LOMBA KOMPETENSI SISWA (LKS)
SEKOLAH MENENGAH KEJURUAN
TINGKAT KAB. TASIKMALAYA
TAHUN 2026

NASKAH SOAL
*(Terbuka/~~Tertutup~~)

Bidang Lomba
IT NETWORK SYSTEM ADMINISTRATION

1. DAFTAR ALAT

1.1. Daftar alat peserta

Alat yang dipersiapkan oleh peserta meliputi:

No	Alat Lomba	Spesifikasi	Jumlah
1	Komputer / Laptop	▪ RAM Minimal 16 GB ▪ HDD Minimal 128 GB ▪ Sistem Operasi Windows 10	1 Unit
2	UPS	UPS 230V 700Watt	1 Buah
3	Mouse	Standard	1 Buah
4	Keyboard	Standard	1 Buah

2. DAFTAR BAHAN

2.1. Bahan Penunjang

Bahan yang dipersiapkan oleh panitia atau juri meliputi:

No	Bahan / Aplikasi	Spesifikasi	Keterangan
Sistem Operasi & Aplikasi			
1	Sistem Operasi Linux	Debian 12.x DLBD	1 Buah
2	VMWare Workstation	VMWare Workstation 17	1 Buah
3	Cisco Packet Tracer	Packet Tracer **8.2**	1 Buah

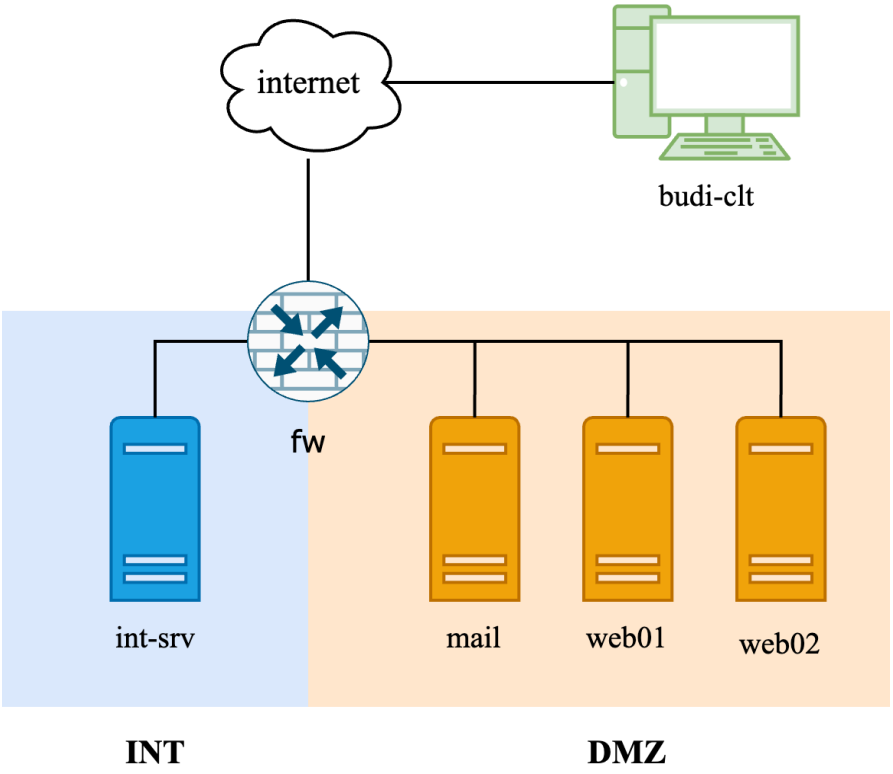
KISI-KISI SOAL

MODULE A
LINUX ENVIRONMENT

DESCRIPTION

This project presents a Linux-based network environment aimed at providing secure and efficient infrastructure management. The provided topology consists of distinct zones: Internal (INT) and Demilitarized Zone (DMZ), separated by a firewall to enforce security and access control policies. Key servers, such as internal services (int-srv), mail, and web servers (mail, web01, and web02), are strategically positioned based on their function and exposure level.

LOGICAL TOPOLOGY



TASK SUMMARY

Part 1 (INT - Internal) focuses on setting up the core infrastructure services on the internal server int- srv.itnsa.id using Debian 12. This includes configuring a DNS server with BIND9 to manage forward and reverse DNS zones for the domain itnsa.id, setting up an LDAP directory using slapd to manage centralized user accounts for email authentication, and creating a Certificate Authority (CA) with OpenSSL to issue trusted certificates for web and mail servers. These configurations ensure secure user authentication, reliable name resolution, and encrypted communications within the network.

Part 2 (DMZ - Demilitarized Zones) involves configuring public-facing services that are securely isolated from the internal network. This includes setting up a mail server (mail.itnsa.id) using Postfix and Dovecot to handle email for the domain itnsa.id, with LDAP-based authentication and TLS encryption using certificates issued by the internal CA. Additionally, two web servers (web-01 and web-02) are configured for high availability using Keepalived and HAProxy, distributing traffic to local Nginx servers. HTTPS is enforced with TLS termination at the HAProxy layer, and all services are validated to work through automation using Ansible from the internal server.

Part 3 (Firewall) focuses on securing and controlling traffic flow between the internal, DMZ, and external networks using the firewall server fw.itnsa.id. This server uses nftables to implement strict rules that allow only necessary traffic, such as internet access for internal and DMZ networks, NAT masquerading for outgoing connections, and port forwarding for web, mail, and DNS services. It also ensures secure remote access by configuring a VPN using WireGuard, allowing external clients to connect to internal resources. The firewall must also allow the mail server to communicate with the LDAP server while blocking all other unspecified traffic to maintain strong network segmentation and security.

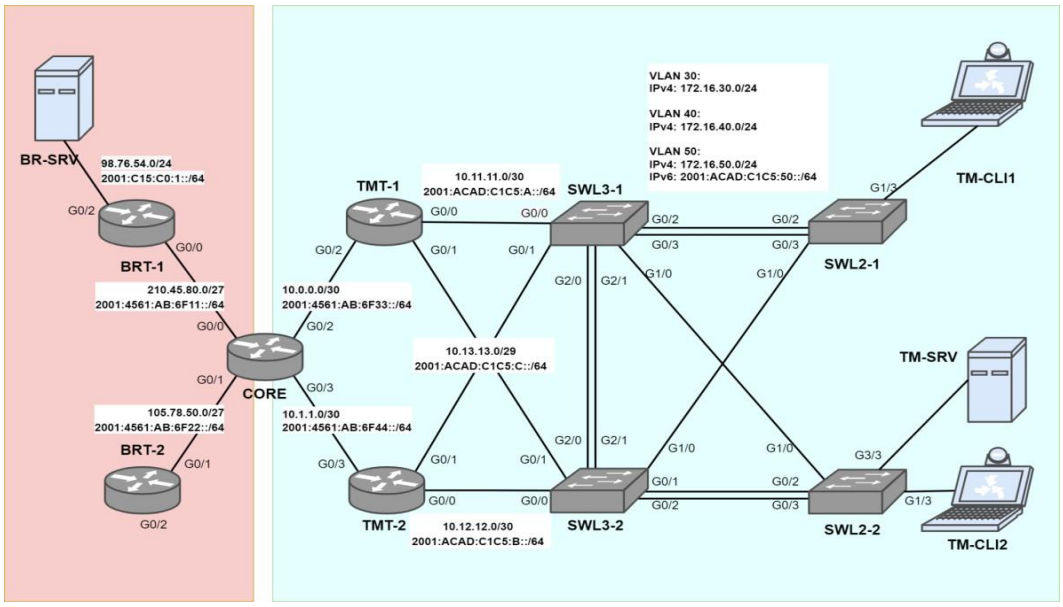
Part 4 (Client) focuses on configuring the client machine budi-clt.itnsa.id to validate the functionality of the entire network. This client represents a remote user who securely connects to internal and DMZ services through a WireGuard VPN. The setup includes creating a local user named budi with sudo access, configuring VPN connectivity to the firewall server fw.itnsa.id, and ensuring that the client can access internal and public services such as https://www.itnsa.id and https://www.int.itnsa.id with valid certificates. Additionally, the email client (e.g., Thunderbird) must be configured for budi.sudarsono@itnsa.id, allowing the user to send and receive email, completing end-to-end testing of DNS, email, VPN, and web services.

MODULE B
NETWORK SYSTEMS – CISCO PACKET TRACER

DESCRIPTION

You work as a Network Engineer at ITNSA.ID Corp. The company is currently rebuilding its network services from scratch. As a company that has branches in various regions, your job is to ensure that network access from one branch to another can run properly. You must ensure that the routing and switching services on each device are in accordance with the previously created design. Before you implement it on a real device, you are asked to simulate it first on Cisco Packet Tracer.

TOPOLOGY



TASK SUMMARY

The Network Systems module will use the Physical PKA mode. Competitors are asked to complete the module by configuring the device. Competitors do not have to use the cable console but may use the CLI. In this PKA mode, participants will not be allowed to see the score or check items, so participants must verify the configuration via the command.

- Basic Configuration
- L2 Switching
  - VLAN & Inter-VLAN Routing
  - EtherChannel
  - VTP
- L3 Routing
  - Static Routing
  - EIGRP
  - OSPF
- Services: NAT; FHRP; DHCP; SNMP; NTP
- Security
  - SSH
  - Port Security

TEST PROJECT

MODUL A – LINUX ENVIRONMENT

IT NETWORK SYSTEMS ADMINISTRATION

Introduction

This Linux Environment project is a practice setup to help you learn how to build and manage a secure computer network using Debian 12. You will configure different servers for specific roles: the internal server handles DNS, user login (LDAP), and digital certificates; the DMZ servers provide email and website services that can be accessed from the internet; the firewall server controls what traffic is allowed in and out, and also sets up a secure VPN connection; and the client computer is used to test everything—like checking if websites and email are working properly through the VPN. This project helps you understand how real companies manage and protect their networks.

Login

Username: root/user

Password: Skills39!

General Configuration

Fully Qualified Domain Name	Ipv4	Services
fw.itnsa.id	INT: 10.10.10.254/24, DMZ: 10.10.20.254/24, WAN: 100.100.100.254/24	VPN (wireguard), firewall (nftables)
int-srv.itnsa.id	INT: 10.10.10.10/24	DNS Server (bind9), LDAP (slapd), CA (openssl), ansible
mail.itnsa.id	DMZ: 10.10.20.10/24	Mail Server (postfix + dovecpt)
web-01.itnsa.id	DMZ: 10.10.20.21/24	Virtual IP(keepalived), HAProxy, Web Server
web-02.itnsa.id	DMZ: 10.10.20.22/24	Virtual IP(keepalived), HAProxy, Web Server
budi-clt.itnsa.id	WAN: 100.100.100.100/24	E-mail client, vpn client

Networking

To make your life a bit easier, networking has been preconfigured on all machines.

Notes

For the assessment process, we use a system that relies on the SSH service. Therefore, you are strictly prohibited from modifying the SSH configuration !!!

Part 1 INT (Internal)

The internal server int-srv.itnsa.id is responsible for providing core infrastructure services, including DNS, LDAP authentication, and certificate authority (CA) functions. This setup ensures centralized user management and secure communication across the network.

int-srv.itnsa.id

DNS

Set up a DNS server using BIND9 to manage domain names.

1. Install & Configure BIND9
2. Create DNS Zones
   - Create a forward zone for: itnsa.id
   - Create a reverse zone for the internal IP address range (for example: 10.10..)
3. Add DNS Records
   - Add forward and reverse records for all servers listed in the general configuration.
   - Add additional records to the table.

Type	Name	Value/Target
A	www	100.100.100.254
A	vrrp	10.10.20.100
CNAME	www.int	vrrp.itnsa.id
MX	@	10 mail.itnsa.id

LDAP

Install and configure LDAP using slapd to manager user accounts. These users will be used to log in to the mail server.

1. Install LDAP use slapd
2. Create LDAP users
   - Create the following users in LDAP. These users will be used for email login (authentication)

Full Name	Username (uid)	Password	Organizational Unit (OU)	Email Address
Administrator	admin	Skills39!	-	-
Boaz Salossa	boaz	Skills39!	Employees	boaz.salossa@itnsa.id
Budi Sudarsono	budi	Skills39!	Employees	budi.sudarsono@itnsa.id

CA

Use OpenSSL to create your own Certificate Authority (CA) and generate certificates for your server (web and mail).

1. Create Root CA
   - Make a Root CA with the name: “ITNSA Root CA”
   - For other fields like Country, State, etc., you can use any value.

- Add attributes
  X509v3 Key Usage: critical
  Certificate Sign
  X509v3 Basic Constraints: critical
  CA:TRUE
- Install ITNSA Root CA on every servers and clients

2. Create Certificates for Servers
   - Generate and sign the following certificates directly using the Root CA:
   - A certificate for the web server, valid for: www.itnsa.id, www.int.itnsa.id
   - A certificate for the mail server, valid for mail.itnsa.id
3. Save All Certificates
   - Save the certificates in this folder: /opt/grading/ca
     - ca.pem: Root CA certificate
     - web.pem: Web server certificate
     - mail.pem: Mail server certificate

Ansible

We will set up Ansible on the server int-srv and make it control server web-02. All ansible file (settings, playbooks, and modules) must be saved in the /etc/ansible directory.

1. Create playbook 01-user.yml
   - This playbook will create a new user on the server
   - Set password Skills39!, but for the username, we will use variables, so they can be changed easily
   - Make the playbook idempotent
   - To run the playbook, use this command:

     ```
     ansible-playbook /etc/ansible/01-user.yml -e user_name=developer
     ```
2. Create playbook 02-web-int.yml
   - This playbook will install Nginx
   - It will also create a virtual host that listens on port 8081
   - When you open the website, it will show the message: “This is web internal”
   - Make the playbook idempotent
   - To run the playbook, use this command:

     ```
     ansible-playbook /etc/ansible/02-web-int.yml
     ```

Part 2 DMZ (Demilitarized Zones)

The DMZ zone hosts public-facing services such as the mail server and high-availability web servers. These servers are isolated from internal systems but must securely communicate with them for functions like LDAP authentication and certificate verification.

mail.itnsa.id

Mail Server

Set up a mail server using Postfix and Dovecot so users can send and receive emails for the domain itnsa.id.

1. Install Mail Server Software
    - Postfix (for sending and receiving emails)
    - Dovecot (for letting users read their emails)
2. Mail Server Configuration
    - The mail server must send and receive emails for the domain: itnsa.id
    - Users should be able to read their emails using IMAP
    - All connections between email clients and the server must use TLS (encryption):
        - If you finished the “CA” (Certificate Authority) task, use the certificate you made for the mail server.
        - If not, create a self-signed certificate.
    - Make sure clients that trust “ITNSA Root CA” can verify the certificate.
3. LDAP Integration (User Login)
    - Configure the folder Maildir for user budi and boaz
    - Make sure the LDAP user named budi (created in the LDAP task) can:
        - Log in using his username(uid)
        - Access his email inbox
    - The email address should be taken from his mail field in LDAP.
    - Test email budi can send email to himself using mailutils

web-01.itnsa.id & web-02.itnsa.id

HA Web

Set up a high-availability reverse proxy system using HAProxy and Keepalived on two servers: web-01 and web-02.

1. Keepalived Configuration (Virtual IP)
    - Create a virtual IP (10.10.20.100/24) that will automatically move to the backup server if the main server goes down.
    - web-01: acts as the MASTER with priority 101
    - web-02: acts as the BACKUP with priority 100
2. HAProxy Configuration for Load Balancing
    - Install and configure HAProxy on both servers (web-01 and web-02) to distribute traffic to two Nginx web servers:
        - web-01: 10.10.20.21:8080
        - web-02: 10.10.20.22:8080
    - All HTTP requests must be redirected to HTTPS.
    - HAProxy should perform TLS termination (HAProxy handles HTTPS and forwards to Nginx using HTTP).

- Add an HTTP header via-proxy: hostname to responses (replace “hostname” with the proxy’s hostname) to help with troubleshooting.
- If you already have a certificate from your CA, use the web certificate (web.pem).
    - Make sure a client that only trusts your root CA can validate the entire certificate chain.
    - If not, create a self-signed certificate.

3. Web Server nginx
    - On web-01 and web-02, install nginx and listen on port 8080 with index.html “Hello from ${hostname}

Part 3 Firewall

The firewall server fw.itnsa.id acts as a secure gateway for internal and DMZ networks. It is responsible for controlling traffic flow, providing internet access, forwarding services, and securing VPN connectivity.

fw.itnsa.id

nftables

Create firewall and NAT rules using nftables to control which traffic is allowed or blocked in your network.

1. Allow Internet Access
   - Devices in the INT (internal) and DMZ networks can access the internet.
2. NAT Masquerade
   - When sending traffic from your network to the internet (through the WAN), the firewall must replace the source IP with its own WAN IP using masquerade NAT.
3. Port Forwarding
   - Forward incoming traffic from the internet to servers in the DMZ:

Port	Protocol	Forward To
80	TCP	10.10.20.100
443	TCP	10.10.20.100
53	TCP/UDP	10.10.10.10

4. VPN Access
   - VPN clients should be able to reach both internal and DMZ networks.
5. Mail Server to LDAP
   - The mail server must be allowed to query the LDAP service running on int-srv01.
6. Block Everything Else
   - Any other traffic that's not mentioned above should be blocked (default deny).

Wireguard VPN

Set up WireGuard as a VPN server so that an external workstation (client) can connect securely to the internal network.

1. Secure VPN Connection
   - Use WireGuard to create a secure tunnel from the client to the internal network.
   - All internet traffic from the client should be routed through the VPN tunnel.
2. Pre-Shared Key (PSK)
   - For extra security, add a pre-shared key to the tunnel (used along with public/private keys).
3. DNS Configuration
   - The client should use the internal DNS server (not public DNS) to resolve hostnames while connected.
4. IP Addressing
   - Use the IP range for the tunnel based on the General Configuration Table (ask or check your given network setup).
5. Save & Enable Configuration
   - Save the WireGuard config as:
     /etc/wireguard/wg0.conf

- Start it using:
  sudo wg-quick up wg0

- Enable it to run at boot (system service):
  sudo systemctl enable wg-quick@wg0

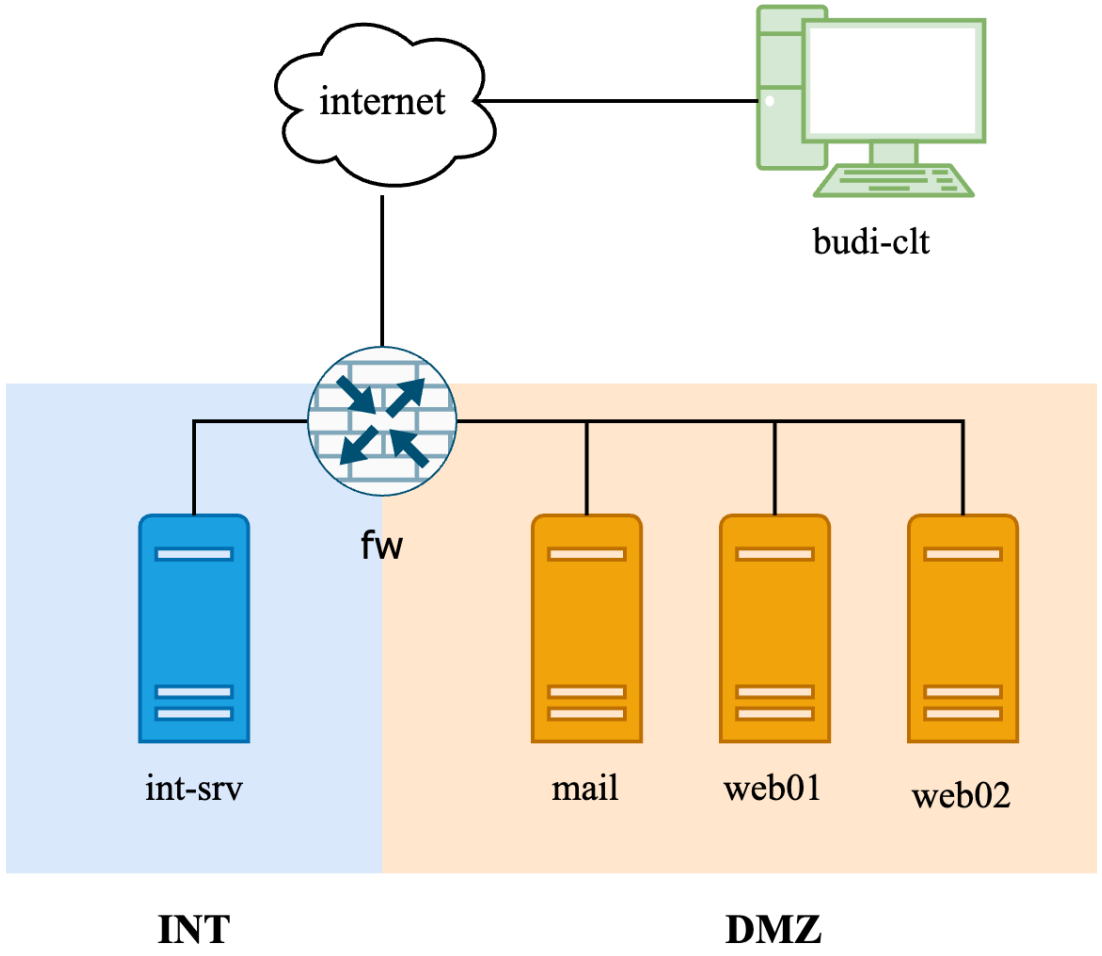
Part 4 Client

The client machine budi.itnsa.id represents a remote workstation that connects securely to internal and DMZ services through VPN. It is used to validate the overall infrastructure by testing access to web, DNS, and email services.

General Configuration

1. Create a new local user budi (Budi Sudarsono), with the password “Skills39!”
   - Make user budi can sudoer without a password
2. Configure VPN WireGuard to fw.itnsa.id
   - Save the WireGuard config as:
     /etc/wireguard/wg0.conf
   - Start it using:
     sudo wg-quick up wg0
   - Enable it to run at boot (system service):
     sudo systemctl enable wg-quick@wg0
3. Can access https://www.itnsa.id via internet, and https://www.int.itnsa.id via vpn without getting errors certificate
4. Set up e-mail budi.sudarsono@itnsa.id in Thunderbird, and can send to himself

Topology



Clarification

Wireguard VPN

for ip address use:
fw: 10.100.100.254/24
budi-clit: 10.100.100.2/24

TEST PROJECT

MODUL – NETWORK SYSTEMS

IT NETWORK SYSTEMS ADMINISTRATION

Introduction

Network technology knowledge is becoming essential nowadays for people who want to build a successful career in any IT engineering field. This test project contains a lot of challenges from real life experience, primarily IT integration and IT outsourcing. If you can complete this project with the high score, you are ready to service the network infrastructure for any multi-branch enterprise.

Description of project and tasks

This test project is designed using a variety of network technologies that should be familiar from the Cisco certification tracks. Tasks are broken down into following configuration sections:

Basic Configuration

- Switching
- Routing
- Services
- Security

All sections are independent but all together they build very complex network infrastructure. Some tasks are simple and straightforward; others may be tricky.

Instructions to the Competitor

Your configuration will be marked with scripts, so therefore we need two important basic configurations:

1. no ip domain-lookup
2. exec-timeout 0 0 on console

Basic Configuration

1. Configure device hostname according to the topology.
2. Configure domain name to “lks2025.id” on all devices.
3. Configure privileged mode password “P@ssw0rd” on all devices.
4. Create user “admin” with password “P@ssw0rd” with maximum privilege.
5. Configure IPv4 and IPv6 address on all devices according to the addressing table.
6. Display banner “Unauthorized Access is Strictly Prohibited” before user authentication on all devices. Use ‘!’ as the delimiting character.

Switching

1. Configure link aggregation on DC switches refer to the list below. The L3 switches must act as a negotiator to perform link aggregation if using negotiation protocol, meanwhile other switch must be configured as the responder.
   a. SWL3-1 (channel 1) <=> SWL2-1 (channel 1) protocol using open-standard protocol
   b. SWL3-1 (channel 2) <=> SWL3-2 (channel 2) without using any negotiation
   c. SWL3-2 (channel 3) <=> SWL2-2 (channel 3) using Cisco proprietary protocol
2. Configure VTP version 2 with SWL3-1 as the VTP Server. Other switches must be configured as VTP client. Use VTP Domain **lks2025.id** and VTP Password **P@ssw0rd** Configure VLAN on the VTP server:
   - VLAN 30 (MANAGEMENT)
   - VLAN 40 (INTERNAL)
   - VLAN 50 (SERVER)
   - VLAN 99 (NATIVE)
3. Configure port connected to the end device as the access port and enable portfast feature on the port. Refer to Topology Diagram for VLAN Access.
4. Configure all port channel interface as the trunk port and only allow the created VLAN to be passed. Configure VLAN 99 as the Native VLAN.

Routing

1. Configure EIGRP routing IPv4 on TM Sites with AS 10.
   a. Advertise network VLANS 30, 40 and 50 on SWL3.
   b. Make sure both TM routers can access all internal networks.
   c. Configure passive interface on an interface that does not require EIGRP updates.
   d. Configure Router ID
      - TMT-1 : 21.21.21.21
      - TMT-2 : 22.22.22.22
      - SWL3-1 : 23.23.23.23
      - SWL3-2 : 24.24.24.24
2. Configure OSPF Routing IPv4 on the CORE and other routers connected to CORE Router with process ID 10.
   a. Advertise all installed networks including interface loopback except Internal TMT network (only network connected to CORE Router).
   b. Configure the passive interface on the interface connected to SWL3.
   c. Configure Router ID
      - BRT-1 : 1.1.1.1
      - BRT-2 : 8.8.8.8

- CORE : 9.9.9.9
- TMT-1 : 2.2.2.2
- TMT-2 : 3.3.3.3

3. Configure default route on SWL3-1 to TMT-1 and SWL3-2 to TMT-2. Use directly connected static route (exit interface).

Services

1. Configure Network Address Translation IPv4
   a. Configure dynamic port translation on TMT-1 and TMT-2 for the LAN subnet. VLAN 30, 40 and 50 IPv4 addresses are translated into IPv4 address of interface connected to the CORE. Create ACL with name VLANS to define source network.
2. Configure FHRP on TM site.
   a. Configure HSRP IPv4 version 2 on TM for VLAN 30, VLAN 40 and VLAN 50 with group number same as the VLAN number.
      - SWL3-1 should be as forwarding packet for VLAN 30 and VLAN 50
      - SWL3-2 should be used as forwarding packet for VLAN 40.
   b. Use the last Host IP of each VLAN as the virtual Router IP.
3. Configure DHCP service for TM site.
   a. Configure DHCPv4 on TMT-2 Router for client on both TM VLANs (VLAN30 & VLAN40).
   b. The IP range available for both pools is only 100 Host IPs from 101 to 200.
   c. Use the virtual IP Router from FHRP as a gateway.
   d. Use TM-SRV as DNS Server.
   e. Make sure both TM clients get IP from TMT-2 router.
4. All Router devices must be synchronizing its time with BR-SRV.

Security

1. Configure SSH version 2 on both TMT-1 and TMT-2 devices.
   a. Use local authentication
   b. Only allow SSH traffic from 172.16.30.0/24 (use SSH as ACL Name)
3. Configure port security on SWL2-1 and SWL2-2 switch that is connected to hosts. Permit maximum 2 MAC Address and save those MAC address on running-config. In case of policy violation, the port should not be err-disabled but only save to syslog.

Addressing Table

DEVICE	INTERFACE	ADDRESS
CORE	Ser0/1/0	210.45.80.1/27 2001:4561:AB:6F11::1/64
	Ser0/1/1	105.78.50.1/27 2001:4561:AB:6F22::1/64
	Ser0/0/0	10.0.0.1/30 2001:4561:AB:6F33::1/64
	Ser0/0/1	10.1.1.1/30 2001:4561:AB:6F44::1/64
BRT-1	Ser0/1/0	210.45.80.2/27 2001:4561:AB:6F11::2/64
	GigabitEthernet0/2	98.76.54.1/24 2001:C15:C0:1::1/64
	Loopback1	1.1.1.1/32
BRT-2	Ser0/1/1	105.78.50.2/27 2001:4561:AB:6F22::2/64
	Loopback1	8.8.8.8/32
BR-SRV	Ethernet0	98.76.54.10/24 2001:C15:C0:1::10/64
TMT-1	GigabitEthernet0/1	10.11.11.1/30 2001:ACAD:C1C5:A::1/64
	GigabitEthernet0/2	10.13.13.1/29 2001:ACAD:C1C5:C::1/64
	Ser0/0/0	10.0.0.2/30 2001:4561:AB:6F33::2/64
TMT-2	GigabitEthernet0/1	10.12.12.1/30 2001:ACAD:C1C5:B::1/64
	GigabitEthernet0/2	10.13.13.2/29 2001:ACAD:C1C5:C::2/64
	Ser0/0/1	10.1.1.2/30 2001:4561:AB:6F44::2/64
SWL3-1	GigabitEthernet0/1	10.11.11.2/30
	GigabitEthernet0/2	10.13.13.4/29
	VLAN30	172.16.30.1/24
	VLAN40	172.16.40.1/24

DEVICE	INTERFACE	ADDRESS
	VLAN50	172.16.50.1/24
SWL3-2	GigabitEthernet0/1	10.12.12.2/30
	GigabitEthernet0/2	10.13.13.3/29
	VLAN30	172.16.30.2/24
	VLAN40	172.16.40.2/24
	VLAN50	172.16.50.2/24
SWL2-1	VLAN30	172.16.30.11/24
SWL2-2	VLAN30	172.16.30.12/24
TM-CLI1	Ethernet0	DHCP
TM-CLI2	Ethernet0	DHCP
TM-SRV	Ethernet0	172.16.50.10/24 2001:ACAD:C1C5:50::10/64

Network Topology