Name: Neemkar Sai Pratheek

Reg .No: 23BCY10062

Department: B-tech

Course : IBM Cybersecurity

Title:Secure Office Network with VLANs, Inter-VLAN Routing & ACLs

Summary:

Designed and implemented a robust and secure office network simulation in Cisco Packet Tracer, focusing on advanced Layer 2 and Layer 3 network segmentation and access control. Successfully configured VLANs (HR, IT, Sales) and established efficient inter-VLAN routing using a "Router-on-a-Stick" topology, effectively overcoming router physical port limitations. Developed and applied Access Control Lists (ACLs) to enforce granular traffic policies, specifically denying IT network access to the HR network while maintaining other critical communication paths. Validated all configurations through comprehensive ping tests, confirming precise adherence to security requirements and demonstrating proficiency in network design, configuration, and troubleshooting.

Problem Statement:

Flat networks allow unrestricted communication between all devices, which leads to potential security risks and inefficient traffic management. This project simulates a secure small-office network using VLANs and ACLs to enforce segmentation and access control between departments.

Objectives:

- Design a logical office network in Cisco Packet Tracer.
- Implement VLANs to segment departments (HR, IT, Sales).
- Configure Inter-VLAN routing using Router-on-a-Stick.
- Apply ACLs to restrict communication between VLANs.
- Validate ACL impact using logical ping and connectivity tests.

Scope of Work:

The project focused on the design and implementation of a segmented small-office network for HR (VLAN 10), IT (VLAN 20), and Sales (VLAN 30) departments. This included configuring VLANs and their respective access ports on a central Layer 2 switch. A "Router-

on-a-Stick" topology was established by configuring a single trunk link between the central switch and a router's GigabitEthernet interface, optimizing router port utilization. Router subinterfaces were created for each VLAN to enable inter-VLAN routing. Static IP addressing was assigned to end devices within their respective VLAN subnets. A Standard Access Control List (ACL) was configured to specifically deny traffic from the IT network (192.168.20.0/24) from accessing the HR network (192.168.10.0/24) and applied outbound on the router's HR VLAN subinterface. Validation included comprehensive ping tests to confirm adherence to ACL policies and overall network connectivity.

Tools & Lab Setup:

- **Primary Tools Used:** Cisco Packet Tracer.
- **Environment Details:**
    - Virtual Machine Setup: Not applicable (direct network simulation within Packet Tracer).
    - Target VM: Not applicable.
    - Network Mode: Simulated switched and routed network environment

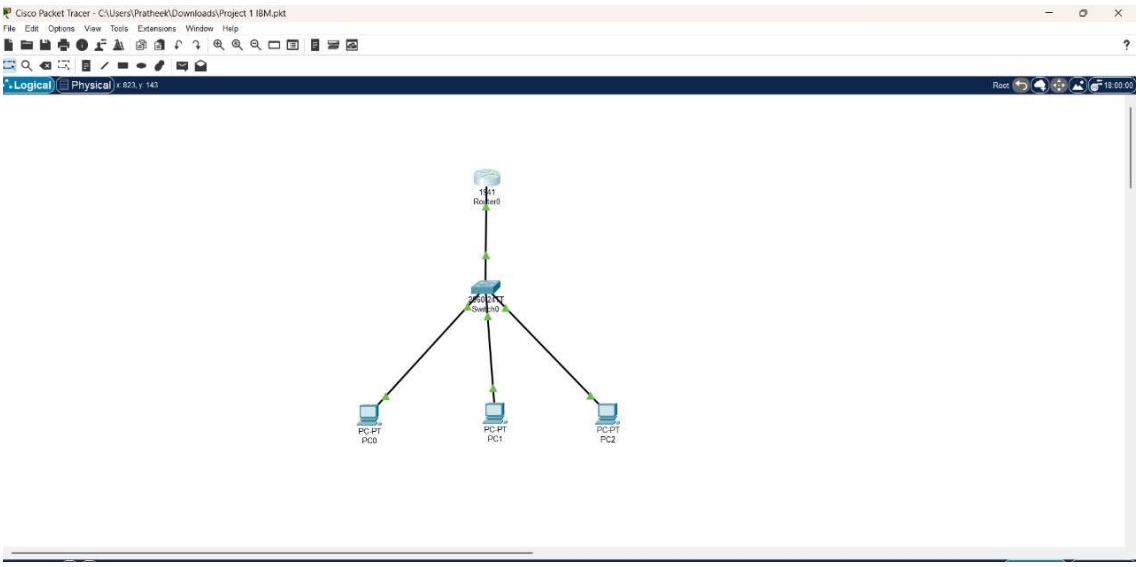
- **Tool Configuration & Commands (summary of key commands used):**
    - **VLAN Configuration:** vlan [VLAN_ID], name [VLAN_NAME], interface [interface_ID], switchport mode access, switchport access vlan [VLAN_ID].
    - **Trunk Link Configuration:** interface [interface_ID], switchport mode trunk, no shutdown.
    - **Router-on-a-Stick Setup:** interface [physical_interface_ID], no shutdown, interface [physical_interface_ID].[VLAN_ID], encapsulation dot1Q [VLAN_ID], ip address [Gateway_IP] [Subnet_Mask].
    - **Access Control Lists (ACLs):** access-list [ACL_NUMBER] deny [Source_Network] [Wildcard_Mask], access-list [ACL_NUMBER] permit any, interface [subinterface_ID], ip access-group [ACL_NUMBER] out.
    - **IP Addressing:** Static IP, Subnet Mask, and Default Gateway configuration on end devices.
    - **Verification:** show vlan brief, show interface trunk, show ip interface brief, show access-lists, ping.

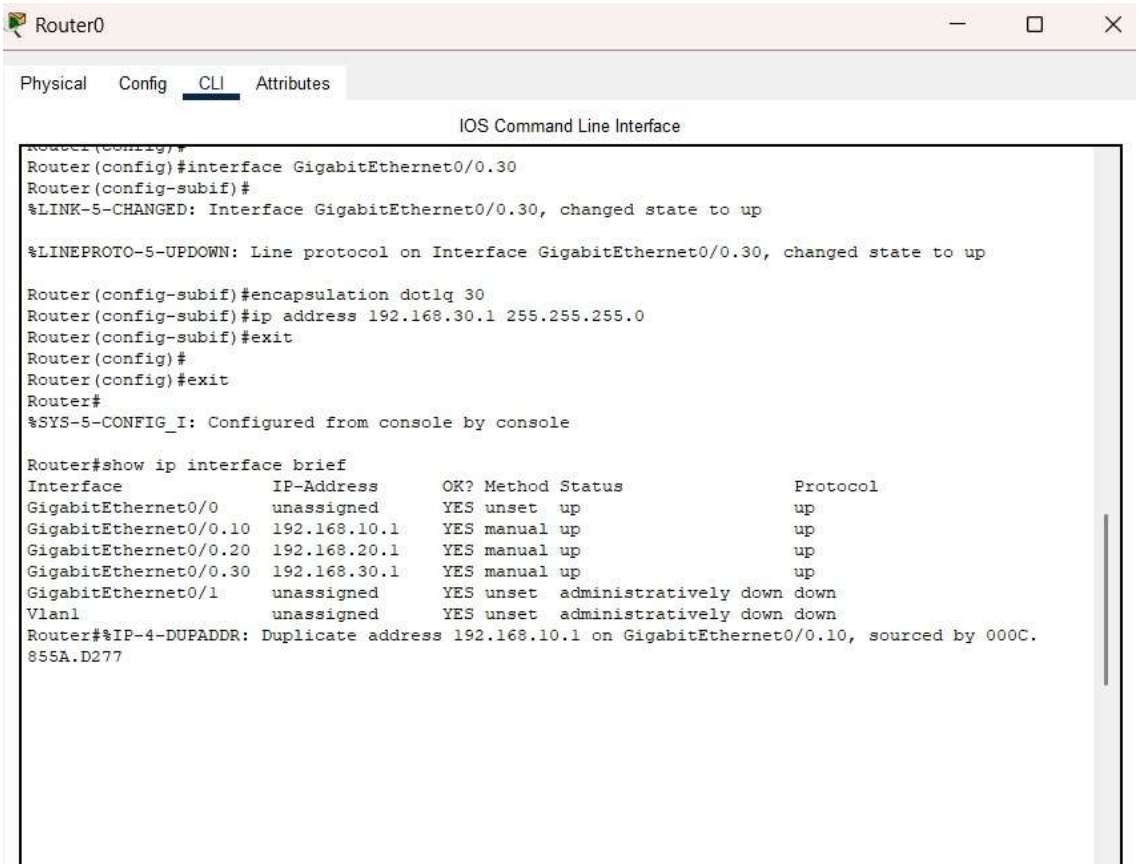
Implementation & Execution Summary

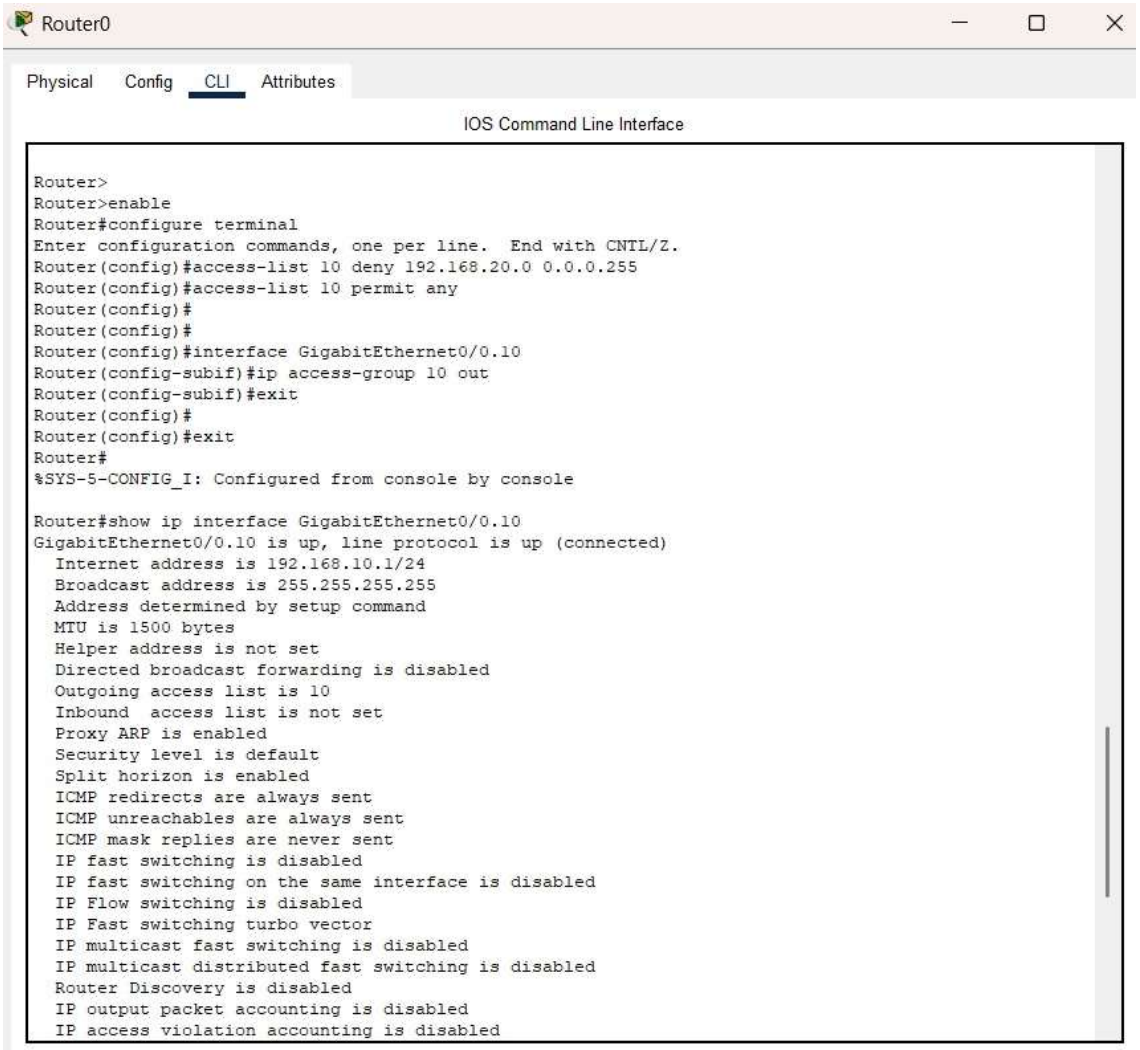
This phase involved the practical configuration and deployment of the secure office network designed in Cisco Packet Tracer. Key steps included:

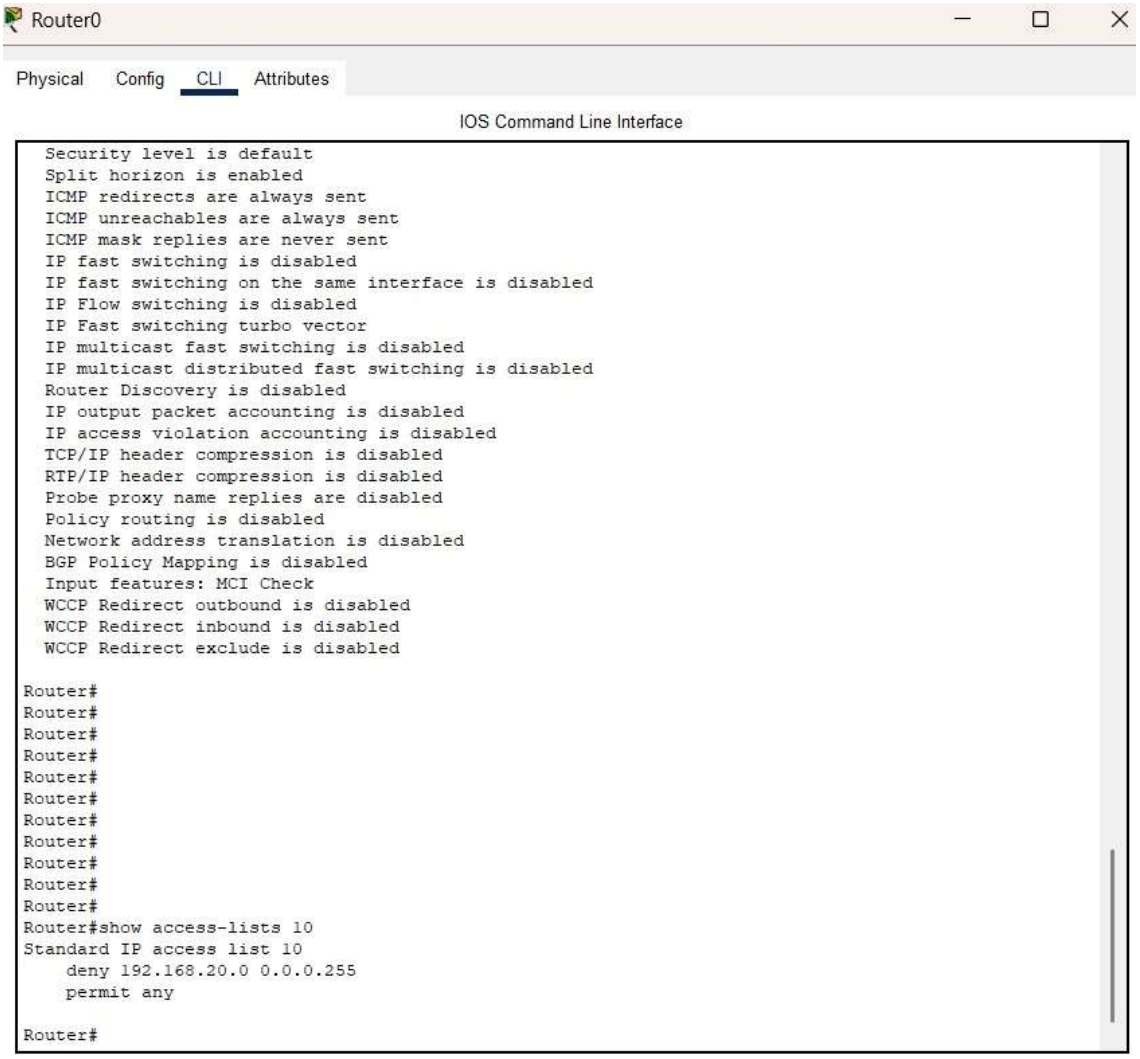
- **VLAN Configuration:** Three distinct VLANs were created: VLAN 10 (HR), VLAN 20 (IT), and VLAN 30 (Sales). Access ports on the central switch (e.g., Fa0/1 for HR, Fa0/2 for IT, Fa0/3 for Sales) were assigned to their respective VLANs.
- **Trunk Link Establishment:** A single FastEthernet0/24 interface on the central switch was configured as a trunk port, allowing traffic for all configured VLANs (1, 10, 20, 30) to traverse to the router.
- **Router-on-a-Stick Setup:** On Router0, the GigabitEthernet0/0 physical interface was activated, and logical subinterfaces (GigabitEthernet0/0.10, Gig0/0.20, Gig0/0.30) were created. Each subinterface was configured with 802.1Q encapsulation for its corresponding VLAN and assigned its respective gateway IP address (e.g., 192.168.10.1 for VLAN 10).
- **Static IP Addressing:** End devices (HR-PC, IT-PC, Sales-PC) were assigned static IP addresses, subnet masks, and default gateways within their respective VLAN subnets.
- **ACL Configuration & Application:** A standard Access Control List (ACL 10) was created on Router0 to deny traffic originating from the IT network (192.168.20.0/24). This ACL was then applied outbound on the GigabitEthernet0/0.10 subinterface (HR VLAN gateway).
- **Validation:** Connectivity tests, primarily using ping commands, were conducted to verify inter-VLAN routing functionality and to confirm the ACL's impact on traffic flow.

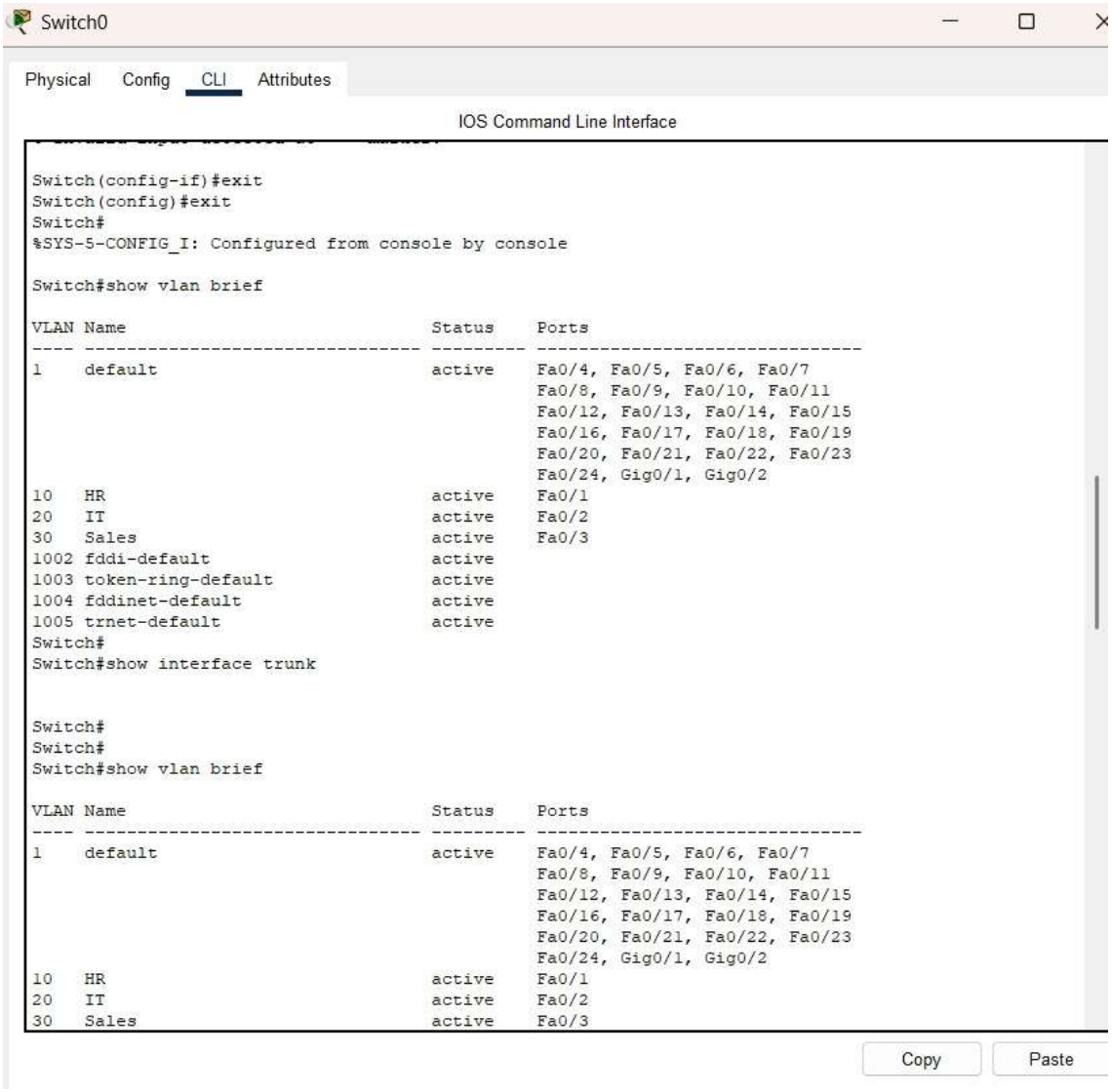
Screenshots:




Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router(config)#interface GigabitEthernet0/0.30
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up
Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES unset up up
GigabitEthernet0/0.10 192.168.10.1 YES manual up up
GigabitEthernet0/0.20 192.168.20.1 YES manual up up
GigabitEthernet0/0.30 192.168.30.1 YES manual up up
GigabitEthernet0/1 unassigned YES unset administratively down down
Vlan1 unassigned YES unset administratively down down
Router#%IP-4-DUPADDR: Duplicate address 192.168.10.1 on GigabitEthernet0/0.10, sourced by 000C.
855A.D277


Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 10 deny 192.168.20.0 0.0.0.255
Router(config)#access-list 10 permit any
Router(config)#
Router(config)#
Router(config)#interface GigabitEthernet0/0.10
Router(config-subif)#ip access-group 10 out
Router(config-subif)#exit
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show ip interface GigabitEthernet0/0.10
GigabitEthernet0/0.10 is up, line protocol is up (connected)
Internet address is 192.168.10.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is 10
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled


Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#show access-lists 10
Standard IP access list 10
deny 192.168.20.0 0.0.0.255
permit any
Router#



Challenges Faced

During the implementation, several key challenges were encountered and successfully resolved:

- **Initial Trunk Port Status:** The switch's FastEthernet0/24 interface, intended as the trunk link to the router, initially showed an "Operational Mode: down" status. This was rectified by ensuring the corresponding router interface was administratively "no shutdown" and active.
- **Router Port Limitations vs. Design:** The initial project design suggested "3 Switches connected to 1 Router". However, given the specific Cisco 1941 router's two GigabitEthernet ports, a direct one-to-one connection for three separate switches was not feasible. This challenge was overcome by adapting the topology to a single central switch connected via one trunk link to the router, implementing the "Router-on-a-Stick" concept for all VLANs.

- **ACL Impact on Bidirectional Communication:** A key challenge in validating the ACL was understanding its precise impact on return traffic. While the ACL was designed to deny IT access to HR, this also resulted in HR-initiated pings to IT appearing to fail (Request timed out) because the IT-sourced reply packets were blocked by the ACL when attempting to return to the HR network. This required careful analysis to confirm the ACL's intended one-way functionality was, in fact, working correctly as per the problem statement.

Findings & Analysis

The project successfully demonstrated the effectiveness of network segmentation and access control:

- **VLANs for Logical Segmentation:** VLANs effectively isolated broadcast domains, ensuring that devices within different departments (HR, IT, Sales) were logically separated even when connected to the same physical switch.
- **Efficient Inter-VLAN Routing:** The "Router-on-a-Stick" configuration proved highly efficient, allowing a single router interface to route traffic between multiple VLANs, thus conserving valuable router physical ports.
- **Granular Access Control:** The configured Standard ACL successfully enforced a specific security policy: traffic from the IT network was explicitly denied access to the HR network. This denial included reply traffic, making IT effectively unreachable by HR, thereby fulfilling the one-way restriction requirement.
- **Policy Compliance:** All other inter-VLAN communication paths not explicitly denied by the ACL (e.g., Sales to HR, Sales to IT) remained functional due to the permit any statement in the ACL, confirming precise policy implementation.

Learning Outcomes

This project provided significant learning outcomes, both technical and professional:

- **Technical Proficiency:** Deepened understanding of VLAN creation, port assignment, and trunking protocols. Gained hands-on experience in configuring Router-on-a-Stick, including subinterface creation, 802.1Q encapsulation, and gateway IP assignments. Mastered the syntax and application of Standard Access Control Lists, including the critical role of the permit any statement and the implications of inbound vs. outbound ACL application on two-way communication. Enhanced skills in network verification and troubleshooting using Cisco IOS show commands (e.g., show vlan, show interface trunk, show ip interface, show access-lists) and ping interpretation.
- **Problem-Solving & Adaptability:** Developed strong problem-solving skills through systematic troubleshooting of connectivity issues, such as inactive trunk links and ACL misinterpretations. Learned the importance of adapting initial network designs to practical hardware limitations (e.g., router port count) while still meeting project objectives.

- **Security Policy Translation:** Gained practical experience in translating high-level security policies (e.g., "deny IT access to HR") into specific, actionable network configurations (ACL rules and placement).

Future Scope

This project serves as a foundational network. Potential enhancements and extensions include:

- **Dynamic Routing Protocols:** Implementing dynamic routing protocols (e.g., OSPF, EIGRP) to allow the network to scale and adapt more efficiently to changes, particularly in a multi-router environment.
- **DHCP Services:** Configuring a DHCP server on the router to automate IP address assignment for end devices, simplifying network management.
- **Extended ACLs:** Utilizing extended ACLs for more granular traffic filtering based on source/destination ports (e.g., denying specific services like HTTP, FTP).
- **Network Address Translation (NAT):** Implementing NAT to allow internal devices to access external networks (e.g., the internet) while conserving public IP addresses.
- **Wireless LAN (WLAN) Integration:** Adding a wireless access point and configuring a secure WLAN for wireless client connectivity, integrating it into existing VLANs.
- **Layer 3 Switching:** Exploring the use of a Layer 3 switch for inter-VLAN routing, which can offer performance advantages over Router-on-a-Stick in certain network designs.
- **Security Enhancements:** Implementing additional security features such as Port Security, Storm Control, and basic firewall functionalities.