**PHINMA ARAULLO UNIVERSITY**

**College of Information Technology and Engineering**

**Bachelor of Science in Information Technology**

**Final Project in**

**ITE 292 - NETWORKING**

**Optimizing Network Resources: IPv6 Adoption for IT Startup Infrastructure**

By:

Pascual, Arenvie

Frias, Samuel

Bermudez, Jeric

Santiago, John Ferry

Dionisio, Rainier Marie

Santos, Francine Fae

**October 2023**

**Description**

The proposal suggests switching to IPv6 in the IT startup's infrastructure since IPv4 addresses are so few and because IPv6 has so many advantages over IPv4. It emphasizes the significance of network assessment, transition plans, design, security considerations, and team training. Adoption of IPv6 promises future-proofing, increased security, scalability, and efficiency. In the end, it's a strategic decision to maximize resources, assuring the business's longevity and competitiveness in a fast-paced digital environment, and lining up with objectives of efficiency, security, and innovation.

**Proposed Topology - The Problem**

Open a new workspace in Cisco Packet Tracer. From the "Devices" panel, drag & drop the following gadgets:

* 2 routers (R1 and R2) (Router R1: Cisco 2911 or 1941; Router R2: Cisco 2911 or 1941)
* 1 switch (SW1) (Cisco 2960, SW1 switch)
* 4 PCs, numbered PC1, PC2, PC3, and PC4.
* 2 laptops
* Use the "Connections" tool to attach the necessary cords to the devices.
* Use a serial cable (serial) to connect the routers.
* Use straight-through Ethernet connections to connect the routers and switches.
* Use Ethernet cables to connect the switches to the PCs in a straight-through fashion.

**Proposed Hardware and Software**

In order to handle the shift to IPv6 successfully, an IT startup's infrastructure often needs suitable gear and software. Hardware compatibility typically comprises network hardware, such as routers, switches, and firewalls, capable of accepting IPv6 traffic. However, specifications may vary depending on the present configuration. Operating systems, programs, and network management tools must all be IPv6-ready or able to be modified to handle IPv6 protocols in order to be considered software compatible. To ensure seamless integration and functionality within an IPv6-enabled network architecture, it is essential to evaluate, plan, and maybe upgrade both hardware and software.

**Proposed IP Addressing Scheme - IP Address Allocation**

| **DEVICES** | **IP ADDRESS** | **SUBNET MASK** |
| --- | --- | --- |
| **Server** | **192.168.100.1** | **255.255.255.0** |
| **R1** | **192.168.1.1** | **255.255.255.0** |
| **R2** | **192.168.1.2** | **255.255.255.0** |
| **S1** |  |  |
| **PC1** | **192.168.1.3** | **255.255.255.0** |
| **PC2** | **192.168.1.4** | **255.255.255.0** |
| **PC3** | **192.168.1.5** | **255.255.255.0** |
| **PC4** | **192.168.1.6** | **255.255.255.0** |
| **L1** | **192.168.1.7** | **255.255.255.0** |
| **L2** | **192.168.1.8** | **255.255.255.0** |

**Configuring IPV6**

Configure IPv6 addresses for the router interfaces as follows:

* Serial0/0/0:

R1: ipv6 address 2001:DB8:0:1::1/64

R2: ipv6 address 2001:DB8:0:2::2/64

* R1:

\*GigabitEthernet0/0: 2001:DB8:0:1::1/64

\*GigabitEthernet0/1: 2001:DB8:0:2::1/64

* R2:

\*GigabitEthernet0/0: 2001:DB8:0:2::2/64

\*GigabitEthernet0/1: 2001:DB8:0:3::1/64

------------------------------------------------

(R1)

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface GigabitEthernet0/0

Router(config-if)#ipv6 address 2001:DB8:0:1::1/64

Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

exit

------------------------------------------------

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface GigabitEthernet0/1

Router(config-if)#ipv6 address 2001:DB8:0:2::1/64

Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Exit

**Proposed Security Measures**

In a startup IT infrastructure, integrating IPv6 requires additional security measures beyond passwords and firewalls. The use of "Intrusion Detection and Prevention Systems" (IDPS) is a method for monitoring network traffic for unusual activity and taking preventive action as needed. It's crucial to create strict access controls and policies to limit who may access the network and what they can access. Strong access controls and rules, as well as the implementation of intrusion detection and prevention systems, are necessary security measures.