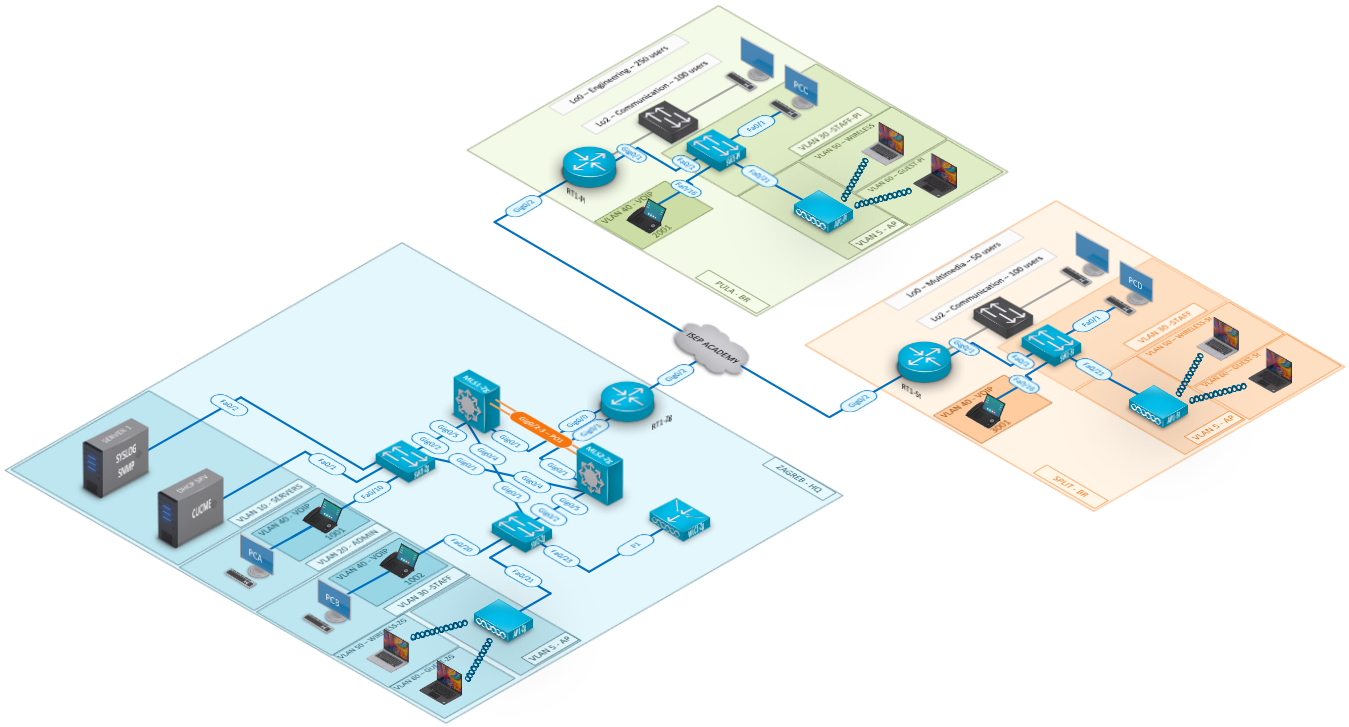
CCNAv7 ENSA Final Exam Topology



Assessment Objectives

- **Part 1: Clear Configs and Reload the Equipment** (1 point)
- **Part 2: Reload Configurations From the Previous Deployment (SRWE)** (2 points)
- **Part 3: Change Interface Configuration** (2 points)
- **Part 4: Configure IPSEC VPN Tunnels** (15 points)
- **Part 5: Configure Routing** (15 points)
- **Part 6: Configure Static and Dynamic NAT** (10 points)
- **Part 7: Deploy Telephony Services** (10 points)
- **Part 8: Implement NTP** (10 points)
- **Part 9: Implement Syslog and SNMP** (15 points)
- **Part 10: Restrict Accesses** (20 points)

Part 11: Execute Configuration Backup with Ansible (10 extra points)

Scenario

The topology represents a Croatian Service company that develops tech gadgets with its headquarters in the capital Zagreb and two branches by the coast, in Pula and Split. Your task is to plan an IP address scheme to fulfill the company needs and to configure all equipment to guarantee full connectivity.

Required Resources

- 3 Router (Cisco 4221/2911 with Cisco IOS XE)
- 4 Switch (Cisco 2960 with Cisco IOS)
- 2 Multi-Layer Switch (Cisco 3560/3650/3750 with Cisco IOS)
- 1 Wireless Lan Controller 2100/2500
- 3 LightWeight Access Points 1702
- 5 PCs (Windows with a terminal emulation program, such as Tera Term)
- 2 Laptops with a wireless NIC
- 4 IPPhones
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Instructions

Part 1: Clear Configs and Reload the Equipment

Total points: 1

- Erase the startup configurations and VLANs from the router and switch and reload the devices.

Register the commands used:

Task	IOS Command
Erase the startup-config file on the Routers	
Reload the Routers	
Erase the startup-config file on the Switches	
Delete the vlan.dat file on the Switches	
Reload the Switches	

Task	IOS Command
Verify the Switches SDM Template	
Clear the WLC Config	
Clear the APs Config	

Part 2: Reload Configurations From the Previous Deployment (SRWE)

Total points: 2

Part 3: Change Interface Configuration

Total points: 2

Step 1: Subnetting

a. The address scheme of the previous deployment (SRWE configuration) will be used in this deployment, with minor changes.

b. The addresses used in the connection between location will now be used in the IPSEC VPN tunnels.

Location	Subnet	Prefix
Zagreb-Pula (Tunnel)	10.0.0.0	/30
Zagreb-Split (Tunnel)	10.0.0.4	/30
Pula-Split (Tunnel)	10.0.0.8	/30

Step 2: Interface addressing

a. Record your IPV4 assign addresses in the table below.

Device	Interface	IP address	Prefix	Description	Gateway
RT1-Zg	Gig0/2	DHCP from ISEP ACADEMY		Internet Connection	N/A
RT1-Pl	Gig0/2	DHCP from ISEP ACADEMY		Internet Connection	N/A
RT1-St	Gig0/2	DHCP from ISEP ACADEMY		Internet Connection	N/A

Step 3: New Voice Networks

a. In Pula and Split the previous address given to the Design Network, simulated by the routers loopback 1 interface will be used for the newly added voice network (add VLAN40 VoIP).

b. Make the necessary changes to adjust this new network.

Part 4: Configure IPSEC VPN Tunnels

Total points: 15

a. To help you with the configuration of the IPSEC VPN Static Tunnel Interface there is a guide in Annex 1.

b. The following parameters must be used:
    a. Policy number 100
        i. Encryption AES 128
        ii. Hash Algorithm SHA
        iii. Authentication Pre-shared
        iv. Diffie-Hellman group 5
    b. Authentication Keys
        i. Connection between Zagreb and Pula – z4gr3bPvl4
        ii. Connection between Zagreb and Split – z4gr3b$pl1t
        iii. Connection between Pula and Split – Pvl4$pl1t
    c. IPSec transform set TSET
        i. Security protocol ESP
        ii. Encryption AES 128
        iii. Hash Algorithm SHA
    d. Crypto Map name CROATIA

Part 5: Configure Routing

Total points: 15

a. Configure OSPF with process ID 100

b. Configure the appropriate interfaces into area 0 (use the interface address)

c. Remove the static routing configuration

d. Configure a static route in each router pointing to the default gateway received by DHCP

e. Redistribute the default route into the OSPF process

f. Verify full connectivity

Part 6: Configure Static and Dynamic NAT

Total points: 10

a. All networks should be allowed to be translated in any of the routers RT1, therefore you must configure a standard access-control list that permits it
b. Configure the dynamic NAT rule and the defined interface accordingly
c. Test the connection from various locations to the Internet
d. In RT1-Zg configure a static NAT rule (port forwarding) to allow external access to the http, https and ssh server in the DHCP-Server.
    a. To activate the http and https server in the DHCP-Server emulated by a router use the following global configuration commands:
        i. ip http server
        ii. ip http secure-server
        iii. ip http authentication local
e. From a computer connected to the ISEP ACADEMY network try to access the http/s server using the external address from RT1-Zg

Part 7: Deploy Telephony Services

Total points: 10

a. The routers that must be configure as Call Manager are:
    a. Router RT1-Pl for Pula
    b. Router RT1-St for Split
    c. DHCP Server for Zagreb
b. Using the information presented in Annex2 and information given by the logical topology configure the telephony services.

Part 8: Implement NTP

Total points: 10

a. RT1-Zg must be synchronized with an external NTP server
b. All other device in the network must synchronized with the Zagreb NTP Server in RT1-Zg

Part 9: Implement Syslog and SNMP

Total points: 15

a. Configure SNMP in all active networking equipment
    a. SNMPv2c with the community string set **cisco** in read only mode
b. Configure the syslog server in all active networking equipment
    a. Trap level – Informational

   b. Logging server – IP address configured in Server 1

c. Configure a the PC that is emulating Server 1 has the Network Monitor Station
   a. Install LibreNMS server on a Virtual Box (https://docs.librenms.org/Installation/Images/)
   b. Configure all device to be monitor by LibreNMS
   c. Configure all device to use LibreNMS as their syslog server (https://docs.librenms.org/Extensions/Syslog/)

Part 10: Restrict Accesses

Total points: 20

a. Configure the following access restriction using ACLs:
   a. GUEST networks must only have access to the Internet
   b. VoIP network must not have access to the Internet
   c. SNMP request must only be made from Server 1
   d. SSH request to the equipment may only originate from the ADMIN and STAFF networks

Part 11: Execute Configuration Backup with Ansible

Total points: 10 Extra

a. Using WSL (windows subsystem for linux) install ansible and configure it to export all intermediate devices configuration.

Annex 1: GRE/IPSEC Tunnel Configuration Template:

```
crypto isakmp policy policynumber
 encr encryption_algorithm
 authentication pre-share
 group diffie_hellman_group_number
crypto isakmp key Keystring address peer_public_address
!
crypto ipsec transform-set transform_set_name esp-3des esp-sha-hmac
!
crypto map crypto_map_name sequence_number ipsec-isakmp
 set peer peer_public_address
 set transform-set        transform_set_name
 match address crypto_acl_name
!
interface Tunnel0
 description tunnel_description
 ip address tunnel_address tunnel_mask_address
 tunnel source local_public_address
 tunnel destination remote_public_address
!
interface connect_to_the_public_address
crypto map crypto_map_name
!
ip access-list extended crypto_acl_name
 permit gre host local_public_address host remote_public_address
 deny   ip any any
```

Annex 2: Telephony Services Configuration Template:

```
! Configure the correct timezone in all equipments
clock timezone WET 0 0
clock summer-time WEST recurring last Sun Mar 1:00 last Sun Oct 2:00
!
ip dhcp pool VOICE
 network voice_network-address voice-netmask
 default-router voice-gateway-address
 dns-server xxx.xxx.xxx.xxx
 option 150 ip voice-gateway-address
 lease x
!
telephony-service
 max-ephones 64
 max-dn 128
 ip source-address voice-gateway-address port 2000
 system message system-message
 cnf-file location flash:
 load 7912 CP7912080004SCCP080108A.sbin
 create cnf-files
!
ephone-dn  1
 number extension-number
!
ephone-dn  2
 number extension-number
!
!
ephone  1
 mac-address mac_address_ipphone1 (MMMM.MMMM.MMMM)
 type 7912
 button  1:1
!The previous line configures the button #1 to directory number 1
!
ephone  2
 mac-address mac_address_ipphone2 (MMMM.MMMM.MMMM)
 type 7912
 button  1:2
!The previous line configures the button #1 to directory number 2
!
ntp server ntp-server-address
```

```
!
dial-peer voice XXXX voip
 description OUTGOING CALLS
 destination-pattern X...
 session-target ipv4:external-voice-router-ip-address

end
```

Before proceeding with the configuration of the telephony service you must upload to the router flash the following file: **`CP7912080004SCCP080108A.sbin`** which is available for download from the ISEP ACADEMY network in the following address: http://172.16.208.100/Materiais/Files/CCNA4