Seattle Cisco Users Group

CCNA Lab Project #2

Joe Rinehart

MBA, CCIE #14256

CCNP/DP/VP

June 2, 2011

Table of Contents

1. Introduction

1.1. The CCNA Certification

Source: http://www.cisco.com/web/learning/le3/le2/le0/le9/learning_certification_type_home.html

The Cisco Certified Network Associate certification has traditionally been the point of entry for many network engineers into the world of Cisco networking. In 2007, Cisco created a new entry-level certification entitled the CCENT, or Cisco Certified Entry Level Technician. To achieve the CCNA certification, candidates must successfully pass the 640-802 CCNA exam (single exam), or the two Interconnecting Cisco Networking Devices exams (640-822 and 640-816).

The CCNA certification validates the skill-sets needed to configure and operate medium-sized routed and/or switched internetworks, including (but not limited to) the following topic areas:

- Mitigation of basic security threats
- Wireless networking
- Frame-Relay Wide Area Networks
- OSPF/EIGRP/RIPV2 IP Routing
- Virtual Local Area Networks (VLANs)
- Ethernet Local Area Networks
- Access Control Lists (ACL's)
- Internet Protocol Version 6

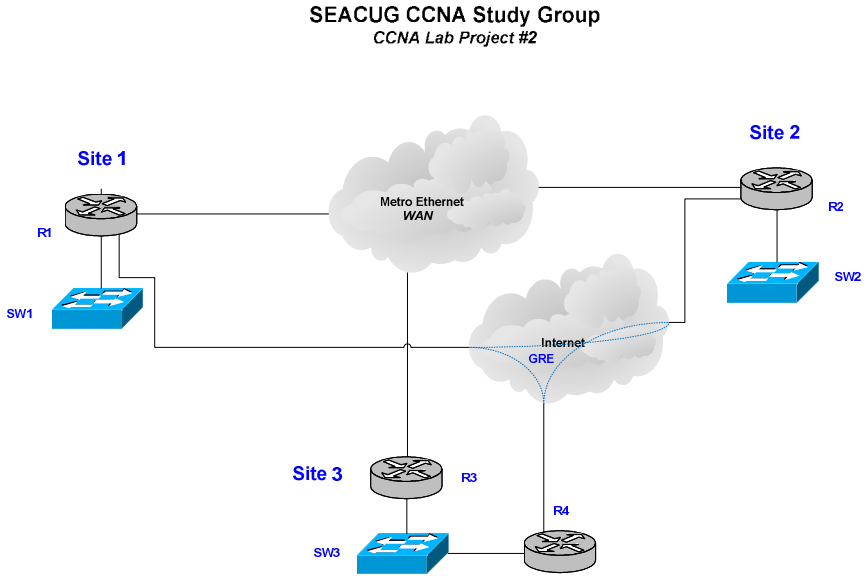
1.2. Purpose of the Lab Project

A thorough understanding of networking concepts is the foundation upon which understanding is essentially built. While theoretical knowledge is important, the application of that knowledge is equally important, and forms the basis for effective performance in real-world environments. Early versions of the CCNA-level certification exams concentrated on factual knowledge, while current exams utilize realistic scenarios that reflect more "hands on" experiences. To satisfy these types of requirements, CCNA students need practical, experience-based exercises.

1.3. Overview

The well-known CCIE Lab exam is composed of an eight-hour set of configuration scenarios designed to test the absolute limits of a candidate's practical knowledge. While the tasks do not represent "best-practice" applications, the challenges certainly demand a thorough knowledge of every technical aspect involved in networking. As the current exam pass-rates will demonstrate, only the most well-prepared participants will possess the discipline and skills to successfully complete the exam requirements. Mirroring the same demands at a level appropriate to the CCNA certification, the CCNA project seeks to create an environment for hands-on experience necessary to successfully complete the certification exam environment.

1.4. Basic Topology

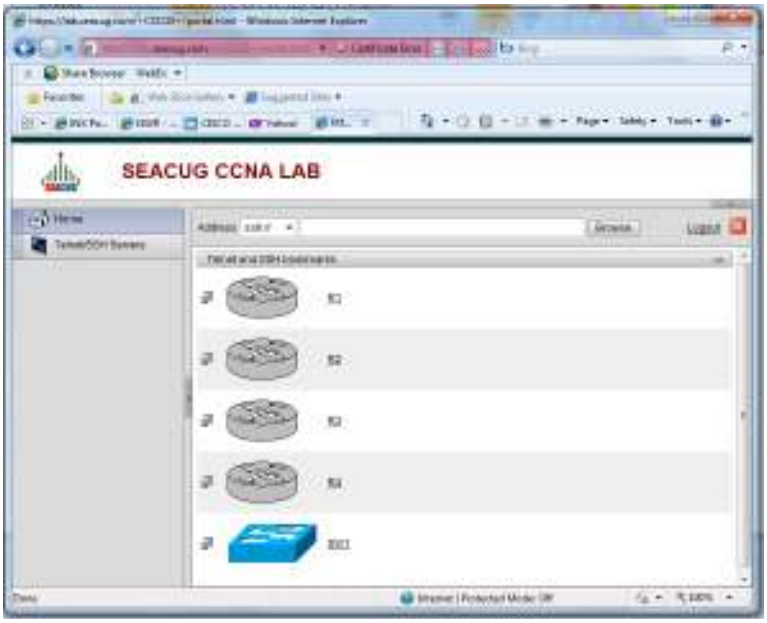


The CCNA project involves the use of four routers and three switches to emulate the complexity of a medium-sized routed and switched network. The topology involves three separate locations/sites across a simulated Metropolitan Ethernet frame-relay Wide Area Network (WAN) as well as distinct Local Area Networks (LANs). In addition, Internet access is included to mirror real-world applications, with VPN backup.

1.5. Lab Access

The Seattle Cisco Users Group (www.seacug.com) provides study opportunities through CCNA study groups, usually held twice a year. At present, INX (www.inxi.com, a premier

Cisco Gold Partner), provides Internet-based access to lab equipment designed to satisfy the requirements of the CCNA project outlined here. An SSL-based clientless Virtual Private Network (VPN) allows secure access to a lab environment compatible with the project requirements. The lab is accessible at https://lab.seacug.com and requires username/password access arranged in advance. The portal appears as follows:



2. Lab Exercises

2.1. Initial Configuration Tasks

The CCNA project requires certain basic configuration information in order to function properly. These requirements lay the foundation of successful completion of all later tasks.

2.1.1. Basic Information

All VLAN, IP Addressing, and interface addressing requirements are as follows:

VLAN Assignments
Management VLAN ID – X IP - 192.168.X.0
Production VLAN ID – X IP - 192.168.XX.0
Internet VLAN ID – 99 IP - 10.99.99.0
X=Site Number

Interface IP Assignments
Loopback 10.X.X.X/32
Metro-E 172.16.123.X
GRE Tunnels R1-R2 172.16.12.X R1-R3 172.16.13.X R2-R3 172.16.23.X
X=Site Number

2.1.2. Configure Device Host Names

All devices used in the project require host names as part of the requirements. Use the following naming conventions:

Routers: RX (X=Site Number)
Switches: SWX (X=Site Number)
Internet Router, Site 3: R4

2.1.3. Configure Device Access

Each device within the overall lab environment has different methods of access that must be configured and secured accordingly. Configure each access method as follows:

- Console Access
    - Create login process to go directly to privileged mode
    - Use password **cisco**
    - No requirement to enter a password to access
- AUX Access (router only)
    - Create login process to enter exec mode
    - Use password **cisco**
    - Login required
- VTY Access (telnet/ssh)
    - Create login process to enter exec mode
    - Use password **cisco**
    - Login required

2.1.4. Configure Basic Security Settings

All devices within a network must implement certain basic security settings in order to ensure consistent operation. Configure these settings as follows:

- Enable Secret
    - Cisco devices require a second password to enter privileged mode, which can be enable (not encrypted) or enable secret (encrypted)
    - Set the enable secret password to **cisco**
    - Do not set the enable (non-encrypted) password
- Secure telnet/ssh access
    - Create an access-list to restrict remote access only within the network
    - Apply the access list in the appropriate location on all devices

2.1.5. Configure Other Basic Device Settings

Specific device settings can simplify management and operation within the network. Configure these settings as follows:

- Set clocks on all devices to Pacific Time, including Daylight Savings Time settings
- Disable devices from using DNS lookups
- Disable web-based access on all devices
- Set login message to “Welcome to the CCNA Metro-E Lab!”
- Set all devices to update their clocks based on the time configured on R4

2.2. Local Device Interface Configuration Tasks

Every networking device in the environment has multiple interfaces that require specific configuration tasks in order to provide connectivity to resources.

2.2.1. VLAN Interfaces

All sites have multiple VLAN segments that require configuration to be applied on the LAN switch as well as the site router. Configure the following VLANs at each site in the topology:

- **Management VLAN**: Used for managing all remote devices by resources at the central data center (R1/R2/R3 Only)
    - Set the VLAN ID to X (X=Site Number)
    - Name the VLAN **MANAGEMENT VLAN**
    - Create IP addressing to allow for 5 usable Hosts
- **Production VLAN**: Used for normal network operations (R1/R2/R3 Only)
    - Set the VLAN ID to XX (X=Site Number)
    - Name the VLAN **PRODUCTION VLAN**
    - Create IP addressing to allow for 20 usable Hosts
- **Internet VLAN**: Used for providing Internet access through the Internet connection at all sites
    - Set the VLAN ID to 99
    - Name the VLAN **INTERNET VLAN**
    - Create IP addressing to allow for 15 usable Hosts

2.2.2. Loopback Interfaces (R1/R2/R3 Only)

Loopback interfaces are logical interfaces that do not go down unless the device itself is no longer operational. Tying device processes to loopback interfaces prevent intermittent issues resulting from links going up and down.

- Create a loopback interface for each router in the network
- Assign the name **Loopback 0** to each loopback interface
- Assign IP subnet for a single host: 10.Y.Y.Y (Y=device number)

2.2.3. Metro-Ethernet WAN Interfaces (R1/R2/R3 Only)

All three sites in the network are linked by a simulated Metropolitan Ethernet Service. Configure WAN access on these interfaces as follows:

- Create subinterfaces using site numbers for reference (e.g., FastEthernet 0/0.1 for R1)
- Specify 802.1Q Encapsulation and Assign to VLAN 123
- Assign IP addresses per diagram, with 12 usable hosts per subnet

2.2.4. GRE VPN Backup WAN Interfaces

Backup network connectivity is required in the event of failure on the Metro-E service. Configure VPN access on the Internet interfaces as follows:

- Create a full-mesh tunnel configuration between all sites
- Specify GRE IP Encapsulation for the tunnels
- Enable CDP on the tunnels
- Specify the source as Fa0/0.99
- Specify the destination as the DHCP assigned address of the destination router
- Assign IP addresses per diagram, with 5 usable hosts per subnet

2.2.5. Internet WAN Interfaces

All sites receive their Internet access locally through an Ethernet handoff:

- Create subinterfaces using 99 as the reference number reference (e.g., FastEthernet 0/0.99)
- Specify 801.1Q Trunking Encapsulation and 99 as the VLAN ID
- Configure the interface to receive its IP addressing information through DHCP from the service provider

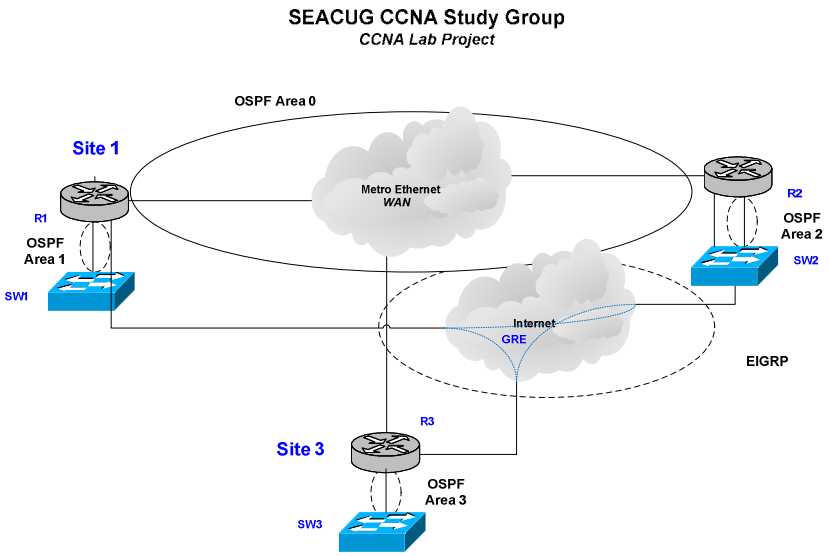
2.2.6. DHCP Configuration

R4 will act as the upstream service provider router, providing Internet access to all sites and providing IP addressing information by DHCP. Configure as follows:

- Enable DHCP on R4 to supply addressing to R3 on VLAN99
- Identify the following parameters:
    - Name the Address Pool **INTERNET_VLAN**
    - Network: 10.99.99.0
    - Default Gateway: 10.99.99.4
    - DNS (use 216.136.95.2 and 64.132.94.250)
    - Exclude IP addresses 10.99.99.1 through 10.99.99.4 from being allocated

2.3. Routing Protocol Configuration Tasks

Multiple routing protocols are in use throughout the network and require careful configuration to ensure correct operation. Refer to the following diagram as a reference point:



2.3.1. OSPF Configuration

OSPF is the primary routing configuration in use throughout the network, and must be operational at all three sites. Configure routing as follows:

- R1 OSPF Configuration
    - Place the Metro Ethernet interface in area 0
    - Place all local VLAN interfaces and the loopback interface in area 1
    - Set **Loopback 0** as the OSPF router-id
- R2 OSPF Configuration
    - Place the Metro Ethernet interface in area 0
    - Place all local VLAN interfaces and the loopback interface in area 2
    - Set Loopback 0 as the OSPF router-id
- R3 OSPF Configuration
    - Place the Metro Ethernet interface in area 0
    - Place all local VLAN interfaces and the loopback interface in area 3
    - Set **Loopback 0** as the OSPF router-id

2.3.2. EIGRP Configuration

EIGRP is in use to provide backup connectivity to the Internet in the event of an outage on the OSPF network. Configure EIGRP routing as follows:

- R1 EIGRP Configuration
    - Use AS Number 111
    - Enable EIGRP on all GRE tunnel interfaces
    - Disable auto summarization
- R2 EIGRP Configuration
    - Use AS Number 111
    - Enable EIGRP on all GRE tunnel interfaces
      Disable auto summarization
- R3 EIGRP Configuration
    - Use AS Number 111
    - Enable EIGRP on all GRE tunnel interfaces
    - Disable auto summarization

2.3.3. Redistribution and Tuning Configuration

With multiple routing protocols in use, full connectivity must be created between protocols to allow consistent communication. Configure as follows:

- Do not redistribute EIGRP or OSPF
- Configure EIGRP to Perform Backup Routing upon Failure of the Metro Ethernet Service
- Do not configure any static routes to accomplish this task
- Verify full reachability:
    - Ping all other devices in the network from each device
    - Successfully telnet to all devices in the network from each device

2.4. Network Address Translation Tasks

All sites within the network utilize addressing from the RFC 1918 Private Addressing space, which are not valid on the Internet. In order to have full Internet connectivity, all internal addressing must be mapped to globally routable addressing space. In addition, an internal web server at Site 2 must also be accessible from the Internet

2.4.1. Configure Port Address Translation for All Internal Hosts

Ensure that all devices at each site within the internal network may access sites on the Internet. Do not apply any filtering to this configuration.

2.4.2. Static Network Address Translation for a Web Server on R2

Http services were previously enabled on R2 and accessible from within the internal network, but need to be available on the Internet for monitoring and management purposes. Using static a NAT entry, point internal web connections to R2's Production VLAN address.

2.5. Security Configuration Tasks

Preventing unauthorized access to devices on the network may be supplied in part by the external ASA firewall, but additional measured need to be implemented to protect information assets.

2.5.1. Create and apply an access that will only allow internal devices to access the management VLAN on all devices.

The company's information security policy stipulates that no users outside of the company are permitted to access internal resources. To prevent unauthorized access, disallow all outside users from accessing the hosts within the protected network.

2.5.2. Block SNMP access to all devices

SNMP protocols are a source of security concerns for the management team and they have elected not to permit it anywhere on the network. Configure the appropriate packet filters/access-lists to block all SNMP access to/from all sites.

2.5.3. Block all external access trying to reach the management VLAN

Remote access has been provided at the primary corporate location for the purpose of managing all internal network resources. Because of the sensitive nature of the data at the corporate locations, external access to the Management VLANs is not permitted by the security policy. Construct an access list to block any attempt at access from the Internet interface.

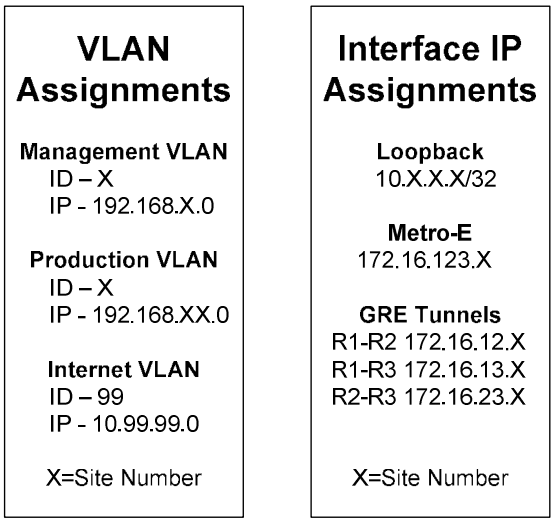
3. Answer Key

The following section outlines detailed, step-by-step solutions to the previous configuration requirements. This allows students to compare their own devices against the answers, keeping in mind that some minor differences may exist. In the SEACUG lab environment, for example, only a single switch is utilized for the topology. Answers are displayed in **bold** following restatement of the original configuration tasks.

3.1. Initial Configuration Tasks

3.1.1. Basic Information

All VLAN, IP Addressing, and interface addressing requirements are as follows:



ANSWERS:

All configuration tasks utilize these addressing specifications.

3.1.2. Configure Device Host Names

All devices used in the project require host names as part of the requirements. Use the following naming conventions:

Routers: RX (X=Site Number)
Switches: SWX (X=Site Number)
Internet Router, Site 3: R4

ANSWERS:

R1

Hostname R1 (lab may already have hostname(s) configured)
R2

Hostname R2 (lab may already have hostname(s) configured)

R3

Hostname R3 (lab may already have hostname(s) configured)

R4

Hostname R4 (lab may already have hostname(s) configured)

SW1

Hostname SW1 (lab may already have hostname(s) configured)

**** If using three switches, substitute SW2, SW3, etc. for additional switches ****

3.1.3. Configure Device Access

Each device within the overall lab environment has different methods of access that must be configured and secured accordingly. Configure each access method as follows:

- Console Access
  - Create login process to go directly to privileged mode
  - Use password **cisco**
  - No requirement to enter a password to access

ANSWERS:

**** The *privilege level* command sets the default permission level available ****
**** The *password* command specifies the access password ****
**** The *login* command causes a required login process*; no login* disables it ****

R1

```
line con 0
password cisco
privilege level 15
no login
```

R2

```
line con 0
password cisco
```

privilege level 15
no login

R3

line con 0
password cisco
privilege level 15
no login

R4

line con 0
password cisco
privilege level 15
no login

SW1

line con 0
password cisco
privilege level 15
no login

**** If using three switches, duplicate configuration for additional switches ****

- AUX Access (router only)
  - Create login process to enter exec mode
  - Use password **cisco**
  - Login required

ANSWERS:

**** The *password* command specifies the access password ****
**** The *login* command causes a required login process*; no login* disables it ****

R1

line aux 0
password cisco
login

R2

line aux 0
password cisco
login

R3

line aux 0
password cisco
login

R4

line aux 0
password cisco
login

- VTY Access (telnet/ssh)
    - Create login process to enter exec mode
    - Use password **cisco**
    - Login required

ANSWERS:

**** Available VTY lines vary by device, each of which is configurable separately****
**** Programming multiple VTY requires specifying the range, the 2620 has 181 ****
**** The *login* command causes a required login process*; no login* disables it ****

R1

line vty 0 181
password cisco
login

R2

line vty 0 181
password cisco
login

R3

line vty 0 181
password cisco
login

R4

line vty 0 988
password cisco
login

SW1

line vty 0 15
password cisco
login

**** If using three switches, duplicate configuration for additional switches ****

3.1.4. Configure Basic Security Settings

All devices within a network must implement certain basic security settings in order to ensure consistent operation. Configure these settings as follows:

- Enable Secret
  - Cisco devices require a second password to enter privileged mode, which can be enable (not encrypted) or enable secret (encrypted)
  - Set the enable secret password to **cisco**
  - Do not set the enable (non-encrypted) password

ANSWERS:

**** The *enable secret* command encrypts the password even in the configuration ****
**** Remember that the passwords you specify are case sensitive ****

R1

Enable secret cisco

R2

Enable secret cisco

R3

Enable secret cisco

R4

Enable secret cisco

SW1

Enable secret cisco

**** If using three switches, duplicate configuration for additional switches ****

- Secure telnet/ssh access

- Create an access-list to restrict remote access only within the network
- Apply the access list in the appropriate location on all devices

ANSWERS:

**** Access control utilizes access lists for these types of functions ****
**** Standard access lists (1-99) filter only by source ****
**** Extended access lists (100-199) can filter by source, destination, TCP/UDP, etc. ****
****At the end of every access list an implicit *deny all* statement ****
**** Specifying all addresses ranges in use will satisfy the requirements ****
**** Applying the list on the Virtual Terminal lines (VTY) is best, using the *access-class* command ****

R1

```
access-list 1 permit 10.2.2.2
access-list 1 permit 10.3.3.3
access-list 1 permit 10.1.1.1
access-list 1 permit 192.168.1.0 0.0.0.7
access-list 1 permit 192.168.11.0 0.0.0.31
access-list 1 permit 192.168.2.0 0.0.0.7
access-list 1 permit 192.168.22.0 0.0.0.31
access-list 1 permit 192.168.3.0 0.0.0.7
access-list 1 permit 192.168.33.0 0.0.0.31
access-list 1 permit 10.99.99.0 0.0.0.31
access-list 1 permit 172.16.123.0 0.0.0.15
access-list 1 permit 172.16.12.0 0.0.0.7
access-list 1 permit 172.16.13.0 0.0.0.7
access-list 1 permit 172.16.23.0 0.0.0.7
access-list 1 deny   any

line vty 0 181
access-class 1 in
```

R2

```
access-list 1 permit 10.2.2.2
access-list 1 permit 10.3.3.3
access-list 1 permit 10.1.1.1
access-list 1 permit 192.168.1.0 0.0.0.7
access-list 1 permit 192.168.11.0 0.0.0.31
access-list 1 permit 192.168.2.0 0.0.0.7
access-list 1 permit 192.168.22.0 0.0.0.31
access-list 1 permit 192.168.3.0 0.0.0.7
access-list 1 permit 192.168.33.0 0.0.0.31
access-list 1 permit 10.99.99.0 0.0.0.31
```

access-list 1 permit 172.16.123.0 0.0.0.15
access-list 1 permit 172.16.12.0 0.0.0.7
access-list 1 permit 172.16.13.0 0.0.0.7
access-list 1 permit 172.16.23.0 0.0.0.7
access-list 1 deny   any

line vty 0 181
access-class 1 in

R3

access-list 1 permit 10.2.2.2
access-list 1 permit 10.3.3.3
access-list 1 permit 10.1.1.1
access-list 1 permit 192.168.1.0 0.0.0.7
access-list 1 permit 192.168.11.0 0.0.0.31
access-list 1 permit 192.168.2.0 0.0.0.7
access-list 1 permit 192.168.22.0 0.0.0.31
access-list 1 permit 192.168.3.0 0.0.0.7
access-list 1 permit 192.168.33.0 0.0.0.31
access-list 1 permit 10.99.99.0 0.0.0.31
access-list 1 permit 172.16.123.0 0.0.0.15
access-list 1 permit 172.16.12.0 0.0.0.7
access-list 1 permit 172.16.13.0 0.0.0.7
access-list 1 permit 172.16.23.0 0.0.0.7
access-list 1 deny   any

line vty 0 181
access-class 1 in

SW1

access-list 1 permit 10.2.2.2
access-list 1 permit 10.3.3.3
access-list 1 permit 10.1.1.1
access-list 1 permit 192.168.1.0 0.0.0.7
access-list 1 permit 192.168.11.0 0.0.0.31
access-list 1 permit 192.168.2.0 0.0.0.7
access-list 1 permit 192.168.22.0 0.0.0.31
access-list 1 permit 192.168.3.0 0.0.0.7
access-list 1 permit 192.168.33.0 0.0.0.31
access-list 1 permit 10.99.99.0 0.0.0.31
access-list 1 permit 172.16.123.0 0.0.0.15
access-list 1 permit 172.16.12.0 0.0.0.7
access-list 1 permit 172.16.13.0 0.0.0.7
access-list 1 permit 172.16.23.0 0.0.0.7
access-list 1 deny   any

line vty 0 15
access-class 1 in

**** If using three switches, duplicate configuration for additional switches ****

3.1.5. Configure Other Basic Device Settings

Specific device settings can simplify management and operation within the network. Configure these settings as follows:

- Set clocks on all devices to Pacific Time
- Disable devices from using DNS lookups
- Enable web-based access on all devices
- Set login message to "Welcome to the CCNA Metro-E Lab!"
- Set all devices to update their clocks based on the time configured on R4

ANSWERS:

**** Setting the system clock is one function done from the command line, not global configuration mode, using the *set clock timezone* command ****
**** Disabling DNS lookups on a device is helpful especially f you mistype a command. The *no ip domain-lookup* command disables this function****
**** Web-based device access is another way to program/monitor devices, with other settings as well. The *ip http server* command enables this ****
**** Displaying a welcome message is another helpful functional that should be used whenever possible. The "message of the day" is configured using the command *banner motd, with the # symbol acting as delimiters* ****

R1

clock timezone PST -8
clock summer-time PDT date Mar 13 2011 2:00 Nov 6 2011 2:00
no ip domain lookup
banner motd #Welcome to the CCNA Metro-E Lab!#
ntp server 10.99.99.4

R2

clock timezone PST -8
clock summer-time PDT date Mar 13 2011 2:00 Nov 6 2011 2:00
no ip domain lookup
banner motd #Welcome to the CCNA Metro-E Lab!#
ntp server 10.99.99.4

R3

clock timezone PST -8
clock summer-time PDT date Mar 13 2011 2:00 Nov 6 2011 2:00
no ip domain lookup
banner motd #Welcome to the CCNA Metro-E Lab!#
ntp server 10.99.99.4

R4

ntp master
no ip domain lookup
banner motd #Welcome to the CCNA LAB!#

SW1

clock timezone PST -8
clock summer-time PDT date Mar 13 2011 2:00 Nov 6 2011 2:00
no ip domain lookup
banner motd #Welcome to the CCNA Metro-E Lab!#
ntp server 10.99.99.4

**** If using three switches, duplicate configuration for additional switches ****

3.2. Local Device Interface Configuration Tasks

Every networking device in the environment has multiple interfaces that require specific configuration tasks in order to provide connectivity to resources.

3.2.1. VLAN Interfaces

All sites have multiple VLAN segments that require configuration to be applied on the LAN switch as well as the site router. Configure the following VLANs at each site in the topology:

ANSWERS:

**** Both the routers and switch(es) require separate and distinct configuration for creating and processing VLANs. The following outline demonstrates the switch portion of the configuration ****

SW1

First, VLANs must be configured from global configuration mode:

vlan 11

vlan 2
vlan 22
vlan 3
vlan 33
vlan 99
vlan 123

To support multiple VLANs, the ports on the switch(es) must be configured for trunking on the connection to the routers:

interface fa0/2
switchport trunk encapsulation dot1q
switchport mode trunk
description Trunk to R1

interface fa0/1
switchport trunk encapsulation dot1q
switchport mode trunk
description Trunk to R2

interface fa0/3
switchport trunk encapsulation dot1q
switchport mode trunk
description Trunk to R3

interface fa0/8
switchport trunk encapsulation dot1q
switchport mode trunk
description Trunk to R4

**** If using three switches, duplicate configuration for additional switches ****

- **Management VLAN**: Used for managing all remote devices by resources at the central data center
    - Set the VLAN ID to X (X=Site Number)
    - Name the VLAN **MANAGEMENT VLAN**
    - Create IP addressing to allow for 15 usable Hosts

ANSWERS:

**** VLAN configuration on a router interface requires the use of subinterfaces for each configured VLAN. The encapsulation type and VLAN ID/number must also be specified on the subinterface ****

**** Choices for an IP subnet depend on the numbers of networks and hosts needed to satisfy requirements. For the Management VLAN, one network is needed, but 5 usable hosts. Subnets could include 192.168.X.0 255.255.255.240 (or**

/28), but that yields 30 usable hosts (too many). 192.168.X.0 255.255.255.248 (or /29) gives 6 usable hosts, which is a better choice **

R1

```
interface fa0/0.1
description Management VLAN
 encapsulation dot1q 1
 ip address 192.168.1.1 255.255.255.248
```

R2

```
interface fa0/0.2
description Management VLAN
 encapsulation isl 2
 ip address 192.168.2.2 255.255.255.248
```

R3

```
interface fa0/0.3
description Management VLAN
 encapsulation isl 3
 ip address 192.168.3.3 255.255.255.248
```

- **Production VLAN**: Used for normal network operations
    - Set the VLAN ID to XX (X=Site Number)
    - Name the VLAN **PRODUCTION VLAN**
    - Create IP addressing to allow for 20 usable Hosts

ANSWERS:

**** VLAN configuration on a router interface requires the use of subinterfaces for each configured VLAN. The encapsulation type and VLAN ID/number must also be specified on the subinterface ****

**** Choices for an IP subnet depend on the numbers of networks and hosts needed to satisfy requirements. For the Production VLAN, one network is needed, but 30 usable hosts. Subnets could include 192.168.XX.0 255.255.255.192 (or /26), but that yields 62 usable hosts (too many). 192.168.XX.0 255.255.255.248 (or/27) gives 30 usable hosts, which is a better choice ****

R1

```
interface fa0/0.11
description Production VLAN
 encapsulation isl 11
 ip address 192.168.11.1 255.255.255.248
```

R2

```
interface fa0/0.22
description Production VLAN
 encapsulation isl 22
 ip address 192.168.22.2 255.255.255.248
```

R3

```
interface fa0/0.33
description Production VLAN
 encapsulation isl 33
 ip address 192.168.33.3 255.255.255.248
```

- **Internet VLAN**: Used for providing Internet access through the Internet connection at **Site 3** (R3/R4)

    - Set the VLAN ID to 99
    - Use 802.1Q encapsulation
    - Name the VLAN **INTERNET VLAN**
    - Do not supply any Internet addresses but allow DHCP to assign them

ANSWERS:

**** VLAN configuration on a router interface requires the use of subinterfaces for each configured VLAN. The encapsulation type and VLAN ID/number must also be specified on the subinterface. ****

R1

```
interface fa0/0.99
description Internet VLAN
 encapsulation dot1q 99
 ip address dhcp
```

R2

```
interface fa0/0.99
description Internet VLAN
 encapsulation dot1q 99
 ip address dhcp
```

R3

```
interface fa0/0.99
description Internet VLAN
 encapsulation dot1q 99
```

ip address dhcp

**** DHCP server configuration will be presented later ****

R4

```
interface fa0/0.99
description Internet VLAN
 encapsulation dot1q 99
 ip address 10.99.99.4 255.255.255.224
```

3.2.2. Loopback Interfaces (R1/R2/R3 Only)

Loopback interfaces are logical interfaces that do not go down unless the device itself is no longer operational. Tying device processes to loopback interfaces prevent intermittent issues resulting from links going up and down.

- Create a loopback interface for each router in the network
- Assign the name **Loopback 0** to each loopback interface
- Assign IP subnet for a single host: 10.Y.Y.Y (Y=device number)

ANSWERS:

R1

```
interface Loopback0
 description Loopback Interface
 ip address 10.1.1.1 255.255.255.255
```

R2

```
interface Loopback0
description Loopback Interface
ip address 10.2.2.2 255.255.255.255
```

R3

```
interface Loopback0
 description Loopback Interface
 ip address 10.3.3.3 255.255.255.255
```

3.2.3. Metro-Ethernet WAN Interfaces (R1/R2/R3 Only)

All three sites in the network are linked by a Metropolitan Ethernet service in a full-mesh topology. Configure WAN access on these interfaces as follows:

- Create Subinterfaces using Site numbers for reference (e.g., Fast Ethernet 0/0.1 for Site 1)
- Specify 802.1Q Encapsulation and Assign to VLAN 123
- Assign IP addresses per diagram, with 12 hosts per subnet

ANSWERS:

**** Metropolitan Ethernet is a newer WAN technology that provides a LAN-like service to locations within a specific geographic region. ****
**** Choices for an IP subnet depend on the numbers of networks and hosts needed to satisfy requirements. Subnets could include 172.16.123.X 255.255.255.224 (or /27), but that yields 30 usable hosts (too many). 172.16.123.X 255.255.255.224 (or /28) gives 16 usable hosts, which is a better choice ****

R1

```
interface FastEthernet0/0.123
 description METRO ETHERNET WAN INTERFACE
 encapsulation dot1Q 123
 ip address 172.16.123.1 255.255.255.240
```

R2

```
interface FastEthernet0/0.123
 description METRO ETHERNET WAN INTERFACE
 encapsulation dot1Q 123
 ip address 172.16.123.2 255.255.255.240
```

R3

```
interface FastEthernet0/0.123
 description METRO ETHERNET WAN INTERFACE
 encapsulation dot1Q 123
 ip address 172.16.123.3 255.255.255.240
```

3.2.4. DHCP Configuration

The VLAN 99 (Internet VLAN) on R1/R2/R3 requires receiving of its IP address through DHCP from R4. Configure as follows:

- Enable DHCP on R4 to supply addressing to R1/R2/R3 on VLAN99
- Identify the following parameters:
    - Network
    - Default Gateway
    - DNS (use 216.136.95.2 and 64.132.94.250)

ANSWERS:

**** Remember that R1/R2/R3 is configured to receive its Internet IP addressing information through DHCP ****

**** Routers can act as DHCP servers when configured properly, by defining a DHCP pool, which can include the network/subnet to use, DNS, and default-router, to name a few. Also, remember to ensure that R4's IP address is not included in the DHCP scope****

R4

```
ip dhcp excluded-address 10.99.99.1 10.99.99.4

ip dhcp pool Internet_VLAN
  network 10.99.99.0 255.255.255.224
  default-router 10.99.99.4
  dns-server 216.136.95.2 64.132.94.250
```

3.2.5. GRE Interfaces (R1/R2/R3 Only)

Backup network connectivity is required in the event of failure on the Metro-E service. Configure VPN access on the Internet interfaces as follows:

- Create a full-mesh tunnel configuration between all sites
- Specify GRE IP Encapsulation for the tunnels
- Enable CDP on the tunnels
- Specify the source as Fa0/0.99
- Specify the destination as the DHCP assigned address of the destination router
- Assign IP addresses per diagram, with 5 usable hosts per subnet

ANSWERS:

**** Generic Routing Encapsulation (GRE) is used to tunnel non-IP protocols through an IP environment, and also frequently used in VPN configurations. In a production setting, the addition of IPSec encryption would be necessary to address security concerns ****

**** Tunnel interfaces require specifying source and destination endpoints in addition to standard interface commands. Since the Internet VLAN interfaces receive IP addressing via DHCP, some extra steps are required. Specifying the fa0/0.99 interface as the source removes some complexity, but you will have to look up the DHCP assigned addresses on the other routers' interfaces to correctly identify the endpoints****

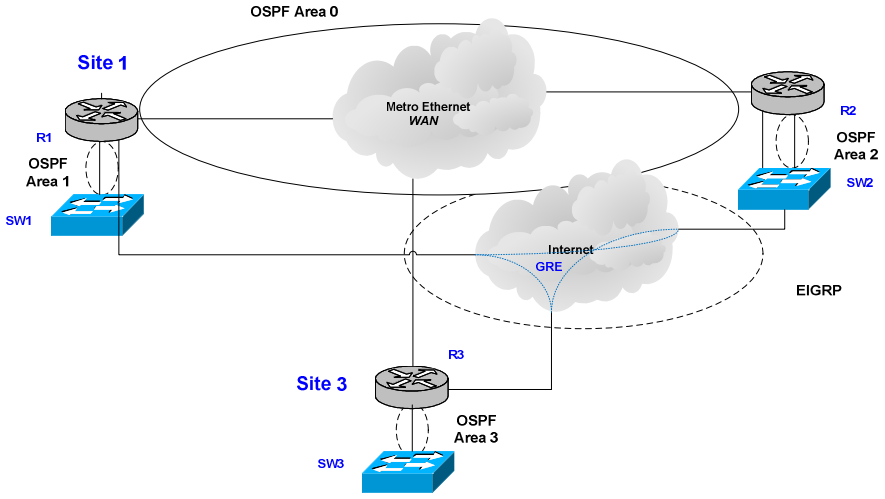
R1

```
interface Tunnel1
```

```
 description VPN BACKUP INTERFACE to R2
 ip address 172.16.12.1 255.255.255.248
 cdp enable
 tunnel source FastEthernet0/0.99
 tunnel destination 10.99.99.5

interface Tunnel2
 description VPN BACKUP INTERFACE to R3
 ip address 172.16.13.1 255.255.255.248
cdp enable
 tunnel source FastEthernet0/0.99
 tunnel destination 10.99.99.6

R2

interface Tunnel2
 description VPN BACKUP INTERFACE to R1
 ip address 172.16.12.2 255.255.255.248
 cdp enable
 tunnel source FastEthernet0/0.99
 tunnel destination 10.99.99.7
!
interface Tunnel3
 description VPN BACKUP INTERFACE to R2
 ip address 172.16.23.2 255.255.255.248
 cdp enable
 tunnel source FastEthernet0/0.99
 tunnel destination 10.99.99.6

R3

interface Tunnel2
 description VPN BACKUP INTERFACE to R2
 ip address 172.16.23.3 255.255.255.248
 cdp enable
 tunnel source FastEthernet0/0.99
 tunnel destination 10.99.99.5
!
interface Tunnel3
 description VPN BACKUP INTERFACE to R1
 ip address 172.16.13.3 255.255.255.248

cdp enable
 tunnel source FastEthernet0/0.99
 tunnel destination 10.99.99.7
```

3.3. Routing Protocol Configuration Tasks

Multiple routing protocols are in use throughout the network and require careful configuration to ensure correct operation. Refer to the following diagram as a reference point:



3.3.1. OSPF Configuration

OSPF is the primary routing configuration in use throughout the network, and must be operational at all three sites. Configure routing as follows:

- R1 OSPF Configuration
    - Set **Loopback 0** as the OSPF router-id
    - Place the Metro Ethernet interface in area 0
    - Place all local VLAN interfaces and the loopback interface in area 1

ANSWERS:

****OSPF is configured from router configuration mode, which is entered by the command *router ospf <process-id>* ****

**** Interfaces are placed in OSPF using the *network* command, using the best practice of the most specific subnets possible. The Metro-E interfaces should be placed in area 0, with Loopback and VLAN interfaces in area 1 respectively ****

R1

```
router ospf 1
 router-id 10.1.1.1
 log-adjacency-changes
```

network 10.1.1.1 0.0.0.0 area 1
network 172.16.123.0 0.0.0.15 area 0
network 192.168.1.0 0.0.0.7 area 1
network 192.168.11.0 0.0.0.31 area 1

- R2 OSPF Configuration
    - Set **Loopback 0** as the OSPF router-id
    - Place the Metro Ethernet interface in area 0
    - Place all local VLAN interfaces and the loopback interface in area 2

ANSWERS:

****OSPF is configured from router configuration mode, which is entered by the command *router ospf <process-id>* ****
**** Interfaces are placed in OSPF using the *network* command, using the best practice of the most specific subnets possible. Interfaces should be placed in area 0 and area 2 as specified****

R2

router ospf 1
router-id 10.2.2.2
log-adjacency-changes
network 10.2.2.2 0.0.0.0 area 2
network 172.16.123.0 0.0.0.15 area 0
network 192.168.2.0 0.0.0.7 area 2
network 192.168.22.0 0.0.0.31 area 2

- R3 OSPF Configuration
    - Set **Loopback 0** as the OSPF router-id
    - Configure link to R2 in area 1
    - Configure loopback in area 1

ANSWERS:

****OSPF is configured from router configuration mode, which is entered by the command *router ospf <process-id>* ****
**** Interfaces are placed in OSPF using the *network* command, using the best practice of the most specific subnets possible. The Metro-E interfaces should be placed in area 0, with Loopback and VLAN interfaces in area 3 respectively ****

R3

router ospf 1
router-id 10.3.3.3

log-adjacency-changes
network 10.3.3.3 0.0.0.0 area 3
network 172.16.123.0 0.0.0.15 area 0
network 192.168.3.0 0.0.0.7 area 3
network 192.168.33.0 0.0.0.31 area 3

3.3.2. EIGRP Configuration

EIGRP is in use to provide backup connectivity to the Internet in the event of an outage on the OSPF network. Configure EIGRP routing as follows:

- R1 EIGRP Configuration
    - Use AS Number 111
    - Enable EIGRP on all GRE tunnel interfaces
    - Disable auto summarization

ANSWERS:

****EIGRP is configured from router configuration mode, which is entered by the command *router eigrp <as-number>* ****
**** Interfaces are placed in EIGRP using the *network* command, using the best practice of the most specific subnets possible ****
**** Automatic network summarization is on by default ****

R1

router eigrp 111
network 172.16.12.0 0.0.0.7
network 172.16.13.0 0.0.0.7
no auto-summary
eigrp router-id 10.1.1.1

- R2 EIGRP Configuration
    - Use AS Number 111
    - Enable EIGRP on all GRE tunnel interfaces
    - Disable auto summarization

ANSWERS:

****EIGRP is configured from router configuration mode, which is entered by the command *router eigrp <as-number>* ****
**** Interfaces are placed in EIGRP using the *network* command, using the best practice of the most specific subnets possible ****
**** Automatic network summarization is on by default ****

R2

router eigrp 111
network 172.16.12.0 0.0.0.7
network 172.16.23.0 0.0.0.7
no auto-summary
eigrp router-id 10.2.2.2

- R3 EIGRP Configuration
    - Use AS Number 111
    - Enable EIGRP on all GRE tunnel interfaces
    - Disable auto summarization

ANSWERS:

****EIGRP is configured from router configuration mode, which is entered by the command *router eigrp <as-number>* ****
**** Interfaces are placed in EIGRP using the *network* command, using the best practice of the most specific subnets possible ****
**** Automatic network summarization is on by default ****

R3

router eigrp 111
network 172.16.13.0 0.0.0.7
network 172.16.23.0 0.0.0.7
no auto-summary
eigrp router-id 10.3.3.3

3.3.3. Redistribution and Tuning Configuration

With multiple routing protocols in use, full connectivity must be created between protocols to allow consistent communication. Configure as follows:

- Do not redistribute EIGRP or OSPF
- Configure EIGRP to Perform Backup Routing upon Failure of the Metro Ethernet Service
- Do not configure any static routes to accomplish this task

ANSWERS:

****When multiple routing protocols are running on a since Cisco device, the router/L2 to decide the reliability or believability of the route. The listing of these distances is as follows: ****

Route Source	Default Distance Values
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown*	255

****Since the administrative distance of EIGRP is lower than OSPF, enabling redistribution could create issues. Another alternative is to redistribute all connected interfaces into EIGRP and adjust the distance of OSPF to 89 to make it the preferred protocol ****

R1

```
router eigrp 111
 redistribute connected

router ospf 1
distance 89
```

R2

```
router eigrp 111
 redistribute connected

router ospf 1
distance 89
```

R3

```
router eigrp 111
 redistribute connected
```

router ospf 1
distance 89

- Verify full reachability:
    - Ping all other devices in the network from each device
    - Successfully telnet to all devices in the network from each device

R1 Routing Table During Steady State Operations

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.99.99.4 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
D       172.16.23.0/29 [90/310044416] via 172.16.13.3, 2d00h, Tunnel2
                       [90/310044416] via 172.16.12.2, 2d00h, Tunnel1
C       172.16.12.0/29 is directly connected, Tunnel1
C       172.16.13.0/29 is directly connected, Tunnel2
C       172.16.123.0/28 is directly connected, FastEthernet0/0.123
     192.168.11.0/27 is subnetted, 1 subnets
C       192.168.11.0 is directly connected, FastEthernet0/0.11
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O IA    10.2.2.2/32 [89/2] via 172.16.123.2, 00:31:43, FastEthernet0/0.123
O IA    10.3.3.3/32 [89/2] via 172.16.123.3, 00:27:15, FastEthernet0/0.123
C       10.99.99.0/27 is directly connected, FastEthernet0/0.99
C       10.1.1.1/32 is directly connected, Loopback0
     192.168.22.0/27 is subnetted, 1 subnets
O IA    192.168.22.0 [89/2] via 172.16.123.2, 00:31:44, FastEthernet0/0.123
     192.168.1.0/29 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0.1
     192.168.2.0/29 is subnetted, 1 subnets
O IA    192.168.2.0 [89/2] via 172.16.123.2, 00:31:44, FastEthernet0/0.123
     192.168.3.0/29 is subnetted, 1 subnets
O IA    192.168.3.0 [89/2] via 172.16.123.3, 00:31:44, FastEthernet0/0.123
     192.168.33.0/27 is subnetted, 1 subnets
O IA    192.168.33.0 [89/2] via 172.16.123.3, 00:24:45, FastEthernet0/0.123
S*   0.0.0.0/0 [254/0] via 10.99.99.4
```

Note that because R1 receives its IP address via DHCP, it also receives a default route to the Internet without any additional configuration.

R1 Routing Table After Simulated Failover (Shutdown on VLAN 123)

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.99.99.4 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
D       172.16.23.0/29 [90/310044416] via 172.16.13.3, 2d00h, Tunnel2
                       [90/310044416] via 172.16.12.2, 2d00h, Tunnel1
C       172.16.12.0/29 is directly connected, Tunnel1
C       172.16.13.0/29 is directly connected, Tunnel2
C       172.16.123.0/28 is directly connected, FastEthernet0/0.123
     192.168.11.0/27 is subnetted, 1 subnets
C       192.168.11.0 is directly connected, FastEthernet0/0.11
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
D EX    10.2.2.2/32 [170/297372416] via 172.16.12.2, 00:00:00, Tunnel1
D EX    10.3.3.3/32 [170/297372416] via 172.16.13.3, 00:00:00, Tunnel2
C       10.99.99.0/27 is directly connected, FastEthernet0/0.99
C       10.1.1.1/32 is directly connected, Loopback0
     192.168.22.0/27 is subnetted, 1 subnets
D EX    192.168.22.0 [170/297246976] via 172.16.12.2, 00:00:02, Tunnel1
     192.168.1.0/29 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0.1
     192.168.2.0/29 is subnetted, 1 subnets
D EX    192.168.2.0 [170/297246976] via 172.16.12.2, 00:00:02, Tunnel1
     192.168.3.0/29 is subnetted, 1 subnets
D EX    192.168.3.0 [170/297246976] via 172.16.13.3, 00:00:02, Tunnel2
     192.168.33.0/27 is subnetted, 1 subnets
D EX    192.168.33.0 [170/297246976] via 172.16.13.3, 00:00:02, Tunnel2
S*   0.0.0.0/0 [254/0] via 10.99.99.4
```

Failover is immediate once the OSPF neighbor was detected as lost

3.4. Network Address Translation Tasks

All sites within the network utilize addressing from the RFC 1918 Private Addressing space, which are not valid on the Internet. In order to have full Internet connectivity, all

internal addressing must be mapped to globally routable addressing space. In addition, an internal web server must also be accessible from the Internet

3.4.1. Configure Port Address Translation for All Internal Hosts

Ensure that all devices within the internal network may access sites on the Internet. Do not apply any filtering to this configuration.

ANSWERS:

****PAT or IP Address Overloading has several steps for successful configuration:**

1. **Create an access-list identifying the addresses to be translated**
2. **Identify the inside and outside interfaces (*ip nat inside* or *outside*)**
3. **Map the access-list to the outside interface using the *ip nat inside source list* statement****

R1

```
access-list 2 permit 10.1.1.1
access-list 2 permit 192.168.1.0 0.0.0.7
access-list 2 permit 192.168.11.0 0.0.0.31
access-list 2 permit 172.16.123.0 0.0.0.15
access-list 2 permit 172.16.12.0 0.0.0.7
access-list 2 permit 172.16.13.0 0.0.0.7
access-list 2 deny   any

interface Loopback0
ip nat inside

interface Tunnel1
ip nat inside

interface Tunnel2
ip nat inside

interface FastEthernet0/0.1
ip nat inside

interface FastEthernet0/0.11
ip nat inside

interface FastEthernet0/0.123
ip nat inside

interface FastEthernet0/0.99
ip nat outside

ip nat inside source list 2 interface FastEthernet0/0.99 overload
```

R2

```
access-list 2 permit 10.2.2.2
access-list 2 permit 192.168.2.0 0.0.0.7
access-list 2 permit 192.168.22.0 0.0.0.31
access-list 2 permit 172.16.123.0 0.0.0.15
access-list 2 permit 172.16.12.0 0.0.0.7
access-list 2 permit 172.16.23.0 0.0.0.7
access-list 2 deny   any

interface Loopback0
ip nat inside

interface Tunnel2
ip nat inside

interface Tunnel3
ip nat inside

interface FastEthernet0/0.2
ip nat inside

interface FastEthernet0/0.22
ip nat inside

interface FastEthernet0/0.123
ip nat inside

interface FastEthernet0/0.99
ip nat outside

ip nat inside source list 2 interface FastEthernet0/0.99 overload
```

R3

```
access-list 2 permit 10.3.3.3
access-list 2 permit 192.168.3.0 0.0.0.7
access-list 2 permit 192.168.33.0 0.0.0.31
access-list 2 permit 172.16.123.0 0.0.0.15
access-list 2 permit 172.16.13.0 0.0.0.7
access-list 2 permit 172.16.23.0 0.0.0.7

access-list 2 permit 10.2.2.2
access-list 2 permit 192.168.2.0 0.0.0.7
access-list 2 permit 192.168.22.0 0.0.0.31
access-list 2 permit 172.16.123.0 0.0.0.15
access-list 2 permit 172.16.12.0 0.0.0.7
access-list 2 permit 172.16.23.0 0.0.0.7
```

access-list 2 deny   any

interface Loopback0
ip nat inside

interface Tunnel2
ip nat inside

interface Tunnel3
ip nat inside

interface FastEthernet0/0.3
ip nat inside

interface FastEthernet0/0.33
ip nat inside

interface FastEthernet0/0.123
ip nat inside

interface FastEthernet0/0.99
ip nat outside

ip nat inside source list 2 interface FastEthernet0/0.99 overload

3.4.2. Static Network Address Translation for a Web Server on R2

Http services were previously enabled on R2 and accessible from within the internal network, but need to be available on the Internet for monitoring and management purposes. Using static a NAT entry, point internal web connections to R2's Production VLAN address.

ANSWERS:

****Static NAT configuration uses a variation of the *ip nat inside* statement but applies it to only a single service, including IP, TCP and UDP ****

R2

**** Mapping the web server uses a static NAT configuration as follows: ****

ip nat inside source static tcp 192.168.22.2 80 interface FastEthernet0/0.99 80

3.5. Security Configuration Tasks

Preventing unauthorized access to devices on the network may be supplied in part by the external ASA firewall, but additional measured need to be implemented to protect information assets.

3.5.1. Create and apply an access that will only allow internal devices to access the management VLAN on all devices at each site.

The company's information security policy stipulates that no users outside of the company are permitted to access internal resources. To prevent unauthorized access, disallow all outside users from accessing the hosts within the protected network.

ANSWERS:

****The access-list used previously for telnet access and PAT also serves another purpose of filtering network traffic. This filter is applied under interfaces using the *ip access-group <number>* command. This serves to underscore the power and versatility of access-list usage ****

****To prevent traffic, placing the access-list filter at the entry point to local management VLAN is the best location****

R1

```
access-list 1 permit 10.2.2.2
access-list 1 permit 10.3.3.3
access-list 1 permit 10.1.1.1
access-list 1 permit 192.168.1.0 0.0.0.7
access-list 1 permit 192.168.11.0 0.0.0.31
access-list 1 permit 192.168.2.0 0.0.0.7
access-list 1 permit 192.168.22.0 0.0.0.31
access-list 1 permit 192.168.3.0 0.0.0.7
access-list 1 permit 192.168.33.0 0.0.0.31
access-list 1 permit 10.99.99.0 0.0.0.31
access-list 1 permit 172.16.123.0 0.0.0.15
access-list 1 permit 172.16.12.0 0.0.0.7
access-list 1 permit 172.16.13.0 0.0.0.7
access-list 1 permit 172.16.23.0 0.0.0.7
access-list 1 deny   any

interface FastEthernet0/0.1
ip access-group 1 out
```

R2

```
access-list 1 permit 10.2.2.2
```

access-list 1 permit 10.3.3.3
access-list 1 permit 10.1.1.1
access-list 1 permit 192.168.1.0 0.0.0.7
access-list 1 permit 192.168.11.0 0.0.0.31
access-list 1 permit 192.168.2.0 0.0.0.7
access-list 1 permit 192.168.22.0 0.0.0.31
access-list 1 permit 192.168.3.0 0.0.0.7
access-list 1 permit 192.168.33.0 0.0.0.31
access-list 1 permit 10.99.99.0 0.0.0.31
access-list 1 permit 172.16.123.0 0.0.0.15
access-list 1 permit 172.16.12.0 0.0.0.7
access-list 1 permit 172.16.13.0 0.0.0.7
access-list 1 permit 172.16.23.0 0.0.0.7
access-list 1 deny any

interface FastEthernet0/0.1
ip access-group 1 out

R3

access-list 1 permit 10.2.2.2
access-list 1 permit 10.3.3.3
access-list 1 permit 10.1.1.1
access-list 1 permit 192.168.1.0 0.0.0.7
access-list 1 permit 192.168.11.0 0.0.0.31
access-list 1 permit 192.168.2.0 0.0.0.7
access-list 1 permit 192.168.22.0 0.0.0.31
access-list 1 permit 192.168.3.0 0.0.0.7
access-list 1 permit 192.168.33.0 0.0.0.31
access-list 1 permit 10.99.99.0 0.0.0.31
access-list 1 permit 172.16.123.0 0.0.0.15
access-list 1 permit 172.16.12.0 0.0.0.7
access-list 1 permit 172.16.13.0 0.0.0.7
access-list 1 permit 172.16.23.0 0.0.0.7
access-list 1 deny any

interface FastEthernet0/0.1
ip access-group 1 out

3.5.2. Block SNMP access to all devices.

SNMP protocols are a source of security concerns for the management team and they have elected not to permit it anywhere on the network. Configure the appropriate packet filters/access-lists to block all SNMP access to/from all sites.

ANSWERS:

****Standard access-lists filter only by source address, while extended addresses can filter on source, destination, protocol, and TCP/UDP ports ****

****Since the implicit *deny-any* is at the end of an access-list, allowing traffic is required or it will block all packets. Additionally, applying this on the WAN links also makes the most sense ****

R1

```
access-list 101 deny   udp any any eq snmp
access-list 101 permit ip any any

interface fa0/0.123
ip access-group 101 in
```

R2

```
access-list 101 deny   udp any any eq snmp
access-list 101 permit ip any any

interface fa0/0.123
ip access-group 101 in
```

R3

```
access-list 101 deny   udp any any eq snmp
access-list 101 permit ip any any

interface fa0/0.123
ip access-group 101 in
```

3.5.3. Block all external access trying to reach the management VLAN

Remote access has been provided at the primary corporate location for the purpose of managing all internal network resources. Because of the sensitive nature of the data at the corporate locations, external access to the Management VLANs is not permitted by the security policy. Construct an access list to block any attempt at access from the Internet interface.

ANSWERS:

****Standard access-lists filter only by source address, while extended addresses can filter on source, destination, protocol, and TCP/UDP ports ****

****Since the implicit *deny-any* is at the end of an access-list, allowing traffic is required or it will block all packets. Additionally, applying this on the Internet VLAN makes the most sense since it is considered the "external" interface****

R1

access-list 102 deny   ip any 192.168.1.0 0.0.0.7
access-list 102 deny   udp any any eq snmp
access-list 102 permit ip any any

interface fa0/0.99
ip access-group 102 in

R2

access-list 102 deny   ip any 192.168.1.0 0.0.0.7
access-list 102 deny   udp any any eq snmp
access-list 102 permit ip any any

interface fa0/0.99
ip access-group 102 in

R3

access-list 102 deny   ip any 192.168.1.0 0.0.0.7
access-list 102 deny   udp any any eq snmp
access-list 102 permit ip any any

interface fa0/0.99
ip access-group 102 in

4. Final Configurations

4.1. R1 Configuration

CONFIGURATION

```
version 12.3
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
!
hostname R1
!
boot-start-marker
boot system flash
boot-end-marker
!
enable secret 5 $1$STvX$B5n3hwezXzvqvchXisjDL1
!
clock timezone PST -8
clock summer-time PDT date Mar 13 2011 2:00 Nov 6 2011 2:00
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
no tag-switching ip propagate-ttl
no tag-switching ip
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
```

```
 description LOOPBACK INTERFACE
 ip address 10.1.1.1 255.255.255.255
 ip access-group 101 in
 ip nat inside
!
interface Tunnel1
 description VPN BACKUP INTERFACE to R2
 ip address 172.16.12.1 255.255.255.248
 ip access-group 101 in
 ip nat inside
 cdp enable
 tunnel source FastEthernet0/0.99
 tunnel destination 10.99.99.5
!
interface Tunnel2
 description VPN BACKUP INTERFACE to R3
 ip address 172.16.13.1 255.255.255.248
 ip access-group 101 in
 ip nat inside
 cdp enable
 tunnel source FastEthernet0/0.99
 tunnel destination 10.99.99.6
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 description MANAGEMENT VLAN
 encapsulation dot1Q 1 native
 ip address 192.168.1.1 255.255.255.248
 ip access-group 1 out
 ip nat inside
!
interface FastEthernet0/0.11
 description PRODUCTION VLAN
 encapsulation dot1Q 11
 ip address 192.168.11.1 255.255.255.224
 ip nat inside
!
interface FastEthernet0/0.99
 description INTERNET INTERFACE
 encapsulation dot1Q 99
 ip address dhcp
 ip access-group 102 in
 ip nat outside
!
```

```
interface FastEthernet0/0.123
 description METRO ETHERNET WAN INTERFACE
 encapsulation dot1Q 123
 ip address 172.16.123.1 255.255.255.240
 ip access-group 101 in
 ip nat inside
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
!
router eigrp 111
 redistribute connected
 network 172.16.12.0 0.0.0.7
 network 172.16.13.0 0.0.0.7
 no auto-summary
 eigrp router-id 10.1.1.1
!
router ospf 1
 router-id 10.1.1.1
 log-adjacency-changes
 network 10.1.1.1 0.0.0.0 area 1
 network 172.16.123.0 0.0.0.15 area 0
 network 192.168.1.0 0.0.0.7 area 1
 network 192.168.11.0 0.0.0.31 area 1
 distance 89
!
ip nat inside source list 2 interface FastEthernet0/0.99 overload
no ip http server
ip classless
!
!
no logging trap
access-list 1 permit 10.2.2.2
access-list 1 permit 10.3.3.3
access-list 1 permit 10.1.1.1
access-list 1 permit 192.168.1.0 0.0.0.7
access-list 1 permit 192.168.11.0 0.0.0.31
access-list 1 permit 192.168.2.0 0.0.0.7
access-list 1 permit 192.168.22.0 0.0.0.31
access-list 1 permit 192.168.3.0 0.0.0.7
access-list 1 permit 192.168.33.0 0.0.0.31
access-list 1 permit 10.99.99.0 0.0.0.31
access-list 1 permit 172.16.123.0 0.0.0.15
access-list 1 permit 172.16.12.0 0.0.0.7
access-list 1 permit 172.16.13.0 0.0.0.7
access-list 1 permit 172.16.23.0 0.0.0.7
access-list 1 deny   any
```

```
access-list 2 permit 10.1.1.1
access-list 2 permit 192.168.1.0 0.0.0.7
access-list 2 permit 192.168.11.0 0.0.0.31
access-list 2 permit 172.16.123.0 0.0.0.15
access-list 2 permit 172.16.12.0 0.0.0.7
access-list 2 permit 172.16.13.0 0.0.0.7
access-list 2 deny   any
access-list 101 deny   udp any any eq snmp
access-list 101 permit ip any any
access-list 102 deny   ip any 192.168.1.0 0.0.0.7
access-list 102 deny   udp any any eq snmp
access-list 102 permit ip any any
!
!
!
!
dial-peer cor custom
!
!
!
banner motd ^CWelcome to the CCNA Metro-E Lab!^C
!
line con 0
 privilege level 15
line aux 0
 password cisco
 login
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 access-class 1 in
 password cisco
 login
line vty 5 181
 access-class 1 in
 password cisco
 login
!
ntp clock-period 17180469
ntp server 10.99.99.4
!
end
```

IP ROUTING TABLE

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
     D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
     N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
     E1 - OSPF external type 1, E2 - OSPF external type 2
     i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
     ia - IS-IS inter area, * - candidate default, U - per-user static route
     o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.99.99.4 to network 0.0.0.0

    172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
D       172.16.23.0/29 [90/310044416] via 172.16.13.3, 2d00h, Tunnel2
                       [90/310044416] via 172.16.12.2, 2d00h, Tunnel1
C       172.16.12.0/29 is directly connected, Tunnel1
C       172.16.13.0/29 is directly connected, Tunnel2
C       172.16.123.0/28 is directly connected, FastEthernet0/0.123
    192.168.11.0/27 is subnetted, 1 subnets
C       192.168.11.0 is directly connected, FastEthernet0/0.11
    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O IA    10.2.2.2/32 [89/2] via 172.16.123.2, 00:27:00, FastEthernet0/0.123
O IA    10.3.3.3/32 [89/2] via 172.16.123.3, 00:27:00, FastEthernet0/0.123
C       10.99.99.0/27 is directly connected, FastEthernet0/0.99
C       10.1.1.1/32 is directly connected, Loopback0
    192.168.22.0/27 is subnetted, 1 subnets
O IA    192.168.22.0 [89/2] via 172.16.123.2, 00:27:21, FastEthernet0/0.123
    192.168.1.0/29 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0.1
    192.168.2.0/29 is subnetted, 1 subnets
O IA    192.168.2.0 [89/2] via 172.16.123.2, 00:27:21, FastEthernet0/0.123
    192.168.3.0/29 is subnetted, 1 subnets
O IA    192.168.3.0 [89/2] via 172.16.123.3, 00:27:21, FastEthernet0/0.123
    192.168.33.0/27 is subnetted, 1 subnets
O IA    192.168.33.0 [89/2] via 172.16.123.3, 00:27:21, FastEthernet0/0.123
S*   0.0.0.0/0 [254/0] via 10.99.99.4
```

OSPF

```
R1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.2.2          1   FULL/BDR        00:00:38    172.16.123.2    FastEthernet0/0.123
10.3.3.3          1   FULL/DR         00:00:30    172.16.123.3    FastEthernet0/0.123

R1#sh ip ospf interface
FastEthernet0/0.123 is up, line protocol is up
  Internet Address 172.16.123.1/28, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 10.3.3.3, Interface address 172.16.123.3
```

```
  Backup Designated router (ID) 10.2.2.2, Interface address 172.16.123.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 3
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 10.2.2.2  (Backup Designated Router)
    Adjacent with neighbor 10.3.3.3  (Designated Router)
  Suppress hello for 0 neighbor(s)
FastEthernet0/0.11 is up, line protocol is up
  Internet Address 192.168.11.1/27, Area 1
  Process ID 1, Router ID 10.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.1.1, Interface address 192.168.11.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
  Index 3/4, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
FastEthernet0/0.1 is up, line protocol is up
  Internet Address 192.168.1.1/29, Area 1
  Process ID 1, Router ID 10.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.1.1, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
  Index 2/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Loopback0 is up, line protocol is up
  Internet Address 10.1.1.1/32, Area 1
  Process ID 1, Router ID 10.1.1.1, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host

R1#sh ip ospf database
```

OSPF Router with ID (10.1.1.1) (Process ID 1)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
10.1.1.1	10.1.1.1	1923	0x80000083	0x00051C	1
10.2.2.2	10.2.2.2	1732	0x80000086	0x00D640	1
10.3.3.3	10.3.3.3	1923	0x80000081	0x00B85C	1

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
172.16.123.3	10.3.3.3	1919	0x8000007B	0x00F655

Summary Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
10.1.1.1	10.1.1.1	1426	0x80000078	0x009119
10.2.2.2	10.2.2.2	215	0x80000003	0x0046D3
10.3.3.3	10.3.3.3	2005	0x80000002	0x001203
192.168.1.0	10.1.1.1	1426	0x80000078	0x004E06
192.168.2.0	10.2.2.2	215	0x80000003	0x0019AC
192.168.3.0	10.3.3.3	740	0x80000078	0x000E3E
192.168.11.0	10.1.1.1	1439	0x80000078	0x004F13
192.168.22.0	10.2.2.2	228	0x80000003	0x00AB1E
192.168.33.0	10.3.3.3	1763	0x80000002	0x001F9D

Router Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
10.1.1.1	10.1.1.1	1439	0x8000007E	0x00E9C7	3

Summary Net Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum
10.2.2.2	10.1.1.1	1921	0x80000001	0x0069B4
10.3.3.3	10.1.1.1	1921	0x80000001	0x0048D2
172.16.123.0	10.1.1.1	1741	0x8000007F	0x00F88E
192.168.2.0	10.1.1.1	1921	0x80000001	0x003C8D
192.168.3.0	10.1.1.1	1921	0x80000001	0x003197
192.168.22.0	10.1.1.1	1921	0x80000001	0x00CEFE
192.168.33.0	10.1.1.1	1921	0x80000001	0x00556D

EIGRP

R1# sh ip eigrp neighbors
IP-EIGRP neighbors for process 111

```
H   Address            Interface      Hold Uptime   SRTT   RTO  Q  Seq
                                      (sec)        (ms)       Cnt Num
0   172.16.12.2        Tu1              13 2d00h     238  5000  0  110
1   172.16.13.3        Tu2              14 2d19h     180  5000  0  97

R1# sh ip eigrp interfaces
IP-EIGRP interfaces for process 111

                   Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface          Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Tu2                1      0/0       180    71/2702     3254         0
Tu1                1      0/0       238    71/2702     3546         0

R1#sh ip eigrp topology
IP-EIGRP Topology Table for AS(111)/ID(10.1.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.2.2.2/32, 0 successors, FD is Inaccessible
       via 172.16.12.2 (297372416/128256), Tunnel1
P 10.3.3.3/32, 0 successors, FD is Inaccessible
       via 172.16.13.3 (297372416/128256), Tunnel2
P 10.99.99.0/27, 1 successors, FD is 28160
       via Rconnected (28160/0)
P 10.1.1.1/32, 1 successors, FD is 128256
       via Rconnected (128256/0)
P 192.168.33.0/27, 0 successors, FD is Inaccessible
       via 172.16.13.3 (297246976/28160), Tunnel2
P 192.168.11.0/27, 1 successors, FD is 28160
       via Rconnected (28160/0)
P 192.168.1.0/29, 1 successors, FD is 28160
       via Rconnected (28160/0)
P 192.168.2.0/29, 0 successors, FD is Inaccessible
       via 172.16.12.2 (297246976/28160), Tunnel1
P 192.168.3.0/29, 0 successors, FD is Inaccessible
       via 172.16.13.3 (297246976/28160), Tunnel2

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.22.0/27, 0 successors, FD is Inaccessible
       via 172.16.12.2 (297246976/28160), Tunnel1
P 172.16.23.0/29, 2 successors, FD is 310044416
       via 172.16.12.2 (310044416/297244416), Tunnel1
       via 172.16.13.3 (310044416/297244416), Tunnel2
P 172.16.12.0/29, 1 successors, FD is 297244416
       via Connected, Tunnel1
```

```
P 172.16.13.0/29, 1 successors, FD is 297244416
        via Connected, Tunnel2
P 172.16.123.0/28, 1 successors, FD is 28160
        via Rconnected (28160/0)

R1#sh ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.1.1.1
  It is an area border router
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.1.1 0.0.0.0 area 1
    172.16.123.0 0.0.0.15 area 0
    192.168.1.0 0.0.0.7 area 1
    192.168.11.0 0.0.0.31 area 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.2.2.2              89      00:30:22
    10.3.3.3              89      00:30:22
  Distance: (default is 89)

Routing Protocol is "eigrp 111"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: connected, eigrp 111
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    172.16.12.0/29
    172.16.13.0/29
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.13.3           90      00:33:28
    172.16.12.2           90      00:33:27
  Distance: internal 90 external 170
```

4.2. R2 Configuration

CONFIGURATION

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$lQgx$orRdAR114FcdUvGfrg4l5/
!
clock timezone PST -8
clock summer-time PDT date Mar 13 2011 2:00 Nov 6 2011 2:00
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
no tag-switching ip
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 description LOOPBACK INTERFACE
 ip address 10.2.2.2 255.255.255.255
 ip access-group 101 in
 ip nat inside
!
interface Tunnel2
 description VPN BACKUP INTERFACE to R1
 ip address 172.16.12.2 255.255.255.248
```

```
 ip access-group 101 in
 ip nat inside
 cdp enable
 tunnel source FastEthernet0/0.99
 tunnel destination 10.99.99.7
!
interface Tunnel3
 description VPN BACKUP INTERFACE to R2
 ip address 172.16.23.2 255.255.255.248
 ip access-group 101 in
 ip nat inside
 cdp enable
 tunnel source FastEthernet0/0.99
 tunnel destination 10.99.99.6
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 ip access-group 1 in
!
interface FastEthernet0/0.2
 description MANAGEMENT VLAN
 encapsulation dot1Q 2
 ip address 192.168.2.2 255.255.255.248
 ip access-group 1 out
 ip nat inside
 no snmp trap link-status
!
interface FastEthernet0/0.22
 description PRODUCTION VLAN
 encapsulation dot1Q 22
 ip address 192.168.22.2 255.255.255.224
 ip nat inside
 no snmp trap link-status
!
interface FastEthernet0/0.99
 description INTERNET INTERFACE
 encapsulation dot1Q 99
 ip address dhcp
 ip access-group 102 in
 ip nat outside
 no snmp trap link-status
!
interface FastEthernet0/0.123
 description METRO ETHERNET WAN INTERFACE
```

```
 encapsulation dot1Q 123
 ip address 172.16.123.2 255.255.255.240
 ip access-group 101 in
 ip nat inside
 no snmp trap link-status
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
!
router eigrp 111
 redistribute connected
 network 172.16.12.0 0.0.0.7
 network 172.16.23.0 0.0.0.7
 no auto-summary
 eigrp router-id 10.2.2.2
!
router ospf 1
 router-id 10.2.2.2
 log-adjacency-changes
 network 10.2.2.2 0.0.0.0 area 2
 network 172.16.123.0 0.0.0.15 area 0
 network 192.168.2.0 0.0.0.7 area 2
 network 192.168.22.0 0.0.0.31 area 2
 distance 89
!
ip nat inside source list 2 interface FastEthernet0/0.99 overload
ip nat inside source static tcp 192.168.22.4 80 interface FastEthernet0/0.99 80
no ip http server
ip classless
!
!
access-list 1 permit 10.2.2.2
access-list 1 permit 10.3.3.3
access-list 1 permit 10.1.1.1
access-list 1 permit 192.168.1.0 0.0.0.7
access-list 1 permit 192.168.11.0 0.0.0.31
access-list 1 permit 192.168.2.0 0.0.0.7
access-list 1 permit 192.168.22.0 0.0.0.31
access-list 1 permit 192.168.3.0 0.0.0.7
access-list 1 permit 192.168.33.0 0.0.0.31
access-list 1 permit 10.99.99.0 0.0.0.31
access-list 1 permit 172.16.123.0 0.0.0.15
access-list 1 permit 172.16.12.0 0.0.0.7
access-list 1 permit 172.16.13.0 0.0.0.7
access-list 1 permit 172.16.23.0 0.0.0.7
access-list 1 deny   any
access-list 2 permit 10.2.2.2
```

```
access-list 2 permit 192.168.2.0 0.0.0.7
access-list 2 permit 192.168.22.0 0.0.0.31
access-list 2 permit 172.16.123.0 0.0.0.15
access-list 2 permit 172.16.12.0 0.0.0.7
access-list 2 permit 172.16.23.0 0.0.0.7
access-list 2 deny   any
access-list 101 permit ip any any
access-list 102 deny   ip any 192.168.1.0 0.0.0.7
access-list 102 deny   udp any any eq snmp
access-list 102 permit ip any any
!
!
!
!
!
banner motd ^CWelcome to the CCNA Metro-E Lab!^C
!
line con 0
 privilege level 15
line aux 0
 password cisco
 login
line vty 0 4
 access-class 1 in
 password cisco
 login
line vty 5 181
 access-class 1 in
 password cisco
 login
!
ntp clock-period 17180742
ntp server 10.99.99.4
!
end
```

IP ROUTING TABLE

```
R2# sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is 10.99.99.4 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.23.0/29 is directly connected, Tunnel3
C       172.16.12.0/29 is directly connected, Tunnel2
D       172.16.13.0/29 [90/310044416] via 172.16.23.3, 2d00h, Tunnel3
                       [90/310044416] via 172.16.12.1, 2d00h, Tunnel2
C       172.16.123.0/28 is directly connected, FastEthernet0/0.123
     192.168.11.0/27 is subnetted, 1 subnets
O IA    192.168.11.0 [89/2] via 172.16.123.1, 00:31:40, FastEthernet0/0.123
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.2.2.2/32 is directly connected, Loopback0
O IA    10.3.3.3/32 [89/2] via 172.16.123.3, 00:31:41, FastEthernet0/0.123
C       10.99.99.0/27 is directly connected, FastEthernet0/0.99
O IA    10.1.1.1/32 [89/2] via 172.16.123.1, 00:31:41, FastEthernet0/0.123
     192.168.22.0/27 is subnetted, 1 subnets
C       192.168.22.0 is directly connected, FastEthernet0/0.22
     192.168.1.0/29 is subnetted, 1 subnets
O IA    192.168.1.0 [89/2] via 172.16.123.1, 00:31:42, FastEthernet0/0.123
     192.168.2.0/29 is subnetted, 1 subnets
C       192.168.2.0 is directly connected, FastEthernet0/0.2
     192.168.3.0/29 is subnetted, 1 subnets
O IA    192.168.3.0 [89/2] via 172.16.123.3, 00:31:42, FastEthernet0/0.123
     192.168.33.0/27 is subnetted, 1 subnets
O IA    192.168.33.0 [89/2] via 172.16.123.3, 00:31:42, FastEthernet0/0.123
S*   0.0.0.0/0 [254/0] via 10.99.99.4
```

OSPF

```
R2#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.1.1          1   FULL/DROTHER    00:00:34    172.16.123.1    FastEthernet0/0.123
10.3.3.3          1   FULL/DR         00:00:37    172.16.123.3    FastEthernet0/0.123

R2#sh ip ospf interface
FastEthernet0/0.123 is up, line protocol is up
  Internet Address 172.16.123.2/28, Area 0
  Process ID 1, Router ID 10.2.2.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.3.3.3, Interface address 172.16.123.3
  Backup Designated router (ID) 10.2.2.2, Interface address 172.16.123.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 4
```

```
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 10.1.1.1
    Adjacent with neighbor 10.3.3.3  (Designated Router)
  Suppress hello for 0 neighbor(s)
FastEthernet0/0.22 is up, line protocol is up
  Internet Address 192.168.22.2/27, Area 2
  Process ID 1, Router ID 10.2.2.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.2.2.2, Interface address 192.168.22.2
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:09
  Index 3/4, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
FastEthernet0/0.2 is up, line protocol is up
  Internet Address 192.168.2.2/29, Area 2
  Process ID 1, Router ID 10.2.2.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.2.2.2, Interface address 192.168.2.2
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:09
  Index 2/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Loopback0 is up, line protocol is up
  Internet Address 10.2.2.2/32, Area 2
  Process ID 1, Router ID 10.2.2.2, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host

R2#sh ip ospf database

        OSPF Router with ID (10.2.2.2) (Process ID 1)

            Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.1.1        10.1.1.1        175         0x80000084 0x00031D 1
```

```
10.2.2.2        10.2.2.2        1977        0x80000086 0x00D640 1
10.3.3.3        10.3.3.3        214         0x80000082 0x00B65D 1

            Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
172.16.123.3    10.3.3.3        214         0x8000007C 0x00F456

            Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.1.1        10.1.1.1        1673        0x80000078 0x009119
10.2.2.2        10.2.2.2        460         0x80000003 0x0046D3
10.3.3.3        10.3.3.3        214         0x80000003 0x001004
192.168.1.0     10.1.1.1        1673        0x80000078 0x004E06
192.168.2.0     10.2.2.2        460         0x80000003 0x0019AC
192.168.3.0     10.3.3.3        986         0x80000078 0x000E3E
192.168.11.0    10.1.1.1        1674        0x80000078 0x004F13
192.168.22.0    10.2.2.2        462         0x80000003 0x00AB1E
192.168.33.0    10.3.3.3        1997        0x80000002 0x001F9D

            Router Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.2.2.2        10.2.2.2        462         0x80000003 0x008691 3

            Summary Net Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.1.1        10.2.2.2        209         0x80000002 0x0073A9
10.3.3.3        10.2.2.2        209         0x80000002 0x0031E5
172.16.123.0    10.2.2.2        1976        0x80000008 0x00D229
192.168.1.0     10.2.2.2        209         0x80000002 0x003096
192.168.3.0     10.2.2.2        209         0x80000002 0x001AAA
192.168.11.0    10.2.2.2        209         0x80000002 0x0031A3
192.168.33.0    10.2.2.2        209         0x80000002 0x003E80

R2# sh ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.2.2.2
  It is an area border router
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.2.2.2 0.0.0.0 area 2
    172.16.123.0 0.0.0.15 area 0
```

```
    192.168.2.0 0.0.0.7 area 2
    192.168.22.0 0.0.0.31 area 2
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.3.3.3             89      00:33:22
    10.1.1.1             89      00:33:22
  Distance: (default is 89)

Routing Protocol is "eigrp 111"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: connected, eigrp 111
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    172.16.12.0/29
    172.16.23.0/29
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.23.3          90      00:36:26
    172.16.12.1          90      00:36:26
  Distance: internal 90 external 170
```

4.3. R3 Configuration

```
CONFIGURATION

version 12.3
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$X5gk$eyWXzOA7wJx/w/IrFfVqL0
!
clock timezone PST -8
clock summer-time PDT date Mar 13 2011 2:00 Nov 6 2011 2:00
no aaa new-model
```

```
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
clns routing
no tag-switching ip
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 description LOOPBACK INTERFACE
 ip address 10.3.3.3 255.255.255.255
 ip access-group 101 in
 ip nat inside
!
interface Tunnel2
 description VPN BACKUP INTERFACE to R2
 ip address 172.16.23.3 255.255.255.248
 ip access-group 101 in
 ip nat inside
 cdp enable
 tunnel source FastEthernet0/0.99
 tunnel destination 10.99.99.5
!
interface Tunnel3
 description VPN BACKUP INTERFACE to R1
 ip address 172.16.13.3 255.255.255.248
 ip access-group 101 in
 ip nat inside
 cdp enable
 tunnel source FastEthernet0/0.99
 tunnel destination 10.99.99.7
!
```

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.3
 description MANAGEMENT VLAN
 encapsulation dot1Q 3
 ip address 192.168.3.3 255.255.255.248
 ip access-group 1 out
 ip nat inside
!
interface FastEthernet0/0.33
 description PRODUCTION VLAN
 encapsulation dot1Q 33
 ip address 192.168.33.3 255.255.255.224
 ip nat inside
!
interface FastEthernet0/0.99
 description INTERNET INTERFACE
 encapsulation dot1Q 99
 ip address dhcp
 ip access-group 102 in
 ip nat outside
!
interface FastEthernet0/0.123
 description METRO ETHERNET WAN INTERFACE
 encapsulation dot1Q 123
 ip address 172.16.123.3 255.255.255.240
 ip access-group 101 in
 ip nat inside
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
!
router eigrp 111
 redistribute connected
 network 172.16.13.0 0.0.0.7
 network 172.16.23.0 0.0.0.7
 no auto-summary
 eigrp router-id 10.3.3.3
!
router ospf 1
 router-id 10.3.3.3
 log-adjacency-changes
 network 10.3.3.3 0.0.0.0 area 3
 network 172.16.123.0 0.0.0.15 area 0
```

```
 network 192.168.3.0 0.0.0.7 area 3
 network 192.168.33.0 0.0.0.31 area 3
 distance 89
!
ip nat inside source list 1 interface FastEthernet0/0.99 overload
no ip http server
ip classless
!
!
access-list 1 permit 10.2.2.2
access-list 1 permit 10.3.3.3
access-list 1 permit 10.1.1.1
access-list 1 permit 192.168.1.0 0.0.0.7
access-list 1 permit 192.168.11.0 0.0.0.31
access-list 1 permit 192.168.2.0 0.0.0.7
access-list 1 permit 192.168.22.0 0.0.0.31
access-list 1 permit 192.168.3.0 0.0.0.7
access-list 1 permit 192.168.33.0 0.0.0.31
access-list 1 permit 10.99.99.0 0.0.0.31
access-list 1 permit 172.16.123.0 0.0.0.15
access-list 1 permit 172.16.12.0 0.0.0.7
access-list 1 permit 172.16.13.0 0.0.0.7
access-list 1 permit 172.16.23.0 0.0.0.7
access-list 1 deny   any
access-list 2 permit 10.3.3.3
access-list 2 permit 192.168.3.0 0.0.0.7
access-list 2 permit 192.168.33.0 0.0.0.31
access-list 2 permit 172.16.123.0 0.0.0.15
access-list 2 permit 172.16.13.0 0.0.0.7
access-list 2 permit 172.16.23.0 0.0.0.7
access-list 2 deny   any
access-list 101 permit ip any any
access-list 102 deny   ip any 192.168.1.0 0.0.0.7
access-list 102 deny   udp any any eq snmp
access-list 102 permit ip any any
!
!
!
!
!
banner motd ^CWelcome to the CCNA Metro-E Lab!^C
!
line con 0
 privilege level 15
line aux 0
 password cisco
 login
line vty 0 4
```

```
 access-class 1 in
 password cisco
 login
line vty 5 181
 access-class 1 in
 password cisco
 login
!
ntp clock-period 17180558
ntp server 10.99.99.4
!
end
```

IP ROUTING TABLE

```
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.99.99.4 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.23.0/29 is directly connected, Tunnel2
D       172.16.12.0/29 [90/310044416] via 172.16.23.2, 2d00h, Tunnel2
                       [90/310044416] via 172.16.13.1, 2d00h, Tunnel3
C       172.16.13.0/29 is directly connected, Tunnel3
C       172.16.123.0/28 is directly connected, FastEthernet0/0.123
     192.168.11.0/27 is subnetted, 1 subnets
O IA    192.168.11.0 [89/2] via 172.16.123.1, 00:34:44, FastEthernet0/0.123
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O IA    10.2.2.2/32 [89/2] via 172.16.123.2, 00:34:45, FastEthernet0/0.123
C       10.3.3.3/32 is directly connected, Loopback0
C       10.99.99.0/27 is directly connected, FastEthernet0/0.99
O IA    10.1.1.1/32 [89/2] via 172.16.123.1, 00:34:45, FastEthernet0/0.123
     192.168.22.0/27 is subnetted, 1 subnets
O IA    192.168.22.0 [89/2] via 172.16.123.2, 00:34:49, FastEthernet0/0.123
     192.168.1.0/29 is subnetted, 1 subnets
O IA    192.168.1.0 [89/2] via 172.16.123.1, 00:34:49, FastEthernet0/0.123
     192.168.2.0/29 is subnetted, 1 subnets
O IA    192.168.2.0 [89/2] via 172.16.123.2, 00:34:49, FastEthernet0/0.123
     192.168.3.0/29 is subnetted, 1 subnets
C       192.168.3.0 is directly connected, FastEthernet0/0.3
     192.168.33.0/27 is subnetted, 1 subnets
```

```
C       192.168.33.0 is directly connected, FastEthernet0/0.33
S*   0.0.0.0/0 [254/0] via 10.99.99.4
```

OSPF

```
R3#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.1.1.1          1   FULL/DROTHER    00:00:35    172.16.123.1    FastEthernet0/0.123
10.2.2.2          1   FULL/BDR        00:00:36    172.16.123.2    FastEthernet0/0.12

R3#sh ip ospf interface
FastEthernet0/0.123 is up, line protocol is up
  Internet Address 172.16.123.3/28, Area 0
  Process ID 1, Router ID 10.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.3.3.3, Interface address 172.16.123.3
  Backup Designated router (ID) 10.2.2.2, Interface address 172.16.123.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:09
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 4
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 10.1.1.1
    Adjacent with neighbor 10.2.2.2  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
FastEthernet0/0.33 is up, line protocol is up
  Internet Address 192.168.33.3/27, Area 3
  Process ID 1, Router ID 10.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.3.3.3, Interface address 192.168.33.3
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Index 2/4, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Loopback0 is up, line protocol is up
  Internet Address 10.3.3.3/32, Area 3
  Process ID 1, Router ID 10.3.3.3, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
```

```
FastEthernet0/0.3 is up, line protocol is up
  Internet Address 192.168.3.3/29, Area 3
  Process ID 1, Router ID 10.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.3.3.3, Interface address 192.168.3.3
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Index 1/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)

R3#sh ip ospf database

        OSPF Router with ID (10.3.3.3) (Process ID 1)

            Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.1.1        10.1.1.1        362         0x80000084 0x00031D 1
10.2.2.2        10.2.2.2        140         0x80000087 0x00D441 1
10.3.3.3        10.3.3.3        400         0x80000082 0x00B65D 1

            Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
172.16.123.3    10.3.3.3        400         0x8000007C 0x00F456

            Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.1.1        10.1.1.1        1860        0x80000078 0x009119
10.2.2.2        10.2.2.2        648         0x80000003 0x0046D3
10.3.3.3        10.3.3.3        400         0x80000003 0x001004
192.168.1.0     10.1.1.1        1860        0x80000078 0x004E06
192.168.2.0     10.2.2.2        648         0x80000003 0x0019AC
192.168.3.0     10.3.3.3        1172        0x80000078 0x000E3E
192.168.11.0    10.1.1.1        1863        0x80000078 0x004F13
192.168.22.0    10.2.2.2        651         0x80000003 0x00AB1E
192.168.33.0    10.3.3.3        151         0x80000003 0x001D9E

            Router Link States (Area 3)

Link ID         ADV Router      Age         Seq#       Checksum Link count
```

10.3.3.3 10.3.3.3 151 0x8000007E 0x001176 3

Summary Net Link States (Area 3)

Link ID	ADV Router	Age	Seq#	Checksum
10.1.1.1	10.3.3.3	403	0x80000002	0x005EBB
10.2.2.2	10.3.3.3	403	0x80000002	0x003DD9
172.16.123.0	10.3.3.3	151	0x80000080	0x00CCB3
192.168.1.0	10.3.3.3	403	0x80000002	0x001BA8
192.168.2.0	10.3.3.3	403	0x80000002	0x0010B2
192.168.11.0	10.3.3.3	403	0x80000002	0x001CB5
192.168.22.0	10.3.3.3	403	0x80000002	0x00A224

EIGRP

R3# sh ip eigrp neighbors
IP-EIGRP neighbors for process 111

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
1	172.16.23.2	Tu2	11	2d19h	137	5000	0	109
0	172.16.13.1	Tu3	14	2d19h	103	5000	0	95

R3# sh ip eigrp interfaces
IP-EIGRP interfaces for process 111

Interface	Xmit Queue Peers	Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Tu3	1	0/0	103	71/2702	2926	0
Tu2	1	0/0	137	71/2702	2914	0

R3# sh ip eigrp topology
IP-EIGRP Topology Table for AS(111)/ID(10.3.3.3)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 10.2.2.2/32, 0 successors, FD is Inaccessible
via 172.16.23.2 (297372416/128256), Tunnel2
P 10.3.3.3/32, 1 successors, FD is 128256
via Rconnected (128256/0)
P 10.99.99.0/27, 1 successors, FD is 28160
via Rconnected (28160/0)
P 10.1.1.1/32, 0 successors, FD is Inaccessible
via 172.16.13.1 (297372416/128256), Tunnel3
P 192.168.33.0/27, 1 successors, FD is 28160
via Rconnected (28160/0)
P 192.168.11.0/27, 0 successors, FD is Inaccessible
via 172.16.13.1 (297246976/28160), Tunnel3

```
P 192.168.1.0/29, 0 successors, FD is Inaccessible
       via 172.16.13.1 (297246976/28160), Tunnel3
P 192.168.2.0/29, 0 successors, FD is Inaccessible
       via 172.16.23.2 (297246976/28160), Tunnel2
P 192.168.3.0/29, 1 successors, FD is 28160
       via Rconnected (28160/0)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.22.0/27, 0 successors, FD is Inaccessible
       via 172.16.23.2 (297246976/28160), Tunnel2
P 172.16.23.0/29, 1 successors, FD is 297244416
       via Connected, Tunnel2
P 172.16.12.0/29, 2 successors, FD is 310044416
       via 172.16.13.1 (310044416/297244416), Tunnel3
       via 172.16.23.2 (310044416/297244416), Tunnel2
P 172.16.13.0/29, 1 successors, FD is 297244416
       via Connected, Tunnel3
P 172.16.123.0/28, 1 successors, FD is 28160
       via Rconnected (28160/0)

R3# sh ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.3.3.3
  It is an area border router
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.3.3.3 0.0.0.0 area 3
    172.16.123.0 0.0.0.15 area 0
    192.168.3.0 0.0.0.7 area 3
    192.168.33.0 0.0.0.31 area 3
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.2.2.2              89      00:37:30
    10.1.1.1              89      00:37:30
  Distance: (default is 89)

Routing Protocol is "eigrp 111"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
```

```
  EIGRP maximum metric variance 1
  Redistributing: connected, eigrp 111
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    172.16.13.0/29
    172.16.23.0/29
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.16.23.2          90      00:40:34
    172.16.13.1          90      00:40:35
  Distance: internal 90 external 170
```

4.4. R4 Configuration

CONFIGURATION

```
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot system flash:c2800nm-adventerprisek9-mz.150-1.M.bin
boot system flash usb1:c2800nm-adventerprisek9-mz.150-1.M.bin
boot-end-marker
!
card type e1 0 0
enable secret 5 $1$Woft$KnObg3Q90YQtwfhBw7SKy.
!
no aaa new-model
!
!
!
clock timezone PST -8
clock summer-time PDT date Mar 13 2011 2:00 Nov 6 2011 2:00
network-clock-participate wic 0
network-clock-participate wic 1
!
dot11 syslog
ip source-route
!
!
ip cef
```

```
ip dhcp excluded-address 10.99.99.1 10.99.99.4
!
ip dhcp pool Internet_VLAN
   network 10.99.99.0 255.255.255.224
   default-router 10.99.99.4
   dns-server 216.136.95.2 64.132.94.250
!
!
ip name-server 216.136.95.2
ip name-server 64.132.94.250
no ipv6 cef
!
multilink bundle-name authenticated
!
license udi pid CISCO2811 sn FTX1240A1NQ
!
interface FastEthernet0/0
 no ip address
 duplex half
 speed auto
 !
!
interface FastEthernet0/0.99
 description INTERNET VLAN
 encapsulation dot1Q 99
 ip address 10.99.99.4 255.255.255.224
!
interface FastEthernet0/1
 ip address 192.168.254.4 255.255.255.0
 ip virtual-reassembly
 duplex half
 speed auto
 !
ip route 0.0.0.0 0.0.0.0 192.168.254.1
!
access-list 1 permit 10.2.2.2
access-list 1 permit 10.3.3.3
access-list 1 permit 10.1.1.1
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.11.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.22.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit 192.168.33.0 0.0.0.255
access-list 1 permit 10.99.99.0 0.0.0.255
access-list 1 permit 172.16.12.0 0.0.0.255
access-list 1 permit 172.16.23.0 0.0.0.255
access-list 1 deny   any
```

```
access-list 1 permit 192.168.1.0 0.0.0.7
access-list 1 permit 192.168.11.0 0.0.0.31
access-list 1 permit 192.168.2.0 0.0.0.7
access-list 1 permit 192.168.22.0 0.0.0.31
access-list 1 permit 192.168.3.0 0.0.0.7
access-list 1 permit 192.168.33.0 0.0.0.31
access-list 1 permit 10.99.99.0 0.0.0.31
access-list 1 permit 172.16.123.0 0.0.0.15
access-list 1 permit 172.16.12.0 0.0.0.7
access-list 1 permit 172.16.13.0 0.0.0.7
access-list 1 permit 172.16.23.0 0.0.0.7
!
!
!
!
!
!
control-plane
 !
!
!
!
banner motd ^CWelcome to the CCNA Metro-E Lab!^C
!
line con 0
 privilege level 15
 password cisco
line aux 0
 password cisco
 login
line vty 0 4
 access-class 1 in
 password cisco
 login
 transport input telnet ssh
line vty 5 988
 access-class 1 in
 password cisco
 login
 transport input telnet ssh
!
scheduler allocate 20000 1000
ntp server 128.249.1.1
end
```

4.5. SW1 Configuration

CONFIGURATION

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SW1-3550
!
enable secret 5 $1$nrbE$yBDx0XOB2MkgzEQ8yxL88/
!
clock timezone PST -8
clock summer-time PDT date Mar 13 2011 2:00 Nov 6 2011 2:00
ip subnet-zero
ip routing
!
no ip domain-lookup
vtp domain null
vtp mode transparent
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan 2-3,11,22,33,99,123
!
!
interface Port-channel1
 switchport trunk encapsulation isl
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

```
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/5
 switchport mode access
!
interface FastEthernet0/6
 switchport mode access
!
interface FastEthernet0/7
 switchport mode dynamic desirable
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk

<configuration interface 0/9 - 48 omitted>

interface Vlan1
 no ip address
!
interface Vlan99
 ip address 10.99.99.2 255.255.255.0
!
ip classless
no ip http server
!
access-list 1 permit 10.2.2.2
access-list 1 permit 10.3.3.3
access-list 1 permit 10.1.1.1
access-list 1 permit 192.168.1.0 0.0.0.7
access-list 1 permit 192.168.11.0 0.0.0.31
access-list 1 permit 192.168.2.0 0.0.0.7
access-list 1 permit 192.168.22.0 0.0.0.31
access-list 1 permit 192.168.3.0 0.0.0.7
access-list 1 permit 192.168.33.0 0.0.0.31
access-list 1 permit 10.99.99.0 0.0.0.31
access-list 1 permit 172.16.123.0 0.0.0.15
access-list 1 permit 172.16.12.0 0.0.0.7
access-list 1 permit 172.16.13.0 0.0.0.7
access-list 1 permit 172.16.23.0 0.0.0.7
access-list 1 deny   any
banner motd ^CWelcome to the CCNA Metro-E Lab!^C
!
line con 0
 privilege level 15
 password cisco
```

```
line vty 0 4
 access-class 1 in
 password cisco
 login
line vty 5 15
 access-class 1 in
 password cisco
 login
!
ntp clock-period 17180530
ntp server 10.99.99.4
!
end
```