1.6 – ENSA - PacketKnows – Configuring Trunks

Addressing Table

Device	Interface	IP Address	Subnet Mask	Switch Port	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	S2 F0/11	10
PC2	NIC	172.17.20.22	255.255.255.0	S2 F0/18	20
PC3	NIC	172.17.30.23	255.255.255.0	S2 F0/6	30
PC4	NIC	172.17.10.24	255.255.255.0	S3 F0/11	10
PC5	NIC	172.17.20.25	255.255.255.0	S3 F0/18	20
PC6	NIC	172.17.30.26	255.255.255.0	S3 F0/6	30

Objectives

- **Part 1: Verify VLANs**
- **Part 2: Configure Trunks**
- **Step 3: Verify connectivity.**

NOTE

- **Power all the devices first by clicking the triangle button on the upper navbar.**
- **Right click the device then click the web console first to configure on the device**
- **Always type “save” when configuring IP addresses of PC’s**

Background

Trunks are required to pass VLAN information between switches. A port on a switch is either an access port or a trunk port. Access ports carry traffic from a specific VLAN assigned to the port. A trunk port by default is a member of all VLANs; therefore, it carries traffic for all VLANs. This activity focuses on creating trunk ports, and assigning them to a native VLAN other than the default.

Part 1: Verify VLANs

Step 1: Display the current VLANs.

a. On **S1**, issue the command that will display all VLANs configured. There should be ten VLANs in total. Notice how all 24 access ports on the switch are assigned to VLAN 1.

b. On S2 and S3, display and verify all the VLANs are configured and assigned to the correct switch ports according to the Addressing Table.

Step 2: Verify loss of connectivity between PCs on the same network.

Although **PC1** and **PC4** are on the same network, they cannot ping one another. This is because the ports connecting the switches are assigned to VLAN 1 by default. In order to provide connectivity between the PCs on the same network and VLAN, trunks must be configured.

Part 2: Configure Trunks

Step 1: Configure trunking on S2 and use VLAN 99 as the native VLAN.

a. Configure e1/0 and e1/1 interfaces on S1 for trunking.

b. Configure VLAN 99 as the native VLAN for e1/0 and e1/1 interfaces on **S1**.

The trunk port takes about a minute to become active due to Spanning Tree. Click **Fast Forward Time** to speed the process. After the ports become active, you will periodically receive the following syslog messages:

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/0 (99), with S3 Ethernet1/0 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/1 (99), with S2 Ethernet1/1 (1).

You configured VLAN 99 as the native VLAN on S1. However, S2 and S3 are using VLAN 1 as the default native VLAN as indicated by the syslog message.

Although you have a native VLAN mismatch, pings between PCs on the same VLAN are now successful. Why?
Pings are successful because trunking has been enabled on S1. Dynamic Trunking Protocol (DTP) has automatically negotiated the other side of the trunk links. In this case, S2 and S3 have now automatically configured the ports attached to S1 as trunking ports.

Step 2: Verify trunking is enabled on S2 and S3.

On **S2** and **S3**, issue the **show interface trunk** command to confirm that DTP has successfully negotiated trunking with S1 on S2 and S3. The output also displays information about the trunk interfaces on S2 and S3.

Which active VLANs are allowed to cross the trunk?
1, 10, 20, 30, and 99.

Step 3: Correct the native VLAN mismatch on IOU1 **and** IOU**3.**

a. Configure VLAN 99 as the native VLAN for the appropriate interfaces on S2 and S3.

b. Issue **show interface trunk** command to verify the correct native VLAN configuration.

Step 3: Verify loss of connectivity.

Try pinging between PC1 and PC4. Although the access ports are assigned to the appropriate VLANs, were the pings successful?