ARAFAT EASIN

Table of Contents

CITY UNIVERSITY NETWORK DESIGN AND IMPLEMENTATION

1 INTRODUCTION

City University is a large educational institution with a diverse set of academic and administrative requirements. It operates across two geographically separate campuses: a **Main Campus**, which serves as the central hub for academic and administrative activities, and a **Smaller Campus**, dedicated to specialized functions, particularly the Faculty of Health Sciences. With these two campuses located 20 miles apart, City University requires a robust and efficient network architecture that can seamlessly interconnect the two sites, enabling reliable communication and data sharing between them.

The Main Campus, spread across three levels, accommodates multiple faculties, administrative departments, and student facilities. The first level houses critical administrative departments such as Management, Human Resources, and Finance, as well as a computer lab for students. The second level is dedicated to the university's library, serving as a shared resource for all faculties. The third level includes student labs, a lecturers' room, and the IT department, which hosts essential services such as the university's web servers and other critical servers that support both campuses.

The Smaller Campus, while more specialized, is equally significant. It primarily supports the Faculty of Health Sciences, with facilities including staff offices and dedicated student labs. Despite its smaller scale, the campus requires secure and reliable connectivity to the Main Campus to ensure smooth operations, access to shared resources, and communication between staff and students.

2 OBJECTIVES

This project aims to design and implement a comprehensive network architecture that fulfills the specific needs of both campuses. The design incorporates:

1. **Scalability:** Ensuring the network can grow with the university, accommodating new faculties, devices, and users in the future.
2. **Security:** Protecting sensitive academic and administrative data through VLAN segmentation, port security, and other measures.
3. **Performance:** Delivering low-latency communication and efficient data routing within and between campuses.
4. **Reliability:** Building redundancy and fault-tolerance into the network to minimize disruptions.

To achieve these objectives, the network design adopts a **hierarchical topology** that organizes devices and connections into core, distribution, and access layers. This structure simplifies management and facilitates modular growth. **VLANs (Virtual Local Area Networks)** are used to segment traffic by department or function, isolating data flows and enhancing security. **Routing protocols** are employed to manage traffic efficiently. **RIPv2 (Routing Information Protocol version 2)** is implemented for dynamic internal routing between subnets, while **static routing** is used to handle external communication, including access to shared servers.

Given the diversity of needs at City University, the project also addresses the practical requirements of device configuration, IP addressing, and inter-campus connectivity. A private IP addressing scheme is implemented to support the VLAN structure, while DHCP services are deployed to streamline IP allocation. Security measures, including port security and VLAN access control, are introduced to protect the network from unauthorized access.

This report outlines the planning, implementation, and evaluation of the network design for City University. It begins with an in-depth exploration of the network design principles, followed by detailed configuration processes, performance testing, and a comprehensive evaluation of scalability, reliability, and security features. Through this project, City University's network is equipped to meet its current operational demands while laying a strong foundation for future expansion.

3 NETWORK DESIGN

3.1 Hierarchical Network Topology

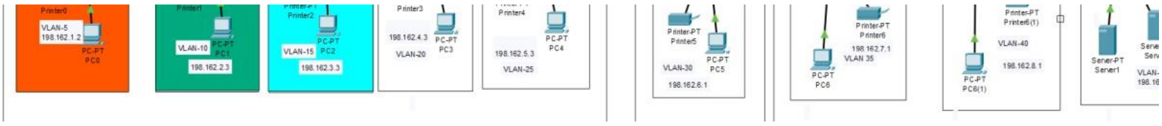
The network architecture employs a **hierarchical design model**, structured into core, distribution, and access layers to ensure scalability and modularity:

- **Core Layer:**
  - Hosts Layer 3 routers responsible for inter-campus connectivity and external routing.
  - Connects the Main Campus router to the Smaller Campus router via a WAN link.
- **Distribution Layer:**
  - Includes Layer 3 switches responsible for VLAN interconnectivity and intra-campus routing.
  - Separates departments and floors for effective traffic management.
- **Access Layer:**
  - Comprises Layer 2 switches connecting end devices, printers, and labs within each VLAN.

3.2 VLAN Design

Each department and functional area is assigned a unique VLAN to isolate traffic and improve network performance:

- **Main Campus VLANs:**
  - VLAN 5: Management Department (`198.162.1.x/24`)
  - VLAN 10: Human Resources (`198.162.2.x/24`)
  - VLAN 15: Finance (`198.162.3.x/24`)
  - VLAN 20: Administrative Office (`198.162.4.x/24`)
  - VLAN 25: Computer Lab (`198.162.5.x/24`)
  - VLAN 30: Library (`198.162.6.x/24`)
  - VLAN 35: Student Labs (`198.162.7.x/24`)
  - VLAN 40: Lecturer’s Room (`198.162.8.x/24`)
  - VLAN 55: IT Department, including servers (`198.162.13.x/24`)
- **Smaller Campus VLANs:**
  - VLAN 45: Student Labs (`198.162.9.x/24`)
  - VLAN 50: Faculty Offices (`198.162.11.X/24`)



3.3 IP Addressing Scheme

To ensure structured traffic flow and scalability, the network employs a private IP addressing scheme:

- Each VLAN uses a **/24 subnet**.
- Inter-campus routing and external server access utilize the **198.162.10.x/24** subnet.
- DHCP dynamically assigns IPs to end devices in designated VLANs.

3.4 Routing Protocols

- **RIPv2:** Configured to dynamically route traffic between VLANs within each campus.
- **Static Routing:** Used for external server communication across the WAN link.

3.5 Physical Connectivity

- Routers (2911 series) interconnect campuses through a dedicated WAN link.
- Core switches (3650 series) aggregate VLAN traffic at the distribution layer.
- Access switches (2960 series) connect end devices, printers, and labs.

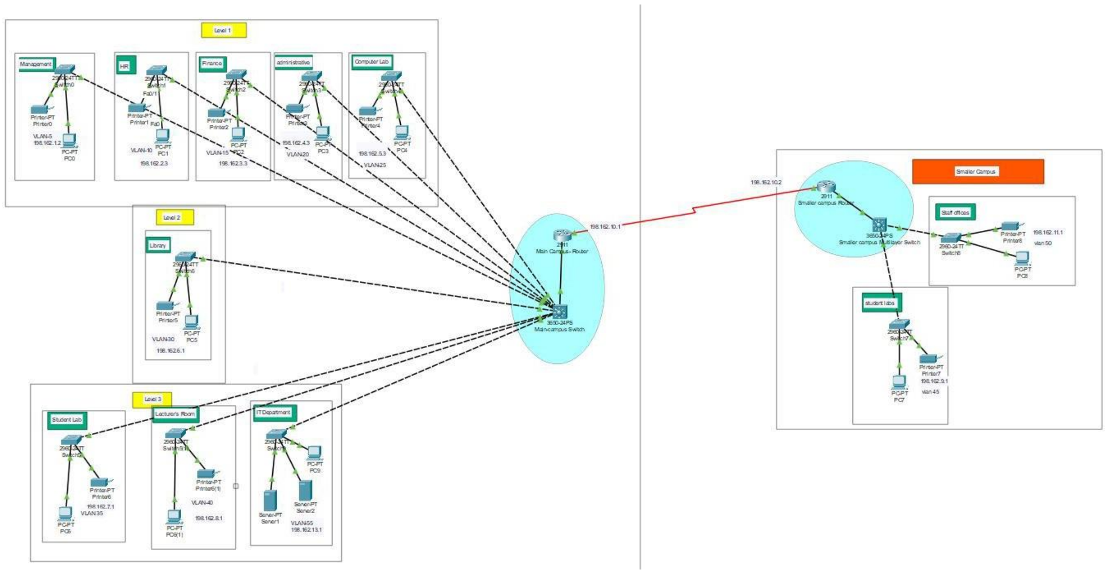


Fig: - NETWORK TOPOLOGY OF CITY UNIVERSITY’S CAMPUSES (left- Main campus , Right- Smaller campus)

4 CONFIGURATION

4.1 VLAN Configuration

VLANs were configured on Layer 2 switches to segment traffic:

```
Bash code


Switch(config)# vlan 5
Switch(config-vlan)# name Management
Switch(config)# vlan 10
Switch(config-vlan)# name HR
...
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 5
```

VLANs were assigned to ports connecting specific departments.

4.2 Inter-VLAN Routing

Layer 3 switches at the distribution layer enable inter-VLAN communication:

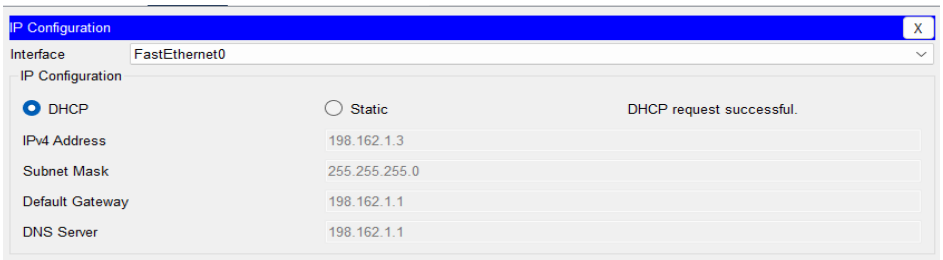
```
Bash code
Switch(config)# ip routing
Switch(config)# interface vlan 5
Switch(config-if)# ip address 198.162.1.1 255.255.255.0
Switch(config)# interface vlan 10
Switch(config-if)# ip address 198.162.2.1 255.255.255.0
```

3.3 DHCP Configuration

Dynamic IP allocation was implemented for end devices:

```
Bash code
Router(config)# ip dhcp pool VLAN5
Router(dhcp-config)# network 198.162.1.0 255.255.255.0
Router(dhcp-config)# default-router 198.162.1.1
...
Router(config)# ip dhcp excluded-address 198.162.1.1 198.162.1.10
```

DHCP scopes were configured for each VLAN to prevent IP conflicts.



IP Configuration

Interface FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address 198.162.1.3

Subnet Mask 255.255.255.0

Default Gateway 198.162.1.1

DNS Server 198.162.1.1

3.4 Routing Protocol Configuration

- **RIPv2:**

  ```
  Bash code
  Router(config)# router rip
  Router(config-router)# version 2
  Router(config-router)# network 198.162.11.1
  Router(config-router)# network 198.162.9.1
  Router(config-router)# network 198.162.10.0
  Router(config-router)#
  ```

- **Static Routing for External Servers:**

  ```
  Bash code
  Router(config)# ip route 0.0.0.0 0.0.0.0 198.162.10.1
  ```

3.5 Security Measures

Switches were configured with port security and VLAN access controls:

```
Bash code
Switch(config)# interface fa0/1
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security violation restrict
```

5 PERFORMANCE EVALUATION

5.1 Connectivity Tests

Connectivity was tested between devices using `ping` and `traceroute` commands:

- Intra-VLAN communication: Successfully verified.
- Inter-VLAN communication: Confirmed through Layer 3 switches.
- WAN connectivity: Tested across the Main and Smaller campuses.

5.2 Network Latency

Simulations in Cisco Packet Tracer indicated low latency for internal VLAN traffic. Inter-campus traffic exhibited slightly higher latency due to the WAN link.

5.3 Troubleshooting

Issues such as incorrect VLAN assignments and missing RIP updates were identified and resolved using Packet Tracer's simulation mode.

6 SCALABILITY ASSESSMENT

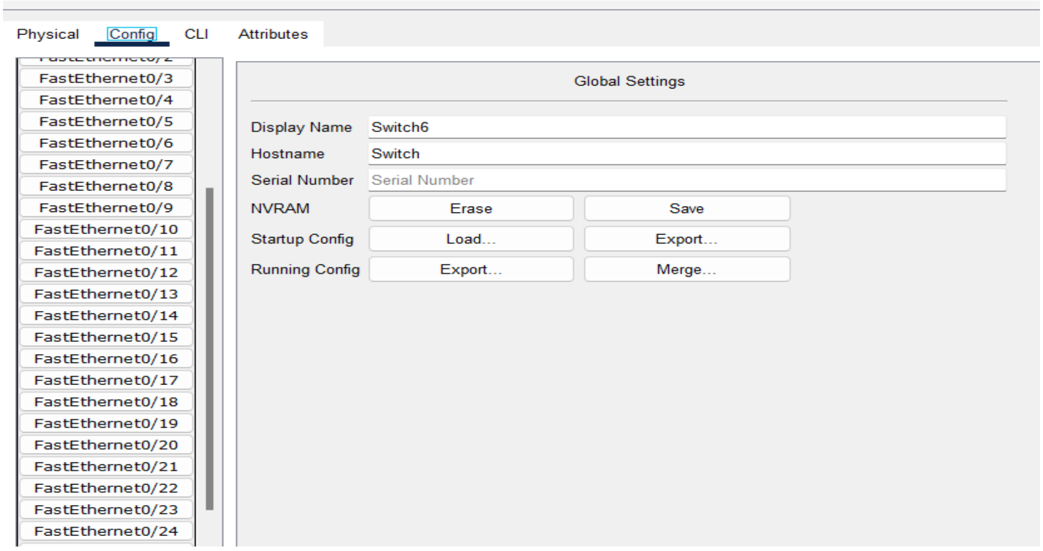
6.1 Future Growth

New VLANs can be added for additional faculties, departments, or administrative units without affecting the existing configuration. New switches at the access layer can connect to the distribution layer with minimal changes to the network topology and additional routers can be integrated at the distribution layer to manage increased traffic or provide enhanced routing capabilities.

The use of a hierarchical network design (core, distribution, and access layers) ensures that each layer can be expanded independently. For instance, new access switches can be added without requiring changes to the core layer, preserving the network's stability.

6.2 IP Address Space

The reserved `/24` subnets ensure adequate address space for future devices.



Global Settings

Display Name: Switch6

Hostname: Switch

Serial Number: Serial Number

7 RELIABILITY AND REDUNDANCY

7.1 Fault Tolerance

- Redundant connections between the core and distribution layers ensure that in case one link fails, traffic can reroute through an alternate path. Protocols like Spanning Tree Protocol (STP) are implemented to prevent loops and ensure these redundant links are utilized efficiently without creating network instability.
- Regularly scheduled backups of router and switch configurations enable quick recovery during hardware failure or configuration errors and backup files are securely stored and updated following significant configuration changes.

7.2 Stability Measures

- Segmentation of the network into multiple VLANs reduces broadcast traffic within each VLAN, improving overall performance. This minimizes the risk of broadcast storms that could degrade the network's performance
- RIPv2 dynamic routing ensures stable traffic management. RIPv2 ensures stable traffic management by dynamically updating routes based on network changes. It automates route recalculations in the event of a link failure, reducing manual intervention and downtime.

8 SECURITY OVERVIEW

8.1 Implemented Features

- **VLAN Isolation:** Prevents unauthorized access between departments.
- **Port Security:** Restricts device connections to prevent rogue access.
- **DHCP Snooping:** Protects against rogue DHCP servers.

8.2 Recommendations

- Enable **Access Control Lists (ACLs)** for additional traffic filtering.
- Implement **802.1X authentication** for secure device access.

9 CRITICAL REFLECTION

9.1 Challenges

- Configuring VLANs across multiple switches required careful planning.
- Static routing for external servers initially caused routing loops, resolved by refining configurations.

9.2 Areas for Improvement

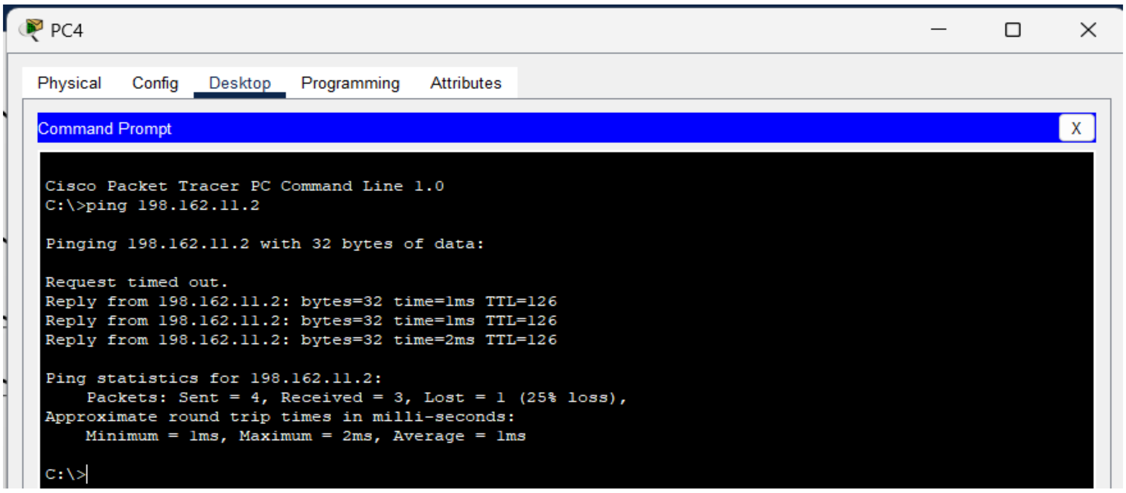
- Incorporate Quality of Service (QoS) for bandwidth-intensive applications.
- Plan for wireless network integration to support mobile devices.

10 CONCLUSION

The network design for City University provides a secure, scalable, and efficient infrastructure that meets the operational needs of both the Main and Smaller campuses. Through a hierarchical topology, the design ensures organized device management and simplifies future expansions. VLAN segmentation enhances security and reduces broadcast traffic, particularly protecting sensitive data in departments like HR and Finance while enabling shared resource access. RIPv2 dynamic routing ensures efficient intra-campus communication, while static routing supports reliable inter-campus connectivity and access to external servers. A private IP addressing scheme ensures scalability, and DHCP simplifies device management by automating IP assignments. Security features like port security, VLAN access control, and DHCP snooping protect against unauthorized access and network threats. Redundant links and failover mechanisms enhance reliability, ensuring uninterrupted connectivity. The modular design also supports future upgrades like QoS and wireless access points to meet evolving demands. Areas for improvement include implementing ACLs and 802.1X authentication to strengthen security and integrating QoS to optimize bandwidth for applications like video conferencing. Overall, the network provides a strong foundation for City University’s current needs and future growth, supporting its mission to deliver quality education in a digitally connected environment.

11 APPENDIX

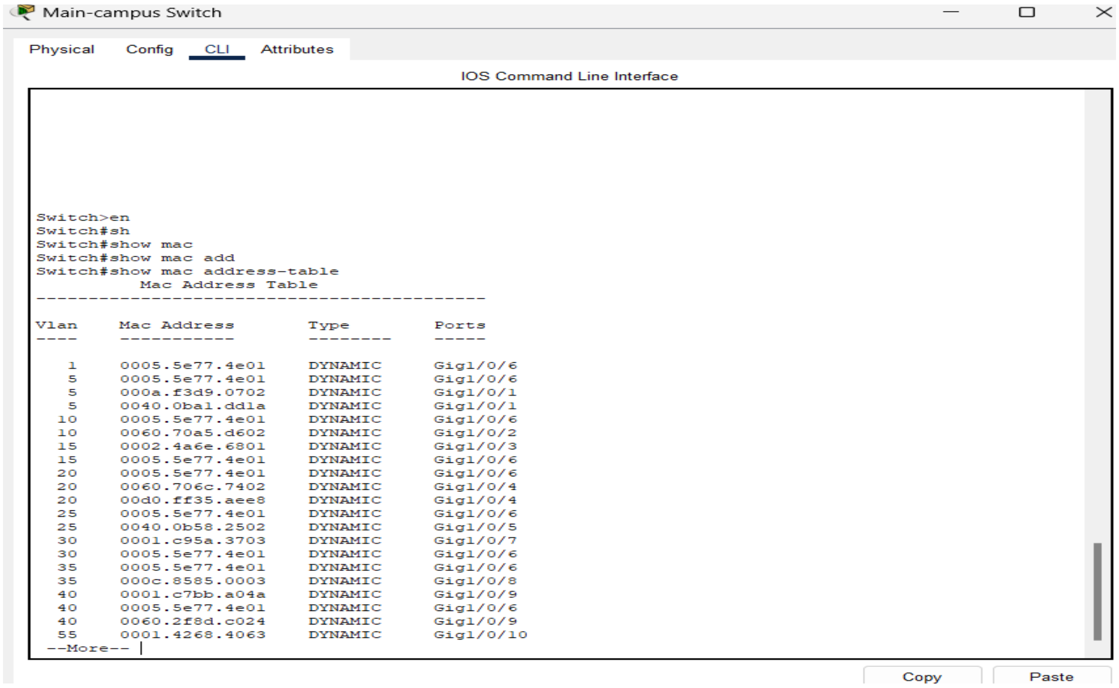
The network design facilitates seamless communication between campuses. As shown in the figure below, PC 8 from the Smaller Campus successfully communicates with devices across the network, demonstrating reliable connectivity and proper routing.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 198.162.11.2

Pinging 198.162.11.2 with 32 bytes of data:

Request timed out.
Reply from 198.162.11.2: bytes=32 time=1ms TTL=126
Reply from 198.162.11.2: bytes=32 time=1ms TTL=126
Reply from 198.162.11.2: bytes=32 time=2ms TTL=126

Ping statistics for 198.162.11.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Figure 1: Successful ping from Smaller Campus PC 8

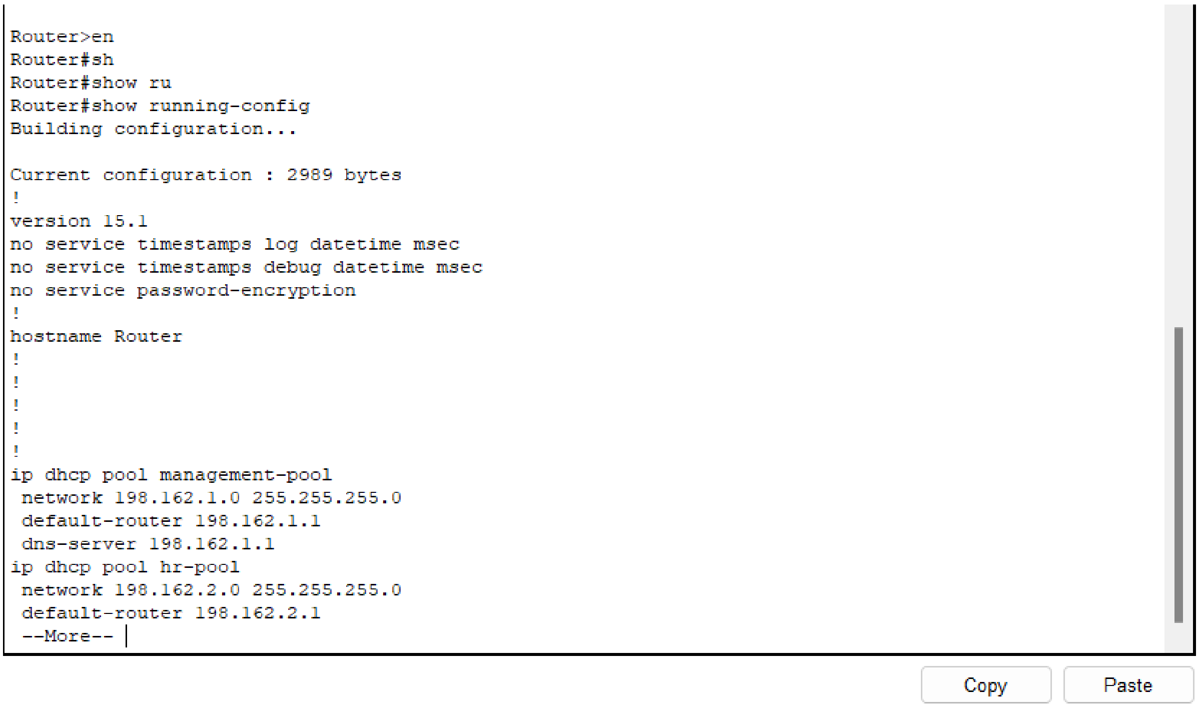
This section provides evidence of port security implementation to enhance network security. The screenshot below demonstrates the configuration of port security on a specific switch interface, showing the allowed number of MAC addresses, violation mode, and current MAC address assignments.



```
Switch>en
Switch#sh
Switch#show mac
Switch#show mac add
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0005.5e77.4e01    DYNAMIC     Gig1/0/6
   5    0005.5e77.4e01    DYNAMIC     Gig1/0/6
   5    000a.f3d9.0702    DYNAMIC     Gig1/0/1
   5    0040.0ba1.dd1a    DYNAMIC     Gig1/0/1
  10    0005.5e77.4e01    DYNAMIC     Gig1/0/6
  10    0060.70a5.d602    DYNAMIC     Gig1/0/2
  15    0002.4a6e.6801    DYNAMIC     Gig1/0/3
  15    0005.5e77.4e01    DYNAMIC     Gig1/0/6
  20    0005.5e77.4e01    DYNAMIC     Gig1/0/6
  20    0060.706c.7402    DYNAMIC     Gig1/0/4
  20    00d0.ff35.aee8    DYNAMIC     Gig1/0/4
  25    0005.5e77.4e01    DYNAMIC     Gig1/0/6
  25    0040.0b58.2502    DYNAMIC     Gig1/0/5
  30    0001.c95a.3703    DYNAMIC     Gig1/0/7
  30    0005.5e77.4e01    DYNAMIC     Gig1/0/6
  35    0005.5e77.4e01    DYNAMIC     Gig1/0/6
  35    000c.8585.0003    DYNAMIC     Gig1/0/8
  40    0001.c7bb.a04a    DYNAMIC     Gig1/0/9
  40    0005.5e77.4e01    DYNAMIC     Gig1/0/6
  40    0060.2f8d.c024    DYNAMIC     Gig1/0/9
  55    0001.4268.4063    DYNAMIC     Gig1/0/10
 --More--
```

Figure 2: Port Security Configuration on FastEthernet0/1

The routing configuration in Main campus router-



```
Router>en
Router#sh
Router#show ru
Router#show running-config
Building configuration...

Current configuration : 2989 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
ip dhcp pool management-pool
 network 198.162.1.0 255.255.255.0
 default-router 198.162.1.1
 dns-server 198.162.1.1
ip dhcp pool hr-pool
 network 198.162.2.0 255.255.255.0
 default-router 198.162.2.1
 --More--
```

Figure 3: Main campus router configuration details.

End