Cisco 900 Series ISR Setup Guide (Basic Home or SMB Network)

This guide will help you configure your Cisco 900 Series ISR with the following features:

- **Three VLANs**: Home, Guest, and IoT
- **Firewall Rules**: Optimized for streaming and gaming
- **Traffic Prioritization**: Using Quality of Service (QoS)

Prerequisites

1. **Cisco 900 Series ISR**: Ensure your router is powered on and connected to your network.
2. **Access to Cisco Command Line Interface (CLI)**: Use a terminal emulator (e.g., PuTTY) to access the router's CLI.
3. **Basic Network Setup**: Have an existing internet connection and basic understanding of Cisco CLI commands.

Step-by-Step Setup

Step 1: Access the Cisco CLI

1. **Connect to the router** using a console cable or via SSH.
2. **Log in** using your admin credentials.

Step 2: Configure VLANs

1. **Enter Global Configuration Mode**:
   shell
   `enable`
   `configure terminal`
2. **Create VLANs** for Home, Guest, and IoT.

Home VLAN

shell

```
vlan 10
name Home
```

Guest VLAN

shell
```
vlan 20
name Guest
```

IoT VLAN

shell
```
vlan 30
name IoT
```

3. **Assign VLANs to Interfaces**:
   shell
   ```
   interface GigabitEthernet0/1
   switchport mode trunk
   switchport trunk allowed vlan 10,20,30
   ```

Step 3: Configure Sub-Interfaces and Assign IP Addresses

1. **Create sub-interfaces** for each VLAN on the WAN interface.

Home VLAN

shell
```
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
```

Guest VLAN

shell
```
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
```

IoT VLAN

shell
```
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
```

```
ip address 192.168.30.1 255.255.255.0
```

Step 4: Configure DHCP for Each VLAN

1. **Enter DHCP Configuration** for each VLAN.

Home VLAN DHCP

shell
```
ip dhcp pool HOME
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 8.8.8.8
```

Guest VLAN DHCP

shell
```
ip dhcp pool GUEST
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
dns-server 8.8.8.8
```

IoT VLAN DHCP

shell
```
ip dhcp pool IOT
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
dns-server 8.8.8.8
```

Step 5: Configure Security and Firewall Rules

1. **Create Access Control Lists (ACLs)** to manage traffic.

Allow Traffic from Home to Internet

shell
```
ip access-list extended HOME_TO_INTERNET
permit ip 192.168.10.0 0.0.0.255 any
```

Allow Traffic from Guest to Internet

shell
```
ip access-list extended GUEST_TO_INTERNET
permit ip 192.168.20.0 0.0.0.255 any
```

Allow Traffic from IoT to Internet

shell
```
ip access-list extended IOT_TO_INTERNET
permit ip 192.168.30.0 0.0.0.255 any
```

Deny Traffic Between VLANs

shell
```
ip access-list extended DENY_INTERVLAN
deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
```

2. **Apply ACLs to Interfaces**:
   shell
   ```
   interface GigabitEthernet0/0.10
   ip access-group HOME_TO_INTERNET in
   ip access-group DENY_INTERVLAN out

   interface GigabitEthernet0/0.20
   ip access-group GUEST_TO_INTERNET in
   ip access-group DENY_INTERVLAN out

   interface GigabitEthernet0/0.30
   ip access-group IOT_TO_INTERNET in
   ip access-group DENY_INTERVLAN out
   ```

Step 6: Configure Traffic Prioritization (QoS)

1. **Create a QoS Policy** for gaming and streaming.

Create Class Maps for Gaming and Streaming

shell
```
class-map match-any STREAMING
match protocol http
match protocol rtsp

class-map match-any GAMING
match protocol tcp
match protocol udp
```

2. **Create Policy Maps** to apply QoS.

shell
```
policy-map PRIORITY_POLICY
class STREAMING
 set dscp af41
class GAMING
 set dscp ef
```

3. **Apply the QoS Policy to Interfaces**:

shell
```
interface GigabitEthernet0/0
service-policy output PRIORITY_POLICY
```

Step 7: Save Configuration and Test

1. **Save your configuration**:
   shell
   ```
   write memory
   ```
2. **Test the network**:
   - Verify that devices on each VLAN receive the correct IP addresses.
   - Test internet connectivity from each VLAN.
   - Monitor QoS to ensure traffic prioritization is functioning correctly.

Additional Tips

- **Secure Access**: Change default passwords and secure management access using SSH.
- **Regular Backups**: Backup your configuration regularly to prevent data loss.
- **Firmware Updates**: Keep your router's firmware updated for security and performance enhancements.

This guide provides a detailed setup for a Cisco 900 Series ISR, allowing you to manage multiple VLANs, optimize traffic for streaming and gaming, and secure your network. Adjust VLAN IDs, IP addresses, and firewall policies as needed to fit your specific requirements.

Revision #3
Created 9 August 2024 13:02:31 by Jarryd
Updated 9 August 2024 13:44:11 by Jarryd