

**COURSE TITLE: COMPUTER NETWORKS**

**COURSE CODE: CSE3204**

**LAB REPORT: Project**

**DATE: 19.05.2024**



**TITLE :** Implementation of Campus area network system

**OBJECTIVE :** Notre Dame University Bangladesh is a respected institution, recently expanding by constructing another campus in Dhaka. The university currently comprises four main faculties: BBA,LLB,ELL, and CSE, offered at both the main and branch campuses. This diverse range of faculties meets the dynamic needs of students and staff, fostering a vibrant academic environment. The information technology department, located at the main campus, is a crucial component, ensuring seamless connectivity and technological integration between the campuses. This central hub manages the intricate network that links them. Presently, the university serves a substantial community of around 1,000 users across both campuses. Anticipating significant growth, the university plans to double the number of users in each department by 2025. This forward-thinking approach highlights the need for a robust and scalable infrastructure, emphasizing scalability throughout the design and implementation stages.

**TOOLS :**

**Software:**

Cisco Packet Tracer

**Component that has been used :**

1.Pc (end devices)

2.PT-Switch (switches)

3.Copper straight through , copper cross-over,serial DCE (connections)

4.LAP-PT (wireless devices)

5.Laptop -PT(end devices)

6. Printer (end devices)

7.TabletPC (end devices)

8.Smartphone - pt (end devices)

9.5506-X (security)

10.3650-24ps(switches)

11.WLC -PT (wireless devices)

12.Server (end devices)

13.2911(routers)

**IP ADDRESS REQUIREMENTS :**

Management Network : Ip address range : 172.16.10.0/24

WLAN : Ip address range : 10.10.0.0./16

LAN : Ip address range : 192.168.0.0/16

DMZ :Ip address range : 10.20.20.0/27

Public addresses : Ip address range : 105.100.50.0/30(for main campus)&Ip address range : 205.200.100.0/30(for branch campus)

Campus Area Network

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Network &**  **Subnet Mask** | **Valid Host Addresses** | **Default Gateway** | **Broadcast Address** |
| WLAN(main & branch) | 10.10.0.0/16 | 10.10.0.1 - 10.10.255.254 | 10.10.0.1 | 10.10.255.254 |
| 10.11.0.0/16 | 10.11.0.1 - 10.10.255.254 | 10.10.0.1 | 10.10.255.254 |
| LAN(main & branch) | 172.16.0.0/24 | 172.16.0.1 - 172.16.255.254 | 172.16.0.1 | 172.16.255.254 |
| 172.17.0.0/24 | 172.17.0.1 - 172.17.255.254 | 172.17.0.1 | 172.17.255.254 |
| Management | 192.168.10.0/24 | 192.168.10.1 -  192.168.10.254 | 192.168.10.0 | 192.168.10.254 |
| DMZ | 10.10.10.0/27 | 10.20.20.1 -10.20.20.30 | 10.20.20.1 | 10.20.20.31 |

|  |  |
| --- | --- |
| **Name** | **Network Address** |
| Cloud Area | 8.0.0.0/8 |
| HQ-ISP-Internet | 20.20.20.0/30 |
| Branch-ISP-Internet | 30.30.30.0/30 |
| ASA0 - ISP | 105.100.50.0/30 |
| ASA1-ISP | 205.200.100.0/30 |
| ASA0-Multilayer Switch 0 | 10.20.20.32/30 |
| ASA0-Multilayer Switch 1 | 10.20.20.36/30 |
| ASA1-Multilayer Switch 2 | 10.20.20.40/30 |
| ASA1-Multilayer Switch 3 | 10.20.20.44/30 |

**Procedure :**

Hierarchical Design: Implementing a hierarchical network model with redundancy to enhance resilience.

ISPs: Establishing connectivity to an ISP Router within the network infrastructure.

WLAN: Equipping each department with a Wireless Access Point (WAP) to provide Wi-Fi access for employees, corporate users, external auditors, and guests, all centrally managed by a Wireless LAN Controller (WLC).

VLAN: Maintaining VLANs with IDs: 10 for Management, 20 for LAN, 50 for WLAN, and 199 for Blackhole, where all unused ports are placed.

EtherChannel: Using the Link Aggregation Control Protocol (LACP) for EtherChannel configuration to improve link aggregation efficiency.

STP PortFast and BPDUguard: Configuring Spanning Tree Protocol (STP) PortFast and BPDUguard to speed up port transitions from blocking to forwarding states.

Subnetting: Applying subnetting techniques to allocate the appropriate number of IP addresses to each network group.

Basic Settings: Configuring fundamental device settings, including hostnames, console passwords, enable passwords, banner messages, password encryption, and disable IP domain lookup.

Inter-VLAN Routing: Enabling communication between devices in all departments by configuring inter-VLAN routing on the multilayer switch.

Core Switch: Assigning IP addresses to multilayer switches to enable both routing and switching functionalities.

DHCP Server: Ensuring that all devices in the network obtain IP addresses dynamically from the DHCP servers located at the server farm site.

HSRP: Implementing the Hot Standby Router Protocol (HSRP) to achieve redundancy, load balancing, and failover capabilities.

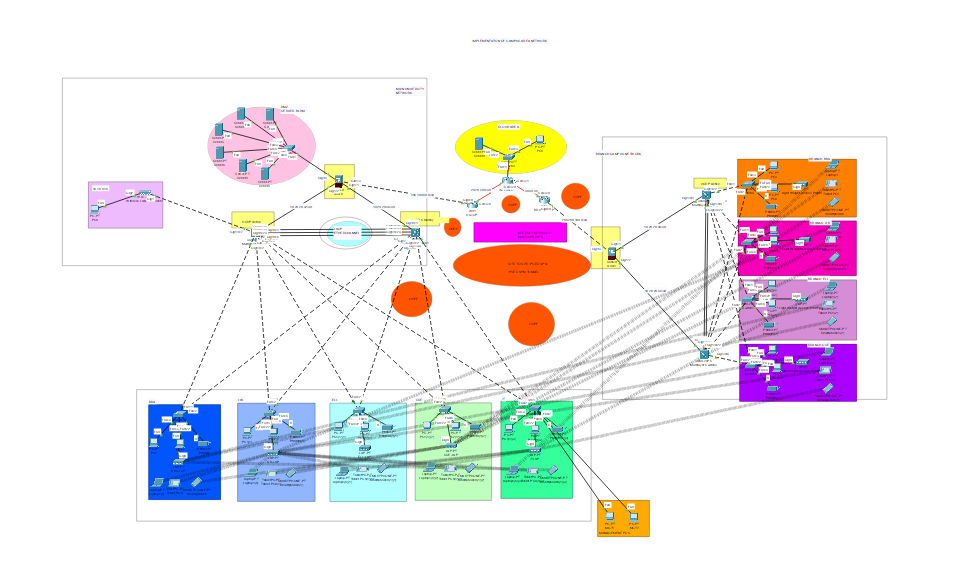
Static Addressing: Allocate static IP addresses for specific devices.

Routing Protocol (OSPF): Use Open Shortest Path First (OSPF) as the routing protocol.

Standard ACL for SSH: Establish a simple standard access control list on the VTY line to permit remote administrative tasks via SSH only for the senior network security engineer's PC.

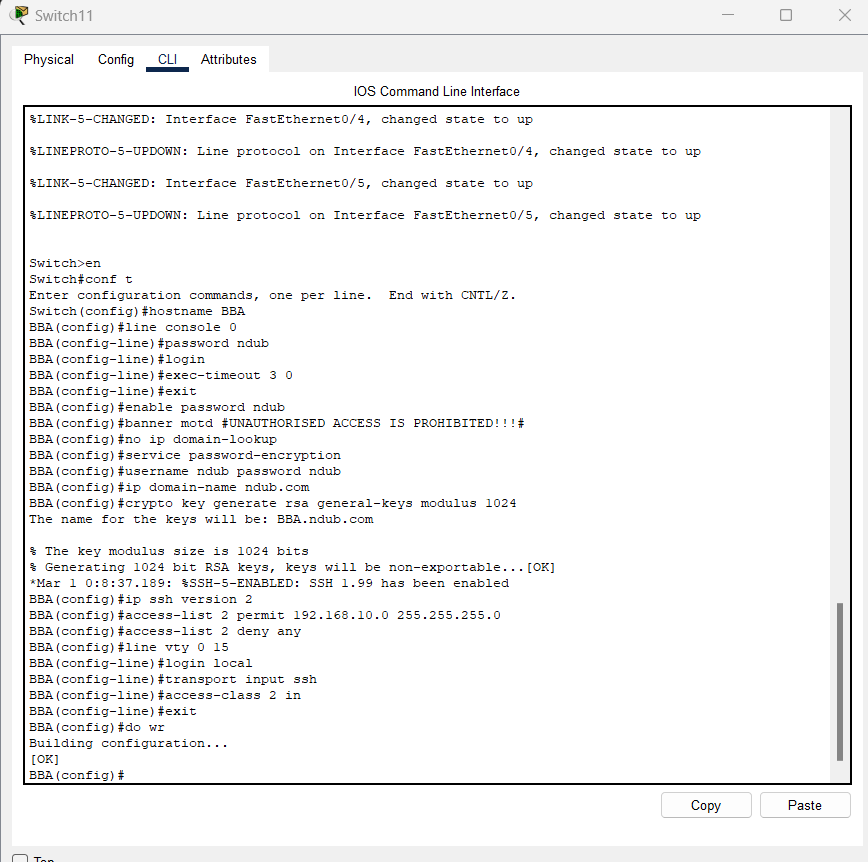
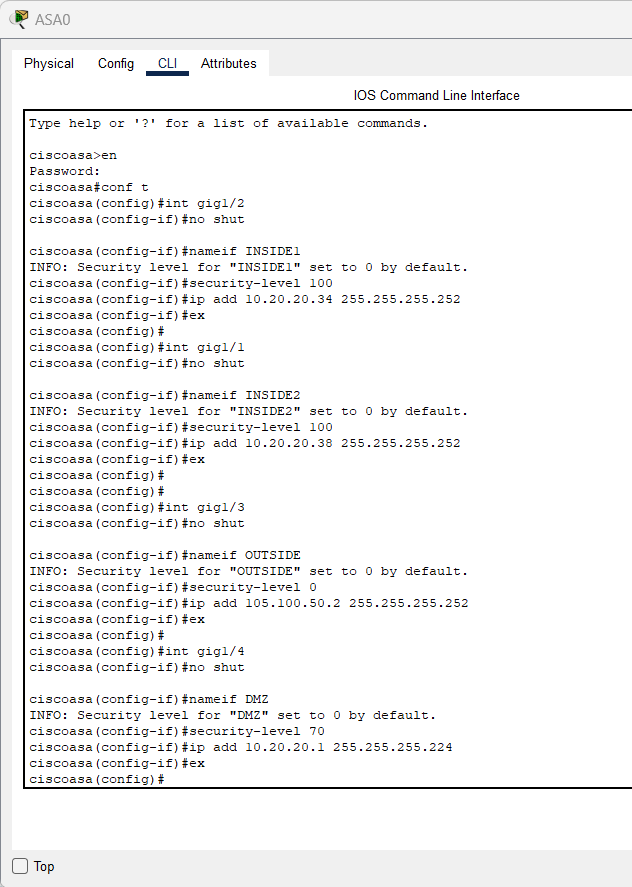
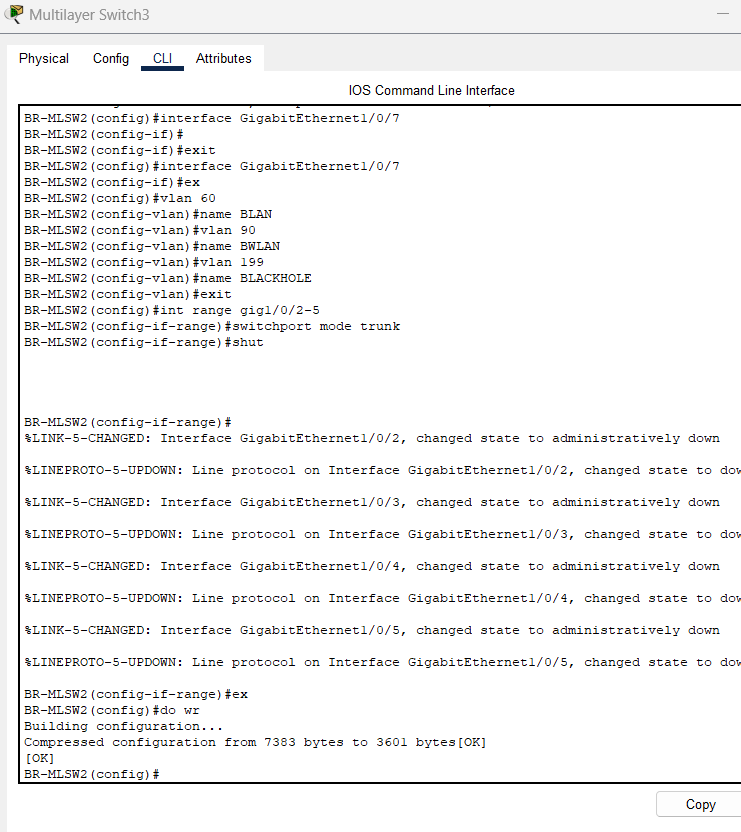
Cisco ASA Firewall: Configure default static routes, basic settings, security levels, zones, and policies on the Cisco ASA firewall to define access control and resource utilization within the network.

**Procedure pictures :**

****

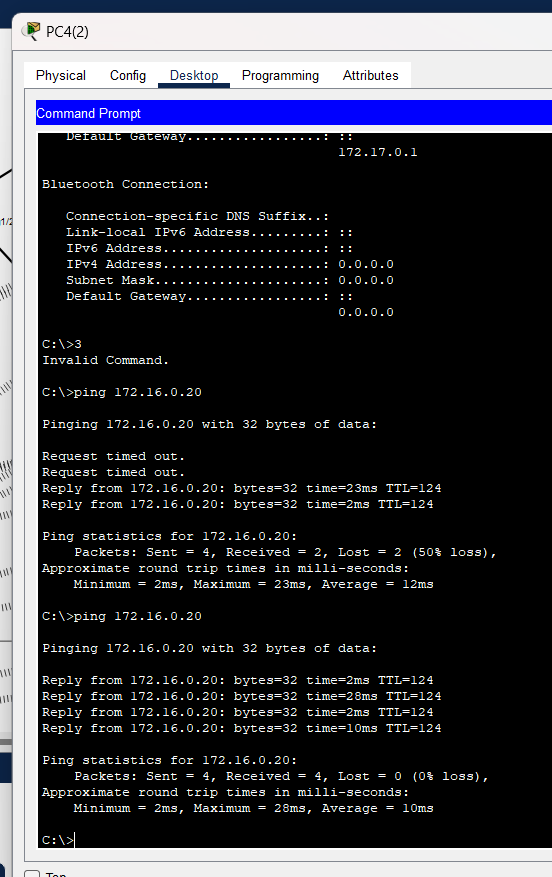
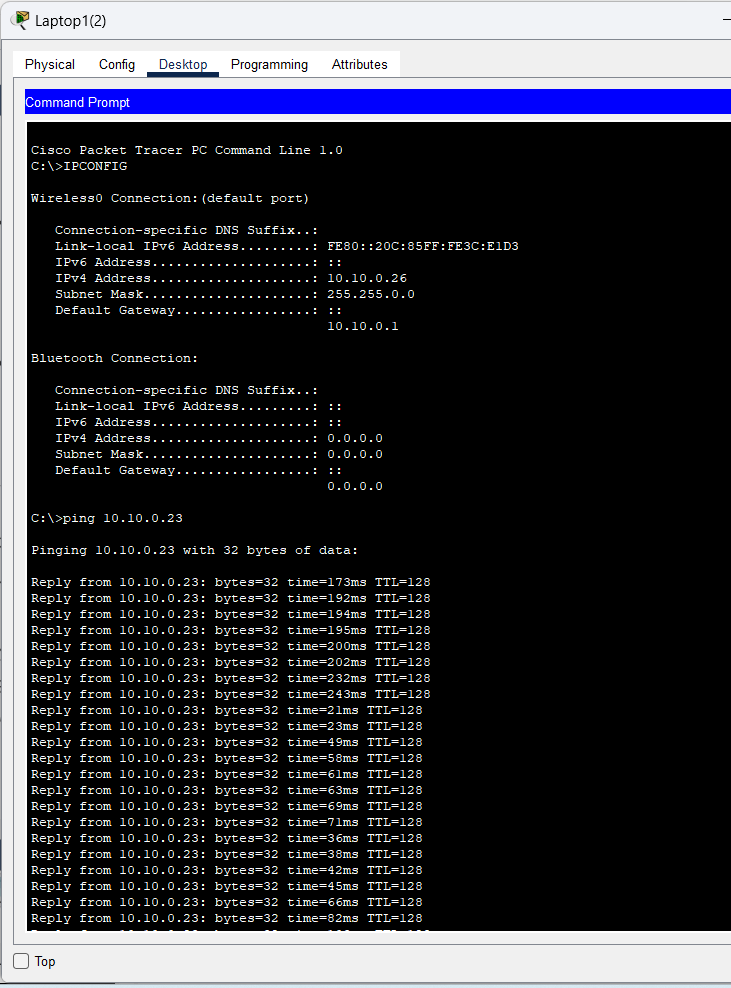
**Figure 1 : Campus Area network**

In the figure 1 , a model has been created where it is shown the path and connection among devices , routers , securities .



**Figure 2 : Some configuration examples**

In figure 2 , some configuration example has been shown to give an idea regarding the communication that has been set up among components

****

**Figure 3 : Some Testing result**

In figure 3 , some testing result has been shown where it was checked whether the wireless network has been configured or not

**RESULT AND ANALYSIS :**

Centralized management of wireless access and efficient traffic segmentation through VLANs enhance performance and security. Network reliability is further improved by EtherChannel, STP configurations, and HSRP. Comprehensive security is maintained through ACLs for SSH and Cisco ASA firewall policies.

**CONCLUSIONS :**

In conclusion, the Cisco-based Campus Area Network (CAN) ensures robust, scalable, and secure infrastructure. It features hierarchical design with redundancy, centralized WAP management, and VLANs for efficient traffic control. EtherChannel with LACP, STP PortFast, and BPDUguard enhance network performance and reliability. Subnetting, inter-VLAN routing, and DHCP simplify IP management. HSRP, static IP addressing, and OSPF ensure high availability and stability. Security is reinforced with ACLs for SSH and Cisco ASA firewall configurations.