PROJECT SCOPE

1.0 .Project Scope

This project focuses on upgrading the network infrastructure of a software development organisation to address performance, security, and scalability issues.

1.1 Current Network Overview and Challenges

The organisation uses a 24-port unmanaged switch with a shared internet connection configured through Windows. An internal server provides FTP and HTTP services.
Key Issues: Network congestion leading to slow performance, lack of security between departments, and limited scalability with a single 192.168.1.0/24 subnet.

1.2 Objectives and Approach

Performance: Use VLANs and managed switches to reduce broadcast traffic and improve speed.
Security: Implement VLAN segmentation and ACLs to control data flow and restrict unauthorised access.
Scalability: Adopt a modular network design and flexible IP addressing to accommodate future growth.

1.3 Scope of Implementation

Network Segmentation: Create VLANs for Sales, Development, Testing, and the server, with tailored access controls.
Hardware Upgrades: Install a managed switch, configure a router for inter-VLAN routing, and implement power redundancy.
Deliverables: Provide an optimised and secure network, with detailed documentation and minimal planned downtime for installation.

This condensed version gives a high-level summary of the project scope while highlighting the key issues, objectives, and implementation plan.

1. NETWORK REQUIREMENTS

1.1 Device List and Quantities

Device	Required Nos.
PCs	5
Laptop	8
Printer	2
Server	1
Router	2
Switch	1
Serial DCE Cable	1
Copper Cross-Over Cables	3
Copper Straight-Through Cables	12

1.2 Key Requirements

Network Segmentation: The network must be divided into separate VLANs for Sales, Development, Testing, and the Server, each with a unique TCP/IP address range to improve performance and security.
Traffic Management: Use a managed switch to handle VLAN traffic and ensure broadcast traffic is confined to its respective segment, reducing congestion.
Access Control: Implement Access Control Lists (ACLs) on the router to restrict inter-departmental communication, with specific permissions for Development and Testing departments to access each other.
Server Protection: Configure the network so that only FTP and HTTP traffic can reach the internal server, blocking all other traffic types.
Hardware Reliability: Use a power backup system (such as a UPS) for critical network components to ensure continuous operation during power outages.

1.3 Hardware List

Components	Quantity	Specification
PCs	2	Standard office desktop with Ethernet connectivity
Laptop	1	Laptop with both Ethernet and wireless connectivity options for
Printer	1	Network printer with Ethernet interface for shared access on the
Server	1	- Mid-range server capable of hosting DNS and web server applications - Dual-core processor, 8GB RAM, 500GB HDD, Ethernet connectivity
Router	2	- Cisco-compatible routers with at least two Gigabit Ethernet ports for internal and external network connections - Cisco 1941 or equivalent for Packet Tracer compatibility
Switch	1	- Managed Ethernet switch with at least 8 ports - Cisco 2960 or equivalent
Serial DCE Cable	1	Serial cable for connecting two routers (for WAN simulation)
Copper Crossover Cable	1	Ethernet crossover cable for direct connection between similar network devices
Copper Straight-Through Cable	5	Standard Ethernet cables for connecting different devices

2.4. HARDWARE CONFIGURATION

2.4.1 Cisco Router Configuration

Router Interfaces

Interface Configuration: Configure interfaces for each VLAN to allow inter-VLAN routing.

2.4.2 Managed Switch Configuration

VLAN Configuration

VLAN Creation: Create VLANs for each department and assign ports accordingly.

2.5 Access Control Lists (ACL) Configuration

2.5.1 ACL Creation

Purpose: Define rules to restrict access between VLANs based on departmental needs.

2.5.2 ACL Explanation

Access Control: The ACL permits only FTP and HTTP traffic from the Sales VLAN to the Server VLAN while denying all other traffic, ensuring that the Sales department cannot access Development and Testing VLANs.

2.6 Summary of Configuration

2.6.1 Documentation

Maintain detailed documentation of all configuration settings for troubleshooting and future reference.

2.6.2 Testing

After configuration, conduct tests to ensure proper communication between VLANs and verify that ACLs are functioning as intended.

These figures illustrate the configuration settings for the interfaces on Router 1 and Router 2, detailing the IP addressing and NAT (Network Address Translation) configurations essential for establishing communication between the internal organisation network and the external internet simulation. Each interface configuration serves a specific role in the network design.

2. NETWORK UPGRADE PLAN

This section outlines the strategic plan for upgrading the organisation's network infrastructure to address existing issues and meet future requirements.

2.1 Implementation Strategy

2.1.1 VLAN Segmentation

Purpose: To separate network traffic by department and reduce congestion.
Approach: Configure VLANs for Sales, Development, Testing, and the Server on a managed switch, with each VLAN having a unique subnet.

2.1.2 Hardware Installation

Router Setup: Install two routers for redundancy and configure them for inter-VLAN routing and internet access.
Managed Switch: Replace the existing unmanaged switch with a managed switch, ensuring VLANs are correctly assigned and configured.

2.1.3 Server Configuration

Security Settings: Apply access control measures to allow only FTP and HTTP traffic to the server.
Performance Optimisation: Fine-tune settings to enhance data transfer speeds and ensure efficient server communication.

2.2 Step-by-Step Implementation

2.2.1 Planning and Design Phase

Network Design: Create detailed diagrams of the upgraded network topology, including VLAN configuration, IP addressing, and hardware placement.
Equipment Procurement: Purchase the necessary hardware, including managed switches, routers, cables, and power backup units.

2.2.2 Configuration Phase

Router Configuration: Set up inter-VLAN routing, ACLs, and security features.
Switch Configuration: Create VLANs, assign ports to appropriate VLANs, and configure trunk ports for communication with the router.

2.2.3 Testing and Validation

Performance Testing: Verify network speed improvements and ensure traffic is correctly segmented.
Security Validation: Test ACLs to ensure proper restrictions are in place and no unauthorised access is possible.

2.3 Post-Implementation Activities

2.3.1 User Training

IT Team Training: Provide comprehensive training for IT staff on managing the new network setup, troubleshooting, and maintaining security.

End User Awareness: Educate users about best practices for accessing network resources securely.

2.3.2 Documentation and Handover

Configuration Manuals: Create detailed documentation on the hardware configuration, VLAN settings, and ACL rules.

Network Diagrams: Provide updated diagrams showing the new network design and key components.

3. EXISTING NETWORK INFRASTRUCTURE TOPLOGY

This section provides an overview of the current network infrastructure, illustrating the layout and components that make up the existing network.

3.1 Current Topology Overview

3.1.1 Network Components

Devices: The existing network consists of PCs, laptops, an unmanaged switch, a server, and shared internet access via a single router.
Connectivity: All devices are connected to the unmanaged switch, which leads to the router that provides internet access and internal connectivity.

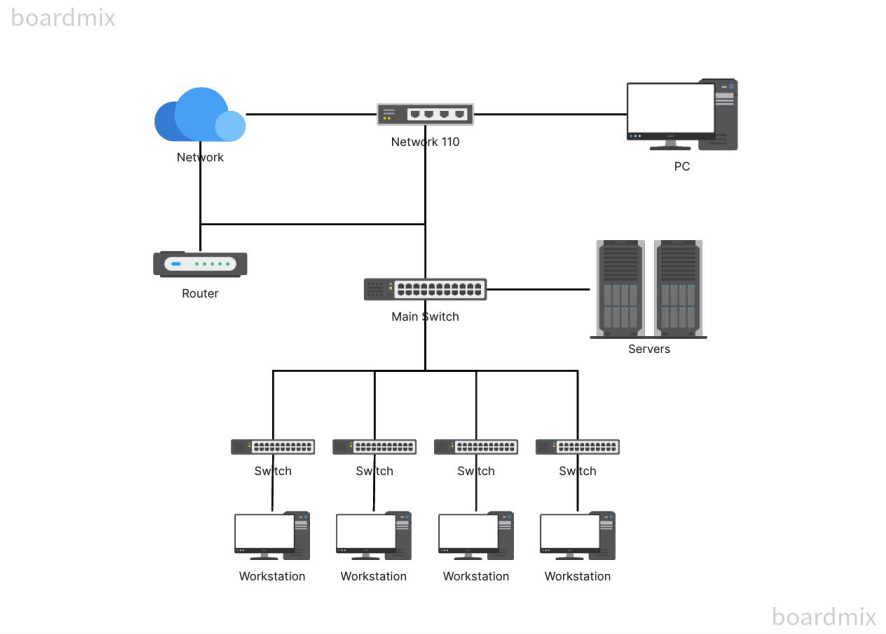
3.1.2 Network Layout

The layout is flat, with all devices on the same subnet (192.168.1.0/24), leading to excessive broadcast traffic and security risks due to the lack of segmentation.

3.2 Diagram of Existing Network Topology

Below is a conceptual diagram representing the existing network topology:

Router: Connects the internal network to the internet.



Unmanaged Switch: Connects all devices on the same local network.
Devices: PCs, laptops, a server, and printers connected directly to the switch.

3.3 Key Issues Identified in the Existing Topology

3.3.1 Performance Limitations

The flat topology results in high levels of broadcast traffic, leading to network congestion and slow performance.

3.3.2 Security Vulnerabilities

Lack of segmentation allows unauthorised access to sensitive data across departments, increasing the risk of data breaches.

3.3.3 Scalability Challenges

The existing setup does not support future growth; adding more devices would further strain the network.

4. NETWORK DESIGN STRATEGY

This section outlines the strategic approach for designing the upgraded network infrastructure, focusing on performance improvement, security enhancement, and scalability.

4.1 Design Objectives

4.1.1 Performance Improvement

Goal: Enhance network speed and reliability by reducing congestion.
Method: Implement VLANs to segment traffic, thereby isolating department communications and minimising broadcast traffic.

4.1.2 Security Enhancement

Goal: Protect sensitive information and restrict unauthorised access between departments.
Method: Use Access Control Lists (ACLs) and VLANs to control traffic flow and enforce security policies.

4.1.3 Scalability

Goal: Create a flexible network that can accommodate future growth.
Method: Design a modular architecture with easy-to-add components and a structured IP addressing scheme.

4.2 Proposed Network Architecture

4.2.1 VLAN Configuration

Sales Department: VLAN ID 10 (Subnet: 192.168.10.0/24)
Development Department: VLAN ID 20 (Subnet: 192.168.20.0/24)
Testing Department: VLAN ID 30 (Subnet: 192.168.30.0/24)
Server Network: VLAN ID 40 (Subnet: 192.168.40.0/24)

4.2.2 Network Topology

Transition from a flat topology to a hierarchical design:

Core Layer: High-capacity routers for inter-VLAN routing and internet access.
Distribution Layer: Managed switches configured with VLANs to control traffic.
Access Layer: End devices (PCs, laptops, printers) connected to the distribution layer switches.

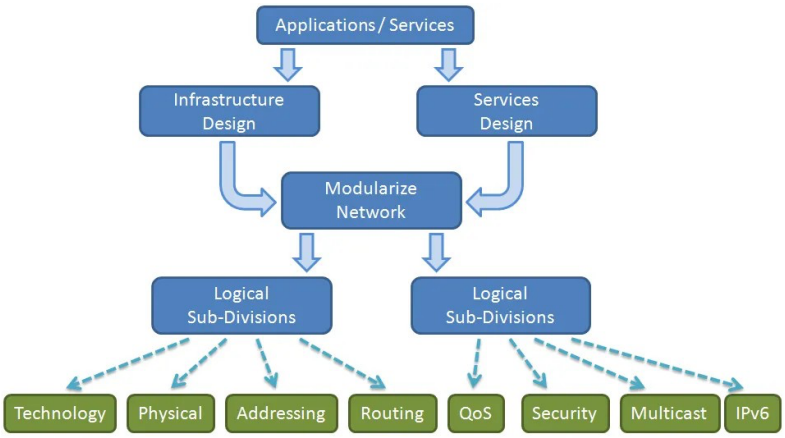


Fig: Architecture Diagram

4.3 Traffic Management Strategy

4.3.1 Quality of Service (QoS)

Implement QoS policies to prioritize critical traffic (e.g., FTP and HTTP for the server) over less critical traffic, ensuring better performance during peak usage.

4.3.2 Monitoring and Maintenance

Establish regular monitoring protocols for network performance and security, allowing for proactive maintenance and issue resolution.

4.4 Implementation Plan

4.4.1 Phased Deployment

Phase 1: Set up VLANs and configure the managed switch.
Phase 2: Install routers and configure inter-VLAN routing with ACLs.
Phase 3: Migrate devices to the new VLANs and conduct testing for performance and security.

4.4.2 Documentation

Create comprehensive documentation detailing network design, configuration settings, and troubleshooting procedures to facilitate ongoing management and future upgrades.

5. TCP/IP NETWORK ADDRESS TABLE

This table outlines the IP addressing scheme for each department and the server.

Department/ Device	VLAN ID	IP Address Range	Subnet Mask	Gateway IP	Number of Hosts
Sales Department	10	192.168.10.2 - 192.168.10.51	255.255.255.0	192.168.10.1	50
Development Department	20	192.168.20.2 - 192.168.20.61	255.255.255.0	192.168.20.1	60
Testing Department	30	192.168.30.2 - 192.168.30.51	255.255.255.0	192.168.30.1	50
Server Network	40	192.168.40.2 - 192.168.40.11	255.255.255.0	192.168.40.1	10

5.1 Domain Name Mapping Table

This table maps domain names to their corresponding IP addresses for internal services.

Domain Name	IP Address	Purpose
sales.department.local	192.168.10.1	Sales VLAN Gateway
dev.department.local	192.168.20.1	Development VLAN Gateway
test.department.local	192.168.30.1	Testing VLAN Gateway
server.department.local	192.168.40.1	Server Gateway
ftp.server.local	192.168.40.2	FTP Server
web.server.local	192.168.40.3	Web Application Server

5.2 NAT Table

This table outlines the NAT configuration for translating private IP addresses to a public IP address for internet access.

Private IP Address	Public IP Address	Translation Type	Protocol
192.168.10.0/24	203.0.113.5	Dynamic NAT	TCP/UDP
192.168.20.0/24	203.0.113.5	Dynamic NAT	TCP/UDP
192.168.30.0/24	203.0.113.5	Dynamic NAT	TCP/UDP
192.168.40.0/24	203.0.113.5	Dynamic NAT	TCP/UDP

Key Considerations

TCP/IP Address Table: Ensures organised addressing and facilitates efficient communication within departments while providing room for growth.
Domain Name Mapping: Simplifies access to internal resources by using human-readable domain names instead of IP addresses.
NAT Table: Allows internal devices to access the internet while hiding their private IP addresses, enhancing security.

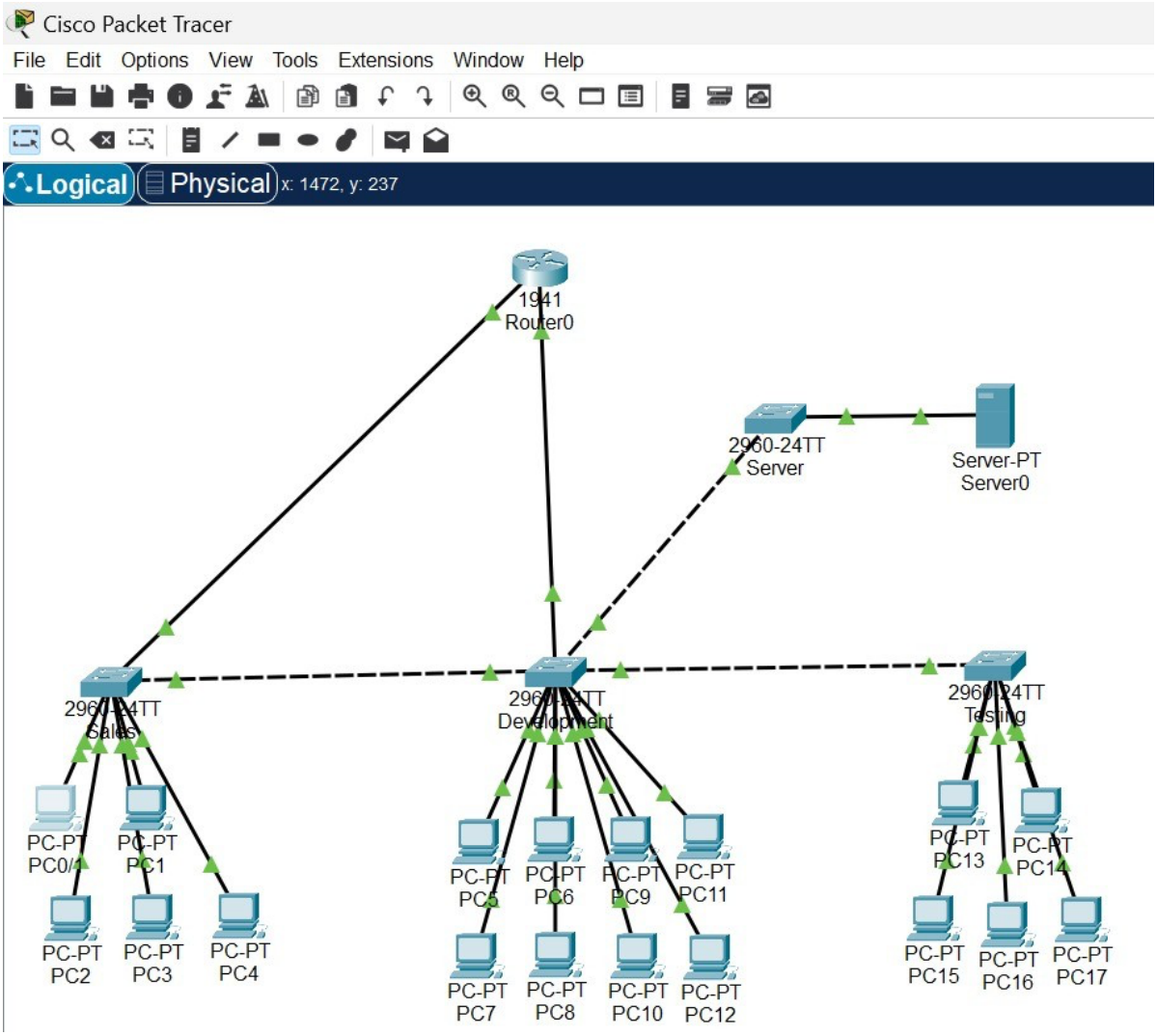
6. UPGRADED INFRASTRUCTURE TOPOLOGY DIAGRAM

6.1 New Topology Overview

6.1.1 Network Components

Devices: The upgraded network includes PCs, laptops, managed switches, routers, and a dedicated server, all organised into distinct VLANs for better performance and security.
Connectivity: Each department is connected through a managed switch that facilitates VLAN segmentation, with a router for inter-VLAN routing and internet access.

6.2 Diagram of Upgraded Network Topology



6.3 Key Features of the Upgraded Topology

6.3.1 VLAN Segmentation
Each department operates on its VLAN, significantly reducing unnecessary broadcast traffic and improving overall network performance.

6.3.2 Enhanced Security
Access Control Lists (ACLs) on the router restrict traffic between VLANs, ensuring sensitive data remains protected from unauthorised access.

6.3.3 Scalability
The hierarchical design allows for easy addition of new devices and departments without major reconfiguration, accommodating future growth.

6.4 Future Considerations

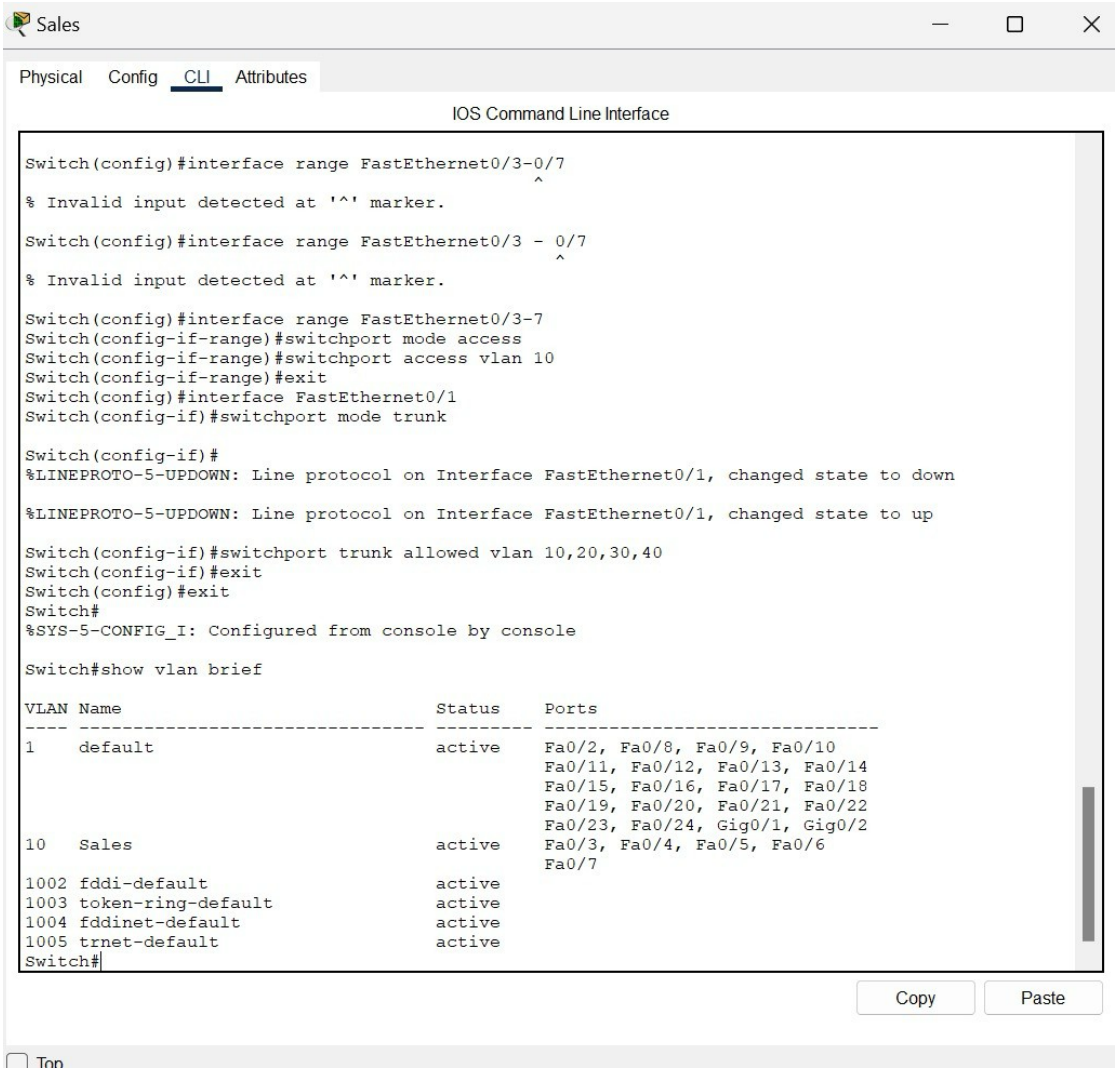
6.4.1 Network Monitoring
Implement network monitoring tools to analyze traffic patterns, detect anomalies, and maintain performance.

6.4.2 Redundancy and Failover
Consider adding redundant connections and failover protocols to ensure network reliability and uptime.

```
Device Name: Router0
Device Model: 1941
Hostname: Router

Port                  Link   VLAN   IP Address         IPv6 Address                            MAC Address
GigabitEthernet0/0    Up     --     <not set>          <not set>                               00D0.973E.5701
GigabitEthernet0/0.10 Up     --     192.168.10.1/24    <not set>                               00D0.973E.5701
GigabitEthernet0/0.20 Up     --     192.168.20.1/24    <not set>                               00D0.973E.5701
GigabitEthernet0/1    Up     --     <not set>          <not set>                               00D0.973E.5702
GigabitEthernet0/1.30 Up     --     192.168.30.1/24    <not set>                               00D0.973E.5702
GigabitEthernet0/1.40 Up     --     192.168.40.1/24    <not set>                               00D0.973E.5702
Vlan1                 Down   1      <not set>          <not set>                               000A.413A.6ECA

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router0
```


Sales
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch(config)#interface range FastEthernet0/3-0/7
% Invalid input detected at '^' marker.
Switch(config)#interface range FastEthernet0/3 - 0/7
% Invalid input detected at '^' marker.
Switch(config)#interface range FastEthernet0/3-7
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#show vlan brief
VLAN Name Status Ports
1 default active Fa0/2, Fa0/8, Fa0/9, Fa0/10
Fa0/11, Fa0/12, Fa0/13, Fa0/14
Fa0/15, Fa0/16, Fa0/17, Fa0/18
Fa0/19, Fa0/20, Fa0/21, Fa0/22
Fa0/23, Fa0/24, Gig0/1, Gig0/2
10 Sales active Fa0/3, Fa0/4, Fa0/5, Fa0/6
Fa0/7
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Switch#
Copy
Paste
Top

7. SOLUTION EXPLANATION

This section provides an in-depth analysis of the proposed network infrastructure upgrade, detailing how each component of the solution addresses the network issues and meets the organisation's requirements. The subsections will explain the rationale and configuration specifics.

8.0 Segmentation Using VLANs

8.1 Purpose of VLANs

Definition: Virtual Local Area Networks (VLANs) are used to divide a physical network into smaller, isolated segments at the data link layer (Layer 2) of the OSI model.

Advantages:

Traffic Isolation: VLANs prevent broadcast traffic from affecting other segments, reducing congestion.

Improved Security: Sensitive departments, such as Development and Testing, can be protected from unauthorised access.

Efficient Traffic Management: VLANs optimise network performance by ensuring that broadcast and multicast traffic stays within its segment.

8.2 VLAN Configuration Strategy

VLAN Assignments:

VLAN 10: Assigned to the Sales department to ensure traffic from Sales does not interfere with other departments.

VLAN 20: Dedicated to the Development team, which needs controlled communication with Testing.

VLAN 30: Used for the Testing department, allowing interaction only with Development as required.

VLAN 40: Configured for the internal server, isolating it from unnecessary traffic.

Trunk Ports: Configured on the managed switches to enable VLAN-tagged traffic between switches and the router.

8.3 Access Control Lists (ACLs) for Traffic Management

8.3.1 Purpose of ACLs

Definition: ACLs are rules applied to network devices to control incoming and outgoing traffic.

Benefits:

Restrict Unauthorised Access: Prevents unauthorised users or departments from accessing sensitive areas of the network.

Traffic Filtering: Ensures only specific types of traffic, such as FTP and HTTP, can reach the server.

8.3.2 ACL Implementation

Configuration Example:

Sales Department Restrictions: Create an ACL that denies traffic from VLAN 10 (Sales) to VLANs 20 and 30 (Development and Testing).

Permitting Development & Testing Communication: Configure an ACL to allow traffic between VLAN 20 and VLAN 30.

Server Traffic Filtering: Set up an ACL on the router to allow only FTP (Port 21) and HTTP (Port 80) traffic to VLAN 40, blocking all other ports for added security.

8.4 Inter-VLAN Routing

8.4.1 Why Inter-VLAN Routing Is Needed

Definition: Inter-VLAN routing enables communication between different VLANs using a Layer 3 device (like a router or Layer 3 switch).

Purpose: Since VLANs inherently do not communicate with each other, routing is necessary to facilitate selective communication, such as allowing Development and Testing to collaborate.

8.4.2 Configuration of Inter-VLAN Routing

Router-on-a-Stick Setup: This involves using a single physical interface on the router configured as a trunk, allowing it to handle traffic from multiple VLANs.

Sub-Interface Configuration: For each VLAN, create a sub-interface on the router and assign the corresponding IP address to act as the default gateway for that VLAN.

8.5 Security Enhancements

8.5.1 Isolating the Server

Server Subnet: Placing the internal server on its dedicated subnet (VLAN 40) isolates it from all other broadcast domains, reducing the risk of unauthorized access and improving performance.

Traffic Filtering: ACLs are used to restrict access to the server, allowing only FTP and HTTP traffic.

8.5.2 Preventing Lateral Movement

Cross-Department Restrictions: ACLs ensure that even if a device on one VLAN is compromised, it cannot communicate freely with other VLANs, limiting potential damage.

8.6 Hardware Considerations

8.6.1 Cisco Managed Switch Configuration

VLAN Setup: Use a managed switch to create and manage VLANs. Each port is assigned to a specific VLAN based on the connected device's department.
Trunk Ports: Configure trunk ports to carry traffic for multiple VLANs between switches and the router.

8.6.2 Cisco Router Configuration

Sub-Interfaces: Configure sub-interfaces on the router for inter-VLAN routing. Each sub-interface is tagged with the appropriate VLAN ID and assigned an IP address.
Routing Protocol: Use a simple static routing setup if the network is relatively small or a dynamic routing protocol like OSPF for scalability.

8.7 Scalability and Future Proofing

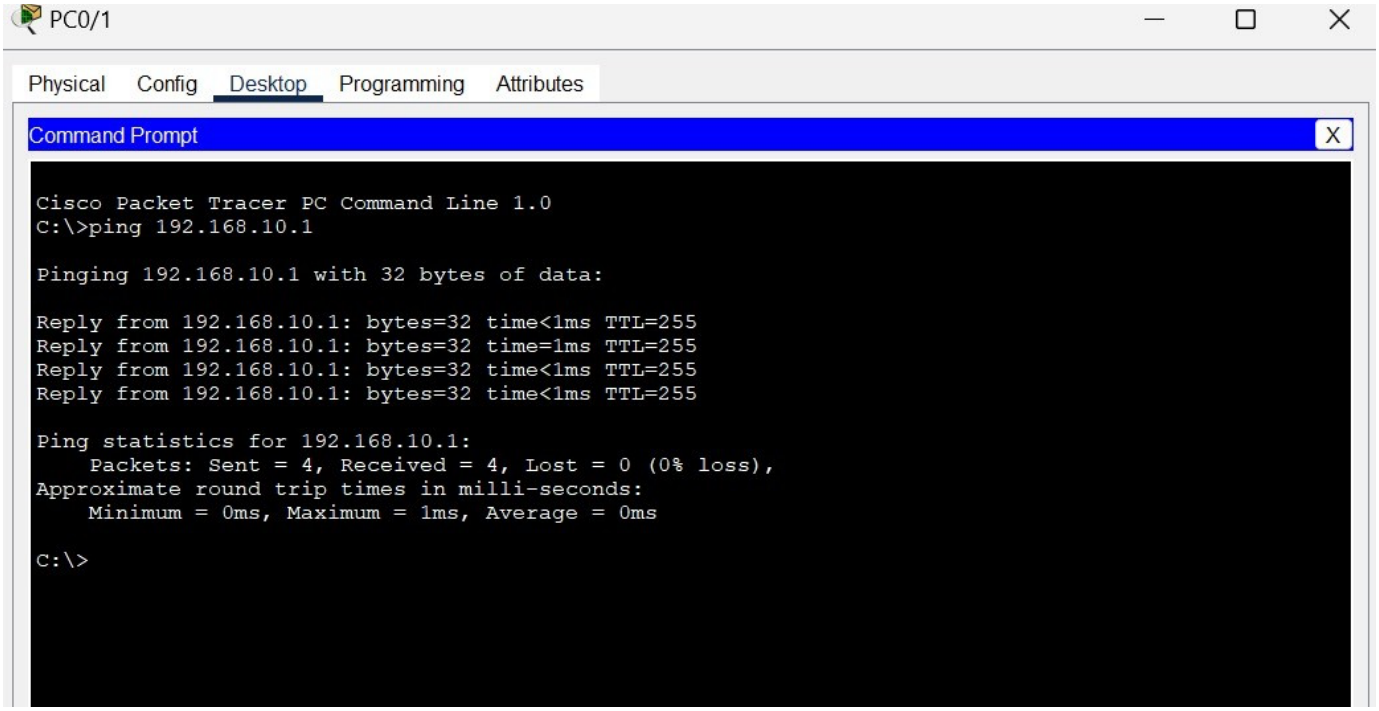
8.7.1 Room for Expansion

IP Address Allocation: The use of /24 subnets ensures that there are enough IP addresses for future growth within each department.
Additional VLANs: The network design allows for adding more VLANs in the future if new departments or functions are created.

8.7.2 Hardware Upgrades

Modular Equipment: Use modular switches and routers that can be easily expanded or upgraded as the organisation grows.
Power Redundancy: Implement an Uninterruptible Power Supply (UPS) system to ensure network reliability.

By following this structured solution, the organisation will benefit from an efficient, secure, and scalable network that meets current needs and is prepared for future demands. The use of VLANs, ACLs, and managed hardware ensures optimal performance and security across all departments.


PC0/1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.1
Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.10.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>

8. CONCLUSION

The network upgrade plan strategically enhances performance, security, and scalability for the organisation. By implementing VLANs, we effectively reduce broadcast traffic and ensure efficient communication within departments. The Cisco router and managed switch configurations provide robust inter-VLAN routing and enforce strict Access Control Lists (ACLs) to safeguard sensitive resources. Domain name mapping simplifies resource access, while NAT facilitates secure internet connectivity. The structured addressing scheme allows for easy expansion, and the hierarchical design ensures future growth is seamlessly accommodated. Overall, this comprehensive approach transforms the network into a more reliable, secure, and scalable infrastructure.

9. REFERENCES

- https://www.cisco.com/c/en/us/support/index.html
- https://www.netacad.com/courses/packet-tracer
- https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html
- https://www.practicalnetworking.net/stand-alone/subnetting/
- https://www.cloudflare.com/learning/dns/what-is-dns/