TEST PROJECT
MODUL B – NETWORK SYSTEMS

IT NETWORK SYSTEMS ADMINISTRATION

KELOMPOK INFORMATION AND COMMUNICATION TECHNOLOGY

LOMBA KOMPETENSI SISWA
SEKOLAH MENENGAH KEJURUAN
TINGKAT NASIONAL KE XXX
TAHUN 2022

Notice

1) Please use default settings if you are not given the details.
2) Please use "Skills39" as default password.
3) Please don't reboot your computer before assessment.

Basic Configuration

1. Configure hostnames for ALL network devices as you see on the topology.
2. Configure domain name lksn2022.id for ALL network devices.
3. Configure **"Skills39"** as enable secret for ALL network devices.(In ASA, it is enable password)
4. Create user admin with password Skills39 from ALL network devices.
   1) Only encrypted hash of password should be stored in configuration.
   2) This use should have maximum privileges.

Di setiap network devices

ON ALL NETWORK ALL DEVICES
Ip domain-name lksn2022.id Enable secret Skills39 Username admin privilege 15 secret admin Jika ada konfigurasi ipv6 maka tambahkan → **ipv6 unicast routing**

L2 Configuration

1. Configure Etherchannel between SW1 and SW2 according to the following requirements.
   1) Use **"1"** as port-channel group number.
   2) Use LACP Protocol.
   3) SW1 should initiate negotiation.
   4) SW2 listen negotiation but does not initiate it itself.
2. Configure trunks on all links between switches including etherchannel.
3. Configure VTPv2 Domain for synchronization of VLAN between switches.
   1) Configure SW3 as VTP Primary server.
   2) Use **"wsc2022.id"** as VTP domain name.
   3) Use **"Skills39"** as VTP password.
4. Configure the following VLANs for ALL Switches inlcluding name vlan.
   1) VLAN 10 (HQ10) – Fa0/1 interface of SW3 should be accessed in this VLAN.
   2) VLAN 20 (HQ20) - Fa0/2 interface of SW3 should be accessed in this VLAN.
5. Configure STP.
   1) SW1 should be STP root of VLAN10. When SW1 is failed, SW2 should become a root.
   2) SW2 should be STP root of VLAN20. When SW2 is failed, SW1 should become a root.
6. If BPDU arrives on the port on SW3 which is connected to PCs, applicable port should be blocked.
7. The port on SW3 which is connected to PCs should be forwarded immediately without waiting.

Point nomor 1 dan 2 L2 Configuration

ON SW1
Int r f0/23-24 Channel-group 1 mode active Int po1 Switchport mode trunk Int f0/4 Switchport mode trunk Int f0/22 Switchport mode trunk

ON SW2
Int r f0/23-24 Channel-group 1 mode passive Int po1 Switchport mode trunk Int f0/4 Switchport mode trunk Int f0/22 Switchport mode trunk

ON SW3
Int r f0/21-22 Switchport mode trunk

Point nomor 3 dan 4 L2 Configuration

ON SW1
vtp version 2 vtp mode server vtp domain wsc2022.id vtp password Skills39 vlan 10 name HQ10 vlan 20 name HQ20

ON SW2
vtp version 2 vtp mode client vtp domain wsc2022.id vtp password Skills39

ON SW3
vtp version 2 vtp mode client

```
vtp password wsc2022.id
vtp password Skills39
int f0/1
switchport access vlan 10
int f0/2
switchport access vlan 20
```

Point nomor 5 L2 Configuration

ON SW1
Spanning tree vlan 10 root primary Spanning tree vlan 20 root secondary

ON SW2
Spanning tree vlan 20 root primary Spanning tree vlan 10 root secondary

Point nomor 6 dan 7 L2 Configuration

ON SW3
Int f0/1 Spanning-tree bpguard enable Spanning-tree mode portfast Int f0/2 Spanning-tree bpguard enable Sppaning-tree mode portfast

L3 Configuration

1. Assign IPv4/IPv6 addresses to interface of network devices according to configuration tables.
2. Configure OSPF with Prosess ID 5
   ISP interface configuration
   Passive interface
3. Configure HSRP for VLAN 10 on R3 and R2
   1) R3 must be active router. If Gig0/1 interface of R3 is failed, R2 must be master router.
   2) Use **"104"** as group number of IPv4 Address and
   3) Use **"192.168.10.254"** as virtual IPv4 address and
   4) HSRP preemption should be enabled.

5) HQ-SRV should use this VIP as default-gateway.

4. Configure HSRP for VLAN 20 on R3 and R2
   1) R3 must be active router. If Gig0/1 interface of R3 is failed, R2 must be active router.
   2) Use version 2.
   3) Use **"20"** as group number
   4) Use "**192.168.20.254"** as the VIP.
   5) HSRP preemption should be enabled.
   6) HQ-CLI should use this VIP as default-gateway.

Point 2 L3 CONFIGURATION

R1
router ospf 5 router-id 1.1.1.1 log-adjacency-changes network 210.103.5.12 0.0.0.3 area 0 network 1.1.1.1 0.0.0.0 area 0

R2
router ospf 5 router-id 2.2.2.2 log-adjacency-changes network 210.103.6.0 0.0.0.3 area 0 network 210.103.5.4 0.0.0.3 area 0 network 2.2.2.2 0.0.0.0 area 0

R3
router ospf 5 router-id 3.3.3.3 log-adjacency-changes network 210.103.5.0 0.0.0.3 area 0 network 210.103.6.0 0.0.0.3 area 0 network 3.3.3.3 0.0.0.0 area 0

ISP
router ospf 5 router-id 5.5.5.5 log-adjacency-changes network 210.103.5.12 0.0.0.3 area 0 network 210.103.5.8 0.0.0.3 area 0 network 210.103.5.0 0.0.0.3 area 0 network 210.103.5.4 0.0.0.3 area 0 network 210.103.5.128 0.0.0.127 area 0

R4
router ospf 5

router-id 4.4.4.4
log-adjacency-changes
network 210.103.5.8 0.0.0.3 area 0
network 210.103.7.128 0.0.0.127 area 0

NOTE: soal tidak menjelaskan secara detail routingnya dan tidak ada ospfv3 jadi hanya routing ipv4

Point 3 dan 4 L3 CONFIGURATION

R3
Int g0/1.10 Standby 104 ip 192.168.10.254 Standby 104 prempt Int g0/1.20 Standby version 2 Standby 20 ip 192.168.20.254 Standby 20 prempt Standby 20 priority 101

R2
Int g0/1.10 Standby 104 ip 192.168.10.254 Standby 104 prempt Standby 104 priority 101 Int g0/1.20 Standby version 2 Standby 20 ip 192.168.20.254 Standby 20 prempt

Service Configuration

1. Configure DHCP Server for VLAN20 network on R3.
   1) 192.168.20.1-10 addresses must be excluded from DHCP assignment.
   2) DHCP clients should use 192.168.20.254 as default-gateway.
2. Configure DHCP Server on R1.
   1) 172.16.10.1-172.16.10.10 addresses must be excluded from DHCP assignment.
   2) DHCP clients should use 172.16.10.254 as default-gateway.
3. Configure PAT on R3, R2, R1 and FW1
   Use name INTERNET-ACCESS for the name ACL
4. Configure SSH version 2 for remote management on ISP.
   1) Use local account.
   2) It must start in exec mode after being authenticated as **admin** user.

Point nomor 1 dan 2 service konfigurasi

R3
Ip dhcp pool VLAN20 Network 192.168.20.0 255.255.255.0 Default router 192.168.20.254 Ip dhcp exclude address 192.168.20.1 192.168.20.10

R1
Ip dhcp pool R1 Network 172.16.10.0 255.255.255.0 Default router 172.16.10.254 Ip dhcp excluded 172.16.10.1 172.16.10.10

Point nomor 3 Service konfigurasi

R3
int s0/0/1 ip nat inside int g0/1 ip nat inside int s0/0/0 ip nat outside ip access-list standart INTERNET-ACCESS permit 192.168.10.0 0.0.0.255 permit 192.168.20.0 0.0.0.255 ip nat inside source list INTERNET-ACCESS interface Serial0/0/0 overload

R2
int s0/0/0 ip nat inside int g0/1 ip nat inside **int s0/0/0** **ip nat outside** ip access-list standart INTERNET-ACCESS permit 192.168.10.0 0.0.0.255 permit 192.168.20.0 0.0.0.255 ip nat inside source list INTERNET-ACCESS interface Serial0/0/1 overload

R1
Int g0/0 Ip nat outside Int g0/1 Ip nat inside ip access-list standart INTERNET-ACCESS

permit 172.160.10.0 0.0.0.255
ip nat inside source list INTERNET-ACCESS interface g0/0 overload

FW1
Int g1/1 Ip add 210.103.5.129 255.255.255.128 Nameif outside Int g1/2 Ip add 172.16.20.254 255.255.255.0 Nameif inside ## by default inside have security level 100 and outside 0 Route OUTSIDE 0.0.0.0 0.0.0.0 2.10.103.5.254 object network NAT subnet 172.16.20.0 255.255.255.0 nat (inside,outside) dynamic interface ## kita harus menambahkan access list agar bias test ping access-list internet extended permit icmp any any access-group internet in interface outside

Point nomor 4 service konfigurasi

ISP
Ip ssh version 2 Crypto key gen rsa Yes 1024 Line vty 0 4 Transport input ssh Login local

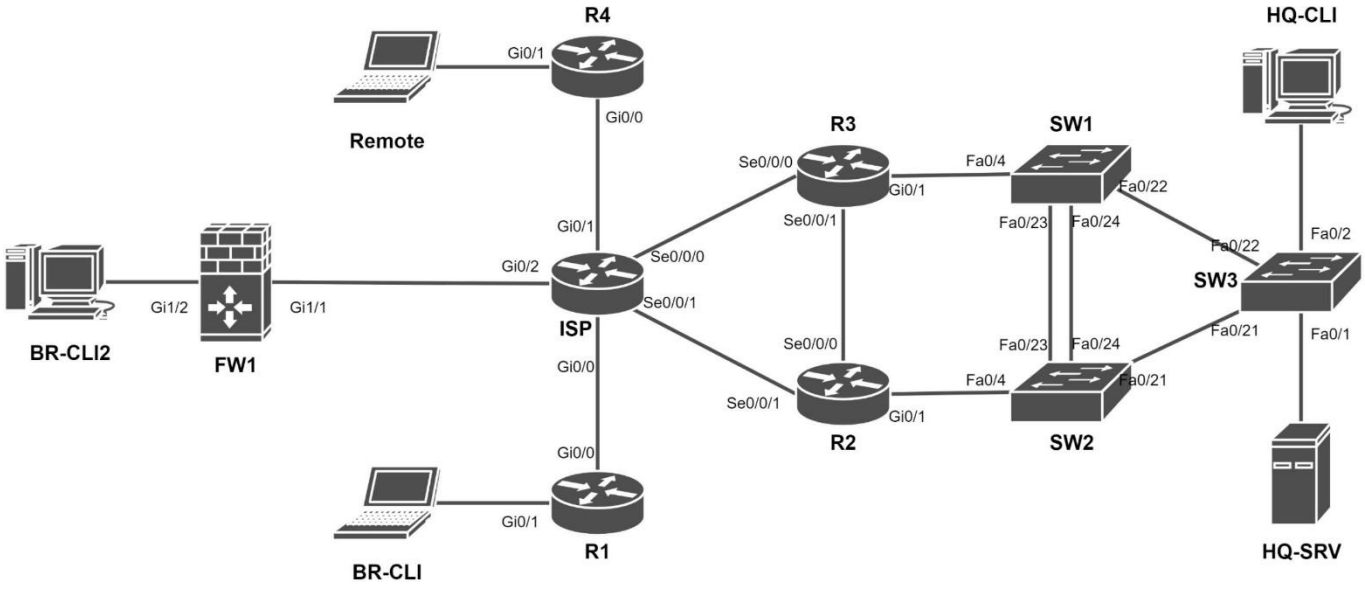
Security Configuration

1. Configure ASA Firewall according to the following requirements.
   1) Set **"outside"** as name of Gig0/0 interface with 0 security-level.
   2) Set **"inside"** as name of Gig0/1 interface with 100 security-level.

Configuration Table

Device	Interface	Address
HQ-SRV	Fe0	192.168.10.1/24
		2001:1010::1/64
HQ-CLI	Ethernet0	DHCP
SW1	Vlan10	192.168.10.10/24
		2001:1010::10/64
	Vlan20	192.168.20.10/24
SW2	Vlan10	192.168.10.20/24
		2001:1010::20/64
	Vlan20	192.168.20.20/24
SW3	Vlan10	192.168.10.30/24
		2001:1010::30/24
	Vlan20	192.168.20.30/24
R3	Gig0/1.10	192.168.10.253/24
		2001:1010::253/64
	Gig0/1.20	192.168.20.253/24
	Serial 0/0/0	210.103.5.1/30
	Serial 0/0/1	210.103.6.2/30
	lo 0	3.3.3.3/32
R2	Gig0/1.10	192.168.10.252/24
		2001:1010::252/64
	Gig0/1.20	192.168.20.252/24
	Serial 0/0/1	210.103.5.5/30
	Serial 0/0/0	210.103.6.1/30
	lo 0	2.2.2.2/32
R1	Gig0/0	210.103.5.13/30
	Gig0/1	172.16.10.254/24
	lo 0	1.1.1.1/32
BR-CLI	Ethernet0	DHCP
ISP	Serial 0/0/0	210.103.5.2/30
	Serial 0/0/1	210.103.5.6/30
	Gig0/1	210.103.5.10/30
	Gig0/2	210.103.5.254/25
	Gig0/0	210.103.5.14/30
	lo 0	8.8.8.8/32

R4	Gig0/0	210.103.5.9/30
	Gig0/1	210.103.7.254/24
	lo 0	4.4.4.4/32
remote	Ethernet0	210.103.7.1/24
FW1	Gig1/1(outside)	210.103.5.129/25
	Gig1/2(inside)	172.16.20.254/24
BR-CLI2	Ethernet0	172.16.20.1/24


R4
HQ-CLI
Gi0/1
Remote
Gi0/0
R3
SW1
Se0/0/0
Fa0/4
Gi0/1
Fa0/22
Se0/0/1
Fa0/23
Fa0/24
Fa0/22
Fa0/2
Gi0/1
Gi0/2
Se0/0/0
SW3
Gi1/2
Gi1/1
Se0/0/1
ISP
Se0/0/0
Fa0/23
Fa0/24
Fa0/21
Fa0/1
Gi0/0
Fa0/4
Fa0/21
Se0/0/1
Gi0/1
R2
SW2
Gi0/0
BR-CLI2
FW1
Gi0/1
R1
HQ-SRV
BR-CLI

Network Topology