Autonomous Network System Design Project

Sharjeel Arif
200388331

Table of Contents

Table of Contents

1.0 Introduction

This report outlines the decisions made on the development of a Network Design of a company with multiple campuses across multiple locations. The report will analyze the network requirements of each campus starting from the ground up. It will outline topologies of connected devices, wired and wireless, as well as IP address allocations for each host. This level will be deemed the bottom level of the hierarchy of the network or more formally, Access Layer This layer is responsible to create a Local Area Network (LAN) within the campuses of this company.

The next level up will be where the distribution of data takes place across the different campuses of this company. This layer will provide the backbone for the Municipal Area Network (MAN) architecture and will be known as the Distribution layer for the entire Network Architecture. This layer will also incorporate security features that will protect the information of data being passed around within the network to guard against attacks from outside the private network. These security features will ensure that the data travelling through the nodes on this network is safe guarded. Additional security features will also be implemented on the Access Layers as well to ensure layer-wide protection against attacks however the distribution layer will be the most heavily guarded, reasons for this will be discussed in this report.

The next layer up will be responsible of network traffic over a wide area network. Since this company has campuses on both the east and west coast of North America, a way to transmit data form coast to coast is needed and will be done over a Wide Area Network (WAN). This layer will be known as the core layer and will also have a form of security that will be discussed in detail in the report.

All of these layers will require protocols that manage routing and transportation of data. These protocols and other logic implemented will be thoroughly discussed in this report. As this report outlines a design for a network that is relatively complex, it is necessary to maintain an order of simplicity so it is easier to understand and provide a detail explanation for each decision. To maintain this order of simplicity I will be starting from the Access Layer and making my way to the Core Layer in this report.

2.0 Hierarchal Design of Network

The main responsibility of the Access Layer is to connect the end user devices (hosts) to the company network because of this the Access Layer tends to be a very complex layer to work with and organize. This layer is responsible for connection topologies between hosts, IP addressing, various equipment, wired and wireless connection to hosts, etc. This section of the report will focus on the decisions made for this layer and why those decisions were made it will also discuss other alternatives and why they were not pursued.

2.1 Connectivity Topology Between Hosts

There are several connectivity technologies that can be used throughout this network on the LAN side. Each topology comes with advantages and disadvantages. This section will discuss the multiple topologies and will give a detailed analysis of why a specific topology was chosen over another.

2.1.1 P2P Topology

This is a simplified diagram of a P2P connected topology. The advantages of this topology are as follows:

- Cabling cost is much less than other topologies
- Easy to install and setup
- Computers only listen to data being sent not responsible and are not responsible for moving data.

The disadvantages include:

- If a common cable fails the entire LAN network goes down
- If network traffic is heavy, it can cause collisions and corruption in data transfers

Decision: Since there are a minimum of 50 hosts in the smallest office of this company I will not be implementing this topology in the companies LAN network due to the fact that if one cable fails other hosts connected in this topology have the potential of going down as well.

2.1.2 Ring Topology

This is a simplified diagram of a ring topology. The advantages of this topology include:

- Easy to install and configure as there can only be a device on either side of a host.
- Equal access to all computers

Disadvantages of this topology include:

- Only offers unidirectional traffic
- Since signals are being read and sent all the time it creates unwanted power consumption
- Difficult to troubleshoot
- Break in ring can cause other hosts to fail

Decision: For the same reason as the P2P topology. I decided to avoid this topology as well for the LAN network.

2.1.3 Bus Topology

This is a simple diagram of a bus topology. The advantages of this topology include:

- Easy to install and configure
- Easy to troubleshoot
- Cost of cabling is cheaper than other topologies

Disadvantages of this topology include:

- If common cable fails, hosts connected will be disconnected
- If network traffic is too much. Performance time significantly increases.

Decision: Since this topology offers no redundancy and performance limitations I will not be using this topology to setup the nodes on the company network.

2.1.4 Star Topology

This is a simple diagram of a start topology. The advantages of this topology include:

- Easy to troubleshoot and modify
- Fast performance

Disadvantages include:

- Cost is far greater than other topologies where the benefits to cost ratio is not justifiable
- Damaged cable can bring down the entire network
- Main node going down can disconnect all the other nodes

Decision: This topology offers some redundancy and troubleshooting ease that is crucial in networks. Therefore, I will be implementing this in the LAN networks in each building connecting the host to the layer 2 switches.

2.1.5 Tree Topology

This is a simple diagram of a tree topology. Advantages of this topology include:

- Failure of a single node will not affect other nodes that are higher up in the tree. Therefore, it offers some redundancy
- Easy to trouble shoot and expand if needed

Disadvantages of this topology include:

- Heavy reliance on lots of cables to connect additional branches in the tree
- Maintenance becomes difficult if more layers are added to the tree

- If highest layer fails or layers that connect lower-level nodes. Then lower-level nodes in the tree will go down.

Decision: This topology does offer a bit of redundancy to the upper-level nodes. However, it lacks that same redundancy is lower-level nodes. For this reason, I will not be implementing it in the company's network

2.1.6 Mesh Topology

This is a simple diagram of a mesh topology. The advantages of this network include:

- Easily expandable without any disruptions to the other nodes
- No traffic problems as each node has a dedicated link
- Very robust and offers redundancy. Redundancy can also be added later on by adding more links and more routes between nodes

Disadvantages of this topology include:

- Installation process is complicated
- Requires more space
- More costly than other topologies due to the dedicated links and increased cost in cables

Decision: Since this topology offers fast connection and data transfer speeds with added redundancy and ease of implementing more nodes to the network. I believe this topology will be the best to setup the company's network with especially in the Distribution layer where multiple LANs are connected as well as connecting multiple MANs together. The cost of implementing this topology on the Access layer does not make as much sense.

2.1.7 More Options

There are other topologies that I have not covered in this section as they are not widely used. It is worth mentioning that for other smaller companies that don't have a lot of capital to work with, there are far cheaper options that will satisfy their needs.

2.1.8 Diagrams of Network Topology

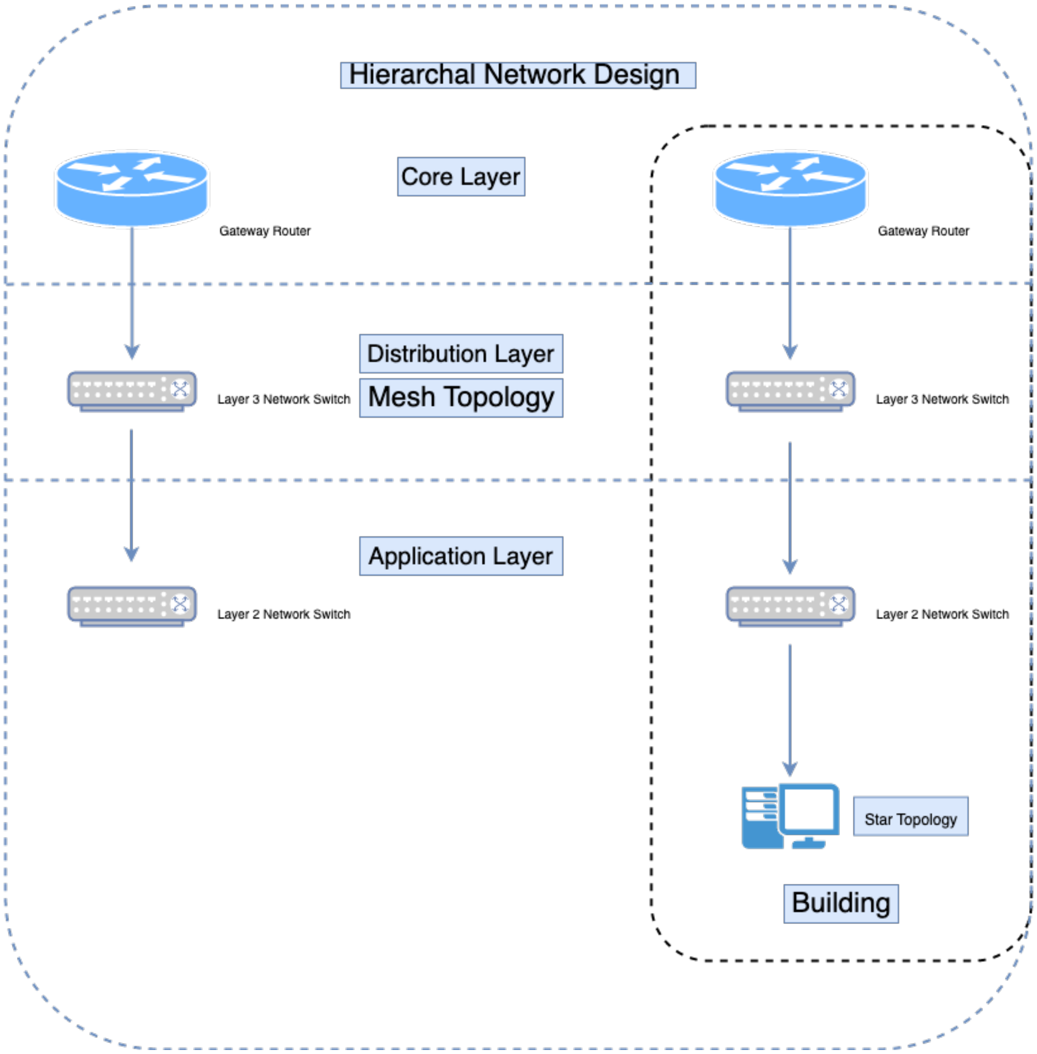


Figure 1: Diagram of Hierarchal Design of Network Topology

The current selection of topologies offers benefits of redundancy and easy troubleshooting. The core layer will provide connection to the WAN through a VPN tunnel. VPN tunneling in the Core layer will also allow for the autonomous systems across North America to be connected together. The VPN tunneling system would allow for extra security by allowing encryption of the tunnel so only hosts connected to the VPN tunnel can access data being passed through the VPN tunnel. VPN tunnels also allow for flexibility and scalability as it can connect autonomous systems together over large distances which is what this project aims to accomplish. Furthermore, utilizing a VPN tunnel allows the company to use existing infrastructure from other companies. This effectively reduces costs as the company will not need to invest in architecture connecting locations that are large distances apart geographically. For the Access layer I plan on using network switches in excess to offer redundancy. I will go into more details later on in the report. To sum it up for now though, having two or three network switches for connecting a multitude layer 2 switches to the LAN grants redundancy and security. The cost will be super high but that's what I got planned out for right now. If I had more time, I would not do this because the amount of layer 3 switches that would need to be stacked and get working together in racks would be way too costly. The company will need to have server rooms to keep these racks cooled which costs money. The company would also be investing in a lot of layer 3 switches depending on how many hosts a layer 3 switch is able to contain, This would be extremely costly in the headquarter building as there are a lot of hosts. The network architecture also becomes way more complex. If I had more time, I would probably implement a VLAN system that we learned in the labs for this class. The VLAN system offers more scalability, less overhead cost, less cost for implementation, less complex network architecture, improved security. The benefits of a VLAN system are far too great to overlook but I just don't have the time to look into this further as I started late and have projects for 433, 371, 463, and Capstone to work on as well.

2.2 Requirements For Functional Groups & Departments

Autonomous System Number	Autonomous Functional Group	Number of Hosts	Requirements Data Transfer Rate	Requirements Scalability
1	Vancouver Building 1	491	100Gbps	Network needs to be scalable for up to 1000 users more
	Vancouver Building 2	1610	100Gbps	
2	Los Angeles	75	100Gbps	
	London	50	100Gbps	
	Montreal	100	100Gbps	
3	Toronto Building 1	2250	100Gbps	
	Toronto Building 2	1450	100Gbps	
4	Boston	431	100Gbps	

Table 1: Requirements for Functional Groups & Departments

After consulting with the company and the clients with the following questionnaire I was able to determine the network requirements and base my decisions on which devices to consider when building the network

2.2.1.1 Network Requirement Questionnaire

The following is a table of questionnaire that was asked of the users of the network and the management and their answers. This questionnaire was conducted to better understand their use case and for me to decide based off their answers what devices to use in the implementation of the network.

Table 2: Network Requirements Questionnaire

Questions	**Answers**
What are the primary needs and goals for the LAN system?	The primary needs and goals for the LAN system are to provide reliable and high-speed connectivity for all company employees and visitors. It should be able to handle the company's critical applications and support wireless access for all users across the company campus.
What types of devices will users bring with them to the company campus?	Users will bring a variety of devices with them to the company campus, including smartphones, tablets, laptops, and desktop computers.
What are the expected user density and usage patterns?	The expected user density and usage patterns will depend on the size of the company and the number of employees and visitors on the campus at any given time. The usage pattern will vary depending on the location and time of day, with higher usage during peak hours.
What are the critical applications that will be running over the LAN?	The company requires 10gbps connections based off the applications they are using. Critical applications include software development tools, cloud-based services, video conferencing and collaboration tools, and data analytics platforms.
What are the user requirements for wireless access?	Users require seamless and reliable wireless access across the entire company campus, including in workspaces, meeting rooms, and public areas. The wireless

	network should be able to support multiple devices per user, and provide adequate bandwidth for high-bandwidth applications such as video streaming and large file transfers.
What are the most critical tasks that staff members perform that rely on the LAN system?	The most critical tasks that staff members perform that rely on the LAN system include software development, cloud-based service access, video conferencing and collaboration, and data analytics. These tasks require high-speed and reliable connectivity to function effectively.
What is the expected level of productivity that can be achieved with a better LAN system?	A better LAN system can significantly improve productivity by reducing network downtime and delays, enabling faster access to critical applications, and providing seamless connectivity for all users across the company campus. This can result in faster software development cycles, improved collaboration and communication, and more efficient data analysis and decision-making.
What are the most data-intensive applications that staff members use on the LAN system?	The most data-intensive applications that staff members use on the LAN system include software development tools, cloud-based services, and data analytics platforms. These applications require high-speed and reliable connectivity to function effectively.
What are the network security requirements for the LAN system?	Identify the security measures that must be implemented to protect the company's sensitive data and ensure compliance with any relevant regulations or standards.
What are the disaster recovery and business continuity requirements for the LAN system?	Determine the disaster recovery and business continuity requirements for the LAN system, including backup and recovery procedures, redundancy, and failover capabilities.

From this questionnaire I was able to better understand the needs of the users and the management staff and how they want their network to perform. The following decisions on device selections were made thanks to the answers from the questionnaire.

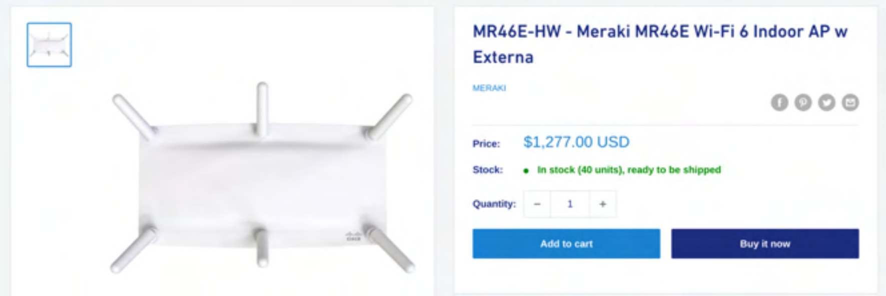
2.2.2 Selection of Network Devices Based off Questionnaire Results

Layer 2 Switch: Cisco Catalyst 2960-L 48PQ-LL Switch

The reason I decided to go with this switch is because this switch can be configured to work with 100 users per star config. It also can be configured to work with VLANS if they company decides they want to go that route in the future.

Ethernet Cable: CAT 7. The reason I decided to go with CAT 7 for the company's network implementation is because it allows for scalability. Furthermore, due to the company's requirements of at least 10Gbps for network applications. Each port on the layer 2 switch can support up to 10 users. If the layer 3 switch it is connected to is outputting 100Gbps per port. This will make more sense in the blueprint.

Wireless Network Access Point:



MR46E-HW - Meraki MR46E Wi-Fi 6 Indoor AP w Externa

MERAKI

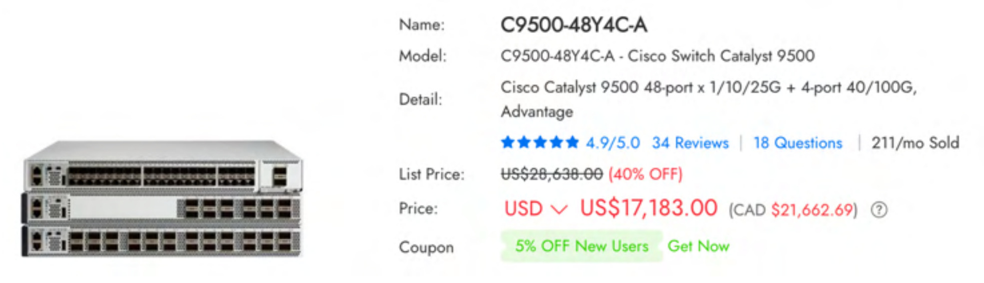
Price: $1,277.00 USD

Stock: ● In stock (40 units), ready to be shipped

Quantity: − 1 +

For the access points I have decided to go with the Cisco Meraki M46E-HW. The reason being is this access point is designed for high density indoor office/campus areas. It is one of the high-end access points that has multiple antennas for better connectivity to the hosts to support dense areas. Furthermore, it offers two Wi-Fi radios 2.4 GHz and 5 GHz. The 2.4 GHz band will offer a smooth transition to the next access point as it reaches further than the 5 GHz band. The 5 GHz band will ensure network speed and connectivity. The 5 GHz band also operates on a variety of different channels ranging from 20 MHz to 160 MHz minimizing congestion on a single channel.

Layer 3 Switch Selection: Cisco Catalyst 9500 48 48Y4C-A.



Name: C9500-48Y4C-A

Model: C9500-48Y4C-A - Cisco Switch Catalyst 9500

Detail: Cisco Catalyst 9500 48-port x 1/10/25G + 4-port 40/100G, Advantage

★★★★★ 4.9/5.0 34 Reviews | 18 Questions | 211/mo Sold

List Price: ~~US$28,638.00~~ (40% OFF)

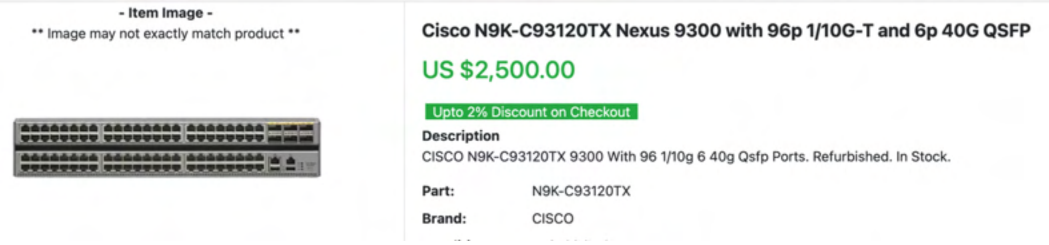
Price: USD US$17,183.00 (CAD $21,662.69)

Coupon 5% OFF New Users Get Now

The reason I have gone with another Cisco product for the Layer 3 Switch is because of ease of cross compatibility with other Cisco devices that I am using. This switch also includes VLAN and other configurations that will be useful in future scalability. It also offers:
Stackable design: This switch can be stacked with other switches in the same family to provide high-performance, scalable network solutions.
PoE support: This switch Power over Ethernet (PoE) and PoE+ for powering network devices such as IP phones and wireless access points.
Advanced security: This switch provides advanced security features such as identity-based access control, TrustSec, and Network Admission Control (NAC) to protect against unauthorized access and data breaches.

2.2.3 Cost Analysis of Topology (Star Topology for End User Hosts)

Assuming that each host requires a 5-meter Cat 7 Ethernet cable, we would need a total of:



- Item Image -
** Image may not exactly match product **

Cisco N9K-C93120TX Nexus 9300 with 96p 1/10G-T and 6p 40G QSFP

US $2,500.00

Upto 2% Discount on Checkout

Description
CISCO N9K-C93120TX 9300 With 96 1/10g 6 40g Qsfp Ports. Refurbished. In Stock.

Part: N9K-C93120TX

Brand: CISCO

Legal (130 hosts) + Accounting (331 hosts) = 461 cables for Vancouver building 1
HQ (1500 hosts) + Engineering (110 hosts) = 1610 cables for Vancouver building 2
Sales (75 hosts) + Sales (50 hosts) + Sales (100 hosts) = 225 cables for Los Angeles, London, and Montreal
Operations 1 (2250 hosts) + Operations 2 (950 hosts) + Sales (500 hosts) = 3700 cables for Toronto building 1
Engineering (331 hosts) + R&D (100 hosts) = 431 cables for Boston
This gives us a total of 7,427 Ethernet cables required for the network. These cables will be UTP.

A quick search of online retailers, Cat 7 cables cost an average price of $20 per cable (Amazon), the total cost of the Ethernet cabling would be approximately $148,540. I will round this number up to account for discrepancies in the estimates to a total of $150,000.

Assuming a maximum of 100 hosts per switch, we would need the following number of switches for each location:

Vancouver building 1: 6 switches (1 for Legal and 1 for Accounting)
Vancouver building 2: 18 switches (1500/100 for HQ and 2 for Engineering)
Los Angeles: 1 switch
London: 1 switch
Montreal: 2 switches (1 for each Sales department)
Toronto building 1: 24 switches (2250/100 for Operations 1, 950/100 for Operations 2, and 10 for Sales)
Boston: 6 switches (4 for Engineering and 2 for R&D)
This gives us a total of 73 layer 2 switches required for the network.

Assuming an average price of $3000 per switch, the total cost for layer 2 switches would be approximately $220,000.

In a half-mesh network, each switch is not connected to every other switch in its location, but only to a subset of other switches. The number of connections required would be:

Vancouver building 1: 1 connection (2 switches)
Vancouver building 2: 8 connections (16 switches)
Los Angeles: 0 connections (1 switch)
London: 0 connections (1 switch)
Montreal: 1 connection (2 switches)
Toronto building 1: 12 connections (24 switches)
Boston: 2 connections (5 switches)
For the cabling, assuming that each switch is located within the same building and requires a 2-meter Cat 7 Ethernet cable to connect to each other switch, the total length of cable required would be:

Vancouver building 1: 2 meters (2 switches)
Vancouver building 2: 128 meters (16 switches)

Los Angeles: 0 meters (1 switch)
London: 0 meters (1 switch)
Montreal: 4 meters (2 switches)
Toronto building 1: 22 meters (24 switches)
Boston: 4 meters (5 switches)

Using Cat 7 Ethernet cables with an average length of 2 meters, the estimated cost of cabling to connect the switches in a half-mesh network would be approximately:

Vancouver building 1: $20 (2 switches)
Vancouver building 2: $3,840 (192 cables for 16 switches)
Los Angeles: $0 (1 switch)
London: $0 (1 switch)
Montreal: $320 (16 cables for 2 switches)
Toronto building 1: $1,440 (72 cables for 24 switches)
Boston: $320 (16 cables for 5 switches)
Therefore, the total estimated cost of cabling for this network would be approximately $5,940. Roughly $6000.

2.3 Wireless Network Configuration

When it comes to implementing a method of connectivity for wireless devices there are also a few options to consider. However, there is one that stands out the most and is the generally accepted way of implementing a wireless network in a large campus of over 100 people. This method is called a wireless mesh network. How a wireless mesh network works is that there is one network that is extended to and has multiple access points throughout the campus. For example, there are two wireless mesh networks available to students at the University of Regina. These networks are uofrGuest and eduroam. These networks are controlled through nodes. Each node receives data from one node and outputs it and also sends it to another node. This way the network is repeated and an access point is created at each node. The same network goes throughout the entire campus. This is what is known as a true mesh network.

There is another option which involves a single node and multiple repeaters acting as an access point. However, these repeaters do not forward the network to another node instead they just act as an access point. This configuration is known as a false mesh network and comes with many limitations and expenses in cabling.

Within this company's network though; I want to use both. For offices that have staff that that house less than or equal to 75 people I want to use a false mesh network as the cost of implementing a true wireless mesh network would be greater than a false mesh wireless network. Another thing to acknowledge is that with 75 hosts or less the false wireless mesh network will not bottleneck if gigabit wireless connection is present. Within buildings that host more than 75 employees I want to implement a true wireless mesh network as with more hosts on a wireless network a false wireless mesh can experience heavy traffic and performance delays.

For the wireless network I want to utilize the Cisco Meraki MR series access points for both the false mesh and the true mesh network. This keeps troubleshooting consistent and all issues with the devices can go directly to Cisco as all the equipment will be Cisco supplied. Unless otherwise stated.

Furthermore, Cisco makes the wireless networks easy to manage as they have their own dedicated software called “Cisco Meraki Dashboard” This dashboard is a cloud-based management tool that can be used to manage access points, switches, and other security appliances. It’s a very power tool to understand what access points have the greatest traffic and what don’t have as much traffic. This information can be useful in the future as the company may want to expand their wireless in office network to support more staff. For these reasons, I will be going with only Cisco devices.

2.3.1 Cost Analysis of Wireless Network Topology

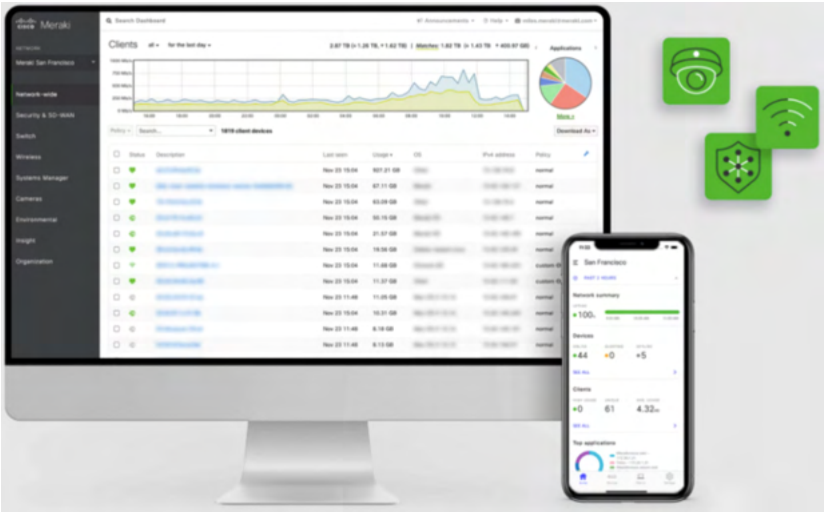


Figure 2: Screenshot of Cisco Meraki Dashboard

The cost analysis of a wireless network is a little bit tricky as it requires me to calculate the approximate size of the building to know where to place the access points and how many access points I need. I have developed floor plans and blueprints of buildings and how the users will be situated to get a better understanding of why I chose the number of access points per location I chose.

Vancouver building 1: 9 access points
Vancouver building 2: 30 access points
Los Angeles: 2 access points

London: 2 access points
Montreal: 3 access points
Toronto building 1: 30 access points
Boston: 9 access points

The total cost for this many access points will come to.
Vancouver building 1: $15,300 (9 access points x $1700 per access point)
Vancouver building 2: $51,000 (30 access points x $1700 per access point)
Los Angeles: $3,400 (2 access points x $1700 per access point)
London: $3,400 (2 access points x $1700 per access point)
Montreal: $5,100 (3 access points x $1700 per access point)
Toronto building 1: $51,000 (30 access points x $1700 per access point)
Boston: $15,300 (9 access points x $1700 per access point)

2.4 Protocol Implementation

The flowing of information within a LAN network in the Access Layer there needs to be a set of protocols in place to ensure fast data transfer, no collisions within a shared medium, and host identification on a network. Luckily there are protocols in place that manage all of this. This section of the report will focus on three main protocol that manage different things on a network. The selection of a routing protocol to manage traffic from node to node, MAC protocol configurations to ensure no collisions on a shared medium, and internet protocol address to identify a host on a network.

2.4.1 Routing Protocol

There are multiple routing protocols available to use depending on the need of the network. There are advantages and disadvantages for each protocol. Since this is a medium sized company, this report will focus on and discuss in detail a select few routing protocols. These protocols include: OSPF and BGP. Other protocols include:

- Routing Information Protocol (RIP)
- Interior Gateway Protocol (IGP)
- Exterior Gateway Protocol (EGP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Intermediate System-to-Intermediate System (IS-IS)

The reason this report does not dive into any of the other protocols aside form OSPF and BGP is because in an industry these are most commonly used and most efficient on a private network.

2.4.1.1 OSPF – Open Shortest Path First

The OSPF protocol utilizes the shortest path first algorithm to transport data in the most efficient way possible. This protocol works well with a mesh network of nodes as there are multiple paths to choose from in a mesh network. Finding the shortest path first (Dijkstra's algorithm/SPF) will ensure a fast connection and quickest path to route information from the source to the destination.

Dijkstra's shortest path first algorithm has a time complexity of O(|N|log|N|) which is 'fair' (according to the Big O notation cheat sheet). In a company the size of the one assigned this is more than enough to ensure no network lag when transporting data.

OSPF is scalable and tracks changes within the topology and can recalculate paths to guarantee the most optimal path for data transfer. OSPF also authenticates protocol changes to keep data relatively secure. Therefore, on the Access Layer for this company's network this protocol would be the best to implement. There is another protocol that this report will look into that can be implemented on another layer for this company's network which is known as BGP.

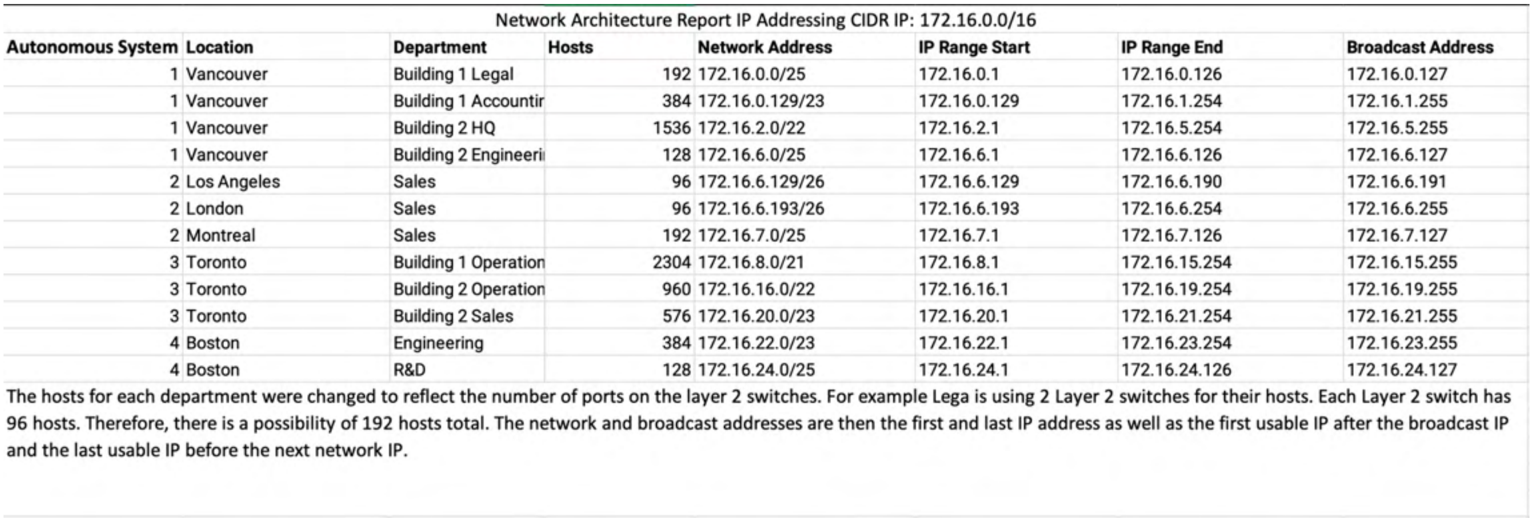
2.4.1.2 BGP – Border Gateway Protocol

The Border Gateway Border Gateway Protocol utilizes the Best Path Vector algorithm. This protocol is highly configurable with variables such as weight, local preference, locally generated, AS_Path length, origin type, multi-exit discriminator, eBGP over iBGP, IGP metric, router ID, cluster list and neighbor IP address (comparitech).

The best path vector algorithm calculates the number of autonomous systems the destination is away from the source. This is the protocol that I have decided to use in the Core layer for the WAN network.

3.0 IP Addressing

For IP Addressing of this network, I have decided to use CIDR to IP address the network. Utilizing the Classless Interdomain Routing approach makes it easier for the company to subnet and supernet within the IP lease that the company has acquired.



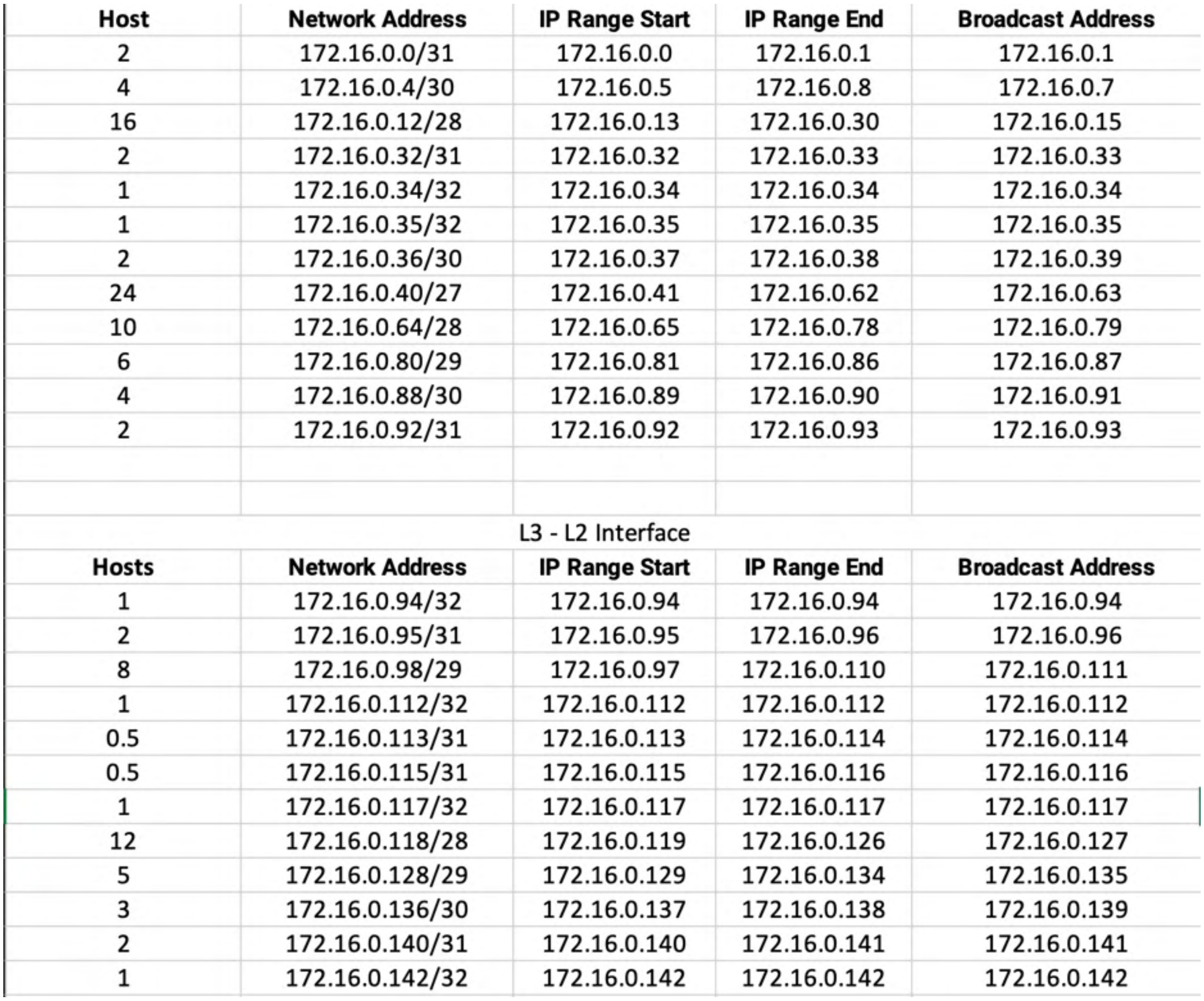
Network Architecture Report IP Addressing CIDR IP: 172.16.0.0/16

Autonomous System	Location	Department	Hosts	Network Address	IP Range Start	IP Range End	Broadcast Address
1	Vancouver	Building 1 Legal	192	172.16.0.0/25	172.16.0.1	172.16.0.126	172.16.0.127
1	Vancouver	Building 1 Accountir	384	172.16.0.129/23	172.16.0.129	172.16.1.254	172.16.1.255
1	Vancouver	Building 2 HQ	1536	172.16.2.0/22	172.16.2.1	172.16.5.254	172.16.5.255
1	Vancouver	Building 2 Engineeri	128	172.16.6.0/25	172.16.6.1	172.16.6.126	172.16.6.127
2	Los Angeles	Sales	96	172.16.6.129/26	172.16.6.129	172.16.6.190	172.16.6.191
2	London	Sales	96	172.16.6.193/26	172.16.6.193	172.16.6.254	172.16.6.255
2	Montreal	Sales	192	172.16.7.0/25	172.16.7.1	172.16.7.126	172.16.7.127
3	Toronto	Building 1 Operation	2304	172.16.8.0/21	172.16.8.1	172.16.15.254	172.16.15.255
3	Toronto	Building 2 Operation	960	172.16.16.0/22	172.16.16.1	172.16.19.254	172.16.19.255
3	Toronto	Building 2 Sales	576	172.16.20.0/23	172.16.20.1	172.16.21.254	172.16.21.255
4	Boston	Engineering	384	172.16.22.0/23	172.16.22.1	172.16.23.254	172.16.23.255
4	Boston	R&D	128	172.16.24.0/25	172.16.24.1	172.16.24.126	172.16.24.127

The hosts for each department were changed to reflect the number of ports on the layer 2 switches. For example Lega is using 2 Layer 2 switches for their hosts. Each Layer 2 switch has 96 hosts. Therefore, there is a possibility of 192 hosts total. The network and broadcast addresses are then the first and last IP address as well as the first usable IP after the broadcast IP and the last usable IP before the next network IP.

The IP addressing was done keeping scalability in mind. This way, if the company decides to expand their operations in the future, the company will be able to add onto their existing network without changing a single thing.

IP addressing for the interfaces can be found in the following tables:



Host	Network Address	IP Range Start	IP Range End	Broadcast Address
2	172.16.0.0/31	172.16.0.0	172.16.0.1	172.16.0.1
4	172.16.0.4/30	172.16.0.5	172.16.0.8	172.16.0.7
16	172.16.0.12/28	172.16.0.13	172.16.0.30	172.16.0.15
2	172.16.0.32/31	172.16.0.32	172.16.0.33	172.16.0.33
1	172.16.0.34/32	172.16.0.34	172.16.0.34	172.16.0.34
1	172.16.0.35/32	172.16.0.35	172.16.0.35	172.16.0.35
2	172.16.0.36/30	172.16.0.37	172.16.0.38	172.16.0.39
24	172.16.0.40/27	172.16.0.41	172.16.0.62	172.16.0.63
10	172.16.0.64/28	172.16.0.65	172.16.0.78	172.16.0.79
6	172.16.0.80/29	172.16.0.81	172.16.0.86	172.16.0.87
4	172.16.0.88/30	172.16.0.89	172.16.0.90	172.16.0.91
2	172.16.0.92/31	172.16.0.92	172.16.0.93	172.16.0.93

L3 - L2 Interface

Hosts	Network Address	IP Range Start	IP Range End	Broadcast Address
1	172.16.0.94/32	172.16.0.94	172.16.0.94	172.16.0.94
2	172.16.0.95/31	172.16.0.95	172.16.0.96	172.16.0.96
8	172.16.0.98/29	172.16.0.97	172.16.0.110	172.16.0.111
1	172.16.0.112/32	172.16.0.112	172.16.0.112	172.16.0.112
0.5	172.16.0.113/31	172.16.0.113	172.16.0.114	172.16.0.114
0.5	172.16.0.115/31	172.16.0.115	172.16.0.116	172.16.0.116
1	172.16.0.117/32	172.16.0.117	172.16.0.117	172.16.0.117
12	172.16.0.118/28	172.16.0.119	172.16.0.126	172.16.0.127
5	172.16.0.128/29	172.16.0.129	172.16.0.134	172.16.0.135
3	172.16.0.136/30	172.16.0.137	172.16.0.138	172.16.0.139
2	172.16.0.140/31	172.16.0.140	172.16.0.141	172.16.0.141
1	172.16.0.142/32	172.16.0.142	172.16.0.142	172.16.0.142

4.0 Floor Plans and Decisions for all Buildings

4.1 Exterior Building Design

The exterior building diagram provided by the management team doesn't seem to have an extraordinary shape. The buildings exhibit a boxed design with a server room externally attached but includes access to from the inside of the main building. The management team of the company provided a diagram for Vancouver Building 1.

This diagram of the building was taken in to account when figuring out how to run the wiring throughout each floor. As well as designing how the Layer 3 and Layer 2 Switches as well as the routers will be stored and cooled within the server room. The management team has also supplied a floor plan for each floor. Stating that the floor plan is consistent with every floor on every building.

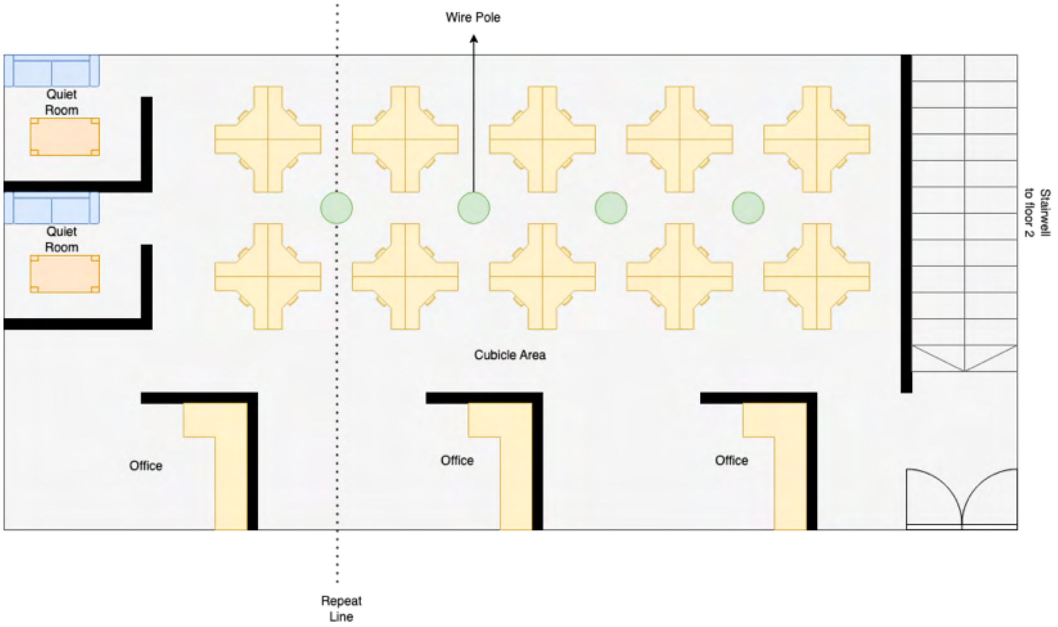
4.2 Floor Plans for All Buildings

The following floor plans accurately depict the layout of all floors of the company owned buildings. The repeat line indicates that there will be more offices and more cubicles prior to the end of the floor.

With the use of this floor plan, we can determine that the majority of the users will be located around the mid-section of the floors not near a wall. For these users, I have decided to run the ethernet cabling from the ceiling down to the actual users using wiring poles. For the users that are near the wall, the ethernet and power will be ran alongside the walls.

Running the cabling from the ceiling down will not only make the work area safer and cleaner, it will also make things easier to troubleshoot as all the wires will be in the ceiling easy to access.

The management team stated that each building will have the same floorplan concept just more floors to assist more users. In my design of this companies network each floor has its own LAN. However, each layer 3 switch can be coupled with multiple layer 2 switches from different LANs to offer more redundancy in case a layer 3 switch fails. This building plan works well with my network architecture design for the company.



4.3 Between Autonomous Systems

This diagram is a good representation of how the different autonomous systems will be connected. The four different autonomous system will be going to a layer 3 switch

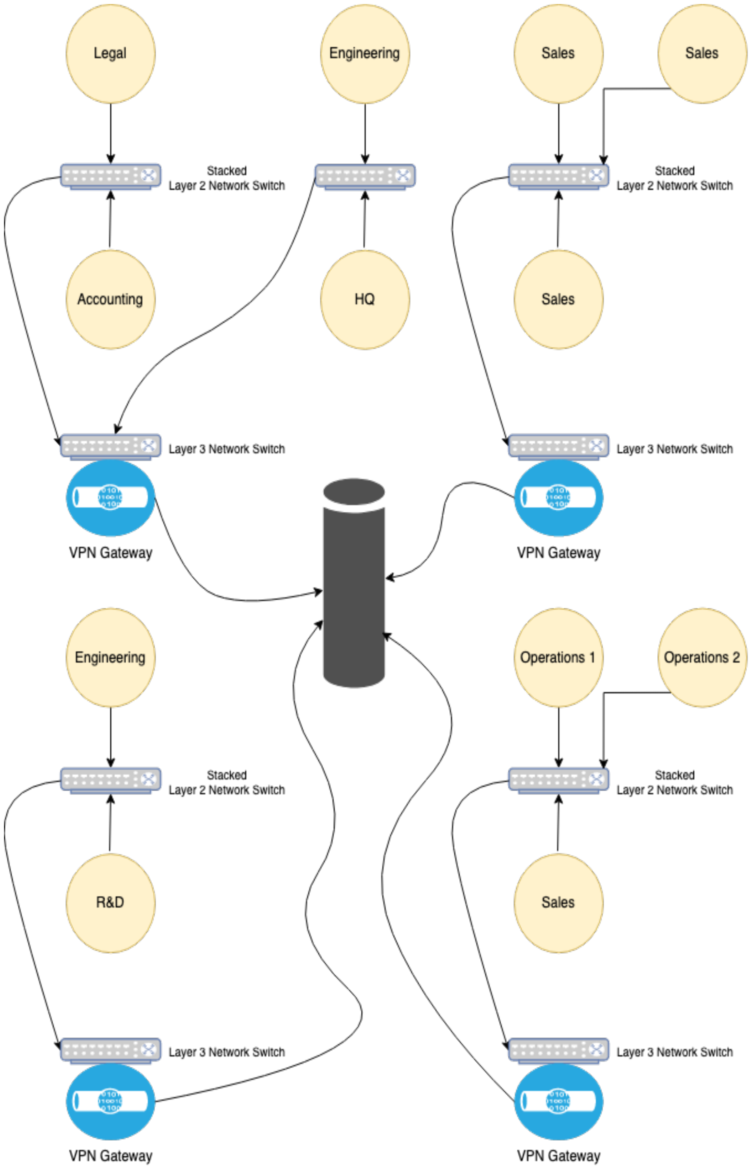


Figure 3: Diagram that shows how the four different autonomous systems will be connected

5.0 References

Fast Cabling. (2021, August 10). How to Get a High-Speed Networking System over Long Distance. Fast Cabling. https://www.fastcabling.com/2021/08/10/how-to-get-a-high-speed-networking-system-over-long-distance/

Cisco. (n.d.). What Is Network Infrastructure? Cisco. https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-infrastructure.html#~components

Stretch, J. (2009). IPv4 Subnetting Reference. Packet Life. https://packetlife.net/media/library/15/IPv4_Subnetting.pdf

Nokia. (n.d.). 7750 Service Router. Nokia. https://www.nokia.com/networks/ip-networks/7750-service-router/

TechTarget. (n.d.). Wireless Mesh Network. TechTarget. https://www.techtarget.com/searchnetworking/definition/wireless-mesh-network#:~:text=In%20a%20wireless%20mesh%20network,can%20connect%20to%20for%20internet.

Medard, M. (2012). Introduction to Digital Communication Systems (MIT Course Lecture). MIT OpenCourseWare. https://ocw.mit.edu/courses/6-02-introduction-to-eecs-ii-digital-communication-systems-fall-2012/resources/mit6_02f12_lec18/

TechTarget. (n.d.). Routing Protocol Types Guide: OSPF, BGP, MPLS, & More. TechTarget. https://www.comparitech.com/net-admin/routing-protocol-types-guide/

Big O Cheat Sheet. (n.d.). Big O Cheat Sheet. https://www.bigocheatsheet.com/

Sugih Jamin. (n.d.). Routing: Link State (LS). EECS 489: Computer Networks (University of Michigan Course Lecture). University of Michigan. https://web.eecs.umich.edu/~sugih/courses/eecs489/lectures/16-RoutingLS.pdf

Sugih Jamin. (n.d.). Routing: Distance Vector (DV). EECS 489: Computer Networks (University of Michigan Course Lecture). University of Michigan. https://web.eecs.umich.edu/~sugih/courses/eecs489/lectures/15-RoutingDV.pdf

Wakamiya, N. (2018). Routing Protocols. IP Network Architecture (NAIST Course Lecture). Nara Institute of Science and Technology. https://iplab.naist.jp/class/2018/materials/lectures/2018-04-routing.pdf

Thom Digital. (n.d.). The Power of Cisco Meraki Systems. Thom Digital. https://thomdigital.com/the-power-of-cisco-meraki-systems/

ServerSupply. (n.d.). Cisco N9K-C93120TX Nexus 9300 Series 96-Port 10G Switch. ServerSupply. https://www.serversupply.com/NETWORKING/SWITCH/96%20PORT/CISCO/N9K-C93120TX_357404.htm

Router-switch.com. (n.d.). C9500-48Y4C-A. Router-switch.com. https://www.router-switch.com/c9500-48y4c-a.html?gclid=CjwKCAjwitShBhA6EiwAq3RqA9geGXwyaXv9FCbRFiheKczA99ILjl9zOgbPHnHL2YCmbqRE_EPA0