

NST21022 - Practical for Network Switching and Routing

Department of Information & Communication Technology

Faculty of Technology, SEUSL

Lab Sheet – 11

Title: Introduction to VLANs

Aim:

- Getting familiar with VLANs and SSH

Task:

- Configure Basic Configuration
- Configure VLANs
- Configure Trunks
- Configure Secure Password and SSH

Use “NST21022 Labsheet 11.pka” file

Activities

Addressing Table

Device	Interface	IP Address	Subnet Mask	VLAN
PC-A	NIC	192.168.1.10	255.255.255.0	10
PC-B	NIC	192.168.2.10	255.255.255.0	20
PC-C	NIC	192.168.3.10	255.255.255.0	30
PC-D	NIC	192.168.1.20	255.255.255.0	10
PC-E	NIC	192.168.2.20	255.255.255.0	20
PC-F	NIC	192.168.3.20	255.255.255.0	30
Management	NIC	192.168.4.20	255.255.255.0	99
S1	VLAN 99	192.168.4.11	255.255.255.0	
S2	VLAN 99	192.168.4.10	255.255.255.0	
S3	VLAN 99	192.168.4.12	255.255.255.0	

Exercise 01: Configure Basic Configuration

1. Configure the hostname for all Switches according to Addressing Table
2. Set the domain name to ccna.com for all switches

S1(config)# ip domain-name ccna.com

Exercise 02: VLAN Configuration

1. On S1 issue the command that displays all VLANs configured. By default, all interfaces are assigned to VLAN1.

NST21022 - Practical for Network Switching and Routing

Department of Information & Communication Technology

Faculty of Technology, SEUSL

2. Notice that each PC can ping the other PC that shares the same subnet.
 - a) PC1 can ping PC4
 - b) PC2 can ping PC5
 - c) PC3 can ping PC6
 3. Create and name VLANs on S1
 - a) Create the following VLANs. Names are case-sensitive and must match the requirement exactly.
 - i. VLAN 10: Staff
- ```
S1#(config)# vlan 10
S1#(config-vlan)# name Staff
```
- b) Create the remaining VLANs.
      - i. VLAN 20: Student
      - ii. VLAN 30: Guest
      - iii. VLAN 99: Management
      - iv. VLAN 150: VOICE
    - c) Verify the VLAN configuration using show vlan brief command
  4. 4. Create the VLANs on S2 and S3
    - a) Use the same commands from Number 3 to create and name the same VLANs on S2 and S3.
    - b) Verify VLAN configuration
  5. Assign VLANs to the active ports on S2.
    - a) Configure the interfaces as access ports and assign the VLANs as follows.
      - i. LAN 10: FastEthernet 0/1

```
S2(config)# interface f0/1
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 10
```

## NST21022 - Practical for Network Switching and Routing

Department of Information & Communication Technology

Faculty of Technology, SEUSL

---

- b) Assign the remaining ports to the appropriate VLAN
  - i. VLAN 20: FastEthernet 0/11
  - ii. VLAN 30: FastEthernet 0/21
  - iii. VLAN 99: FastEthernet 0/24
- 6. Assign VLANs to the active ports on S3.
  - a) S3 uses the same VLAN access port assignments as S2. Configure the interfaces as access ports and assign the VLANs as follows:
    - i. VLAN 10: FastEthernet 0/1
    - ii. VLAN 20: FastEthernet 0/11
    - iii. VLAN 30: FastEthernet 0/21
- 7. 7. Assign the VOICE VLAN to FastEthernet 0/1 on S3.
  - a) Configure FastEthernet 0/11 for Cisco IP Phone and PC-D.

The S3 F0/1 interface must be configured to support user traffic to PC-D using VLAN 10 and voice traffic to the IP phone using VLAN 150. The interface must also enable QoS and trust the Class of Service (CoS) values assigned by the IP phone. IP voice traffic requires a minimum amount of throughput to support acceptable voice communication quality. This command helps the switchport to provide this minimum amount of throughput.

```
S3(config)# interface f0/1
S3(config-if)# mls qos trust cos
S3(config-if)# switchport voice vlan 150
```

8. Verify loss of connectivity.

Previously, PCs that shared the same network could ping each other successfully.

Study the output of from the following command on S2 and answer the following questions based on your knowledge of communication between VLANs. Pay close attention to the Gig0/1 port assignment.

*S2# show vlan brief*

- a) Try pinging between PC-A and PC-D

### **Exercise 03: Configure Trunks**

1. Configure trunking on S1 and use VLAN 99 as the native VLAN.

- a) Configure G0/1 and G0/2 interfaces on S1 for trunking.

*S1(config)# interface range g0/1 - 2*

*S1(config-if)# switchport mode trunk*

- b) Configure VLAN 99 as the native VLAN for G0/1 and G0/2 interfaces on S1.

*S1(config-if)# switchport trunk native vlan 99*

The trunk port takes about a short time to become active due to Spanning Tree Protocol. After the ports become active, you will periodically receive the following syslog messages:

*%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (99), with S3 GigabitEthernet0/2 (1).*

*%CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (99), with S2 GigabitEthernet0/1 (1).*

you configured VLAN 99 as the native VLAN on S1. S2 and S3 are using VLAN as the default native VLAN as indicated by the syslog message.

2. Correct the native VLAN mismatch on S2 and S3.
  - 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 configured.
3. Verify configurations on S2 and S3.
  - a) Issue the show interface interface switchport command to verify that the native VLAN is now 99.

- b) Use the show vlan command to display information regarding configured VLANs.

**Exercise 04: Configure Secure Password and SSH**

1. Configure IP address for Management VLAN according to Addressing Table and enable interface status
2. Create a user of your choosing with a strong encrypted password.

*S2(config)# username root secret cisco*

3. Generate 1024-bit RSA keys.

Note: In Packet Tracer, enter the crypto key generate rsa command and press Enter to continue.

*S2(config)# crypto key generate rsa*

The name for the keys will be: RTA.CCNA.com. Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

*How many bits in the modulus [512]: 1024*

4. Configure all VTY lines for SSH access and use the local user profiles for authentication.

*S2(config)# line vty 0 4*

*S2(config-line)# transport input ssh*

*S2(config-line)# login local*

5. Set the EXEC mode timeout to 6 minutes on the VTY lines.

*S2(config-line)# exec-timeout 6*

6. Save the configuration to NVRAM.
7. Access the command prompt on the desktop of Management PC to establish an SSH connection to S2. Open a command prompt

*C:\> ssh /?*

*Packet Tracer PC SSH*

*Usage: SSH -l username target*

*C:\>*

8. Configure SSH to S1 and S3