Design and Implementation of a Secure Office LAN with RIP Routing, ACLs, SSH Encryption

[*]Note: Sub-titles are not captured in Xplore and should not be used

Chejarla Anish
Electronics and Communication
Amrita Vishwa Vidyapeetham
Kollam, India
anishchejarla@gmail.com

Tamminaina Siva Kumar
Electronics and Communication
Amrita Vishwa Vidyapeetham
Kollam, India
email address or ORCID

Murakonda Chanakya
Electronics and Communication
Amrita Vishwa Vidyapeetham
Kollam, India
mchanukya2439@gmail.com

Murapaka Venkatesh
Electronics and Communication
Amrita Vishwa Vidyapeetham
Kollam, India
email address or ORCID

Kambham Mourya
Electronics and Communication
Amrita Vishwa Vidyapeetham
Kollam, India
email address or ORCID

***Abstract*—The design and implementation of a secure Local Area Network (LAN) that is appropriate for a contemporary office setting are presented in this project. Departments are divided among three interconnected routers in a mesh configuration, which is the network topology. The dynamic Routing Information Protocol (RIP v2) is used to establish routing, allowing for scalable and effective inter-network communication. Multiple layers are used to enforce security: SSH-based remote access guarantees encrypted administrative control, while Access Control Lists (ACLs) limit unwanted departmental communication. In order to safeguard router access, privilege-level configurations and local passwords are also used to manage user authentication. A GRE-based VPN tunnel is created between routers to mimic secure site-to-site communication, enabling selective data flow over links with ACL restrictions. The project also investigates real-time testing, ACL rule structuring, and IP addressing techniques. or Math in Paper Title or Abstract.**

***Index Terms*—Secure LAN Architecture, Routing Information Protocol (RIP v2), Access Control Lists (ACLs), Virtual Private Network (VPN)**

I. Introduction

In the ever-changing world of business networking, creating a scalable and secure Local Area Network (LAN) is now essential to guaranteeing data security and business continuity. In order to prevent unauthorized access and data breaches, modern office environments enforce strict security boundaries while requiring flexible interdepartmental communication. Even though they are simple to set up, traditional flat networks frequently lack scalability, resilience, and access control.

In this paper, a multi-router LAN architecture set up in a mesh topology is implemented to address these issues. With the help of the Routing Information Protocol version 2 (RIP v2), dynamic routing is made possible, allowing for effective route propagation and network change adaptation. Multiple layers of security are in place, including Access Control Lists (ACLs) to control access and encrypted remote access via SSH for administrative sessions.

II. Methodology

We used Cisco Packet Tracer to create a safe LAN environment in an office setting by breaking the project up into a series of structured phases. The whole thing went like this:

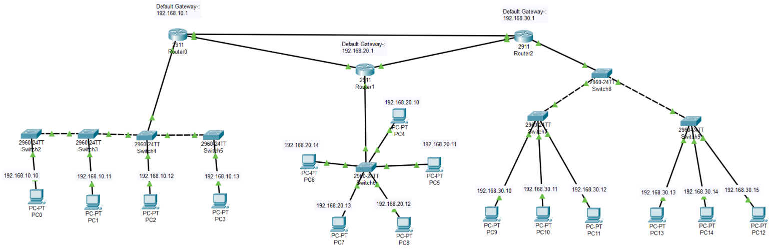


Fig. 1. Network Design Overview

A. Planning the design and layout of the network

Set up a mesh topology with three routers (R0, R1, and R2) to make sure there are backups and strong communication. Connected each router to a different LAN, which stood for a different office department. Set up point-to-point connections between routers using /30 subnets to make the best use of IP addresses.

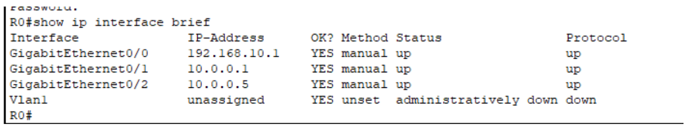
Identify applicable funding agency here. If none, delete this.

B. IP Addressing and Subnetting

Gave each LAN a private IPv4 address range: R0 LAN: 192.168.10.0/24 R1 LAN: 192.168.20.0/24 R2 LAN: 192.168.30.0/24 Used the 10.0.0.0/30 subnet to talk between routers: R0 R1, R1 R2, R2 R0

C. Device Configuration

Set up IP addresses on all the computers, switches, and router interfaces. Used the right kinds of cables: Copper Straight-Through: PC to Switch and Switch to Router Copper Cross-Over: Router to Router Enabled interfaces that don't shut down.

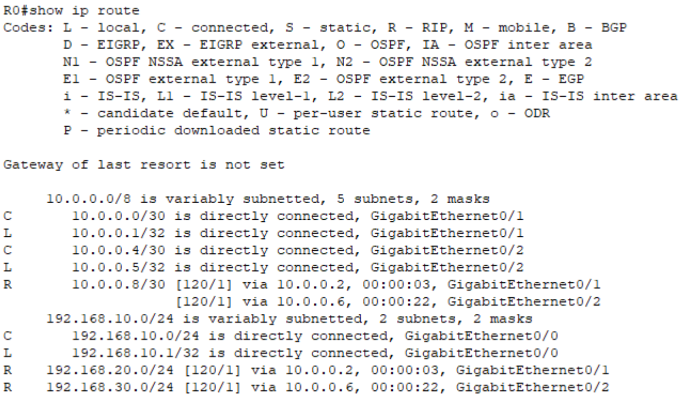


```
Password:
R0#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.10.1    YES manual up                    up
GigabitEthernet0/1     10.0.0.1        YES manual up                    up
GigabitEthernet0/2     10.0.0.5        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R0#
```

Fig. 2. IP Configuration

D. Routing Protocol Implementation (RIP)

Route sharing was automated by configuring RIP v2 on every router. router rip version two network statements for every network that is connected Routing was confirmed using show ip route.



```
R0#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.0.0.0/30 is directly connected, GigabitEthernet0/1
L       10.0.0.1/32 is directly connected, GigabitEthernet0/1
C       10.0.0.4/30 is directly connected, GigabitEthernet0/2
L       10.0.0.5/32 is directly connected, GigabitEthernet0/2
R       10.0.0.8/30 [120/1] via 10.0.0.2, 00:00:03, GigabitEthernet0/1
                    [120/1] via 10.0.0.6, 00:00:22, GigabitEthernet0/2
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
R    192.168.20.0/24 [120/1] via 10.0.0.2, 00:00:03, GigabitEthernet0/1
R    192.168.30.0/24 [120/1] via 10.0.0.6, 00:00:22, GigabitEthernet0/2
```

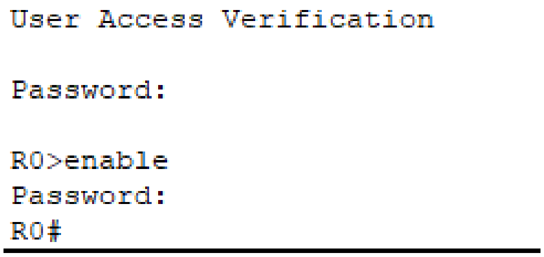
Fig. 3. IP routes

E. Device Security with Passwords

Enable secret for secure privileged EXEC access. Passwords for the console and VTY were configured: line console 0, login, and password line vty 0 4: login, password Password encryption was enabled using: service password-encryption

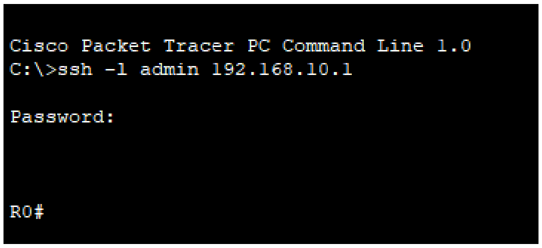
F. Enabling SSH for Secure Remote Access

created a privileged user and set a domain name. pairs of generated RSA keys (crypto key generate rsa 1024). VTY lines are restricted to only accept SSH: transport input SSH Log in locally Command prompt verification: ssh -l admin ¡router$_ip >$



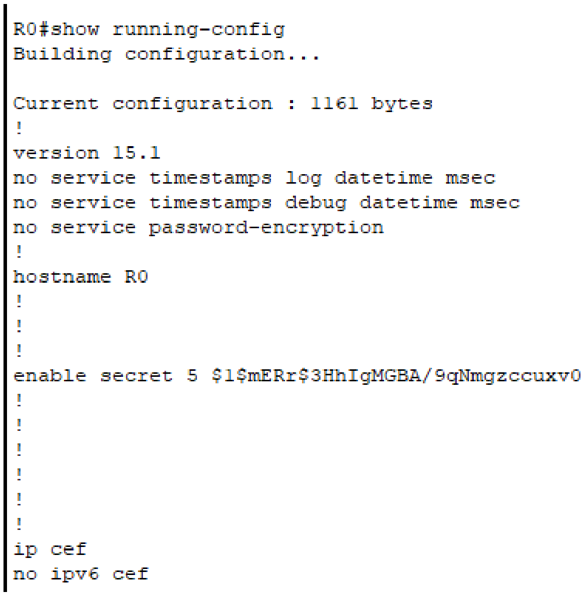
```
User Access Verification

Password:

R0>enable
Password:
R0#
```

Fig. 4. Console and Enable Password



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.10.1

Password:



R0#
```

Fig. 5. SSH Remote Access Test



```
R0#show running-config
Building configuration...

Current configuration : 1161 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R0
!
!
!
enable secret 5 $1$mERr$3HhIgMGBA/9qNmgzccuxv0
!
!
!
!
!
!
ip cef
no ipv6 cef
```

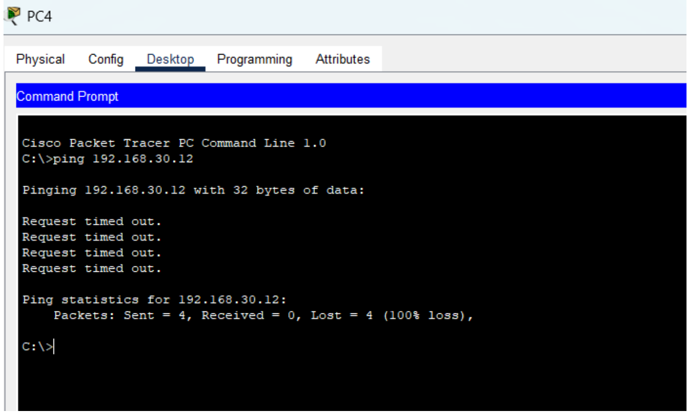
Fig. 6. IP Configuration

G. ACL (Access Control List) Implementation

Extended ACLs were created to limit communication between departments. An example of blocking R2-to-R1 traffic on R1: IP denied by access-list 20 0.0.0.255 192.168.30.0 0.0.0.255 192.168.20.0 access-list 20 permit IP of any applied on the appropriate interface using IP access-group 20 in. Ping tests and show access-lists were used for verification.

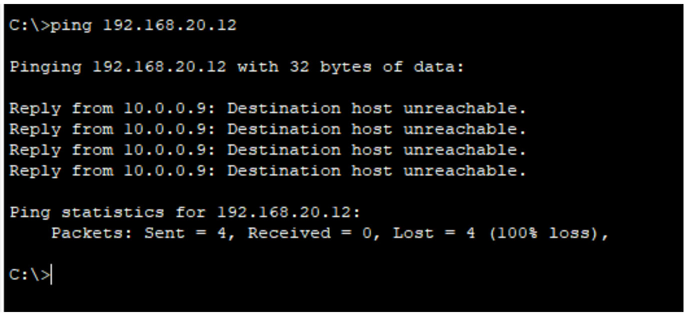
Results

The secure LAN network was effectively installed and tested in Cisco Packet Tracer, proving the efficacy of security



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.12

Pinging 192.168.30.12 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.30.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Fig. 7. ACL working R1-R2



```
C:\>ping 192.168.20.12

Pinging 192.168.20.12 with 32 bytes of data:

Reply from 10.0.0.9: Destination host unreachable.
Reply from 10.0.0.9: Destination host unreachable.
Reply from 10.0.0.9: Destination host unreachable.
Reply from 10.0.0.9: Destination host unreachable.

Ping statistics for 192.168.20.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Fig. 8. ACL working R2-R1

through layered design of the network. The outcomes achieved confirm the functional and security objectives created for the simulation of the office network.

A. Network Connectivity

All routers (R0, R1, R2) and terminals were properly configured with IP addresses and routing enabled through RIP version 2. Ping tests that were successful across all subnets prior to ACL implementation ensured there was complete connectivity. /30 subnetting on inter-router links minimized address wastage and provided efficient management of IPs.

B. Routing Protocol Verification

The RIP protocol facilitated dynamic route learning. This was verified using the show ip route command on all the routers, where routes learned via RIP were shown with accurate next-hop information. Route updates were propagated correctly, facilitating constant end-to-end communication.

C. Secure Remote Access

SSH was enabled on every router to provide remote access encrypted. A local user account with admin privileges was created and RSA key pairs were generated. VTY lines were locked down to only accept SSH connections and were set to use local authentication. SSH sessions to the routers were successfully initiated using the command: ssh -l admin [router ip].

D. ACL Functionality and Traffic Control

Access Control Lists (ACLs) were set to limit traffic between R2 (192.168.30.0/24) and R1 (192.168.20.0/24). Tests revealed pings from R2 to R1 were unsuccessful, but other communications continued working. Confirmation that the show access-lists command revealed hit counts on the deny rule demonstrated the ACL was indeed filtering traffic.

E. Device Security

All routers' console and VTY lines were password protected. The service password-encryption command effectively encrypted plaintext passwords in the running config. This kept the device config from being viewed by unauthorized users.

Conclusion

This project successfully demonstrates the design and simulation of a secure, scalable, and segmented Local Area Network (LAN) architecture tailored for a modern office environment. By employing a mesh topology with dynamic RIP v2 routing, the network ensures redundancy and seamless inter-departmental connectivity. The structured IP addressing and subnetting provided a foundation for efficient traffic management and clear network segmentation.

Layered security was implemented through the use of Access Control Lists (ACLs), encrypted remote access via SSH, and router privilege configurations, effectively limiting unauthorized access and reinforcing administrative control. The integration of a GRE-based VPN tunnel enabled secure communication across restricted interfaces, emulating real-world site-to-site secure data flow. Comprehensive testing confirmed that ACLs, routing, and remote access mechanisms performed as expected, highlighting the practicality and reliability of the overall LAN design. This implementation lays a robust groundwork for future enhancements involving enterprise-grade protocols and advanced security systems.

Future work

While the current implementation uses RIP v2, ACLs, and SSH-based access control to successfully demonstrate a secure and functional LAN environment, more sophisticated routing protocols like OSPF or EIGRP can be included in future iterations of this project. These protocols are perfect for enterprise-level deployments because they provide superior scalability, convergence, and support for hierarchical routing. Furthermore, logical departmentalization can be facilitated by the integration of VLANs across switches, which improves security and traffic management even more. To automate identity-based user access control, dynamic VLAN assignment utilizing protocols like 802.1x with RADIUS may also be investigated. Additionally, adding IPSec encryption to the GRE-based VPN would replicate a secure site-to-site communication channel in the real world. Production-grade WAN security procedures would be more accurately reflected by this improvement. Additionally, network monitoring could be