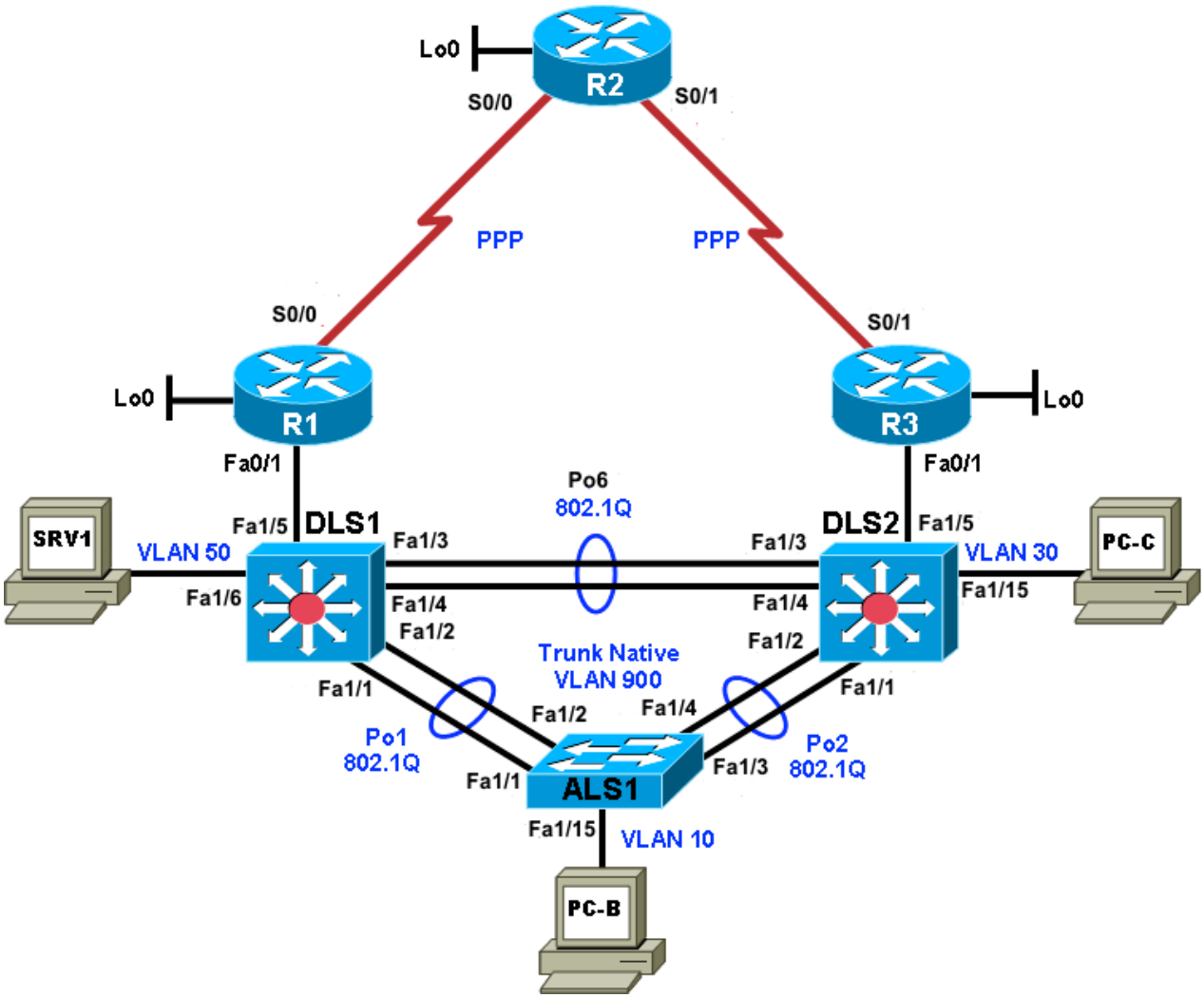
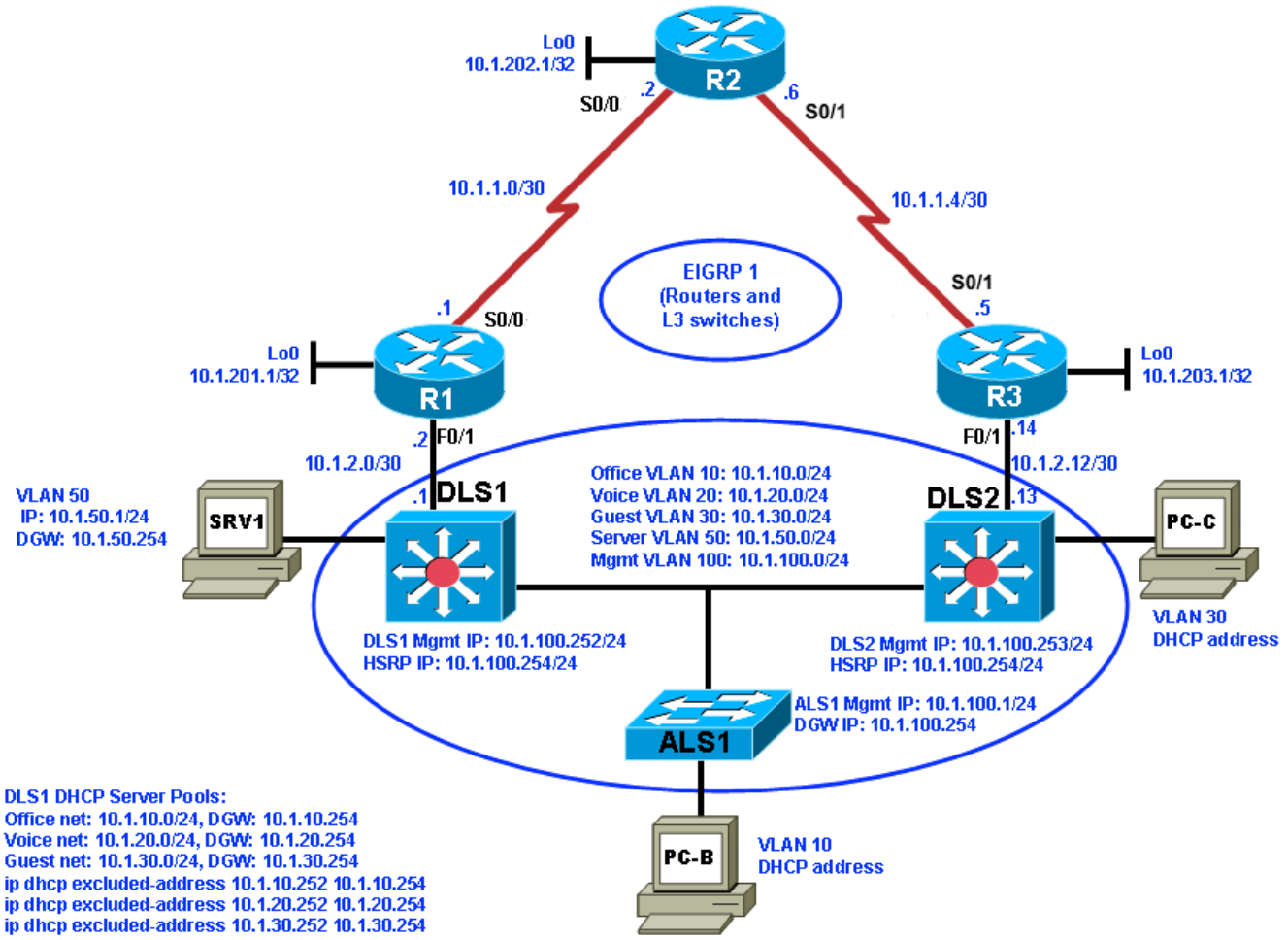
Lab 4-1, Layer 2 Connectivity and Spanning Tree

Physical Topology



Logical Topology



Objectives

- Load the device configuration files for each trouble ticket.
- Diagnose and resolve Layer 2 connectivity problems.
- Diagnose and resolve spanning-tree problems.
- Document the troubleshooting progress, configuration changes, and problem resolution.

Background

User computers, servers, and printers all connect to the access layer of the hierarchical model. With hundreds or thousands of hosts attached, access devices such as Layer 2 switches are a common source of networking issues. Physical and data-link problems at the access layer can include hardware, cabling, VLAN assignment, spanning tree, trunking protocol, or port security issues.

In this lab, you will troubleshoot various Layer 2 problems. For each task or trouble ticket, the scenario and symptoms are described. While troubleshooting, you will discover the cause of the problem, correct it, and then document the process and results.

Physical and Logical Topology Diagrams

The physical and logical topologies, including interface designations and IP addresses, are provided to assist the troubleshooting effort.

Lab Structure

This lab is divided into two main sections.

Section 1—Trouble Tickets and Troubleshooting Logs

This section includes multiple tasks. Each task is associated with a trouble ticket (TT) and introduces one or more errors on one or more devices. If time is a consideration, each task or trouble ticket can be performed independently.

Section 2—Troubleshooting Reference Information

This section provides general Layer 2 troubleshooting information that can be applied to any of the trouble tickets in this lab. Sample troubleshooting flows are provided, along with examples of useful commands and output. If time permits, it is recommended that you read through Section 2 prior to starting on the trouble tickets.

Note: Any changes made to the baseline configurations or topology (other than errors introduced) are noted in the trouble ticket so that you are aware of them prior to beginning the troubleshooting process.

Section 1—Trouble Tickets and Troubleshooting Logs

Task 1: Trouble Ticket Lab 41-A (1 Issue)

Step 1: Review trouble ticket Lab 41-A.

Late yesterday afternoon, access switch ALS1 failed, and you discovered that the power supply was not working. A junior colleague was tasked with replacing ALS1 with a comparable switch.

When you arrived this morning, you asked him how things went. He told you that he had stayed late trying to reconfigure ALS1, but was not entirely successful. Users are unable to use Telnet to connect to ALS1 (10.1.100.1) from SRV1. In addition, syslog messages from ALS1 are not being received on SRV1.

Your task is to diagnose the issues and restore switch ALS1 as a fully functional access switch on the network.

Step 2: Load the device trouble ticket configuration files for 41-A.

a. On each device issue the command **41-A**

b. In GNS3, go to **File**, select **Save Project As,** click Yes to Message and give it name **TSHOOT-41A**

c. Shut down GNS3, restart this new project. Restart all the devices.

Step 3: Clear mac address table on DSL1 and DSL2

a. `DLS1#clear mac`

b. `DLS2#clear mac`

Step 4: Check DHCP addresses on PC-B and PC-C.

Ensure that PC-B and PC-C are configured as DHCP clients and have the expected IP addresses.

Note: Problems introduced into the network by the trouble ticket might prevent one or both of these PCs from acquiring an IP address. Do not assign either PC a static address.

Step 5: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions, methods, and processes, and procedure and communication improvements.

_____

_____

_____

_____

Task 2: Trouble Ticket Lab 41-B (1 Issue)

Step 1: Review trouble ticket Lab 41-B.

This morning, the help desk received a call from an external consultant that needed access to the SRV1 guest account (simulated by ping). Her PC, PC-C, was plugged into one of the outlets that is patched to the guest VLAN on switch DLS2. However, she has not been able to get an IP address and cannot get onto the network.

Your task is to diagnose and solve this problem, making sure that the consultant gets access to SRV1.

Step 2: Load the device trouble ticket configuration files for 41-B.

a. On each device issue the command **41-B**

b. In GNS3, go to **File**, select **Save Project As,** click Yes to Message and give it name **TSHOOT-41B**

c. Shut down GNS3, restart this new project. Restart all the devices.

Step 3: Clear mac address table on DSL1 and DSL2

a. DLS1#**clear mac**

b. DLS2#**clear mac**

Step 4: Check DHCP addresses on PC-B and PC-C.

Ensure that PC-B and PC-C are configured as DHCP clients and have the expected IP addresses.

Note: Problems introduced into the network by the trouble ticket might prevent one or both of these PCs from acquiring an IP address. Do not assign either PC a static address.

Step 5: Document trouble ticket debrief notes.

Use this space to make notes of the key learning points that you picked up during the discussion of this trouble ticket with your instructor. The notes can include problems encountered, solutions applied, useful commands employed, alternate solutions and methods, and procedure and communication improvements.

_____

_____

_____

_____

_____

_____

_____

Section 2—Troubleshooting Reference Information

General Troubleshooting Process

As a general guideline, you can use the following general troubleshooting process described in the course:

1. Define the problem (symptoms).
2. Gather information.
3. Analyze the information.
4. Propose a hypothesis (possible cause).
5. Test the hypothesis.
6. Eliminate or accept the hypothesis.
7. Solve the problem.
8. Document the problem.

Command Summary

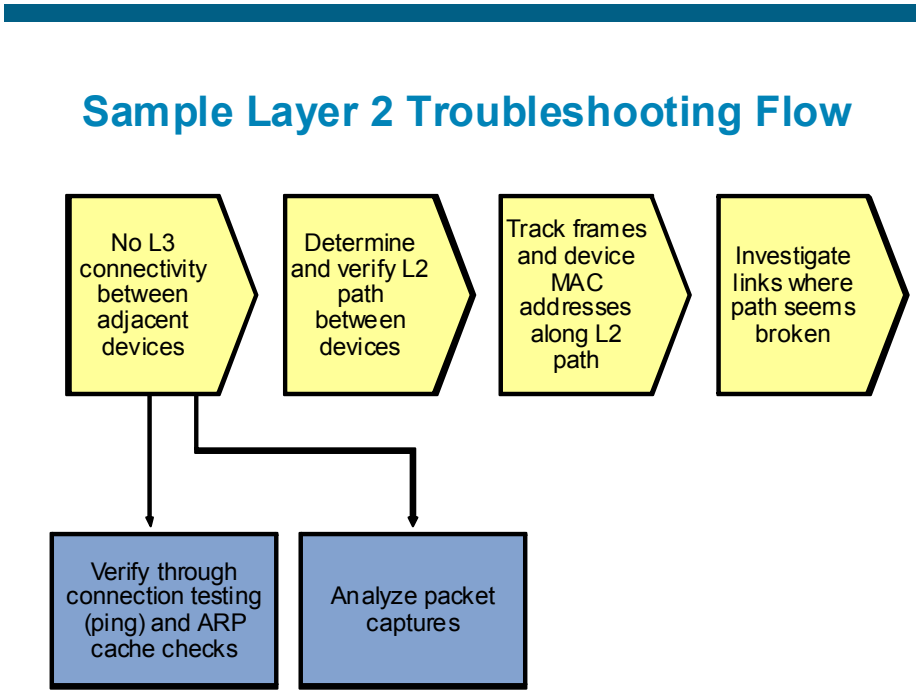
The table lists useful commands for this lab. The sample output is shown on following pages.

Command	Key Information Displayed
clear arp-cache	Clears ARP entries and resets aging.
show arp	Displays the IP address, MAC address, and interface.
show interfaces status	Displays link status, speed, duplex, trunk or VLAN membership, and interface descriptions.
show cdp neighbors (detail)	Displays device ID and type and confirms that a link is operational at the data link layer in both directions, including the sending and receiving ports. The **detail** option gives the remote device IP address.
show spanning-tree vlan *vlan#*	Displays all essential parameters that affect the topology, such as root port, designated ports, port state, and port type, as well as the spanning-tree mode implemented.
show spanning-tree inconsistentports	Displays a more detailed description of the type of port inconsistency and what might be causing it.
show spanning-tree summary	Displays the spanning-tree mode and the VLANs for which this switch is the root bridge. VLANs are listed along with the number of ports in various STP states.
show mac address-table address *mac-addr*	Displays the MAC address and interface entry in the table for the specified host.
show mac-address-table interface *intf-id*	Displays all MAC addresses that were learned on the specified port.
show vlan brief	Displays an overview of all existing VLANs and the ports

	within them. Trunk ports are not listed.
show vlan id *vlan#*	Displays whether the VLAN exists and, if so, which ports are assigned to it. Includes trunk ports on which the VLAN is allowed.
show interfaces *type/#*	Displays interface status, IP address/prefix, load, duplex, speed and packet statistics and errors.
show interfaces trunk	Displays all trunk ports, the operational status, trunk encapsulation, and native VLAN, as well as the list of allowed VLANs, active VLANs, and the VLANs in Spanning Tree Forwarding state for the trunk.
show interfaces *type/#* **switchport**	Checks all VLAN-related parameters for a specific interface (access ports and trunk ports).
show etherchannel summary	Displays port channels, the member ports, and flags indicating status.

Lab 4-1 Sample Troubleshooting Flows

The figure illustrates an example of a method that you could follow to diagnose and resolve Layer 2 problems.



Usually, you start troubleshooting the Layer 2 connectivity between devices because you have discovered that there is no Layer 3 connectivity between two adjacent Layer 2 hosts, such as two hosts in the same VLAN or a host and its default gateway. The following are typical symptoms that could lead you to start examining Layer 2 connectivity:

- Failing pings between adjacent devices. (This can also be caused by a host-based firewall that is blocking pings.)

- Address Resolution Protocol (ARP) failures. After clearing the ARP cache and triggering a connection attempt (for instance, by using ping), ARP entries show up as incomplete or are missing.
- Packets are not being received, which is shown by using a packet sniffer on the receiving host.

Confirm or Deny Layer 3 Connectivity

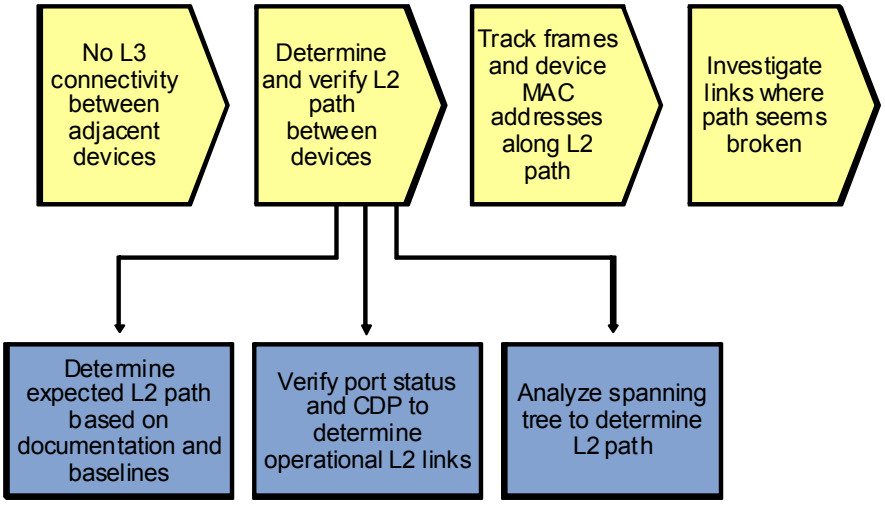
```
DLS1#ping 10.1.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

DLS1#clear arp-cache


DLS1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.10.1              0   0007.e963.ce53  ARPA   Vlan10
Internet  10.1.2.1               -   0017.5a5b.b442  ARPA   FastEthernet0/5
Internet  10.1.50.1              0   0007.e963.ce53  ARPA   Vlan50
Internet  10.1.100.1             0   001b.0c6d.8f41  ARPA   Vlan100
Internet  10.1.100.254           -   0000.0c07.ac64  ARPA   Vlan100
Internet  10.1.100.253           0   0017.5a53.a3c1  ARPA   Vlan100
Internet  10.1.100.252           -   0017.5a5b.b441  ARPA   Vlan100
Internet  10.1.50.252            -   0017.5a5b.b446  ARPA   Vlan50
Internet  10.1.50.254            -   0000.0c07.ac32  ARPA   Vlan50
Internet  10.1.20.252            -   0017.5a5b.b444  ARPA   Vlan20
Internet  10.1.30.252            -   0017.5a5b.b445  ARPA   Vlan30
Internet  10.1.10.252            -   0017.5a5b.b443  ARPA   Vlan10
```

The most relevant fields in the output are the IP address, hardware address, and interface fields, because these give you the essential information that you are usually looking for when you issue the **show arp** command.

The age field is also relevant. By default, ARP entries are cached for four hours. To make sure that you are looking at current information, you can use the **clear arp-cache** command to flush existing entries from the cache.

If there is a "-" in the age field instead of a number, this entry is local to the switch. These entries represent locally configured IP and MAC addresses, and the switch will respond to ARP requests for these entries.

Sample Layer 2 Troubleshooting Flow



If you have determined that the problem is most likely a Layer 2 or Layer 1 problem, you want to reduce the scope of the potential failures. You can diagnose Layer 2 problems with the following common troubleshooting method:

- Determine the Layer 2 path. Based on documentation, baselines, and knowledge of your network in general, the first step is to determine the path that you would expect frames to follow between the affected hosts. Determining the expected traffic path beforehand helps you in two ways: It gives you a starting point for gathering information about what is actually happening on the network, and it makes it easier to spot abnormal behavior. The second step in determining the Layer 2 path is to follow the expected path and verify that the links on the expected path are actually up and forwarding traffic. If the actual traffic path is different from your expected path, this step might give you clues about the particular links or protocols that are failing and the cause of these failures.
- Track the flow of traffic across the Layer 2 path. By following the expected Layer 2 path and verifying that frames actually flow along that path, you can likely find the spot where the connectivity is failing.
- When you have found the spot where the connectivity is failing, examine the link or links where the path is broken. Now you can apply targeted troubleshooting commands to find the root cause of the problem. Even if you cannot find the underlying cause of the problem yourself, by reducing the scope of the problem, you have a better-defined problem that can be escalated to the next level of support.

Although there are many different approaches to troubleshooting Layer 2 problems, the elements mentioned above will most likely be part of any methodical approach. These elements are not necessarily executed in the presented order. Determining the expected path and verifying the actual path often go hand-in-hand.

To determine the traffic path between the affected hosts, you can combine knowledge from the following sources:

- **Documentation and baselines:** Documentation that was written during design and implementation usually contains information about the intended traffic paths between the hosts. If the documentation does not provide this information, you can usually reconstruct the expected flow of traffic by analyzing network diagrams and configurations.
- **Link status across the path:** A very straightforward check after you have determined the expected path of the traffic is to verify that all ports and links in the path are operational.

- **Spanning-tree topology:** In Layer 2 networks that have a level of redundancy built into the topology, analyze the operation of Spanning Tree Protocol (STP) to determine which of the available links will be used.

Verify Link Status

```
DLS1#show interfaces status

Port      Name               Status       Vlan     Duplex  Speed Type
Fa0/1     Channel to ALS1    connected    trunk    a-full  a-100 10/100BaseTX
Fa0/2     Channel to ALS1    connected    trunk    a-full  a-100 10/100BaseTX
Fa0/3     Channel to DLS2    connected    trunk    a-full  a-100 10/100BaseTX
Fa0/4     Channel to DLS2    connected    trunk    a-full  a-100 10/100BaseTX
Fa0/5     FE to R1           notconnect   routed     full    100 10/100BaseTX
Fa0/6     FE to SRV1         connected    50       a-full  a-100 10/100BaseTX
Fa0/7     Unused             disabled     999        auto   auto 10/100BaseTX
<output omitted>
Fa0/24    Unused             disabled     999        auto   auto 10/100BaseTX
Gi0/1     Unused             disabled     999        auto   auto Not Present
Gi0/2     Unused             disabled     999        auto   auto Not Present
Po1       Channel to ALS1    connected    trunk    a-full  a-100
Po10      Channel to DLS2    connected    trunk    a-full  a-100
```

To determine link status on switches, the **`show interfaces status`** command is useful because it gives a brief overview of all the interfaces on the switch as well as contains important elements, such as link status, speed, duplex, trunk or VLAN membership, and interface descriptions. If the link is up, the Status field shows “connected.” If it is down up, “notconnect” is in the Status field. If the link has been administratively shut down, the status is “disabled.”

```
DLS1#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
R1.tshoot.net    Fas 0/5           151          R S I     1841      Fas 0/1
ALS1.tshoot.net  Fas 0/2           153            S I     WS-C2960- Fas 0/2
ALS1.tshoot.net  Fas 0/1           153            S I     WS-C2960- Fas 0/1
DLS2.tshoot.net  Fas 0/4           172          R S I     WS-C3560- Fas 0/4
DLS2.tshoot.net  Fas 0/3           172          R S I     WS-C3560- Fas 0/3
```

If the Cisco Discovery Protocol is enabled between the switches and routers, you can use the **`show cdp neighbor`** command to confirm that a link is operational at the data link layer in both directions. Also, it is essential in uncovering cabling problems because it records both the sending and receiving ports, as can be seen in the output above.

Analyze Spanning Tree

```
ALS1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     0017.5a5b.b400
             Cost        12
             Port        56 (Port-channel1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001b.0c6d.8f00
```

```
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------

Fa0/18              Desg FWD 19        128.18   P2p Edge
Po1                 Root FWD 12        128.56   P2p
Po2                 Altn BLK 12        128.64   P2p
```

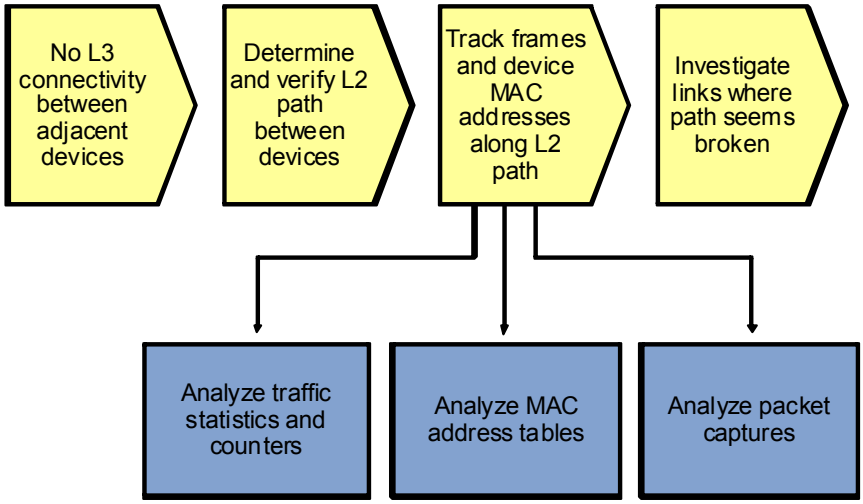
To analyze the spanning-tree topology and the consequences that STP has for the Layer 2 path, the **show spanning-tree vlan** *vlan-id* command is a good starting point. It lists all essential parameters that affect the topology, such as the root port, designated ports, port state, and port type.

Typical values for the port status field are BLK (blocking) and FWD (forwarding). You might also see LIS or LTN (listening), and LRN (learning) while STP is converging.

The states LBK (loopback), DWN (down), or BKN (broken) typically indicate problems. If the value is BKN, the Type field indicates what is causing the broken status. Possible values are ROOT_Inc, LOOP_Inc, PVID_Inc, TYPE_Inc, or PVST_Inc. To get a more detailed description of the type of inconsistency and what might be causing it, you can examine the output of the **show spanning-tree inconsistentports** command. Interface Type and information includes:

- P2p or Shr to indicate the link type (typically based on duplex status – P2p is full-duplex and Shr is half-duplex or shared Ethernet).
- Edge for edge (PortFast) ports.
- Bound for boundary ports when this switch is running 802.1s (MST) and the other switch is running a different spanning-tree variety. The output also indicates which other type of STP was detected on the port.
- Peer for peer ports when this switch is running Per VLAN Spanning Tree Plus (PVST+) or Per VLAN Rapid Spanning Tree Plus (PVRST+) and the other switch is running a different standard variety of STP (802.1D or 802.1s MST).

Sample Layer 2 Troubleshooting Flow



After you have determined the Layer 2 path between the two affected hosts, you can start tracking the traffic between the hosts as it is being switched along the path. The most direct approach to tracking the traffic is to capture packets at set points along the path by using a packet sniffer. Tracking packets in real time is a fairly intensive procedure, and technical limitations might restrict the links where traffic captures could be collected. However, it is the most definitive proof that traffic is or is not flowing along specific paths and links. A less labor-intensive method is to track the flow of traffic by analyzing MAC address tables or traffic statistics. These methods are less direct, because you are not looking at the actual traffic itself but at traces left by the passing of frames.

In a network that has not yet gone into production, packet statistics can help you see where traffic is flowing. On live networks, the test traffic that you are generating will be lost against the background of the live traffic patterns in most cases. However, if the switches that you are using have the capability to track packet statistics for access lists, you might be able to write an access list that matches the specific traffic that you are interested in and isolate the traffic statistics for that type of traffic.

A method of tracing traffic that can be used under all circumstances is analyzing the process of MAC address learning along the Layer 2 path. When a switch receives a frame on a particular port and for a particular VLAN, it records the source MAC address of that frame together with the port and VLAN in the MAC address table. Therefore, if the MAC address of the source host is recorded in a switch but not on the next switch in the path, it indicates a communication problem between these switches for the VLAN concerned, and the link between these switches should be examined.

Analyze MAC Address Tables

```
DLS1#show mac address-table

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 <Output omitted>
  50    0000.0c07.ac32    STATIC      CPU
  50    0007.e963.ce53    DYNAMIC     Fa0/6
```

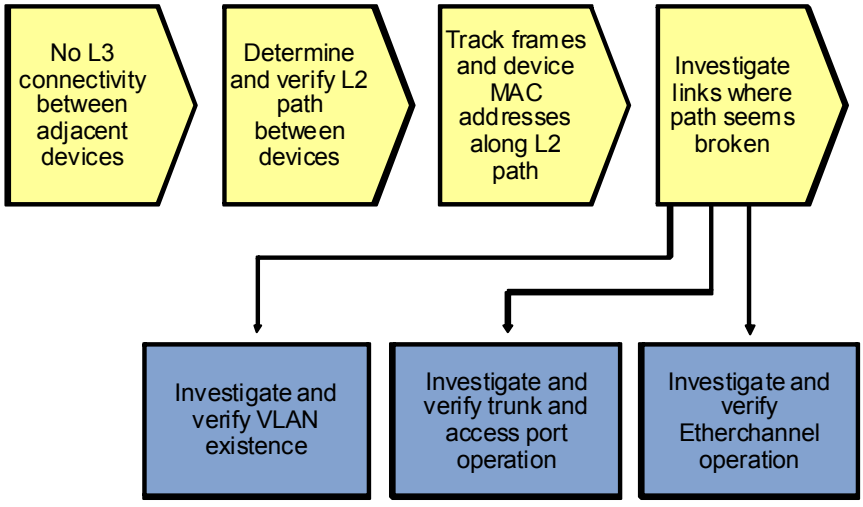
```
  50    0017.5a53.a385    DYNAMIC     Po10
  50    0017.5a53.a3c6    DYNAMIC     Po10
  10    0000.0c07.ac0a    DYNAMIC     Po10
  10    000b.db04.a5cd    DYNAMIC     Po1
  20    0000.0c07.ac14    DYNAMIC     Po10
  20    0017.5a53.a385    DYNAMIC     Po10
  30    0000.0c07.ac1e    DYNAMIC     Po10
 100    0000.0c07.ac64    STATIC      CPU
 100    0017.5a53.a3c1    DYNAMIC     Po10
 100    001b.0c6d.8f41    DYNAMIC     Po1
Total Mac Addresses for this criterion: 32


DLS1#show mac address-table address 0000.0c07.ac0a
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0000.0c07.ac0a    DYNAMIC     Po10
Total Mac Addresses for this criterion: 1
```

You can use the **show mac-address-table** command to check the content of the MAC address table. Because this table usually contains hundreds to thousands of entries, you can narrow the results to find what you are looking for by using command options.

If you are looking for the MAC address of a specific host, use the **show mac-address-table address** *mac-address* option.

Another useful option is **show mac-address-table interface** *intf-id*, which shows which MAC addresses were learned on a specific port.

Sample Layer 2 Troubleshooting Flow



After you have found the spot in the Layer 2 path where one switch is learning the source MAC address and the next switch is not, examine the link between those two switches carefully.

When trying to determine what could cause the MAC address not to be learned on the next switch, consider the following questions:

- Does the VLAN exist on the next switch?
- Is there an operational trunk between the two switches?
- Is the VLAN allowed on the trunk between the switches?
- If an EtherChannel is between the switches, is the EtherChannel fully operational?

Verify VLAN Existence

```
ALS1#show vlan brief

VLAN Name                         Status    Ports
---- ------------------------     --------- -------------------------------
1    default                      active
10   OFFICE                       active    Fa0/18
20   VOICE                        active    Fa0/18
30   GUEST                        active
100  MGMT                         active
900  NATIVE                       active
999  UNUSED                       active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                            Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                            Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                            Fa0/17, Fa0/19, Fa0/20, Fa0/21
                                            Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                            Gi0/2
1002 fddi-default                       act/unsup
1003 token-ring-default                 act/unsup
1004 fddinet-default                    act/unsup
1005 trnet-default                      act/unsup
```

To get a quick overview of all existing VLANs, use the **show vlan brief** command. However, this command does not list the trunk ports. For instance, in the sample output above, trunk ports F0/1, F0/2, F0/3, and F0/4 are not listed. FastEthernet 0/18 is listed as the only port in VLANs 10 and 20.

```
ALS1#show vlan id 10

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
10   OFFICE                           active    Fa0/18, Po1, Po2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
10   enet  100010     1500  -      -      -        -    -        0      0
```

To verify the existence of a particular VLAN on a switch, use the **show vlan id** *vlan-id* command. This command shows you whether the VLAN exists and which ports are assigned to it. This command includes trunk ports that the VLAN is allowed on. For the same VLAN 10 that was referenced in the previous output, you now see interface port channel 1 and port channel 2 listed as ports that are associated with VLAN 10.

Verify Trunk Operation

```
ALS1#show interfaces trunk
```



```
Port        Mode             Encapsulation  Status        Native vlan
Po1         on               802.1q         trunking      900
Po2         on               802.1q         trunking      900

Port        Vlans allowed on trunk
Po1         10,20,30,100
Po2         10,20,30,100

Port        Vlans allowed and active in management domain
Po1         10,20,30,100
Po2         10,20,30,100

Port        Vlans in spanning tree forwarding state and not pruned
Po1         10,30,100
Po2         20
```

The easiest way to get an overview of trunk operation is by using the **show interface trunk** command. Not only does it list trunk status, trunk encapsulation, and the native VLAN, but it also lists the allowed VLANs, active VLANs, and VLANs in Spanning Tree Forwarding state for the trunk. The last list can be very helpful in determining whether frames for a particular VLAN will be forwarded on a trunk.

For instance, in the example, you can see that both interface port channel 1 and port channel 2 allow VLANs 10, 20, 30, and 100, but VLANs 10, 30, and 100 are forwarded on port channel 1, while VLAN 20 is forwarded on port channel 2.

Verify VLAN Port Status

```
ALS1#show interfaces fastEthernet 0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (OFFICE)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 20 (VOICE)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none

<Output Omitted>
```

To check all VLAN-related parameters for a specific interface, use the **show interface** *intf-id* **switchport** command. This command applies to access ports as well as trunk ports. For instance, in the example output, the port is configured as a static access port in VLAN 10, and VLAN 20 is assigned to the port as a voice VLAN.

Verify EtherChannel Operation

```
ALS1#show etherchannel summary
Flags:  D - down        P - bundled 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

        M - not in use, minimum links not met
        u - unsuitable for bundling
        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)          -        Fa0/1(P)    Fa0/2(P)
2      Po2(SU)          -        Fa0/3(P)    Fa0/4(P)
```

When an EtherChannel is configured between the switches and you suspect that EtherChannel operation could be causing the communication failure between the switches, you can verify this by using the **show etherchannel summary** command. Although the command output is fairly self-explanatory, the typical things to look for is the lowercase “s” flag, which indicates that a physical interface is suspended because of incompatibility with the other ports in the channel or the uppercase “D” flag, which indicates that an interface (physical or port channel) is down.