CCNA 200-301 v1.1

MODULE 4 — IP Services

Complete Hands-on Training Labs

Topology • Sequential Device Configuration • Verification Output • Troubleshooting

NETWORK GUIDE ACADEMY

Instructor / Student Lab Guide

Scope: CCNA v1.1 Module 4 — IP Services objectives 4.1 through 4.10. The labs intentionally use one configuration path per device and then move forward to verification and troubleshooting

Module 4 lab map

Lab	Topic	Primary skill
4.1	NAT/PAT	Static NAT, dynamic pool NAT and PAT/overload
4.2	NTP	Server/master and client synchronization
4.3	DHCP and DNS roles	Address assignment and name resolution workflow
4.4	SNMP	Polling, MIB/OID concepts and traps
4.5	Syslog	Central logging, facilities and severity levels
4.6	DHCP client and relay	ip address dhcp and ip helper-address
4.7	QoS PHB	Classification, marking, queuing, policing and shaping
4.8	SSH	Secure remote CLI access
4.9	TFTP/FTP	Configuration backup and transfer
4.10	SPAN/RSPAN/ERSPAN	Supplemental operational traffic mirroring lab

How to use this workbook

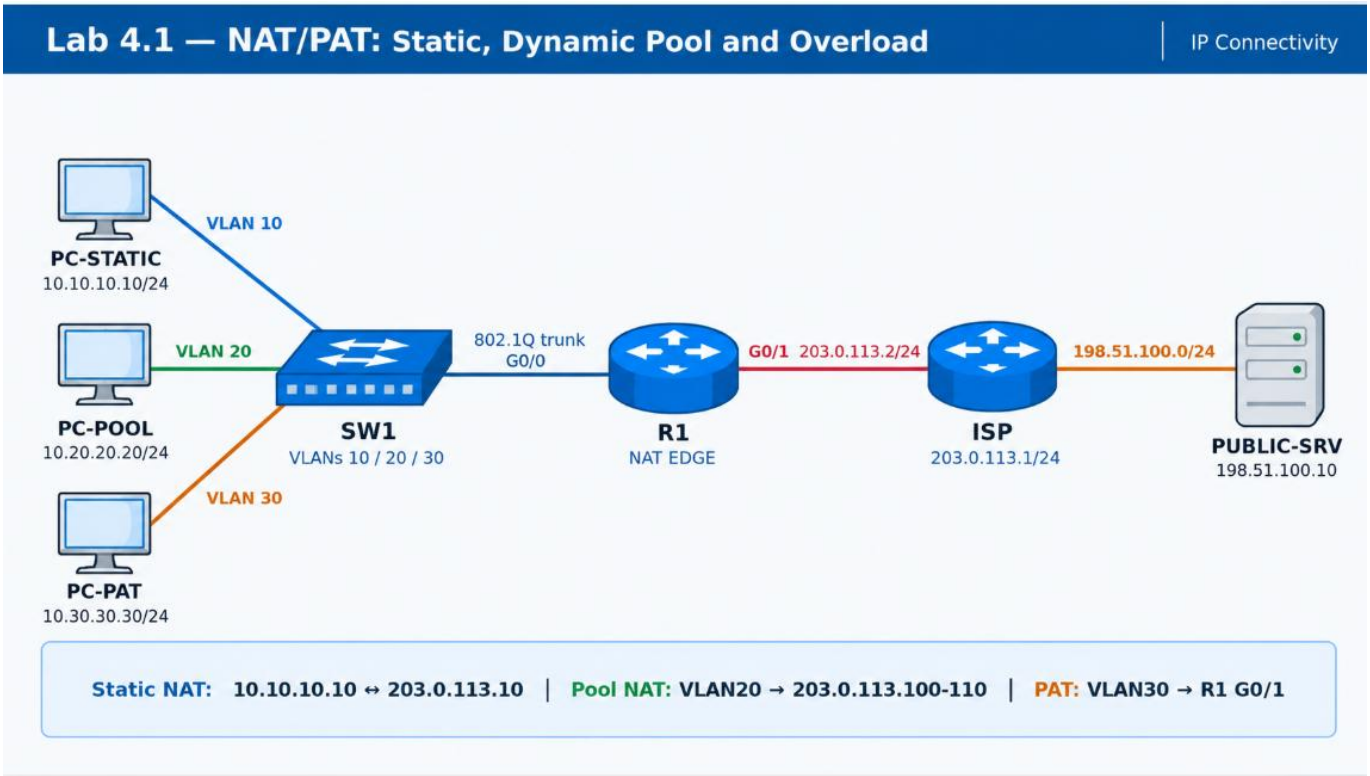
1. Build the topology exactly as shown and apply the addressing plan.
2. Configure devices in the order presented. Do not skip directly to later devices.
3. Run each verification command immediately after its related configuration.
4. Compare your output with the sample output and read the “What to verify” bullets.
5. Run the end-to-end test, then perform the controlled fault/recovery exercise where provided.

Exam alignment: Cisco CCNA 200-301 v1.1 lists IP Services objectives 4.1 through 4.9. Lab 4.10 is included as an operations-focused supplemental lab for traffic analysis and troubleshooting.

Lab 4.1 — NAT/PAT: Static, Dynamic Pool and Overload

Configure three distinct inside source translation methods on one edge router so each method can be verified independently without overlapping source subnets.

Lab topology



Addressing / device plan

Device / Interface	IP address	Gateway / next hop	Purpose
PC-STATIC	10.10.10.10/24	10.10.10.1	Static NAT host
PC-POOL	10.20.20.20/24	10.20.20.1	Dynamic pool source
PC-PAT	10.30.30.30/24	10.30.30.1	PAT source
R1 G0/1	203.0.113.2/24	203.0.113.1	NAT outside
ISP G0/0	203.0.113.1/24	—	Toward R1
ISP G0/1	198.51.100.1/24	—	Public server LAN
PUBLIC-SRV	198.51.100.10/24	198.51.100.1	Internet test server

Lab objectives

- Configure VLANs 10/20/30 and an 802.1Q router-on-a-stick inside interface.
- Configure static NAT for one server/host, dynamic pool NAT for VLAN 20 and PAT for VLAN 30.
- Verify translation type, inside local/global values, hit counters and end-to-end reachability.

Step 1 — Configure SW1

```
enable
configure terminal
hostname SW1
!
vlan 10
 name STATIC_NAT
vlan 20
 name DYNAMIC_POOL
vlan 30
 name PAT_USERS
!
interface GigabitEthernet0/1
 description TRUNK_TO_R1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30
 no shutdown
!
interface GigabitEthernet0/2
 description PC_STATIC
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
!
interface GigabitEthernet0/3
 description PC_POOL
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast
!
interface GigabitEthernet0/4
 description PC_PAT
 switchport mode access
 switchport access vlan 30
 spanning-tree portfast
end
write memory
```

SW1 verification

```
SW1# show interfaces trunk
Port        Mode   Encapsulation  Status     Native vlan
Gi0/1       on     802.1q         trunking   1

Port        Vlans allowed on trunk
Gi0/1       10,20,30

SW1# show vlan brief
10   STATIC_NAT      active   Gi0/2
20   DYNAMIC_POOL    active   Gi0/3
30   PAT_USERS       active   Gi0/4
```

What to verify

- Gi0/1 is trunking and carries VLANs 10, 20 and 30.
- Each PC access port is in the intended VLAN.

Step 2 — Configure R1 NAT edge

```
enable
configure terminal
hostname R1
!
interface GigabitEthernet0/0
 no shutdown
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.20.20.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.30.30.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/1
 description TO_ISP
 ip address 203.0.113.2 255.255.255.0
 ip nat outside
 no shutdown
!
ip route 0.0.0.0 0.0.0.0 203.0.113.1
!
! Static one-to-one translation
ip nat inside source static 10.10.10.10 203.0.113.10
!
! Dynamic pool translation for VLAN 20
ip access-list standard NAT-POOL-SOURCES
 permit 10.20.20.0 0.0.0.255
ip nat pool PUBLIC-POOL 203.0.113.100 203.0.113.110 netmask 255.255.255.0
ip nat inside source list NAT-POOL-SOURCES pool PUBLIC-POOL
!
! PAT/overload for VLAN 30
ip access-list standard PAT-SOURCES
 permit 10.30.30.0 0.0.0.255
ip nat inside source list PAT-SOURCES interface GigabitEthernet0/1 overload
end
write memory
```

R1 verification before traffic

```
R1# show ip interface brief | include GigabitEthernet0/0|GigabitEthernet0/1
GigabitEthernet0/0       unassigned      YES unset  up  up
GigabitEthernet0/0.10    10.10.10.1      YES manual up  up
GigabitEthernet0/0.20    10.20.20.1      YES manual up  up
GigabitEthernet0/0.30    10.30.30.1      YES manual up  up
GigabitEthernet0/1       203.0.113.2     YES manual up  up

R1# show ip nat translations
Pro  Inside global       Inside local       Outside local      Outside global
---  203.0.113.10        10.10.10.10        ---                ---
```

What to verify

- Inside subinterfaces are up/up and marked as NAT inside in the running configuration.
- The static mapping exists immediately, before any user traffic.
- Dynamic pool and PAT entries appear only after matching traffic is generated.

Step 3 — Configure ISP

```
enable
configure terminal
hostname ISP
interface GigabitEthernet0/0
 description TO_R1
 ip address 203.0.113.1 255.255.255.0
 no shutdown
interface GigabitEthernet0/1
 description PUBLIC_SERVER_LAN
 ip address 198.51.100.1 255.255.255.0
 no shutdown
end
write memory
```

Step 4 — Configure end devices

Device	IP / mask	Default gateway
PC-STATIC	10.10.10.10 /24	10.10.10.1
PC-POOL	10.20.20.20 /24	10.20.20.1
PC-PAT	10.30.30.30 /24	10.30.30.1
PUBLIC-SRV	198.51.100.10 /24	198.51.100.1

Step 5 — Generate traffic and verify translations

```
PC-STATIC> ping 198.51.100.10
Success rate is 100 percent

PC-POOL> ping 198.51.100.10
Success rate is 100 percent

PC-PAT> ping 198.51.100.10
Success rate is 100 percent

R1# show ip nat translations
Pro  Inside global      Inside local       Outside local      Outside global
icmp 203.0.113.10:12    10.10.10.10:12     198.51.100.10:12   198.51.100.10:12
icmp 203.0.113.100:7    10.20.20.20:7      198.51.100.10:7    198.51.100.10:7
icmp 203.0.113.2:31     10.30.30.30:31     198.51.100.10:31   198.51.100.10:31
---  203.0.113.10       10.10.10.10        ---                ---

R1# show ip nat statistics
Total active translations: 4 (1 static, 3 dynamic; 3 extended)
Outside interfaces:
  GigabitEthernet0/1
Inside interfaces:
  GigabitEthernet0/0.10, GigabitEthernet0/0.20, GigabitEthernet0/0.30
Hits: 27  Misses: 0
```

What to verify

- PC-STATIC uses inside global 203.0.113.10.
- PC-POOL receives an address from 203.0.113.100-110.
- PC-PAT shares 203.0.113.2 and is distinguished by a translated identifier/port.
- NAT hit counters increase when traffic crosses the router.

Controlled test — clear dynamic translations only

```
R1# clear ip nat translation *
R1# show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  203.0.113.10      10.10.10.10        ---                ---
```

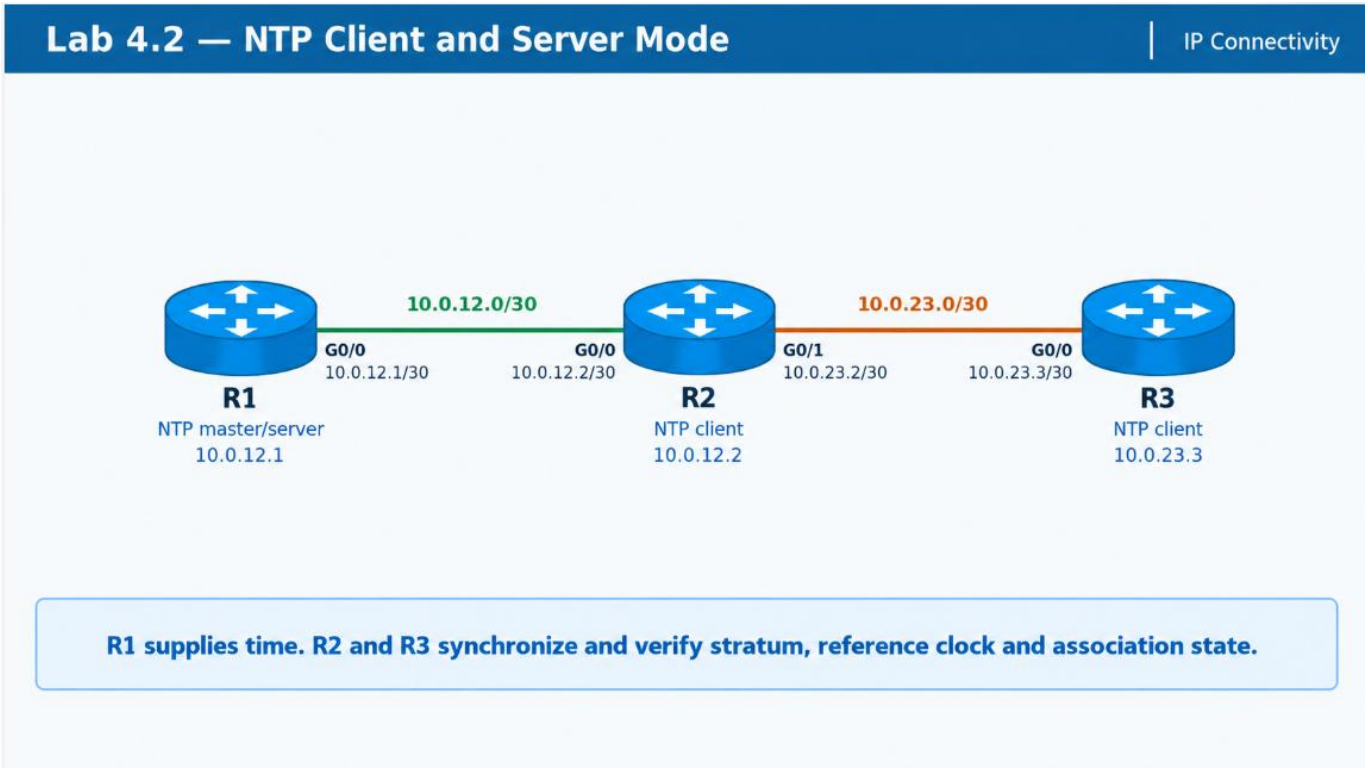
What to verify

- Dynamic pool and PAT entries disappear.
- The configured static translation remains.

Lab 4.2 — NTP Client and Server Mode

Configure one router as an authoritative lab-time source and synchronize two downstream routers to it.

Lab topology



Addressing / device plan

Device / Interface	IP address	Connected to	Role
R1 G0/0	10.0.12.1/30	R2 G0/0	NTP master/server
R2 G0/0	10.0.12.2/30	R1 G0/0	Client
R2 G0/1	10.0.23.2/30	R3 G0/0	Transit
R3 G0/0	10.0.23.3/30	R2 G0/1	Client

Lab objectives

- Configure R1 as NTP master/server.
- Configure R2 and R3 as NTP clients.
- Verify stratum, reference clock, synchronized state and peer selection.

Step 1 — Configure R1 NTP server

```
enable
configure terminal
hostname R1
clock timezone IST 5 30
interface GigabitEthernet0/0
 ip address 10.0.12.1 255.255.255.252
 no shutdown
ntp master 3
end
write memory
```

R1 verification

```
R1# show ntp status
Clock is synchronized, stratum 3, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz

R1# show clock detail
22:15:31.442 IST Tue Oct 20 2026
Time source is NTP
```

What to verify

- R1 reports synchronized state.
- R1 advertises the configured lab stratum.
- The router is ready to answer NTP requests.

Step 2 — Configure R2

```
enable
configure terminal
hostname R2
clock timezone IST 5 30
interface GigabitEthernet0/0
 ip address 10.0.12.2 255.255.255.252
 no shutdown
interface GigabitEthernet0/1
 ip address 10.0.23.2 255.255.255.252
 no shutdown
ntp server 10.0.12.1 prefer
end
write memory
```

R2 verification

```
R2# show ntp associations
  address         ref clock       st   when   poll reach  delay  offset   disp
*~10.0.12.1       127.127.1.1      3     34     64   377  1.12   -0.48   1.05
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R2# show ntp status
Clock is synchronized, stratum 4, reference is 10.0.12.1
```

What to verify

- The asterisk identifies the selected system peer.
- Reach 377 indicates successful recent NTP exchanges.
- R2 is one stratum higher than R1.

Step 3 — Configure R3

```
enable
configure terminal
hostname R3
clock timezone IST 5 30
interface GigabitEthernet0/0
 ip address 10.0.23.3 255.255.255.252
 no shutdown
ip route 10.0.12.0 255.255.255.252 10.0.23.2
ntp server 10.0.12.1
end
write memory
```

R3 verification

```
R3# show ntp associations
  address         ref clock       st   when   poll reach  delay  offset   disp
*~10.0.12.1       127.127.1.1      3     21     64   377  2.08    0.31   0.84

R3# show ntp status
Clock is synchronized, stratum 4, reference is 10.0.12.1
```

What to verify

- R3 has IP reachability to the NTP server.
- R3 is synchronized to 10.0.12.1 and shows a valid reach value.

Controlled failure — remove reachability to the time source

```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# shutdown

R3# show ntp status
Clock is unsynchronized, stratum 16, no reference clock
```

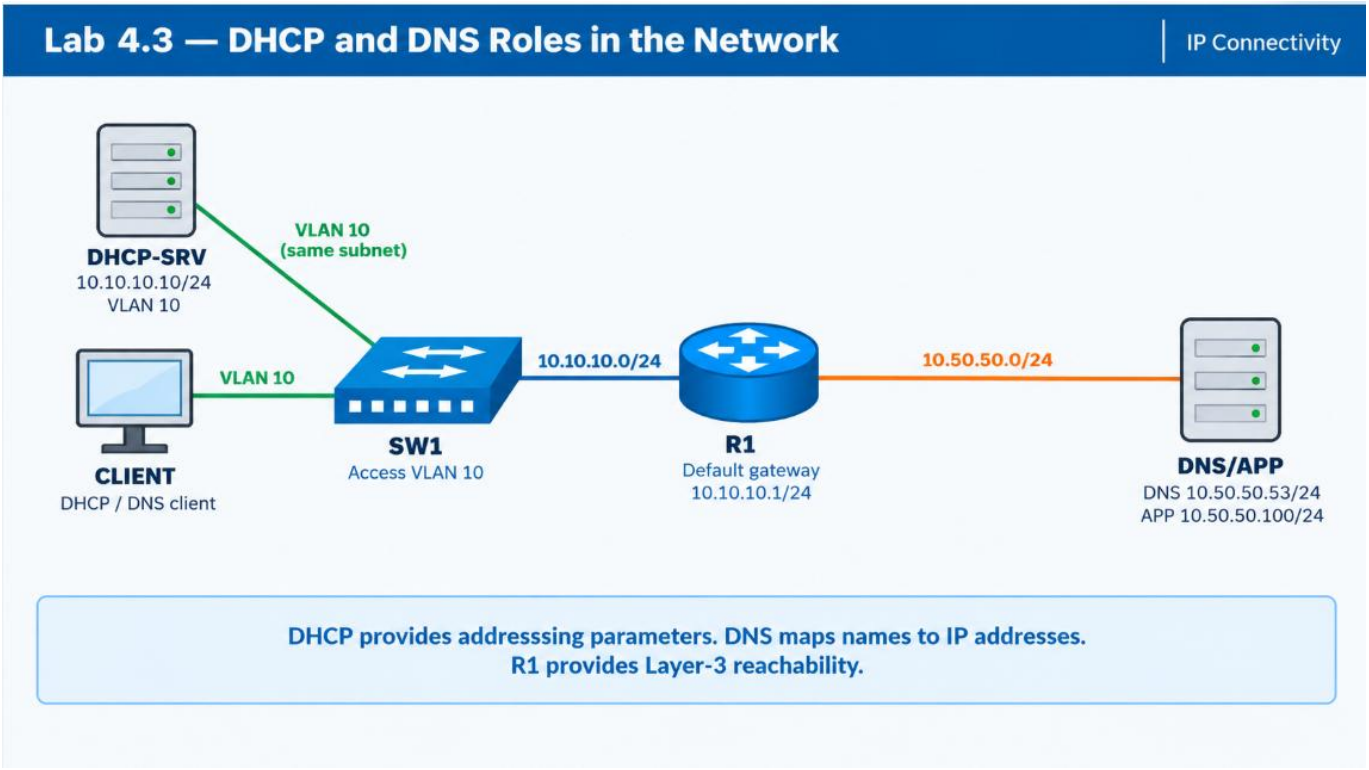
What to verify

- After NTP times out, the client eventually becomes unsynchronized.
- Restore the interface with no shutdown and confirm synchronization returns.

Lab 4.3 — DHCP and DNS Roles in the Network

Observe the complete client workflow: obtain Layer-3 settings by DHCP, then resolve an application name by DNS and reach the application server.

Lab topology



Addressing / device plan

Device	IP address	Default gateway	Purpose
CLIENT	DHCP	10.10.10.1	User endpoint
R1 G0/0	10.10.10.1/24	—	Client gateway
R1 G0/1	10.50.50.1/24	—	Server gateway
DHCP-SRV	10.10.10.10/24	10.10.10.1	DHCP service
DNS-SRV	10.50.50.53/24	10.50.50.1	DNS service
APP-SRV	10.50.50.100/24	10.50.50.1	Application

Lab objectives

- Configure VLAN 10 access and routed connectivity to the server LAN.
- Configure DHCP service parameters on the server.
- Configure DNS A-record resolution for app.nga.lab.
- Verify the client lease, DNS server value, name resolution and application reachability.

Step 1 — Configure SW1

```
enable
configure terminal
hostname SW1
vlan 10
 name USERS
interface GigabitEthernet0/1
 description CLIENT
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
interface GigabitEthernet0/24
 description TO_R1
 switchport mode access
 switchport access vlan 10
end
write memory
```

Step 2 — Configure R1

```
enable
configure terminal
hostname R1
interface GigabitEthernet0/0
 description USER_LAN
 ip address 10.10.10.1 255.255.255.0
 no shutdown
interface GigabitEthernet0/1
 description SERVER_LAN
 ip address 10.50.50.1 255.255.255.0
 no shutdown
end
write memory
```

R1 verification

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status  Protocol
GigabitEthernet0/0     10.10.10.1      YES manual up      up
GigabitEthernet0/1     10.50.50.1      YES manual up      up
```

What to verify

- Both client and server networks are directly connected and up/up.

Step 3 — Configure DHCP-SRV service

Setting	Value
Server IP	10.10.10.10 /24
Default gateway	10.10.10.1
DHCP pool name	USERS
Network / mask	10.10.10.0 /24
Default router option	10.10.10.1
DNS server option	10.50.50.53
Lease range	10.10.10.100 - 10.10.10.199

On Packet Tracer Server: Services → DHCP → On. Create the USERS pool with the values above. The DHCP server is deliberately placed on the same client subnet in this role-focused lab, so the client broadcast can reach it directly. The routed DHCP relay behavior is configured separately in Lab 4.6.

Step 4 — Configure DNS and application services

Server	Service action
DNS-SRV 10.50.50.53	Services → DNS → On; add A record app.nga.lab = 10.50.50.100
APP-SRV 10.50.50.100	Enable HTTP service or another reachable application service

Step 5 — Client observation

```
CLIENT> ipconfig /all
IPv4 Address.....: 10.10.10.100
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 10.10.10.1
DNS Servers.....: 10.50.50.53
DHCP Enabled.....: Yes

CLIENT> nslookup app.nga.lab
Server:  10.50.50.53
Name:    app.nga.lab
Address: 10.50.50.100

CLIENT> ping app.nga.lab
Reply from 10.50.50.100: bytes=32 time<1ms TTL=127
```

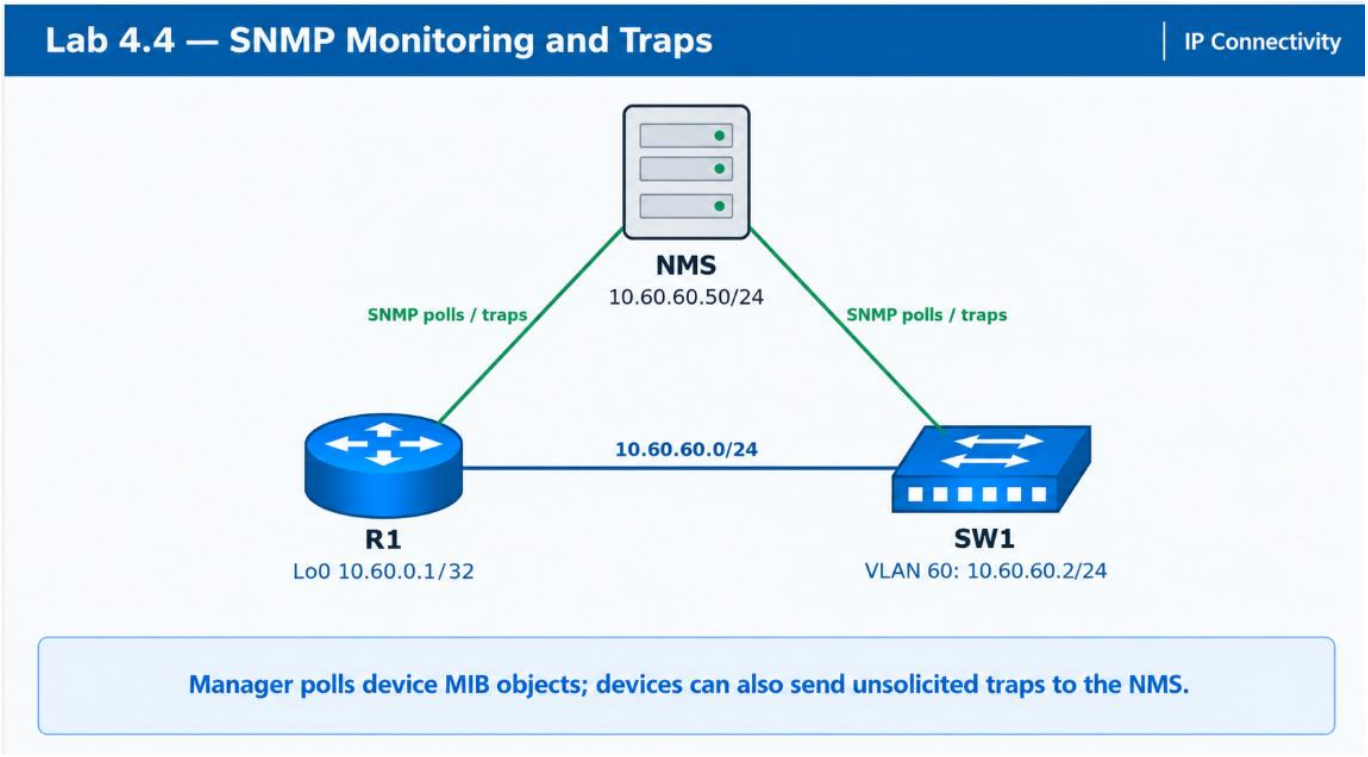
What to verify

- DHCP gives the client an IP address, mask, default gateway and DNS-server option.
- DNS resolves app.nga.lab to 10.50.50.100.
- The client can reach the resolved application address.
- DHCP answers “How do I address myself?”; DNS answers “What IP belongs to this name?”

Lab 4.4 — SNMP Monitoring and Traps

Configure basic SNMPv2c polling/trap behavior on a router and switch, then verify the management-plane settings.

Lab topology



Addressing / device plan

Device / Interface	IP address	Role
NMS	10.60.60.50/24	Management station
R1 Lo0	10.60.0.1/32	Managed router
R1 G0/0	10.60.60.1/24	Management LAN
SW1 VLAN60	10.60.60.2/24	Managed switch

Lab objectives

- Configure read-only SNMP communities and device metadata.
- Configure an NMS trap destination.
- Verify SNMP engine counters and trap configuration.
- Differentiate manager, agent, MIB and OID roles.

Step 1 — Configure R1 SNMP agent

```
enable
configure terminal
hostname R1
interface GigabitEthernet0/0
 ip address 10.60.60.1 255.255.255.0
 no shutdown
interface Loopback0
 ip address 10.60.0.1 255.255.255.255
!
snmp-server community NGA-RO RO
snmp-server location Training-Lab-Rack-A
snmp-server contact admin@networkguideacademy.com
snmp-server host 10.60.60.50 version 2c NGA-RO
snmp-server enable traps
end
write memory
```

R1 verification

```
R1# show snmp community
Community name: NGA-RO
Community Index: NGA-RO
Community SecurityName: NGA-RO
storage-type: nonvolatile       active

R1# show snmp | include packets|traps
  28 SNMP packets input
  31 SNMP packets output
  2 Trap PDUs

R1# show running-config | include ^snmp-server
snmp-server community NGA-RO RO
snmp-server location Training-Lab-Rack-A
snmp-server contact admin@networkguideacademy.com
snmp-server host 10.60.60.50 version 2c NGA-RO
snmp-server enable traps
```

What to verify

- The community is RO, not RW.
- The NMS address is configured as the trap destination.
- SNMP packet counters increase when the NMS polls the device.

Step 2 — Configure SW1 SNMP agent

```
enable
configure terminal
hostname SW1
vlan 60
 name MANAGEMENT
interface Vlan60
 ip address 10.60.60.2 255.255.255.0
 no shutdown
ip default-gateway 10.60.60.1
snmp-server community NGA-RO RO
snmp-server location Training-Lab-Access-1
snmp-server contact admin@networkguideacademy.com
snmp-server host 10.60.60.50 version 2c NGA-RO
snmp-server enable traps
end
write memory
```

SW1 verification

```
SW1# show ip interface brief | include Vlan60
Vlan60              10.60.60.2     YES manual up                    up

SW1# show snmp | include packets|traps
  15 SNMP packets input
  18 SNMP packets output
  1 Trap PDU
```

What to verify

- The management SVI is up/up and can reach the NMS.
- SNMP request/response counters show polling activity.

SNMP operational interpretation

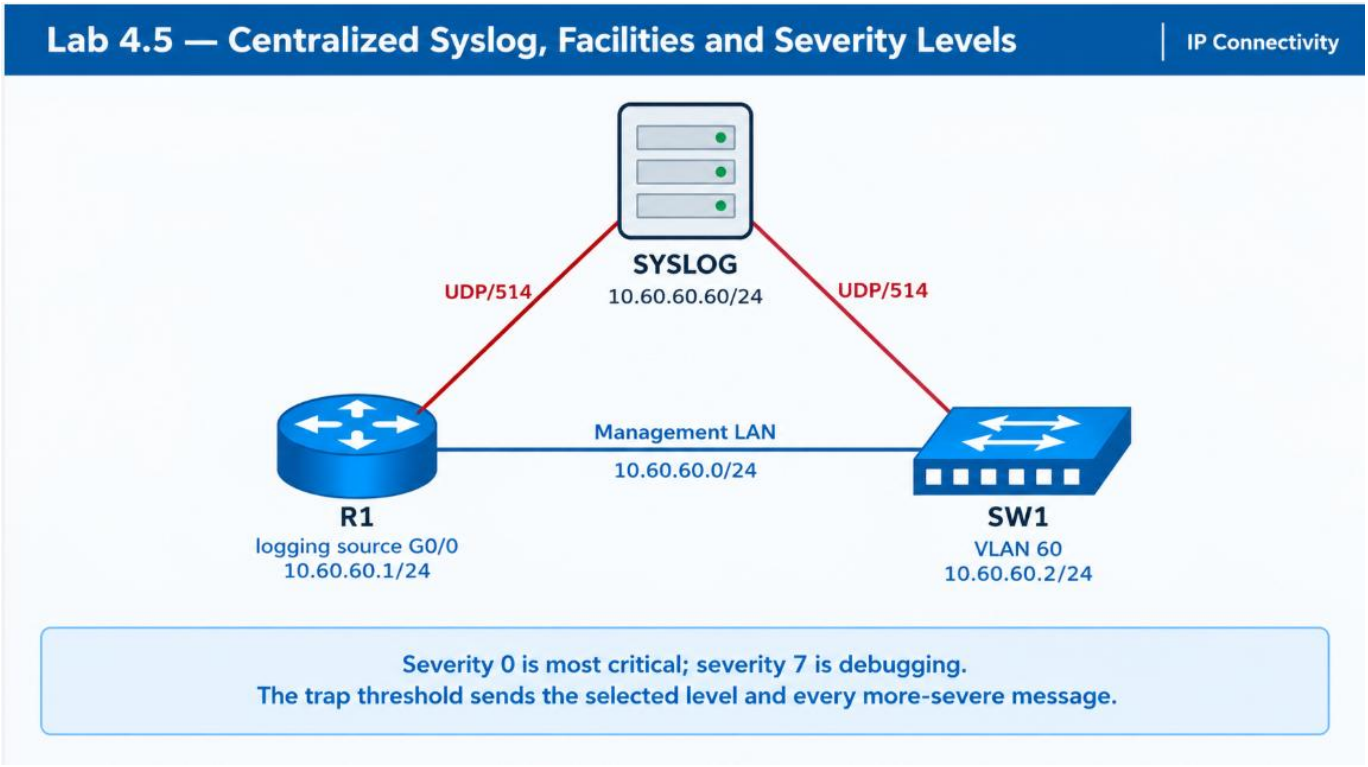
Term	Meaning
Manager/NMS	System that polls agents and receives notifications.
Agent	SNMP process running on the managed device.
MIB	Hierarchical database describing manageable objects.
OID	Identifier for one managed object/leaf in the MIB.
Trap	Unsolicited event notification from agent to manager.

Security note: SNMPv2c community strings are clear-text credentials. Production environments should prefer SNMPv3 when supported and required by policy.

Lab 4.5 — Centralized Syslog, Facilities and Severity Levels

Send device events to a central syslog server and interpret severity filtering.

Lab topology



Addressing / device plan

Device / Interface	IP address	Role
SYSLOG	10.60.60.60/24	Central collector
R1 G0/0	10.60.60.1/24	Router source
SW1 VLAN60	10.60.60.2/24	Switch source

Lab objectives

- Enable timestamped local and remote logging.
- Set a remote trap threshold and facility.
- Generate an interface event and confirm local and remote logs.
- Interpret severity values 0 through 7.

Step 1 — Configure R1 logging

```
enable
configure terminal
hostname R1
service timestamps log datetime msec localtime show-timezone
interface GigabitEthernet0/0
 ip address 10.60.60.1 255.255.255.0
 no shutdown
logging buffered 16384 informational
logging host 10.60.60.60
logging trap notifications
logging facility local6
logging source-interface GigabitEthernet0/0
end
write memory
```

R1 verification

```
R1# show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited)
    Console logging: level debugging
    Buffer logging:  level informational, 18 messages logged
    Trap logging: level notifications, 9 message lines logged
        Logging to 10.60.60.60  (udp port 514, audit disabled)
        Logging Source-Interface: GigabitEthernet0/0
    Facility: local6
```

What to verify

- Remote logging points to 10.60.60.60 over UDP/514.
- Trap level notifications means severity 0 through 5 are sent.
- The configured facility is local6.

Step 2 — Configure SW1 logging

```
enable
configure terminal
hostname SW1
service timestamps log datetime msec localtime show-timezone
vlan 60
 name MANAGEMENT
interface Vlan60
 ip address 10.60.60.2 255.255.255.0
 no shutdown
ip default-gateway 10.60.60.1
logging buffered 8192 informational
logging host 10.60.60.60
logging trap notifications
logging facility local6
logging source-interface Vlan60
end
write memory
```

Step 3 — Generate a test event

```
R1(config)# interface GigabitEthernet0/2
R1(config-if)# shutdown
R1(config-if)# no shutdown

R1# show logging | include GigabitEthernet0/2
*Oct 20 22:42:18.112 IST: %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively
down
*Oct 20 22:42:20.119 IST: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
```

What to verify

- The message contains a timestamp, facility/mnemonic and severity number.
- Severity 5 (notifications) is sent because the remote threshold is notifications.
- Severity 3 is more critical and is also sent.

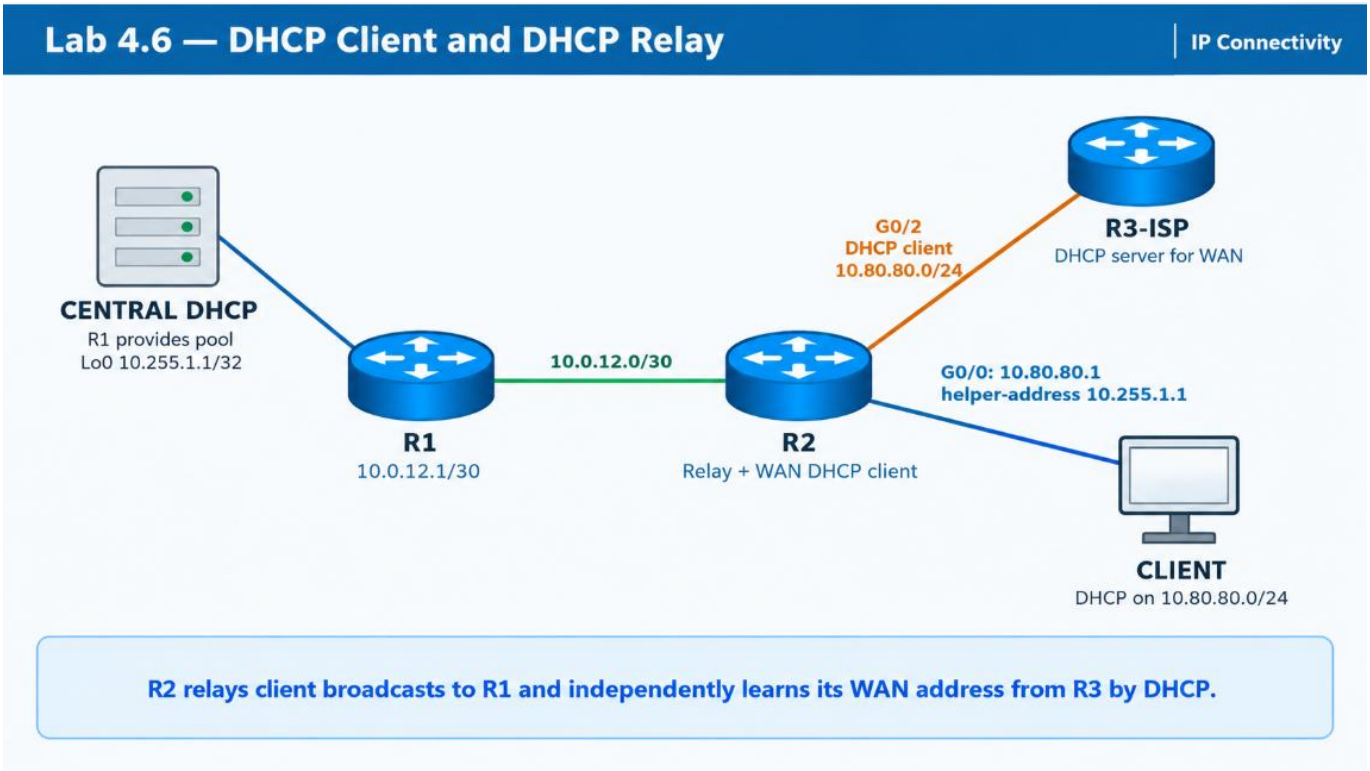
Syslog severity reference

Level	Name	Relative urgency
0	Emergencies	System unusable
1	Alerts	Immediate action
2	Critical	Critical condition
3	Errors	Error condition
4	Warnings	Warning condition
5	Notifications	Normal but significant
6	Informational	Informational
7	Debugging	Debug detail

Lab 4.6 — DHCP Client and DHCP Relay

Configure R2 to relay LAN DHCP broadcasts to a centralized IOS DHCP server on R1 while R2 also learns a separate WAN address from an ISP-side DHCP server on R3.

Lab topology



Addressing / device plan

Device / Interface	IP address	Purpose
R1 G0/0	10.0.12.1/30	Central DHCP reachability
R1 Lo0	10.255.1.1/32	Helper destination
R2 G0/0	10.80.80.1/24	Client gateway + relay
R2 G0/1	10.0.12.2/30	Toward R1
R2 G0/2	DHCP	WAN DHCP client
R3 G0/0	172.20.0.1/24	ISP DHCP server LAN
CLIENT	DHCP	10.80.80.0/24

Lab objectives

- Configure R1 as centralized DHCP server for the 10.80.80.0/24 client LAN.
- Configure R2 LAN interface with ip helper-address.
- Configure R3 to provide a DHCP WAN lease to R2.
- Verify client binding, relay operation and R2 DHCP-learned address.

Step 1 — Configure R1 centralized DHCP server

```
enable
configure terminal
hostname R1
interface GigabitEthernet0/0
 ip address 10.0.12.1 255.255.255.252
 no shutdown
interface Loopback0
 ip address 10.255.1.1 255.255.255.255
!
ip route 10.80.80.0 255.255.255.0 10.0.12.2
!
ip dhcp excluded-address 10.80.80.1 10.80.80.20
ip dhcp pool REMOTE-USERS
 network 10.80.80.0 255.255.255.0
 default-router 10.80.80.1
 dns-server 10.50.50.53
 domain-name nga.lab
 lease 1
end
write memory
```

R1 verification before client request

```
R1# show ip dhcp pool REMOTE-USERS
Pool REMOTE-USERS :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 20
```

What to verify

- The pool network matches the remote client subnet, not the R1-R2 transit.
- Default router is R2 LAN address 10.80.80.1.

Step 2 — Configure R3 ISP-side DHCP service

```
enable
configure terminal
hostname R3-ISP
interface GigabitEthernet0/0
 ip address 172.20.0.1 255.255.255.0
 no shutdown
ip dhcp excluded-address 172.20.0.1 172.20.0.99
ip dhcp pool CPE-WAN
 network 172.20.0.0 255.255.255.0
 default-router 172.20.0.1
 dns-server 8.8.8.8
end
write memory
```

Step 3 — Configure R2 relay and DHCP client

```
enable
configure terminal
hostname R2
interface GigabitEthernet0/0
 description CLIENT_LAN
 ip address 10.80.80.1 255.255.255.0
 ip helper-address 10.255.1.1
 no shutdown
interface GigabitEthernet0/1
 description TO_R1
 ip address 10.0.12.2 255.255.255.252
 no shutdown
interface GigabitEthernet0/2
 description WAN_DHCP_CLIENT
 ip address dhcp
 no shutdown
ip route 10.255.1.1 255.255.255.255 10.0.12.1
end
write memory
```

R2 verification

```
R2# show ip interface GigabitEthernet0/0 | include Helper
  Helper address is 10.255.1.1

R2# show ip interface brief | include GigabitEthernet0/2
GigabitEthernet0/2     172.20.0.100    YES DHCP   up  up

R2# show dhcp lease
Temp IP addr: 172.20.0.100 for peer on Interface: GigabitEthernet0/2
Temp sub net mask: 255.255.255.0
   DHCP Lease server: 172.20.0.1, state: 5 Bound
```

What to verify

- R2 LAN has helper address 10.255.1.1.
- R2 G0/2 address method is DHCP and the interface is up/up.
- show dhcp lease reports Bound state and the DHCP server address.

Step 4 — Request a lease from the remote client

```
CLIENT> ipconfig /renew
DHCP request successful.

CLIENT> ipconfig /all
IPv4 Address.....: 10.80.80.21
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 10.80.80.1
DNS Servers.....: 10.50.50.53
DHCP Enabled.....: Yes
```

```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/            Lease expiration        Type
             Hardware address
10.80.80.21     0100.50ba.1234.56      Oct 21 2026 10:48 PM    Automatic
```

What to verify

- The client receives an address from R1 even though its DHCP broadcast could not cross R2 without relay.
- R1 records the binding from the remote 10.80.80.0/24 pool.

Controlled fault — remove the relay helper

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# no ip helper-address 10.255.1.1

CLIENT> ipconfig /renew
DHCP request failed / no address offered
```

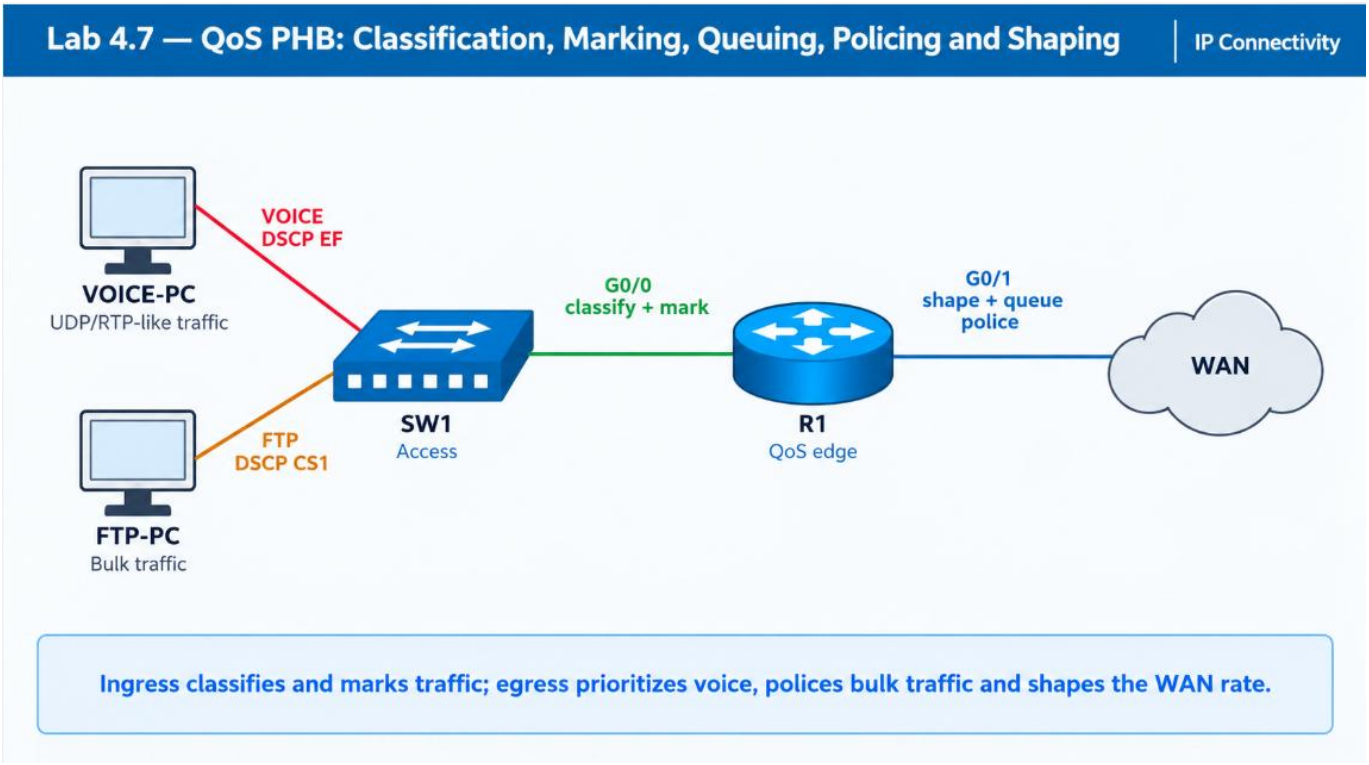
What to verify

- Without the helper, the routed boundary stops the DHCP broadcast.
- Restore ip helper-address 10.255.1.1 and renew again.

Lab 4.7 — QoS PHB: Classification, Marking, Queuing, Policing and Shaping

Use Modular QoS CLI to demonstrate the per-hop behaviors named in the CCNA blueprint while keeping the policy structure visible and verifiable.

Lab topology



Addressing / device plan

Device / Interface	IP address	Gateway / next hop	Purpose
VOICE-PC	10.100.10.10/24	10.100.10.1	Voice-like UDP
FTP-PC	10.100.10.20/24	10.100.10.1	Bulk FTP
R1 G0/0	10.100.10.1/24	—	LAN ingress
R1 G0/1	192.0.2.1/30	192.0.2.2	WAN egress

Lab objectives

- Classify voice-like and bulk FTP traffic with named ACLs.
- Mark traffic on ingress using DSCP.
- Apply a hierarchical egress policy: shape the parent WAN rate, prioritize voice, allocate bulk bandwidth and police bulk traffic.
- Verify counters and drop/mark behavior with show policy-map interface.

Step 1 — Configure R1 base addressing and classifiers

```
enable
configure terminal
hostname R1
interface GigabitEthernet0/0
 description USER_LAN
 ip address 10.100.10.1 255.255.255.0
 no shutdown
interface GigabitEthernet0/1
 description WAN
 ip address 192.0.2.1 255.255.255.252
 no shutdown
!
ip access-list extended ACL-VOICE
 permit udp 10.100.10.0 0.0.0.255 any range 16384 32767
ip access-list extended ACL-BULK-FTP
 permit tcp host 10.100.10.20 any eq 21
!
class-map match-any CM-VOICE
 match access-group name ACL-VOICE
class-map match-any CM-BULK
 match access-group name ACL-BULK-FTP
end
```

Step 2 — Configure ingress marking

```
configure terminal
policy-map MARK-IN
 class CM-VOICE
  set dscp ef
 class CM-BULK
  set dscp af11
 class class-default
  set dscp default
interface GigabitEthernet0/0
 service-policy input MARK-IN
end
```

Step 3 — Configure egress queuing, policing and shaping

```
configure terminal
policy-map WAN-CHILD
 class CM-VOICE
  priority percent 20
 class CM-BULK
  bandwidth percent 30
  police 1000000 conform-action transmit exceed-action drop
 class class-default
  fair-queue
!
policy-map WAN-PARENT
 class class-default
  shape average 5000000
  service-policy WAN-CHILD
!
interface GigabitEthernet0/1
 service-policy output WAN-PARENT
end
write memory
```

Platform note: QoS feature availability and exact counters vary by IOS/IOS XE platform and simulator. The policy illustrates the PHB concepts tested by CCNA; use a platform that supports MQC for the hands-on portion.

Step 4 — Verify the ingress policy

```
R1# show policy-map interface GigabitEthernet0/0 input
 GigabitEthernet0/0
  Service-policy input: MARK-IN

    Class-map: CM-VOICE (match-any)
      240 packets, 48000 bytes
      Match: access-group name ACL-VOICE
      QoS Set
        dscp ef
          Packets marked 240

    Class-map: CM-BULK (match-any)
      90 packets, 118000 bytes
      QoS Set
        dscp af11
          Packets marked 90
```

What to verify

- Voice packets match CM-VOICE and are marked EF.
- Bulk FTP packets match CM-BULK and are marked AF11.
- Counters increase only when matching traffic is generated.

Step 5 — Verify hierarchical WAN policy

```
R1# show policy-map interface GigabitEthernet0/1 output
 GigabitEthernet0/1
  Service-policy output: WAN-PARENT

    Class-map: class-default (match-any)
      512 packets, 624000 bytes
      shape (average) cir 5000000, bc 20000, be 20000
      target shape rate 5000000
      Service-policy : WAN-CHILD

        Class-map: CM-VOICE (match-any)
          240 packets, 48000 bytes
          Priority: 20% (1000 kbps)

        Class-map: CM-BULK (match-any)
          190 packets, 510000 bytes
          Bandwidth 30% (1500 kbps)
          police: cir 1000000 bps
            conformed 420000 bytes; actions: transmit
            exceeded 90000 bytes; actions: drop

        Class-map: class-default (match-any)
          82 packets, 66000 bytes
          Fair-queue
```

What to verify

- Parent policy shapes aggregate WAN traffic to 5 Mbps.
- Voice receives strict-priority treatment up to the configured policy allowance.
- Bulk class has bandwidth allocation and policing; exceeded bytes are dropped.

- Class-default uses fair queuing for uncategorized traffic.

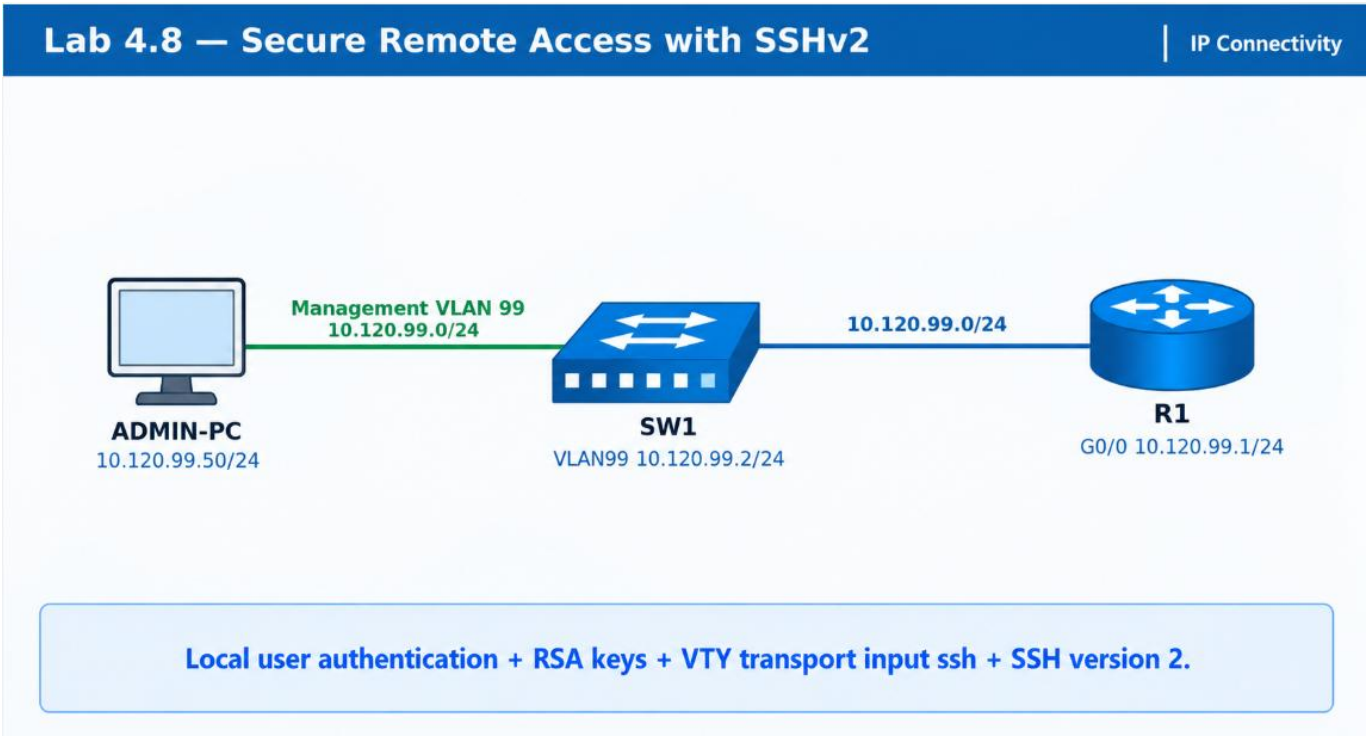
PHB interpretation

PHB concept	What this lab demonstrates
Classification	ACL/class-map places packets into classes.
Marking	Ingress policy sets DSCP EF or AF11.
Queuing	Child policy separates voice, bulk and default queues.
Congestion management	Priority/bandwidth decisions matter when output is congested.
Policing	Bulk traffic above CIR can be dropped immediately.
Shaping	Parent policy buffers/schedules aggregate traffic toward an average rate.

Lab 4.8 — Secure Remote Access with SSHv2

Configure local authentication and SSHv2 on a router and switch, then verify encrypted remote CLI access from an administrator PC.

Lab topology



Addressing / device plan

Device / Interface	IP address	Default gateway	Role
ADMIN-PC	10.120.99.50/24	10.120.99.1	SSH client
R1 G0/0	10.120.99.1/24	—	Router management
SW1 VLAN99	10.120.99.2/24	10.120.99.1	Switch management

Lab objectives

- Configure management addressing.
- Create local privileged users, domain names and RSA keys.
- Restrict VTY lines to SSH only and use local authentication.
- Verify SSH version, session establishment and active users.

Step 1 — Configure R1 SSH

```
enable
configure terminal
hostname R1
ip domain-name nga.lab
username netadmin privilege 15 secret Ccna-Lab-2026!
interface GigabitEthernet0/0
 ip address 10.120.99.1 255.255.255.0
 no shutdown
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 login local
 transport input ssh
 exec-timeout 10 0
end
write memory
```

R1 verification

```
R1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 2048 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): R1.nga.lab
```

What to verify

- SSH version is 2.0.
- RSA keys exist and the hostname/domain form the key identity.
- VTY configuration allows SSH rather than Telnet.

Step 2 — Configure SW1 SSH

```
enable
configure terminal
hostname SW1
ip domain-name nga.lab
username netadmin privilege 15 secret Ccna-Lab-2026!
vlan 99
 name MANAGEMENT
interface Vlan99
 ip address 10.120.99.2 255.255.255.0
 no shutdown
ip default-gateway 10.120.99.1
crypto key generate rsa modulus 2048
ip ssh version 2
line vty 0 4
 login local
 transport input ssh
 exec-timeout 10 0
end
write memory
```

Step 3 — Connect from ADMIN-PC

```
ADMIN-PC> ssh -l netadmin 10.120.99.1
Password: **************
R1#

ADMIN-PC> ssh -l netadmin 10.120.99.2
Password: **************
SW1#
```

```
R1# show users
    Line       User       Host(s)              Idle       Location
*  2 vty 0     netadmin   idle                 00:00:12   10.120.99.50

R1# show ssh
Connection Version Mode Encryption  Hmac     State          Username
0          2.0     IN   aes256-ctr  hmac-sha2 Session started netadmin
```

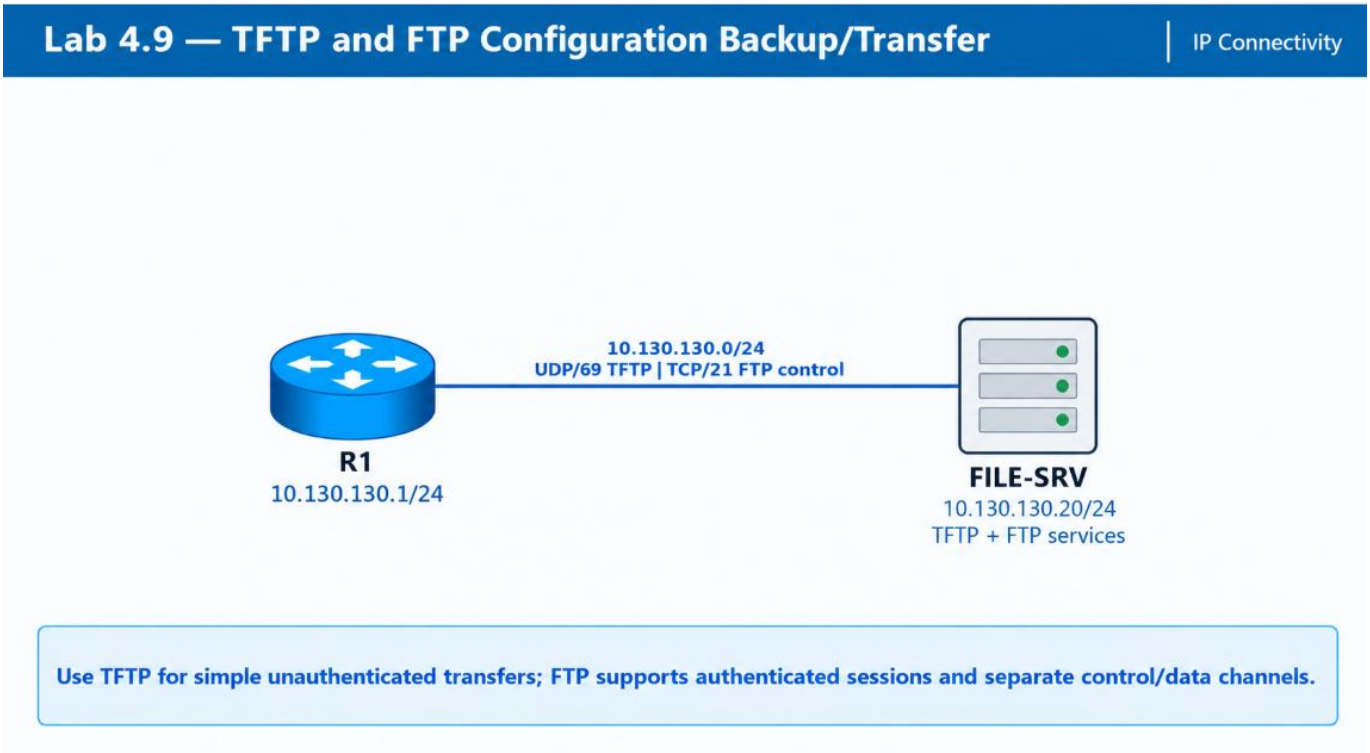
What to verify

- Login succeeds using the local username database.
- The remote client source address is visible in show users.
- show ssh confirms a version 2 encrypted session.

Lab 4.9 — TFTP and FTP Configuration Backup/Transfer

Back up the router configuration with both TFTP and FTP and compare their operational behavior.

Lab topology



Addressing / device plan

Device / Interface	IP address	Role
R1 G0/0	10.130.130.1/24	Router
FILE-SRV	10.130.130.20/24	TFTP and FTP server

Lab objectives

- Configure IP reachability to a file server.
- Back up running configuration by TFTP.
- Configure FTP credentials and back up by FTP.
- Verify successful byte transfer and server-side file creation.

Step 1 — Configure R1 and test reachability

```
enable
configure terminal
hostname R1
interface GigabitEthernet0/0
 ip address 10.130.130.1 255.255.255.0
 no shutdown
ip ftp username backupuser
ip ftp password 0 BackupLab2026!
end
write memory

R1# ping 10.130.130.20
!!!!!
Success rate is 100 percent (5/5)
```

What to verify

- The file server is reachable before starting any copy operation.
- FTP credentials are configured only once and reused by the FTP copy command.

Step 2 — TFTP backup

```
R1# copy running-config tftp:
Address or name of remote host []? 10.130.130.20
Destination filename [r1-confg]? R1-running-TFTP.cfg
!!
1842 bytes copied in 0.812 secs (2268 bytes/sec)
```

What to verify

- The transfer completes without timeout.
- The TFTP server shows R1-running-TFTP.cfg.
- TFTP uses UDP/69 and does not provide user authentication.

Step 3 — FTP backup

```
R1# copy running-config ftp:
Address or name of remote host []? 10.130.130.20
Destination filename [r1-confg]? R1-running-FTP.cfg
Writing R1-running-FTP.cfg !
1842 bytes copied in 0.936 secs (1968 bytes/sec)
```

What to verify

- FTP authenticates with the configured username/password.
- The FTP server shows R1-running-FTP.cfg.
- FTP control uses TCP/21; unlike TFTP, FTP is session-oriented and authenticated.

Optional controlled restore exercise

Use this only in a disposable lab. Replacing startup configuration can affect the next reload.

```
R1# copy tftp: startup-config
Address or name of remote host []? 10.130.130.20
Source filename []? R1-running-TFTP.cfg
Destination filename [startup-config]?
Accessing tftp://10.130.130.20/R1-running-TFTP.cfg...
Loading R1-running-TFTP.cfg from 10.130.130.20: !
[OK - 1842 bytes]
1842 bytes copied in 0.705 secs
```

What to verify

- The source file is read from the server.
- The destination is startup-config; the running configuration is not immediately replaced.

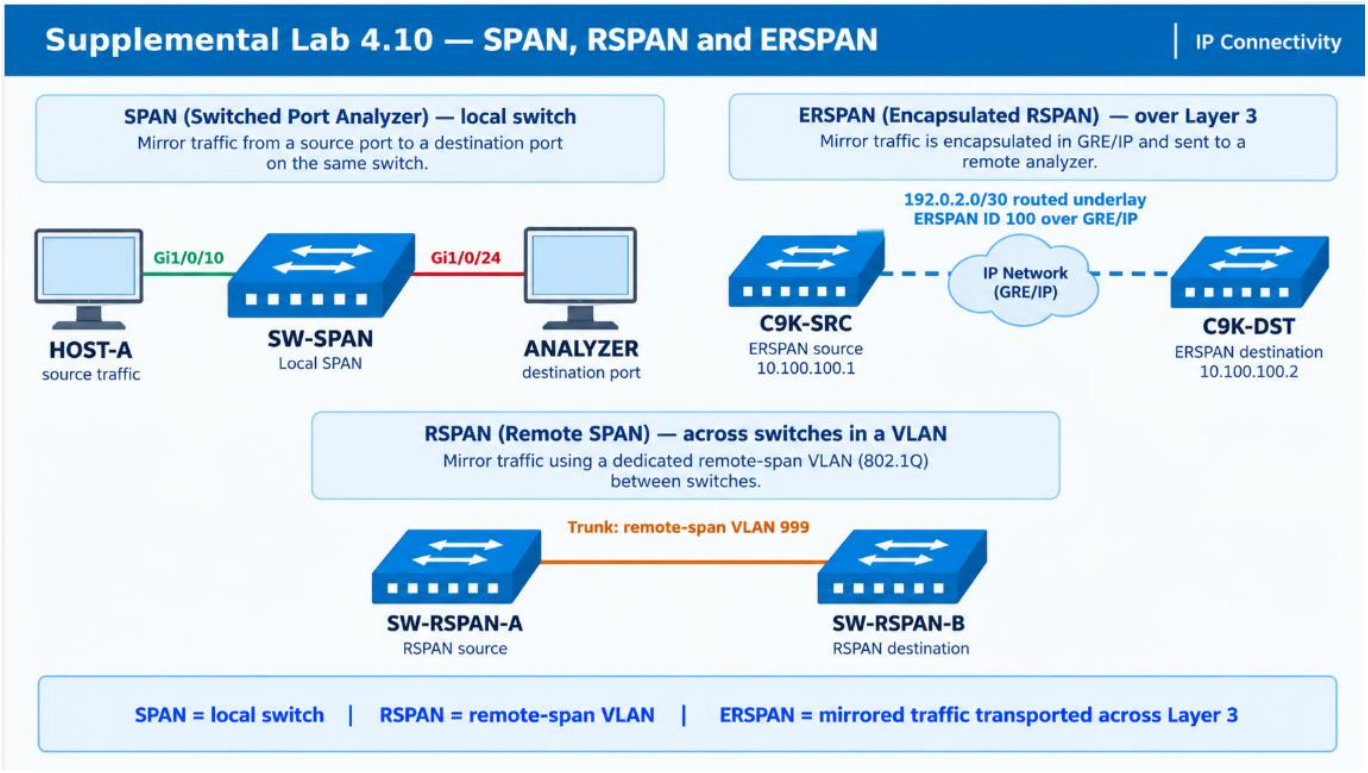
TFTP vs FTP quick comparison

Feature	TFTP	FTP
Transport	UDP	TCP
Default control port	69	21
Authentication	None in the protocol	Username/password
Operational use	Simple device/file transfer	Authenticated file transfer
Reliability	Application relies on TFTP acknowledgements over UDP	TCP provides reliable transport

Supplemental Lab 4.10 — SPAN, RSPAN and ERSPAN

Practice three traffic-mirroring models used in operational troubleshooting. This section is supplemental to the CCNA v1.1 IP Services 4.1-4.9 blueprint.

Lab topology



Lab objectives

- Configure local SPAN on one switch.
- Configure RSPAN across two Layer-2 switches with remote-span VLAN 999.
- Configure ERSPAN source and destination sessions on IOS XE Catalyst 9000-style syntax.
- Verify monitor-session state and understand where the analyzer receives mirrored frames.

Part A — Local SPAN on SW-SPAN

```
enable
configure terminal
hostname SW-SPAN
interface GigabitEthernet1/0/10
 description SOURCE_HOST
 no shutdown
interface GigabitEthernet1/0/24
 description PACKET_ANALYZER
 no shutdown
monitor session 1 source interface GigabitEthernet1/0/10 both
monitor session 1 destination interface GigabitEthernet1/0/24
end
```

Verify local SPAN

```
SW-SPAN# show monitor session 1
Session 1
---------
Type               : Local Session
Source Ports       :
    Both           : Gi1/0/10
Destination Ports  : Gi1/0/24
    Encapsulation  : Native
          Ingress  : Disabled
```

What to verify

- Session type is Local.
- Gi1/0/10 is mirrored in both directions.
- Gi1/0/24 is the analyzer destination port.

Part B — RSPAN across SW-RSPAN-A and SW-RSPAN-B

Configure SW-RSPAN-A — source switch

```
enable
configure terminal
hostname SW-RSPAN-A
vlan 999
 name RSPAN-VLAN
 remote-span
interface GigabitEthernet1/0/48
 description TRUNK_TO_SW-RSPAN-B
 switchport mode trunk
 switchport trunk allowed vlan add 999
monitor session 2 source interface GigabitEthernet1/0/10 both
monitor session 2 destination remote vlan 999
end
```

Configure SW-RSPAN-B — destination switch

```
enable
configure terminal
hostname SW-RSPAN-B
vlan 999
 name RSPAN-VLAN
 remote-span
interface GigabitEthernet1/0/48
 description TRUNK_TO_SW-RSPAN-A
 switchport mode trunk
 switchport trunk allowed vlan add 999
monitor session 2 source remote vlan 999
monitor session 2 destination interface GigabitEthernet1/0/24
end
```

Verify RSPAN

```
SW-RSPAN-A# show vlan remote-span
VLAN  Type  Remote SPAN VLAN
999   enet  Yes

SW-RSPAN-A# show monitor session 2
Session 2
---------
Type               : Remote Source Session
Source Ports          : Both : Gi1/0/10
Dest RSPAN VLAN        : 999

SW-RSPAN-B# show monitor session 2
Session 2
---------
Type               : Remote Destination Session
Source RSPAN VLAN       : 999
Destination Ports      : Gi1/0/24
```

What to verify

- VLAN 999 is explicitly marked remote-span on both switches.
- The trunk carries VLAN 999 end-to-end.
- The source switch sends mirrored traffic into RSPAN VLAN 999; the destination switch takes it from VLAN 999 and delivers it to the analyzer port.

Part C — ERSPAN across Layer 3

ERSPAN syntax and scale depend on IOS XE platform/release. The following follows Catalyst 9300-style source/destination session syntax.

Configure C9K-SRC

```
enable
configure terminal
hostname C9K-SRC
interface Loopback0
 ip address 10.100.100.1 255.255.255.255
interface GigabitEthernet1/0/48
 no switchport
 ip address 192.0.2.1 255.255.255.252
 no shutdown
ip route 10.100.100.2 255.255.255.255 192.0.2.2
monitor session 3 type erspan-source
 description NGA_ERSPAN_SOURCE
 source interface GigabitEthernet1/0/10 both
 destination
  erspan-id 100
  ip address 10.100.100.2
  origin ip address 10.100.100.1
 exit
 no shutdown
end
```

Configure C9K-DST

```
enable
configure terminal
hostname C9K-DST
interface Loopback0
 ip address 10.100.100.2 255.255.255.255
interface GigabitEthernet1/0/48
 no switchport
 ip address 192.0.2.2 255.255.255.252
 no shutdown
ip route 10.100.100.1 255.255.255.255 192.0.2.1
monitor session 3 type erspan-destination
 destination interface GigabitEthernet1/0/24
 source
  erspan-id 100
  ip address 10.100.100.2
 exit
 no shutdown
end
```

Verify ERSPAN

```
C9K-SRC# show monitor session 3
Session 3
---------
Type               : ERSPAN Source Session
Status             : Admin Enabled
Source Ports         : Both : Gi1/0/10
Destination IP Address : 10.100.100.2
Destination ERSPAN ID  : 100
Origin IP Address      : 10.100.100.1

C9K-DST# show monitor session 3
Session 3
---------
Type               : ERSPAN Destination Session
Status             : Admin Enabled
Destination Ports      : Gi1/0/24
Source IP Address      : 10.100.100.2
Source ERSPAN ID       : 100
```

What to verify

- Source and destination sessions use the same ERSPAN ID.
- The destination IP is local to the ERSPAN destination switch.
- Layer-3 routing must exist between source origin and destination IP.
- The analyzer connected to C9K-DST Gi1/0/24 receives decapsulated mirrored traffic.

SPAN family comparison

Feature	SPAN	RSPAN	ERSPAN
Scope	One switch	Layer-2 switched domain	Routed IP network
Transport	Local switching fabric	Remote-span VLAN	GRE-encapsulated IP
Special requirement	Destination analyzer port	remote-span VLAN on participating switches	IP reachability + supported ERSPAN platform
Best fit	Same-switch capture	Capture across nearby switches	Capture across Layer-3 boundaries

Module 4 — Final Verification Checklist

Area	Core verification commands / evidence
NAT/PAT	show ip nat translations; show ip nat statistics; end-to-end ping
NTP	show ntp associations; show ntp status; show clock detail
DHCP/DNS	Client ipconfig; nslookup; show ip dhcp binding where IOS server is used
SNMP	show snmp; show snmp community; NMS poll/trap evidence
Syslog	show logging; central server event reception; severity interpretation
DHCP relay/client	show ip interface (helper); show dhcp lease; show ip dhcp binding
QoS	show policy-map interface input/output; class counters; mark/drop/shape evidence
SSH	show ip ssh; show ssh; show users
TFTP/FTP	Successful copy output; file visible on server
SPAN/RSPAN/ERSPAN	show monitor session; remote-span VLAN state; ERSPAN IP/ID match

Common troubleshooting sequence

1. Check Layer 1/2 state first: interfaces, VLANs and trunks.
2. Check IP addressing, masks, gateways and routing.
3. Check the service-specific binding or association state.
4. Check counters before and after generating test traffic.
5. Change only one variable at a time during fault isolation.
6. After recovery, rerun the same verification command that originally proved the failure.