Hotel management system for VLAN Configuration in Cisco Packet Tracer

To configure a VLAN (Virtual Local Area Network) for a Hotel Management System in Cisco Packet Tracer, the typical approach involves segmenting the network into different VLANs for departments like reception, housekeeping, management, and guest services. This allows better traffic management, security, and isolation between different sections of the network.

Below are the steps and commands to configure VLANs in Cisco Packet Tracer for a Hotel Management System.

**Scenario**

* **Reception VLAN** (ID: 10)
* **Housekeeping VLAN** (ID: 20)
* **Management VLAN** (ID: 30)
* **Guest VLAN** (ID: 40)

Each department will have a different VLAN, and we will use a switch and a router to handle inter-VLAN routing.

**Step-by-Step Procedure**

**1. Create VLANs on the Switch**

First, assign the ports on the switch to their respective VLANs.

1. Open Cisco Packet Tracer.
2. Add a **switch** (e.g., 2960 switch).
3. Add **PCs** to represent the devices in each VLAN.
4. Connect each PC to the switch using cables.

**Commands to Configure VLANs**

1. Open the switch's CLI.
2. Enter global configuration mode:

A black rectangular object with a black stripe

Description automatically generated

Switch> enable

Switch# configure terminal

1. Create VLANs for the hotel departments:

A screenshot of a computer program

Description automatically generated

Switch(config)# vlan 10

Switch(config-vlan)# name Reception

Switch(config-vlan)# exit

Switch(config)# vlan 20

Switch(config-vlan)# name Housekeeping

Switch(config-vlan)# exit

Switch(config)# vlan 30

Switch(config-vlan)# name Management

Switch(config-vlan)# exit

Switch(config)# vlan 40

Switch(config-vlan)# name Guest

Switch(config-vlan)# exit

1. Assign ports to VLANs (e.g., ports for Reception on VLAN 10):

A screenshot of a computer program

Description automatically generated

Switch(config)# interface fastethernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

Switch(config-if)# exit

Switch(config)# interface fastethernet 0/2

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 20

Switch(config-if)# exit

Switch(config)# interface fastethernet 0/3

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 30

Switch(config-if)# exit

Switch(config)# interface fastethernet 0/4

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 40

Switch(config-if)# exit

**2. Configure Trunk Port for Router Connectivity**

A trunk port is required to allow the switch to communicate with the router for inter-VLAN routing.

1. On the switch, configure a trunk port to the router:

A screenshot of a computer

Description automatically generated

Switch(config)# interface fastethernet 0/24

Switch(config-if)# switchport mode trunk

Switch(config-if)# exit

**3. Configure Inter-VLAN Routing on the Router**

The router is required to route traffic between different VLANs.

1. Add a **router** (e.g., 2811 router) and connect it to the switch via the trunk port (Fa0/24).
2. Access the router CLI:

A black rectangular object with a black stripe

Description automatically generated

Router> enable

Router# configure terminal

1. **Create sub-interfaces on the router for each VLAN:**

A screenshot of a computer program

Description automatically generated

Router(config)# interface gigabitethernet 0/0.10

Router(config-subif)# encapsulation dot1Q 10

Router(config-subif)# ip address 192.168.10.1 255.255.255.0

Router(config-subif)# exit

Router(config)# interface gigabitethernet 0/0.20

Router(config-subif)# encapsulation dot1Q 20

Router(config-subif)# ip address 192.168.20.1 255.255.255.0

Router(config-subif)# exit

Router(config)# interface gigabitethernet 0/0.30

Router(config-subif)# encapsulation dot1Q 30

Router(config-subif)# ip address 192.168.30.1 255.255.255.0

Router(config-subif)# exit

Router(config)# interface gigabitethernet 0/0.40

Router(config-subif)# encapsulation dot1Q 40

Router(config-subif)# ip address 192.168.40.1 255.255.255.0

Router(config-subif)# exit

**4. Assign IP Addresses to VLAN PCs**

For each PC in the VLAN, assign an IP address from the corresponding VLAN’s subnet.

1. **Reception VLAN (VLAN 10)**
   * IP: 192.168.10.2
   * Subnet Mask: 255.255.255.0
   * Default Gateway: 192.168.10.1
2. **Housekeeping VLAN (VLAN 20)**
   * IP: 192.168.20.2
   * Subnet Mask: 255.255.255.0
   * Default Gateway: 192.168.20.1
3. **Management VLAN (VLAN 30)**
   * IP: 192.168.30.2
   * Subnet Mask: 255.255.255.0
   * Default Gateway: 192.168.30.1
4. **Guest VLAN (VLAN 40)**
   * IP: 192.168.40.2
   * Subnet Mask: 255.255.255.0
   * Default Gateway: 192.168.40.1

**5. Test Connectivity**

1. Use the **Ping** command on each PC to test connectivity within the VLAN and across VLANs. For example:
   * Ping from a **Reception PC (192.168.10.2)** to a **Housekeeping PC (192.168.20.2)**.
   * If everything is set up correctly, the ping should be successful, indicating inter-VLAN routing is functioning.

**6. Optional: DHCP Configuration**

You can configure a DHCP server on the router to automatically assign IP addresses to devices in each VLAN.

**Summary of Configuration**

* VLANs were created on the switch for each hotel department.
* Ports were assigned to respective VLANs.
* A trunk port was set up to allow inter-VLAN routing.
* The router was configured with sub-interfaces to route between VLANs.

This setup will segment network traffic and ensure each department has its own VLAN, isolating it from the others and improving network performance and security.

Hospital Management System In VLAN

Configuration

To configure VLANs (Virtual Local Area Networks) for a Hospital Management System in Cisco Packet Tracer, we will segment the network into different VLANs for departments such as administration, doctors, nurses, patient records, and guest Wi-Fi. This segmentation enhances security, network efficiency, and isolation of different traffic types within the hospital.

**Scenario**

We will create the following VLANs:

* **Administration VLAN** (ID: 10)
* **Doctors VLAN** (ID: 20)
* **Nurses VLAN** (ID: 30)
* **Patient Records VLAN** (ID: 40)
* **Guest Wi-Fi VLAN** (ID: 50)

This setup helps to ensure that sensitive hospital data, such as patient records, remains isolated from general traffic like guest Wi-Fi, while still allowing essential communication between departments.

**Step-by-Step Procedure**

* 1. **Set Up VLANs on the Switch**

Begin by creating VLANs for each department.

1. Open **Cisco Packet Tracer**.
2. Add a **Cisco 2960 switch** to your topology.
3. Add **PCs or devices** to represent various users (administration, doctors, nurses, etc.).
4. Use appropriate **cables** to connect the devices to the switch.

**Commands to Configure VLANs**

1. Access the switch's CLI
2. Enter global configuration mode:

A black rectangular object with a black stripe

Description automatically generated

Switch> enable

Switch# configure terminal

1. Create VLANs for each department:

A screenshot of a computer program

Description automatically generated

Switch(config)# vlan 10

Switch(config-vlan)# name Administration

Switch(config-vlan)# exit

Switch(config)# vlan 20

Switch(config-vlan)# name Doctors

Switch(config-vlan)# exit

Switch(config)# vlan 30

Switch(config-vlan)# name Nurses

Switch(config-vlan)# exit

Switch(config)# vlan 40

Switch(config-vlan)# name Patient\_Records

Switch(config-vlan)# exit

Switch(config)# vlan 50

Switch(config-vlan)# name Guest\_WiFi

Switch(config-vlan)# exit

Assign ports on the switch to each VLAN. For example, connect the devices for the **Administration VLAN (VLAN 10)** to port 1:

A screenshot of a computer

Description automatically generated

Switch(config)# interface fastethernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

Switch(config-if)# exit

Repeat this for other departments by connecting their respective devices to the appropriate ports on the switch:

A screenshot of a computer

Description automatically generated

```

Switch(config)# interface fastethernet 0/2

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 20

Switch(config-if)# exit

Switch(config)# interface fastethernet 0/3

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 30

Switch(config-if)# exit

Switch(config)# interface fastethernet 0/4

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 40

Switch(config-if)# exit

Switch(config)# interface fastethernet 0/5

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 50

Switch(config-if)# exit

**2. Configure a Trunk Port for Router Connectivity**

To enable communication between VLANs (inter-VLAN routing), you will need to configure a trunk port that connects the switch to a router.

1. On the switch, set one of the ports (e.g., **FastEthernet 0/24**) to trunk mode:

A black screen with white text

Description automatically generated

Switch(config)# interface fastethernet 0/24

Switch(config-if)# switchport mode trunk

Switch(config-if)# exit

This port will be used for inter-VLAN traffic, allowing it to carry traffic from all VLANs.

**3. Configure Inter-VLAN Routing on the Router**

A router is required for communication between different VLANs. We'll use a router with sub-interfaces for each VLAN.

1. Add a **Cisco 2811 router** to your topology.
2. Connect the router to the switch using the trunk port.
3. Access the router’s CLI:

A black rectangular object with a black rectangle

Description automatically generated

Router> enable

Router# configure terminal

Create sub-interfaces on the router for each VLAN. Each sub-interface corresponds to a VLAN, and each is assigned an IP address to act as a gateway for the devices in that VLAN.

A screenshot of a computer

Description automatically generated

Router(config)# interface gigabitethernet 0/0.10

Router(config-subif)# encapsulation dot1Q 10

Router(config-subif)# ip address 192.168.10.1 255.255.255.0

Router(config-subif)# exit

Router(config)# interface gigabitethernet 0/0.20

Router(config-subif)# encapsulation dot1Q 20

Router(config-subif)# ip address 192.168.20.1 255.255.255.0

Router(config-subif)# exit

Router(config)# interface gigabitethernet 0/0.30

Router(config-subif)# encapsulation dot1Q 30

Router(config-subif)# ip address 192.168.30.1 255.255.255.0

Router(config-subif)# exit

Router(config)# interface gigabitethernet 0/0.40

Router(config-subif)# encapsulation dot1Q 40

Router(config-subif)# ip address 192.168.40.1 255.255.255.0

Router(config-subif)# exit

Router(config)# interface gigabitethernet 0/0.50

Router(config-subif)# encapsulation dot1Q 50

Router(config-subif)# ip address 192.168.50.1 255.255.255.0

Router(config-subif)# exit

Each sub-interface is assigned to a VLAN and will act as the default gateway for that VLAN.

**4. Assign IP Addresses to Hospital Devices**

Next, assign static IP addresses to the devices in each VLAN, or configure DHCP if needed.

1. **Administration VLAN (VLAN 10)**:
   * IP Address: 192.168.10.2
   * Subnet Mask: 255.255.255.0
   * Default Gateway: 192.168.10.1
2. **Doctors VLAN (VLAN 20)**:
   * IP Address: 192.168.20.2
   * Subnet Mask: 255.255.255.0
   * Default Gateway: 192.168.20.1
3. **Nurses VLAN (VLAN 30)**:
   * IP Address: 192.168.30.2
   * Subnet Mask: 255.255.255.0
   * Default Gateway: 192.168.30.1
4. **Patient Records VLAN (VLAN 40)**:
   * IP Address: 192.168.40.2
   * Subnet Mask: 255.255.255.0
   * Default Gateway: 192.168.40.1
5. **Guest Wi-Fi VLAN (VLAN 50)**:
   * IP Address: 192.168.50.2
   * Subnet Mask: 255.255.255.0
   * Default Gateway: 192.168.50.1

**5. Test the VLAN Configuration**

To ensure that the VLANs and inter-VLAN routing are functioning correctly, use the **Ping** command to test connectivity between devices within and across VLANs.

For example:

* Ping from a **Doctor’s PC (192.168.20.2)** to an **Administration PC (192.168.10.2)**.
* Ping from a **Nurse’s PC (192.168.30.2)** to a **Patient Records PC (192.168.40.2)**.

If the configuration is correct, the pings should succeed, verifying that inter-VLAN routing is functioning

**6. Optional: Configure DHCP for VLANs**

You can also configure a DHCP server on the router to automatically assign IP addresses to the devices in each VLAN.

1. In the router configuration, add DHCP pools for each VLAN:

A screenshot of a computer

Description automatically generated

Router(config)# ip dhcp pool ADMINISTRATION

Router(dhcp-config)# network 192.168.10.0 255.255.255.0

Router(dhcp-config)# default-router 192.168.10.1

Router(dhcp-config)# exit

Router(config)# ip dhcp pool DOCTORS

Router(dhcp-config)# network 192.168.20.0 255.255.255.0

Router(dhcp-config)# default-router 192.168.20.1

Router(dhcp-config)# exit

Router(config)# ip dhcp pool NURSES

Router(dhcp-config)# network 192.168.30.0 255.255.255.0

Router(dhcp-config)# default-router 192.168.30.1

Router(dhcp-config)# exit

Router(config)# ip dhcp pool PATIENT\_RECORDS

Router(dhcp-config)# network 192.168.40.0 255.255.255.0

Router(dhcp-config)# default-router 192.168.40.1

Router(dhcp-config)# exit

Router(config)# ip dhcp pool GUEST\_WIFI

Router(dhcp-config)# network 192.168.50.0 255.255.255.0

Router(dhcp-config)# default-router 192.168.50.1

Router(dhcp-config)# exit

**Summary**

* **VLANs** were configured for each hospital department.
* Each **VLAN** was assigned a unique subnet.
* **Trunking** was configured between the switch and router for inter-VLAN communication.
* **Inter-VLAN routing** was set up using router sub-interfaces.
* IP addresses were assigned to devices in each VLAN, and a DHCP server can be optionally configured.

This setup ensures security and efficiency in handling the network traffic of a hospital, maintaining privacy for critical departments while providing essential communication across different parts of the network.