White Paper

Cisco Catalyst 6500 Voice Deployment Guide

The Cisco® Catalyst® 6500 Series platform is widely deployed as the premier switch platform of choice for small enterprise networks, large multinational companies, and transcontinental service providers. One of the emerging technologies gaining particular interest across this customer set is the integration of voice across a traditional data network. Many questions arise when considering implementing voice applications over a Cisco Catalyst 6500-based network, including: How can I differentiate my voice traffic from data traffic from a quality-of-service (QoS) perspective? Can I easily provision the network for voice? How can I monitor and troubleshoot voice problems? How can I protect my traffic so that untrusted sources cannot listen to my voice calls?

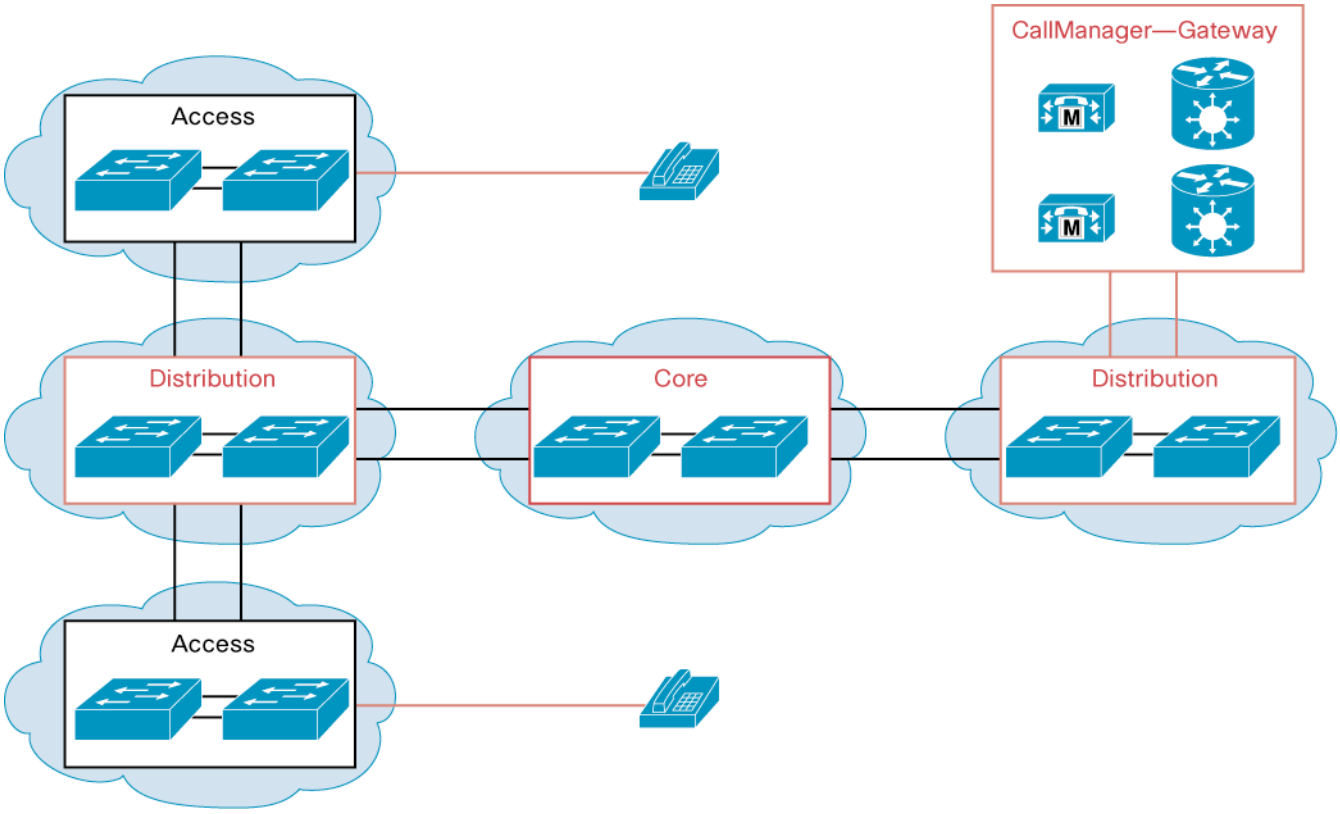
This document provides simple deployment recommendations based on Cisco Catalyst 6500 Series Switches running Cisco IOS® Software Modularity to optimize Cisco Unified Communications in the areas of security, availability, management, and service delivery (QoS).

Using a traditional campus network design model as a reference point, the document provides recommendations for each of these areas as they relate to handling converged voice applications throughout the various layers of that network.

DEPLOYMENT OVERVIEW

For illustration purposes, this document refers to a traditional 3-tier campus model consisting of access, distribution, and core switches, with Cisco Unified Communications devices connected to the access switches and call managers and gateway devices attached to a given distribution block (Figure 1).

Figure 1. Three-Tier Reference Model for VoIP Deployment



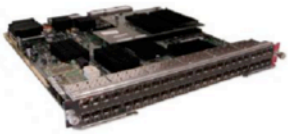
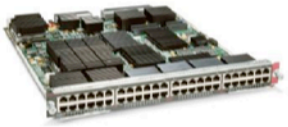
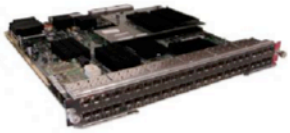
The network is divided into the following submodules:

- Access layer 1 (10-Gigabit Ethernet uplinks)
- Access layer 2 (Gigabit Ethernet uplinks)
- Distribution layer 1 (access layer aggregation)
- Distribution layer 2 (server and services aggregation)
- Core layer

Additionally, Cisco Systems® recommends deployment of the modules shown in Figure 2 in each of the network layers.

Figure 2. Module Deployment

Supervisor Engine	Modules
Access Layer 1	
 Supervisor Engine 32; 8 Gigabit Ethernet	 Part number WS-X6148A-45AF
Access Layer 2	
 Cisco Catalyst 6500 Series Supervisor Engine 32; 10 Gigabit Ethernet	 Part number WS-X6148A-GE-AF

Supervisor Engine	Modules		
Distribution Layer 1			
 Cisco Catalyst 6500 Series Supervisor Engine 720	 Part number WS-X6704-10GE	 Part number WS-X6724-SFP	 Part number WS-X6748-GE-TX
Distribution Layer 2			
 Supervisor Engine 720	 Part number WS-X6704-10GE	 Part number WS-X6724-SFP	 Part number WS-SVC-NAM2

Supervisor Engine	Modules
Core Layer	
 Supervisor Engine 720	 Part number WS-X6704-10GE

DEPLOYMENT DETAILS

A detailed breakdown of Cisco recommendations regarding how to best deploy a Cisco Unified Communications solution over a network that has been architected with the Cisco Catalyst 6500 Series Switches follows.

The sections are subdivided into global recommendations and access-, distribution-, and core-layer requirements.

Global Recommendations

This section details recommendations for all switches in the network and includes items such as Cisco IOS Software Modularity and CPU protection mechanisms.

Cisco IOS Software Modularity

Availability is critical to traditional voice networks. If failures occur or if software needs to be upgraded, system downtime must be minimal. Cisco IOS Software Modularity is recommended to meet this requirement throughout the network with the view of increasing network uptime.

Cisco IOS Software Modularity offers the ability to efficiently restart a process (to minimize unplanned downtime) and allows for online patching of various subsystems.

Patching occurs on a subsystem level, and restarting initiates on a processwide level. Previously a system needed to be reloaded if a process was either not responding anymore or needed to be patched. With software modularity the administrator has greater control at the process level. The patching function of software modularity allows the customer to react in a timelier manner to security advisories (PSIRT—Product Security Incident Response Team). A patch can be applied online and can also be removed if needed. Patches can be applied during runtime, depending on the part of the operating system being patched. This process is referred to as In Service Software Patching (ISSP).

Because this feature is an enhancement to the existing Cisco IOS Software, a minimal amount of training is required for those familiar with the Cisco IOS command-line interface (CLI). Software modularity is currently shipping on the Cisco Catalyst 6500 Series Supervisor Engine 720 with Cisco IOS Software Release 12.2(18)SXF4.

In order use the patching capabilities of Cisco IOS Software Modularity, you must “install” the image:

```
6509-Access#install file disk0:s3223-ipservicesk9-vz.122-18.SXF3 bootdisk:/sys
Source filename [s3223-ipservicesk9-vz.122-18.SXF3]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!<…snip…>
Verifying checksums of extracted files
Verifying installation compatibility
Finalizing installation ...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!<…snip…>
Computing and verifying file checksums
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!<…snip…>
Writing installation meta-data. Please wait ...
[DONE]
```


CPU Protection

Because the network now carries both voice and mission-critical data, it is important to protect the network itself from malicious or nondeliberate (such as virus outbreaks) attacks. In today's world a multitude of widely available tools can exploit inherent vulnerabilities in a network device, one of these being the switch control plane (CPU).

Although enterprise-class switches today make minimal use of the CPU to forward traffic, it is still a vital part of the switch because the CPU is responsible for important tasks such as learning the topology of the network. This requirement necessitates active measures to ensure the CPU is adequately protected. Control Plane Policing (CoPP) and Control Plane Rate Limiters (CPRL) can assist in this area.

Control Plane Policing

CoPP allows filtering and rate limiting of traffic sent to the route processor. The CoPP capability is achieved by using existing QoS policers and applying them to a new interface, the "control-plane" interface. This interface is attached to the route processor (refer to the control-plane interface in Figure 3). As a result, a control-plane policy rate limits traffic destined for the route-processor CPU (CoPP affects only input packets, not output packets), and it can thus prevent denial-of-service (DoS) traffic from congesting the route-processor CPU.

CoPP-configured policies depend heavily on the customer environment and where the switch is used in this environment. For example, an enterprise access layer switch and an enterprise core switch may run different protocols, and the expected CPU load for a given common protocol is different in these two environments. The following methodology can be used to determine the right CoPP policies for a given switch:

1. Determine the classification scheme for your network: enumerate the known types of traffic that access the route processor and divide them into categories (classes). Examples of categories include an Exterior Gateway Protocol (EGP) class, Interior Gateway Protocol (IGP) class, management class, reporting class, monitoring class, critical application class, undesirable class, and default class.
2. Classify traffic going to the route-processor CPU using access control lists (ACLs). For each category identified in Step 1, different types of traffic can be further categorized using granular access control entries, narrowing the ACL permit statements to allow only known authorized source addresses.
3. Review identified traffic, adjust the classification, and apply liberal CoPP policies for each class of traffic. It is essential to apply a corresponding policing action for each class, because the Cisco Catalyst 6500 Series ignores classes that do not have a corresponding policing action. If the traffic in a given class should not be rate limited, configure a transmit policing conform action with a high rate and a policing exceed action of drop (for example, **police 31500000 conform-action transmit exceed-action drop**). Alternatively, both **conform-action** and **exceed-action** could be set to transmit, but doing so will allocate a default policer as opposed to a dedicated policer with its own hardware counters.

Refine CoPP policies based on CoPP and software Access Control Entry (ACE) counters. On the Cisco Catalyst 6500 Series, the administrator can use the following commands to collect these statistics: **show policy-map control-plane** [input class <class_name**>],** **show mls qos ip**, and **show access-list**.

The following is a configuration example of CoPP for the reporting class of traffic such as Internet Control Message Protocol (ICMP). It is first essential to use the "mls qos" CLI to allow hardware CoPP DoS mitigation. Access lists and class maps should then be defined to match the ICMP traffic. The following CoPP policy map limits reporting traffic to 100 kbps. After the policy map is applied to the control-plane interface with the **service-policy** input command, ICMP traffic to the route processor is limited to 100 kbps in hardware.

Enable QoS globally:
6509-Core(config)# mls qos

Create an access-list matching on ICMP traffic:
6509-Core(config)# access-list 101 permit icmp any any

Create a class map to reference the ICMP access list:

6509-Core(config)# class-map reporting

6509-Core(config-cmap)# match access-group 101

Create a policy map that references the class map and define a policer to drop the traffic after the committed information rate (CIR) (100 kbps) has been reached:

6509-Core(config)# policy-map control-plane-policy

6509-Core(config-pmap)# class reporting

6509-Core(config-pmap-c)# police 100000 conform-action transmit exceed-action drop

Apply the policer under the control-plane interface:

6509-Core(config)# control-plane

6509-Core(config-cp)# service-policy input control-plane-policy

Control Plane Rate Limiting

The Cisco Catalyst 6500 Series Supervisor Engine 32 and Supervisor Engine 720 support platform-specific, hardware-based rate limiters for special networking scenarios resembling DoS attacks. These hardware CPU rate limiters are called "special-case" rate limiters because they cover a specific predefined set of IPv4, IPv6, unicast, and multicast DoS attack scenarios. These DoS attack scenarios identify special cases where traffic needs to be processed by the switch-processor or route-processor CPU. Examples include multicast traffic for which a destination prefix cannot be found in the routing table, dropped traffic that needs to be processed by the CPU to send an ICMP unreachable message back to the source, and special packet types that cannot be identified with an access list.

For a list of recommended rate limiters, refer to Appendix A.

UDLD

Unidirectional Link Detection Protocol (UDLD) is a useful feature designed to detect and recover from links that have become unidirectional or faulty over time. This feature allows the switch to reduce the likelihood of black-holing traffic or the formation of spanning-tree loops. UDLD is an important feature in a unified communications environment because it helps maximize network availability, and if link degradation occurs, it helps ensure that partially degraded links are disabled, minimizing traffic loss and the potential for formation of loops.

The Cisco Catalyst 6500 Series Switch periodically transmits UDLD packets to neighbor devices on LAN ports with UDLD enabled. If the packets are echoed back within a specific timeframe and they are lacking a specific acknowledgment (echo), the link is flagged as unidirectional and the LAN port is shut down.

With UDLD aggressive mode enabled, when a port stops receiving UDLD packets from an established neighbor, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled.

Cisco recommends enabling UDLD globally and aggressive UDLD on the fiber uplink ports of the access switches. Note that aggressive UDLD is enabled on all fiber ports when aggressive UDLD is enabled globally.

The following commands enable UDLD and aggressive UDLD globally:

6509-Access(config)#udld enable

6509-Access(config)#udld aggressive

To verify the UDLD state of a port, execute the following command:

```
6509-Access#sh udld tenGigabitEthernet 5/1
Interface Te5/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5
 Entry 1
 ---
 Expiration time: 41
 Device ID: 1
 Current neighbor state: Bidirectional
 Device name: SMG0823N1ST
 Port ID: Te1/1
 Neighbor echo 1 device: SAL0802SHHM
 Neighbor echo 1 port: Te5/1
 Message interval: 15
 Time out interval: 5
 CDP Device name: 6509-Distribution
```

Generic Online Diagnostics

High availability is a critical objective for networks enabled for Cisco Unified Communications. The Cisco Catalyst 6500 provides a robust set of high-availability features to help maximize system uptime and overall network availability. Primary among the features that support high availability is the Generic Online Diagnostics (GOLD) feature.

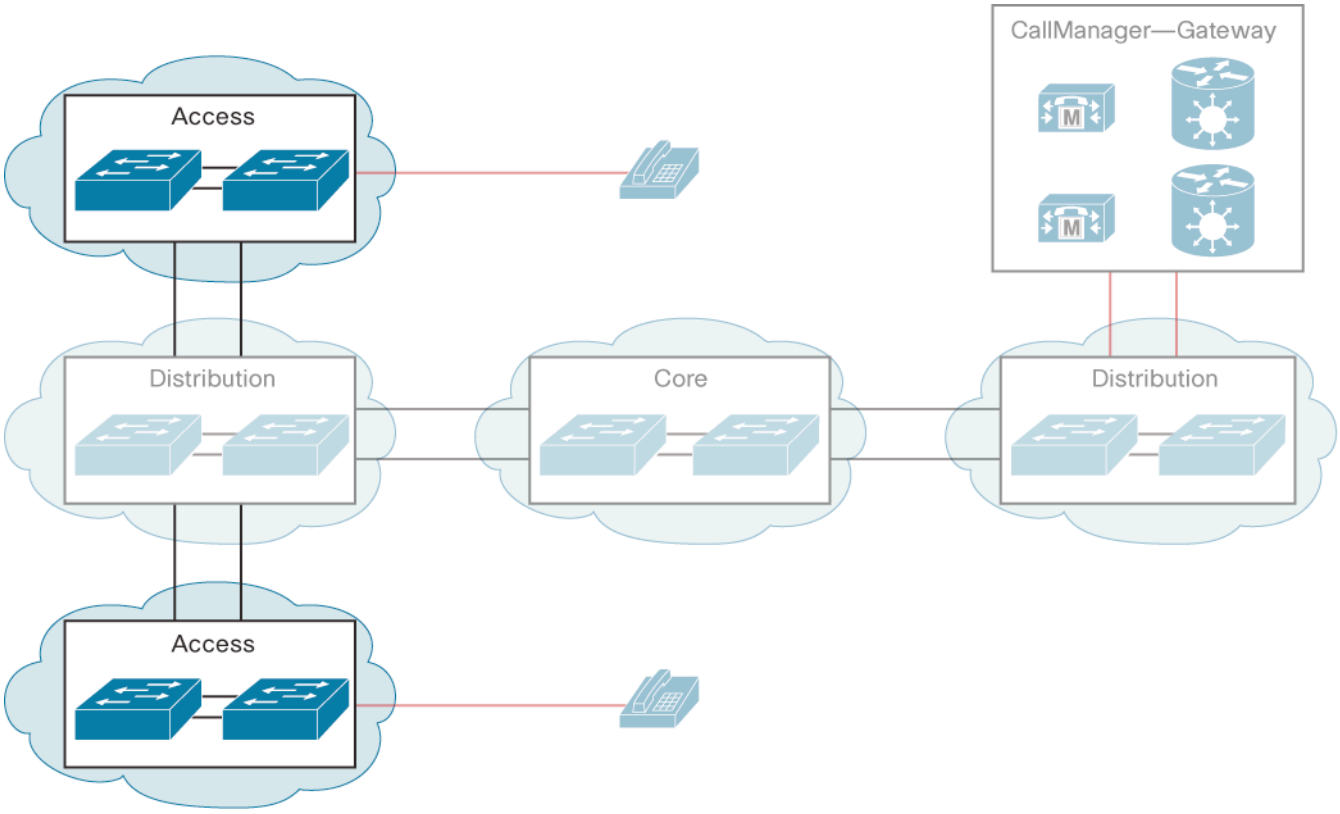
During bootup of a supervisor engine or module, such as a service or interface module (card), the GOLD process checks several functions before allowing the component to become active, thereby eliminating activation of faulty modules. From minimal to exhaustive test sets can be run against the hardware at startup time. Runtime diagnostics include nondisruptive monitoring tests that run in the background at selected intervals to pick up developing problems—unstable supervisors or modules switched out of service—and disruptive tests, which can be initiated on demand or scheduled as regular maintenance.

Note that the default settings of GOLD are adequate for the purposes of proactively detecting faults that may occur through the operating lifecycle of the Cisco Catalyst 6500. However, if you need to enable further diagnostics, refer to the following documentation: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/diags.htm

Access Layer

The role of switches in the access layer is to provide initial connectivity for end hosts and IP-enabled phones. Hence, it is here that most efforts with regard to QoS, security, availability, and management should be focused (Figure 3).

Figure 3. Access Layer Considerations



Access layer 1 consists primarily of mixtures of 10/100/1000 connected devices as well as Cisco IP phones. Note that the only Cisco IP phone currently capable of supporting 10/100/1000 connectivity is the Cisco Unified IP Phone 7971G-GE.

Because of the requirement of supporting multiple 10/100/1000 devices, Cisco recommends uplinking access switches to the distribution layer through 10 Gigabit Ethernet links. Additionally, the recommended choice of line cards to deploy here is the Cisco Enhanced 48-port 10/100/1000BASE-T Ethernet Switching Module (part number WS-X6148A-GE-45AF), which provides 48 ports of 10/100/1000, IEEE 802.3af Power over Ethernet (PoE) capabilities on each port, as well as extensive queues and thresholds for QoS purposes.

Access layer 2 consists primarily of 10/100 devices as well as non-Gigabit Ethernet-enabled Cisco IP phones. For the purposes of illustration, these devices are connected to the distribution layer through Gigabit Ethernet links. The recommended choice of line cards to deploy in this scenario is the Cisco Enhanced 48-port 10/100/1000BASE-T Ethernet Switching Module (part number WS-X6148A-45AF), which provides 48 ports of 10/100 connectivity, IEEE 802.3af PoE capabilities for each port, as well as extensive queues and thresholds for QoS purposes.

The following sections address access layers 1 and 2.

Basic Connectivity

End users and Cisco IP phones can be connected to the Cisco Catalyst 6500 in two ways:

- IP phone and end workstations each using a separate switch port
- A single port for IP phone with the workstation daisy-chained off the phone

This guide uses the daisy-chain deployment model for illustration purposes (Figure 4).

Figure 4. Daisy-Chain Model for Phone and Workstation Connectivity

Select a port to configure:
6509-Access(config)#interface GigabitEthernet 1/1

Configure the port as a Layer 2 port in the access mode:
6509-Access(config-if)#switchport
6509-Access(config-if)#switchport mode access

Define the voice VLAN:
6509-Access(config-if)#switchport voice vlan 100

Define the data VLAN:
6509-Access(config-if)#switchport access vlan 10

Configure the port as a host port:
6509-Access(config-if)#switchport host

Enable inline power:
6509-Access(config-if)#power inline auto

These commands configure the port to be an access-mode switchport, enable spanning-tree PortFast, and assign the voice VLAN ID (VVID) as VLAN 100 and the data VLAN (PC connected to the IP phone) as VLAN 10. Power is automatically provided and negotiated between the IP phone and the switchport by using Cisco Discovery Protocol—this protocol provides better power consumption because it allows the phone to negotiate power from the switch, resulting in a lower power value being reserved by the switch for that given device, as opposed to the full 15.4W of power normally required by an IEEE 802.3af Class 3 device.

Quality of Service

In order to ensure that voice traffic has preferential treatment through the switched network, we need to be able to guarantee that voice traffic is always queued correctly. In doing so, we assume a full trust policy on the switch interface. The “full trust” policy assumes a Cisco IP phone is connected to the port to which this policy is applied, because the IP phone is responsible for remarking the PC traffic to class of service (CoS) = 0. If a PC is instead directly connected to an interface with full trust policy and its traffic is untagged, the switch marks the traffic CoS = 0. However, if the directly connected PC is marking its traffic with a CoS value, the switch accepts it because the port is configured to trust any received CoS.

Phone Uplink Considerations

For the Cisco Catalyst 6500 to act as an access switch for Cisco Unified IP Phone models 7940, 7960, and 7970 + PC, the following is required for a full trust policy:

1. Enable QoS globally on the switch.
2. Configure interfaces used for IP phones:
   - Enable trust so the switch accepts the phone CoS markings.
   - Extend the trust boundary to the access port on the IP phone and mark PC traffic as CoS = 0.
   - Enable input queue scheduling.

- Configure CoS-to-queue mapping.
- Configure output scheduling.
- Configure CoS-to-differentiated services code point (DSCP) mapping.
- Optionally configure a policy for additional application traffic marking or policing (not covered).

3. Configure uplink interfaces to the distribution switch:
   - Enable trust to accept markings from the distribution switch. This trust can be either CoS or DSCP trust.
   - Enable input queue scheduling.
   - Configure CoS-to-queue mapping.
   - Configure output scheduling.
   - Verify and configure CoS-to-DSCP mapping.
   - Optionally configure a policy for additional application traffic marking or policing (not covered).

Enable QoS on the switch globally:
6509-Access(config)#mls qos

Accept the incoming Layer 2 CoS, letting the switch accept the phone marking of voice traffic at CoS = 5 and voice control traffic at CoS = 3 and enabling input scheduling:
6509-Access(config-if)#mls qos trust cos

Instruct the IP phone to rewrite the PC traffic to CoS = 0:
6509-Access(config-if)#mls qos trust extend cos 0

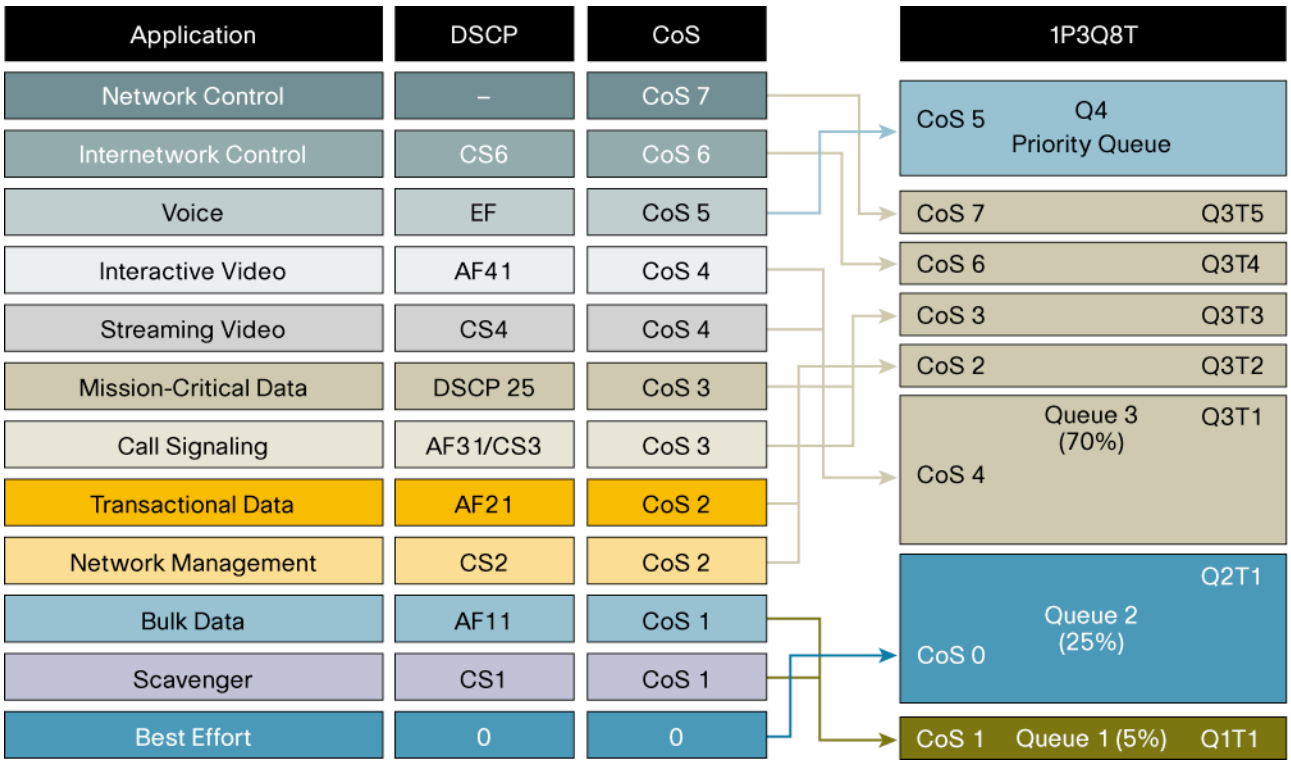
Because Cisco recommends using the Enhanced 48-port 10/100/1000BASE-T Ethernet Switching Module (part number WS-X6148A-GE-45AF or WS-X6148A-45AF) line cards here, the usable queue-structure types are shown in Table 1.

Table 1. Queues

Module Part Number	Receive Queues	Transmit Queues
WS-X6148A-GE-45AF	1q2t	1p3q8t
WS-X6148A-45AF	1p1q4t	1p3q8t

The map and allocation scheme is identified in Figure 5.

Figure 5. Suggested Mappings for 1p3q8t Queue Structures



Allocate buffer space for the three Weighted Round Robin (WRR) queues: 5 percent for Q1, 25 percent for Q2, and 40 percent for Q3 (Priority Queue—Q4 automatically uses the remaining bandwidth—30 percent):

6509-Access(config-if)#wrr-queue queue-limit 5 25 40

Allocate relative weights for the servicing between the three WRR queues: 5:25:70 (Q1:Q2:Q3):

6509-Access(config-if)#wrr-queue bandwidth 5 25 70

Enable WRED for all three WRR queues:

6509-Access(config-if)#wrr-queue random-detect 1

6509-Access(config-if)#wrr-queue random-detect 2

6509-Access(config-if)#wrr-queue random-detect 3

Configure WRED minimum and maximum thresholds for Q1:

6509-Access(config-if)#wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100

6509-Access(config-if)#wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100

Configure WRED minimum and maximum thresholds for Q2:

6509-Access(config-if)#wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100

6509-Access(config-if)#wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100

Configure WRED minimum and maximum thresholds for Q3:

6509-Access(config-if)#wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100

6509-Access(config-if)#wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100

Place CoS = 1 (Scavenger/Bulk) in queue 1 threshold 1:
6509-Access(config-if)#wrr-queue cos-map 1 1 1

Place CoS = 0 (best effort) in queue 2 threshold 1:
6509-Access(config-if)#wrr-queue cos-map 2 1 0

Place CoS = 4 (video) in queue 3 threshold 1:
6509-Access(config-if)#wrr-queue cos-map 3 1 4

Place CoS = 2 (network management and transactional data) in queue 3 threshold 2:
6509-Access(config-if)#wrr-queue cos-map 3 2 2

Place CoS = 3 (call signaling and mission critical) in queue 3 threshold 3:
6509-Access(config-if)#wrr-queue cos-map 3 3 3

Place CoS = 6 (internetwork control—IP routing) in queue 3 threshold 4:
6509-Access(config-if)#wrr-queue cos-map 3 4 6

Place CoS = 7 (network control—spanning tree) in queue 3 threshold 5:
6509-Access(config-if)#wrr-queue cos-map 3 5 7

Place CoS = 5 (voice over IP [VoIP]) into the strict priority queue:
6509-Access(config-if)#priority-queue cos-map 1 5

Modify the CoS-to-DSCP mapping. The recommended settings are DSCP = CS3 (24) for VoIP control and DSCP = EF (46) for VoIP media traffic. To map the Layer 2 CoS correctly to these DSCP values, you must modify the switch default CoS-to-DSCP mappings. All CoS values are shown, though only 0, 3, and 5 are directly related to IP telephony:
6509-Access(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 54

Access Switch Uplink Considerations

After you configure the access port queuing, you must also configure the uplink interfaces to the distribution switch. This process involves enabling trust for Ethernet frames coming into the trunk port, enabling output scheduling, and manipulating the CoS-to-queue mapping entrance criteria, mapping the CoS values to the appropriate DSCP value.

This section assumes we are using either the Cisco Catalyst 6500 Supervisor Engine 32-10GE or Supervisor Engine 32-8GE uplink interfaces that have the queue structures given in Table 2.

Table 2. Supervisor Engine Interfaces

Supervisor Engine Part Number	Receive Queues	Transmit Queues
WS-SUP32-GE-3B	2q8t	1p3q8t
WS-SUP32-10GE-3B	2q8t	1p3q8t

Accept incoming DSCP markings if incoming traffic is known to be properly marked at Layer 3:
6509-Access(config-if)#mls qos trust dscp

Alternatively, accept incoming CoS markings if incoming traffic is known to be properly marked at Layer 2 only. Note also that by trusting CoS, you get the added advantage of using the receive queues:
6509-Access(config-if)#mls qos trust cos

If we are trusting CoS, verify CoS-to-DSCP mapping. This mapping should have been set up in the global configuration. Map CoS = 5 to DSCP = EF (46) and CoS = 3 to DSCP = CS3 (24):

6509-Access(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 54

Allocate buffer space for the three WRR queues: 5 percent for Q1, 25 percent for Q2, and 40 percent for Q3 (Priority Queue—Q4 automatically grabs the remainder bandwidth—30 percent):

6509-Access(config-if)#wrr-queue queue-limit 5 25 40

Allocate relative weights for the servicing between the three WRR queues: 5:25:70 (Q1:Q2:Q3):

6509-Access(config-if)#wrr-queue bandwidth 5 25 70

Enable Weighted Random Early Detection (WRED) for all three WRR queues:

6509-Access(config-if)#wrr-queue random-detect 1

6509-Access(config-if)#wrr-queue random-detect 2

6509-Access(config-if)#wrr-queue random-detect 3

Configure WRED minimum and maximum thresholds for Q1:

6509-Access(config-if)#wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100

6509-Access(config-if)#wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100

Configure WRED minimum and maximum thresholds for Q2:

6509-Access(config-if)#wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100

6509-Access(config-if)#wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100

Configure WRED minimum and maximum thresholds for Q3:

6509-Access(config-if)#wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100

6509-Access(config-if)#wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100

Place CoS = 1 (scavenger/bulk) in queue 1 threshold 1:

6509-Access(config-if)#wrr-queue cos-map 1 1 1

Place CoS = 0 (best effort) in queue 2 threshold 1:

6509-Access(config-if)#wrr-queue cos-map 2 1 0

Place CoS = 4 (video) in queue 3 threshold 1:

6509-Access(config-if)#wrr-queue cos-map 3 1 4

Place CoS = 2 (network management and transactional data) in queue 3 threshold 2:

6509-Access(config-if)#wrr-queue cos-map 3 2 2

Place CoS = 3 (call signaling and mission critical) in queue 3 threshold 3:

6509-Access(config-if)#wrr-queue cos-map 3 3 3

Place CoS = 6 (internetwork control—IP routing) in queue 3 threshold 4:

6509-Access(config-if)#wrr-queue cos-map 3 4 6

Place CoS = 7 (network control—spanning tree) in queue 3 threshold 5:

6509-Access(config-if)#wrr-queue cos-map 3 5 7

Place CoS = 5 (VoIP) into the strict priority queue:

6509-Access(config-if)#priority-queue cos-map 1 5

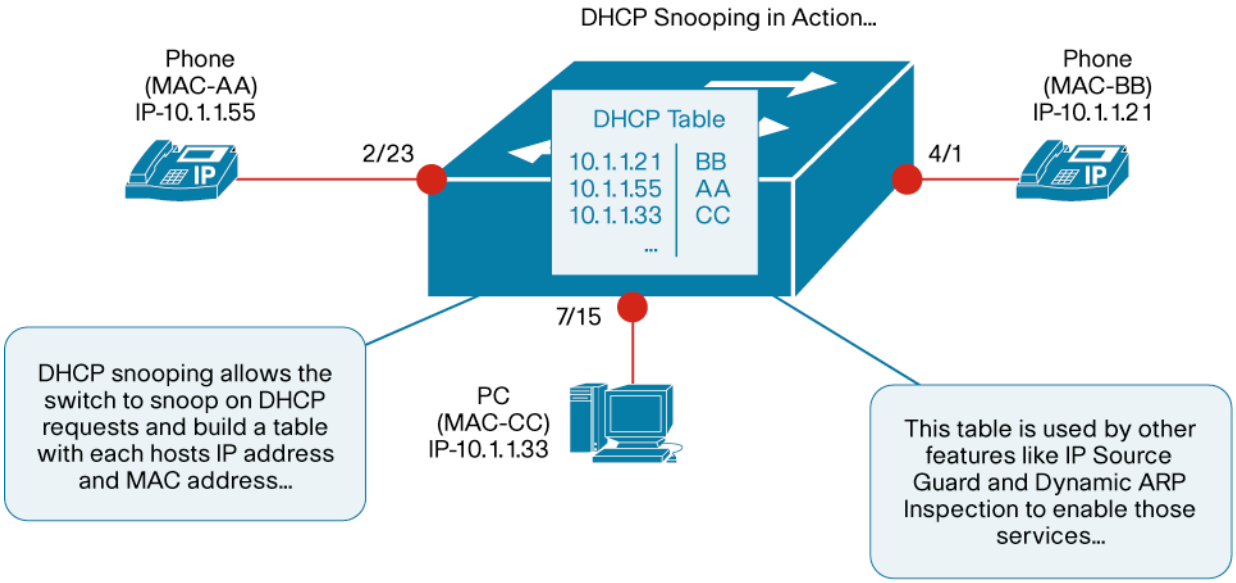
Security

With the advent of the number of hacking tools that are freely available on the Internet today, the network administrator is continually burdened with the task of maintaining a secure network. Coupled with the tight integration of IP Communications and privacy concerns, it is even more important for security to be designed into a network enabled for voice.

DHCP Snooping

One method to ensure the validity of a user's identity is to associate and track a workstation IP to MAC address binding. The DHCP Snooping feature allows us to do this by building up a table of DHCP-provided IP addresses. This process is illustrated in Figure 6.

Figure 6. DHCP Snooping Allows the Binding of IP to MAC Addresses



To configure DHCP Snooping the following must be performed:

Globally enable DHCP Snooping:
6509-Access(config)#ip dhcp snooping

Enable DHCP Snooping on the required VLANs:
6509-Access(config)#ip dhcp snooping vlan 10,100

When DHCP Snooping is enabled, it drops all DHCP responses until an uplink port is enabled as a trusted port. To configure a Layer 2 port as a trusted port, perform the following:
6509-Access(config)#interface port-channel 2
6509-Access(config-if)#ip dhcp snooping trust

If your DHCP server does not understand DHCP option 82, the insertion of this field must be disabled because it is enabled by default:
6509-Access(config)#no ip dhcp snooping information option

The configuration can be confirmed using the following command:

```
6509-Access#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,100
```



```
DHCP snooping is operational on following VLANs:
10,100
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface Trusted Rate limit (pps)
------------------------ ------- ----------------
Port-channel2 yes unlimited
```

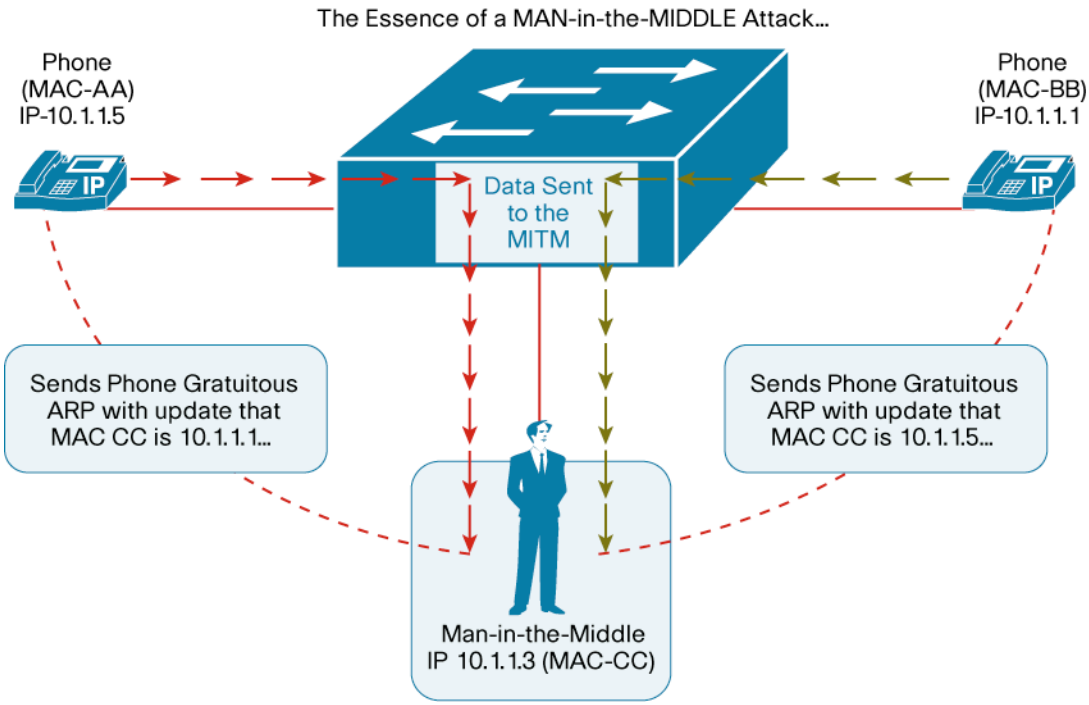
When a host requests an IP address through DHCP, the binding information can also be viewed using the following command:

```
6509-Access#sh ip dhcp snooping bind
MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
00:0C:29:C3:6D:2E 192.168.10.11 86137 dhcp-snooping 10 GigabitEthernet1/2
Total number of bindings: 1
```

Dynamic ARP Inspection

A common example of an invasion of privacy is one that allows unauthorized users to tap into other users' telephone conversations and record or play back sensitive information. This process can be achieved using widely available man-in-the-middle attack tools, illustrated in Figure 7.

Figure 7. How Man-in-the-Middle Attacks Can Be Used to Snoop VoIP Calls



To mitigate against this type of attack, the Cisco Catalyst 6500 can verify MAC-IP address bindings and filter out any anomalous activity.

To do you so, first you must enable DHCP Snooping as described previously.

Next, enable Dynamic ARP Inspection (DAI) on the required VLANs:

6509-Access(config)#ip arp inspection vlan 10,100

Additionally, configure the uplink interfaces toward the distribution switches as trusted interfaces for the purposes of DAI:

6509-Access(config)#int po1

6509-Access(config-if)#ip arp inspection trust

When DAI is enabled, every Address Resolution Protocol (ARP) frame that it receives from untrusted interfaces (those interfaces that have not explicitly been configured as trusted interfaces for DAI) are validated against the DHCP Snooping binding table. Recall this command used previously:

```
6509-Access#sh ip dhcp snooping binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
00:14:69:A9:55:37 192.168.100.10 447661 dhcp-snooping 100 GigabitEthernet1/1
00:0C:29:C3:6D:2E 192.168.10.11 612091 dhcp-snooping 10 GigabitEthernet1/2
Total number of bindings: 2
```

In this example, we can see that DHCP Snooping has learned two IP MAC address bindings. When DAI is enabled, for all untrusted interfaces, the Cisco Catalyst 6500 compares ARP frames received from those respective ports against the DHCP Snooping binding table and drops any frames with an invalid IP MAC binding.

The following output shows various invalid ARP frames that have been dropped by DAI:

```
6509-Access#
6d00h: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/2, vlan
10.([0004.23af.7999/10.1.99.23/0000.0000.0000/10.1.99.22/20:54:49 UTC Tue Feb 14 2006])
6d00h: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/2, vlan
10.([0004.23af.7999/10.1.99.23/0000.0000.0000/10.1.99.22/20:54:51 UTC Tue Feb 14 2006])
6d00h: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/2, vlan
10.([0004.23af.7999/10.1.99.23/0000.0000.0000/10.1.99.22/20:55:21 UTC Tue Feb 14 2006])
```

To view summary statistics for DAI, use the following command:

```
6509-Access#sh ip arp inspection statistics vlan 10
 Vlan Forwarded Dropped DHCP Drops ACL Drops
 ---- --------- ------- ---------- ----------
 10 3 19 19 0
 Vlan DHCP Permits ACL Permits Source MAC Failures
 ---- ------------ ----------- -------------------
 10 1 0 0
 Vlan Dest MAC Failures IP Validation Failures
 ---- ----------------- ----------------------
 10 0 0
```

Availability

Both system and network availability are crucial to a converged voice and data network. This section analyzes both aspects and provides recommendations for each.

Deployment of Redundant Supervisors

To maintain an always-available network, the access switches in question should be deployed in a redundant-supervisor configuration, eliminating a single point of failure. Additionally, these supervisor engines should be configured in such a state that they are running in Stateful SwitchOver/NonStop Forwarding (SSO/NSF) mode. Note that this mode is the default mode of operation, assuming that both supervisors are running the same level of software.

A sample default configuration is shown here as a reference:

6509-Access(config)#redundancy

6509-Access(config-red)#mode sso

The following commands can be used to verify the redundancy states:

```
6509-Access#sh module
Mod Ports Card Type Model Serial No.
--- ----- -------------------------------------- ------------------ -----------
 1 48 48-port 10/100/1000 RJ45 EtherModule WS-X6148A-GE-45AF SAD092108HB
 5 3 Supervisor Engine 32 10GE (Active) WS-SUP32-10GE-3B SAD09330B3E
 6 3 Supervisor Engine 32 10GE (Hot) WS-SUP32-10GE-3B SAD09330B60
6509-Access#sh redundancy
Redundant System Information :
------------------------------
 Available system uptime = 6 days, 2 hours, 40 minutes
Switchovers system experienced = 0
 Standby failures = 2
 Last switchover reason = none
 Hardware Mode = Duplex
 Configured Redundancy Mode = sso
 Operating Redundancy Mode = sso
 Maintenance Mode = Disabled
 Communications = Up
Current Processor Information :
------------------------------
 Active Location = slot 5
 Current Software state = ACTIVE
 Uptime in current state = 6 days, 2 hours, 40 minutes
 Image Version = Cisco Internetwork Operating System Software
IOS (tm) s3223_rp Software (s3223_rp-IPSERVICES_WAN-M), Version 12.2(18)SXF2, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Thu 19-Jan-06 02:20 by dchih
 BOOT = sup-bootdisk:,1;
 BOOTLDR =
 Configuration register = 0x2102
Peer Processor Information :
----------------------------
```



```
 Standby Location = slot 6
 Current Software state = STANDBY HOT
 Uptime in current state = 6 days, 2 hours, 18 minutes
 Image Version = Cisco Internetwork Operating System Software
IOS (tm) s3223_rp Software (s3223_rp-IPSERVICES_WAN-M), Version 12.2(18)SXF2, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Thu 19-Jan-06 02:20 by dchih
 BOOT = sup-bootdisk:,1;
 BOOTLDR =
 Configuration register = 0x2102
```

Spanning Tree

The Spanning Tree Protocol is used to resolve a loop-free Layer 2 topology. In a typical campus access-distribution model, the connectivity is usually through Layer 2 802.1Q trunks and, therefore, spanning tree is crucial. It is also recommended at this point that either Rapid Spanning Tree (802.1w) or Multiple Spanning Tree (802.1s) be deployed to minimize potential reconvergence time.

Assuming that we are deploying Rapid Per-VLAN Spanning Tree (PVST), the following configuration should be entered on the access switches: **6509-Access(config)#spanning-tree mode rapid-pvst**

This command globally enables Rapid PVST+ on the access switch. No further configuration is required in this instance. Refer to the "Distribution Layer" deployment section for further configuration details. The following output represents the spanning-tree topology for the voice VLAN in question:

```
6509-Access#sh spanning-tree vlan 100
VLAN0100
 Spanning tree enabled protocol rstp
 Root ID Priority 8192
 Address 000f.f8aa.9864
 Cost 2
 Port 641 (TenGigabitEthernet6/1)
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Bridge ID Priority 32768
 Address 000e.d688.a464
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Aging Time 300
Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/1 Desg FWD 19 128.1 Edge P2p
Gi1/3 Desg FWD 19 128.3 Edge P2p
Gi1/4 Desg FWD 19 128.4 Edge P2p
Te5/1 Altn BLK 2 128.513 P2p
Te6/1 Root FWD 2 128.641 P2p
```


Management

A host of tools are available to ease the management and ongoing efforts of deploying or supporting a VoIP environment on the Cisco Catalyst 6500. The following sections describe some of them.

Embedded Event Manager

Embedded Event Manager (EEM) is a service running in Cisco IOS Software that allows you to track events on a switch. Because it is part of Cisco IOS Software, it can use multiple event detectors that are integrated in the system that would otherwise be more difficult to track with external network management systems. In addition, EEM offers an interface to the Tool Command Language (TCL) scripting language, which adds a great deal of flexibility. Users can write their own scripts that are executed on the switch based on triggers such as counters, syslog messages, Simple Network Management Protocol (SNMP) traps, GOLD, timer services, or Portable Operating System Interface (POSIX) process events such as restarts of processes, etc.

EEM applets that offer a simpler way to provide more basic functions can be written. These applets do not require the use of TCL scripts.

A sample use of EEM in a Cisco Unified Communications environment might be when a Cisco Unified IP phone is plugged into a wall jack and the connected Cisco Catalyst 6500 switch detects that the link is now "up" and issues a Cisco Discovery Protocol exchange with the phone to obtain device information. If this information indicates that the endpoint is a Cisco Unified IP phone, then the switch port can be automatically configured for voice using the Cisco IOS Software EEM feature in the Cisco Catalyst 6500 by automatically applying the appropriate QoS configurations. An example of such a script can be found in Appendix B.

NetFlow

NetFlow is a well-known networking technology that has been available for quite some time. Beginning as a switching technology, it then evolved into a feature acceleration mechanism and a highly flexible monitoring instrument. In modern switch and router architectures, NetFlow switching has been completely replaced by Cisco Express Forwarding as the primary packet-switching algorithm of the system; however, it still remains very popular as a monitoring and feature acceleration technology.

In this capacity we are interested in using NetFlow to allow us to monitor and track voice calls as well as data traffic on the access switch. Even though the access device is a pure Layer 2 switch, we can still enable Bridged NetFlow and export monitored information to a collector (such as the Cisco NetFlow Collector [NFC] or the Network Analysis Module [NAM]).

In order to enable Bridged NetFlow on the access switches, first change the flow mask you wish to use, followed by the export version:

```
6509-Access(config)#mls flow ip interface-full
6509-Access(config)#mls nde sender version 5
6509-Access(config)#ip flow ingress layer2-switched vlan 10,100
6509-Access(config)#ip flow-export version 5
```

For each VLAN you want to monitor bridged traffic for, create a Switched Virtual Interface (SVI), assign an IP address, and enable flow monitoring on the interface:

```
6509-Access(config)#interface Vlan10
6509-Access(config-if)#ip address 192.168.10.6 255.255.255.0
6509-Access(config-if)#ip flow ingress
```

Finally, specify the collector or analyzer you wish to send the flow records to:

```
6509-Access(config)#ip flow-export destination 172.26.196.31 3000
```

Capacity Monitoring

Built into the Cisco Catalyst 6500 is the ability to monitor various loads, capacities, and available resources. One of the important aspects to monitor in the access layer for Cisco Unified IP deployments are the power-consumption levels.

The Cisco Catalyst 6500 has a useful command to allow administrators to verify power use as part of the **show platform hardware capacity** outputs:

```
6509-Access#show platform hardware capacity power
Power Resources
 Power supply redundancy mode: administratively redundant
 operationally non-redundant (single power supply)
 System power: 1171W, 30W (3%) inline, 529W (45%) total allocated
 Powered devices: 3 total, 2 Class3, 0 Class2, 0 Class1, 0 Class0, 1 Cisco
```

AutoQoS and Smartports Macros

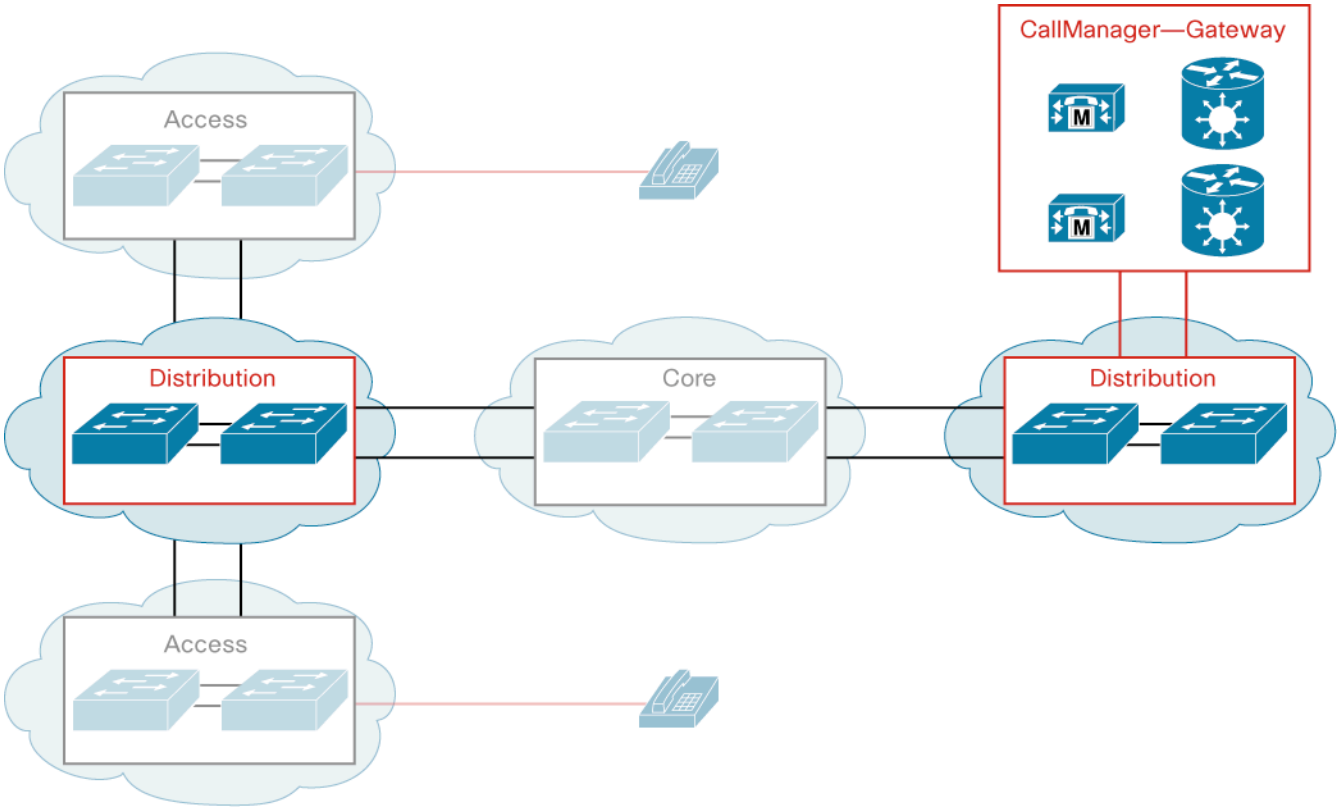
AutoQoS and Smartports make configuration to automate the provisioning of VoIP services easy. Support for both AutoQoS and Smartports on the Cisco Catalyst 6500 is planned for a future software release during the Q4 CY06 timeframe.

Distribution Layer

The distribution layer refers to a group of switches that aim to aggregate multiple access switches, providing an easy way to scale, manage, and maintain your network. As uplink devices from the access layer, the distribution layer may contain varying modules, depending on the uplink of choice. Depending on port density, either the 24-Port Gigabit Ethernet Switching Module or 48-Port Gigabit Ethernet Switching Module (part number WS-X6724-SFP or WS-X6748-SFP) can be deployed to aggregate Gigabit Ethernet-attached access switches. For 10 Gigabit Ethernet-attached access switches, the 4-Port 10 Gigabit Ethenet Switch Module (part number WS-X6704-10GE) should be deployed as the downlink. Additionally, for directly attached call managers or other application servers, the 48-Port 10/100/100BASE-T Fabric-Enabled Switching Module (part number WS-X6748-GE-TX) should be deployed to provide scalable, high-capacity connectivity. To further scale the performance of the system, distributed forwarding cards (DFCs) can also be deployed to offload forwarding lookups from the centralized supervisor engine. Depending on the policy feature card (PFC) version your system is operating, Cisco recommends matching the DFC version as well. For example, if your Supervisor Engine 720 has a PFC3B installed, then a DFC3B (part number WS-F6700-DFC3B) should also be installed on the modules.

Another use of the distribution layer is to host any services modules that may be required to be integrated into the network. Services modules such as the Cisco Catalys 6500 Series Network Analysis Module (part number WS-SVC-NAM-2) or the Cisco Catalyst 6500 Series Communications Media Module (part number WS-SVC-CMM) are examined here. Note that in larger networks, services modules can also be located in a separate services aggregation block (Figure 8).

Figure 8. The Distribution and Services Block



Basic Connectivity

Connectivity in the distribution block is relatively straightforward. Access switches are dual-homed to two distribution switches usually through Layer 2 802.1Q trunk connections. Note that best-practice campus design mandates that only one VLAN be carried per access layer switch, but because at least two VLANs need to be addressed here (voice and data VLANs), the downlink to the access switch must be a Layer 2 trunk.

The connectivity between the two distribution switches here could either be a Layer 2 trunk or a Layer 3 connection. With Layer 2 trunking, the combination of distribution and access switches forms a Layer 2 loop and, therefore, we must rely on the Spanning Tree Protocol to resolve a loop-free topology. A more scalable way of implementing this protocol is to use a Layer 3 link between the two distribution switches, allowing for better link usage and dependency on the Gateway Load Balancing Protocol (GLBP) for first-hop redundancy (refer to the "Availability" section for more information).

Quality of Service

Because traffic has already been marked or classified at the access layer, the only required QoS feature in the distribution layer trusts the markings and then queues packets based on those markings. Likewise, from the neighboring distribution switches or from the core layer, trusting must also be implemented.

Enable QoS globally on the switch:
6509-Distribution(config)#mls qos

Allow Layer 2 CoS markings from the access layer to be trusted—also enable input queuing and scheduling:
6509-Distribution(config-if)#mls qos trust cos

For Layer 3 connections uplinking either to the core layer or to neighboring distribution switches, DSCP values should be used because Layer 2 CoS is no longer carried on the wire. Note that this directive also applies to Cisco CallManager systems that are directly connected to the distribution layer. For these interfaces, allow Layer 3 DSCP markings to be trusted:

6509-Distribution(config-if)#mls qos trust dscp

Cisco recommends the modules listed in Table 3 for interswitch connectivity.

Table 3. Modules for Interswitch Connectivity

Module Part Number	Receive Queues	Transmit Queues
WS-X6704-10GE	1q8t or 8q8t with DFC	1p7q8t
WS-X6724-SFP or WS-X6748-SFP	1q8t or 2q8t with DFC	1p3q8t

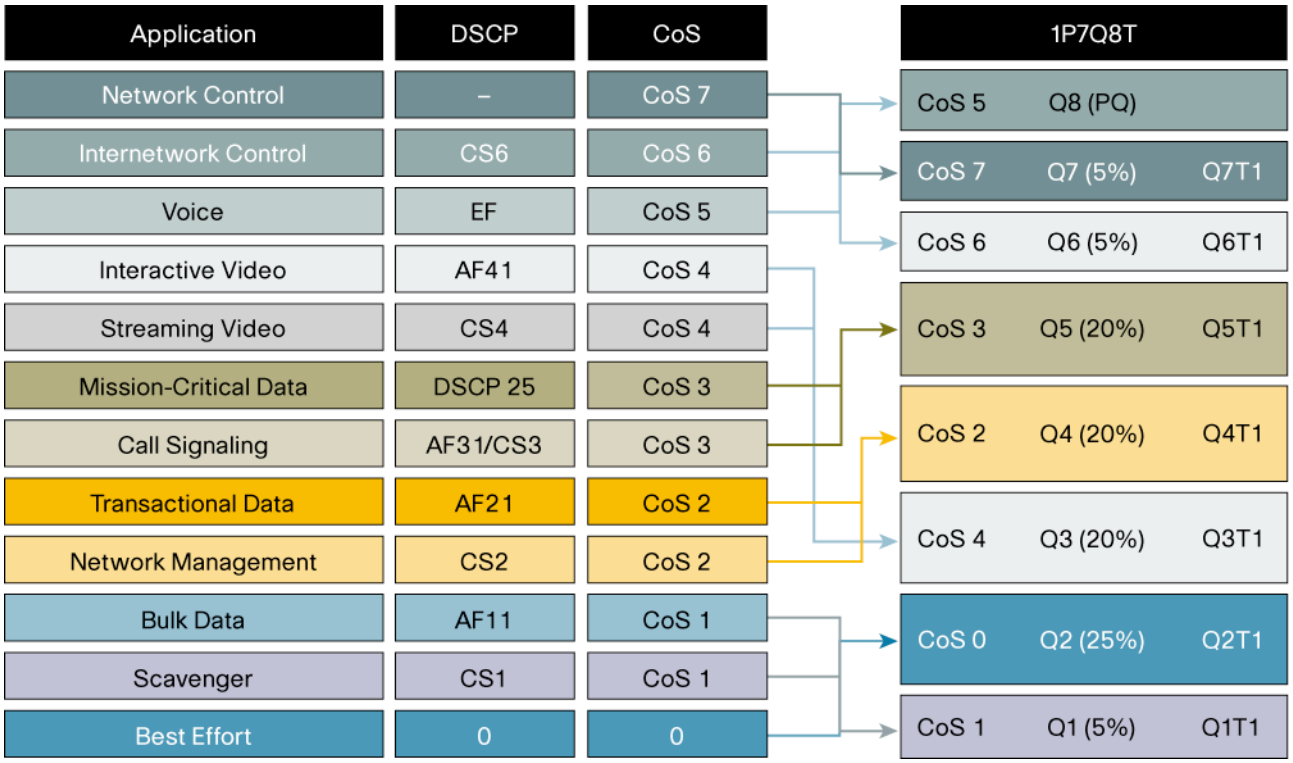
Cisco recommends the modules listed in Table 4 for Cisco CallManager or other application server connectivity.

Table 4. Modules for Cisco CallManager Connectivity

Module Part Number	Receive Queues	Transmit Queues
WS-X6748-GE-TX	1q8t or 2q8t with DFC	1p3q8t

For the 1p3q8t queue structures, refer to Figure 5 for the recommended queue mappings. For the 1p7q8t queue structures, refer to Figure 9 for the recommended queue mappings.

Figure 9. Suggested Mappings for 1p7q8t Queue Structures



4-Port 10 Gigabit Ethernet Switching Module (WS-X6704-10GE) QoS

Allocate buffer space for the seven WRR queues: 5 percent for Q1, 25 percent for Q2, 10 percent for Q3, 10 percent for Q4, 10 percent for Q5, 5 percent for Q6, and 5 percent for Q7 (Priority Queue—Q8 automatically grabs the remainder bandwidth—30 percent):

6509-Distribution(config-if)#wrr-queue queue-limit 5 25 10 10 10 5 5

Allocate relative weights for the servicing between the seven WRR queues: 5:25:20:20:20:5:5 (Q1:Q2:Q3:Q4:Q5:Q6:Q7):

6509-Distribution(config-if)#wrr-queue bandwidth 5 25 20 20 20 5 5

Enable WRED for all seven WRR queues:

6509-Distribution(config-if)#wrr-queue random-detect 1
6509-Distribution(config-if)#wrr-queue random-detect 2
6509-Distribution(config-if)#wrr-queue random-detect 3
6509-Distribution(config-if)#wrr-queue random-detect 4
6509-Distribution(config-if)#wrr-queue random-detect 5
6509-Distribution(config-if)#wrr-queue random-detect 6
6509-Distribution(config-if)#wrr-queue random-detect 7

Configure WRED minimum and maximum thresholds for Q1–Q7:

6509-Distribution(config-if)#wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
6509-Distribution(config-if)#wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100

Repeat this configuration for all eight queues:

Place CoS = 1 (scavenger/bulk) in queue 1 threshold 1:

6509-Distribution(config-if)#wrr-queue cos-map 1 1 1

Place CoS = 0 (best effort) in queue 2 threshold 1:

6509-Distribution(config-if)#wrr-queue cos-map 2 1 0

Place CoS = 4 (video) in queue 3 threshold 1:

6509-Distribution(config-if)#wrr-queue cos-map 3 1 4

Place CoS = 2 (network management and transactional data) in queue 4 threshold 1:

6509-Distribution(config-if)#wrr-queue cos-map 4 1 2

Place CoS = 3 (call signaling and mission critical) in queue 5 threshold 1:

6509-Distribution(config-if)#wrr-queue cos-map 5 1 3

Place CoS = 6 (internetwork control—IP routing) in queue 6 threshold 1:

6509-Distribution(config-if)#wrr-queue cos-map 6 1 6

Place CoS = 7 (network control—spanning tree) in queue 7 threshold 1:

6509-Distribution(config-if)#wrr-queue cos-map 7 1 7

Place CoS = 5 (VoIP) into the strict priority queue:

6509-Distribution(config-if)#priority-queue cos-map 1 5

24/48-Port Gigabit Ethernet Switching Module (WS-X6724/6748-SFP or WS-X6748-GE-TX) QoS

Allocate buffer space for the three WRR queues: 5 percent for Q1, 25 percent for Q2, and 40 percent for Q3 (Priority Queue—Q4 automatically grabs the remainder bandwidth—30 percent):

6509-Distribution(config-if)#wrr-queue queue-limit 5 25 40

Allocate relative weights for the servicing between the three WRR queues: 5:25:70 (Q1:Q2:Q3):
6509-Distribution(config-if)#wrr-queue bandwidth 5 25 70

Enable WRED for all three WRR queues:
6509-Distribution(config-if)#wrr-queue random-detect 1
6509-Distribution(config-if)#wrr-queue random-detect 2
6509-Distribution(config-if)#wrr-queue random-detect 3

Configure WRED minimum and maximum thresholds for Q1:
6509-Distribution(config-if)#wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
6509-Distribution(config-if)#wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100

Configure WRED minimum and maximum thresholds for Q2:
6509-Distribution(config-if)#wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
6509-Distribution(config-if)#wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100

Configure WRED minimum and maximum thresholds for Q3:
6509-Distribution(config-if)#wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
6509-Distribution(config-if)#wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100

Place CoS = 1 (scavenger/bulk) in queue 1 threshold 1:
6509-Distribution(config-if)#wrr-queue cos-map 1 1 1

Place CoS = 0 (best effort) in queue 2 threshold 1:
6509-Distribution(config-if)#wrr-queue cos-map 2 1 0

Place CoS = 4 (video) in queue 3 threshold 1:
6509-Distribution(config-if)#wrr-queue cos-map 3 1 4

Place CoS = 2 (network management and transactional data) in queue 3 threshold 2:
6509-Distribution(config-if)#wrr-queue cos-map 3 2 2

Place CoS = 3 (call signaling and mission critical) in queue 3 threshold 3:
6509-Distribution(config-if)#wrr-queue cos-map 3 3 3

Place CoS = 6 (internetwork control—IP routing) in queue 3 threshold 4:
6509-Distribution(config-if)#wrr-queue cos-map 3 4 6

Place CoS = 7 (network control—spanning tree) in queue 3 threshold 5:
6509-Distribution(config-if)#wrr-queue cos-map 3 5 7

Place CoS = 5 (VoIP) into the strict priority queue:
6509-Distribution(config-if)#priority-queue cos-map 1 5

Availability

In the campus design model, the distribution layer is the termination points for Layer 3, so it is at this point that access switches are dual-homed to provide first-hop Layer 3 redundancy. The following section investigates both features.

Spanning Tree

In the previous access layer switch section, we identified that the Rapid Spanning Tree Protocol is used to provide a fast and reliable mechanism to resolve Layer 2 loops. It is therefore at the distribution layer where we terminate the Layer 2 boundary while providing an efficient load-balancing scheme.

Rapid PVST supports this feature by allowing each VLAN to run its own instance of spanning tree. By electing different root switches for each VLAN, we can achieve load balancing by having the access switches block on different port or VLAN instances.

Following the previous example, if we have two VLANs (VLAN 10 for data and VLAN 100 for voice), we could elect different distribution switches as the root for each of these VLANs. The following configuration accomplishes this setup:

Enable Rapid PVST:
6509-Distribution-1(config)#spanning-tree mode rapid-pvst

Configure this switch to be the spanning-tree root for data VLAN (10) and secondary root for voice VLAN (100):
6509-Distribution-1(config)#spanning-tree vlan 10 root primary
6509-Distribution-1(config)#spanning-tree vlan 100 root secondary

This configuration should also be applied on the second distribution switch, but it should be the primary root for the voice VLAN and secondary root for the data VLAN:
6509-Distribution-1(config)#spanning-tree vlan 10 root secondary
6509-Distribution-1(config)#spanning-tree vlan 100 root primary

If this setup is correct, we should see that Distribution-2 is the root for VLAN 100 (voice VLAN):

```
6509-Distribution-2#sh spanning-tree vlan 100
VLAN0100
 Spanning tree enabled protocol rstp
 Root ID Priority 8192
 Address 000f.f8aa.9864
 This bridge is the root
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Bridge ID Priority 8192
 Address 000f.f8aa.9864
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Aging Time 300
Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Te1/1 Desg FWD 2 128.1 P2p
Gi2/1 Desg FWD 4 128.129 P2p
Po1 Desg FWD 1 128.1665 P2p
```

Note on the access switch we should see that one of the uplink ports has gone into blocking mode:

```
6509-Access#sh spanning-tree vlan 100
VLAN0100
 Spanning tree enabled protocol rstp
 Root ID Priority 8192
 Address 000f.f8aa.9864
 Cost 2
 Port 641 (TenGigabitEthernet6/1)
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Bridge ID Priority 32768
 Address 000e.d688.a464
```



```
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Aging Time 300
Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/1 Desg FWD 19 128.1 Edge P2p
Gi1/3 Desg FWD 19 128.3 Edge P2p
Gi1/4 Desg FWD 19 128.4 Edge P2p
Te5/1 Altn BLK 2 128.513 P2p
Te6/1 Root FWD 2 128.641 P2p
```

An alternative to this design is to have a Layer 3 link between the two distribution switches. This design is recommended as long as the following criteria are met:

- No Layer 2 connections are required between the two distribution switches.
- There are no direct server connections on the two distribution switches.

If these criteria are met, spanning tree plays a lesser role because no logical Layer 2 loop is formed. Hence both uplinks on the access switches will forward for the same VLAN, allowing us to take advantage of the WRR load-balancing capabilities of GLBP.

Gateway Load Balancing Protocol

Because the distribution switches also provide first-hop Layer 3 redundancy, it is here that GLBP should be deployed for termination of the Layer 2 domain.

The GLBP feature provides automatic router backup for IP hosts configured with a single default gateway on an IEEE 802.3 LAN. Multiple first-hop routers on the LAN combine to offer a single virtual first-hop IP router while sharing the IP packet forwarding load. Other routers on the LAN may act as redundant GLBP routers that become active if any of the existing forwarding routers fail.

GLBP performs a similar—but not identical—function for the user as the Hot Standby Router Protocol (HSRP) and the Virtual Router Redundancy Protocol (VRRP). GLBP provides load balancing over multiple routers (gateways) using a single virtual IP address and multiple virtual MAC addresses. Each host is configured with the same virtual IP address, and all routers in the virtual router group participate in forwarding packets.

To configure GLBP, use the following configuration on Distribution-1:

```
6509-Distribution-1(config)#interface Vlan10
6509-Distribution-1(config-if)#glbp 10 ip 192.168.10.1
6509-Distribution-1(config-if)#glbp 10 priority 110
6509-Distribution-1(config-if)#glbp 10 preempt


6509-Distribution-1(config)#interface Vlan100
6509-Distribution-1(config-if)#glbp 100 ip 192.168.100.1
```

Use the following on Distribution-2:

```
6509-Distribution-2(config)#interface Vlan10
6509-Distribution-2(config-if)#glbp 10 ip 192.168.10.1
6509-Distribution-2(config)#interface Vlan100
6509-Distribution-2(config-if)#glbp 100 ip 192.168.100.1
6509-Distribution-2(config-if)#glbp 100 priority 110
6509-Distribution-2(config-if)#glbp 100 preempt
```


To verify the configuration:

```
6509-Distribution-2#sh glbp vlan 100
Vlan100 - Group 100
 State is Active
 4 state changes, last state change 4d20h
 Virtual IP address is 192.168.100.1
 Hello time 3 sec, hold time 10 sec
 Next hello sent in 0.712 secs
 Redirect time 600 sec, forwarder time-out 14400 sec
 Preemption enabled, min delay 0 sec
 Active is local
 Standby is 192.168.100.2, priority 100 (expires in 8.556 sec)
 Priority 110 (configured)
 Weighting 100 (default 100), thresholds: lower 1, upper 100
 Load balancing: round-robin
 Group members:
 000f.f8aa.9800 (192.168.100.3) local
 000f.f8aa.9c00 (192.168.100.2)
 There are 2 forwarders (1 active)
 Forwarder 1
 State is Listen
 MAC address is 0007.b400.6401 (learnt)
 Owner ID is 000f.f8aa.9c00
 Redirection enabled, 598.024 sec remaining (maximum 600 sec)
 Time to live: 14398.024 sec (maximum 14400 sec)
 Preemption enabled, min delay 30 sec
 Active is 192.168.100.2 (primary), weighting 100 (expires in 7.652 sec)
 Arp replies sent: 993
 Forwarder 2
 State is Active
 3 state changes, last state change 4d20h
 MAC address is 0007.b400.6402 (default)
 Owner ID is 000f.f8aa.9800
 Redirection enabled
 Preemption enabled, min delay 30 sec
 Active is local, weighting 100
 Arp replies sent: 993
```

Manageability

The distribution layer switches have extra requirements from the manageability perspective, including exporting Layer 2 and Layer 3 flow information through NetFlow Data Export as well as the provisioning of the NAM for the purposes of flow statistics collection, analysis, generic traffic monitoring, as well as monitoring voice-specific applications.

NetFlow Monitoring and Export

As discussed in the "Access Layer" section, NetFlow can be a powerful tool in analysis of traffic and capacity planning. To enable NetFlow monitoring and export on the distribution switch, configure the following:

6509-Distribution(config)#mls flow ip interface-full

6509-Distribution(config)#mls nde sender version 5

6509-Distribution(config)#ip flow ingress layer2-switched vlan 10,100

6509-Distribution(config)#ip flow-export version 5

For each VLAN you want to monitor traffic for (both bridged and Layer 3 routed), enable flow monitoring on the interface:

6509-Distribution(config)#interface Vlan10

6509-Distribution(config-if)#ip flow ingress

Finally, specify the collector or analyzer you wish to send the flow records to:

6509-Distribution(config)#ip flow-export destination 172.26.196.31 3000

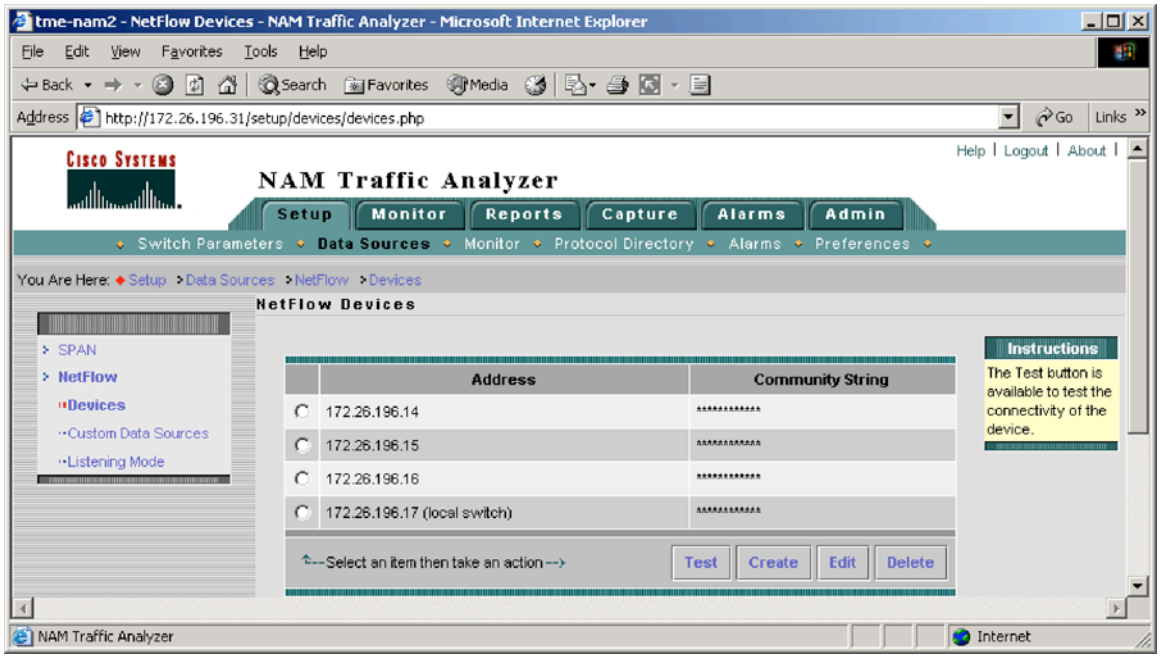
Network Analysis Module

Cisco NAM is an integrated traffic-monitoring solution for Cisco Catalyst 6500 Series switches that enables greater visibility into all layers of the network. It provides real-time and historical traffic analysis, performance monitoring, and quick troubleshooting and proactive monitoring for both data and voice networks. The Cisco NAM-1 and NAM-2 offer high-capacity monitoring and are easy to deploy and use with the embedded, Web-based traffic analyzer interface.

Cisco NAM as a NetFlow Collector or Analyzer

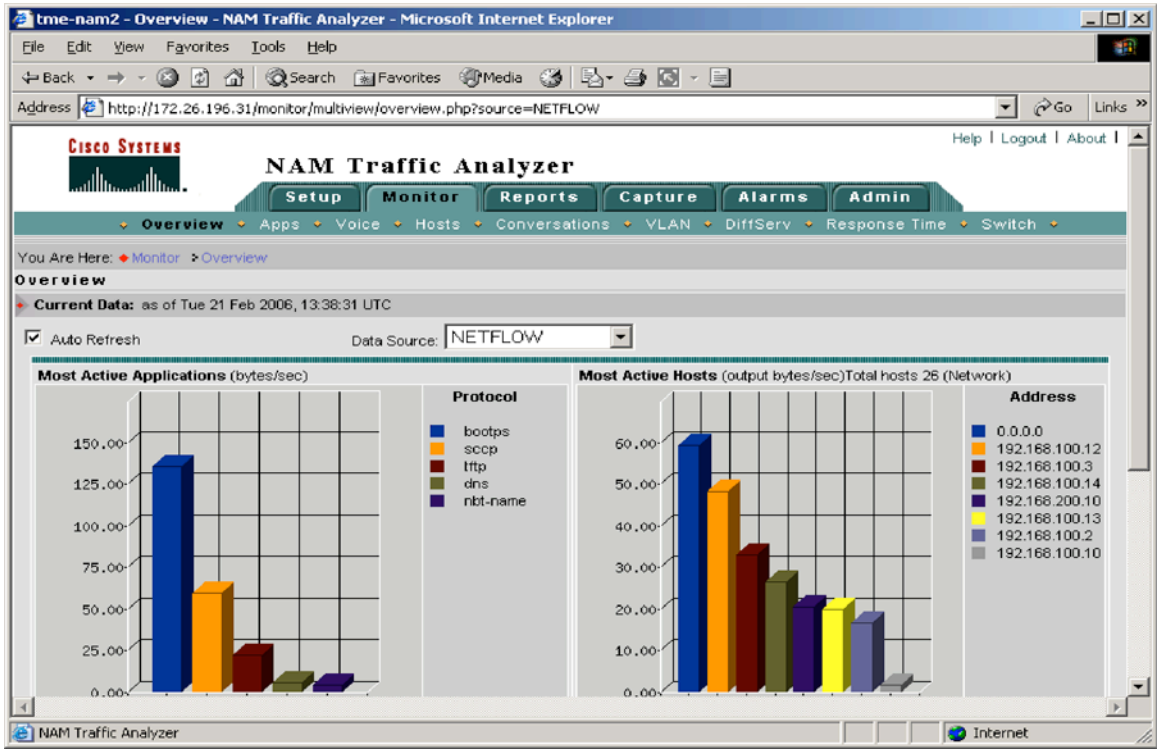
Assuming the module is operational, you can set up the NAM for NetFlow collection by first adding each NetFlow Exporter (switch) on the NAM Setup tab. Go to Setup → Data Sources, where you can select Devices under the NetFlow section (Figure 10). Here you can either add each device manually or have the NAM discover the devices by listening to any exported records sent to it.

Figure 10. Setting Up NetFlow Devices for Analysis



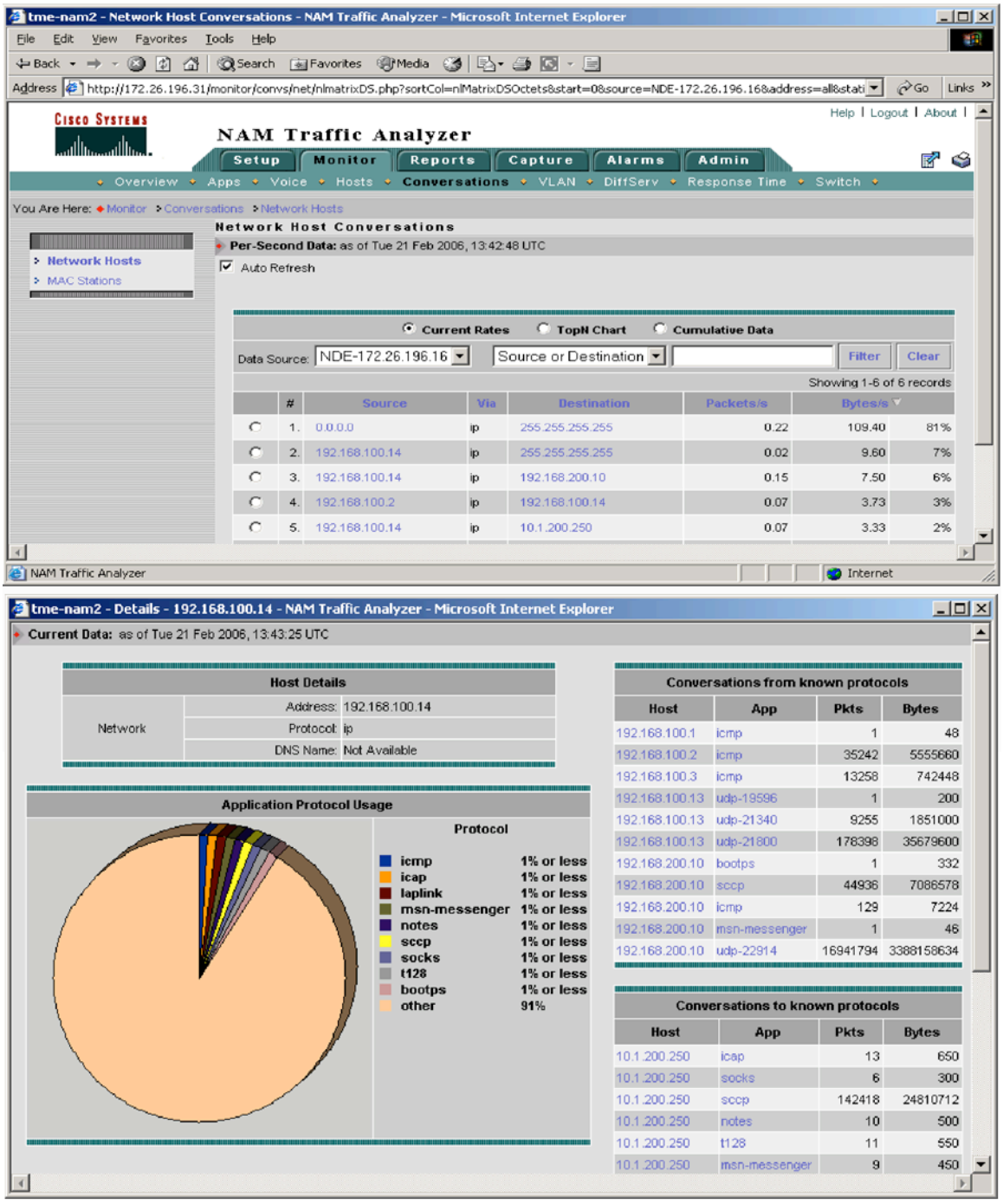
After the appropriate devices are added to the NAM for NetFlow monitoring, you can view this information by selecting Monitor → Overview, followed by the NetFlow switch profile you just created (Figure 11).

Figure 11. Cisco NAM as a NetFlow Collector and Analyzer



It is then also possible to analyze specific flow information pertaining to a given device, including the access switches exporting bridged NetFlow information under the Conversations section of the window (Figure 12).

Figure 12. Analyzing Detailed Flow Information



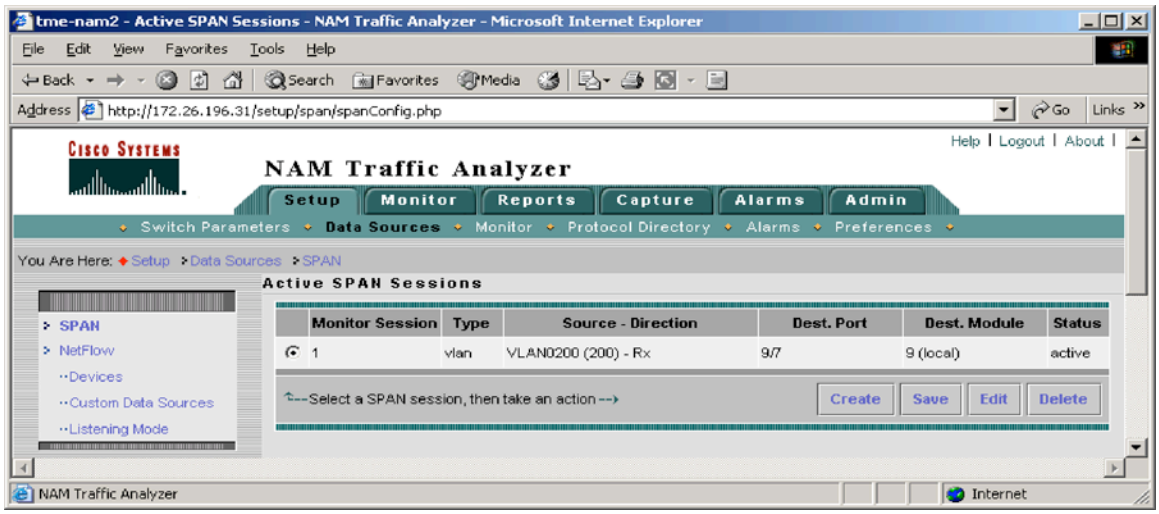
Cisco NAM as a Voice Monitoring Tool

Cisco NAM can also be used as an extensive voice monitoring tool, allowing the collection and verification of voice quality reported through Call Data Reporting (CDR) on the Cisco CallManager. To enable the collection of voice traffic, do the following:

Enable a VLAN Switched Port Analyzer (SPAN) or remote VLAN SPAN session to monitor the VLAN of the Cisco CallManager or cluster. This process can be accomplished either through the GUI on the NAM or by using the command-line interface (CLI) on the switch.

Using the GUI of the NAM, go to the Setup tab and select Data Sources → SPAN. Create a SPAN session corresponding to the VLAN of the Cisco CallManager or cluster (Figure 13):

Figure 13. Setting Up SPAN to Monitor Cisco CallManager Information



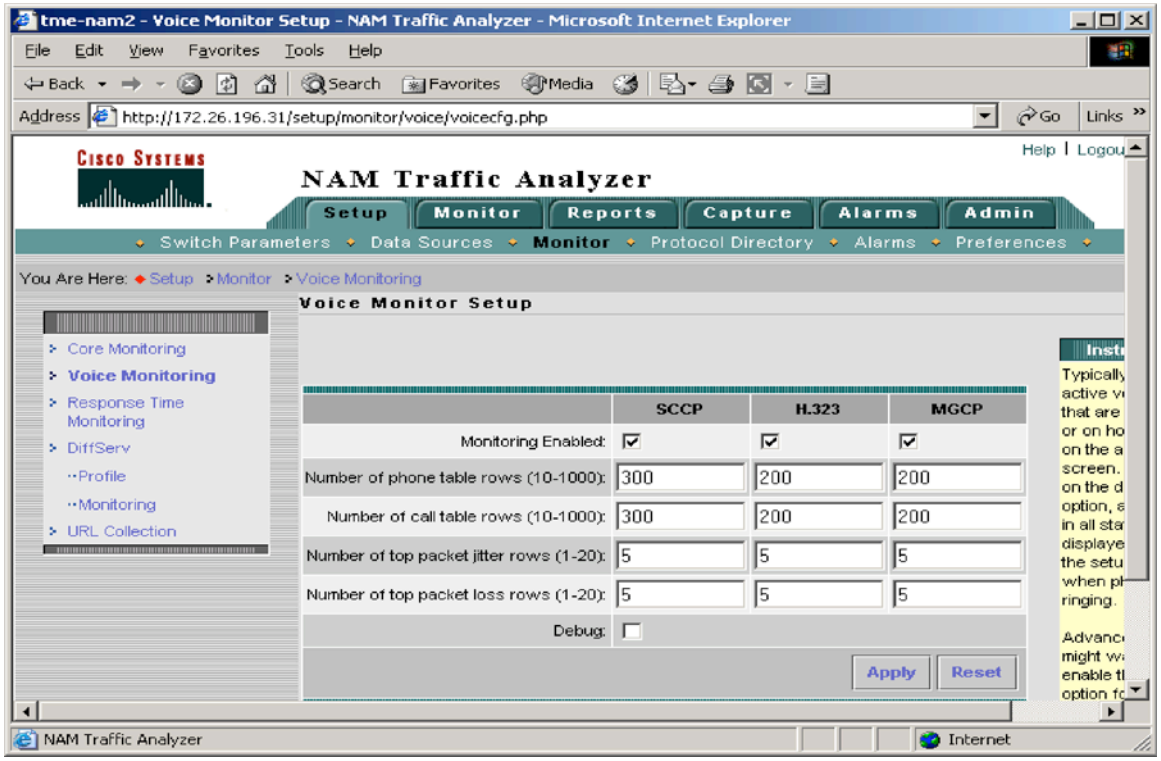
This process automatically sets up the following CLI on the local switch:

monitor session 1 source vlan 200 rx

monitor session 1 destination analysis-module 9 data-port 1 ingress learning

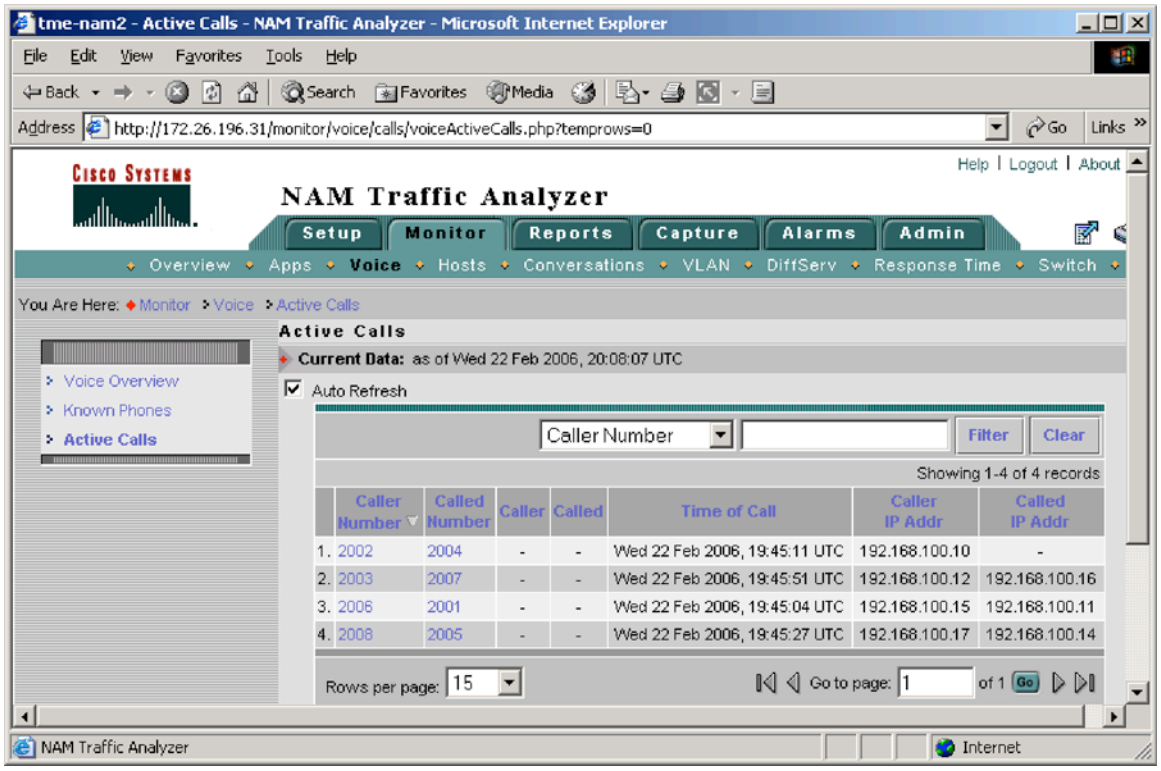
Now enable the appropriate data to monitor by going into the Setup tab and selecting Monitor → voice Monitoring (Figure 14):

Figure 14. Enabling Traffic to Be Monitored



After this monitoring is set up, it is possible to monitor information such as active voice calls and summary phone-quality information after the call is completed (Figure 15):

Figure 15. Monitoring Active Voice Calls



Communications Media Module

The Cisco Communication Media Module (CMM) Voice Features Module for the Cisco Catalyst 6500 Series supports interconnectivity between the public switched telephone network (PSTN) and traditional private-branch-exchange (PBX) systems and IP Communications and VoIP networks; additionally, it supports media services, such as media termination point (MTP), transcoding, and temporary conferences.

Benefits of this module include the following:

- Interoperability between IP Communications networks and the PSTN
- Audioconference and transcoding services as an integrated component of the converged network
- SNMP management capabilities

Cisco CMM Overview

The Cisco CMM acts as the VoIP gateway and media services module by using H.323, Media Gateway Control Protocol (MGCP), and Session Initiation Protocol (SIP) protocols with Cisco CallManager and other call agents. The CMM can support single or multiple Cisco CallManager servers in an IP Communications network.

These VoIP gateway and media services features are provided through the four different types of CMM port adapters, as shown in Table 5.

Table 5. Cisco CMM Port Adapters

Cisco CMM Port Adapter Part Numbers	Description
WS-SVC-CMM-6T1 **WS-SVC-CMM-6E1**	The 6-port T1 and E1 port adapters have onboard digital-signal-processor (DSP) resources that allow you to connect the interfaces to the PSTN or PBXs through T1 channel associated signaling (CAS)/E1 R2 or T1/E1 ISDN Primary Rate Interface (PRI). The DSP resources on the port adapters provide packetization, echo cancellation, fax relay, tone detection and generation, concealment, and jitter buffers.
WS-SVC-CMM-24FXS	The 24-port foreign-exchange-station (FXS) port adapter has onboard DSP resources that allow the FXS interfaces to emulate the central office or PBX analog trunk lines by providing service to analog phones and fax machines, which behave as if connected to a standard central office or PBX line.
WS-SVC-CMM-ACT	The ACT port adapter, also referred to as the media card, has DSP resources for conferencing, transcoding, and MTP services. A CMM with an ACT port adapter supports a single conference with up to 64 participants. A single ACT port adapter supports up to 128 audioconference ports, which can be distributed among different conferences of two or more parties.

Cisco CMM Operational Modes

The Cisco CMM operates in MGCP, Cisco H.323, or SIP mode. The following sections give information about the CMM operational modes.

H.323 Mode

Compared to MGCP, H.323 requires more configuration on the gateway because the gateway must maintain the dial plan and route pattern. The gateway must have enough information to direct calls to the correct endpoints, which may be through a port adaptor (T1/E1 and FXS) and H.323-capable devices.

Configuring H.323 mode on the Cisco CMM is similar to configuring H.323 on other Cisco IOS Software voice gateways. To configure the CMM by using H.323 mode, refer to the following documentation:

- *Cisco IOS H.323 Configuration Guide*
- Tech Note: *Configuring a Cisco IOS H.323 Gateway for Use with Cisco CallManager*

For H.323 configuration examples, refer to the "Configuration Examples for Cisco Communication Media Module Voice Features for Cisco Catalyst 6500 Series and Cisco 7600 Series" section on page 46 of the "Cisco Communication Media Module Voice Features for Cisco Catalyst 6500 Series and Cisco 7600 Series," at the following link:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xy8/gtcmm.pdf

MGCP Mode

In MGCP mode, also referred to as gateway mode, the Cisco CMM registers explicitly with Cisco CallManager, one registration for every gateway type. In MGCP mode, you do not need to configure the dial peers, voice ports, controllers, and so on. Cisco CallManager is aware of the configuration and does the routing to endpoints.

Configuring MGCP mode on the Cisco CMM is similar to configuring MGCP on other Cisco IOS Software voice gateways. To configure the CMM by using MGCP mode, refer to the following documentation:

- *Cisco IOS MGCP and Related Protocols Configuration Guide*
- Tech Note: *Configuring the Cisco IOS MGCP Gateway*

For MGCP configuration examples, refer to the "Configuration Examples for Cisco Communication Media Module Voice Features for Cisco Catalyst 6500 Series and Cisco 7600 Series" section on page 46 of the "Cisco Communication Media Module Voice Features f or Cisco Catalyst 6500 Series and Cisco 7600 Series," at the following link:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xy8/gtcmm.pdf

SIP Mode

SIP signaling interfaces connect Cisco CallManager registered devices and SIP networks that are served by a SIP proxy server. Multiple logical SIP signaling interfaces can be configured in Cisco CallManager and associated with route groups, route lists, and route patterns.

Configuring SIP mode on the Cisco CMM is similar to configuring SIP on other Cisco IOS Software voice gateways. To configure the CMM by using SIP mode, refer to the following documentation:

- Cisco IOS SIP Configuration Guide
- Cisco SIP Proxy Server documentation

For SIP configuration examples, refer to the *Cisco IOS SIP Configuration Guide*.

Core Layer

The core layer of the campus network is a centralized aggregation domain that contains little (or no) features and acts primarily as a very fast, low-latency switch or routing fabric (Figure 16).

Figure 16. The Core Layer

In this capacity, Cisco recommends deploying a Supervisor Engine 720 with high-speed interfaces such as the 4-port 10 Gigabit Ethernet Switching Module (part number WS-X6704-10GE). Additionally, the interfaces will primarily be Layer 3, with Layer 2 connectivity having been already terminated at the distribution layer.

Our only point of interest here therefore is QoS.

Quality of Service

From a QoS perspective, because traffic has already been marked at the access layer, all that is required to occur at the core layer is interface queuing. Additionally, because all received traffic should be Layer 3, DSCP should be trusted.

Enable QoS globally on the switch:
6509-Core(config)#mls qos

Trust DSCP markings from distribution layer switches:
6509-Core(config-if)#mls qos trust dscp

Cisco recommends the 4-port 10 Gigabit Ethernet Switching Module (part number WS-X6704-10GE) for interswitch connectivity; this module contains the queue or threshold structures given in Table 6.

Table 6. Queue Structures for [DESCRIPTIVE WORDS] Module

Module Part Number	Receive Queues	Transmit Queues
WS-X6704-10GE	1q8t or 8q8t with DFC	1p7q8t

4-port 10 Gigabit Ethernet Switching Module (WS-X6704-10GE) QoS

Allocate buffer space for the seven WRR queues: 5 percent for Q1, 25 percent for Q2, 10 percent for Q3, 10 percent for Q4, 10 percent for Q5, 5 percent for Q6, and 5 percent for Q7 (Priority Queue—Q8 automatically grabs the remainder bandwidth—30 percent)
6509-Core(config-if)#wrr-queue queue-limit 5 25 10 10 10 5 5

Allocate relative weights for the servicing between the seven WRR queues: 5:25:20:20:20:5:5 (Q1:Q2:Q3:Q4:Q5:Q6:Q7):
6509-Core(config-if)#wrr-queue bandwidth 5 25 20 20 20 5 5

Enable WRED for all seven WRR queues:
6509-Core(config-if)#wrr-queue random-detect 1
6509-Core(config-if)#wrr-queue random-detect 2
6509-Core(config-if)#wrr-queue random-detect 3
6509-Core(config-if)#wrr-queue random-detect 4
6509-Core(config-if)#wrr-queue random-detect 5
6509-Core(config-if)#wrr-queue random-detect 6
6509-Core(config-if)#wrr-queue random-detect 7

Configure WRED minimum and maximum thresholds for Q1–Q7:
6509-Core(config-if)#wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
6509-Core(config-if)#wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100

Repeat this configuration for all eight queues.

Place CoS = 1 (scavenger/bulk) in queue 1 threshold 1:
6509-Core(config-if)#wrr-queue cos-map 1 1 1

Place CoS = 0 (best effort) in queue 2 threshold 1:
6509-Core(config-if)#wrr-queue cos-map 2 1 0

Place CoS = 4 (video) in queue 3 threshold 1:
6509-Core(config-if)#wrr-queue cos-map 3 1 4

Place CoS = 2 (network management and transactional data) in queue 4 threshold 1:
6509-Core(config-if)#wrr-queue cos-map 4 1 2

Place CoS = 3 (call signaling and mission critical) in queue 5 threshold 1:
6509-Core(config-if)#wrr-queue cos-map 5 1 3

Place CoS = 6 (internetwork control—IP routing) in queue 6 threshold 1:
6509-Core(config-if)#wrr-queue cos-map 6 1 6

Place CoS = 7 (network control—spanning tree) in queue 7 threshold 1:
6509-Core(config-if)#wrr-queue cos-map 7 1 7

Place CoS = 5 (VoIP) into the strict priority queue:
6509-Core(config-if)#priority-queue cos-map 1 5

APPENDIX A—RECOMMENDED CPRLS

The following is a list of CPRLs that can be used as a basis. Note that networks differ, so these values should be tuned accordingly.

- Forwarding Information Base (FIB) glean cases rate limiter—This rate limiter allows packets requiring ARP that need to be punted to the route-processor CPU:
  Switch(config)#mls rate-limit unicast cef glean 1000 10
- Multicast FIB-miss rate limiter—Layer 3 flows that cannot be hardware switched are still forwarded in the software by routers:
  Switch(config)#mls rate-limit multicast ipv4 fib-miss 10000 10

- Ingress and egress ACL bridged packets rate limiter—This rate limiter specifies that rate packets be punted up to the route-processor CPU as a result of an ingress or egress ACL:
  Switch(config)#mls rate-limit unicast acl input 500 10
  Switch(config)#mls rate-limit unicast acl output 500 10
- Time-to-live (TTL) failure rate limiter—This rate limiter works when a unicast or multicast packet fails the TTL check and is directed to the route-processor CPU.
  Switch(config)#mls rate-limit all ttl-failure 500 10
- Unicast IP options rate limiter—This rate limiter specifies the rate at which unicast IPv4 packets with IP options are punted up to the route-processor CPU. It is available on systems with PFC3B and PFC3BXL.
  Switch(config)#mls rate-limit unicast ip options 10 1
- Multicast IP options rate limiter—This rate limiter specifies the rate at which multicast IPv4 packets with IP options are punted up to the route-processor CPU. It is available on systems with PFC3B and PFC3BXL.
  Switch(config)#mls rate-limit multicast ipv4 ip-option 10 1
- FIB miss rate limiter—If there is no route in the routing table, this hardware-based rate limiter allows packets punted to the route-processor CPU to generate ICMP-unreachable messages.
  Switch(config)#mls rate-limit unicast ip icmp unreachable no-route 500 10
- ICMP unreachable (ACL drop) rate limiter—This rate limiter drops most of the packets denied by an ACE in hardware. It leaks a certain number of packets to the route-processor CPU to generate ICMP-unreachable messages.
  Switch(config)#mls rate-limit unicast ip icmp unreachable acl-drop 500 10
- IP errors rate-limiter—This rate limiter specifies the rate at which unicast IP packets with errors are punted up to the route-processor CPU. Errors include bad Layer 3 checksum and Layer 2/3 length mismatch.
  Switch(config)#mls rate-limit unicast ip errors 500 10
- Universal Reverse Path Forwarding (URPF) hardware-to-CPU rate limiter—This rate limiter specifics the rate at which packets failing RPF checks are punted up to the route-processor CPU:
  Switch(config)#mls rate-limit unicast rpf-failure 500 10
- Multicast partial-signaling-controller rate-limiter—A multicast flow might be partially switched instead of completely hardware-switched; the rate limiter controls traffic from multicast partial-SC flows that are leaked to the route-processor CPU for processing—it does not consume limited hardware resources:
  Switch(config)#mls rate-limit multicast ipv4 partial 10000 10
- Multicast Internet Group Management Protocol (IGMP) (Layer 2) rate limiter—This rate limiter configures the rate at which IGMP packets are punted to the route-processor CPU:
  Switch(config)#mls rate-limit multicast ipv4 igmp 5000 10

APPENDIX B—SAMPLE EEM TCL SCRIPT

The following EEM script can be used to automatically detect that a Cisco Unified IP phone has been connected and configure the port to take advantage of the function:

```
::cisco::eem::event_register_syslog pattern "%LINK-3-UPDOWN"
#-------------------------------------------------------------------
# EEM policy to monitor for a connected Cisco IP Phone.
# Upon an event trigger, the policy will add QoS commands to switchport
# connected to the phone
#
# May 2006 - Carl Solder (csolder@cisco.com)
#
# Copyright (c) 2006 by cisco Systems, Inc.
# All rights reserved.
#-------------------------------------------------------------------
# The namespace import commands that follow import some cisco TCL extensions
# that are required to run this script
namespace import ::cisco::eem::*
namespace import ::cisco::lib::*
# Query the information for the EEM event that triggered this policy
# This is the bit of code that sets the variables for SYSLOG message
array set arr_einfo [event_reqinfo]
if {$_cerrno != 0} {
 set result [format "component=%s; subsys err=%s; posix err=%s;\n%s" \
    $_cerr_sub_num $_cerr_sub_err $_cerr_posix_err $_cerr_str]
√error $result
}
# Set variable $msg with the SYSLOG message that was captured by this event
set msg $arr_einfo(msg)
# Prime the variables with a null value
set msg_type "Null"
set state "Null"
# Check that the SYSLOG message is a link up/down
regexp {([^ ]*changed state to up)} $msg match state
# Check message is link up
if {$state == "changed state to up"} {
 # Prime the variable $intf with a null value
 set intf "Null"
 # Extract interface name from SYSLOG message
 regexp {([^ ]*.Ethernet.*[0-9])} $msg intf
 # Open the CLI and run the show cdp command
 if [catch {cli_open} result] {
 error $result $errorInfo
 } else {
```



```
 array set cli1 $result
 }
 if [catch {cli_exec $cli1(fd) "en"} result] {
 error $result $errorInfo
 }
 if [catch {cli_exec $cli1(fd) "show cdp neighbor $intf detail"} result] {
 error $result $errorInfo
 }
 # see if show command output contains Cisco IP phone keyword
 set phone "Null"
 regexp {(IP.Phone)} $result phone
 if {$phone == "IP Phone"} {
 # apply the QoS commands to the named interface
 if [catch {cli_exec $cli1(fd) "conf t"} result] {
 error $result $errorInfo
 }
 if [catch {cli_exec $cli1(fd) "mls qos"} result] {
 error $result $errorInfo
 }
 if [catch {cli_exec $cli1(fd) "interface $intf"} result] {
 error $result $errorInfo
 }
 if [catch {cli_exec $cli1(fd) "mls qos trust cos"} result] {
 error $result $errorInfo
 }
 if [catch {cli_exec $cli1(fd) "mls qos trust extend cos 0"} result] {
 error $result $errorInfo
 }
 if [catch {cli_exec $cli1(fd) "mls qos map cos-dscp 0 10 18 26 34 46 48 56"} result] {
 error $result $errorInfo
 }
 if [catch {cli_close $cli1(fd) $cli1(tty_id)} result] {
 error $result $errorInfo
 }
 action_syslog msg "QoS Configuration added to interface $intf for attached IP Phone"
 }
}
```


Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in USA 206717.BL 06/06