Chapter 7:
Preparing the Campus Infrastructure for Advanced Services



CCNP SWITCH: Implementing IP Switching

Cisco | Networking Academy®
Mind Wide Open™

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

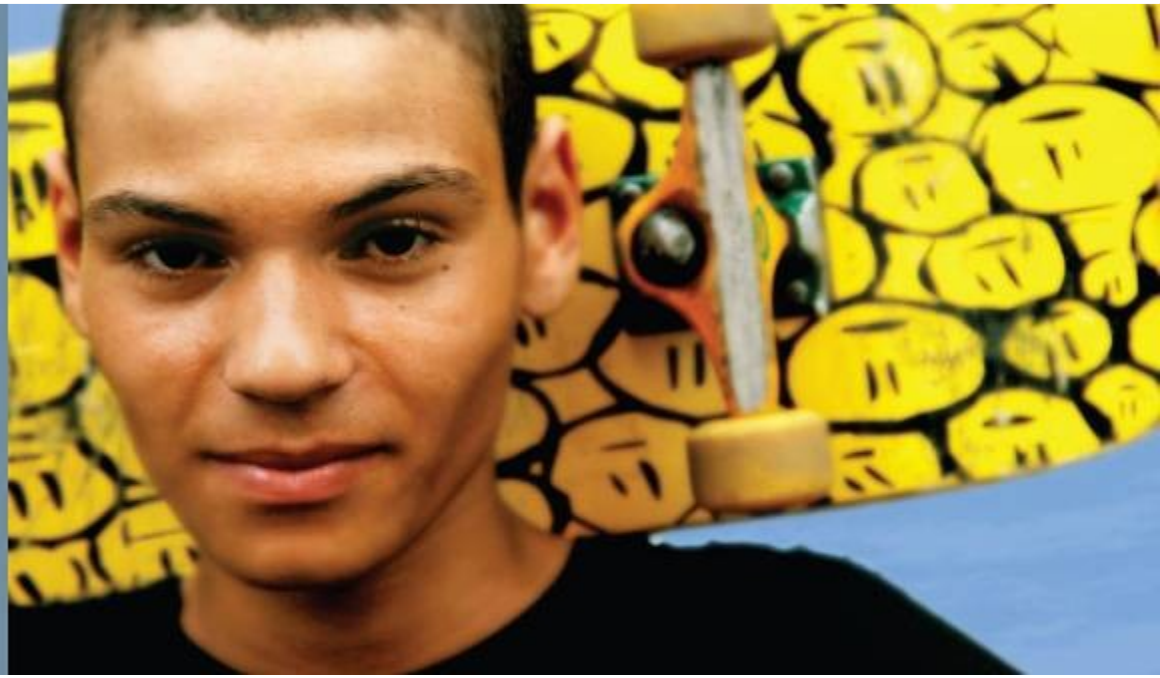


Chapter 7 Objectives

- Assess the impact of WLAN's, voice and video on campus infrastructure operations.
- Describe quality of service in a campus infrastructure to support advanced services.
- Implement multicast in a campus infrastructure to support advanced services.
- Prepare campus networks for the integration of wireless LANs.
- Prepare campus networks for the integration of voice.
- Prepare campus networks for the integration of video.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Planning for Wireless, Voice, and Video Applications in the Campus Network



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Purpose of Wireless Network Implementations in the Campus Network

- **Productivity:** Users gain productivity through the ability to access resources while in meetings, training, presentations, and at lunch.
- **Mobility:** Users on the go within the campus can be mobile with access to campus resources, such as e-mail.
- **Enhanced collaboration:** Wireless networks enable enhanced user collaboration through the benefit of a network without wires.
- **Campus interconnectivity:** Wireless networks have the capability to interconnect remote offices and offsite networks that cannot interconnect to the campus network over traditional physical network cable.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Purpose of Voice in the Campus Network

- More efficient use of bandwidth and equipment
- Lower costs for telephony network transmission
- Consolidation of voice and data network expense
- Increased revenue from new service
- Capability to leverage access to new communications devices
- Flexible pricing structure
- Emphasis on greater innovation in service

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Purpose of Video Deployments in the Campus Network

- **Collaboration:** Video conferencing technologies such as TelePresence and the video support in WebEx support enhanced collaboration.
- **Cost-savings:** Video technologies reduce travel costs by enabling remote users to attend meetings, trainings, and so on without being physically present.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Planning for the Campus Network to Support Wireless Technologies

1. Introduction to Wireless LAN's (WLAN's)
2. Cisco WLAN Solutions Applied to Campus Networks
3. Comparing and Contrasting WLAN's and LAN's
4. Standalone Versus Controller-Based Approaches to WLAN Deployments in the Campus Network
5. Gathering Requirements for Planning a Wireless Deployment

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



1. Introduction to Wireless LAN's

Wireless Data Communication Methods

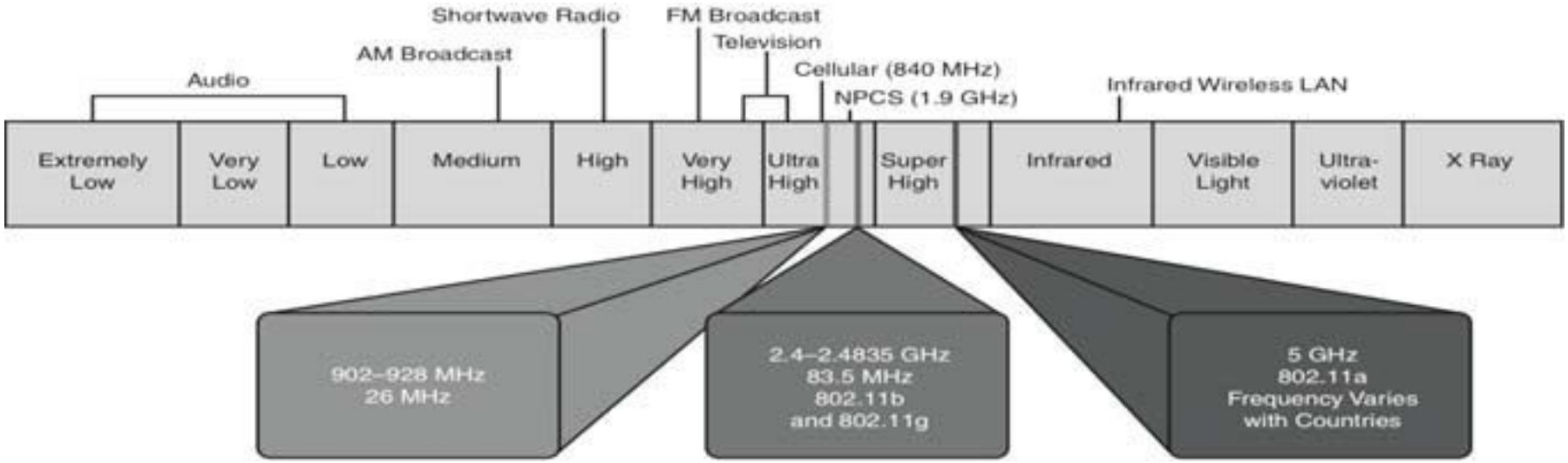
- Infrared (III): High data rates, lower cost, and short distance
- Narrowband: Low data rates, medium cost, license required, limited distance
- Spread spectrum: Limited to campus coverage, medium cost, high data rates
- Personal Communications Service (PCS): Low data rates, medium cost, citywide coverage
- Cellular: Low to medium cost, national and worldwide coverage (typical cell phone carrier)
- Ultra-wideband (UWB): Short-range high-bandwidth coverage

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

1. Introduction to Wireless LAN's

Spread Spectrum Technology

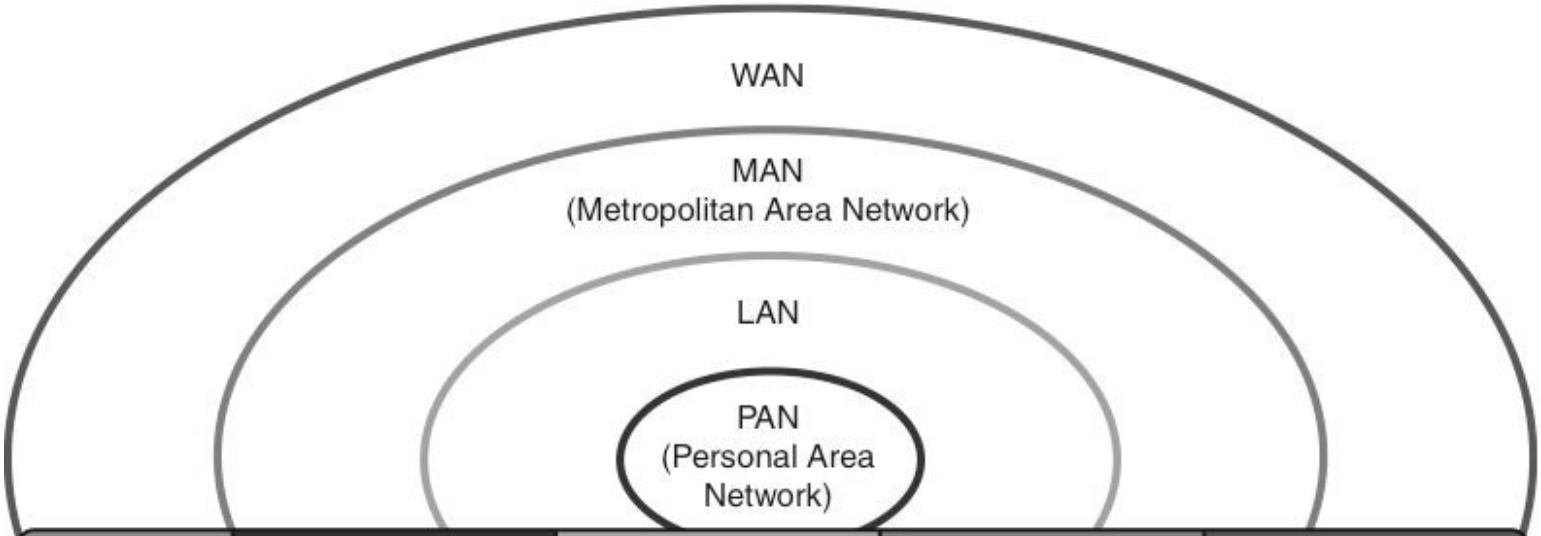
- 900-MHz band: 902 MHz to 928 MHz
- 2.4-GHz band: 2.4 GHz to 2.483 GHz
- 5-GHz band: 5.150 MHz to 5.350 MHz, 5.725 MHz to 5.825 MHz, with some countries supporting middle bands between 5.350 MHz and 5.825 MHz



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

1. Introduction to Wireless LAN's

Wireless Technologies

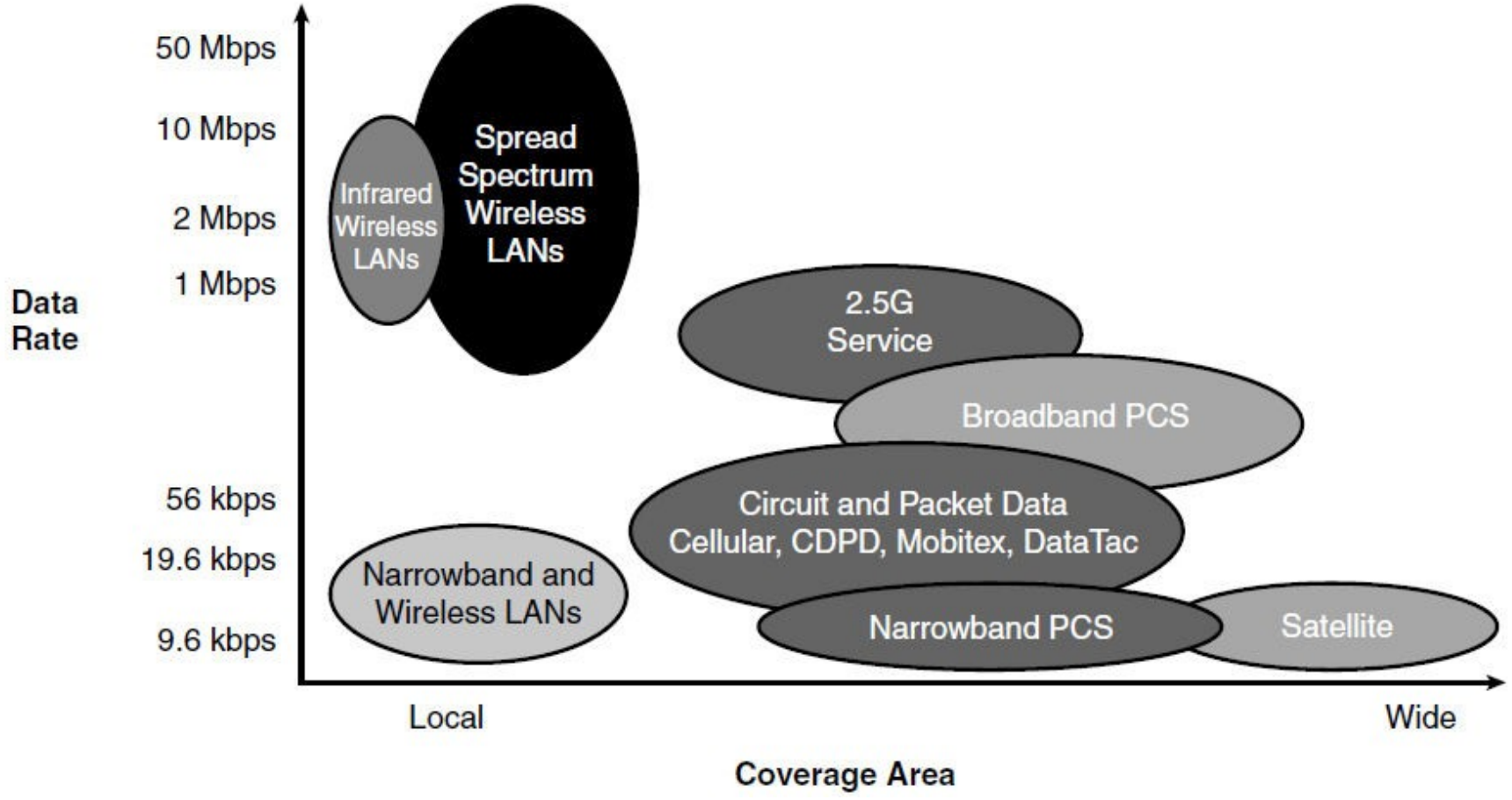


	PAN	LAN	MAN	WAN
Standards	Bluetooth	IEEE 802.11a/b/g, HyperLAN2	802.16 MMDS, LMDS	GSM, GPRS, CDMA, 2.5–3G
Speed	<1 Mbps	2–54+ Mbps	22+ Mbps	10–384 kbps
Range	Short	Medium	Medium-long	Long
Applications	Peer-to-Peer, Device to Device	Enterprise Networks	Fixed, Last-mile Access	PDAs, Mobile Phones, Cellular Access

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

1. Introduction to Wireless LAN's

Data Rates and Coverage Areas



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



2. Cisco WLAN Solutions Applied to Campus Networks

Cisco Unified Wireless Network

- Client devices
- Mobility platform
- Network unification
- World-class network management
- Unified advanced services

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



3. Comparing and Contrasting WLAN's and LAN's

WLAN's:

- Users move freely around a facility.
- Users enjoy real-time access to the wired LAN at wired Ethernet speeds.
- Users access all the resources of wired LAN's.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



3. Comparing and Contrasting WLAN's and LAN's

WLAN's versus LAN's (1):

- Both WLANs and wired LANs define the physical and data link layers and use MAC addresses.
- In WLANs, radio frequencies are used as the physical layer of the network.
- WLANs use carrier sense multiple access collision avoidance (CSMA/CA) instead of carrier sense multiple access collision detection (CSMA/CD), which is used by Ethernet LANs.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



3. Comparing and Contrasting WLAN's and LAN's

WLAN's versus LAN's (2):

- WLANs use a different frame format than wired Ethernet LANs. Additional information for WLANs is required in the Layer 2 header of the frame.
- Radio waves used by WLANs have problems not found in wires.
- Connectivity issues in WLANs can be caused by coverage problems, RF transmission, multipath distortion, and interference from other wireless services or other WLANs.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



3. Comparing and Contrasting WLAN's and LAN's

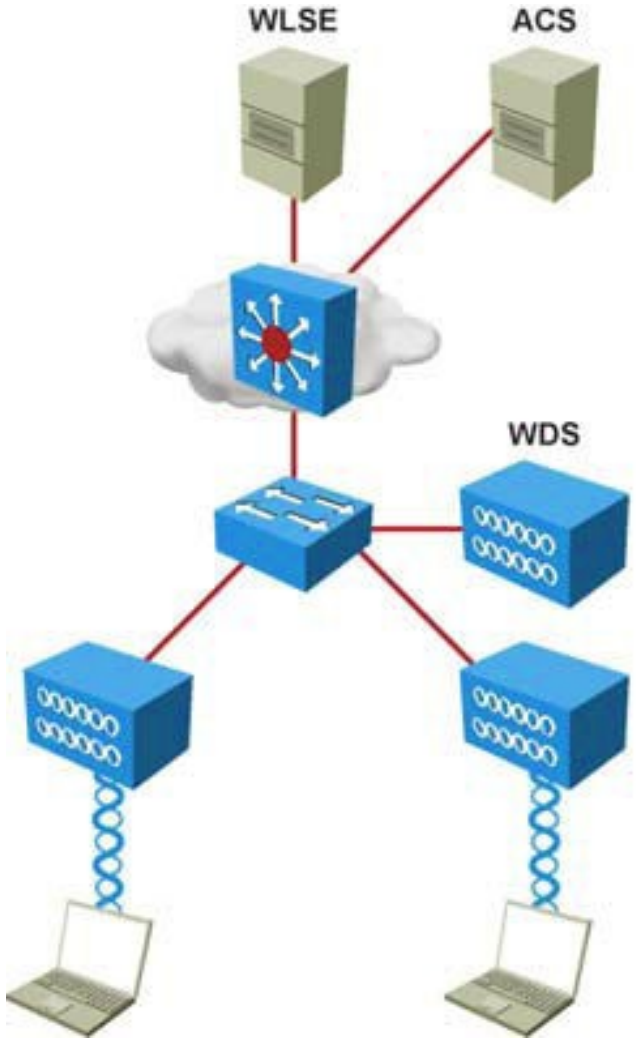
WLAN's versus LAN's (3):

- Privacy issues are possible because radio frequencies can reach outside the facility and physical cable plan.
- In WLANs, mobile clients are used to connect to the network.
- Mobile devices are often battery-powered.
- WLAN's must follow country-specific regulations for RF power and frequencies.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Standalone WLAN Solution:

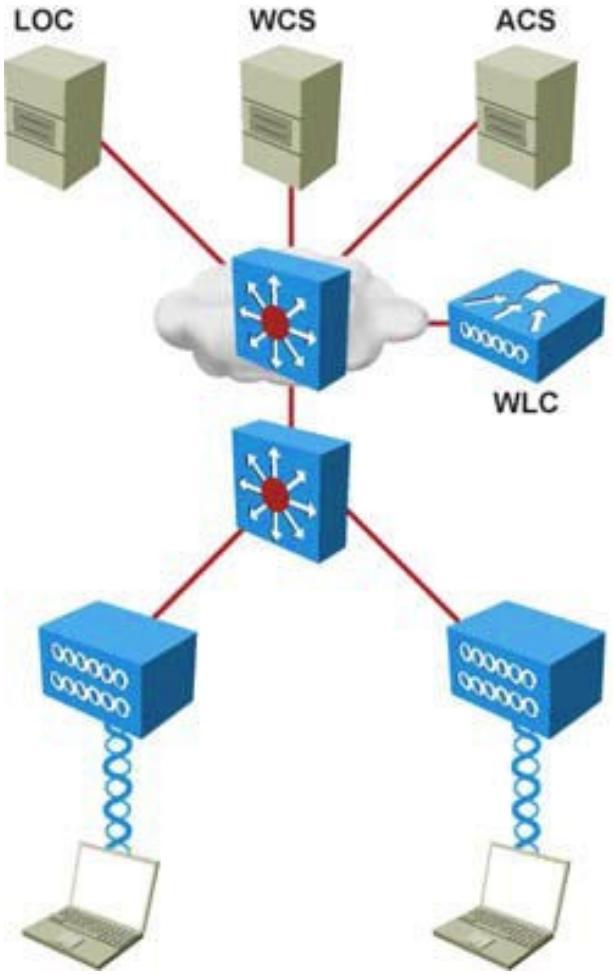
- Access Control Server (ACS)
  - RADIUS/TACACS+
- Cisco Wireless LAN Solution Engine (WLSE)
  - Centralized management and monitoring
- Wireless Domain Services (WDS)
  - Management support for WLSE
- Network infrastructure
- Standalone access points



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Controller-Based WLAN Solution (1)

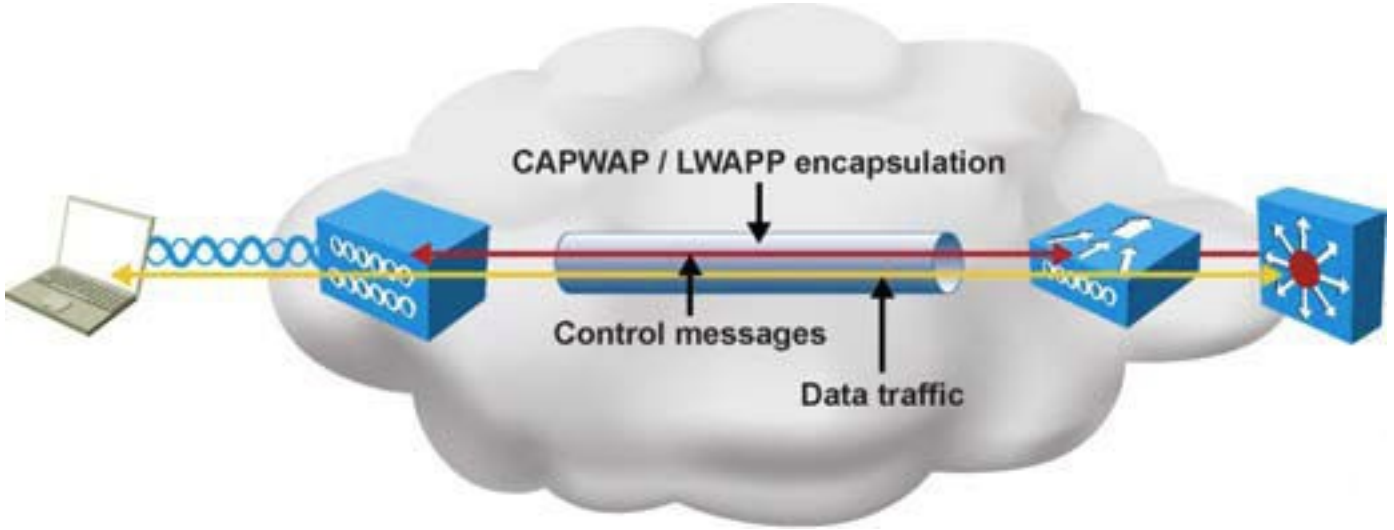
- Access Control Server (ACS):
  - RADIUS/TACACS+
- Wireless Control System (WCS)
  - Centralized management and monitorin
- Location appliance
  - Location tracking
- Wireless LAN Controller (WLC)
  - AP and WLAN configuration
- Network infrastructure
  - PoE switch and router
- Controller-based access points



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Controller-Based WLAN Solution (2)

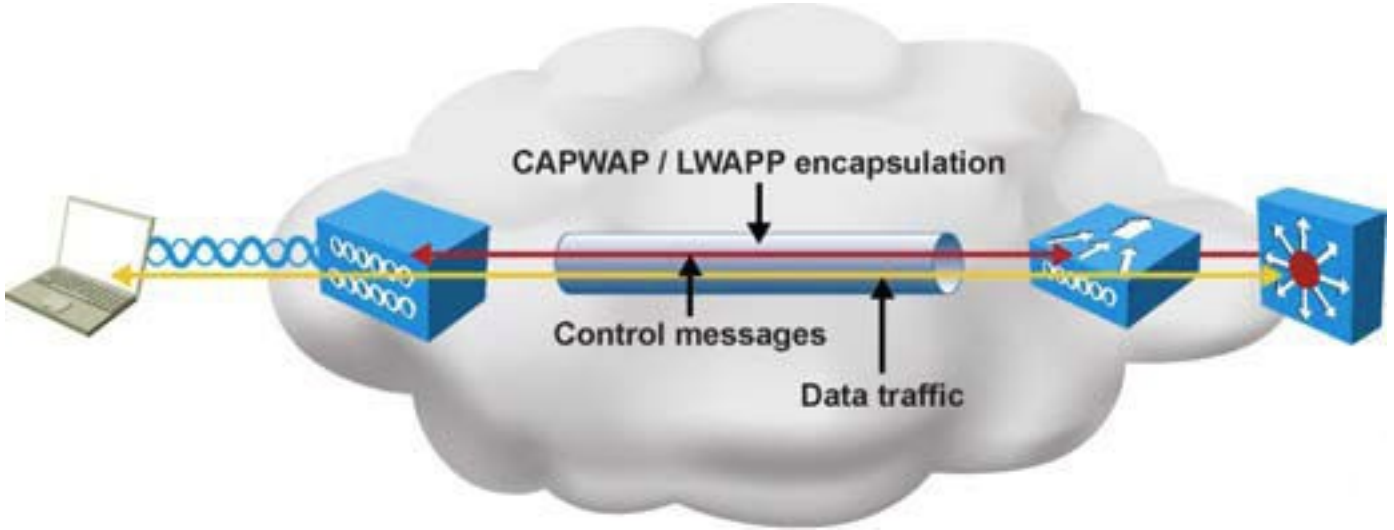
- Processes of 802.11 wireless protocols split between AP's and WLC (aka, "split MAC")



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Controller-Based WLAN Solution (3)

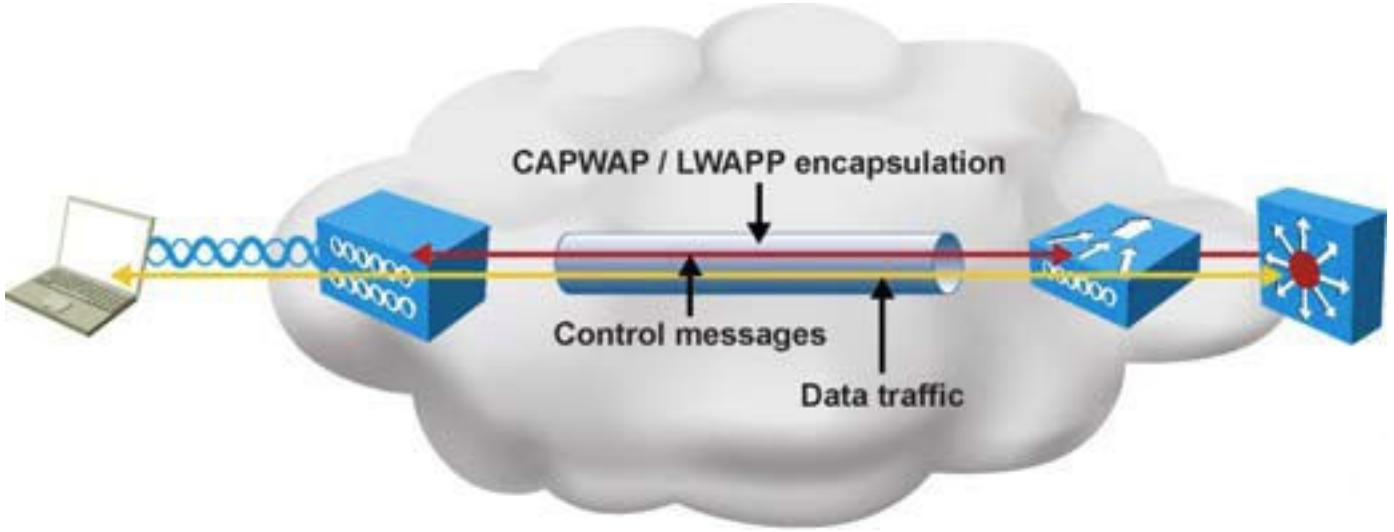
- AP MAC functions:
  - 802.11: Beacons, probe responses
  - 802.11 control: Packet acknowledgment and transmission.
  - 802.11e: Frame queuing and packet prioritization.
  - 802.11i: MAC layer data encryption and decryption.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Controller-Based WLAN Solution (4)

- Wireless LAN Controller MAC functions:
  - 802.11 MAC management: Association requests and actions.
  - 802.11e: Resource reservation.
  - 802.11i: Authentication and key management.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

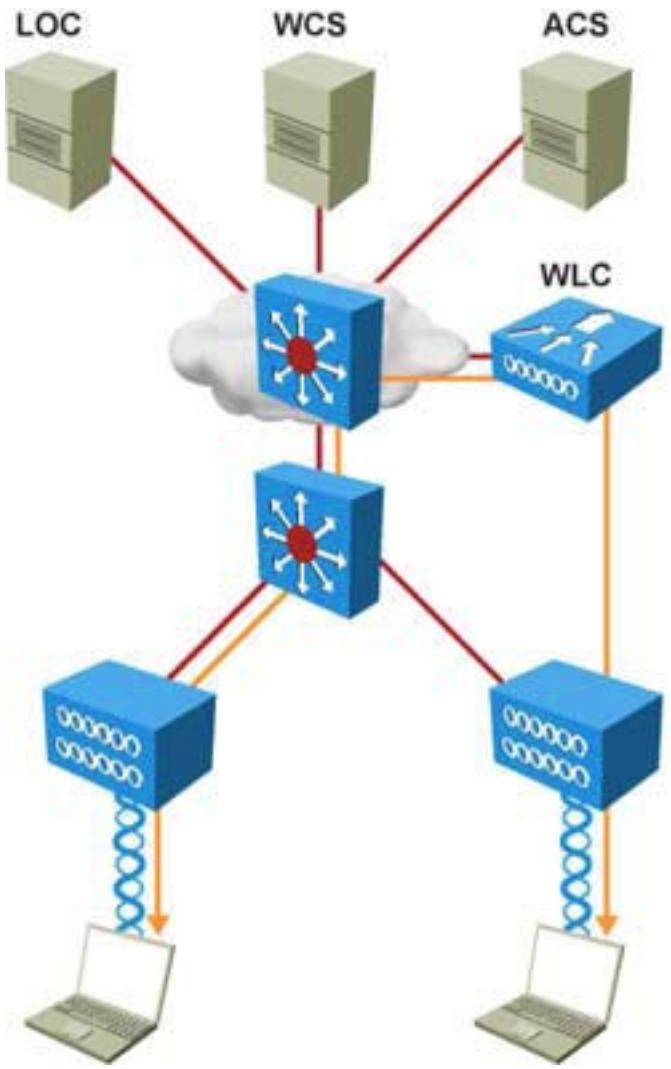
Controller-Based WLAN Solution (5)

- Traffic Handling in Controller-Based Solutions
  - Data and control messages are encapsulated between the access point and the WLAN controller using the Control and Provisioning of Wireless Access Points (CAPWAP) method or the Lightweight Access Point Protocol (LWAPP). Although both are standards-based, LWAPP was never adopted by any other vendor other than Cisco.
  - Control traffic between the access point and the controller is encapsulated with the LWAPP or CAPWAP and encrypted.
  - The data traffic between the access point and controller is also encapsulated with LWAPP or CAPWAP. The data traffic is not encrypted. It is switched at the WLAN controller, where VLAN tagging and quality of service (QoS) are also applied.
  - The access point accomplishes real-time frame exchange and certain real-time portions of MAC management. All client data traffic is sent via the WLAN controller.
  - WLAN controller and access point can be in the same or different broadcast domains and IP subnets. Access points obtain an IP address via DHCP, and then join a controller via a CAPWAP or LWAPP discovery mechanism.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

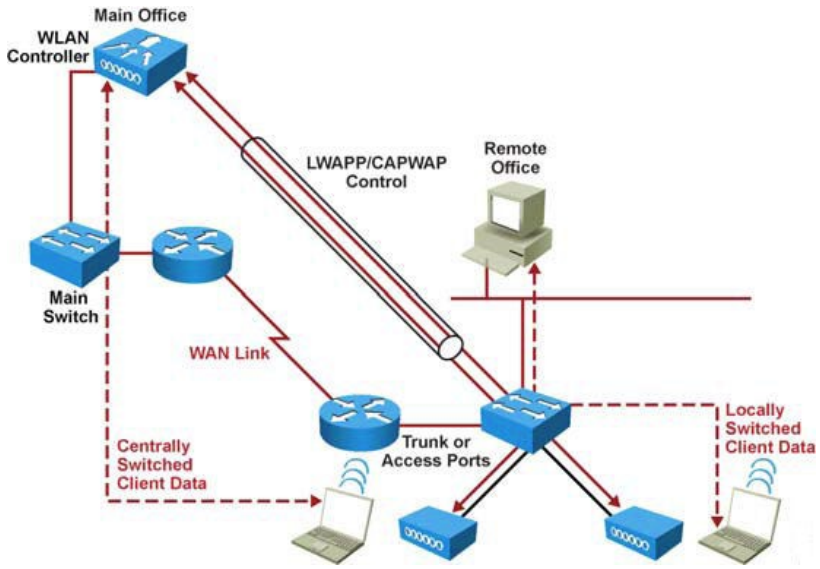
Controller-Based WLAN Solution (6)

- Traffic Flow in a Controller-Based Solution
  - Traffic between two wireless mobile stations is forwarded from the access points to the controller and then sent to wireless mobile stations.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Controller-Based WLAN Solution (7)



- Hybrid Remote Edge Access Points (HREAP)
- Provides high-availability of controller-based wireless solutions in remote offices.
- AP's still offer wireless client connectivity when their connection to the WLC is lost.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Comparison of Standalone and Controller-Based Solutions

Object/Action	Standalone	Controller-Based
Access point	Standalone IOS	Controller-based delivered IOS
Configuration	Via access point	Via WLC
Operation	Independent	Dependent on WLC
Management and monitoring	Via WLSE	Via WCS
Redundancy	Via multiple access points	Via multiple WLC's

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Planning Deployment and Implementation

- Determine how many ports of what type are needed and how they should be configured.
- Check existing network to verify how the requirements can integrate into the existing deployment.
- Plan additional equipment needed to fulfill the requirements.
- Plan implementation.
- Implement new network components.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Sample Test Plan

- Can you reach the AP or WLC from management stations?
- Can the AP reach the DHCP server?
- Does the AP get an IP address from the DHCP server?
- Can the WLC reach the Radius or TACACS+ server?
- Does the client get an IP address?
- Can the client access network, server, or Internet services?

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Planning for the Campus Network to Support Voice

- Unified Communications
- Campus Network Design Requirements for Deploying VoIP

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Unified Communications

- **IP Phone:** Provides IP voice to the desktop.
- **Gatekeeper:** Provides connection admission control (CAC), bandwidth control and management, and address translation.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Unified Communications - Gateway

- Provides translation between VoIP and non-VoIP networks, such as the public switched telephone network (PSTN). It also provides physical access for local analog and digital voice devices, such as telephones, fax machines, key sets, and PBXs.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Unified Communications – Multipoint Control Unit

- Provides real-time connectivity for participants in multiple locations to attend the same videoconference or meeting.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Unified Communications – Call Agent

- Provides call control for IP phones, CAC, bandwidth control and management, and telephony address translation for IP addresses or telephone numbers.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Unified Communications – Application Server

- Provides services such as voice mail, unified messaging, and Cisco Unified Communications Manager Attendant Console.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Unified Communications – Videoconference Station

- Provides access for end-user participation in videoconferencing. The videoconference station contains a video capture device for video input and a microphone for audio input. The user can view video streams and hear the audio that originates at a remote user station.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Campus Network Design Requirements for Deploying VoIP

QoS Requirements for Voice

- Voice packets are small, typically between 60 bytes and 120 bytes in size.
- VoIP cannot tolerate drop or delay because it can lead to poor voice quality.
- VoIP uses UDP because TCP retransmit capabilities are useless for voice.
- For optimal voice quality, delay should be less than 150 ms one way.
- Acceptable packet loss is 1 percent.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Comparing Voice and Data Traffic



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

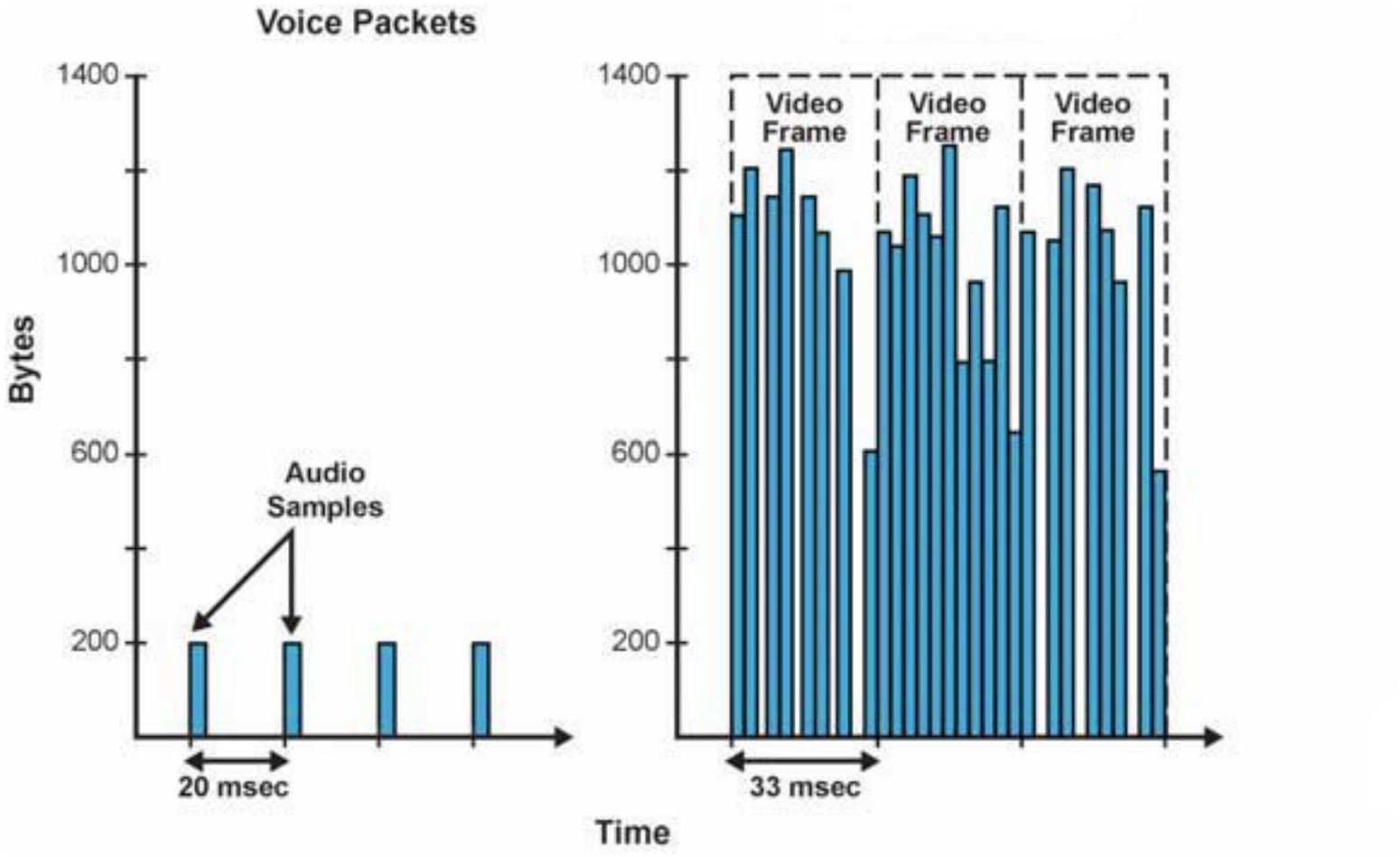


Planning for the Campus Network to Support Video

- Voice and Video Traffic
- Video Traffic Flow in the Campus Network
- Design Requirements for Voice, Data, and Video in the Campus Network

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

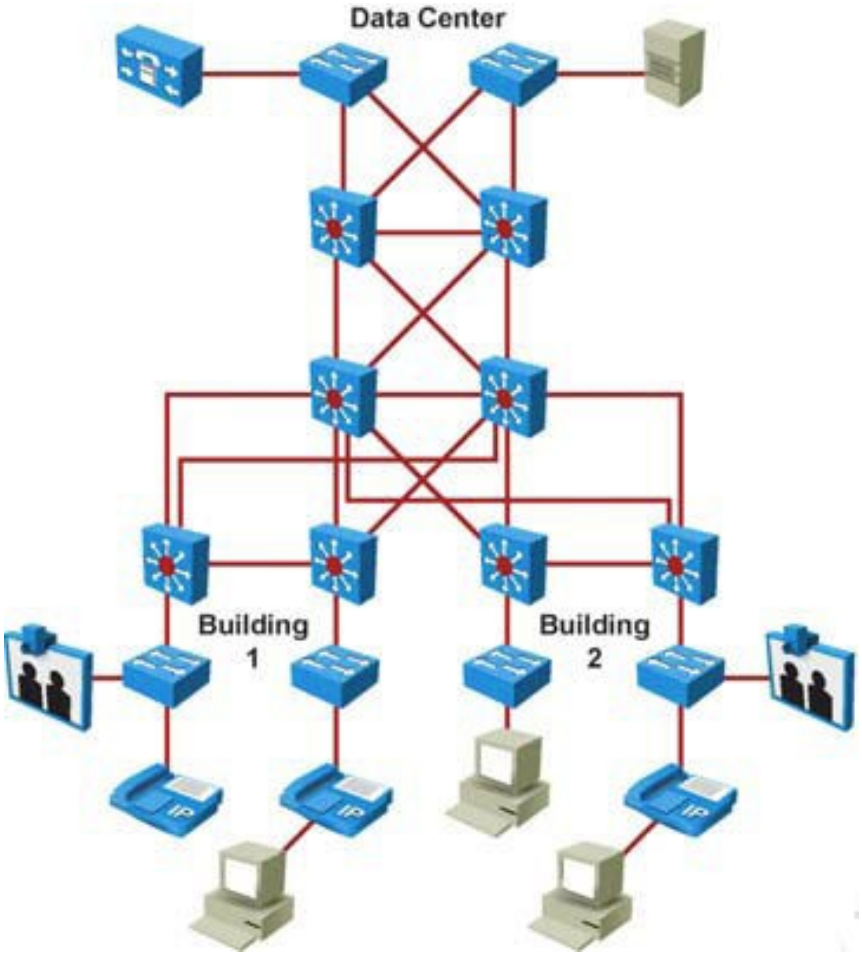
Planning for the Campus Network to Support Video – Voice and Video Traffic



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Planning for the Campus Network to Support Video – Video Traffic Flow in the Campus Network

- Determine which applications will be deployed:
  - Peer-to-peer applications, such as TelePresence
  - Video streaming applications, such as video-on-demand training
  - Video TV-type applications, such as Cisco IP TV
  - IP Surveillance applications for security



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Planning for the Campus Network to Support Video – Design Requirements for Voice, Data, and Video in the Campus Network

Requirement	Data	Voice	Video
Bandwidth	High	Low	High
Delay	If less than a few msec, not applicable	Less than 150 msec	Less than 150 msec for real-time video
Jitter	Not applicable	Low	Low
Packet Loss	Less than 5%	Less than 1%	Less than 1%
Availability	High	High	High
Inline Power	No	Optional	Optional for select devices
Security	High	Medium	Low or Medium
Provisioning	Medium Effort	Significant Effort	Medium Effort

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Understanding QoS



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

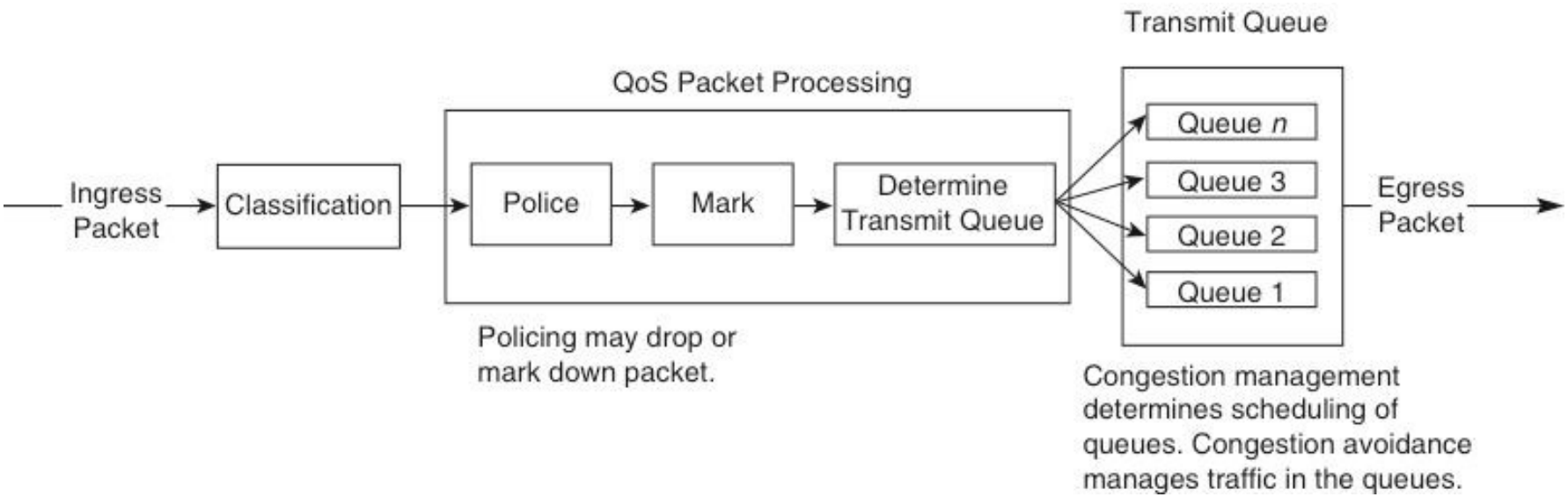


QoS Service Models

- **Best-effort service:** The standard form of connectivity without guarantees. This type of service, in reference to Catalyst switches, uses first-in, first-out (FIFO) queues, which simply transmit packets as they arrive in a queue with no preferential treatment.
- **Integrated service:** IntServ, also known as hard QoS, is a reservation of services. In other words, the IntServ model implies that traffic flows are reserved explicitly by all intermediate systems and resources.
- **Differentiated service:** DiffServ, also known as soft QoS, is class-based, in which some classes of traffic receive preferential handling over other traffic classes. Differentiated services use statistical preferences, not a hard guarantee such as integrated services. In other words, DiffServ categorizes traffic and then sorts it into queues of various efficiencies.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Cisco QoS Model



- Traffic classification and marking
- Traffic shaping and policing
- Congestion management
- Congestion avoidance

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Scenarios for AutoQoS

- Small to medium-sized businesses that must deploy IP telephony quickly but lack the experience and staffing to plan and deploy IP QoS services.
- Large customer enterprises that need to deploy Cisco telephony solutions on a large scale, while reducing the costs, complexity, and time frame for deployment, and ensuring that the appropriate QoS for voice applications is set in a consistent fashion
- International enterprises or service providers requiring QoS for VoIP where little expertise exists in different regions of the world and where provisioning QoS remotely and across different time zones is difficult

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



AutoQoS Aids Successful QoS Deployment

- Application classification
- Policy generation
- Configuration
- Monitoring and reporting
- Consistency

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Traffic Classification and Marking

- DSCP, ToS, and CoS
- Packet Classification Methods

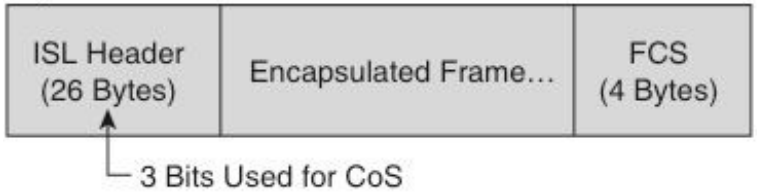
© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

DSCP, ToS, and CoS

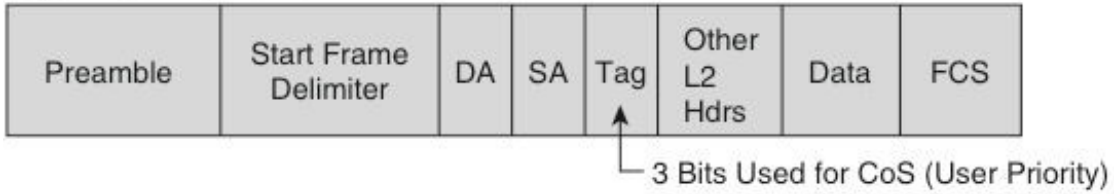
Typical Ethernet Packet



Layer 2 ISL Frame



Layer 2 802.1Q Frame



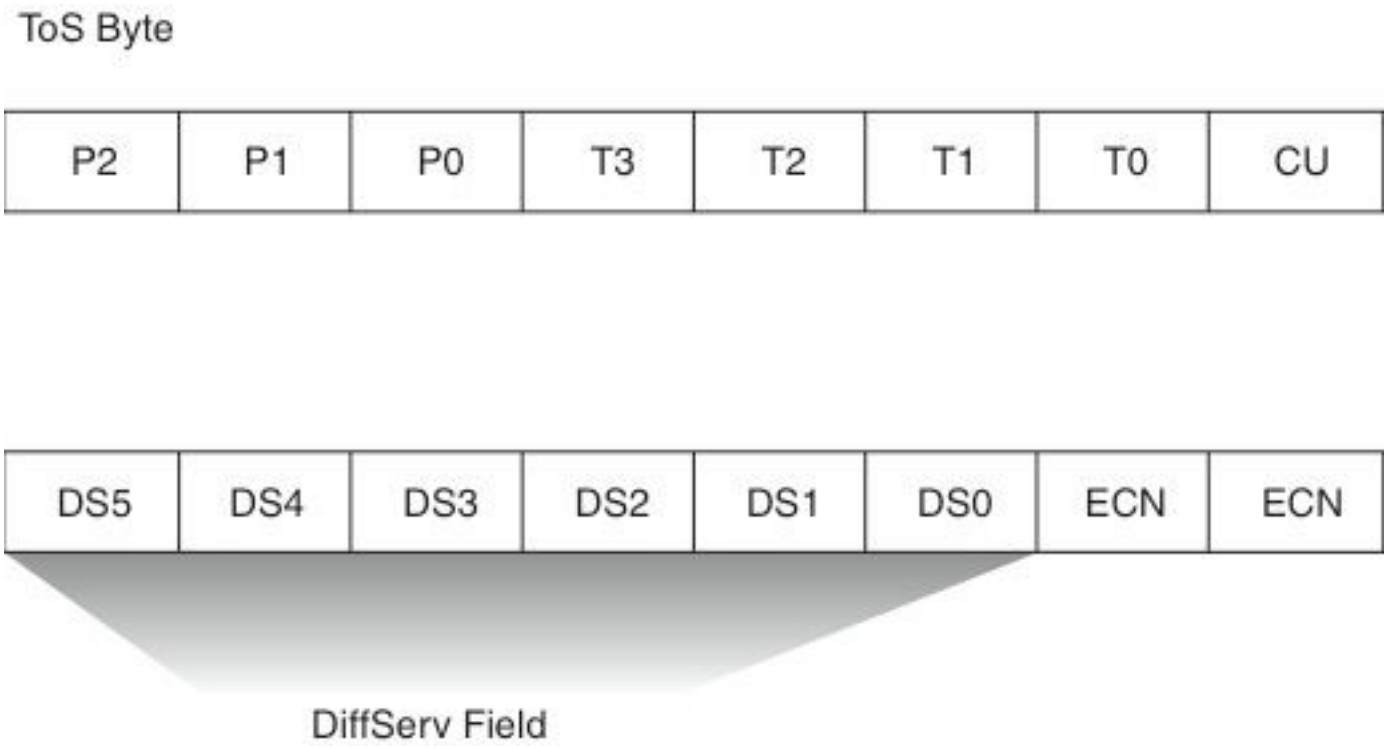
Layer 3 IPv4 Packet



IP Precedence: 3 Most Significant Bits (MSBs) of ToS
DSCP: 6 MSBs of ToS

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Differentiated Services Code Point (DSCP)



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Cisco Switch Packet Classification Methods

- Per-interface trust modes
- Per-interface manual classification using specific DSCP, IP Precedence, or CoS values
- Per-packet based on access lists
- Network-Based Application Recognition (NBAR)

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



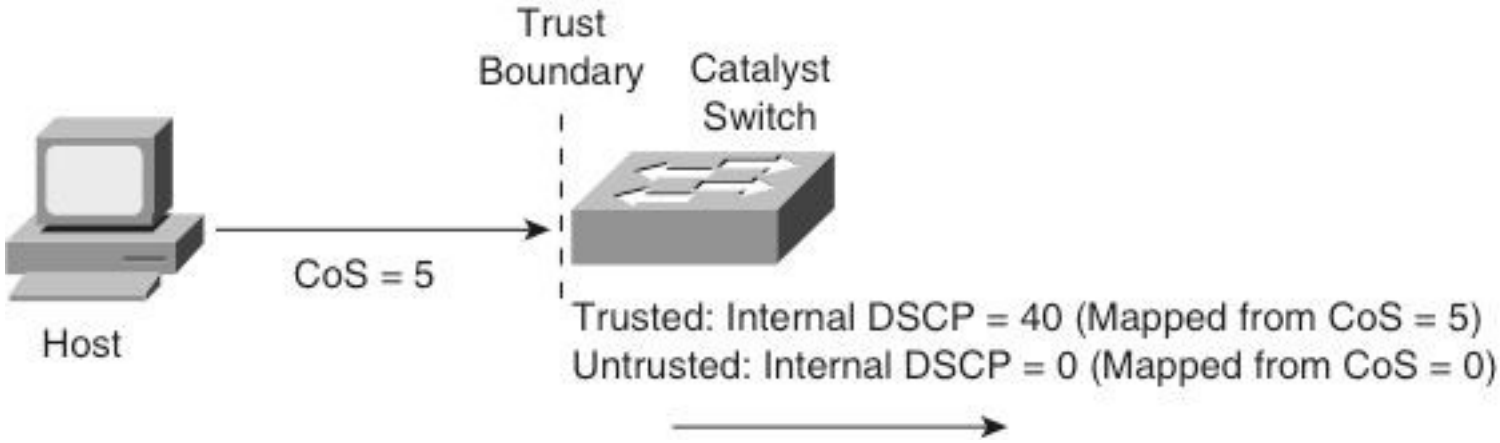
Trust Boundaries and Configurations

Default CoS-to-DSCP Mapping								
CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Default IP Precedence-to-DSCP Mapping								
IP Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

QoS Trust



- The Cisco Catalyst switch QoS trust concept relies on the configurable port trust feature. When the switch trusts CoS for ingress packets on a port basis, the switch maps the ingress value to the respective DSCP value. When the ingress interface QoS configuration is untrusted, the switch uses 0 for the internal DSCP value for all ingress packets.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

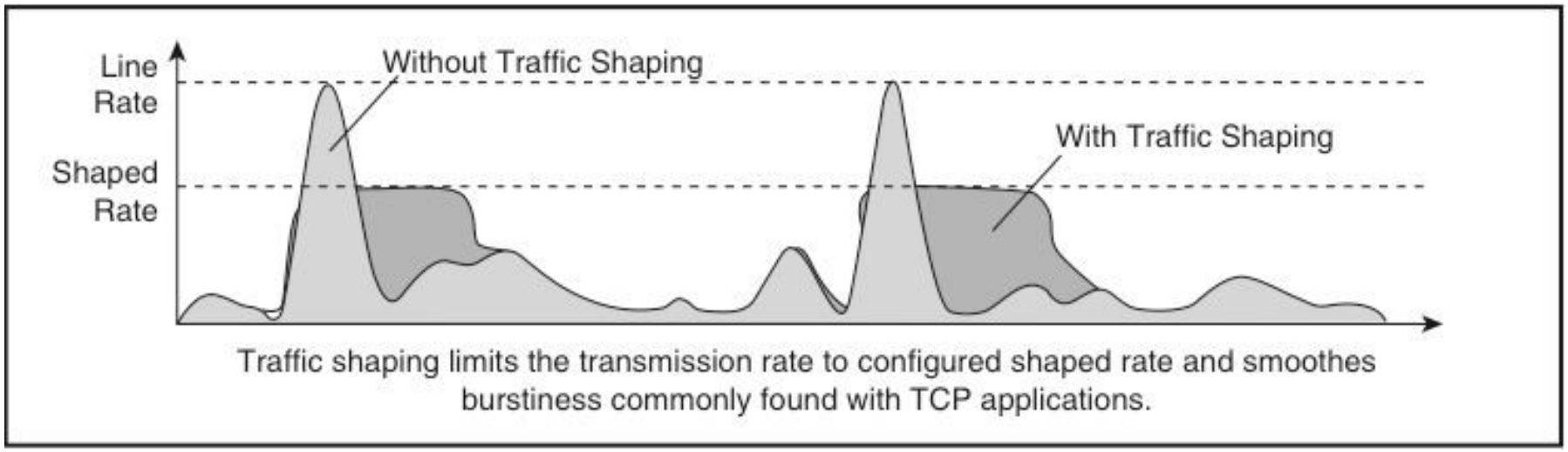
Marking

- Marking refers to changing the DSCP, CoS, or IP Precedence bits on ingress frames on a Catalyst switch.
- Marking is configurable on a per-interface basis or via a policy map.
- Marking alters the DSCP value of packets, which in turn affects the internal DSCP.
- For instance, an example of marking would be to configure a policy map to mark all frames from a video server on a per-interface basis to a DSCP value of 40, resulting in an internal DSCP value of 40 as well.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Traffic Shaping

- Traffic shaping meters traffic rates and delays (buffers) excessive traffic so that the traffic rates stay within a desired rate limit. As a result, shaping smoothes excessive bursts to produce a steady flow of data.

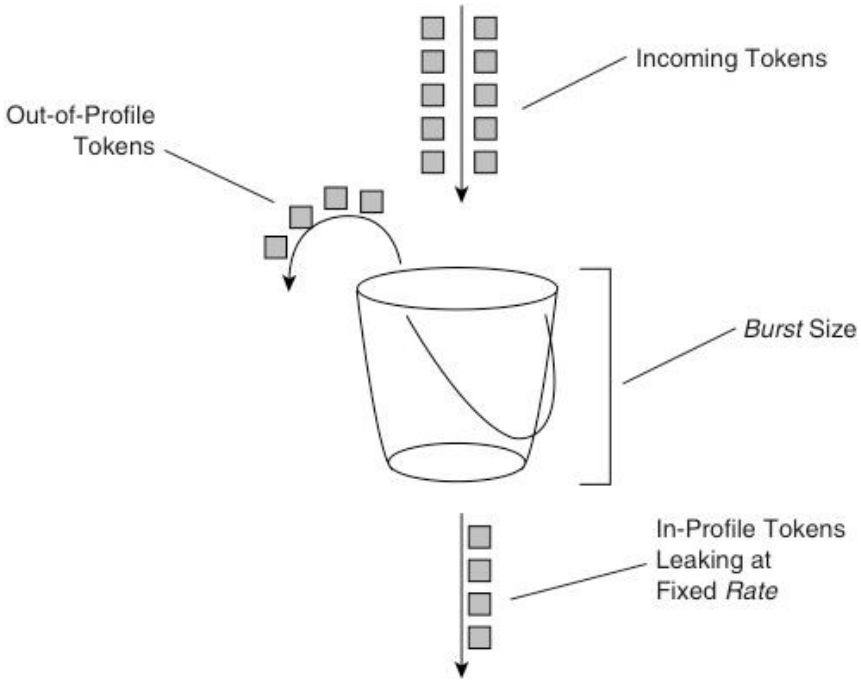


Traffic shaping limits the transmission rate to configured shaped rate and smoothes burstiness commonly found with TCP applications.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Traffic Policing

- Traffic policing takes a specific action for out-of-profile traffic above a specified rate. Policing does not delay or buffer traffic.
- The action for traffic that exceeds a specified rate is usually drop; however, other actions are permissible, such as trusting and marking.
- Policing follows the leaky token bucket algorithm, which allows for bursts of traffic as opposed to rate limiting.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



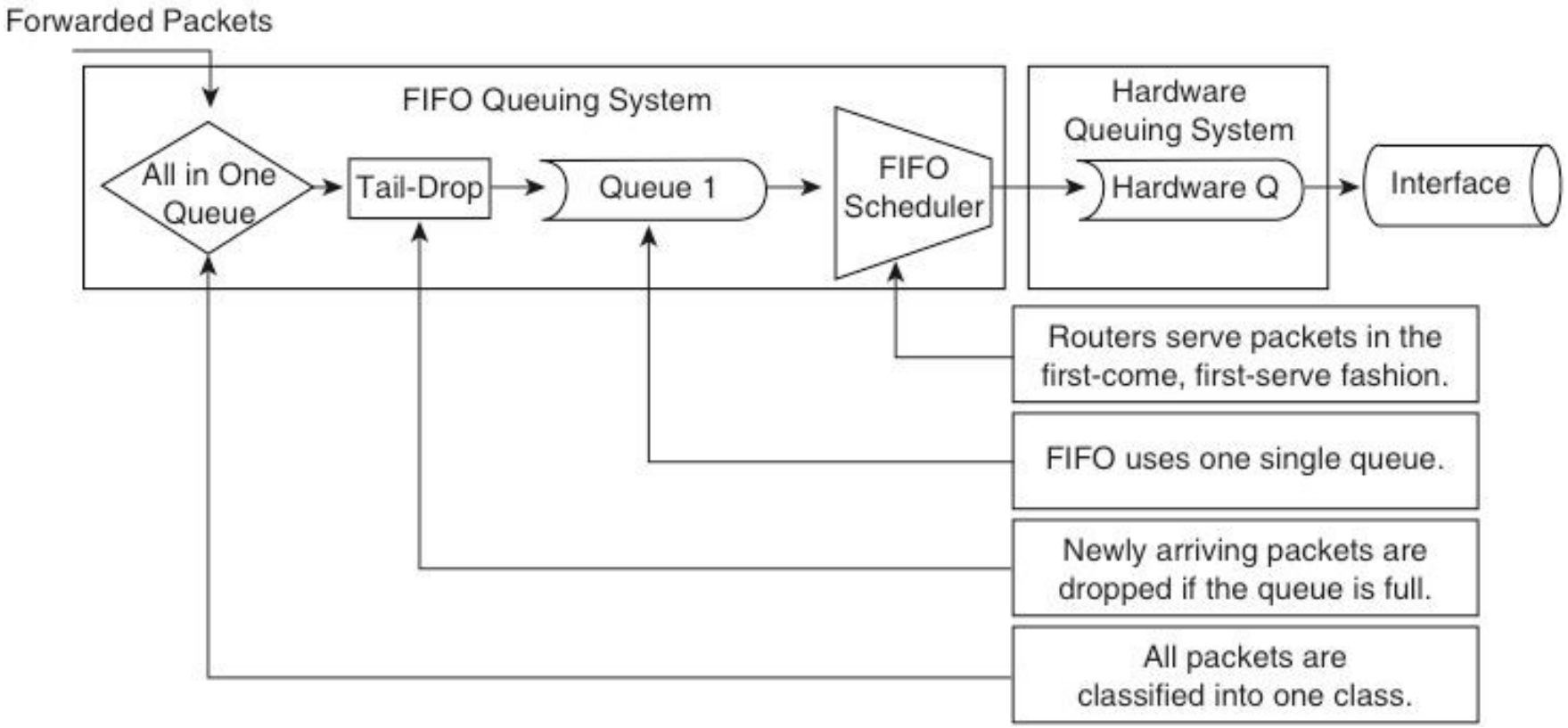
Congestion Management

- FIFO queuing
- Weighted round robin (WRR) queuing
- Priority queuing
- Custom queuing

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Congestion Management – FIFO Queuing

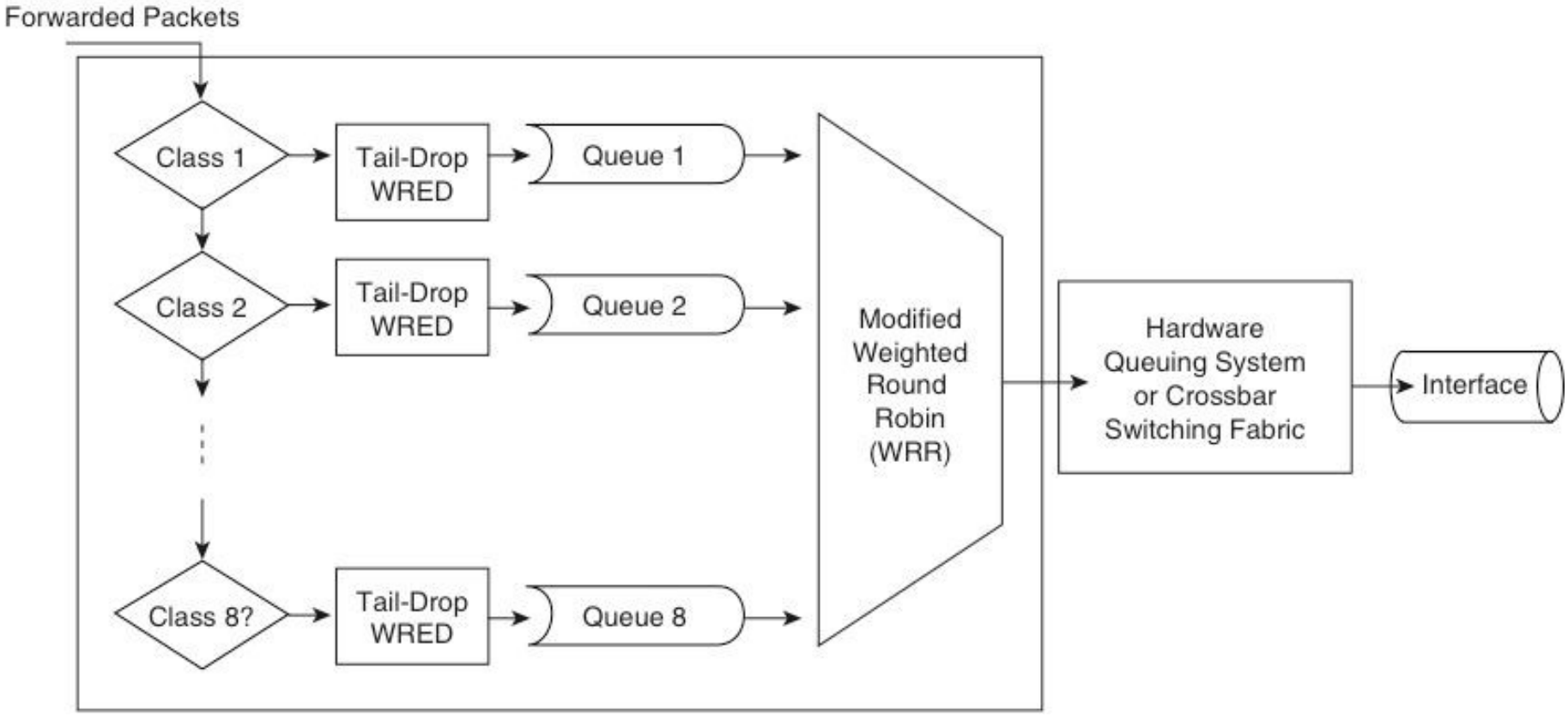
- FIFO queuing places all egress frames into the same queue. Essentially, FIFO queuing does not use classification.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Congestion Management – WRR Queuing

- Weighted round robin queuing uses a configured weight value for each egress queue.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Congestion Management – Priority Queuing

- One method of prioritizing and scheduling frames from egress queues is to use priority queuing. When applying strict priority to one of these queues, the switch schedules frames from that queue if there are frames in that queue before servicing any other queue. Cisco switches ignore WRR scheduling weights for queues configured as priority queues; most Catalyst switches support the designation of a single egress queue as a priority queue.
- Priority queuing is useful for voice applications in which voice traffic occupies the priority queue. However, since this type of scheduling can result in queue starvation in the non-priority queues, the remaining queues are subject to the WRR queuing to avoid this issue.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Congestion Management – Custom Queuing

- Another method of queuing available on Cisco switches strictly for WAN interfaces is Custom Queuing (CQ), which reserves a percentage of available bandwidth for an interface for each selected traffic type. If a particular type of traffic is not using the reserved bandwidth, other queues and types of traffic might use the remaining bandwidth.
- CQ is statically configured and does not provide for automatic adaptation for changing network conditions. In addition, CQ is not recommended on high-speed WAN interfaces; refer to the configuration guides for CQ support on LAN interfaces and configuration details.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Congestion Avoidance

- Congestion-avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottleneck points.
- The two congestion avoidance algorithms used by Cisco switches are:
  - Tail Drop – this is the default algorithm
  - Weighted Random Early Detection (WRED)

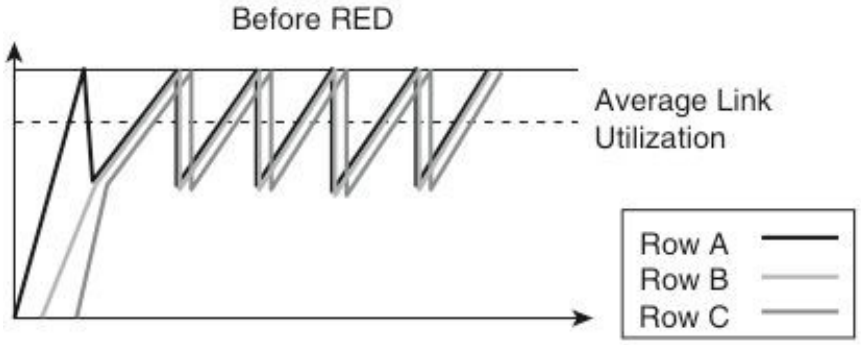
© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

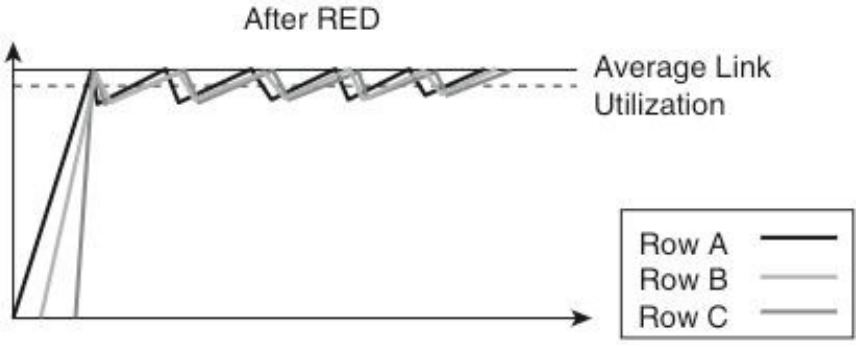
Congestion Avoidance – Tail Drop

- The dropping of frames usually affects ongoing TCP sessions. Arbitrary dropping of frames with a TCP session results in concurrent TCP sessions simultaneously backing off and restarting, yielding a “saw-tooth” effect. As a result, inefficient link utilization occurs at the congestion point (TCP global synchronization).
- Aggressive TCP flows might seize all space in output queues over normal TCP flow as a result of tail drop.
- Excessive queuing of packets in the output queues at the point of congestion results in delay and jitter as packets await transmission.
- No differentiated drop mechanism exists; premium traffic is dropped in the same manner as best-effort traffic.
- Even in the event of a single TCP stream across an interface, the presence of other non-TCP traffic might congest the interface. In this scenario, the feedback to the TCP protocol is poor; as a result, TCP cannot adapt properly to the congested network.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Congestion Avoidance – WRED (1)



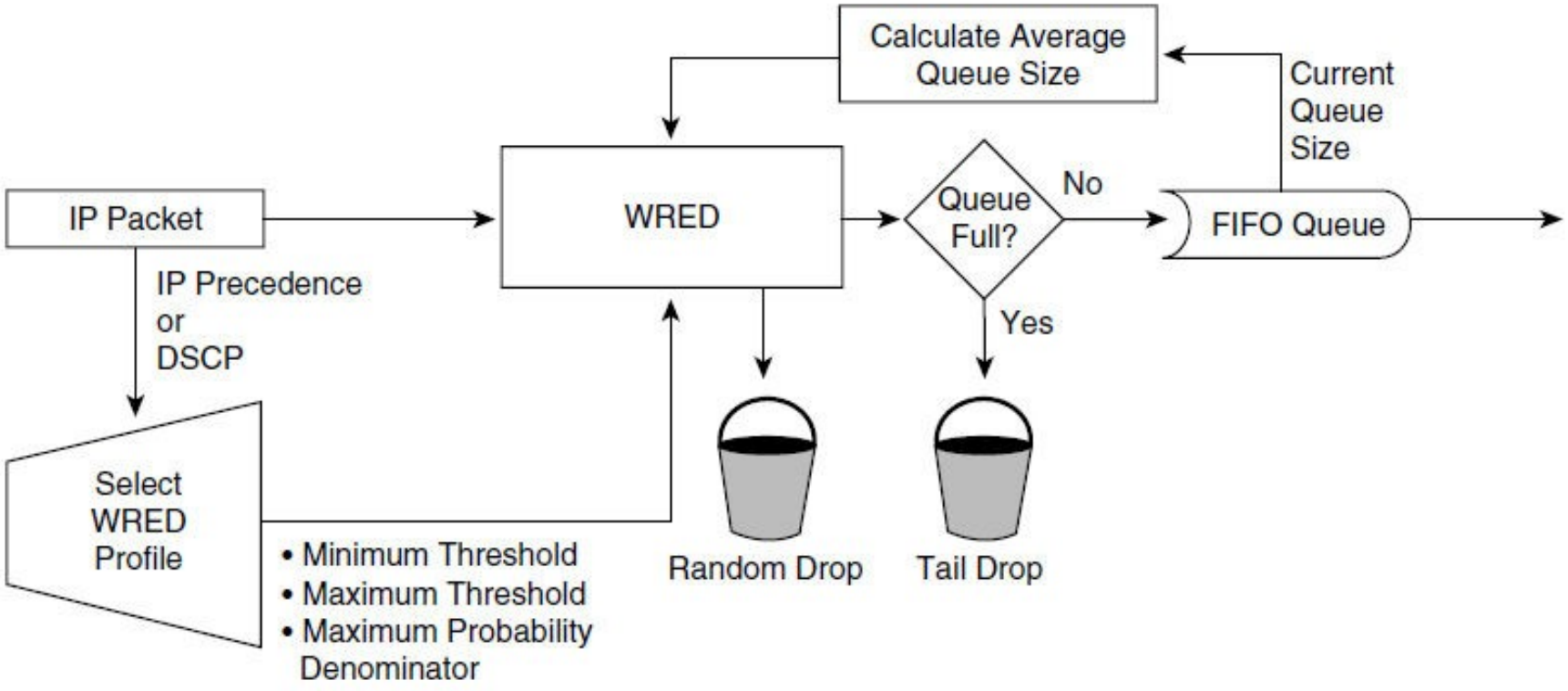


- TCP synchronization prevents average link utilization close to the link bandwidth.
- Tail drops cause TCP sessions to go into slow start.

- Average link utilization is much closer to link bandwidth.
- Random drops from RED cause TCP sessions to reduce window sizes.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Congestion Avoidance – WRED (2)



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

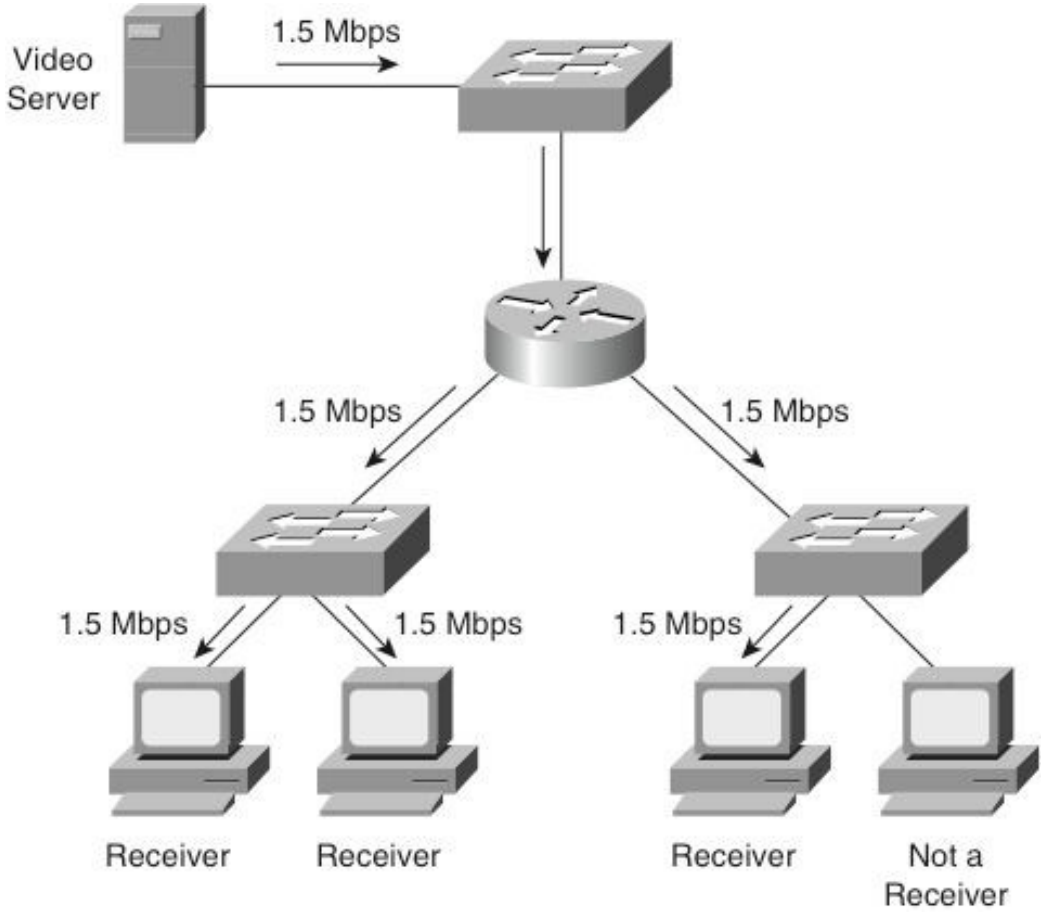
Implementing IP Multicast in the Campus Network



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

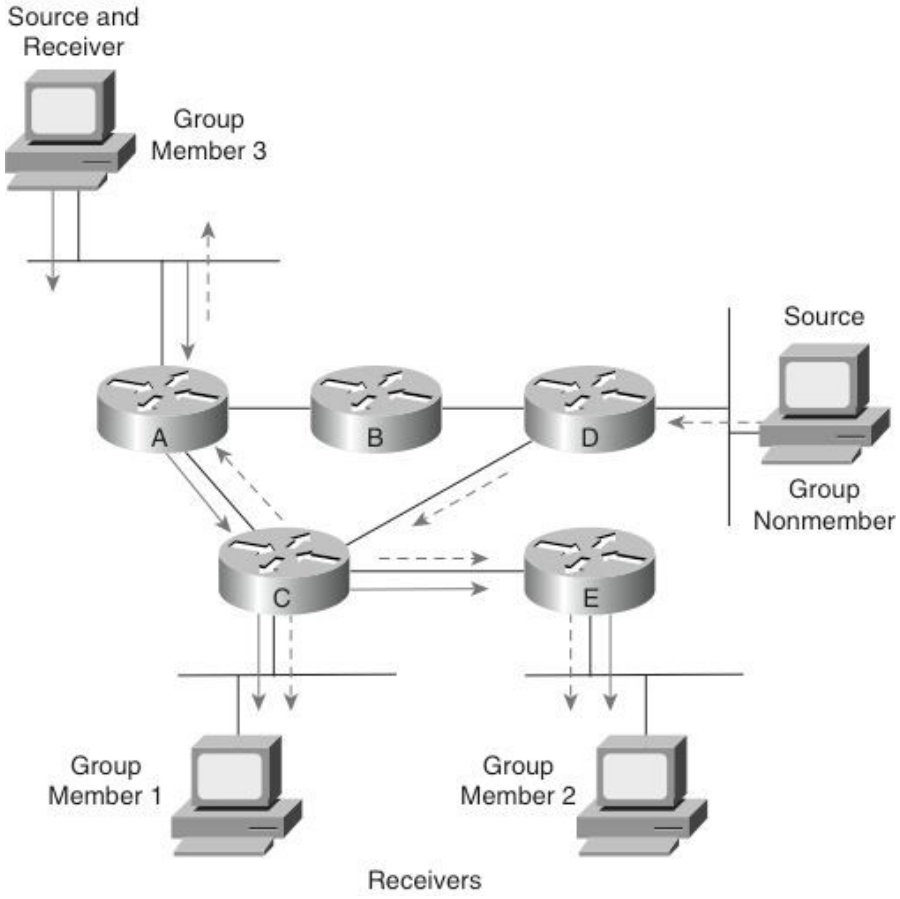
Introduction to IP Multicast

- IP multicast is the transmission of IP data packets to a host group that is defined by a single IP address called a multicast IP address.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Multicast Group Membership

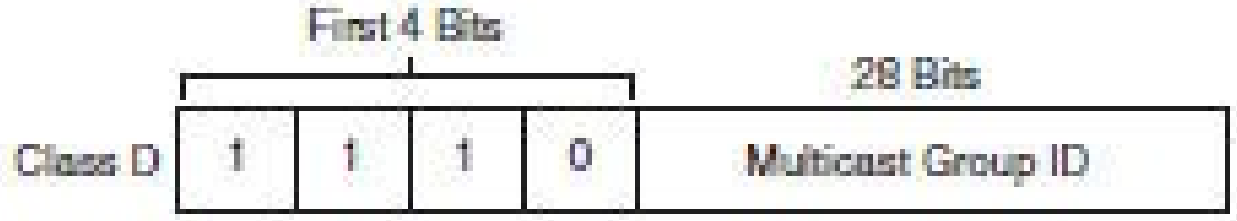


- IP multicast traffic uses UDP as the transport layer protocol.
- To avoid duplication, multicast routing protocols use reverse path forwarding (RPF).

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Multicast IP Address Structure

- IP multicast uses Class D addresses, which range from 224.0.0.0 to 239.255.255.255.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Multicast IP Address Structure

Description	Range
Reserved link local addresses	224.0.0.0 to 224.0.0.255
Globally scoped addresses	224.0.1.0 to 238.255.255.255
Source-specific multicast addresses	232.0.0.0 to 232.255.255.255
GLOP addresses	233.0.0.0 to 233.255.255.255
Limited-scope addresses	239.0.0.0 to 239.255.255.255

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Reserved Link Local Addresses

- 224.0.0.0 to 224.0.0.255
  - Used by network protocols on a local network segment; routers do not forward packets in this address range; sent with a TTL of 1.
  - OSPF uses 224.0.0.5 and 224.0.0.6.
  - RIPv2 uses 224.0.0.9
  - EIGRP uses 224.0.0.10
  - 224.0.0.1: all-hosts group.
  - 224.0.0.2: all-routers group.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Globally Scoped Addresses

- Addresses in the range 224.0.1.0 to 238.255.255.255
  - Companies use these addresses to multicast data between organizations and across the Internet.
  - Multicast applications reserve some of these addresses for use through IANA. For example, IANA reserves the IP address 224.0.1.1 for NTP.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Source-Specific Multicast (SSM) Addresses

- Addresses in the 232.0.0.0 to 232.255.255.255 range
  - SSM is an extension of Protocol Independent Multicast (PIM).
  - Forwarding decisions are based on both group and source addresses, denoted (S,G) and referred to as a channel.
  - Source address makes each channel unique.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

GLOP Addresses

- Specified by RFC 3180.
- 233/8 – reserved for statically defined addresses by organizations that already have an autonomous system number.
- GLOP is not an acronym.
- The autonomous system number of the domain is embedded into the second and third octets of the 233.0.0.0-233.255.255.255 range. For example, the autonomous system 62010 is written in hexadecimal format as F23A. Separating the two octets F2 and 3A results in 242 and 58 in decimal format, respectively. These values result in a subnet of 233.242.58.0/24 that is globally reserved for autonomous system 62010 to use.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

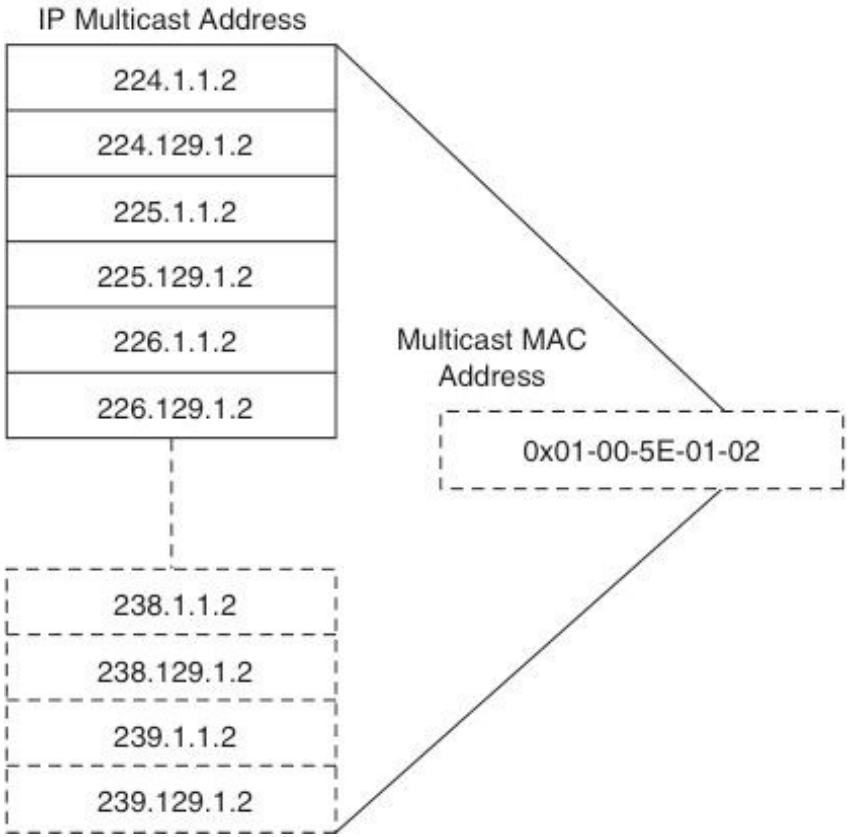
Limited-Scope Addresses

- Addresses in the 239.0.0.0 to 239.255.255.255 range.
- Described in RFC 2365, “Administratively Scoped IP Multicast”.
- Constrained to a local group or organization. Companies, universities, or other organizations use limited-scope addresses to have local multicast applications where edge routers to the Internet do not forward the multicast frames outside their intranet domain.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Multicast MAC Address Structure

- Multicast MAC addresses start with the 25-bit prefix 0x01-00-5E, which in binary is 00000001.00000000.01011110.0xxxxxxx.xxxxxxxx.xxxxxxxx, where x represents a wildcard bit. The 25th bit set to 0.



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Reverse Path Forwarding (RPF)

- The router looks up the source address in the unicast routing table to determine whether it arrived on the interface that is on the reverse path (lowest-cost path) back to the source.
- If the packet has arrived on the interface leading back to the source, the RPF check is successful, and the router replicates and forwards the packet to the outgoing interfaces.
- If the RPF check in the previous step fails, the router drops the packet and records the drop as an RPF failed drop.

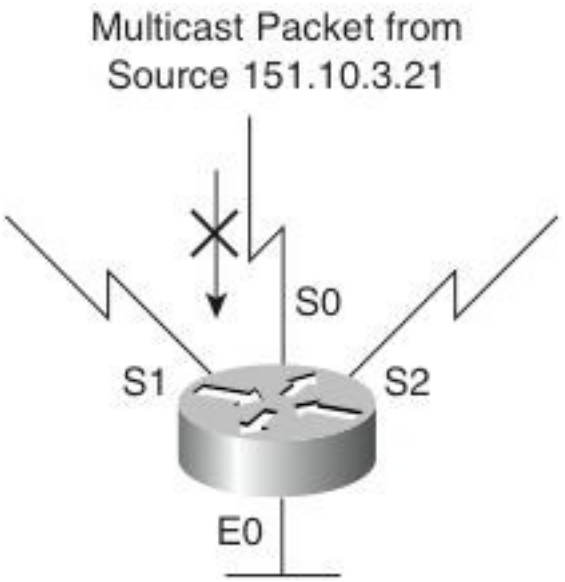
© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

RPF Example

RPF Check Fails!

Multicast Route Table	
Network	Interface
151.10.0.0/16	S1
198.14.32.0/24	S0
204.1.16.0/24	E0

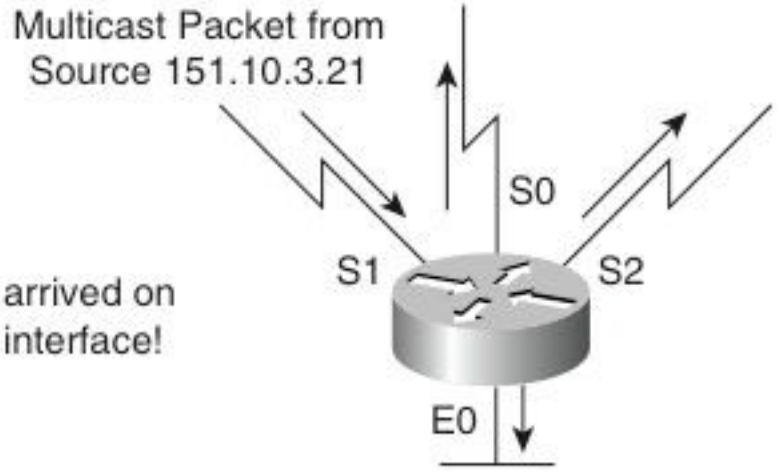
Packet arrived on wrong interface! Discard packet.



RPF Check Succeeds!

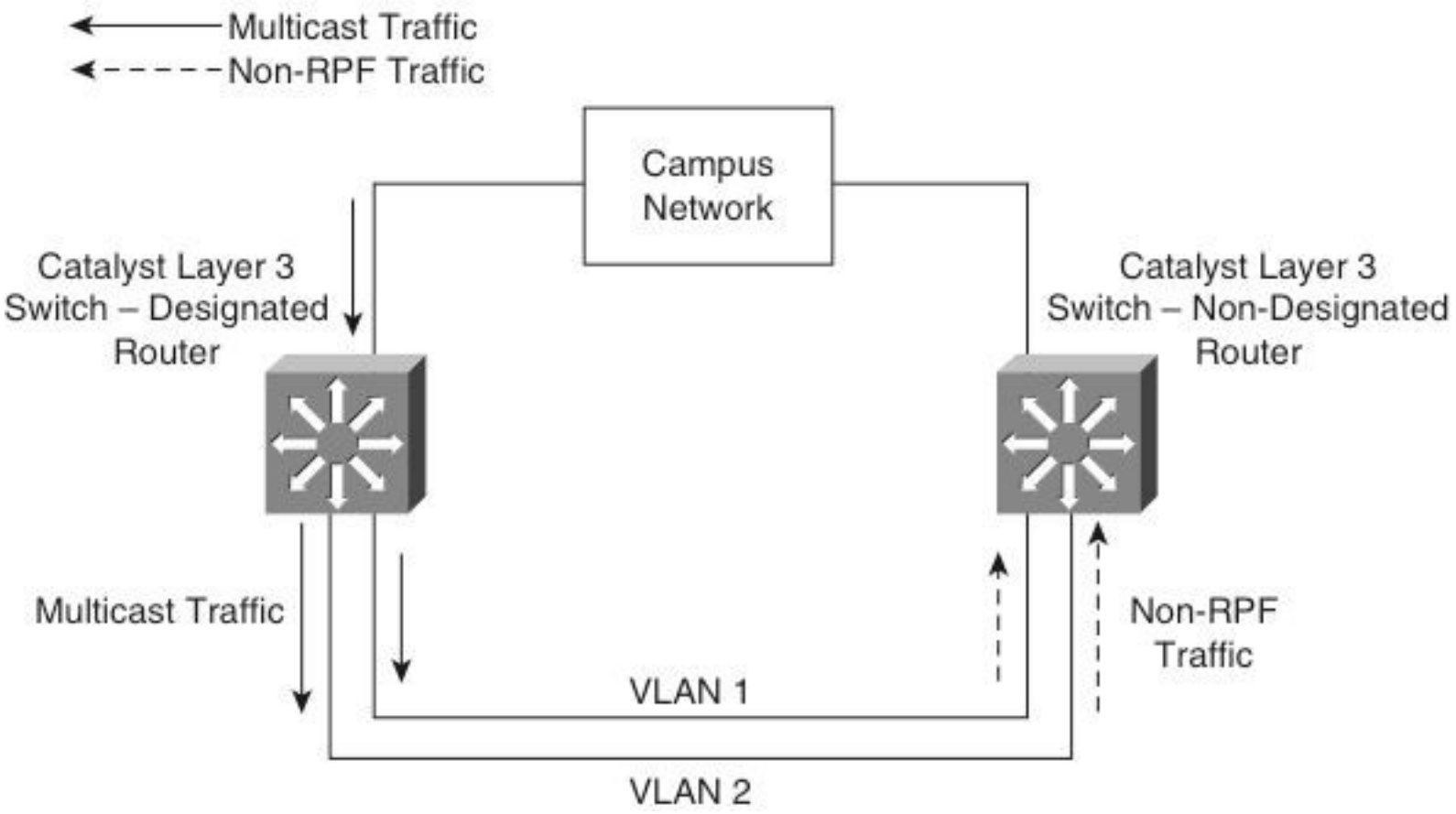
Multicast Route Table	
Network	Interface
151.10.0.0/16	S1
198.14.32.0/24	S0
204.1.16.0/24	E0

Packet arrived on correct interface!



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Non-RPF Multicast Traffic



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

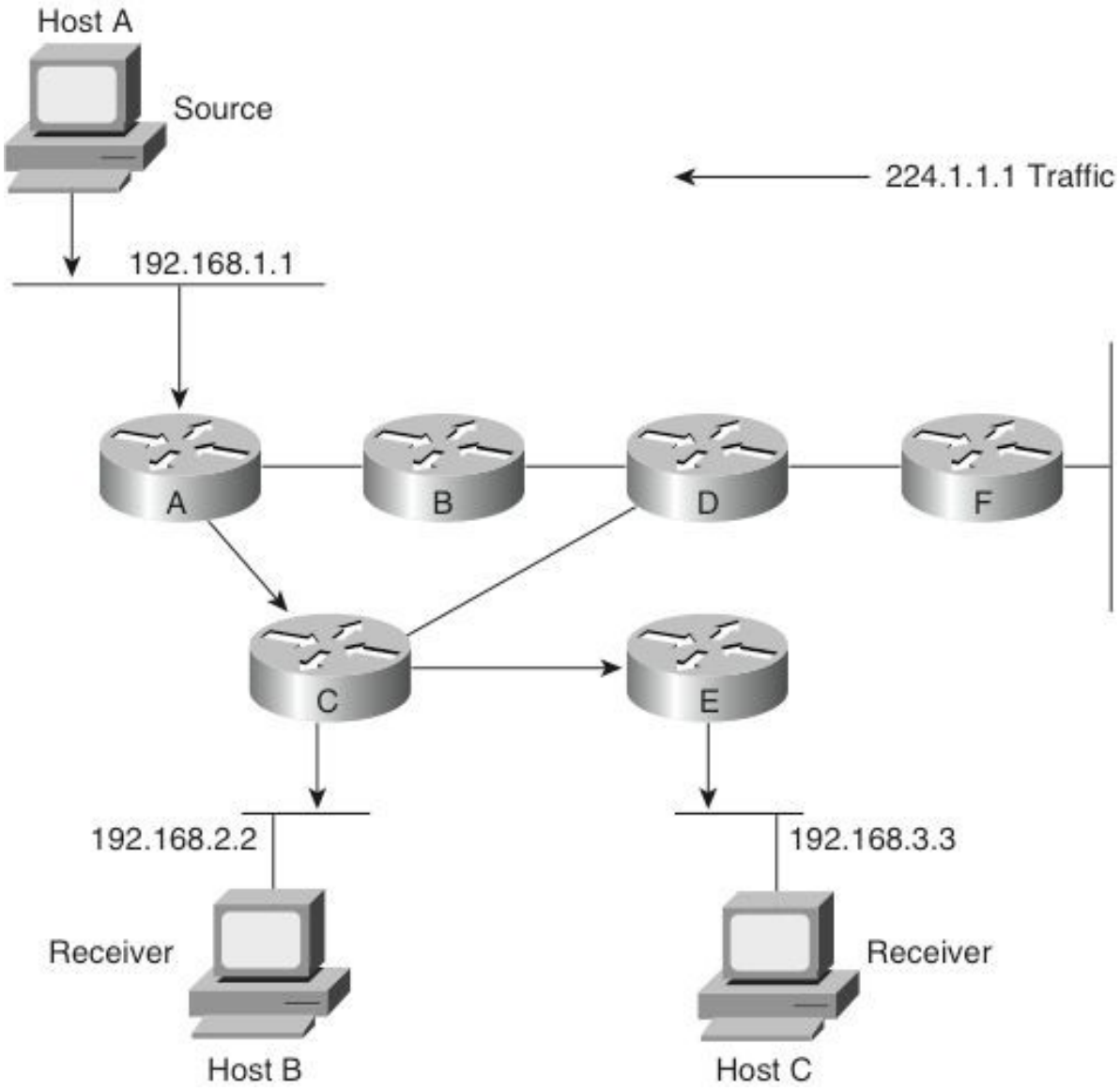


Multicast Forwarding Trees

- Multicast-capable routers create multicast distribution trees that control the path that IP multicast traffic takes through the network to deliver traffic to all receivers.
- The two types of distribution trees are:
  - Source trees
  - Shared trees

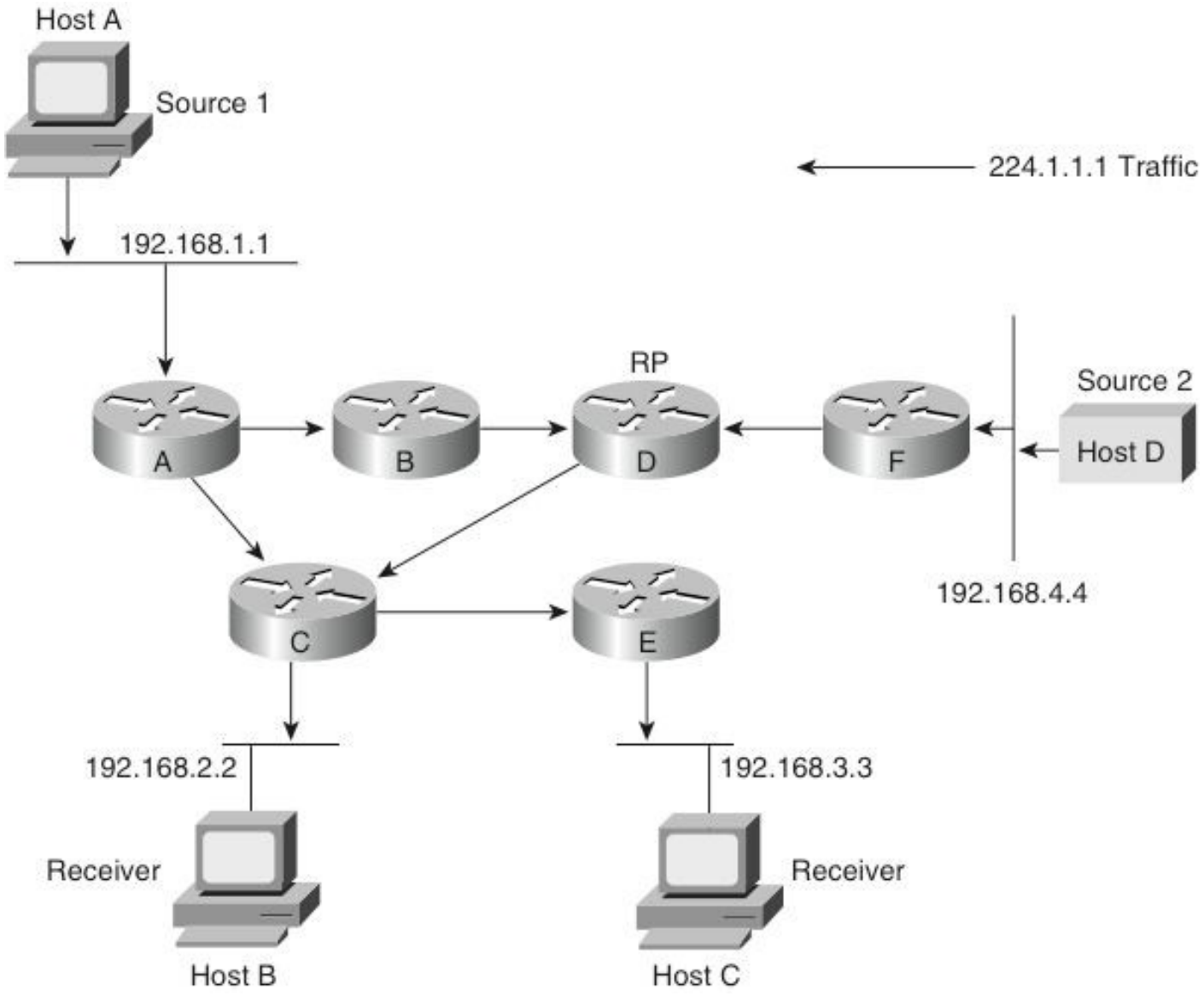
© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Source Trees



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

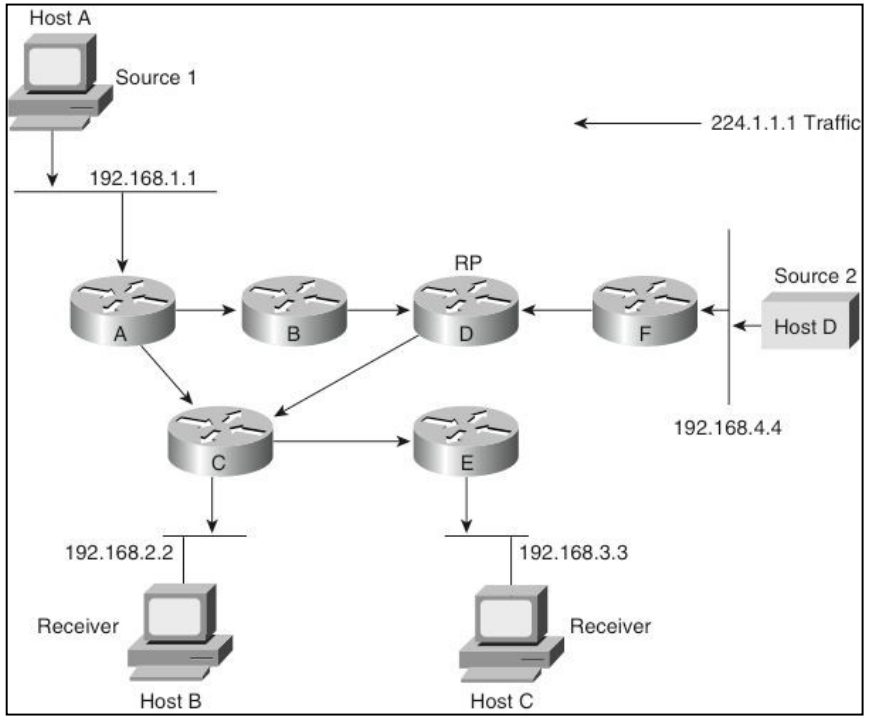
Shared Trees



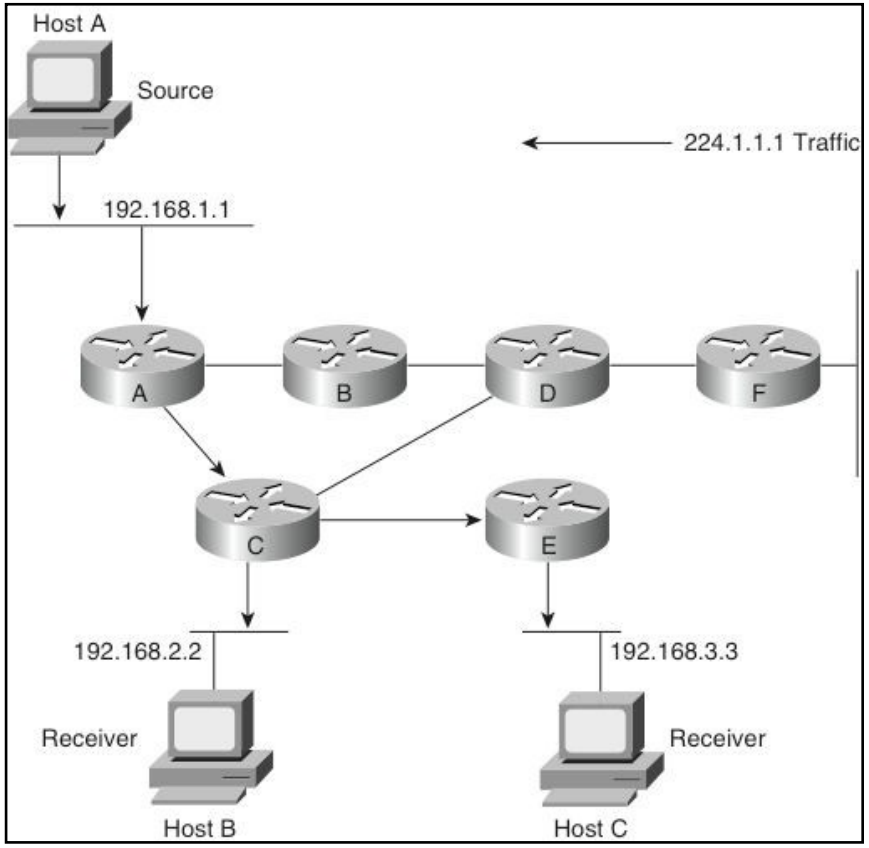
© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Comparing Source Trees and Shared Trees

Shared Tree



Source Tree



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



IP Multicast Protocols

- IP multicast uses its own routing, management, and Layer 2 protocols.
- Two important multicast protocols:
  - Protocol Independent Multicast (PIM)
  - Internet Group Management Protocol (IGMP)

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

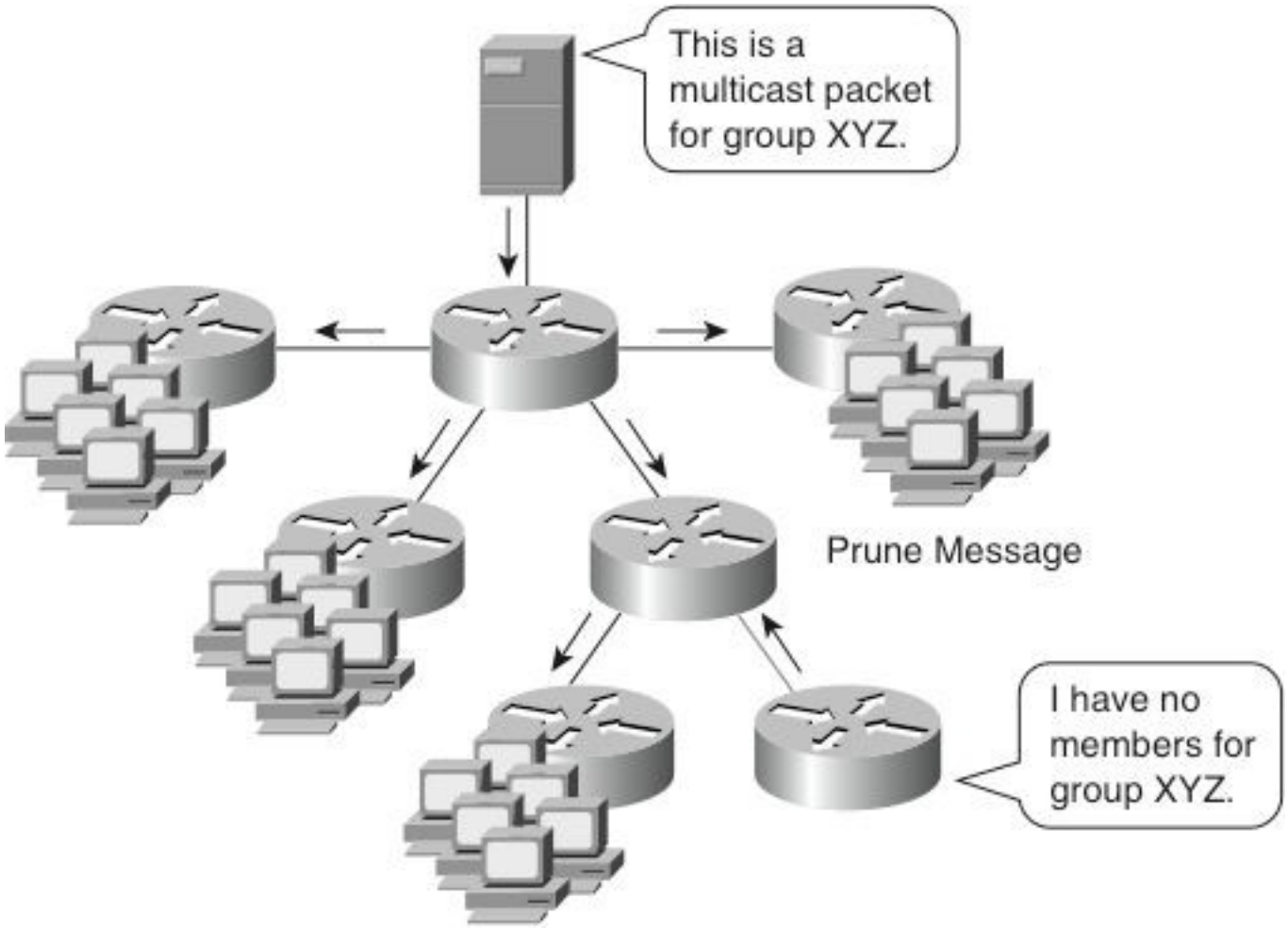


Protocol Independent Multicast (PIM)

- PIM has two versions: 1 and 2.
- PIM has four modes of operation:
  - PIM dense mode
  - PIM sparse mode
  - PIM sparse-dense mode
  - PIM bidirectional

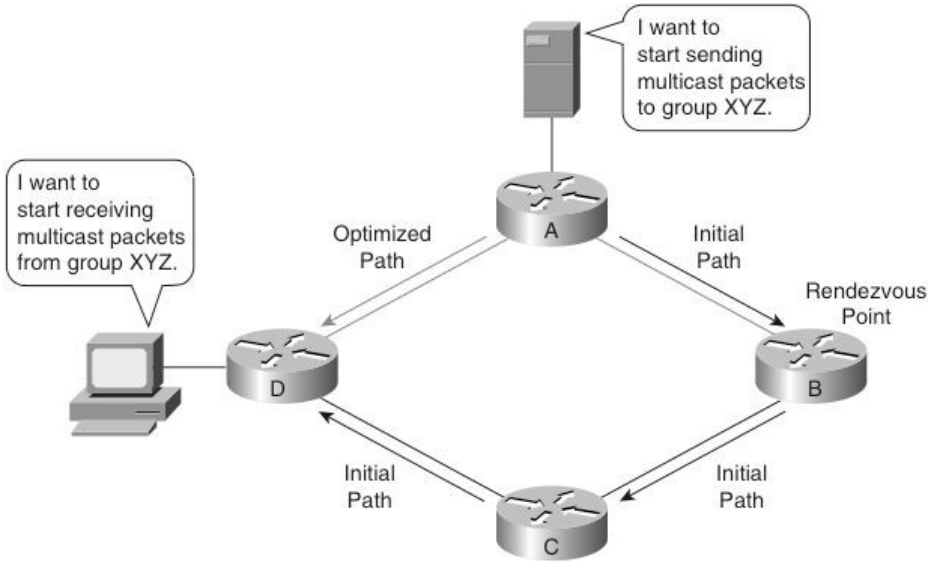
© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

PIM Dense Mode (PIM-DM) - Obsolete



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

PIM Sparse Mode (PIM-SM)



- PIM-SM is optimized for environments where there are many multipoint data streams.
- When planning for multicast deployments in the campus network, choose PIM-SM with IP under the following scenarios:
  - There are many multipoint data streams.
  - At any given moment, there are few receivers in a group.
  - The type of traffic is intermittent or busty.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



PIM Sparse-Dense Mode

- Enables individual groups to use either sparse or dense mode depending on whether RP information is available for that group.
- If the router learns RP information for a particular group, sparse mode is used.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

PIM Bidirectional (Bidir-PIM)

- Extension of PIM-SM.
- Suited for multicast networks with a large number of sources.
- Can forward source traffic toward RP upstream on shared tree without registering sources (as in PIM-SM).
- Introduces mechanism called designated forwarder (DF).

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

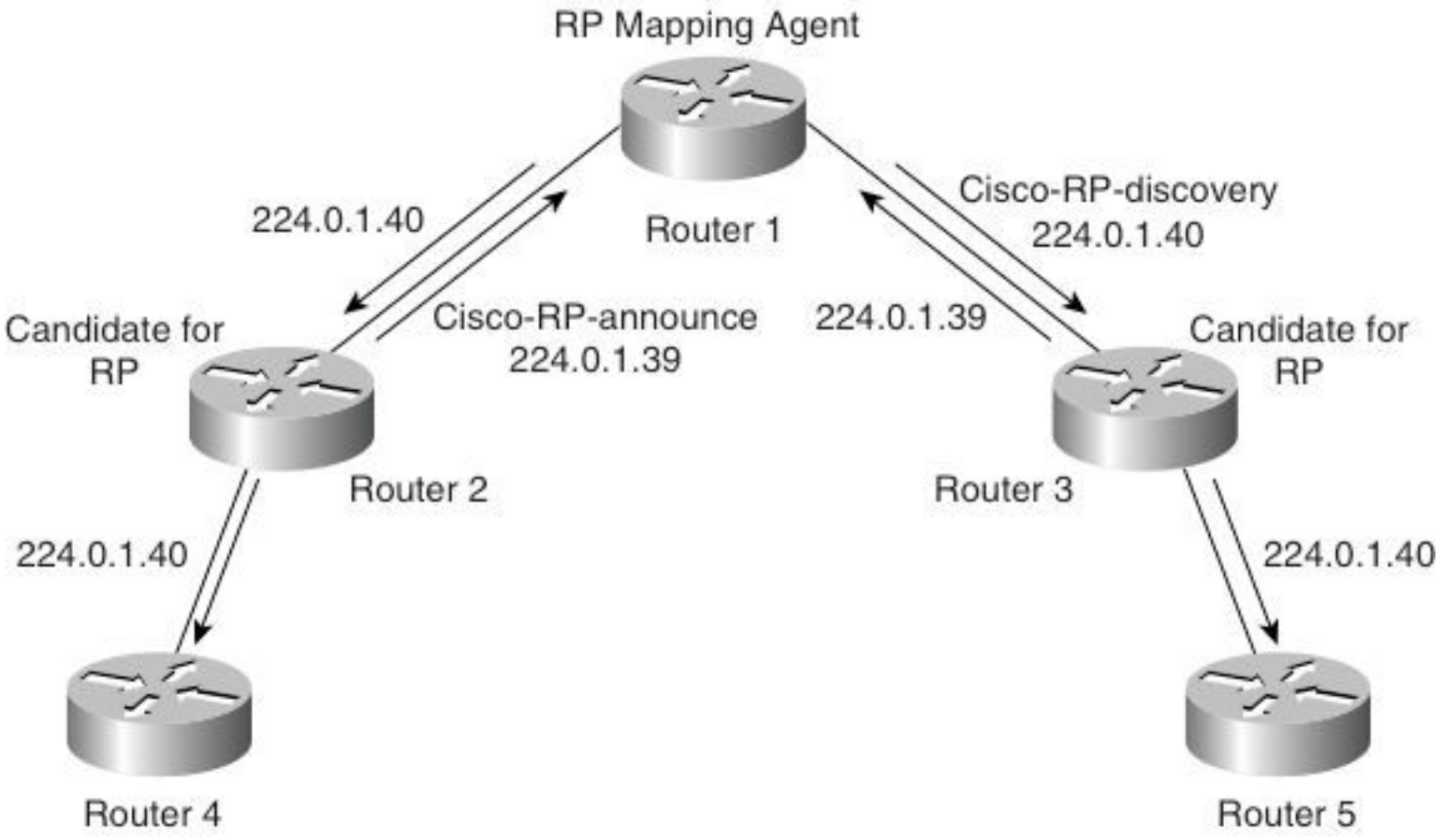


Automating Distribution of RP

- Auto-RP
- Bootstrap router (BSR)
- Multicast Source Discovery Protocol (MSDP)-Anycast-RP

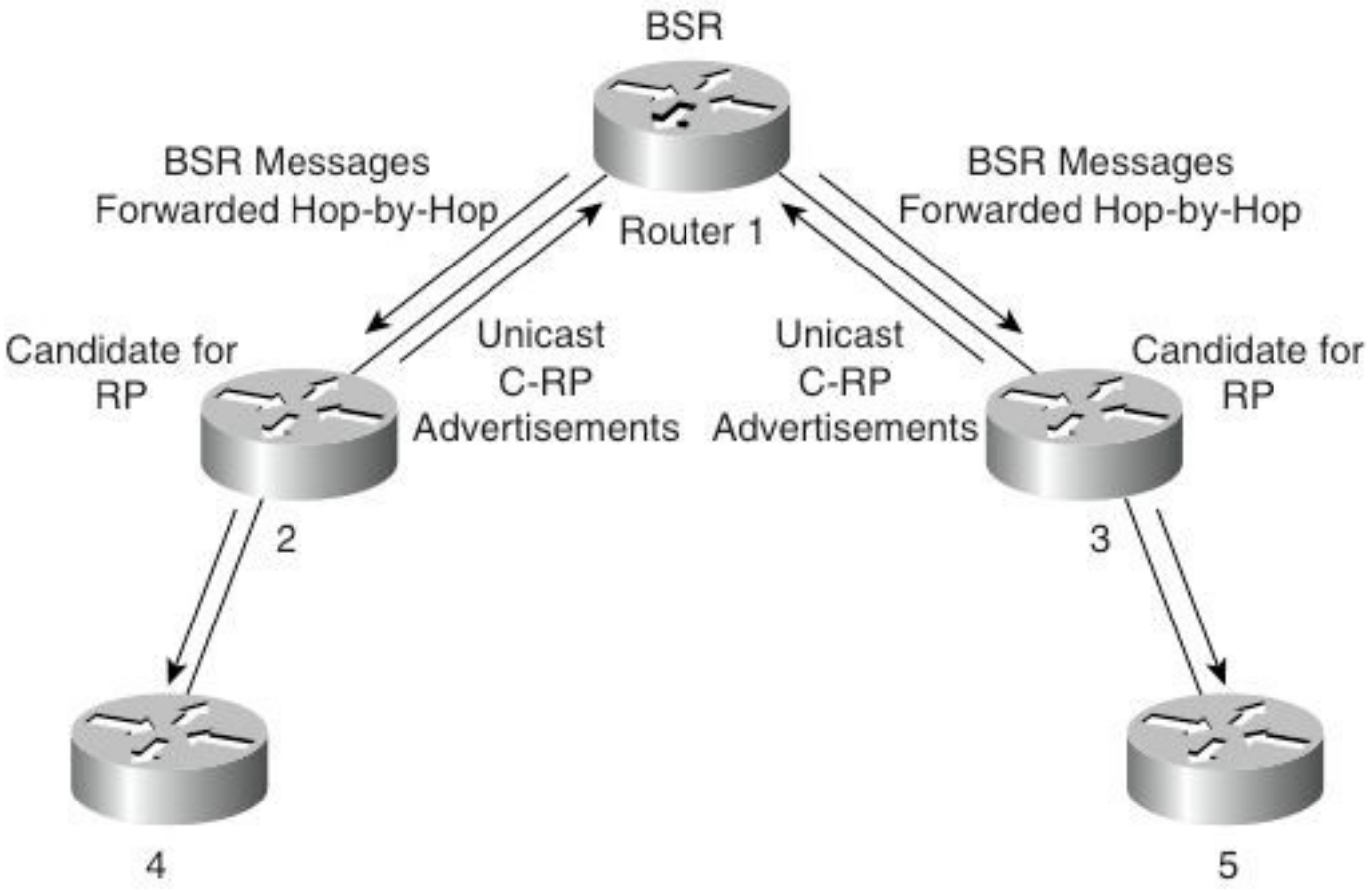
© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Auto-RP



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Bootstrap Router



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Comparison and Compatibility of PIM Version 1 and PIM Version 2

- PIM version 2 IETF standard.
- Cisco-recommended version.
- Interoperates with PIM-v1 and PIM-v2 routers.
- BSR RP-distribution mechanism in PIM-v2 specifications, but can also use Auto-RP.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Internet Group Management Protocol (IGMP)

- IGMP Versions:
  - IGMP version 1 (IGMPv1) RFC 1112
  - IGMP version 2 (IGMPv2) RFC 2236
  - IGMP version 3 (IGMPv3) RFC 3376
  - IGMP version 3 lite (IGMPv3 lite)

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

IGMPv1

- IGMP host membership query messages sent periodically to determine which multicast groups have members on the router's directly attached LAN's.
- IGMP query messages are addressed to the all-host group (224.0.0.1) and have an IP TTL equal to 1.
- When the end station receives an IGMP query message, the end station responds with a host membership report for each group to which the end station belongs.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

IGMPv2

- Types of IGMPv2 messages:
  - Membership query
  - Version 2 membership report
  - Leave report
  - Version 1 membership report
- The group-specific query message enables a router to transmit a specific query to one particular group. IGMPv2 also defines a leave group message for the hosts, which results in lower leave latency.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

IGMPv3

- Enables a multicast receiver to signal to a router the groups from which it wants to receive multicast traffic and from which sources to expect traffic.
- IGMPv3 messages:
  - Version 3 membership query
  - Version 3 membership report
- Receivers signal membership to a multicast host group in INCLUDE mode or EXCLUDE mode.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

IGMPv3 Lite

- Cisco-proprietary transitional solution toward SSM.
- Supports SSM applications when hosts do not support IGMPv3.
- Requires Host Side IGMP Library (HSIL).

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



IGMP Snooping

- IP multicast constraining mechanism.
- Dynamically configures L2 ports to forward multicast traffic only to those ports with hosts wanting to receive it.
- Operates on multilayer switches.
- Examines IGMP join and leave messages.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Configuring IGMP Snooping (1)

- **Step 1.** Enable IGMP snooping globally. (By default, it is enabled globally.)

  ```
  Switch(config)# ip igmp snooping
  ```

- **Step 2.** (Optional.) Switches add multicast router ports to the forwarding table for every Layer 2 multicast entry. The switch learns of such ports through snooping IGMP queries, flowing PIM and DVMRP packets, or interpreting CGMP packets from other routers. Configure the IGMP snooping method. The default is PIM.

  ```
  Switch(config)# ip igmp snooping vlan vlan-id mrouter learn
  [cgmp | pim-dvmrp]
  ```

- **Step 3.** (Optional.) If needed, configure the router port statically. By default, IGMP snooping automatically detects the router ports.

  ```
  Switch(config)# ip igmp snooping vlan vlan-id mrouter
  interface interface-num
  ```


© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Configuring IGMP Snooping (2)

- **Step 4.** (Optional.) Configure IGMP fast leave if required.

  `Switch(config)# ip igmp snooping vlan vlan-id fast-leave`

  `Switch(config)# ip igmp snooping vlan vlan-id immediate-leave`

- **Step 5.** (Optional.) By default, all hosts register and add the MAC address and port to the forwarding table automatically. If required, configure a host statically on an interface. Generally, static configurations are necessary when troubleshooting or working around IGMP problems.

  `Switch(config)# ip igmp snooping vlan vlan-id static mac-address interface interface-id`

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Configuring IP Multicast (1)

- **Step 1.** Enable multicast routing on Layer 3 globally.

  ```
  Switch(config)# ip multicast-routing
  ```

- **Step 2.** Enable PIM on the interface that requires multicast.

  ```
  Switch(config-if)# ip pim [dense-mode | sparse-mode | sparse-dense-mode]
  ```

- **Step 3.** (Optional.) Configure RP if you are running PIM sparse mode or PIM sparse-dense mode. The Cisco IOS Software can be configured so that packets for a single multicast group can use one or more RPs. It is important to configure the RP address on all routers (including the RP router). To configure the address of the RP, enter the following command in global configuration mode:

  ```
  Switch(config)# ip pim rp-address ip-address [access-list-number] [override]
  ```


© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Configuring IP Multicast (2)

- **Step 4.** (Optional.) To designate a router as the candidate RP for all multicast groups or for a particular multicast group by using an access list, enter the following command in global configuration mode:

  Switch(config)# **ip pim send-rp-announce** *interface-type interface-number* **scope** *ttl* **[group-list** *access-list-number***] [interval** *seconds***]**

  - The TTL value defines the multicast boundaries by limiting the number of hops that the RP announcements can take.
- **Step 5**. (Optional.) To assign the role of RP mapping agent on the router configured in Step 4 for AutoRP, enter the following command in global configuration mode:

  Switch(config)# **ip pim send-rp-discovery scope** *ttl*

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Configuring IP Multicast (3)

- **Step 6.** (Optional.) All systems using Cisco IOS Release 11.3(2)T or later start in PIM version 2 mode by default. In case you need to re-enable PIM version 2 or specify PIM version 1 for some reason, use the following command:

```
Switch(config-if)# ip pim version [1 | 2]
```

- **Step 7.** (Optional.) Configure a BSR border router for the PIM domain so that bootstrap messages do not cross this border in either direction. This ensures that different BSRs will be elected on the two sides of the PIM border. Configure this command on an interface such that no PIM version 2 BSR messages will be sent or received through the interface.

```
Switch(config-if)# ip pim bsr-border
```


© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Configuring IP Multicast (4)

- **Step 8.** (Optional.) To configure an interface as a BSR candidate, issue the following command:

  `Switch(config)# ip pim bsr-candidate` *`interface-type hash-mask-length`* **[***`priority`***]**

  - The *`hash-mask-length`* is a 32-bit mask for the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. Priority is configured as a number from 0 to 255. The BSR with the largest priority is preferred. If the priority values are the same, the device with the highest IP address is selected as the BSR. The default is 0.
- **Step 9.** (Optional.) To configure an interface as an RP candidate for BSR router for particular multicast groups, issue the following command:

  `Switch(config)# ip pim rp-candidate` *`interface-type interface-number`* **`ttl`** *`group-list access-list`*

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Sparse Mode Configuration Example

- PIM-SM in Cisco IOS with RP at 10.20.1.254

```
Router# conf t
Router(config)# ip multicast-routing
Router(config)# interface vlan 1
Router(config-if)# ip pim sparse-mode
Router(config-if)# interface vlan 3
Router(config-if)# ip pim sparse-mode
Router(config-if)# exit
Router(config)# ip pim rp-address 10.20.1.254
```


© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Sparse-Dense Mode Configuration Example

- PIM sparse-dense mode with a candidate BSR

```
Router(config)# ip multicast-routing
Router(config)# interface vlan 1
Router(config-if)# ip pim sparse-dense-mode
Router(config-if)# exit
Router(config)# ip pim bsr-candidate vlan 1 30 200
```


© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Auto-RP Configuration Example

- Auto-RP advertising IP address of VLAN 1 as RP

```
Router(config)# ip multicast-routing
Router(config)# interface vlan 1
Router(config-if)# ip pim sparse-dense-mode
Router(config-if)# exit
Router(config)# ip pim send-rp-announce vlan 1 scope 15 group-list 1
Router(config)# access-list 1 permit 225.25.25.0.0.0.0.255
Router(config)# exit
```


© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Preparing the Campus Infrastructure to Support Wireless



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

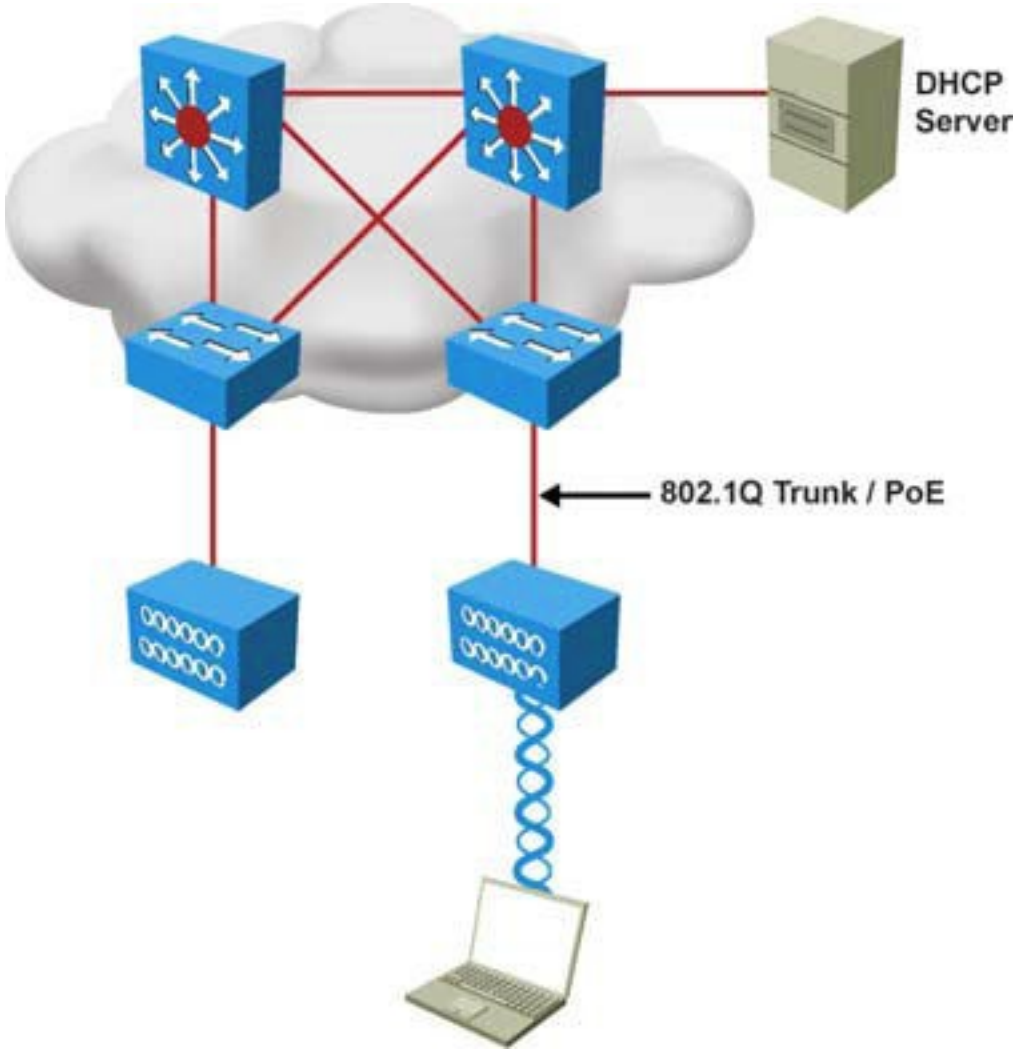


Wireless LAN Parameters

- Range
- Interference
- Performance
- Security

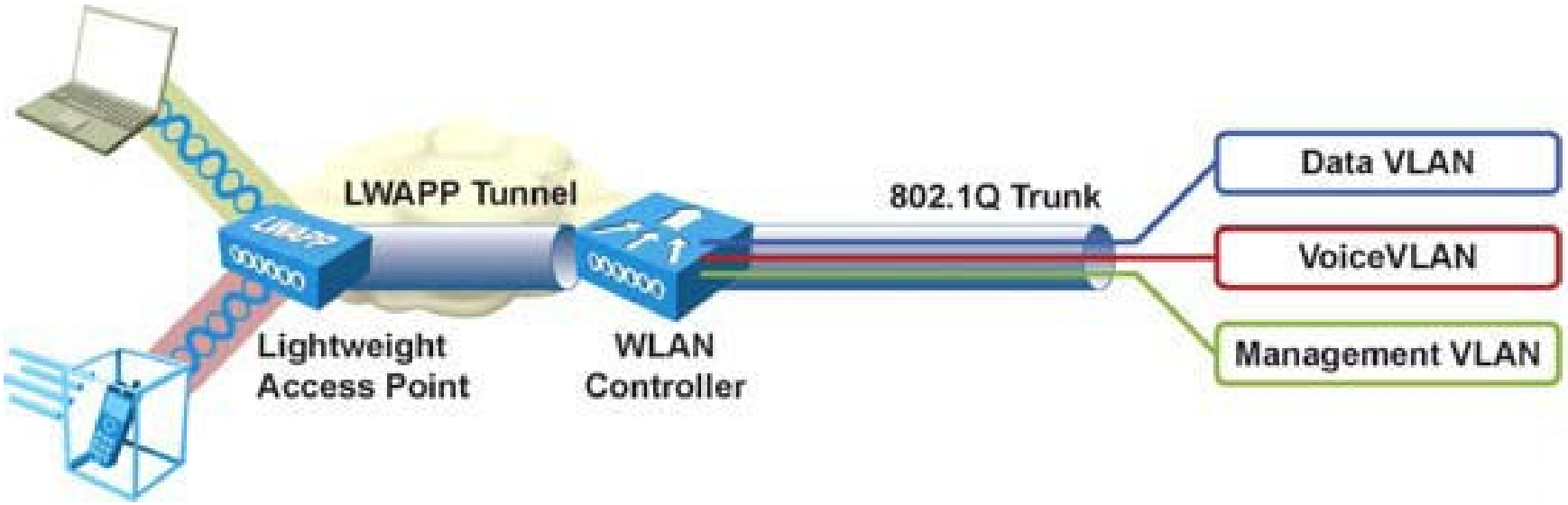
© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Preparing the Campus Network for Integration of a Standalone WLAN Solution



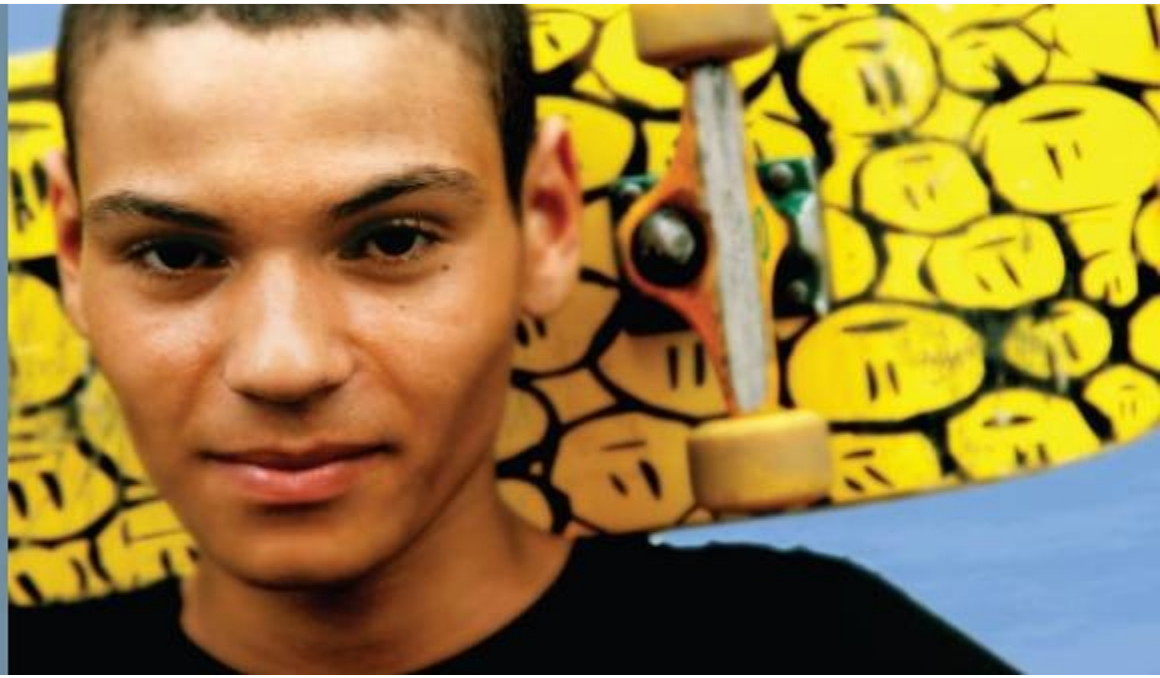
© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Preparing the Campus Network for Integration of a Controller-Based WLAN Solution



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Preparing the Campus Infrastructure to Support Voice



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

IP Telephony Components

- IP phones
- Switches with inline power
- Call-processing manager
- Voice gateway

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Configuring Switches to Support VoIP

- Voice VLAN’s
- QoS
- Power over Ethernet (PoE)

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Voice VLAN's



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Configuring Voice VLAN's

- **Step 1**. Ensure that QoS is globally enabled with the command **mls qos** and enter the configuration mode for the interface on which you want to configure Voice VLANs.
- **Step 2.** Enable the voice VLAN on the switch port and associate a VLAN ID using the interface command **switchport voice vlan** *vlan-id*.
- **Step 3.** Configure the port to trust CoS or trust DSCP as frames arrive on the switch port using the **mls qos trust cos** or **mls qos trust dscp** commands, respectively. Recall that the **mls qos trust cos** command directs the switch to trust ingress CoS values whereas **mls qos trust dscp** trusts ingress DSCP values. Do not confuse the two commands as each configures the switch to look at different bits in the frame for classification.
- **Step 4.** Verify the voice VLAN configuration using the command **show interfaces** *interface-id* **switchpor**t.
- **Step 5.** Verify the QoS interface configuration using the command **show mls qos interface** *interface-id*.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Voice VLAN Configuration Example

- Interface FastEthernet0/24 is configured to set data devices to VLAN 1 by default and VoIP devices to the voice VLAN 700.
- The switch uses CDP to inform an attached IP Phone of the VLAN. As the port leads to an end device, portfast is enabled.

```
<output omitted>
!
mls qos
!
<output omitted>
!
interface FastEthernet0/24
switchport mode dynamic desirable
switchport voice vlan 700
mls qos trust cos
power inline auto
spanning-tree portfast
!
<output omitted>
```


© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



QoS for Voice Traffic from IP Phones

- Define trust boundaries.
- Use CoS or DSCP at trust boundary.

```
<output omitted>
!
mls qos
!
<output omitted>
!
interface FastEthernet0/24
switchport mode dynamic desirable
switchport voice vlan 700
mls qos trust cos
power inline auto
spanning-tree portfast
!
<output omitted>
```


© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Power over Ethernet

- Power comes through Category 5e Ethernet cable.
- Power provided by switch or power injector.
- Either IEEE 802.3af or Cisco inline power. New Cisco devices support both.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Inline Power Configuration Example

- The command **show power inline** displays the configuration and statistics about the used power drawn by connected powered devices and the capacity of the power supply.

```
Switch# show power inline fa0/24
Interface Admin  Oper       Power   Device              Class  Max
                            (Watts)
--------- ------ ---------- ------- ------------------- -----  ----
Fa0/24    auto   on         10.3 IP Phone CP-7970G      3      15.4


Interface  AdminPowerMax    AdminConsumption
             (Watts)            (Watts)
---------- -------------- ------------------
Fa0/24         15.4               15.4
```


© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Additional Network Requirements for VoIP

- Cisco IP phone receives IP address and downloads configuration file via TFTP from Cisco Unified Communications Manager (CUCM) or CUCM Express (CUCME).
- IP phone registers with CUCM or CUCME and obtains its line extension number.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Preparing the Campus Infrastructure to Support Video



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Video Applications

- Peer-to-peer video
- TelePresence
- IP surveillance
- Digital media systems

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Configuring Switches to Support Video

- Packet loss of less than 0.5 percent
- Jitter of less than 10 ms one-way
- Latency of less than 150 ms one-way

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Best Practices for TelePresence

- Classify and mark traffic by using DSCP as close to its edge as possible, preferably on the first-hop access layer switch. If a host is trusted, allow the trusted hosts to mark their own traffic.
- Trust QoS on each inter-switch and switch-to-router links to preserve marking as frames travel through the network. See RFC 4594 for more information.
- Limit the amount of real-time voice and video traffic to 33 percent of link capacity; if higher than this, TelePresence data might starve out other applications resulting in slow or erratic performance of data applications.
- Reserve at least 25 percent of link bandwidth for the best-effort data traffic.
- Deploy a 1 percent Scavenger class to help ensure that unruly applications do not dominate the best-effort data class.
- Use DSCP-based WRED queuing on all TCP flows, wherever possible.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Chapter 7 Summary (1)

- When planning for a wireless deployment, carefully consider the standalone WLAN solution and the controller-based solution. For networks of more than a few access points, the best practice is to use a controller-based solution.
- When preparing for a wireless deployment, verify your switch port configuration as a trunk port. Access points optionally support trunking and carry multiple VLAN’s. Wireless clients can map to different SSID’s, which it turn might be carried on different VLAN’s.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Chapter 7 Summary (2)

- When planning for a voice implementation in the campus network, the use of QoS and the use of a separate VLAN for voice traffic is recommended. PoE is another option to power Cisco IP Phones without the use of an AC/DC adapter.
- When preparing for the voice implementation, ensure that you configure QoS as close to the edge port as possible. Trusting DSCP or CoS for ingress frames is normally recommended.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Chapter 7 Summary (3)

- When planning for a video implementation, determine whether the video application is real-time video or on-demand video. Real-time video requires low latency and sends traffic in bursts at high bandwidth.
- When preparing for a video implementation such as TelePresence, consult with a specialist or expert to ensure the campus network meets all the requirements in terms of bandwidth and QoS.

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



Chapter 7 Labs

- **Lab 7-1 Configuring Switches for IP Telephony Support**
- **Lab 7-2 Configuring a WLAN Controller**
- **Lab 7-3 Voice and Security in a Switched Network - Case Study**

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public

Resources

- Catalyst 3560 Command Reference:

  www.cisco.com/en/US/partner/docs/switches/lan/catalyst3560/software/release/12.2_55_se/command/reference/3560_cr.html

- Configuring QoS:

  www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_55_se/configuration/guide/swqos.html

- Configuring IP Multicast:

  www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_55_se/configuration/guide/swqos.html

- Configuring IGMP Snooping:

  www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_55_se/configuration/guide/swigmp.html

© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public



© 2007 – 2010, Cisco Systems, Inc. All rights reserved. Cisco Public