PRA TEST PROJECT
MODUL D - NETWORK SYSTEMS

IT NETWORK SYSTEMS ADMINISTRATION

KELOMPOK INFORMATION AND COMMUNICATION TECHNOLOGY

Dokumen ini merupakan Pra-Test Project yang menjadi subject perubahan maksimal 30% untuk Actual Test Project. Pelaksanaan kompetisi LKS Nasional nanti akan menggunakan Actual Test Project yang akan dipublikasi pada saat kompetisi. Perubahan itu meliputi Topology, Functionality, Aplikasi dan Task yang diminta.

Introduction

NeWaduhtwork 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 are able to complete this project with a high score, you are definitely 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
- WAN and VPN

All sections are independent but all together they build very complex network infrastructure. Some tasks are pretty simple and straightforward; others may be tricky. You may see that some technologies are expected to work on top of other technologies. For example, IPv6 routing is expected to run on top of configured VPNs, which are, in turn, expected to run on top of IPv4 routing, which is, in turn, expected to run on top of PPPoE, and so on. It is important to understand that if you are unable to come up with a solution in the middle of such a technology stack it doesn't mean that the rest of your work will not be graded at all. For example, you may not configure IPv4 routing that is required for VPN because of IP reachability but you can use static routes and then continue to work with VPN configuration and everything that runs on top. You won't receive points for IPv4 routing in this case but you will receive points for everything that you made operational on top as long as functional testing is successful.

Instructions Notice 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

Both configurations are already preconfigured on all switches and routers, so do not change these configurations.

Instructions to the Competitor

1. Read all tasks in each section before proceeding with any configuration. The completion of any item may require the completion of any previous or later item.
2. Points are awarded for working configurations only. Test the functionality of all the requirements before you submit the test project. Be careful, because as you configure one part, you may break a previous requirement or configuration.
3. No partial points can be granted for any aspect; all requirements need to be fulfilled to receive the points for the aspect. Some requirements depend on other aspect's requirements, either before or after the current aspect.
4. Save your configurations frequently; accidents do and will happen.
5. All virtual machines are pre-installed. Use admin\Skill39 local credentials to access windows virtual machines and root\Skill39 to access linux virtual machines. Do not change these passwords.
6. Hosts are preconfigured but check the configuration and change it when necessary.
7. Please use industrial best practice where possible!

Basic configuration

1. Configure hostnames for all network devices as you see on the topology.
2. Configure domain name **lks2023.id** for all network devices on the topology.
3. Configure **Skill39** as a privileged mode password for all devices.
4. Only PBKDF2 hash of the password should be stored in configuration.
5. Configure IPv4/IPv6 address for all network devices as you see on the topology.
6. Configure GMT +7 as a timezone for all network devices.

Switching

1. Configure VTP on all switches to synchronize VLANs. It should be possible to modify VLAN database only from L3SW-1, and VLAN databases of all the other switchies should be synchronized from L3SW-1. VLAN database on all switches should contain following VLANs.
    a. VLAN 10 with name SRV
    b. VLAN 20 with name CLI
2. Configure all links between switches as trunk port.
    a. Do not use dynamic negotiation protocol.
    b. Configure manual pruning so that only created VLANs are allowed forwarding.
3. Configure EtherChannel between switches.
    a. Use following port-channel numbers:
        i. 1 - between switches L3SW-1 and L3SW-2
        ii. 2 - between switches L3SW-1 and L2SW-1
        iii. 3 - between switches L3SW-2 and L2SW-2
    b. The aggregated channel between L3SW-1 and L3SW-2 do not use dynamic negotiation protocol.
    c. The aggregated channel between L3SW-1 and L2SW-1 use a Cisco proprietary protocol for dynamic negotiation.

   d. The aggregated channel between L3SW-2 and L2SW-2 use a standard protocol for dynamic negotiation.
   e. L3SW-1 and L3SW-2 should initiate negotiation and the other devices should respond but don’t initiate.
   f. Configure the load balancing and forwarding method with source and destination MAC address.
4. Spanning tree configuration.
   a. L3SW-1 should be root bridge of VLAN10. If L3SW-1 goes down L3SW-2 should take over as the root bridge.
   b. L3SW-2 should be root bridge of VLAN20. If L3SW-2 goes down L3SW-1 should take over as the root bridge.
   c. The traffic from ES-CLI should pass through L3SW-1.
   d. Configure port which is connected to end device so that it immediately begins forwarding when connected.

Routing

1. Configure FHRP on L3SW1 and L3SW2.
   a. Use Hot Standby Router Protocol v2 for VLAN 10.
      i. L3SW1 should be used as the default gateway.
      ii. Use 104 as the group number of IPv4, and 106 as the group number of IPv6.
      iii. Use 192.168.10.254 as virtual IPv4 address and 2001:624C:3201:10::254 as virtual IPv6 address.
   b. Use a Hot Standby Router Protocol v2 for VLAN 20.
      i. L3SW2 should be used as the default gateway.
      ii. Use 204 as the group number of IPv4, and 206 as the group number of IPv6.
      iii. Use 192.168.20.254 as virtual IPv4 address and 2001:624C:3201:20::254 as Virtual IPv6 address.
2. Configure default route to ISP on both EST-1 and EST-2.
3. Configure OSPF.
   a. Use OSPF area 0 and instance number 11.
   b. Advertise only Public IP on all routers.
   c. Advertise the default route to the OSPF neighbour.
   d. Configure OSPF so that routing updates are not sent into networks where they are not required.

Services

1. Configure DHCP
   a. ES-CLI can obtain IP address automatically.
   b. All DHCP client should use WS-SRV as DNS Server.
2. Configure NAT
   a. When ES-CLI communicate with internet, these IP address should be translated to 103.76.14.1 - 103.76.14.10
3. Configure remote monitoring using SNMP
   a. Configure device location Surabaya, Indonesia
   b. Configure system contact admin@lksn2023.id

    c. Cacti monitoring server is pre-configured on ES-SRV. You can use it to check weather SNMP is working correctly or not via http://192.168.10.1/cacti (username: admin, password: Skill39)
    d. In Cacti, you must to configure templates for EST-1 and EST-2.
4. Configure ISP as NTP server. All network devices should synchronize time from ISP.

Security

1. Configure hostnames for all network devices as you see on the topology
2. Configure SSH version 2 for remote access on EST-1 and EST-2.
    a. Use RADIUS server for authentication.
        i. UseHQ-SRVasRADIUSserver.
        ii. Use Skill39 as the shared key.
        iii. Test RADIUS authentication using following users with password Skill39:
            - username user1 with maximum priviledge level
            - username user2 with priviledge level 5
    b. User user2 should be able to configure any interface IP settings and administratively enable or disable any of these interfaces.
    c. If RADIUS server goes down, use local account as backup authentication method.
    d. Ensure only ES-CLI is allowed to access via SSH.
3. Configure port-security on the port which is connected to ES-CLI using following parameters:
    a. Maximum MAC address – 2
    b. In case of policy violation, security message should be displayed on the console, port should be disabled.
    c. Recover disabled port after 3 minutes.

VPN

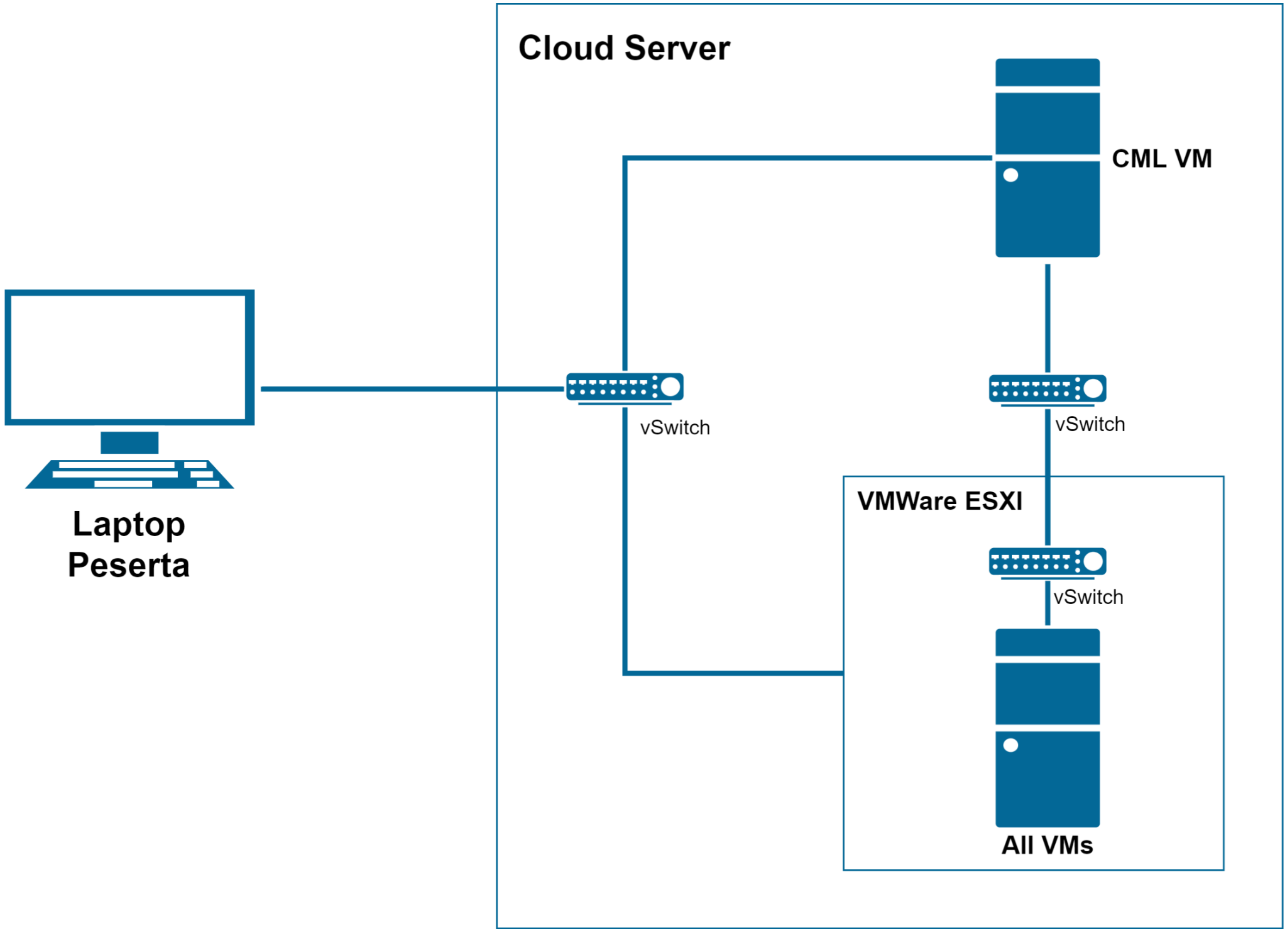
1. Configure a site to site VPN connection between EST-1 and WST-1
    a. Use tunnel0 interface
    b. Use IKEv2

Configure Table

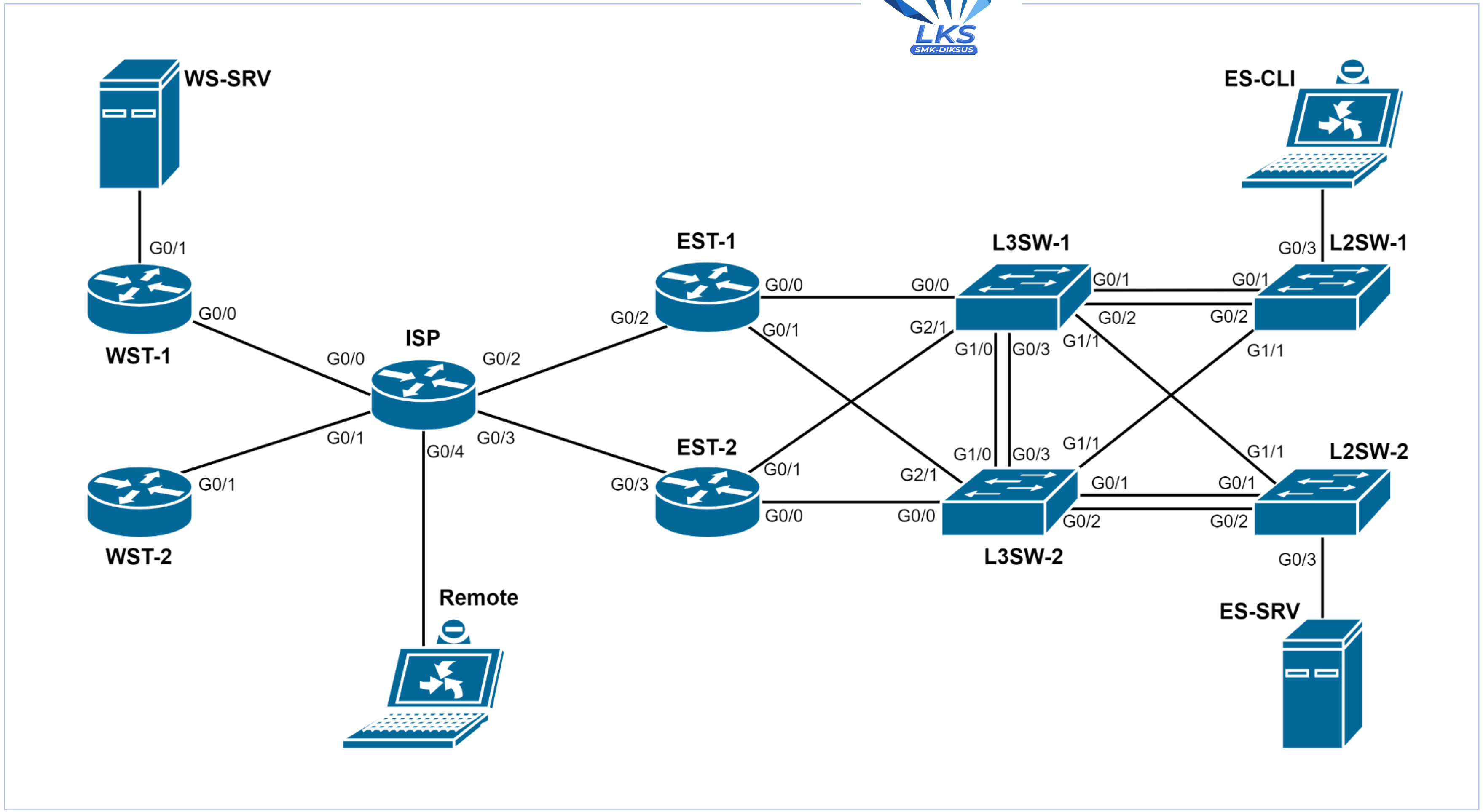
Site	Device	Interface	Address
Internet	ISP	GigabitEthernet0/0	3.0.180.254/24
		GigabitEthernet0/1	3.0.190.254/24
		GigabitEthernet0/2	13.228.27.254/24
		GigabitEthernet0/3	13.229.28.254/24
		GigabitEthernet0/4	194.233.70.254/24
	Remote	Ethernet 0	194.233.70.101/24
WEST	WST-1	GigabitEthernet0/0	3.0.180.201/24
		GigabitEthernet0/1	10.0.0.254/24
	WST-2	GigabitEthernet0/0	3.0.190.202/24
	WS-SRV	Ethernet 0	10.0.0.101/24
EAST	EST-1	GigabitEthernet0/0	11.11.11.2/30
		GigabitEthernet0/1	12.12.12.2/30
		GigabitEthernet0/2	13.228.27.200/24
	EST-2	GigabitEthernet0/0	11.11.11.6/30
		GigabitEthernet0/1	12.12.12.6/30
		GigabitEthernet0/3	13.229.28.200/24
	L3SW-1	GigabitEthernet0/0	11.11.11.1/30
		GigabitEthernet2/1	12.12.12.5/30
		Vlan 10	192.168.10.253/24
		Vlan 20	192.168.20.253/23
	L3SW-2	GigabitEthernet0/0	11.11.11.5/30
		GigabitEthernet2/1	12.12.12.1/30
		Vlan 10	192.168.10.252/24
		Vlan 20	192.168.20.252/23

	L2SW-1	Vlan 10	192.168.10.200/24
	L2SW-2	Vlan 10	192.168.10.201/24
	ES-CLI		192.168.20.x/24 (DHCP)
	ES-SRV		192.168.10.1/24

Physical Diagram



Network Topology


WS-SRV
G0/1
WST-1
G0/0
G0/0
ISP
G0/2
G0/1
G0/1
WST-2
G0/4
G0/3
Remote
EST-1
G0/2
G0/0
G0/1
EST-2
G0/3
G0/1
G0/0
L3SW-1
G0/0
G2/1
G1/0
G0/3
G1/1
G0/1
G0/2
L3SW-2
G0/0
G2/1
G1/0
G0/3
G1/1
G0/1
G0/2
ES-CLI
G0/3
L2SW-1
G0/1
G0/2
G1/1
L2SW-2
G1/1
G0/1
G0/2
G0/3
ES-SRV

.