TEST PROJECT IT NETWORK SYSTEMS ADMINISTRATION

Module C - Cisco Environment

WSC2017_TP39_ModuleC

Submitted by:
Jit How (Kravitz) Hwang SG
Benjamin Callar FR
Christian Schöndorfer AT
Sonia E Cardenas CO
Almut Leykauff-Bothe DE
Jae Ha Lee KR
José Daniel Medeiros PT
Aleksandr Gorbachev RU
Kevin Large UK

CONTENTS

This Test Project proposal consists of the following documentation/files:

1. WSC2017_TP39_Module_C_EN.docx

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 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 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 TO THE COMPETITOR

It is very important to read the whole test project first. However, be aware that not all tasks are written in chronological order. Some sections may require configuration from other sections below them. For example, task 6 in the "Basic configuration" section asks you to configure authentication using RADIUS server which obviously will not work if you do not apply all necessary configurations from the "Switching configuration" section that comes right after. It is your responsibility to manage your time effectively and the sequence you decide to complete the tasks.

As mentioned above, do not waste your time if you're stuck with some tasks. You can use temporary solution (if you have technology stack dependency) and continue to work with other tasks, this may allow you to go back afterwards and fix things that are not working properly if you still have time. In addition, we recommend that you to check all your previous work when you complete following modules.

The RADIUS server is already preconfigured with rsyslog, freeradius, tftpd and snmpd to save your time, you are only required to complete the necessary configuration from your side.

EQUIPMENT, MACHINERY, INSTALLATIONS, AND MATERIALS REQUIRED

It is expected that all Test Projects can be completed by Competitors based on the equipment and materials specified in the Infrastructure List.

MARKING SCHEME

According to the WorldSkills Standards Specifications within current Technical Description all marks for this test project module fall into section 7 «Configuring network devices» which has a maximum mark of 20. Marking scheme is also divided into configuration sections as you see in test project (one sub criterion = one section). Each sub criterion has approximately the same weight. Aspects within each section have different weights depending on aspects count and their complexity.

Marking scheme is designed in the way that every configuration aspect is graded only once. For example, in the “Basic configuration” section you are required to configure hostnames for all devices but it will be checked on only one device and graded only once. The same configuration aspect may be checked and graded more than once if it’s done with different configuration options for different devices or for different device classes. For example, in the “Basic configuration” section you are required to configure local AAA model for all devices but it differs for BR3 router and FW1, FW2 firewalls.

Any details about how and from which exact devices experts will perform checking and grading of your work are contained in “How to Mark” document. These details are subject to 30% changes as well as the aspects in marking scheme.

**NOTE: Refer to the diagram on the last page for quick specification reference.
Please use the default configuration if you are not given the details.
All user account on ALL machines should have a password of Skill39 unless otherwise specified. Pre-supplied virtual machines that the competitor needs to logon to will also be pre-configured with this password.
Use the default account and password for Cisco VIRL.
All supplied software and files needed to complete this project can be found in the software.iso file in the datastore.**

You are reminded to extract configuration in VM Maestro before you leave the competition site.

NETWORK ISLAND TASK

BASIC CONFIGURATION

1. Configure hostnames for ALL devices as you see on the topology
2. Configure domain name **wsi2017.com** for ALL network devices on the topology
3. Create user **wsc2017** with password **cisco1** on ALL devices
    a. Only scrypt hash of the password should be stored in configuration. (This requirement only applies to the routers and switches, NOT the ASA Firewalls)
    b. User should have maximum privileges.
4. Configure new AAA model for ALL devices.
    a. Remote console (vty) authentication should use local username database.
    b. After successful authentication on vty line users should automatically land in privileged mode (except for FW1 and FW2).
    c. Enable login authentication on local console.
    d. After successful authentication on local console user should land in user mode with minimal privileges (privilege level 1).
    e. After successful authentication on local console of BR3 router user should automatically land in privileged mode with maximal privileges.
5. Configure RADIUS authentication for all remote consoles (vty) on HQ1 router.
    a. Authentication sequence:
        i. RADIUS server
        ii. Local username database
    b. Use “cisco1” as the shared key.
    c. Use port numbers 1812 for authentication and 1813 for accounting.
    d. IP address of the RADIUS server is 192.168.10.10
    e. Configure automatic authorization — after successful authentication on RADIUS server user should automatically land in privileged mode with maximal privileges.
    f. Test RADIUS authentication using **radius/cisco1** credentials.
6. Configure **wsi** as a privileged mode password for ALL devices.
    a. Password should be stored in configuration in plain text (not in hash), except for FW1 and FW2.
    b. Configure privileged mode authorization on FW1 and FW2. When entering privileged mode, authenticated username should be used automatically (no username prompt) and only password of authenticated user should be prompted. For example:

```
#Connect to FW1 using SSH or Console
Username: wsc2017
Password: cisco1
Type help or '?' for a list of available commands.
FW1> enable
Password: cisco1
FW1#
```

    c. Set the mode where all the passwords in the configuration are stored as a reversible cipher text.
7. Create all necessary interfaces, subinterfaces and loopbacks on ALL devices. Use IP addressing according to the L3 diagram.
    a. 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 and 192.168.10.53 for SW3.

   b. For HQ1 and HQ2 use automatic IPv6 addresses generation (EUI-64) for LAN1 subnet.

8. ALL devices should be accessible using SSH protocol version 2. For FW1 and FW2, allow SSH connection on the “inside” interface.
9. Configure current local time zone (GST/GMT +4) on HQ1 router.

SWITCHING CONFIGURATION

1. Configure VTP version 2 on SW1, SW2 and SW3. Use SW3 as VTP server, SW1 and SW2 as clients. Use **WSI** as VTP domain name and **2017** as a password. VLAN database on all switches should contain following VLANs:
   a. VLAN 101 with name LAN1.
   b. VLAN 102 with name LAN2.
   c. VLAN 103 with name EDGE.
2. On SW1, SW2 and SW3 switches configure dynamic trunking protocol:
   a. For Gi1/1-2 ports on SW3 switch configure mode that will listen for trunk negotiation but won’t initiate it itself.
   b. For Gi1/1 ports on SW1 switch and for Gi1/2 ports on SW2 switch configure mode that will initiate trunk negotiation.
   c. Configure ports Gi0/1-3 on SW1 and SW2 for traffic transmission using IEEE 802.1q protocol.
3. Configure link aggregation between switches SW1 and SW2. Use following port-channel number 1.
   a. SW1 switch should use PAgP desirable mode.
   b. SW2 switch should use PAgP auto mode.
4. Configure spanning tree protocol:
   a. For ALL switches use STP protocol version which is compatible with 802.1w standard.
   b. SW1 switch should be STP root in VLAN 101. In case of SW1 failure, SW2 should become a root.
   c. SW3 switch should be STP root in VLAN 102. In case of SW3 failure, SW1 should become a root.
   d. SW2 switch should be STP root in VLAN 103. In case of SW2 failure, SW3 should become a root.
   e. For traffic transmission in VLANs 101, 102 and 103 on SW1 and SW2 use ports that are not participating in channel-groups.
5. Turn on security mechanism that prevents STP root change on SW1 port which is connected to RADIUS VM. In case a superior BPDU arrives on this port, the port should transfer to root-inconsistent state.
6. Configure port on SW2 switch which is connected to PC1 VM so that it goes to Forwarding state without waiting for STP recalculation.
7. LAN1 subnet traffic between HQ1 router and SW3 switch should be forwarded without IEEE 802.1q tag.

ROUTING CONFIGURATION

1. Configure EIGRP with AS number 2017 on ISP, HQ1, HQ2, BR2 and BR3 routers according to the routing diagram. Enable routing updates authentication. Use MD5 algorithm with **WSI** key.
2. Configure BGP on ISP, HQ1, HQ2, BR2 and BR3 according to the routing diagram.
   a. Routers HQ1 and HQ2 should exchange routing updates using iBGP
   b. Configure route filtering so that route 209.136.0.0/16 won’t be present in routing table on HQ1 router.
3. Configure OSPFv2 on HQ1, HQ2, BR2, BR3 routers and FW1, FW2 firewalls according to the routing diagram.
4. Configure OSPFv3 on HQ1, HQ2, BR2 and BR3 routers according to the routing diagram. Router HQ1 should be configured as DR, HQ2 — as BDR.
5. On BR2 router configure OSPF route redistribution for Loopback30 subnet into EIGRP AS 2017.
6. Configure routing policy on HQ1 router so that ICMP and UDP traffic from Loopback101 subnet to Loopback30 subnet goes through ISP router.

SERVICES CONFIGURATION

1. 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 INET11 and INET22 subnets respectively.
2. Configure first-hop redundancy protocols on HQ1 and HQ2 routers:
   a. Configure GLBP group for LAN1 subnet:
      i. Group number 101
      ii. Use 192.168.10.252 as the virtual IP address
      iii. Configure priority 151 for HQ1 router and 101 for HQ2 router.
   b. Configure HSRP group for LAN2 subnet:
      i. Group number 201
      ii. Use 192.168.20.252 as the virtual IP address
      iii. Configure priority 121 for HQ1 router and 111 for HQ2 router.
      iv. Configure MD5 authentication. Key string is “cisco1”
3. Configure DHCP using following parameters:
   a. On HQ1 router for LAN subnet:
      i. Network address — 192.168.10.0/24;
      ii. Default gateway — virtual IP address of GLBP group;
      iii. DNS server — 192.168.10.10;
      iv. Exclude first 50 usable addresses from DHCP pool.
      v. DHCP server should assigned 192.168.10.10 to the “RADIUS” server.
      vi. Make sure “RADIUS” server and “PC01” are configured as DHCP clients.

SECURITY CONFIGURATION

1. Configure role-based access control on BR3 router:
   a. Create **user1**, **user2**, **user3**, **user4** and **user5** with **cisco1** password.
      i. **user1** should be authorized to issue all privileged mode commands except “**show version**” and “**show ip route**” but should be able to issue “**show ip ***” commands.

        ii. **user2** should be authorized to issue all user (unprivileged) mode commands including “**show version**” but not “**show ip route**”.

    b. Create view-context “**show_view**”:
        i. Include “**show version**” command
        ii. Include all unprivileged commands of “**show ip ***”
        iii. Include “**who**” command
        iv. **user3** should land in this context after successful authentication on local or remote console.

    c. Create view-context “**ping_view**”:
        i. Include “**ping**” command
        ii. Include “**traceroute**” command
        iii. **user4** should land in this context after successful authentication on local or remote console.

    d. Create superview-context that combines these 2 contexts. **user5** should land in this superview-context after successful authentication on local or remote console.

    e. 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).

2. On port of SW2 switch which is connected to PC1 VM enable and configure port-security using following parameters:
    a. Maximum MAC addresses — 2
    b. MAC addresses should be automatically saved in running configuration.
    c. In case of policy violation, security message should be displayed on the console; port should not go to err-disabled state.
3. Turn on DHCP snooping on SW1 switch for LAN1 subnet. Use internal flash to keep DHCP-snooping database.
4. Turn on dynamic ARP inspection on SW1 for LAN1 subnet. Create access control list that permits static IP address 192.168.10.10 for RADIUS server.

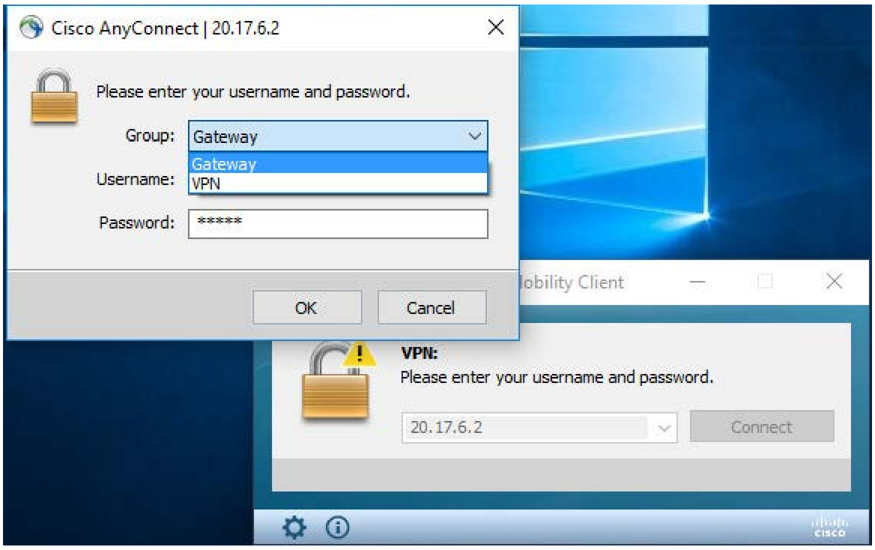
MONITORING AND BACKUP CONFIGURATION

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

WAN & VPN CONFIGURATION

1. Configure ISP router as PPPoE server and BR3 router as PPPoE client. Use PAP for authentication with **papuser\cisco1** credentials.

2. Configure DMVPN on HQ1, HQ2, BR2 and BR3 routers:
    a. Use Tunnel100 as VTI for all routers;
    b. Configure MTU 1400 on all VTIs;
    c. Configure IP addressing according to the VPN-diagram;
    d. Use GRE Multipoint mode;
    e. Use Loopback interface as tunnel source interface on each router according to the VPN-diagram;
    f. NHRP configuration:
        i. Network ID — **100**
        ii. Authentication key — **wsi2017**
    g. Use HQ1 router as DMVPN hub NHS server;
    h. Spoke routers should not use hub router for traffic transmission between each other;
3. Configure IKEv2 IPsec Site-to-Site VPN on FW1, FW2 firewalls:
    a. Phase 1 parameters:
        i. Hash – MD5
        ii. Encryption – AES-128
        iii. DH group – 5
        iv. Authentication – pre-shared key (**cisco1**)
    b. Phase 2 parameters:
        i. Protocol – ESP
        ii. Encryption – AES-128
        iii. Hash – MD5
    c. 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.
4. Configure SSL VPN server on FW2 firewall:
    a. Create local user **vpnuser** with **cisco1** password.
    b. Users should be able to connect using AnyConnect client. Deployment package is located on PC1 desktop.
    c. Create VPN address pool using following addresses: 10.255.255.1 - 10.255.255.30
    d. Create two tunnel groups — VPN and Gateway. After connection on login prompt user should be able to choose tunnel group from drop-down menu as shown on the picture below.



Cisco AnyConnect | 20.17.6.2

Please enter your username and password.

Group: Gateway

Username:

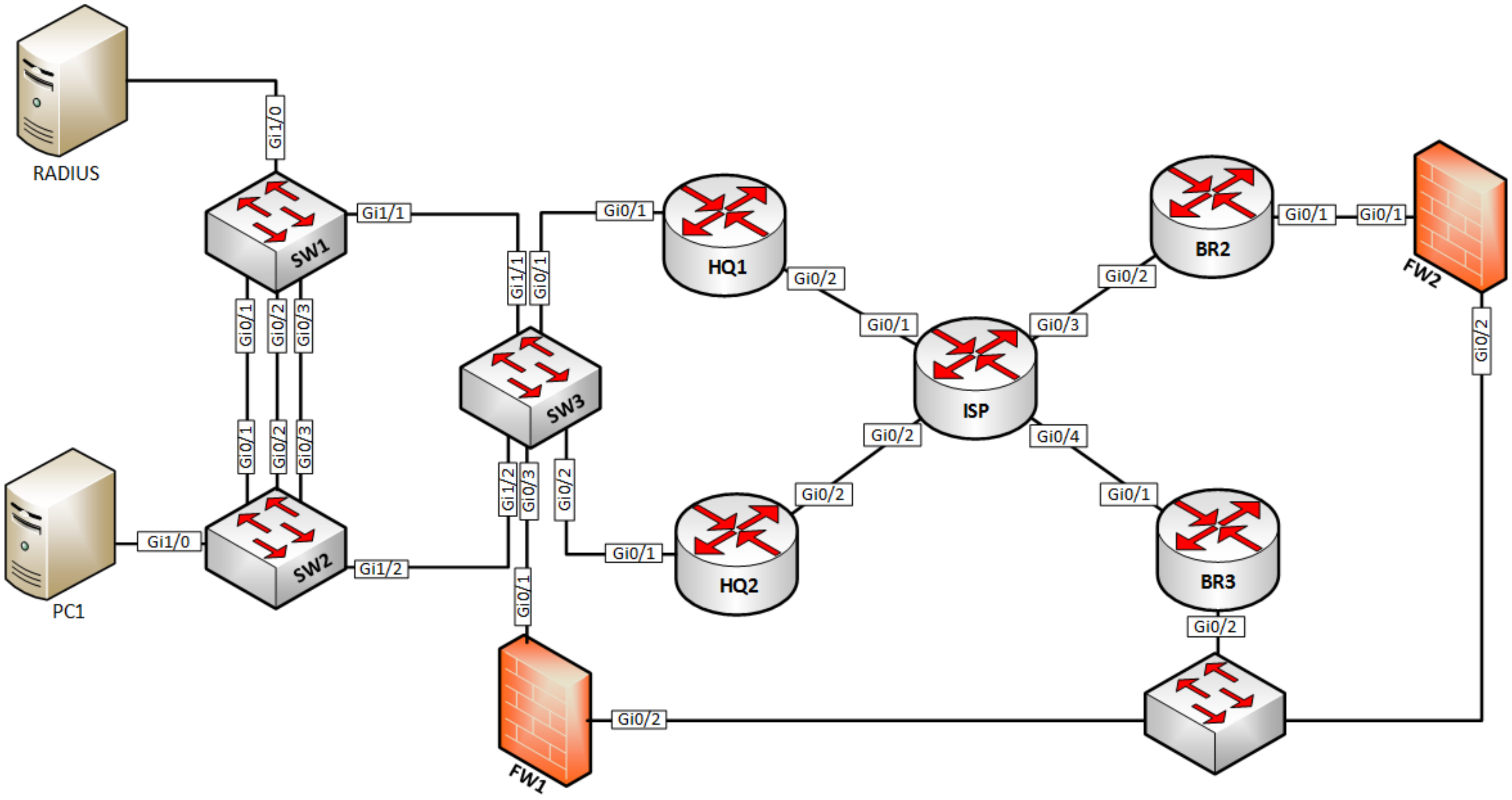
Password: *****

e. When choosing **VPN** profile client should receive secure-route list, which contains only route to Loopback20 subnet.

f. When choosing **Gateway** profile all traffic should be tunneled through SSL VPN tunnel.

d. When connecting from PC1, IP address of Loopback20 should be accessible for ICMP echo requests (using any connection profile).

Network Island.
L1 diagram



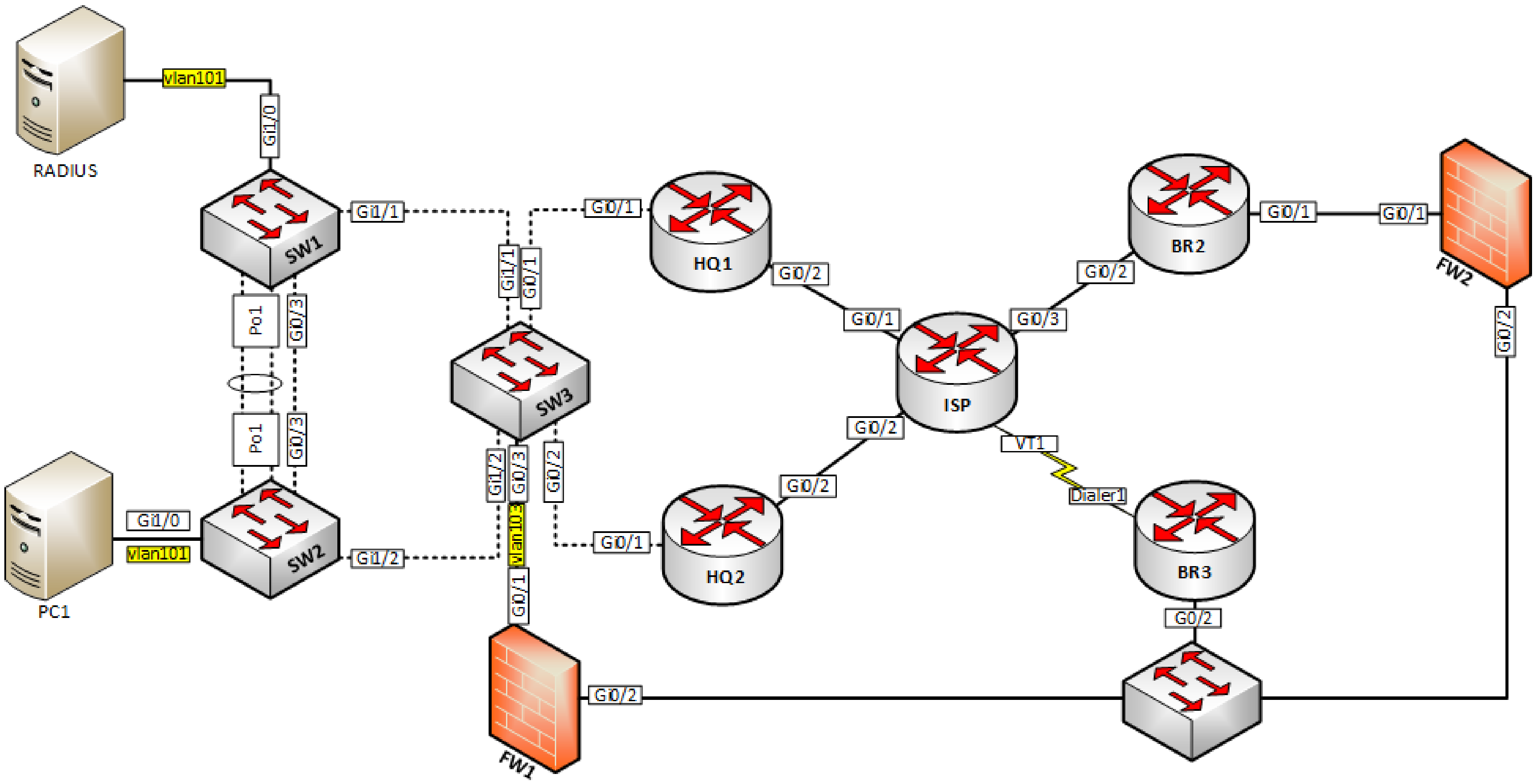
Legend

.... Ethernet IEEE 802.1Q trunk

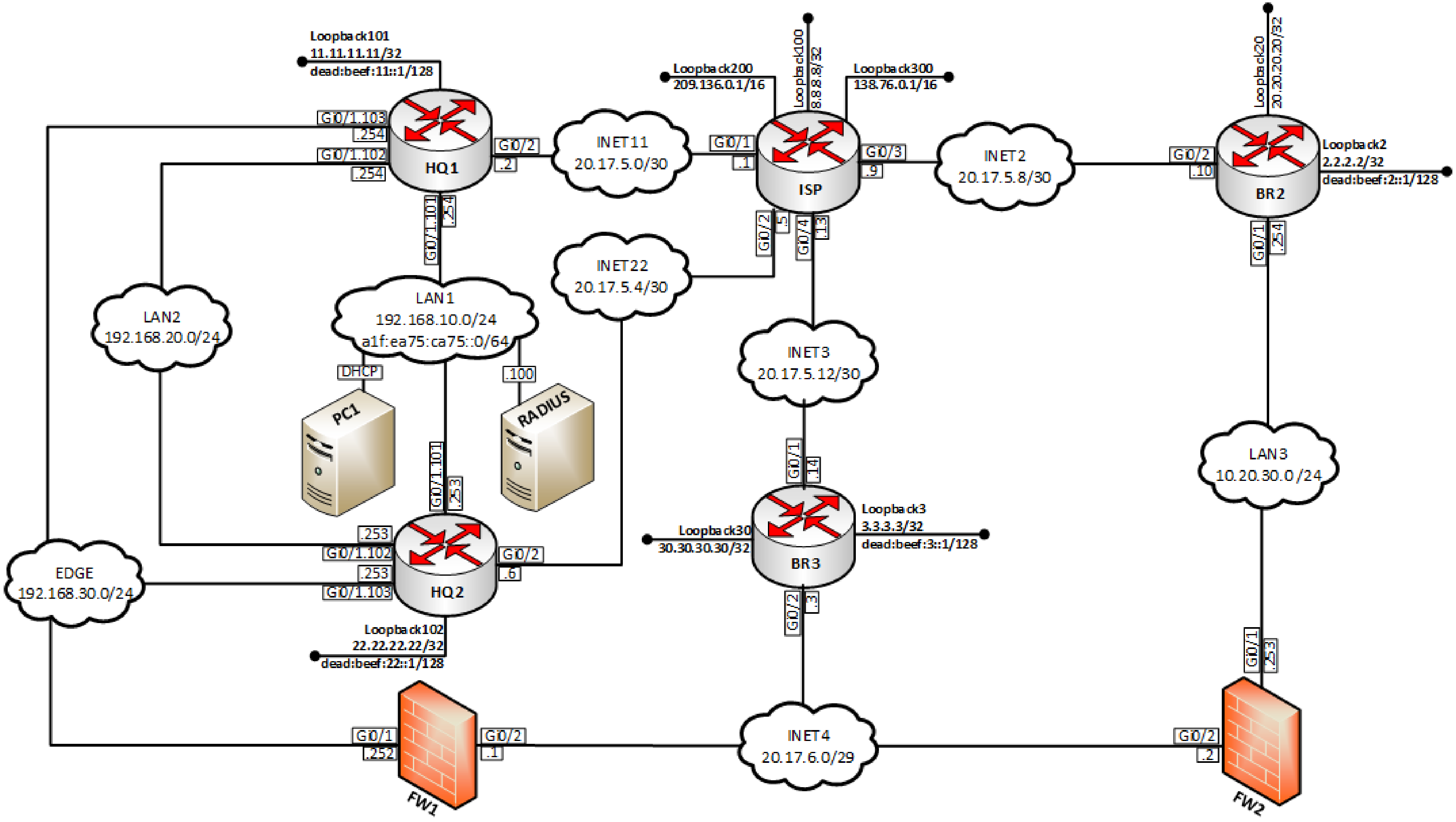
—vlan101— Ethernet IEEE 802.3 access port

....O.... Etherchannel

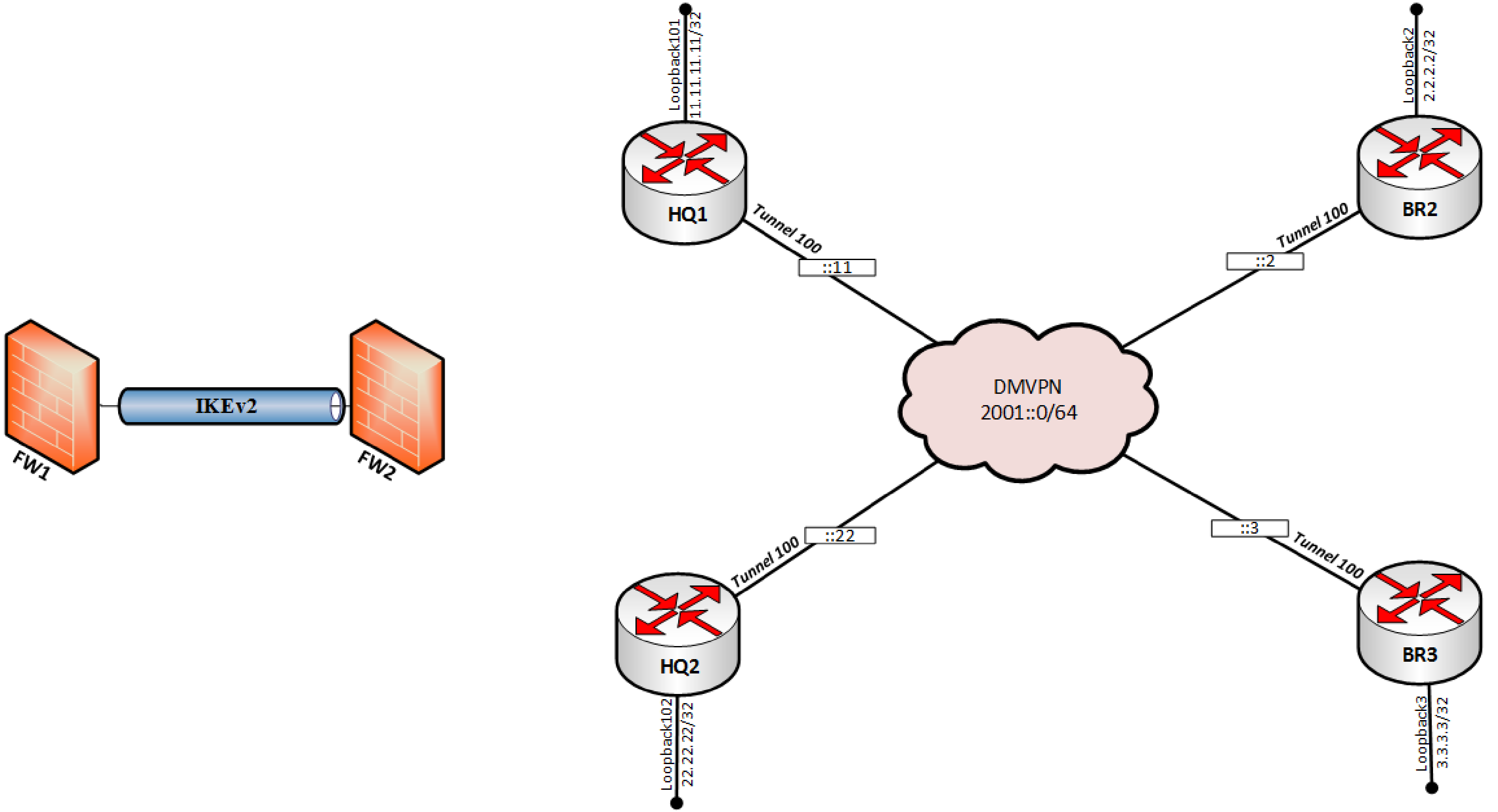
Network Island.
L2 diagram



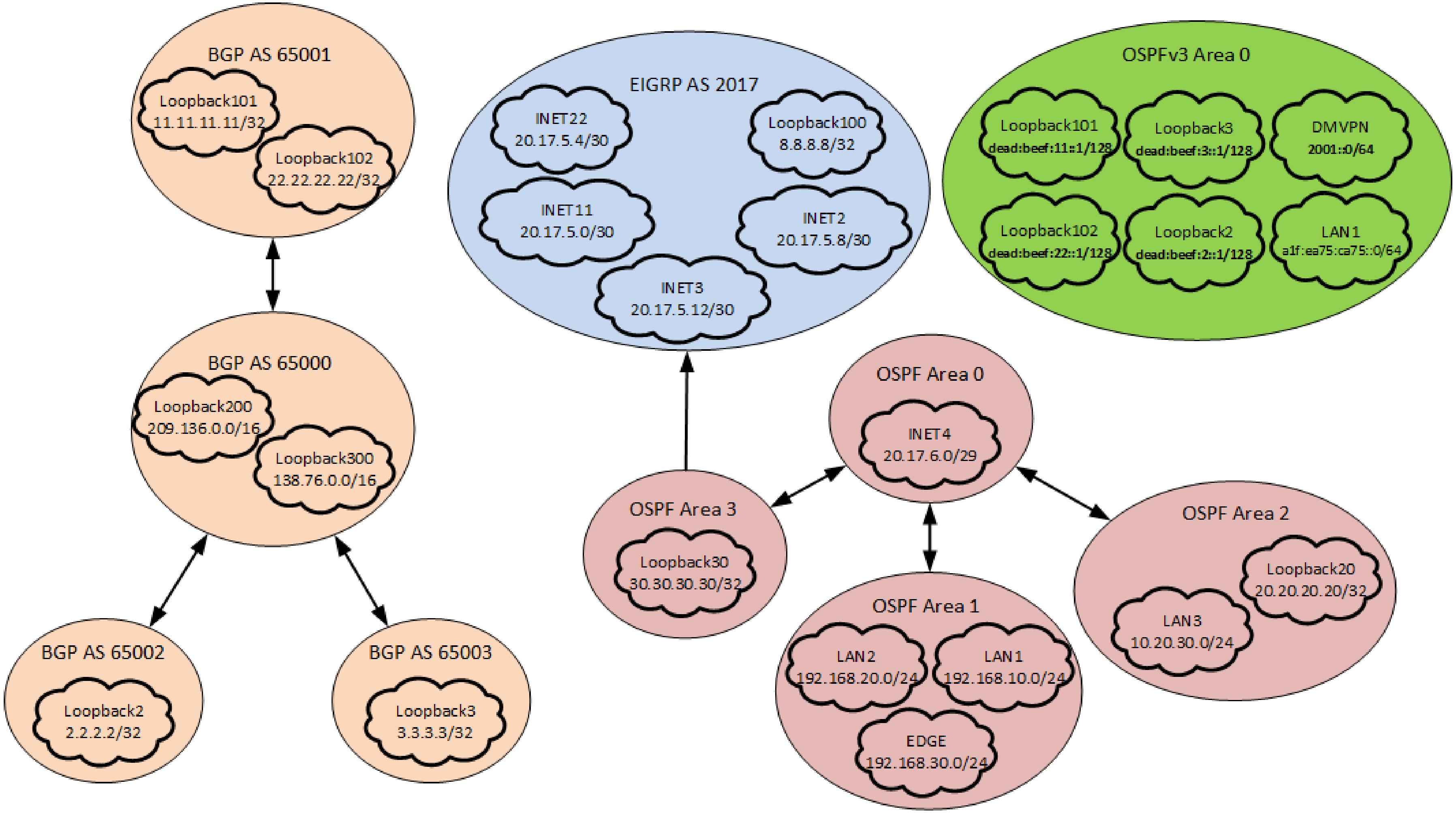
Network Island.
L3 diagram



Network Island.
WAN & VPN diagram



Network Island.
Routing diagram


BGP AS 65001
Loopback101
11.11.11.11/32
Loopback102
22.22.22.22/32
EIGRP AS 2017
INET22
20.17.5.4/30
Loopback100
8.8.8.8/32
INET11
20.17.5.0/30
INET2
20.17.5.8/30
INET3
20.17.5.12/30
OSPFv3 Area 0
Loopback101
dead:beef:11::1/128
Loopback3
dead:beef:3::1/128
DMVPN
2001::0/64
Loopback102
dead:beef:22::1/128
Loopback2
dead:beef:2::1/128
LAN1
a1f:ea75:ca75::0/64
BGP AS 65000
Loopback200
209.136.0.0/16
Loopback300
138.76.0.0/16
OSPF Area 0
INET4
20.17.6.0/29
OSPF Area 3
Loopback30
30.30.30.30/32
OSPF Area 2
Loopback20
20.20.20.20/32
LAN3
10.20.30.0/24
OSPF Area 1
LAN2
192.168.20.0/24
LAN1
192.168.10.0/24
EDGE
192.168.30.0/24
BGP AS 65002
Loopback2
2.2.2.2/32
BGP AS 65003
Loopback3
3.3.3.3/32