# **Depi Graduation Project**

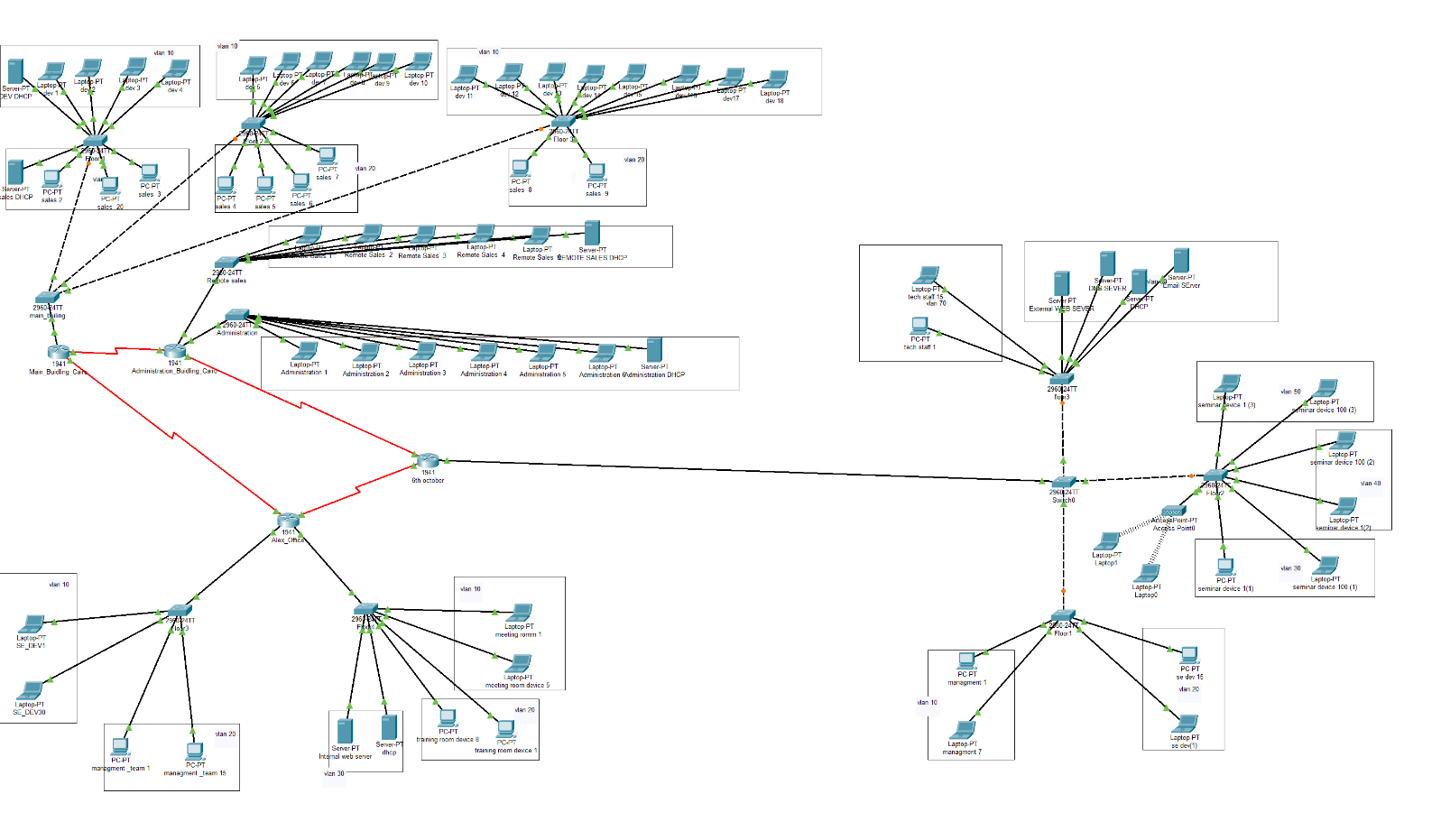
Building and Securing a Small Network

Group Code: Cai1\_ISS1\_S1e

Team Members:

* Ahmed Hossam Eldin Mohamed Ahmed Mobarak
* Ahmad Alaa Eldin Abdelmoniem Sayed
* Mahmoud Mohamed Mahmoud Ahmed
* Ahmed Emad Ahmed Ghoneim

# Network Design and Configuration

Network design Diagram: 

* Number of networks: 20
* Number of Switches: 12
* Number of routers:4
* Number of switches that have VLANs configured: 10
* Total VLANs: 13

159.10.7.0 is the network we want to subnet:

Class b subnetting table:

|  |  |  |
| --- | --- | --- |
| Subnet | Host | Subnet mask |
| 1 | 65536 | /16 |
| 2 | 32768 | /17 |
| 4 | 16384 | /18 |
| 8 | 8129 | /19 |
| 16 | 4096 | /20 |
| 32 | 2048 | /21 |
| 64 | 1024 | /22 |
| 128 | 512 | /23 |
| 256 | 256 | /24 |
| 512 | 128 | /25 |
| 1024 | 64 | /26 |
| 2048 | 32 | /27 |
| 4096 | 16 | /28 |
| 8192 | 8 | /29 |
| 16384 | 4 | /30 |
| 32768 | 2 | /31 |
| 65536 | 1 | /32 |

Network Subnetting:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Network id | Subnet mask | Number of hosts | Broadcast id | Network/ department | Range of ips | Max number of available hosts | Branch |
| 159.10.0.0 | /24 | 256 | 159.10.0.255 | Not used | 159.10.0.1- 159.10.0.254 | 254 | .. |
| 159.10.1.0 | /24 | 256 | 159.10.1.255 | Not used | 159.10.1.1- 159.10.1.255 | 254 | .. |
| .. | .. | .. | .. | .. | .. | .. | .. |
| 159.10.7.0 | /24 | 256 | 159.10.7.255 | Seminar room 1 | 159.10.7.1- 159.10.7.254 | 254 | 6th October |
| 159.10.8.0 | /26 | 64 | 159.10.8.63 | Software Dev | 159.10.8.1- 159.10.8.62 | 62 | Alex – VLAN |
| 159.10.8.64 | 255.255.255.192 | 64 | 159.10.8.127 | R&D | 159.10.8.65- 159.10.8.126 | 62 | Cairo – VLAN |
| 159.10.8.128 | /27 | 32 | 159.10.8.159 | Software Dev | 159.10.8.129- 159.10.8.158 | 30 | 6th October |
| 159.10.8.160 | 255.255.255.224 | 32 | 159.10.8.191 | Sales and Marketing | 159.10.8.161- 159.10.8.190 | 30 | Cario |
| 159.10.8.192 | /27 | 32 | 159.10.8.223 | Management team | 159.10.8.193- 159.10.8.222 | 30 | Alex |
| 159.10.8.224 | /27 | 32 | 159.10.8.255 | Tech Staff | 159.10.8.225- 159.10.8.254 | 30 | 6th October |
| 159.10.9.0 | 255.255.255.240 | 16 | 159.10.9.15 | Administration | 159.10.9.1- 159.10.9.14 | 14 | Cario |
| 159.10.9.16 | /28 | 16 | 159.10.9.31 | Remote Sales | 159.10.9.17- 159.10.9.30 | 14 | Cario |
| 159.10.9.32 | /28 | 16 | 159.10.9.47 | Training Room | 159.10.9.33- 159.10.9.46 | 14 | Alex |
| 159.10.9.48 | /28 | 16 | 159.10.9.63 | Management & Admin Staff | 159.10.9.49- 159.10.9.62 | 14 | 6th October |
| 159.10.9.64 | /29 | 8 | 159.10.9.71 | Meeting room | 159.10.9.65- 159.10.9.70 | 6 | Alex |
| 159.10.9.72 | /29 | 8 | 159.10.9.79 | Server room | 159.10.9.73- 159.100.9.78 | 6 | Alex |
| 159.10.9.80 | /29 | 8 | 159.10.9.87 | Server room | 159.10.9.81- 159.10.9.86 | 6 | 6th October |
| 159.10.9.88 | /30 | 4 | 159.10.9.91 | Router |  | 2 |  |
| 159.10.9.92 | /30 | 4 | 159.10.9.95 | Router |  | 2 |  |
| 159.10.9.96 | /30 | 4 | 159.10.9.99 | Router |  | 2 |  |
| 159.10.9.104 | /30 | 4 | 159.10.9.103 | Router |  | 2 |  |
| 159.10.9.104 | Not used |  |  |  |  |  |  |
| 159.10.10.0 | /24 | 256 | 159.10.10.255 | Seminar room2 | 159.10.10.1- 159.10.10.254 | 254 | 6thOctober LAN |
| 159.10.11.0 | /24 | 256 | 159.10.11.255 | Seminar room3 | 159.10.11.1- 159.10.11.254 | 254 | 6thOctober LAN |

* Initial Configuration Scripts for routers and switches ex:

**# Global Configuration Mode**

**hostname Router1 # Change hostname for each router (Router2, Router3, Router4)**

**# Set enable secret password**

**enable secret cisco**

**# Set console password**

**line console 0**

**password cisco**

**login**

**exit**

**# Set vty (SSH) password**

**line vty 0 4**

**password cisco**

**login**

**exit**

**# Set interface IP addresses based on your topology**

**interface GigabitEthernet0/0**

**ip address 159.10.x.x 255.255.255.x # Assign the correct IP for each router based on your IP plan**

**no shutdown**

**# Configure default routes (optional based on design)**

**ip route 0.0.0.0 0.0.0.0 159.10.x.x # Modify according to your routing plan**

**# Save the configuration**

**write memory**

# VLANs and Inter-VLAN Routing

* Head office building Cairo branch floor 1,2,3 switches configuration:
* Connected to a main switch and the router is connected using a router on a stick technique.
* Each VLAN has its own server and both are on floor 1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Switch Name | Model | IP address | VLAN number | VLAN name | Default gateway |
| Floor 1 | 2960-24TT | 159.10.8.162 | VLAN 20 | Sales | 159.10.8.161 |
| Floor 1 | 2960-24TT | 159.10.8.66 | VLAN 10 | R&D | 159.10.8.65 |
| Floor 2 | 2960-24TT | 159.10.8.162 | VLAN 20 | Sales | 159.10.8.161 |
| Floor 2 | 2960-24TT | 159.10.8.66 | VLAN 10 | R&D | 159.10.8.65 |
| Floor 3 | 2960-24TT | 159.10.8.162 | VLAN 20 | Sales | 159.10.8.161 |
| Floor 3 | 2960-24TT | 159.10.8.66 | VLAN 10 | R&D | 159.10.8.65 |

* Cairo Administration Building consists of two switches each has 1 LAN.
* Each LAN has a DHCP server.
* Administration server: 159.10.9.2
* Remote Sales server: 159.10.9.18

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Switch Name | Model | IP address | VLAN number | VLAN name | Default Gateway |
| Administration | 2960-24TT | 159.10.9.0 |  |  | 159.10.9.1 |
| Remote Sales | 2960-24TT | 159.10.9.16 |  |  | 159.10.9.17 |

* Alex Building:
* There are two floors:
  + Floor 3 has a switch that has 2 VLANs.
  + Floor 4 has a switch that has 3 VLANs.
* There is one DHCP server in the server room: 159.10.9.74
* It has a pool set for all VLANs:
  + The server room also has an internal web server of IP address: 159.10.9.76
  + It has the HTTPs service set for all networks in the company: [www.internal.com](http://www.internal.com)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Switch name | Model | IP address | VLAN number | VLAN name | Default gateway |
| Floor 3 | 2690-24TT | 159.10.8.2/26 | VLAN 10 | SWE DEV | 159.10.8.1/26 |
| Floor 3 | 2690-24TT | 159.10.8.194/27 | VLAN20 | Management team | 159.10.8.193/27 |
| Floor 4 | 2690-24TT | 159.10.9.66/29 | VLAN10 | Meeting room | 159.10.9.65/29 |
| Floor 4 | 2690-24TT | 159.10.9.34/28 | VLAN 20 | Training room | 159.10.9.33/28 |
| Floor 4 | 2690-24TT | 159.10.9.74/29 | VLAN 30 | Server room | 159.10.9.73/29 |

* 6th October Building has 7 networks in total:
  + Floor 1 has 2 VLANs: the SWE DEV and the Management & Administration.
  + Floor 2 has 3 VLANs: Seminar room 1,2,3.
    - Seminar room 3 has an access point for students and clients to connect of password: 1234567890.
  + Floor 3 has 2 VLANs: the server room that has:
    - DHCP server: 159.10.9.83/29 has pools set for all 6th October branch.
    - DNS server: 159.10.9.84/29 that is set for internal and external websites.
    - External server: 159.10.9.85/29 has the https service set for: [www.aast.edu.eg](http://www.aast.edu.eg)
    - Email server: 159.10.9.86/29 that has the email service set with domain: mail.aast.edu.eg

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Switch name | Model | IP address | VLAN number | VLAN name | Default gateway |
| Floor 1 | 2960-24TT | 159.10.9.50/28 | VLAN 10 | Management | 159.10.9.49/28 |
| Floor 1 | 2960-24TT | 159.10.8.130/27 | VLAN 20 | SWE DEV | 159.10.8.129/27 |
| Floor 2 | 2960-24TT | 159.10.7.2/24 | VLAN 30 | Seminar 1 | 159.10.7.1/24 |
| Floor 2 | 2960-24TT | 159.10.10.2/24 | VLAN 40 | Seminar 2 | 159.10.10.1/24 |
| Floor 2 | 2960-24TT | 159.10.11.2/24 | VLAN 50 | Seminar 3 | 159.10.11.1/24 |
| Floor 3 | 2960-24TT | 159.10.9.82/29 | VLAN 60 | Server room | 159.10.9.81/29 |
| Floor 3 | 2960-24TT | 159.10.8.226/27 | VLAN 70 | Tech Staff | 159.10.8.225/27 |

* All routers are connected static.
* All passwords in the project are cisco
* Except the access point password is: 1234567890

# Network Security Implementation

* V-Lans & Security configuration Scripts:

1-VLANs and Inter-VLAN Routing :

**# On each switch, configure VLANs (already done above in the switch setup).**

**vlan 10**

**name R&D**

**vlan 20**

**name Sales**

**# Router-on-a-Stick Configuration (on router handling Inter-VLAN routing)**

**interface GigabitEthernet0/0**

**no shutdown**

**# Sub-interfaces for VLANs**

**interface GigabitEthernet0/0.10**

**encapsulation dot1Q 10**

**ip address 159.10.8.1 255.255.255.192 # R&D Subnet**

**no shutdown**

**interface GigabitEthernet0/0.20**

**encapsulation dot1Q 20**

**ip address 159.10.8.129 255.255.255.224 # Sales Subnet**

**no shutdown**

**# Save the configuration**

**write memory**

2- Security Configuration Scripts (Example):

**# Port security on switches**

**interface GigabitEthernet0/1**

**switchport mode access**

**switchport access vlan 10**

**switchport port-security**

**switchport port-security maximum 2**

**switchport port-security violation restrict**

**switchport port-security mac-address sticky**

**no shutdown**

**# Enable SSH on switches (for remote access)**

**ip domain-name example.com**

**crypto key generate rsa**

**1024**

**ip ssh version 2**

**line vty 0 4**

**transport input ssh**

**exit**

3- Basic Firewall Rules on Routers:

**ip access-list extended FIREWALL-IN**

**deny tcp any any eq 23 # Block Telnet**

**deny tcp any any eq 21 # Block FTP**

**permit tcp any any eq 80 # Allow HTTP**

**permit tcp any any eq 443 # Allow HTTPS**

**permit icmp any any # Allow ping**

**permit ip any any**

**exit**

**# Apply firewall rules to the router interfaces**

**interface GigabitEthernet0/0**

**ip access-group FIREWALL-IN in**

**no shutdown**

**exit**

**# Save the configuration**

**write memory**

* Effectiveness of the implemented security measures:

To evaluate the effectiveness of the implemented security measures for your small network project, consider the following key metrics and observations:

1. Port Security

- Objective: Prevent unauthorized devices from connecting to the network.

- Implementation: Configured port security on all access ports, limiting the number of MAC addresses allowed per port and setting violation actions (e.g., `restrict` or `shutdown`).

- Effectiveness:

- High: Successfully blocks unauthorized devices attempting to connect by restricting unrecognized MAC addresses.

- Observed Impact: Ports entering violation mode for unauthorized devices; legitimate users have stable connectivity.

- Recommendation: Periodically review the port security logs to ensure no false positives and adjust the allowed MAC addresses list if necessary.

2. Access Control Lists (ACLs)

- Objective: Control access to network segments and critical resources by filtering traffic based on IP addresses, protocols, and ports.

- Implementation: ACLs applied to restrict access between VLANs, block insecure services like Telnet (port 23) and FTP (port 21), while allowing secure traffic (HTTP, HTTPS, ICMP).

- Effectiveness:

- High: Properly filtered traffic according to policy, with successful blocks on unauthorized access attempts to sensitive VLANs.

- Observed Impact: Reduction in unwanted traffic between VLANs, controlled access to critical services, with no interruption in legitimate communication.

- Recommendation: Regularly update ACLs to match evolving security needs and new threats.

3. VLAN Segmentation and Inter-VLAN Routing

- Objective: Isolate departments and limit broadcast domains to enhance security.

- Implementation: VLANs implemented for different departments and segments (e.g., R&D, Sales, Management), with inter-VLAN routing via a Router-on-a-Stick configuration.

- Effectiveness:

- High: Successfully isolated network traffic; unauthorized access between VLANs was blocked. Routing between VLANs only occurred through controlled paths.

- Observed Impact: Improved network performance, reduced broadcast traffic, and enhanced security with segmentation.

- Recommendation: Continuously monitor VLAN traffic for anomalies and ensure that only authorized VLANs have access to shared resources.

4. Basic Firewall Rules

- Objective: Provide a baseline level of security by blocking insecure protocols and allowing necessary traffic.

- Implementation: Firewall rules deployed on routers to block insecure protocols (e.g., Telnet, FTP) and allow secure web traffic (HTTP, HTTPS).

- Effectiveness:

- Moderate to High: Reduced exposure to common attack vectors by blocking insecure protocols. Allowed necessary traffic with minimal disruption.

- Observed Impact: Limited malicious traffic attempts; successful access for legitimate traffic such as web services.

- Recommendation: Consider implementing more advanced firewall solutions if the network size increases or if additional threats are identified.

5. SSH for Remote Management

- Objective: Secure remote management access to network devices.

- Implementation: Disabled Telnet and enabled SSH for secure remote management.

- Effectiveness:

- High: Secured all remote management sessions, encrypting communication between administrators and devices.

- Observed Impact: No unauthorized remote access attempts; secure SSH sessions established with no issues.

- Recommendation: Keep SSH keys and passwords updated regularly and monitor access logs.

6. Password Policies and Encryption

- Objective: Ensure that sensitive data and administrative access are protected with strong credentials.

- Implementation: Strong enable and console passwords applied; encryption enabled for passwords.

- Effectiveness:

- Moderate to High: Increased difficulty of unauthorized access; devices are better protected with encrypted passwords.

- Observed Impact: No successful unauthorized access attempts; increased administrator accountability.

- Recommendation: Implement a strong password policy that includes regular updates and complexity requirements.

Overall Assessment:

- Successes: Security measures effectively protected the network, preventing unauthorized access and segmenting traffic according to the security policy. Key services were accessible without interruptions, and insecure protocols were properly blocked.

- Challenges: Balancing security and usability required careful ACL tuning. Some initial false positives with port security needed adjustment.

- Performance: Network performance remained stable under security settings, with no significant latency introduced by ACLs or VLAN configurations.

# Final Testing

* Test network functionality, security, and connectivity:

Before and after applying the ACL on Router Sub-Interfaces

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer screen

Description automatically generated

Connectivity between same Vlan ex Vlan 10:

A screenshot of a computer

Description automatically generated

Firewall rules and security policies script :

A screenshot of a computer

Description automatically generated