LOMBA KETERAMPILAN SISWA

SEKOLAH MENENGAH KEJURUAN

TINGKAT NASIONAL XXV 2017

MODUL C
PT – CHALLENGES

IT NETWORK SYSTEMS ADMINISTRATION

LKS2017_ITNSA_MODUL_C

Instructions

The competition has a fixed start and finish time. You must decide how to best divide your time. Please **carefully** read the following instructions!

When the competition time ends, please save your file and add your ID in the end of the filename (change the XX), leave the Cisco Packet Tracer program and your workstation in a running state.

DO NOT FORGET TO SAVE YOUR PACKET TRACER FILE REGULARLY!
(The Cisco Packet Tracer program may crash and you could lose marks!)

Description of project and tasks

Network diagram has preconfigured.
All devices can be connected with IPv4 and IPv6 according to the instruction below!

ALL INFRASTRUCTURE, SERVERS AND CLIENTS

1. Configure according to the network diagram and tables.
2. Configure host name, enable mode password (encrypted), SSH version 2 with 1024 bit RSA keys, logging synchronous in line vty 0-4 and users in the table 5.

ISP ROUTER

1. For ease of administration, enable SSH with local authentication, isp.net for domain name.
2. Do not configure any kind of static or dynamic routing.
3. Configure PPP CHAP authentication on the Serial Link between ISP and HQ router with Skills39 as the password.

HQ / BRANCH ROUTERES

1. See the appendix to understand IP addressing, services and network diagram.
2. Configure an IPv6 over IPv4 Point-to-Point ipv6ip between the two routers, going through the ISP router.
3. Configure default static route to ISP using next-hop address, EIGRPv6 and OSPFv3 routing via tunnel. OSPFv3 routing serves as a backup routing protocol. When EIGRPv6 is running then we should only see EIGRPv6 routes in the routing table.

HQ EIGRPv6 100 Routing	**BRANCH EIGRPv6 100 Routing**
Fdab:cdef:1::/64	Fdab:cdef:3::/64
Fdab:cdef:4::/64	Fdab:cdef:4::/64
Fdab:cdef:7::/64	

HQ OSPFv6 area 0 Routing with process ID 100	BRANCH OSPFv6 area 0 Routing with process ID 100
Fdab:cdef:1::/64	Fdab:cdef:3::/64
Fdab:cdef:4::/64	Fdab:cdef:4::/64
Fdab:cdef:7::/64	

-Don't send routing updates on interface serial0/0/0

4. Configure High Availability routing for the MGMT IPV4 with group 1. Use a protocol that will use only one of the two routers, preferably the HQ router.

5. Configure VoIP system with the following settings:

Site	Extension	Ephone-DN	Device	Server
HQ	101	1	IP phone LUXVOIP	10.0.0.1/24
HQ	102	2	Softphone WINLAPTOP	
Branch	201	1	IP phone WINVOIP	172.16.0.1/24

-Enable auto assign from directory number 1 to 10.
-Max phone and directory are 20.
-IP phone/softphone can communicate between HQ and Branch site.
-DHCP information in the DHCP Services section.
-Clock time zone UTC 7

6. Configure AAA to authenticate SSH logins, idnux.local for domain-name, the radius server is LUXSRV for HQ and WINSRV for BRANCH, Skills39 for radius-key and use cisco local user as a fall back if RADIUS becomes unavailable.
7. Restrict SSH access to the MGMT IPv6 and IPv4 network, MGMT-IPv6-net and MGMT-net for ACL-name with the standard type.
8. Configure time synchronization with the NETLUXSRV NTP server that has authentication to use it. Use key 1 and Password Skills39.
9. Send logs to the syslog server at LUXSRV for HQ and WINSRV for BRANCH.
10. Configure NAT overload in HQ for MGMT IPv4 Network for internet access, Use MGMT-net for ACL so WINLAPTOP can access NETLUXSRV.

REMOTE ASA 5505

1. For ease of administration, enable SSH with local authentication, idnux.local for domain-name. It should accessible from the inside network.
2. Create object network named INSIDE to specify an inside network and configure NAT for internet access using outside interface so REMWINTOP can access NETLUXSRV.
3. Create object network named DMZLUXSRV to specify a single host and configure NAT for HTTP and HTTPS on DMZLUXSRV to accessible from the outside network with IP 1.1.1.19.
4. Configure ACL named FROM-INTERNET to allow HTTP and HTTPS access from the outside network to the DMZLUXSRV.

HQSW / BRANCH SWITCHES

1. For ease of administration, enable SSH with local authentication, idnux.local for domain-name.
2. Configure portfast on all access ports.
3. Configure an Etherchannel on ports Gig0/1-Gig0/2 on both switches. Use a standard based protocol.
4. Use Port-Channel 1 for both Vlan 99 and Vlan 12.

HQSW - C2960 SWITCH

1. Configure port security; WINLAPTOP is the only device allowed on the MGMT Vlan on Fa0/13 with violation shutdown the port.
2. Configure port F0/11 to receive all traffic that is received and sent on port F0/5.
3. Configure DHCP snooping on F0/21, F0/22, Fa0/13 and a port connected to IPphone. Enable on All VLANs. No IP DHCP snooping information option.
4. On the Etherchannel on ports Gig0/1-Gig0/2, this switch should not attempt to negotiate an EtherChannel.

BRANCHSW - C2960 SWITCH

1. Configure DHCP snooping on F0/21, FA0/22, and port connected to IPphone. Enable on All VLANs. No IP DHCP snooping information option.
2. On the Etherchannel on ports Gig0/1-Gig0/2, this switch should attempt to negotiate an EtherChannel

DHCP Services

1. Configure DHCP service on ISP, HQ, BRANCH, HQSW and REMOTE with the setting in the table 4.

APPENDIX

TABLE 1. IP ADDRESSING TABLE

Device	IPv4	IPv6	Interface
ISP	1.1.1.1/29		S0/0/0
	1.1.1.9/29		S0/0/1
	1.1.1.17/29		Gig0/0
	1.1.1.65/26		Gig0/1
NETLUXTOP	DHCP from Server: 1.1.1.65		FA0
NETLUXSRV	1.1.1.70/26		FA0
HQ	1.1.1.10/29		S0/0/0
	10.0.10.1/24	fdab:cdef:1::1/64	GE0/0.11
		fdab:cdef:2::1/64	GE0/0.12
	10.0.0.1/24		GE0/1.10
	10.0.1.1/24	fdab:cdef:7::1/64	GE0/1.99
	10.0.1.254/24		GE0/1.99 STANDBY
		fdab:cdef:4::1/64	Tunnel0
BRANCH	1.1.1.2/29		S0/0/0
	10.0.30.1/24	fdab:cdef:3::1/64	GE0/0.21
		fdab:cdef:2::2/64	GE0/0.12
	172.16.0.1/24		GE0/1.20
	10.0.1.2/24	fdab:cdef:7::2/64	GE0/1.99
	10.0.1.254/24		GE0/1.99 STANDBY
		fdab:cdef:4::2/64	Tunnel0
LUXSRV	10.0.10.2/24	fdab:cdef:1::2/64	FA0
LUXTOP		fdab:cdef:2::10/64	FA0
LUXVOIP	172.16.0.X from DHCP 172.16.0.1		FA0
WINLAPTOP	10.0.1.x from DHCP Server: 10.0.1.3	fdab:cdef:7::10/64	FA0
HQSW			FA/21 trunk port to HQ Gig0/1 with native VLAN 99
			FA0/22 trunk port to HQ Gig0/0
	10.0.1.3/24		VLAN99
BRANCHSW			FA/21 trunk port to HQ Gig0/1 with native VLAN 99
			FA0/22 trunk port to HQ Gig0/0
	10.0.1.4/24		VLAN99
WINSRV	10.0.30.2/24	fdab:cdef:3::2/64	FA0
WINTOP		fdab:cdef:2::20/64	FA0
WINVOIP	172.16.0.X from DHCP 172.16.0.1		FA0
REMOTE	1.1.1.18/29		E0 (VLAN 2 Outside)

			Security level 0
	192.168.0.1/25		E1 (VLAN 1 Inside) Security level 100
	192.168.0.129/25		E2 (VLAN 3 DMZ) Security level 50 No forward interface to inside
REMWINTOP	DHCP from Server: 192.168.0.1		FA0
DMZLUXSRV	192.168.0.130/25		FA0

TABLE 2.VTP AND VLAN ASSIGNMENT

VTP Version 2	
VTP DOMAIN:	skills.org
VTP PASSWORD:	Skills39
VTP SERVER:	HQSW
VTP CLIENT:	BRANCHSW

HQSW			
VLAN ID	**VLAN NAME**	**PORTS**	**NETWORK**
10	LUXVOIP	F0/1 - F0/4 (Voice VLAN; Data VLAN is 12)	10.0.0.0/24
11	LUXSRV	F0/5 - F0/8	fdab:cdef:1::/64 10.0.10.0/24
12	LUXWINTOP	F0/1-F0/4, F0/9 - F0/12	fdab:cdef:2::/64
99	MGMT	F0/13 - F0/16	10.0.1.0/24 and fdab:cdef:7::/64
99	*NATIVE VLAN*		

BRANCHSW			
VLAN ID	**VLAN NAME**	**PORTS**	**NETWORK**
20	WINVOIP	F0/1 - F0/4 (Voice VLAN; Data VLAN is 12)	172.16.0.0/24
21	WINSRV	F0/5 - F0/8	fdab:cdef:3::/64 10.0.30.0/
12	LUXWINTOP	F0/1-F0/4, F0/9 - F0/12	fdab:cdef:2::/64
99	MGMT	F0/13 - F0/16	10.0.1.0/24 and fdab:cdef:7::/64
99	*NATIVE VLAN*		

TABLE 3. SPANNING TREE

SPANNING TREE FOR VLAN 99	
PRIMARY ROOT BRIDGE	HQSW
SECONDARY ROOT BRIDGE	BRANCHSW
HQSW LINKS	Gig0/1, Gig0/2
BRANCHSW LINKS	Gig0/1, Gig0/2
VLANS ALLOWED ON LINKS	99,12
NATIVE VLAN	99

SPANNING TREE FOR VLAN 12	
PRIMARY ROOT BRIDGE	BRANCHSW
SECONDARY ROOT BRIDGE	HQSW
HQSW LINKS	Gig0/1, Gig0/2
BRANCHSW LINKS	Gig0/1, Gig0/2
VLANS ALLOWED ON LINKS	99,12
NATIVE VLAN	99

TABLE 4. DHCP SERVERS

DHCP SERVERS					
SERVER	**POOL NAME**	**NETWORK**	**DEFAULT ROUTER**	**IP EXCLUDE**	**ADDRESS RANGE**
ISP	NETLUX	1.1.1.64/26		1.1.1.65-1.1.1.75	Use any IP address range from the correct subnet
HQ	LUXVOIP	10.0.0.0/24	10.0.0.1	10.0.0.1-10.0.0.20	
BRANCH	WINVOIP	172.16.0.0/24	172.16.0.1	172.16.0.1-172.16.0.20	
HQSW	MGMT-V4	10.0.1.0/24	10.0.1.254	10.0.1.1-10.0.1.4	
REMOTE	dhcpd	192.168.0.0/25	192.168.0.1	-	192.168.0.10-192.168.0.40

TABLE 5. USER ACCOUNTS

CISCO MANAGEMENT ACCOUNTS		
ACCOUNT	**PASSWORD (encrypted)**	**PRIVILEDGE LEVEL**
root	Skills39	15
cisco	Skills39a	1
enable secret	Skills39	

RADIUS USER ACCOUNTS	
ACCOUNT	PASSWORD
super	Skills39
basic	Skills39a

TABLE 6. ENABLED SERVICE

HOST	SERVICES
NETLUXSRV	NTP Authentication Key 1

HOST	SERVICES
LUXSRV	RADIUS port 1645, Client = HQ with Key = Skills39
	SYSLOG

HOST	SERVICES
WINSRV	RADIUS port 1645, Client = BRANCH with Key = Skills39
	SYSLOG

HOST	SERVICES
DMZLUXSRV	HTTP
	HTTPS

NETWORK DIAGRAM