Cisco Solutions for Financial and Branch Banking— Design and Deployment Guide

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

Cisco Solutions for Financial and Branch Banking

CONTENTS

CHAPTER 1

Solution Overview

Revised: August 6th, 2010

Cisco® Validated Designs (CVDs) are network architecture solutions that are created so customers can deploy their networks with confidence. This CVD is based on financial industry requirements with a specific focus on branch banking. It tests multiple technologies over multiple topologies, as well as Cisco Borderless Networks and EnergyWise. These validated designs give the financial and branch banking industry the ability to tackle key concerns, such as competitive consolidations, diverse branch sizes and needs, lower operating costs, rapid deployment of micro-branches and ATMs, high availability, code stability, and new service deployment. All of these areas were simultaneously tested and include direct feedback from banking customers.

The financial and branch banks face many challenges, some of which are:

- Buyouts and consolidations
- Diverse office sizes and needs
- High operating costs
- Rapid deployment of micro-branches and ATMs
- High availability and code stability
- Server consolidation
- New Service Deployment
- Compliance issues

These challenges require a specific feature set assembled in a value-added way to help reduce the business impacts. This validated design assures that multiple IOS features can operate simultaneously in the manner promised by Cisco. Before releasing this CVD, financial branch-based tests were performed over a variety of topologies with a wide range of features ranging from:

- Diverse sets of WAN interfaces: nXT1, T3, 3G, Ethernet, nX56k Frame Relay
- Device integration
  - Routing
  - Switching
  - Security
  - Cisco Wide Area Applications Services (WAAS) acceleration
  - Unified Communications-Cisco Unified Survivable Remote Site Telephony
- Borderless Networking
  - Same services in the branch as in headquarters

  - Services On Demand, decoupling software from software
- High-speed branch WAN performance
- Cisco® EnergyWise
- High availability
- Network Manageability

Cisco Solution Strengths

Cisco Integrated Services Routers Generation 2

The Cisco® Integrated Services Router Generation 2 (ISR G2) products are the latest addition to the tremendously successful integrated services router (ISR) portfolio. The Cisco ISR G2s are part of the Cisco Borderless Network Architecture that enables business innovation and growth across all remote sites. The next-generation architecture delivers a new workshops experience by meeting the performance requirements for the next generation of WAN and network services, enabling the cost-effective delivery of high-definition collaboration at the branch office and providing the secure transition to the next generation of cloud and virtualized network services. Designed for optimal service delivery on a single platform, the Cisco ISR G2s give businesses greater power to deliver a superior customer experience and deploy services ‘on demand’ as business needs dictate, meanwhile you can reduce overall operating costs.

What Problems Does the Cisco ISR G2s Products Help Solve?

With the number of employees growing at the branch office, financial teams are challenged to securely and efficiently connect remote locations at minimal cost. The Cisco ISR G2 products not only address critical branch-office challenges, like the first generation of ISRs, but they also introduce revolutionary ways to make the remote office more productive, more collaborative, and more operationally efficient. These new innovations enable financial branch offices to do the following:

- Deliver next-generation WAN and network service requirements.
- Deliver next-generation LAN with the same services in the branch as in headquarters using Cisco EtherSwitch Service modules.
  - Same feature/roadmap/software train as Catalyst switches, one software version to test/validate for both the branch and headquarters. Lower total cost of ownership, routing plus switching solution.
- Become more productive through increased video-based collaboration and rich-media services.
- Securely transition to cloud and virtualized network services.
- Minimize energy consumption and costs to support corporate sustainability.
- Enable financial teams to scale services worldwide.
- Rapidly deploy micro branches such as Automated Teller Machines (ATM) and Kiosk locations.

- Transition toward Ethernet handoff technologies from legacy technologies.

Why Should you Upgrade to a Cisco ISR G2 Product?

The Cisco ISR G2 portfolio builds upon the market success of the first generation of ISRs, plus it offers new enhancements that deliver greater value to your business, such as (followed by bulleted list):

- Video-ready branch office for a superior customer experience with new services that transform the branch-office workspace.
- Service virtualization to deliver highly effective business innovation that achieves unparalleled service.
- Operational excellence providing the lowest total cost of ownership (TCO) with scalability, operational flexibility, and simplicity based on best-in-class service integration, innovative pay-as-you-grow model, and optimized energy efficiency.
- Increased branch-office uptime with enhanced availability features.
- Greater energy efficiency with slot-based controls to decrease costs and support sustainability.
- Simplified deployment with a single Cisco IOS Software image.
- Investment protection with support for most of the prior generation of integrated services router.

Management Capabilities and Applications

Cisco Integrated Services Router G2s provide extensive support for standard SNMP MIBs and syslog messages, and allows for comprehensive network management using Cisco or third-party network management systems (NMSs). Cisco-embedded management capabilities provide comprehensive network management functions, from proactive diagnostics to Web 2.0 open interface to policy-based automation.

Cisco ISR G2s provide the network platform for borderless services. As you run more services on your network, you can use IP SLAs to monitor critical network traffic performance indicators, including delay, jitter, and link availability. IP SLAs mimic real-world traffic to proactively identify service-level problems before your users do. Integrating with a broad set of Cisco and third-party NMS applications, IP SLAs set the standard for leadership in proactive performance monitoring.

Flexible NetFlow (FNF) is the next generation in NetFlow technology. As more services and applications, such as business video run in the network, FNF provides the visibility of the network infrastructure needed for optimizing resource usage and planning capacity, reducing operation costs, and detecting security incidents. FNF provides more flexibility and scalability beyond traditional NetFlow by enabling customization of traffic identification, such as source, destination, timing, and application information. Furthermore, FNF provides enhanced network anomaly and security detection to help quickly identify and remediate security risks.

For more about supported 3rd-party applications, Cisco management applications, or embedded management capabilities on Cisco ISR G2s, see:

http://www.cisco.com/en/US/prod/routers/isrg2_management_capabilities_app.html#~third-party

Cisco Borderless Network Architecture

Cisco® Borderless Network Architecture is designed to help IT balance demanding business challenges and changing business models promoted by the influx of consumer devices into the business world. Borderless networks help IT evolve its infrastructure to deliver seamless and secure access in a world with many new and shifting borders.

As people embrace new technologies as part of their daily lives, a second shift is occurring. A new generation of customers and employees is entering the workforce. This new generation is multimedia savvy and socially connected. They bring highly mobile, highly portable video devices into the workplace or business, and they come with the expectation that video will be part of their interaction with employees, customers, and partners. Thus, IT must deal not only with new devices and usage models, but also with changing business practices that place huge new demands on the core infrastructure.

In today's modern workplace, it is increasingly common that primary business resources, including data centers, applications, employees, and customers, are all outside the traditional business perimeter. Extending business borders around all these people and resources taxes your IT department. IT simply cannot scale when every project is an exception to traditional IT design and management practices. IT needs a better way to scale and manage users and customers in any location, because users may be using virtually any device to access almost any application located anywhere in the world. Cisco's Borderless Network Architecture empowers IT to efficiently manage access from multiple locations, from multiple devices, and to applications that can be located anywhere.

The research firm In-Stat estimates that by 2012 more than 1.3 billion Wi-Fi devices will have reached the market. There is a dramatic shift occurring toward ubiquitous wired and wireless access, but many organizations still treat wired and wireless networks as separate entities. Cisco® Borderless Network Architecture provides the framework to unify wired and wireless access, including security, access control, and performance management across many different device types.

Enabling Secure Access, Anywhere, with Any Device

Another primary shift is how and where users access information. In the past, data and applications were housed on the premises, and users were also generally on the premises. Today, many organizations tap into talent pools all around the world. Workers might be full-time remote employees or contractors. Applications might be hosted off-site or even in the cloud, but traditional IT still treats these crucial resources as internal entities. With Cisco's Borderless Network Architecture, IT can unify its approach to securely delivering applications to users in a highly distributed environment. The crucial element to scaling secure access is a policy-based architecture that allows IT to implement centralized access controls with enforcement throughout the network, from server, to infrastructure, to client.

At the heart of borderless networks is a new technical architecture based on three important principles:

- Decoupling hardware from software.
- Unifying the computing, storage, and networking.
- Standardizing policy throughout the unified system.

Cisco Borderless Network Architecture Five-Phase Plan

These design principles are exposed through innovations across Cisco's routing, switching, wireless, security, application optimization, and network management products. With these principles in mind, Cisco is implementing a five-phase plan to deliver a next-generation architecture that delivers seamless, secure, reliable communications to any device, in any location, accessing any resource.

Cisco's Borderless Network Architecture is implemented as a five-phase plan that moves from baseline services to advanced policy management and integration that ultimately delivers the borderless experience.

1. The first phase of the borderless network evolution establishes critical borderless network services that serve as the foundation for advanced collaboration and rich-media applications. These services include medianet and Cisco® EnergyWise, connection management, and resilience and control services.

2. The second phase focuses on borderless user services, including mobility services, security services, and application performance services. These services simplify the user experience, creating a seamless user experience while enhancing IT's control over highly distributed and mobile client devices.
3. The third phase implements borderless policy, enabling IT to implement unified policies that govern how users access the network from different devices and locations.
4. The fourth phase provides a borderless integration framework, extending borderless network services to third-party devices and systems through open APIs and partnerships.
5. The final phase delivers the borderless experience, combining user and network services, policy, and integration together to realize the anytime, anywhere experience that is borderless networks.

Cisco EnergyWise

Many financial branch locations are closed at specific and predictable times of the day. During that time, many devices continue to run, which usually raises utility bills and causes damage to the environment. This problem can be successfully resolved by using Cisco® EnergyWise services. EnergyWise is implemented across Cisco's routing, switching, and wireless portfolios; providing measurement, monitoring, and the control of energy usage from network devices and network-attached IT devices. Cisco EnergyWise gives the user a network-based framework process to discover, monitor, optimize, advise, and regulate energy needs for the business. It encompasses a highly intelligent network-based approach to communicate messages that control energy between network devices and endpoints.

When combined with Cisco® Network Building Mediator, organizations can take a whole-facility approach to energy management that can quickly add up to substantial operational savings and reduced environmental impact.

Cisco® EnergyWise is a new energy management architecture that allows IT operations and facilities to measure and fine-tune power usage to realize significant cost savings. Cisco EnergyWise focuses on reducing power utilization on all devices connected to a Cisco network, ranging from Power over Ethernet (PoE) devices such as IP phones and wireless access points, to IP-enabled building and lighting controllers. It uses an intelligent network-based approach, allowing IT and building facilities operations to understand, optimize, and control power across an entire corporate infrastructure, potentially affecting any powered device. Cisco EnergyWise provides IT professionals with a new method to understand power usage and justify energy costs.

Cisco® EnergyWise is an energy management architecture designed to measure power consumption and optimize power usage, resulting in effective delivery of power across the enterprise. IT professionals can quickly optimize the power consumed in a building, and the result is immediate cost savings with a clear return on investment.

Cisco EnergyWise measures current power consumption, automates and takes actions to optimize power levels, and advises how much power is being consumed to demonstrate cost saving. After power consumption is understood, regulation using Cisco EnergyWise network protocols provides command and control of power usage. Energy consumed per location can easily be found with a realistic view of power consumed per wiring closet, building floor, or campus building.

More Information

For additional details about the many ways Cisco routing, security and application platforms help financial institutions address business and networking issues, please visit
Design Zone for Financial Services,

http://www.cisco.com/en/US/netsol/ns825/networking_solutions_program_home.html.

CHAPTER 2

Deploying the Solution

This chapter provides a description of the three branch banking solutions, their topologies, and a quick deployment method using working example configurations. Select the appropriate network topology for your business environment.

ATM/Kiosk Branch

ATM/Kiosk Branch requirements include a security element and a high availability element. The Cisco Integrated Services Routers Generation 2 (ISR G2) allow these types of services to reside within the same router and provide maximum performance and feature coverage, which results in the lowest total cost of ownership (TCO).

ATM/Kiosk Branch uses a Cisco 1941 ISR G2 and runs Cisco® Internet Operating System (IOS) version 15.0(1)M3, which is representative of branches, ATMs, and other financial kiosks connected to a corporate head-end. WAN connections are generally low speed and use a dial backup or other low cost broadband connection as a backup. In a common ATM example, the network will be deployed with a WAN link connected to a Frame Relay cloud and it can utilize a 3G card for backup in the event of a WAN failure. The 3G card is used as an excellent alternative to a terrestrial backup solution provided cellular service is available.

EIGRP and BGP are deployed on the branch router to allow the customer the flexibility of selecting the routing protocol deployment within the network. BGP is used as the preferred routing protocol to allow deployment of sites across a service provider. EIGRP is used for 3G backup and will connect directly back to the company in an event of WAN link failure.

Security features covered in this topology include AAA, TACACS, DMVPN, NHRP, and GRE tunneling for encrypted data transport to ensure secure delivery of customer data across the WAN. SSH is enabled to provide secure access to the router.

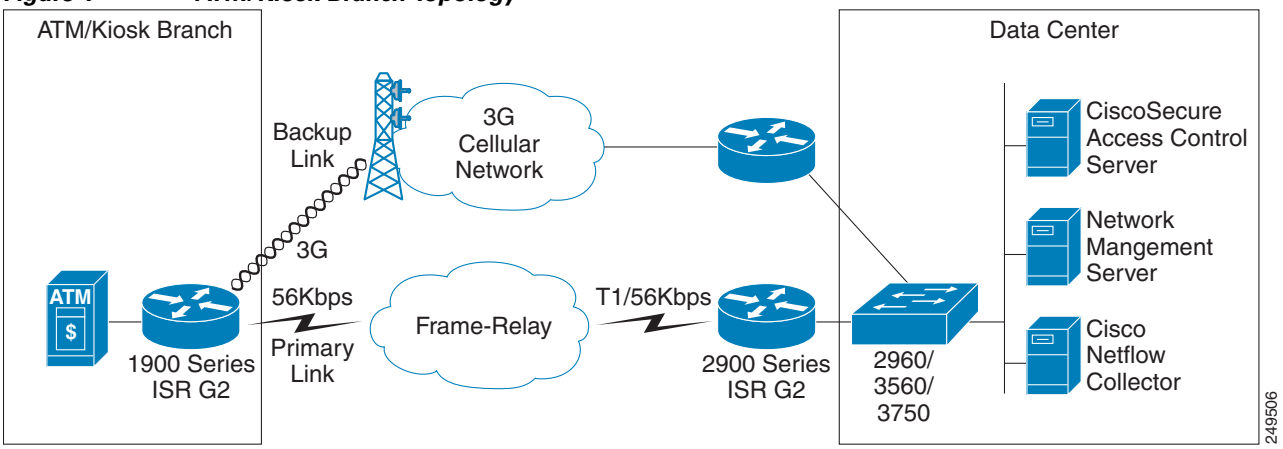
SNMP, NTP, and logging allow for external management of the routers and can aid in the proactive support of the network as well as in the historical performance and troubleshooting.

High availability features in the ATM/Kiosk Branch is supported with a 3G dial solution that allows connectivity in the event of a WAN failure.

This solution uses the following interface for feature support.

- HWIC-3G
- WIC-1DSU-56K4
- WIC-4A/S

Figure 1 ATM/Kiosk Branch Topology



Example

```
!
!
!!! Frame-Relay sub interface (PVC) configuration !!!
interface Serial0/1/0.1 point-to-point
 ip address 10.10.50.1 255.255.255.0
 frame-relay interface-dlci 100
!
!!! 3G Cellular interface Configurations !!!
interface Cellular0/0/0
 no ip address
 ip virtual-reassembly
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
 async mode interactive
 ppp ipcp dns request
!
!!! Dialer interface Configurations !!!
interface Dialer1
 ip address negotiated
 ip virtual-reassembly
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 0
 dialer string cdma
 dialer persistent
 ppp ipcp dns request
!
!!! EIGRP Routing configuration !!!
!!! Add tunnel1/tunnel2 and LAN networks into EIGRP configuration !!!
router eigrp 100
 network 10.10.10.0 0.0.0.255
 network 10.10.11.0 0.0.0.255
```

```
 network 10.10.40.0 0.0.0.255
!
!!! BGP Routing configuration !!!
!!! Add Frame-relay and loopback networks into BGP configuration !!!
router bgp 1841
 no synchronization
 bgp log-neighbor-changes
 network 10.10.30.5 mask 255.255.255.255
 network 10.10.50.0 mask 255.255.255.0
 neighbor 10.10.50.5 remote-as 2851
 no auto-summary
!
ip local policy route-map track-primary-if
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!!! Serial0/1/0.1 FR PVC is used as primary interface and
!!! 3G/Dialer interface is used as backup interface configuration !!!
ip route 10.20.20.5 255.255.255.255 Serial0/1/0.1 track 1
ip route 10.20.20.5 255.255.255.255 Dialer1 253
!
!!! Define an IP SLA for reachability tracking !!!
ip sla 1
 icmp-echo 10.10.60.5 source-interface Serial0/1/0.1
 frequency 5
ip sla schedule 1 life forever start-time now
!
access-list 102 permit ip any host 10.10.60.5
!
!!! Define route-map for the IP SLA 1 for reachability tracking !!!
route-map track-primary-if permit 10
 match ip address 102
 set interface Serial0/1/0.1 Null0
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line 0/0/0
 exec-timeout 0 0
 password C!sc0221
 script dialer cdma
 modem InOut
 no exec
 transport input all
 transport output all
line vty 0
 exec-timeout 1 0
 transport input all
line vty 1 4
 exec-timeout 0 0
 transport input all
 exception data-corruption buffer truncate
 scheduler allocate 20000 1000
!
!!! Configure NTP server address for NTP time sync !!!
ntp update-calendar
ntp server 10.10.60.5
end
```

Survivable Voice Enabled Branch

Survivable Voice Enabled Branch requirements include a wide variety of features ranging from security to Voice. The Cisco Integrated Services Routers Generation 2 (ISR G2) allow these types of services, and others, to reside within the same router and provide maximum performance and feature coverage which results in the lowest total cost of ownership (TCO).

Survivable Voice Enabled Branch has a Cisco 2900 ISR G2 running Cisco Internet Operating System (IOS), version 15.0(1)M3, which is connected to the corporate head-end via a 6 T1 bundle running MLPPP. Any data at the branch is marked and classified for priority before it is sent over an encrypted tunnel to the head-end. T1 circuits in a bundle allow for significant cost savings compared to provisioning a higher speed T3 circuit.

OSPF and EIGRP have been deployed on the branch router to allow the customer the flexibility of making a choice of routing protocol deployment within the network. EIGRP is being used over GRE tunnels to the corporate site and OSPF is being used to the service provider.

Security features covered in this topology include AAA, Zone Based Firewall, IPSe, and GRE tunneling for encrypted data transport to ensure secure delivery of customer data across the WAN. Zone Based Firewall further allows the customer to prevent the injection of undesirable traffic into the network.

IP SLA and QoS gives the Survivable Voice Enabled Branch the ability to deliver specific customer service levels and allow for a better experience. IP SLA and QOS allows the user to tune performance and prioritize customer critical applications such as Voice applications, where high latency can reduce voice quality and the user experience.

Voice is supported through the Call Manager at the corporate site and can use QOS to give priority to voice calls to ensure calls are always of the highest quality. Survivable Remote Site Telephony (SRST) and MGCP Call Control Backup give added flexibility to voice deployments.

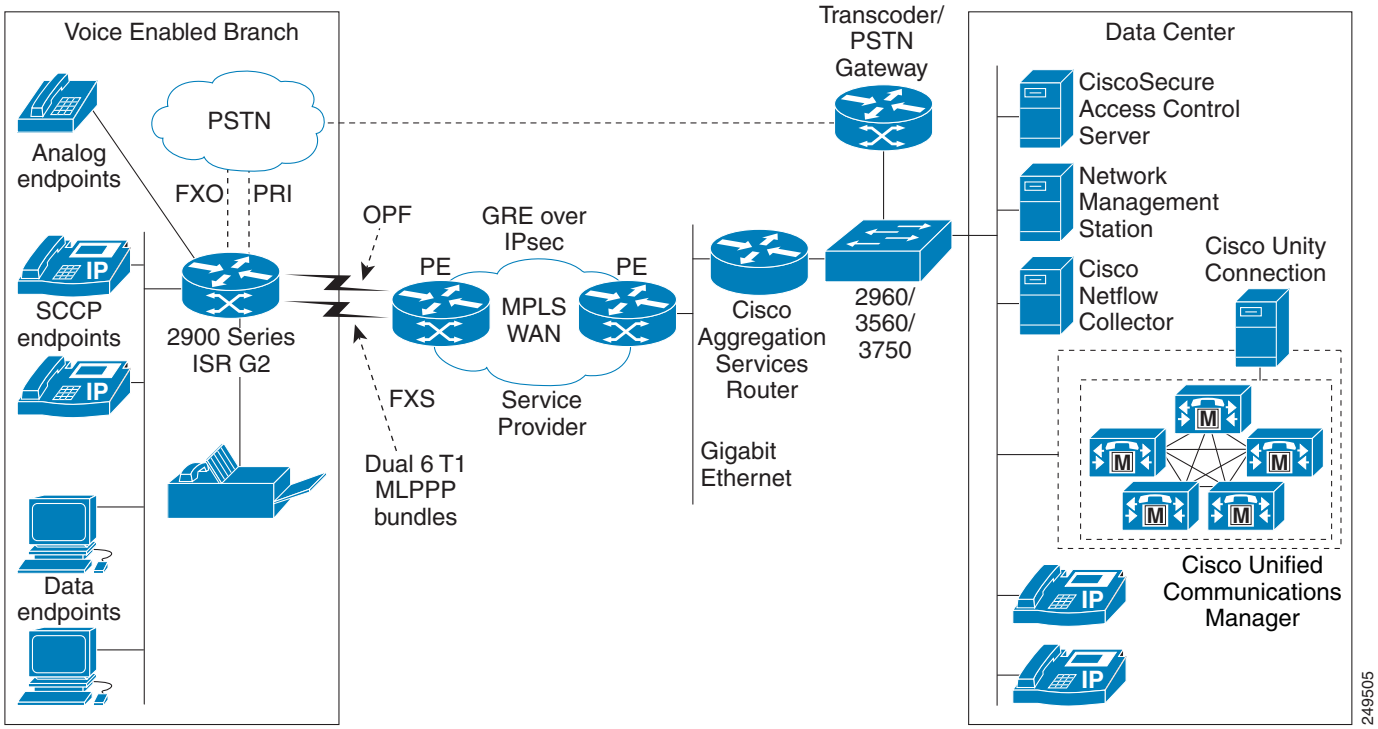
SNMP, NTP, and logging allow for external management of the routers and can aide in the proactive support of the network as well as in the historical performance and troubleshooting. SSHv2 provides secure remote access to the branch routers.

High availability features in the Survivable Voice Enabled Branch are supported with MLPPP for link redundancy, SRST and MGCP Call Control Backup for the remote branch to continue functioning even if the main WAN link is down. For voice, Cisco® Unity Connection was used for voicemail. MGCP was the primary call-control protocol. Cisco EnergyWise is enabled on the router to reduce power consumption.

This solution uses the following modules and interface for feature support:

- VWIC2-2MFT-T1/E1
- VWIC2-1MFT-T1/E1
- HWIC-4T1/E1
- PVDM2-64
- NME-16ES-1G-P
- VIC2-2FXS
- VIC2-2FXO
- VIC3-4FXS/DID

Figure 2 Survivable Voice Enabled Branch Topology



Examples

The Cisco 2911 ISR G2 is a low rack unit (LRU) platform, as such not all of the Survivable Voice Enabled Branch voice modules and dual-multilink interface can be simultaneously installed into the chassis. The following configurations provide module and interface combinations based on common use-case scenarios:

- Survivable Voice Enabled Branch—Voice and Data, page 2-5
- Survivable Voice Enabled Branch—Data, page 2-14
- Headquarters External Transcoder, page 2-24

Survivable Voice Enabled Branch—Voice and Data

This configuration scenario includes one 6T1 multilink bundle and one GRE-over-IPSEC tunnel for both Voice and data traffic.

```
2911-Med-BR1#sh run
Building configuration...


Current configuration : 11215 bytes
!
! Last configuration change at 20:15:28 UTC Fri May 28 2010 by admin
!
version 15.0
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
```

```
!
hostname 2911-Med-BR1
!
boot-start-marker
boot system flash:c2900-universalk9-mz.SPA.150-1.M2.7
boot-end-marker
!
card type t1 0 0
card type t1 0 1
card type t1 0 2
logging buffered 64000
enable password 7 02150C5E0E120E2D
!
!
!
!
!
network-clock-participate wic 1
no network-clock-participate wic 2
!
no ipv6 cef
ip source-route
ip cef
!
!
ip multicast-routing
!
! dhcp pool  is configured for the customer-site phones
ip dhcp pool CUCM7.1.3
   network 10.1.146.0 255.255.255.0
   option 150 ip 192.168.200.100 192.168.200.101
   default-router 10.1.146.1
!
!
no ip domain lookup
ip inspect log drop-pkt
!
multilink bundle-name authenticated
!
!
!
!
isdn switch-type primary-4ess
!
crypto pki token default removal timeout 0
!
!
voice-card 0
 dsp services dspfarm
!
!
!
voice service voip
!
!
!Energywise configuration is enabled on the branch router.

energywise domain cisco security shared-secret 0 cisco
energywise importance 100
energywise keywords cisco
energywise neighbor 10.1.147.152 43441
!
!
! MGCP gateway fall-back transition to default h323 configuration.
```

```
application
 global
  service alternate default
 !
!
license udi pid CISCO2911/K9 sn FTX1405A1Z1
hw-module pvdm 0/0
!
hw-module sm 1
!
!
!
username user1 password 7 094F471A1A0A
!
redundancy
!
!
controller T1 0/0/0
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/0/1
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/1/0
 cablelength long 0db
 pri-group timeslots 1-24 service mgcp
!
controller T1 0/2/0
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/2/1
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/2/2
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/2/3
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!

!
! A 6-class LLQ QOS Model is defined. Class maps are configured to match and classify
packets based on dscp values. This is applied on the outbound WAN side.


class-map match-all QOS-CALLCONTROL
 match ip dscp cs3
class-map match-all QOS-TRANSACTIONAL
 match access-group 132
class-map match-all QOS-NETMGMT
 match ip dscp cs2
class-map match-all QOS-VOICE
```

```
 match ip dscp ef
class-map match-all QOS-BULKDATA
 match ip dscp cs6
!
!
! Policy-maps are defined in LLQ  pattern where Voice is given priority over the rest
classes.Bandwidth allocation is done for various traffic patterns.

policy-map LLQ-OUT
 class QOS-VOICE
    priority percent 40
 class QOS-CALLCONTROL
    bandwidth remaining percent 20
 class QOS-TRANSACTIONAL
    bandwidth remaining percent 8
 class QOS-BULKDATA
    bandwidth remaining percent 5
 class QOS-NETMGMT
    bandwidth remaining percent 3
 class class-default
    queue-limit 1024 packets



 ! zone-based firewall is configured to inspect ftp traffic .class-map, policy-map, and
zones are defined.
class-map type inspect match-any ftp-traffic
 match protocol ftp

policy-map type inspect ftppolicy
 class type inspect ftp-traffic
  inspect
 class class-default
  pass
!
zone security financials
 description HQ financial documents
zone security users
 description bank internal employees
zone-pair security zp1 source users destination financials
 service-policy type inspect ftppolicy
zone-pair security zp2 source financials destination users
 service-policy type inspect ftppolicy
!


translation-rule 10
 Rule 1 5000 710995000
!
!
!

! steps to configure Encryption for GRE tunnel.

!create access-list to define the traffic for encryption
access-list 120 permit gre host 172.16.87.54 host 172.16.85.58


! Internet security association and key management protocol (ISAKMP), ISAKMP key  and
IPSEC transform set  are defined. Encryption is AES and pre-shared (PSK) authentication is
used where shared secrets are pre-defined.
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisc0123 address 172.16.85.58
```

```
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set strong esp-aes esp-md5-hmac
 mode transport
!

!crypto map  is defined

crypto map vpn 10 ipsec-isakmp
 set peer 172.16.85.58
 set security-association replay window-size 1024
 set transform-set strong
 match address 120
!
!

!
interface Loopback0
 ip address 10.10.11.184 255.255.255.255
 !
!

! GRE tunnel configuration is defined. This is one end of the gre tunnel.
interface Tunnel0
 ip address 192.168.16.1 255.255.255.0
 ip pim sparse-dense-mode
 zone-member security financials
 load-interval 30
 keepalive 5 3
!description  Tunnel with the physical interface  6xT1 MLPPP
 tunnel source Multilink1
 tunnel destination 172.16.85.58
 !
!
interface Multilink1
 ip address 172.16.87.54 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
ip virtual-reassembly max-reassemblies 1024
 load-interval 30
 ppp multilink
 ppp multilink group 1
 ppp multilink fragment disable
! description crypto map is applied on this WAN interface
 crypto map vpn
 !description qos is applied on this WAN interface for all outbound traffic
 service-policy output LLQ-OUT
!
interface Multilink2
 no ip address
 ppp multilink
 ppp multilink group 2
 !
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 !
!
interface GigabitEthernet0/1
 no ip address
```

```
 load-interval 30
 duplex auto
 speed auto
 !
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 !
!
interface Serial0/0/0:0
 bandwidth 1536
 no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 ppp multilink group 1
 ppp multilink endpoint string bundle1
 no fair-queue
 !
!
interface Serial0/0/1:0
 bandwidth 1536
 no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 ppp multilink group 1
 ppp multilink endpoint string bundle1
 no fair-queue
 !
!
interface Serial0/1/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-ni
 isdn incoming-voice voice
 isdn bind-l3 ccm-manager
 no cdp enable
 !
!
interface Serial0/2/0:0
 bandwidth 1536
 no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 ppp multilink group 1
 ppp multilink endpoint string bundle1
 no fair-queue
 !
!
interface Serial0/2/1:0
 bandwidth 1536
 no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 ppp multilink group 1
 ppp multilink endpoint string bundle1
 no fair-queue
 !
```

```
!
interface Serial0/2/2:0
 bandwidth 1536
 no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 ppp multilink group 1
 ppp multilink endpoint string bundle1
 no fair-queue
 !
!
interface Serial0/2/3:0
 bandwidth 1536
 no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 ppp multilink group 1
 ppp multilink endpoint string bundle1
 no fair-queue
 !
!
!This is the interface connecting the Integrated switch service module (Etherswitch
module).
interface GigabitEthernet1/0
ip address 192.168.20.1 255.255.255.0
 load-interval 30
 !
!
interface GigabitEthernet1/0.1
!description This interface acts as a default gateway for VLAN 146. encapsulation dot1Q
146.
 ip address 10.1.146.1 255.255.255.0
 zone-member security users
 ntp broadcast
!
interface GigabitEthernet1/0.2
! description This interface acts as a default gateway for VLAN147.
 encapsulation dot1Q 147
 ip address 10.1.147.1 255.255.255.0
 ip pim sparse-dense-mode
 zone-member security users
!
!
!
! EIGRP Routing for GRE tunnel is defined.
router eigrp 10
 network 10.1.146.0 0.0.0.255
 network 10.1.147.0 0.0.0.255
 network 192.168.16.1 0.0.0.0
 neighbor 192.168.16.2 Tunnel0
!

!OSPF routing for the PE-CE routing is defined.
router ospf 109
 router-id 172.16.85.54
 log-adjacency-changes
 redistribute connected
 network 10.10.11.184 0.0.0.0 area 109
 network 172.16.87.52 0.0.0.3 area 109
!
!
!
```

```
ip forward-protocol nd


no ip http server
no ip http secure-server




!
control-plane
 !
!
voice-port 0/1/0:23
 echo-cancel coverage 64
!
voice-port 0/3/0
 echo-cancel coverage 64
 timing hookflash-out 50
 station-id name fxs
 station-id number 8000
!
voice-port 0/3/1
 echo-cancel coverage 64
 timing hookflash-out 50
 station-id name fax
 station-id number 8000
!
!call-manager fallback mgcp configuration is defined.
ccm-manager fallback-mgcp
ccm-manager redundant-host 192.168.200.101
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 192.168.200.100
ccm-manager config
!


!mgcp configuration with call-agent as CALL-MANAGER is defined below.
mgcp
mgcp call-agent 192.168.200.100 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000 action notify
mgcp modem passthrough voip mode nse
mgcp package-capability rtp-package
mgcp package-capability sst-package
mgcp package-capability pre-package
mgcp default-package fxr-package
no mgcp package-capability res-package
no mgcp timer receive-rtcp
mgcp timer nse-response t38 250
mgcp sdp simple
mgcp fax rate 9600
mgcp fax t38 gateway force
mgcp rtp payload-type g726r16 static
mgcp bind control source-interface Tunnel0
mgcp bind media source-interface Tunnel0
!
mgcp profile default
!
!
dial-peer voice 100 pots
 service mgcpapp
 destination-pattern 5000
```

```
 translate-outgoing called 10
 port 0/1/0:23
!
dial-peer voice 200 pots
 service mgcpapp
 port 0/1/0:23
!
dial-peer voice 300 pots
 service mgcpapp
 destination-pattern 2...
 incoming called-number .T
 direct-inward-dial
 port 0/1/0:23
!
dial-peer voice 400 voip
 destination-pattern 5...
!
dial-peer voice 999030 pots
 service mgcpapp
 port 0/3/0
!
dial-peer voice 999031 pots
 service mgcpapp
 port 0/3/1
!
dial-peer voice 500 voip
 destination-pattern 971099....
 session target ipv4:192.168.200.100
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback cisco
!
dial-peer voice 70000 voip
 destination-pattern 7....
 session target ipv4:192.168.200.100
!
dial-peer voice 70001 pots
 port 0/3/1
!
!
!
!
gatekeeper
 shutdown
!
!

!SRST configuration is defined.
call-manager-fallback
 max-conferences 8 gain -6
 transfer-system full-consult
 ip source-address 10.1.146.1 port 2000
 max-ephones 25
 max-dn 25
 voicemail 5000
 call-forward noan 5000 timeout 30
 mwi relay
!
!ntp configuration is defined below. Branch router (and all other devices in the network)
is sync'd to a central NTP server which provides reliable time.

ntp source GigabitEthernet1/0.1
ntp update-calendar
ntp server 192.168.201.102 prefer source GigabitEthernet1/0.1
```

```
line con 0
line aux 0
line vty 0 4

scheduler allocate 20000 1000

end

2911-Med-BR1#$
```

Survivable Voice Enabled Branch—Data

This configuration scenario includes a dual multilink bundle and dual GRE-over-IPSEC tunnel scenario for only data traffic.

```
2911-Med-BR1#sh run
Building configuration...


Current configuration : 13484 bytes
!
! Last configuration change at 00:54:11 UTC Fri Jul 2 2010 by admin
!
version 15.0
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
!
hostname 2911-Med-BR1
!
boot-start-marker
boot system flash:c2900-universalk9-mz.SPA.150-1.M2.12
boot-end-marker
!
card type t1 0 0
card type t1 0 1
card type t1 0 2
card type t1 0 3
logging buffered 64000
enable password 7 02150C5E0E120E2D
!
!
!
network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate wic 3
!
no ipv6 cef
!

ip source-route
ip cef
!
!
ip multicast-routing
!
!dhcp pool is configured for customer-site phones

ip dhcp pool CUCM7.1.3
   network 10.1.146.0 255.255.255.0
```

```
   option 150 ip 192.168.200.100 192.168.200.101
   default-router 10.1.146.1
!
!
no ip domain lookup
ip inspect log drop-pkt
ip accounting-threshold 2000
!
multilink bundle-name authenticated
!
!
!
!
isdn switch-type primary-4ess
!

!Energywise configuration is enabled on the branch router
energywise domain cisco security shared-secret 0 cisco
energywise importance 100
energywise keywords cisco
energywise neighbor 10.1.147.152 43441
!
crypto pki token default removal timeout 0
!
!
voice-card 0
 dsp services dspfarm
!
!
!
voice service voip
!
!
!
!
!
application
 global
  service alternate default
 !
!
license udi pid CISCO2911/K9 sn FTX1405A1Z1
hw-module pvdm 0/0
!
hw-module sm 1
!
!
!
username user1 password 7 094F471A1A0A
!
redundancy
!
!
controller T1 0/0/0
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/0/1
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/1/0
```

```
 cablelength long 0db
 pri-group timeslots 1-24 service mgcp
!
controller T1 0/2/0
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/2/1
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/2/2
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/2/3
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/3/0
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/3/1
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/3/2
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
controller T1 0/3/3
 clock source line independent
 cablelength long 0db
 channel-group 0 timeslots 1-24
!
!
!A 6-class LLQ QOS Model is defined. Class maps are configured to match and classify
packets based on dscp values. This is applied on the outbound WAN side.


class-map match-all QOS-CALLCONTROL
 match ip dscp cs3
class-map match-all QOS-TRANSACTIONAL
 match access-group 132
class-map match-all QOS-NETMGMT
 match ip dscp cs2
class-map match-all QOS-VOICE
 match ip dscp ef
class-map match-all QOS-BULKDATA
 match ip dscp cs6
!
!Policy-maps are defined in LLQ  pattern where Voice is given priority over the rest
classes.Bandwidth allocation is done for various traffic patterns.
```

```
policy-map WRED
 class class-default
    fair-queue
     random-detect
    queue-limit 1024 packets

!Policy-map WRED was created for interface congestion scenarios in the network, it gets
applied on the outbound wan interface to avoid interface congestion.

policy-map LLQ-OUT
 class QOS-VOICE
    priority percent 40
 class QOS-CALLCONTROL
    bandwidth remaining percent 20
 class QOS-TRANSACTIONAL
    bandwidth remaining percent 8
 class QOS-BULKDATA
    bandwidth remaining percent 5
 class QOS-NETMGMT
    bandwidth remaining percent 3
 class class-default
    queue-limit 1024 packets

! zone-based firewall is configured to inspect ftp traffic .class-map, policy-map, and
zones are defined.

class-map type inspect match-any ftp-traffic
 match protocol ftp
policy-map type inspect ftppolicy
 class type inspect ftp-traffic
  inspect
 class class-default
  pass
!
zone security financials
 description HQ financial documents
zone security users
 description bank internal employees
zone-pair security zp1 source users destination financials
 service-policy type inspect ftppolicy
zone-pair security zp2 source financials destination users
 service-policy type inspect ftppolicy
!
translation-rule 10
 Rule 1 5000 710995000
!
!
translation-rule 20
 Rule 1 70000 7109970000
!
!
! steps to configure Encryption for GRE tunnel.

! create access-list to define the traffic for encryption.
access-list 120 permit gre host 172.16.87.54 host 172.16.85.58
access-list 140 permit gre host 172.16.88.10 host 172.16.86.18

! internet security association and key management protocol (ISAKMP), ISAKMP key  and
IPSEC transform set are defined. Encryption is AES and pre-shared (PSK) authentication is
used where shared secrets are pre-defined.


crypto isakmp policy 10
 authentication pre-share
```

```
crypto isakmp key cisc0123 address 172.16.85.58
crypto isakmp key cisco address 172.16.86.18
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set strong esp-aes esp-md5-hmac
 mode transport
crypto ipsec df-bit clear
!

! crypto map is defined.

crypto map vpn 10 ipsec-isakmp
 set peer 172.16.85.58
 set security-association replay window-size 1024
 set transform-set strong
 match address 120
!
crypto map vpn2 10 ipsec-isakmp
 set peer 172.16.86.18
 set security-association replay window-size 1024
 set transform-set strong
 match address 140
!
!
!
!
!
interface Loopback0
 ip address 10.10.11.184 255.255.255.255
 !
!
! GRE tunnel configuration is defined. This is one end of the gre Tunnel for 1st mlppp
bundle.

interface Tunnel0
 ip address 192.168.16.1 255.255.255.0
 ip pim sparse-dense-mode
 zone-member security financials
 ip igmp join-group 239.0.10.10
 load-interval 30
 keepalive 5 3
description associate Tunnel with the physical interface  6xT1 MLPPP
 tunnel source Multilink1
 tunnel destination 172.16.85.58
 !
! GRE tunnel 2 configuration is defined. This is one end of the gre Tunnel for 2nd MLPPP
bundle.
interface Tunnel10
 ip address 192.168.15.1 255.255.255.0
 zone-member security financials
 description associate Tunnel with the physical interface  6xT1 MLPPP
tunnel source Multilink2
 tunnel destination 172.16.86.18
 !
!
interface Multilink1
 ip address 172.16.85.54 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip virtual-reassembly max-reassemblies 1024
 load-interval 30
 ppp multilink
```

```
 ppp multilink group 1
description crypto map is applied on this WAN interface
 crypto map vpn
 ! description qos is applied on this WAN interface for all outbound traffic
 service-policy output LLQ-OUT

crypto ipsec df-bit copy
 !

!
interface Multilink2
 ip address 172.16.88.10 255.255.255.248
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip ospf cost 10
 ppp multilink
 ppp multilink group 2
 description crypto map is applied on this WAN interface
crypto map vpn2
description qos is applied on this WAN interface for all outbound traffic
 service-policy output LLQ-OUT
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 !
!
interface GigabitEthernet0/1
 no ip address
 load-interval 30
 duplex auto
 speed auto
 !
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 !
!
interface Serial0/0/0:0
 bandwidth 1536
 no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 ppp multilink group 1
 ppp multilink endpoint string bundle1
 no fair-queue
 !
!
interface Serial0/0/1:0
 bandwidth 1536
 no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 ppp multilink group 1
 ppp multilink endpoint string bundle1
 no fair-queue
 !
```

```
!
interface Serial0/1/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-ni
 isdn incoming-voice voice
 no cdp enable
 !
!
interface Serial0/2/0:0
 bandwidth 1536
 no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 ppp multilink group 1
 ppp multilink endpoint string bundle1
 no fair-queue
 !
!
interface Serial0/2/1:0
 bandwidth 1536
 no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 ppp multilink group 1
 ppp multilink endpoint string bundle1
 no fair-queue
 !
!
interface Serial0/2/2:0
 bandwidth 1536
 no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 ppp multilink group 1
 ppp multilink endpoint string bundle1
 no fair-queue
 !
!
interface Serial0/2/3:0
 bandwidth 1536
 no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 ppp multilink group 1
 ppp multilink endpoint string bundle1
 no fair-queue
 !
!
interface Serial0/3/0:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 2
 ppp multilink endpoint string bundle2
 !
!
interface Serial0/3/1:0
 no ip address
 encapsulation ppp
```

```
 ppp multilink
 ppp multilink group 2
 ppp multilink endpoint string bundle2
 !
!
interface Serial0/3/2:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 2
 ppp multilink endpoint string bundle2
 !
!
interface Serial0/3/3:0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 2
 ppp multilink endpoint string bundle2
 !
!
interface GigabitEthernet1/0
description interface to connect to integrated switch module
 ip address 192.168.20.1 255.255.255.0
 load-interval 30
 !
!
interface GigabitEthernet1/0.1
description This interface acts as a default gateway for VLAN 146
encapsulation dot1Q 146
 ip address 10.1.146.1 255.255.255.0
 zone-member security users
 ntp broadcast
!
interface GigabitEthernet1/0.2
 description This interface acts as a default gateway for VLAN 147
encapsulation dot1Q 147
 ip address 10.1.147.1 255.255.255.0
 ip pim sparse-dense-mode
 zone-member security users
!
!
! EIGRP Routing for GRE tunnel is defined.
router eigrp 10

 network 10.1.146.0 0.0.0.255
 network 10.1.147.0 0.0.0.255
 network 192.168.15.0
 network 192.168.16.0
 neighbor 192.168.16.2 Tunnel0
 neighbor 192.168.15.2 Tunnel10
!
! OSPF routing for the PE-CE routing is defined.

router ospf 109
 router-id 172.16.85.54
 log-adjacency-changes
 network 10.10.11.184 0.0.0.0 area 109
 network 172.16.87.52 0.0.0.3 area 109
 network 172.16.88.8 0.0.0.7 area 109
!

!
ip forward-protocol nd
```

```
!
ip pim rp-address 192.168.200.1



no ip http server
no ip http secure-server


!


access-list 100 permit ip 192.168.0.0 0.0.255.255 any




access-list 150 permit udp any any eq snmp
!

!cdp configuration
cdp timer 5
cdp holdtime 20
!
!
!
!
control-plane
 !
!
!
voice-port 0/1/0:23
 echo-cancel coverage 64
!
!call-manager fallback mgcp configuration is defined

ccm-manager fallback-mgcp
ccm-manager redundant-host 192.168.200.101
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 192.168.200.100
ccm-manager config
!
!mgcp configuration with call-agent as CALL-MANAGER is defined below

mgcp
mgcp call-agent 192.168.200.100 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode nte-gw
mgcp rtp unreachable timeout 1000 action notify
mgcp modem passthrough voip mode nse
mgcp package-capability rtp-package
mgcp package-capability sst-package
mgcp package-capability pre-package
mgcp default-package fxr-package
no mgcp package-capability res-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp rtp payload-type g726r16 static
mgcp bind control source-interface Tunnel0
mgcp bind media source-interface Tunnel0
!
mgcp profile default
!
```

```
!
dial-peer voice 100 pots
 service mgcpapp
 destination-pattern 5000
 translate-outgoing called 10
 port 0/1/0:23
!
dial-peer voice 200 pots
 service mgcpapp
 port 0/1/0:23
!
dial-peer voice 300 pots
 service mgcpapp
 destination-pattern 2...
 incoming called-number .T
 direct-inward-dial
 port 0/1/0:23
!
dial-peer voice 400 voip
 destination-pattern 5...
!
dial-peer voice 999031 pots
 service mgcpapp
!
dial-peer voice 500 voip
 destination-pattern 971099....
 session target ipv4:192.168.200.100
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback cisco
!
dial-peer voice 70000 voip
 destination-pattern 7....
 session target ipv4:192.168.200.100
!
dial-peer voice 70001 pots
!
dial-peer voice 999030 pots
 service mgcpapp
!
!
!
!
gatekeeper
 shutdown
!
! SRST configuration

call-manager-fallback
 max-conferences 8 gain -6
 transfer-system full-consult
 ip source-address 192.168.146.1 port 2000
 max-ephones 25
 max-dn 25
 voicemail 5000
 call-forward noan 5000 timeout 30
 mwi relay
!
!
ntp configuration is defined below. Branch router (and all other devices in the network)
is sync'd to a central NTP server, which provides reliable time.

ntp source GigabitEthernet1/0.1
ntp update-calendar
ntp server 192.168.201.102 prefer source GigabitEthernet1/0.1
```

```
line con 0
line aux 0
line vty 0 4
 transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000


2911-Med-BR1#
```

Headquarters External Transcoder

```
HQ-Transcoder#sh run
Building configuration...


Current configuration : 3109 bytes
!
! Last configuration change at 19:55:30 UTC Fri May 28 2010
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ-Transcoder
!
boot-start-marker
boot system flash:c2801-adventerprisek9-mz.150-1.M2.7
boot-end-marker
!
card type t1 0 1
logging buffered 50000000
!
no aaa new-model
!
!
!
network-clock-participate wic 1
dot11 syslog
ip source-route
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
isdn switch-type primary-ni
!
!
!
voice service voip
```

```
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback cisco
!
!
!
!
voice-card 0
 dsp services dspfarm
!
!
!
!
!
license udi pid CISCO2801 sn FHK084510HC
archive
 log config
  hidekeys
!
redundancy
!
!
controller T1 0/1/0
 clock source internal
 cablelength long 0db
 pri-group timeslots 1-24
!
controller T1 0/1/1
 cablelength long 0db
!
!
translation-rule 10
 Rule 1 710995000 5000
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.200.110 255.255.255.0
 load-interval 30
 duplex auto
 speed auto
 !
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 !
!
interface Serial0/1/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-ni
 isdn incoming-voice voice
 no cdp enable
 !
!
!
router eigrp 10
```

```
 network 40.0.0.0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
!
!
!
!
!
!
control-plane
 !
!
disable-eadi
!
voice-port 0/0/0
 station-id number 70000
!
voice-port 0/0/1
!
voice-port 0/1/0:23
!
!**************** dspfarm external conference/transcode/mtp configuration *******
!
sccp local FastEthernet0/0
sccp ccm 192.168.200.100 identifier 1 priority 1 version 7.0
sccp
!
sccp ccm group 1
 bind interface FastEthernet0/0
 associate ccm 1 priority 1
 associate profile 3 register trans-2911
 associate profile 2 register mtp-2911
 associate profile 1 register confer-2911
 switchover method immediate
!
dspfarm profile 3 transcode universal
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 codec g729br8
 codec g722-64
 codec g723r53
 codec g723r63
 maximum sessions 4
 associate application SCCP
!
dspfarm profile 1 conference
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 codec g729br8
 codec g722-64
 maximum sessions 1
 associate application SCCP
```

```
!
dspfarm profile 2 mtp
 codec g711ulaw
 maximum sessions software 3
 associate application SCCP
!
dial-peer voice 100 voip
 destination-pattern 5...
 session target ipv4:192.168.200.100
 dtmf-relay h245-alphanumeric
!
dial-peer voice 200 voip
 destination-pattern 4...
 session target ipv4:192.168.200.100
!
dial-peer voice 300 pots
 destination-pattern 71099T
 port 0/1/0:23
!
dial-peer voice 400 voip
 destination-pattern 970319.....
 dtmf-relay h245-signal
 fax-relay ecm disable
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback cisco
!
dial-peer voice 500 pots
 destination-pattern 970319.....
 port 0/0/0
!
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end

HQ-Transcoder#
```

Integrated Switch

```
switch-es#sh run
Building configuration...

Current configuration : 8576 bytes
!
! Last configuration change at 19:21:24 UTC Thu Apr 20 1905
! NVRAM config last updated at 18:40:55 UTC Thu Apr 20 1905
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SWITCH-ES
!
```

```
boot-start-marker
boot-end-marker
!
!
!
!
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
no ip domain-lookup
!
!
!
mls qos map policed-dscp  24 26 46 to 0
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos
!

******** energywise configuration **********
energywise domain cisco security shared-secret 0 cisco
energywise importance 100
```

```
energywise name m-line
energywise keywords cisco
!
crypto pki trustpoint TP-self-signed-1770627072
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1770627072
 revocation-check none
 rsakeypair TP-self-signed-1770627072
!
!
crypto pki certificate chain TP-self-signed-1770627072
 certificate self-signed 01
  30820242 308201AB A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31373730 36323730 3732301E 170D3933 30333031 30303031
  31325A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 37373036
  32373037 3230819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100C959 6B84601D E6ED39BF F87B97AD EDE42D91 1C5DD98A 0B08BD08 4D42FB45
  BDC3BFBA ECE41648 4EAD10D4 3B267E88 10FBA105 4AF7AEF9 22ED5E4F E829284E
  F0D94C23 0A444C2A 7D4C6DC0 D56B9BAE 489C592E 984FF891 423D92C7 FD326394
  10855FB7 AA2B05B1 EB5996C7 9A233FFA 6519E5DE 2EDB9AF2 F617BDB1 4F085F15
  0B3D0203 010001A3 6A306830 0F060355 1D130101 FF040530 030101FF 30150603
  551D1104 0E300C82 0A535749 5443482D 45532E30 1F060355 1D230418 30168014
  725574E7 95CA4388 030A055C 6BBE8021 EA6DC827 301D0603 551D0E04 16041472
  5574E795 CA438803 0A055C6B BE8021EA 6DC82730 0D06092A 864886F7 0D010104
  05000381 81009EE1 63566A1D 5743C193 606793B3 31BA0953 1D6C6E48 F9BCCD96
  2DF43E29 112C7458 C4A832FE F4537D39 731E99D8 98E84238 F8DEA00A 741A5F5E
  945C9A18 677AC87A 65675579 2AA89533 AC51BA42 CBAB8E75 94F78D28 2CFDFBCF
  2D5AFAA3 32E92B76 7B4F0064 85FAF829 98D54EA2 73D44A77 E3476B22 3AB82B73
  A448F11F 69CB
  quit
!
!
!
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
class-map match-all AutoQoS-VoIP-RTP-Trust
 match ip dscp ef
class-map match-all AutoQoS-VoIP-Control-Trust
 match ip dscp cs3  af31
!
!
policy-map AutoQoS-Police-CiscoPhone
 class AutoQoS-VoIP-RTP-Trust
  set dscp ef
  police 320000 8000 exceed-action policed-dscp-transmit
 class AutoQoS-VoIP-Control-Trust
  set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
!
!
!
interface FastEthernet1/0/1
 switchport access vlan 147
 switchport mode access
 switchport voice vlan 146
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
```

```
 mls qos trust device cisco-phone
 mls qos trust cos
 energywise level 10 recurrence importance 95 at 0 6 * * *
 energywise level 0 recurrence importance 95 at 0 4 * * *
 energywise importance 100
 energywise keywords cisco
 energywise name m-line-phone3
 auto qos voip cisco-phone
 spanning-tree portfast
 service-policy input AutoQoS-Police-CiscoPhone
!
interface FastEthernet1/0/2
 switchport access vlan 147
 switchport mode access
 switchport voice vlan 146
 spanning-tree portfast
!
interface FastEthernet1/0/3
 description *** pagent br****
 switchport access vlan 147
 spanning-tree portfast
!
interface FastEthernet1/0/4
 switchport access vlan 147
 switchport voice vlan 146
 spanning-tree portfast
!
interface FastEthernet1/0/5
 switchport access vlan 147
 switchport voice vlan 146
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 energywise level 10 recurrence importance 95 at 0 6 * * *
 energywise level 0 recurrence importance 95 at 0 4 * * *
 energywise importance 100
 energywise keywords cisco
 energywise name m-line-phone
 auto qos voip cisco-phone
 spanning-tree portfast
 service-policy input AutoQoS-Police-CiscoPhone
!
interface FastEthernet1/0/6
 switchport access vlan 147
 switchport voice vlan 146
 srr-queue bandwidth share 10 10 60 20
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 energywise level 10 recurrence importance 95 at 0 6 * * *
 energywise level 0 recurrence importance 95 at 0 4 * * *
 energywise importance 100
 energywise keywords cisco
 energywise name m-line-phone2
 auto qos voip cisco-phone
 spanning-tree portfast
 service-policy input AutoQoS-Police-CiscoPhone
!
interface FastEthernet1/0/7
 switchport access vlan 147
!
interface FastEthernet1/0/8
 switchport access vlan 147
```

```
!
interface FastEthernet1/0/9
 switchport access vlan 147
!
interface FastEthernet1/0/10
 switchport access vlan 147
!
interface FastEthernet1/0/11
 switchport access vlan 147
!
interface FastEthernet1/0/12
 switchport access vlan 147
!
interface FastEthernet1/0/13
 switchport access vlan 147
!
interface FastEthernet1/0/14
 switchport access vlan 147
!
interface FastEthernet1/0/15
 switchport access vlan 147
!
interface FastEthernet1/0/16
!
interface GigabitEthernet1/0/1
 switchport access vlan 147
 switchport trunk encapsulation dot1q
 switchport mode trunk
 shutdown
!
interface GigabitEthernet1/0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
!
interface Vlan1
 no ip address
!
interface Vlan147
 ip address 192.168.147.151 255.255.255.0
!
ip classless
ip http server
ip http secure-server
!
ip sla enable reaction-alerts
!
alias exec si show ip interface brief
alias exec sr show run | begin ^router
alias exec c conf t
alias exec s show run
alias exec sib show ip bgp
alias exec cib clear ip bgp
alias exec sir show ip route
alias exec cir clear ip route
!
line con 0
line vty 0 4
 no login
 length 0
line vty 5 15
 no login
!
end
```

High Availability Branch with Survivable Voice

High Availability Branch with Survivable Voice requirements include high availability, security, efficient use of bandwidth, and energy efficiency. The Cisco Integrated Services Routers Generation 2 (ISR G2) allow these types of services, and others, to reside within the same router and provide maximum performance and feature coverage, which results in the lowest total cost of ownership (TCO).

The financial branch has two Cisco 3900 ISR G2s running Cisco Internet Operating System (IOS) version 15.0(1)M3, and they are connected to each other via multi-group HSRP. These Cisco 3900 ISR G2s are connected over the WAN using high-speed links to either a single head-end, or if further redundancy is needed, dual head-end routers. Any data at the branch is marked and classified and sent through the WAAS module for WAN Optimization before it is encrypted using GETVPN and sent to the head-end. WAN Optimization allows for better usage of the WAN links, as well as customer perceived performance increases.

BGP is used as the routing protocol between PE-CE allowing for large prefix support and a wide choice of providers. Security features covered in this topology include AAA and TACACS for authentication and logging, GET VPN for any-to-any connectivity of other remote branches allowing simpler and easier secure deployments and connections. GET VPN's features also allow higher scalability by avoiding a full logical mesh as well as simpler configuration and overall support.

WAAS, IP SLA, and QoS give the High Availability Branch with Survivable Voice additional ability to deliver specific customer service levels and allow for a better experience. WAAS allows the most efficient use of the WAN pipes and in many scenarios will give the perception that the WAN connection is far superior than the actual link speeds. IP SLA and QoS allows the user to tune the performance and prioritize customer critical applications' such as Voice applications where high latency can reduce voice quality and user experience.

SNMP, NTP and Syslog allows for external management of the routers and can aide in proactive support of the network as well as historical performance and troubleshooting. SSHv2 provides secure remote access to the branch routers. Flexible NetFlow is used to acquire operational data and use that data to understand how the network is behaving. Data is exported to a collector at the Data Center.

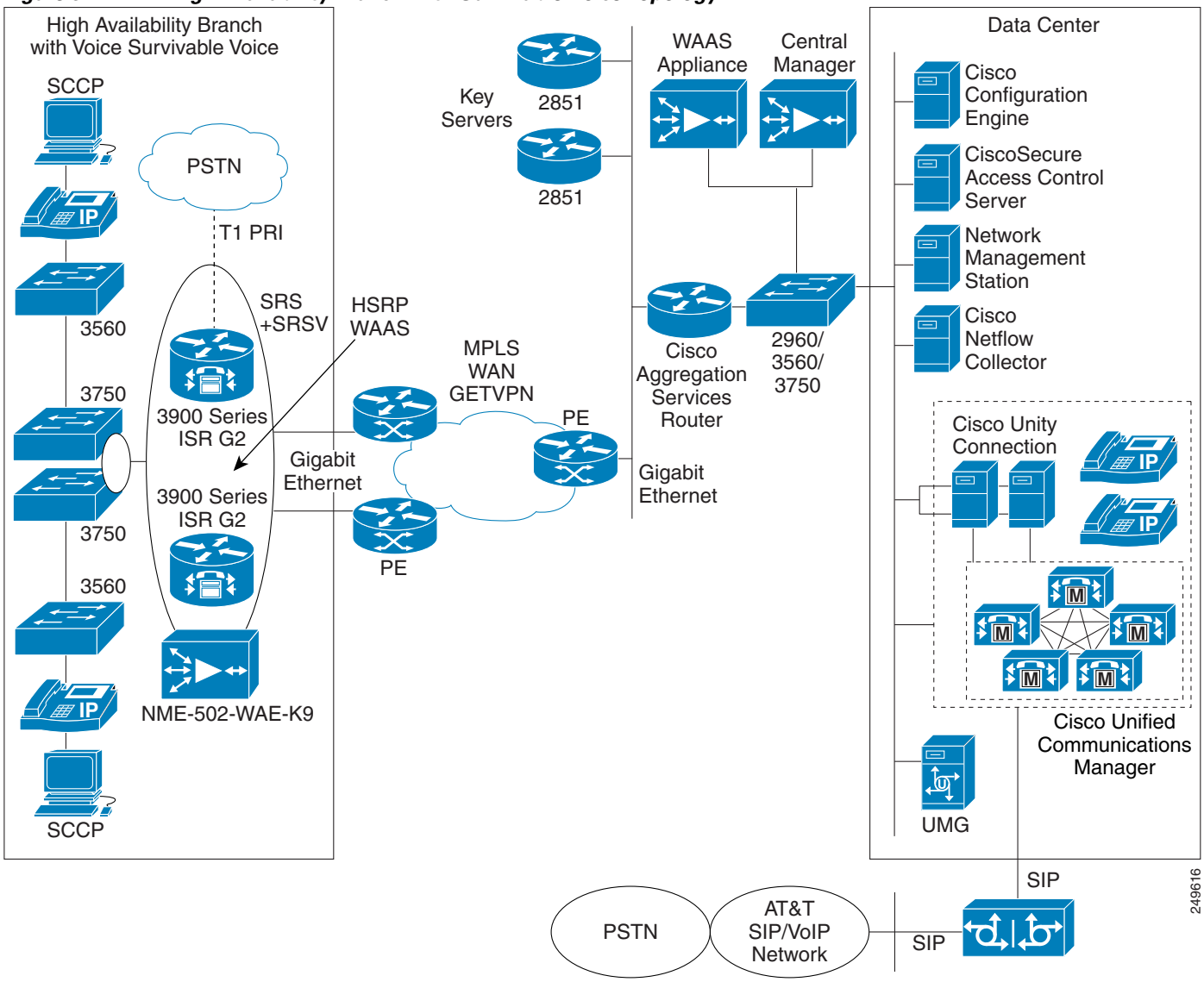
Voice is supported through the Call Manager at the corporate site, and can use QoS to give priority to voice calls to ensure calls are always of the highest quality. PSTN access for branch users is provided by a SIP trunk terminated by a CUBE server that is deployed at the Data Center.

High availability is critical to the High Availability Branch with Survivable Voice and is supported with the Cisco 3900 ISR G2 dual power supplies, multiple branch routers and potentially multiple head-end routers, multiple HSRP groups, and Survivable Remote Site Telephony (SRST/SRSV). Cisco EnergyWise is enabled on the router to reduce power consumption.

This solution uses the following modules for feature support:

- VWIC2-1MFT-T1/E1
- NME-CUE
- NME-WAE-502-K9
- NME-UMG

Figure 3 High Availability Branch with Survivable Voice Topology



Examples

Branch Configurations

Headquarter Configurations

Branch Router 1

```
!
version 15.0
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname 3945-LBR-1
!
boot-start-marker
boot system flash:c3900-universalk9-mz.SPA.150-1.M2.13
boot-end-marker
!
card type t1 0 0
logging buffered 5000000
enable password lab
!
clock timezone PST -7
network-clock-participate wic 0
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-3732185865
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3732185865
 revocation-check none
 rsakeypair TP-self-signed-3732185865
!
!
crypto pki certificate chain TP-self-signed-3732185865
 certificate self-signed 02
  3082024D 308201B6 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33373332 31383538 3635301E 170D3130 30363330 32313038
  30355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37333231
  38353836 3530819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100EB1F 952F8FC6 A34E4798 14C3DDBB 433DF03A 6A2D950E 99191169 4ED7B7BA
  F19B5F9D 92741338 54B0500A 52B90826 D2C027BB D7298433 9C000428 C2732864
  28A04B44 A3BCDBEC A3E1F505 3A98FD80 79CBA878 6D872863 F8A6A992 C0F103EB
```

```
  C1D0FA66 EF7BBF36 A19A7A04 CF6D9AC1 3689F8DD 9F32FD80 9924AC29 FD3967BB
  AA1F0203 010001A3 75307330 0F060355 1D130101 FF040530 030101FF 30200603
  551D1104 19301782 154D4C49 4E452D4C 42522D31 2E6D6C69 6E652E63 6F6D301F
  0603551D 23041830 16801491 EC4AAC0C 22751632 76C44A2C 2BA6735F FCC81F30
  1D060355 1D0E0416 041491EC 4AAC0C22 75163276 C44A2C2B A6735FFC C81F300D
  06092A86 4886F70D 01010405 00038181 00B9D1D7 3028632D 5151D7D5 AFBA5CBD
  2C11E0BA 31DBB398 F85B4D8B 2728BB5C FE0BD39C 0E2E46A6 3F7DA1C7 D2B4A859
  A2155BCF 0825C917 3C7EE23C 5F29F7E0 26D2DBFB D98D2C40 74C6D336 783DB920
  FAFC77F9 6C77A0AE 9E4A92EC 91B86054 225362BA CB8D46D7 F397F5AA 8919C33C
  832FEABE 53854138 742C3BDC C8AE80A2 39
        quit
no ipv6 cef
!
ip source-route
ip cef
!
ip multicast-routing
! A range of addresses which are used for the router interfaces are excluded from being
assigned to the branch IP phones using DHCP.
ip dhcp excluded-address 10.1.150.1 10.1.150.10
!
! A DHCP pool is created on the branch router to provide IP addresses to the branch IP
phones.
ip dhcp pool BRANCH_PHONES
   network 10.1.150.0 255.255.255.0
   option 150 ip 192.168.200.100
   default-router 10.1.150.10

! Only packets matching the access-list 120 are chosen for WCCP redirection. This enables
control over which packets are intercepted and redirected by WCCP for WAAS.
ip wccp 61 redirect-list 120
ip wccp 62 redirect-list 120
!
multilink bundle-name authenticated
!
parameter-map type inspect global
!
isdn switch-type primary-5ess

! EnergyWise is enabled on the branch router.
energywise domain mline security shared-secret 0 cisco
!
voice-card 0
!
application
 global
  service alternate Default
 !
!
license udi pid C3900-SPE150/K9 sn FOC14090YW1
hw-module pvdm 0/0
 energywise activitycheck
!
hw-module sm 2
!
hw-module sm 4
!
!
!
username lab password 0 lab
!
redundancy
!
!
```

```
controller T1 0/0/0
 cablelength long 0db
 pri-group timeslots 1-24
!
track 1 interface GigabitEthernet0/1 line-protocol
!
```

! An eight class QoS model is defined. Class maps are configured to match and classify packets based on DSCP values/protocol types/ACLs. This is used on the INBOUND LAN side.

```
class-map match-all qos-callcontrol
 match protocol skinny
class-map match-all qos-buscrit
 match access-group 111
class-map match-all qos-transactional
 match access-group 112
class-map match-all qos-netmgmt
 match protocol snmp
class-map match-all qos-voice
 match protocol rtp
class-map match-all qos-routing
 match  dscp cs6
class-map match-all qos-scavenger
 match  dscp cs1
class-map match-any qos-bulkdata
 match protocol ftp
 match protocol smtp
 match access-group 110
```

! An eight class QoS model is defined. Class maps are configured to match and classify packets based on DSCP values. This is used on the OUTBOUND WAN side.

```
class-map match-all CALLCONTROL
 match  dscp cs3
class-map match-all BUSCRIT
 match  dscp af31
class-map match-all TRANSACTIONAL
 match  dscp af21
class-map match-all NETMGMT
 match  dscp cs2
class-map match-all VOICE
 match  dscp ef
class-map match-all ROUTING
 match  dscp cs6
class-map match-all SCAVENGER
 match  dscp cs1
class-map match-all BULKDATA
 match  dscp af11
!
```

! A policy map is defined, specifying the bandwidth allocation to the various classes. Shaping is configured to limit the traffic to 10% of the available link bandwidth.

```
policy-map OUTBOUND-WAN-CLASSIFY
 class BULKDATA
    bandwidth percent 5
 class ROUTING
    bandwidth percent 3
 class NETMGMT
    bandwidth percent 3
 class CALLCONTROL
    bandwidth percent 5
 class VOICE
    bandwidth percent 20
```

```
 class TRANSACTIONAL
    bandwidth percent 8
 class BUSCRIT
    bandwidth percent 10
 class SCAVENGER
    bandwidth percent 1
 class class-default
    bandwidth percent 45
policy-map OUTBOUND-WAN-SHAPE
 class class-default
    shape average percent 10
  service-policy OUTBOUND-WAN-CLASSIFY

! Policy map is defined to remark INBOUND traffic at the LAN edge.

policy-map INBOUND_LAN_REMARKING
 class qos-callcontrol
  set dscp cs3
 class qos-buscrit
  set dscp af31
 class qos-transactional
  set dscp af21
 class qos-netmgmt
  set dscp cs2
 class qos-voice
  set dscp ef
 class qos-routing
  set dscp cs6
 class qos-scavenger
  set dscp cs1
 class qos-bulkdata
  set dscp af11
!
! IKE Phase 1 (ISAKMP) policy is defined. Encryption is AES and pre-shared (PSK)
authentication is used where shared secrets are pre-defined in the encryption devices.
! This is required to enable the GETVPN GM (Group member) and the KS (Key server) to
authenticate each other.

crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
 lifetime 1200
crypto isakmp key 1234567ABCDEFG address 172.16.81.3
crypto isakmp key 1234567ABCDEFG address 172.16.81.4
!

! GETPVN GDOI group is configured using the same identify defined on the KS (Key Server).
The IP addresses of the key servers are specified.
crypto gdoi group getvpn
 identity number 1234
 server address ipv4 172.16.81.3
 server address ipv4 172.16.81.4
!
! The crypto map is defined with the "gdoi" type which indicates GETVPN. The crypto map is
applied to the WAN interface i.e. Gig0/1.
crypto map getvpn-map 10 gdoi
 set group getvpn
!
interface Loopback0
 ip address 10.1.3.1 255.255.255.255
 !
!
interface GigabitEthernet0/0
```

```
 description LAN
 no ip address
 load-interval 30
 duplex full
 speed 1000
 !
 service-policy input INBOUND_LAN_REMARKING  ! The service policy is applied to the LAN
interface to remark packets, thus preventing hosts from setting precedence values and
gaining undesired higher priority.
!

! This is the subinterface for the VOICE traffic. HSRP is configured with authentication.
The virtual IP is specified.
! Priority is configured such that under normal operation this branch router will be the
Active router.
interface GigabitEthernet0/0.150
 description VOICE VLAN
 encapsulation dot1Q 150
 ip address 10.1.150.1 255.255.255.0
 standby 1 ip 10.1.150.10
 standby 1 priority 200
 standby 1 preempt
 standby 1 authentication 1234ABCD
 standby 1 track 1 decrement 110
!

! This is the subinterface for the DATA traffic. 2 HSRP groups are configured with
authentication.
! Priorities are configured such that under normal operation, this branch router is the
Active router for group 1 and the standby router for group 2. The roles are reversed on
the other branch router.
! This enables load balancing if branch hosts are organized and configured such that their
default gateways are different HSRP virtual IPs.

interface GigabitEthernet0/0.151
 description DATA VLAN
 encapsulation dot1Q 151
 ip address 10.1.151.1 255.255.255.0
 ip wccp 61 redirect in ! WAAS TCP promiscuous mode group 61 configured for traffic
redirection
 ip pim sparse-mode ! Multicast PIM sparse-mode is configured.
 ip igmp join-group 224.1.1.1
 standby 1 ip 10.1.151.10
 standby 1 priority 200
 standby 1 preempt
 standby 1 authentication 1234ABCD
 standby 1 track 1 decrement 110
 standby 2 ip
 standby 2 preempt
 standby 2 authentication ABCD1234
!

! This is the WAN interface.
interface GigabitEthernet0/1
 ip address 172.16.80.1 255.255.255.0
 ip wccp 62 redirect in ! WAAS TCP promiscuous mode group 62 configured for traffic
redirection
 ip pim sparse-mode
 load-interval 30
 duplex full
 speed 1000
 crypto map getvpn-map ! The crypto map is applied to this interface so that traffic
entering/leaving this interface can be encrypted according to the ACLs defined on the KS.
 !
```

```
service-policy output OUTBOUND-WAN-SHAPE ! The previously configured policy map is applied
to the interface for all outbound traffic.
!
interface Serial0/0/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-5ess
 isdn incoming-voice voice
 no cdp enable
 !
!

! This interface corresponds to the CUE module running SRSV-CUE software.
! In SRST mode, voicemail is stored locally on this module and uploaded to the central
Cisco Unity Connection when the WAN link is restored.
! It works in conjunction with the UMG (Unified Messaging Gateway) located centrally at
the Data Center.

interface Integrated-Service-Engine2/0
 ip address 10.1.4.20 255.255.255.0
 service-module ip address 10.1.5.30 255.255.255.0
 !Application: SRSV-CUE Running on NME
 service-module ip default-gateway 10.1.4.20
 no keepalive
 !
!

! This interface corresponds to the WAAS module running WAAS software.
! WAAS providess WAN optimization using compression, tranport file optimization and
caching services.

interface Integrated-Service-Engine4/0
 ip address 10.1.6.20 255.255.255.0
 ip wccp redirect exclude in
 service-module ip address 10.1.7.30 255.255.255.0
 !Application: Restarted at Wed Jun 16 12:08:00 2010
 service-module ip default-gateway 10.1.6.20
 no keepalive
 !
!

! The PE-CE routing protocol is eBGP.

router bgp 600
 no synchronization
 bgp log-neighbor-changes
 network 10.1.4.0 mask 255.255.255.0
 network 10.1.5.0 mask 255.255.255.0
 network 10.1.6.0 mask 255.255.255.0
 network 10.1.7.0 mask 255.255.255.0
 network 10.1.150.0 mask 255.255.255.0
 network 10.1.151.0 mask 255.255.255.0
 network 172.16.80.0 mask 255.255.255.0
 network 10.1.3.1 mask 255.255.255.255
 neighbor 172.16.80.2 remote-as 65000
 no auto-summary
!
ip forward-protocol nd
!
ip pim rp-address 172.16.81.2
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
```

```
ip http timeout-policy idle 60 life 86400 requests 10000
ip flow-export source Loopback0
!
ip route 10.1.3.2 255.255.255.255 10.1.151.2
!
access-list 110 remark MATCH DSCP AF11 HOSTS
access-list 110 permit ip 10.1.151.16 0.0.0.15 any
access-list 111 remark MATCH DSCP AF21 HOSTS
access-list 111 permit ip 10.1.151.80 0.0.0.15 any
access-list 112 remark MATCH DSCP AF31 HOSTS
access-list 112 permit ip 10.1.151.96 0.0.0.15 any
access-list 120 remark WAAS REDIRECT ACL
access-list 120 permit ip 10.1.151.0 0.0.0.255 192.168.201.0 0.0.0.255
access-list 120 permit ip 192.168.201.0 0.0.0.255 10.1.151.0 0.0.0.255
nls resp-timeout 1
cpd cr-id 1
!
control-plane
!
voice-port 0/0/0:23

! The 2 dial-peers are used in SRST mode when the WAN link is down.
! The branch router falls back to H.323 mode and these dial-peers handle inbound and
outbound calls from/to the PSTN.

dial-peer voice 100 pots
 description ** INBOUND FROM PSTN **
 incoming called-number 408555....
 direct-inward-dial
 port 0/0/0:23
!
dial-peer voice 200 pots
 description ** OUTBOUND TO PSTN **
 destination-pattern 9T
 port 0/0/0:23
!

! This dial-peer is required to route calls to the SRSV-CUE module so that PSTN callers
can leave voicemail for branch users in SRST mode.

dial-peer voice 5000 voip
 destination-pattern 5000
 session protocol sipv2
 session target ipv4:10.1.4.30
 codec g711ulaw
!

gatekeeper
 shutdown
!

! SRST is enabled. 5000 is the voicemail pilot number. Busy/No Answer situations result in
caller being directed to the SRSV-CUE module to leave voicemail.

call-manager-fallback
 max-conferences 8 gain -6
 transfer-system full-consult
 ip source-address 10.1.150.1 port 2000
 max-ephones 10
 max-dn 10
 voicemail 5000
 call-forward busy 5000
 call-forward noan 5000 timeout 8
!
```

```
line con 0
 exec-timeout 0 0
line aux 0
line 131
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line 259
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 password lab
 transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000

! Branch router (and all other devices in the network) is sync'd to a central NTP server
which provides reliable time.

ntp source Loopback0
ntp update-calendar
ntp server 172.16.81.4

3945-LBR-1#
```

Branch Router 2

```
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 3945-LBR-2
!
boot-start-marker
boot system flash:c3900-universalk9-mz.SPA.150-1.M2.13
boot-end-marker
!
logging buffered 5000000
!
memory-size iomem 15
clock timezone PST -7
!
crypto pki trustpoint TP-self-signed-3139033350
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3139033350
 revocation-check none
 rsakeypair TP-self-signed-3139033350
!
crypto pki certificate chain TP-self-signed-3139033350
 certificate self-signed 01
  30820252 308201BB A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
```

```
  69666963 6174652D 33313339 30333333 3530301E 170D3130 30343039 32333532
  34305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 31333930
  33333335 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100A461 17A078DA A658562D E86CB102 480EE254 BACBDC04 E7E4C310 95A6FD8D
  A551B7D1 9B20763D F2196ED3 3E5DDAB6 05E70C3F 9BEEDA28 799C044A 1AA3324E
  DC66616F 1723F33E 43FBA5EF A8025C9B F3F1E287 BC1C5A77 99ED6F20 991D260C
  AA048E58 857CE22D 3826AC2B 82EB4BD3 095AEA5F B200D058 3A82DBCA F7740C30
  56770203 010001A3 7A307830 0F060355 1D130101 FF040530 030101FF 30250603
  551D1104 1E301C82 1A4D4C49 4E452D4C 42522D32 2E796F75 72646F6D 61696E2E
  636F6D30 1F060355 1D230418 30168014 A8D13438 E766D0C7 A17B0565 C0C80D82
  87487001 301D0603 551D0E04 160414A8 D13438E7 66D0C7A1 7B0565C0 C80D8287
  48700130 0D06092A 864886F7 0D010104 05000381 8100329D CA3AB7E8 D560F6DD
  86D2D878 A943240E 124609BF 89ABEAB2 BA702976 429E0AB4 12C06610 C2F04E25
  A77867BE ADB67033 B4FF42A9 EC9D4EF8 75EA56A7 B06D39FF BF46D7DB 690598AC
  269D2C00 6CBA9132 1A1740FF 2F39E161 C70C4056 B019FCBC 31594688 609529B6
  D357DF3C 9C108149 E3DD952C 9A7F7C28 6407A1FC 7C45
        quit
no ipv6 cef
!
ip source-route
ip cef
!
no ip domain lookup
ip domain name yourdomain.com
!
multilink bundle-name authenticated
!
!
! EnergyWise is enabled on the branch router
energywise domain mline security shared-secret 0 cisco
!
license udi pid C3900-SPE150/K9 sn FOC13102BR1
license boot module c3900 technology-package uck9
hw-module sm 4
!
redundancy
!
track 1 interface GigabitEthernet0/1 line-protocol

! An eight class QoS model is defined. Class maps are configured to match and classify
packets based on DSCP values/protocol types/ACLs. This is used on the INBOUND LAN side.

class-map match-all qos-callcontrol
 match protocol skinny
class-map match-all qos-buscrit
 match access-group 111
class-map match-all qos-transactional
 match access-group 112
class-map match-all qos-netmgmt
 match protocol snmp
class-map match-all qos-voice
 match protocol rtp
class-map match-all qos-routing
 match  dscp cs6
class-map match-all qos-scavenger
 match  dscp cs1
class-map match-any qos-bulkdata
 match protocol ftp
 match protocol smtp
 match access-group 110

! An eight class QoS model is defined. Class maps are configured to match and classify
packets based on DSCP values. This is used on the OUTBOUND WAN side.
```

```
class-map match-all CALLCONTROL
 match  dscp cs3
class-map match-all BUSCRIT
 match  dscp af31
class-map match-all TRANSACTIONAL
 match  dscp af21
class-map match-all NETMGMT
 match  dscp cs2
class-map match-all VOICE
 match  dscp ef
class-map match-all ROUTING
 match  dscp cs6
class-map match-all SCAVENGER
 match  dscp cs1
class-map match-all BULKDATA
 match  dscp af11
!
```

```
! A policy map is defined, specifying the bandwidth allocation to the various classes.
Shaping is configured to limit the traffic to 10% of the available link bandwidth.

policy-map OUTBOUND-WAN-CLASSIFY
 class BULKDATA
    bandwidth percent 5
 class ROUTING
    bandwidth percent 3
 class NETMGMT
    bandwidth percent 3
 class CALLCONTROL
    bandwidth percent 5
 class VOICE
    bandwidth percent 20
 class TRANSACTIONAL
    bandwidth percent 8
 class BUSCRIT
    bandwidth percent 10
 class SCAVENGER
    bandwidth percent 1
 class class-default
    bandwidth percent 45
policy-map OUTBOUND-WAN-SHAPE
 class class-default
    shape average percent 10
  service-policy OUTBOUND-WAN-CLASSIFY

! Policy map is defined to remark INBOUND traffic at the LAN edge.

policy-map INBOUND_LAN_REMARKING
 class qos-callcontrol
  set dscp cs3
 class qos-buscrit
  set dscp af31
 class qos-transactional
  set dscp af21
 class qos-netmgmt
  set dscp cs2
```

```
 class qos-voice
  set dscp ef
 class qos-routing
  set dscp cs6
 class qos-scavenger
  set dscp cs1
 class qos-bulkdata
  set dscp af11
!
! IKE Phase 1 (ISAKMP) policy is defined. Encryption is AES and pre-shared (PSK)
authentication is used where shared secrets are pre-defined in the encryption devices.
! This is required to enable the GETVPN GM (Group member) and the KS (Key server) to
authenticate each other.
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
 lifetime 1200
crypto isakmp key 1234567ABCDEFG address 172.16.81.3
crypto isakmp key 1234567ABCDEFG address 172.16.81.4
!

! GETPVN GDOI group is configured using the same identify defined on the KS (Key Server).
The IP addresses of the key servers are specified.
crypto gdoi group getvpn
 identity number 1234
 server address ipv4 172.16.81.3
 server address ipv4 172.16.81.4
!

! The crypto map is defined with the "gdoi" type which indicates GETVPN. The crypto map is
applied to the WAN interface i.e. Gig0/1.
crypto map getvpn-map 10 gdoi
 set group getvpn
!
interface Loopback0
 ip address 10.1.3.2 255.255.255.255
 !
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 !
 service-policy input INBOUND_LAN_REMARKING  ! The service policy is applied to the LAN
interface to remark packets, thus preventing hosts from setting precedence values and
gaining undesired higher priority.
!

! This is the subinterface for the VOICE traffic. HSRP is configured with authentication.
The virtual IP is specified.
! Priority is default (100). Under normal operation this branch router will be the Standby
router.

interface GigabitEthernet0/0.150
 encapsulation dot1Q 150
 ip address 10.1.150.2 255.255.255.0
 standby 1 ip
 standby 1 preempt
 standby 1 authentication 1234ABCD
 standby 1 track 1 decrement 15
!
```

```
! This is the subinterface for the DATA traffic. 2 HSRP groups are configured with
authentication.
! Priorities are configured such that under normal operation, this branch router is the
Active router for group 1 and the standby router for group 2. The roles are reversed on
the other branch router.
! This enables load balancing if branch hosts are organized and configured such that their
default gateways are different HSRP virtual IPs.

interface GigabitEthernet0/0.151
 description DATA VLAN
 encapsulation dot1Q 151
 ip address 10.1.151.2 255.255.255.0
 ip pim sparse-mode ! Multicast PIM sparse-mode is configured
 ip igmp join-group 224.1.1.1
 standby 1 ip
 standby 1 preempt
 standby 1 authentication 1234ABCD
 standby 1 track 1 decrement 15
 standby 2 ip 10.1.151.9
 standby 2 priority 200
 standby 2 preempt
 standby 2 authentication ABCD1234
!

! This is the WAN interface.
interface GigabitEthernet0/1
 ip address 172.16.82.1 255.255.255.252
 duplex auto
 speed auto
 crypto map getvpn-map ! The crypto map is applied to this interface so that traffic
entering/leaving this interface can be encrypted according to the ACLs defined on the KS.
 !
service-policy output OUTBOUND-WAN-SHAPE! The previously configured policy map is applied
to the interface for all outbound traffic.
!

! The PE-CE routing protocol is eBGP
router bgp 500
 no synchronization
 bgp log-neighbor-changes
 network 10.1.150.0 mask 255.255.255.0
 network 10.1.151.0 mask 255.255.255.0
 network 172.16.82.0 mask 255.255.255.0
 network 10.1.3.2 mask 255.255.255.255
 neighbor 172.16.82.2 remote-as 65000
 no auto-summary
!
ip forward-protocol nd
!
ip pim rp-address 172.16.81.2
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 10.1.3.1 255.255.255.255 10.1.151.1
!
!Branch router is configured to respond to IP SLA traffic.
ip sla responder

logging trap warnings
logging source-interface Loopback0
logging 192.168.201.104
```

```
!
access-list 110 remark MATCH DSCP AF11 HOSTS
access-list 110 permit ip 10.1.151.16 0.0.0.15 any
access-list 111 remark MATCH DSCP AF21 HOSTS
access-list 111 permit ip 10.1.151.80 0.0.0.15 any
access-list 112 remark MATCH DSCP AF31 HOSTS
access-list 112 permit ip 10.1.151.96 0.0.0.15 any
!
control-plane
 !
line con 0
 exec-timeout 0 0
line aux 0
line 131
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line 259
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 password lab
 transport input all
!
scheduler allocate 20000 1000

! Branch router (and all other devices in the network) is sync'd to a central NTP server
which provides reliable time.

ntp source Loopback0
ntp update-calendar
ntp server 172.16.81.4

3945-LBR-2#
```

NME-WAE-502-K9

```
! WAAS version 4.1.5f (build b2 Apr 20 2010)
!
device mode application-accelerator
!
!
hostname LBR-WAE-502
!
clock timezone PST -7 0
!
!
!
!
!
primary-interface GigabitEthernet 1/0
!
!
!
```

```
interface GigabitEthernet 1/0
 ip address 10.1.7.30 255.255.255.0
 no autosense
 bandwidth 1000
 full-duplex
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
!
ip default-gateway 10.1.5.20
!
no auto-register enable
!
! ip path-mtu-discovery is disabled in WAAS by default
!
!
!
!
ntp server 172.16.81.4
!
!
wccp router-list 1 10.1.151.1
wccp tcp-promiscuous router-list-num 1
wccp version 2
!
!
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
username admin print-admin-password 1 29D5C31BFF3D8D25AAD3B435B51404EE
7D891AB402CAF2E89CCDD33ED54333AC
!
!
!
!
authentication login local enable primary
authentication configuration local enable primary
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
policy-engine application
   set-dscp copy
```

```
name Authentication
name Backup
name CAD
name Call-Management
name Conferencing
name Console
name Content-Management
name Directory-Services
name Email-and-Messaging
name Enterprise-Applications
name File-System
name File-Transfer
name Instant-Messaging
name Name-Services
name P2P
name Printing
name Remote-Desktop
name Replication
name SQL
name SSH
name Storage
name Streaming
name Systems-Management
name VPN
name Version-Management
name WAFS
name Web
name SSL
name Other
classifier AFS
   match dst port range 7000 7009
exit
classifier AOL
   match dst port range 5190 5193
exit
classifier Altiris-CarbonCopy
   match dst port eq 1680
exit
classifier Amanda
   match dst port eq 10080
exit
classifier AppSocket
   match dst port eq 9100
exit
classifier Apple-AFP
   match dst port eq 548
exit
classifier Apple-NetAssistant
   match dst port eq 3283
exit
classifier Apple-iChat
   match dst port eq 5297
   match dst port eq 5298
exit
classifier BFTP
   match dst port eq 152
exit
classifier BGP
   match dst port eq 179
exit
classifier BMC-Patrol
   match dst port eq 6161
   match dst port eq 6162
   match dst port eq 8160
```

```
   match dst port eq 8161
   match dst port eq 6767
   match dst port eq 6768
   match dst port eq 10128
exit
classifier BackupExpress
   match dst port eq 6123
exit
classifier Basic-TCP-services
   match dst port range 1 19
exit
classifier BitTorrent
   match dst port range 6881 6889
   match dst port eq 6969
exit
classifier Borland-Interbase
   match dst port eq 3050
exit
classifier CIFS
   match dst port eq 139
   match dst port eq 445
exit
classifier CU-SeeMe
   match dst port eq 7640
   match dst port eq 7642
   match dst port eq 7648
   match dst port eq 7649
exit
classifier CVS
   match dst port eq 2401
exit
classifier Cisco-CallManager
   match dst port eq 2748
   match dst port eq 2443
exit
classifier Citrix-ICA
   match dst port eq 1494
   match dst port eq 2598
exit
classifier Clearcase
   match dst port eq 371
exit
classifier CommVault
   match dst port range 8400 8403
exit
classifier Connected-DataProtector
   match dst port eq 16384
exit
classifier ControlIT
   match dst port eq 799
exit
classifier DNS
   match dst port eq 53
exit
classifier Danware-NetOp
   match dst port eq 6502
exit
classifier Documentum
   match dst port eq 1489
exit
classifier Double-Take
   match dst port eq 1100
   match dst port eq 1105
exit
```

```
classifier EMC-Celerra-Replicator
   match dst port eq 8888
exit
classifier EMC-SRDFA-IP
   match dst port eq 1748
exit
classifier FCIP
   match dst port eq 3225
exit
classifier FTP-Control
   match dst port eq 21
exit
classifier FTP-Data
   match src port eq 20
exit
classifier FTPS
   match dst port eq 990
exit
classifier FTPS-Control
   match src port eq 989
exit
classifier Filenet
   match dst port range 32768 32774
exit
classifier Gnutella
   match dst port range 6346 6349
   match dst port eq 6355
   match dst port eq 5634
exit
classifier Grouper
   match dst port eq 8038
exit
classifier HP-OpenMail
   match dst port eq 5755
   match dst port eq 5757
   match dst port eq 5766
   match dst port eq 5767
   match dst port eq 5768
   match dst port eq 5729
exit
classifier HP-OpenView
   match dst port range 7426 7431
   match dst port eq 7501
   match dst port eq 7510
exit
classifier HP-Radia
   match dst port eq 3460
   match dst port eq 3461
   match dst port eq 3464
   match dst port eq 3466
exit
classifier HTTP
   match dst port eq 80
   match dst port eq 8080
   match dst port eq 8000
   match dst port eq 8001
   match dst port eq 3128
exit
classifier HTTPS
   match dst port eq 443
exit
classifier HotLine
   match dst port range 5500 5503
exit
```

```
classifier IBM-DB2
   match dst port eq 523
exit
classifier IBM-NetView
   match dst port range 729 731
exit
classifier IBM-TSM
   match dst port range 1500 1502
exit
classifier IBM-Tivoli
   match dst port eq 94
   match dst port eq 627
   match dst port eq 1965
   match dst port eq 1580
   match dst port eq 1581
exit
classifier IPP
   match dst port eq 631
exit
classifier IRC
   match dst port eq 531
   match dst port range 6660 6669
exit
classifier Intel-Proshare
   match dst port range 5713 5717
exit
classifier InterSystems-Cache
   match dst port eq 1972
exit
classifier Internet-Mail
   match dst port eq 25
   match dst port eq 110
   match dst port eq 143
   match dst port eq 220
exit
classifier Internet-Mail-secure
   match dst port eq 995
   match dst port eq 993
   match dst port eq 465
exit
classifier Jabber
   match dst port eq 5222
   match dst port eq 5269
exit
classifier Kazaa
   match dst port eq 1214
exit
classifier Kerberos
   match dst port eq 88
   match dst port eq 2053
   match dst port eq 754
   match dst port eq 888
   match dst port eq 543
   match dst port eq 464
   match dst port eq 544
   match dst port eq 749
exit
classifier L2TP
   match dst port eq 1701
exit
classifier LANDesk
   match dst port eq 9535
   match dst port range 9593 9595
exit
```

```
classifier LDAP
   match dst port eq 389
   match dst port eq 8404
exit
classifier LDAP-Global-Catalog
   match dst port eq 3268
exit
classifier LDAP-Global-Catalog-Secure
   match dst port eq 3269
exit
classifier LDAP-secure
   match dst port eq 636
exit
classifier Laplink-Host
   match dst port eq 1547
exit
classifier Laplink-PCSync
   match dst port eq 8444
exit
classifier Laplink-PCSync-secure
   match dst port eq 8443
exit
classifier Laplink-ShareDirect
   match dst port eq 2705
exit
classifier Legato-NetWorker
   match dst port eq 7937
   match dst port eq 7938
   match dst port eq 7939
exit
classifier Legato-RepliStor
   match dst port eq 7144
   match dst port eq 7145
exit
classifier Liquid-Audio
   match dst port eq 18888
exit
classifier Lotus-Notes
   match dst port eq 1352
exit
classifier Lotus-Sametime-Connect
   match dst port eq 1533
exit
classifier MDaemon
   match dst port eq 3000
   match dst port eq 3001
exit
classifier MS-Chat
   match dst port eq 6665
   match dst port eq 6667
exit
classifier MS-Content-Replication-Service
   match dst port eq 560
   match dst port eq 507
exit
classifier MS-EndPointMapper
   match dst port eq 135
exit
classifier MS-Message-Queuing
   match dst port eq 1801
   match dst port eq 2101
   match dst port eq 2103
   match dst port eq 2105
exit
```

```
classifier MS-NetMeeting
   match dst port eq 522
   match dst port eq 1503
   match dst port eq 1731
exit
classifier MS-NetShow
   match dst port eq 1755
exit
classifier MS-SQL
   match dst port eq 1433
exit
classifier MS-Terminal-Services
   match dst port eq 3389
exit
classifier MSN-Messenger
   match dst port eq 1863
   match dst port range 6891 6900
exit
classifier MySQL
   match dst port eq 3306
exit
classifier NFS
   match dst port eq 2049
exit
classifier NNTP
   match dst port eq 119
exit
classifier NNTP-secure
   match dst port eq 563
exit
classifier NTP
   match dst port eq 123
exit
classifier Napster
   match dst port eq 8875
   match dst port eq 7777
   match dst port eq 6700
   match dst port eq 6666
   match dst port eq 6677
   match dst port eq 6688
exit
classifier NetApp-SnapMirror
   match dst port range 10565 10569
exit
classifier NetIQ
   match dst port eq 2220
   match dst port eq 2735
   match dst port range 10113 10116
exit
classifier Netopia-Timbuktu
   match dst port eq 407
   match dst port range 1417 1420
exit
classifier Netopia-netOctopus
   match dst port eq 1917
   match dst port eq 1921
exit
classifier Novell-Groupwise
   match dst port eq 1677
   match dst port eq 1099
   match dst port eq 9850
   match dst port eq 7205
   match dst port eq 3800
   match dst port eq 7100
```

```
   match dst port eq 7180
   match dst port eq 7101
   match dst port eq 7181
   match dst port eq 2800
exit
classifier Novell-NetWare
   match dst port eq 524
exit
classifier Novell-ZenWorks
   match dst port range 1761 1763
   match dst port eq 517
   match dst port eq 2544
   match dst port eq 8039
   match dst port eq 2037
exit
classifier OpenVPN
   match dst port eq 1194
exit
classifier Oracle
   match dst port eq 66
   match dst port eq 1525
   match dst port eq 1521
exit
classifier Other-Secure
   match dst port eq 261
   match dst port eq 448
   match dst port eq 684
   match dst port eq 695
   match dst port eq 994
   match dst port eq 2252
   match dst port eq 2478
   match dst port eq 2479
   match dst port eq 2482
   match dst port eq 2484
   match dst port eq 2679
   match dst port eq 2762
   match dst port eq 2998
   match dst port eq 3077
   match dst port eq 3078
   match dst port eq 3183
   match dst port eq 3191
   match dst port eq 3220
   match dst port eq 3410
   match dst port eq 3424
   match dst port eq 3471
   match dst port eq 3496
   match dst port eq 3509
   match dst port eq 3529
   match dst port eq 3539
   match dst port eq 3660
   match dst port eq 3661
   match dst port eq 3747
   match dst port eq 3864
   match dst port eq 3885
   match dst port eq 3896
   match dst port eq 3897
   match dst port eq 3995
   match dst port eq 4031
   match dst port eq 5007
   match dst port eq 5989
   match dst port eq 5990
   match dst port eq 7674
   match dst port eq 9802
   match dst port eq 12109
```

```
exit
classifier PCAnywhere
   match dst port eq 73
   match dst port range 5631 5632
   match dst port eq 65301
exit
classifier PCMail-Server
   match dst port eq 158
exit
classifier PDMWorks
   match dst port eq 30000
   match dst port eq 40000
exit
classifier PPTP
   match dst port eq 1723
exit
classifier Pervasive-SQL
   match dst port eq 1583
exit
classifier PostgreSQL
   match dst port eq 5432
exit
classifier ProjectWise-FileTransfer
   match dst port eq 5800
exit
classifier QMTP
   match dst port eq 209
exit
classifier Qnext
   match dst port eq 44
   match dst port eq 5555
exit
classifier RAdmin
   match dst port eq 4899
exit
classifier RTSP
   match dst port eq 554
   match dst port eq 8554
exit
classifier Remote-Anything
   match dst port range 3999 4000
exit
classifier Remote-Replication-Agent
   match dst port eq 5678
exit
classifier Rsync
   match dst port eq 873
exit
classifier SAP
   match dst port range 3200 3219
   match dst port range 3221 3224
   match dst port range 3226 3267
   match dst port range 3270 3282
   match dst port range 3284 3305
   match dst port range 3307 3388
   match dst port range 3390 3399
   match dst port range 3600 3659
   match dst port range 3662 3699
exit
classifier SASL
   match dst port eq 3659
exit
classifier SIP-secure
   match dst port eq 5061
```

```
exit
classifier SOAP
   match dst port eq 7627
exit
classifier SQL-Service
   match dst port eq 156
exit
classifier SSH
   match dst port eq 22
exit
classifier SSL-Shell
   match dst port eq 614
exit
classifier SUN-Xprint
   match dst port eq 8100
exit
classifier Scalable-SQL
   match dst port eq 3352
exit
classifier Service-Location
   match dst port eq 427
exit
classifier Siebel
   match dst port eq 8448
   match dst port eq 2320
   match dst port eq 2321
exit
classifier Simple-FTP
   match dst port eq 115
exit
classifier SoulSeek
   match dst port eq 2234
   match dst port eq 5534
exit
classifier Sun-RPC
   match dst port eq 111
exit
classifier Sybase-SQL
   match dst port eq 1498
   match dst port eq 2638
   match dst port eq 2439
   match dst port eq 3968
exit
classifier Symantec-AntiVirus
   match dst port eq 2847
   match dst port eq 2848
   match dst port eq 2967
   match dst port eq 2968
   match dst port eq 38037
   match dst port eq 38292
exit
classifier TACACS
   match dst port eq 49
exit
classifier TFTP
   match dst port eq 69
exit
classifier TFTPS
   match dst port eq 3713
exit
classifier Telnet
   match dst port eq 23
   match dst port eq 107
   match dst port eq 513
```

```
exit
classifier Telnets
   match dst port eq 992
exit
classifier UniSQL
   match dst port eq 1978
   match dst port eq 1979
exit
classifier Unix-Printing
   match dst port eq 515
   match dst port eq 170
exit
classifier Unix-Remote-Execution
   match dst port eq 514
   match dst port eq 512
exit
classifier VDOLive
   match dst port eq 7000
exit
classifier VNC
   match dst port range 5801 5809
   match dst port range 6900 6909
exit
classifier Veritas-BackupExec
   match dst port eq 6101
   match dst port eq 6102
   match dst port eq 6106
   match dst port eq 3527
   match dst port eq 1125
exit
classifier Veritas-NetBackup
   match dst port eq 13720
   match dst port eq 13721
   match dst port eq 13782
   match dst port eq 13785
exit
classifier Vmware-VMConsole
   match dst port eq 902
exit
classifier VoIP-Control
   match dst port eq 1300
   match dst port eq 2428
   match dst port range 2000 2002
   match dst port range 1718 1720
   match dst port eq 5060
   match dst port range 11000 11999
exit
classifier VocalTec
   match dst port eq 1490
   match dst port eq 6670
   match dst port eq 25793
   match dst port eq 22555
exit
classifier WAAS-FlowMonitor
   match dst port eq 7878
exit
classifier WASTE
   match dst port eq 1337
exit
classifier WBEM
   match dst port eq 5987
   match dst port eq 5988
exit
classifier WINS
```

```
      match dst port eq 42
      match dst port eq 137
      match dst port eq 1512
   exit
   classifier WinMX
      match dst port eq 6699
   exit
   classifier X400
      match dst port eq 102
   exit
   classifier XWindows
      match dst port range 6000 6063
   exit
   classifier Yahoo-Messenger
      match dst port range 5000 5001
      match dst port eq 5050
      match dst port eq 5100
   exit
   classifier eDonkey
      match dst port range 4661 4662
   exit
   classifier ezMeeting
      match dst port range 10101 10103
      match dst port range 26260 26261
   exit
   classifier iFCP
      match dst port eq 3420
   exit
   classifier iSCSI
      match dst port eq 3260
   exit
   classifier iSNS
      match dst port eq 3205
   exit
   map basic
      name File-System classifier AFS action optimize full
      name Instant-Messaging classifier AOL action pass-through
      name Remote-Desktop classifier Altiris-CarbonCopy action pass-through
      name Backup classifier Amanda action optimize DRE no compression none
      name Printing classifier AppSocket action optimize full
      name File-System classifier Apple-AFP action optimize full
      name Remote-Desktop classifier Apple-NetAssistant action pass-through
      name Instant-Messaging classifier Apple-iChat action pass-through
      name File-Transfer classifier BFTP action optimize full
      name Other classifier BGP action optimize full
      name Systems-Management classifier BMC-Patrol action pass-through
      name Backup classifier BackupExpress action optimize DRE no compression none
      name Other classifier Basic-TCP-services action pass-through
      name P2P classifier BitTorrent action pass-through
      name SQL classifier Borland-Interbase action optimize full
      name WAFS classifier CIFS action optimize full accelerate cifs
      name Conferencing classifier CU-SeeMe action pass-through
      name Version-Management classifier CVS action optimize full
      name Call-Management classifier Cisco-CallManager action pass-through
      name Remote-Desktop classifier Citrix-ICA action optimize full
      name Version-Management classifier Clearcase action optimize full
      name Backup classifier CommVault action optimize DRE no compression none
      name Backup classifier Connected-DataProtector action optimize DRE no compression
none
      name Remote-Desktop classifier ControlIT action optimize DRE no compression none
      name Name-Services classifier DNS action pass-through
      name Remote-Desktop classifier Danware-NetOp action optimize DRE no compression none
      name Content-Management classifier Documentum action optimize full
      name Replication classifier Double-Take action optimize full
```

```
      name Replication classifier EMC-Celerra-Replicator action optimize full
      name Storage classifier EMC-SRDFA-IP action optimize full
      name Storage classifier FCIP action optimize full
      name File-Transfer classifier FTP-Control action pass-through
      name File-Transfer classifier FTP-Data action optimize full
      name File-Transfer classifier FTPS action optimize DRE no compression none
      name File-Transfer classifier FTPS-Control action pass-through
      name Content-Management classifier Filenet action optimize full
      name P2P classifier Gnutella action pass-through
      name P2P classifier Grouper action pass-through
      name Email-and-Messaging classifier HP-OpenMail action optimize full
      name Systems-Management classifier HP-OpenView action pass-through
      name Systems-Management classifier HP-Radia action optimize full
      name Web classifier HTTP action optimize full accelerate http
      name SSL classifier HTTPS action optimize DRE no compression none
      name P2P classifier HotLine action pass-through
      name SQL classifier IBM-DB2 action optimize full
      name Systems-Management classifier IBM-NetView action pass-through
      name Backup classifier IBM-TSM action optimize full
      name Systems-Management classifier IBM-Tivoli action optimize full
      name Printing classifier IPP action optimize full
      name Conferencing classifier Intel-Proshare action pass-through
      name SQL classifier InterSystems-Cache action optimize full
      name Email-and-Messaging classifier Internet-Mail action optimize full
      name Email-and-Messaging classifier Internet-Mail-secure action optimize DRE no
compression none
      name Instant-Messaging classifier Jabber action pass-through
      name P2P classifier Kazaa action pass-through
      name Authentication classifier Kerberos action pass-through
      name VPN classifier L2TP action optimize DRE no compression none
      name Systems-Management classifier LANDesk action optimize full
      name Directory-Services classifier LDAP action optimize full
      name Directory-Services classifier LDAP-Global-Catalog action optimize full
      name Directory-Services classifier LDAP-Global-Catalog-Secure action pass-through
      name Directory-Services classifier LDAP-secure action pass-through
      name Remote-Desktop classifier Laplink-Host action optimize DRE no compression none
      name Remote-Desktop classifier Laplink-PCSync action optimize DRE no compression
none
      name Remote-Desktop classifier Laplink-PCSync-secure action optimize DRE no
compression none
      name P2P classifier Laplink-ShareDirect action pass-through
      name Backup classifier Legato-NetWorker action optimize DRE no compression none
      name Backup classifier Legato-RepliStor action optimize DRE no compression none
      name Streaming classifier Liquid-Audio action optimize full
      name Email-and-Messaging classifier Lotus-Notes action optimize full
      name Instant-Messaging classifier Lotus-Sametime-Connect action pass-through
      name Email-and-Messaging classifier MDaemon action optimize full
      name Instant-Messaging classifier MS-Chat action pass-through
      name Replication classifier MS-Content-Replication-Service action optimize DRE no
compression none
      name Other classifier MS-EndPointMapper action optimize DRE no compression none
accelerate MS-port-mapper
      name Other classifier MS-Message-Queuing action optimize full
      name Conferencing classifier MS-NetMeeting action pass-through
      name Streaming classifier MS-NetShow action optimize full
      name SQL classifier MS-SQL action optimize full
      name Remote-Desktop classifier MS-Terminal-Services action optimize DRE no
compression none
      name Instant-Messaging classifier MSN-Messenger action pass-through
      name SQL classifier MySQL action optimize full
      name File-System classifier NFS action optimize full accelerate nfs
      name Email-and-Messaging classifier NNTP action optimize full
      name Email-and-Messaging classifier NNTP-secure action optimize DRE no compression
none
```

```
      name Other classifier NTP action pass-through
      name P2P classifier Napster action pass-through
      name Replication classifier NetApp-SnapMirror action optimize full
      name Systems-Management classifier NetIQ action pass-through
      name Remote-Desktop classifier Netopia-Timbuktu action optimize DRE no compression
none
      name Systems-Management classifier Netopia-netOctopus action pass-through
      name Email-and-Messaging classifier Novell-Groupwise action optimize full
      name File-System classifier Novell-NetWare action optimize full
      name Systems-Management classifier Novell-ZenWorks action optimize full
      name VPN classifier OpenVPN action optimize DRE no compression none
      name SQL classifier Oracle action optimize full
      name Other classifier Other-Secure action pass-through
      name Remote-Desktop classifier PCAnywhere action optimize DRE no compression none
      name Email-and-Messaging classifier PCMail-Server action optimize full
      name CAD classifier PDMWorks action optimize full
      name VPN classifier PPTP action optimize DRE no compression none
      name SQL classifier Pervasive-SQL action optimize full
      name SQL classifier PostgreSQL action optimize full
      name Content-Management classifier ProjectWise-FileTransfer action optimize full
      name Email-and-Messaging classifier QMTP action optimize full
      name P2P classifier Qnext action pass-through
      name Remote-Desktop classifier RAdmin action optimize DRE no compression none
      name Streaming classifier RTSP action optimize full accelerate video
      name Remote-Desktop classifier Remote-Anything action optimize DRE no compression
none
      name Replication classifier Remote-Replication-Agent action optimize DRE no
compression none
      name Replication classifier Rsync action optimize full
      name Authentication classifier SASL action pass-through
      name Call-Management classifier SIP-secure action pass-through
      name Other classifier SOAP action optimize full
      name SQL classifier SQL-Service action optimize full
      name SSH classifier SSH action optimize DRE no compression none
      name Console classifier SSL-Shell action pass-through
      name Printing classifier SUN-Xprint action optimize full
      name SQL classifier Scalable-SQL action optimize full
      name Name-Services classifier Service-Location action pass-through
      name Enterprise-Applications classifier Siebel action optimize full
      name File-Transfer classifier Simple-FTP action optimize full
      name P2P classifier SoulSeek action pass-through
      name File-System classifier Sun-RPC action pass-through
      name SQL classifier Sybase-SQL action optimize full
      name Other classifier Symantec-AntiVirus action optimize full
      name Authentication classifier TACACS action pass-through
      name File-Transfer classifier TFTP action optimize full
      name File-Transfer classifier TFTPS action optimize DRE no compression none
      name Console classifier Telnet action pass-through
      name Console classifier Telnets action pass-through
      name SQL classifier UniSQL action optimize full
      name Printing classifier Unix-Printing action optimize full
      name Console classifier Unix-Remote-Execution action pass-through
      name Streaming classifier VDOLive action optimize full
      name Backup classifier Veritas-BackupExec action optimize DRE no compression none
      name Backup classifier Veritas-NetBackup action optimize DRE no compression none
      name Remote-Desktop classifier Vmware-VMConsole action optimize DRE no compression
none
      name Call-Management classifier VoIP-Control action pass-through
      name Conferencing classifier VocalTec action pass-through
      name Systems-Management classifier WAAS-FlowMonitor action optimize DRE no
compression LZ
      name P2P classifier WASTE action pass-through
      name Systems-Management classifier WBEM action pass-through
      name Name-Services classifier WINS action pass-through
```

```
      name P2P classifier WinMX action pass-through
      name Email-and-Messaging classifier X400 action optimize full
      name Remote-Desktop classifier XWindows action optimize DRE no compression none
      name Instant-Messaging classifier Yahoo-Messenger action pass-through
      name P2P classifier eDonkey action pass-through
      name Conferencing classifier ezMeeting action pass-through
      name Storage classifier iFCP action optimize full
      name Storage classifier iSCSI action optimize full
      name Name-Services classifier iSNS action pass-through
      name Instant-Messaging classifier IRC action pass-through
      name Enterprise-Applications classifier SAP action optimize full
      name Remote-Desktop classifier VNC action optimize DRE no compression none
   exit
   map adaptor WAFS transport
      name WAFS All action optimize full
   exit
   map adaptor EPM 1544f5e0-613c-11d1-93df-00c04fd7bd09
      name Email-and-Messaging All action pass-through
   exit
   map adaptor EPM ms-sql-rpc
      name SQL All action optimize full
   exit
   map adaptor EPM mapi
      name Email-and-Messaging All action optimize full accelerate mapi
   exit
   map adaptor EPM ms-ad-replication
      name Replication All action optimize full
   exit
   map adaptor EPM ms-frs
      name Replication All action optimize full
   exit
   map adaptor EPM f5cc5a18-4264-101a-8c59-08002b2f8426
      name Email-and-Messaging All action pass-through
   exit
   map other optimize full
exit
!
central-manager address 192.168.203.5
cms enable
!
!
!
!
!
! End of WAAS configuration
LBR-WAE-502#
```

NME-CUE

```
clock timezone America/Los_Angeles

hostname MLINE-CUE

ip domain-name mline.com

line console
  length 0

system language preferred "en_US"

ip name-server 192.168.201.104
```

```
ntp server 172.16.81.4 prefer

software download server url "ftp://127.0.0.1/ftp" credentials hidden
"6u/dKTN/hsEuSAEfw40XlF2eFHnZfyUTSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfG
WTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmP"

log trace local enable

site name local
 end site

license agent max-sessions 9

privilege ViewPrivateList create
privilege ManagePrompts create
privilege manage-passwords create
privilege local-broadcast create
privilege ViewRealTimeReports create
privilege manage-users create
privilege broadcast create
privilege ViewHistoricalReports create
privilege vm-imap create
privilege ManagePublicList create

groupname Broadcasters create

privilege ViewPrivateList description "Privilege to view private list"
privilege ManagePrompts description "Privilege to create, modify, or delete system
prompts"
privilege manage-passwords description "Privilege to reset user passwords"
privilege local-broadcast description "Privilege to send local broadcast messages"
privilege ViewRealTimeReports description "Privilege to view realtime reports"
privilege manage-users description "Privilege to create, modify, and delete users and
groups"
privilege broadcast description "Privilege to send local or remote broadcast messages"
privilege ViewHistoricalReports description "Privilege to view historical reports"
privilege vm-imap description "Privilege to manage personal voicemail via IMAP client"
privilege ManagePublicList description "Privilege to manage public lists"
privilege ViewPrivateList operation voicemail.lists.private.view
privilege ManagePrompts operation system.debug
privilege ManagePrompts operation prompt.modify
privilege manage-passwords operation user.pin
privilege manage-passwords operation user.password
privilege manage-passwords operation system.debug
privilege local-broadcast operation system.debug
privilege local-broadcast operation broadcast.local
privilege ViewRealTimeReports operation report.realtime
privilege manage-users operation user.mailbox
privilege manage-users operation user.pin
privilege manage-users operation user.notification
privilege manage-users operation user.configuration
privilege manage-users operation user.password
privilege manage-users operation system.debug
privilege manage-users operation user.remote
privilege manage-users operation group.configuration
privilege broadcast operation broadcast.remote
privilege broadcast operation system.debug
privilege broadcast operation broadcast.local
privilege ViewHistoricalReports operation report.historical.view
privilege vm-imap operation voicemail.imap.user
privilege ManagePublicList operation voicemail.lists.public
privilege ManagePublicList operation system.debug
```

```
groupname Administrators member cisco
groupname Broadcasters privilege broadcast

restriction msg-notification create
restriction msg-notification min-digits 1
restriction msg-notification max-digits 30
restriction msg-notification dial-string preference 1 pattern * allowed

backup server url "ftp://127.0.0.1/ftp" credentials hidden
"EWlTygcMhYmjazXhE/VNXHCkplVV4KjescbDaLa4fl4WLSPFvv1rWUnfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfG
WTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmP"

calendar biz-schedule systemschedule
 open day 1 from 00:00 to 24:00
 open day 2 from 00:00 to 24:00
 open day 3 from 00:00 to 24:00
 open day 4 from 00:00 to 24:00
 open day 5 from 00:00 to 24:00
 open day 6 from 00:00 to 24:00
 open day 7 from 00:00 to 24:00
 end schedule

ccn application autoattendant aa
 description "autoattendant"
 enabled
 maxsessions 32
 script "aa.aef"
 parameter "dialByExtnAnytime" "false"
 parameter "busOpenPrompt" "AABusinessOpen.wav"
 parameter "dialByExtnAnytimeInputLength" "4"
 parameter "operExtn" ""
 parameter "welcomePrompt" "AAWelcome.wav"
 parameter "disconnectAfterMenu" "false"
 parameter "dialByFirstName" "false"
 parameter "busClosedPrompt" "AABusinessClosed.wav"
 parameter "allowExternalTransfers" "false"
 parameter "holidayPrompt" "AAHolidayPrompt.wav"
 parameter "businessSchedule" "systemschedule"
 parameter "MaxRetry" "3"
 end application

ccn application callrouter aa
 description "callrouter"
 enabled
 maxsessions 32
 script "call_router.aef"
 parameter "rootCallHandlerObjectId" "40cf3e77-d75e-4672-8812-41ac7d3760a3"
 parameter "aaUri" "http://localhost/aa/vxml/callhandler.jsp"
 end application

ccn application ciscomwiapplication aa
 description "ciscomwiapplication"
 enabled
 maxsessions 32
 script "setmwi.aef"
 parameter "CallControlGroupID" "0"
 parameter "strMWI_OFF_DN" "8001"
 parameter "strMWI_ON_DN" "8000"
 end application

ccn application msgnotification aa
 description "msgnotification"
 enabled
 maxsessions 32
```

```
 script "msgnotify.aef"
 parameter "logoutUri" "http://localhost/voicemail/vxmlscripts/mbxLogout.jsp"
 parameter "DelayBeforeSendDTMF" "1"
 end application

ccn application promptmgmt aa
 description "promptmgmt"
 enabled
 maxsessions 32
 script "promptmgmt.aef"
 parameter "appManagementScript" ""
 end application

ccn application voicemail aa
 description "voicemail"
 enabled
 maxsessions 32
 script "voicebrowser.aef"
 parameter "uri" "http://localhost/voicemail/vxmlscripts/login.vxml"
 parameter "logoutUri" "http://localhost/voicemail/vxmlscripts/mbxLogout.jsp"
 end application

ccn engine
 end engine

ccn reporting historical
 database local
 description "se-11-0-0-30"
 end reporting

ccn subsystem sip
 mwi sip sub-notify
 end subsystem

ccn trigger http urlname msgnotifytrg
 application "msgnotification"
 enabled
 maxsessions 2
 end trigger

ccn trigger http urlname mwiapp
 application "ciscomwiapplication"
 enabled
 maxsessions 1
 end trigger

ccn trigger sip phonenumber 5000
 application "callrouter"
 enabled
 maxsessions 32
 end trigger

service phone-authentication
 end phone-authentication

service voiceview
 enable
 end voiceview

voicemail callerid
voicemail broadcast recording time 300
voicemail default messagesize 240
voicemail notification restriction msg-notification
voicemail live-record beep duration 0
```

```
voicemail mailbox owner "MLINE_High Availibility Branch with Voice Survivable Voice_PH1"
size 3600
 end mailbox

voicemail mailbox owner "MLINE_High Availibility Branch with Voice Survivable Voice_PH2"
size 3600
 end mailbox

list name allvoicemailusers number 99991 create

list name allvoicemailenabledcontacts number 99992 create


end
MLINE-CUE#
```

Key Server 1

```
Building configuration...


Current configuration : 3405 bytes
!
! Last configuration change at 11:48:36 PST Fri Jun 18 2010
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname MLINE-LBR-KS1
!
boot-start-marker
boot system flash:c2800nm-adventerprisek9-mz.M2.13
boot-end-marker
!
logging message-counter syslog
logging buffered 5000000
!
no aaa new-model
clock timezone PST -7
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
no ip domain lookup
ip domain name yourdomain.com
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
!
!
!
!
!
!
!
voice-card 0
!
!
!
!
!
archive
 log config
  hidekeys
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp key 1234567ABCDEFG address 172.16.80.1
crypto isakmp key 1234567ABCDEFG address 172.16.81.2
crypto isakmp key 1234567ABCDEFG address 172.16.81.4
crypto isakmp key 1234567ABCDEFG address 172.16.83.2
crypto isakmp key 1234567ABCDEFG address 172.16.82.1
crypto isakmp keepalive 15 periodic
!
!
crypto ipsec transform-set mygdoi-trans esp-aes esp-sha-hmac
!
crypto ipsec profile gdoi-profile-getvpn
 set security-association lifetime seconds 7200
 set transform-set mygdoi-trans
!
crypto gdoi group getvpn
 identity number 1234
 server local
  rekey retransmit 40 number 2
  rekey authentication mypubkey rsa getvpn-export-general
  rekey transport unicast
  sa ipsec 1
   profile gdoi-profile-getvpn
   match address ipv4 199
   replay time window-size 5
  address ipv4 172.16.81.3
  redundancy
   local priority 100
   peer address ipv4 172.16.81.4
!
!
!
!
!
!
```

```
!
interface GigabitEthernet0/0
 ip address 172.16.81.3 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
ip http server
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
ip route 172.16.0.0 255.255.0.0 172.16.81.2
!
access-list 100 remark ACL policies pushed to authenticated group members
access-list 199 permit ip 10.1.150.0 0.0.0.255 192.168.200.0 0.0.0.255
access-list 199 permit ip 10.1.151.0 0.0.0.255 192.168.200.0 0.0.0.255
access-list 199 permit ip 10.1.150.0 0.0.0.255 192.168.201.0 0.0.0.255
access-list 199 permit ip 10.1.151.0 0.0.0.255 192.168.201.0 0.0.0.255
access-list 199 permit ip 192.168.200.0 0.0.0.255 10.1.150.0 0.0.0.255
access-list 199 permit ip 192.168.200.0 0.0.0.255 10.1.151.0 0.0.0.255
access-list 199 permit ip 192.168.201.0 0.0.0.255 10.1.150.0 0.0.0.255
access-list 199 permit ip 192.168.201.0 0.0.0.255 10.1.151.0 0.0.0.255
access-list 199 permit ip host 10.1.3.1 192.168.201.0 0.0.0.255
access-list 199 permit ip 192.168.201.0 0.0.0.255 host 10.1.3.1
access-list 199 permit ip host 10.1.3.2 192.168.201.0 0.0.0.255
access-list 199 permit ip 192.168.201.0 0.0.0.255 host 10.1.3.2

!
control-plane
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet
line vty 5 15
 privilege level 15
 login local
 transport input telnet
!
scheduler allocate 20000 1000
ntp source GigabitEthernet0/1
ntp update-calendar
ntp server 172.16.81.4
end

MLINE-LBR-KS1#
```

Key Server 2

```
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname MLINE-LBR-KS2
!
boot-start-marker
boot system flash:c2800nm-adventerprisek9-mz.150-1.M2.13
boot-end-marker
!
logging buffered 5000000
!
no aaa new-model
!
!
!
clock timezone PST -7
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
no ip domain lookup
ip domain name yourdomain.com
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
voice-card 0
!
!
!
!
!
license udi pid CISCO2851 sn FTX1411AKZU
!
redundancy
!
!
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp key 1234567ABCDEFG address 172.16.80.1
crypto isakmp key 1234567ABCDEFG address 172.16.81.2
```

```
crypto isakmp key 1234567ABCDEFG address 172.16.81.3
crypto isakmp key 1234567ABCDEFG address 172.16.83.2
crypto isakmp key 1234567ABCDEFG address 172.16.82.1

crypto isakmp keepalive 15 periodic
!
!
crypto ipsec transform-set mygdoi-trans esp-aes esp-sha-hmac
!
crypto ipsec profile gdoi-profile-getvpn
 set security-association lifetime seconds 7200
 set transform-set mygdoi-trans
!
crypto gdoi group getvpn
 identity number 1234
 server local
  rekey retransmit 40 number 2
  rekey authentication mypubkey rsa getvpn-export-general
  rekey transport unicast
  sa ipsec 1
   profile gdoi-profile-getvpn
   match address ipv4 199
   replay time window-size 5
  address ipv4 172.16.81.4
  redundancy
   local priority 200
   peer address ipv4 172.16.81.3
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 172.16.81.4 255.255.255.248
 duplex auto
 speed auto
 !
!
interface GigabitEthernet0/1
 description ** CONNECTION TO EXTERNAL NTP SERVER 171.68.10.150 **
 ip address 172.25.222.132 255.255.255.0
 duplex auto
 speed auto
 !
!
ip forward-protocol nd
ip http server
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 172.16.0.0 255.255.0.0 172.16.81.2
ip route 171.68.10.150 255.255.255.255 172.25.222.1
!
access-list 100 remark ACL policies pushed to authenticated group members
access-list 199 permit ip 10.1.150.0 0.0.0.255 192.168.200.0 0.0.0.255
access-list 199 permit ip 10.1.151.0 0.0.0.255 192.168.200.0 0.0.0.255
access-list 199 permit ip 10.1.150.0 0.0.0.255 192.168.201.0 0.0.0.255
access-list 199 permit ip 10.1.151.0 0.0.0.255 192.168.201.0 0.0.0.255
access-list 199 permit ip 192.168.200.0 0.0.0.255 10.1.150.0 0.0.0.255
access-list 199 permit ip 192.168.200.0 0.0.0.255 10.1.151.0 0.0.0.255
access-list 199 permit ip 192.168.201.0 0.0.0.255 10.1.150.0 0.0.0.255
access-list 199 permit ip 192.168.201.0 0.0.0.255 10.1.151.0 0.0.0.255
```

```
access-list 199 permit ip host 10.1.3.1 192.168.201.0 0.0.0.255
access-list 199 permit ip 192.168.201.0 0.0.0.255 host 10.1.3.1
access-list 199 permit ip host 10.1.3.2 192.168.201.0 0.0.0.255
access-list 199 permit ip 192.168.201.0 0.0.0.255 host 10.1.3.2
!

control-plane
!
alias exec coop show crypto gdoi ks coop
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
line vty 5 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
!
scheduler allocate 20000 1000
ntp source GigabitEthernet0/1
ntp update-calendar
ntp server 171.68.10.150 version 3
end

MLINE-LBR-KS2#
```

Headquarters Aggregation Router

```
version 15.0
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname mline-Headend-CE
!
boot-start-marker
boot system flash:c3900-universalk9-mz.SPA.150-1.M2.13
boot-end-marker
!
logging buffered 5000000
no logging monitor
enable password lab
!

aaa new-model
!
!
aaa authentication login default local
!
!
!
!
!
aaa session-id common
!
```

```
!
!
clock timezone PST -7
!
crypto pki token default removal timeout 0
!
!
no ipv6 cef
ip source-route
ip cef
!
!
ip multicast-routing

********** DHCP configuration for Voice ********
ip dhcp excluded-address 192.168.200.100 192.168.200.254
!
ip dhcp pool CUCM7.1.3
   network 192.168.200.0 255.255.255.0
   option 150 ip 192.168.200.100
   default-router 192.168.200.1
!
!
no ip domain lookup

! Only packets matching the access-list 120 are chosen for WCCP redirection. This enables
control over which packets are intercepted and redirected by WCCP for WAAS.

ip wccp 61 redirect-list 120
ip wccp 62 redirect-list 120


multilink bundle-name authenticated
!
voice-card 0
!
license udi pid C3900-SPE150/K9 sn FOC140942FG
license boot module c3900 technology-package uck9
hw-module pvdm 0/0
!
username admin password 0 cisco
username lab password 0 lab
!
redundancy
!
!


!Create access-list to define the traffic for encryption (GREoverIPsec)

access-list 130 permit gre host 172.16.85.58 host 172.16.87.54
access-list 136 permit gre host 172.16.86.18 host 172.16.88.10

! Internet security association and key management protocol (ISAKMP), ISAKMP key  and
IPSEC transform set

crypto isakmp policy 10
 authentication pre-share
!
crypto isakmp key cisc0123 address 172.16.87.54

crypto isakmp key cisco address 172.16.88.10

crypto ipsec transform-set strong esp-3des esp-md5-hmac
```

```
 mode transport

! crypto map configs for GREoverIPsec

crypto map vpn 10 ipsec-isakmp
 set peer 172.16.87.54
 set security-association replay window-size 1024
 set transform-set strong
 match address 130
!
crypto map vpn2 10 ipsec-isakmp
 set peer 172.16.88.10
 set security-association replay window-size 1024
 set transform-set strong
 match address 136



! IKE Phase 1 (ISAKMP) policy is defined. Encryption is AES and pre-shared (PSK)
authentication is used where shared secrets are pre-defined in the encryption devices.
! This is required to enable the GETVPN GM (Group member) and the KS (Key server) to
authenticate each other.

crypto isakmp policy 50
 encr aes
 authentication pre-share
 group 2
 lifetime 1200

crypto isakmp key 1234567ABCDEFG address 172.16.81.3
crypto isakmp key 1234567ABCDEFG address 172.16.81.4

crypto isakmp keepalive 10
!
!

! GETPVN GDOI group is configured using the same identify defined on the KS (Key Server).
The IP addresses of the key servers are specified.

crypto gdoi group getvpn
 identity number 1234
 server address ipv4 172.16.81.3
 server address ipv4 172.16.81.4
!

! crypto map is defined with the "gdoi" type which indicates GETVPN. The crypto map is
applied to the WAN interface
crypto map getvpn-map 50 gdoi
 set group getvpn
!

interface Loopback0
 ip address 10.10.11.185 255.255.255.255
 !
!

 !
*******description ******* GRE over IPSEC TUNNEL 1 ************
interface Tunnel0
 ip address 192.168.16.2 255.255.255.0
 ip pim sparse-dense-mode
 ip igmp join-group 239.0.10.10
 keepalive 5 3
 tunnel source GigabitEthernet0/1.1
```

```
 tunnel destination 172.16.87.54
 !
!
********description ******** GRE over IPSEC Tunnel 2  for dual Multilink bundle scenario
**************
interface Tunnel10
 ip address 192.168.15.2 255.255.255.0
 keepalive 5 3
 tunnel source GigabitEthernet0/1.4
 tunnel destination 172.16.88.10
 !
!
 !
!
interface GigabitEthernet0/0
 no ip address
 ip pim sparse-mode
 load-interval 30
 duplex auto
 speed auto
 !
!
interface GigabitEthernet0/0.200
 description VOICE VLAN
 encapsulation dot1Q 200
 ip address 192.168.200.1 255.255.255.0
!
interface GigabitEthernet0/0.201
 description DATA VLAN
 encapsulation dot1Q 201
 ip address 192.168.201.1 255.255.255.0
 ip wccp 61 redirect in ! WAAS TCP promiscuous mode group 61 configured for traffic
redirection
 ip pim sparse-mode
!
!
interface GigabitEthernet0/0.203
 description ** WAAS SUBNET **
 encapsulation dot1Q 203
 ip address 192.168.203.1 255.255.255.0
 ip wccp redirect exclude in
!
interface GigabitEthernet0/1
 no ip address
 ip pim sparse-mode
 load-interval 30
 duplex auto
 speed auto
 !
!

interface GigabitEthernet0/1.1
******description WAN interface for Voice Enabled Branch tunnel 0******
 encapsulation dot1Q 10
 ip address 172.16.85.58 255.255.255.0
 ip ospf network point-to-point
 crypto map vpn ! crypto map applied to the WAN interface
!

! There are 2 WAN interfaces participating in GETVPN. They correspond to 2 different VRFs
configured
! on the MPLS PE router.

interface GigabitEthernet0/1.2
```

```
 encapsulation dot1Q 20
 ip address 172.16.81.2 255.255.255.0
 ip wccp 62 redirect in ! WAAS TCP promiscuous mode group 62 configured for traffic
redirection
 ip pim sparse-mode
 crypto map getvpn-map ! The crypto map is applied to this interface so that traffic
entering/leaving this interface can be encrypted according to the ACLs defined on the KS
!
interface GigabitEthernet0/1.3
 encapsulation dot1Q 30
 ip address 172.16.83.2 255.255.255.0
 ip wccp 62 redirect in
 crypto map getvpn-map ! ! The crypto map is applied to this interface so that traffic
entering/leaving this interface can be encrypted according to the ACLs defined on the KS

!

interface GigabitEthernet0/1.4
****** description WAN interface for Voice Enabled Branch tunnel 10*****
 encapsulation dot1Q 40
 ip address 172.16.86.18 255.255.255.0
 ip ospf network point-to-point
 crypto map vpn2
!
interface GigabitEthernet0/2
 shutdown
 duplex auto
 speed auto
 !
!
!
! EIGRP routing for GRE over IPSEC tunnel

router eigrp 10
 network 10.1.200.0 0.0.0.255
 network 10.1.201.0 0.0.0.255
 network 10.1.202.0 0.0.0.255
 network 192.168.15.0
 network 192.168.16.0
 redistribute static
 neighbor 192.168.16.1 Tunnel0
 neighbor 192.168.15.1 Tunnel10
!
! PE-CE ROUTING
router ospf 109
 router-id 172.16.80.58
 log-adjacency-changes
 network 10.10.11.185 0.0.0.0 area 109
 network 172.16.85.56 0.0.0.3 area 109
 network 172.16.86.16 0.0.0.7 area 109
!
router ospf 110
 router-id 172.16.81.2
 log-adjacency-changes
 network 192.168.200.0 0.0.0.255 area 110
 network 192.168.201.0 0.0.0.255 area 110
 network 192.168.203.0 0.0.0.255 area 110
 network 172.16.81.0 0.0.0.255 area 110
!
router ospf 200
 router-id 172.16.83.2
 log-adjacency-changes
 redistribute ospf 110 subnets
 network 192.168.200.0 0.0.0.255 area 200
```

```
 network 192.168.201.0 0.0.0.255 area 200
 network 172.16.83.0 0.0.0.255 area 200
!

ip forward-protocol nd
!

! Multicast  configuration

ip pim rp-address 192.168.200.1
ip pim ssm default
ip mroute 192.168.201.0 255.255.255.0 Tunnel0

no ip http server
no ip http secure-server
!

ip sla responder

! IP SLA operations configured here target the branch routers which are configured
! as IP SLA responders.

ip sla 1
 udp-jitter 10.1.150.1 64000 source-ip 192.168.200.1 codec g729a
ip sla schedule 1 start-time now
ip sla 2
 udp-jitter 10.1.151.1 5000 num-packets 1000
ip sla schedule 2 start-time now
ip sla 3
 icmp-jitter 10.1.151.1 source-ip 192.168.201.1
ip sla schedule 3 start-time now

**********SYSLOG configuration **********
logging trap warnings
logging 192.168.201.104

access-list 120 remark WAAS REDIRECT ACL
access-list 120 permit ip 10.1.151.0 0.0.0.255 192.168.201.0 0.0.0.255
access-list 120 permit ip 192.168.201.0 0.0.0.255 10.1.151.0 0.0.0.255

!
nls resp-timeout 1
cpd cr-id 1
!
!
control-plane
 !
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password lab
 transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000


! NTP configuration
```

```
ntp source GigabitEthernet0/1.2
ntp update-calendar
ntp server 172.16.81.4
end

mline-Headend-CE#
```

Cisco Unified Messaging Gateway

```
MLINE-LBR-UMG#show run
Building configuration...


Current configuration : 1972 bytes
!
! Last configuration change at 11:42:51 PST Thu Jul 1 2010
! NVRAM config last updated at 11:42:52 PST Thu Jul 1 2010
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname MLINE-LBR-UMG
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
!
!
!
clock timezone PST -7
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
ip domain name yourdomain.com
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
voice-card 0
!
!
```

```
!
!
!
license udi pid CISCO2851 sn FTX1411AKZT
!
redundancy
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 192.168.200.104 255.255.255.0
 duplex auto
 speed auto
!
!
interface GigabitEthernet0/1
 no ip address
     shutdown
 duplex auto
 speed auto
 !
!
interface Integrated-Service-Engine1/0
 ip address 10.1.8.20 255.255.255.0
 service-module ip address 10.1.9.30 255.255.255.0
 !Application: Cisco UMG running on NME
 service-module ip default-gateway 10.1.8.20
 no keepalive
 !
!
router ospf 110
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 110
 network 192.168.200.0 0.0.0.255 area 110
!
ip forward-protocol nd
ip http server
ip http access-class 23
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 192.168.200.1
!
control-plane
!
line con 0
 exec-timeout 0 0
line aux 0
line 66
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 privilege level 15
```

```
 login local
 transport input telnet
line vty 5 15
 privilege level 15
 login local
 transport input telnet
!
scheduler allocate 20000 1000
ntp update-calendar
ntp server 80.80.81.4
end

MLINE-LBR-UMG#
```

NME-UMG

```
clock timezone America/Los_Angeles

hostname MLINE-UMG

ip domain-name mline.com

line console
  length 0

system language preferred "en_US"

ip name-server 192.168.201.104

ntp server 172.16.81.4 prefer

software download server url "ftp://127.0.0.1/ftp" credentials hidden
"6u/dKTN/hsEuSAEfw40XlF2eFHnZfyUTSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfG
WTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmP"

log trace local enable
license agent max-sessions 9

username cisco create

groupname Administrators member cisco

backup server url "ftp://127.0.0.1/ftp" credentials hidden
"EWlTygcMhYmjazXhE/VNXHCkplVV4KjescbDaLa4fl4WLSPFvv1rWUnfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfG
WTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmP"

registration
 end registration

end
MLINE-UMG
```

List of Features

Table 1 lists the features that are incorporated in the ATM/Kiosk Branch, Survivable Voice Enabled Branch, and High Availability Branch with Survivable Voice solutions. Each row in the table includes the feature name and a link to configuration documentation on Cisco.com.

Table 1 List of Features

Features	Document
3G	*3G High-Speed WAN Interface Card Solution Deployment Guide* http://www.cisco.com/en/US/docs/routers/access/1800/1861/software/guide/3g_sol_dg.html
AAA	*Cisco IOS Security Configuration Guide: Securing User Services, Release 15.1* http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/15_1/sec_user_services_15_1_book.html
BGP	*Cisco IOS IP Routing: BGP Configuration Guide, Release 15.1,* http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/15_1/irg_15_1_book.html
DHCP	*Cisco IOS IP Addressing Configuration Guide, Release 15.1,* *http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/15_1/iad_15_1_book.html*
DMVPN	*Cisco IOS Security Configuration Guide: Secure Connectivity, Release 15.1,* http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/15_1/sec_secure_connectivity_15_1_book.html
EIGRP	*Cisco IOS IP Routing: EIGRP Configuration Guide, Release 15.1,* http://www.cisco.com/en/US/docs/ios/iproute_eigrp/configuration/guide/15_1/ire_15_1_book.html
Flexible NetFlow	*Cisco Getting Started with Configuring Cisco IOS Flexible NetFlow, Release 15.1* http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/get_start_cfg_fnflow_ps10592_TSD_Products_Configuration_Guide_Chapter.html
Frame Relay	*Cisco IOS Wide-Area Networking Configuration Guide, Release 15.1,* http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/15_1/wan_15_1_book.html
GET VPN	*Cisco IOS VPN Configuration Guide,* http://www.cisco.com/en/US/docs/security/vpn_modules/6342/vpn_cg.html
GRE	*Cisco Generic Routing Encapsulation (GRE),* http://www.cisco.com/en/US/tech/tk827/tk369/tk287/tsd_technology_support_sub-protocol_home.html
HSRP	*Cisco IOS IPv6 Configuration Guide, Release 12.4T,* http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4t/ipv6_12_4t_book.html
IP Multicast	*Cisco IOS IP Multicast Configuration Guide, Release 15.1* http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/15_1/imc_15_1_book.html
IPSEC	*Cisco IOS Security Configuration Guide: Secure Connectivity, Release 15.1,* http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/15_1/sec_secure_connectivity_15_1_book.html
IPSLA	*Cisco IOS IP SLAs Configuration Guide, Release 15.1,* http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/15_1/sla_15_1_book.html
MGCP	*Cisco IOS MGCP and Related Protocols Configuration Guide, Release 15.1* http://www.cisco.com/en/US/docs/ios/voice/mgcp/configuration/guide/15_1/vm_15_1_book.html
MLPPP	*Cisco IOS Dial Configuration Guide, Release 15.1,* http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/15_1/dia_15_1_book.html

Table 1 List of Features

Features	Document
NHRP	*Cisco IOS IP Addressing Services Configuration Guide, Release 12.4,* http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/12_4/iad_12_4_book.html
NTP	*Cisco Network Time Protocol (NTP) Introduction,* http://www.cisco.com/en/US/tech/tk648/tk362/tk461/tsd_technology_support_sub-protocol_home.html
OSPF	*Cisco IOS IP Routing: OSPF Configuration Guide, Release 15.1* http://www.cisco.com/en/US/docs/ios/iproute_ospf/configuration/guide/15_1/iro_15_1_book.html
QoS	*Cisco IOS Quality of Service Solutions Configuration Guide, Release 15.1,* http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/15_1/qos_15_1_book.html
SNMP	*Cisco IOS Network Management Configuration Guide, Release 15.1, SNMP Support,* http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/15_1/nm_15_1_book.html
SRST	*Cisco Unified Survivable Remote Site Telephony Configuration Guides,* http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html
SSH	*Cisco IOS Security Configuration Guide: Securing User Services, Release 15.1,* http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/15_1/sec_user_services_15_1_book.html
Syslog	*Cisco IOS Network Management Configuration Guide, Release 15.1*, http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/15_1/nm_15_1_book.html
TACACS	*Cisco IOS Security Configuration Guide, Release 15.1, Security Server Protocols,* http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/15_1/sec_user_services_15_1_book.html
WAAS	*Cisco Wide Area Application Services (WAAS) Software Configuration Guides,* http://www.cisco.com/en/US/products/ps6870/products_installation_and_configuration_guides_list.html
ZBFW	*Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 15.1,* http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/15_1/sec_data_plane_15_1_book.html

Verifying Functionality

Use the following sections to verify services, memory and CPU, and the features that are part of the solution.

Verify Common Services

Use the following show commands and debug commands to verify common services used across all financial branch Cisco Validated Designs (CVDs). To view or print the commands, use the *Command Lookup* tool on Cisco.com by entering the keywords "command lookup" in the Cisco.com search field. A Cisco.com user account is required to use the tool. If you do not have a user account, you can create one,

https://tools.cisco.com/RPF/register/register.do.

Table 2 lists common services that are running in the background in the Cisco Validated Designs, and commands you can use to verify operations and configuration. Debug commands are listed after the table to help you troubleshoot services that are not running properly.

Table 2 Common Services Show Commands

Services	Show Commands	Command Description
CDP	**show cdp neighbors** **show cdp** **show cdp neighbors detail**	Use this command to show CDP neighbors.
		Use this command to verify the configured values of CDP parameters on the router.
		Use this command to check which Cisco devices are connected to the router.
EnergyWise	**show energywise statistics**	Use this command to display the counters for all events and errors.
	show energywise recurrences	Use this command to check the number of recurrences of a predefined energywise policy.
	show energywise	Use this command to display the energywise status and settings for the energywise enabled router.
IP SLA	**show ip sla statistics** **show ip sla responder**	Use this command to display the IP SLA type configured and related statistics on the router.
		Use this command to display the IP SLA responder-related statistics on the router. For instance, this command would be applicable when the router is configured as IP SLA responder.
NetFlow	**show ip flow export** **show ip cache flow**	Use these commands to verify the NetFlow packets exported to the NetFlow collector engine from the branch router.

Table 2 Common Services Show Commands

Services	Show Commands	Command Description
NTP	**show ntp status** **show ntp associations**	Use this command to verify whether the router, which is configured as an NTP client, is synced to the configured NTP server.
		Use this command to verify which NTP server the router is synced.
SNMP	**show snmp**	Use this command to verify the snmp packets/traps/events sent to a configured SNMP server from the router.
SSHv2	**show ip ssh** **show ssh** **show ip flow export** **show ip cache flow**	Use this command to check the SSH version and configuration.
		Use this command to check the state of the current SSH connections (if any) on the router.
		Use this command to check the SSH version and configuration.
		Use this command to check the state of the current SSH connections (if any) on the router.
Zero Touch	**show cns event connections** **show cns config connections**	Use this command to show the status of communication between the embedded CNS agent in the IOS and the event handler on the Cisco Configuration Engine.
		Use this command to show the status of communication between the embedded CNS agent in the IOS and the configuration handler on the Cisco Configuration Engine.

Debug Commands

- debug tacacs
- debug aaa
- debug ip sla error
- debug ip sla trace
- debug flow exporter
- debug snmp packets
- debug ntp packets
- debug ip ssh

Verify Memory and CPU

Table 3 lists commands that you enter on the command line interface to learn about memory and CPU statistics for the router.

Table 3 Memory and CPU Show Commands

Show Commands	Command Description
show process cpu sorted	Use this command to display sorted detailed CPU utilization statistics.
show process memory sorted	Use this command to show memory used.
show process cpu history	Use this command to display detailed CPU utilization statistics (CPU use per process) when Cisco IOS or Cisco IOS Software Modularity images are running.
show debug memory leaks summary	Use this command to display a summary of detected memory leaks.

Verify Features

The following features are included in the ATM/Kiosk Branch, Survivable Voice Enabled Branch, and High Availability Branch with Survivable Voice solutions. Use the following show commands and debug commands to verify common services in the Cisco Validated Designs (CVDs). To view or print the commands, use the *Command Lookup* tool on Cisco.com. A Cisco.com user account is required to use the tool. If you do not have a user account, you can create one,

https://tools.cisco.com/RPF/register/register.do.

- Cisco Unified SRSV-CUE, page 2-84
- EnergyWise, page 2-85
- Fax, page 2-85
- Frame Relay, page 2-85
- HSRP, page 2-86
- Multicast, page 2-86
- NetFlow, page 2-87
- PRI, page 2-87
- QoS, page 2-87
- SSHv2, page 2-90
- Voice, page 2-90
- Wide Area Application Services (WAAS), page 2-93

Cisco Unified SRSV-CUE

Table 4 provides commands that verify Cisco Unified SRSV-CUE operations and configurations.

Table 4 Cisco Unified SRSV-CUE Show Commands

Show Commands	Command Description
show srsv auto-attendant	Use this command to display the status of the auto-attendant configuration that is provisioned by the Cisco UMG.
show srsv configuration	Use this command to display the SRSV configuration.
show ccn application	Use this command to display the currently configured applications.
show ccn engine	Use this command to display details of the configured Cisco Unity Express software engine.
show ccn subsystem jtapi	Use this command to display the JTAPI subsystem parameters.
show system language installed	Use this command to display the languages that are available for use.
show voicemail configuration	Use this command to display the configured *From* address for outgoing e-mail.
show voicemail detail	Use this command to display the details for a general delivery mailbox or a subscriber with the name value.
show voicemail limits	Use this command to display default values for all mailboxes.
show voicemail mailboxes	Use this command to display all configured mailboxes and their current storage status.
show voicemail mailboxes	Use this command to display all configured mailboxes and their current storage status.
show voicemail messages future	Use this command to display all messages scheduled for future delivery.
show voicemail users	Use this command to list all the local voicemail subscribers.

Debug Commands

- trace srsx srsv-engine all
- show trace buffer tail

EnergyWise

Table 5 provides commands that display EnergyWise settings and configurations.

Table 5 EnergyWise Show Commands

Show Commands	Command Description
show energywise neighbors	Use this command to delete the discovered neighbors and end points running agents or clients from the EnergyWise neighbor table.
show energywise	Use this command to display the EnergyWise settings, the status of the domain member, and the status of the switch port with a connected end point.
show energywise version	Use this command to display the EnergyWise version.

Fax

Table 6 provides commands that verify fax operations and configurations.

Table 6 Fax Show Commands

Show Commands	Command Description
show voip rtp conn	Use this command to display Real-Time Transport Protocol (RTP) event packets.
show call active voice	Use this command to display call information for calls in progress.
show sccp conn	Use this command when the fax transcoder is involved.

Debug Commands

- debug mgcp packets
- debug voip rtp packets
- debug sccp conn

Frame Relay

Table 7 provides a command that verifies Frame Relay statistics.

Table 7 Frame Relay Show Command

Show Command	Command Description
show frame-relay pvc [*number*]	Use this command to display statistics like input/output packets/bytes and packet drops for specifics configured on frame-relay encapsulated interfaces on the router.

Debug Commands

- debug frame-relay events
- debug frame-relay packet

HSRP

Table 8 provides a command that verifies HSRP groups and interface.

Table 8 High Availability Show Command

Show Command	Command Description
show standby	Use this command to show the different HSRP groups and the associated interfaces. It also displays useful information about the current role of the router (active/standby), priorities, authentication string (if any), and interfaces being tracked.

Debug Commands

- debug standby packets
- debug standby events

Multicast

Table 9 provides commands that verify the Protocol Independent Multicast (PIM) neighbor relationships.

Table 9 Multicast Show Commands

Show Commands	Command Description
show ip pim neighbor	Use this command to display information about PIM neighbors discovered by PIMv1 router query messages or PIMv2 hello messages.
show ip igmp groups	Use this command to display the multicast groups with receivers that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).
show ip pim rp mapping	Use this command to display the mappings for the PIM group to the active rendezvous points.
show ip mroute	Use this command to display the contents of the multicast routing (mroute) table.
show ip multicast	Use this command to display information about IP multicast global configuration parameters.

Debug Commands

- debug ip mpacket
- debug ip mfib ps

NetFlow

Table 10 provides commands that verify NetFlow operations and configurations.

Table 10 NetFlow Show Commands

Show Commands	Command Description
show ip flow export	Use this command to display the status and the statistics for NetFlow accounting data export, including the main cache and all other enabled caches.
show ip flow top-talkers	Use this command to display the statistics for the NetFlow aggregated top talkers or not aggregated top flows.
show ip cache flow	Use this command to display a summary of the NetFlow accounting statistics.

PRI

Table 11 provides a command that verifies PRI channel information.

Table 11 PRI Channels Show Commands

Show Commands	Command Description
show isdn status	Use this command to show information about memory, Layer 2 and Layer 3 timers, and the status of PRI channels.

Debug Commands

- debug isdn q931
- debug isdn q921

QoS

Table 12 provides commands that display statistics and configurations for the QoS policies on router interfaces.

Table 12 Quality of Service Show Commands

Show Commands	Command Description
show class-map	Use this command to display all of the class maps and their matching criteria.
show policy-map interface	Use this command to display the statistics and the configuration of the input and output policies that are attached to an interface.

Debug Commands

- debug qos events
- debug qos stats
- debug qos cce

Routing

Table 13 provides commands that verify routing configurations.

Table 13 Routing Show Commands

Show Commands	Command Description
show ip bgp	Use this command to display the bgp related configurations on the router.
show ip eigrp	Use this command to display the eigrp related configurations on the router.
show ip route bgp	Use this command to display bgp routes discovered on the router.
show ip route eigrp	Use this command to display eigrp routes discovered on the router.
show ip bgp neighbor	Use this command to display all the bgp neighbors of the router.
show ip eigrp neighbor	Use this command to display all the eigrp neighbors of the router.
show ip route	Use this command to display all the routes in the routing table of the router.
show ip route track	Use this command to display the state of the routing table (up/down) for the routes tracked on the router.
show ip mroute active	Use this command to display the contents of the multicast routing (mroute) table, which displays the rate that active sources are sending to multicast groups in kilobits per second.
show ip mroute count	Use this command to display the contents of the multicast routing (mroute) table, which displays statistics about the group and source, including number of packets, packets per second, average packet size, and bytes per second.

Debug Commands

- debug bgp all events
- debug eigrp packets
- debug bgp ipv4 unicast/multicast

Security

- IPSec, page 2-89
- Zone-based Firewall, page 2-89
- GETVPN, page 2-89

IPSec

Table 14 provides commands that verify common security features and operations.

Table 14 Security—IPSEC Show Commands

Show Commands	Command Description
show crypto ipsec sa	Use this command to display the settings used by current security associations (SAs).
show crypto isakmp sa	Use this command to display current IKE SA's.
show crypto isakmp policy	Use this command to display the parameters for each Internet Key Exchange (IKE) policy.

Debug Commands

- debug crypto ipsec
- debug crypto isakmp

Zone-based Firewall

Table 15 provides commands that verify Zone-based Firewall policies and statistics.

Table 15 Zone-based Firewall Show Commands

Show Commands	Command Description
show zone-pair security	Use this command to display the source zone, destination zone, and policy attached to the zone-pair.
show zone security	Use this command to display zone security information.
show policy-map type inspect zone-pair	Use this command to display the runtime inspect type policy map statistics and information such as sessions existing on a specified zone pair.

Debug Commands

- debug zone-security events

GETVPN

Table 16 provides commands that verify VPN operations.

Table 16 Security Show Commands

Show Commands	Command Description
show crypto gdoi gm	Use this command to verify that the GETVPN Group Member (GM) (that is, router) has successfully registered to a key server.
show crypto gdoi gm acl	Use this command to display the ACLs that have been downloaded from the Key Server. It also displays the local configured ACLs, if any. These ACLs determine the traffic that is selected for encryption.

Table 16 Security Show Commands

Show Commands	Command Description
show crypto gdoi gm replay	Use this command if TBAR is configured. It displays the TBAR parameters. If there are TBAR errors, this command helps you check the time change between this GM and other GMs.
show crypto ipsec sa	Use this command to display the IPSec security associations currently established on the router. When interpreting the output, remember that the SAs are unidirectional and they are unique in each security protocol.
show crypto gdoi ks members	Use this command only on the Key Server. Use it to display the group members that are currently in the GETVPN group and managed by the key server(s).
show crypto gdoi ks coop	Use this command only on the Key Server. Use it when multiple key servers are operating in COOP mode. This command displays the state of the key servers (Active/Secondary, priority, and so on).
show crypto gdoi ks policy	Use this command only on the Key Server. Use it to display the TEK and KEK policy currently configured and applied to the group members.

Debug Commands

- debug crypto gdoi gm
- debug crypto gdoi ks
- debug crypto ipsec

SSHv2

Table 17 provides commands that verify SSHv2 operations.

Table 17 SSHv2 Show Commands

Show Commands	Command Description
show ssl	Use this command to display the status of Secure Shell (SSH) server connections on the router.
show ip ssh	Use this command to display the version and configuration data for Secure Shell (SSH).

Voice

Voice Calls

Table 18 provides commands that verify Voice call operations and configurations.

Table 18 Voice Show Commands

Show Commands	Command Description
show voice call summary	Use this command to display calls from PSTN to customer-site/headquarters or vice versa through PRI.
show call active voice br	Use this command to display call information.
show voip rtp conn	Use this command to display Real-Time Transport Protocol (RTP) named event packets.
show sccp connection	Use this command if the call goes to voicemail and there is transcoding.
show call active voice echo-canceller summary	Use this command to display the state of echo canceller.
show call active voice summary	Use this command to display a summary of voice call information in progress.

Debug Commands

- debug isdn q931
- debug isdn q921
- debug sccp all
- debug mgcp packets
- debug voip rtp conn

MGCP

Table 19 provides commands that verify Voice MGCP gateway operations and configurations. Table 20 provides commands that verify MGCP fallback operations.

Table 19 Voice MGCP Gateway Show Commands

Show Commands	Command Description
show ccm-manager	Use this command to verify the active and redundant configured Cisco CallManager servers. It also indicates whether the gateway is currently registered with the Cisco CallManager.
show mgcp	Use this command to verify the status of the router MGCP parameters. You should refer to the IP address of the Cisco CallManager server that you use. All other parameters remain in their default state in this configuration.
show mgcp endpoint	Use this command to show the voice ports (endpoints) that are under MGCP control in the router. This command verifies which voice ports have been bound to the MGCP application.

Table 19 Voice MGCP Gateway Show Commands

Show Commands	Command Description
show mgcp connection	Use this command to display any active MGCP connections. This corresponds to the MGCP Member Configuration identifier in Cisco CallManager. It tells you which port on the router is the endpoint in the call.
show voice port mod_number/slot_number /port_number	Use this command to verify the current status and configuration of the voice ports on the router.
show mgcp statistics	Use this command to show statistical information related to MGCP activity on the router.
show dial-peer voice summary	Use this command to display dial-peer information.
show sccp	Use this command to verify if the external transcoder is registered to the Call-manager.

Table 20 MGCP Fallback Show Commands

Show Commands	Command Description
show call-manager-fallback all	Use this command to display the detailed configuration of all CiscoIP Phones, voice ports, and dial peers in your network during Cisco CallManager fallback.
show call-manager-fallback dial-peer	Use this command to display the output for the dial peers during Cisco CallManager fallback.
show ccm-manager fallback-mgcp	Use this command to display a list of Cisco CallManager servers and their current status and availability.

Debug Commands

- debug mgcp [all | errors | events | packets | parser]
- debug ccm-manager events

Voice Security

Table 21 provides commands that verify Voice security features and operations.

Table 21 Voice Show Commands

Show Commands	Command Description
show crypto isakmp sa	Use this command to display the state of isakmp security associations currently established on the router.
show crypto session detail	Use this command to display the state of the crypto tunnel established on the router.
show dmvpn detail	Use this command to display the state of the DMVPN tunnel, tunnel source/destination ip addresses, and NBMA peers on the router.

Table 21 Voice Show Commands

Show Commands	Command Description
show ip nhrp summary	Use this command to display NBMA and NHRP related information on the router.
show ephone registered	Use this command in SRST mode to verify that the SCCP phones are registered to the router.
show isdn stat	Use this command to check the status of the ISDN PRI connection to the PSTN.
show dial-peer voice summary	Use this command to see a summary of the dial-peers and the status.
show voip rtp connections	Use this command to check all active RTP connections (IPs and ports) on the router. It is useful on the CUBE device where there are two legs of media being bridged.
show call active voice brief	Use this command to see a summary of all voice connections currently active on the router. It includes information on Tx/Rx packets, codecs used, and the endpoint IP addresses.

Debug Commands

- debug voice ccapi inout
- debug isdn q931
- debug voip rtp packet
- debug ccsip all
- debug ephone detail
- debug dmvpn all all
- debug crypto ipsec

Wide Area Application Services (WAAS)

Table 22 provides a command that is entered from the Cisco Internet Operating System (IOS) command prompt on the router. The command also verifies Cisco Web Cache Communication Protocol (WCCP) on the WAE device.

Table 22 WAAS Router-Side Show Command

Show Commands	Command Description
show ip wccp	Use this command to display the global WCCP information, including the configured service groups, statistics on pkts seen/redirected to the WAAS module, and the router identifier and version. This is a useful command to verify that the basic WAAS module is up and running on the router.

Table 23 lists commands that are entered from the WAE device command prompt, and they verifies WCCP on the WAE device.

Table 23 WAE Module Show Commands

Show Commands	Command Description
show wccp	Use this command to display the WCCP information for a Cisco WAE device.
show wccp gre	Use this command to display the Cisco WCCP generic routing encapsulation (GRE) packet-related information.
show wccp routers	Use this command to display the routers seen or not seen by this Cisco WAE device.
show wccp status	Use this command to display the version of Cisco WCCP that is enabled and running.
show device-mode configuredcurrent	Use this command to display the configured or current device mode of a Cisco Wide Area Application Services (WAAS) device.
show device-mode configured/current	Use this command to display the configured or current device mode of a Cisco Wide Area Application Services (WAAS) device.
show egress-methods	Use this command to display the egress method that is configured and being used on a particular Cisco WAE device.
show cifs connectivity peers	Use this command to display run-time information on edge-core connectivity and a list of connected cores.
show cifs sessions count	Use this command to display run-time information about the active CIFS sessions and the number of pending CIFS requests.
show cifs sessions list	Use this command to display run-time information on active CIFS sessions and a listing of connected CIFS sessions.
show policy-engine application classified	Use this command to display information about the specified application classifier or all classifiers if no application is specified. It includes the application name and the match statement that defines the interesting traffic.
show statistics cifs	Use this command to display the CIFS statistics information.
show statistics dre detail	Use this command to display data redundancy elimination (DRE) general statistics for a Cisco WAE device.
show statistics tfo detail	Use this command to display TFO statistics for a Cisco WAE device. It is a useful command for debug problems such as connection overload and checking the total number of hits.

Debug Commands

- debug wccp events
- debug wccp errors

CHAPTER 3

Management Information Databases

This chapter provides a list of the MIBS that are included in the solutions.

- ATM/Kiosk Branch
- Voice Enabled Branch
- High Availibility Branch with Voice Survivable Voice

Table 3-1 ATM/Kiosk Branch

MIB	Description
CISCO-BGP4-MIB	This MIB provides BGP status and statistics.
CISCO-CDP-MIB	This MIB contains information related to CDP and enables SNMP agents to obtain information about a device's neighbor.
CISCO-NETFLOW-MIB	This MIB provides a method for getting netflow cache information, and current netflow configuration and statistics.
CISCO-NTP-MIB	This MIB enables users to monitor the status of NTP on a device.
CISCO-IPSEC-MIB	This IPSec MIB allows IPSec configuration monitoring and IPSec status monitoring using SNMP.
CISCO-EIGRP-MIB	This MIB provides EIGRP status and statistics.
CISCO-FRAME-RELAY-MIB	This MIB provides Frame Relay statistics.

Table 3-2 Voice Enabled Branch

MIB	Description
CISCO-CLASS-BASED-QOS-MIB	This MIB provides read access to QoS configuration and statistics information for Cisco platforms that support the modular QoS command line interface.
CISCO-EIGRP-MIB	This MIB provides EIGRP statistics.
CISCO-ENERGYWISE-MIB	This MIB is used to manage and optimize Cisco power extensions specifications.
CISCO-IPSEC-MIB	This MIB allows IPSec configuration monitoring and IPSec status monitoring using SNMP.

Table 3-2 Voice Enabled Branch

MIB	Description
CISCO-ICSUDSU-MIB	This MIB is used to monitor the T1 interfaces.
CISCO-NETFLOW-MIB	This MIB provides a simple and easy method to get netflow cache information, and current netflow configuration and statistics.

Table 3-3 High Availibility Branch with Voice Survivable Voice

MIB	Description
CISCO-BGP4-MIB	This MIB provides BGP status and statistics.
CISCO-CDP-MIB	This MIB contains information related to CDP and enables SNMP agents to obtain information about a device's neighbor.
CISCO-CLASS-BASED-QOS-MIB	This MIB provides read access to QoS configuration and statistics information for Cisco platforms that support the modular QoS command line interface.
CISCO-ENERGYWISE-MIB	This MIB is used to manage and optimize Cisco power extensions specifications.
CISCO-ENVMON-MIB	This MIB tracks the status of the environment monitor on devices.
CISCO-HSRP-MIB	The HSRB MIB enables SNMP get operations to allow network devices to get reports about HSRP groups in a network from the network management station.
CISCO-ISDN-MIB	This MIB provides status on ISDN channels.
CISCO-NETFLOW-MIB	This MIB provides a way to get netflow cache information, and current netflow configuration and statistics.
CISCO-NTP-MIB	This MIB enables users to monitor the status of NTP on a device.
CISCO-IPSEC-MIB	This MIB allows IPSec-configuration monitoring and IPSec-status monitoring using SNMP.