

Troubleshooting Fundamentals Lab – Phase 1.3

Objective

Host C is unable to communicate with hosts A and B. Investigate the issue and resolve it if possible.

Topology Overview

There are three hosts. **Hosts A and B** are connected to **SW1**. **Host C** is connected to **SW2**. There is an **inter-switch** link between SW1 and SW2.

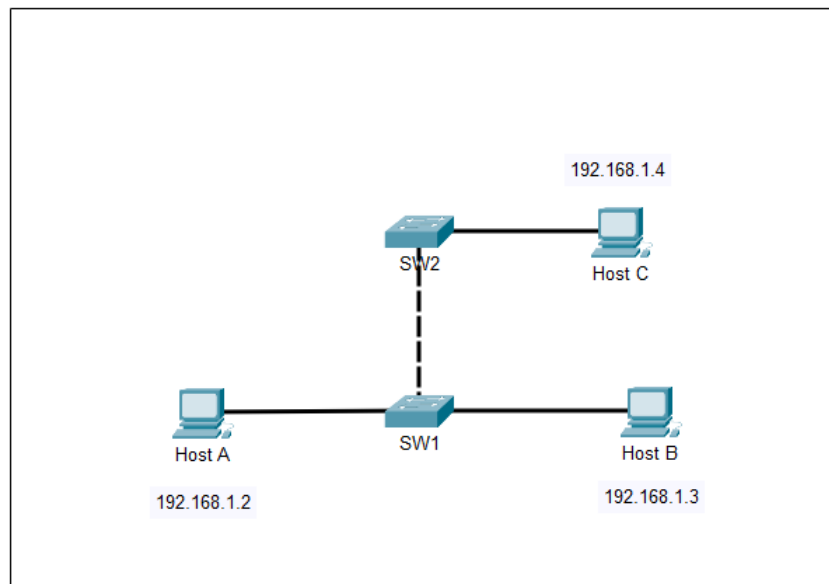


Figure 1 – Lab Topology

Step 1 – Verify the Problem

From **Host C**, ping hosts **A** and **B**.

Result: **Ping fails**

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>|
```

Figure 2 – Unsuccessful ping from host C to hosts A and B

The Issue is confirmed.

Step 2 – Decide Where to Start

With the issue confirmed, it is understood that **Host C does not have reachability to hosts A and B**. We could immediately begin checking physical components, but doing so would skip an opportunity to gather additional useful information. Before selecting a starting point, it is helpful to ask another question:

Can hosts A and B communicate with each other?

The answer to this question provides valuable clues that help determine both the most logical starting point and which device is most relevant to examine first. Checking expectations against another device helps reveal whether the issue is localized to one part of the network or more widespread.

From **Host A**, ping host **B**.
Result: **Ping Succeeds**

These results reveal several important details:

- Hosts A and B can communicate.
- Their respective switchports are likely functioning correctly.
- The issue is most likely localized to Host C, its switchport, or SW1 and SW2.

What must be true for communication to work? Each requirement becomes something that can be verified.

Layer 1 – Physical Requirements

For Host C to communicate with the network, several physical requirements must be true.

- Host C must be powered on.
- The cabling between Host C and SW2 must be correct and operational.
- The cabling between SW1 and SW2 must be correct and operational.
- The switchport connected to Host C must show the status of **connected**.
- The inter-switch link between SW1 and SW2 must show the status of **connected**.

If these requirements are validated as true, the issue is less likely to be caused by a Layer 1 problem. Maintaining a structured troubleshooting approach, the next logical step is to examine **Layer 2**.

Layer 2 – Data Link Requirements

- The ports connected to the hosts must be assigned to the **same VLAN**.
- The ports between SW1 and SW2 must both operate as trunks or both operate as access ports in the same VLAN.
- If the inter-switch link is configured as a trunk, the VLAN used by the hosts must be allowed on the trunk.

Step 3 – Switch Verification

On SW1 and SW2, examine the switchport status and VLAN assignments.

```
show interface status
```

Observation:

- All host-facing switchports are assigned to **VLAN 10**.
- SW1's connection toward SW2 is configured as a **trunk**
- SW2's connection toward SW1 is configured as an **access port** assigned to default **VLAN 1**.

```
SW1#show int status
Port      Name      Status      Vlan      Duplex  Speed  Type
Fa0/1     Host_A    connected   10        a-full  a-100  10/100BaseTX
Fa0/2     Host_B    connected   10        a-full  a-100  10/100BaseTX
Fa0/3     notconnect 1          auto      auto    10/100BaseTX
Fa0/4     SW2       connected   trunk     a-full  a-100  10/100BaseTX
```

Figure 3 – SW1 show interface status output

```
SW2#sh int status
Port      Name      Status      Vlan      Duplex  Speed  Type
Fa0/1     SW1       connected   1         a-full  a-100  10/100BaseTX
Fa0/2     Host_C    connected   10        a-full  a-100  10/100BaseTX
Fa0/3     notconnect 1          auto      auto    10/100BaseTX
```

Figure 4 – SW2 show interface status output

This mismatch explains the problem. One side of the inter-switch link is operating as a trunk while the other side is operating as an access port in VLAN 1. As a result, traffic for VLAN 10 cannot traverse the link correctly.

Step 4 – Correct and Validate

On the SW2, reconfigure the port connected to SW1 as a trunk.

```
interface fa0/1
 switchport mode trunk
```

Note: Configuring both inter-switch ports as access ports in **VLAN 10** would also have been a valid solution. However, this lab expects **SW2's switchport** to be configured as a **trunk**.

```
SW2#show int status
Port      Name      Status      Vlan      Duplex  Speed  Type
Fa0/1     SW1       connected   trunk     a-full  a-100  10/100BaseTX
Fa0/2     Host_C    connected   10        a-full  a-100  10/100BaseTX
Fa0/3                     notconnect  1         auto    auto   10/100BaseTX
```

Figure 5 – SW2 show interface status output

To verify trunk operations, use:

```
show interface trunk
```

Figure 5 shows that SW2's connection toward SW1 is now configured as a trunk. However, if connectivity is tested immediately after the change, the ping may still fail. This is because **Spanning Tree Protocol** must transition the link through its states before forwarding traffic.

```
SW2#sh int trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     none

SW2#
```

Figure 6 – SW2 show interface trunk output one

The output of the command will reveal details about trunks configured on a switch. Important details are:

- Encapsulation is configured for **802.1Q**
- The **native VLAN** is the default **VLAN 1**
- VLANs **allowed** on the trunk are **1 - 1005**
- VLANs allowed and **active** in management domain include **1 and 10**
- VLANs in spanning tree **forwarding state and not pruned**

That last line is especially important. A VLAN can be allowed on a trunk and still not forward traffic if Spanning Tree has not yet placed it into the forwarding state. If the VLAN is not listed on that final line, traffic for that VLAN will not successfully traverse the trunk. Forgetting this can make it seem like the problem has not been resolved when, in fact, the network is still converging.

After approximately **50 seconds**, Spanning Tree completes its transition, and **VLAN 10** should appear in the final line of the output.

```
SW2#show int trunk
Port      Mode      Encapsulation  Status        Native vlan
Fa0/1     on        802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10

SW2#
```

Figure 7 – SW2 show interface trunk output two

Re-test ping.

Result: Pings succeed