Name:

Rack Number:

Instructions:

1. Please read the entire paper before you start.
2. Use of calculators strictly prohibited. No cell phone allowed.
3. Use of commserver is compulsory. (No points for using it, but negative 5 for not using it)
4. Make necessary assumptions; just don't change the network, and addition of extra physical connections is strictly prohibited.
5. Please clean up all the devices before you leave (Negative 10 for not cleaning your devices).
6. Everything will be tested before giving out any perfect points. Partials will not be granted.
7. If at all there is any proved discrepancy in the paper then points will be awarded based on appropriate solution that you have. You can contact a SA if you have doubts in the paper
8. ‘Copy Run start’ or ‘write mem’ at regular intervals to ensure that you don’t lose your configurations if a device crashes.

Important tip: Keep calm and don’t panic! ☺

Background:

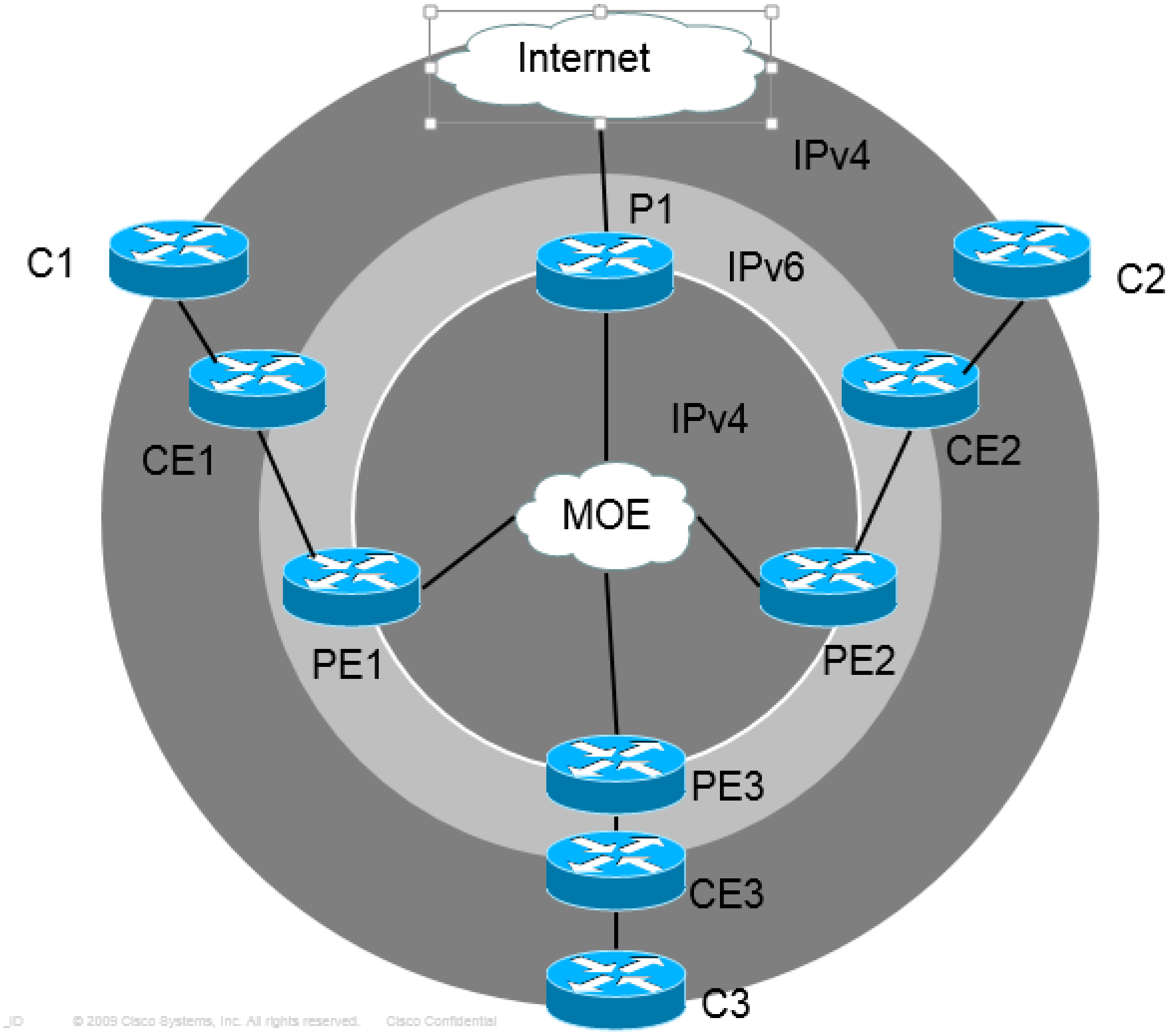
You have been tasked with connecting three locations in Colorado for the government. There are three sites: Boulder, Denver, and Longmont. All the three sites have to behave like one seamless network under the Colorado administration.

On your first day as a network administrator, you realize that all of the sites are IPv4 compatible only. You have got push from your management to use IPv6. In that transition, you have deployed edge routers as dual-stack as a first step towards IPv6 adoption. In addition all the sites are located at various locations and need to connect to each other via the ISP Level 5.

For configuring this network, Level 5 has provided you access to its core and edge equipment. You find that Level 5 believes that its core needs to be simple and cost-effective which is why Level 5 has implemented metro-ethernet in its core.

Design the network in such a way that all users are able to connect with each other on all sites.

Best of Luck!


Internet
IPv4
C1
P1
IPv6
C2
CE1
IPv4
CE2
MOE
PE1
PE2
PE3
CE3
C3
_ID © 2009 Cisco Systems, Inc. All rights reserved. Cisco Confidential

<u>The “Merged” Topology:</u>

1. **Global IP Addressing:**

- ARIN has assigned Level-5 Telecom an IPv6 block of 266X:XX::/32. Level-5 Telecom decides to use an IPv4 space of 60.X.0.0/16 for MetroEthernet and MPLS network and an IPv6 block of 266X:XX::/48 inside their Core network.
- The Colorado government has been assigned an IPv6 block of 266X:XX:X::/48 from the ISP where X is your rack number. The IPv6 block must be sub-netted and used for connection between customer edge and service provider network for all three sites.
- The Colorado government has decided to use 192.168.1X.0/24 to connect their CE routers with C routers. Use optimal IPv4 sub-netting on point to point links especially on the CE to C link.
- You are free to allocate a /64 IPV6 network on each CE to PE link.

2. **Colorado's Internal network:**

- <u>Longmont Site:</u>
  <u>IPv4 Address:</u>

Uses a private IPv4 address space of 172.16.X.0./21 where “X” is the rack number and the groups of IPv4 users are as follows:

S/N	Unit	Number of Users	Address Assignment
1	Users	756	Static
2	Administration	123	Static

- Boulder Site:
  IPv4 Address:
  Use a private IPv4 address space of 172.2X.0.0/19 where “X” is the rack number and the Groups of IPv4 users are as follows:

S/N	Unit	Number of Users	Address Assignment
1	Users	2000	Static
2	Administration	128	Static

- Denver -
  IPv4 Addressing:
  Use a private IPv4 address space of 172.30.6X.0/17 where “X” is the rack number and the groups of IPv4 users are as follows:

S/N	Unit	Number of Users	Address Assignment
1	Users	987	Static
2	Administration	203	Static

Page for IP Addressing **(Note: 0 points for v4. Negative marks if you get v4 addressing wrong)**

Please indicate the global and private addressing used in the global and private networks of Level 5 and the 4 sites.

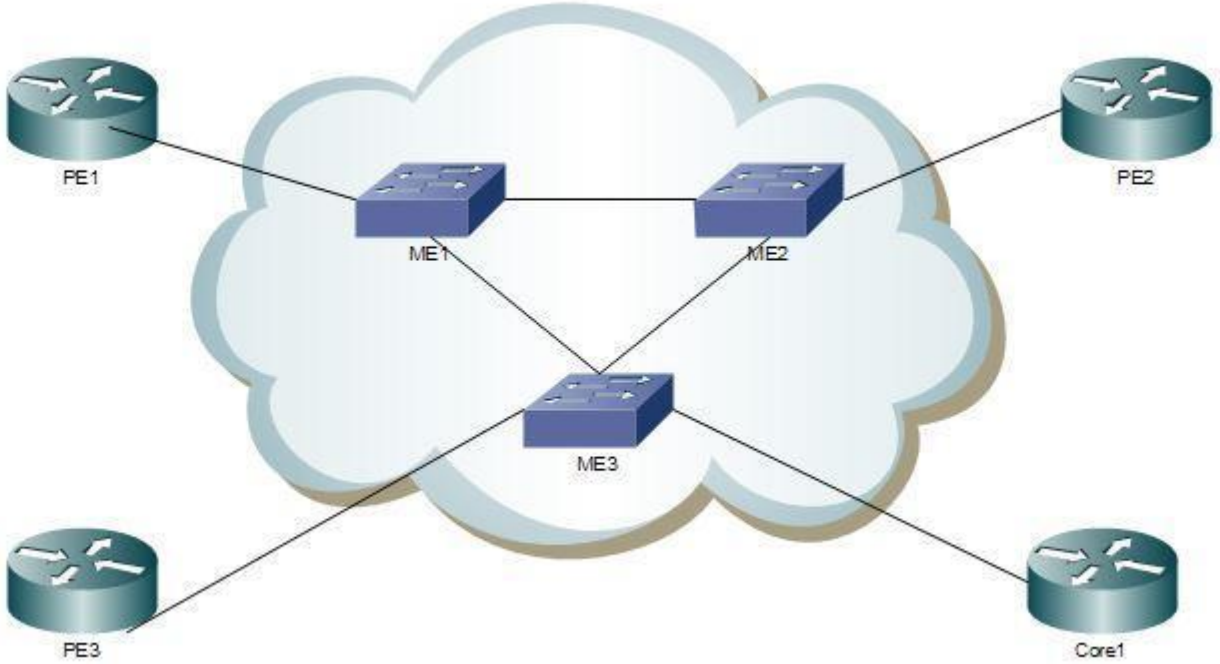
TLEN 5460: Telecommunications Systems Lab
Final Practical: Fall 2014

MetroEthernet [5 points]:

- Level 5 has chosen a MetroEthernet QinQ cloud to provide a layer 2 connectivity to all the sites.
- The PE and CORE1 (P1) routers are connected to Metro switches in the core and the topology for that has been shared with you.
- The PE and CORE1 (P1) router interfaces that connect to the MetroSwitch tag the packet with a Vlan tag of 7X where X is the number of your rack. The Metro Switches add a metro tag of 2X and pass it between them.

Checklist:

- The metro tag should show if traffic is sniffed in the core network
- Assign IPv4 addresses appropriately
- Maintain connectivity on link failure
- If MPLS is not working at this stage, make the rest of the network run on Metro to get marks for that.



5. MPLS [15 points]

- Level 5 Telecom is trying to provide traffic engineering towards it customers by utilizing all of its available circuits. Level 5 runs its MPLS TE network on top of its metro ethernet cloud.

TLEN 5460: Telecommunications Systems Lab
Final Practical: Fall 2014

- Level 5 has a SLA with the Colorado government to provide it a dedicated link for its traffic between its sites. Only Colorado sites' traffic should pass through these tunnels. Remember no traffic from Colorado destined to the Internet or the Level 5 core traffic should pass through these Tunnels.

- In addition to providing dedicated links, Level 5 also has an SLA to provide bandwidth of 200kbps for all the sites.

- The three edge routers of Level 5 have 6 tunnels between them to create a full mesh connectivity between the sites. Level 5 has also provided Colorado with a high priority tunnel **Tunnel 7** with a 200kbps guaranteed bandwidth that follows the same path as Tunnel 1. When Tunnel 7 is signaled, it should tear down Tunnel 1 and the traffic should pass through Tunnel 7. Tunnel 7 should NOT have a dynamic path.

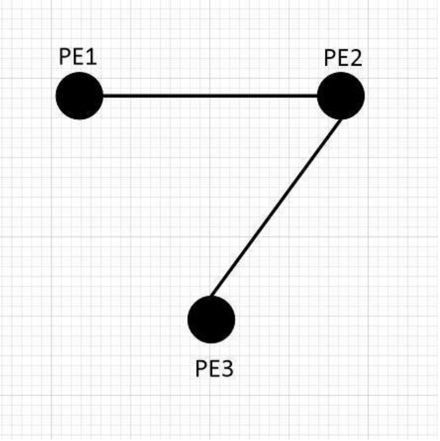
- There are a few restrictions made by Level 5 to you when designing this topology.
    - The total bandwidth that is the bandwidth of the sum of all interfaces on a PE router should not exceed 800kbps. E.g. On the PE3 router, the sum of the bandwidth assigned to the two interfaces and their sub-interfaces should not exceed 800kbps.
    - The use of static routes are permitted to route traffic through the tunnel

    - The PE routers should not form LDP neighborship with each other in order to reduce the CPU utilization on them
    - All MPLS tunnels should automatically check for better paths available and optimize to them every 100 seconds
    - Do not use random IP addresses to source you MPLS tunnels, use IPs from the block assigned to Level 5.
    - All MPLS should be signaled by RSVP and should have static strict EROs. No backup or loose EROs will be considered
    - Make sure that labels are seen if a traceroute is done from any customer site.

- The 6 MPLS tunnel paths are as follows:

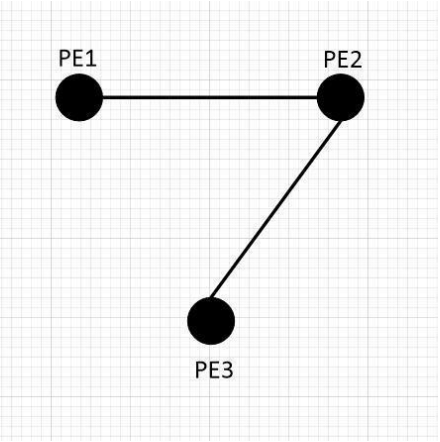
Tunnel 1

Path: PE1- PE2 - PE3
Bandwidth Requested: 200Kbps



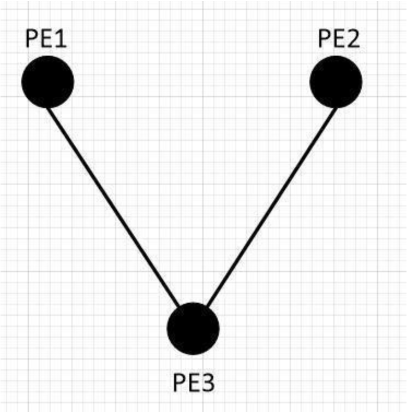
Tunnel 2

Path: PE3- PE2 – PE1
Bandwidth Requested: 200Kbps



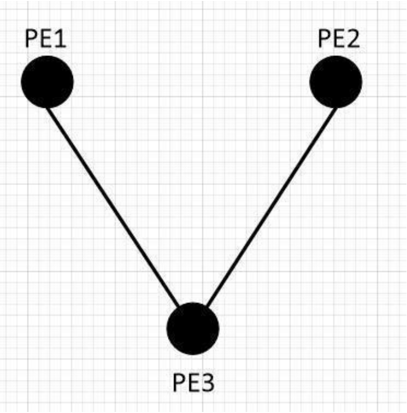
Tunnel 3

Path: PE1- PE3 – PE2
Bandwidth Requested: 200Kbps



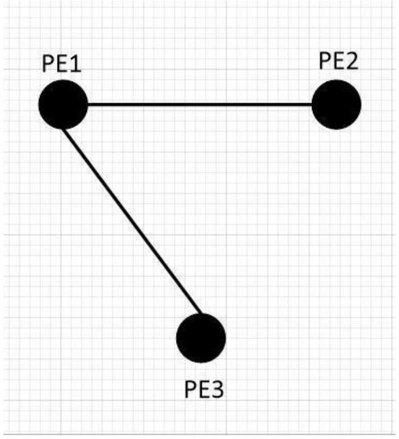
Tunnel 4

Path: PE2 - PE3 – PE1
Bandwidth Requested: 200Kbps



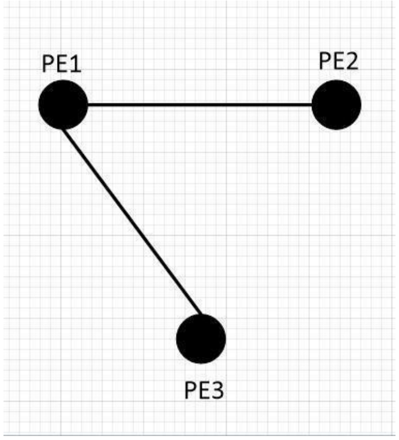
<u>Tunnel 5</u>

Path: PE2 – PE1 – PE3
Bandwidth Requested: 200Kbps



<u>Tunnel 6</u>

Path: PE3 – PE1 – PE2
Bandwidth Requested: 200Kbps



<u>Checklist:</u>

- MPLS tunnels should be up/up with static EROs
- The bandwidth at the interfaces should be within the limits for the SLA
- Only Colorado goverment site to site traffic should pass through the tunnels
- Each tunnel should have a backup path but should not use it unless the main one fails
- At this point if you are unable to make explicit path work then switch over to dynamic and continue the paper for the remaining marks

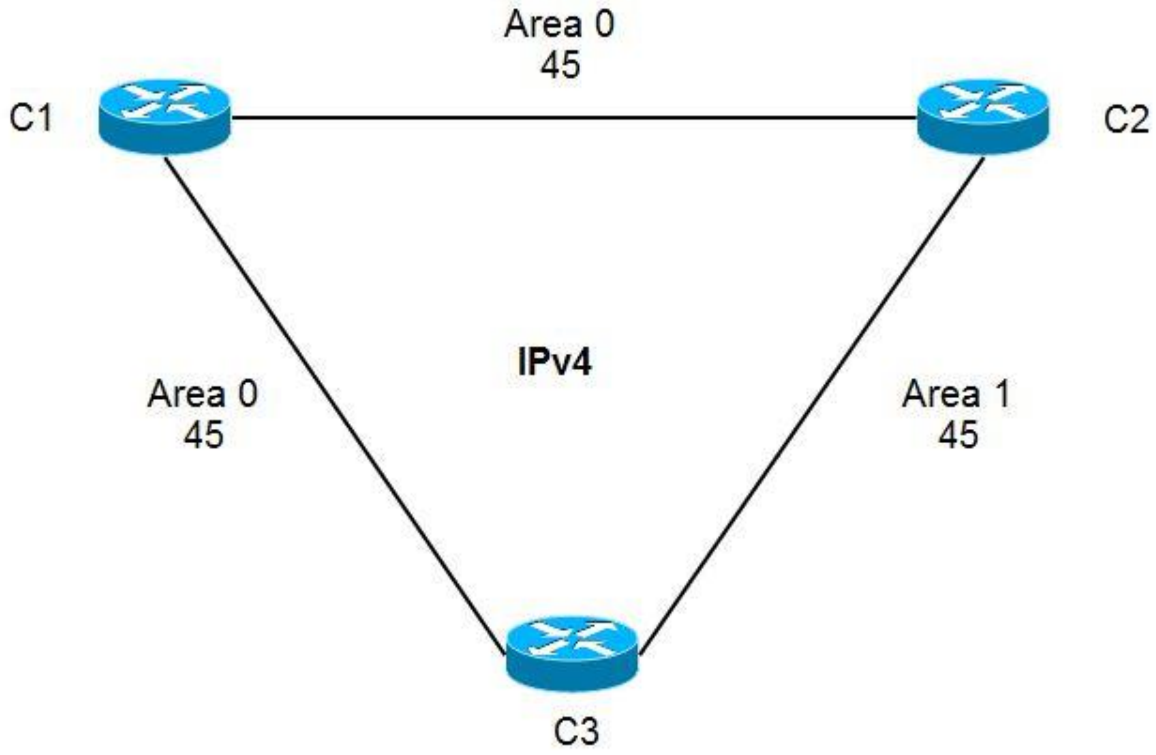
7. **IGP [15 points]:**

<u>Customer Routing:</u>

- The customer routers (C1, C2 and C3) are running only IPv4. The Boulder site is the backbone area of the OSPF process 45 and all the networks behind the router are in the backbone area. Longmont and Denver are present in area 1 of the OSPF 45 process.

Make use of GRE tunnels for the sites at Longmont and Denver to be able to connect to the Boulder backbone OSPF area. The security restrictions that Colorado has for this method of tunneling is that all the traffic that passes through the GRE tunnel should be encrypted including the OSPF traffic that passes through it

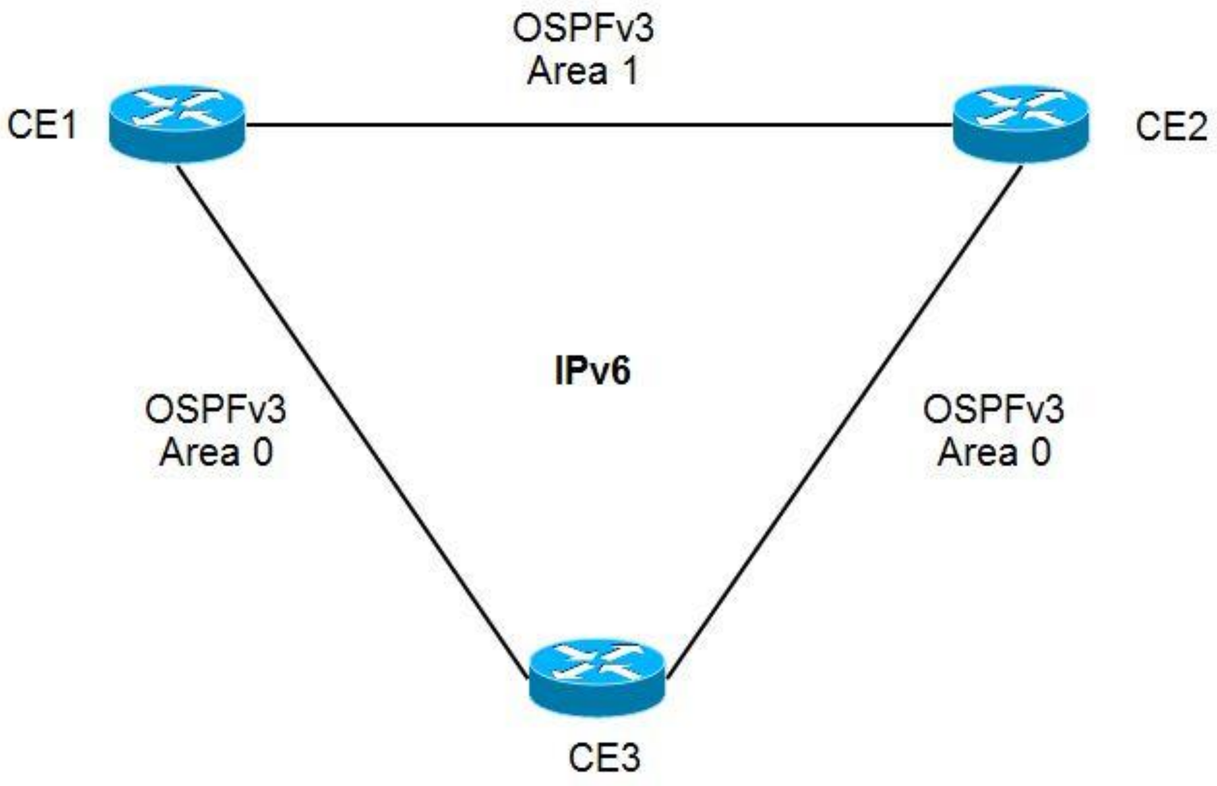
- Refer to the topology provided to you for implementing the OSPF process



Customer Edge Routing:

- The Denver site is in the backbone area of the OSPF v3 process 65. The Boulder and Longmont sites are in area 1 and connect to it via OSPF v3 process 65.

- Refer to the diagram provided to you to implement the topology



Routing between Level 5 and the Colorado network:

Devices	Routing Protocol v4	Routing Protocol v6
CE1 – PE1	OSPF 10 area 0	OSPF 10 area 0
CE2 – PE2	RIP v2	RIPng
CE3 – PE3	OSPF 110 area 0	OSPF 110 area 0

Routing inside the Level 5 Core:

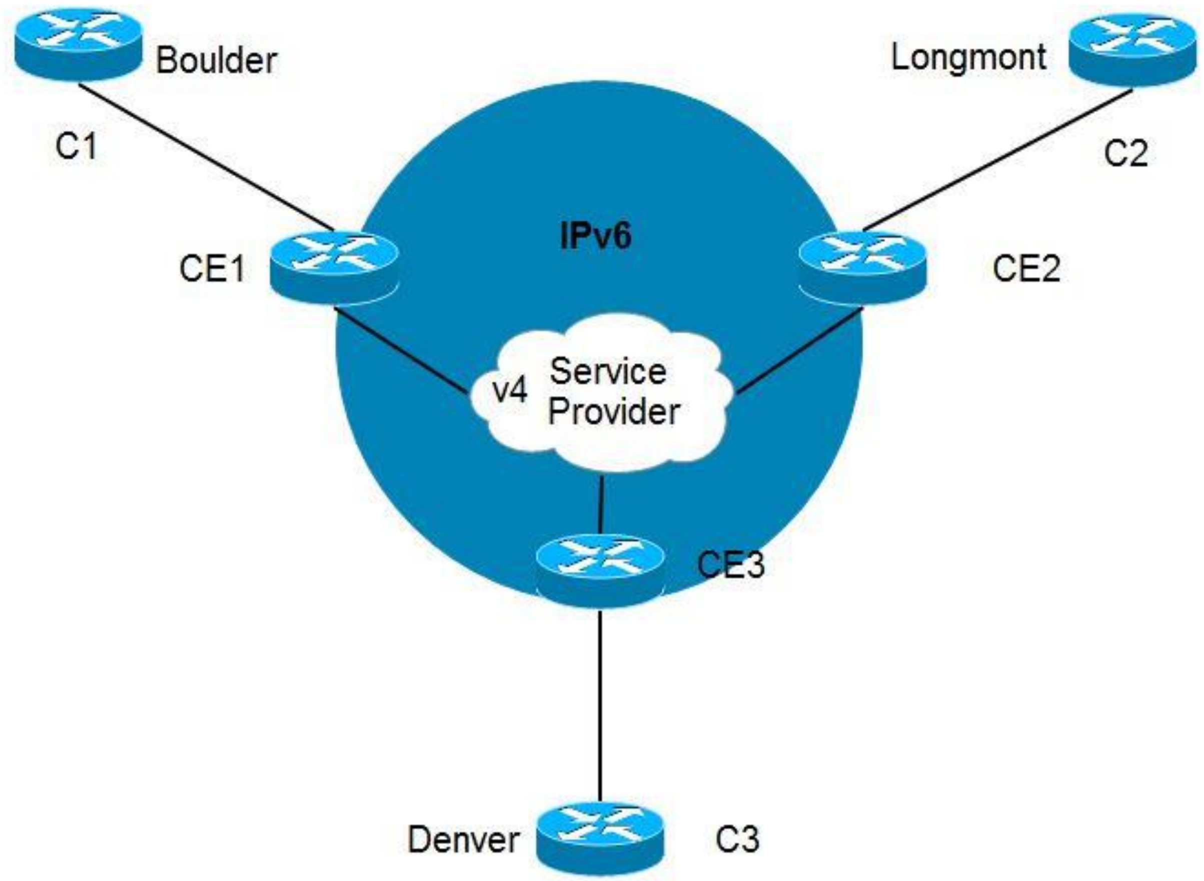
- The Level 5 core uses OSPF process ID 80 for all the PE routers to communicate with each other
- The CORE1(P1) router provides the core a route to reach the Internet
- The CE routers send all their traffic to the PE router they are connected to in order to be able to reach outside their network.

8. Redistribution [10 points]

- Enable redistribution at specific points inside the network topology to obtain reachability. The redistribution should be optimum.

Checklist:

- Redistribution should not be forming loops
- There should be full end-to-end connectivity
- The metrics for redistribution should be appropriate
- The private networks of any of the 3 sites and the Level 5 core should not be seen in each other's route table.



9. IPv6 Tunnelling: [15 points]

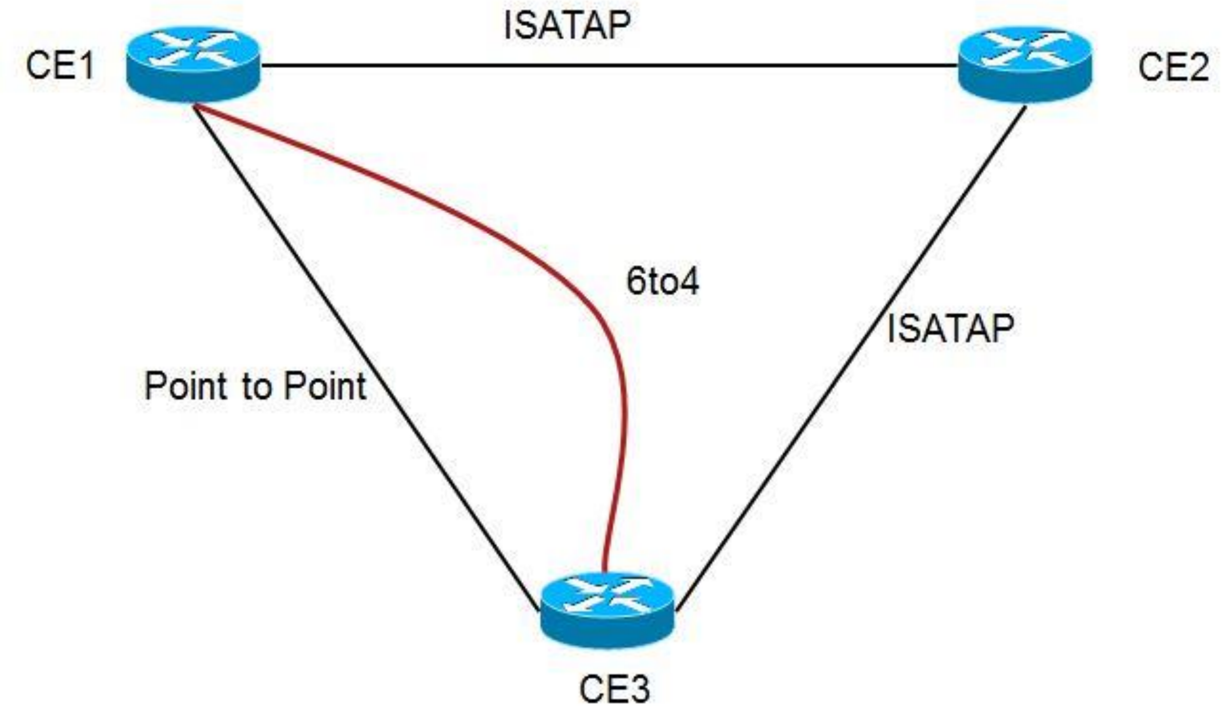
- The email and database servers located at the Boulder core and Denver site should be able to connect to each other via a 6 to 4 tunnel
- A hub and spoke ISATAP tunnel should be present between the Longmont, Boulder and Denver sites with the Longmont site as the hub and with Boulder and Denver as the spokes.
- IPv6 users at the Boulder and the Denver office should use the a backup path for the IPv6 via the native IPv6 point to point link (GRE) in the Level 5 core. This path should be taken if 6to4 and ISATAP fail.

Checklist:

- All tunnels should be up/up
- Use appropriate IPv4 and IPv6 addresses for tunneling

- The traffic should be going over the primary tunnels and the backup should be in the order provide to you

- IPv6 traffic should be encrypted.
- NAT-PT translations should be appropriate
- The routing inside the GRE and ISATAP tunnels should be as specified in the IGP objective



10. IPSec [10 points]

- The hosts in the User networks across all the Colorado sites should send encrypted traffic via policy based IPsec.
- The Administration across all the three sites should be able to communicate securely to each other via route based IPSec passing through the GRE tunnels already created.
- Secure IPv6 traffic also between all the sites that are IPv6 capable.

Checklist

- Access-lists should be configured properly for appropriate users to take the correct tunnel.
- Crypto-maps should be implemented at the right place. Hint: Consider link failures.
- Security Associations should be appropriate.
- Encrypted traffic should flow inside the MPLS tunnels.
- Ensure the Policy based tunnel is configured correctly.

11. NAT [5 points]:

- Only administration department host should be able to connect to the Internet via the public IP discovered on the CORE1(P1) interface

12. Access Lists [5 points]:

- Only users inside Colorado's Administration network should be able to remotely manage all the network devices.
- Any incoming request except ICMP from the Internet should be blocked at all PE and CE routers. Punch holes for necessary connectivity for IPsec etc.
  Hint: Do this at the end or you might take your network down!
- Only an IT head can access the devices in the Level 5 network. Hint: You can create loopbacks on the devices to emulate an IT network.

13. Internet [15 points]:

- The Internet service is provided to Colorado via Level 5's CORE1(P1) router.
- The Level 5 provider buys transit from a local Internet service provider. The local provider has installed their equipment in your lab. There is a common switch provided for all of you. **Do not MESS with this switch**.
- To provide Internet access you will just need plug your device in the equipment provided to you by the local ISP and receive an IP address.
- Use appropriate DNS server for resolving IP addresses.

14. SSH [5 points]:

- For security reasons the Colorado administration does not manage its devices on the traditional port 22 assigned for SSH
- Use SSH port-forwarding starting at port 5X40 to remotely access devices that support it.
- The Admin for Colorado uses SSH to remotely manage devices on the IPv4 and IPv6 networks (where possible).
- Enable ssh timeout to 60s after a period of inactivity and an authentication retry limit of 3.
- At a time, 7 administrators can ssh to a single router.
- Use other forms of remote management where SSH is not possible