21BDS0340

Abhinav Dinesh Srivatsa

Information Security and Audit Lab

Task – III

**Question 1**

Aim: To create 2 LAN’s with a dynamic routing connection

Tools and Concepts Required:

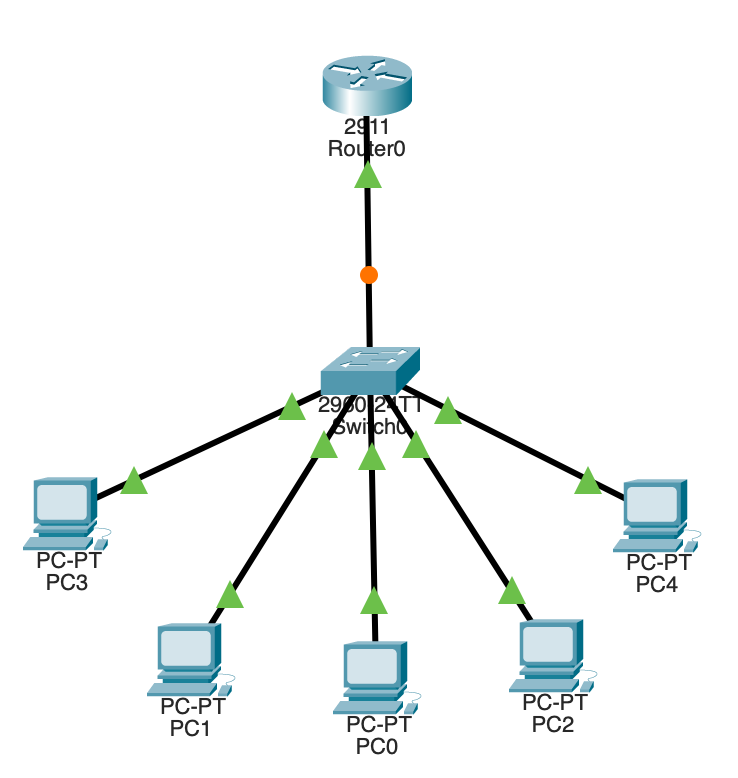
* Cisco Packet Tracer
* Switch
* Hub
* Router
* Personal Computers
* Wiring

Procedure:

* Create LAN1 using switch with 5 PC
* Create LAN2 using hub with 5 PC
* Interconnect the routers and configure the routing table for dynamic routing
* Understand the packet transmission across the LAN

Output:

Create LAN1 using switch with 5 PC:



Create LAN2 using hub with 5 PC:

A diagram of a computer network

Description automatically generated with low confidence

Interconnect the routers and configure the routing table for dynamic routing:

A diagram of a computer network

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

Understand the packet transmission across the LAN:

A picture containing text, screenshot, font, black

Description automatically generated

Security Analysis:

|  |  |  |
| --- | --- | --- |
| Vulnerabilities | Threats | Attack |
| Outdated software | Physical access with insider access | Malware infection to hardware by insider access |
| Weak passwords | Unauthorised access by gaining a password | Denial of service by blocking hub access |
| Lack of encryption | Data theft by insider attacks | Phishing by insider attack |
| Direct offline hub and switch access |  |  |

Prevention:

* Keeping the nodes and hub in a sperate room for nobody to access directly.
* Encrypt and mandate strong password usage

Result:

This network is extremely secure, but all the nodes can only connect to each other and none of them to the internet. This type of connection is very good for local file storages and broadcasting. This also enables different LANs to connect with each other through the usage of a router.

**Question 2**

Aim: Create 2 servers with one accessible through CLI only and one from browser only

Tools and Concepts Required:

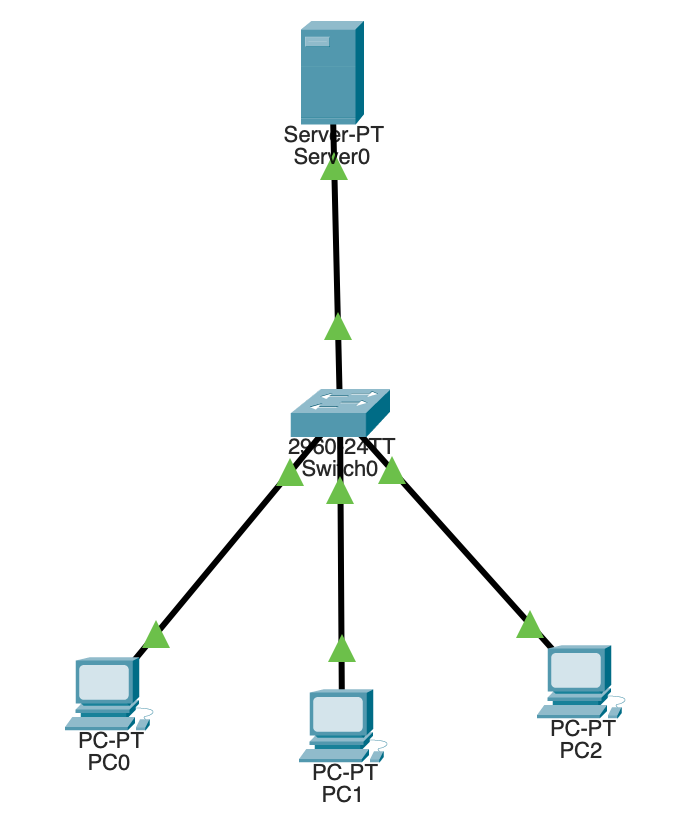
* Cisco Packet Tracer
* Switch
* Router
* Personal Computers
* Server
* Wiring

Procedure:

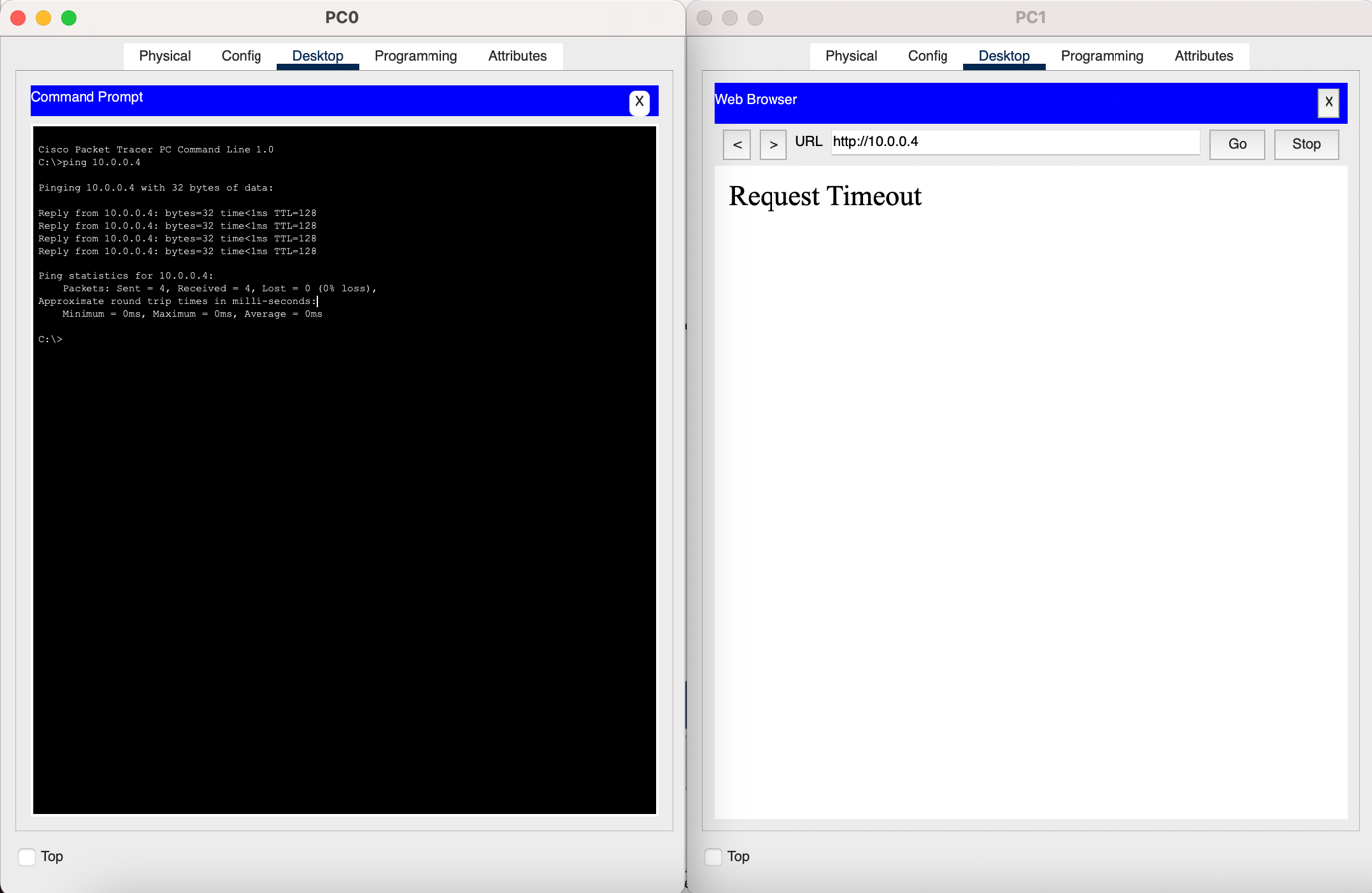
* Create server 1 with a switch and 3 PC
* Server 1 can only be accessed from CLI
* Create server 2 with a switch and 2 PC
* Server 2 can only be accessed from browser

Output:

Create server 1 with a switch and 3 PC:



Server 1 can only be accessed from CLI:

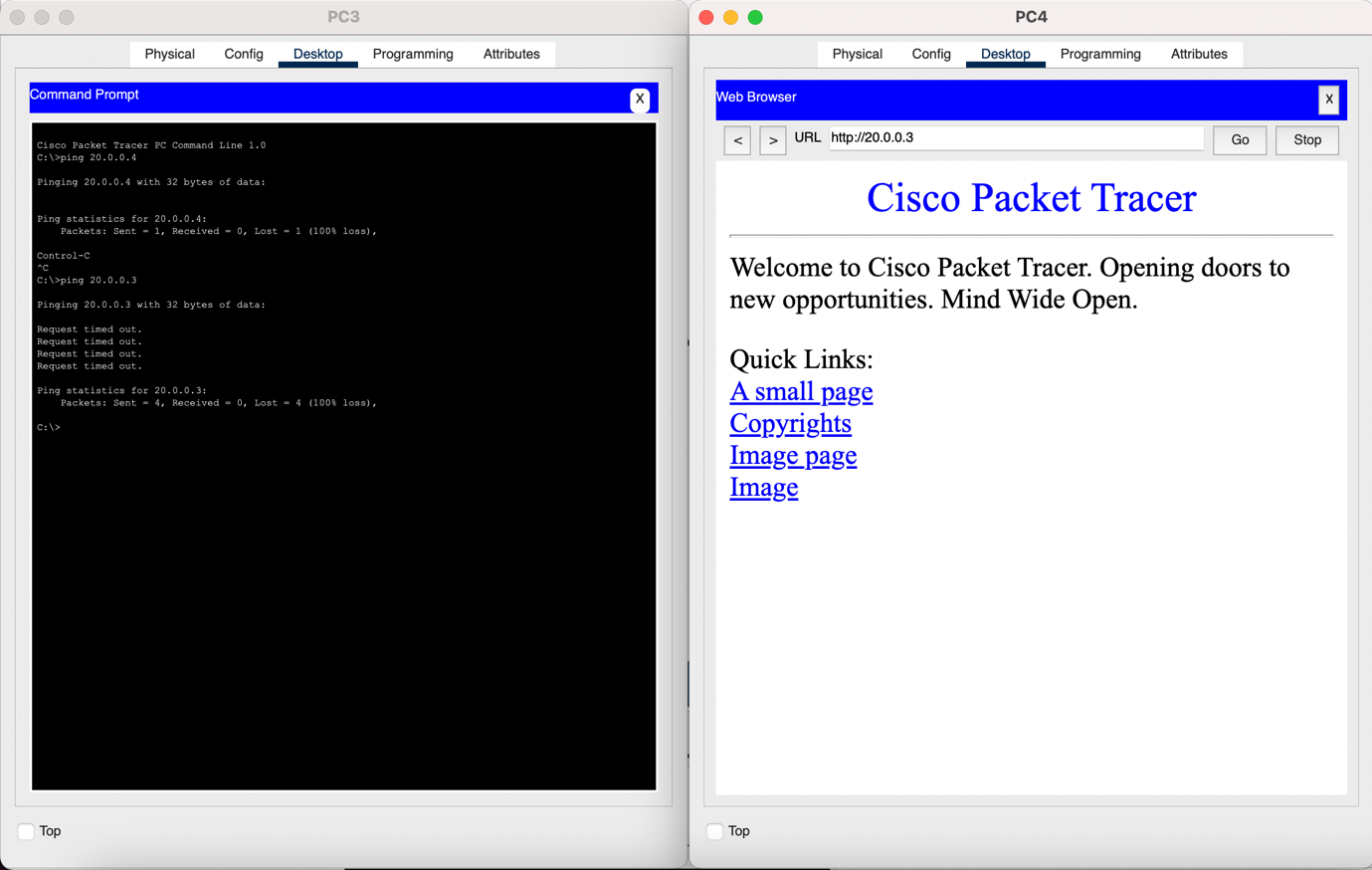


Create server 2 with a switch and 2 PC:

A picture containing tripod

Description automatically generated

Server 2 can only be accessed from browser:



Security Analysis:

|  |  |  |
| --- | --- | --- |
| Vulnerabilities | Threats | Attack |
| Outdated software | Physical access with insider access | Malware infection to hardware by insider access |
| Weak passwords | Unauthorised access by gaining a password | Denial of service by blocking hub access |
| Lack of encryption | Data theft by insider attacks | Phishing by insider attack |
| Direct offline switch access |  |  |

Prevention:

* Keeping the nodes and hub in a sperate room for nobody to access directly.
* Encrypt and mandate strong password usage
* The usage of the firewall prevents users from the second server to access the CLI, which can prevent unwanted installation and access

Result:

This network is secure, but all the nodes can only access to the server they are assigned to and not to the rest of the internet. The implementation of the firewall on both servers allows for added security and allows more repudiation on servers.