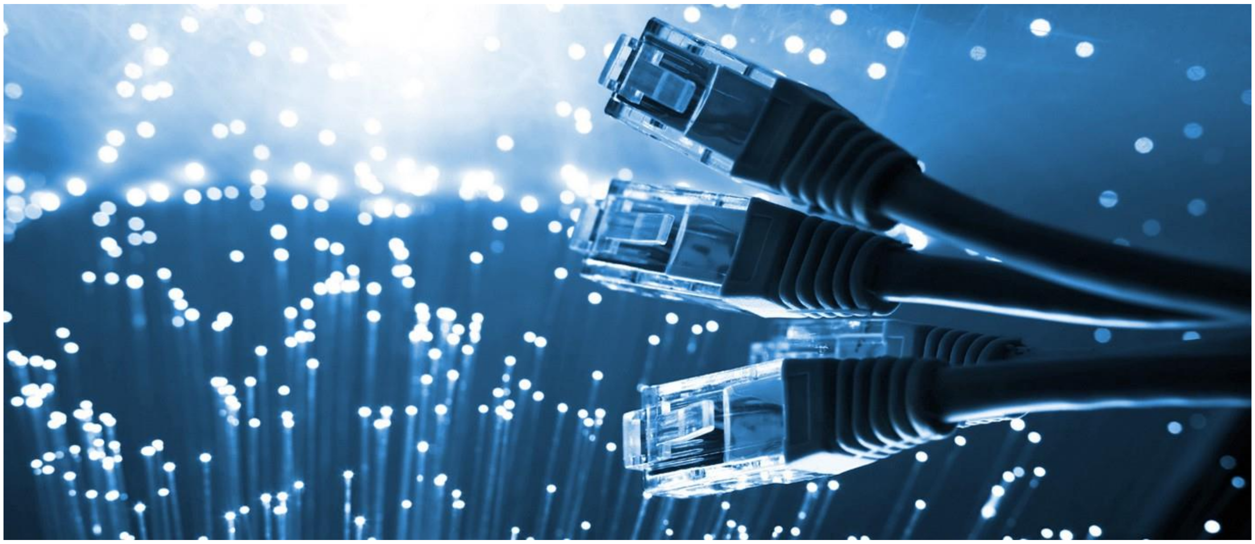
Project

Phase I LAN Design



Submitted By

Uddeshya Sinha

IN 723 Advanced Networking

Feb-June 2018

Lecturer

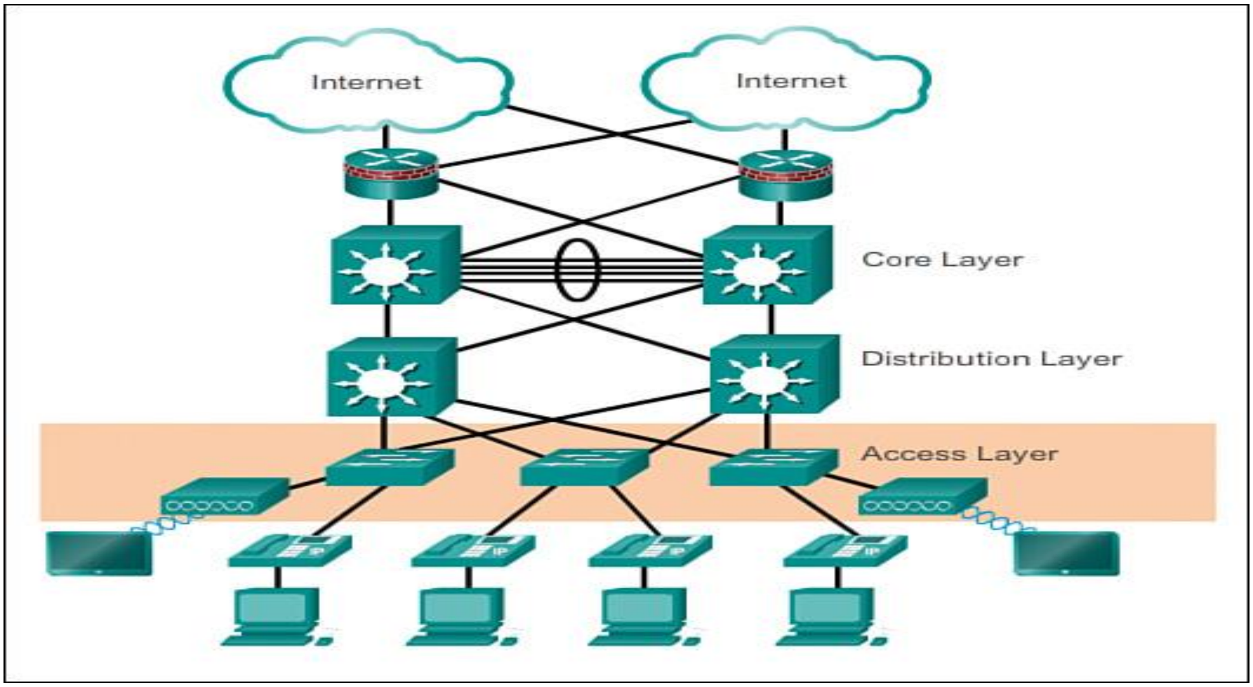
Michael Holtz

Date: **Friday 4th May**

High Level Design

LAN or Local Area Network is referred to as a collection of routers, switches, cables, modems, servers, PCs etc. communicating with each other which spans a distinct geographical area such as an office, college or a commercial establishment. Typically, there are three types of LAN networks depending upon the number of devices serviced – small, medium or large.

For LAN design, we have adopted the Cisco hierarchical (three-layer) internetworking model for designing a reliable, scalable, and cost-efficient internetwork. A hierarchical network design breaks the complex network into 3 smaller and manageable layers. In addition, the ***three-tier hierarchical design*** maximizes performance, network availability, and the ability to scale the network design. The 3 layers are **Core**, **Distribution** and **Access**. An example of 3-layer design can be seen below. (Academy, 2014)



Major benefits of the hierarchical model is as follows:

1) **Modularity**- By breaking down the complex network into modules, the network becomes easier to manage and design.

2) **Resiliency**- We separate different functionalities by creating separate layers, which then helps the network to run efficiently in both normal and abnormal conditions. It ensures the ability of the network to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation. ("Resilience (network)", n.d.)

3) **Flexibility**- In any enterprise environment, there is always a possibility of expansion, and hence adding new devices or increasing the capacity of the network can easily be done without the need for any replacement of the hardware devices.

Access-Layer

This layer provides the host computers and the end users to connect to the network. In our network design, there are 5 layer-2 access switches. Each of these switches has a separate **VLAN** running on them. **Rapid Spanning Tree Protocol** is ran across all of the access switches. Since, the switch interfaces connecting to the end-devices has a very less chance of forming loops, spanning tree **portfast** is enabled on each of these interfaces. As all of the access switches handles separate VLANs, the end-device interfaces are made **access ports**. Acting as the front door to a network, the access layer employs **access lists** designed to prevent unauthorized users from gaining entry. An access-list is implemented to permit the users from Management VLAN to access other switches. **Port security** is enabled to prevent any unauthorized PC to interact with the network. The links between the Access switches and the Distribution switches are layer 2 and is configured to allow trunking. For additional security, the switches are configured to use encrypted passwords so that the privilege EXEC mode is only accessed by legitimate users. For allowing the management VLAN PCs to access the switches remotely, a username and password is put in place. Since, the access switches are all layer 2, a virtual interface for Management VLAN is setup along with a default-gateway so that these switches know where to forward the traffic. Lastly, the unused ports are shutdown for security purposes.

Distribution Layer

The distribution layer handles all of the routing as it runs layer 3 switches. It aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. This layer provides redundancy and load-balancing by defining multiple paths through which traffic can flow in congestion. Protects core from high density peering and problems in access layer. ("The Cisco three-layered hierarchical model", n.d.) On all of the interfaces linking to access-layer, trunking mode is set on. Virtual interfaces are setup for VLANs. Since, Spanning tree is ran across the distribution switches, for VLAN 10 and 20, Distribution Switch 1 is set as root and Switch 2 as secondary root in case the former fails. Similarily, for the remaining VLANs, Switch 2 is set as root and Switch 1 as secondary root when Switch 1 fails. HSRP is configured so that in case a switch fails, all of the routing traffic will be taken over by the other switch. Layer 3 Etherchannel is configured between the distribution switches. For the interfaces linking the distribution switches to the core layer are all Layer 3 and routing is enabled on them. Distribution layer also provides Quality of Service and policy-based routing. OSPF is ran across the distribution layer for routing decisions.

Core Layer

The core layer is known for its high availability and fast convergence. For keeping the core layer fast enough, security features such as access lists are not implemented as these tasks can be very CPU-intensive. ("The Cisco three-layered hierarchical model", n.d.) The core aggregates the traffic from all the distribution layer devices, so it must be capable of forwarding large amounts of data quickly. The core operates at layer 3 and is used for both fast switching and routing.

Technologies Used:

1) **Virtual LAN or VLAN**

VLANs are used in a network to create logical sub-networks. Creating VLANs is very crucial in an enterprise environment as it groups together hosts that either belong to the same department as these devices communicate with each other more often. VLANs are good for enhancing the security as it doesn't allow hosts from a different VLAN to unnecessarily interfere with other VLANs. If two devices from the same department has to communicate and they belong to different switches, they use **trunking.** Trunking can be configured between two switches by making the trunk ports between them. But, if different VLANs want to communicate with each other, Inter-VLAN routing is required which is done by routers or L3 Switches. In our network, we have 5 different VLANs- each for a host group.

VLAN 10 – Admin

VLAN 20- Sales and Marketing

VLAN 30- HR

VLAN 40- Finance

VLAN 99- Management

***Why are VLANs used and how does it helps our customers*?**

Since every customer belongs to one of the above VLANs, it helps in segmenting the traffic and prevents unnecessary interference from any other VLAN. Hosts from either group work under their own domain.

2) **Rapid Spanning Tree Protocol**

STP identifies loop-free paths and chooses the best of them. It is used in avoiding switching loops and broadcast storms which results from them. STP blocks ports which are unusable for now and unblocks them when required. STP determines a root bridge for every VLAN and it is decided via an election process. When a switch is first powered on, it believes it is the root bridge for every VLAN. Hence, the election is carried out to determine the true root bridge. It starts via the exchange of BPDU's between switches. Each switch has a Bridge ID or BID and it consists of a 2-byte priority and the MAC address of the switch. By default, all switches have a priority of 32768. So, the switch with the lowest MAC address is crowned as the root for that VLAN. There are a total of 5 stages a port on the switch can be in. After the election, every port on every switch is in either the forwarding mode or the blocking mode. Every port on the root bridge is in forwarding mode. Rapid STP is an advance version and it has been known to have the fastest convergence. Rapid STP has only 3 port stages.

***Why was Rapid STP chosen and how does it helps our customers*?**

Rapid STP has a very fast convergence rate than that of the traditional STP. For every VLAN there is a primary root and a secondary root in case the primary one fails. This ensures availability of the VLANs so that the hosts are up and running without any link failure. ("The Advantages of Spanning Tree Protocol | Techwalla.com", n.d.) Even if there is a link failure, Rapid STP has an error detection rate of 6 seconds and hence it shifts the load to the other switch immediately preventing any kind of disruption in service. We are using STP on both the access layer and the distribution layer.

For VLAN 10 and VLAN 20- **Distribution Switch1 is the primary and Switch2 the secondary**.

For VLAN 30, 40 and 99- **Distribution Switch2 is the primary and Switch1 the secondary**.

3) **Access-List or ACL**

Access-lists are a bunch of permissions attached to every port on the switch. It is one of the most important security feature in a network as it can be configured to allow/deny traffic from various sources. There are two types of ACLs- standard and extended. Standard ACLs only takes into account the source IP address when filtering traffic. Whereas, Extended ACLs provide with other filtering options such as the destination IP address or matching packets according to the protocol or the ports. Standard ACLs are applied as close to the destination as possible and extended ACLs as close as possible to the source of the traffic to be filtered. There is always an implicit deny at the out port of every ACL which is changed according to the requirements otherwise, all the traffic would be blocked. While defining ACLs, it should be specified to filter incoming traffic or outgoing traffic.

***Why are ACLs used and how does it helps our customers*?**

In our network, ACLs are applied at both the access layer and the distribution layer for filtering non-legitimate traffic. At the access-layer, it is configured to permit connections from the Management VLAN as well. On both the access and the distribution switches, deny traffic from any other network address other than the 10.7.0.0 network. This helps in not only securing our VLANs but also from various threats outside of the network. Since, it prevents rogue traffic, ACLs ensures availability all the time by providing secure access for our customers. Our customers don’t need to worry about the loss or exposure of the sensitive information.

4) **OSPF**

OSPF is a routing protocol that runs on the layer 3 switches in our network design i.e. on between distribution layer switches, between core layer switches and between core-distribution. OSPF determines the shortest path and calculates the entire route information along that path. OSPF L3 devices build their routing tables by exchanging Hello packets and LSAs. After the exchange, the devices run Dijkstra's algorithm, determine the shortest path and add the best path into the routing table. ("Open Shortest Path First", n.d.)

For our network, we use a single area (area 0) OSPF consisting of the two Distribution L3 switches and the two Core L3 switches. We use loopback address to choose a DR and a BDR. In our network, we use the core switches as the DR and the BDR.

***Why is OSPF used and how does it helps our customers*?**

It improves scalability as it is designed to work with larger networks. OSPF uses small hello packets to verify link operation without transferring large tables. OSPF can route packets by different criterion based on their type of service field. Routes can be tagged with arbitrary values, easing interoperation. The main advantage of link state routing (OSPF) is that complete knowledge of topology allows routers to calculate routes that satisfy the incoming request hence satisfying the customer requests with ease. OSPF is useful for traffic engineering purposes where routes can be manipulated to meet different service requirements. ("The Pros and Cons of OSPF and EIGRP", 2009)

Other Option – EIGRP

EIGRP allows you to summarize at any interface and it reduces the amount of update traffic, it reduces the length of routing tables, and sets boundaries for queries. EIGRP is known for its fast convergence and has more versatility and adaptability than its OSPF rival. But, in contrast to EIGRP which is a CISCO-proprietary, OSPF will run on any device as it's based on open standard. ("The Pros and Cons of OSPF and EIGRP", 2009)

5) **HSRP**

Hot standby routing protocol enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. When HSRP is configured on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers. HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. One of the routers is selected to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address should the designated active router fail. (Support, Products, Switches & Guides, n.d.)

***Why is HSRP used and how does it helps our customers*?**

HSRP improves network availability by creating the illusion of a virtual router and thus having a active router and a standby router as backup. If one of the router fails, all of the load falls over to the backup router.

HSRP is easy to configure, and the protocol does not affect the routing tables or hosts configuration.

Other Options

Virtual Router Redundancy Protocol (VRRP)

An open-standard IEEE alternative to Cisco's HSRP, providing the same functionality. It has the concept of Master which is the virtual router and backup (all non-master routers). It is known to provide a very simple network management, high adaptability and low network overhead. One of its weakness is that it uses no security because the offered method of authentication is very weak. ("First Hop Redundancy protocol comparison (HSRP,VRRP,GLBP) with the diagram", n.d.)

Gateway Load Balancing Protocol (GLBP)

GLBP is another one of Cisco proprietary First hop redundancy protocol. It is the only protocol which actually provides load-balancing as compared to HSRP or VRRP. It also has the same idea of an active virtual gateway and the standby backup routers. It offers higher availability by eliminating single-point of failure same as HSRP or VRRP. Most important aspect of GLBP is its automatic load balancing. Since all hosts on a subnet can use a common default gateway while load balancing is still achieved, administration of multiple groups and gateways is unnecessary, hence the lower administration cost. Major concession point is that it is not open-source and it results in higher complexity on network management as a result of high number of configurable parameters to take into consideration. ("First Hop Redundancy protocol comparison (HSRP,VRRP,GLBP) with the diagram", n.d.)

6) **Etherchannels**

Etherchannel is the logical bundling of physical connections. It is used to gather more bandwidth and etherchannel provides automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, Etherchannel redirects traffic from the failed link to the remaining links in the channel without intervention and when the link comes backup, the links bandwidth is automatically added to the group. Etherchannel can be deployed at both layer 2 and layer 3 but it is important to remember that ports placed inside of an etherchannel should be running at same speed and have same duplex settings. There are two Etherchannel negotiation protocols- LACP (industry-standard) and PAGP (Cisco). There are different modes depending on the protocol used such as “active” and “passive” for LACP which is identical to “desirable” and “auto” in PAGP. For our network, we are using the mode “on” which means a group can be formed when both end switches of the etherchannel are operating on the “on” mode.

***Why is Etherchannel used and how does it helps our customers*?**

Etherchannel as we know groups several FastEthernet ports and use them as a single logical channel. Since, etherchannel allows up to 8 ports in one channel, it not only increases the bandwidth but also provides great redundancy. Even though STP generally blocks all the unused ports but when there is one etherchannel link, STP recognizes it as a single active link and hence, none of the ports in the etherchannel are blocked.

IP Address Allocation

	SUBNET	**MASK**	**Network Address**	**Broadcast Address**	**First Useable Address**	**Last Useable Address**	**Number of Hosts/subnet**
VLAN 10-**Admin**	10.7.10.0	24	10.7.10.0	10.7.10.255	10.7.10.1	10.7.10.254	254
VLAN 20-**Sales and Marketing**	10.7.20.0	24	10.7.20.0	10.7.20.255	10.7.20.1	10.7.20.254	254
VLAN 30-**HR**	10.7.30.0	24	10.7.30.0	10.7.30.255	10.7.30.1	10.7.30.254	254
VLAN 40-**Finance**	10.7.40.0	24	10.7.40.0	10.7.40.255	10.7.40.1	10.7.40.254	254
VLAN 99-**Management**	10.7.99.0	24	10.7.99.0	10.7.99.255	10.7.99.1	10.7.99.254	254
P2P	10.7.100.0	30	10.7.100.0	10.7.100.3	10.7.100.1	10.7.100.2	2
P2P	10.7.100.4	30	10.7.100.4	10.7.100.7	10.7.100.5	10.7.100.6	2
P2P	10.7.100.8	30	10.7.100.8	10.7.100.11	10.7.100.9	10.7.100.10	2
P2P	10.7.100.12	30	10.7.100.12	10.7.100.15	10.7.100.13	10.7.100.14	2
P2P	10.7.100.16	30	10.7.100.16	10.7.100.19	10.7.100.17	10.7.100.18	2
P2P	10.7.100.20	30	10.7.100.20	10.7.100.23	10.7.100.21	10.7.100.22	2
P2P	10.7.100.24	30	10.7.100.24	10.7.100.27	10.7.100.25	10.7.100.26	2
P2P	10.7.100.28	30	10.7.100.28	10.7.100.31	10.7.100.29	10.7.100.30	2
P2P	10.7.100.32	30	10.7.100.32	10.7.100.35	10.7.100.33	10.7.100.34	2

Customer Questions:

Q1: The customer has requested that subnet allocations are easy to summarise, understand and support. You must describe why this is true for your design

There are 14 subnets in total. There are 5 VLANs – 10 for Admin, 20 for Sales and Marketing, 30 for HR, 40 for Finance and 99 for Management. A subnet mask of /24 is used so that there are enough addresses for each group and also for future growth. There are 9 point to point links of which 2 are reserved for WAN.

For the ease of customers, VLSM is not done on the address block 10.7.0.0/16 and all of the VLANs are given a mask of 24 giving a total of 256 addresses per group. There are extra addresses for each group which could be found useful in future if the number of employees increases.

Q2: The design should indicate cabling layout (physical topology diagram) and specifications as appropriate (copper, fibre etc) and why.

For most of the cabling layout, Unshielded Twisted Pair Category 5 copper cables are used which run at 100Mbps also known as 100BASE-TX or Fast Ethernet. These type of cables are very cheap as compared to others and they run in both directions (full-duplex). FastEthernet is sufficient for high-bandwidth-consuming clients or servers. We are running FastEthernet from the access layer to the core layer and its maximum segment length is 100m. The reason for Fast Ethernet running at each layer is because it is sufficient since our enterprise network is not very big right now. But, in the future, Gigabit Ethernet could be used between the core switches for maximum speed and also between the distribution switches. RJ-45 connector is deployed in the current infrastructure. The RJ-45 plug is a male component, crimped at the end of the cable.

There are 2 types of cabling wiring- straight through and cross-over. Both are used are being used for different purposes. The links between access layer switches and the host PCs are all straight through cabling and all other links (switch-switch) are cross-over cables. McQuerry, 2004)

Q3: The Company's existing LAN deployments utilize L2 VLANS and STP from the distribution layer to the access layer, however the company will consider layer 3 to the access layer if a compelling argument can be made that considers both pros and cons.

Using layer 3 at the access layer could help in many ways. For example, if all the access layer switches are running layer 3 then there isn't going to be any switching loops and hence there will be no blocked links. Also, by moving to a Routed Access layer, we can have faster convergence, faster failover, improved stability, as well as increased security as there will be no need of implementing root guard, loop guard etc. There is no need for VLAN trunking configuration or HSRP tuning to load-balance uplinks. L3 devices restrict broadcast traffic such as ARP and DHCP broadcasts to the local network. This reduces overall traffic levels by allowing administrators to divide networks into smaller parts and restrict broadcasts to only that sub-network. ("Routed or Switched Access Layer: Why not Both? - PacketLife.net", n.d.)

But running layer 3 at access layer could have some problems as well. Layer 3 does improves performance and failover but it makes things difficult in terms of flexibility and simplicity. This is because routing at access layer requires more expensive multi-layer switches. For small enterprises and startups, L2 switching is far better as it is easy to deploy and inexpensive to use.

Q4: The customer requests you give consideration for ACTIVE, ACTIVE gateways. Can it be done? Is it recommended?

ACTIVE –ACTIVE gateway is run by GLBP as opposed to other First Hop Redundancy Protocols like HSRP and VRPP. GLBP follows the same concept of active and standby routers but unlike HSRP or VRPP, it load balances between different routers and they do not sit idle wasting bandwidth. GLBP can be used to utilize all of the available bandwidth through different routers as every router is involved in forwarding of packets. GLBP is better than HSRP or VRPP in respect to performance and utilization of bandwidth. But GLBP is a Cisco proprietary protocol so it can't be run in devices other than cisco and it results in higher complexity on network management as a result of high number of configurable parameters to take into consideration. GLBP can be deployed instead of HSRP but for our simple enterprise-LAN, GLBP could make things really complicated.

Q5: The customer would like you to advise if DHCP be located centrally or locally? Why or why not?

DHCP servers should be deployed locally and not centrally. Firstly, DHCP can be configured on switches and if one of the switches fail, the hosts could acquire the dynamically generated IP addresses from other switches running DHCP. Secondly, if there is a failure in the central data location, hosts would not be able to get an IP address and there is no redundancy in the central data center. Also, there could be security considerations in putting the DHCP server outside the network in a data center as a firewall might be required to protect it outside the network.

Security Considerations

The security considerations are as follows:

1) Only the Management VLAN (99) can access all the switches.

2) All the switches has been setup with passwords restricting the privilege access.

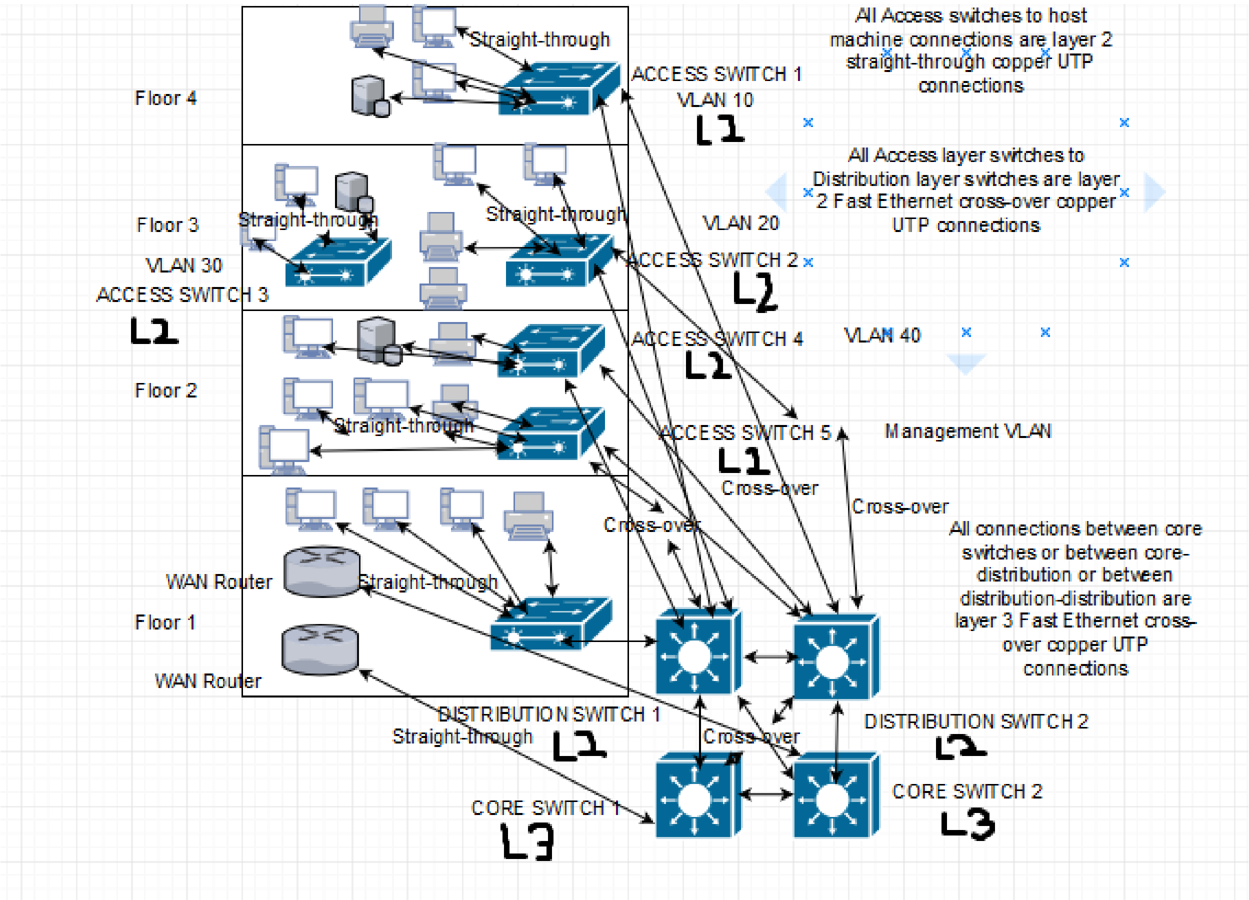
3) All the links which are not being used by the distribution switches are put into Root Guard so that a rogue switch doesn't become the root.

4) In all the layer 2 switches, port-security is setup to allow some maximum mac addresses and also turning on the sticky option

5) OSPF MD5 authentication is enabled in the Layer3 Switches.

6) Unused ports are being administratively shutdown so that no one from outside the network could connect to it.

PHYSICAL TOPOLOGY



Physical Topology Diagram

The Physical Topology spans over 4 floors having VLANs distributed across the floors. Floor 4 has the Admin VLAN 10 hosts. Similarly, VLAN 20 and 30 on Floor 3, VLAN 40 and 99 on Floor 2. Each floor has hosts which are either PCs, printers or servers. Each floor has access switches on them. The ground floor has the layer 3 Distribution switches and layer 3 Core switches. The core switches connects to the WAN routers on the ground floor. All the connection links are 100Mbps Fast Ethernet UTP copper cables. RJ45 connectors are used as well.

Floor 1- Core Switch1 and Core Switch2, Distribution Switch1 and Distribution Switch2

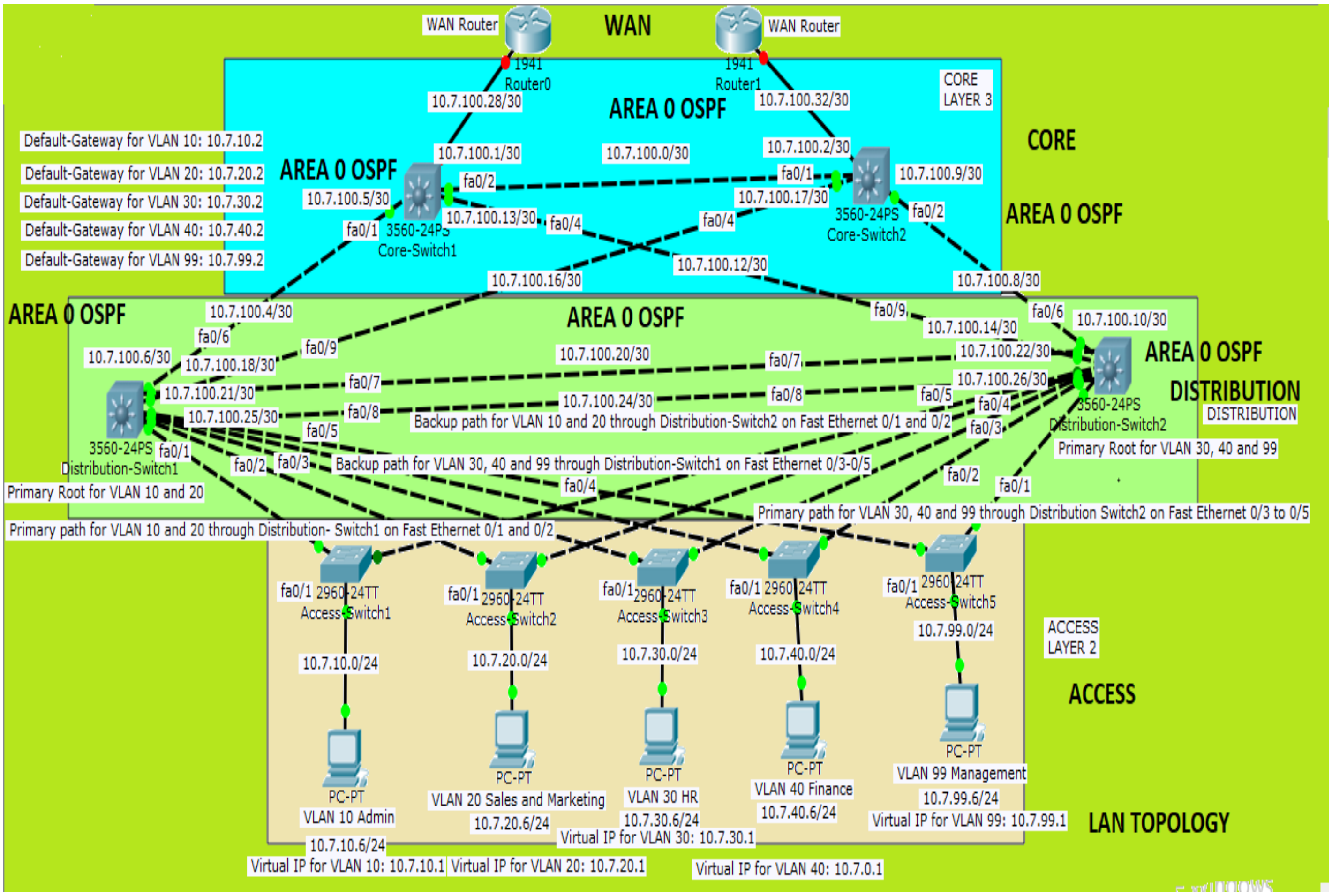
WAN Routers

Floor 2- Access Switch4 and Access Switch5

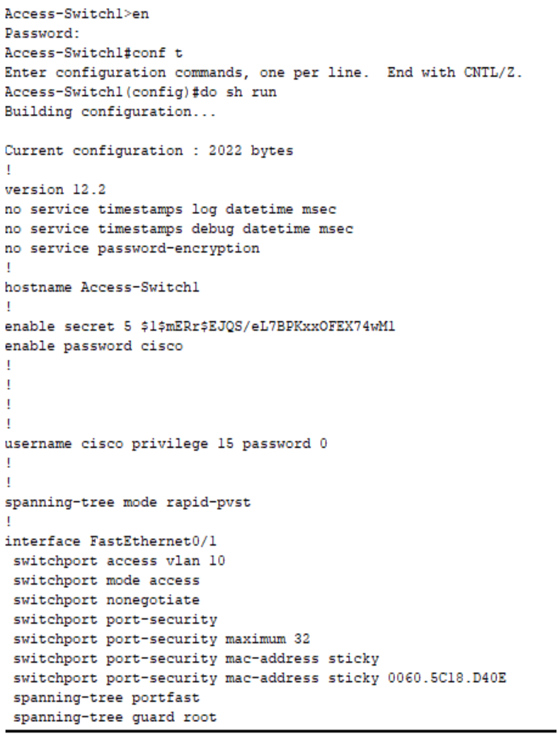
Floor 3- Access Switch2 and Access Switch3

Floor 4- Access Switch1

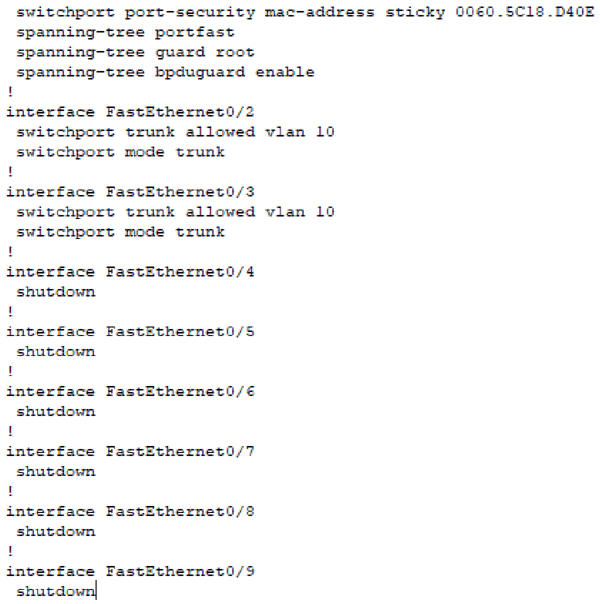
Logical Topology



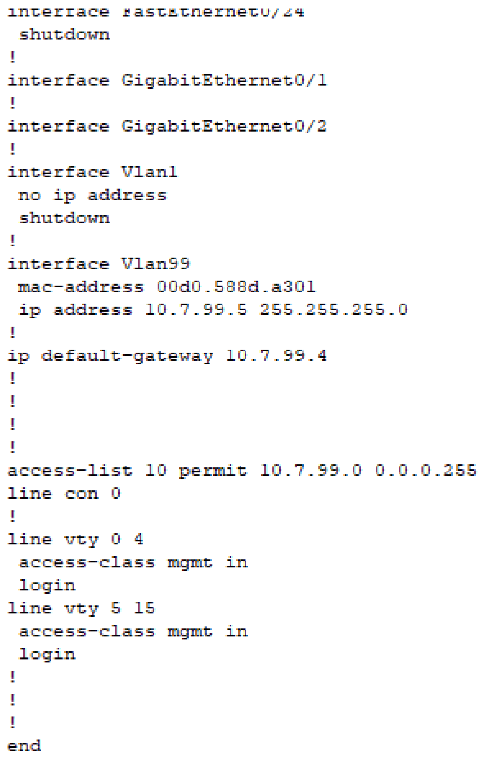
Working Configurations (Toasty Answers, 2015)



```
Access-Switch1>en
Password:
Access-Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Access-Switch1(config)#do sh run
Building configuration...

Current configuration : 2022 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Access-Switch1
!
enable secret 5 $1$mERr$EJQS/eL7BPKxxOFEX74wM1
enable password cisco
!
!
!
!
username cisco privilege 15 password 0
!
!
spanning-tree mode rapid-pvst
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 32
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0060.5C18.D40E
 spanning-tree portfast
 spanning-tree guard root
```



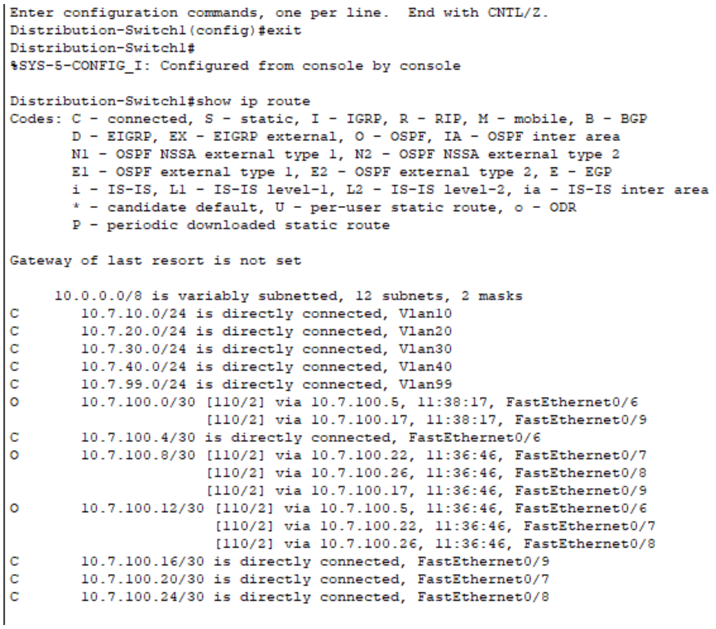
```
 switchport port-security mac-address sticky 0060.5C18.D40E
 spanning-tree portfast
 spanning-tree guard root
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport trunk allowed vlan 10
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk allowed vlan 10
 switchport mode trunk
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 shutdown
!
interface FastEthernet0/9
 shutdown
```



```
interface FastEthernet0/24
 shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 mac-address 00d0.588d.a301
 ip address 10.7.99.5 255.255.255.0
!
ip default-gateway 10.7.99.4
!
!
!
!
access-list 10 permit 10.7.99.0 0.0.0.255
line con 0
!
line vty 0 4
 access-class mgmt in
 login
line vty 5 15
 access-class mgmt in
 login
!
!
!
end
```

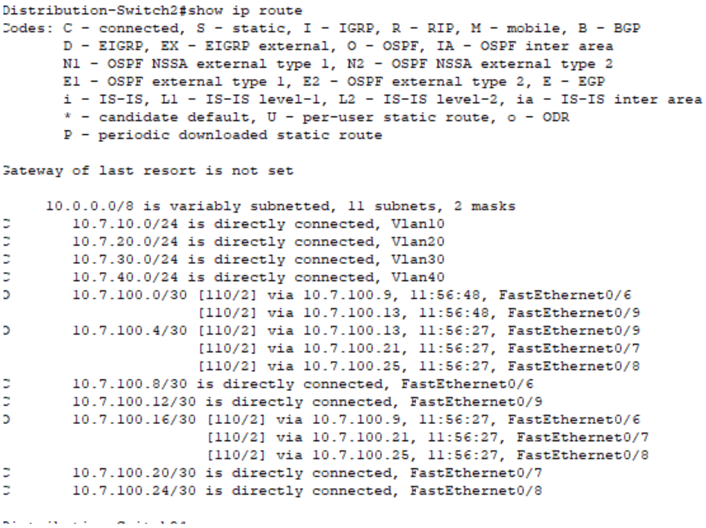
Access-Switch1 Config

All other Access Switches has the same configuration.



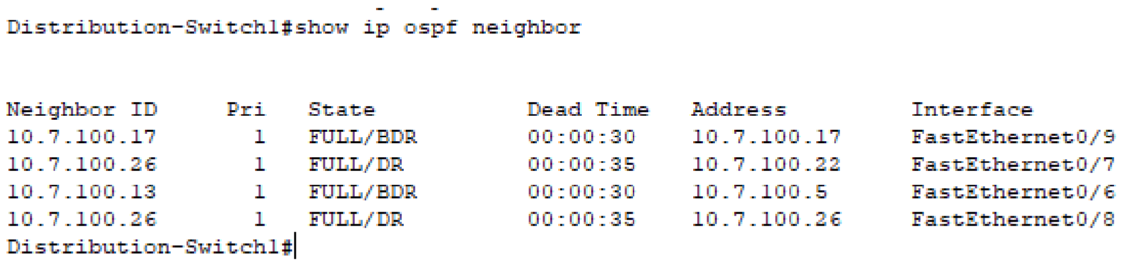
```
Enter configuration commands, one per line.  End with CNTL/Z.
Distribution-Switch1(config)#exit
Distribution-Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Distribution-Switch1#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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 not set

     10.0.0.0/8 is variably subnetted, 12 subnets, 2 masks
C       10.7.10.0/24 is directly connected, Vlan10
C       10.7.20.0/24 is directly connected, Vlan20
C       10.7.30.0/24 is directly connected, Vlan30
C       10.7.40.0/24 is directly connected, Vlan40
C       10.7.99.0/24 is directly connected, Vlan99
O       10.7.100.0/30 [110/2] via 10.7.100.5, 11:38:17, FastEthernet0/6
                      [110/2] via 10.7.100.17, 11:38:17, FastEthernet0/9
C       10.7.100.4/30 is directly connected, FastEthernet0/6
O       10.7.100.8/30 [110/2] via 10.7.100.22, 11:36:46, FastEthernet0/7
                      [110/2] via 10.7.100.26, 11:36:46, FastEthernet0/8
                      [110/2] via 10.7.100.17, 11:36:46, FastEthernet0/9
O       10.7.100.12/30 [110/2] via 10.7.100.5, 11:36:46, FastEthernet0/6
                       [110/2] via 10.7.100.22, 11:36:46, FastEthernet0/7
                       [110/2] via 10.7.100.26, 11:36:46, FastEthernet0/8
C       10.7.100.16/30 is directly connected, FastEthernet0/9
C       10.7.100.20/30 is directly connected, FastEthernet0/7
C       10.7.100.24/30 is directly connected, FastEthernet0/8
```

Show ip route on Distribution-Switch1



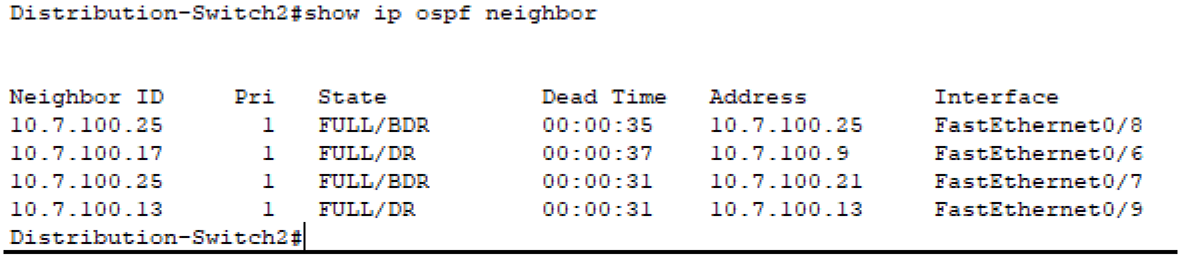
```
Distribution-Switch2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, 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 not set

     10.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
C       10.7.10.0/24 is directly connected, Vlan10
C       10.7.20.0/24 is directly connected, Vlan20
C       10.7.30.0/24 is directly connected, Vlan30
C       10.7.40.0/24 is directly connected, Vlan40
O       10.7.100.0/30 [110/2] via 10.7.100.9, 11:56:48, FastEthernet0/6
                      [110/2] via 10.7.100.13, 11:56:48, FastEthernet0/9
O       10.7.100.4/30 [110/2] via 10.7.100.13, 11:56:27, FastEthernet0/9
                      [110/2] via 10.7.100.21, 11:56:27, FastEthernet0/7
                      [110/2] via 10.7.100.25, 11:56:27, FastEthernet0/8
C       10.7.100.8/30 is directly connected, FastEthernet0/6
C       10.7.100.12/30 is directly connected, FastEthernet0/9
O       10.7.100.16/30 [110/2] via 10.7.100.9, 11:56:27, FastEthernet0/6
                       [110/2] via 10.7.100.21, 11:56:27, FastEthernet0/7
                       [110/2] via 10.7.100.25, 11:56:27, FastEthernet0/8
C       10.7.100.20/30 is directly connected, FastEthernet0/7
C       10.7.100.24/30 is directly connected, FastEthernet0/8
```

Show ip route on Distribution-Switch2



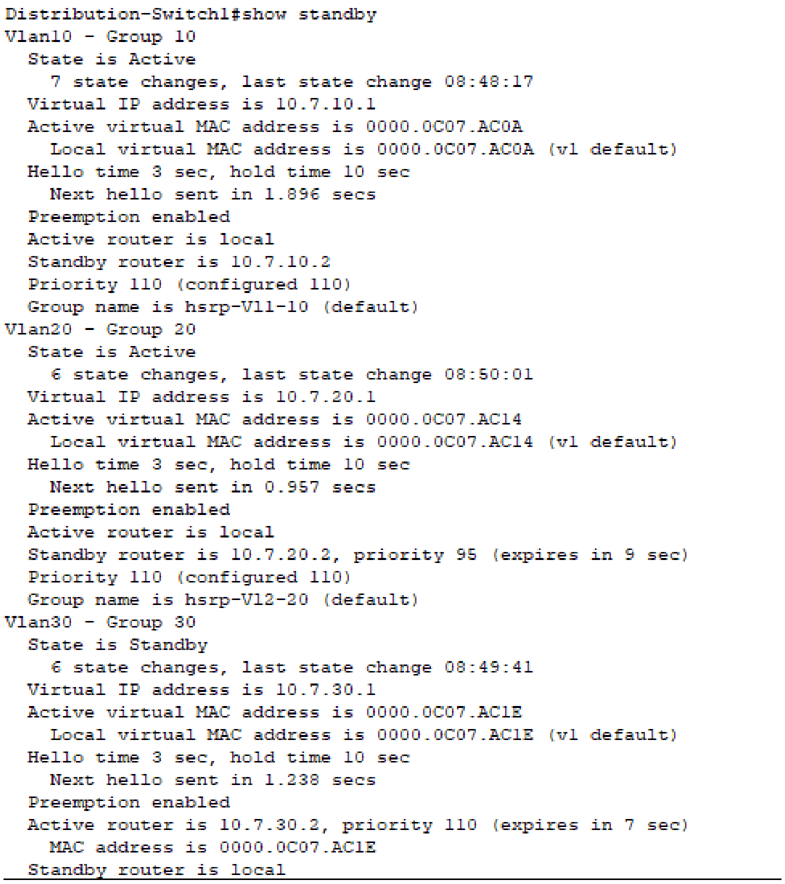
```
Distribution-Switch1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
10.7.100.17       1   FULL/BDR        00:00:30    10.7.100.17     FastEthernet0/9
10.7.100.26       1   FULL/DR         00:00:35    10.7.100.22     FastEthernet0/7
10.7.100.13       1   FULL/BDR        00:00:30    10.7.100.5      FastEthernet0/6
10.7.100.26       1   FULL/DR         00:00:35    10.7.100.26     FastEthernet0/8
Distribution-Switch1#
```

Show ip ospf neighbor on Distribution-Switch1



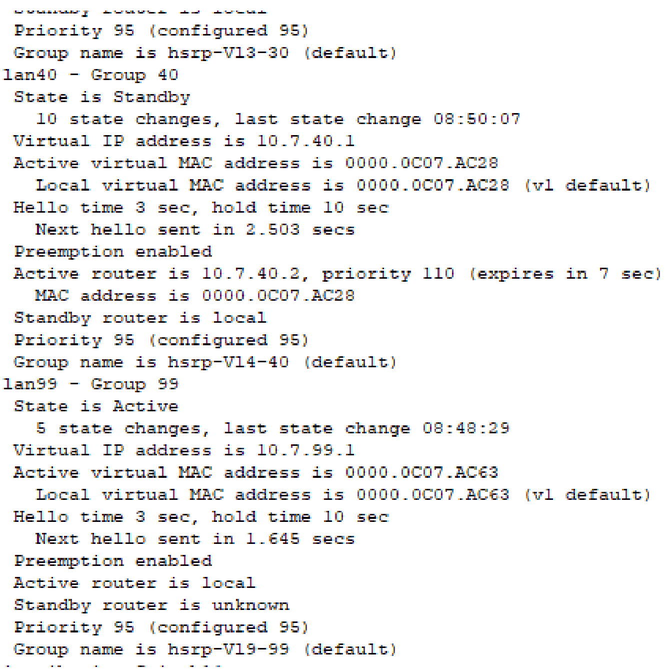
```
Distribution-Switch2#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
10.7.100.25       1   FULL/BDR        00:00:35    10.7.100.25     FastEthernet0/8
10.7.100.17       1   FULL/DR         00:00:37    10.7.100.9      FastEthernet0/6
10.7.100.25       1   FULL/BDR        00:00:31    10.7.100.21     FastEthernet0/7
10.7.100.13       1   FULL/DR         00:00:31    10.7.100.13     FastEthernet0/9
Distribution-Switch2#
```

Show ip ospf neighbor on Distribution-Switch2



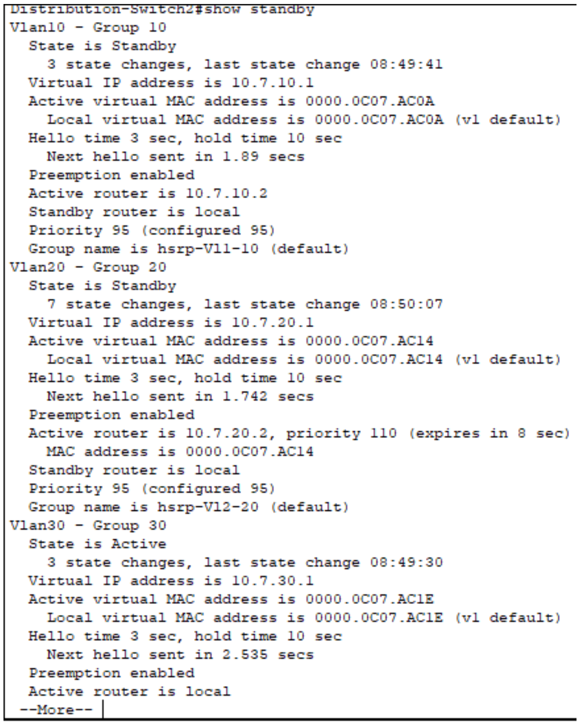
```
Distribution-Switch1#show standby
Vlan10 - Group 10
  State is Active
    7 state changes, last state change 08:48:17
  Virtual IP address is 10.7.10.1
  Active virtual MAC address is 0000.0C07.AC0A
    Local virtual MAC address is 0000.0C07.AC0A (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.896 secs
  Preemption enabled
  Active router is local
  Standby router is 10.7.10.2
  Priority 110 (configured 110)
  Group name is hsrp-Vl1-10 (default)
Vlan20 - Group 20
  State is Active
    6 state changes, last state change 08:50:01
  Virtual IP address is 10.7.20.1
  Active virtual MAC address is 0000.0C07.AC14
    Local virtual MAC address is 0000.0C07.AC14 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.957 secs
  Preemption enabled
  Active router is local
  Standby router is 10.7.20.2, priority 95 (expires in 9 sec)
  Priority 110 (configured 110)
  Group name is hsrp-Vl2-20 (default)
Vlan30 - Group 30
  State is Standby
    6 state changes, last state change 08:49:41
  Virtual IP address is 10.7.30.1
  Active virtual MAC address is 0000.0C07.AC1E
    Local virtual MAC address is 0000.0C07.AC1E (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.238 secs
  Preemption enabled
  Active router is 10.7.30.2, priority 110 (expires in 7 sec)
    MAC address is 0000.0C07.AC1E
  Standby router is local
```

Show standby on Distribution-Switch1_part1



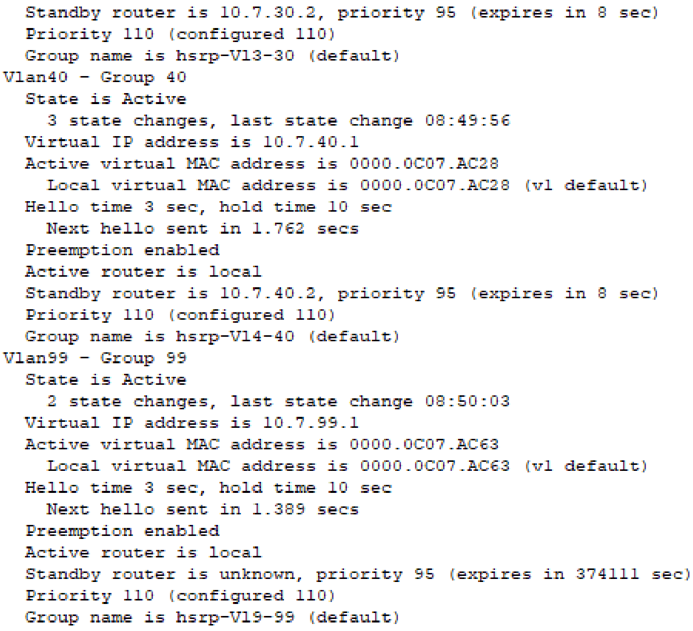
```
 Standby router is local
 Priority 95 (configured 95)
 Group name is hsrp-Vl3-30 (default)
lan40 - Group 40
 State is Standby
   10 state changes, last state change 08:50:07
 Virtual IP address is 10.7.40.1
 Active virtual MAC address is 0000.0C07.AC28
   Local virtual MAC address is 0000.0C07.AC28 (v1 default)
 Hello time 3 sec, hold time 10 sec
   Next hello sent in 2.503 secs
 Preemption enabled
 Active router is 10.7.40.2, priority 110 (expires in 7 sec)
   MAC address is 0000.0C07.AC28
 Standby router is local
 Priority 95 (configured 95)
 Group name is hsrp-Vl4-40 (default)
lan99 - Group 99
 State is Active
   5 state changes, last state change 08:48:29
 Virtual IP address is 10.7.99.1
 Active virtual MAC address is 0000.0C07.AC63
   Local virtual MAC address is 0000.0C07.AC63 (v1 default)
 Hello time 3 sec, hold time 10 sec
   Next hello sent in 1.645 secs
 Preemption enabled
 Active router is local
 Standby router is unknown
 Priority 95 (configured 95)
 Group name is hsrp-Vl9-99 (default)
```

Show standby on Distribution-Switch1_part2



```
Distribution-Switch2#show standby
Vlan10 - Group 10
  State is Standby
    3 state changes, last state change 08:49:41
  Virtual IP address is 10.7.10.1
  Active virtual MAC address is 0000.0C07.AC0A
    Local virtual MAC address is 0000.0C07.AC0A (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.89 secs
  Preemption enabled
  Active router is 10.7.10.2
  Standby router is local
  Priority 95 (configured 95)
  Group name is hsrp-Vl1-10 (default)
Vlan20 - Group 20
  State is Standby
    7 state changes, last state change 08:50:07
  Virtual IP address is 10.7.20.1
  Active virtual MAC address is 0000.0C07.AC14
    Local virtual MAC address is 0000.0C07.AC14 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.742 secs
  Preemption enabled
  Active router is 10.7.20.2, priority 110 (expires in 8 sec)
    MAC address is 0000.0C07.AC14
  Standby router is local
  Priority 95 (configured 95)
  Group name is hsrp-Vl2-20 (default)
Vlan30 - Group 30
  State is Active
    3 state changes, last state change 08:49:30
  Virtual IP address is 10.7.30.1
  Active virtual MAC address is 0000.0C07.AC1E
    Local virtual MAC address is 0000.0C07.AC1E (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.535 secs
  Preemption enabled
  Active router is local
 --More--
```

Show standby on Distribution-Switch2_part1



```
  Standby router is 10.7.30.2, priority 95 (expires in 8 sec)
  Priority 110 (configured 110)
  Group name is hsrp-Vl3-30 (default)
Vlan40 - Group 40
  State is Active
    3 state changes, last state change 08:49:56
  Virtual IP address is 10.7.40.1
  Active virtual MAC address is 0000.0C07.AC28
    Local virtual MAC address is 0000.0C07.AC28 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.762 secs
  Preemption enabled
  Active router is local
  Standby router is 10.7.40.2, priority 95 (expires in 8 sec)
  Priority 110 (configured 110)
  Group name is hsrp-Vl4-40 (default)
Vlan99 - Group 99
  State is Active
    2 state changes, last state change 08:50:03
  Virtual IP address is 10.7.99.1
  Active virtual MAC address is 0000.0C07.AC63
    Local virtual MAC address is 0000.0C07.AC63 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.389 secs
  Preemption enabled
  Active router is local
  Standby router is unknown, priority 95 (expires in 374111 sec)
  Priority 110 (configured 110)
  Group name is hsrp-Vl9-99 (default)
```

Show standby on Distribution-Switch2_part2

L3 Etherchannel configuration between Distribution-Switch1 and Distribution-Switch2

Distribution-Switch1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Distribution-Switch1(config)# int range f0/7-8

Distribution-Switch1(config-if-range)# channel-group 2 mode on

Distribution-Switch1(config-if-range)# no shut

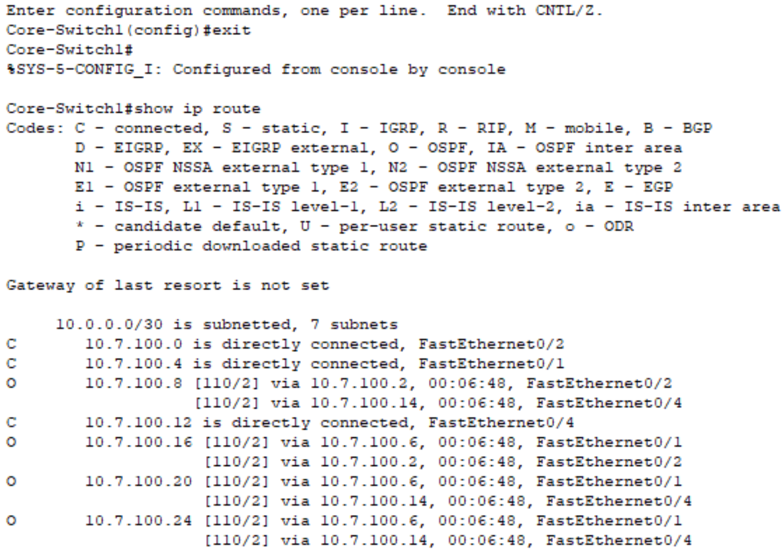
Distribution-Switch2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Distribution-Switch2(config)# int range f0/7-8

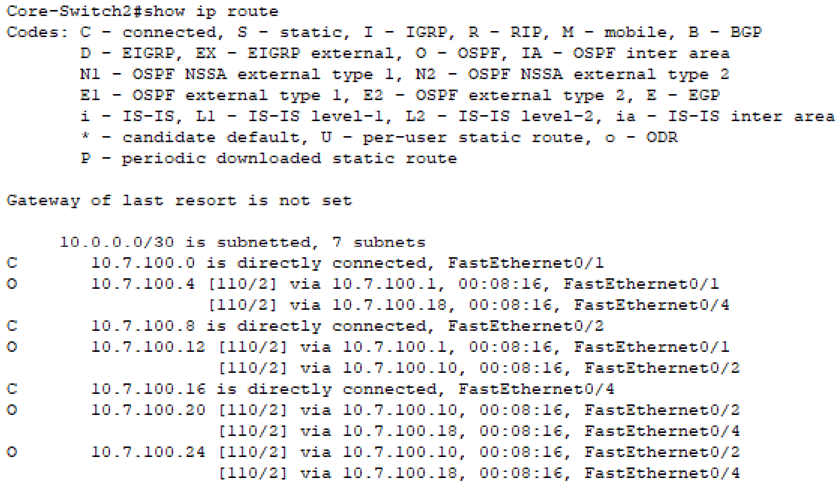
Distribution-Switch2(config-if-range)# channel-group 2 mode on

Distribution-Switch2(config-if-range)# no shut



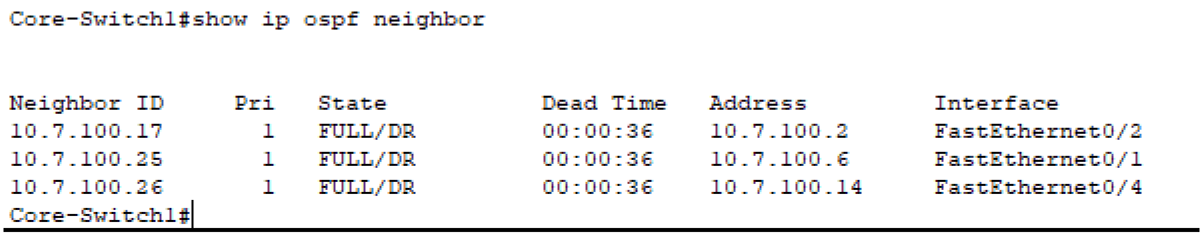
```
Enter configuration commands, one per line.  End with CNTL/Z.
Core-Switch1(config)#exit
Core-Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Core-Switch1#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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 not set

     10.0.0.0/30 is subnetted, 7 subnets
C       10.7.100.0 is directly connected, FastEthernet0/2
C       10.7.100.4 is directly connected, FastEthernet0/1
O       10.7.100.8 [110/2] via 10.7.100.2, 00:06:48, FastEthernet0/2
                   [110/2] via 10.7.100.14, 00:06:48, FastEthernet0/4
C       10.7.100.12 is directly connected, FastEthernet0/4
O       10.7.100.16 [110/2] via 10.7.100.6, 00:06:48, FastEthernet0/1
                    [110/2] via 10.7.100.2, 00:06:48, FastEthernet0/2
O       10.7.100.20 [110/2] via 10.7.100.6, 00:06:48, FastEthernet0/1
                    [110/2] via 10.7.100.14, 00:06:48, FastEthernet0/4
O       10.7.100.24 [110/2] via 10.7.100.6, 00:06:48, FastEthernet0/1
                    [110/2] via 10.7.100.14, 00:06:48, FastEthernet0/4
```

Show ip route on Core-Switch1



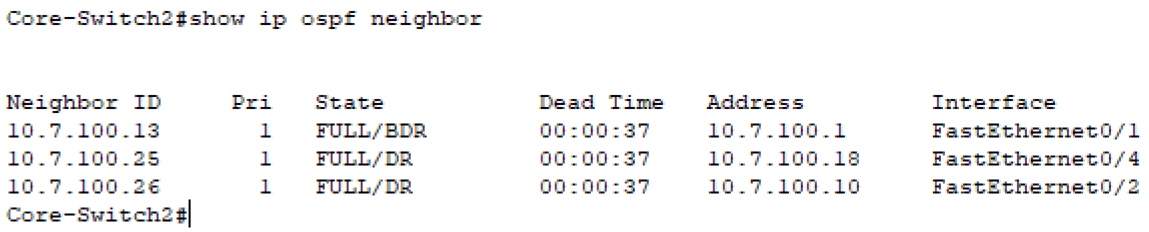
```
Core-Switch2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, 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 not set

     10.0.0.0/30 is subnetted, 7 subnets
C       10.7.100.0 is directly connected, FastEthernet0/1
O       10.7.100.4 [110/2] via 10.7.100.1, 00:08:16, FastEthernet0/1
                   [110/2] via 10.7.100.18, 00:08:16, FastEthernet0/4
C       10.7.100.8 is directly connected, FastEthernet0/2
O       10.7.100.12 [110/2] via 10.7.100.1, 00:08:16, FastEthernet0/1
                    [110/2] via 10.7.100.10, 00:08:16, FastEthernet0/2
C       10.7.100.16 is directly connected, FastEthernet0/4
O       10.7.100.20 [110/2] via 10.7.100.10, 00:08:16, FastEthernet0/2
                    [110/2] via 10.7.100.18, 00:08:16, FastEthernet0/4
O       10.7.100.24 [110/2] via 10.7.100.10, 00:08:16, FastEthernet0/2
                    [110/2] via 10.7.100.18, 00:08:16, FastEthernet0/4
```

Show ip route on Core-Switch2



```
Core-Switch1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
10.7.100.17       1   FULL/DR         00:00:36    10.7.100.2      FastEthernet0/2
10.7.100.25       1   FULL/DR         00:00:36    10.7.100.6      FastEthernet0/1
10.7.100.26       1   FULL/DR         00:00:36    10.7.100.14     FastEthernet0/4
Core-Switch1#
```

Show ip ospf neighbor on Core-Switch1



```
Core-Switch2#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
10.7.100.13       1   FULL/BDR        00:00:37    10.7.100.1      FastEthernet0/1
10.7.100.25       1   FULL/DR         00:00:37    10.7.100.18     FastEthernet0/4
10.7.100.26       1   FULL/DR         00:00:37    10.7.100.10     FastEthernet0/2
Core-Switch2#
```

Show ip ospf neighbor on Core-Switch2

Time Sheet

Activity	Date	Time Spent	Description
Understanding the hierarchical model	**26/4/2018**	**60-80 minutes**	**Cisco Best Practices for LAN design, advantages, collapsed two-tier design**
STP, Etherchannel Revision	**28/4/2018**	**120 minutes**	**I forgot most of the stuff so I went through the slides.**
Created subnets	**30/4/2018**	**20 minutes**	**VLSM to create subnets for different VLANs and point to point links.**
Physical media and layout research	**30/4/2018**	**30 minutes**	**A quick overview of all the cables, layout etc.**
Searching for physical topology examples online	**30/4/2018**	**60 minutes**	**I found nothing significant relating to the physical topology.**
Change subnets so that it is easier for customers to understand.	**1/4/2018**	**10 minutes**	**After talking to my teacher, it seemed as if VLSM is not a great idea and then I changed it to a**

			simple subnet scheme.
HSRP vs GLBP	1/5/2018	20 minutes	Decided to work on HSRP since GLBP doesn’t work on Packet Tracer
Physical Topology	2/5/2018	120 minutes	Very difficult to find a good drawing software online
Customer Questions	2/5/2018	150 minutes	Browsed the internet for some of the customer questions and noted it down separately
Explained the chosen technologies	3/5/2018	90 minutes	It took a lot of time to explain and also provide alternatives for the technologies.
Configuration in Packet Tracer	3/5/2018	150 minutes	It took me a long time to get everything working except for ospf and the etherchannel.
Troubleshooting ospf	3/5/2018	40-60 minutes	Turns out that I did many mistakes in assigning the point to point links.
Corrected the point to point links	3/5/2018	60 minutes	Point to point links corrected and added to the configuration in Packet Tracer but the link between the distribution switches is still down.
Disable port channel between the distribution switches link	3/5/2018	30 minutes	I made a channel-group between the distribution switches and it caused the line protocol to go up but the interface went down. OSPF between the links not working so I

			disabled the port channel.
Added ospf again	4/5/2018	30 minutes	Even after no port-channel, the links were still down so I configured the IP addresses again and entered ospf commands again.
Adding everything in the word document	4/5/2018	220-240 minutes	Configurations are working fine. It took a long time to add everything to the project report, changing the p2p links in physical diagram, adding screenshots of config, answering customer questions etc.
Time sheeting	4/5/2018	40 minutes	The time sheeting task only took about 40 minutes
Referencing	4/5/2018	60 minutes	No Comments

References

Toasty Answers. (2015). *#12 Distribution Layer Configuration* [Video]. Retrieved from https://www.youtube.com/watch?v=cRcgYLeC2sY&t=776s

Academy, C. (2014). Hierarchical Network Design Overview (1.1) > Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design. Retrieved from http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

Resilience (network). Retrieved from https://en.wikipedia.org/wiki/Resilience_(network)

The Cisco three-layered hierarchical model. Retrieved from https://searchnetworking.techtarget.com/tutorial/The-Cisco-three-layered-hierarchical-model

The Advantages of Spanning Tree Protocol | Techwalla.com. Retrieved from https://www.techwalla.com/articles/the-advantages-of-spanning-tree-protocol

Open Shortest Path First. Retrieved from https://en.wikipedia.org/wiki/Open_Shortest_Path_First

The Pros and Cons of OSPF and EIGRP. (2009). Retrieved from https://gotechsf.wordpress.com/2009/09/05/the-pros-and-cons-of-ospf-and-eigrp/

Support, P., Products, E., Switches, C., & Guides, C. Catalyst 3560 Software Configuration Guide, Release 12.2(52)SE - Configuring HSRP [Cisco Catalyst 3560 Series Switches]. Retrieved from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swhsrp.html

First Hop Redundancy protocol comparison (HSRP,VRRP,GLBP) with the diagram. Retrieved from http://cisconetworkingcenter.blogspot.co.nz/2013/01/first-hop-redundancy-protocol.html

McQuerry, S. (2004). Choosing LAN Cabling Options > CCNA Self-Study: Network Media (The Physical Layer). Retrieved from http://www.ciscopress.com/articles/article.asp?p=169686&seqNum=3

Routed or Switched Access Layer: Why not Both? - PacketLife.net. Retrieved from http://packetlife.net/blog/2010/sep/24/routed-or-switched-access-layer-why-not-both/