config-if)# ip dhcp snooping trust ! Disables DHCP snooping
Switch-Dist(config)# interface g1/0/2 ! Enters gigabit Ethernet configuration mode
Switch-Dist(config-if)# ip dhcp snooping trust ! Disables DHCP snooping

Switch-Access(config)# ip dhcp snooping ! Enables DHCP snooping globally on the switch
Switch-Access(config)# ip dhcp snooping vlan 301-302 ! Enables DHCP snooping for specified
VLANs
Switch-Access(config)# interface Port-Channel1 ! Enters EtherChannel configuration mode
Switch-Access(config-if)# ip dhcp snooping trust ! Disables DHCP snooping
Switch-Access(config)# interface range Port-Channel 1 - 2 ! Enters EtherChannel
configuration mode
Switch-Access(config-if)# ip dhcp snooping trust ! Disables DHCP snooping
Switch-Access(config)# interface range g1/0/1 - 4 ! Enters gigabit Ethernet configuration
mode
Switch-Access(config-if)# ip dhcp snooping trust ! Disables DHCP snooping
```

DHCP Snooping Verification

To verify your Dynamic Host Configuration Protocol (DHCP) snooping configuration, enter the following command.

```
Switch-Access# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
301-303
Insertion of option 82 is enabled
```

BPDU Guard Implementation

The following is an example for configuring port security on all trunk ports.

```
Switch-Dist(config-if)# interface range Port-channel 1 - 2 ! Enters Ether channel
configuration mode
Switch-Dist(config-if-range)# spanning-tree bpduguard disable ! Disables BPDU guard
Switch-Dist(config)# interface range g1/0/2 ! Enters gigabit Ethernet configuration mode
Switch-Dist(config-if)# spanning-tree bpduguard enable ! Enables BPDU guard
Switch-Dist(config)# interface range f1/0/5 - 16 ! Enters Fast Ethernet configuration mode
Switch-Dist(config-if)# spanning-tree bpduguard enable ! Enables BPDU guard
Switch-Access(config-if)# interface Port-channel 1 ! Enters EtherChannel configuration
mode
Switch-Access(config-if)# spanning-tree bpduguard disable ! Disables BPDU guard
Switch-Access(config)# interface range g1/0/5 - 52 ! Enters gigabit Ethernet configuration
mode
Switch-Access(config-if)# spanning-tree bpduguard enable ! Enables BPDU guard
```

Management Services Implementation

NetFlow Implementation

Cisco IOS NetFlow efficiently collects and measure data as it enters specific router interface. This data can be used for network traffic accounting and network planning.

NetFlow can be configured to collect data for top flows, and the data can be used for further analysis.

```
Router(config)# ip flow-top-talkers ! Enabled NetFlow to capture traffic statistics for 
top flows
Router(config-flow-top-talkers)# top 5 ! Specifies the maximum number of top talkers
Router(config-flow-top-talkers)# sort-by packets ! Specifies to sort top talkers by number 
of bytes
Router(config-flow-top-talkers)# cache-timeout 100 ! Specifies the time up to which top 
talkers statistics collected
Router(config-flow-top-talkers)# exit
Router(config)# exit
```

NetFlow Verification

To verify your NetFlow configuration, enter the following command:

```
Router# show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Mu1           10.0.0.22       Local         10.0.0.8        2F 0000 0000    28
Mu1           10.0.0.27       Local         10.0.0.10       32 AAB6 2992    28
Tu1           172.16.0.10      Null          224.0.0.10      58 0000 0000    27
3 of 5 top talkers shown. 3 flows processed.

Router#
```

SNMP Implementation

Simple Network Management Protocol (SNMP) is an application layer protocol which facilitates the exchange of management information between a network device and an SNMP server. This information can be used for network management and troubleshooting.

SNMP is enabled to send traps for specific events that will be used for troubleshooting. Two SNMP communities with different privileges were configured.

```
Router(config)# ip access-list standard Full ! List of clients with full access to SNMP 
agent
Router(config-std-nacl)# permit host 172.16.4.5
Router(config-std-nacl)# exit
Router(config)# ip access-list standard Browse ! List of clients with browse access to
SNMP agent
Router(config-std-nacl)# permit host 10.0.0.6
Router(config-std-nacl)# exit
Router(config)# snmp-server community RW-ACCESS rw Full ! Enables SNMP community with
Read/Write access to server
Router(config)# snmp-server community RO-ACCESS ro Browse ! Enables SNMP community with
Read-Only access to server
Router(config)# snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart ! Enables notification for various router events
Router(config)# snmp-server enable traps eigrp ! Enables EIGRP notification
Router(config)# snmp-server enable traps flash insertion removal ! Enables Flash
Insertion/Removal notification
Router(config)# snmp-server enable traps envmon ! Enables Environmental monitor
notification
Router(config)# snmp-server enable traps bgp ! Enables BGP protocol notification
Router(config)# snmp-server enable traps memory bufferpeak ! Enables Memory buffer peak
notification
Router(config)# snmp-server enable traps hsrp ! Enables HSRP notification
Router(config)# snmp-server enable traps ospf state-change ! Enables OSPF protocol
state-change notification
Router(config)# snmp-server enable traps ospf errors ! Enables OSPF error notification
Router(config)# snmp-server enable traps ospf retransmit ! Enables OSPF LSA retransmit
notification
Router(config)# snmp-server enable traps ospf lsa ! Enables OSPF LSA notification
Router(config)# snmp-server enable traps ospf cisco-specific state-change
nssa-trans-change
! Enables OSPF NSSA state change notification
Router(config)#  snmp-server enable traps ospf cisco-specific state-change shamlink
interface-old ! Enables OSPF replaced interface shamlink notification
Router(config)# snmp-server enable traps ospf cisco-specific state-change shamlink
neighbor  ! Enables OSPF neighbor shamlink transition notification
Router(config)# snmp-server enable traps ospf cisco-specific errors ! Enables OSPF
nonvirtual interface mismatch error notification
Router(config)# snmp-server enable traps ospf cisco-specific retransmit ! Enables OSPF
retransmit error notification
Router(config)# snmp-server enable traps ospf cisco-specific lsa ! Enables OSPF LSA
notification
Router(config)# snmp-server enable traps cpu threshold ! Enables CPU threshold violation
notification
Router(config)#
```

NTP Implementation

Network Time Protocol (NTP) is used to synchronize the time in local devices to a radio clock or atomic clock attached to the time server. Synchronized time in all the network devices is helpful for troubleshooting and understanding logging messages.

```
Router(config)# ntp authenticate ! Enables NTP authentication
Router(config)# ntp authentication-key 1234 md5 NTP-KEY ! Specifies authentication key and
Password
Router(config)# ntp trusted-key 1234 ! Specifies the key number to be used for
authentication
Router(config)# ntp server 172.16.0.60 key 1234 ! Specifies central site NTP server
address and key

Switch-Dist (config)# ntp authenticate ! Enables NTP authentication
Switch-Dist (config)# ntp authentication-key 1234 md5 NTP-KEY ! Specifies authentication
key and Password
Switch-Dist (config)# ntp trusted-key 1234 ! Specifies the key number to be used for
authentication
```

```
Switch-Dist (config)# ntp server 172.16.0.60 key 1234 ! Specifies central site NTP server
address and key

Switch-Access (config)# ntp authenticate ! Enables NTP authentication
Switch-Access (config)# ntp authentication-key 1234 md5 NTP-KEY ! Specifies authentication
key and Password
Switch-Access (config)# ntp trusted-key 1234 ! Specifies the key number to be used for
authentication
Switch-Access (config)# ntp server 172.16.0.60 key 1234 ! Specifies central site NTP
server address and key
```

Set time zone and daylight saving for a specific time zone. The following example uses U.S. Pacific Standard Time zone.

```
Router(config)# clock timezone pst -8 ! Sets the time zone
Router(config)# clock summer-time pdt recurring ! Sets daylight savings time
Switch-Dist(config)# clock timezone pst -8 ! Sets the time zone
Switch-Dist(config)# clock summer-time pdt recurring ! Sets daylight savings time

Switch-Access(config)# clock timezone pst -8 ! Sets the time zone
Switch-Access(config)# clock summer-time pdt recurring ! Sets daylight savings time
```

NTP Verification

To verify your NTP configuration, enter the following command:

```
Router# show ntp status
Clock is synchronized, stratum 4, reference is 10.66.66.11
nominal freq is 250.0000 Hz, actual freq is 249.9966 Hz, precision is 2**18
reference time is CC70BD86.5EFBE4E6 (02:16:54.371 PDT Tue Sep 9 2008)
clock offset is -0.0255 msec, root delay is 0.79 msec
root dispersion is 0.11 msec, peer dispersion is 0.05 msec
Router#
```

IP SLA Implementation

An IP Service Level Agreement (SLA) is a management tool running on Cisco IOS software that can be used to analyze IP service levels for IP applications and services in order to increase the network productivity and to reduce the frequency of network outages.

In the Services Ready Medium Branch Network architecture, the User Datagram Protocol (UDP)-echo operation is used to test end-to-end connectivity and response time, and UDP jitter is used to measure packet variability.

```
Router(config)# ip sla 10 ! Configures IP SLA operation with specified ID
Router(config-ip-sla)# udp-echo 209.165.201.10 65535 source-ip 209.165.201.9 source-port
65000 ! Performs UDP echo operation between two Loopback Interfaces
Router(config-ip-sla-udp)# frequency 30 ! Sets the rate at which a specified IP SLA
operation repeats
Router(config)# ip sla 20 ! Configures IP SLA operation with specified ID
Router(config-ip-sla-udp)# udp-jitter 209.165.201.10 65535 source-ip 209.165.201.9
source-port 65000 ! Performs UDP jitter operation between two Loopback Interfaces
Router(config-ip-sla-jitter)# frequency 30 ! Sets the rate at which a specified IP SLA
operation repeats

Router(config-ip-sla-udp)# exit
Router(config)# ip sla schedule 10 start-time now life forever ! Starts the IP SLA
operation now and runs it indefinitely
Router(config)# ip sla schedule 20 start-time now life forever ! Starts the IP SLA
operation now and runs it indefinitely
```

IP SLA Verification

To verify your IP SLA configuration, enter the following command:

```
Router# show ip sla statistics

Round Trip Time (RTT) for       Index 10
        Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: *22:45:46.259 pst Mon Feb 2 2009
Latest operation return code: No connection
Number of successes: 0
Number of failures: 3
Operation time to live: Forever



Round Trip Time (RTT) for       Index 20
        Latest RTT: 0 milliseconds
Latest operation start time: *20:22:59.119 pst Mon Feb 2 2009
Latest operation return code: Socket bind error
RTT Values:
        Number Of RTT: 0                RTT Min/Avg/Max: 0/0/0 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 0
        Source to Destination Latency one way Min/Avg/Max: 0/0/0 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 0/0/0 milliseconds
Jitter Time:
        Number of SD Jitter Samples: 0
        Number of DS Jitter Samples: 0
        Source to Destination Jitter Min/Avg/Max: 0/0/0 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/0/0 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0           Loss Destination to Source: 0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 0
        Mean Opinion Score (MOS): 0
Number of successes: 0
Number of failures: 4
Operation time to live: Forever
```

Syslog Implementation

Apply following commands to enable syslog logging.

```
Router(config)# service timestamps log datetime msec localtime show-timezone ! Instructs
the system to timestamp syslog messages
Router(config)# logging 172.16.0.90 ! Identifies syslog server
Router(config)# logging trap notifications ! Log notice messages and above
Router(config)# logging facility local2 ! Specifies the facility level used by the syslog
messages
Router(config)# logging buffered 4096 ! Sets size of internal log buffer

Switch-Access(config)# service timestamps log datetime msec localtime show-timezone !
Instructs the system to timestamp syslog messages
Switch-Access (config)# logging 172.16.0.90 ! Identifies syslog server
Switch-Access (config)# logging trap notifications ! Log notice messages and above
Switch-Access (config)# logging facility local2 ! Specifies the facility level used by the
syslog messages
Switch-Access (config)# logging buffered 4096 ! Sets size of internal log buffer
```

```
Switch-Dist(config)# service timestamps log datetime msec localtime show-timezone !
Instructs the system to timestamp syslog messages
Switch-Dist (config)# logging 172.16.0.90 ! Identifies syslog server
Switch-Dist (config)# logging trap notifications ! Log notice messages and above
```

Cisco Configuration Professional Implementation

Monitoring of the Services Ready Medium Branch Network was done with the Cisco Configuration Professional in monitor mode. Cisco Configuration Professional provides an overview of router status and performance metrics without having to use the Cisco IOS command-line interface. Figure 5 shows the monitor overview, which includes information such as CPU and memory usage, interface status, firewall status, and VPN status.

Figure 5 Cisco Configuration Professional Monitor Overview

Figure 6 shows the interface status for the Gigabit Ethernet interface, which includes packets in and packets out, and bandwidth usage.

Figure 6 Cisco Configuration Professional Gigabit Ethernet Interface Status

Figure 7 shows the interface status for the tunnel interface.

Figure 7 Cisco Configuration Professional Tunnel Interface Status

Figure 8 shows the VPN status for the DMVPN tunnel, which includes encapsulation and decapsulation packets and send and receive error packets.

Figure 8 Cisco Configuration Professional VPN Status

Figure 9 shows the interface traffic analysis.

Figure 9 Cisco Configuration Professional Traffic Analysis

Cisco Configuration Engine Implementation

There are several steps required to enable deployment with the Cisco Configuration Engine. First, *bootstrap configuration* must be applied to each device. The boostrap configuration is either preloaded or obtained from a centrally hosted DHCP server through option 150. In the Services Ready Medium Branch Network, both routers and all switches were preloaded with the following bootstrap configuration.

```
Router(config)# cns trusted-server all-agents cce.example.com ! Specifies trusted server
for CNS agent
Router(config)# cns id hardware-serial ! Identifies this devices by its serial number to
CCE
Router(config)# cns id hardware-serial event ! Identifies this devices by its serial
number to CCE event logging component
Router(config)# cns event cce.example.com ! Enables event agent
Router(config)# cns config initial cce.example.com 80 ! Initiates an initial configuration
on CCE server port 80
Router(config)# cns config partial cce.example.com 80 ! Initiates an incremental
configuration on CCE server port 80
Router(config)# cns exec 80 ! Enables CNS agent

Switch-Access(config)# cns trusted-server all-agents cce.example.com ! Specifies trusted
server for CNS agent
Switch-Access(config)# cns id hardware-serial ! Identifies this devices by its serial
number to CCE
```

```
Switch-Access(config)# cns id hardware-serial event ! Identifies this devices by its
serial number to CCE event logging component
Switch-Access(config)# cns event cce.example.com ! Enables event agent
Switch-Access(config)# cns config initial cce.example.com 80 ! Initiates an initial
configuration on CCE server port 80
Switch-Access(config)# cns config partial cce.example.com 80 ! Initiates an incremental
configuration on CCE server port 80
Switch-Access(config)# cns exec 80 ! Enables CNS agent

Switch-Dist(config)# cns trusted-server all-agents cce.example.com ! Specifies trusted
server for CNS agent
Switch-Dist(config)# cns id hardware-serial ! Identifies this devices by its serial number
to CCE
Switch-Dist(config)# cns id hardware-serial event ! Identifies this devices by its serial
number to CCE event logging component
Switch-Dist(config)# cns event cce.example.com ! Enables event agent
Switch-Dist(config)# cns config initial cce.example.com 80 ! Initiates an initial
configuration on CCE server port 80
Switch-Dist(config)# cns config partial cce.example.com 80 ! Initiates an incremental
configuration on CCE server port 80
Switch-Dist(config)# cns exec 80 ! Enables CNS agent
```

Secondly, the device CNS ID must be entered into the CCE server prior to powering on of branch devices. Each device CNS is associated with Cisco IOS image to be loaded onto the device and a configuration toolkit. The Services Ready Medium Branch Network provides following 10 CCE toolkits:

- **Configuration for zero-touch deployment with Cisco Configuration Engine**
  - Bootstrap Configuration for routers and switches
- **Router**
  - Gigabit Ethernet WAN interface, active primary and standby backup WAN links, OSPF routing, DMVPN over primary and backup WAN links, and Cisco Unified CME with SCCP configured IP Phones and H.323 trunking to the central site.
  - Four T1 WAN interface bundle with MLPPP encapsulation, active primary and standby backup WAN links, EIGRP routing, GETVPN over primary and DMVPN over backup WAN links, and Cisco Unified CME with SIP configured IP Phones and SIP trunking to central site.
  - Four T1 WAN interface bundle with MLFR encapsulation, simultaneously active primary and backup WAN links, EIGRP routing, DMVPN over primary and backup WAN links, and Cisco Unified SRST with SCCP configured IP Phones and H.323 trunking to central site.
  - T3 WAN interface with Frame Relay encapsulation, simultaneously active primary and backup WAN links, OSPF routing, GETVPN over primary and DMVPN over backup WAN links, and Cisco Unified SRST with SIP configured IP Phones and SIP trunking to central site.
- **Distribution Switches**
  - A 16-port EtherSwitch service module with 2 two-link EtherChannel trunks and DMZ VLAN on access ports.
- **Access Switches**
  - A 48-port access switch with a two-link EtherChannel trunk and Data and Voice VLANs on access ports.

Downloading and Using the Configuration Toolkit

Download the templates from the following location:

- Configuration Templates for Services Ready Large Branch Network

To use the configuration templates for manual configurations, download them to a TFTP server that is accessible from the routers and switches. To use the configuration templates with Cisco Configuration Engine (CCE) 3.0, complete the following steps:

Step 1 Log in to CCE and navigate to **Tools > Template Manager**.

Step 2 In the Template Manager window, shown in Figure 10, click **Add Template**. The Template Engine window appears.

Figure 10 CCE Template Manager

Step 3 In the Template Engine window, shown in Figure 11, choose the best template engine for your specific environment, and then click **Next**. The CCE Configuration Editor window appears.

Figure 11 CCE Template Engine

Step 4 From the list of configuration templates, copy the configuration template that best meets your needs from one of the above listed configuration templates and paste it into the CCE Configuration Editor, shown in Figure 12.

Figure 12 CCE Configuration Editor

Step 5 Customize the configuration to meet the needs of your specific environment. After editing the configuration, name and save the configuration.

Step 6 Navigate to the Device Manager window, shown in Figure 13, and click **Add Device**.

Figure 13 CCE Device Manager

Step 7 In the Create Device Editor window, shown in Figure 14, assign a Device Name, a Unique ID that corresponds to the configuration name specified in Step 5, and a Device Type. Click **Next**. The Device Group Selector window appears.

Figure 14 CCE Create Device Editor

Step 8 Choose group membership as shown in Figure 15. CCE supports management of devices as groups. See the CCE documentation for details on how to manage devices as a group. Click **Next**. The Device Group Selector window appears.

Figure 15 CCE Device Group Selector

Step 9 In the Device Identification Assignment window, shown in Figure 16, enter the Event ID, Config ID, and Image ID (CCE supports the ability to distribute Cisco IOS software images; see the CCE documentation for additional information) for the Device Type. Click **Finish**.

Note These IDs must match the identification provided in the device Bootstrap Configuration.

Figure 16 CCE Device Identification Assignment

Step 10 Repeat this procedure for all routers and switches.

Voice Services Implementation

This section describes the implementation of two scenarios for voice services:

- Distributed infrastructure and branch endpoints are controlled by Cisco Unified Communications Manager Express (Cisco Unified CME). Local branch voice mail is provided through Cisco Unity Express access.
- Centralized call control with Cisco Unified Communications Manager (Cisco Unified CM). Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) is configured in case of WAN failure.

The following high-level steps must be performed for each telephony service:

1. Configure voice connectivity.
2. Perform telephony service setup.
3. Install IP Phones.
4. Configure voice gateway.
5. Configure dial plan.
6. Set up transcoding and conferencing.
7. Implement Music on Hold.
8. Integrate voice mail.
9. Configure emergency services.

PRI-Trunk and FXS Port Implementation

A 12- channel T1 PRI trunk was used to connect the router to the public switched telephone network (PSTN).

```
Router(config)# card type t1 0 ! Declares network module in slot 0 operational in T1 mode
Router(config)# isdn switch-type primary-4ess ! Acts as Primary 4ESS switch interface to
the PSTN network
Router(config)# network-clock-participate wic 0 ! Enables MFT card to synchronize with NTP
server
Router(config)# controller T1 0/0/0 ! Enters T1 controller configuration mode
Router(config-controller)# pri-group timeslots 1-12 ! Configures Non-facility associated
signaling for first 12 channels of the T1 link
Router(config-controller)# exit
```

The following configuration applies to analog Foreign Exchange Service (FXS) ports.

```
Router(config)# voice-port0/3/0 ! Enters voice port configuration mode
Router(config-voiceport)# station-id name ANALOG-1 ! Assigns a name for the voice port
Router(config-voiceport)# exit

Router(config)# voice-port0/3/1! Enters voice port configuration mode
Router(config-voiceport)# station-id name ANALOG-2 ! Assigns a name for the voice port
Router(config-voiceport)# exit

Router(config)# voice-port0/3/2 ! Enters voice port configuration mode
Router(config-voiceport)# station-id name ANALOG-3 ! Assigns a name for the voice port
Router(config-voiceport)# exit

Router(config)# voice-port0/3/3 ! Enters voice port configuration mode
Router(config-voiceport)# station-id name ANALOG-4 ! Assigns a name for the voice port
Router(config-voiceport)# exit
```

In the Services Ready Medium Branch network 4xT1, the serial interface utilizes compressed RTP to place calls over the WAN. There are several ways to configure cRTP. In the following implantation, cRTP is configured on the QoS class map:

```
Router(config)# policy-map EIGHT-CLASS-V3PN-EDGE ! Defines child policy map
Router(config-pmap)# class VOICE ! Matches traffic classified by VOICE class-map
Router(config-pmap-c)# compress header ip rtp ! Enables cRTP compression
Router(config-pmap-c)# exit
```

The Services Ready Medium Branch Networks has been tested with both SIP- and SCCP-enabled phones. Each phone type requires a different configuration. To implement SCCP-based phones, follow the SCCP instructions in the "Cisco Unified CME with SCCP Endpoints Implementation" section on page 93. To implement SIP-based phones, follow SIP instructions in the "Cisco Unified CME with SIP Endpoints Implementation" section on page 110.

To implement the various voice services described in the following sections, several resources are necessary at the central site. Table 2 lists these resources and the associated IP addresses that are used in the implementation instructions.

Table 2 Central Site Resources Required for Voice Implementation

Resource	IP Address
NTP Server	172.16.0.60
Cisco Call Manager	172.16.200.10
Message Wait Indicator Server	172.16.0.110
Music on Hold Multicast Group	239.1.1.1

Cisco Unified CME with SCCP Endpoints Implementation

Cisco Unified CME with SCCP Endpoints: Telephony Service Setup

The Cisco IOS software provides an automated mechanism for configuring IP telephony services.

```
Router(config)# telephony-service setup ! Enters into Unified CME start setup mode

 --- Cisco IOS Telephony Services Setup ---

Do you want to setup DHCP service for your IP Phones? [yes/no]: no

Do you want to start telephony-service setup? [yes/no]: yes
Configuring Cisco IOS Telephony Services :

  Enter the IP source address for Cisco IOS Telephony Services :10.0.1.2
  Enter the Skinny Port for Cisco IOS Telephony Services :  [2000]:
  How many IP Phones do you want to configure :  [0]: 75 ! User configurable number of
  phones up to maximum of 240 on 3900 ISRs
  Do you want dual-line extensions assigned to phones? [yes/no]: yes
  What Language do you want on IP Phones :
        0  English
        1  French
        2  German
        3  Russian
        4  Spanish
        5  Italian
        6  Dutch
        7  Norwegian
        8  Portuguese
        9  Danish
        10 Swedish
        11 Japanese
 [0]: ! Maintains default English language
  Which Call Progress tone set do you want on IP Phones :
        0  United States
        1  France
        2  Germany
        3  Russia
        4  Spain
        5  Italy
        6  Netherlands
        7  Norway
        8  Portugal
        9  UK
        10  Denmark
        11  Switzerland
        12  Sweden
        13  Austria
        14  Canada
        15  Japan
 [0]: ! Maintains default United States call progress tone
  What is the first extension number you want to configure : 5001

Do you have Direct-Inward-Dial service for all your phones? [yes/no]: yes
  Enter the full E.164 number for the first phone :4085555001 ! Assigns DID number

Do you want to forward calls to a voice message service? [yes/no]: yes
  Enter extension or pilot number of the voice message service:5444
  Call forward No Answer Timeout : [18]: ! Maintains default value of 18 seconds.
  Possible values are from 5 to 60000 seconds

Do you wish to change any of the above information? [yes/no]: no
CNF-FILES: Clock is not set or synchronized,
                retaining old versionStamps

 ---- Setup completed config ---

Router(config)#
*Sep 10 05:37:10.207:  percentLINK-3-UPDOWN: Interface ephone_dsp DN 1.2, changed state to
up
*Sep 10 05:37:10.207:  percentLINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to
up
*Sep 10 05:37:10.207:  percentLINK-3-UPDOWN: Interface ephone_dsp DN 2.2, changed state to
up
*Sep 10 05:37:10.207:  percentLINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed state to
up
*Sep 10 05:37:10.207:  percentLINK-3-UPDOWN: Interface ephone_dsp DN 3.2, changed state to
up
*Sep 10 05:37:10.207:  percentLINK-3-UPDOWN: Interface ephone_dsp DN 4.1, changed state to
up
*Sep 10 05:37:10.207:  percentLINK-3-UPDOWN: Interface ephone_dsp DN 4.2, changed state to
up
```

Cisco Unified CME with SCCP Endpoints: IP Phone Installation and Configuration

In the Services Ready Medium Branch Network, IP Phones are installed by simply connecting them to ports on the access layer switches. Because all the ports offer Power-over-Ethernet, no additional power cables are necessary. After they are installed, the phones are configured with the default configuration that was generated during the telephony setup in the previous section. However, if the IP Phone firmware needs to be upgraded in the future, enter the following commands.

Note The following configuration is not required with the Cisco IOS software image used for the Services Ready Medium Branch Network validation.

```
Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telephony)# load 7960-7940 P00308000900 ! Loads telephony SCCP firmware
files for 7960 to 7940 phones
Router(config-telephony)# load 7942 SCCP42.8-3-2S ! Loads telephony SCCP firmware files
for 7942 phones
Router(config-telephony)# load 7962 SCCP62.8-3-2S ! Loads telephony SCCP firmware files
for 7962 phones
Router(config-telephony)# load 7965 SCCP65.8-3-2S ! Loads telephony SCCP firmware files
for 7965 phones
Router(config-telephony)# load 7971 SCCP71.8-3-2S ! Loads telephony SCCP firmware files
for 7971 phones
Router(config-telephony)# load 7985 cmterm_7985.4-1-6-0 ! Loads telephony SCCP firmware
for 7985 video phone
```

Apply the following command after defining the new ephone type.

```
Router(config-telephony)# load 7937 cmterm_7937.1-2-1-0 ! Loads telephony SCCP firmware
files for 7937 conference station

Router(config-telephony)# create cnf-files ! Builds XML configuration file for SCCP phones
Router(config-telephony)# exit
```

This guide provides Cisco IOS software commands for setting up IP Phones. Alternatively, a graphical user interface (GUI) allows the configuration of directory numbers through a web interface. To set up the web configuration tool, use the following instructions to enable the services on the router:

```
Router(config)# ip http server ! Enables HTTP server
Router(config)# ip http path flash: ! Specifies location of HTTP files in IOS
Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telephony)# web admin system name admin password c1$k0SyS ! Defines username
and password for system administrator
Router(config-telephony)# dn-webedit ! Enables ability to configure directory numbers
Router(config-telephony)# time-webedit ! Enables ability to configure phone time
Router(config-telephony)# exit

Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telephony)# max-ephones 100 ! Sets the maximum number of phones that can
register with Cisco CME
Router(config-telephony)# max-dn 200! Sets the maximum number of directory numbers (two
for each phone)
Router(config-telephony)# ip source-address 10.0.1.2 port 2000 secondary 10.0.1.1 ! Sets
IP address used for phone registration and secondary router for backup
Router(config-telephony)# time-zone 5 ! Sets time zone to Pacific Standard/Daylight Time
Router(config-telephony)# no auto-reg-ephone ! Disables registration of unconfigured
phones
Router(config-telephony)# voicemail 5444 ! Defines number for speed dialing voicemail from
phone
Router(config-telephony)# system message Your current options ! Message displayed on IP
Phones
```

```
Router(config-telphony)# secondary-dialtone 9 ! Provides dial tone for PSTN calls
Router(config-telphony)# transfer-system full-blind ! Transfers calls without consultation
Router(config-telphony)# transfer-pattern 9......... ! Allows transfers for all calls
originating from PSTN
Router(config-telphony)# transfer-pattern 4......... ! Allows transfers for all calls
originating in area code starting with "4"
Router(config-telphony)# call-forward pattern .T ! Allows call forwarding for all calls
Router(config-telephony)# exit

Router(config)# ephone-template 1 ! Defines ephone configuration template tag
Router(config-ephone-template)# softkeys hold Join Newcall Resume Select ! Softkey display
when the connected party is on hold
Router(config-ephone-template)# softkeys idle ConfList Join Newcall Pickup Redial !
Softkey display when the phone is idle
Router(config-ephone-template)# softkeys seized Redial Endcall Cfwdall Pickup Callback
Meetme ! Softkey display when caller is attempting to call but has not been connected yet
Router(config-ephone-template)# softkeys connected Trnsfer Hold Confrn Endcall ! Softkey
display when connection to remote point has been established
Router(config-ephone-template)# exit
```

Apply the following configuration to all IP Phones 1 to 100. Set the unique DN number and assign the desired extension to each phone.

```
Router(config)# ephone-dn 1 dual-line ! Enters directory number configuration mode
Router(config-ephone-dn)# number 5001 ! Configures phone (or extension) number for this
directory number
Router(config-ephone-dn)# call-forward busy 5444 ! Forwards call for a busy extension to
voicemail
Router(config-ephone-dn)# call-forward noan 5444 timeout 10 ! Forwards call for an
extension that does not answer to voicemail after 10 seconds of ringing
Router(config-ephone-dn)# exit

Router(config)# ephone 1! Enters phone configuration mode
Router(config-ephone)# ephone-template 1 ! Associates phone with configuration template
Router(config-ephone)# button 1:1 ! Associates phone with directory number 1:2, 1:3, etc.
Router(config-ephone)# exit
```

To configure soft phone, use the following example.

```
Router(config)# ephone 120! Enters phone configuration mode
Router(config-ephone)# type CIPC ! Specifies that this is softphone
Router(config-ephone)# ephone-template 1 ! Associates phone with configuration template
Router(config-ephone)# button 1:120 ! Associates phone with directory number 1:2, 1:3,
etc.
Router(config-ephone)# exit
```

In Cisco IOS 12.4(20)T and later, apply the following configuration to define a conference station.

```
Router(config)# ephone-type 7937 ! Enters ephone-type template configuration mode
Router(config-ephone-type)# device-id 431 ! Specifies 7937 conference station device id
Router(config-ephone-type)# device-type 7937 ! Specifies device type
Router(config-ephone-type)# device-name 7936 Conference Station ! Assigns name to the
device type
Router(config-ephone-type)# num-buttons 1 ! Number of line buttons supported
Router(config-ephone-type)# num-presentations 6 ! Number of call presentations lines
Router(config-ephone-type)# exit

Router(config)# ephone-dn 110 dual-line ! Enters directory number configuration
Router(config-ephone-dn)# number 5110 ! Configures extension (or phone) number for this
directory number
Router(config-ephone-dn)# name Engineering Conference Room ! Associates a name with this
directory number
Router(config-ephone-dn)# exit
Router(config)# ephone 110! Enters phone configuration mode
Router(config-ephone)# button 1:110 ! Associates phone with directory number
Router(config-ephone)# exit
```

Generate the configuration file.

```
Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telephony)# create cnf-files ! Builds XML configuration file for SCCP phones
Router(config-telephony)# reset all ! Reloads the phone configuration
Router(config-telephony)# exit
```

Cisco Unified CME with SCCP Endpoints: H.323 Voice Gateway Implementation

The following configuration enables VoIP on the network and sets up H.323 dial peers between the branch gateway and the destination telephone networks.

```
Router(config)# voice service voip ! Enters voice service configuration mode
Router(config-voi-srv)# allow-connections h323 to h323 ! Enables calls h323 endpoint to 
h323 endpoint
Router(config-voi-srv)# allow-connections h323 to SIP ! Enables calls from h323 endpoint 
to SIP endpoint
Router(config-voi-srv)# exit
```

Cisco Unified CME with SCCP Endpoints: Dial Plan Implementation

Ten dial peers were defined for the Services Ready Medium Branch Network: central site, local calls, two 911 emergency services dial peers, voice mail, auto attendant, long distance, international calling, and fax pass-through or fax relay. Voice mail and emergency services dial peers are described in the "Cisco Unified CME with SIP Endpoints: Voice Mail and Auto Attendant Integration" section on page 115.

```
Router(config)# dial-peer voice 1 voip ! Enters dial peer to central site configuration 
mode
Router(config-dial-peer)# dtmf-relay h245-alphanumeric ! Specifies H.245 alphanumeric 
method for relaying dual tone multifrequency tones
Router(config-dial-peer)# destination-pattern 408....... ! Specifies area code prefix for 
central site dial peer
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial 
peer address
Router(config-peer)# exit

Router(config)# dial-peer voice 2 pots ! Enters dial peer for local area calls 
configuration mode
Router(config-dial-peer)# destination-pattern 9....... ! Specifies area code prefix for 
central site dial peer
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 3 pots ! Enters dial peer for long distance calls 
configuration mode
Router(config-dial-peer)# destination-pattern 91.......... ! Specifies area code prefix 
for central site dial peer
Router(config-dial-peer)# prefix 1 ! Prefix that the system adds automatically to the dial 
string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
Router(config)# dial-peer voice 4 pots ! Enters dial peer for international calls
configuration mode
Router(config-dial-peer)# destination-pattern 9011T ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 011 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

When calls over the WAN exceed the maximum allocated bandwidth, they are redirected to PSTN.

```
Router(config)# dial-peer voice 15 pots ! Enters dial peer for PSTN bypass configuration
mode
Router(config-dial-peer)# destination-pattern 408....... ! Specifies destination pattern
Router(config-dial-peer)# port 0/0/23 ! Specifies outgoing/incoming interface for calls
Router(config-dial-peer)# preference 1 ! Sets the dial peer preference order
Router(config-dial-peer)# prefix 408 ! Prefix that the system adds automatically to the
dial string
```

If you are using fax pass-through, apply the following configuration.

```
Router(config)# dial-peer voice 6 voip ! Enters dial peer for fax passthrough
configuration mode
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-dial-peer)# fax protocol pass-through g711ulaw  ! Configures fax passthrough
with G.711 codec
Router(config-peer)# exit
```

If you are using fax relay, apply the following configuration.

```
Router(config)# dial-peer voice 7 voip ! Enters dial peer for fax relay configuration mode
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-dial-peer)# fax-relay ecm disable ! Disables fax relay ECM
Router(config-dial-peer)# fax rate 9600 ! Selects fax transmission rate
Router(config-dial-peer)# fax protocol t38 ! Sets the T.38 fax relay protocol
Router(config-dial-peer)# codec g711ulaw ! Configures fax relay with G.711 codec
Router(config-peer)# exit
```

Cisco Unified CME with SCCP Endpoints: CAC Implementation

RSVP is not supported with Cisco Unified CME. A limited workaround is possible by setting a limit on the number of voice calls that can be placed over the WAN.

```
Router(config)# dial-peer voice 1 voip ! Enters dial peer to central site configuration
mode
Router(config-dial-peer)# max-con 36 ! Sets the maximum number of WAN based calls to 36
Router(config-dial-peer)# exit
```

Cisco Unified CME with SCCP Endpoints: Transcoding and Conferencing Implementation

Transcoding compresses and decompresses voice streams to match endpoint-device capabilities. Transcoding is required when an incoming voice stream is digitized and compressed (by means of a codec) to save bandwidth and the local device does not support that type of compression.

```
Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telphony)# sdspfarm units 4! Specifies number of DSP farms that can register
with SCCP server
Router(config-telphony)# sdspfarm transcode sessions 5 ! Specifies maximum number of
simultaneous transcoding sessions
Router(config-telphony)# sdspfarm tag 2 CONFERENCE ! Creates DSP farm profile
Router(config-telphony)# sdspfarm tag 3 TRANSCODE ! Creates DSP farm profile
Router(config-telphony)# conference hardware ! Configures CME for multiparty conferencing
Router(config-telphony)# exit

Router(config)# voice-card 0 ! Enters DSP farm configuration mode
Router(config-voicecard)# dsp services dspfarm ! Enables DSP services
Router(config-voicecard)# exit
Router(config)# sccp local GigabitEthernet2/0.2 ! Sets the interface for conferencing and
transcoding to register with CME
Router(config)# sccp ccm 10.0.1.1 identifier 1 version 5.0.1 ! Associates conferencing and
transcoding with CME
Router(config)# sccp ! Enables SCCP globally
Router(config)# sccp ccm group 1 ! Creates SCCP group and enters SCCP configuration mode
Router(config-sccp-ccm)# associate ccm 1 priority 1 ! Associates SCCP group 1 with CME
Router(config-sccp-ccm)# associate profile 2 register CONFERENCE ! Associates DSP farm
profile with with a SCCP group
Router(config-sccp-ccm)# associate profile 3 register TRANSCODE ! Associates DSP farm
profile with with a SCCP group
Router(config-sccp-ccm)# exit

Router(config)# dspfarm profile 2 transcode ! Enters DSP farm profile configuration mode
Router(config-dspfarm-profile)# codec g711ulaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g711alaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729ar8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729abr8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729r8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec pass-through ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# maximum sessions 5 ! Specifies maximum number of
simultaneous sessions supported by this profile
Router(config-dspfarm-profile)# associate application sccp ! Associates SCCP with this DSP
farm profile
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit

Router(config)# dspfarm profile 3 conference ! Enters DSP farm profile configuration mode
Router(config-dspfarm-profile)# codec g711ulaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g711alaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729ar8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729abr8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729r8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729br8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# maximum sessions 3 ! Specifies maximum number of
simultaneous sessions supported by this profile
Router(config-dspfarm-profile)# associate application sccp ! Associates SCCP with this DSP
farm profile
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit

Router(config)# ephone-dn 241 dual-line ! Enters directory number configuration mode
Router(config-ephone-dn)# number 5555 ! Associates telephone extension with this directory
number
Router(config-ephone-dn)# conference ad-hoc ! Configures ad-hoc conferencing
Router(config-ephone-dn)# no huntstop ! Continues call hunting if line is unavailable
Router(config-ephone-dn)# exit

Router(config)# ephone-dn 242 dual-line ! Enters directory number configuration mode
Router(config-ephone-dn)# number 5555 ! Associates telephone extension with this directory
number
```

```
Router(config-ephone-dn)# conference ad-hoc ! Configures ad-hoc conferencing
Router(config-ephone-dn)# no huntstop ! Continues call hunting if line is unavailable
Router(config-ephone-dn)# preference 1 ! Sets dial peer preference order
Router(config-ephone-dn)# exit

Router(config)# ephone-dn 243 dual-line ! Enters directory number configuration mode
Router(config-ephone-dn)# number 5555 ! Associates telephone extension with this directory
number
Router(config-ephone-dn)# conference ad-hoc ! Configures ad-hoc conferencing
Router(config-ephone-dn)# huntstop ! Stop hunting for lines, all conferencing lines are
occupied
Router(config-ephone-dn)# preference 2 ! Sets dial peer preference order
Router(config-ephone-dn)# exit

Router(config)# ephone-dn 244 dual-line ! Enters directory number configuration mode
Router(config-ephone-dn)# number 5666 ! Associates telephone extension with this directory
number
Router(config-ephone-dn)# conference meetme ! Configures meet me conferencing
Router(config-ephone-dn)# no huntstop ! Continues call hunting if line is unavailable
Router(config-ephone-dn)# exit

Router(config)# ephone-dn 245 dual-line ! Enters directory number configuration mode
Router(config-ephone-dn)# number 5666 ! Associates telephone extension with this directory
number
Router(config-ephone-dn)# conference meetme ! Configures meet me conferencing
Router(config-ephone-dn)# no huntstop ! Continues call hunting if line is unavailable
Router(config-ephone-dn)# preference 1 ! Sets dial peer preference order
Router(config-ephone-dn)# exit

Router(config)# ephone-dn 246 dual-line ! Enters directory number configuration mode
Router(config-ephone-dn)# number 5666 ! Associates telephone extension with this directory
number
Router(config-ephone-dn)# conference meetme ! Configures meet me conferencing
Router(config-ephone-dn)# huntstop ! Stop hunting for lines, all conferencing lines are
occupied
Router(config-ephone-dn)# preference 2 ! Sets dial peer preference order
Router(config-ephone-dn)# exit
```

Cisco Unified CME with SCCP Endpoints: Music on Hold Implementation

Music on Hold (MOH) is an audio stream that is played to PSTN and VoIP G.711 or G.729 callers who are placed on hold by phones in a Cisco Unified Communications Manager Express (Cisco Unified CME) system. This audio stream is intended to reassure callers that they are still connected to their calls.

```
Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telephony)# moh music-on-hold.au ! Specifies music on hold file
Router(config-telephony)# exit
```

Cisco Unified CME with SCCP Endpoints: Voice Mail and Auto Attendant Integration

Voice mail is provided by the Cisco Unity Express service module either in the Advanced Integration Module 2 (AIM2) form factor or the Network Module (NME) form factor. The AIM2 module requires the following configuration.

To configure the NME, substitute *Integrated-Service-Engine 2/0* for *Service-Engine 0/1*

```
Router(config)# interface Service-Engine 0/1 ! Enters Cisco Unity Express configuration
mode
```

```
Router(config-if)# ip address 10.0.2.86 255.255.255.252 ! Assigns ip address to the
service engine router interface
Router(config-if)# service-module ip address 10.0.2.85 255.255.255.252 ! Assigns IP
address to service module internal interface
Router(config-if)# service-module ip default-gateway 10.0.2.86 ! Assigns default gateway
for the service module
Router(config-if)# zone-member security Private ! Assigns Cisco Unity Express to private
security zone
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# ip route 10.0.2.884 255.255.255.252 Service-Engine 0/1 ! Adds a static
route entry to direct traffic to the module
```

Cisco Unity Express uses SIP as its signaling protocol and requires a SIP dial peer.

```
Router(config)# dial-peer voice 7 voip ! Enters dial peer for voicemail configuration mode
Router(config-dial-peer)# destination-pattern 5444 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.1.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit

Router(config)# dial-peer voice 9 voip ! Enters dial peer for Auto Attendant configuration
mode
Router(config-dial-peer)# destination-pattern 5000 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.2.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2 ! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify ! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit
```

The following configuration turns on the message wait indicator.

```
Router(config)# ephone-dn 19 ! Enters directory number configuration mode
Router(config-ephone-dn)# number 8000.... ! Phone number for placing MWI notification call
Router(config-ephone-dn)# mwi on ! When call placed to this DN turn MWI on

Router(config-ephone-dn)# ephone-dn 20 ! Enters directory number configuration mode
Router(config-ephone-dn)# number 8001.... ! Phone number for placing MWI notificztion call
Router(config-ephone-dn)# mwi off ! When call placed to this DN turn MWI off
```

Additional Cisco Unified CME configuration is performed through a Web-based user interface as shown in Figure 17 through Figure 22. Figure 17 shows the login prompt window.

Figure 17 Cisco Unified CME Login Prompt

Figure 18 shows the Cisco Unified CME import users window.

Figure 18 Importing Cisco Unified CME Users

Figure 19 shows the Cisco Unified CME defaults window.

Figure 19 Configuring Mailbox Defaults

Figure 20 shows the call handling configuration window.

Figure 20 Configuring Call Handling

Figure 21 shows the Cisco Unified CME configuration verification window.

Figure 21 Verifying Configuration

Figure 22 shows the Cisco Unified CME configuration status window.

Figure 22 Reviewing Configuration Status

Cisco Unified CME with SCCP Endpoints: Emergency Services Implementation

The following is the implementation of emergency number calling for North America. The PRI trunk is used for placing emergency calls.

```
Router(config)# dial-peer voice 10 pots ! Enters dial peer for emergency calls
configuration mode
Router(config-dial-peer)# destination-pattern 911 ! Specifies North America emergency
number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 11 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# destination-pattern 9911 ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 911 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

Cisco Unified CME with SCCP Endpoints Verification

```
Router(config)# show ephone phone-load
DeviceName        CurrentPhoneload       PreviousPhoneload      LastReset
=====================================================================

SEP796000060053   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060052   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060051   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060050   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060049   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060059   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060058   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060057   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060056   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060055   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060054   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060063   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060062   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060061   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060060   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060042   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060041   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060040   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060043   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060044   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060045   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060046   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060047   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060048   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized
SEP796000060086   SCCP41.8-3-2S          SCCP41.8-3-2S          Initialized

Router# show telephony-service ephone-template
ephone-template 1
softkeys hold  Join Newcall Resume Select
softkeys idle  ConfList Join Newcall Pickup Redial RmLstC
softkeys seized  Redial Endcall Cfwdall Pickup Callback Meetme
softkeys connected  Trnsfer Hold Confrn Endcall
conference drop-mode never
conference add-mode all
conference admin: No
max-calls-per-button 8
busy-trigger-per-button 0
privacy default
Always send media packets to this router: No
Preferred codec: g711ulaw
keepalive 30 auxiliary 30
User Locale: US
Network Locale: US


Router# show ephone

ephone-1[0] Mac:001C.58FB.7640 TCP socket:[7] activeLine:0 REGISTERED in SCCP ver 12/9
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:12
IP:10.0.1.11 53063 7965  keepalive 126205 max_line 6
button 1: dn 1  number 5001 CH1   IDLE         CH2   IDLE
Preferred Codec: g722-64


ephone-2[1] Mac:001E.4AF1.38D4 TCP socket:[-1] activeLine:0 UNREGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:7
IP:0.0.0.0 0 Unknown 0  keepalive 0 max_line 0
```

```
Preferred Codec: g711ulaw


ephone-3[2] Mac:001C.58F9.BD38 TCP socket:[2] activeLine:0 REGISTERED in SCCP ver 12/9
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:12
IP: 10.0.1.12 51579 7962  keepalive 126880 max_line 6
button 1: dn 2  number 5002 CH1   IDLE         CH2   IDLE
Preferred Codec: g711ulaw


Router# show telephony-service ephone
Number of Configured ephones 75 (Registered 75)
ephone 1
Device Security Mode: Non-Secure
mac-address 001C.58FB.7640
type 7965
button  1:1
keepalive 30 auxiliary 30
max-calls-per-button 8
busy-trigger-per-button 0
ephone-template 1
Always send media packets to this router: No
Preferred codec: g711ulaw
conference drop-mode never
conference add-mode all
conference admin: No
privacy: Yes
privacy button: No
user-locale US
network-locale US

Router# show telephony-service
CONFIG (Version=4.1(0))
=====================
Version 4.1(0)
Cisco Unified Communications Manager Express
For on-line documentation please see:
www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/ip_ks/index.htm

ip source-address 192.168.0.1 port 2000
max-ephones 120
max-dn 200
max-conferences 3
dspfarm units 4
dspfarm transcode sessions 3
conference software
hunt-group report delay 1 hours
hunt-group logout DND
max-redirect 5
cnf-file location: system:
cnf-file option: PER-PHONE-TYPE
network-locale[0] US   (This is the default network locale for this box)
network-locale[1] US
network-locale[2] US
network-locale[3] US
network-locale[4] US
user-locale[0] US    (This is the default user locale for this box)
user-locale[1] US
user-locale[2] US
user-locale[3] US
user-locale[4] US
srst mode auto-provision is OFF
srst ephone template is 0
srst dn template is 0
srst dn line mode is single
time-format 12
date-format mm-dd-yy
timezone 0 Greenwich Standard Time
no transfer-pattern is configured, transfer is restricted to local SCCP phones only.
keepalive 30 auxiliary 30
timeout interdigit 10
timeout busy 10
timeout ringing 180
timeout ringin-callerid 8
timeout night-service-bell 12
caller-id name-only: enable
web admin system name Admin
web admin customer name Customer
edit DN through Web:  disabled.
edit TIME through web:  disabled.
Log (table parameters):
     max-size: 150
     retain-timer: 15
transfer-system full-consult
local directory service: enabled.
Extension-assigner tag-type ephone-tag.
```

Cisco Unified CME with SIP Endpoints Implementation

Cisco Unified CME with SIP Endpoints: Telephony Service Setup

Configure the SIP gateway at the branch router.

```
Router(config)# voice service voip ! Enters voice service configuration mode
Router(config-voi-srv)# allow-connections SIP to SIP ! Enables calls from SIP endpoint to
SIP endpoint
Router(config-voi-srv)# sip ! Enters SIP configuration mode
Router(config-voi-sip)# registrar server expires max 120 min 60 ! Sets the SIP Phone
keepalive.  The phone will check every 2 minutes whether it is registered with Cisco CME
in case the router lost its registration information during reboot
Router(config-voi-sip)# bind control source-interface GigabitEthernet2/0.2 ! Specifies SIP
to Voice VLAN binding
Router(config-voi-sip)# bind media source-interface GigabitEthernet2/0.2 ! Specifies SIP
to Voice VLAN binding
Router(config-voi-sip)# exit
Router(config-voi-srv)# exit
```

Cisco Unified CME with SIP Endpoints: IP Phone Installation and Configuration

In the Services Ready Medium Branch Network, IP Phones are installed by simply connecting them to ports on the access layer switches. Because all the ports offer Power over Ethernet, no additional power cables are necessary. Once installed, phones are configured with the default configuration generated during the Cisco Unified CME installation. However, if IP Phone firmware needs to be upgraded in the future, issue the following commands.

Note The following configuration is not required with the Cisco IOS software image used for the Services Ready Medium Branch Network validation.

```
Router(config)# voice register global ! Enters voice register configuration mode
Router(config-register-global)# mode cme ! Enables cme mode in the register
Router(config-register-global)# load 7960-7940 P0S3-08-3-00 ! Loads SIP firmware files for 
7960-7940 phones
Router(config-register-global)# load 7961 SIP61.8-3-2S ! Loads SIP firmware files for 7961 
phone
Router(config-register-global)# load 7962 SIP62.8-3-2S ! Loads SIP firmware files for 7962 
phone
Router(config-register-global)# load 7965 SIP65.8-3-2S ! Loads SIP firmware files for 7965 
phone
Router(config-register-global)# load 7971 SIP71.8-3-2S ! Loads SIP firmware files for 7971 
phone

Router(config-register-global)# create profile ! Generates provisioning file
Router(config-register-global)# exit
```

To configure Cisco Unified CME with SIP endpoints from the command line, apply the following configuration.

```
Router(config)# voice register global ! Enters voice configuration mode
Router(config-register-global)# mode cme ! Enables CME mode in the register
Router(config-register-global)# max-pool 100 ! Sets the maximum number of SIP Phones
Router(config-register-global)# max-dn 200 ! Sets the maximum number of directory numbers 
(two for each phone)
Router(config-register-global)# source-address 10.0.1.2 port 2000 ! Sets IP address used 
for phone registration
Router(config-register-global)# dst auto-adjust ! Enables automatic adjustment of Daylight 
Savings Time
Router(config-register-global)# timezone 5 ! Sets time zone to Pacific Standard/Daylight 
Time
Router(config-register-global)# voicemail 5444 ! Defines number for speed dialing 
voicemail from phone
Router(config-register-global)# ntp-server 172.16.0.60 ! Synchronizes clock on the phones 
with the specified NTP server
Router(config-register-global)# exit
Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telphony)# secondary-dialtone 9 ! Provides dial tone for PSTN calls
Router(config-telphony)# exit
```

Apply the following configuration to all IP Phones 1 to 100. Set a unique DN number and assign the desired extension to each phone.

```
Router(config)# voice register dn 1 ! Enters directory configuration mode
Router(config-register-dn)# number 5001! Configures extension number for this directory 
number
Router(config-register-dn)# call-forward b2bua busy 5444 ! Forwards calls for a busy 
extension to voicemail
Router(config-register-dn)# call-forward b2bua noan 5444 timeout 10 ! Forwards calls for a 
no answer extension to voicemail after 10 seconds of running
```

```
Router(config-register-dn)# call-forward b2bua mailbox 5444 ! Designates a mailbox at the
end of call forward chaingRouter(config-register-dn)# mwi ! Configures Voicemail indicator
Router(config-register-dn)# exit

Router(config)# voice register pool 1 ! Enters voice register pool configuration mode
Router(config-register-pool)# id mac 00E1.CB13.0395 ! Explicitly identifies the phone
Router(config-register-pool)# type 7960 ! Defines phone type for the SIP phone being
configured.  Other types are 7942, 7945, 7961, 7962, 7965, 7971
Router(config-register-pool)# number 1 dn 1! Associates phone 1 with directory number 1
Router(config-register-pool)# exit
```

Generate a configuration file.

```
Router(config)# voice register global ! Enters voice register configuration mode
Router(config-register-global)# create profile ! Generates provisioning file
Router(config-register-global)# reset ! Reboots the SIP phone
Router(config-register-global)# exit
```

Cisco Unified CME with SIP Endpoints: SIP Voice Gateway Implementation

The SIP voice gateway is responsible for connecting the branch VoIP network to the PSTN and to the central site telephony network. The following configuration enables VoIP on the network and sets up SIP dial peers between the branch gateway and the destination telephone networks. IP Phones are configured for SIP signaling.

```
Router(config)# voice service voip ! Enters voice service configuration mode
Router(config- voi-srv)# allow-connections SIP to h323 ! Enables calls from SIP endpoint
to h323 endpoint
Router(config-voi-srv)# allow-connections SIP to SIP ! Enables calls between SIP endpoints
```

Cisco Unified CME with SIP Endpoints: Dial Plan Implementation

Ten dial peers were defined for the Services Ready Medium Branch Network: central site, local calls, two 911 emergency services dial peers, voicemail, Auto Attendant, long distance, international calling, and fax pass-through or fax relay. Voice mail, Auto Attendant, and emergency services dial peers are described in the "Cisco Unified CME with SIP Endpoints: Voice Mail and Auto Attendant Integration" section on page 115 and "Cisco Unified CME with SIP Endpoints: Emergency Services Implementation" section on page 116.

To provide automatic dialing without pressing the dial button, apply the following dial plan configuration.

```
Router(config)# voice register dialplan 1 ! Enters dial plan configuration mode
Router(config-register-dialplan)# type 7940-7960-others ! Specifies all phones
Router(config-register-dialplan)# pattern 1 9......... ! Matches outbound PSTN traffic
Router(config-register-dialplan)# pattern 1 4......... ! Matches central site traffic
Router(config-register-dialplan)# exit

Router(config)# voice register pool 1 ! Enters register configuration mode
Router(config-register-pool)# dialplan 1 ! Assigns dial plan to phones
Router(config-register-pool)# exit ! Assigns dial plan to phones

Router(config)# dial-peer voice 1 voip ! Enters dial peer to central site configuration
mode
Router(config-dial-peer)# session protocol sipv2 ! Enables SIP for voicemail communication
Router(config-dial-peer)# dtmf-relay rtp-nte ! Specifies Network Time Protocol method for
relaying pressed digit tones
Router(config-dial-peer)# destination-pattern 408....... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
```

```
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit

Router(config)# dial-peer voice 2 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# destination-pattern 9....... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 3 pots ! Enters dial peer for long distance calls
configuration mode
Router(config-dial-peer)# destination-pattern 91.......... ! Specifies area code prefix
for central site dial peer
Router(config-dial-peer)# prefix 1 ! Prefix that the system adds automatically to the dial
string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 4 pots ! Enters dial peer for international calls
configuration mode
Router(config-dial-peer)# destination-pattern 9011T ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 011 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

When calls over the WAN exceed the maximum allocated bandwidth, they are redirected to PSTN.

```
Router(config)# dial-peer voice 15 pots ! Enters dial peer for PSTN bypass configuration
mode
Router(config-dial-peer)# destination-pattern 408....... ! Specifies destination pattern
Router(config-dial-peer)# port 0/0/23 ! Specifies outgoing/incoming interface for calls
Router(config-dial-peer)# preference 1 ! Sets the dial peer preference order
Router(config-dial-peer)# prefix 408 ! Prefix that the system adds automatically to the
dial string
```

If you are using fax pass-through, apply the following configuration.

```
Router(config)# dial-peer voice 6 voip ! Enters dial peer for fax passthrough
configuration mode
Router(config-dial-peer)# session protocol sipv2 ! Enables SIP for voicemail communication
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-dial-peer)# fax protocol pass-through g711ulaw ! Configures fax passthrough
with G.711 codec
Router(config-peer)# exit
```

If you are using fax relay, apply the following configuration.

```
Router(config)# dial-peer voice 7 voip ! Enters dial peer for fax relay configuration mode
Router(config-dial-peer)# session protocol sipv2 ! Enables SIP for voicemail communication
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-dial-peer)# fax-relay ecm disable ! Disables fax relay ECM
Router(config-dial-peer)# fax rate 9600 ! Selects fax transmission rate
Router(config-dial-peer)# fax protocol t38 ! Sets the T.38 fax relay protocol
Router(config-dial-peer)# codec g711ulaw ! Configures fax relay with G.711 codec
Router(config-peer)# exit
```

Cisco Unified CME with SIP Endpoints: CAC Implementation

Resource Reservation Protocol (RSVP) is not supported with Cisco Unified CME. A limited workaround is possible by setting a limit on the number of voice calls that can be placed over the WAN.

```
Router(config)# dial-peer voice 1 voip ! Enters dial peer to central site configuration 
mode
Router(config-dial-peer)# max-con 36 ! Sets the maximum number of WAN based calls to 36
Router(config-dial-peer)# exit
```

Cisco Unified CME with SIP Endpoints: Transcoding Implementation

Transcoding compresses and decompresses voice streams to match end device capabilities. Transcoding is required when an incoming voice stream is digitized and compressed (by means of a codec) to save bandwidth and the local device does not support that type of compression. Conferencing is not supported with SIP and Cisco Unified CME.

```
Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telephony)# max-ephones 100 ! Sets the maximum number of phones that can 
register with Cisco CME
Router(config-telephony)# max-dn 100 ! Sets the maximum number of directory numbers (two 
for each phone)
Router(config-telphony)# sdspfarm units 4 ! Specifies number of DSP farms that can 
register with SCCP server
Router(config-telphony)# sdspfarm transcode sessions 5 ! Specifies maximum number of 
simultaneous transcoding sessions
Router(config-telphony)# sdspfarm tag 3 TRANSCODE ! Creates DSP farm profile
Router(config-telphony)# exit

Router(config)# voice-card 0 ! Enters DSP farm configuration mode
Router(config-voicecard)# dsp services dspfarm ! Enables DSP services
Router(config-voicecard)# exit

Router(config)# dspfarm profile 3 ! Enters DSP farm profile configuration mode
Router(config-dspfarm-profile)# codec g711ulaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g711alaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729ar8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729abr8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729r8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec pass-through ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# maximum sessions 5 ! Specifies maximum number of 
simultaneous sessions supported by this profile
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit
```

Cisco Unified CME with SIP Endpoints: Music on Hold Implementation

MOH is an audio stream that is played to PSTN and VoIP G.711 or G.729 callers who are placed on hold by phones in a Cisco Unified CME system. This audio stream is intended to reassure callers that they are still connected to their calls.

```
Router(config)# telephony-service ! Enters telephony configuration mode
Router(config-telephony)# moh music-on-hold.au ! Specifies music on hold file
Router(config-telephony)# exit
```

Cisco Unified CME with SIP Endpoints: Voice Mail and Auto Attendant Integration

Voice mail is provided by the Cisco Unity Express service module either in the Advanced Integration Module 2 (AIM2) form factor or the Network Module (NME) form factor. The AIM2 module requires the following configuration. To configure the NME, substitute *Integrated-Service-Engine 2/0* for *Service-Engine 0/1*.

```
Router(config)# interface Service-Engine 0/1 ! Enters Cisco Unity Express configuration
mode
Router(config-if)# ip address 10.0.2.86 255.255.255.252 ! Assigns ip address to the
service engine router interface
Router(config-if)# service-module ip address 10.0.2.85 255.255.255.252 ! Assigns IP
address to service module internal interface
Router(config-if)# service-module ip default-gateway 10.0.2.86 ! Assigns default gateway
for the service module
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# ip route 10.0.2.84 255.255.255.252 Service-Engine 0/1 ! Adds a static
route entry to direct traffic to the module
```

Configure a dial peer for voice mail, because Cisco Unity Express uses SIP as its signaling protocol.

```
Router(config)# dial-peer voice 8 voip ! Enters dial peer for voicemail configuration mode
Router(config-dial-peer)# destination-pattern 5444 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.2.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify ! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit

Router(config)# dial-peer voice 9 voip ! Enters dial peer for autoattendant configuration
mode
Router(config-dial-peer)# destination-pattern 5000 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.2.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit

Router(config)# sip-ua ! Enters SIP user agent configuration mode
Router(config-sip-ua)# mwi-server ipv4:172.16.0.110 expires 3600 port 5060 transport udp
! Sets Cisco Unified Manager address for providing message wait indicator
Router(config-voi-sip)# exit

Router# service-module Service-Engine 0/1 session ! Sessions into the CUE service module

CUE(config)# ccn application voicemail ! Enters voicemail configuration mode
CUE(config-application)# description "Cisco Voicemail" ! Sets user friendly name for
voicemail application
CUE(config-application)# maxsessions 4 ! Sets maximum number of users concurrently
listening to voicemail
CUE(config-application)# exit

CUE(config)# ccn trigger sip phonenumber 5444 ! Assigns number that will trigger voicemail
CUE(config-trigger)# application voicemail ! Assigns voicemail to the call trigger
CUE(config-trigger)# enabled ! Turns the trigger on
CUE(config-trigger)# maxsessions 4 ! Sets maximum number of users concurrently listening
to voicemail
CUE(config-trigger)# exit
CUE(config)# exit
```

Create user mailboxes. Repeat the following steps for all users.

```
CUE# username John create ! Creates mailbox for user John
CUE# configure terminal
CUE(config)# username John phonenumber 5001 ! Asigns mailbox for John to extension
CUE(config)# exit

CUE# configure terminal
CUE(config)# voice mailbox owner John ! Enters configuration mode for voicemail mailbox
CUE(config-mailbox)# description "John's Mailbox" ! Sets user friendly description
CUE(config-mailbox)# enable ! Turns the mailbox on
CUE(config-mailbox)# expiration time 14 ! Sets expiration time for voicemail to two weeks
CUE(config-mailbox)# mailboxsize 600 ! Sets voicemail box size to 10 minutes of messages
CUE(config-mailbox)# messagesize 120 ! Sets maximum message size to 2 minutes
CUE(config-mailbox)# exit
```

Cisco Unified CME with SIP Endpoints: Emergency Services Implementation

The following is the implementation of emergency number calling for North America. The PRI trunk is used for placing emergency calls.

```
Router(config)# dial-peer voice 10 pots ! Enters dial peer for emergency calls
configuration mode
Router(config-dial-peer)# destination-pattern 911 ! Specifies North America emergency
number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 11 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# destination-pattern 9911 ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 911 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

Cisco Unified SRST with SCCP Endpoints Implementation

Cisco Unified SRST provides Cisco Unified CM with fallback support for Cisco IP Phones that are attached to a Cisco router on a branch network. Cisco Unified SRST enables routers to provide call-handling support for Cisco IP Phones when they lose connection to a remote primary, secondary, or tertiary Cisco Unified CM, or when WAN connection is operationally down.

Cisco Unified SRST with SCCP Endpoints: Telephony Service Setup

Configure Cisco Unified SRST at the central site Cisco Unified CM as shown in Figure 23. The Cisco Unified SRST reference name is used in configuring the Cisco Unified SRST device pool as shown in Figure 24.

Figure 23 Cisco Unified SRST Configuration in Cisco Unified CM

Figure 24 Cisco Unified SRST Device Pool Configuration in Cisco Unified CM

Configure the Cisco Unified SRST fallback mode at the branch router.

```
Router(config)# call-manager-fallback ! Enters call manager fallback configuration mode
Router(config-cm-fallback)# ip source-address 10.0.1.2 port 2000 ! Sets IP address for
phone registration
Router(config-cm-fallback)# max-dn 200 dual-line ! Sets the maximum number of directory
numbers and configures dual channel
Router(config-cm-fallback)# max-ephones 100 ! Sets the maximum number of IP Phones
Router(config-cm-fallback)# exit
```

Cisco Unified SRST with SCCP Endpoints: IP Phone Installation and Configuration

In the Services Ready Medium Branch Network, IP Phones are installed by simply connecting them to ports on the access layer switches. Because all the ports offer Power over Ethernet, no additional power cables are necessary. After installation, the phones are configured with a default configuration generated during the telephony setup in the previous section.

```
Router(config)# clock timezone PST -8 ! Sets the timezone for display on IP Phones
Router(config)# call-manager-fallback ! Enters call manager fallback configuration mode
Router(config-cm-fallback)# user-locale US ! Sets the language for display on IP Phones
Router(config-cm-fallback)# system message primary Your current options ! Sets message for
display on IP Phones
Router(config-cm-fallback)# secondary-dialtone 9 ! Provides dial tone for PSTN calls
Router(config-cm-fallback)# call-forward  busy 5444 ! Forwards busy calls to voicemail
Router(config-cm-fallback)# call-forward  noan 5444 timeout 10 ! Forwards busy calls to
voicemail after 10 minutes of ringing
```

```
Router(config-cm-fallback)# dialplan-pattern 1 408555.... extension-length 4 ! Creates
dialplan pattern that expands extension numbers to full E.164 numbers
Router(config-cm-fallback)# transfer-system full-blind ! Transfers calls without
consultation
Router(config-cm-fallback)# transfer-pattern 9.........! Allows transfers for all calls
originating from PSTN
Router(config-cm-fallback)# transfer-pattern 4.........! Allows transfers for all calls
originating in area code starting with "4"
Router(config-cm-fallback)# transfer-system full-consult ! Consults call before transfer
on second line
Router(config-cm-fallback)# call-forward pattern .T ! Allows call forwarding for all calls

Router(config-cm-fallback)# exit
```

Cisco Unified SRST with SCCP Endpoints: H.323 Voice Gateway Implementation

The following configuration enables VoIP on the network and sets up H.323 dial peers between the branch gateway and the destination telephone network, as shown in Figure 25, Figure 26, and Figure 27.

Figure 25 H.323 Gateway Cisco Unified CM Configuration

Figure 26 H.323 Gateway Cisco Unified CM Configuration 2?

Figure 27 H.323 Gateway Cisco Unified CM Configuration for Cisco Unified SRST Mode

Cisco Unified SRST with SCCP Endpoints: Dial Plan Implementation

Twelve dial peers were defined for the Services Ready Medium Branch Network:

- Central site WAN
- Central site PSTN
- Local calls
- Four 911 emergency services dial peers
- Voice mail
- Auto Attendant
- Long distance
- International calling
- Fax pass through or fax relay

Voice mail and emergency services dial peers are described in the“Cisco Unified SRST with SCCP Endpoints: Voice Mail and Auto Attendant Integration” section on page 126 and the “Cisco Unified SRST with SCCP Endpoints: Emergency Services Implementation” section on page 127.

```
Router(config)# dial-peer voice 1 pots ! Enters dial peer for central site calls
Router(config-dial-peer)# destination-pattern 5.... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 1408555 ! Prefix that the system adds automatically to
the dial string
```

```
Router(config-dial-peer)# incoming called-number .T ! Associates dial peer with any
incoming number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

When calls over the WAN exceed the maximum allocated bandwidth, they are redirected to PSTN.

```
Router(config)# dial-peer voice 15 pots ! Enters dial peer for PSTN bypass configuration
mode
Router(config-dial-peer)# destination-pattern 408....... ! Specifies destination pattern
Router(config-dial-peer)# port 0/0/23 ! Specifies outgoing/incoming interface for calls
Router(config-dial-peer)# preference 1 ! Sets the dial peer preference order
Router(config-dial-peer)# prefix 408 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# exit

Router(config)# dial-peer voice 2 voip ! Enters dial peer to central site configuration
mode
Router(config-dial-peer)# dtmf-relay h245-alphanumeric ! Specifies H.245 method for
relaying pressed digit tones
Router(config-dial-peer)# destination-pattern 408....... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-peer)# exit

Router(config)# dial-peer voice 3 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# destination-pattern 9....... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 4 pots ! Enters dial peer for long distance calls
configuration mode
Router(config-dial-peer)# destination-pattern 91.......... ! Specifies area code prefix
for central site dial peer
Router(config-dial-peer)# prefix 1 ! Prefix that the system adds automatically to the dial
string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 5 pots ! Enters dial peer for international calls
configuration mode
Router(config-dial-peer)# destination-pattern 9011T ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 011 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

If using fax pass-through, apply the following configuration.

```
Router(config)# dial-peer voice 6 voip ! Enters dial peer for fax passthrough
configuration mode
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
```

```
Router(config-dial-peer)# fax protocol pass-through g711ulaw ! Configures fax passthrough
with G.711 codec
Router(config-peer)# exit
```

If using fax relay, apply the following configuration.

```
Router(config)# dial-peer voice 7 voip ! Enters dial peer for fax relay configuration mode
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-dial-peer)# fax-relay ecm disable ! Disables fax relay ECM
Router(config-dial-peer)# fax rate 9600 ! Selects fax transmission rate
Router(config-dial-peer)# fax protocol t38 ! Sets the T.38 fax relay protocol
Router(config-dial-peer)# codec g711ulaw ! Configures fax relay with G.711 codec
Router(config-peer)# exit
```

Cisco Unified SRST with SCCP Endpoints: RSVP Implementation

The following implementation applies to Cisco Unified SRST branch voice deployments. Use the following commands on the tunnel interface for DMVPN, WAN primary, and on the WAN interface for GETVPN.

Note On the four T1 WAN links, the maximum bandwidth that can be managed by RSVP is 4550 kp/s.

```
Router(config)# interface Tunnel 1 ! Enters tunnel interface configuration mode
Router(config-if)# ip rsvp bandwidth 8112 ! Sets maximum allowed bandwidth for voice (see
Table 20) plus video (512 kb/s)
Router(config-if)# ip rsvp data-packet classification none ! Turns off per-packet data
processing
Router(config-if)# ip rsvp resource-provider none ! Specifies no resource provider for the
traffic flows
Router(config-if)# ip rsvp policy local identity RSVP-VOICE ! Creates RSVP policy for
voice
Router(config-rsvp-local-policy)# maximum bandwidth group 7600! Sets maximum bandwidth for
voice
Router(config-rsvp-local-policy)# forward all ! Forwards all traffic for this policy
Router(config-rsvp-local-policy)# exit
Router(config-if)# ip rsvp policy local identity RSVP-VIDEO ! Creates RSVP policy for
video
Router(config-rsvp-local-policy)# maximum bandwidth group 512 ! Sets maximum bandwidth for
video
Router(config-rsvp-local-policy)# forward all ! Forwards all traffic for this policy
Router(config-rsvp-local-policy)# exit
Router(config-if)# ip rsvp policy local default ! Default policy for traffic that does not
matchin above identifiers
Router(config-if)# exit

Router(config)# ip rsvp policy identity RSVP-VIDEO policy-locator .*VideoStream.*
! Creates a policy for matching video traffic
Router(config)# ip rsvp policy identity RSVP-VOICE policy-locator .*AudioStream.*
! Creates a policy for matching voice traffic
Router(config)# ip rsvp policy preempt ! Enables preempting of lower reservation by higher
reservation
```

The RSVP policy must be applied on the voice VLAN interface.

```
Branch(config)# interface GigabitEthernet2/0.2 ! Enters gigabit Ethernet sub-interface 2
configuration mode
Router(config-if)# ip rsvp bandwidth ! Enables RSVP on the interface
Router(config-if)# exit
```

Cisco Unified SRST with SCCP Endpoints: Transcoding and Conferencing Implementation

Transcoding compresses and decompresses voice streams to match end device capabilities. Transcoding is required when an incoming voice stream is digitized and compressed (by means of a codec) to save bandwidth and the local device does not support that type of compression.

```
Router(config)# call-manager-fallback ! Enters call manager fallback configuration mode
Router(config-cm-fallback)# max-conferences 3 ! Specifies the maximum number of
simultaneous conferences
Router(config-cm-fallback)# exit

Router(config)# voice-card 0 ! Enters DSP farm configuration mode
Router(config-voicecard)# dsp services dspfarm ! Enables DSP services
Router(config-voicecard)# exit
Router(config)# sccp local GigabitEthernet2/0.2 ! Sets the interface for conferencing and
transcoding to register with CME
Router(config)# sccp ccm  10.0.1.2 identifier 1 version 5.0.1 ! Associates conferencing
and transcoding with CME
Router(config)# sccp ! Enables SCCP globally
Router(config)# sccp ccm group 1 ! Creates SCCP group and enters SCCP configuration mode
Router(config-sccp-ccm)# associate ccm 1 priority 1 ! Associates SCCP group 1 with CME
Router(config-sccp-ccm)# associate profile 3 register CONFERENCE ! Associates DSP farm
profile with with a SCCP group
Router(config-sccp-ccm)# associate profile 2 register TRANSCODE ! Associates DSP farm
profile with with a SCCP group
Router(config-sccp-ccm)# exit

Router(config)# dspfarm profile 2 transcode ! Enters DSP farm profile configuration mode
Router(config-dspfarm-profile)# codec g711ulaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g711alaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729ar8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729abr8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729r8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec pass-through ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# maximum sessions 5 ! Specifies maximum number of
simultaneous sessions supported by this profile
Router(config-dspfarm-profile)# associate application sccp ! Associates SCCP with this DSP
farm profile
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit

Router(config)# dspfarm profile 3 conference ! Enters DSP farm profile configuration mode
Router(config-dspfarm-profile)# codec g711ulaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g711alaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729ar8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729abr8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729r8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729br8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# maximum sessions 3 ! Specifies maximum number of
simultaneous sessions supported by this profile
Router(config-dspfarm-profile)# associate application sccp ! Associates SCCP with this DSP
farm profile
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit
```

Transcoding and conferencing are configured on the remote Cisco Unified CM as shown in Figure 28 and Figure 29.

Figure 28 Transcoding Configuration for Cisco Unified SRST Mode

Figure 29 Conferencing Configuration for Cisco Unified SRST Mode

Cisco Unified SRST with SCCP Endpoints: Music on Hold Implementation

Music on hold (MOH) is an audio stream that is played to PSTN and VoIP G.711 or G.729 callers who are placed on hold by phones in a Cisco Unified CME system. This audio stream is intended to reassure callers that they are still connected to their calls.

```
Router(config)# call-manager-fallback ! Enters call manager fallback configuration mode
Router(config-cm-fallback)# moh music-on-hold.au ! Specifies music on hold file
Router(config-cm-fallback)# multicast moh 239.1.1.1 port 16384 ! Uses multicast for MoH
Router(config-cm-fallback)# exit
```

Cisco Unified SRST with SCCP Endpoints: Voice Mail and Auto Attendant Integration

Voice mail is provided by the Cisco Unity Express service module either in the Advanced Integration Module 2 (AIM2) form factor or the Network Module (NME) form factor. The AIM2 module requires the following configuration. To configure the NME, substitute *Integrated-Service-Engine 2/0* for *Service-Engine 0/1*.

```
Router(config)# interface service-engine 0/1 ! Enters Cisco Unity Express configuration
mode
Router(config-if)# ip address 10.0.2.86 255.255.255.252 ! Assigns ip address to the
service engine router interface
Router(config-if)# service-module ip address 10.0.2.85 255.255.255.252 ! Assigns IP
address to service module internal interface
Router(config-if)# service-module ip default-gateway 10.0.2.86 ! Assigns default gateway
for the service module
Router(config-if)# zone-member security Private ! Assigns Cisco Unity Express to private
security zoneRouter(config-if)# no shutdown
Router(config-if)# exit
Router(config)# ip route 10.0.2.84 255.255.255.252 Service-Engine 0/1 ! Adds a static
route entry to direct traffic to the module
```

Configure a dial peer for voice mail because Cisco Unity Express uses SIP as its signaling protocol.

```
Router(config)# dial-peer voice 8 voip ! Enters dial peer for voicemail configuration mode
Router(config-dial-peer)# destination-pattern 5444 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.2.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit

Router(config)# dial-peer voice 9 voip ! Enters dial peer for autoattendant configuration
mode
Router(config-dial-peer)# destination-pattern 5000 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.2.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit
```

The local Cisco Unity Express software must be registered with the Cisco Unified CM software at the central site. The following reference provides implementation details:

http://cisco.com/en/US/products/sw/voicesw/ps5520/products_configuration_example09186a0080289ef0.shtml

Additional Cisco Unity Express configuration is performed through a web-based user interface, as shown in Figure 17 through Figure 22.

Cisco Unified SRST with SCCP Endpoints: Emergency Services Implementation

The following provides implementation of emergency number calling for North America. The PRI trunk is used to place emergency calls. Each 911 call is selectively routed to the closest Public Safety Answering Point (PSAP), based on the caller's location. In addition, the caller's phone number and address automatically display on a terminal at the PSAP. The PSAP can quickly dispatch emergency help, even if the caller is unable to communicate the caller's location. Also, if the caller disconnects prematurely, the PSAP has the information it needs to contact the 911 caller.

```
Router(config)# voice emergency response location 1 ! Enters emergency response
configuration mode
Router(cfg-emrgncy-resp-location)# elin 1 4085555150 ! Specifies ELIN number provided by
PSAP
Router(cfg-emrgncy-resp-location)# name Bdlg 22, Floor 2 ! Internal location name
Router(cfg-emrgncy-resp-location)# subnet 1 10.0.1.0 255.255.255.0 ! Assigns Voice VLAN
subnet as origination of the emergency call
Router(cfg-emrgncy-resp-location)# subnet 2 10.0.4.0 255.255.255.0 ! Assigns backup Voice
VLAN subnet as origination of the emergency call
Router(cfg-emrgncy-resp-location)# exit

Router(config)# dial-peer voice 10 pots ! Enters dial peer for emergency calls
configuration mode
Router(config-dial-peer)# emergency response zone ! Replaces local extension with ELIN
number
Router(config-dial-peer)# destination-pattern 911 ! Specifies North America emergency
number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 11 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# emergency response zone ! Replaces local extension with ELIN
number
Router(config-dial-peer)# destination-pattern 9911 ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 911 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 12 pots ! Enters dial peer for ELIN callback configuration
mode
Router(config-dial-peer)# incoming called-number 4085555150 ! Specifies ELIN number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# emergency response callback ! Identifies the ELIN dial peer
Router(config-peer)# exit

Router(config)# dial-peer voice 13 pots ! Enters dial peer for ELIN callback configuration
mode
Router(config-dial-peer)# incoming called-number 4085555150 ! Specifies ELIN number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# emergency response callback ! Identifies the ELIN dial peer
Router(config-peer)# exit
```

Cisco Unified SRST with SIP Endpoints Implementation

- Cisco Unified SRST with SIP Endpoints: Telephony Service Setup, page 128
- Cisco Unified SRST with SIP Endpoints: Cisco Unified SRST Fallback Mode at the Branch Router, page 130
- Cisco Unified SRST with SIP Endpoints: IP Phone Installation and Configuration, page 131
- Cisco Unified SRST with SIP Endpoints: SIP Voice Gateway Implementation, page 131
- Cisco Unified SRST with SIP Endpoints: Dial Plan Implementation, page 133
- Cisco Unified SRST with SIP Endpoints: RSVP Implementation, page 135
- Cisco Unified SRST with SIP Endpoints: Transcoding and Conferencing Implementation, page 135
- Cisco Unified SRST with SIP Endpoints: Music on Hold Implementation, page 138
- Cisco Unified SRST with SIP Endpoints: Voice Mail and Auto Attendant Integration, page 138
- Cisco Unified SRST with SIP Endpoints: Emergency Services Implementation, page 139

Cisco Unified SRST provides Cisco Unified CM with fallback support for Cisco IP Phones that are attached to a Cisco router on a branch network. Cisco Unified SRST enables routers to provide call-handling support for Cisco IP Phones when they lose connection to a remote primary, secondary, or tertiary Cisco Unified CM, or when WAN connection is operationally down.

Cisco Unified SRST with SIP Endpoints: Telephony Service Setup

Configure the Cisco Unified SRST at Cisco Unified CM of the central site, as shown in Figure 30. The Cisco Unified SRST reference name is used in configuring Cisco Unified SRST device pools as shown in Figure 31.

Figure 30 Cisco Unified SRST Configuration in Cisco Unified CM

Figure 31 Cisco Unified SRST Device Pool Configuration in Cisco Unified CM

Cisco Unified SRST with SIP Endpoints: Cisco Unified SRST Fallback Mode at the Branch Router

```
Router(config)# voice register global ! Enters voice configuration mode
Router(config-register-global)# max-pool 100 ! Sets the maximum number of SIP Phones
Router(config-register-global)# max-dn 200 ! Sets the maximum number of directory numbers
(two for each phone)
Router(config-register-global)# system message Your current options ! Sets message for
display on IP Phones
Router(config-register-global)# dialplan-pattern 1 4085555... extension-length 4 ! Creates
dialplan pattern that expands extension numbers to full E.164 numbers
Router(config-register-global)# exit

Router(config)# voice register pool 1 ! Enters voice register pool configuration mode
Router(config-register-pool)# id network 10.0.1.0 255.255.255.0 ! Identifies Voice VLAN
with SIP Phones
Router(config-register-pool)# proxy 172.16.0.20 preference 1 monitor probe icmp-ping !
Defines remote proxy dialpeer and method to monitor the state of the peer
Router(config-register-pool)# call-forward  b2bua busy 5444 ! Forwards busy calls to
voicemail
Router(config-register-pool)# call-forward  b2bua noan 5444 timeout 10 ! Forwards busy
calls to voicemail after 10 minutes of ringing
Router(config-register-pool)# codec g711ulaw ! Sets the codec for local calls
Router(config-register-pool)# exit
```

Cisco Unified SRST with SIP Endpoints: IP Phone Installation and Configuration

In Cisco Unified SRST mode, the Cisco Unified CM controls IP Phone firmware installation and configuration.

Cisco Unified SRST with SIP Endpoints: SIP Voice Gateway Implementation

The following configuration enables VoIP on the network and sets up SIP dial peers between the branch gateway and the destination telephone networks, as shown in Figure 32, Figure 33, and Figure 34.

Figure 32 SIP Trunk Cisco Unified CM Configuration (1 of 3)

Figure 33 SIP Trunk Cisco Unified CM Configuration (2 of 3)

Figure 34 SIP Trunk Cisco Unified CM Configuration (3 of 3)

Cisco Unified SRST with SIP Endpoints: Dial Plan Implementation

Twelve dial peers were defined for the Services Ready Medium Branch Network: central site WAN, central site PSTN, local calls, four 911 emergency services dial peers, voice mail, auto attendant, long distance, international calling and fax pass-through or fax relay. Voice mail, auto attendant and emergency services dial peers are described in the "Cisco Unified SRST with SIP Endpoints: Voice Mail and Auto Attendant Integration" section on page 138 and in the "Cisco Unified SRST with SIP Endpoints: Emergency Services Implementation" section on page 139.

```
Router(config)# dial-peer voice 1 pots ! Enters dial peer for central site calls
Router(config-dial-peer)# destination-pattern 5.... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 1408555 ! Prefix that the system adds automatically to
the dial string
Router(config-dial-peer)# incoming called-number .T ! Associates dial peer with any
incoming number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 2 voip ! Enters dial peer to central site configuration
mode
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# dtmf-relay rtp-nte ! Specifies Network Time Protocol method for
relaying pressed digit tones
Router(config-dial-peer)# destination-pattern 408....... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
```

```
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit

Router(config)# dial-peer voice 3 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# destination-pattern 9....... ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 4 pots ! Enters dial peer for long distance calls
configuration mode
Router(config-dial-peer)# destination-pattern 91.......... ! Specifies area code prefix
for central site dial peer
Router(config-dial-peer)# prefix 1 ! Prefix that the system adds automatically to the dial
string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 5 pots ! Enters dial peer for international calls
configuration mode
Router(config-dial-peer)# destination-pattern 9011T ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 011 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
```

When calls over the WAN exceed the maximum allocated bandwidth, they are redirected to PSTN.

```
Router(config)# dial-peer voice 15 pots ! Enters dial peer for PSTN bypass configuration
mode
Router(config-dial-peer)# destination-pattern 408....... ! Specifies destination pattern
Router(config-dial-peer)# port 0/0/23 ! Specifies outgoing/incoming interface for calls
Router(config-dial-peer)# preference 1 ! Sets the dial peer preference order
Router(config-dial-peer)# prefix 408 ! Prefix that the system adds automatically to the
dial string
```

If using fax pass-through, apply the following configuration.

```
Router(config)# dial-peer voice 6 voip ! Enters dial peer for fax passthrough
configuration mode
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-dial-peer)# fax protocol pass-through g711ulaw ! Configures fax passthrough
with G.711 codec
Router(config-peer)# exit
```

If using fax relay, apply the following configuration.

```
Router(config)# dial-peer voice 7 voip ! Enters dial peer for fax relay configuration mode
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# destination-pattern 4085555333 ! Specifies local number of fax
machine
Router(config-dial-peer)# session target ipv4:172.16.200.10 ! Specifies central site dial
peer address
Router(config-dial-peer)# fax-relay ecm disable ! Disables fax relay ECM
Router(config-dial-peer)# fax rate 9600 ! Selects fax transmission rate
Router(config-dial-peer)# fax protocol t38 ! Sets the T.38 fax relay protocol
Router(config-dial-peer)# codec g711ulaw ! Configures fax relay with G.711 codec
Router(config-peer)# exit
```

Cisco Unified SRST with SIP Endpoints: RSVP Implementation

The following implementation applies to Cisco Unified SRST branch voice deployments. Apply the following commands on the tunnel interface for DMVPN, WAN primary, and for the WAN interface for GETVPN.

```
Router(config)# interface Tunnel 1 ! Enters tunnel interface configuration mode
Router(config-if)# ip rsvp bandwidth 8112 ! Sets maximum allowed bandwidth for voice (see
Table 18) plus video (512 Mbps)
Router(config-if)# ip rsvp data-packet classification none ! Turns off per-packet data
processing
Router(config-if)# ip rsvp resource-provider none ! Specifies no resource provider for the
traffic flows
Router(config-if)# ip rsvp policy local identity RSVP-VOICE ! Creates RSVP policy for
voice
Router(config-rsvp-local-policy)# maximum bandwidth group 7600! Sets maximum bandwidth for
voice
Router(config-rsvp-local-policy)# forward all ! Forwards all traffic for this policy
Router(config-rsvp-local-policy)# exit
Router(config-if)# ip rsvp policy local identity RSVP-VIDEO ! Creates RSVP policy for
video
Router(config-rsvp-local-policy)# maximum bandwidth group 512 ! Sets maximum bandwidth for
video
Router(config-rsvp-local-policy)# forward all ! Forwards all traffic for this policy
Router(config-rsvp-local-policy)# exit
Router(config-if)# ip rsvp policy local default ! Default policy for traffic that does not
matchin above identifiers
Router(config-if)# exit

Router(config)# ip rsvp policy identity RSVP-VIDEO policy-locator .*VideoStream.* !
Creates a policy for matching video traffic
Router(config)# ip rsvp policy identity RSVP-VOICE policy-locator .*AudioStream.* !
Creates a policy for matching voice traffic
Router(config)# ip rsvp policy preempt ! Enables preempting of lower reservation by higher
reservation
```

The RSVP policy must be applied on the voice VLAN interface.

```
Branch(config)# interface GigabitEthernet2/0.2 ! Enters gigabit Ethernet sub-interface 2
configuration mode
Router(config-if)# ip rsvp bandwidth ! Enables RSVP on the interface
Router(config-if)# exit
```

Cisco Unified SRST with SIP Endpoints: Transcoding and Conferencing Implementation

Transcoding compresses and decompresses voice streams to match end device capabilities. Transcoding is required when an incoming voice stream is digitized and compressed (by means of a codec) to save bandwidth and the local device does not support that type of compression. Transcoding and conferencing are configured on the Cisco Call Manager of the central site, as shown in Figure 35 and Figure 36.

```
Router(config)# voice-card 0 ! Enters DSP farm configuration mode
Router(config-voicecard)# dsp services dspfarm ! Enables DSP services
Router(config-voicecard)# exit
Router(config)# sccp local GigabitEthernet2/0.2 ! Sets the interface for conferencing and
transcoding to register with CME
Router(config)# sccp ccm  10.0.1.2 identifier 1 version 5.0.1 ! Associates conferencing
and transcoding with CME
```

```
Router(config)# sccp ! Enables SCCP globally
Router(config)# sccp ccm group 1 ! Creates SCCP group and enters SCCP configuration mode
Router(config-sccp-ccm)# associate ccm 1 priority 1 ! Associates SCCP group 1 with CME
Router(config-sccp-ccm)# associate ccm 2 priority 2 ! Associates SCCP group 2 with CME
Router(config-sccp-ccm)# associate profile 3 register CONFERENCE ! Associates DSP farm
profile with with a SCCP group
Router(config-sccp-ccm)# associate profile 2 register TRANSCODE ! Associates DSP farm
profile with with a SCCP group
Router(config-sccp-ccm)# exit

Router(config)# dspfarm profile 2 transcode ! Enters DSP farm profile configuration mode
Router(config-dspfarm-profile)# codec g711ulaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g711alaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729ar8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729abr8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729r8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec pass-through ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# maximum sessions 5 ! Specifies maximum number of
simultaneous sessions supported by this profile
Router(config-dspfarm-profile)# associate application sccp ! Associates SCCP with this DSP
farm profile
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit

Router(config)# dspfarm profile 3 conference ! Enters DSP farm profile configuration mode
Router(config-dspfarm-profile)# codec g711ulaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g711alaw ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729ar8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729abr8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729r8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# codec g729br8 ! Specifies codec supported by DSP farm
Router(config-dspfarm-profile)# maximum sessions 3 ! Specifies maximum number of
simultaneous sessions supported by this profile
Router(config-dspfarm-profile)# associate application sccp ! Associates SCCP with this DSP
farm profile
Router(config-dspfarm-profile)# no shutdown
Router(config-dspfarm-profile)# exit
```

Figure 35 Transcoding Configuration for Cisco Unified SRST Mode

Figure 36 Conferencing Configuration for Cisco Unified SRST Mode

Cisco Unified SRST with SIP Endpoints: Music on Hold Implementation

Music on hold (MOH) is implemented at the Unified Call Manager at the central site. Please see the following instructions to implement MOH in Cisco Unified CM:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/6_1_1/ccmfeat/fsmoh.html

Cisco Unified SRST with SIP Endpoints: Voice Mail and Auto Attendant Integration

Voice mail is provided by the Cisco Unity Express service module either in the Advanced Integration Module 2 (AIM2) form factor or the Network Module (NME) form factor. The AIM2 module requires the following configuration. To configure the NME, substitute *Integrated-Service-Engine 2/0* for *Service-Engine 0/1*.

```
Router(config)# interface Service-Engine 0/1 ! Enters Cisco Unity Express configuration
mode
Router(config-if)# ip address 10.0.2.86 255.255.255.252 ! Assigns IP address to the
service engine router interface
Router(config-if)# service-module ip address 10.0.2.85 255.255.255.252 ! Assigns IP
address to service module internal interface
Router(config-if)# service-module ip default-gateway 10.0.2.86 ! Assigns default gateway
for the service module
Router(config-if)# zone-member security Private ! Assigns Cisco Unity Express to private
security zone
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# ip route 10.0.2.84 255.255.255.252 Service-Engine 0/1 ! Adds a static
route entry to direct traffic to the module
```

Configure a dial peer for voice mail, because Cisco Unity Express uses SIP as its signaling protocol.

```
Router(config)# dial-peer voice 8 voip ! Enters dial peer for voicemail configuration mode
Router(config-dial-peer)# destination-pattern 5444 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.2.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit

Router(config)# dial-peer voice 9 voip ! Enters dial peer for autoattendant configuration 
mode
Router(config-dial-peer)# destination-pattern 5000 ! Specifies mailbox extension
Router(config-dial-peer)# session target ipv4:10.0.2.85 ! Specifies voicemail address
Router(config-dial-peer)# session protocol sipv2! Enables SIP for voicemail communication
Router(config-dial-peer)# codec g711ulaw ! Specifies codec for voicemail messages
Router(config-dial-peer)# b2bua ! Enables SIP to SCCP forwarding
Router(config-dial-peer)# dtmf-relay sip-notify! Specifies DTMF relay method
Router(config-dial-peer)# no vad ! Disables voice activity detection
Router(config-peer)# exit
```

The local Cisco Unity Express software must be registered with Cisco Unified CM software at the central site. The following reference provides implementation details:

http://cisco.com/en/US/products/sw/voicesw/ps5520/products_configuration_example09186a0080289ef0.shtml

Additional Cisco Unity Express configuration is performed through a web-based user interface, as shown in Figure 17 through Figure 22.

Cisco Unified SRST with SIP Endpoints: Emergency Services Implementation

The following example implements emergency number calling for North America. The PRI trunk is used for placing emergency calls. Each 911 call is selectively routed to the closest PSAP based on the caller's location. In addition, the caller's phone number and address automatically display on a terminal at the PSAP. The PSAP can quickly dispatch emergency help, even if the caller is unable to communicate the caller's location. Also, if the caller disconnects prematurely, the PSAP has the information it needs to contact the 911 caller.

```
Router(config)# voice emergency response location 1 ! Enters emergency response 
configuration mode
Router(cfg-emrgncy-resp-location)# elin 1 4085555150 ! Specifies ELIN number provided by 
PSAP
Router(cfg-emrgncy-resp-location)# subnet 1 10.0.1.0 255.255.255.0 ! Assigns Voice VLAN 
subnet as origination of the emergency call
Router(cfg-emrgncy-resp-location)# subnet 2 10.0.4.0 255.255.255.0 ! Assigns backup Voice 
VLAN subnet as origination of the emergency call

Router(cfg-emrgncy-resp-location)# exit

Router(config)# dial-peer voice 10 pots ! Enters dial peer for emergency calls 
configuration mode
Router(config-dial-peer)# emergency response zone ! Replaces local extension with ELIN 
number
Router(config-dial-peer)# destination-pattern 911 ! Specifies North America emergency 
number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit
Router(config)# dial-peer voice 11 pots ! Enters dial peer for local area calls
configuration mode
Router(config-dial-peer)# emergency response zone ! Replaces local extension with ELIN
number
Router(config-dial-peer)# destination-pattern 9911 ! Specifies area code prefix for
central site dial peer
Router(config-dial-peer)# prefix 911 ! Prefix that the system adds automatically to the
dial string
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# port 0/0/0:23 ! Specifies outgoing/incoming interface for calls
Router(config-peer)# exit

Router(config)# dial-peer voice 12 pots ! Enters dial peer for ELIN callback configuration
mode
Router(config-dial-peer)# incoming called-number 4085555150 ! Specifies ELIN number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# emergency response callback ! Identifies the ELIN dial peer
Router(config-peer)# exit

Router(config)# dial-peer voice 13 pots ! Enters dial peer for ELIN callback configuration
mode
Router(config-dial-peer)# incoming called-number 4085555150 ! Specifies ELIN number
Router(config-dial-peer)# direct-inward-dial ! Enables DID numbers
Router(config-dial-peer)# emergency response callback ! Identifies the ELIN dial peer
Router(config-peer)# exit
```

Optimization Services Implementation

Cisco WAAS Implementation

In the Services Ready Medium Branch Network, the Cisco NME-WAE-522 network module was used to optimize the Common Internet File System (CIFS), FTP, and HTTP traffic.

Two types of configuration are applied to devices that run Cisco Wide Area Application Services (Cisco WAAS):

- Router and Cisco WAE module configuration
- Central manager configuration

After the router and module configurations are complete, the Cisco Wide Area Application Engine (Cisco WAE) module can be registered with the central manager. Registration with the central manager requires that all router configuration steps be complete, and that the Cisco WAE be able to connect to the central manager. After the Cisco WAE has been registered and activated with the central manager, all additional configuration options can be set through the central manager device groups.

The central manager configuration provides the remaining configuration for the entire Cisco WAAS deployment. The central manager configuration options can be applied at the device or device group level. To simplify the deployment and management of the Cisco WAAS solution, the Services Ready Medium Branch Network uses device groups as the primary central manager configuration method.

Router and Cisco WAE Module Configuration

The router provides Cisco Web Cache Communication Protocol (Cisco WCCP) interception points for Cisco WAAS. Cisco WCCP redirection allows the router to redirect traffic to Cisco WAAS for optimization. Various methods of interception and redirection are supported by routers and switches. Redirection methods depend on the speed requirements and the router or switch platform. This deployment uses both generic router encapsulation (GRE) redirection and Layer 2 (L2) redirection.

The loopback interface on the router is essential for identifying the router ID. Although any IP address can be used to identify the router ID, the loopback interface is preferred over the physical interfaces. Loopback interfaces are always available, and there are no physical ties to them. Other routing protocols also use loopback interfaces as the preferred method for naming the router ID. If the IP address is tied to a specific physical interface, and the physical interface fails, then the IP address becomes unavailable, causing unexpected problems for the Cisco WCCP groups.

The Cisco WCCPv2 services 61 and 62, also known as *TCP promiscuous mode services*, allow the Cisco WCCP to transparently intercept and redirect traffic to the Cisco WAE module. Service 61 redirects ingress traffic, and service 62 redirects egress traffic. Services 61 and 62 are both needed to redirect bidirectional traffic flow. Passwords should be assigned to Cisco WCCP groups to prevent rogue traffic interception and redirection.

```
Branch(config)# ip wccp 61 ! Enables WCCP services
Branch(config)# ip wccp 62 ! Enables WCCP services
Branch(config)# ip inspect WAAS enable ! Enables inspection of packets coming from WAE
Branch(config)# interface Integrated-Service-Engine 1/0 ! Enters WAE module configuration
mode
Branch(config-if)# ip address 10.0.2.90 255.255.255.252 ! Assigns IP address to the
backplane interface
Branch(config-if)# ip wccp redirect exclude in ! Excludes packets received on this
interface from redirection to prevent a traffic loop
Branch(config-if)# zone-member security Private ! Assigns the interface to a private zone
Branch(config-if)# service-module ip address 10.0.2.89 255.255.255.252 ! Assigns IP
address to service module internal interface
Branch(config-if)# service-module ip default-gateway 10.0.2.90 ! Assigns default gateway
for the service module
Branch(config-if)# no keepalive ! Disables keep alive for the interface
Branch(config-if)# exit
Router(config)# ip route 10.0.2.88 255.255.255.252 Integrated-Service-Engine 1/0 ! Adds a
static route entry to direct traffic to the module
```

Apply WCCP redirection on WAN, Tunnel, and LAN interfaces

```
Branch(config)# interface Serial3/0.1 point-to-point ! Enters Tunnel interface
configuration mode
Branch(config)# ip wccp 62 redirect in ! Enables WCCP redirection on the WAN interface

Branch(config)# interface Tunnel1 ! Enters Tunnel interface configuration mod
Branch(config)# ip wccp 62 redirect in ! Enables WCCP redirection on the Tunnel interface

Branch(config)# interface GigabitEthernet2/0.1 ! Enters Tunnel interface configuration
mode
Branch(config)# ip wccp 61 redirect in ! Enables WCCP redirection on the Tunnel interface
```

Configurations for LAN, WAN, and tunnel interfaces are provided in the "WAN Services Implementation" section on page 4, the "LAN Services Implementation" section on page 10, and the "Security Services Implementation" section on page 44.

Additional Cisco WAE–Application Accelerator Configuration

Additional commands are necessary to complete the Cisco WAE implementation.

```
Router(config)# service-module integrated-Service-Engine 1/0 session ! Sessions into the
WAE service module
Trying 10.0.2.90, 2066 ... Open



Cisco Wide Area Application Engine Console

Username: admin
Password:
System Initialization Finished.
WAE(config)# device mode application-accelerator ! Sets the WAE module to application
acceleration mode (the default)
WAE(config)# primary-interface GigabitEthernet 1/0 ! Sets the primary interface for
traffic interception and delivery
WAE(config)# ip name-server 172.16.0.70 ! Assigns central site DNS server for the module
WAE(config)# ntp server 172.16.0.60! Assigns central site NTP server for the module
WAE(config)# central-manager address 172.16.100.1 ! Assigns the Central Manager for the
module
WAE(config)# wccp router-list 1 10.0.2.90 ! Adds the router to the WCCPv2 router list
WAE(config)# wccp tcp-promiscuous router-list-num 1 ! Enables TCP promiscuous mode to
accept all traffic on the router’s primary interface
```

The Cisco WCCP configuration for TCP promiscuous mode services 61 and 62 succeeded. The Cisco WCCP configuration for TCP promiscuous mode services succeeded. Remember to configure Cisco WCCP services 61 and 62 on the corresponding router.

```
WAE(config)# wccp version 2 ! Enables WCCP version 2
WAE(config)# cms enable ! Initializes the local database and connects to the central
manager
```

The following traffic interception policies can be automatically configured from the Cisco WAE central manager. The CLI version of these policies is provided for demonstration purposes and as a starting point for customization.

```
WAE(config)# policy-engine application name File-Transfer ! Creates a new application name
for FTP traffic
WAE(config)# policy-engine application name WEB ! Creates a new application name for HTTP
traffic
WAE(config)# policy-engine application name WAFS ! Creates a new application name for file
system traffic
WAE(config)# policy-engine application classifier FTP-Control ! Creates application
classifier for FTP control traffic
WAE(config-app-cls)# match dst port eq 21 ! Matches traffic with destination port 21
WAE(config-app-cls)# exit
WAE(config-pol-eng-app)# exit
WAE(config)# policy-engine application classifier FTP-Data ! Creates application
classifier for FTP data traffic
WAE(config-app-cls)# match dst port eq 20 ! Matches traffic with destination port 20
WAE(config-app-cls)# exit
WAE(config-pol-eng-app)# exit
WAE(config)# policy-engine application classifier HTTP ! Creates application classifier
for HTTP traffic
WAE(config-app-cls)# match dst port eq 80 ! Matches traffic with destination port 80
WAE(config-app-cls)# match dst port eq 8080 ! Matches traffic with destination port 8080
WAE(config-app-cls)# match dst port eq 8000 ! Matches traffic with destination port 8000
WAE(config-app-cls)# match dst port eq 8001 ! Matches traffic with destination port 8001
WAE(config-app-cls)# match dst port eq 3128 ! Matches traffic with destination port 3128
WAE(config-app-cls)# exit
WAE(config-pol-eng-app)# exit
WAE(config)# policy-engine application classifier CIFS ! Creates application classifier
for CIFS traffic
WAE(config-app-cls)# match dst port eq 139 ! Matches traffic with destination port as 139
WAE(config-app-cls)# match dst port eq 445 ! Matches traffic with destination port as 445
WAE(config-app-cls)# exit
WAE(config-pol-eng-app)# exit
WAE(config)# policy-engine application map basic name File-Transfer classifier FTP-Control
action pass-through ! Assigns FTP application to a classifier and specifies the action to
be taken for matching FTP control traffic
WAE(config)# policy-engine application map basic name File-Transfer classifier FTP-Data
action optimize full ! Assigns FTP application to a classifier and specifies the action to
be taken for matching FTP data traffic
WAE(config)# policy-engine application map basic name Web classifier HTTP action optimize
full ! Assigns HTTP application to a classifier and specifies the action to be taken for
matching HTTP traffic
WAE(config)# policy-engine application map basic name WAFS classifier CIFS action optimize
full accelerate cifs-adaptor ! Assigns WAFS application to a classifier and specifies the
action to be taken for matching CIFS traffic. Uses CIFS specific application adaptor
WAE(config)# policy-engine application map adaptor WAFS transport name WAFS All action
optimize full ! Assigns WAFS application to a classifier and specifies the action to be
taken for matching CIFS traffic
```

Activating the Application Accelerators

For security purposes, Cisco WAEs that are being added to the Cisco WAAS network need to be approved by the Cisco WAAS network administrator. This security feature prevents unauthorized devices from joining the Cisco WAAS network. This section provides steps for activating all the inactive devices.

To activate the devices, from the Cisco WAAS Central Manager window, choose **Devices** > **Devices**.

1. In the taskbar, click the **Activate All Inactive WAEs** icon, shown in the red box in Figure 37, to activate the two inactive Cisco WAEs.

Figure 37 Devices Window

2. The Activate All Inactive WAE window appears, as shown in Figure 38. By default, the **Create a new location for each inactive WAE** option is chosen.

Figure 38 Activating Inactive Cisco WAEs

3. Click **Submit** at the bottom of the page.

4. When a Transaction Warning dialog box appears, click **OK**, and then click **Submit**. The current state of the core and edge Cisco WAEs is now listed as pending instead of inactive, as shown in the red box in the middle of Figure 39. Notice in the red box at the top of the Figure 39 that the system status has changed to orange, with two devices reporting Major.

Figure 39 Pending Devices

5. After a few minutes, all devices show Online in the Status column, as shown in Figure 40.

Figure 40 Online Devices

Cisco WAE–Central Manager Implementation

The central manager is the management component of Cisco WAAS. The central manager provides a GUI for configuration, monitoring, and management of multiple branch-office and data center Cisco WAEs. The central manager can scale to support thousands of Cisco WAE devices for large-scale deployments. The central manager must be used in order to make configuration changes through the web interface. If the central manager fails, the Cisco WAEs continue to function; however, changes cannot be made using the web pages on the central manager until the central manager comes back online.

The Cisco WAEs need to connect to the central manager at the initial setup. The registration process adds the Cisco WAE to the central manager and initializes the local Cisco WAE database. When disk encryption on the Cisco WAE is enabled, the central manager must be available to distribute the encryption key if the Cisco WAE reboots.

Centralized reporting can be obtained from the central manager. Individually, the Cisco WAEs provide basic statistics through the CLI and local-device GUI. Systemwide application statistics are available from the central manager GUI. Detailed reports such as total traffic reduction, application mix, and pass-through traffic are available from the central manager GUI.

```
WAE-CM(config)# device mode central-manager ! Sets the WAE device to central manager mode.
The device is set to application acceleration by default
WAE-CM(config)# primary-interface GigabitEthernet 1/0 ! Sets the primary interface for
traffic interception and delivery
WAE-CM(config)# interface GigabitEthernet 1/0 ! Enters gigabit Ethernet configuration mode
for the specified port
WAE-CM(config-if)# ip address 172.16.100.1 255.255.255.0 ! Assigns IP address for the
interface
WAE-CM(config-if)# no shutdown
The interface was up.
WAE-CM(config-if)# exit
WAE-CM(config)# ip default-gateway 192.168.0.2 ! Assigns default gateway for the central
manager
WAE-CM(config)# ntp server 172.16.0.60 ! Assigns NTP server for the central manager
WAE-CM(config)# cms enable ! Starts centralized management service
```

Verify that the Cisco WAAS central manager process has successfully started by using an Internet Explorer browser to go to the following URL to start the Cisco WAAS Central Manager GUI shown in Figure 41:

https://cm_server_ip or host_name:8443

Figure 41 Cisco WAAS Central Manager GUI

1. Log in using the following default credentials:

   Username: admin

   Password: default

   The Devices window shown in Figure 42 appears.

Figure 42 Devices Window

   For ease of use and to start collecting statistics earlier, you need to change a few parameters. In the following steps, you extend the central manager session timeout interval and modify the intervals by which the Cisco WAAS central manager or Cisco WAE pulls or pushes data to and from the Cisco WAAS Central Manager.

2. Choose **System** > **Configuration**. The Config Properties window shown in Figure 43 appears.

Figure 43 Config Properties Window

3. Choose **ALL** from the Rows drop-down list shown in the red box in Figure 43.
4. Click the **Edit** icon next to the parameter to change each of the parameters in the red boxes 2 to 5 in Figure 43 to the following values:

   cdm.session.timeout: 100

   System.datafeed.pollRate: 60

   System.healthmonitor.collectRate: 30

   System.monitoring.collectRate: 60

Caveats

- Zone-based firewall does not support inspection of SIP and SCCP in releases earlier than Cisco IOS Release 12.4(20)T. See DDTS CSCsm79679.
- Zone-based firewall does not support stateful switchover.
- Message waiting indicator (MWI) does not work during router failover.
- Cisco Unified CME does not work with HSRP.
- Cisco web Cache Communication Protocol (Cisco WCCP) version 2 is not Virtual Routing and Forwarding (VRF) aware and does not work if multiple VRF interfaces (VRF-lite) are configured on the customer edge (CE) router.
- Call preservation is not supported during HSRP. Only local IP Phone calls may be preserved.
- Traffic shaping is not supported over virtual access interfaces with PPP over ATM. See DDTS CSCsm77478.
- VRF-aware IP SLA is not supported in releases earlier than Cisco IOS Release 12.4(20)T.

- Bidirectional Forwarding Detection (BFD) is supported only on Gigabit Ethernet interfaces. Support for additional WAN encapsulations such as Frame Relay and PPP is planned for future releases.
- GETVPN is not VRF aware in releases earlier than Cisco IOS Release 12.4(20)T.
- When registered to Cisco Unified CME, the Cisco Unified IP Conference Station 7936 running firmware version 1.1 continues to display message prompts such as “hold” and “enter number” after the call has ended. See DDTS CSCsm61235.