Troubleshooting Converged Networks

CCNP TSHOOT: Maintaining and Troubleshooting IP Networks

Chapter 8 Objectives

- Troubleshoot Wireless issues in a converged network supporting wireless devices and clients.
- Troubleshoot network issues in a converged network supporting Unified Communications.
- Troubleshoot network issues in a converged network supporting video.

Troubleshooting Wireless Issues in a Converged Network

Section Overview

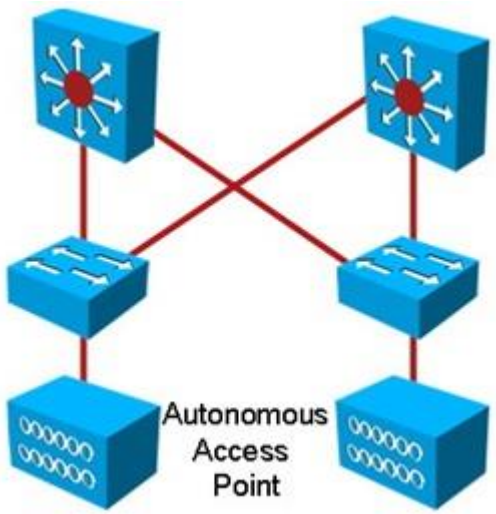
- The focus of this section is on the readiness of the wired network to support wireless deployments and the impact of wireless traffic and services on the rest of the network.
- This includes network services such as:
  - Power over Ethernet (PoE)
  - Dynamic Host Configuration Protocol (DHCP)
  - Quality of service (QoS)
  - Security
- The Cisco Unified Wireless Network is composed of five interconnected element:
  - Client devices
  - Access points
  - Network unification
  - World-class network management
  - Mobility services

Common Wireless Integration Issues

- Designing (and troubleshooting) a wireless network that integrates into a campus network requires several factors to be considered:
  - Is the wireless network based on the autonomous model or will it be based on its counterpart, the split MAC model (using lightweight access points and wireless controllers)?
  - What are the switch capabilities and requirements in terms of PoE, trunking, wireless local-area network (WLAN)-to-VLAN mapping, security, and QoS?
  - How will the Lightweight Access Point Protocol (LWAPP) be handled?
  - What type of roaming will the network support?

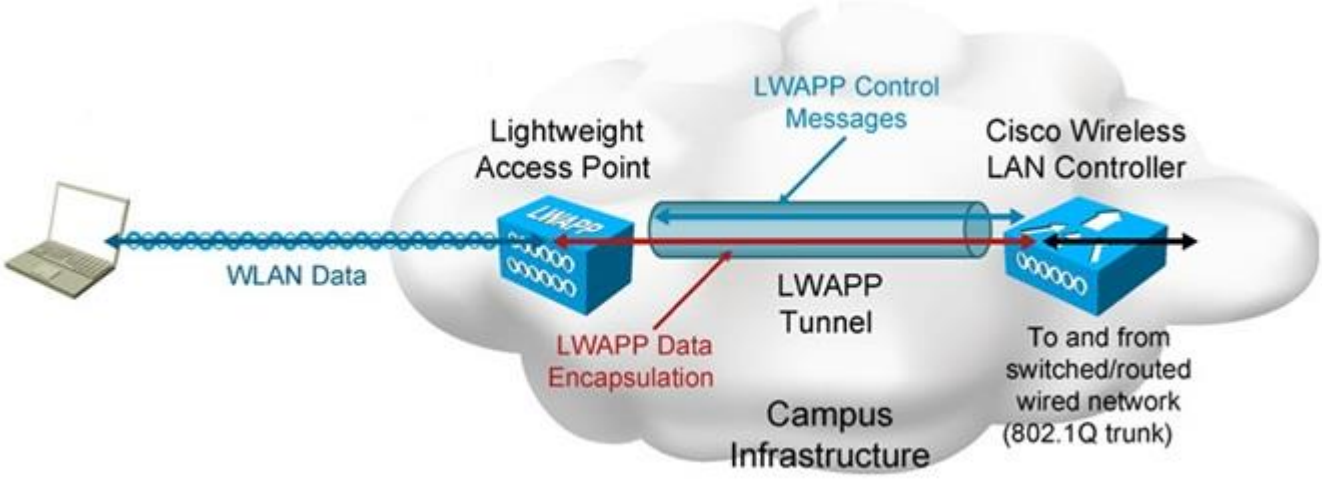
Standalone Wireless Solution

- Autonomous access points (APs) provide all the wireless services.
- Deployment is based on those APs functioning as critical wireless devices.
- Other network devices provide services such as PoE, security and QoS.
- Network servers, such as the Cisco Secure Access Control Server (ACS), are used for security and implement protocols such as RADIUS and TACACS+.



Split MAC or Lightweight Solution

- The controller-based architecture splits the processing of the IEEE 802.11 protocol between two devices: The AP and a centralized Cisco wireless LAN controller (WLC).
- The processing of the 802.11 data and management protocols and the AP functionality is also divided between the two devices.
- This approach is called *split MAC* or *lightweight*.
- Communications between the devices (lightweight APs and the WLCs) are implemented through LWAPP tunnels.



Wireless Integration Issues – Cont.

- The model used defines where and how to troubleshoot potential problems when integrating the wireless infrastructure into a campus LAN.
- The location of power source equipment, the configuration of trunks, and the mapping between WLANs and VLANs are important in gathering information for troubleshooting.
- The wireless security solution is important in the proper transport of protocols such as LWAPP across the wired network.
- Firewalls and access control lists (ACLs) must allow the protocol between APs and Cisco WLCs.

Wireless Integration Issues – Cont.

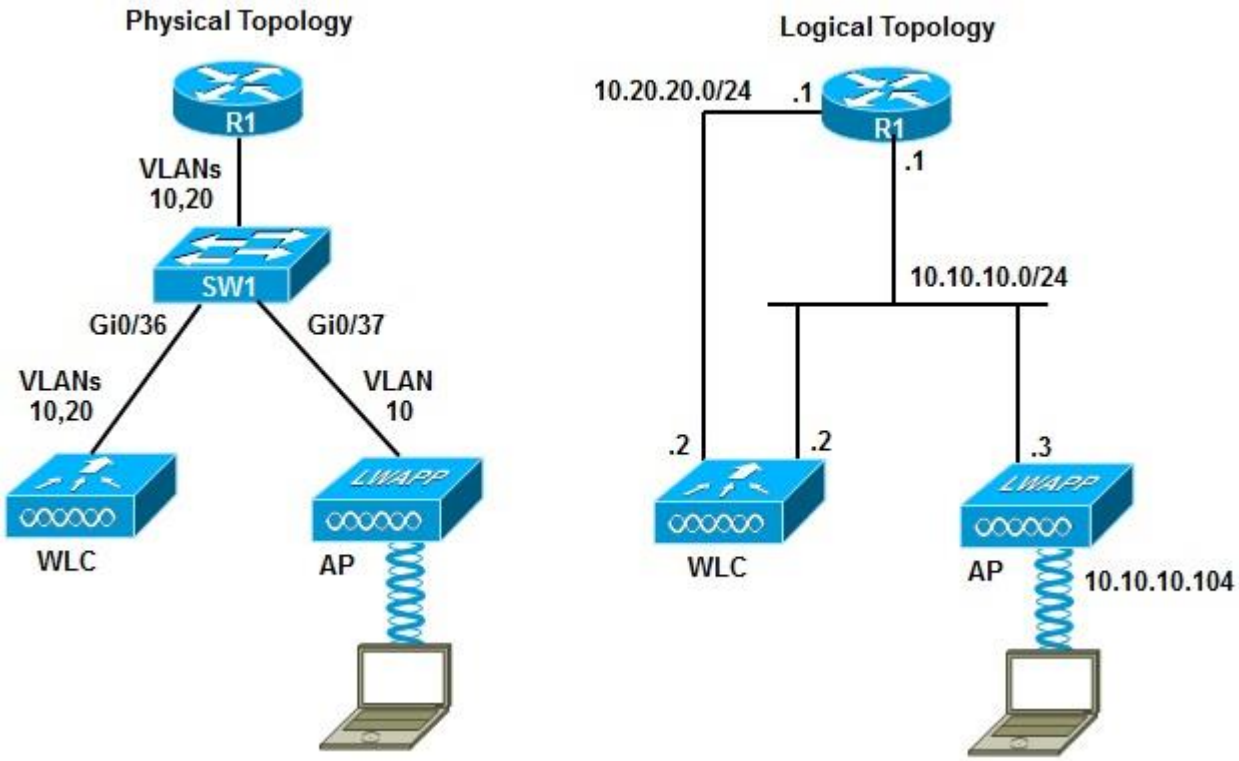
Some common wireless integration issues include:

- **Traffic flow from client to WAP** - Even if there is radio frequency (RF) connectivity between the AP and the client, there can still be a problem at the side where traffic flows from the client, through the AP, to the rest of the network.
- **WLC issues** - In a controller-based solution, the boundary between the wireless and the wired network is the Cisco WLC because traffic is tunneled between the AP and the WLC.
- **Filtering issues** - If any filters are configured on either the Ethernet side or the radio side of the AP, disable them temporarily, until you resolve connectivity issues.
- **IP addressing issues** – IP addressing typically needs to be investigated, especially in roaming scenarios.
- **QoS issues** - Maintaining QoS markings consistently across wireless-to-wired boundaries is important.
- **Other potential issues** – Can be related to the network services typically provided by the switches that are connected to APs (such as POE).

Wireless Integration Issue Tools

- Use an appropriate troubleshooting approach (top-down, bottom-up, divide-and-conquer, etc.).
- Use your knowledge of switching during information gathering. Issues may be related to trunking, VLANs, and switch port configuration.
- Use a design tool such as the Cisco Power Calculator for POE issues.
- Useful wireless troubleshooting commands:
  - **`show vlan`**
  - **`show interfaces status`**
  - **`show interfaces trunk`**
  - **`show interfaces switchport`**
  - **`show access-lists`**
  - **`show cdp neighbors`**

WLAN Connectivity Troubleshooting Example 1: Misconfigured Trunk



WLAN Troubleshooting Example 1 – Cont.

- Wireless service has stopped and clients are not able to associate to the AP.
- From the wired PCs used for troubleshooting, it is not possible to connect to the AP or the WLC, using either Secure Shell (SSH) or HTTP-Secure (HTTPS).
- Use a bottom-up approach and start with the access switch
- Use the **`show cdp neighbors`** command to to identify which ports are connected to the controller and access point.
- Based on the results shown the WLC connects to interface Gi0/36 and the AP connects to interface Gi0/37.

```
SW1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce Holdtme Capability Platform         Port ID
ap             Gig 0/37      128        T I     AIR-LAP125       Gig 0
521-8          Gig 0/39      135                AIR-LAP521       Fas 0
521-7          Gig 0/34      122                AIR-LAP521       Fas 0
Cisco_9a:8c:e0 Gig 0/36      175        H       AIR-WLC210       Unit - 0 Slot
- 0 Port - 1
```

WLAN Troubleshooting Example 1 – Cont.

- Next, examine the status of the interfaces with the **`show interface status`** command.
- The Gi0/37 interface connected to the AP is associated to VLAN 10, and the Gi0/36 interface connected to the WLC is configured as trunk.

```
SW1# show interface status
Port     Name      Status       vlan    Duplex    Speed  Type
Gi0/1              notconnect   1       auto      auto   10/100/1000BaseTX
Gi0/2              notconnect   1       auto      auto   10/100/1000BaseTX
<output omitted>
Gi0/34             connected    1       a-full    a-100  10/100/1000BaseTX
Gi0/35             notconnect   1       auto      auto   10/100/1000BaseTX
Gi0/36             connected    trunk   a-full    a-100  10/100/1000BaseTX
Gi0/37             connected    10      a-full    a-1000 10/100/1000BaseTX
Gi0/38             notconnect   1       auto      auto   10/100/1000BaseTX
Gi0/39             connected    1       a-full    a-100  10/100/1000BaseTX
<output omitted>
```

WLAN Troubleshooting Example 1 – Cont.

- Find out which VLANs are used for AP to WLC communication, which VLAN is used for client traffic, and whether the access point is operational and registering to the WLC using LWAPP or Control and Provisioning of Wireless Access Points (CAPWAP).
- The AP has a static IP address and the WLC and the AP should be on the same VLAN, but the WLC is not seeing registration requests from the AP.
- The static IP address on the AP rules out DHCP preventing the AP from initiating an LWAPP request.
- The Layer 1 and Layer 2 status of the interfaces are operational for both the wired and wireless side, for both the AP and the WLC.

WLAN Troubleshooting Example 1 – Cont.

- If the AP cannot register with the WLC, it will not be able to service client requests.
- The AP's request originates from interface Gi0/37, which is associated to VLAN 10, and must traverse the trunk link associated with Gi0/36 to reach the WLC.
- Verify that VLAN 10 is allowed on the trunk interface (Gi 0/36), using the **`show interfaces switchport`** command.
- The output shown reveals that only VLAN 1 is enabled (allowed) on the trunk.
- Other VLANs such as VLAN 10 are not allowed on the trunk.

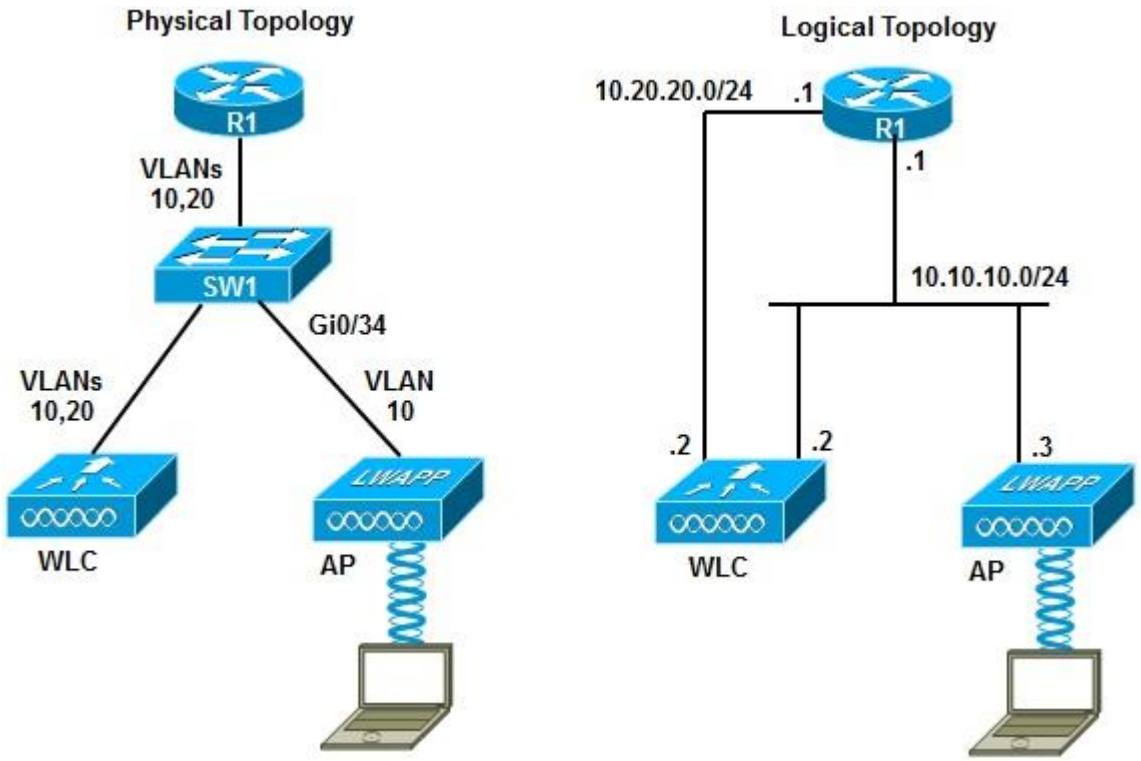
```
SW1# show interfaces switchport | begin 0/36
Name: Gi0/36
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
<output omitted>
Trunking VLANs Enabled: 1
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
<output omitted>
```

WLAN Troubleshooting Example 1 – Cont.

- The wireless team tells you that the client VLAN is 10, and that the management VLAN is 20.
- Add the appropriate VLANs to the list of allowed VLANs on the trunk interface to correct the problem.
- Use the **`switchport trunk allowed vlan add 10,20`** command so that VLANs 10 and 20 are allowed on the trunk interface Gi 0/36.

```
SW1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# interface g0/36
SW1(config-if)# switchport trunk allowed vlan add 10,20
SW1(config-if)# end
SW1#
```

WLAN Connectivity Troubleshooting Example 2: Duplex and Trust Issues



WLAN Troubleshooting Example 2 – Cont.

- The wireless operations team complains about the reliability and performance of wireless traffic.
- The symptom they observe is that the AP interface pointing to the wired network goes up and down intermittently, and when the port is operational, there is a substantial slowdown on Voice over WLAN.
- First, display the log and look for clues about the interface (Gi 0/34) that apparently goes up and down intermittently.
- Next, use the **show logging | include 0/34** command on SW1, which indicates a duplex mismatch problem.

```
SW1# show logging | include 0/34
00:12:00: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
GigabitEthernet0/34 (not half duplex), with 521-7 FastEthernet0 (half duplex)
00:13:00: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
GigabitEthernet0/34 (not half duplex), with 521-7 FastEthernet0 (half duplex)
00:14:00: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
GigabitEthernet0/34 (not half duplex), with 521-7 FastEthernet0 (half duplex)
00:15:00: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
GigabitEthernet0/34 (not half duplex), with 521-7 FastEthernet0 (half duplex)
<output omitted>
```

WLAN Troubleshooting Example 2 – Cont.

- There is a duplex mismatch, but you should see the duplex mismatch messages on the console, too.
- The **`show logging`** command on SW1 indicates that console logging is disabled, which makes sense for a production switch.
- If you enable it, you will see the duplex mismatch messages.
- Fix the duplex problem by configuring the interface for full-duplex 100 Mbps.
- Note that it is a good practice to find out why the interface was set to half duplex to begin with.

```
SW1# show logging
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 0
flushes,
0 overruns, xml disabled, filtering disabled
Console logging: disabled
<output omitted>

SW1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# int g0/34
SW1(config-if)# duplex full
SW1(config-if)# speed 100
SW1(config-if)# end
```

WLAN Troubleshooting Example 2 – Cont.

- After fixing the SW1 Gi0/34 duplex problem, the wireless team informs you that the AP comes up and does not go down again
- They are still experiencing performance issues, especially for VoIP traffic coming from the wireless network.
- Use the **`show processes cpu`** command to determine if high CPU utilization is an issue
- The output shows a relatively low level of utilization at this point and not too far off baseline for this device.

```
SW1# show processes CPU
CPU utilization for five seconds: 4%/0%; one minute: 6%, five minutes: 5%
PID Runtime(ms)  Invoked uSecs  5Sec    1Min   5Min  TTY Process
1             0        5     0  0.00%  0.00%  0.00%    0 Chunk Manager
2             0      275     0  0.00%  0.00%  0.00%    0 Load Meter
3             0       33     0  0.00%  0.00%  0.00%    0 SpanTree Helper
4          1019      149  6838  0.00%  0.07%  0.05%    0 Check heaps
5             0        1     0  0.00%  0.00%  0.00%    0 Pool Manager
6             0        2     0  0.00%  0.00%  0.00%    0 Timers
7           118      845   139  0.00%  0.00%  0.00%    0 ARP Input
8             0        1     0  0.00%  0.00%  0.00%    0 AAA_SERVER_DEADT
9             0        2     0  0.00%  0.00%  0.00%    0 AAA high-capacit
<output omitted>
```

WLAN Troubleshooting Example 2 – Cont.

- Wireless voice traffic may not be properly prioritized when entering the network.
- Possibly, the voice traffic may not be tagged with proper QoS priorities.
- With LWAPP deployment, the AP uses the differentiated services code point (DSCP) field to tag packets.
- Check to see whether the switch port is honoring that using the **`show mls qos int gi0/34`** command to display the trust boundary settings.
- The output indicates that the switch does not trust anything coming from the AP.

```
SW1# show mls qos int g0/34
GigabitEthernet0/34
trust state: not trusted
trust mode: not trusted
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: None
qos mode: port-based
```

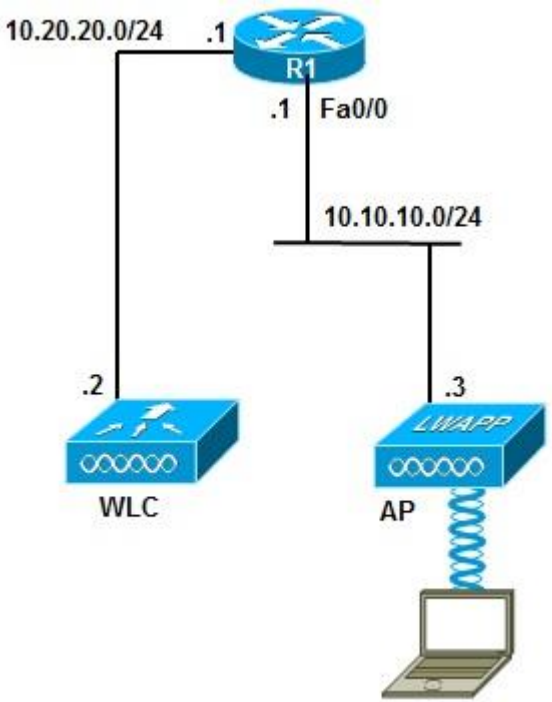
WLAN Troubleshooting Example 2 – Cont.

- Set the switch port (Gi0/34) to trust DSCP values using the **`mls qos trust dscp`** command.
- The output of the **`show mls qos`** command now indicates that the switch is trusting DSCP values.
- The wireless network support staff confirm that performance issues are alleviated for VoWLAN traffic.

```
SW1(config)# int g0/34
SW1(config-if)# mls qos trust dscp
SW1(config-if)# end
SW1#

SW1# show mls qos int g0/34
GigabitEthernet0/34
trust state: trust dscp
trust mode: trust dscp
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: None
qos mode: port-based
```

WLAN Connectivity Troubleshooting Example 3: LWAPP Denied by New Security



WLAN Troubleshooting Example 3 - Cont.

- The wireless team tells you that wireless operations have stopped and that none of the APs are able to register to the WLC.
- Based on a recent change in security policy, you find that Cisco IOS firewall services were installed in router R1.
- Router R1 is performing inter-VLAN routing and the reported symptom points to the possibility of LWAPP traffic being denied by the firewall.
- Cisco IOS Software allows the firewall to be configured using one of two methods:
  - The classical Cisco IOS firewall
  - The zone-based policy firewall

WLAN Troubleshooting Example 3 – Cont.

- A check of the zone-based policy using the **`show zone-pair security`** command produces an error message indicating there are no zone-based policies configured on this router.
- Next, check for interface ACLs on the router using the **`show ip interface`** command for the R1 interface pointing to the AP side of the connection.
- This reveals an ACL called FIREWALL applied inbound to the R1 interface Fa0/0.

```
R1# show ip interface Fa0/0
FastEthernet0/0 is up, line protocol is up
Inbound access list is FIREWALL
<output omitted>
```

WLAN Troubleshooting Example 3 – Cont.

- Display access lists on R1 using the **show access-list** command. The FIREWALL ACL allows routing protocols and management protocols such as SSH.
- The LWAPP ports, AP-to-WLC control messages (UDP 12223) and user traffic (UDP port 12222) through the LWAPP tunnel are not permitted by the firewall.
- Designers of the security policy must be aware of the services and applications running on the network.

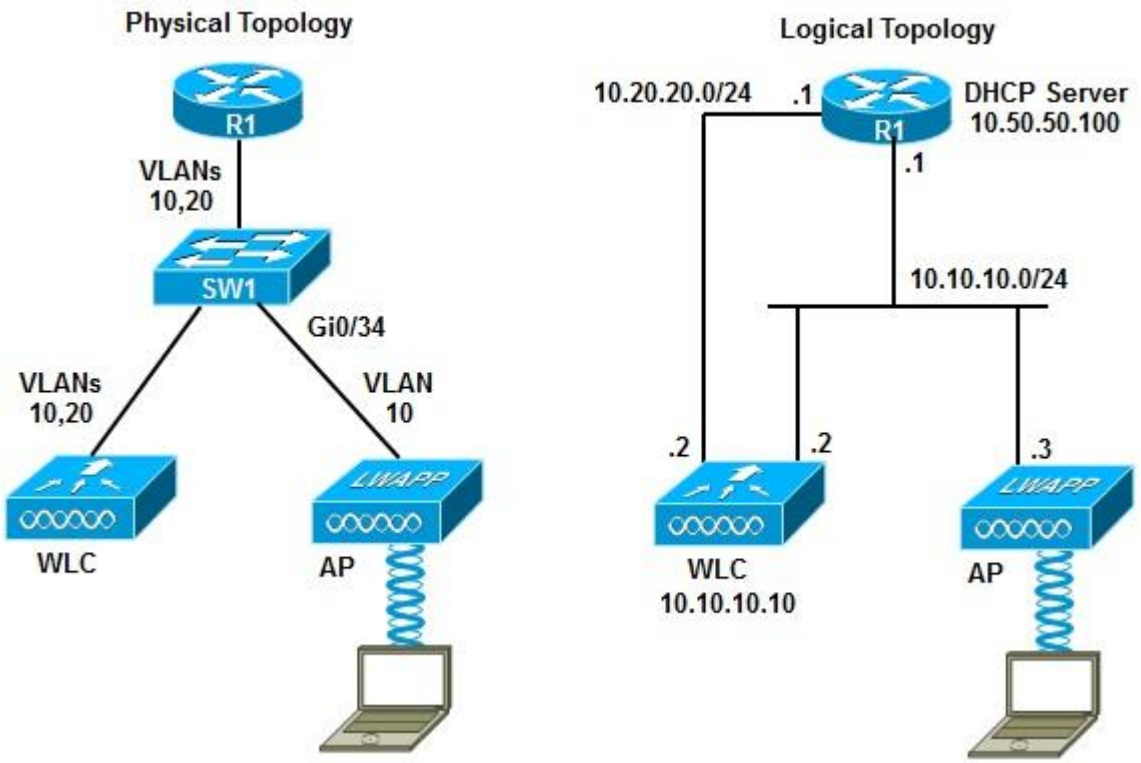
```
R1# show access-list
Extended IP access list 100
    10 permit udp 10.10.10.0 0.0.0.255 any eq 12223
    20 permit udp any any eq 12223
Extended IP access list FIREWALL
    10 permit icmp any any echo-reply
    20 permit tcp any any eq www
    30 permit tcp any any eq ftp
    40 permit tcp any any eq ftp-data
    50 permit tcp any any eq telnet
    60 permit tcp any anyeq smtp
    70 permit tcp any any eq pop3
    80 permit eigrp any any
    90 permit udp any any eq rip
```

WLAN Troubleshooting Example 3 – Cont.

- Add a line to the ACL, and a remark indicating why this line was added.
- Permit UDP 12222 for user data traffic, and UDP 12223 for AP-to-WLC control messages.
- The wireless team reports that this fix seems to have solved the problem.
- Monitor the accuracy of the change and the potential implications it might have.
- The **`show access-lists`** command can displa the number of packets matching each ACL line.

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip access-list extended FIREWALL
R1(config-ext-nacl)# remark ---allowing LWAPP control and data ports---
R1(config-ext-nacl)# permit udp any any range 12222 12223
R1(config-ext-nacl)# end
```

WLAN Connectivity Troubleshooting Example 4: DHCP Issues



WLAN Troubleshooting Example 4 - Cont.

- The AP and the WLC are in different VLANs.
- Router R1 is performing inter-VLAN routing and also acts as the DHCP server for the APs.
- The wireless team states that none of the APs can register to the WLC.
- All APs are DHCP clients but are not able to obtain their IP address from the DHCP server (which is R1 at address 10.50.50.100).
- APs must first obtain an IP address lease from the DHCP server.
- After the APs have obtained an IP address, they can register with the WLC.

WLAN Troubleshooting Example 4 – Cont.

The **show ip dhcp server statistics** command shows some statistics but no conclusions can be drawn. Clear the statistics using the **clear ip dhcp server statistics** command and reissue the **show** command, which shows no activity this time.

```
R1# clear ip dhcp server statistics
R1#
R1# show ip dhcp server statistics
Memory usage             5317
Address pools            1
Database agents          0
Automatic bindings       2
Manual bindings          0
Expired bindings         0
Malformed messages       0

Message                  Received
BOOTREQUEST              0
DHCPDISCOVER             0
DHCPREQUEST              0
DHCPDECLINE              0
DHCPRELEASE              0
DHCPINFORM               0

Message                  Sent
BOOTREPLY                0
DHCPOFFER                0
DHCPPACK                 0
DHCPNAK                  0
```

WLAN Troubleshooting Example 4 - Cont.

- The **`debug ip udp`** command shows no reference to UDP port 67 (DHCP client).
- The DHCP clients (APs) are in a different subnet than the DHCP server so this could be a DHCP relay agent problem.
- Use the show run interface gi0/34 command for the port that points to the APs, but there is no ip-helper address command.
- This switchport is associated to VLAN 10, so inspect interface VLAN 10 instead. There is no IP Helper-address configured there either.

```
SW1# show running-config interface g0/34
Building configuration...
Current configuration : 108 bytes
!
interface GigabitEthernet0/34
 switchport access vlan 10
 switchport mode access
 mls qos trust dscp
end

SW1# show running-config interface vlan 10
Building configuration...
Current configuration : 61 bytes
!
interface vlan10
 ip address 10.10.10.1 255.255.255.0
end
```

WLAN Troubleshooting Example 4 - Cont.

- The **`show running | include helper`** command reveals that one IP helper address is configured on the switch
- It is pointing to an old DHCP server address and it is not on the right interface.
- On interface VLAN 10 enter the correct IP helper address.
- The **debug** results now show UDP packets arriving at the DHCP server (R1).

```
SW1# show running-config | include helper
ip helper-address 10.100.100.100
SW1#
SW1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# int vlan 10
SW1(config-if)# ip helper-address 10.50.50.100
SW1(config-if)# end
SW1#

R1#
02:13:57: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
02:13:58: DHCPD: assigned IP address 10.10.10.115 to client 0100.1bd5.1324.42.
02:13:58: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=308
02:13:58: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=308
02:13:58: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
```

WLAN Troubleshooting Example 4 - Cont.

- The wireless support team verifies the successful AP IP address assignment; however, there is still no registration into the WLC.
- The wireless operations team tells you to check the configuration of option 43 on the DHCP server.
- On the DHCP server, you display the details of the address pool using the **`show ip dhcp pool`** command and there is no option 43 configured.

```
R1# show running-config | section ip dhcp pool
ip dhcp pool vlan10
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
```

WLAN Troubleshooting Example 4 - Cont.

- Option 43 is used to inform the DHCP client of the WLC AP-management IP address.
- Use the **ip dhcp pool** command for VLAN 10 and enter the AP-management IP address as part of option 43.
- The command format is **option 43**, followed by the correct IP address in hexadecimal format, as shown in the example.
- If there is only one WLC management address, the Length is 04 (hex), and in this case the WLC management IP address is 10.10.10.10, which is 0a0a0a0a (hex).

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip dhcp pool vlan10
R1(dhcp-config)# option 43 hex f1040a0a0a0a
R1(dhcp-config)# end
R1#
```

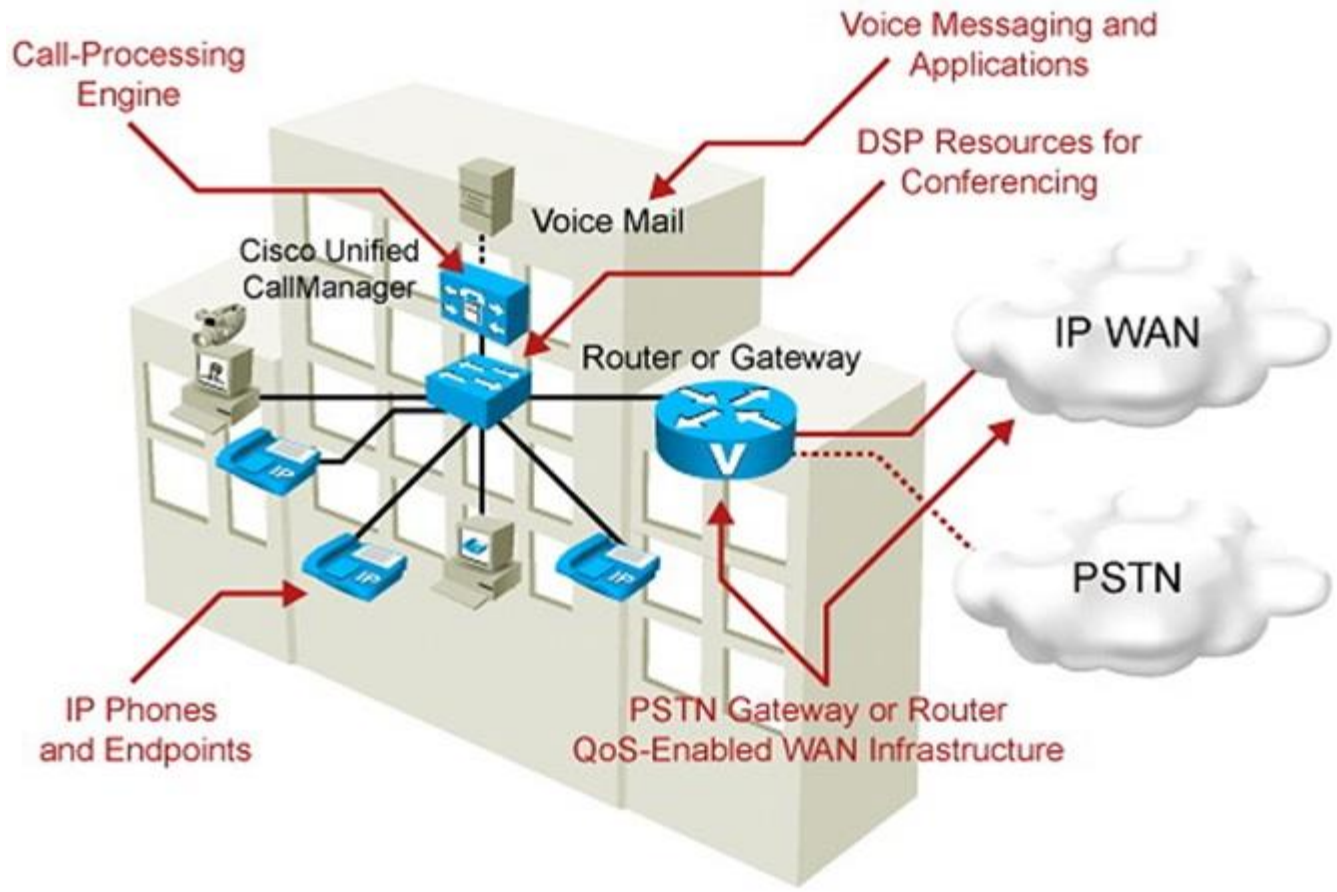
Troubleshooting Unified Communications Issues in a Converged Network

Section Overview

- The focus of this section is convergence, an integral part of most networks.
- It deals with the readiness of a campus network to support converged services, such as unified communications or IP telephony.
- IP telephony services provided over the campus infrastructure require the coexistence of data and voice.
- Types of traffic are differentiated and delay-sensitive voice traffic is prioritized using QoS policies to mark and qualify traffic as it traverses the campus switch blocks.
- VLANs keep voice traffic separate from other data.
- The underlying routing and switching infrastructure must providing a reliable, efficient, and secure transport for signaling traffic and the gateway traffic to forward calls to the PSTN or WAN destinations.

Unified Communications Integration Issues

The converged network shows the main elements such as voice gateway, CUCM, Cisco Unity (for voice mail), telephony endpoints (IP phones, conference units), LAN router and switches, WAN, and PSTN.



Unified Communications Design

- The following list summarizes the design considerations of integrating unified communications into a campus network.
- These can involve multiple components of the network, multiple layers of the OSI model, multiple integrated technologies and potentially, multiple operations and support teams within an organization.
  - **Quality of service:** Bandwidth, delay, jitter, packet loss, network QoS readiness, trust boundaries, switch QoS
  - **High availability:** STP/RSTP, HSRP/GLBP/VRRP
  - **Security:** Traffic segregation (voice versus data VLANs), firewalling/filtering
  - **Provisioning and management:** PoE, DHCP, TFTP, NTP, CDP, trunking, VLANs

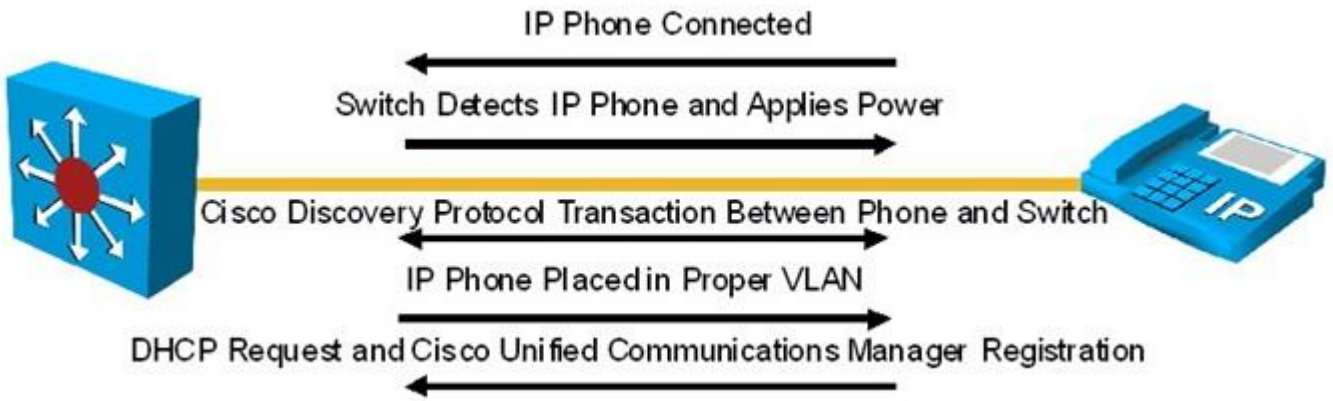
Unified Communications Components

In addition to QoS and VLAN management issues, the Unified Communications network requires specific components that might become additional sources of problems. These are services that use the underlying VLAN and switching infrastructure:

- Power (PoE) must be readily available to endpoints.
- Repositories of firmware and configuration files through TFTP
- Time synchronization (Network Time Protocol [NTP]) for cryptographic authentication
- Cisco Discovery Protocol (CDP) to facilitate the IP phone booting process
- DHCP must be accessible to provide IP information for the phone

Unified Communications – IP Phones

- Support engineers need to be familiar with the IP phone boot process.
- Several devices, services, and protocols need to work in harmony for the successful initialization and startup of the IP phone.



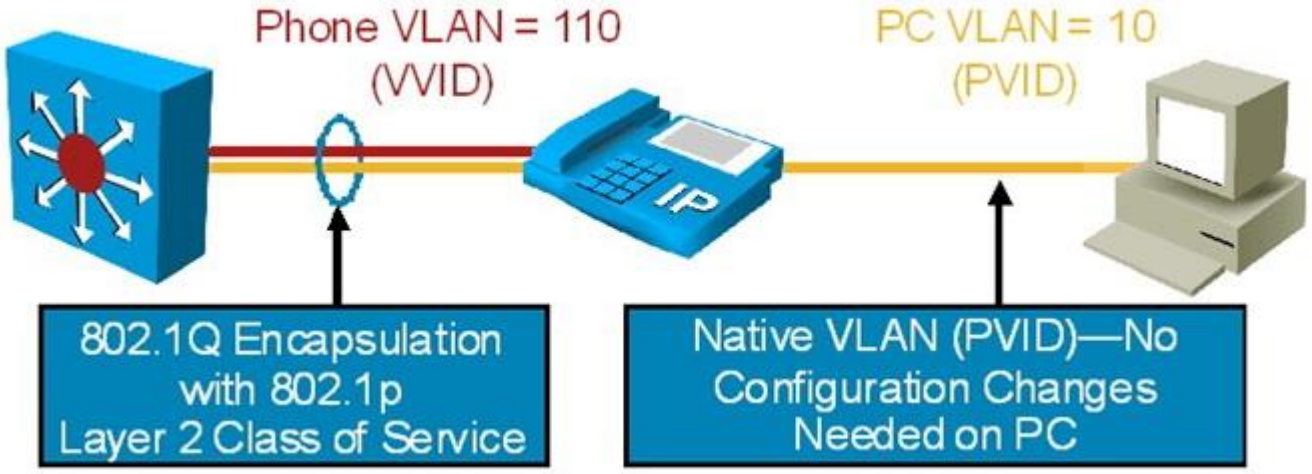
IP Phone Boot Process

The following is the IP phone boot process :

- **Step 1.** The IP phone powers on.
- **Step 2.** The phone performs a power-on self-test, or POST.
- **Step 3.** The phone boots.
- **Step 4.** The phone uses CDP to learn the voice VLAN.
- **Step 5.** The phone initializes the IP stack.
- **Step 6.** The IP phone sends DHCP broadcasts.
- **Step 7.** The DHCP server selects a free IP address from the pool and sends it, along with the other parameters, including option 150.
- **Step 8.** The IP phone initializes, applying the IP configuration to the IP stack.
- **Step 9.** The IP phone requests a configuration file from the TFTP server defined in Option 150.

VLAN Considerations

- The VLAN architecture is very important, and knowing the voice and data VLANs is crucial.
- Also, knowing how voice and data traffic is carried across switch ports help in troubleshooting efforts.
- The figure shows that the voice VLAN uses IEEE 802.1Q encapsulation and that Voice (Auxiliary) and Data VLANs Are Carried over the Same Port.
- Data traffic remains untagged and uses the native VLAN.
- The switch port where the IP phone connects is configured as an access port, but it supports an auxiliary VLAN called the voice VLAN.



Troubleshooting Scenarios

- IP phones might become out of sync in terms of digital certificate verification if network services are not available, are misconfigured, or are simply not reachable.
- An IP phone might not obtain the right amount of power, if CDP is missing.
- A misconfigured DHCP server might prevent IP phones from obtaining
- their configuration files if option 150 is not enabled.
- QoS architectures might render voice traffic useless.
- Security controls might interfere with control protocols and could also filter required signaling protocols, crucial in VoIP operations.
- Protocols and ports in standard IP telephony deployments include:
  - Real-Time Transport Protocol (RTP) and its UDP port ranges
  - Session Initiation Protocol (SIP) on TCP port 5060
  - H323 on TCP port 1720.

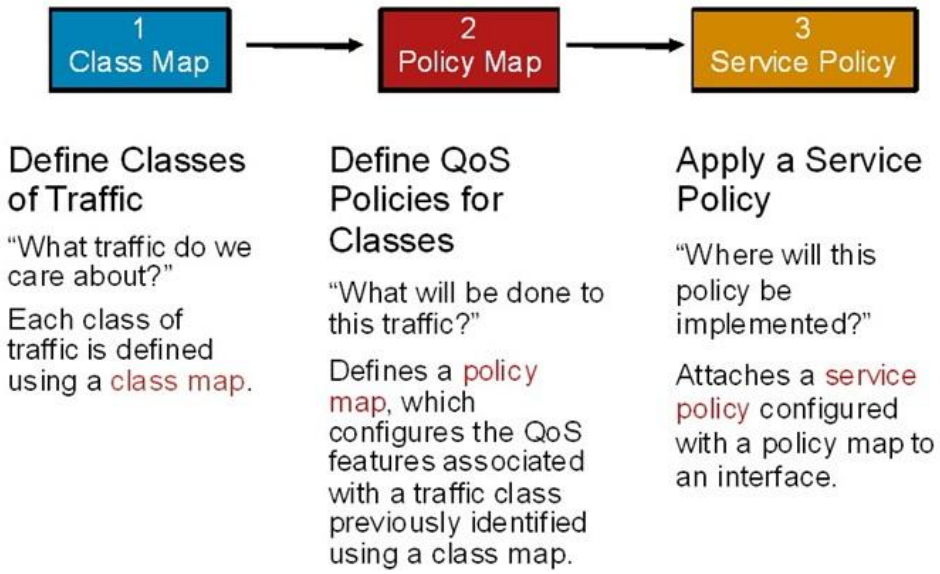
Modular QoS CLI (MQC)

- On most Cisco IOS devices, MQC is used to configure QoS.
- MQC allows you to configure policies once and apply them to multiple interfaces and different devices.
- MQC syntax is not platform specific.
- It decouples the traffic classification components from the policy components.
- You can apply the same policy to different traffic classes without having to create it multiple times.

QoS Policy

Configuring a QoS policy using Cisco IOS MQC has three main components:

- Class maps: Create classification templates for use in policy maps.
- Policy maps: Create a traffic policy to configure the QoS features to be associated with classified traffic.
- Service policy: Assigns a policy map to an interface for incoming or outgoing traffic.



Unified Communications Commands

- After class maps, policy maps, and service policies are configured on the device interfaces, several useful troubleshooting commands are available.
- To summarize the status of the QoS components, use:
  - **show policy-map interface** on routers
  - **show mls qos** on switches
- You can also use appropriate show and debug commands to examine the more traditional services such as DHCP and CDP.
- In converged networks, troubleshoot IP phone issues in this order:
  1. **PoE**
  2. **CDP**
  3. **DHCP**
  4. **TFTP**

Converged Network Troubleshooting Commands

Focus	Command

Switching	`show interfaces trunk`
	`show interfaces switchport`
	`show vlan`
	`show errdisable recovery`

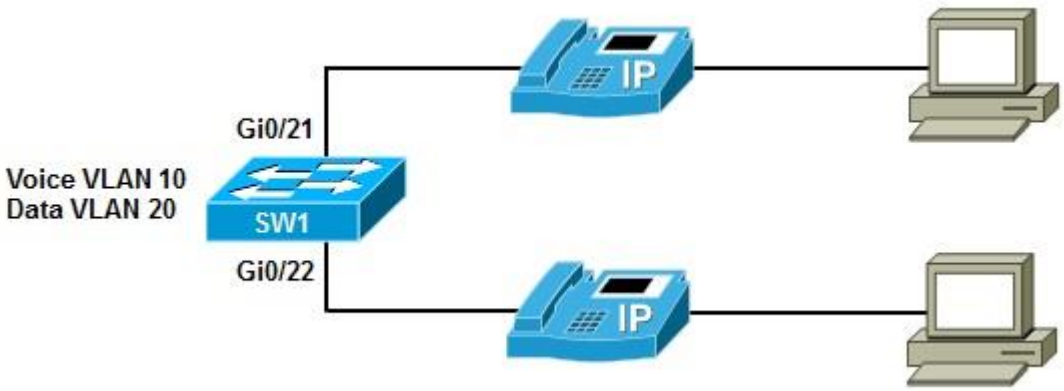
Auto-QoS	`show auto qos` `show auto discovery qos`

IP services	`show ip dhcp pool`
	`show ip dhcp server`
	`show ntp status`

IP communications	`debug ephone`
Security	`show crypto engine connections active`

Example 1: Port Security and Voice VLAN Issues

- The problem is that the IP phones will not boot and initialize.
- They have no access to the IP network.
- The problem occurs in multiple areas of the network, but not all.
- The issue seems to be permanent, and not intermittent.
- In those switches where the problem IP phones are connected, it is not clear whether all IP phones have the same problem.



Voice Troubleshooting Example 1 – Cont.

- This issue seems to be a network-wide problem so the wiring closets where the symptoms were detected are identified to try to find a common recent change, upgrade, or incident recently happening.
- The change logs for the affected wiring closets show a recent change on VLAN Trunking Protocol (VTP) domains and configuration.
- Check the status and configuration of the port for the failing IP phone using the **`show interfaces status`** command for the interface where the phone is connected.

```
SW1# show interfaces g0/21 status
Port    Name               Status       Vlan Duplex Speed  Type
Gi0/21 Phone number 1   err-disabled 20   auto   auto   10/100/1000BaseTX
```

Voice Troubleshooting Example 1 – Cont.

- The port status for Gi0/21 is err-disabled.
- Use the command **`show interface status err-disabled`** command to list the ports in this state along with the reasons for this state.
- Based on the output in the example, the reason for the error is a port security violation.

```
SW1# show port-security interface g0/21
Port Security                   : Enabled
Port Status                     : Secure-shutdown
Violation Mode                  : Shutdown
Aging Time                      : 0 mins
Aging Type                      : Absolute
SecureStatic Address Aging      : Disabled
Maximum MAC Addresses           : 1
Total MAC Addresses             : 1
Configured MAC Addresses        : 1
Sticky MAC Addresses            : 0
Last Source Address:vlan        : 0021.7098.30ab:20
Security Violation Count        : 1
```

Voice Troubleshooting Example 1 – Cont.

- The output of the **`show port-security interface`** command shows that the maximum allowed MAC addresses on the port is set to 1.
- That setting is probably why the problem has occurred.
- A maximum of one MAC address is allowed on the interface, yet some of the phones have PCs connected to them, and both the phone and the PC send packets.
- This means that two MAC addresses will be reported on the port, which is beyond the maximum allowed.

```
SW1# show port-security interface g0/21
Port Security : Enabled
Port Status : Secure-shutdown
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:vlan : 0021.7098.30ab:20
Security Violation Count : 1
Switch#
```

Voice Troubleshooting Example 1 – Cont.

- You are informed that this setting is not needed on IP phone switch ports.
- Use the **`show running interface`** command to display the configuration for the interfaces.
- Port security allows a single static MAC address.

```
SW1# sh run int g0/21
Building configuration...
Current configuration : 200 bytes
!
Interface GigabitEthernet0/21
 description Phone number 1
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security mac-address 000b.8572.1810
end
```

Voice Troubleshooting Example 1 – Cont.

- To remove the port security configuration, use the **no switchport port-security** command and the **no** version of all commands related to port security.
- Before removing the erroneous commands, reset the interface using the **shutdown** command. Enter the **no shutdown** command afterwards.
- Check the status of the interface and the status shows as connected.
- However, there is still a problem and the IP phones are down.

```
SW1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# int g0/21
SW1(config-if)# shutdown
SW1(config-if)# no switchport port-security
SW1(config-if)# no switchport port-security mac-address 000b.8572.1810
SW1(config-if)# no shutdown
SW1(config-if)# end

SW1# show interface g0/21 status
Port     Name              Status      Vlan  Duplex  Speed   Type
Gi0/21   Phone number 1    connected   20    a-full  a-1000  10/100/1000BaseTX
```

Voice Troubleshooting Example 1 – Cont.

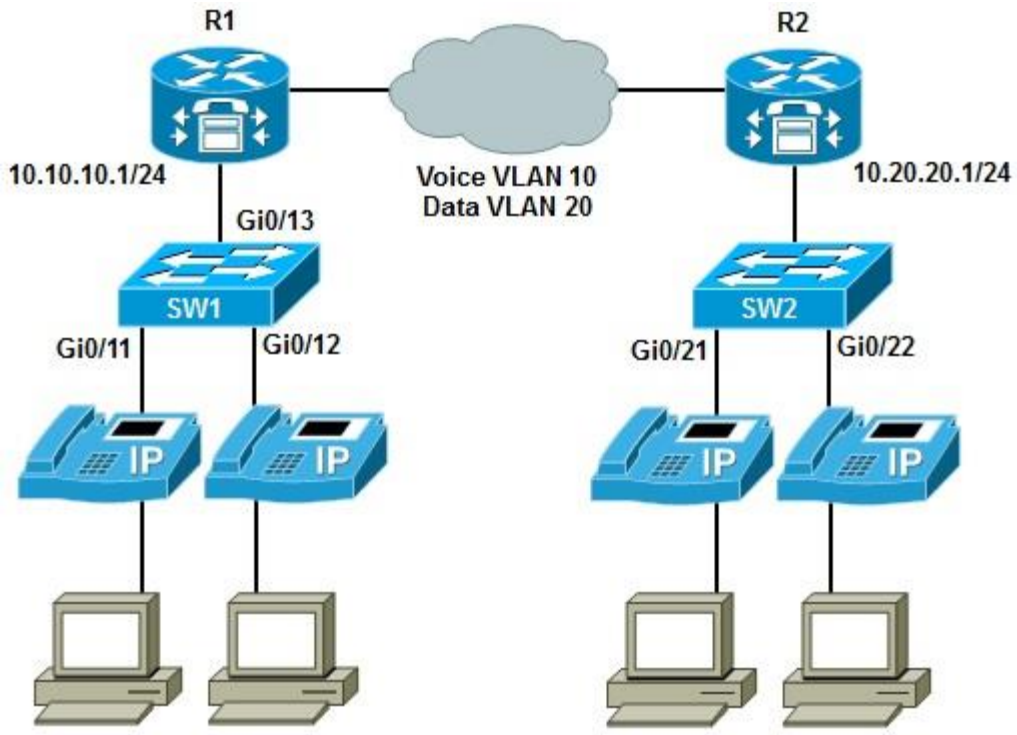
- A review of the running configuration shows that voice VLAN is not configured for the port.
- A review of the configuration template for IP phone switch ports reveals that the interfaces are missing the trust boundary settings and have no voice VLAN configuration
- Configure one interface according to the configuration template for testing.
- Set the voice VLAN using the **`switchport voice vlan 10`** command and trust IP phone markings using the **`mls qos trust cos`** and **`mls qos trust device ip-phone`** commands.
- Check the configuration using the **`show interfaces switchport`** command.

```
SW1(config)# int g0/21
SW1(config-if)# switchport voice vlan 10
SW1(config-if)# mls qos trust cos
SW1(config-if)# mls qos trust device cisco-phone
SW1(config-if)#

SW1# show interfaces switchport g0/21
Name: Gi0/21
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (VLAN0020)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 10 (VLAN0010)
<output omitted>
```

Example 2: Invalid Marking of VoIP Packets

Users from one building complain about their experience with voice calls and claim that it is choppy, they lose connections frequently, and at some point voice conversations are intermittent. the problem is worse for branch-to-branch calls.



Voice Troubleshooting Example 2 – Cont.

- To gathering measurable information, ask the following questions:
  - How often do you observe the reported symptoms?
  - Is there a particular time of the day in which they commonly occur?
  - Is the perceived quality the same when calling internal extension numbers and as it is when calling outside numbers?
  - How often are you unable to obtain a dial tone? For how long does this condition remain?
  - Which locations of the network are experiencing the problem (building/branch)?
  - Are the problematic devices connected to the same wiring closet?
- A comparison to baseline QoS metrics shows that end-to-end delay for voice traffic has doubled across the campus.

Voice Troubleshooting Example 2 – Cont.

- A comparison to baseline QoS metrics shows that end-to-end delay for voice traffic has doubled across the campus.
- Packet-loss percentages are close to baseline at about 1 percent.
- The latency numbers show that a QoS issue exists.
- The policy trend in this campus is to push QoS settings toward the distribution and access layers.
- Check the access switch first, and then move up to the distribution layer switch or router, trying to confirm the QoS settings.

Voice Troubleshooting Example 2 – Cont.

The SW1 CPU utilization 5-minute average is 25 percent. Access port Gi0/11 bandwidth utilization is normal at around 1.5%. The trunk uplink utilization is normal.

```
SW1# show processes cpu
CPU utilization for five seconds: 99%/22%; one minute: 58%, five minutes: 25%
PID Runtime(ms)  Invoked  uSecs   5Sec  1Min  5Min  TTY   Process
1            0       15      0  0.00% 0.00% 0.00%    0   Chunk Manager
2            9     1131      7  0.00% 0.00% 0.00%    0   Load Meter
3            0        1      0  0.00% 0.00% 0.00%    0   CEF RP IPC Backg
<output omitted>

SW1# show interfaces gi0/11
5 minute input rate 729000 bits/sec, 847 packets/sec
5 minute output rate 14150000 bits/sec, 1129 packets/sec
   104911 packets input, 13035040 bytes, 0 no buffer
   Received 22020 broadcasts (110 multicasts)
<output omitted>

SW1# show interfaces gi0/13
GigabitEthernet0/13 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 0023.5d08.568d (bia 0023.5908.568d)
  Description: to Cisco phone
  MTU 1504 bytes, BW 100000 Kbit, DLY 100 usec,
  reliability 255/255, txload 5/255, rxload 6/255
<output omitted>
```

Voice Troubleshooting Example 2 – Cont.

- The documentation indicates that IP phones represent the trust boundary, and that the DSCP markings are being used throughout the network.
- Phones are allowed to tag their own packets with high priorities, in this instance DSCP value EF (Expedited Forwarding).
- The command **`show mls qos interface`** on one of the access switch ports pointing to the phones reveals that the port is trusted and that DSCP values are being maintained and not reset.

```
SW1# show mls qos int g0/11
GigabitEthernet0/11
trust state: trust dscp
trust mode: trust dscp
trust enabled flag: ena
COS override: dis
Default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
qos mode: port-based
```

Voice Troubleshooting Example 2 – Cont.

The distribution layer in this network is collapsed at the branch router level. Verify QoS settings on R1. The **`show policy-map interface`** command reveals that policy “Reclassify” Is Applied to Fa0/0 inbound.

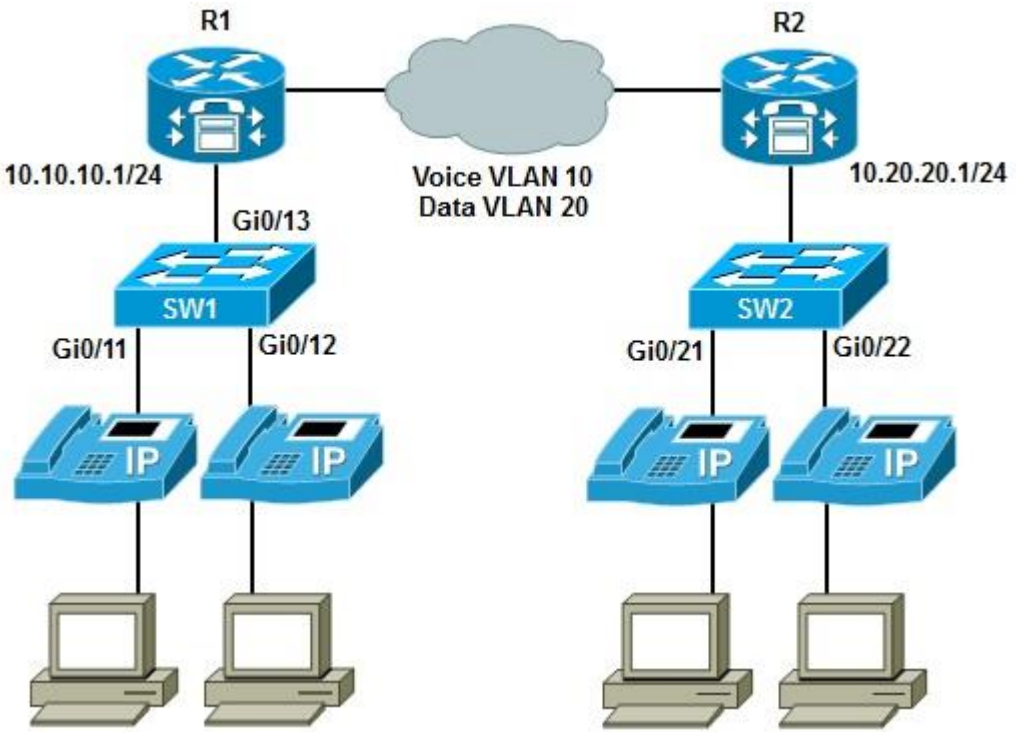
```
R1# show policy-map interface
FastEthernet0/0
Service-policy input: reclassify
 Class-map: signaling (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
  Match: protocol h323
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: protocol sip
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: protocol mgcp
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS set
    dscp af11
      Packets marked 0

 Class-map: voice (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: protocol rtp audio
  QoS Set
    dscp af31
      Packets marked 0
<output omitted>
```

Voice Troubleshooting Example 2 – Cont.

- The **reclassify** policy attached to the R1 Fa0/0 interface reclassifies and re-marks packets coming into this interface.
- The “QoS Set” section within the VOICE class tells us that VOICE traffic is being classified and tagged with the DSCP value AF31.
- Voice traffic is typically classified with DSCP value EF, the highest priority.
- The voice traffic class is being reclassified into a lower priority and is being incorrectly marked down.
- The impact of this improper remarking is that QoS policies such as bandwidth reservation, priority queuing, and preferred path selection are not enforced.
- Voice traffic is suffering because of the identified voice remarking mistake.
- Once this error is fixed, the VOICE problems are solved.

Example 3: ACL and Trunk Issues



Voice Troubleshooting Example 3 – Cont.

- A recent security audit has resulted in new security policies being put in place.
- The IP phones are not able to initialize and obtain their base configuration.
- Those settings are obtained from configuration files stored in the TFTP server, which is the local branch router.
- The local branch router is also serving as a call agent, performing call routing, Call Admission Control (CAC), and other IP telephony functions.
- Due to the recent change in security policy, Cisco IOS firewall services were installed in some key routers of the network.
- The reported symptom is that the IP phones cannot initialize and obtain their settings, or make calls.
- A check of SW1 and R1 shows no zone based policies or ACLs.

Voice Troubleshooting Example 3 – Cont.

An ACL called FIREWALL is applied to the R1 Fa0/0 interface. This interface points to the access switch and the IP phones.

```
R1# show ip interfaces
FastEthernet0/0 is up, line protocol is up
Internet address is 10.10.10.1/24
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is FIREWALL
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
<output omitted>
```

Voice Troubleshooting Example 3 – Cont.

Now display the access list s on R1. The ACL allows traditional traffic such as HTTP, FTP, and SSH.

```
R1# show access-list
Standard IP access list 23
    10 permit 10.10.10.0, wildcard bits 0.0.0.7
    20 permit 172.29.128.128, wildcard bits 0.0.0.31
    30 permit 10.10.50.0, wildcard bits 0.0.0.255 (2 matches)
    40 permit 10.10.60.0, wildcard bits 0.0.0.255

Extended IP access list FIREWALL
    10 permit tcp any any eq telnet (500 matches)
    20 permit tcp any any eq 22
    30 permit tcp any host 10.10.60.60 eq www
    40 permit tcp any host 10.10.60.60 eq 443
    50 permit udp any any
```

Voice Troubleshooting Example 3 – Cont.

- The IP phone registers to the router using Skinny Client Control Protocol (SCCP), which is also referred to as “Skinny.”
- SCCP runs over TCP and uses port 2000. The ACL on R1 dows not permit TCP port 2000.
- Change the access list to allow the SCCP traffic.

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip access-list extended FIREWALL
R1(config-ext-nacl)# permit tcp any any eq 2000
R1(config-ext-nacl)# end
R1#
```

Voice Troubleshooting Example 3 – Cont.

- For testing, initiate one of the IP phones and see whether it is able to make calls.
- Use the **debug ephone register** command to help determine whether phones are trying to register and obtain their settings from Cisco Unified Communications Manager Express.
- Initialize the phone and the debug displays no output.
- The phones are still not registering.

```
R1# debug ephone register
EPHONE registration debugging is enabled
R1#
```

Voice Troubleshooting Example 3 – Cont.

- Perhaps the trunk between the access switch and the router is not allowing SCCP traffic.
- The **`show interfaces trunk`** command reveals that the voice VLAN (10) is not allowed across the trunk from the switch to the router.
- Correct the problem by issuing the **`switchport trunk allowed vlan add 10`** on the trunk interface.

```
SW1# show interface trunk
Port      Mode         Encapsulation   Status    Native vlan
Gi0/13    on           802.1q          trunking  50
Port      Vlans allowed on trunk
Gi0/13    1,50,60
<output omitted>

SW1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)# int Gi0/13
SW1(config-if)# switchport trunk allowed vlan add 10
SW1(config-if)# end
```

Voice Troubleshooting Example 3 – Cont.

The IP phone is now registering to the router and obtaining its IP telephony settings as indicated in the **debug** output phone activity messages.

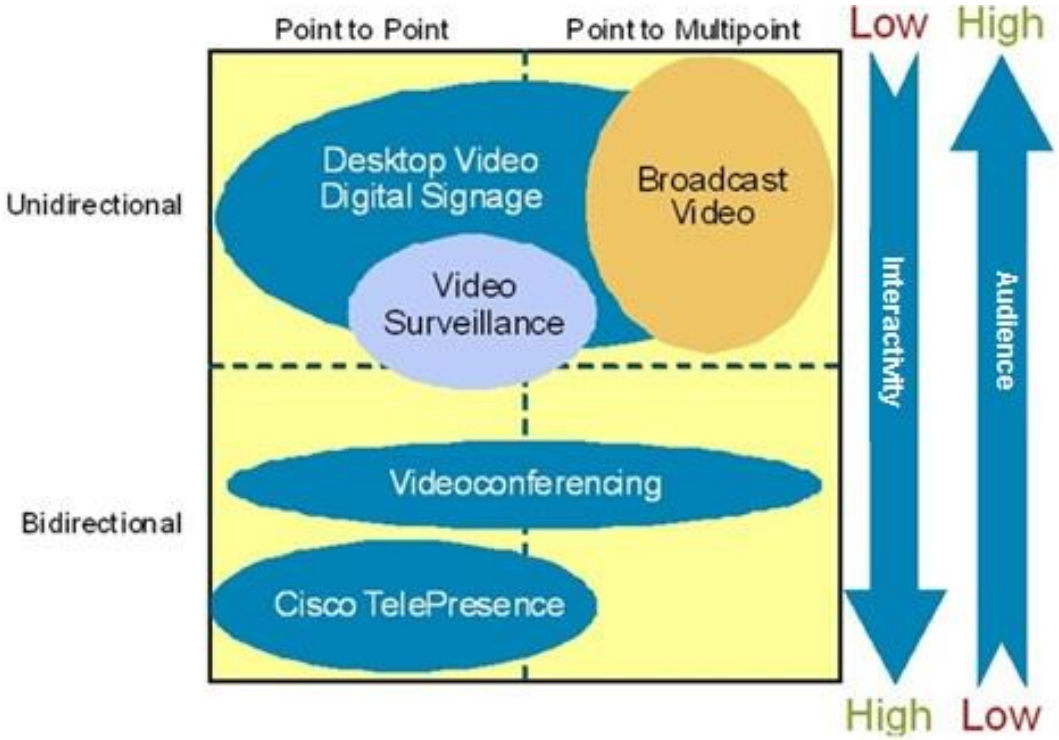
```
*Sep 1 17:22:37.155: ephone-1[0/1][SEP0023331B9090]:ButtonTemplate buttonCount=2
totalButtonCount=2 buttonOffset=0
*Sep 1 17:22:37.155: ephone-1[0/1][SEP0023331B9090]:Configured 0 speed dial buttons
*Sep 1 17:22:37.159: ephone-1[0/1]:StationSoftKeyTemplateReqMessage
*Sep 1 17:22:37.159: ephone-1[0/1]:StationSoftKeyTemplateReqMessage
*Sep 1 17:22:37.171: ephone-1[0/1]:StationSoftKeySetReqMessage
*Sep 1 17:22:37.171: ephone-1[0/1]:StationSoftKeySetReqMessage
*Sep 1 17:22:37.175: ephone-1[0/1][SEP0023331B9090]:StationLineStatReqMessage from
ephone line 2
*Sep 1 17:22:37.175: ephone-1[0/1][SEP0023331B9090]:StationLineStatReqMessage from
ephone line 2 Invalid DN -1
*Sep 1 17:22:37.175: ephone-1[0/1][SEP0023331B9090]:StationLineStatResMessage sent
to ephone (1 of 2)
*Sep 1 17:22:37.175: ephone-1[0/1][SEP0023331B9090]:StationLineStatReqMessage from
ephone line 1
*Sep 1 17:22:37.179: ephone-1[0/1]:StationLineStatReqMessage ephone line 1 DN 1 =
1000 desc = 1000 label =
```

Troubleshooting Video Issues in a Converged Network

Section Overview

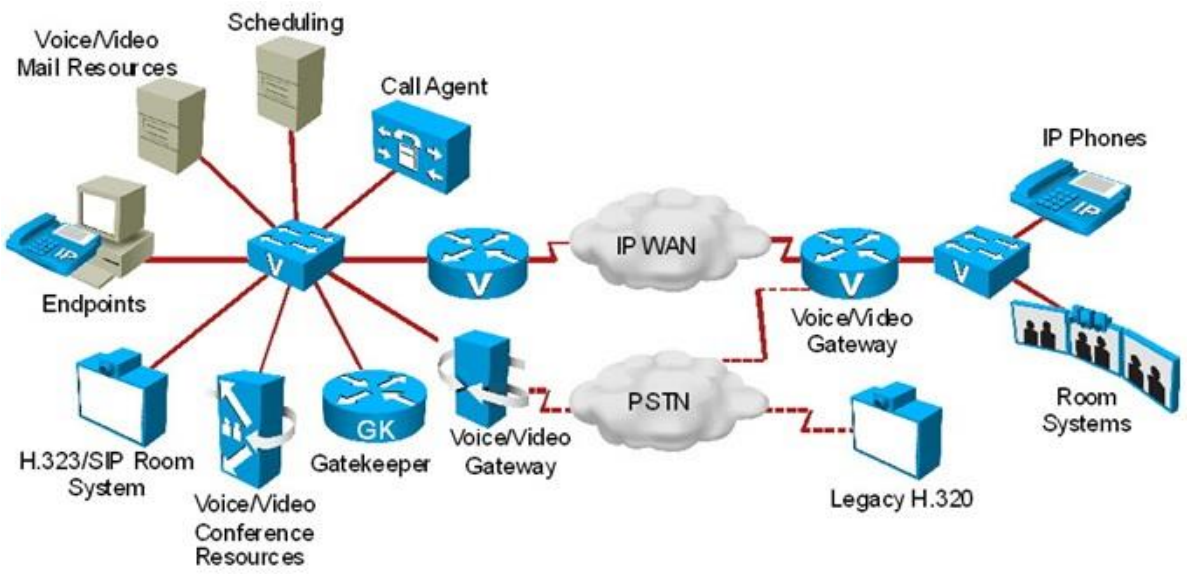
- This section addresses the challenge of troubleshooting the network infrastructure supporting video and rich media traffic.
- Several media-rich applications are available for enterprises:
  - High-definition room-based interactive video such as Cisco TelePresence
  - Standard-definition desktop collaboration applications such as Cisco Unified Videoconferencing Systems.
- Streaming and broadcast types of video applications include:
  - Digital signage
  - Video on demand (VoD)
  - Video surveillance.
- Video applications have different characteristics in terms of:
  - Interactivity
  - Network traffic volume
  - Audience
  - Requirements for underlying network infrastructure and services.

Troubleshooting Video Issues in a Converged Network: Video Application Types



Common Video-Integration Issues

- Several components and infrastructure services are shared between video and voice applications.
- Sometimes the endpoints are the same, or at least integrated and some of the critical protocols, such as SIP, are also the same.
- SIP is a signaling protocol that is used to initiate, manage, and terminate voice calls but also video sessions.
- The end user experiences an integrated service.
- Devices s ere.



Common Video-Integration Issues

- Both Video and voice applications need end-to-end QoS.
- Video is much more bandwidth intensive and very bursty.
- A high-definition stream can require more than 20-Mbps bandwidth for delivery over the network.
- Video packet sizes are much larger.
- Each type of video application has unique requirements and characteristics.
- The table shows the QoS requirements for some of the main video applications.

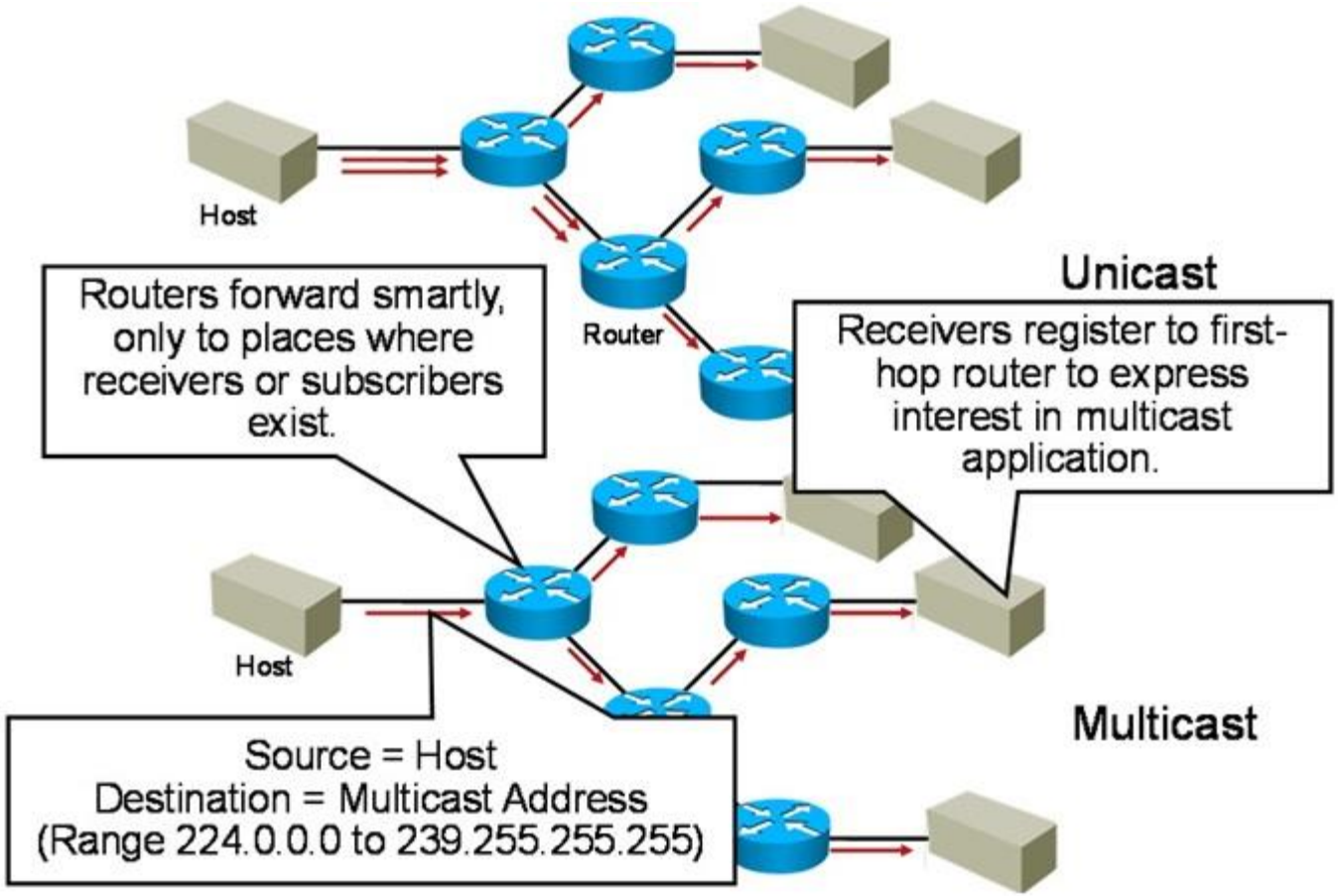
Metric	Video Collaboration	Cisco TelePresence	Video Surveillance
Latency	200 ms	150 ms	500 ms
Jitter	10 ms	10 ms	10 ms
Loss	0.05%	0.05%	0.5%

Common Video-Integration Issues – Cont.

- Video applications require high availability and millisecond-level network service recovery.
- Video traffic cannot accept unpredictable or large network recovery timeouts.
- Convergence targets will be higher, and packet loss due to network outage must be minimal.
- Redundancy design, convergence of routing protocols and spanning tree are extremely critical.
- Building a multicast-aware network is another important consideration.
- Security in a video-enabled network, similar to voice deployments, might need to permit protocols such as:
  - SIP
  - H.323
  - SCCP (Skinny)
  - RTP
  - RTCP
  - Possibly others

Multicast Operation

Multicast traffic is used to send the same data packets to multiple receivers efficiently. If unicast were used, the transmitter would send one copy for each receiver.

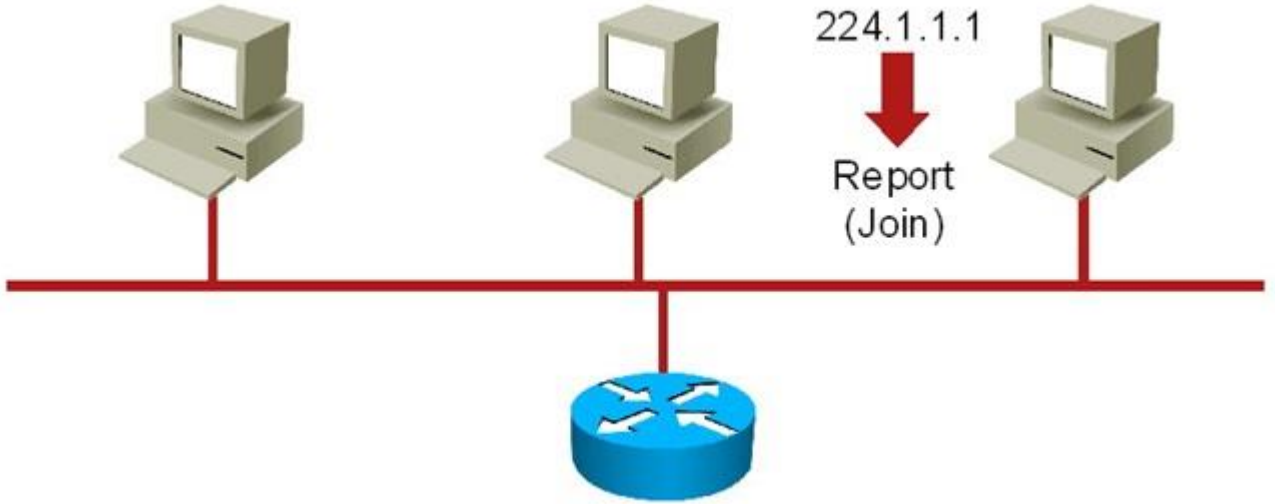


Multicast Operation – Cont.

- The sender sends only one copy of a single data packet addressed to a group of receivers.
- Multicast groups IP addresses that use the Class D address space.
- Class D addresses are denoted by the high-order 4 bits of the address set to 1110. This results in the range of addresses 224.0.0.0 through 239.255.255.255.
- Downstream multicast routers replicate and forward the data packet to all those branches where subscribers exist.
- Receivers express their interest in multicast traffic by registering at their first-hop router.
- This model and resulting protocols saves reduces resource utilization on routers and switches and improves QoS and the user experience.
- There are two main protocols involved:
  - **Protocol Independent Multicast (PIM)** – routers advertise multicast receivers
  - **Internet Group Management Protocol (IGMP)** – receivers subscribe to and leave groups

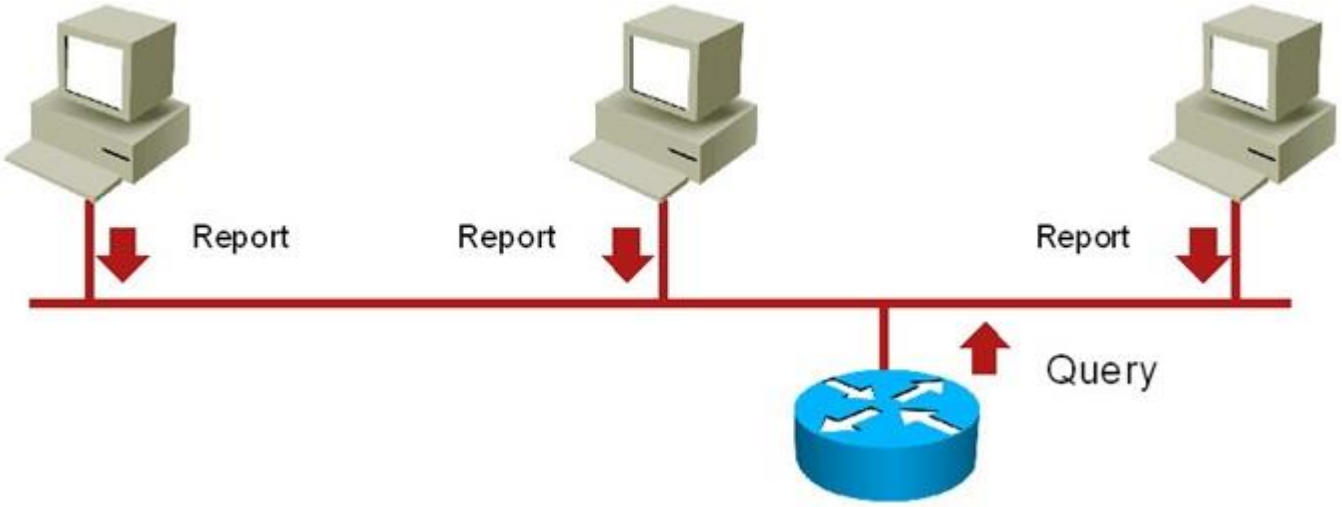
Multicast Operation – Cont.

- The figure illustrates a multicast client joining a multicast group using IGMP.
- Members joining a multicast group send an unsolicited report indicating their interest.
- This action reduces join latency for the end system joining if no other members are present.
- Once the Membership Report is received by the router, it advertises to the rest of the network.
- Multicast sources will forward traffic directed to the group to this router.



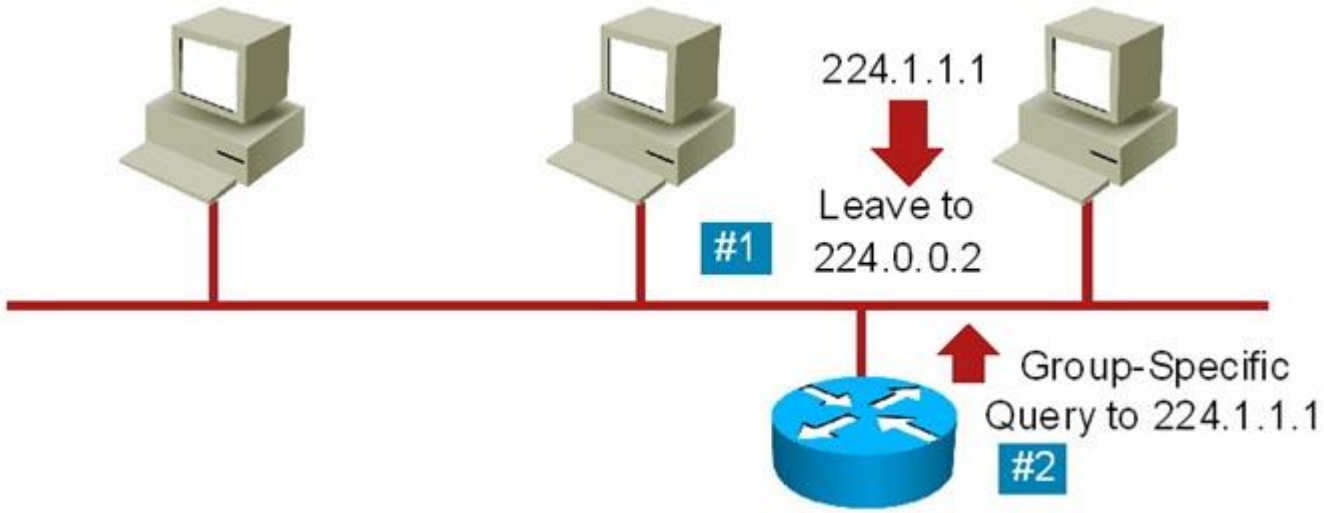
Multicast Operation – Cont.

- The multicast group remains active and is advertised by the router as long as there are members in the group within that network segment.
- As long as there is at least one member, the group will remain active.



Multicast Operation – Cont.

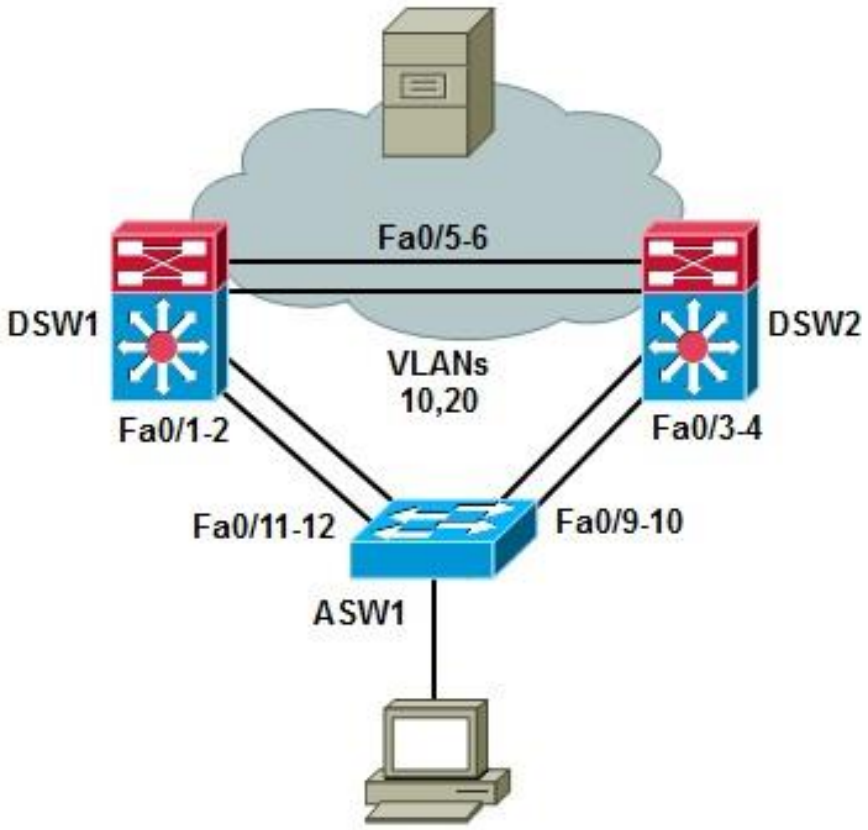
- When a user terminates a multicast-based application the application sends a “leave” message to the router.
- The router then sends a query, just to verify whether there are still members of the group in the segment.
- If a device replies, the group remains active and the router advertises it.
- If no reports are received, the router stops advertising the group to the r



Troubleshooting Video Integration Issues

- Common video-integration issues include the following:
  - Excessive bandwidth utilization
  - Poor quality (lack of QoS)
  - Security issues (filtering of key protocols, and stateful requirements)
  - Multicast issues
- QoS is a common problem due to the bursty nature of video traffic
- Video traffic tends to monopolize the available bandwidth but is also delay-sensitive.
- Network security can interfere with video traffic. Firewalls, ACLs, and other security controls can get in the way of protocols such as RTP, RTCP, SIP, H.323, and others.
- Multicast configuration, if enabled in the network, is always a source of potential issues.
  - Common IGMP problems are related to group filtering, where routers might not accept join request from certain multicast group addresses.
  - Another potential multicast issue is related to differences in IGMP versions between the router and the hosts sending multicast traffic.

Video-Integration Troubleshooting Example 1: Performance Issues Due to STP Topology



Video Troubleshooting Example 1 – Cont.

- Users are complaining about “poor” performance of their video application.
- In the switched network in the figure the video clients reside in two VLANS, 10 and 20, implemented in the access switch.
- The access switch is serviced by two distribution switches that connect the clients to the campus network, where the video server resides.
- The distribution switches have recently been upgraded to a new version of Cisco IOS Software.
- After the change, users started complaining about the poor performance.
- The exact symptoms, as told by the users of the application is choppy video, long download and buffering times, and that streaming video stops every few seconds for the application to buffer video frames.

Video Troubleshooting Example 1 – Cont.

The **`show interfaces status`** command indicates the four trunks connecting this switch to the distribution layer switches are connected and trunking.

```
ASW1# show interfaces status
Port      Name      Status    vlan    Duplex    Speed   Type
Fa0/1               disabled  1         auto     auto   10/100BaseTX
Fa0/2               disabled  1         auto     auto   10/100BaseTX
Fa0/3             connected  10      a-full    a-100   10/100BaseTX
Fa0/4               disabled  1         auto     auto   10/100BaseTX
Fa0/5               disabled  1         auto     auto   10/100BaseTX
Fa0/6               disabled  1         auto     auto   10/100BaseTX
Fa0/7               disabled  1         auto     auto   10/100BaseTX
Fa0/8               disabled  1         auto     auto   10/100BaseTX
Fa0/9    To DSW2  connected trunk a-full a-100 10/100BaseTX
Fa0/10   To DSW2  connected trunk a-full a-100 10/100BaseTX
Fa0/11   To DSW1  connected trunk a-full a-100 10/100BaseTX
Fa0/12   To DSW1  connected trunk a-full a-100 10/100BaseTX
Fa0/13              disabled  1         auto     auto   10/100BaseTX
<output omitted>
```

Video Troubleshooting Example 1 – Cont.

The **`show interfaces switchport`** command on trunk interface Fa0/9 shows that all VLANs are allowed and the interface is enabled and active. This trunk is a member of an EtherChannel bundle, port channel 1.

```
ASW1# show interfaces fa0/9 switchport
Name: Fa0/9
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk (member of bundle Po1)
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: on
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<output omitted>
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Video Troubleshooting Example 1 – Cont.

Use the **`show etherchannel summary`** command on ASW1. The output shows two bundles, one for each distribution layer switch.

```
ASW1# show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3 S - Layer2
        U - in use f - failed to allocate aggregator
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 2
Number of aggregators: 2

Group   Port-channel   Protocol    Ports
------------------------------------------------------
1       Po1(SU)            -       Fa0/9(P)  Fa0/10(P)
2       Po2(SU)            -       Fa0/11(P) Fa0/12(P)
```

Video Troubleshooting Example 1 – Cont.

The **`show interfaces po1`** command indicates traffic and utilization levels for port channel 1 (interfaces Fa0/9 and Fa0/10) are low.

```
ASW1# show interfaces po1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 001b.0c91.7f8a (bia 001b.0c91.7f8a)
  Description: TO DSW2
  MTU 1500 bytes, BW 200000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 100Mb/s, link type is auto, media type is unknown
  input flow-control is off, output flow-control is unsupported
  Members in this channel: Fa0/9 Fa0/10
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 02:34:07, output hang never
  Last clearing of "show interface" counters 01:16:51
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 619000 bits/sec, 59 packets/sec
  5 minute output rate 616000 bits/sec, 54 packets/sec
     275043 packets input, 354702160 bytes, 0 no buffer
     Received 23141 broadcasts (0 multicast)
--More--
```

Video Troubleshooting Example 1 – Cont.

The **`show interfaces po2`** command indicates the 5 minute packet output rate for port channel 2 (interfaces Fa0/11 and Fa0/12) is 0.

```
ASW1# show interfaces po2
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 001b.0c91.7f8a (bia 001b.0c91.7f8a)
  Description: TO DSW1
  MTU 1500 bytes, BW 200000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 100Mb/s, link type is auto, media type is unknown
  input flow-control is off, output flow-control is unsupported
  Members in this channel: Fa0/11 Fa0/12
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 02:35:01, output hang never
  Last clearing of "show interface" counters 01:17:38
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 2000 bits/sec, 4 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     24200 packets input, 1796256 bytes, 0 no buffer
     Received 23272 broadcasts (0 multicast)type: ARPA, ARP Timeout 04:00:00
```

Video Troubleshooting Example 1 – Cont.

The **`show interfaces trunk`** command indicates Po2 allows all VLANs but none are in forwarding state. The port is in Blocking state for all the VLANs. The built-in network redundancy is not set up correctly. Only one of the two uplinks is being used.

```
ASW1# show int trunk
Port        Mode Encapsulation Status Native vlan
Po1         on 802.1q trunking 1
Po2         on 802.1q trunking 1

Port        vlans allowed on trunk
Po1         1-4094
Po2         1-4094

Port        vlans allowed and active in management domain
Po1         1, 10, 20, 30, 40, 50, 60
Po2         1, 10, 20, 30, 40, 50, 60

Port        vlans in spanning tree forwarding state and not pruned
Po1         1, 10, 20, 30, 40, 50, 60
Po2         none
```

Video Troubleshooting Example 1 – Cont.

The **`show spanning-tree blockedports`** command confirms that all VLANs are blocking on port channel 2.

```
ASW1# show spanning-tree blockedports
Name          Blocked Interfaces List
____________  ____________________

VLAN0001      Po2
VLAN0010      Po2
VLAN0020      Po2
VLAN0030      Po2
VLAN0040      Po2
VLAN0050      Po2
VLAN0060      Po2
Number of blocked ports (segments) in the system : 7
```

Video Troubleshooting Example 1 – Cont.

The **`show spanning-tree summary`** command reveals that the spanning-tree mode is Rapid PVST. You need to find out why the switch is choosing to block all VLANs on Po2.

```
ASW1# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short
Name            Blocking Listening Learning Forwarding STP Active
VLAN0001               1         0        0          1          2
VLAN0010               1         0        0          2          3
VLAN0020               1         0        0          1          2
VLAN0030               1         0        0          1          2
VLAN0040               1         0        0          1          2
```

Video Troubleshooting Example 1 – Cont.

The **`show spanning-tree root`** command indicates that the root ID is the same for all VLANs. Po1 is the selected root port for all VLANs, which means Po2 is the alternate port for all VLANs.

```
ASW1# show spanning-tree root
                                        Root    Hello  Max   Fwd   Root Port
vlan         Root ID                    Cost    Time   Age   Dly
-----------  -------------------- -----  -------  ----  ----  ---------
VLAN0001     32769 0012.7f4b.ba80    12       2     20    15   Po1
VLAN0010     32769 0012.7f4b.ba80    12       2     20    15   Po1
VLAN0020     32769 0012.7f4b.ba80    12       2     20    15   Po1
VLAN0030     32769 0012.7f4b.ba80    12       2     20    15   Po1
VLAN0040     32769 0012.7f4b.ba80    12       2     20    15   Po1
VLAN0050     32769 0012.7f4b.ba80    12       2     20    15   Po1
VLAN0060     32769 0012.7f4b.ba80    12       2     20    15   Po1
```

Video Troubleshooting Example 1 – Cont.

Use the **`show spanning-tree root`** command on DSW1 indicates it has no Root Port for any VLAN. DSW1 is the root for all VLANs.

```
DSW1# show spanning-tree root
                                        Root    Hello  Max   Fwd   Root Port
vlan         Root ID                    Cost    Time   Age   Dly
-----------  -------------------- -----  -------  ----  ----  ---------
VLAN0001     32769 0012.7f4b.ba80    0      2     20    15
VLAN0010     32769 0012.7f4b.ba80    0      2     20    15
VLAN0020     32769 0012.7f4b.ba80    0      2     20    15
VLAN0030     32769 0012.7f4b.ba80    0      2     20    15
VLAN0040     32769 0012.7f4b.ba80    0      2     20    15
VLAN0050     32769 0012.7f4b.ba80    0      2     20    15
VLAN0060     32769 0012.7f4b.ba80    0      2     20    15
```

Video Troubleshooting Example 1 – Cont.

- To correct the problem, you can designate DSW1 as the root for VLANs 10, 30, and 50, and DSW2 as the root for VLANs 20, 40, and 60.
- There is an IOS macro that allows you to specify the switch to be the primary or the back up root for one or more VLANs.
- Use that macro to make DSW1 the primary root for VLANs 10, 30, and 50, and to make it secondary root for VLANs 20, 40, and 60. Do the opposite on the DSW2 switch.

```
DSW1(config)# spanning-tree vlan 10,30,50 root primary
DSW1(config)# spanning-tree vlan 20,40,60 root secondary
DSW1(config)#

==========================================================

DSW2(config)# spanning-tree vlan 10,30,50 root secondary
DSW2(config)# spanning-tree vlan 20,40,60 root primary
DSW2(config)#
```

Video Troubleshooting Example 1 – Cont.

After STP reconverges, reissue previous commands. STP is blocking for the correct VLANs on Po1 and Po2 and the Root Port varies based on VLAN.

```
ASW1# show spanning-tree blockedports
Name          Blocked Interfaces List
----------    ----------------------
VLAN0001      Po2
VLAN0010      Po2
VLAN0020      Po1
VLAN0030      Po2
VLAN0040      Po1
VLAN0050      Po2
VLAN0060      Po1
Number of blocked ports (segments) in the system : 7

ASW1# show spanning-tree root
                                        Root    Hello  Max   Fwd   Root Port
vlan         Root ID                    Cost    Time   Age   Dly
-----------  -------------------- -----  -------  ----  ----  ---------
VLAN0001     32769 0012.7f4b.ba80    12       2     20    15   Po1
VLAN0010     32769 0012.7f4b.ba80    12       2     20    15   Po1
VLAN0020     32769 0012.7f4b.ba80    12       2     20    15   Po2
VLAN0030     32769 0012.7f4b.ba80    12       2     20    15   Po1
VLAN0040     32769 0012.7f4b.ba80    12       2     20    15   Po2
VLAN0050     32769 0012.7f4b.ba80    12       2     20    15   Po1
VLAN0060     32769 0012.7f4b.ba80    12       2     20    15   Po2
```

Video Troubleshooting Example 1 – Cont.

Recheck traffic statistics on Po1 and Po2. Both links are now being used somewhat evenly, as shown in the output.

```
ASW1# show int po1 | include rate
Queueing strategy: fifo
5 minute input rate 1443000 bits/sec, 143 packets/sec
5 minute output rate 1501000 bits/sec, 272 packets/sec


ASW1# show int po2 | include rate
Queueing strategy: fifo
5 minute input rate 1163000 bits/sec, 107 packets/sec
5 minute output rate 1162000 bits/sec, 103 packets/sec
```

Video Troubleshooting Example 1 – Cont.

- Verify that the network is resilient to a failure on these links (one at the time).
- Shut down both ports in the Po1 EtherChannel bundle.
- Spanning tree should reconverge and unblock ports.
- The output from the **`show spanning-tree blockedports`** command indicates that no ports are blocked after the link failure.

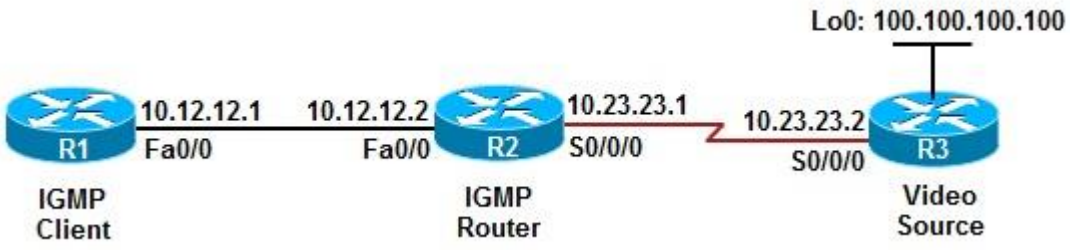
```
ASW1(config)# interface range fa0/9-10
ASW1(config-if-range)#shutdown
ASW1(config-if-range)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to
down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-3-UPDOWN: Interface Port-channel1, changed state to down
ASW1#


ASW1# show spanning-tree blockedports
Name Blocked Interfaces List
-------------------- ------------------------------------
Number of blocked ports (segments) in the system : 0
```

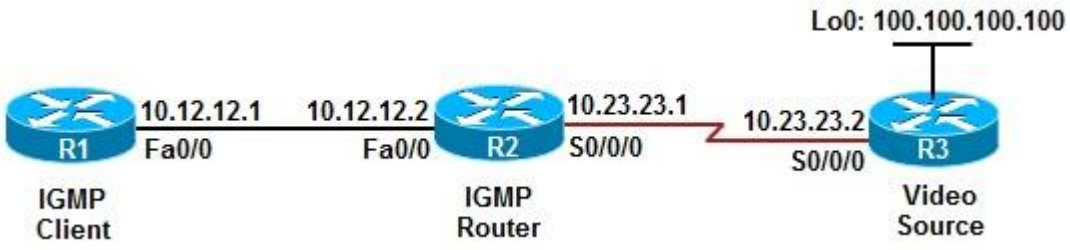
Example 2: IP Multicast Configuration Error

- This network simulates an IGMP network, with R1 acting as an IGMP client, similar to a PC running a video application and joining multicast groups.
- R2 acts as the first-hop router, listening to IGMP join and leave transactions.
- R3 acts as the video server, pushing multicast traffic downstream. The video server is simulated by the loopback interface on R3.
- R2 and R3 are preconfigured to communicate multicast group information through Protocol Independent Multicast (PIM).
- R1 and R2 are preconfigured to use IGMP to allow R1 to join multicast groups.



Video Troubleshooting Example 2 – Cont.

- The problem is that users in the R1 LAN are not able to watch the video stream.
- They are able to connect to the server and request the video, but the video stream is not reaching them after that.
- The application team has verified that the software is installed correctly and the server is configured properly, and they suspect the network is to blame.
- The video application is the only one that is not working so IP reachability and routing issues are not likely the problem.



Video Troubleshooting Example 2 – Cont.

- This is a multicast issue and end devices must join a multicast group before they can receive traffic directed to that group.
- On R2, use the **`show ip igmp groups`** command to see the multicast groups the hosts in this LAN have joined.
- R1 is not joining any group. The group in the example output is on the S0/0/0 interface, while R1 is on the LAN interface Fa0/0.

```
R2# show ip igmp group
IGMP Connected Group Membership
Group Address  Interface   Uptime    Expires  Last Reporter Group Accounted
224.0.1.40     Serial0/0/0 00:08:48  Stopped  10.23.23.2
```

Video Troubleshooting Example 2 – Cont.

The **`show ip igmp membership`** command, which shows all members of all groups, does not list the IP address of R1 (10.12.12.1) anywhere.

```
R2# show ip igmp membership
Flags:  A - aggregate, T - tracked
        L - Local, S - static, V - virtual, R - Reported through v3
        I - v3lite, U - Urd, M - SSM (S,G) channel
        1,2,3 - The version of IGMP the group is in

Channel/Group-Flags:
        / - Filtering entry (Exclude mode (S,G), Include mode (*,G)
Reporter:
        <mac-or-ip-address> - last reporter if group is not explicitly tracked
        <n>/<m> - <n> reporter in include mode, <m> reporter in exclude

Channel/Group      Reporter    Uptime    Exp    Flags    Interface
*.224.0.1.40       10.23.23.2  00:09:24  stop   2LA      Se0/0/0
```

Video Troubleshooting Example 2 – Cont.

- Activate **`debug ip igmp`** on R2.
- From R1 to simulate joining a group by entering the command **`ip igmp joingroup`**.
- The debug output on R2 shows no activity.

```
R2# debug ip igmp
IGMP debugging is on
R2#


R1# config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface fa0/0
R1(config-if)# ip igmp join-group 224.8.8.8
R1(config-if)#
```

Video Troubleshooting Example 2 – Cont.

On R2, the only interface where IGMP Is enabled is S0/0/0. IGMP is not enabled on R2's Fa0/0 interface so R1 could not join the multicast group.

```
R2# show ip igmp interface
Serial0/0/0 is up, line protocol is up
  Internet address is 10.23.23.2/24
  IGMP is enabled on interface
  Current IGMP host version is 2
  Current IGMP router version is 2
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Last member query count is 2
  Last member query response interval is 1000 ms
  Inbound IGMP access group is not set
  IGMP activity: 1 joins, 0 leaves
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  IGMP querying router is 0.0.0.0 (this system)
  Multicast groups joined by this system (number of users):
     224.0.1.40(1)
```

Video Troubleshooting Example 2 – Cont.

Configure IGMP on router R2's Fa0/0 interface by enabling PIM on this interface. The **debug** output shows R2 sending IGMP Version 2 query and receiving a report from R1 (10.12.12.1 joining the multicast group 224.8.8.8).

```
R1# config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface fa0/0
R1(config-if)# ip pim sparse-dense-mode
R1(config-if)#

R2#
IGMP(0): Send v2 init Query on FastEthernet0/0
%PIM-5-DRCHG: Dr change from neighbor 0.0.0.0 to 10.12.12.2 on interface
FastEthernet0/0
IGMP(0): Received v2 Report on FastEthernet0/0 from 10.12.12.1 for 224.8.8.8
IGMP(0): Received Group record for group 224.8.8.8, mode 2 from 10.12.12.1 for
0
sources
IGMP(0): WAVL Insert group: 224.8.8.8 interface: FastEthernet0/0Successful
IGMP(0): Switching to EXCLUDE mode for 224.8.8.8 on FastEthernet0/0
IGMP(0): Updating EXLUDE group timer for 224.8.8.8
IGMP(0): MRT Add/Update FastEthernet0/0 for (*,224.8.8.8) by 0
```

Video Troubleshooting Example 2 – Cont.

IGMP Is now enabled on both the R2 S0/0/0 and Fa0/0 Interfaces.

```
R2# show ip igmp interface
Serial0/0/0 is up, line protocol is up
Internet address is 10.23.23.2/24
IGMP is enabled on interface
Current IGMP host version is 2
Current IGMP router version is 2
IGMP query interval is 60 seconds
<output omitted>

FastEthernet0/0 is up
Internet address is 10.12.12.2/24
IGMP is enabled on interface
Current IGMP host version is 2
Current IGMP router version is 2
IGMP query interval is 60 seconds
<output omitted>
```

Video Troubleshooting Example 2 – Cont.

Multicast group 224.8.8.8 is now known on Fa0/0 with last reporter as R1 (10.12.12.1). A Ping to the multicast address 224.8.8.8 from R3 receives a reply from R1.

```
R2# show ip igmp group
IGMP Connected Group Membership
Group      Interface         Uptime  Expires   Last Reporter  Group Accounted
Address
224.8.8.8  FastEthernet0/0   00:08:48 00:02:51  10.12.12.1
224.0.1.40 Serial0/0/0       00:19:43 stopped   10.23.23.2


R3# ping 224.8.8.8
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 224.8.8.8, timeout is 2 seconds:
Reply to request 0 from 10.12.12.1, 1 mss
```

Chapter 8 Summary: WLAN

- Troubleshooting a wireless network requires the following considerations:
  - Is the wireless network based on the autonomous model or the split MAC (lightweight) model?
  - What are the switch capabilities and requirements in terms of Power over Ethernet (PoE), trunking, WLAN-to-VLAN mapping, security, and quality of service (QoS)?
  - How will the Lightweight Access Point Protocol (LWAPP) be handled?
  - What type of roaming will the network support?
- Common wireless integration issues include:
  - Problems at the wireless to wired boundary:
    - Autonomous model - AP has a wired connection to a switch.
    - Split MAC model - Lightweight AP (LWAP) communicates with wireless LAN controller (WLC) using LWAPP.

Chapter 8 Summary: WLAN – Cont.

- Common wireless integration issues – Cont.
  - Filters might be blocking traffic:
    - Radio and Ethernet side of the APs must be checked
    - Filters might block LWAPP or security/authentication
    - LWAPP control uses UDP port 12223,and LWAPP data uses UDP port 12222.
  - Wireless QoS and wired QoS mapping might be incorrect: QoS markings must be maintained and remain consistent across wireless-to-wired boundaries.
  - PoE issues: The PoE supplied to the AP by the switch must be adequate.
  - Trunk issues: All trunks must be checked to make sure they allow appropriate VLANs.

Chapter 8 Summary: WLAN – Cont.

- Some useful switch troubleshooting commands to support wireless LANS are:
  - **`show interfaces switchport`**
  - **`show interfaces status`**
  - **`show interfaces trunk`**
  - **`show interface interface switchport`**
  - **`show access-lists`**

Chapter 8 Summary: Voice

- The design and troubleshooting considerations of integrating unified communications into a campus LAN are:
- **QoS:** Adequate trust boundaries, plus proper router and switch QoS configurations.
- **High availability:** Usage of resilient technologies such as RSTP and HSRP.
- **Security:** Implementation of voice VLAN(s) and accurate filters and firewall configurations.
- **Availability and correct provisioning of other services:** PoE, DHCP, TFTP, NTP, CDP, and so on.

Chapter 8 Summary: Voice – Cont.

- The IP phone boot process consists of these main steps:
  - Step 1. The IP phone powers on.
  - Step 2. The phone performs a power-on self-test (POST).
  - Step 3. The phone boots.
  - Step 4. The phone uses CDP to learn the voice VLAN.
  - Step 5. The phone initializes the IP stack.
  - Step 6. The IP phone sends DHCP requests to obtain an IP address.
  - Step 7. The DHCP server selects a free IP address from the pool and sends it, along with the other parameters, including option 150 (TFTP server).
  - Step 8. The IP phone initializes, applying the IP configuration to the IP stack.
  - Step 9. The IP phone requests a configuration file from the TFTP server defined in option 150.

Chapter 8 Summary: Voice – Cont.

- Useful converged network troubleshooting commands include the following:
  - **`show interface trunk`**
  - **`show interfaces switchport`**
  - **`show vlan`**
  - **`show errdisable recovery`**
  - **`show auto qos`**
  - **`show auto discovery qos`**
  - **`show ip dhcp pool`**
  - **`show ip dhcp server`**
  - **`show ntp status`**
  - **`debug ephone`**
  - **`show crypto engine connections active`**

Chapter 8 Summary: Video

Video-integration considerations and requirements are:

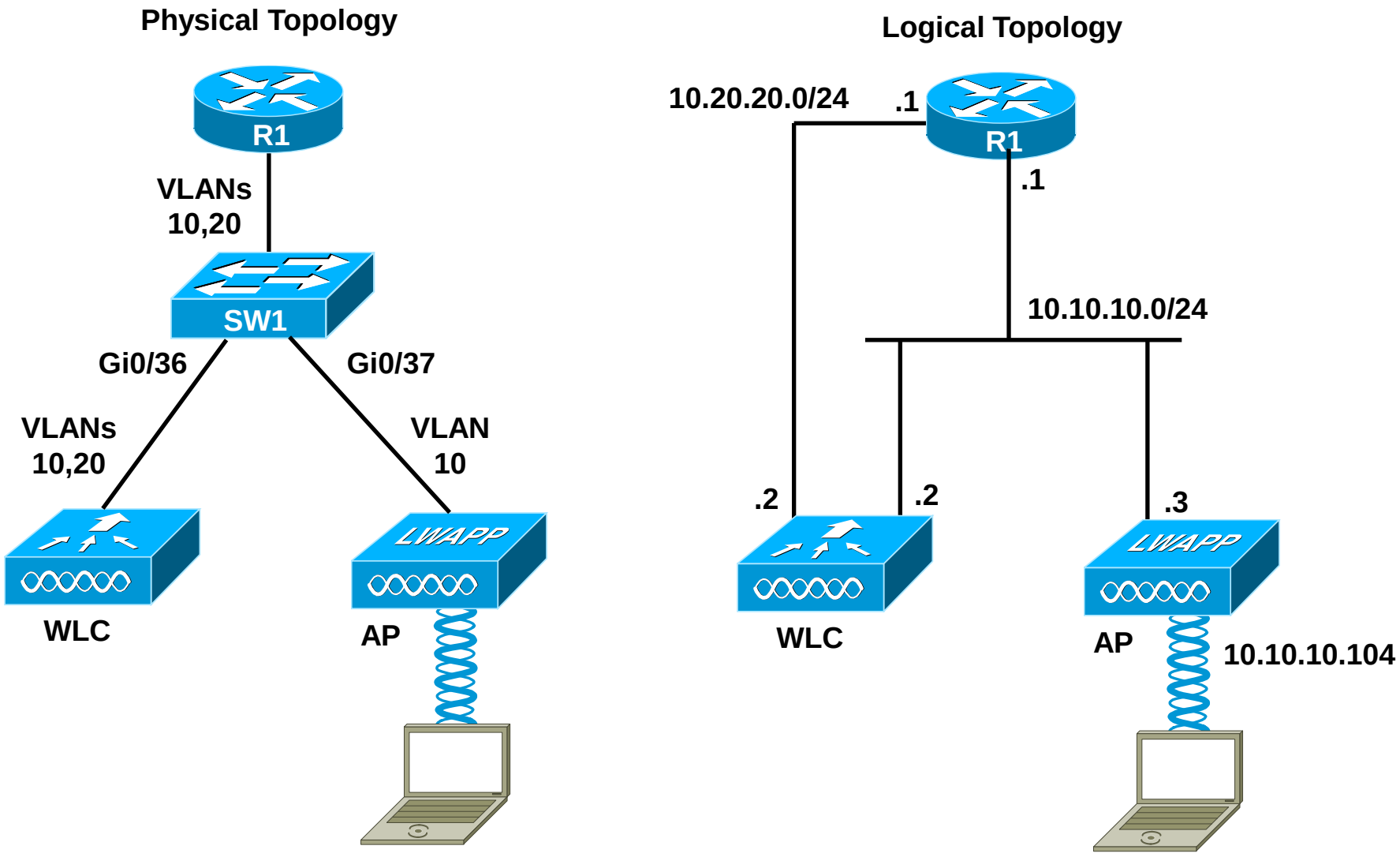
- **Quality of service**: QoS considerations for video are not quite the same as VoIP; video requires more bandwidth and can be bursty.
- **High availability**: Video applications require millisecond-level network service recovery because video traffic cannot withstand unpredictable or large network recovery timeouts.
- **Multicast**: Improper router and switch multicast (PIM, IGMP, and so on) configurations impede operation of multicast-based video applications.
- **Security**: Access control and threat management mechanisms must consider the various protocols and traffic flows that result from a video-enabled network and allow them in the network in a controlled manner.

Chapter 8 Summary: Video – Cont.

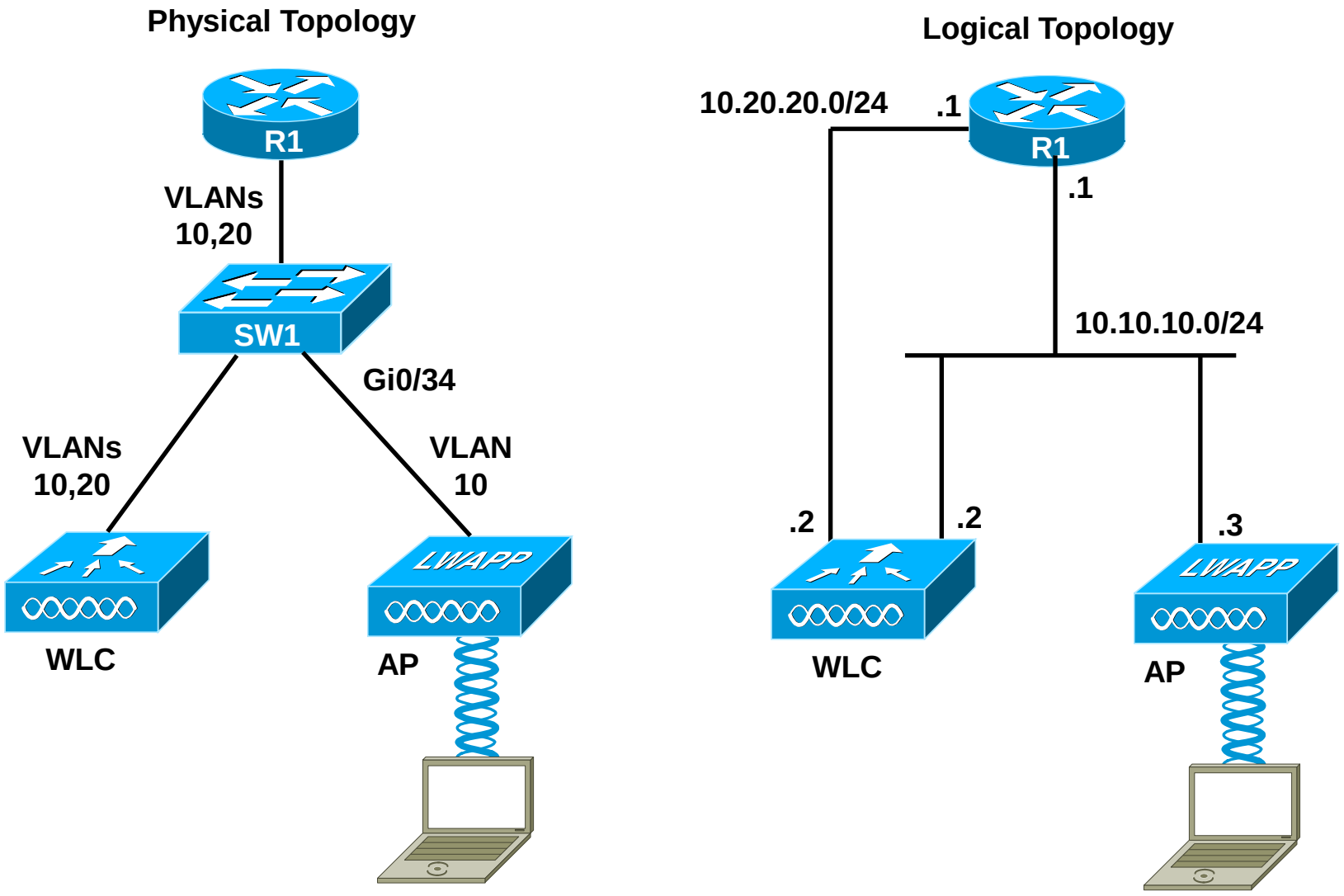
Common video-integration issues include the following:

- Excessive bandwidth utilization
- Lack of control
- Poor quality (lack of QoS)
- Security issues (filtering of key protocols, and stateful requirements)
- Multicast issues

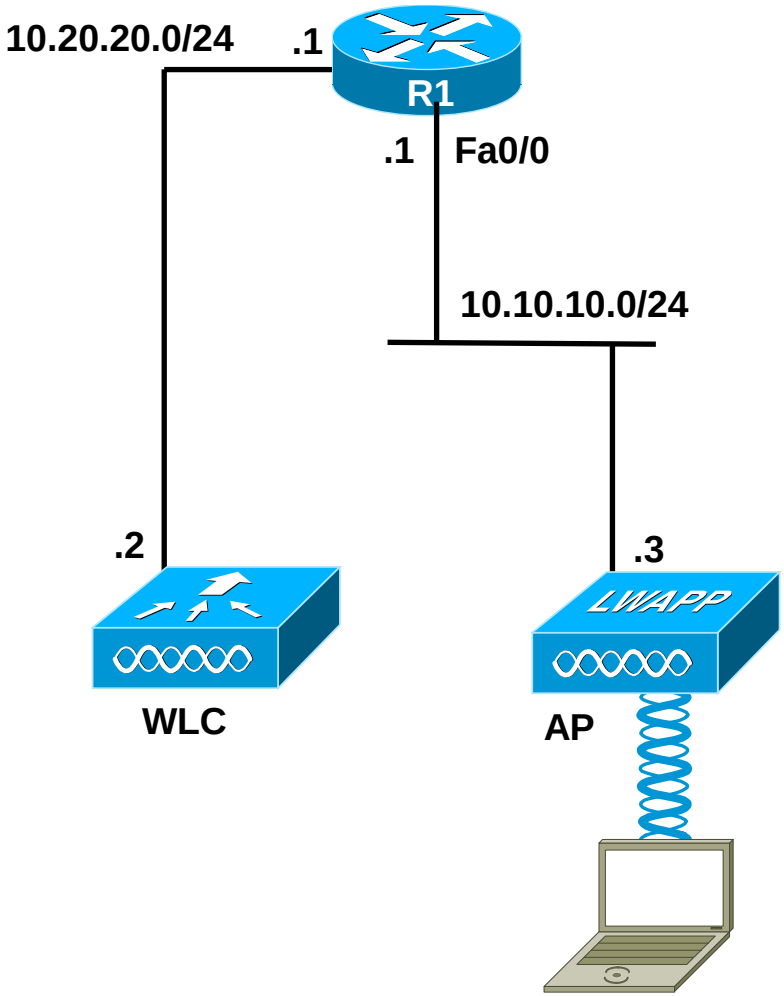
WLAN Troubleshooting Example 1



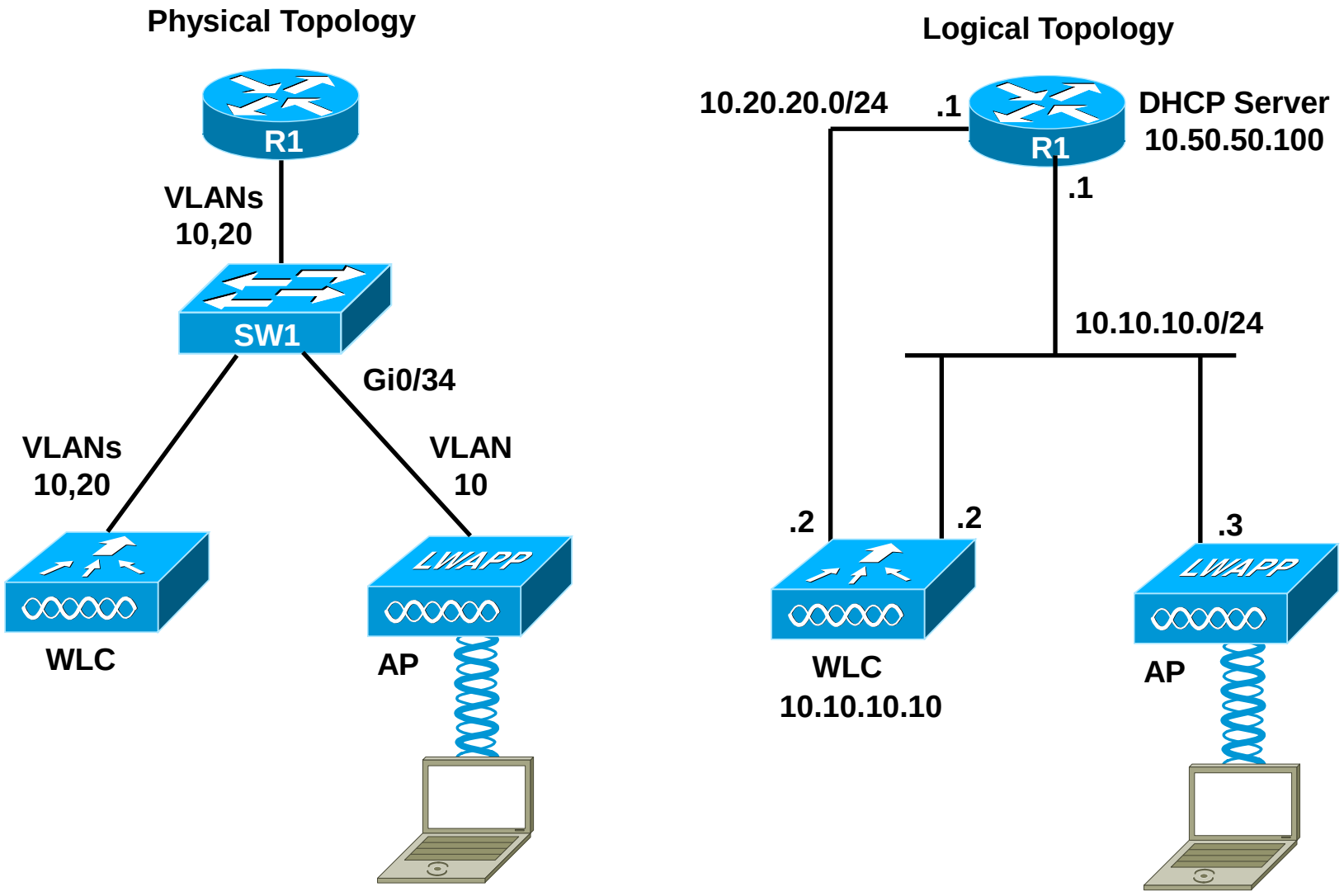
WLAN Troubleshooting Example 2



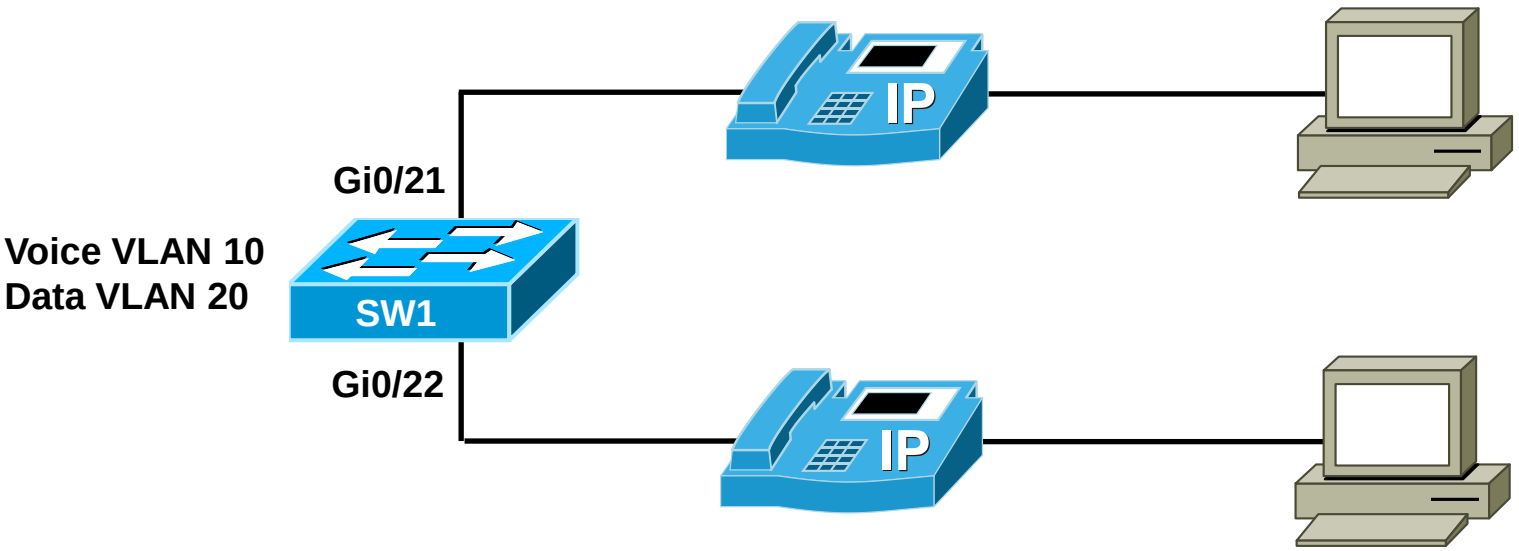
WLAN Troubleshooting Example 3



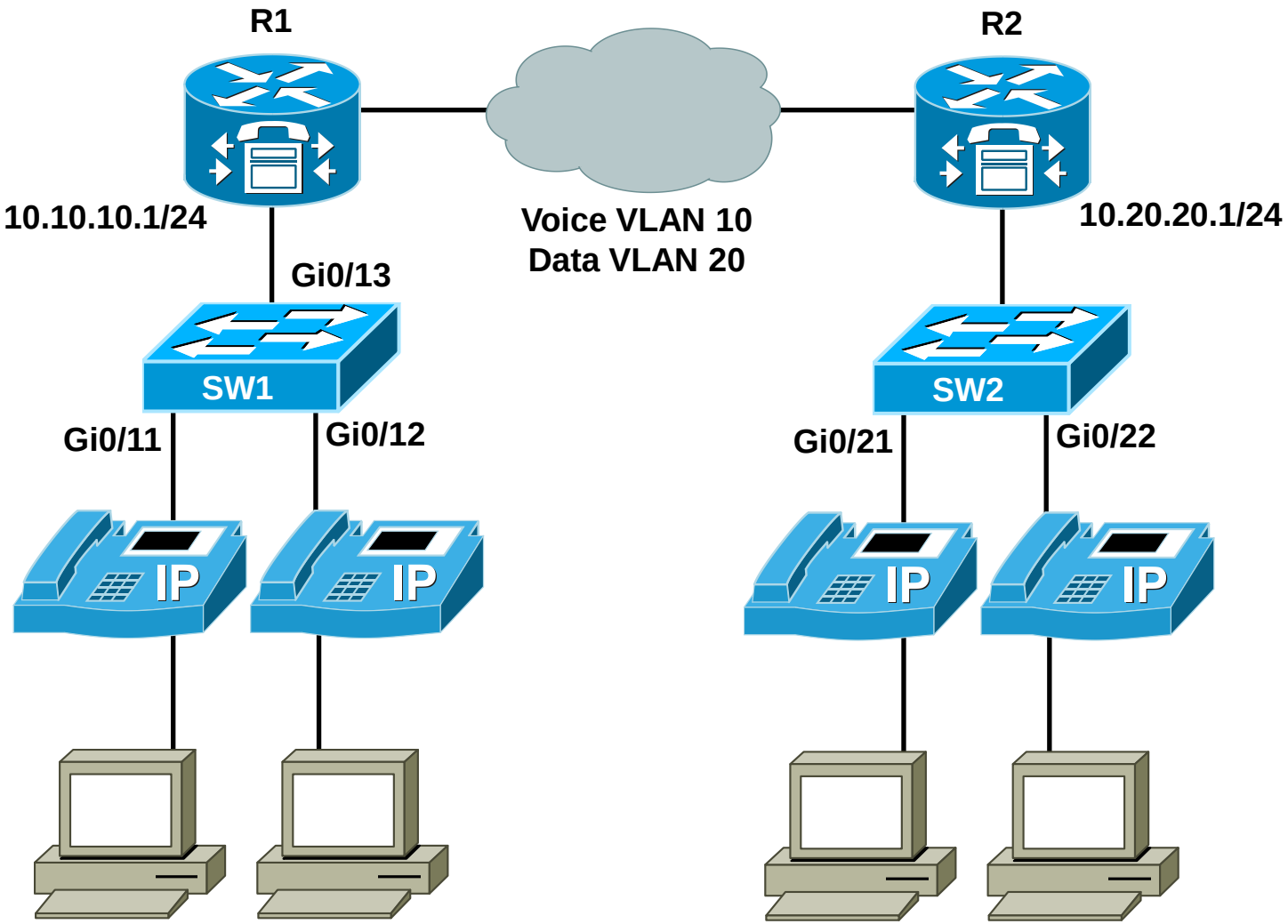
WLAN Troubleshooting Example 4



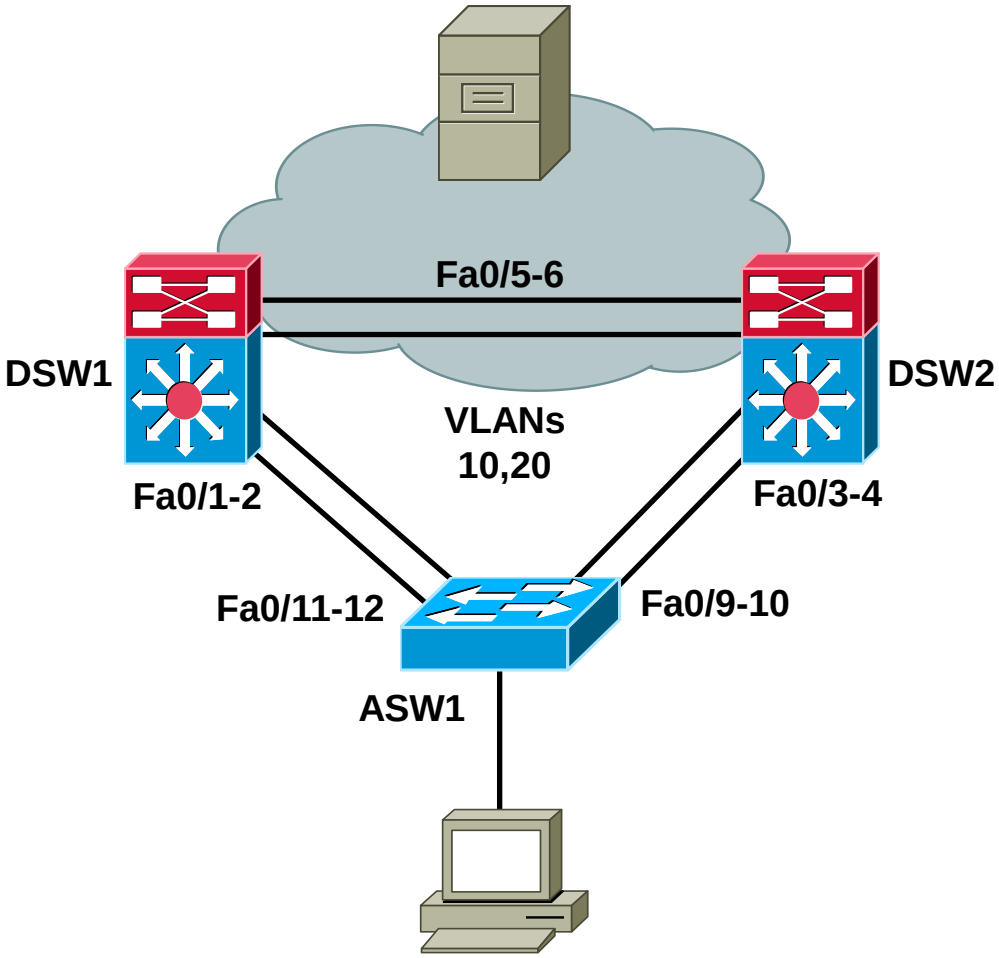
Unified Communications Troubleshooting Example 1



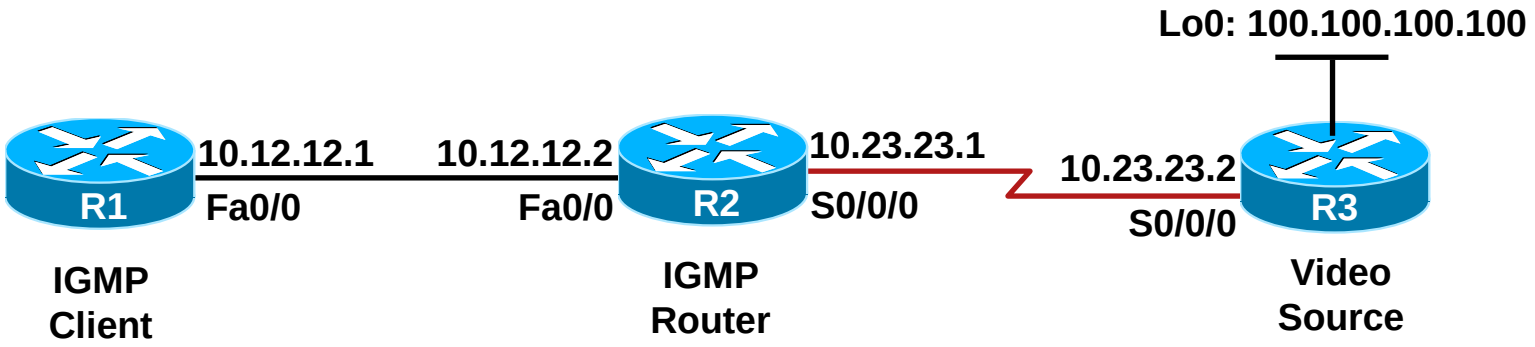
Unified Communications Troubleshooting Examples 2 & 3



Video Troubleshooting Example 1



Video Troubleshooting Example 2



.2

Slides adapted by Vladimír Veselý and Matěj Grégr
partially from official course materials
but the most of the credit goes to CCIE#23527 Ing. Peter Palúch, Ph.D.

Last update: 2012-09-09