Packet Tracer – Skills Integration Challenge

1. Topology



Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| S1 | VLAN 88 | 172.31.88.2 | 255.255.255.0 | 172.31.88.1 |
| S2 | VLAN 88 | 172.31.88.3 | 255.255.255.0 | 172.31.88.1 |
| S3 | VLAN 88 | 172.31.88.4 | 255.255.255.0 | 172.31.88.1 |
| PC1 | NIC | 172.31.10.21 | 255.255.255.0 | 172.31.10.1 |
| PC2 | NIC | 172.31.20.22 | 255.255.255.0 | 172.31.20.1 |
| PC3 | NIC | 172.31.30.23 | 255.255.255.0 | 172.31.30.1 |
| PC4 | NIC | 172.31.10.24 | 255.255.255.0 | 172.31.10.1 |
| PC5 | NIC | 172.31.20.25 | 255.255.255.0 | 172.31.20.1 |
| PC6 | NIC | 172.31.30.26 | 255.255.255.0 | 172.31.30.1 |

1. VLANs and Port Assignment Table

|  |  |  |
| --- | --- | --- |
| Ports | Assignment | Network |
| F0/7 - 12 | VLAN 10 - Sales | 172.31.10.0/24 |
| F0/13 -20 | VLAN 20 - Production | 172.31.20.0/24 |
| F0/1 - 6 | VLAN 30 - Marketing | 172.31.30.0/24 |
| Interface VLAN 88 | VLAN 88 - Management | 172.31.88.0/24 |
| Trunks | VLAN 99 - Native | N/A |

Scenario

In this activity, two switches are completely configured. On a third switch, you are responsible for assigning IP addressing to the Switch Virtual Interface, configuring VLANs, assigning VLANs to interfaces, configuring trunking, and performing basic switch security.

1. Requirements

**S1** and **S2** are fully configured. You cannot access these switches. You are responsible for configuring **S3** with the following requirements:

* IP addressing and default gateway configuration, according to the **Addressing Table**.
* Create, name, and assign VLANs according to the **VLANs and Port Assignment Table**.
* Assign the native VLAN 99 to the trunk port and disable DTP.
* Restrict the trunk to only allow VLANs 10, 20, 30, 88, and 99.
* Use VLAN 99 as the native VLAN on the trunk ports.
* Configure basic switch security on S3.
  1. Encrypted secret password of **itsasecret**
  2. Console password of **letmein**
  3. VTY password of **c1$c0** (where 0 is the number zero)
  4. Encrypted plain text passwords
  5. MOTD banner with the message **Authorized Access Only!!**
  6. Disable unused ports.
* Configure port security on **F0/6**.
  1. Only two unique devices are allowed to access the port.
  2. Learned MACs are added to the running configuration.
  3. Secure the interface so that a notification is sent when there is a violation, but the port is not disabled.
* Verify the PCs in the same VLAN can now ping each other.