CSE 320 - Computer Networks

LAB Session 4

27.03.2024

Packet Tracer:
https://www.packettracernetwork.com/download/download-packet-tracer.html
https://skillsforall.com/resources/lab-downloads?courseLang=en-US

Packet Tracer Everywhere: https://github.com/PTAnywhere/ptAnywhere-installation

1. Router:

The goal of this lab is to demonstrate the setup and configuration of a network topology where three routers are connected to a central router, with each router having three PCs connected. This will facilitate the understanding of inter-router communication, subnetting, and routing of traffic between multiple subnets.

Equipment Setup:

- Central Router (R0)
- Edge Routers (R1, R2, R3)
- **Switches (S1, S2, S3)**
- PCs (PC0A, PC0B for R1; PC1A, PC1B for R2; PC2A, PC2B for R3)

Network Design Subnetting Scheme:

- R0-R1 Link: 192.168.1.0/30
- R0-R2 Link: 192.168.2.0/30
- R0-R3 Link: 192.168.3.0/30
- R1 PCs Network: 192.168.10.0/24
- R2 PCs Network: 192.168.20.0/24
- R3 PCs Network: 192.168.30.0/24

Configuration Steps:

1. **Central Router (R0) Configuration:**

```
hostname R0
interface gig0/0
 ip address 192.168.1.1 255.255.255.252
 no shutdown
interface gig0/1
 ip address 192.168.2.1 255.255.255.252
 no shutdown
interface gig0/2
 ip address 192.168.3.1 255.255.255.252
 no shutdown
```

2. **Edge Router R1 Configuration:**

```
hostname R1
interface gig0/0
 ip address 192.168.1.2 255.255.255.252
 no shutdown
interface gig0/1
 ip address 192.168.10.1 255.255.255.0
 no shutdown

! DHCP Configuration
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp pool PC0
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 8.8.8.8
```

3. Repeat similar configurations for R2 and R3, adjusting IP addresses and DHCP settings according to the subnetting scheme.

4. **Static Routing Configuration on R0:**

```
ip route 192.168.10.0 255.255.255.0 192.168.1.2
ip route 192.168.20.0 255.255.255.0 192.168.2.2
ip route 192.168.30.0 255.255.255.0 192.168.3.2
```

5. **Static Routing on Edge Routers (Example for R1):**

```
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

6. **Repeat for R2 and R3, directing the traffic to the central router (R0) as the gateway.**

TAKE HOME

Access Control Lists (ACLs) are used to filter traffic entering or leaving a network interface on Cisco routers. They can permit or deny traffic based on criteria such as source and destination IP addresses, protocols, and ports. Here's how to implement ACLs on edge routers in your network setup, with an example scenario where we want to restrict access between certain PCs in different subnets.

Scenario Example:

- Network Setup: Edge Router R1 connects to two PCs (PC0A and PC0B) in the subnet 192.168.10.0/24.
- Goal: Deny PC0A (192.168.10.2) access to the subnet 192.168.20.0/24 behind Edge Router R2 but allow all other devices in 192.168.10.0/24 subnet access.
- Step 1: Define the ACL

On Router R1, we'll define an extended ACL that denies traffic from PC0A to the 192.168.20.0/24 subnet and permits all other traffic.

```
R1# configure terminal
R1(config)# access-list 101 deny ip host 192.168.10.2 192.168.20.0
0.0.0.255
R1(config)# access-list 101 permit ip 192.168.10.0 0.0.0.255 any
```

- **access-list 101 deny ip host 192.168.10.2 192.168.20.0 0.0.0.255**: This command creates an extended ACL (numbered 101) that denies IP traffic from a single host (PC0A with IP 192.168.10.2) to the entire 192.168.20.0/24 subnet.
- **access-list 101 permit ip 192.168.10.0 0.0.0.255 any:** This command permits all other IP traffic from the 192.168.10.0/24 subnet to any destination.

Apply the ACL to an Interface

ACLs take effect only when they are applied to an interface. In this scenario, apply the ACL to the outbound interface on R1 that routes traffic towards R2.

Assuming the interface connecting R1 to the central router (and then to R2) is GigabitEthernet0/1:

```
R1(config)# interface GigabitEthernet0/1
R1(config-if)# ip access-group 101 out
R1(config-if)# exit
```

- **ip access-group 101 out**: Applies the ACL to outgoing traffic from the interface. Replace GigabitEthernet0/1 with the correct interface on your router.

Verify the ACL Configuration

After applying the ACL, it's essential to verify that it's correctly filtering traffic as intended:

```
R1# show access-lists
R1# show ip interface GigabitEthernet0/1
```

- **show access-lists:** Displays all access lists configured on the router and the number of packet hits for each rule.
- **show ip interface GigabitEthernet0/1:** Shows detailed information about the interface, including any access lists applied.

Testing:

- From PC0A (192.168.10.2), try pinging a device in the 192.168.20.0/24 subnet. The ping should fail due to the ACL.
- From another device in the 192.168.10.0/24 subnet (not PC0A), try pinging a device in the 192.168.20.0/24 subnet. This ping should succeed if the ACL is configured correctly.

Submit your final work on router setup with ACL
. Deadline: 10/04/2024 23:59