Submission

- This lab aims to help you connect the dots of all the topics we covered until now.
- The lab will be divided in 5 parts. After completing all the parts - defence of the lab + answer to some questions.
- The questions which might appear in the defence will be made available at the end of each lab part.

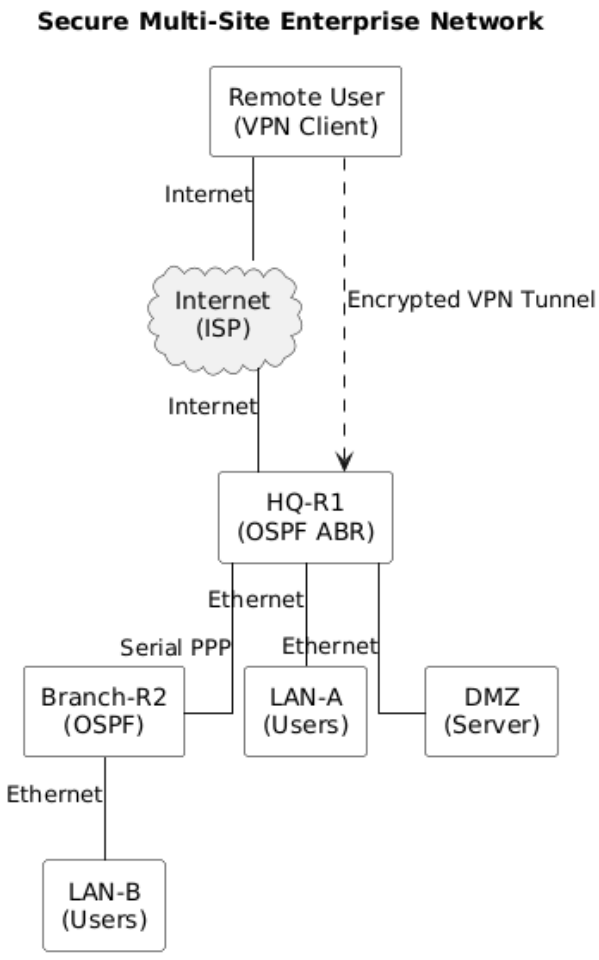
LAB STORY

A company ACME-EDU has: Headquarters (HQ), Branch Office, Remote users (VPN), Internet connectivity via ISP, Central authentication server (RADIUS)

You are hired to:

- Implement dynamic routing
- Secure the network
- Control traffic with ACLs
- Enable NAT for Internet access
- Configure WAN links
- Deploy VPNs
- Centralize authentication with AAA + RADIUS

TOPOLOGY (Logical)



PART 1 - LAB TASKS

1. Configure OSPFv2 for IPv4:
    - Area 0 at HQ
    - Area 10 at Branch
2. Configure OSPFv3 for IPv6
3. Manually set Router IDs
4. Configure passive interfaces
5. Influence DR/BDR election
6. Advertise a default route
7. Verify neighbor relationships and LSDB

Configure OSPFv2 for IPv4

Area 0 (R1)

```
conf t
router ospf 1
 router-id 1.1.1.1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
exit
```

Area 10 (R2)

```
conf t
router ospf 1
 router-id 2.2.2.2
 network 10.0.0.0 0.0.0.255 area 10
 network 192.168.2.0 0.0.0.255 area 10
exit
```

Configure OSPFv3 for IPv6

Enable IPv6 routing (BOTH routers)

```
conf t
ipv6 unicast-routing
```

Enable OSPFv3 on interfaces (recommended method)

HQ (R1)

```
conf t
interface g0/0
 ipv6 ospf 10 area 0
exit

interface s0/0/0
 ipv6 ospf 10 area 0
exit
```

Branch (R2)

```
conf t
interface g0/0
 ipv6 ospf 10 area 10
exit

interface s0/0/0
 ipv6 ospf 10 area 10
exit
```

Manually set Router IDs (OSPFv2 + OSPFv3)

Router ID is mandatory and shared by OSPFv2 and OSPFv3.

```
router ospfv3 10
 router-id 1.1.1.1
```

(Use `2.2.2.2` on R2)

After setting Router ID:

```
clear ip ospf process
clear ipv6 ospf process
```

Configure Passive Interfaces

Purpose:

- Advertise networks
- Do NOT send OSPF Hellos to end hosts

HQ (R1)

```
router ospf 1
 passive-interface g0/0
```

Branch (R2)

```
router ospf 1
 passive-interface g0/0
```

Do NOT make the WAN link passive.

Influence DR / BDR election

DR election applies on broadcast networks(Ethernet).

Increase priority on HQ to force DR

```
interface g0/0
 ip ospf priority 200
```

Default priority = `1` Priority `0` = never DR

Advertise a Default Route

1 — Create default route (HQ only)

```
ip route 0.0.0.0 0.0.0.0 <ISP-next-hop>
```

2 — Inject default into OSPF

```
router ospf 1
 default-information originate
```

Now Branch routers learn a default route via OSPF.

Verification — NEIGHBORS & LSDB

Neighbor relationships

```
show ip ospf neighbor
```

Expected:

- State = `FULL`
- Correct DR / BDR

LSDB inspection

```
show ip ospf database
```

Look for:

- Type 1 (Router LSAs)
- Type 2 (Network LSAs)
- Type 3 (Summary LSAs)

IPv6 neighbors

```
show ipv6 ospf neighbor
```

Routing table confirmation

```
show ip route ospf
show ipv6 route ospf
```

Part 1 - QUESTIONS:

1. Why OSPF is more suitable than RIP for this network topology?
2. Why the passive interfaces should be configured and what problem do they prevent?
3. How the ROUTER ID is selected on your routers?
4. Why does OSPF use LSAa instead of sending full routing tables?
5. What happens when you change the OSPF priority on an interface?
6. What would happen if Area 10 were configured as a stub area?
7. How is the default route advertised in OSPF, and where is it visible?

PART 2 — LAB TASKS

- Harden routers against basic attacks
- Implement centralized authenticatio using AAA + RADIUS
- Restrict management access
- Configure traffic monitoring using SPAN
- Understand the security separation between management plane and data plane

2.1 Device Hardening (R1 and R2)

Reduce the attack surface and ensure secure local and remote access.

Configuration (R1 and R2)

```
conf t
no ip domain-lookup
service password-encryption
security passwords min-length 10
login block-for 60 attempts 3 within 60
banner motd ^CUnauthorized access prohibited.^C

enable secret Adm1nP@ss!
username admin privilege 15 secret Adm1nP@ss!

ip domain-name acme-edu.local
crypto key generate rsa modulus 1024

line con 0
 logging synchronous
 exec-timeout 10 0
 login local

line vty 0 4
 transport input ssh
 exec-timeout 10 0
 login local

no ip http server
no ip http secure-server
end
wr
```

What we did now?

- Disabled insecure services (HTTP, Telnet)
- Forced SSH for remote management
- Protect against brute-force attacks
- Ensured encrypted credentials in configuration

2.2 Centralized Authentication — RADIUS Server

Move user authentication from individual routers to a central server.

RADIUS Server (Packet Tracer Server)

- IP address: `172.16.1.10/24`
- Default gateway: `172.16.1.1`
- Services → AAA → ON

- Create users:
    - `netadmin / CcnaR0cks!`
    - `student1 / LabPass123!`

2.3 AAA + RADIUS Configuration (R1 and R2)

Enable Authentication, Authorization, Accounting using RADIUS with local fallback.

Configuration (R1 and R2)

```
conf t
aaa new-model

radius server RAD1
 address ipv4 172.16.1.10 auth-port 1812 acct-port 1813
 key RadKey123

aaa group server radius RAD-GRP
 server name RAD1

aaa authentication login VTY-AUTH group RAD-GRP local
aaa authorization exec VTY-AUTH group RAD-GRP local if-authenticated
aaa accounting exec VTY-ACCT start-stop group RAD-GRP

line vty 0 4
 login authentication VTY-AUTH
 authorization exec VTY-AUTH
 accounting exec VTY-ACCT
 transport input ssh
end
wr
```

Verification

```
show run | section aaa
show aaa servers
test aaa group radius RAD-GRP netadmin CcnaR0cks! legacy
```

2.4 SPAN — Traffic Monitoring (HQ Switch)

Allow traffic inspection without disrupting network communication.

Configuration (HQ Switch)

```
conf t
monitor session 1 source interface fa0/1 both
```

```
monitor session 1 destination interface fa0/24
end
show monitor session 1
```

Part 2 — QUESTIONS

1. What is the difference between local authentication and RADIUS-based authentication?
2. Why is `aaa new-model` required before any AAA configuration?
3. What happens if the RADIUS server becomes unreachable?
4. Why is SSH preferred over Telnet for device management?
5. Which plane of the network (control, data, management) is protected by AAA?
6. What type of traffic is visible on a SPAN destination port?
7. Why is accounting useful in enterprise networks?

PART 3 — Access Control Lists (ACLs)

- Protect router management access
- Control user traffic between HQ and Branch
- Apply ACLs using best-practice placement rules

3.1 Secure VTY Access Using Standard ACL

Restrict who can remotely manage routers.

Configuration (R1 and R2)

```
conf t
ip access-list standard VTY_ONLY
 permit 192.168.1.0 0.0.0.255
 deny any log

line vty 0 4
 access-class VTY_ONLY in
end
wr
```

- Standard ACLs filter only source IP
- Applied to VTY lines, not interfaces
- Protects the management plane

3.2 Extended ACL — Branch Traffic Policy

Policy Requirements

- Branch users:
  - Can access DNS + HTTP/HTTPS

    - Cannot access HQ LAN
- Apply closest to the source

Configuration (R2)

```
conf t
ip access-list extended BRANCH_POLICY
 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 log

 permit udp 192.168.2.0 0.0.0.255 any eq 53
 permit tcp 192.168.2.0 0.0.0.255 any eq 53
 permit tcp 192.168.2.0 0.0.0.255 any eq 80
 permit tcp 192.168.2.0 0.0.0.255 any eq 443
 permit icmp 192.168.2.0 0.0.0.255 any

 deny ip any any log

interface g0/0
 ip access-group BRANCH_POLICY in
end
wr
```

Verification

```
show ip interface g0/0
show access-lists BRANCH_POLICY
```

3.3 (Optional) Outside-In ACL on HQ Router

Allow Internet access only to the public web server (after NAT).

```
conf t
ip access-list extended OUTSIDE_IN
 permit tcp any host 203.0.113.20 eq 80
 permit tcp any host 203.0.113.20 eq 443
 deny ip any 192.168.1.0 0.0.0.255 log
 deny ip any 192.168.2.0 0.0.0.255 log
 permit ip any any

interface g0/1
 ip access-group OUTSIDE_IN in
end
wr
```

Part 3 — Questions

1. Why is a standard ACL sufficient for VTY protection?
2. Why should extended ACLs be placed closest to the source?
3. What happens if the implicit `deny any` is not considered?
4. Why is ICMP sometimes allowed even in restrictive ACLs?
5. What is the difference between applying an ACL to:
    - an interface
    - VTY lines
6. How does ACL logging help during troubleshooting?
7. What security risks exist if outside-in ACLs are not configured?

PART 4 — Network Address Translation (NAT)

- Configure PAT (NAT overload) for Internet access
- Configure Static NAT for a public server
- Observe and interpret the NAT translation table
- Distinguish between inside and outside NAT roles

4.1 Define NAT Inside and Outside Interfaces (HQ Router)

NAT must know:

- which interfaces face private networks (inside)
- which interface faces the public Internet (outside)

Incorrect designation = NAT will not work.

Assumptions (HQ Router)

- `G0/0` → HQ LAN (`192.168.1.0/24`)
- `S0/0/0` → Branch side
- `G0/2` → DMZ (`172.16.1.0/24`)
- `G0/1` → ISP / Internet

Configuration (R1)

```
conf t
interface g0/0
 ip nat inside
exit

interface s0/0/0
 ip nat inside
exit

interface g0/2
 ip nat inside
exit

interface g0/1
```

```
 ip nat outside
exit
end
wr
```

- Inside interfaces contain private IP addresses
- Outside interface connects to ISP
- NAT translations occur from inside → outside

4.2 PAT (NAT Overload) — Internet Access for Users

Allow multiple internal hosts to share one public IP address.

PAT uses:

- source IP
- source port

to uniquely identify sessions.

Configuration (R1)

```
conf t
ip access-list standard NAT_INSIDE
 permit 192.168.1.0 0.0.0.255
 permit 192.168.2.0 0.0.0.255

ip nat inside source list NAT_INSIDE interface g0/1 overload
end
wr
```

- Standard ACL identifies which internal addresses are translated
- `overload` enables port translation
- This is the most common NAT type in real networks

4.3 Static NAT — Public Access to DMZ Web Server

Expose an internal server to the Internet using a fixed public IP.

Assumptions

- DMZ web server: `172.16.1.20`
- Public IP: `203.0.113.20`

Configuration (R1)

```
conf t
ip nat inside source static 172.16.1.20 203.0.113.20
```

```
end
wr
```

- One-to-one address mapping
- Required for servers that must be reachable from outside
- Often combined with ACLs for security

4.4 NAT Verification and Troubleshooting

Verification Commands

```
show ip nat translations
show ip nat statistics
```

Clear NAT Table (for testing)

```
clear ip nat translation *
```

Look for:

- Inside local ↔ inside global addresses
- Port numbers (PAT)
- Active translation counters

Part 4 — QUESTIONS

1. Why is NAT required in IPv4 networks?
2. What is the difference between inside local and inside global addresses?
3. Why is PAT more scalable than static NAT?
4. What happens if the NAT table becomes full?
5. Why is a standard ACL sufficient for defining NAT sources?
6. Can NAT be considered a security mechanism? Why or why not?
7. Why is static NAT typically combined with ACLs or firewalls?

PART 5 — WAN Technologies and VPNs

- Configure a PPP WAN link between HQ and Branch
- Secure the WAN using CHAP authentication
- Understand WAN encapsulation and authentication
- Configure a Site-to-Site IPSec VPN
- (Optional) Configure Remote-Access VPN concepts

5.1 WAN Link Configuration — PPP with CHAP

PPP provides:

- Encapsulation
- Authentication
- Link monitoring

CHAP ensures credentials are not sent in clear text.

Configuration — HQ Router (R1)

```
conf t
username R2 secret ChapSecret!

interface s0/0/0
 ip address 10.0.0.1 255.255.255.0
 encapsulation ppp
 ppp authentication chap
 no shutdown
exit
end
wr
```

Configuration — Branch Router (R2)

```
conf t
username R1 secret ChapSecret!

interface s0/0/0
 ip address 10.0.0.2 255.255.255.0
 encapsulation ppp
 ppp authentication chap
 no shutdown
exit
end
wr
```

- CHAP uses challenge–response
- Passwords are never transmitted
- Usernames must match the remote router hostname

Verification

```
show interfaces s0/0/0
show ppp all
```

5.2 Site-to-Site IPSec VPN (HQ ↔ Branch)

Secure traffic between HQ and Branch over an untrusted network.

VPN ensures:

- Confidentiality
- Integrity
- Authentication

5.2.1 Define Interesting Traffic

Configuration (R1)

```
ip access-list extended VPN-TRAFFIC
 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

- Defines which traffic should be encrypted
- Must match exactly on both ends

5.2.2 IKE Phase 1 (ISAKMP)

Configuration (R1)

```
crypto isakmp policy 10
 encr aes
 hash sha
 authentication pre-share
 group 2
 lifetime 86400

crypto isakmp key IpsecPSK! address <R2-public-IP>
```

- Establishes a secure control channel
- Negotiates encryption and authentication parameters

5.2.3 IKE Phase 2 (IPSec)

```
crypto ipsec transform-set TS esp-aes esp-sha-hmac
 mode tunnel
```

5.2.4 Crypto Map and Interface Binding

```
crypto map CMAP 10 ipsec-isakmp
 set peer <R2-public-IP>
 set transform-set TS
```

```
 match address VPN-TRAFFIC

interface g0/1
 crypto map CMAP
```

- Crypto map ties together:
  - peer
  - traffic
  - encryption
- Must be applied to the outside interface

5.2.5 Verification

```
show crypto isakmp sa
show crypto ipsec sa
```

Generate traffic:

- Ping from `192.168.1.x` to `192.168.2.x`

Part 5 — QUESTIONS

1. Why is PPP preferred over HDLC in enterprise WANs?
2. What security advantage does CHAP have over PAP?
3. Why must CHAP usernames match remote router hostnames?
4. What is the purpose of “interesting traffic” in IPSec?
5. Difference between IKE Phase 1 and Phase 2?
6. Why must crypto maps be applied to an interface?
7. What happens if IPSec ACLs do not match on both sides?
8. Difference between Site-to-Site and Remote-Access VPNs?
9. Can VPN replace NAT? Why or why not?