Balai Pengembangan Talenta Indonesia
Pusat Prestasi Nasional
Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi

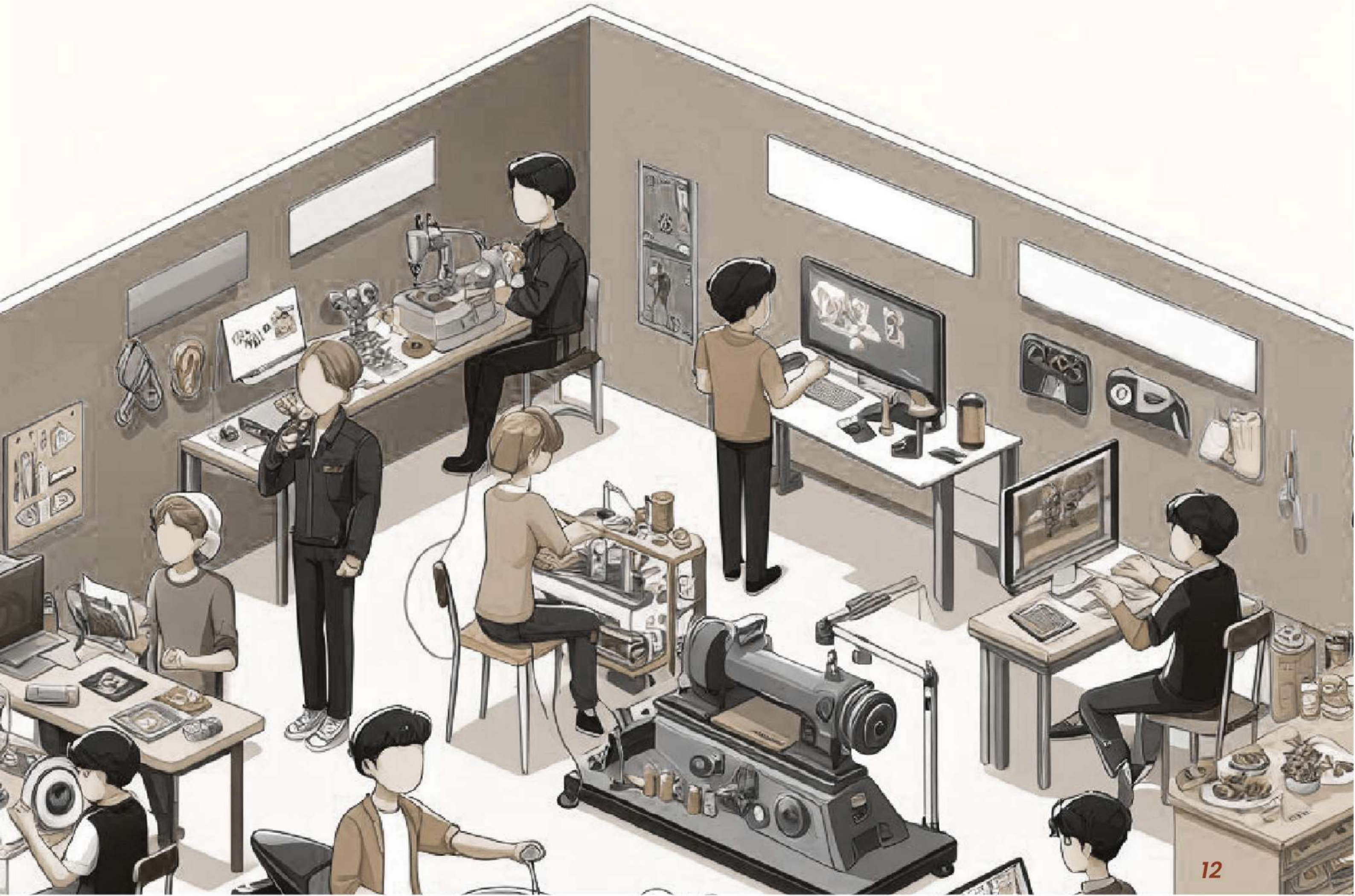
MERDEKA BELAJAR

LKS SMK
TINGKAT NASIONAL

SMK

Soal Lomba Kompetensi Siswa Nasional 2024

Teknologi Informasi Sistem Administrasi Jaringan *(IT Network System Administration)*



MERDEKA BERPRESTASI
Talenta Vokasi Menginspirasi

ACTUAL TEST PROJECT
MODUL D – NETWORK SYSTEMS

IT NETWORK SYSTEMS ADMINISTRATION

LOMBA KOMPETENSI SISWA SMK
TINGKAT NASIONAL 2024

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

Equipment, machinery, installations, and materials required

It is expected that all Test Projects can be completed by Competitors based on the equipment and materials specified in the Infrastructure List. Server VMs on this test project are preconfigured with following roles and service.

VIRTUAL MACHINE	ROLES/SERVICES	CREDENTIALS
BR-SRV	NTP	root/ P@ssw0rd!
TM-SRV	SNMP, DNS, WEB, Cacti	root/ P@ssw0rd!
TMCL1, TMCL2	Client	user/P@ssw0rd!

Basic Configuration

1. Configure device hostname according to the topology.
2. Configure domain name to “lksn2024.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.
7. Configure device timezone to GMT+7 on all devices.

Switching

1. Configure VTP version 3 on all switches. Configure SWL3-1 as the VTP Server. Other switches must be configured as VTP client. Configure VLAN on the VTP server:
   - VLAN 30 (MANAGEMENT)
   - VLAN 40 (INTERNAL)
   - VLAN 50 (SERVER)
   - VLAN 99 (NATIVE)
2. 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
3. Configure port connected to the end device as the access port and enable portfast feature on the port.
4. Configure port connected to the switch as the trunk port and only allow the created VLAN to be passed. Disable negotiation protocol and make sure frame that is passed through this trunk port is tagged using open-standard protocol. Configure VLAN 99 as the Native VLAN.

Routing

1. Configure EIGRP routing IPv4 on TM Sites.
   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.
2. Configure OSPF Routing IPv4 on the ISP and other Routers connected to it.
   a. Advertise all installed networks including interface loopback except Internal TMT network (only network connected to ISP Router).
   b. Configure the passive interface on the interface connected to SWL3.
3. Configure default route on SWL3-1 to TMT-1 and SWL3-2 to TMT-2.

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 ISP.
2. Configure FHRP on HQ site and BR1 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. Configure SNMP to monitor TMT-1 and TMT-2. SNMP server pre-configured on TM-SRV
   a. Set contact to admin@lksn2024.id
   b. Set location to **Jakarta, Indonesia**
   c. Use SNMPv3 with username **netmon** and password **Skill39!**
   d. Cacti monitoring server is pre-configured on TM-SRV. You can use it to check whether SNMP is working correctly or not via **http://monitor.lksn2024.id** (username: admin, password: P@ssw0rd)
5. Configure NTP on all network devices. All network 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. User with maximum privilege must be set to privileged mode after login.
   c. Only allow SSH traffic from 172.16.30.0/24

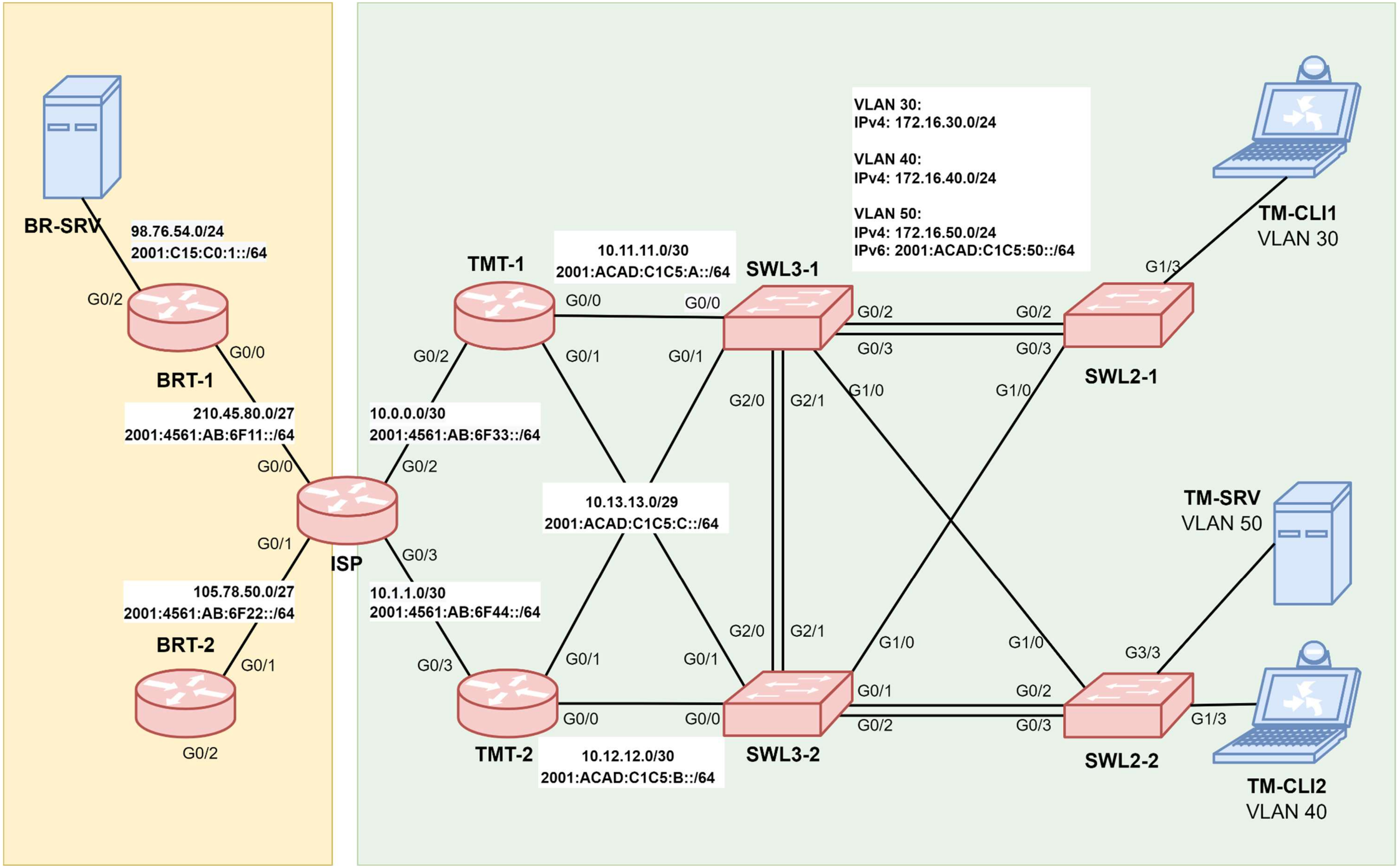
3. Configure port security on SWL2-1 and SWL2-2 switch that is connected to hosts. Permit maximum 2 MAC Address and save those MAC address on running-config. In case of policy violation, the port should not be err-disabled but only save to syslog.

Addressing Table

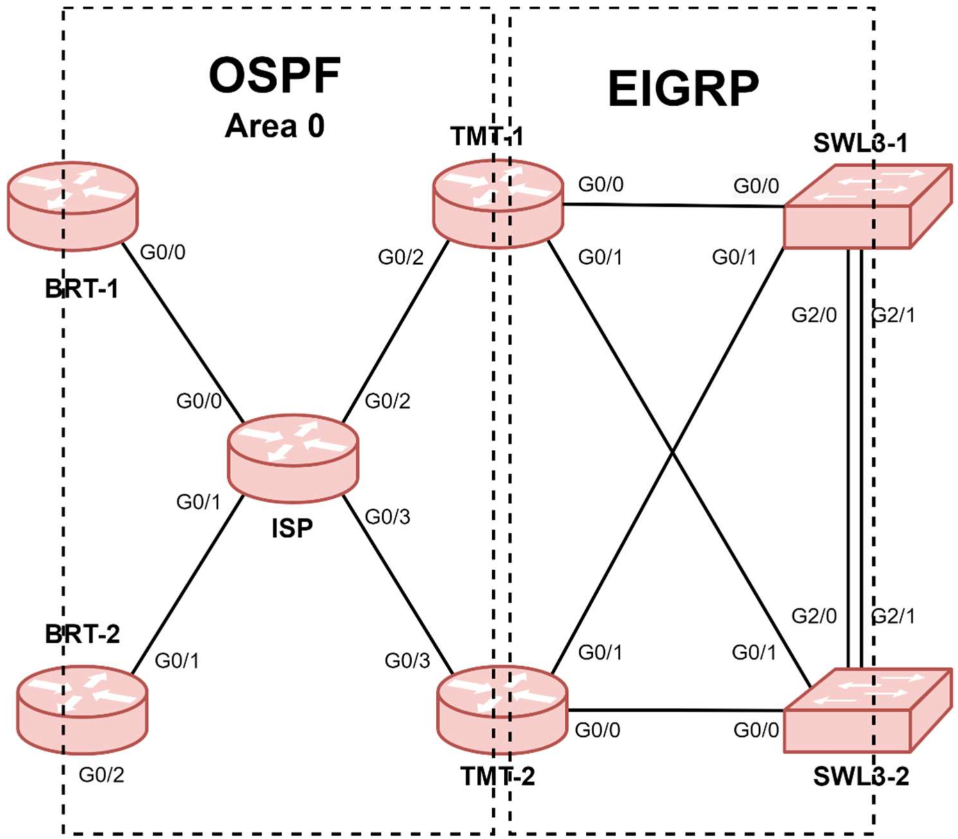
DEVICE	INTERFACE	ADDRESS
ISP	GigabitEthernet0/0	210.45.80.1/27 2001:4561:AB:6F11::1/64
	GigabitEthernet0/1	105.78.50.1/27 2001:4561:AB:6F22::1/64
	GigabitEthernet0/2	10.0.0.1/30 2001:4561:AB:6F33::1/64
	GigabitEthernet0/3	10.1.1.1/30 2001:4561:AB:6F44::1/64
BRT-1	GigabitEthernet0/0	210.45.80.2/27 2001:4561:AB:6F11::2/64
	GigabitEthernet0/2	98.76.54.1/24 2001:C15:C0:1::1/64
	Loopback1	1.1.1.1/32
BRT-2	GigabitEthernet0/1	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	GigabitEthernet0/0	10.11.11.1/30 2001:ACAD:C1C5:A::1/64
	GigabitEthernet0/1	10.13.13.1/29 2001:ACAD:C1C5:C::1/64
	GigabitEthernet0/2	10.0.0.2/30 2001:4561:AB:6F33::2/64
TMT-2	GigabitEthernet0/0	10.12.12.1/30 2001:ACAD:C1C5:B::1/64
	GigabitEthernet0/1	10.13.13.2/29 2001:ACAD:C1C5:C::2/64
	GigabitEthernet0/3	10.1.1.2/30 2001:4561:AB:6F44::2/64
SWL3-1	GigabitEthernet0/0	10.11.11.2/30

		2001:ACAD:C1C5:A::2/64
	GigabitEthernet0/1	10.13.13.4/29 2001:ACAD:C1C5:C::4/64
	VLAN30	172.16.30.1/24
	VLAN40	172.16.40.1/24
	VLAN50	172.16.50.1/24 2001:ACAD:C1C5:50::1/64
SWL3-2	GigabitEthernet0/0	10.12.12.2/30 2001:ACAD:C1C5:B::2/64
	GigabitEthernet0/1	10.13.13.3/29 2001:ACAD:C1C5:C::3/64
	VLAN30	172.16.30.2/24
	VLAN40	172.16.40.2/24
	VLAN50	172.16.50.2/24 2001:ACAD:C1C5:50::2/64
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



Routing Diagram


OSPF
Area 0
EIGRP
BRT-1
G0/0
BRT-2
G0/1
G0/2
ISP
G0/0
G0/1
G0/2
G0/3
TMT-1
G0/2
G0/0
G0/1
TMT-2
G0/3
G0/1
G0/0
SWL3-1
G0/0
G0/1
G2/0
G2/1
SWL3-2
G2/0
G2/1
G0/1
G0/0