Test Project

IT Network Systems Administration

Module A – Cisco Network Environment

Submitted by:
ITNSA-ID Team

Contents

Introduction to Test Project

This Test Project proposal consists of the following document/file:

- LKSN2019_ITNETWORK_MODUL_A.pdf

Introduction

Network technologies knowledge has become 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 the high score, you are definitely ready to implement 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
- WAN
- Routing
- Services
- Security
- Monitoring and backup
- WAN and VPN

All sections are independent but all together they build very complex network infrastructure. Some tasks are pretty simple and straight forward; 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 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.

NOTE:

RADIUS VM (Debian 9.5)
Username : **root / skill39**
Password : **Skill39**

PC1 (Ubuntu 16.04)
Username : **skill39**
Password : **Skill39**

NETWORK ISLAND TASK

BASIC CONFIGURATION

- Configure domain name **lksn2019.com** for HQ2, BR1, and FW2
- Create user **lksn2019** with password **yogyakarta** on HQ2, BR1, and FW2
    - Only scrypt hash of the password should be stored in configuration. (This requirement only applies to the routers, NOT the ASA Firewalls)
    - User should have maximum privileges.
- Configure new AAA model for HQ2, BR1, and FW2.
    - Remote console (vty) authentication should use local username database.
    - After successful authentication on vty line users should automatically land in privileged mode (except for FW2).
    - Enable login authentication on local console.
    - After successful authentication on local console user should land in user mode with minimal privileges (privilege level 1).
    - After successful authentication on local console of BR1 router user should automatically land in privileged mode with maximal privileges.
- Configure RADIUS authentication for all remote consoles (vty) on HQ2 router.
    - Authentication sequence:
        - RADIUS server
        - Local username database
    - Use “cisco1” as the shared key.
    - Use port numbers 1812 for authentication and 1813 for accounting.
    - IP address of the RADIUS server is 192.168.10.10
    - Configure automatic authorization — after successful authentication on RADIUS server user should automatically land in privileged mode with maximal privileges.
    - Test RADIUS authentication using **radius/cisco1** credentials.
- Configure **diy** as a privileged mode password for HQ2, BR1, and FW2.
    - Password should be stored in configuration in plain text (not in hash).
    - Configure privileged mode authorization on FW2. For example:

```
#Connect to FW1 using SSH or Console
Username: lksn2019
Password: yogyakarta
Type help or '?' for a list of available commands.
FW1> enable
Password: diy
FW1#
```

    - Set the mode where all the passwords in the configuration are stored as a reversible cipher text.
- Create all necessary interfaces, subinterfaces and loopbacks on ALL devices. Use IP addressing according to the L3 diagram.
    - Use VLAN101 as a virtual interface for SW1, SW2 and SW3 switches. Use IP address
        - 192.168.10.51 for SW1
        - 192.168.10.52 for SW2
        - 192.168.10.53 for SW3.
    - For HQ1 and HQ2 use automatic IPv6 addresses generation (EUI-64) for LAN1 subnet.
- HQ2, BR1, and FW2 devices should be accessible using SSH protocol version 2. For FW2 allow SSH connection on the “inside” interface.
- Configure current local time zone (GMT +7) on HQ1 router.

SWITCHING CONFIGURATION

- Configure VTP version 2 on SW1, SW2 and SW3. Use SW1 as VTP server, SW2 and SW3 as clients. Use **LKSN** as VTP domain name and **2019** as a password. VLAN database on all switches should contain following VLANs:
    - VLAN 101 with name LAN1.
    - VLAN 102 with name VOICE.
    - VLAN 103 with name EDGE.
- On SW1, SW2 and SW3 switches configure dynamic trunking protocol:
    - For Gi1/1 and Gi2/1 ports on SW1 switch configure mode that will listen for trunk negotiation but won't initiate it itself.
    - For Gi1/1 ports on SW2 switch and for Gi2/1 ports on SW3 switch configure mode that will initiate trunk negotiation.
    - Configure ports Gi0/1-3 on SW1 and SW2 for traffic transmission using IEEE 802.1q protocol.
- Configure link aggregation between switches SW1 and SW2. Use following port-channel number 1.
    - SW2 switch should use PAgP desirable mode.
    - SW3 switch should use PAgP auto mode.
- Configure spanning tree protocol:
    - For ALL switches use STP protocol version which is compatible with 802.1w standard.
    - SW2 switch should be STP root in VLAN 101. In case of SW2 failure, SW3 should become a root.
    - SW1 switch should be STP root in VLAN 102. In case of SW3 failure, SW2 should become a root.
    - SW3 switch should be STP root in VLAN 103. In case of SW1 failure, SW1 should become a root.
    - For traffic transmission in VLANs 101, 102 and 103 on SW1 and SW2 use ports that are not participating in channel-groups.
- Turn on root guard on SW2 port which is connected to RADIUS VM.
- Configure portfast on SW3 switch which is connected to PC1.
- LAN1 subnet traffic between HQ1 router and SW1 switch should be forwarded without IEEE 802.1q tag.

ROUTING CONFIGURATION

- Configure EIGRP with AS number 2019 on ISP1, ISP2, HQ1, HQ2 and BR1 routers according to the routing diagram. Enable routing updates authentication. Use MD5 algorithm with **DIY** key.
- Configure BGP on ISP1, ISP2, HQ1, and HQ2 according to the routing diagram.
    - Routers HQ1 and HQ2 should exchange routing updates using iBGP
    - Configure route filtering so that route 209.136.0.0/16 won't be present in routing table on HQ1 router.
- Configure OSPFv2 on HQ1, HQ2, BR1 routers and FW1, FW2 firewalls according to the routing diagram.
- Configure OSPFv3 on HQ1, HQ2, and BR1 routers according to the routing diagram.
- On BR1 router configure OSPF route redistribution only for Loopback10 subnet into EIGRP AS 2019.

SERVICES CONFIGURATION

- Configure dynamic port translation on HQ1 and HQ2 routers for LAN1 subnet so that all internal IPv4 addresses are translated into IPv4 address of the interface which is connected to the INET10 and INET20 subnets respectively.
- Configure first-hop redundancy protocols on HQ1 and HQ2 routers:
    - Configure GLBP group for LAN1 subnet:
        - Group number 100
        - Use 192.168.10.252 as the virtual IP address
        - Configure priority 151 for HQ1 router and 101 for HQ2 router.
    - Configure HSRP group for LAN2 subnet:
        - Group number 200
        - Use 192.168.20.252 as the virtual IP address
        - Configure priority 121 for HQ1 router and 111 for HQ2 router.
- Configure DHCP using following parameters:
    - On HQ1 router for LAN subnet:
        - Network address — 192.168.10.0/24;
        - Default gateway — virtual IP address of GLBP group;
        - DNS server — 192.168.10.10;
        - Exclude first 50 usable addresses from DHCP pool.
        - DHCP server should assigned 192.168.10.10 to the "RADIUSSRV" server.
    - Make sure "RADIUSSRV" server and "PC1" are configured as DHCP clients

SECURITY CONFIGURATION

- Configure role-based access control on BR1 router:
    - Create **user1**, **user2**, **user3** with **yogyakarta** password.
    - Create view-context "**show_view**":
        - Include "**show version**" command
        - Include all unprivileged commands of "**show ip ***"
        - Include "**who**" command
        - **user1** should land in this context after successful authentication on local or remote console.
    - Create view-context "**ping_view**":
        - Include "**ping**" command
        - Include "**traceroute**" command

        - **user2** should land in this context after successful authentication on local or remote console.
    - Create superview-context that combines these 2 contexts. **user3** should land in this superview-context after successful authentication on local or remote console.
    - Make sure that users cannot issue any other commands within contexts that are assigned to them (except show banner and show parser, which are implicitly included in any view).
- On port of SW3 switch which is connected to PC1 enable and configure port-security using following parameters:
    - Maximum MAC addresses — 2
    - MAC addresses should be automatically saved in running configuration.
    - In case of policy violation, security message should be displayed on the console; port should not go to err-disabled state.
- Turn on DHCP snooping on SW2 switch for LAN1 subnet. Use internal flash to keep DHCP-snooping database.

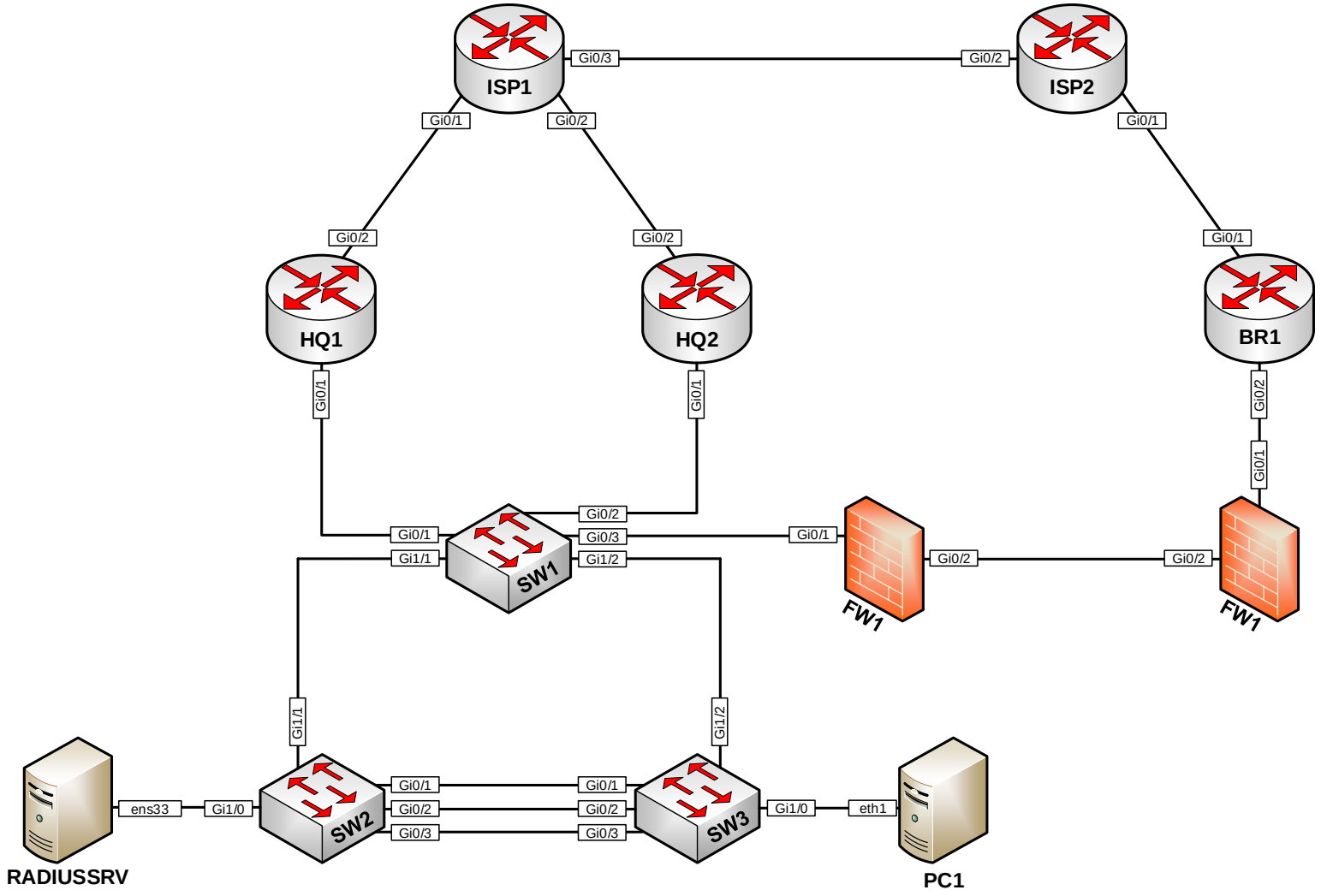
MONITORING AND BACKUP CONFIGURATION

- Configure logging of system messages on HQ1 router and FW1 firewall. All logs including informational messages should be sent to the RADIUSRV server (location **/var/log/hq1.log** and **/var/log/fw1.log**).
- Configure SNMP v2c on HQ1 router and FW1 firewall :
    - Use read-only community string **snmp_ro**
    - Configure device location **Indonesia, ID**
    - Configure system contact **admin@lksn2019.org**
- Configure configuration backup on HQ1 router:
    - Backup copy of running configuration should be automatically saved on RADIUS server using TFTP each time configuration is saved (copied to startup);
    - Use following naming convention for backup files: <hostname><time>.cfg
    - Location for configuration backup files is **/srv/tftp/** on RADIUSSRV server

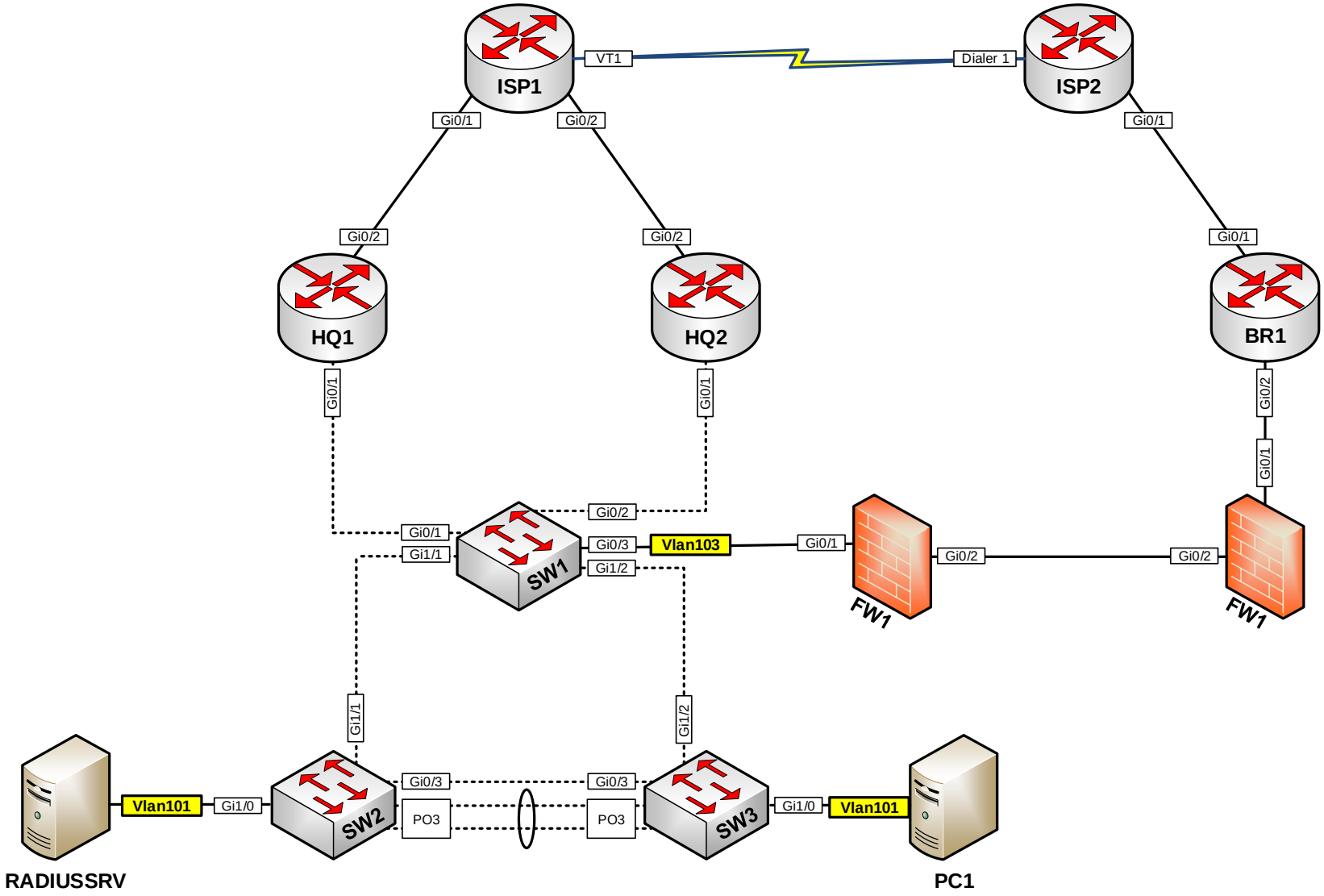
WAN & VPN CONFIGURATION

- Configure ISP1 router as PPPoE server and ISP2 router as PPPoE client. Use PAP for authentication with **papuser\yogyakarta** credentials.
- Configure GRE tunnel between HQ1 and BR1 routers:
    - Use Tunnel100 as VTI for all routers;
    - Assign IPv6 addresses 2001::1/64 and 2001::2/64 for tunnel of HQ1 and BR1 respectfully;
- Configure IKEv2 IPsec Site-to-Site VPN on FW1, FW2 firewalls:
    - Phase 1 parameters:
        - Hash – MD5
        - Encryption – AES-128
        - DH group – 5
        - Authentication – pre-shared key (**cisco1**)
    - Phase 2 parameters:
        - Protocol – ESP
        - Encryption – AES-128
        - Hash – MD5
    - For transmission through IPsec tunnel permit all TCP traffic from network of IP address of HQ2 subinterface in LAN2 subnet to network of IP address of BR2 interface in LAN3 subnet.

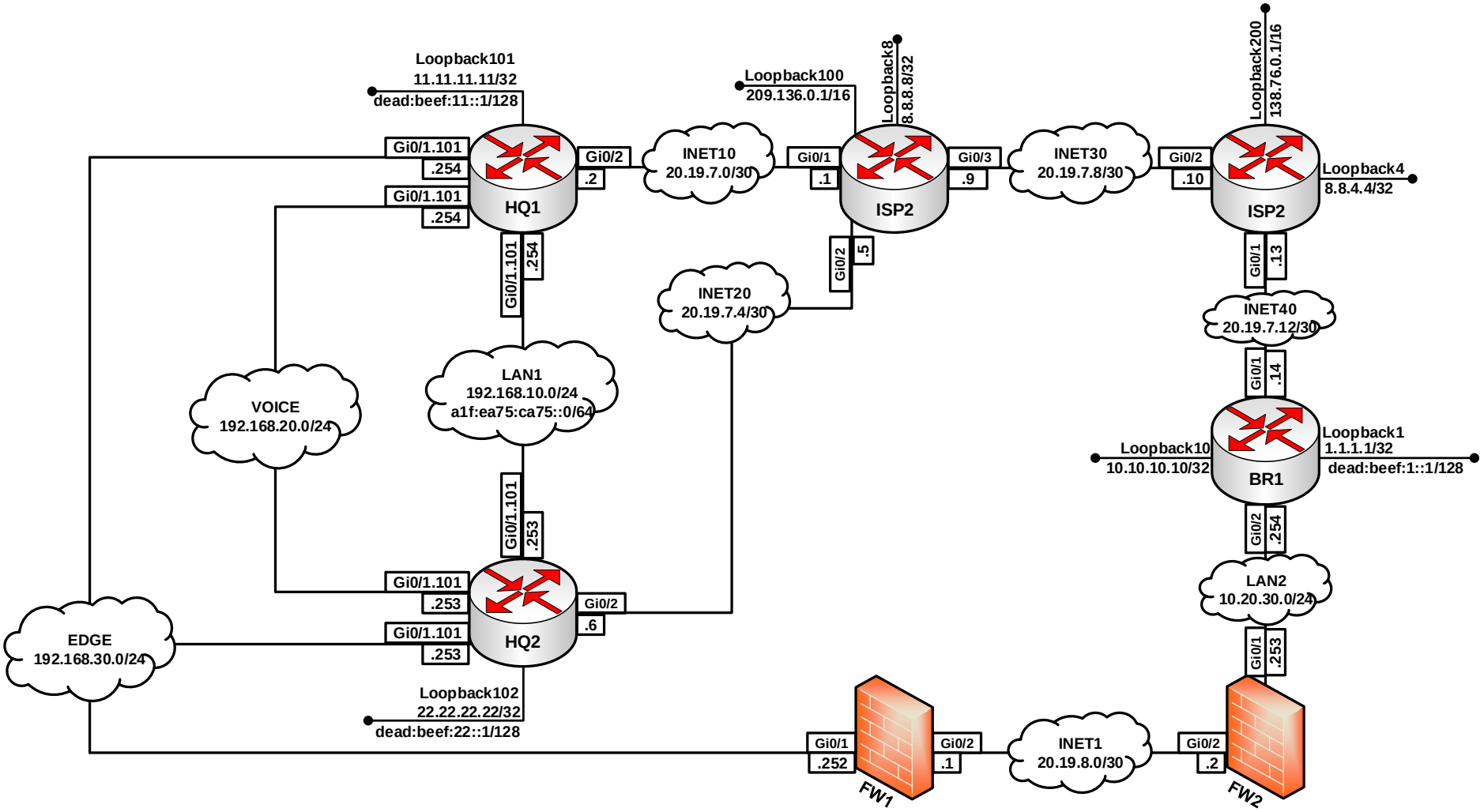
LAYER 1 NETWORK DIAGRAM



LAYER 2 NETWORK DIAGRAM



LAYER 3 NETWORK DIAGRAM



ROUTING DIAGRAM