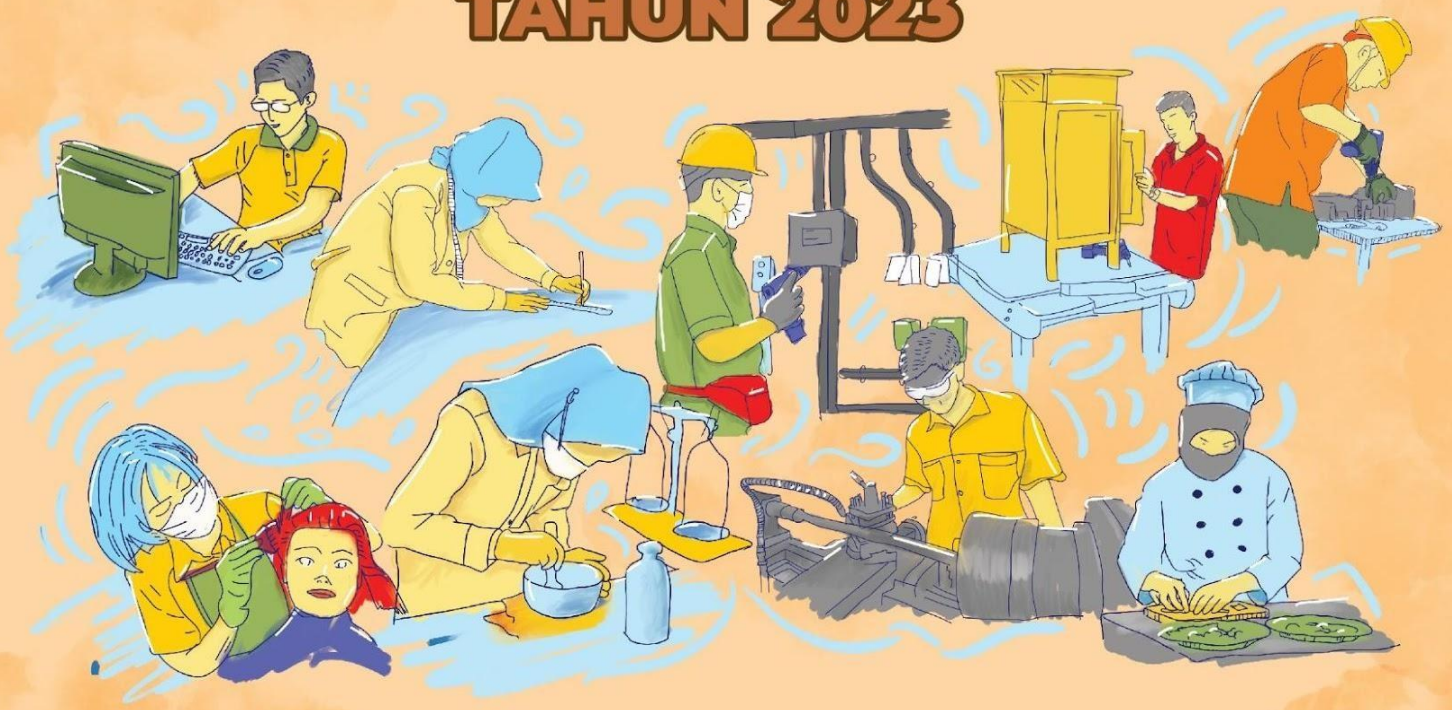
BALAI PENGEMBANGAN TALENTA INDONESIA
PUSAT PRESTASI NASIONAL
SEKRETARIAT JENDERAL
KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI

MERDEKA BELAJAR

LKS SMK-DIKSUS

SOAL

LOMBA KOMPETENSI SISWA SMK TINGKAT NASIONAL TAHUN 2023



BIDANG LOMBA

Teknologi Informasi Sistem Administrasi Jaringan

(IT Network System Administration)

MERDEKA BERPRESTASI
Talenta Vokasi Menginspirasi

ACTUAL TEST PROJECT
MODUL C – NETWORK SYSTEMS

IT NETWORK SYSTEMS ADMINISTRATION

KELOMPOK INFORMATION AND COMMUNICATION TECHNOLOGY

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 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 pre configured 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 **cisco** as a password for local credentials to access desktop 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. Configure IPv4/IPv6 address for all network devices as you see on the topology.
5. Configure all network interfaces on ES-SRV and WS-SRV from ens35 to ens3.
6. Configure GMT +7 as a timezone for all network devices.

Basic configuration on ALL devices
Line console 0 exec-timeout **0 0** no ip domain-lookup ip domain-name lks2023.id enable secret Skill39 clock timezone GMT +7 hostname (sesuai dengan masing” network devices)

Switching

1. Configure VTP on all switches to synchronize VLANs. It should be possible to modify VLAN database only from L3SW-1 with VTP version 3, 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
        iv. The aggregated channel between L3SW-1 and L3SW-2 do not use dynamic

negotiation protocol.

b. The aggregated channel between L3SW-1 and L2SW-1 use a Cisco proprietary protocol for dynamic negotiation.
c. The aggregated channel between L3SW-2 and L2SW-2 use a standard protocol for dynamic negotiation.
d. L3SW-1 and L3SW-2 should initiate negotiation and the other devices should respond but don't initiate.
e. 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 Configure port which is connected to end device so that it immediately begins forwarding when connected.

Untuk mengerjakan soal bagian switching kita harus tau mana yang harus di kerjakan terlebih dahulu.

L3SW-1
Int g0/3 Channel-group 1 mode on Int g1/0 Channel-group 1 mode on Int po1 Switchport trunk encapsulation dot1q Switchport mode trunk Int g1/1 Switchport trunk encapsulation dot1q Switchport mode trunk Int r g0/1-2 Channel-group 2 mode desirable Int po2 Switchport trunk encapsulation dot1q Switchport mode trunk port-channel load-balance src-dst-mac vtp version 3 vtp mode server vtp primary vlan 10 name SRV vlan 20 name CLI spanning-tree vlan 10 root primary spanning-tree vlan 20 root secondary

L3SW-2
Int g0/3 Channel-group 1 mode on Int g1/0 Channel-group 1 mode on int g1/1 Switchport trunk encapsulation dot1q Switchport mode trunk Int po1

```
Switchport trunk encapsulation dot1q
Switchport mode trunk

Int r g0/1-2
Channel-group 3 mode active
Int po3
Switchport trunk encapsulation dot1q
Switchport mode trunk
port-channel load-balance src-dst-mac
Vtp version 3
Vtp mode client

spanning-tree vlan 10 root secondary
spanning-tree vlan 20 root primary
```

L2SW-1

```
Int r g0/1-2
Channel-group 2 mode auto
Int po2
Switchport trunk encapsulation dot1q
Switchport mode trunk
Int g1/1
Switchport trunk encapsulation dot1q
Switchport mode trunk
port-channel load-balance src-dst-mac
Vtp version 3
Vtp mode client
Int g1/1
Spanning-tree vlan 20 cost 100
int g0/0
switchport mode access
switchport access vlan 20
```

L2SW-2

```
Int r g0/1-2
Channel-group 3 mode passive
Int po3
Switchport trunk encapsulation dot1q
Switchport mode trunk
Int g1/1
Switchport trunk encapsulation dot1q
Switchport mode trunk
port-channel load-balance src-dst-mac
Vtp version 3
Vtp mode client
Int g0/3
Switchport mode access
Switchport access vlan 10
```

Routing

1. Configure FHRP on L3SW-1 and L3SW-2.
    a. Use Hot Standby Router Protocol v2 for VLAN 10.

i. L3SW-1 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. L3SW-2 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 EIGRP
   a. use as number 39
   b. make sure network vlan 10 and 20 can be reach EST-1
4. Configure static route on both L3SW to EST-1
5. Configure OSPF.
   a. Use OSPF area 0 and instance number 11.
   b. Advertise only Public IP on all routers.
   c. Configure OSPF so that routing updates are not sent into networks where they are not required.

L3SW-1

Ipv6 unicast
Int vlan 10
Standby version 2
Standby 104 ip 192.168.10.254
Standby 104 preempt
Standby 106 ipv6 **2001:624C:3201:10::254/64**
standby 106 preempt

Int vlan 20
Standby version 2
Standby 204 ip 192.168.20.254
Standby 204 priority 99
Standby 204 preempt
Standby 206 ipv6 **2001:624C:3201:20::254/64**
Standby 206 preempt
Standby 206 priority 99

L3SW-2

Ipv6 unicast
Int vlan 10
Standby version 2
Standby 104 ip 192.168.10.254
Standby 104 preempt
Standby 104 priority 99
Standby 106 ipv6 **2001:624C:3201:10::254/64**
Standby 106 priority 99
standby 106 preempt

Int vlan 20
Standby version 2
Standby 204 ip 192.168.20.254
Standby 204 preempt

Standby 206 ipv6 **2001:624C:3201:20::254/64**
Standby 206 preempt

EST-1

```
ip route 0.0.0.0 0.0.0.0 13.228.27.254
ip route 192.168.10.0 255.255.255.0 11.11.11.1
ip route 192.168.20.0 255.255.255.0 11.11.11.1
router eigrp 39
network 11.11.11.0 0.0.0.3
network 12.12.12.0 0.0.0.3

router ospf 11
passive-interface default
no passive-interface GigabitEthernet0/2
network 13.228.27.0 0.0.0.255 area 0
network 103.76.14.0 0.0.0.255 area 0
 int g0/3
 ip add 103.76.14.10 255.255.255.0 secondary
```

EST-2

```
ip route 0.0.0.0 0.0.0.0 13.229.28.254
 router eigrp 39
network 11.11.11.4 0.0.0.3
 network 12.12.12.4 0.0.0.3
router ospf 11
passive-interface default
no passive-interface GigabitEthernet0/3
 network 13.229.28.0 0.0.0.255 area 0
 network 103.76.14.0 0.0.0.255 area 0
 int g0/2
ip add 103.76.14.5 255.255.255.0 secondary
```

ISP

```
router ospf 11
passive-interface default
no passive-interface GigabitEthernet0/0
 no passive-interface GigabitEthernet0/1
 no passive-interface GigabitEthernet0/2
 no passive-interface GigabitEthernet0/3
 network 3.0.180.0 0.0.0.255 area 0
 network 3.0.190.0 0.0.0.255 area 0
 network 13.228.27.0 0.0.0.255 area 0
 network 13.229.28.0 0.0.0.255 area 0
```

WST-1

```
router ospf 11
passive-interface default
no passive-interface GigabitEthernet0/0
network 3.0.180.0 0.0.0.255 area 0
```

WST-2
router ospf 11 passive-interface default no passive-interface GigabitEthernet0/0 network 3.0.190.0 0.0.0.255 area 0

L3SW-1
ip route 103.76.14.0 255.255.255.0 11.11.11.2 router eigrp 39 network 11.11.11.0 0.0.0.3 network 12.12.12.4 0.0.0.3 network 192.168.10.0 network 192.168.20.0

L3SW-2
ip route 103.76.14.0 255.255.255.0 12.12.12.2 router eigrp 39 network 11.11.11.4 0.0.0.3 network 12.12.12.0 0.0.0.3 network 192.168.10.0 network 192.168.20.0

Services

1. Configure DHCP
    a. DHCP server must be configure on L3SW-1
    b. ES-CLI can obtain IP address automatically.
    c. 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 and monitoring for EST-1 and EST-2 (minimum uptime must be monitor).
4. Configure ISP as NTP server. All network devices should synchronize time from ISP.

L3SW-1
ip dhcp pool VLAN20 Network 192.168.20.0 255.255.255.0 Default-router 192.168.20.254 Dns-server 10.0.0.101 ntp server (ip to EST) prefer # lakukan juga ntp ini di L3SW-2

EST-1
Int r g0/0-1 Ip nat inside Int g0/2 Ip nat outside Ip access-list standart NAT Permit 192.168.20.0 0.0.0.255 ip nat pool NAT 103.76.14.1 103.76.14.10 netmask 255.255.255 ip nat inside source list NAT pool NAT overload snmp-server location Surabaya,Indonesia snmp-server contact **admin@lks2023.id** snmp-server community EST-1 ntp server (ip to ISP) prefer

EST-2
Int r g0/0-1 Ip nat inside Int g0/3 Ip nat outside Ip access-list standar NAT Permit 192.168.20.0 0.0.0.255 ip nat pool NAT 103.76.14.1 103.76.14.10 netmask 255.255.255.0 ip nat inside source list NAT pool NAT overload snmp-server location Surabaya,Indonesia snmp-server contact **admin@lks2023.id** snmp-server community EST-2 ntp server (ip to ISP) prefer

WST
ntp server (ip to ISP) prefer

L2SW
ntp server (ip to L3SW) prefer

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. Use ES-SRV as RADIUSserver.
        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.

EST
Ip ssh version 2 Crypto key gen rsa 1024 Aaa new-model Radius server AAA address ipv4 192.168.10.1 auth-port 1812 acct-port 1813 key Skills39 aaa authentication login default group radius local AAA authorization exec default group radius local line vty 0 4 transport input ssh login auth default access-class NAT in privilege exec level 5 conf t privilege configure level 5 interface privilege interface level 5 sh privilege interface level 5 no sh privilege interface level 5 ip address int g0/0 switchport port-security mac-address stiky switchport port-security maximum 2 switchport port-security violation shutdown switchport port-security errdisable recovery interval 180

VPN

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

EST-1

```
Int tun0
Ip add 10.255.255.2 255.255.255.252
tun source g0/2
tun des 3.0.180.201
```

WST-1

```
Int tun0
Ip add 10.255.255.1 255.255.255.252
tun source g0/0
tun des 13.228.27.200
```

For ikev2

```
 crypto ikev2 proposal VPN-IKEv2-Proposal
 encryption aes-gcm-256
 prf sha384
 group 20
!
crypto ikev2 policy VPN-IKEv2-Policy
 proposal VPN-IKEv2-Proposal
!
crypto ikev2 keyring VPN-IKEv2-Keyring
 peer openbsd
  address <openbsd_ip>
  pre-shared-key local ThisShouldBeAStrongPassword
  pre-shared-key remote ThisShouldBeAStrongPassword
 !
!
crypto ikev2 profile VPN-IKEv2-Profile
 match identity remote address <openbsd_ip> 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local VPN-IKEv2-Keyring
!
crypto ipsec transform-set ESP-AESGCM-256 esp-gcm 256
 mode transport
!
crypto ipsec profile VPN-IKEv2-IPsec-Profile
 set transform-set ESP-AESGCM-256
 set pfs group20
 set ikev2-profile VPN-IKEv2-Profile
!
interface Tunnel0
 ip address <cisco_tunnel_ip> 255.255.255.252
 tunnel source <cisco_ip>
 tunnel destination <openbsd_ip>
tunnel protection ipsec profile VPN-IKEv2-IPsec-Profile
```

Last switching

Switchport trunk allowed vlan 10,20
No switchport trunk allowed vlan 1
Lakukan di semua interface trunk

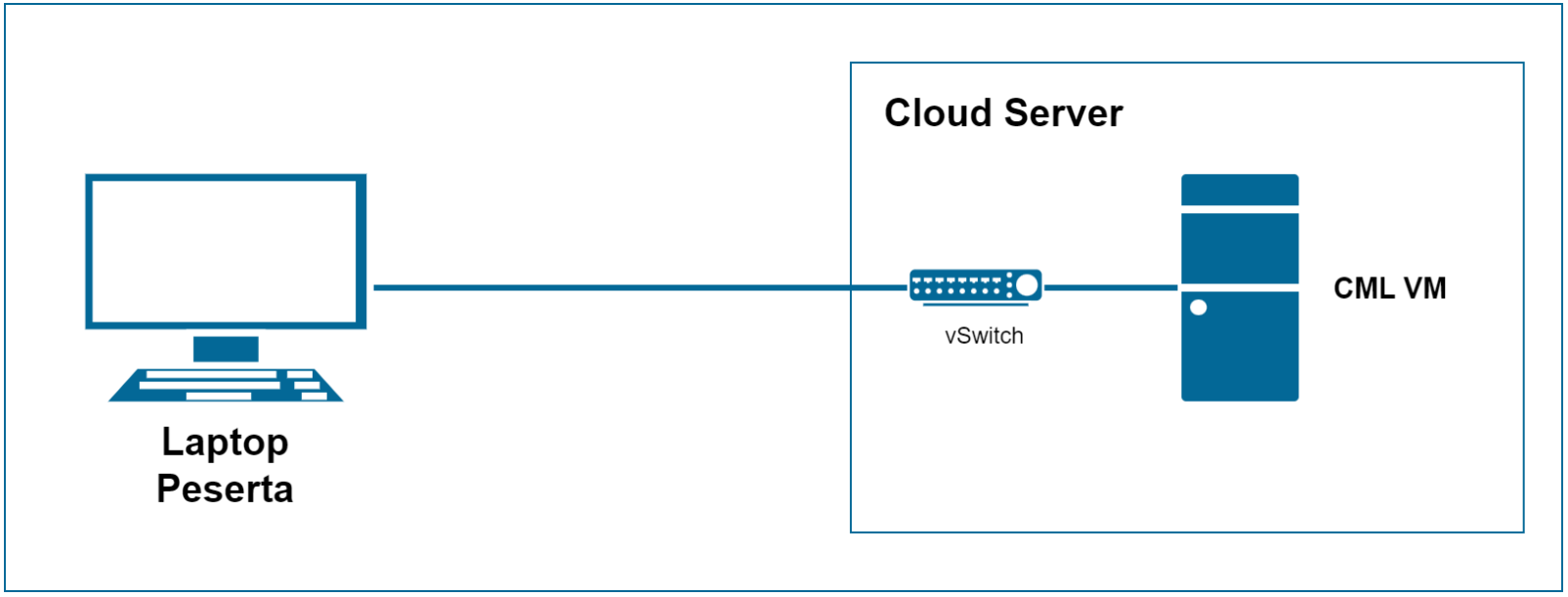
Configure Table

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
		Loopback0	1.1.1.1
WEST	WST-1	GigabitEthernet0/0	3.0.180.201/24
		GigabitEthernet0/1	10.0.0.254/24
		Tunnel0	10.255.255.1/30
	WST-2	GigabitEthernet0/0	3.0.190.202/24
	WS-SRV	ens3	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
		Tunnel0	10.255.255.2/30
	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	192.168.20.253/24
	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	192.168.20.252/24
	L2SW-1	Vlan 10	192.168.10.200/24

	L2SW-2	Vlan 10	192.168.10.201/24
	ES-CLI	ens3	192.168.20.x/24 (DHCP)
	ES-SRV	ens3	192.168.10.1/24

Physical Diagram



Network Topology