12. Troubleshooting LANs

TROUBLESHOOTING

On an exam, you'll be asked to find the root cause of a problem and either fix it or answer questions.

- Sim Questions—change config
- Simlet Questions—answer questions using 5-10 show commands

General Technique

- Problem Isolation & Documentation—confirm the problem, determine subset of devices and cables that may be part of the problem, document results.
- Resolve or Escalate—Find the root cause and fix. Escalate if unable.
- Verify or Monitor—Either verify the fix with show commands or monitor over time.

SWITCH INTERFACES

Interface Status can be reported as one term or two, depending on the command used

Command	Line Status + Protocol Status (e.g. up/up)	Interface Status (e.g. connected)
`show interfaces [ fa0/1 ]`	X	X
`show interfaces description`	X	
`show interfaces status`		X

Interface Status Meanings and correlations

Line Status	Protocol Status	Interface Status	Cause
admin Down	down	disabled	Shutdown command in interface config
down	down	notconnect	Bad cable or device on the other end is off or err-disabled
up	down	notconnect	(Doesn't happen on switch interfaces.)
down	down (err-disabled)	err-disabled	Port security has disabled this end
up	up	connected	

DUPLEX AND SPEED ISSUES

If both duplex and speed are specified, Cisco disables negotiation. Non-negotiation defaults are in Chapter 9.

Duplex Mismatch—If one side has 10/full or 100/full explicitly set, that side won't negotiate. The other side's autonegotiation will sense the speed and match it (Cisco), but use half-duplex, per the default rules (half for 10/100, full for gigabit and better).

To find a duplex mismatch, watch the collision and late collision counters on "show interfaces" (yellow in "show interfaces fa0/11," below).

The command "show interfaces" won't tell you whether an interface's speed was negotiated or manually set. For that you must use "show interfaces status."

```
SW# show interfaces status
```

Tells HOW an interface got its speed and duplex. For example, a-full (automatic) vs full (manual)

```
Port      Name               Status       Vlan       Duplex  Speed Type
…
Fa0/9     BRO                notconnect   22           auto   auto 10/100BaseTX
Fa0/10    PROTOLAB           connected    22           full    100 10/100BaseTX
Fa0/11    ALUM               connected    3          a-full  a-100 10/100BaseTX
…
SW# show interfaces fa0/10
```

No indication that speed and duplex were manually set

```
FastEthernet0/10 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is a418.753c.8d8a (bia a418.753c.8d8a)
  Description: PROTOLAB
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  …
SW# show interfaces fa0/11
FastEthernet0/11 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is a418.753c.8d8b (bia a418.753c.8d8b)
  Description: ALUM
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     24355446 packets input, 3992292582 bytes, 0 no buffer
     Received 17715 broadcasts (380 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 380 multicast, 0 pause input
     0 input packets with dribble condition detected
     42079931 packets output, 15174089046 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

Interface Counters—remember that CSMA/CD is used during half duplex and off during full duplex.

Counter	Meaning
Runts	Frames smaller than 64-byte minimum (including header and trailer)
Giants	Frames bigger than 1518-bytes (incl. header & trailer)
Input Errors	Total of many other counters: runts, giants, no buffer, CRC, frame overrun, & ignored
CRC	Frame-check math failed, possibly due to collision
Frame	Received frames that were illegal format, perhaps ending with a partial byte, possible collision
Packets Output	Total packets successfully forwarded out the interface
Output Errors	
Collisions	Collisions during a send from this interface. If you're half-duplex, these could be normal.
Late Collisions	Collisions that happened after the 64th byte of a frame. Probably a duplex mismatch (one side wasn't using CSMA/CD to listen before talking). The half-duplex side will increment this counter, the full-duplex side won't realize there's a problem.

Switch Forwarding Decisions

Because the connection to the router (fa 0/1) is trunked, the same MAC address shows up once for each VLAN. If another switch were connected to a port, *all* of the MAC addresses connected to that switch might show up on the one port leading to that switch.

```
SW# show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  22    0005.5e2f.40c0    DYNAMIC     Fa0/10
  22    0016.cba6.9f58    DYNAMIC     Gi0/1
  22    0016.cbad.3e8a    DYNAMIC     Fa0/17
  22    0018.bad1.a460    DYNAMIC     Fa0/1
  22    f0de.f12b.116f    DYNAMIC     Gi0/2
   2    0018.bad1.a460    DYNAMIC     Fa0/1
   2    00c0.02d1.a512    DYNAMIC     Fa0/12
   2    10dd.b1d1.ada7    DYNAMIC     Fa0/14
   1    0018.bad1.a460    DYNAMIC     Fa0/1
   3    000d.939d.e192    DYNAMIC     Fa0/11
   3    0018.bad1.a460    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 11
```

Forwarding Logic:

- Input Interface Processing
  - Does port security filter the frame?
  - What's the frame's VLAN? (for access port, it's the port's VLAN; for a trunk, it's tagged.)
- Forwarding Decision
  - Unicast, Known MAC—send it out the interface with that MAC
  - Unicast, Unknown MAC or Broadcast—flood it out all ports in that VLAN, including trunks that don't restrict that VLAN, but not out the port it came in on.

Steps to troubleshoot:

- Identify ports with port security (can also use "sho run | begin interface")

```
SW# show port-security
```

- Is a violation currently occurring?
  - Violation Mode = Shutdown—interface err-disabled and port security port status = secure-down
  - Violation Mode = Restrict—Interface status "connected" and port security port status = "secure-up." Check the "show port-security interface fa0/20" command for a violation count (bottom line)
  - Violation Mode = Protect—Interface status "connected" and *no* violation count! The "last source address" may even be an allowed one. The only way to *prove* that frames are being discarded is to change the violation mode to restrict or shutdown. Shutdown would leave the offending mac in "show port-security interface fa0/20." Both would put it in a syslog message.

```
SW# show interfaces fa0/20 status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/20    LJ8550dn           err-disabled 2            auto   auto 10/100BaseTX

SW# show port-security interface fa0/20
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Hopefully, the last two entries wouldn't be zeroes on a test. Once the port is shutdown by port security, the violation counter will stop incrementing.

Steps to fix

- Resolve the actual cause
- If the port is err-disabled, enter interface config mode and do a "shutdown" followed by "no shutdown."

For the test, check the config and compare to real MAC addresses.

- Wrong MAC address(es) may be configured
- Maximum number of MAC addresses may be set too low

For a switch to forward a frame, the VLAN of that frame must exist and be active. There are four things to watch for / correct:

- Correct interfaces in correct VLANs
  - Identify which interfaces are access interfaces
  - If need to fix, use interface config command "switchport access vlan 20"
- A switch won't forward frames from VLANs that don't exist on that switch or are shutdown. For example, in a daisy chain of 3 switches, the middle switch must also have defined a VLAN that you hope to forward between the two end switches and have it "up." Since we're turning VTP off in CCENT, switches won't automatically learn from each other.

  show vlan [brief]

  Will always show defined VLANs.

  show running-config

  Won't show defined VLANs on VTP clients or servers (those switches have their VLANs stored in vlan.dat) Will show defined VLANs for VTP transparent or disabled.

  show vtp status

  Will tell you if VTP is client, server, transparent, or disabled
- Disabled VLANs—a VLAN can be active or "act/lshut" status. A switch will only pass traffic in active VLANs.

  show vlan [brief]

  The status column will tell you if the VLAN is active

  ```
  SW(config)# [no] shutdown vlan 10
  SW(config)# vlan 10
  SW(config-vlan)# [no] shutdown
  ```

  Two different ways to shutdown / activate a VLAN
- Misconfigured Trunks
  - Two switchports with "switchport mode dynamic auto" won't trunk; one must be "dynamic desirable."

    show interfaces fa0/1 switchport

    Administrative mode will tell you if "dynamic auto," etc. Operational mode will say if trunked.
  - An exam can manually create a situation where one end is trunked and the other not, so check the operational trunking states of both sides.

    ```
    S1(config-if)# switchport mode trunk
    S1(config-if)# switchport nonegotiate

    S2(config-if)# switchport mode dynamic desirable
    ```

    Negotiations will fail and this side won't be trunked. 802.1q tagged frames from the other side will be discarded