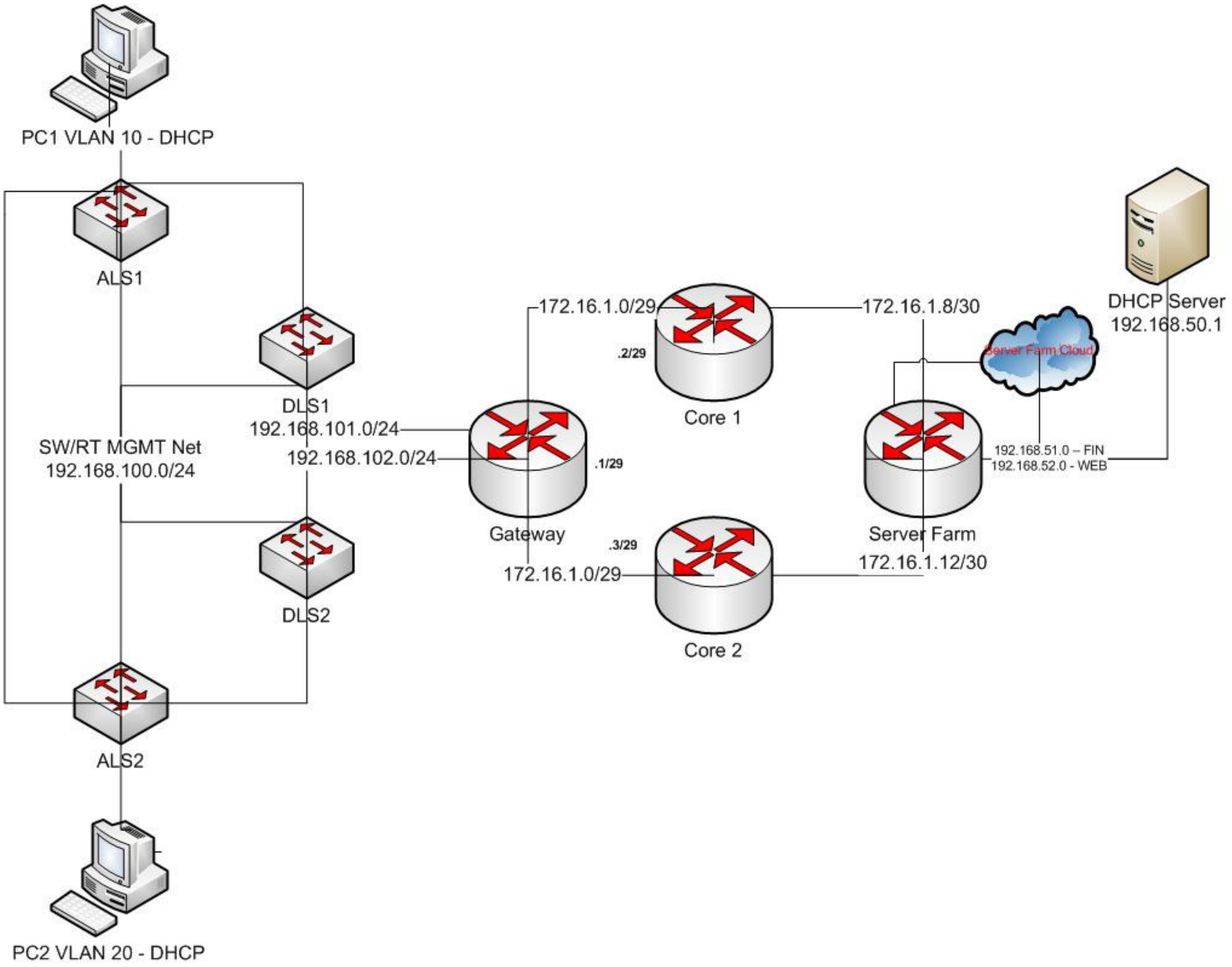
Lab 4 – Advanced Network Configurations



BEFORE YOU BEGIN – Clear all router/switch configurations and VLANs using the Introduction Lab as a guide if needed.

For this lab you will need:

- HQ - 5 Internal Subnets (VLANs)
  - VLAN 10 - 192.168.10.0/24 – PC with DHCP
  - VLAN 20 - 192.168.20.0/24 – PC with DHCP
  - VLAN 100 – 192.168.100.0/24 – used for switch and router management.
  - VLAN 101 – 192.168.101.0/24 – used for uplink to Gateway from DLS1

  - VLAN 102 – 192.168.102.0/24 – used for uplink to Gateway from DLS2 (possibly through trunks)

- Ethernet WAN Subnets and VLANs
  - 172.16.1.0/29 – Subnet for Routers GW, Core1, Core2 - VLAN 4
  - 172.16.1.8/30 – Subnet for Core1 to Server Router – VLAN8
  - 172.16.1.12/30 – Subnet for Core2 to Server Router VLAN12
- Server Farm Subnets
  - LB0 - 192.168.50.0 – AD (DHCP Server)
  - LB1 - 192.168.51.0 – Finance Server
  - LB2 - 192.168.52.0 – Web Server
- 6 Routers (2 used for hosts, 1 gateway router, 1 Server Farm Router, 2 WAN Routers)
- 2 Dist Layer 3 switch (DLS), 2 Layer 2 switches (ALS)

Start with a diagram/drawing. In doing this task, you will find what you need for the lab topology based on your pod diagram by figuring out what equipment and ports are needed.

Stuck? Ask your instructor or TA for assistance! This part is a crucial skill that you will need throughout the course.

Important! Review technologies from Labs 1-3, you will need to refer back.

Now that you have your diagram and ports laid out, we can start to configure the devices.

PART A - Basic Lab Setup:

Setup IP addressing as shown in the diagram, and in directions above. At this point you may not be able to ping between these IPs due to layer 2 access ports and trunks not being setup, and no layer 3 routing in place.

You will be setting up telnet and some AAA later in the lab, so make sure each router has an enable secret of ccie-1824.

Switching/VLANS - VTP and Spanning Tree:

VTP:

Setup VTP so the DLS switches are servers, ALS clients, and the VTP domain is your pod name/number, ie., POD1

VLANs:

Setup your VLANs on a VTP server, the VLANs you will need are outlined above.

Spanning tree:

Setup your spanning tree as follows:

DLS1 is Root Primary for VLANs 4,8,10,12,100,101

DLS2 is Root Primary for VLANs 20,102

You will need to setup all trunks between your switches as Etherchannels. Also, your trunks should **ONLY** carry the VLANs that are needed between those switches.

You will want to make sure your host traffic takes an optimal path back to the root. Also, your hosts should not wait for spanning tree to go through a full conversion each time they are brought online. You should also protect those ports from hearing BPDUs on those interfaces.

Hosts:

Setup IP addressing for your hosts to get DHCP from the DHCP server, 192.168.50.1 (LB0, SF Router). You will setup the DHCP server later. Disable IP routing on your "hosts".

Routing at HQ:

Setup EIGRP routing between DLS 1/2 and your gateway router. Your HQ location will be using EIGRP exclusively. You will redistribute with OSPF in the Core later in the lab.

Server Farm prep:

On your server farm router, you will need to simulate 3 servers using LB addresses, as outlined above. You will use the web and finance servers later in the lab. For now, setup the DHCP scopes for your 2 end user VLANs using the LB address of 192.168.50.1 as your DHCP server. (You will need a ip helper-address command on the proper interfaces for your end user VLANs.)

Routing with the Core and Server Farm:

All routing with the Core, Server Farm, and Gateway should be done according to your ISP, which runs OPSF. Setup all OSPF networks in area 0. Check your OSPF with your verification commands. Which router is the DR? Change it to a Core router if it isn't! (Priority, or highest LB method)

Route Redistribution:

Setup mutual route redistribution on your gateway router, between OSPF and EIGRP. This should be verified on both sides. Check your Distribution layer switch and your Server Farm router for all routes.

Verify that your hosts are now getting addresses via DHCP from the server farm subnets. Your helper address for DHCP should be configured on the gateway interfaces for the hosts, and should be the IP address used for the DHCP server.

PART B:

HSRP:

Setup HSRP with 2 Standby instances, use instance 10 for HSRP for vlan 10, primary router should be DLS1; Use instance 20 for VLAN 20, primary is DLS2. Verify all setup using the show standby command. Also, test your failover.

Now track your interfaces up to the Gateway routers. You should decrement your priority number enough so if you lose your uplink, it will take the other gateway.

Security at HQ, SSH with ACLs:

Setup ssh access to your gateway router so that only PC2 can get access. You will need the following commands to setup SSH and generate keys:

```
crypto key generate rsa general-keys modulus 1024
```

```
crypto ipsec security-association replay window-size 1024
```

```
ip ssh version 2
```

Use the line vty commands to make sure only SSH access is allowed on your lines. Also, you will need to use and access-class command to apply and access list so only PC2 can SSH to the device. Telnet should not be allowed.

AAA - Authentication:

Now that you have SSH setup, setup AAA authentication using a local username and password:

```
username GWADMIN password 0 ccie-1824
```

Use a Message of the day banner, use a AAA authentication login and login failed banner.

ACLs:

Setup an ACL that allows the following, and ensure proper placement on the network.

All traffic should be allowed to the web server for port 80.

DHCP traffic should only be allowed to the DHCP server.

Web traffic to the finance server should only be allowed for the subnet that PC1 resides on, no other traffic on any other port should be allowed to that server.

Lab Challenges:

1. Setup rapid spanning tree throughout the environment.
2. Setup MST in the environment so VLANs 10 and 20 use different instances, and distribute all other VLANs evenly between the 2 instances.
    a. Use the following Cisco link as a reference:

       http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/72844-MST.html
3. Setup the environment to use VRRP instead of HSRP. Use the chapter on router redundancy to help you.