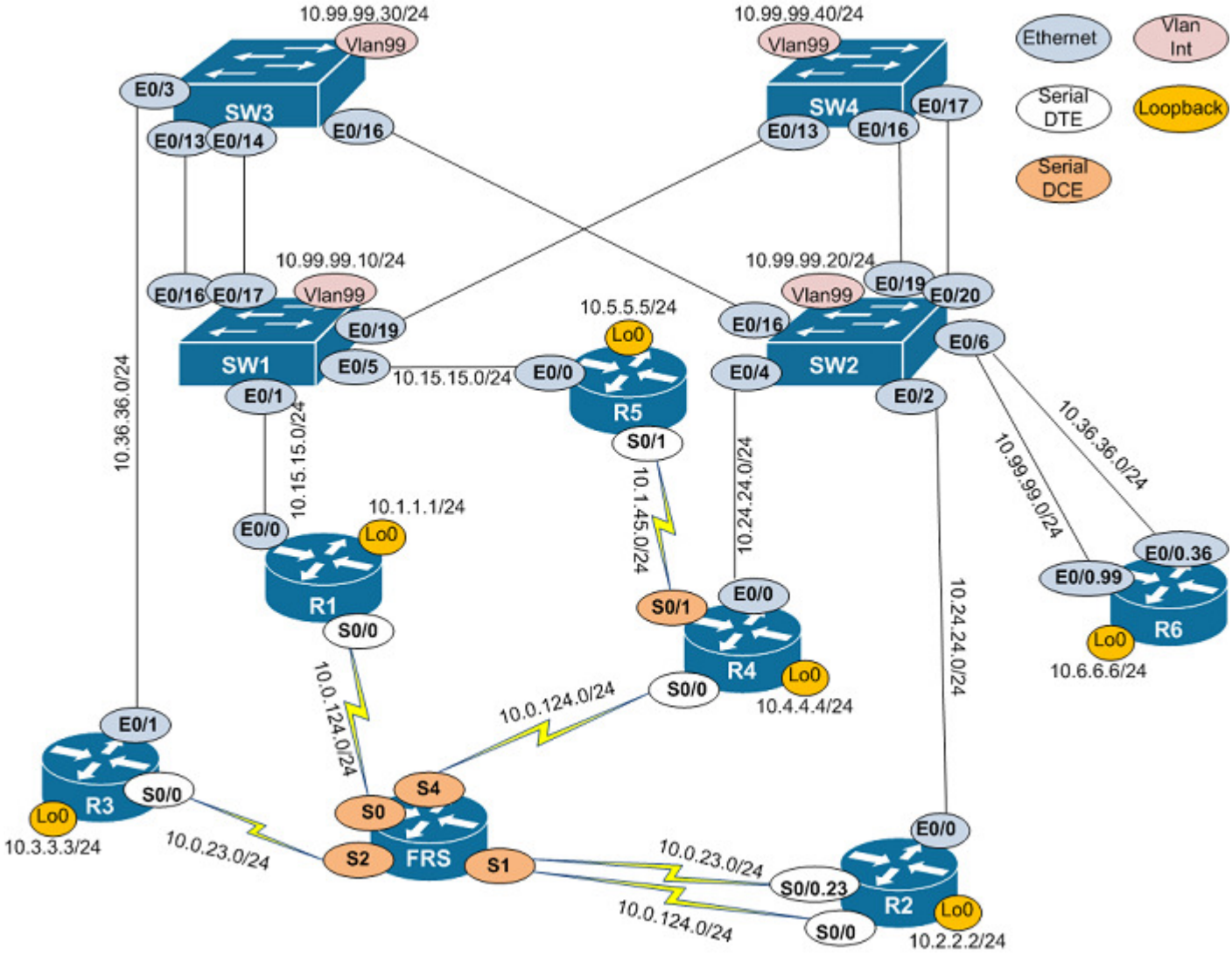
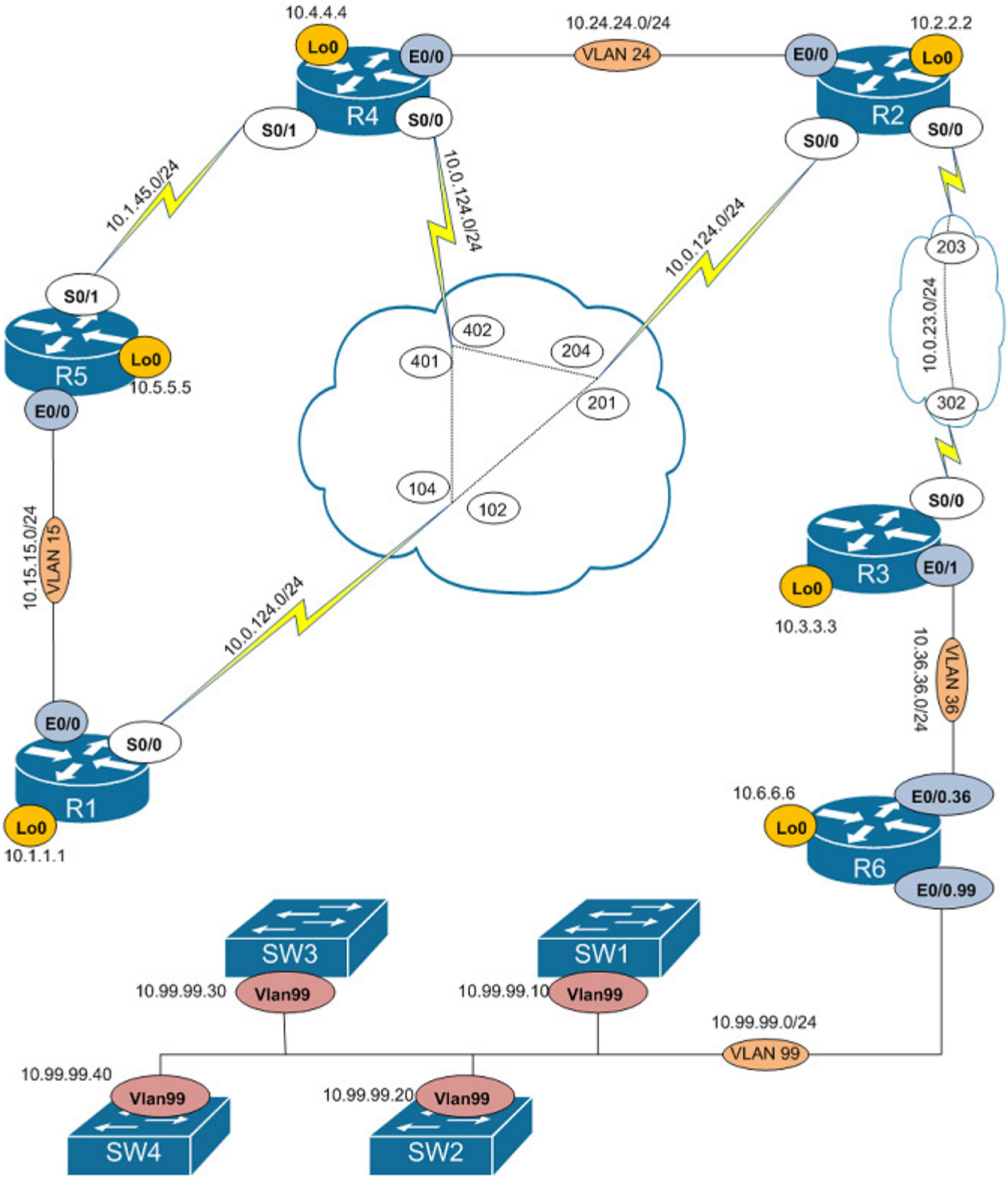
Technologies Covered

- Base Router Configuration
- Interface Configurations
- Virtual LAN (VLAN) Configuration [SVI & Etherchannel]
- IP Addressing
- Frame Relay [Static, IETF, LMI]
- RIP Routing
- EIGRP Routing
- OSPF Routing
- Static Routing
- Redistribution
- Network Address Translation (NAT)
- TCL Scripts / Lab Verification


10.99.99.30/24
Vlan99
SW3
E0/3
E0/13
E0/14
E0/16
10.99.99.40/24
Vlan99
SW4
E0/13
E0/16
E0/17
Ethernet
Vlan Int
Serial DTE
Loopback
Serial DCE
10.99.99.10/24
Vlan99
SW1
E0/16
E0/17
E0/19
E0/5
E0/1
10.99.99.20/24
Vlan99
SW2
E0/16
E0/19
E0/20
E0/6
E0/4
E0/2
10.5.5.5/24
Lo0
R5
E0/0
S0/1
10.15.15.0/24
10.36.36.0/24
10.15.15.0/24
10.1.45.0/24
10.24.24.0/24
10.99.99.0/24
10.36.36.0/24
10.1.1.1/24
Lo0
R1
E0/0
S0/0
R4
E0/0
S0/1
S0/0
Lo0
10.4.4.4/24
R6
E0/0.36
E0/0.99
Lo0
10.6.6.6/24
10.0.124.0/24
10.0.124.0/24
10.24.24.0/24
R3
E0/1
S0/0
Lo0
10.3.3.3/24
10.0.23.0/24
FRS
S4
S0
S2
S1
10.0.23.0/24
10.0.124.0/24
R2
E0/0
S0/0.23
S0/0
Lo0
10.2.2.2/24



ALL networks are /24

The purpose of this lab is to help you understand basic router and switch configuration, as well as introduce new technologies. Your goal for this lab is to configure a fully routed network so that each device can communicate with every other device.

Connect to your POD

Connect to a POD using any of the methods from previous labs

Base Configuration

When starting this lab, there are some basic things that will need to be done on every device. The following should be done at the start of every lab:

- Configure the device hostname
- Disable domain-name lookup
- Configure password encryption
- Set console timeout
- Configure `logging synchronous` on the console line
- Configure an enable secret of CCIE-1824 so you can use telnet

Remember that as you go through your lab to verify things as you do them.
Before moving on to routing, you should verify all local subnet connectivity.
Before moving on to redistribution, you should verify all intra routing process connectivity.

Interface Configuration

Turn on all necessary ports on all routers and switches. This Lab will use Loopback interfaces. Be sure to create them. Be sure to keep unnecessary ports administratively down & down. Remember to verify directly connected neighbors!

Use the show ip int brief, show int, ping, etc., to verify your interfaces.

Virtual Local Area Networks (VLANs)

Configure trunks on the following links: Pass only needed VLANs through these Trunks. Use the links shown on your PHYSICAL diagram.

- Switch 1 and Switch 4
- Switch 2 and Switch 3
- Switch 1 and Switch 3
- Switch 2 and Switch 4

Configure “Router to Switch” links appropriately; either as Access or Trunk ports as shown in your logical diagram.

Configure Switch 1 as a VTP server and the remaining Switches as VTP Clients. Put them in domain 'lab3' with password 'ccie-1824'.

Make sure VTP is functioning properly by checking VLANs and VTP Statuses on all Switches. Use the following commands:

Show vtp stat
Show vlan

Switch Virtual Interface

Switch Virtual Interface (SVI) are *LOGICAL* interfaces on Switches. They are created with the ***"Interface vlan [vlan number]"*** command.

Create SVIs on the Switches. Refer to the Diagram for the correct VLAN number.

EtherChannel

An EtherChannel combines multiple *PHYSICAL* links into one *LOGICAL* link. Think of it as bundling several links into one big link. There are two encapsulation types for EtherChannel, LACP and PAgP. LACP is open standard. PAgP is Cisco proprietary.

Create two EtherChannels, one using the links between Switch 1 & 3, and the other between Switch 2 & 4. Use Channel Group 1. Enable the EtherChannel to use Cisco proprietary encapsulation, unconditionally. Create a Port Channel Interface. Make sure it's interface number matches your Channel Group number.

***The Channel Group prepares EtherChannel. The Port Channel Interface is your bundled *LOGICAL* link. In order for EtherChannel to function properly, you must configure this Port Channel Interface as you would a regular *PHYSICAL* trunk link.

IP Addressing

Configure IP Addresses on all interfaces (including SVIs and Loopbacks) except those attached to Frame Relay subnets. Verify connectivity between devices on a common subnet.

In order for the switches to be able to communicate with the rest of the network, they need default routes. Configure a default gateway on all Switches to point to **10.99.99.6**.

Frame Relay [Static, IETF, LMI]

We will introduce you to two new aspects of Frame Relay, IETF and LMI type. IETF is a Frame Relay encapsulation type that allows inter-operability between Cisco and non-Cisco devices. Local Management Interface types (LMI) are interface level 'encapsulation' types. LMI status messages are sent out Frame Relay interfaces. There are three LMI types: Cisco, ANSI, and Q933.

Configure Static Frame Relay. Set up the FRS and devices connected to the Frame Relay Cloud. Remember the configuration differences between Static and Dynamic Frame Relay. Instead of your regular Cisco proprietary Frame Relay encapsulation type, use IETF. Set Frame Relay interfaces to use LMI type ANSI. Frame Relay may not function properly due to mismatched LMI types. Change some to see what happens in a mismatch. Sub-interfaces should be POINT-TO-POINT.

RIP Routing

The network command in an IGP does two things: It enables network updates out all interfaces that match that network address, and it starts advertising all networks that match that network address.

Configure RIP version 2 on Routers 3 and 6. Make sure RIP is advertised on VLAN 36 ONLY. Advertise the loopbacks on R3 and R6. Verify configuration and routing table.

EIGRP Routing

Configure EIGRP on Routers 2, and 3 using Autonomous System 23. Advertise all local networks with a /24 wildcard mask. Advertise the loopbacks on R2 and R3, also with a /24 mask. Do not auto-summarize. ("no auto-summary" is now default in 15.x versions) Verify configuration and routing table using the following commands:

Show ip route
Show ip eigrp neighbors
Show ip eigrp topology
Show ip eigrp interfaces

OSPF Routing

Configure OSPF on Routers 1, 2, 4, and 5. Use Process ID 12. Put all OSPF Routers in Area 0. Advertise all local networks with a /24 wildcard mask.

There are some additional things you should note with OSPF in this Lab. In order for OSPF to work over this Frame Relay, the network type needs to be changed. By default, OSPF uses Non-Broadcast Multi Access (**NBMA**), which does not discover neighbors automatically. An additional command is needed on OSPF Router Interfaces that are connected to Frame Relay. Change the OSPF Network type on Routers 1, 2, and 4 to **BROADCAST**.

Use the "ip ospf network " command to do this, example:

ip ospf network broadcast

By default, OSPF advertises loopback interfaces with a host mask. A host mask is a subnet mask with a value of 255.255.255.255 or /32. We need to change the Network Type to advertise a loopback with its actual mask. Change the OSPF Network type on all OSPF Router Loopbacks to **POINT-TO-POINT**

Static Routing

Static Routing is routing in its simplest form. Because of its basic nature, you have complete control over the packet's path. However, static routing cannot adapt to any changes in links or ip addresses. It also requires manual configuration for EVERY route on EVERY router. This may work for smaller networks that do not change much, but it becomes impossible for larger networks.

Configure a static route on Router 3 to Router 6's loopback 10.6.6.6. You can configure it with either *next-hop address* or *egress interface*.

Redistribution

Perform mutual Redistribution on Router 3 between EIGRP and RIP. Perform mutual Redistribution on Router 2 between EIGRP and OSPF. Redistribute the static route on Router 3 into both EIGRP and RIP. Verify Layer 3 connectivity and routing tables.

You can use the following example of redistribution. Also, use the show ? command after the redistribute “protocol” command to see what will be needed for seed metrics.

Examples:

GATEWAY(config-router)#router rip
GATEWAY(config-router)#redistribute ospf 1 metric 4
GATEWAY(config-router)#
GATEWAY(config-router)#router ospf 1
GATEWAY(config-router)#redistribute rip metric 1000 subnets

Note that in this example the seed metric for OSPF routes INTO RIP needs a seed metric for “hops”, and RIP INTO OSPF redistribution needs a “cost” seed metric.

Network Address Translation (NAT)

Network Address Translation is a temporary solution to the lack of IPv4 addresses. It allows for the expansion of one public address into many private ones. For example, there is one Router that connects out to the Internet. We will refer to the Internet side as the "outside". The other side, your internal network, will be referred to as the "inside". The Internet will see your entire internal network as ONE PUBLIC IP ADDRESS. As you know, private IPs are not routable. The Router that acts as the gateway between the Internet and internal network. Your book has excellent coverage of the topic. We will be configuring PAT (NAT Overloading) and using a loopback as one of the inside ip addresses. Use your book as a reference.

- Configure PAT on Router 1
- The FastEthernet interface i.e 10.15.15.1 is your "outside" pool
- Name your NAT Pool "FR_NAT"
- Use an address range of 192.168.254.1 to 192.168.254.254 for your "inside" address
- Set the IP address of the "Inside" interface (Looback 1) to 192.168.254.1

- Verify by using **debug ip nat** and then pinging from R1 using the loopback as source. After that also use the **show ip nat translations** command

TCL Scripts / Lab Verification

For any ping that fails, go back and recheck the previous sections of the lab. Do the best you can to troubleshoot. If you cannot figure it out, call over a TA to help you.

```
tclsh
foreach address {
   10.15.15.1
10.1.1.1
10.0.124.1
10.24.24.2
10.2.2.2
10.0.23.2
10.0.124.2
10.36.36.3
10.3.3.3
10.0.23.3
10.24.24.4
10.4.4.4
10.0.124.4
10.1.45.4
10.15.15.5
10.5.5.5
10.1.45.5
10.99.99.6
10.36.36.6
10.6.6.6
10.99.99.10
10.99.99.20
10.99.99.30
10.99.99.40
} {
   ping $address
   }
tclquit
```