BSc (Hons) Ethical Hacking and Network Security

COBSCEHNS24.1P

Report on Portfolio - Network Implementation

Coursework

Student Name: P. D. S. D. JAYATHILAKE

Coventry Index Number: 15386478

NIBM Index Number: COBSCEHNS24.1P-006

Faculty of Engineering, Environment and Computing

School of Computing, Electronics and Mathematics

Coventry University, London.

School of Computing

National Institute of Business Management

Colombo 07.

March 2025

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

PART 1: Network Implementation for Sport & Leisure Plc

1.1   Introduction

SPORT & LEISURE PLC is an apparel export company that operates from a head office and two branch offices. The head office provides backhauling internet access through a single ISP, while secure IPsec tunnels over an MPLS link connect the branches to the head office. The **headquarters, with an IP range of 192.168.10.0/24**, connects to **Branch 01 (192.168.20.0/24)** and **Branch 02 (192.168.30.0/24)** through secure IPsec tunnels over an MPLS link. This setup ensures that all internet traffic from the branches flows through the main router at the head office, allowing for incorporated control and monitoring. The head office hosts critical services such as ERP, VOICE, and VIDEO, which need priority handling through Quality of Service (QoS) policies. In addition, the company aims to maintain reliability and scalability by incorporating redundancy measures and designing the network so it can accommodate future growth. The main objectives of this network implementation are to guarantee secure connectivity between all sites, provide centralized backhauling management for internet access, prioritize critical traffic for optimal performance, and ensure the network can adapt as the company expands.

1.2   Network Architecture & Design

1.2.1 Network Topology
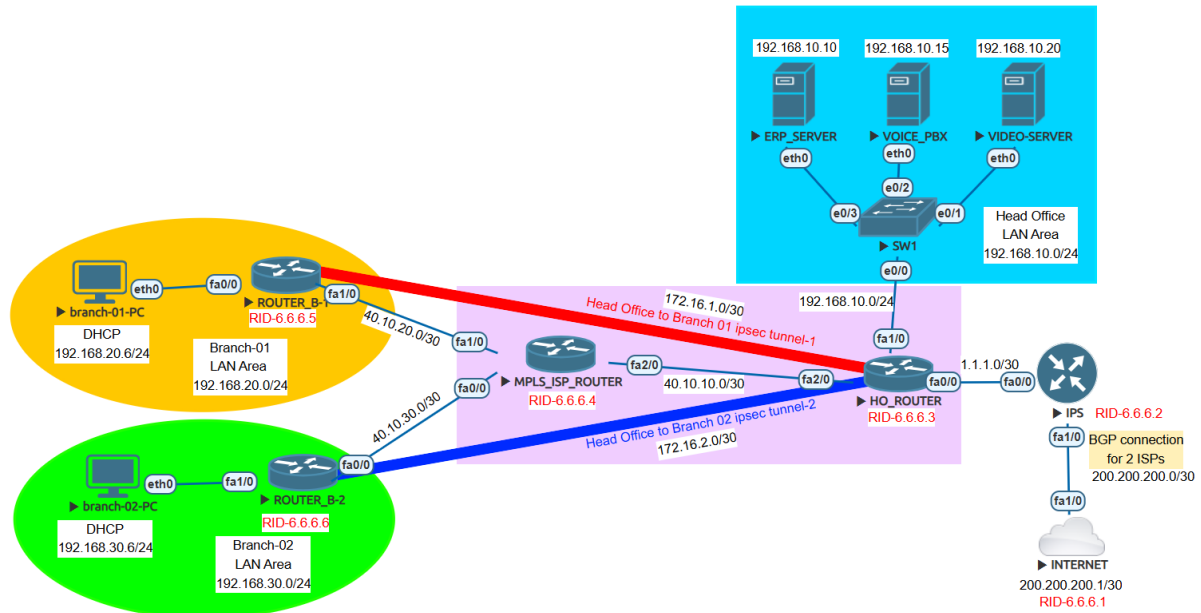
Figure 1:Network Topology

The network topology contains various networking devices, including routers, switches, servers, and end-user devices. These devices are interconnected to ensure seamless communication and efficient data flow across the network.

❖ **Routers**

The network includes multiple routers to facilitate connectivity and route between different locations. The routers used in the topology are:

- INTERNET Router
- ISP Router
- HEAD OFFICE Router
- MPLS ISP Router
- BRANCH-01 Router
- BRANCH-02 Router

❖ **Switches**

A Main Switch is used to handle Layer 2 switching and interconnect different network segments efficiently.

❖ **Servers**

Various servers are implemented in the topology to support enterprise operations. The servers included are in the Head Office:

- ERP Server (Enterprise Resource Planning)
- VOICE PBX Server (Voice over IP Communication)
- VIDEO Conferencing Server (Video communication services)

❖ **End Devices**

End-user devices such as PCs are used for accessing network resources. The devices include:

- BRANCH-01 PC
- BRANCH-02 PC

❖ **Tunnels**

To establish secure communication between different sites, the topology includes:

- Tunnel-01 for Head Office to Branch 01
- Tunnel-02 for Head Office to Branch 02

❖ **Device Versions I Used in EVE-NG**
- **Router Version**

The routers are configured using Cisco IOS 7200 (C7200-ADVENTERPRISEK9-M) with Version 15.3(3) XB12.

- **Switch Version**

The switch is configured using Cisco IOS Solaris (I86BI_LINUXL2-ADVENTERPRISEK9-M) with Version 15.1 (Experimental).

- **PC & Server Version**

The PCs and servers are simulated using Virtual PC Simulator (VPCS) – Version 1.3 (0.8.1).

1.2.2 IP Addressing Scheme

No.	Device Name	Network Address / Subnetmask	Assign Interface	IP Address
01	INTERNET Router	200.200.200.0/30	Fa 1/0	200.200.200.1
02	ISP Router	1.1.1.0/30	Fa 0/0	1.1.1.1
		200.200.200.0/30	Fa 1/0	200.200.200.2
03	HEAD OFFICE Router	1.1.1.0/30	Fa 0/0	1.1.1.2
		192.168.10.0/24	Fa 1/0	192.168.10.1
		40.10.10.0/30	Fa 2/0	40.10.10.1
04	MPLS ISP Router	40.10.30.0/30	Fa 0/0	40.10.30.1
		40.10.20.0/30	Fa 1/0	40.10.20.1
		40.10.10.0/30	Fa 2/0	40.10.10.2
05	Branch-01 Router	192.168.20.0/24	Fa 0/0	192.168.20.1
		40.10.20.0/30	Fa 1/0	40.10.20.2
06	Branch-02 Router	40.10.30.0/30	Fa 0/0	40.10.30.2
		192.168.30.0/24	Fa 1/0	192.168.30.1
07	Head Office Switch	192.168.10.0/24	e 0/0	
			e 0/1	
			e 0/2	
			e 0/3	
08	ERP server	192.168.10.0/24	eth0	192.168.10.10
09	VOICE PBX server	192.168.10.0/24	eth0	192.168.10.15
10	VIDEO Conferencing server	192.168.10.0/24	eth0	192.168.10.20
11	Branch-01 PC	192.168.20.0/24	eth0	DHCP
12	Branch-02 PC	192.168.30.0/24	eth0	DHCP
13	Tunnel-01	172.16.1.0/30	Fa 1/0	172.16.1.2
			Fa 2/0	172.16.1.1
14	Tunnel-02	172.16.2.0/30	Fa 0/0	172.16.2.2
			Fa 2/0	172.16.2.1

Table 1:IP Addressing Scheme

1.2.3 Routing Strategy in the Network Topology

The network uses a combination of BGP and OSPF routing protocols to ensure efficient communication between different segments.

- INTERNET to ISP Network (200.200.200.0/30) – Routed using BGP for external connectivity.

- ISP to HEAD OFFICE Router (1.1.1.0/30) – Routed using OSPF for dynamic internal routing.

- HEAD OFFICE Router to MPLS ISP Router (40.10.10.0/30) – Uses OSPF for internal connectivity.

- MPLS ISP Router to BRANCH-01 Router (40.10.20.0/30) – Uses OSPF for branch connectivity.

- MPLS ISP Router to BRANCH-02 Router (40.10.30.0/30) – Uses OSPF for branch connectivity.

This strategy ensures seamless routing across different network segments while maintaining scalability and efficiency.

1.3   Implementation & Simulation

1.3.1 Software Used for implementation

- EVE-NG

```
root@eve-ng:~#
root@eve-ng:~# dpkg -l eve-ng
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name           Version      Architecture Description
+++-==============-============-============-=================================================
ii  eve-ng         6.2.0-4      amd64        A new generation software for networking labs.
root@eve-ng:~# 
```

Figure 2:EVE-NG version

- Cisco Packet Tracer
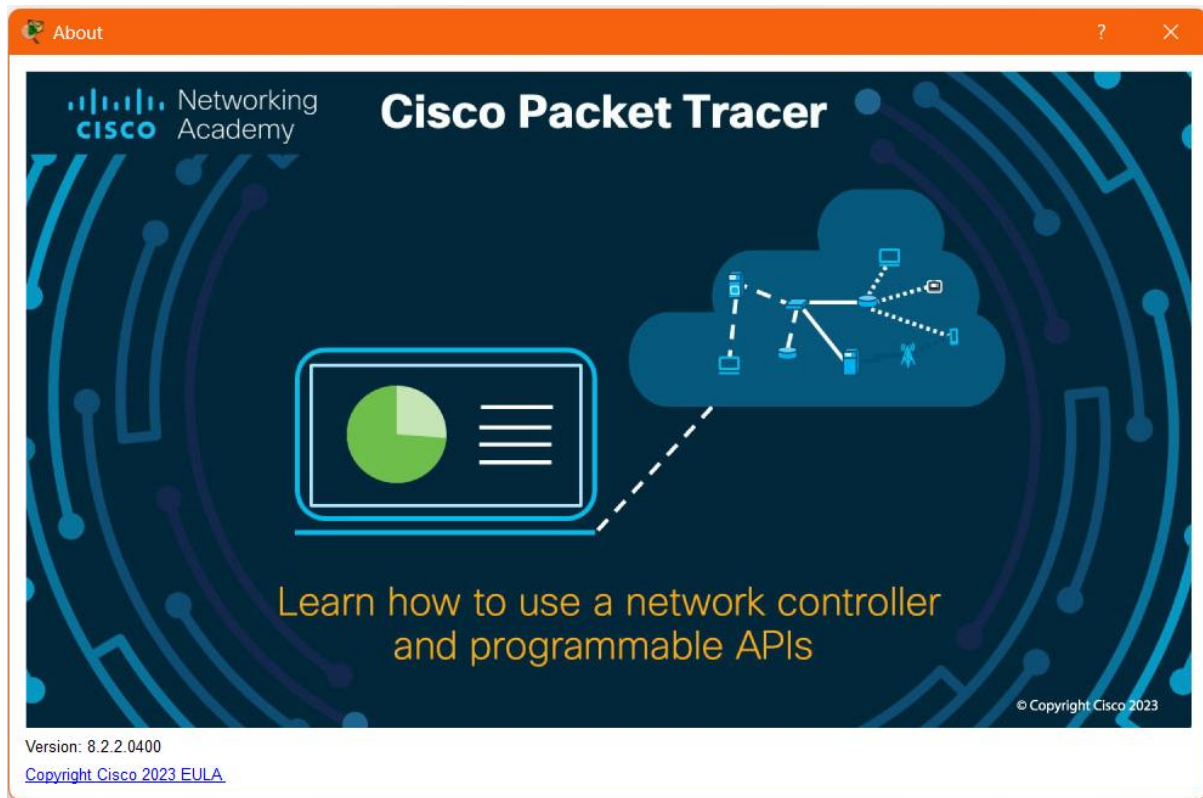
Figure 3:cisco packet tracer version

1.3.2 Configurations and Verifications

1.3.2.1   INTERNET Router Configurations

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname INTERNET
INTERNET(config)#banner motd #Unauthorized access prohibited...!#
INTERNET(config)#no ip domain lookup
INTERNET(config)#security passwords min-length 9
INTERNET(config)#enable secret cisco@123
INTERNET(config)#service password-encryption
INTERNET(config)#ip ssh version 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
INTERNET(config)#ip domain name slPLC.lk
INTERNET(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: INTERNET.slPLC.lk

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 6 seconds)

INTERNET(config)#login block-for 100 attempts 3 within 100
INTERNET(config)#username admin password cisco@123
INTERNET(config)#line console 0
INTERNET(config-line)#login local
INTERNET(config-line)#exec-timeout 10 0
INTERNET(config-line)#exit
INTERNET(config)#line vty 0 15
INTERNET(config-line)#login local
INTERNET(config-line)#exec-timeout 10 0
INTERNET(config-line)#exit
INTERNET(config)#
*Mar 27 04:04:10.403: %SSH-5-ENABLED: SSH 2.0 has been enabled
INTERNET(config)#
```

Figure 4: Internet Router Basic Access Control Configuration

```
INTERNET(config)#
INTERNET(config)#
INTERNET(config)#interface fastEthernet 1/0
INTERNET(config-if)#ip address 200.200.200.1 255.255.255.252
INTERNET(config-if)#no shutdown
INTERNET(config-if)#exit
INTERNET(config)#
*Mar 27 04:05:04.939: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Mar 27 04:05:05.939: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
INTERNET(config)#
```

Figure 5:Internet Router Interface Configuration

```
INTERNET(config)#
INTERNET(config)#
INTERNET(config)#router bgp 65002
INTERNET(config-router)#bgp router-id 6.6.6.1
INTERNET(config-router)#bgp log-neighbor-changes
INTERNET(config-router)#neighbor 200.200.200.2 remote-as 65001
INTERNET(config-router)#
*Mar 27 04:05:37.991: %BGP-5-ADJCHANGE: neighbor 200.200.200.2 Up
INTERNET(config-router)#
INTERNET(config-router)#
```

Figure 6:Internet Router Routing Configuration

```
INTERNET#show ip interface brief
Interface              IP-Address      OK? Method Status                 Protocol
FastEthernet0/0        unassigned      YES unset  administratively down  down
FastEthernet1/0        200.200.200.1   YES manual up                     up
FastEthernet2/0        unassigned      YES unset  administratively down  down
FastEthernet3/0        unassigned      YES unset  administratively down  down
INTERNET#
INTERNET#
INTERNET#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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/30 is subnetted, 1 subnets
B        1.1.1.0 [20/0] via 200.200.200.2, 01:14:11
      40.0.0.0/30 is subnetted, 3 subnets
B        40.10.10.0 [20/100] via 200.200.200.2, 01:11:17
B        40.10.20.0 [20/100] via 200.200.200.2, 00:56:59
B        40.10.30.0 [20/100] via 200.200.200.2, 00:56:59
      172.16.0.0/30 is subnetted, 2 subnets
B        172.16.1.0 [20/100] via 200.200.200.2, 00:35:40
B        172.16.2.0 [20/100] via 200.200.200.2, 00:29:50
B     192.168.10.0/24 [20/100] via 200.200.200.2, 01:11:17
B     192.168.20.0/24 [20/100] via 200.200.200.2, 00:37:19
B     192.168.30.0/24 [20/100] via 200.200.200.2, 00:31:49
      200.200.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        200.200.200.0/30 is directly connected, FastEthernet1/0
L        200.200.200.1/32 is directly connected, FastEthernet1/0
INTERNET#
INTERNET#show ip bgp
BGP table version is 14, local router ID is 6.6.6.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop         Metric LocPrf Weight Path
 *>  1.1.1.0/30       200.200.200.2         0             0 65001 ?
 *>  40.10.10.0/30    200.200.200.2       100             0 65001 ?
 *>  40.10.20.0/30    200.200.200.2       100             0 65001 ?
 *>  40.10.30.0/30    200.200.200.2       100             0 65001 ?
 *>  172.16.1.0/30    200.200.200.2       100             0 65001 ?
 *>  172.16.2.0/30    200.200.200.2       100             0 65001 ?
 *>  192.168.10.0     200.200.200.2       100             0 65001 ?
 *>  192.168.20.0     200.200.200.2       100             0 65001 ?
 *>  192.168.30.0     200.200.200.2       100             0 65001 ?
INTERNET#
```

Figure 7:Internet Router Configuration Verifications

1.3.2.2 ISP Router Configurations

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#banner motd #Unauthorized access prohibited...!#
ISP(config)#no ip domain lookup
ISP(config)#security passwords min-length 9
ISP(config)#enable secret cisco@123
ISP(config)#service password-encryption
ISP(config)#ip ssh version 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
ISP(config)#ip domain name slPLC.lk
ISP(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: ISP.slPLC.lk

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 5 seconds)

ISP(config)#login block-for 100 attempts 3 within 100
ISP(config)#username admin password cisco@123
ISP(config)#line console 0
ISP(config-line)#login local
ISP(config-line)#exec-timeout 10 0
ISP(config-line)#exit
ISP(config)#line vty 0 15
ISP(config-line)#login local
ISP(config-line)#exec-timeout 10 0
ISP(config-line)#exit
ISP(config)#
ISP(config)#
*Mar 27 04:01:14.343: %SSH-5-ENABLED: SSH 2.0 has been enabled
ISP(config)#
```

Figure 8:ISP Router Basic Access Control Configuration

```
ISP(config)#
ISP(config)#interface fastEthernet 0/0
ISP(config-if)#ip address 1.1.1.1 255.255.255.252
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#interface fastEthernet 1/0
ISP(config-if)#ip address 200.200.200.2 255.255.255.252
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#
*Mar 27 04:01:52.331: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 27 04:01:52.419: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Mar 27 04:01:53.331: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Mar 27 04:01:53.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
ISP(config)#
```

Figure 9:ISP Router Interface Configuration

```
ISP(config)#
ISP(config)#router ospf 1
ISP(config-router)#router-id 6.6.6.2
ISP(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
ISP(config-router)#network 1.1.1.1 0.0.0.0 area 0
ISP(config-router)#redistribute bgp 65001 subnets
ISP(config-router)#default-information originate
ISP(config-router)#exit
ISP(config)#
ISP(config)#
*Mar 27 04:02:29.887: %OSPF-5-ADJCHG: Process 1, Nbr 6.6.6.3 on FastEthernet0/0 from LOADING to FULL, Loading Done
ISP(config)#
ISP(config)#router bgp 65001
ISP(config-router)#bgp log-neighbor-changes
ISP(config-router)#redistribute ospf 1 metric 100
ISP(config-router)#neighbor 200.200.200.1 remote-as 65002
ISP(config-router)#exit
ISP(config)#
ISP(config)#
*Mar 27 04:05:37.391: %BGP-5-ADJCHANGE: neighbor 200.200.200.1 Up
ISP(config)#
ISP(config)#ip route 0.0.0.0 0.0.0.0 200.200.200.1
ISP(config)#
```

Figure 10:ISP Router Routing Configurations

```
ISP#show ip interface brief
Interface               IP-Address      OK? Method Status                Protocol
FastEthernet0/0         1.1.1.1         YES manual up                    up
FastEthernet1/0         200.200.200.2   YES manual up                    up
FastEthernet2/0         unassigned      YES unset  administratively down down
FastEthernet3/0         unassigned      YES unset  administratively down down
ISP#
ISP#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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 200.200.200.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 200.200.200.1
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/30 is directly connected, FastEthernet0/0
L        1.1.1.1/32 is directly connected, FastEthernet0/0
      40.0.0.0/30 is subnetted, 3 subnets
O        40.10.10.0 [110/20] via 1.1.1.2, 01:16:32, FastEthernet0/0
O        40.10.20.0 [110/30] via 1.1.1.2, 01:02:13, FastEthernet0/0
O        40.10.30.0 [110/30] via 1.1.1.2, 01:02:13, FastEthernet0/0
      172.16.0.0/30 is subnetted, 2 subnets
O        172.16.1.0 [110/10010] via 1.1.1.2, 00:40:55, FastEthernet0/0
O        172.16.2.0 [110/10010] via 1.1.1.2, 00:35:04, FastEthernet0/0
O     192.168.10.0/24 [110/20] via 1.1.1.2, 01:16:32, FastEthernet0/0
O     192.168.20.0/24 [110/40] via 1.1.1.2, 00:42:33, FastEthernet0/0
O     192.168.30.0/24 [110/40] via 1.1.1.2, 00:37:03, FastEthernet0/0
      200.200.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        200.200.200.0/30 is directly connected, FastEthernet1/0
L        200.200.200.2/32 is directly connected, FastEthernet1/0
ISP#
ISP#show ip ospf neighbor

Neighbor ID     Pri   State      Dead Time   Address       Interface
6.6.6.3           1   FULL/BDR   00:00:33    1.1.1.2       FastEthernet0/0
ISP#
ISP#show ip bgp
BGP table version is 14, local router ID is 200.200.200.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  1.1.1.0/30       0.0.0.0                  0          32768 ?
 *>  40.10.10.0/30    1.1.1.2                100         32768 ?
 *>  40.10.20.0/30    1.1.1.2                100         32768 ?
 *>  40.10.30.0/30    1.1.1.2                100         32768 ?
 *>  172.16.1.0/30    1.1.1.2                100         32768 ?
 *>  172.16.2.0/30    1.1.1.2                100         32768 ?
 *>  192.168.10.0     1.1.1.2                100         32768 ?
 *>  192.168.20.0     1.1.1.2                100         32768 ?
 *>  192.168.30.0     1.1.1.2                100         32768 ?
ISP#
ISP#
```

Figure 11:ISP Router Configuration Verifications

1.3.2.3   HEAD OFFICE Router Configurations

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname HO_ROUTER
HO_ROUTER(config)#banner motd #Unauthorized access prohibited...!#
HO_ROUTER(config)#no ip domain lookup
HO_ROUTER(config)#security passwords min-length 9
HO_ROUTER(config)#enable secret cisco@123
HO_ROUTER(config)#service password-encryption
HO_ROUTER(config)#ip ssh version 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
HO_ROUTER(config)#ip domain name slPLC.lk
HO_ROUTER(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: HO_ROUTER.slPLC.lk

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 4 seconds)

HO_ROUTER(config)#login block-for 100 attempts 3 within 100
HO_ROUTER(config)#username admin password cisco@123
HO_ROUTER(config)#line console 0
HO_ROUTER(config-line)#login local
HO_ROUTER(config-line)#exec-timeout 10 0
HO_ROUTER(config-line)#exit
HO_ROUTER(config)#line vty 0 15
HO_ROUTER(config-line)#login local
HO_ROUTER(config-line)#exec-timeout 10 0
HO_ROUTER(config-line)#exit
HO_ROUTER(config)#
*Mar 27 03:37:18.727: %SSH-5-ENABLED: SSH 2.0 has been enabled
HO_ROUTER(config)#
```

Figure 12:Head Office Router Basic Access Control Configuration

```
HO_ROUTER(config)#
HO_ROUTER(config)#interface fastEthernet 0/0
HO_ROUTER(config-if)#ip address 1.1.1.2 255.255.255.252
HO_ROUTER(config-if)#no shutdown
HO_ROUTER(config-if)#exit
HO_ROUTER(config)#interface fastEthernet 1/0
HO_ROUTER(config-if)#ip address 192.168.10.1 255.255.255.0
HO_ROUTER(config-if)#no shutdown
HO_ROUTER(config-if)#exit
HO_ROUTER(config)#interface fastEthernet 2/0
HO_ROUTER(config-if)#ip address 40.10.10.1 255.255.255.252
HO_ROUTER(config-if)#no shutdown
HO_ROUTER(config-if)#exit
HO_ROUTER(config)#
*Mar 27 03:38:05.447: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 27 03:38:05.579: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Mar 27 03:38:05.711: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to up
*Mar 27 03:38:06.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Mar 27 03:38:06.579: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
*Mar 27 03:38:06.711: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to up
HO_ROUTER(config)#
```

Figure 13:Head Office Router Interface Configuration

```
HO_ROUTER(config)#router ospf 1
HO_ROUTER(config-router)#router-id 6.6.6.3
HO_ROUTER(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
HO_ROUTER(config-router)#network 1.1.1.0 0.0.0.3 area 0
HO_ROUTER(config-router)#network 40.10.10.0 0.0.0.3 area 0
HO_ROUTER(config-router)#network 192.168.10.0 0.0.0.255 area 0
HO_ROUTER(config-router)#exit
HO_ROUTER(config)#
*Mar 27 04:30:54.107: %OSPF-5-ADJCHG: Process 1, Nbr 6.6.6.2 on FastEthernet0/0 from LOADING to FULL, Loading Done
*Mar 27 04:30:54.739: %OSPF-5-ADJCHG: Process 1, Nbr 6.6.6.4 on FastEthernet2/0 from LOADING to FULL, Loading Done
HO_ROUTER(config)#
HO_ROUTER(config)#
```

Figure 14:Head Office Router Routing Configuration

```
HO_ROUTER(config)#
HO_ROUTER(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.25
HO_ROUTER(config)#ip dhcp pool HO_DHCP
HO_ROUTER(dhcp-config)#network 192.168.10.0 255.255.255.0
HO_ROUTER(dhcp-config)#default-router 192.168.10.1
HO_ROUTER(dhcp-config)#dns-server 8.8.8.8
HO_ROUTER(dhcp-config)#exit
HO_ROUTER(config)#
```

Figure 15:Head Office Router DHCP Configurations

```
HO_ROUTER#show ip interface brief
Interface                 IP-Address      OK? Method Status                 Protocol
FastEthernet0/0           1.1.1.2         YES manual up                     up
FastEthernet1/0           192.168.10.1    YES manual up                     up
FastEthernet2/0           40.10.10.1      YES manual up                     up
FastEthernet3/0           unassigned      YES unset  administratively down  down
NVI0                      1.1.1.2         YES unset  up                     up
Tunnel1                   172.16.1.1      YES manual up                     up
Tunnel2                   172.16.2.1      YES manual up                     up
HO_ROUTER#
HO_ROUTER#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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 1.1.1.1 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 1.1.1.1, 01:22:08, FastEthernet0/0
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/30 is directly connected, FastEthernet0/0
L        1.1.1.2/32 is directly connected, FastEthernet0/0
      40.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        40.10.10.0/30 is directly connected, FastEthernet2/0
L        40.10.10.1/32 is directly connected, FastEthernet2/0
O        40.10.20.0/30 [110/20] via 40.10.10.2, 01:07:51, FastEthernet2/0
O        40.10.30.0/30 [110/20] via 40.10.10.2, 01:07:51, FastEthernet2/0
      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.16.1.0/30 is directly connected, Tunnel1
L        172.16.1.1/32 is directly connected, Tunnel1
C        172.16.2.0/30 is directly connected, Tunnel2
L        172.16.2.1/32 is directly connected, Tunnel2
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, FastEthernet1/0
L        192.168.10.1/32 is directly connected, FastEthernet1/0
O     192.168.20.0/24 [110/30] via 40.10.10.2, 00:48:11, FastEthernet2/0
O     192.168.30.0/24 [110/30] via 40.10.10.2, 00:42:41, FastEthernet2/0
HO_ROUTER#
HO_ROUTER#show ip ospf neighbor

Neighbor ID     Pri   State         Dead Time   Address         Interface
6.6.6.6           0   FULL/  -      00:00:37    172.16.2.2      Tunnel2
6.6.6.5           0   FULL/  -      00:00:33    172.16.1.2      Tunnel1
6.6.6.4           1   FULL/BDR      00:00:35    40.10.10.2      FastEthernet2/0
6.6.6.2           1   FULL/DR       00:00:33    1.1.1.1         FastEthernet0/0
HO_ROUTER#
HO_ROUTER#
```

Figure 16:Head Office Router Configuration Verifications

```
HO_ROUTER(config)#
HO_ROUTER(config)#access-list 10 permit 192.168.10.0 0.0.0.255
HO_ROUTER(config)#access-list 10 permit 192.168.20.0 0.0.0.255
HO_ROUTER(config)#access-list 10 permit 192.168.30.0 0.0.0.255
HO_ROUTER(config)#ip nat inside source list 10 interface FastEthernet0/0 overl$
HO_ROUTER(config)#
*Mar 27 03:47:45.903: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
HO_ROUTER(config)#
HO_ROUTER(config)#interface FastEthernet0/0
HO_ROUTER(config-if)#ip nat outside
HO_ROUTER(config-if)#exit
HO_ROUTER(config)#interface FastEthernet1/0
HO_ROUTER(config-if)#ip nat inside
HO_ROUTER(config-if)#exit
HO_ROUTER(config)#interface FastEthernet2/0
HO_ROUTER(config-if)#ip nat inside
HO_ROUTER(config-if)#exit
HO_ROUTER(config)#
```

Figure 17:Head Office Router NAT(PAT) Configuration

```
HO_ROUTER#
HO_ROUTER#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 1.1.1.2:23613     192.168.10.15:23613 200.200.200.1:23613 200.200.200.1:23613
icmp 1.1.1.2:23869     192.168.10.15:23869 200.200.200.1:23869 200.200.200.1:23869
icmp 1.1.1.2:24125     192.168.10.15:24125 200.200.200.1:24125 200.200.200.1:24125
icmp 1.1.1.2:21309     192.168.20.6:21309 200.200.200.1:21309 200.200.200.1:21309
icmp 1.1.1.2:21821     192.168.20.6:21821 200.200.200.1:21821 200.200.200.1:21821
icmp 1.1.1.2:22077     192.168.20.6:22077 200.200.200.1:22077 200.200.200.1:22077
icmp 1.1.1.2:22589     192.168.30.6:22589 200.200.200.1:22589 200.200.200.1:22589
icmp 1.1.1.2:22845     192.168.30.6:22845 200.200.200.1:22845 200.200.200.1:22845
icmp 1.1.1.2:23101     192.168.30.6:23101 200.200.200.1:23101 200.200.200.1:23101
HO_ROUTER#
```

Figure 18:Head Office Router NAT(PAT) Configuration Verifications

```
HO_ROUTER(config)#
HO_ROUTER(config)#ip access-list extended ERP-QOS-CLSMP
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.10 192.168.20.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.10 192.168.30.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#exit
HO_ROUTER(config)#ip access-list extended VOICE-VIDEO-QOS-CLSMP
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.15 192.168.20.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.15 192.168.30.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.20 192.168.20.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.20 192.168.30.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#exit
HO_ROUTER(config)#class-map match-any ERP-TRAFFIC
HO_ROUTER(config-cmap)#match access-group name ERP-QOS-CLSMP
HO_ROUTER(config-cmap)#exit
HO_ROUTER(config)#
HO_ROUTER(config)#class-map match-any VOICE-VIDEO-TRAFFIC
HO_ROUTER(config-cmap)#match access-group name VOICE-VIDEO-QOS-CLSMP
HO_ROUTER(config-cmap)#match protocol rtp
HO_ROUTER(config-cmap)#match protocol rtcp
HO_ROUTER(config-cmap)#match protocol sip
HO_ROUTER(config-cmap)#exit
HO_ROUTER(config)#policy-map HO-OUTBOUND-QOS
HO_ROUTER(config-pmap)#class ERP-TRAFFIC
HO_ROUTER(config-pmap-c)#priority percent 40
HO_ROUTER(config-pmap-c)#set dscp af31
HO_ROUTER(config-pmap-c)#
HO_ROUTER(config-pmap-c)#class VOICE-VIDEO-TRAFFIC
HO_ROUTER(config-pmap-c)#priority percent 30
HO_ROUTER(config-pmap-c)#set dscp ef
HO_ROUTER(config-pmap-c)#
HO_ROUTER(config-pmap-c)#class class-default
HO_ROUTER(config-pmap-c)#fair-queue
HO_ROUTER(config-pmap-c)#exit
HO_ROUTER(config-pmap)#exit
HO_ROUTER(config)#interface fastEthernet 1/0
HO_ROUTER(config-if)#ip policy route-map SELECTIVE_TUNNEL
HO_ROUTER(config-if)#exit
HO_ROUTER(config)#interface fastEthernet 2/0
HO_ROUTER(config-if)#service-policy output HO-OUTBOUND-QOS
HO_ROUTER(config-if)#exit
HO_ROUTER(config)#_
```

Figure 19:Head Office Router QOS Configuration

```
HO_ROUTER#show policy-map interface fastEthernet 2/0
 FastEthernet2/0

  Service-policy output: HO-OUTBOUND-QOS

    queue stats for all priority classes:
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 172/35972

    Class-map: ERP-TRAFFIC (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name ERP-QOS-CLSMP
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 40% (40000 kbps), burst bytes 1000000, b/w exceed drops: 0

      QoS Set
        dscp af31
          Packets marked 0

    Class-map: VOICE-VIDEO-TRAFFIC (match-any)
      172 packets, 28748 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name VOICE-VIDEO-QOS-CLSMP
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol rtp
        172 packets, 28748 bytes
        5 minute rate 0 bps
      Match: protocol rtcp
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol sip
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (30000 kbps), burst bytes 750000, b/w exceed drops: 0

      QoS Set
        dscp ef
          Packets marked 172

    Class-map: class-default (match-any)
      2164 packets, 317126 bytes
      5 minute offered rate 4000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops/flowdrops) 0/0/0/0
      (pkts output/bytes output) 2163/324638
      Fair-queue: per-flow queue limit 16 packets
HO_ROUTER#
```

Figure 20:Head Office Router QOS Configuration Verifications

```
HO_ROUTER(config)#interface Tunnel 1
HO_ROUTER(config-if)#ip address 172.16.1.1 255.255.255.252
HO_ROUTER(config-if)#tunnel source FastEthernet2/0
HO_ROUTER(config-if)#tunnel destination 40.10.20.2
HO_ROUTER(config-if)#tunnel mode ipsec ipv4
HO_ROUTER(config-if)#tunnel protection ipsec profile MYPROFILE
HO_ROUTER(config-if)#qos pre-classify
HO_ROUTER(config-if)#exit
HO_ROUTER(config)#
*Mar 28 05:15:17.971: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
*Mar 28 05:15:18.019: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
HO_ROUTER(config)#interface Tunnel 2
HO_ROUTER(config-if)#ip address 172.16.2.1 255.255.255.252
HO_ROUTER(config-if)#tunnel source FastEthernet2/0
HO_ROUTER(config-if)#tunnel destination 40.10.30.2
HO_ROUTER(config-if)#tunnel mode ipsec ipv4
HO_ROUTER(config-if)#tunnel protection ipsec profile MYPROFILE
HO_ROUTER(config-if)#qos pre-classify
HO_ROUTER(config-if)#exit
HO_ROUTER(config)#
*Mar 28 05:15:26.203: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state to down
HO_ROUTER(config)#ip access-list extended TO_BRANCH01
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.10 192.168.20.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.15 192.168.20.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.20 192.168.20.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#exit
HO_ROUTER(config)#ip access-list extended TO_BRANCH02
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.10 192.168.30.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.15 192.168.30.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.20 192.168.30.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#exit
HO_ROUTER(config)#route-map SELECTIVE_TUNNEL permit 10
HO_ROUTER(config-route-map)#match ip address TO_BRANCH01
HO_ROUTER(config-route-map)#set interface Tunnel1
HO_ROUTER(config-route-map)#exit
HO_ROUTER(config)#route-map SELECTIVE_TUNNEL permit 20
HO_ROUTER(config-route-map)#match ip address TO_BRANCH02
HO_ROUTER(config-route-map)#set interface Tunnel2
HO_ROUTER(config-route-map)#exit
HO_ROUTER(config)#
```

Figure 21:Head Office Router GRE tunnels Configuration

```
HO_ROUTER(config)#router ospf 1
HO_ROUTER(config-router)#network 172.16.1.1 0.0.0.0 area 0
HO_ROUTER(config-router)#network 172.16.2.1 0.0.0.0 area 0
HO_ROUTER(config-router)#exit
HO_ROUTER(config)#exit
HO_ROUTER#write
Building configuration...
[OK]
HO_ROUTER#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

*Mar 28 05:18:29.855: %SYS-5-CONFIG_I: Configured from console by console[OK]
HO_ROUTER#
HO_ROUTER#
```

Figure 22:Head Office Router GRE tunnels Routing Configuration

```
HO_ROUTER(config)#
HO_ROUTER(config)#crypto isakmp policy 10
HO_ROUTER(config-isakmp)# encr aes
HO_ROUTER(config-isakmp)# hash sha
HO_ROUTER(config-isakmp)# authentication pre-share
HO_ROUTER(config-isakmp)# group 2
HO_ROUTER(config-isakmp)#exit
HO_ROUTER(config)#crypto isakmp key mysecretkey address 40.10.20.2
HO_ROUTER(config)#crypto isakmp key mysecretkey address 40.10.30.2
HO_ROUTER(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
HO_ROUTER(cfg-crypto-trans)#crypto ipsec profile MYPROFILE
HO_ROUTER(ipsec-profile)# set transform-set MYSET
HO_ROUTER(ipsec-profile)#exit
HO_ROUTER(config)#
HO_ROUTER(config)#
```

Figure 23::Head Office Router IPSec Configuration

```
HO_ROUTER#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state           conn-id status
40.10.30.2      40.10.10.1      QM_IDLE             1004 ACTIVE
40.10.10.1      40.10.20.2      QM_IDLE             1001 ACTIVE
40.10.20.2      40.10.10.1      QM_IDLE             1002 ACTIVE
40.10.10.1      40.10.30.2      QM_IDLE             1003 ACTIVE

IPv6 Crypto ISAKMP SA

HO_ROUTER#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
HO_ROUTER#
HO_ROUTER#
```

Figure 24: Head Office Router (IKE-phase-01) Security Associations (SA) Configuration Verifications

```
HO_ROUTER#show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 40.10.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 40.10.20.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1532, #pkts encrypt: 1532, #pkts digest: 1532
    #pkts decaps: 1544, #pkts decrypt: 1544, #pkts verify: 1544
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 40.10.10.1, remote crypto endpt.: 40.10.20.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet2/0
     current outbound spi: 0xCF52C61E(3478308382)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xA2D1A6FD(2731648765)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 11, flow_id: SW:11, sibling_flags 80004040, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4344596/3256)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xCF52C61E(3478308382)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 12, flow_id: SW:12, sibling_flags 80004040, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4344596/3256)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Figure 25: Head Office Router (IKE-phase-02) Security Associations (SA) tunnel-01 Configuration Verifications

```
interface: Tunnel2
    Crypto map tag: Tunnel2-head-0, local addr 40.10.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 40.10.30.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 922, #pkts encrypt: 922, #pkts digest: 922
    #pkts decaps: 925, #pkts decrypt: 925, #pkts verify: 925
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 40.10.10.1, remote crypto endpt.: 40.10.30.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet2/0
     current outbound spi: 0x9E9B0E9B(2660961947)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x37DEAEB3(937340595)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 5, flow_id: SW:5, sibling_flags 80000040, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/189)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0xC5E6024A(3320185418)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 7, flow_id: SW:7, sibling_flags 80004040, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/190)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0x67484032(1732788274)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 9, flow_id: SW:9, sibling_flags 80004040, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4319598/190)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x446748D7(1147619543)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 6, flow_id: SW:6, sibling_flags 80000040, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/189)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0x6CC2BDBB(1824701883)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 8, flow_id: SW:8, sibling_flags 80004040, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4608000/190)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0x9E9B0E9B(2660961947)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 10, flow_id: SW:10, sibling_flags 80004040, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4319598/190)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
HO_ROUTER#
```

Figure 26: Head Office Router (IKE-phase-02) Security Associations (SA) tunnel-02 Configuration Verifications

1.3.2.4   MPLS ISP Router Configurations

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname MPLS_ISP_R
MPLS_ISP_R(config)#banner motd #Unauthorized access prohibited...!#
MPLS_ISP_R(config)#no ip domain lookup
MPLS_ISP_R(config)#security passwords min-length 9
MPLS_ISP_R(config)#enable secret cisco@123
MPLS_ISP_R(config)#service password-encryption
MPLS_ISP_R(config)#ip ssh version 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
MPLS_ISP_R(config)#ip domain name slPLC.lk
MPLS_ISP_R(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: MPLS_ISP_R.slPLC.lk

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 6 seconds)

MPLS_ISP_R(config)#login block-for 100 attempts 3 within 100
MPLS_ISP_R(config)#username admin password cisco@123
MPLS_ISP_R(config)#line console 0
MPLS_ISP_R(config-line)#login local
MPLS_ISP_R(config-line)#exec-timeout 10 0
MPLS_ISP_R(config-line)#exit
MPLS_ISP_R(config)#line vty 0 15
MPLS_ISP_R(config-line)#login local
MPLS_ISP_R(config-line)#exec-timeout 10 0
MPLS_ISP_R(config-line)#exit
MPLS_ISP_R(config)#
*Mar 27 03:50:29.771: %SSH-5-ENABLED: SSH 2.0 has been enabled
MPLS_ISP_R(config)#
```

Figure 27:MPLS ISP Router Basic Access Control Configuration

```
MPLS_ISP_R(config)#
MPLS_ISP_R(config)#interface fastEthernet 0/0
MPLS_ISP_R(config-if)#ip address 40.10.30.1 255.255.255.252
MPLS_ISP_R(config-if)#no shutdown
MPLS_ISP_R(config-if)#exit
MPLS_ISP_R(config)#interface fastEthernet 1/0
MPLS_ISP_R(config-if)#ip address 40.10.20.1 255.255.255.252
MPLS_ISP_R(config-if)#no shutdown
MPLS_ISP_R(config-if)#exit
MPLS_ISP_R(config)#interface fastEthernet 2/0
MPLS_ISP_R(config-if)#ip address 40.10.10.2 255.255.255.252
MPLS_ISP_R(config-if)#no shutdown
MPLS_ISP_R(config-if)#exit
MPLS_ISP_R(config)#
MPLS_ISP_R(config)#
MPLS_ISP_R(config)#
*Mar 27 03:51:12.787: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 27 03:51:12.919: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Mar 27 03:51:12.975: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to up
*Mar 27 03:51:13.787: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Mar 27 03:51:13.919: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
*Mar 27 03:51:13.975: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to up
MPLS_ISP_R(config)#
```

Figure 28:MPLS ISP Router Interface Configurations

```
MPLS_ISP_R(config)#
MPLS_ISP_R(config)#router ospf 1
MPLS_ISP_R(config-router)#router-id 6.6.6.4
MPLS_ISP_R(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
MPLS_ISP_R(config-router)#network 40.10.10.0 0.0.0.3 area 0
MPLS_ISP_R(config-router)#network 40.10.20.0 0.0.0.3 area 0
MPLS_ISP_R(config-router)#network 40.10.30.0 0.0.0.3 area 0
MPLS_ISP_R(config-router)#exit
MPLS_ISP_R(config)#
*Mar 27 03:52:02.095: %OSPF-5-ADJCHG: Process 1, Nbr 6.6.6.3 on FastEthernet2/0 from LOADING to FULL, Loading Done
MPLS_ISP_R(config)#
*Mar 27 03:54:55.275: %OSPF-5-ADJCHG: Process 1, Nbr 6.6.6.5 on FastEthernet1/0 from LOADING to FULL, Loading Done
*Mar 27 03:58:45.083: %OSPF-5-ADJCHG: Process 1, Nbr 6.6.6.6 on FastEthernet0/0 from LOADING to FULL, Loading Done
```

Figure 29:MPLS ISP Router Routing Configurations

```
MPLS_ISP_R#
MPLS_ISP_R#show ip interface brief
Interface              IP-Address      OK? Method Status                 Protocol
FastEthernet0/0        40.10.30.1      YES manual up                     up
FastEthernet1/0        40.10.20.1      YES manual up                     up
FastEthernet2/0        40.10.10.2      YES manual up                     up
FastEthernet3/0        unassigned      YES unset  administratively down  down
MPLS_ISP_R#
MPLS_ISP_R#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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 40.10.10.1 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 40.10.10.1, 01:12:47, FastEthernet2/0
      1.0.0.0/30 is subnetted, 1 subnets
O        1.1.1.0 [110/20] via 40.10.10.1, 01:12:47, FastEthernet2/0
      40.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        40.10.10.0/30 is directly connected, FastEthernet2/0
L        40.10.10.2/32 is directly connected, FastEthernet2/0
C        40.10.20.0/30 is directly connected, FastEthernet1/0
L        40.10.20.1/32 is directly connected, FastEthernet1/0
C        40.10.30.0/30 is directly connected, FastEthernet0/0
L        40.10.30.1/32 is directly connected, FastEthernet0/0
      172.16.0.0/30 is subnetted, 2 subnets
O        172.16.1.0 [110/10010] via 40.10.20.2, 00:50:53, FastEthernet1/0
                    [110/10010] via 40.10.10.1, 00:51:27, FastEthernet2/0
O        172.16.2.0 [110/10010] via 40.10.30.2, 00:45:27, FastEthernet0/0
                    [110/10010] via 40.10.10.1, 00:45:37, FastEthernet2/0
O     192.168.10.0/24 [110/20] via 40.10.10.1, 01:12:47, FastEthernet2/0
O     192.168.20.0/24 [110/20] via 40.10.20.2, 00:53:16, FastEthernet1/0
O     192.168.30.0/24 [110/20] via 40.10.30.2, 00:47:46, FastEthernet0/0
MPLS_ISP_R#
MPLS_ISP_R#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
6.6.6.6           1   FULL/BDR        00:00:36    40.10.30.2      FastEthernet0/0
6.6.6.5           1   FULL/BDR        00:00:38    40.10.20.2      FastEthernet1/0
6.6.6.3           1   FULL/DR         00:00:35    40.10.10.1      FastEthernet2/0
MPLS_ISP_R#
MPLS_ISP_R#
```

Figure 30:MPLS ISP Router Configuration Verifications

1.3.2.5　　　BRANCH-01 Router Configurations

```
Router>
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Branch_01_R
Branch_01_R(config)#banner motd #Unauthorized access prohibited...!#
Branch_01_R(config)#no ip domain lookup
Branch_01_R(config)#security passwords min-length 9
Branch_01_R(config)#enable secret cisco@123
Branch_01_R(config)#service password-encryption
Branch_01_R(config)#ip ssh version 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
Branch_01_R(config)#ip domain name slPLC.lk
Branch_01_R(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: Branch_01_R.slPLC.lk

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

Branch_01_R(config)#login block-for 100 attempts 3 within 100
Branch_01_R(config)#username admin password cisco@123
Branch_01_R(config)#line console 0
Branch_01_R(config-line)#login local
Branch_01_R(config-line)#exec-timeout 10 0
Branch_01_R(config-line)#exit
Branch_01_R(config)#line vty 0 15
Branch_01_R(config-line)#login local
Branch_01_R(config-line)#exec-timeout 10 0
Branch_01_R(config-line)#exit
Branch_01_R(config)#
Branch_01_R(config)#
*Mar 27 03:53:30.987: %SSH-5-ENABLED: SSH 2.0 has been enabled
Branch_01_R(config)#
```

Figure 31:Branch-01 Router Basic Access Control Configuration

```
Branch_01_R(config)#
Branch_01_R(config)#
Branch_01_R(config)#interface fastEthernet 0/0
Branch_01_R(config-if)#ip address 192.168.20.1 255.255.255.0
Branch_01_R(config-if)#no shutdown
Branch_01_R(config-if)#exit
Branch_01_R(config)#interface fastEthernet 1/0
Branch_01_R(config-if)#ip address 40.10.20.2 255.255.255.252
Branch_01_R(config-if)#no shutdown
Branch_01_R(config-if)#exit
Branch_01_R(config)#
Branch_01_R(config)#
*Mar 27 03:54:14.015: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 27 03:54:14.103: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Mar 27 03:54:15.015: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Mar 27 03:54:15.103: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
Branch_01_R(config)#
```

Figure 32:Branch-01 Router Interface Configurations

```
Branch_01_R(config)#
Branch_01_R(config)#router ospf 1
Branch_01_R(config-router)#router-id 6.6.6.5
Branch_01_R(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
Branch_01_R(config-router)#network 40.10.20.0 0.0.0.3 area 0
Branch_01_R(config-router)#network 192.168.20.0 0.0.0.255 area 0
Branch_01_R(config-router)#exit
Branch_01_R(config)#
Branch_01_R(config)#
*Mar 27 03:54:55.227: %OSPF-5-ADJCHG: Process 1, Nbr 6.6.6.4 on FastEthernet1/0 from LOADING to FULL, Loading Done
Branch_01_R(config)#
```

Figure 33:Branch-01 Router Routing Configuration

```
Branch_01_R#
Branch_01_R#show ip interface brief
Interface                IP-Address      OK? Method Status                Protocol
FastEthernet0/0          192.168.20.1    YES manual up                    up
FastEthernet1/0          40.10.20.2      YES manual up                    up
FastEthernet2/0          unassigned      YES unset  administratively down down
FastEthernet3/0          unassigned      YES unset  administratively down down
Tunnel1                  172.16.1.2      YES manual up                    up
Branch_01_R#
Branch_01_R#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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 40.10.20.1 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 40.10.20.1, 00:50:25, FastEthernet1/0
      1.0.0.0/30 is subnetted, 1 subnets
O        1.1.1.0 [110/30] via 40.10.20.1, 00:50:25, FastEthernet1/0
      40.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O        40.10.10.0/30 [110/20] via 40.10.20.1, 00:50:25, FastEthernet1/0
C        40.10.20.0/30 is directly connected, FastEthernet1/0
L        40.10.20.2/32 is directly connected, FastEthernet1/0
O        40.10.30.0/30 [110/20] via 40.10.20.1, 00:50:25, FastEthernet1/0
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.16.1.0/30 is directly connected, Tunnel1
L        172.16.1.2/32 is directly connected, Tunnel1
O        172.16.2.0/30 [110/10020] via 40.10.20.1, 00:42:42, FastEthernet1/0
O     192.168.10.0/24 [110/30] via 40.10.20.1, 00:50:25, FastEthernet1/0
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, FastEthernet0/0
L        192.168.20.1/32 is directly connected, FastEthernet0/0
O     192.168.30.0/24 [110/30] via 40.10.20.1, 00:44:41, FastEthernet1/0
Branch_01_R#
Branch_01_R#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
6.6.6.3           0   FULL/  -        00:00:32    172.16.1.1      Tunnel1
6.6.6.4           1   FULL/DR         00:00:36    40.10.20.1      FastEthernet1/0
Branch_01_R#
Branch_01_R#
```

Figure 34:Branch-01 Router Configuration Verifications

```
Branch_01_R(config)#
Branch_01_R(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.5
Branch_01_R(config)#ip dhcp pool branch-01
Branch_01_R(dhcp-config)#network 192.168.20.0 255.255.255.0
Branch_01_R(dhcp-config)#default-router 192.168.20.1
Branch_01_R(dhcp-config)#dns-server 8.8.8.8
Branch_01_R(dhcp-config)#exit
Branch_01_R(config)#
Branch_01_R(config)#
```

Figure 35:Branch-01 Router DHCP Configurations

```
Branch_01_R(config)#
Branch_01_R(config)#ip access-list extended ERP-QOS-CLSMP
Branch_01_R(config-ext-nacl)#$92.168.20.0 0.0.0.255 host 192.168.10.10
Branch_01_R(config-ext-nacl)#exit
Branch_01_R(config)#
Branch_01_R(config)#ip access-list extended VOICE-VIDEO-QOS-CLSMP
Branch_01_R(config-ext-nacl)#$92.168.20.0 0.0.0.255 host 192.168.10.15
Branch_01_R(config-ext-nacl)#$92.168.20.0 0.0.0.255 host 192.168.10.20
Branch_01_R(config-ext-nacl)#exit
Branch_01_R(config)#
Branch_01_R(config)#class-map match-any ERP-TRAFFIC
Branch_01_R(config-cmap)#match access-group name ERP-QOS-CLSMP
Branch_01_R(config-cmap)#exit
Branch_01_R(config)#
Branch_01_R(config)#class-map match-any VOICE-VIDEO-TRAFFIC
Branch_01_R(config-cmap)#match access-group name VOICE-VIDEO-QOS-CLSMP
Branch_01_R(config-cmap)#match protocol rtp
Branch_01_R(config-cmap)#match protocol rtcp
Branch_01_R(config-cmap)#match protocol sip
Branch_01_R(config-cmap)#exit
Branch_01_R(config)#
Branch_01_R(config)#policy-map B1-OUTBOUND-QOS
Branch_01_R(config-pmap)#class ERP-TRAFFIC
Branch_01_R(config-pmap-c)#priority percent 40
Branch_01_R(config-pmap-c)#set dscp af31
Branch_01_R(config-pmap-c)#
Branch_01_R(config-pmap-c)#class VOICE-VIDEO-TRAFFIC
Branch_01_R(config-pmap-c)#priority percent 30
Branch_01_R(config-pmap-c)#set dscp ef
Branch_01_R(config-pmap-c)#
Branch_01_R(config-pmap-c)#class class-default
Branch_01_R(config-pmap-c)#fair-queue
Branch_01_R(config-pmap-c)#exit
Branch_01_R(config-pmap)#exit
Branch_01_R(config)#interface FastEthernet0/0
Branch_01_R(config-if)#ip policy route-map SELECTIVE_TUNNEL
Branch_01_R(config-if)#exit
Branch_01_R(config)#
Branch_01_R(config)#interface fastEthernet 1/0
Branch_01_R(config-if)#service-policy output B1-OUTBOUND-QOS
Branch_01_R(config-if)#exit
Branch_01_R(config)#
```

Figure 36:Branch-01 Router QOS Configurations

```
Branch_01_R#show policy-map interface fastEthernet 1/0
 FastEthernet1/0

  Service-policy output: B1-OUTBOUND-QOS

    queue stats for all priority classes:
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0

    Class-map: ERP-TRAFFIC (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name ERP-QOS-CLSMP
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 40% (40000 kbps), burst bytes 1000000, b/w exceed drops: 0

      QoS Set
        dscp af31
          Packets marked 0

    Class-map: VOICE-VIDEO-TRAFFIC (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name VOICE-VIDEO-QOS-CLSMP
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol rtp
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol rtcp
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol sip
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (30000 kbps), burst bytes 750000, b/w exceed drops: 0

      QoS Set
        dscp ef
          Packets marked 0

    Class-map: class-default (match-any)
      1294 packets, 194696 bytes
      5 minute offered rate 2000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops/flowdrops) 0/0/0/0
      (pkts output/bytes output) 1294/198028
      Fair-queue: per-flow queue limit 16 packets
Branch_01_R# █
```

Figure 37:Branch-01 Router QOS Configuration Verifications

```
Branch_01_R(config)#
Branch_01_R(config)#interface Tunnel 1
Branch_01_R(config-if)#ip address 172.16.1.2 255.255.255.252
Branch_01_R(config-if)#tunnel source FastEthernet1/0
Branch_01_R(config-if)#tunnel destination 40.10.10.1
Branch_01_R(config-if)#tunnel mode ipsec ipv4
Branch_01_R(config-if)#tunnel protection ipsec profile MYPROFILE
Branch_01_R(config-if)#qos pre-classify
Branch_01_R(config-if)#exit
Branch_01_R(config)#
Branch_01_R(config)#ip access-list extended TO_HO_SPECIFIC
Branch_01_R(config-ext-nacl)#
*Mar 28 05:42:28.035: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
*Mar 28 05:42:28.087: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
*Mar 28 05:42:29.699: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
Branch_01_R(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 host 192.168.10.$
Branch_01_R(config-ext-nacl)#$92.168.20.0 0.0.0.255 host 192.168.10.15
Branch_01_R(config-ext-nacl)#$92.168.20.0 0.0.0.255 host 192.168.10.20
Branch_01_R(config-ext-nacl)#exit
Branch_01_R(config)#route-map SELECTIVE_TUNNEL permit 10
Branch_01_R(config-route-map)#match ip address TO_HO_SPECIFIC
Branch_01_R(config-route-map)#set interface Tunnel1
Branch_01_R(config-route-map)#exit
Branch_01_R(config)#router ospf 1
Branch_01_R(config-router)#network 172.16.1.2 0.0.0.0 area 0
Branch_01_R(config-router)#
Branch_01_R(config-router)#
*Mar 28 05:43:03.807: %OSPF-5-ADJCHG: Process 1, Nbr 6.6.6.3 on Tunnel1 from LOADING to FULL, Loading Done
Branch_01_R(config-router)#
```

Figure 38:Branch-01 Router GRE tunnel Configuration

```
Branch_01_R(config)#crypto isakmp policy 10
Branch_01_R(config-isakmp)#encr aes
Branch_01_R(config-isakmp)#hash sha
Branch_01_R(config-isakmp)#authentication pre-share
Branch_01_R(config-isakmp)#group 2
Branch_01_R(config-isakmp)#exit
Branch_01_R(config)#crypto isakmp key mysecretkey address 40.10.10.1
Branch_01_R(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
Branch_01_R(cfg-crypto-trans)#crypto ipsec profile MYPROFILE
Branch_01_R(ipsec-profile)#set transform-set MYSET
Branch_01_R(ipsec-profile)#exit
Branch_01_R(config)#
Branch_01_R(config)#
```

Figure 39:Branch-01 Router IPSec Configurations

```
Branch_01_R#
Branch_01_R#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst              src              state           conn-id status
40.10.10.1       40.10.20.2       QM_IDLE            1001 ACTIVE
40.10.20.2       40.10.10.1       QM_IDLE            1002 ACTIVE

IPv6 Crypto ISAKMP SA

Branch_01_R#
Branch_01_R#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Branch_01_R#
Branch_01_R#
Branch_01_R#
```

Figure 40:Branch-01 Router (IKE-phase-01) Security Associations (SA) Configuration Verifications

```
Branch_01_R#
Branch_01_R#show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 40.10.20.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 40.10.10.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1579, #pkts encrypt: 1579, #pkts digest: 1579
    #pkts decaps: 1567, #pkts decrypt: 1567, #pkts verify: 1567
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 40.10.20.2, remote crypto endpt.: 40.10.10.1
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
     current outbound spi: 0xA2D1A6FD(2731648765)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xCF52C61E(3478308382)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 5, flow_id: SW:5, sibling_flags 80000040, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4171448/2961)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xA2D1A6FD(2731648765)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 6, flow_id: SW:6, sibling_flags 80000040, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4171448/2961)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
Branch_01_R#
```

Figure 41:Branch-01 Router (IKE-phase-02) Security Associations (SA) tunnel Configuration Verifications

1.3.2.6   BRANCH-02 Router Configurations

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Branch_02_R
Branch_02_R(config)#banner motd #Unauthorized access prohibited...!#
Branch_02_R(config)#no ip domain lookup
Branch_02_R(config)#security passwords min-length 9
Branch_02_R(config)#enable secret cisco@123
Branch_02_R(config)#service password-encryption
Branch_02_R(config)#ip ssh version 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
Branch_02_R(config)#ip domain name slPLC.lk
Branch_02_R(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: Branch_02_R.slPLC.lk

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 9 seconds)

Branch_02_R(config)#login block-for 100 attempts 3 within 100
Branch_02_R(config)#username admin password cisco@123
Branch_02_R(config)#line console 0
Branch_02_R(config-line)#login local
Branch_02_R(config-line)#exec-timeout 10 0
Branch_02_R(config-line)#exit
Branch_02_R(config)#line vty 0 15
Branch_02_R(config-line)#login local
Branch_02_R(config-line)#exec-timeout 10 0
Branch_02_R(config-line)#exit
Branch_02_R(config)#
Branch_02_R(config)#
Branch_02_R(config)#
Branch_02_R(config)#
*Mar 27 03:57:28.119: %SSH-5-ENABLED: SSH 2.0 has been enabled
Branch_02_R(config)#
```

Figure 42:Branch-02 Router Basic Access Control Configuration

```
Branch_02_R(config)#
Branch_02_R(config)#interface fastEthernet 0/0
Branch_02_R(config-if)#ip address 40.10.30.2 255.255.255.252
Branch_02_R(config-if)#no shutdown
Branch_02_R(config-if)#exit
Branch_02_R(config)#interface fastEthernet 1/0
Branch_02_R(config-if)#ip address 192.168.30.1 255.255.255.0
Branch_02_R(config-if)#no shutdown
Branch_02_R(config-if)#exit
Branch_02_R(config)#
*Mar 27 03:58:08.499: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 27 03:58:08.587: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Mar 27 03:58:09.499: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Mar 27 03:58:09.587: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
Branch_02_R(config)#
```

Figure 43:Branch-02 Router Interface Configurations

```
Branch_02_R(config)#
Branch_02_R(config)#router ospf 1
Branch_02_R(config-router)#router-id 6.6.6.6
Branch_02_R(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
Branch_02_R(config-router)#network 40.10.30.0 0.0.0.3 area 0
Branch_02_R(config-router)#network 192.168.30.0 0.0.0.255 area 0
Branch_02_R(config-router)#exit
Branch_02_R(config)#
*Mar 27 03:58:44.879: %OSPF-5-ADJCHG: Process 1, Nbr 6.6.6.4 on FastEthernet0/0 from LOADING to FULL, Loading Done
Branch_02_R(config)#
```

Figure 44:Branch-02 Router Routing Configurations

```
Branch_02_R#show ip interface brief
Interface               IP-Address      OK? Method Status                Protocol
FastEthernet0/0         40.10.30.2      YES manual up                    up
FastEthernet1/0         192.168.30.1    YES manual up                    up
FastEthernet2/0         unassigned      YES unset  administratively down down
FastEthernet3/0         unassigned      YES unset  administratively down down
Tunnel2                 172.16.2.2      YES manual up                    up
Branch_02_R#
Branch_02_R#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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 40.10.30.1 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 40.10.30.1, 00:46:26, FastEthernet0/0
       1.0.0.0/30 is subnetted, 1 subnets
O         1.1.1.0 [110/30] via 40.10.30.1, 00:46:26, FastEthernet0/0
       40.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O         40.10.10.0/30 [110/20] via 40.10.30.1, 00:46:26, FastEthernet0/0
O         40.10.20.0/30 [110/20] via 40.10.30.1, 00:46:26, FastEthernet0/0
C         40.10.30.0/30 is directly connected, FastEthernet0/0
L         40.10.30.2/32 is directly connected, FastEthernet0/0
       172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O         172.16.1.0/30 [110/10020] via 40.10.30.1, 00:46:26, FastEthernet0/0
C         172.16.2.0/30 is directly connected, Tunnel2
L         172.16.2.2/32 is directly connected, Tunnel2
O      192.168.10.0/24 [110/30] via 40.10.30.1, 00:46:26, FastEthernet0/0
O      192.168.20.0/24 [110/30] via 40.10.30.1, 00:46:26, FastEthernet0/0
       192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.168.30.0/24 is directly connected, FastEthernet1/0
L         192.168.30.1/32 is directly connected, FastEthernet1/0
Branch_02_R#
Branch_02_R#show ip ospf neighbor

Neighbor ID     Pri   State         Dead Time   Address         Interface
6.6.6.3           0   FULL/  -      00:00:37    172.16.2.1      Tunnel2
6.6.6.4           1   FULL/DR       00:00:37    40.10.30.1      FastEthernet0/0
Branch_02_R#
Branch_02_R#
```

Figure 45:Branch-02 Router Configuration Verifications

```
Branch_02_R(config)#
Branch_02_R(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.5
Branch_02_R(config)#ip dhcp pool branch-02
Branch_02_R(dhcp-config)#network 192.168.30.0 255.255.255.0
Branch_02_R(dhcp-config)#default-router 192.168.30.1
Branch_02_R(dhcp-config)#dns-server 8.8.8.8
Branch_02_R(dhcp-config)#exit
Branch_02_R(config)#
```

Figure 46:Branch-02 Router DHCP Configurations

```
Branch_02_R(config)#
Branch_02_R(config)#ip access-list extended ERP-QOS-CLSMP
Branch_02_R(config-ext-nacl)#$92.168.30.0 0.0.0.255 host 192.168.10.10
Branch_02_R(config-ext-nacl)#exit
Branch_02_R(config)#
Branch_02_R(config)#ip access-list extended VOICE-VIDEO-QOS-CLSMP
Branch_02_R(config-ext-nacl)#$92.168.30.0 0.0.0.255 host 192.168.10.15
Branch_02_R(config-ext-nacl)#$92.168.30.0 0.0.0.255 host 192.168.10.20
Branch_02_R(config-ext-nacl)#exit
Branch_02_R(config)#
Branch_02_R(config)#class-map match-any ERP-TRAFFIC
Branch_02_R(config-cmap)#match access-group name ERP-QOS-CLSMP
Branch_02_R(config-cmap)#exit
Branch_02_R(config)#
Branch_02_R(config)#class-map match-any VOICE-VIDEO-TRAFFIC
Branch_02_R(config-cmap)#match access-group name VOICE-VIDEO-QOS-CLSMP
Branch_02_R(config-cmap)#match protocol rtp
Branch_02_R(config-cmap)#match protocol rtcp
Branch_02_R(config-cmap)#match protocol sip
Branch_02_R(config-cmap)#exit
Branch_02_R(config)#
Branch_02_R(config)#policy-map B2-OUTBOUND-QOS
Branch_02_R(config-pmap)#class ERP-TRAFFIC
Branch_02_R(config-pmap-c)#priority percent 40
Branch_02_R(config-pmap-c)#set dscp af31
Branch_02_R(config-pmap-c)#
Branch_02_R(config-pmap-c)#class VOICE-VIDEO-TRAFFIC
Branch_02_R(config-pmap-c)#priority percent 30
Branch_02_R(config-pmap-c)#set dscp ef
Branch_02_R(config-pmap-c)#
Branch_02_R(config-pmap-c)#class class-default
Branch_02_R(config-pmap-c)#fair-queue
Branch_02_R(config-pmap-c)#exit
Branch_02_R(config-pmap)#exit
Branch_02_R(config)#
Branch_02_R(config)#interface fastEthernet 0/0
Branch_02_R(config-if)#service-policy output B2-OUTBOUND-QOS
Branch_02_R(config-if)#exit
Branch_02_R(config)#
Branch_02_R(config)#interface FastEthernet 1/0
Branch_02_R(config-if)#ip policy route-map SELECTIVE_TUNNEL
Branch_02_R(config-if)#exit
Branch_02_R(config)#
Branch_02_R(config)#
```

Figure 47:Branch-02 Router QOS Configurations

```
Branch_02_R#show policy-map interface fastEthernet 0/0
 FastEthernet0/0

  Service-policy output: B2-OUTBOUND-QOS

    queue stats for all priority classes:
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 10/2092

    Class-map: ERP-TRAFFIC (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name ERP-QOS-CLSMP
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 40% (40000 kbps), burst bytes 1000000, b/w exceed drops: 0

      QoS Set
        dscp af31
          Packets marked 0

    Class-map: VOICE-VIDEO-TRAFFIC (match-any)
      10 packets, 1672 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name VOICE-VIDEO-QOS-CLSMP
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol rtp
        10 packets, 1672 bytes
        5 minute rate 0 bps
      Match: protocol rtcp
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol sip
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (30000 kbps), burst bytes 750000, b/w exceed drops: 0

      QoS Set
        dscp ef
          Packets marked 10

    Class-map: class-default (match-any)
      778 packets, 114297 bytes
      5 minute offered rate 1000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops/flowdrops) 0/0/0/0
      (pkts output/bytes output) 778/116533
      Fair-queue: per-flow queue limit 16 packets
Branch_02_R#
```

Figure 48:Branch-02 Router QOS Configuration Verifications

```
Branch_02_R(config)#
Branch_02_R(config)#interface Tunnel 2
Branch_02_R(config-if)#ip address 172.16.2.2 255.255.255.252
Branch_02_R(config-if)#tunnel source FastEthernet0/0
Branch_02_R(config-if)#tunnel destination 40.10.10.1
Branch_02_R(config-if)#tunnel mode ipsec ipv4
Branch_02_R(config-if)#tunnel protection ipsec profile MYPROFILE
Branch_02_R(config-if)#qos pre-classify
Branch_02_R(config-if)#exit
Branch_02_R(config)#
Branch_02_R(config)#ip access-list extended TO_HO_SPECIFIC
Branch_02_R(config-ext-nacl)#$92.168.30.0 0.0.0.255 host 192.168.10.10
Branch_02_R(config-ext-nacl)#$92.168.30.0 0.0.0.255 host 192.168.10.15
Branch_02_R(config-ext-nacl)#$92.168.30.0 0.0.0.255 host 192.168.10.20
Branch_02_R(config-ext-nacl)#exit
Branch_02_R(config)#
Branch_02_R(config)#route-map SELECTIVE_TUNNEL permit 10
Branch_02_R(config-route-map)#match ip address TO_HO_SPECIFIC
Branch_02_R(config-route-map)#set interface Tunnel2
Branch_02_R(config-route-map)#exit
Branch_02_R(config)#
*Mar 28 05:48:17.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state to down
*Mar 28 05:48:17.175: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Branch_02_R(config)#
*Mar 28 05:48:19.727: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state to up
Branch_02_R(config)#
Branch_02_R(config)#router ospf 1
Branch_02_R(config-router)#network 172.16.2.2 0.0.0.0 area 0
Branch_02_R(config-router)#
Branch_02_R(config-router)#
*Mar 28 05:48:27.115: %OSPF-5-ADJCHG: Process 1, Nbr 6.6.6.3 on Tunnel2 from LOADING to FULL, Loading Done
Branch_02_R(config-router)#exit
Branch_02_R(config)#
```

Figure 49:Branch-02 Router GRE tunnel Configurations

```
Branch_02_R(config)#
Branch_02_R(config)#crypto isakmp policy 10
Branch_02_R(config-isakmp)# encr aes
Branch_02_R(config-isakmp)# hash sha
Branch_02_R(config-isakmp)# authentication pre-share
Branch_02_R(config-isakmp)# group 2
Branch_02_R(config-isakmp)#exit
Branch_02_R(config)#crypto isakmp key mysecretkey address 40.10.10.1
Branch_02_R(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
Branch_02_R(cfg-crypto-trans)#crypto ipsec profile MYPROFILE
Branch_02_R(ipsec-profile)# set transform-set MYSET
Branch_02_R(ipsec-profile)#exit
Branch_02_R(config)#
Branch_02_R(config)#
Branch_02_R(config)#
```

Figure 50:Branch-02 Router IPSec Configurations

```
Branch_02_R#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst              src              state           conn-id status
40.10.10.1       40.10.30.2       QM_IDLE            1001 ACTIVE
40.10.30.2       40.10.10.1       QM_IDLE            1002 ACTIVE

IPv6 Crypto ISAKMP SA

Branch_02_R#
Branch_02_R#
Branch_02_R#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:    AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #2 (1024 bit)
        lifetime:                86400 seconds, no volume limit
Branch_02_R#
```

Figure 51:Branch-02 Router (IKE-phase-01) Security Associations (SA) Configuration Verifications

```
Branch_02_R#
Branch_02_R#show crypto ipsec sa

interface: Tunnel2
    Crypto map tag: Tunnel2-head-0, local addr 40.10.30.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 40.10.10.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 974, #pkts encrypt: 974, #pkts digest: 974
    #pkts decaps: 972, #pkts decrypt: 972, #pkts verify: 972
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 40.10.30.2, remote crypto endpt.: 40.10.10.1
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x599F2F5B(1503604571)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xDB90EC7B(3683708027)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 7, flow_id: SW:7, sibling_flags 80000040, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4234306/3268)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x599F2F5B(1503604571)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 8, flow_id: SW:8, sibling_flags 80000040, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4234306/3268)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
Branch_02_R# █
```

Figure 52:Branch-02 Router (IKE-phase-02) Security Associations (SA) Configuration Verifications

1.3.2.7   Head Office Switch Configurations

```
Switch>enable
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname HO_SWITCH
HO_SWITCH(config)#banner motd #Unauthorized access prohibited...!#
HO_SWITCH(config)#no ip domain lookup
HO_SWITCH(config)#enable secret cisco@123
HO_SWITCH(config)#service password-encryption
HO_SWITCH(config)#ip ssh version 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
HO_SWITCH(config)#ip domain name slPLC.lk
HO_SWITCH(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: HO_SWITCH.slPLC.lk

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

HO_SWITCH(config)#login block-for 100 attempts 3 within 100
HO_SWITCH(config)#username admin password cisco@123
HO_SWITCH(config)#line console 0
HO_SWITCH(config-line)#login local
HO_SWITCH(config-line)#exec-timeout 10 0
HO_SWITCH(config-line)#exit
HO_SWITCH(config)#
HO_SWITCH(config)#
*Mar 28 07:04:14.947: %SSH-5-ENABLED: SSH 2.0 has been enabled
HO_SWITCH(config)#
HO_SWITCH#wr
Building configuration...
Compressed configuration from 1010 bytes to 739 bytes[OK]
HO_SWITCH#
*Mar 28 07:04:19.766: %SYS-5-CONFIG_I: Configured from console by console
HO_SWITCH#
HO_SWITCH#cop r st
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 1010 bytes to 739 bytes[OK]
HO_SWITCH#
HO_SWITCH#
```

Figure 53:Head Office Switch Basic Access Control Configuration

1.3.2.8   ERP server Configurations

```
VPCS>
VPCS> set pcname ERP-SERVER

ERP-SERVER> ip 192.168.10.10 255.255.255.0 192.168.10.1
Checking for duplicate address...
ERP-SERVER : 192.168.10.10 255.255.255.0 gateway 192.168.10.1

ERP-SERVER> show ip

NAME        : ERP-SERVER[1]
IP/MASK     : 192.168.10.10/24
GATEWAY     : 192.168.10.1
DNS         :
MAC         : 00:50:79:66:68:0a
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500

ERP-SERVER> ping 192.168.20.6

84 bytes from 192.168.20.6 icmp_seq=1 ttl=61 time=50.555 ms
84 bytes from 192.168.20.6 icmp_seq=2 ttl=61 time=48.886 ms
84 bytes from 192.168.20.6 icmp_seq=3 ttl=61 time=58.640 ms
84 bytes from 192.168.20.6 icmp_seq=4 ttl=61 time=39.167 ms
84 bytes from 192.168.20.6 icmp_seq=5 ttl=61 time=47.277 ms

ERP-SERVER> save
Saving startup configuration to startup.vpc
.  done

ERP-SERVER>
```

Figure 54:Head office ERP server Configurations

1.3.2.9 VOICE PBX server Configurations

```
VPCS>
VPCS> set pcname voice-server

voice-server> ip 192.168.10.15 255.255.255.0 192.168.10.1
Checking for duplicate address...
voice-server : 192.168.10.15 255.255.255.0 gateway 192.168.10.1

voice-server> show ip

NAME          : voice-server[1]
IP/MASK       : 192.168.10.15/24
GATEWAY       : 192.168.10.1
DNS           :
MAC           : 00:50:79:66:68:09
LPORT         : 20000
RHOST:PORT    : 127.0.0.1:30000
MTU           : 1500

voice-server> ping 192.168.20.6

84 bytes from 192.168.20.6 icmp_seq=1 ttl=61 time=62.013 ms
84 bytes from 192.168.20.6 icmp_seq=2 ttl=61 time=62.001 ms
84 bytes from 192.168.20.6 icmp_seq=3 ttl=61 time=50.517 ms
84 bytes from 192.168.20.6 icmp_seq=4 ttl=61 time=51.058 ms
84 bytes from 192.168.20.6 icmp_seq=5 ttl=61 time=61.349 ms

voice-server> save
Saving startup configuration to startup.vpc
.  done

voice-server>
```

Figure 55:Head office Voice server Configurations

1.3.2.10 VIDEO Conferencing server Configurations

```
VPCS> set pcname videoConfSvr

videoConfSvr> ip 192.168.10.20 255.255.255.0 192.168.10.1
Checking for duplicate address...
videoConfSvr : 192.168.10.20 255.255.255.0 gateway 192.168.10.1

videoConfSvr> show ip

NAME          : videoConfSvr[1]
IP/MASK       : 192.168.10.20/24
GATEWAY       : 192.168.10.1
DNS           :
MAC           : 00:50:79:66:68:08
LPORT         : 20000
RHOST:PORT    : 127.0.0.1:30000
MTU           : 1500

videoConfSvr> ping 192.168.20.6

84 bytes from 192.168.20.6 icmp_seq=1 ttl=61 time=50.848 ms
84 bytes from 192.168.20.6 icmp_seq=2 ttl=61 time=33.728 ms
84 bytes from 192.168.20.6 icmp_seq=3 ttl=61 time=40.101 ms
84 bytes from 192.168.20.6 icmp_seq=4 ttl=61 time=31.307 ms
84 bytes from 192.168.20.6 icmp_seq=5 ttl=61 time=61.618 ms

videoConfSvr> save
Saving startup configuration to startup.vpc
.  done

videoConfSvr> ▮
```

Figure 56:Head office Video Conferencing server Configurations

1.3.2.11   BRANCH-01 PC Configurations

```
branch-01-pc> set pcname branch-01-pc

branch-01-pc> ip dhcp
DORA IP 192.168.20.6/24 GW 192.168.20.1

branch-01-pc> dhcp
DORA IP 192.168.20.6/24 GW 192.168.20.1

branch-01-pc> show ip

NAME          : branch-01-pc[1]
IP/MASK       : 192.168.20.6/24
GATEWAY       : 192.168.20.1
DNS           : 8.8.8.8
DHCP SERVER   : 192.168.20.1
DHCP LEASE    : 86366, 86400/43200/75600
MAC           : 00:50:79:66:68:06
LPORT         : 20000
RHOST:PORT    : 127.0.0.1:30000
MTU           : 1500

branch-01-pc>
branch-01-pc>
branch-01-pc>
branch-01-pc> save
Saving startup configuration to startup.vpc
.   done

branch-01-pc> █
```

Figure 57:Branch-01 PC IP Configurations

```
branch-01-pc>
branch-01-pc> trace 192.168.10.10
trace to 192.168.10.10, 8 hops max, press Ctrl+C to stop
 1   192.168.20.1    5.859 ms   8.999 ms   9.106 ms
 2   172.16.1.1    40.145 ms   40.767 ms   40.889 ms
 3   *192.168.10.10    72.126 ms (ICMP type:3, code:3, Destination port unreachable)

branch-01-pc> ping 200.200.200.1

84 bytes from 200.200.200.1 icmp_seq=1 ttl=251 time=70.318 ms
84 bytes from 200.200.200.1 icmp_seq=2 ttl=251 time=55.667 ms
84 bytes from 200.200.200.1 icmp_seq=3 ttl=251 time=60.022 ms
84 bytes from 200.200.200.1 icmp_seq=4 ttl=251 time=42.780 ms
84 bytes from 200.200.200.1 icmp_seq=5 ttl=251 time=79.360 ms

branch-01-pc>
```

Figure 58:Branch-01 PC traceroute and Internet

1.3.2.12   BRANCH-02 PC Configurations

```
VPCS> set pcname branch-02-pc

branch-02-pc> ip dhcp
DDORA IP 192.168.30.6/24 GW 192.168.30.1

branch-02-pc> show ip

NAME          : branch-02-pc[1]
IP/MASK       : 192.168.30.6/24
GATEWAY       : 192.168.30.1
DNS           : 8.8.8.8
DHCP SERVER   : 192.168.30.1
DHCP LEASE    : 86387, 86400/43200/75600
MAC           : 00:50:79:66:68:07
LPORT         : 20000
RHOST:PORT    : 127.0.0.1:30000
MTU           : 1500

branch-02-pc> save
Saving startup configuration to startup.vpc
.  done

branch-02-pc> █
```

Figure 59:Branch-01 PC IP Configurations

```
branch-02-pc> trace 192.168.10.10
trace to 192.168.10.10, 8 hops max, press Ctrl+C to stop
 1    192.168.30.1   9.271 ms  8.752 ms  9.954 ms
 2    172.16.2.1    50.359 ms  41.301 ms  41.105 ms
 3    *192.168.10.10   71.913 ms (ICMP type:3, code:3, Destination port unreachable)

branch-02-pc> ping 200.200.200.1

84 bytes from 200.200.200.1 icmp_seq=1 ttl=251 time=54.306 ms
84 bytes from 200.200.200.1 icmp_seq=2 ttl=251 time=60.671 ms
84 bytes from 200.200.200.1 icmp_seq=3 ttl=251 time=48.440 ms
84 bytes from 200.200.200.1 icmp_seq=4 ttl=251 time=54.726 ms
84 bytes from 200.200.200.1 icmp_seq=5 ttl=251 time=59.483 ms

branch-02-pc> █
```

Figure 60:Branch-02 PC traceroute and Internet

1.3.2.13 Wireshark Verifications of IPSec ESP Configurations
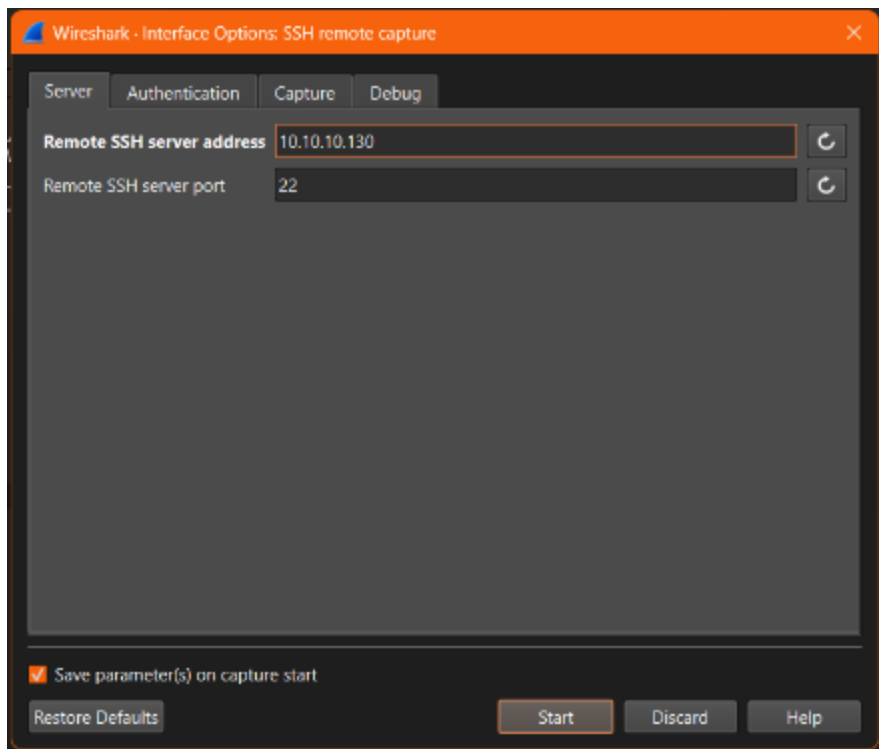

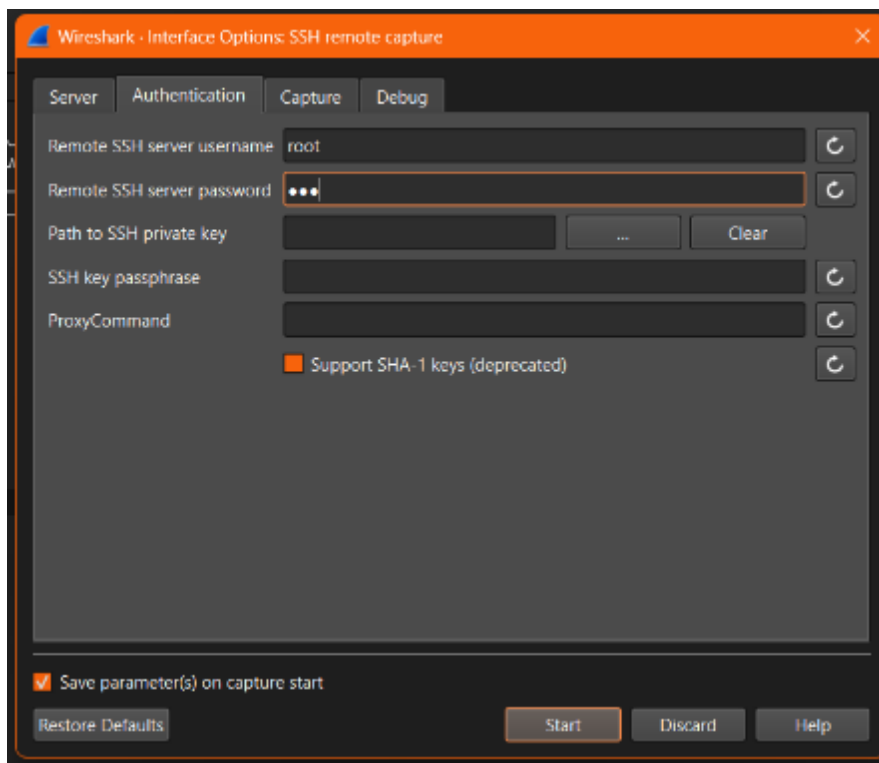*Figure 61:Wireshark Step-01*

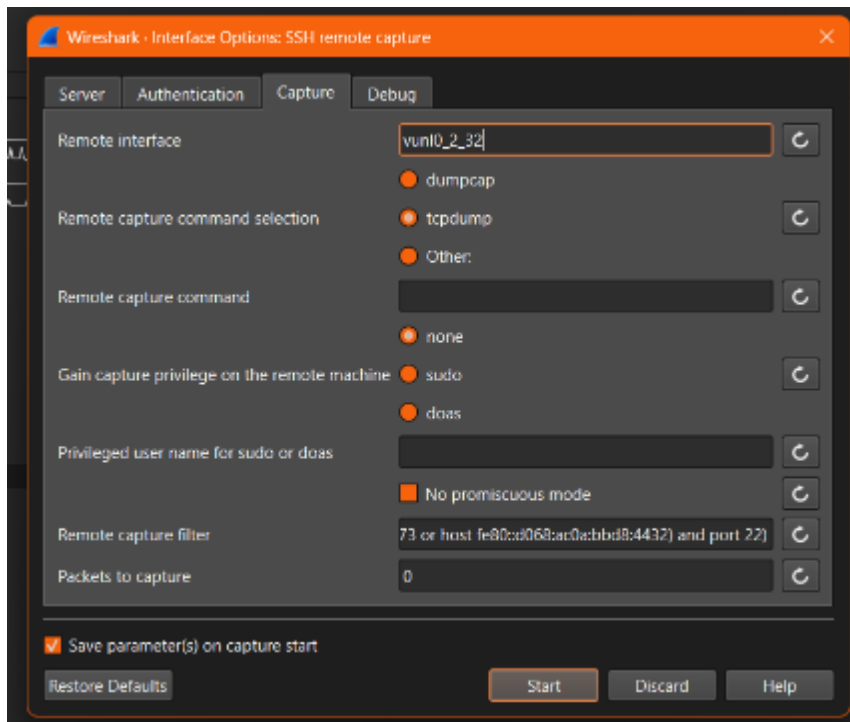*Figure 62:Wireshark Step-02*

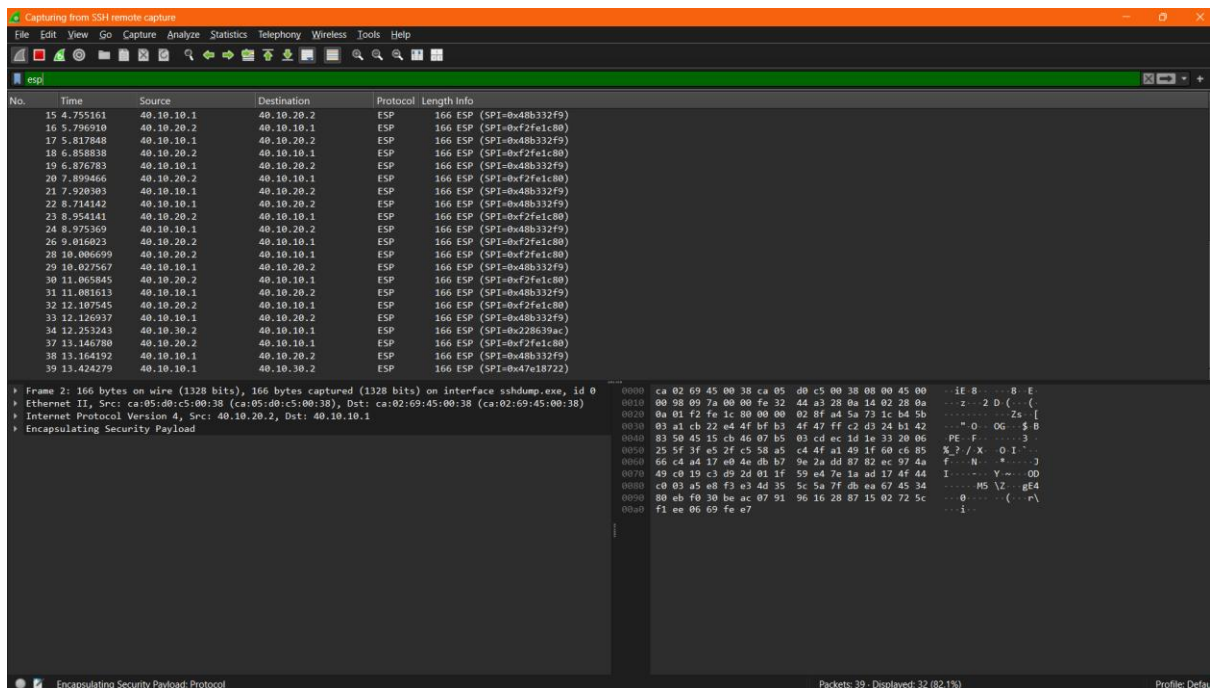*Figure 63:Wireshark Step-03*

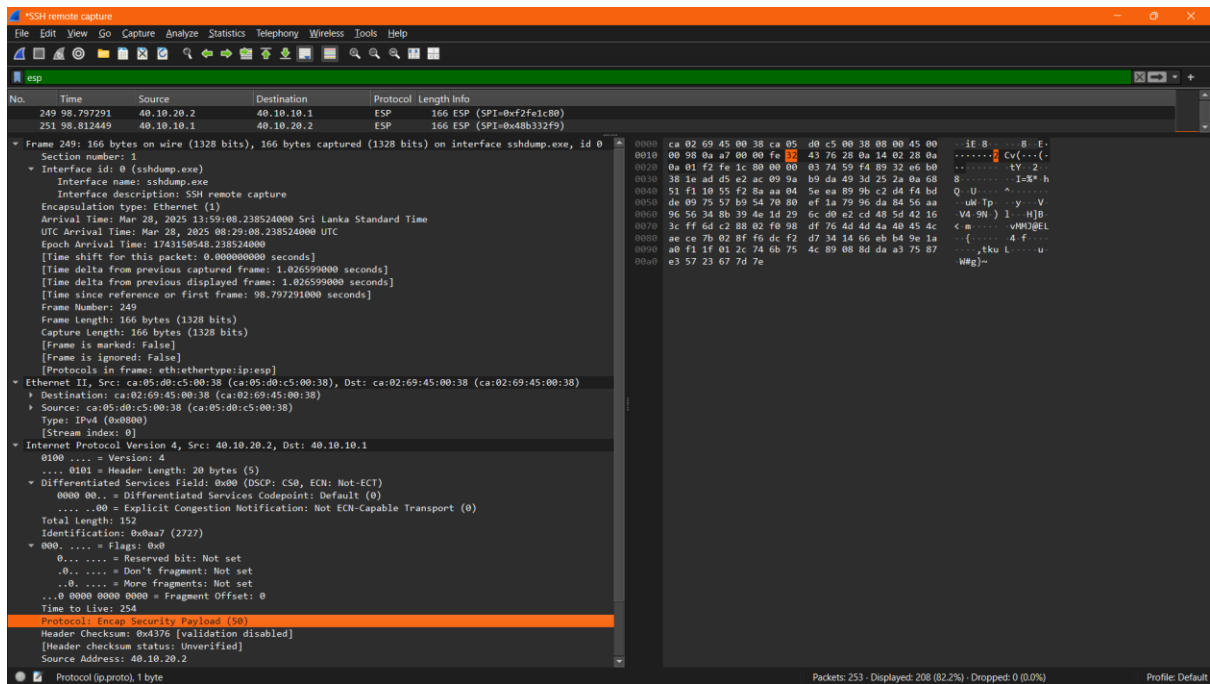*Figure 64:Wireshark Step-04 Filter ESP (Encapsulating Security Payload)*

Figure 65:Wireshark Step-05 ESP Packet Expansion

1.4 Quality of Service (QoS) Implementation & Verification

1.4.1 HEAD OFFICE Router QOS Configurations and Verification

```
HO_ROUTER(config)#
HO_ROUTER(config)#ip access-list extended ERP-QOS-CLSMP
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.10 192.168.20.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.10 192.168.30.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#exit
HO_ROUTER(config)#ip access-list extended VOICE-VIDEO-QOS-CLSMP
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.15 192.168.20.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.15 192.168.30.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.20 192.168.20.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#permit ip host 192.168.10.20 192.168.30.0 0.0.0.255
HO_ROUTER(config-ext-nacl)#exit
HO_ROUTER(config)#class-map match-any ERP-TRAFFIC
HO_ROUTER(config-cmap)#match access-group name ERP-QOS-CLSMP
HO_ROUTER(config-cmap)#exit
HO_ROUTER(config)#
HO_ROUTER(config)#class-map match-any VOICE-VIDEO-TRAFFIC
HO_ROUTER(config-cmap)#match access-group name VOICE-VIDEO-QOS-CLSMP
HO_ROUTER(config-cmap)#match protocol rtp
HO_ROUTER(config-cmap)#match protocol rtcp
HO_ROUTER(config-cmap)#match protocol sip
HO_ROUTER(config-cmap)#exit
HO_ROUTER(config)#policy-map HO-OUTBOUND-QOS
HO_ROUTER(config-pmap)#class ERP-TRAFFIC
HO_ROUTER(config-pmap-c)#priority percent 40
HO_ROUTER(config-pmap-c)#set dscp af31
HO_ROUTER(config-pmap-c)#
HO_ROUTER(config-pmap-c)#class VOICE-VIDEO-TRAFFIC
HO_ROUTER(config-pmap-c)#priority percent 30
HO_ROUTER(config-pmap-c)#set dscp ef
HO_ROUTER(config-pmap-c)#
HO_ROUTER(config-pmap-c)#class class-default
HO_ROUTER(config-pmap-c)#fair-queue
HO_ROUTER(config-pmap-c)#exit
HO_ROUTER(config-pmap)#exit
HO_ROUTER(config)#interface fastEthernet 1/0
HO_ROUTER(config-if)#ip policy route-map SELECTIVE_TUNNEL
HO_ROUTER(config-if)#exit
HO_ROUTER(config)#interface fastEthernet 2/0
HO_ROUTER(config-if)#service-policy output HO-OUTBOUND-QOS
HO_ROUTER(config-if)#exit
HO_ROUTER(config)#_
```

Figure 66:Head Office Router QOS Configuration

```
HO_ROUTER#show policy-map interface fastEthernet 2/0
 FastEthernet2/0

  Service-policy output: HO-OUTBOUND-QOS

   queue stats for all priority classes:
     Queueing
     queue limit 64 packets
     (queue depth/total drops/no-buffer drops) 0/0/0
     (pkts output/bytes output) 172/35972

   Class-map: ERP-TRAFFIC (match-any)
     0 packets, 0 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: access-group name ERP-QOS-CLSMP
       0 packets, 0 bytes
       5 minute rate 0 bps
     Priority: 40% (40000 kbps), burst bytes 1000000, b/w exceed drops: 0

     QoS Set
       dscp af31
         Packets marked 0

   Class-map: VOICE-VIDEO-TRAFFIC (match-any)
     172 packets, 28748 bytes
     5 minute offered rate 0000 bps, drop rate 0000 bps
     Match: access-group name VOICE-VIDEO-QOS-CLSMP
       0 packets, 0 bytes
       5 minute rate 0 bps
     Match: protocol rtp
       172 packets, 28748 bytes
       5 minute rate 0 bps
     Match: protocol rtcp
       0 packets, 0 bytes
       5 minute rate 0 bps
     Match: protocol sip
       0 packets, 0 bytes
       5 minute rate 0 bps
     Priority: 30% (30000 kbps), burst bytes 750000, b/w exceed drops: 0

     QoS Set
       dscp ef
         Packets marked 172

   Class-map: class-default (match-any)
     2164 packets, 317126 bytes
     5 minute offered rate 4000 bps, drop rate 0000 bps
     Match: any
     Queueing
     queue limit 64 packets
     (queue depth/total drops/no-buffer drops/flowdrops) 0/0/0/0
     (pkts output/bytes output) 2163/324638
     Fair-queue: per-flow queue limit 16 packets
HO_ROUTER#
```

Figure 67:Head Office Router QOS Configuration Verifications

1.4.2 BRANCH-01 Router QOS Configurations and Verification

```
Branch_01_R(config)#
Branch_01_R(config)#ip access-list extended ERP-QOS-CLSMP
Branch_01_R(config-ext-nacl)#$92.168.20.0 0.0.0.255 host 192.168.10.10
Branch_01_R(config-ext-nacl)#exit
Branch_01_R(config)#
Branch_01_R(config)#ip access-list extended VOICE-VIDEO-QOS-CLSMP
Branch_01_R(config-ext-nacl)#$92.168.20.0 0.0.0.255 host 192.168.10.15
Branch_01_R(config-ext-nacl)#$92.168.20.0 0.0.0.255 host 192.168.10.20
Branch_01_R(config-ext-nacl)#exit
Branch_01_R(config)#
Branch_01_R(config)#class-map match-any ERP-TRAFFIC
Branch_01_R(config-cmap)#match access-group name ERP-QOS-CLSMP
Branch_01_R(config-cmap)#exit
Branch_01_R(config)#
Branch_01_R(config)#class-map match-any VOICE-VIDEO-TRAFFIC
Branch_01_R(config-cmap)#match access-group name VOICE-VIDEO-QOS-CLSMP
Branch_01_R(config-cmap)#match protocol rtp
Branch_01_R(config-cmap)#match protocol rtcp
Branch_01_R(config-cmap)#match protocol sip
Branch_01_R(config-cmap)#exit
Branch_01_R(config)#
Branch_01_R(config)#policy-map B1-OUTBOUND-QOS
Branch_01_R(config-pmap)#class ERP-TRAFFIC
Branch_01_R(config-pmap-c)#priority percent 40
Branch_01_R(config-pmap-c)#set dscp af31
Branch_01_R(config-pmap-c)#
Branch_01_R(config-pmap-c)#class VOICE-VIDEO-TRAFFIC
Branch_01_R(config-pmap-c)#priority percent 30
Branch_01_R(config-pmap-c)#set dscp ef
Branch_01_R(config-pmap-c)#
Branch_01_R(config-pmap-c)#class class-default
Branch_01_R(config-pmap-c)#fair-queue
Branch_01_R(config-pmap-c)#exit
Branch_01_R(config-pmap)#exit
Branch_01_R(config)#interface FastEthernet0/0
Branch_01_R(config-if)#ip policy route-map SELECTIVE_TUNNEL
Branch_01_R(config-if)#exit
Branch_01_R(config)#
Branch_01_R(config)#interface fastEthernet 1/0
Branch_01_R(config-if)#service-policy output B1-OUTBOUND-QOS
Branch_01_R(config-if)#exit
Branch_01_R(config)#
```

Figure 68:Branch-01 Router QOS Configuration

```
Branch_01_R#show policy-map interface fastEthernet 1/0
 FastEthernet1/0

  Service-policy output: B1-OUTBOUND-QOS

    queue stats for all priority classes:
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0

    Class-map: ERP-TRAFFIC (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name ERP-QOS-CLSMP
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 40% (40000 kbps), burst bytes 1000000, b/w exceed drops: 0

      QoS Set
        dscp af31
          Packets marked 0

    Class-map: VOICE-VIDEO-TRAFFIC (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name VOICE-VIDEO-QOS-CLSMP
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol rtp
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol rtcp
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol sip
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (30000 kbps), burst bytes 750000, b/w exceed drops: 0

      QoS Set
        dscp ef
          Packets marked 0

    Class-map: class-default (match-any)
      1294 packets, 194696 bytes
      5 minute offered rate 2000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops/flowdrops) 0/0/0/0
      (pkts output/bytes output) 1294/198028
      Fair-queue: per-flow queue limit 16 packets
Branch_01_R#
```

Figure 69:Branch-01 Router QOS Configuration Verification

1.4.3 BRANCH-02 Router QOS Configurations and Verification

```
Branch_02_R(config)#
Branch_02_R(config)#ip access-list extended ERP-QOS-CLSMP
Branch_02_R(config-ext-nacl)#$92.168.30.0 0.0.0.255 host 192.168.10.10
Branch_02_R(config-ext-nacl)#exit
Branch_02_R(config)#
Branch_02_R(config)#ip access-list extended VOICE-VIDEO-QOS-CLSMP
Branch_02_R(config-ext-nacl)#$92.168.30.0 0.0.0.255 host 192.168.10.15
Branch_02_R(config-ext-nacl)#$92.168.30.0 0.0.0.255 host 192.168.10.20
Branch_02_R(config-ext-nacl)#exit
Branch_02_R(config)#
Branch_02_R(config)#class-map match-any ERP-TRAFFIC
Branch_02_R(config-cmap)#match access-group name ERP-QOS-CLSMP
Branch_02_R(config-cmap)#exit
Branch_02_R(config)#
Branch_02_R(config)#class-map match-any VOICE-VIDEO-TRAFFIC
Branch_02_R(config-cmap)#match access-group name VOICE-VIDEO-QOS-CLSMP
Branch_02_R(config-cmap)#match protocol rtp
Branch_02_R(config-cmap)#match protocol rtcp
Branch_02_R(config-cmap)#match protocol sip
Branch_02_R(config-cmap)#exit
Branch_02_R(config)#
Branch_02_R(config)#policy-map B2-OUTBOUND-QOS
Branch_02_R(config-pmap)#class ERP-TRAFFIC
Branch_02_R(config-pmap-c)#priority percent 40
Branch_02_R(config-pmap-c)#set dscp af31
Branch_02_R(config-pmap-c)#
Branch_02_R(config-pmap-c)#class VOICE-VIDEO-TRAFFIC
Branch_02_R(config-pmap-c)#priority percent 30
Branch_02_R(config-pmap-c)#set dscp ef
Branch_02_R(config-pmap-c)#
Branch_02_R(config-pmap-c)#class class-default
Branch_02_R(config-pmap-c)#fair-queue
Branch_02_R(config-pmap-c)#exit
Branch_02_R(config-pmap)#exit
Branch_02_R(config)#
Branch_02_R(config)#interface fastEthernet 0/0
Branch_02_R(config-if)#service-policy output B2-OUTBOUND-QOS
Branch_02_R(config-if)#exit
Branch_02_R(config)#
Branch_02_R(config)#interface FastEthernet 1/0
Branch_02_R(config-if)#ip policy route-map SELECTIVE_TUNNEL
Branch_02_R(config-if)#exit
Branch_02_R(config)#
```

Figure 70:Branch-02 Router QOS Configuration

```
Branch_02_R#show policy-map interface fastEthernet 0/0
 FastEthernet0/0

  Service-policy output: B2-OUTBOUND-QOS

    queue stats for all priority classes:
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 10/2092

    Class-map: ERP-TRAFFIC (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name ERP-QOS-CLSMP
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 40% (40000 kbps), burst bytes 1000000, b/w exceed drops: 0

      QoS Set
        dscp af31
          Packets marked 0

    Class-map: VOICE-VIDEO-TRAFFIC (match-any)
      10 packets, 1672 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name VOICE-VIDEO-QOS-CLSMP
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol rtp
        10 packets, 1672 bytes
        5 minute rate 0 bps
      Match: protocol rtcp
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol sip
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (30000 kbps), burst bytes 750000, b/w exceed drops: 0

      QoS Set
        dscp ef
          Packets marked 10

    Class-map: class-default (match-any)
      778 packets, 114297 bytes
      5 minute offered rate 1000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops/flowdrops) 0/0/0/0
      (pkts output/bytes output) 778/116533
      Fair-queue: per-flow queue limit 16 packets
Branch_02_R#
```

Figure 71:Branch-02 Router QOS Configuration Verification

1.5   Wi-Fi Deployment Strategy in PLC

For Wi-Fi Access Points deployment in SPORT & LEISURE PLC, Engineers should do their best to deliver the best Wi-Fi coverage, performance, and security across the branches and the Head Office, SPORT & LEISURE PLC should use a deployment plan that is well-structured. This must include the following key recommendations:

1. **Deploying an Extended Service Set (ESS) with Optimized Channels**

   - Use multiple Wi-Fi Access Points (APs) to create an Extended Service Set (ESS) across the premises.

   - Assign non-overlapping channels (1, 9, 11) for 2.4GHz frequency to reduce interference.

   - For 5GHz, use dynamic frequency selection (DFS) channels to optimize performance and minimize congestion.

   - Ensure seamless roaming between APs by maintaining the same SSID and password across all Basic Service Sets (BSS) for user mobility.

2. **Centralized Management with Wireless LAN Controller (WLC)**

   - Deploy Lightweight Access Points (LWAPs) managed by a centralized Wireless LAN Controller (WLC) for efficient configuration, monitoring, and security enforcement.

   - The WLC will handle automatic channel selection and power management between APs.

   - Implement the number of user limitations as load balancing to distribute users across multiple APs.

3. **Conduct a Site Survey Before Deployment**

- Perform a Wi-Fi site survey to identify black spots and high-interference zones before installing APs.

- Use Wi-Fi heat mapping tools to determine the best locations for AP placement.

- Ensure proper AP positioning covers all areas while minimizing signal overlapping and interference.

4. **Use High-Performance and High-Secure Access Points**

- Purchase Wi-Fi 6 (802.11ax) APs with 5GHz support for better speed, efficiency, and lower latency.

- Ensure APs support WPA3 or WPA2 security protocols for strong encryption and authentication.

- Disable legacy protocols (WEP, WPA) to prevent security vulnerabilities.

5. **Implement Access Control and Bandwidth Management**

- Set up role-based access control to restrict Wi-Fi access privileges for employees and guests.

- Create a separate guest network (SSID) with internet-only access to prevent unauthorized access to internal resources.

- Use Quality of Service (QoS) to prioritize business-critical applications and limit bandwidth for non-essential activities.

- Implement MAC address or 802.1X authentication-based filtering for additional security Because of that low level security devices can't connect to the WLAN.

By following the above strategies, SPORT & LEISURE PLC will achieve a high-performance, secure, and scalable Wi-Fi network that supports seamless user mobility, effective management, and strong security controls across Head Office and the two branches.

1.6   Business Continuity & Reliability Plan (BCP)

To ensure a highly reliable network across Head Office and two branch locations, SPORT &
LEISURE PLC should implement LAN design with redundancy and Business Continuity
Planning (BCP) strategies to prevent downtime and ensure continued operations in case of
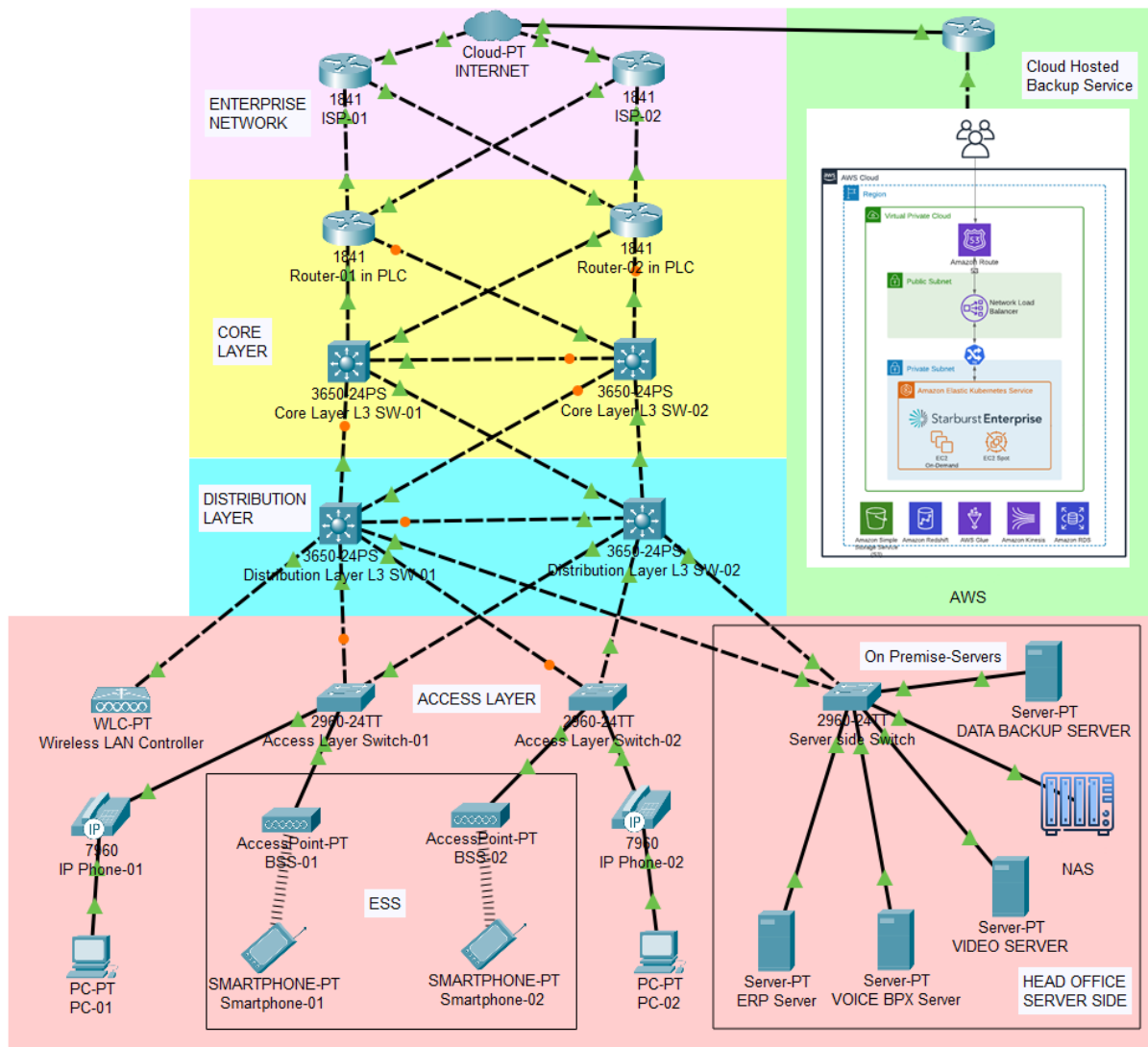failures.

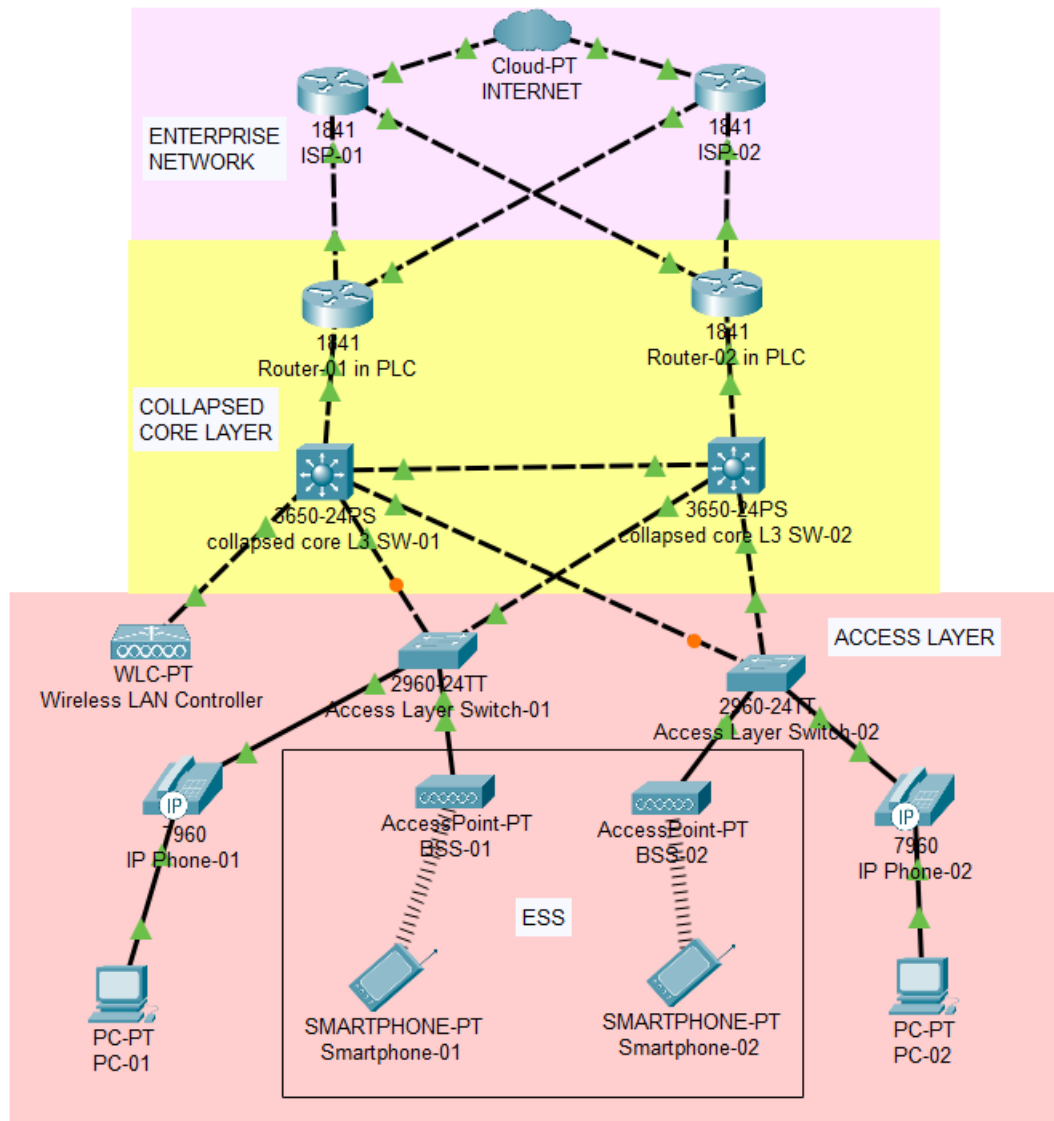*Figure 72:Head Office 3 tier architecture LAN design*

Figure 73:Branches collapsed architecture LAN design

- According to Above Network Topology *(Figure-72),* rather than having a single ISP connection (single-homed) as earlier, engineers can architecture a dual multi-homed connection for better bandwidth in their Head Office.

- According to the above topology *(Figure-72)*, engineers can use the 3-2-1 backup model as their backup strategy, with a differential backup solution every week.

- They can maintain export apparel databases and their marketing website both on-premises and in a cloud instance like AWS EC2 & S3 bucket for better BCP.

- On-premises ERP, VOICE, and VIDEO servers can also be deployed on VMware-ESXi to ensure High Availability (HA) and Fault Tolerance (FT).

- PLC engineers can configure the Gateway Load Balancing Protocol (GLBP) on Layer 3 devices to ensure network traffic load balancing between the main and redundant network devices and cables.

- They should improve the configured QoS solution to ensure better traffic management and install a firewall to monitor any suspicious ingress (incoming) and egress (outgoing) network traffic.

- Applying EtherChannel/Link Aggregation Control Protocol (LACP) will increase bandwidth and provide link redundancy. If one link in the aggregated group fails, traffic can still flow through the remaining links.

- Rapid Spanning Tree Protocol (RSTP) should be implemented to prevent network loops and ensure faster convergence.

- Ensuring that network devices like switches and routers have redundant power supplies can prevent outages due to power failures.

- Establishing a secondary site (warm or hot site) with RAID-5 replicated data and infrastructure will allow operations to continue in case of a major disaster at one of the primary locations.

- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) should be minimized to ensure faster recovery and minimal data loss, improving business continuity and reducing downtime.

- This LAN network has Scalability with the company growth, but it is highly expensive. Engineers can switch to Cloud Services as an alternative solution for this.

PART 2: Distributed Systems

2.1   Distributed Systems Design Goals in Content Streaming

A distributed system is a collection of autonomous computing elements that work together and appear to users as a single coherent system to provide a combined service. These systems share resources, communicate over a network, and coordinate operations to function as a single entity. Key characteristics of a distributed system include **resource sharing**: where nodes share hardware performance, **Distribution Transparency**: Users experience the system as a single entity despite its distributed nature, **Openness**: Supports multiple devices, platforms, and protocols, **Scalability**: Can expand horizontally and vertically to handle more users and data efficiently, and **fault tolerance**: allowing the system to continue functioning even if some nodes fail.

2.1.1 Resource Sharing

resource sharing where virtual nodes share hardware performance or in a peer-to-peer (P2P) model, users' devices contribute bandwidth to help stream content to other users (like torrent), supporting distributed storage and network resources efficiently. In a client-server model, content is served from dedicated servers, where the network, storage, and computing resources are shared among multiple users. Content Delivery Networks (CDNs) and edge caching further optimize resource utilization by distributing content closer to users.

2.1.2 Distribution Transparency

The goal of distribution transparency in content streaming distributed system is to hide the fact that resources are distributed across multiple systems. That can guide users to experience the service as a single coherent system. That can be achieved by the well implemented middleware software. There are 7 distribution transparency technologies in a distributed system.

- **Access Transparency:** Users simply watch a video without worrying about how the data is retrieved to their devices.

- **Location Transparency:** Content is streamed from various sources (servers, peers, CDNs) without users knowing where it is stored.

- **Relocation Transparency:** ensures users aren't aware if an object/data is moved during in use.

- **Migration Transparency:** hides the movement of objects between locations for optimization.

- **Replication Transparency:** The system automatically selects the best source, whether from a replicated server or a cached version, without user interference.

- **Concurrency Transparency:** manages parallel access to shared resources, ensuring smooth user experiences.

- **Failure Transparency:** If a server or peer fails, the system seamlessly switches to another source to avoid interruptions.

2.1.3 Openness

Content streaming services support multiple devices, Platforms and operating systems (smartphones, Smartwatches, smart TVs and Computers) by using standard worldwide device design or software design protocols. They also integrate with Content Delivery Networks and cloud providers, ensuring flexibility and easy updates (adding new video/images formats and converting the uploaded format into another supported format for other platforms).

2.1.4 Scalability

The content streaming system must be highly scalable horizontally and vertically to handle and hold large number of users and the vast amount of content they generate. This involves several dimensions of scalability:

- **Size Scalability:** The system handles millions of users through replication, caching, and data partitioning.

- **Geographical Scalability:** CDNs distribute content globally, reducing latency and improving performance.

- **Administrative Scalability:** managing growth in Services, Server Nodes, users, or system complexity without significantly increasing administrative effort. It is achieved through **Decentralization** (blockchain), **Automation** (Kubernetes), **Delegated policies**, And **Self-healing designs**.

2.1.5 Real-World Example of Content Streaming Distributed System

Good examples of distributed systems are content streaming systems like Netflix, YouTube, Spotify and Pinterest which distributes media content across multiple servers, CDNs, and caches data in region edge servers to ensure smooth streaming and load balancing. **Examples:**

2.1.5.1   Video Content Streaming Distributed System

- Netflix
- YouTube

2.1.5.2   Audio Content Streaming Distributed System

- Spotify
- Apple Music

2.1.5.3   Image Content Streaming Distributed System

- Pinterest
- Pexels

CONCLUSION

In conclusion, to enhance the reliability and performance of the network for SPORT & LEISURE PLC, it is essential to implement a robust and scalable LAN design that contains redundancy, high availability, and fault tolerance. By introducing multi-homed ISP connections, optimizing QoS for traffic, and deploying a Business Continuity Plan (BCP), the company can ensure continuous operations even in the event of network failures. Additionally, improvements in Wi-Fi access point deployment, combining modern security measures, and utilizing advanced technologies like EtherChannel and GLBP will support the network's efficiency. A well-designed network architecture, along with effective monitoring and management strategies, will enable the company to handle future expansion while ensuring reliability, security, and seamless connectivity for its operations across multiple locations.

REFERENCES

Cisco, Inc (2025). *CCNP Enterprise: Advanced Routing.*

> https://www.netacad.com/courses/ccnp-enterprise-advanced-routing?courseLang=en-US

Cisco, Inc (2025). *CCNP Enterprise: Core Networking.*

> https://www.netacad.com/courses/ccnp-enterprise-core-networking?courseLang=en-US

Cisco, Inc (2025). *Cisco Packet Tracer.* https://www.netacad.com/cisco-packet-tracer

Cisco, Inc (2025). *The Cisco Learning Network.* https://learningnetwork.cisco.com/s/

EVE-NG Ltd. (2025). *EVE-NG Community Edition.* https://customers.eve-ng.net/eve-ce-prod-6.2.0-4-full.iso

Kevin Wallace Training, LLC. (2019) *Net Talk - GRE over IPsec.* Google LLC.

> https://www.youtube.com/@kwallaceccie

René Molenaar (CCIE #41726 instructor). (2013). *Single/Dual Homed and Multi-homed Designs in CCNA Routing & Switching ICND2 200-105.* https://networklessons.com/cisco/ccna-routing-switching-icnd2-200-105/singledual-homed-and-multi-homed-designs