Network Design Project Report

06/04/2021
ENEL 492: Design of Computer Networks

Arpan Dhamane
Professor: Irfan Al- Anbagi

Table of Contents

Network Layout

Specifications and Requirements

The requirements of a network can be divided into 8 sections; ID/Name, Date, Type, Description, Gathered/Derived, Locations, Status, and Priority. (Referred to: *Network Analysis, Architecture and Design Third Edition by James D. McCabe* Textbook)

We can take certain assumptions regarding what each department requires for a repeatable requirements list for different locations. For a more detailed requirements list, we would typically be consulting with the company in regards to additional information. An example would be the network speed, network budget, etc.

Requirements Table per department

Accounting:

ID/Name	Date	Type	Description	Gathered/Derived	Locations	Status	Priority
1	N/A	User	370 users	Assumed from Management	Vancouver Building 1	Info	TBD
2	N/A	Application	Primary: Payroll Applications are mission critical, require fast speeds and 100% uptime Secondary: Email, Word processing, VOIP, internal and external web access	Assumption: gathered from Management	Vancouver Building 1	TBD	TBD
3	N/A	Device	Need multiple printers/fax machines	Assumption: gathered from Management	Vancouver Building 1	TBD	TBD
4	N/A	Network	Use minimum of T1 access to Data	Assumption: gathered from Network Staff	Vancouver Building 1	TBD	TBD

5	N/A	Other	N/A	N/A	Vancouver Building 1	TBD	TBD

Legal:

ID/Name	Date	Type	Description	Gathered/Derived	Locations	Status	Priority
1	N/A	User	130 users	Assumed from Management	Vancouver Building 1	Info	TBD
2	N/A	Application	Email, Word processing, VOIP, internal and external web access	Assumption: gathered from Management	Vancouver Building 1	TBD	TBD
3	N/A	Device	Need multiple printers/fax machines	Assumption: gathered from Management	Vancouver Building 1	TBD	TBD
4	N/A	Network	Use minimum of T1 access to Data	Assumption: gathered from Network Staff	Vancouver Building 1	TBD	TBD
5	N/A	Other	N/A	N/A	Vancouver Building 1	TBD	TBD

HQ:

ID/Name	Date	Type	Description	Gathered/Derived	Locations	Status	Priority
1	N/A	User	1500 users	Assumed from Management	Vancouver Building 2	Info	TBD
2	N/A	Application	Primary: Database access is mission critical Secondary: Email, Word processing, VOIP, internal and external web access.	Assumption: gathered from Management	Vancouver Building 2	TBD	TBD

3	N/A	Device	Primary: Server connections required for entire network Secondary: Need multiple printers/fax machines	Assumption: gathered from Management	Vancouver Building 2	TBD	TBD
4	N/A	Network	Use minimum of T1 access to Data	Assumption: gathered from Network Staff	Vancouver Building 2	TBD	TBD
5	N/A	Other	N/A	N/A	Vancouver Building 2	TBD	TBD

Engineering:

ID/Name	Date	Type	Description	Gathered/Derived	Locations	Status	Priority
1	N/A	User	410 users	Assumed from Management	Vancouver Building 2, Boston Building	Info	TBD
2	N/A	Application	Email, Word processing, VOIP, internal and external web access	Assumption: gathered from Management	Vancouver Building 2, Boston Building	TBD	TBD
3	N/A	Device	Primary: GigE NICs user workstations Secondary: need multiple printers/fax machines	Assumption: gathered from Management	Vancouver Building 2, Boston Building	TBD	TBD
4	N/A	Network	Use minimum of T1 access to Data	Assumption: gathered from Network Staff	Vancouver Building 2, Boston Building	TBD	TBD

5	N/A	Other	N/A	N/A	Vancouver Building 2, Boston Building	TBD	TBD

Sales:

ID/Name	Date	Type	Description	Gathered/Derived	Locations	Status	Priority
1	N/A	User	725 users	Assumed from Management	Los Angeles, London, Montreal, Toronto Building 1	Info	TBD
2	N/A	Application	Email, Word processing, VOIP, internal and external web access	Assumption: gathered from Management	Los Angeles, London, Montreal, Toronto Building 1	TBD	TBD
3	N/A	Device	Need multiple printers/fax machines	Assumption: gathered from Management	Los Angeles, London, Montreal, Toronto Building 1	TBD	TBD
4	N/A	Network	Use minimum of T1 access to Data	Assumption: gathered from Network Staff	Los Angeles, London, Montreal, Toronto Building 1	TBD	TBD
5	N/A	Other	N/A	N/A	Los Angeles, London, Montreal, Toronto Building 1	TBD	TBD

Operations:

ID/Name	Date	Type	Description	Gathered/Derived	Locations	Status	Priority
1	N/A	User	3200 users	Assumed from Management	Toronto Building 1	Info	TBD

2	N/A	Application	Primary: Database, Visualization applications need minimum of 150 Kb/s for each session Secondary: Email, Word processing, VOIP, internal and external web access	Assumption: gathered from Management	Toronto Building 1	TBD	TBD
3	N/A	Device	Need multiple printers/fax machines	Assumption: gathered from Management	Toronto Building 1	TBD	TBD
4	N/A	Network	Use minimum of T1 access to Data	Assumption: gathered from Network Staff	Toronto Building 1	TBD	TBD
5	N/A	Other	N/A	N/A	Toronto Building 1	TBD	TBD

R&D:

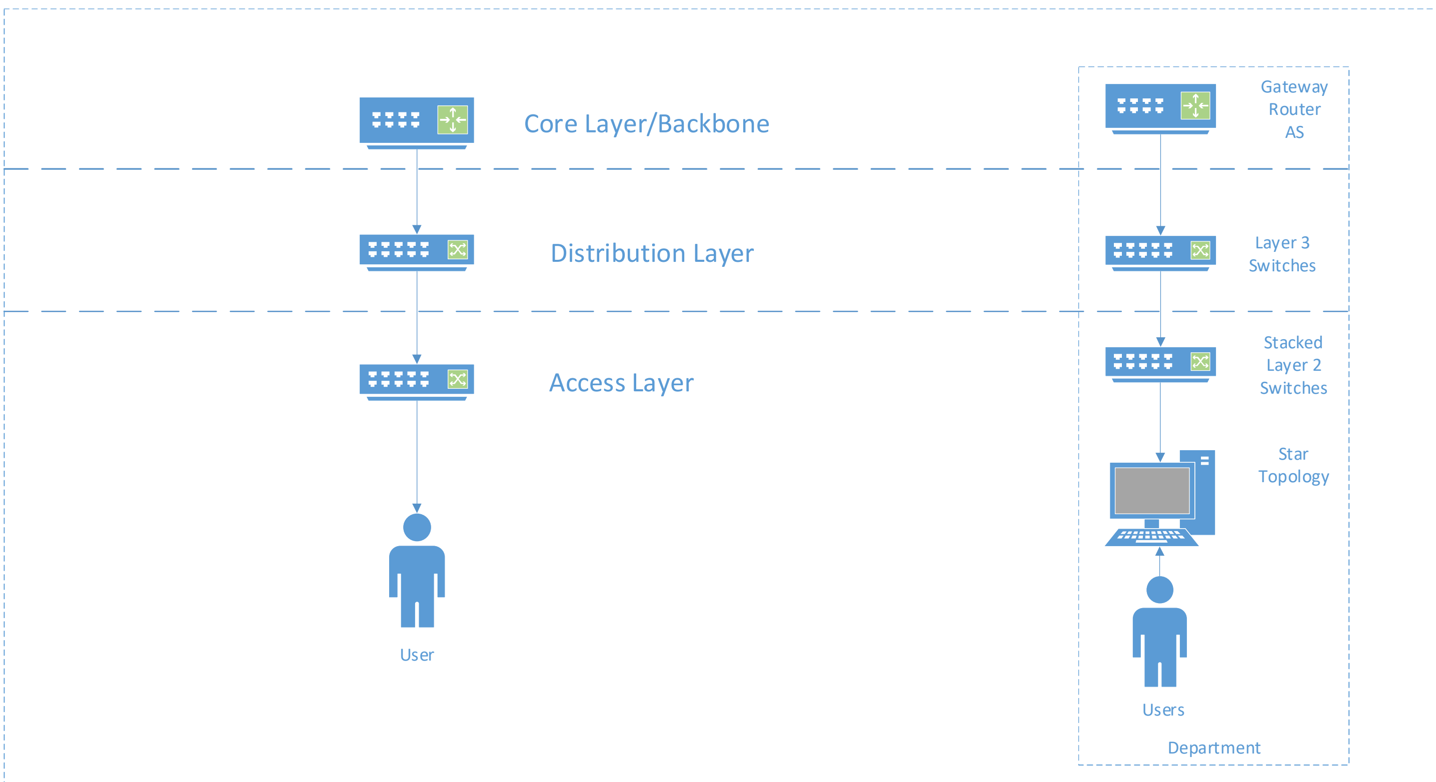
ID/Name	Date	Type	Description	Gathered/Derived	Locations	Status	Priority
1	N/A	User	3200 users	Assumed from Management	Toronto Building 1	Info	TBD
2	N/A	Application	Primary: GigE NICs user workstations Secondary: Email, Word processing, internal and external web access	Assumption: gathered from Management	Toronto Building 1	TBD	TBD
3	N/A	Device	Need multiple	Assumption: gathered from Management	Toronto Building 1	TBD	TBD

			printers/fax machines				
4	N/A	Network	Use minimum of T1 access to Data	Assumption: gathered from Network Staff	Toronto Building 1	TBD	TBD
5	N/A	Other	N/A	N/A	Toronto Building 1	TBD	TBD

Selection of Topology

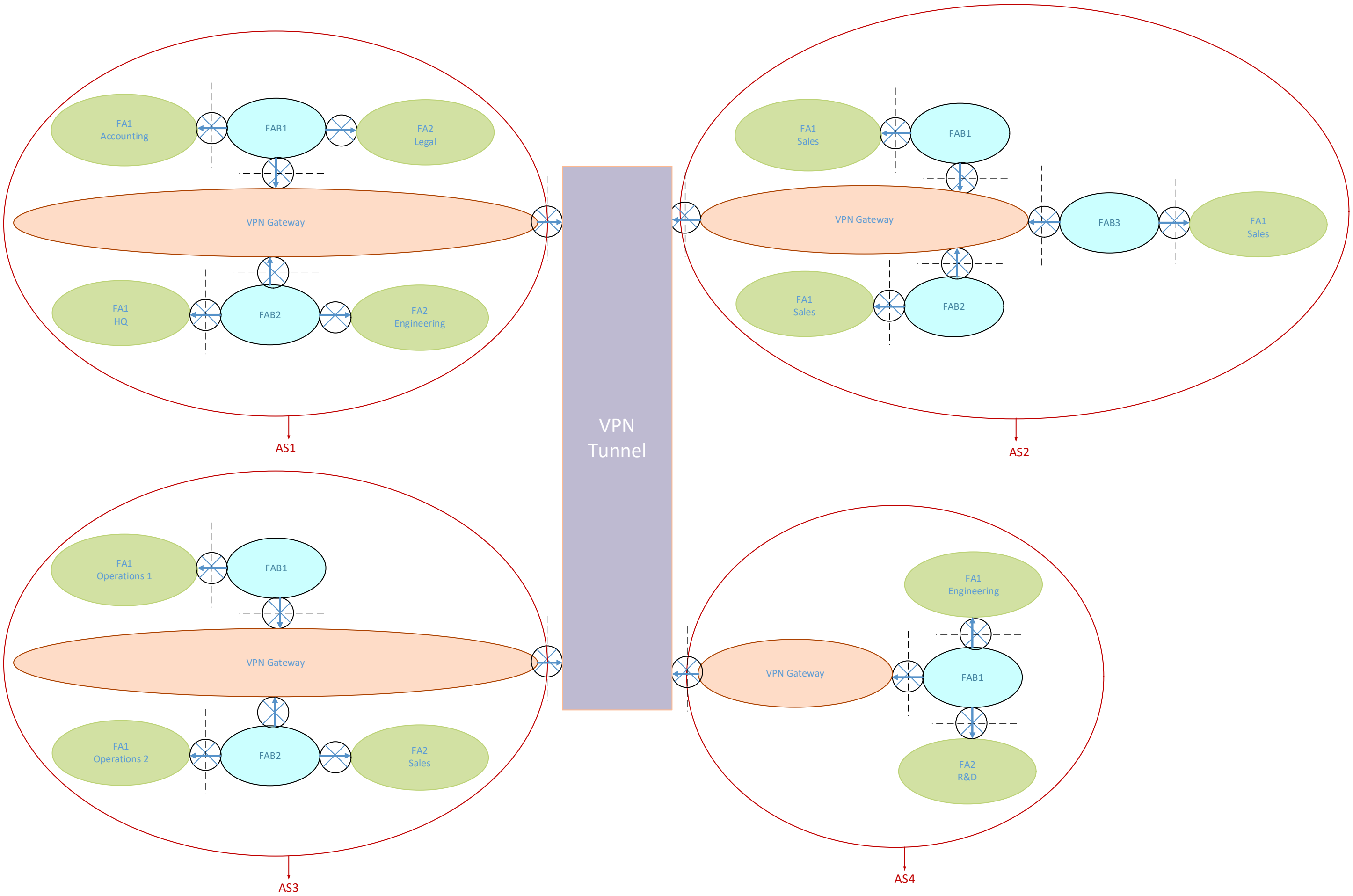
Hierarchical Approach

There are three approaches that can be looked at for designing our network. First of all, we can create a multitude of subnets for each department by creating sub divisions. Second, revising the first approach by stacking the switches. This eliminates the need for multiple subnets per department. Lastly, a VLAN combined with stacking switches approach can be used to connect the floors instead of going off of departments. I have gone with the second approach due to time constraints for reworking all my diagrams. I would pick the third approach but the Capstone and ENEL 482 projects have hindered my time.

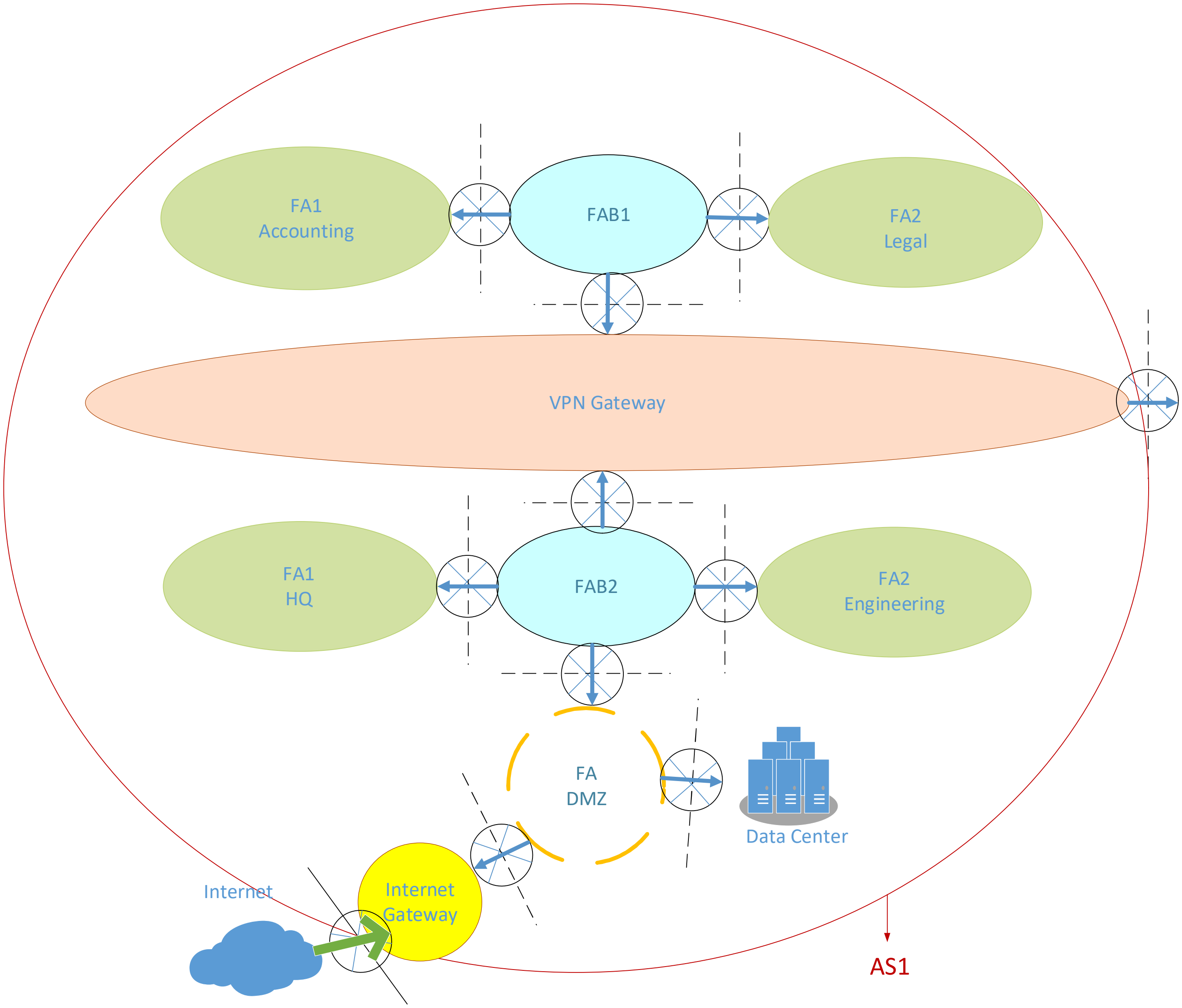


The Core Layer is providing connections and routing for the VPN. The VPN is used to connect all the Autonomous Systems together through a VPN tunnel. This way, we have a secure network that can only be accessed by the company. The Distribution Layer is used to control the connection between the access and core layer of the network. In our case, we are creating domains using these Layer 3 switches. These Layer 3 switches will be used for future upgradability to VLAN connections.

Functional Areas:



Addition areas for internet and Data center Access through DMZ:

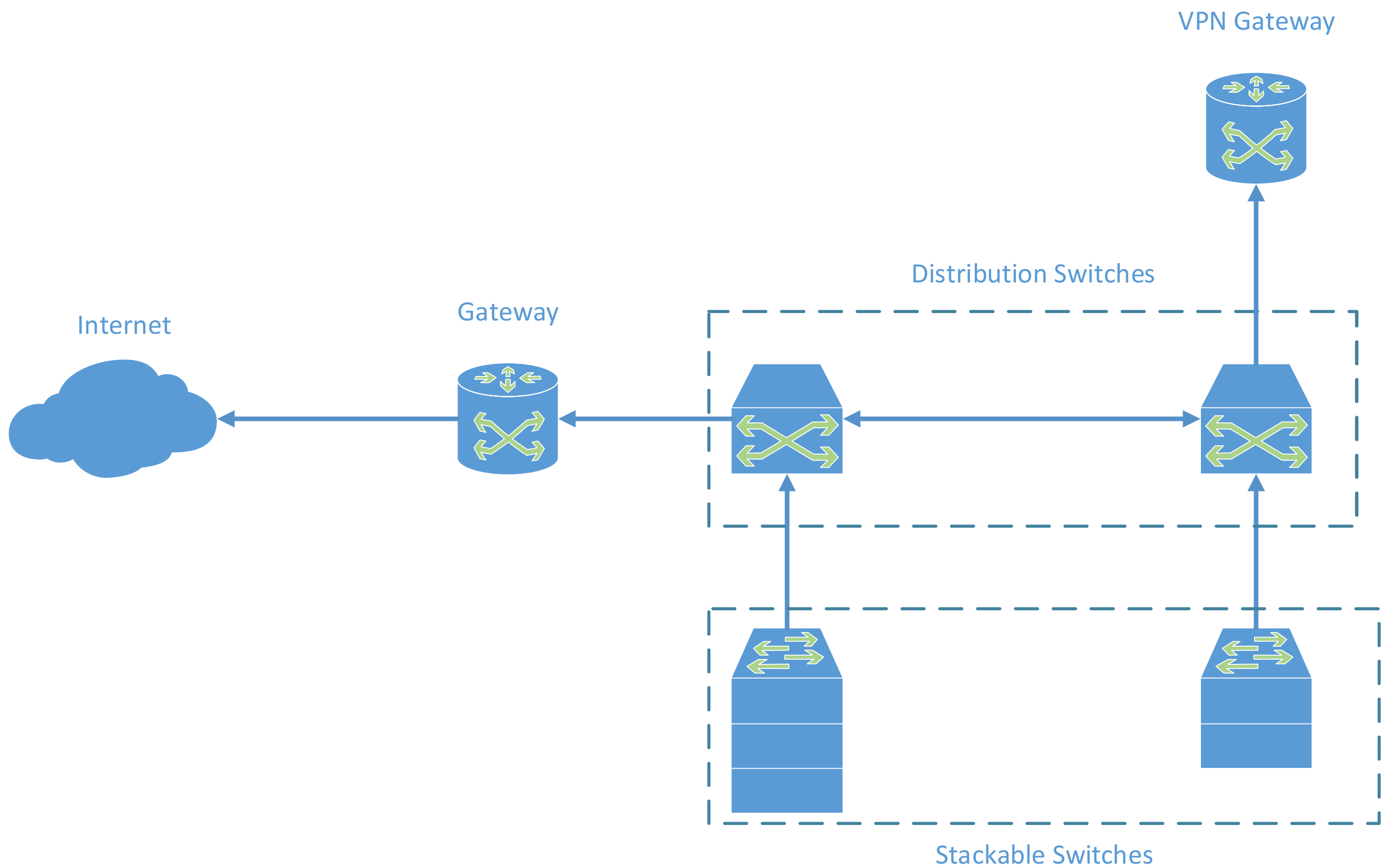


Network Traffic

The traffic flow of this network will be dependent on both internal and external access. Let us assume that external access is not permitted, but if it was, we would use Figure 4.45 (Flow Model for Flow Type 3) from the textbook '*Network Analysis, Architecture, and Design 3rd Edition by James D. McCabe'* as reference to create a flow model for external access.

By considering the labs done in ENEL 492, we can discuss the internal traffic flow of the autonomous systems (AS#).

AS1: As shown in the functional area map, we have our data center and access to the internet connected through the DMZ functional area. The gateway is connected to the buildings layer 3 switches.



This approach gives us very slow speeds. To increase the connection speed, we can use a firewall to create a DMZ area where certain services are disabled, such as heavy http loads (prevent video streaming). The firewall also gives better security to the network since we can block certain services and protocols that may expose the network. Access to other application requirements can be fulfilled by giving access to the company's data center to increase work efficiency. Let us assume a process takes too long to do on the host computer, we can use the data center to run the process in a container rack, where mini computers do all the process. To improve speeds, we would use a cloud-based server farm provided by 3rd parties such as Amazon or Google.

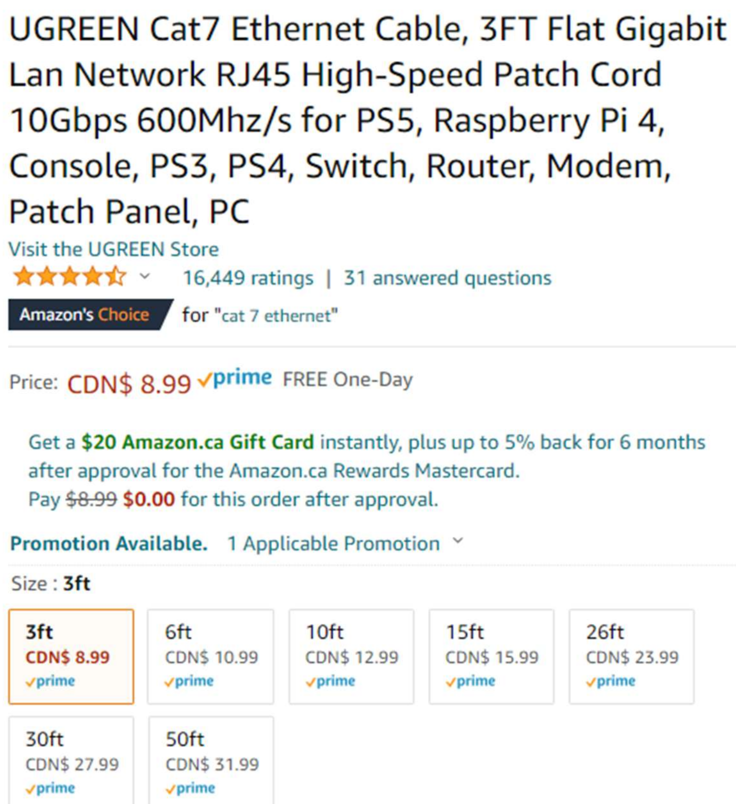
*Note: simulations in Riverbed and using other tools to check on specific traffics in each area is the ideal way.

Network Architecture

Network Components

*Note: We would be using morphological charts to compare different network components for the best cost benefit analysis, but for now I have just compared them in terms of reliability and expandability.

Cables:
*Note: 6685 Cat7 Ethernet Cables in total



https://www.amazon.ca/UGREEN-Performance-Shielded-Ethernet-Stranded/dp/B00QV1F1C4

Switches:
48 ports per switches

16 switches for AS1 B1 Accounting
7 switches for AS1 B1 Legal
62 switches for AS1 B2 HQ
6 switches for AS1 B2 Engineering
4 switches for AS2 Los Angeles Sales
3 switches for AS2 London Sales
5 switches for AS2 Montreal Sales
92 switches for AS3 B1 Operations

39 switches for AS3 B2 Operations
21 switches for AS3 B2 Sales
13 switches for AS4 Boston Engineering
5 switches for AS4 Boston R&D

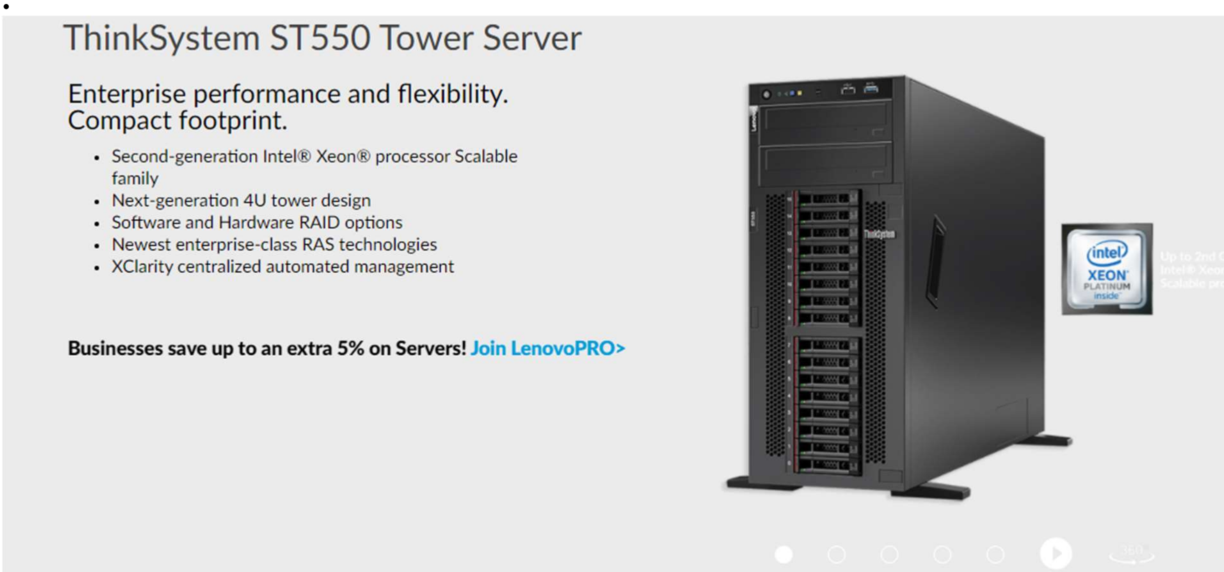
*additional switches were added to each department per AS to account for the Layer 3 switches

https://www.allhdd.com/networking-devices/switch/48-port/cisco-c9500-48y4c-a-nbp/

Primary Connection:
According to the labs, we would choose a minimum speed of T1 protocol. For the purpose of keeping things fast/reliable SONET, Fiber, or Ethernet are some good options depending on the locations. We can use Ethernet service provide by a 3rd party, such as Bell. They provide speeds up to 10 Gbps.
https://business.bell.ca/shop/medium-large/internet-private-networks/ethernet

*VLAN connectivity provided for future scaling/improvements

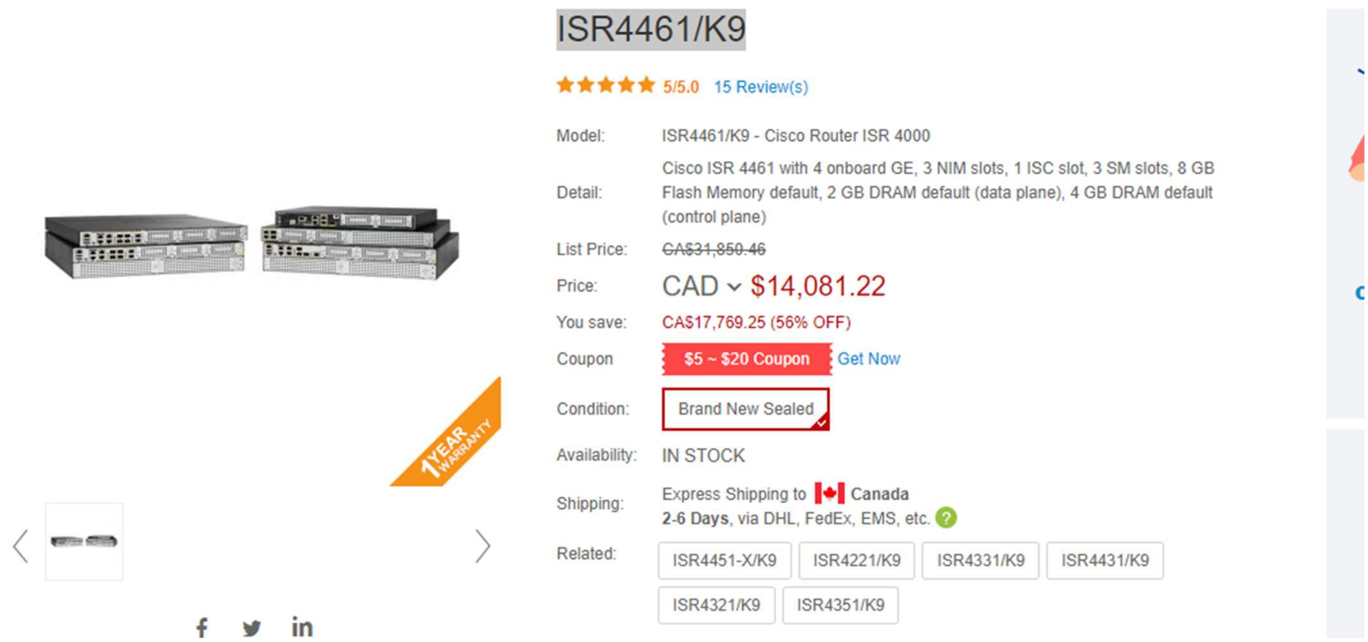
Servers:



https://www.lenovo.com/ca/en/data-center/servers/towers/ThinkSystem-ST550/p/7X10A0B7NA?gclid=Cj0KCQjwyN-DBhCDARIsAFOELTmsbUJnQARaE2yMbDlFPRXICgdI4THvkCpBkyWRT364PbScfT59ilMaAo7zEALw_wcB&gclsrc=aw.ds

One or many servers will be used for different departments to process long term data. As well to access a database. Cost: $3,633.44 CAD

Gateway Routers:
3 Routers for AS1
3 Routers for AS2
1 Router for AS3
1 Router for AS4



https://www.router-switch.com/isr4461-k9.html

Cost-Benefit Analysis

Cables: Cat7 was picked because of its speed and upgradability for the future. When comparing to Cat6 and Cat5, we do not get nearly the same data rate. With the assumption of upgrading the network speeds/maintaining currently high levels of speeds and affordability, we can justify that Cat7 cables are an appropriate option.

Switches: The switches above were chosen because we can make future improvements on the network for VLANs and have expandability for the company. Hence why each L2 switch only hosts 25 users but has 48 ports. The cost is increased with this approach as we need more switches per station, but the network's reliability and redundancy also improve.

Primary Connection: The current ethernet connection was chosen for future VLAN integration into the system and for a variable bandwidth. We can take data in for each month to see where more bandwidth is being used to optimize for connection cost. If a fix connection was used (T1), we would have to rework the entire network connections for upgradability.

Servers: The servers and database are there to keep company information privately store and to maintain efficiency in work flow. The use of servers allows for a multitude of applications to be run externally from the internal network. A future advancement/improvement we be to move to cloud-based computing, but would increase costs significantly compared to owning/maintaining. The benefit of using a cloud data center is the guarantied uptime compared to a self-maintained database.

Gateway Routers: The router selected above allows for MPLS VPN and the internet. The system also has a large throughput for good connection speeds. When comparing to other routers, they have a multitude of ports for expansions, and support 10 Gbp/s LAN connections. As for the price, they are quite expensive compared to some other routers but those routers do not provide nearly the same number of features. This would hinder future expansions and would cost the company more to upgrade/rework the network in the future. A Wi-Fi router can also be implemented for wireless internet connectivity but it would be really slow because there is only one Internet gateway. (The further you are from B2, the slower the internet)

Conclusively, all the components allow a replicable model that can be used throughout the network and to expand the network in the future.

Interconnection of Components

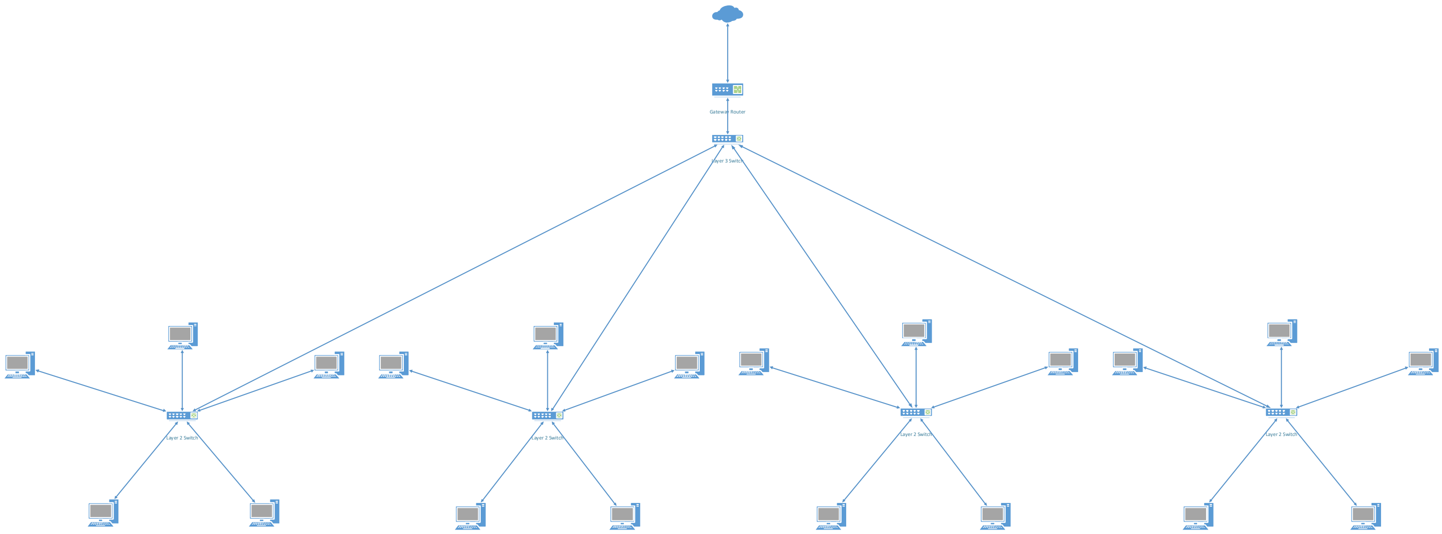


Figure. Twenty hosts connected to network

The figure above shows how the hosts will be connected to their respective switches. Instead of five hosts per switches, we would have 25 host per switch. For redundancy, higher level switches (layer 3 switch) are connected together with individual connections to a gateway router. The router is used to access the network's VPN tunnel, and connect to the internet after passing through a firewall. The firewall will only allow access to certain services. The service restrictions are dependent on the company and can be programmed into the firewall.

The reason why a star topology was used for connecting the hosts to a layer 2 switch is because of its flexibility and low installation cost. The topology is flexible because we are able to increase or decrease the number of hosts connected without disrupting the rest of the connections. A downfall that may occur, if the central node fail, all the hosts connected to it will lose their connections. To minimize this problem, we would just have less hosts connecting to a switch, but at the cost of increasing the number of switches.

*VLANs is recommended to eliminate the broadcast domains created by current design. It is both cost effective and reliable.

Availability, Redundancy, and Survivability

During the examination of this network, we can see the various areas where availability, redundancy and survivability are needed as per the requirements table. In regards to availability, we have made decisions that allow for great uptimes for our system. For example, using a third-party cloud and ethernet, the system will be constantly maintained and run through external private servers. The only issue that occurs would be the subscription cost of third-party. The make the network redundant, we have connected floors together via stackable switches (both L2 and L3). This would allow algorithms to use a routing table for routing data in the most optimized way. For survivability, the network can maintain service if a failure occurs because of the measures taken for the redundancy of the network. A more optimal solution can be implemented where more we have more than one gateway router per AS, but would significantly increase our financial cost. If the company is very software based and is willing to spend more on the system's availability, redundancy and survivability, then adding additional measures would be a good choice. A network management system can be considered. A basic approach with three angles would be to first have the ability to detect faults automatically. Then we can take certain countermeasures to reroute the network for maintaining service. Lastly, we can optimize the performance of the network by examining the different traffics in the network.

IP Addressing

IP Address Design

Since 25 per switch (48 port per switch)

Network Address: 192.168.6.9/12
Subnet Mask: 255.255.0.0/16

We then get 16 subnets using the mask above. This allows for 65,636 hosts per subnet.

AS1	AS2	AS3	AS4
15 x 48 = 720 hosts for Accounting 6 x 48 = 288 hosts for Legal 60 x 48 = 2280 hosts for HQ 5 x 48 = 240 hosts for Engineering	3 x 48 = 144 hosts for Sales 2 x 48 = 96 hosts for Sales 4 x 48 = 192 hosts for Sales	90 x 48 = 4320 hosts for Operations 1 38 x 48 = 1824 hosts for Operations 2 20 x 48 = 960 hosts for Sales	12 x 48 = 576 hosts for Engineering 4 x 48 = 192 hosts for R&D

Subnet ID	Subnet Address	Host Address Range	Broadcast Address	Department	Locations
1	192.160.0.0	192.160.0.1 - 192.160.255.254	192.160.255.255	Accounting	Vancouver Building 1
2	192.161.0.0	192.161.0.1 - 192.161.255.254	192.161.255.255	Legal	Vancouver Building 1
3	192.162.0.0	192.162.0.1 - 192.162.255.254	192.162.255.255	HQ	Vancouver Building 2
4	192.163.0.0	192.163.0.1 - 192.163.255.254	192.163.255.255	Engineering	Vancouver Building 2
5	192.164.0.0	192.164.0.1 - 192.164.255.254	192.164.255.255	Sales	Los Angeles
6	192.165.0.0	192.165.0.1 - 192.165.255.254	192.165.255.255	Sales	London
7	192.166.0.0	192.166.0.1 - 192.166.255.254	192.166.255.255	Sales	Montreal
8	192.167.0.0	192.167.0.1 - 192.167.255.254	192.167.255.255	Operations 1	Toronto Building 1
9	192.168.0.0	192.168.0.1 - 192.168.255.254	192.168.255.255	Operations 2	Toronto Building 2
10	192.169.0.0	192.169.0.1 - 192.169.255.254	192.169.255.255	Sales	Toronto Building 2
11	192.170.0.0	192.170.0.1 - 192.170.255.254	192.170.255.255	Engineering	Boston
12	192.171.0.0	192.171.0.1 - 192.171.255.254	192.171.255.255	R&D	Boston
13	192.172.0.0	192.172.0.1 - 192.172.255.254	192.172.255.255	TBD	TBD
14	192.173.0.0	192.173.0.1 - 192.173.255.254	192.173.255.255	TBD	TBD
15	192.174.0.0	192.174.0.1 - 192.174.255.254	192.174.255.255	TBD	TBD
16	192.175.0.0	192.175.0.1 - 192.175.255.254	192.175.255.255	TBD	TBD

Because we are subnetting based on departments, we can now expand our system by up to 4 departments with a host capacity of 65,636 hosts per department.

Routing Protocols

Referring back to the functional area diagram above, the network uses IPv4 for its internal device connections and MPLS for connecting the Autonomous Systems together. If a 3rd party VPN is used, they are able to connect with IPv4 or IPv6 networks. IPv4 was chosen because we did not need to drastically increase the number of subnets and hosts. If a significant number of work force is increased (in the millions), then IPv6 would be a better option as it provides more room for expansion. Because we have chosen ethernet as our connection, we can use MPLS for our VPN. MPLS allows for predetermined routing that takes the faster way, and increase the efficiency of the network, assuming that the network allows for BGP or RIP. Each VPN has its own VRF (VPN Routing or Forwarding instance) and uses an IP routing table (we can obtain this by CEF (Cisco Express Forwarding table). By configuring MP-BGP, we can allow an address family to exist in the MPLS backbone. This ultimately creates the VPN for the entire network. The reason we picked MPLS was because of the router VPN connection capability through MPLS.
Referred to https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13733-mpls-vpn-basic.html and https://www.cisco.com/c/dam/global/fr_ca/training-events/pdfs/Intro_to_mpls.pdf

Protocols
MPLS VPN protocols:
OSPF or IS-IS – check if destination network can be reached
BGP, RSVP or TDP – labels the destination network for mapping

An addition benefit of using MPLS-based VPNs is the simplicity to group the services with users, and each transport of data is separated to the individual connections.

Intranet Protocols:
VOIP – for telephoning through the network
IMAP – for electronic messaging
IPv4 – for identifying hosts and the subnet of each AS
IPP – for running devices such as printers.

Internet Protocols:
TCP/IP, UDP/IP, SFTP, HTTP – used to access certain services of internet.

Some protocols may be limited to the bandwidth or just completely denied access through the firewall for security and network efficiency purposes.

Network Blueprints

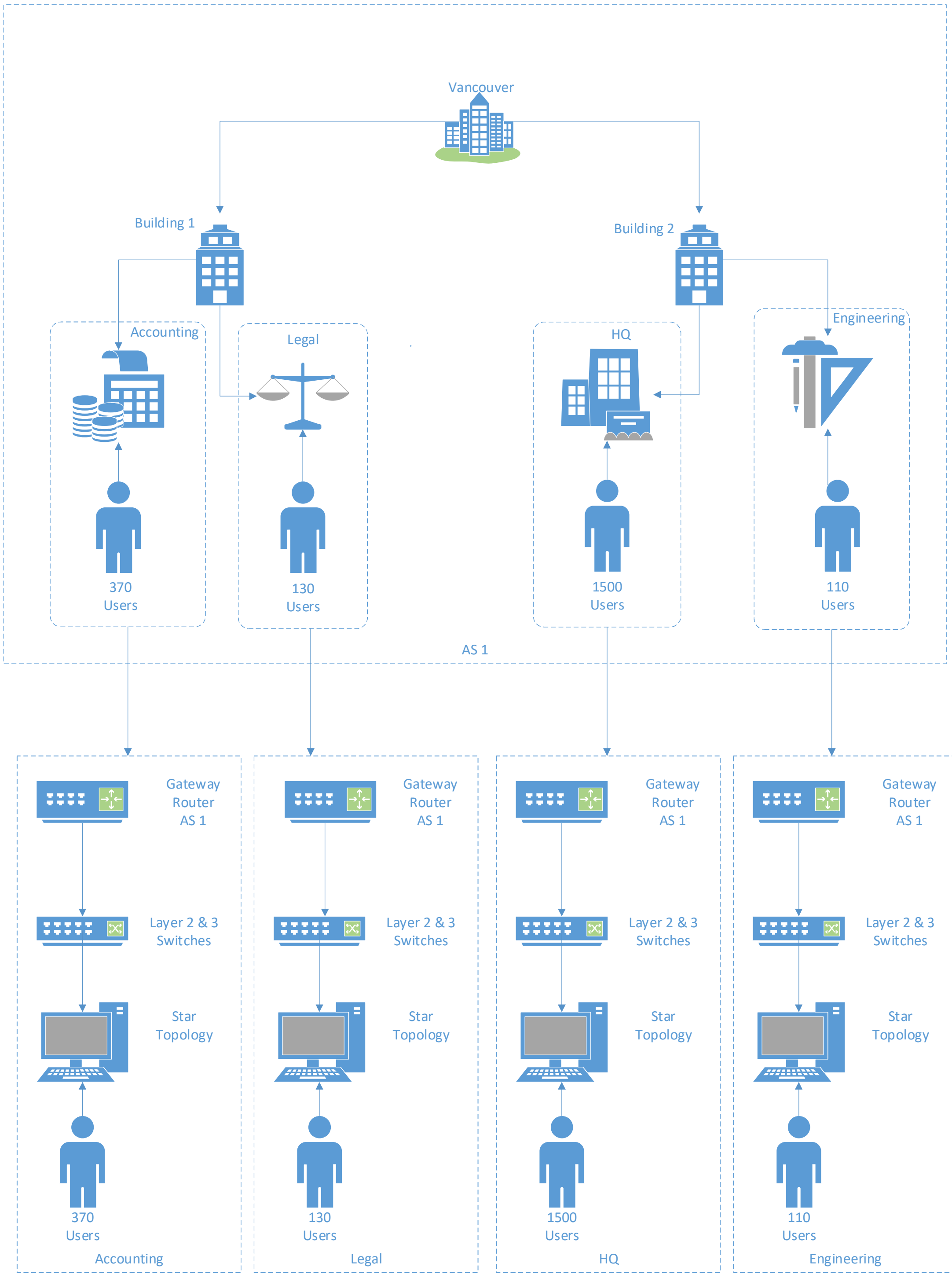


Figure. Autonomous System 1

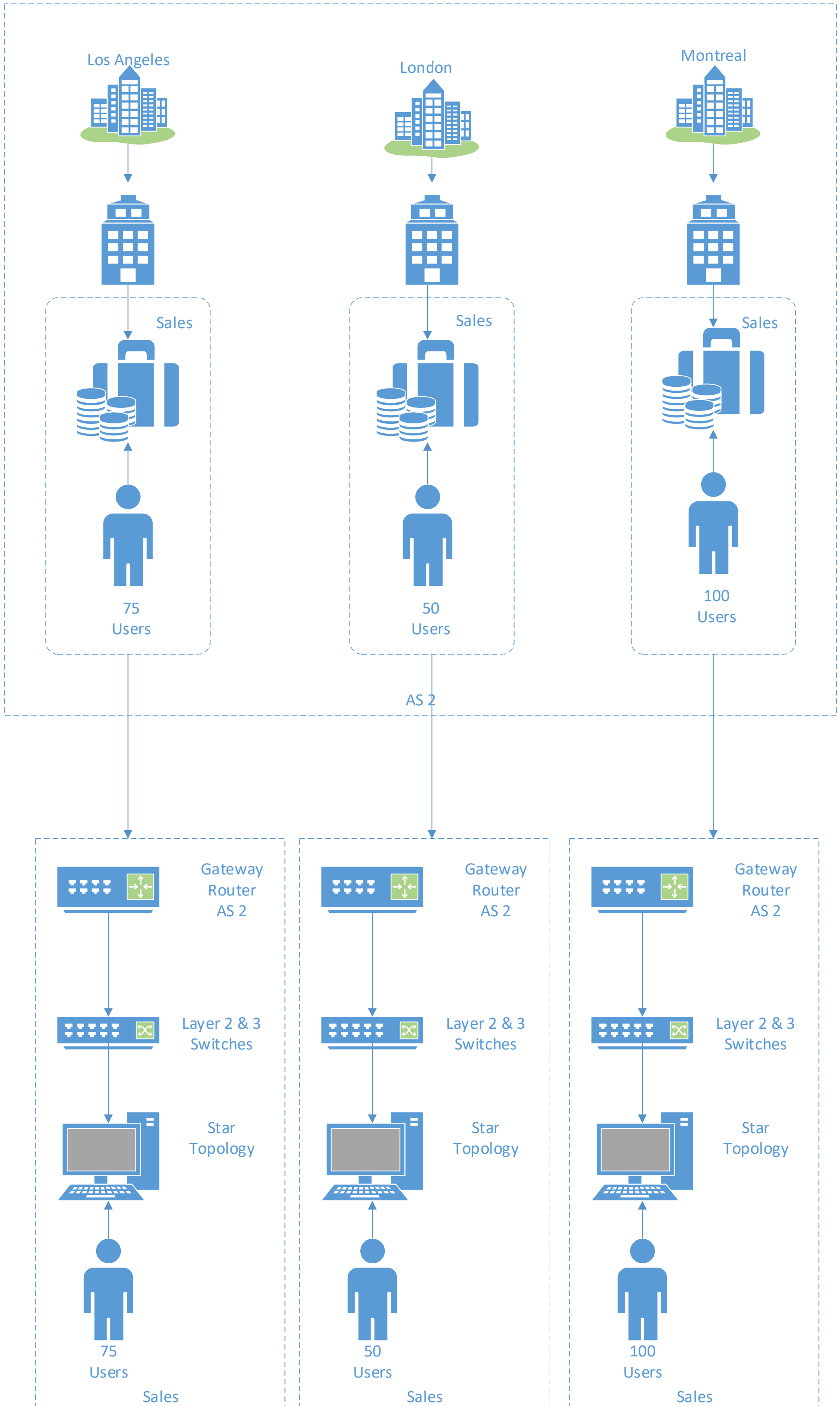


Figure. Autonomous System 2

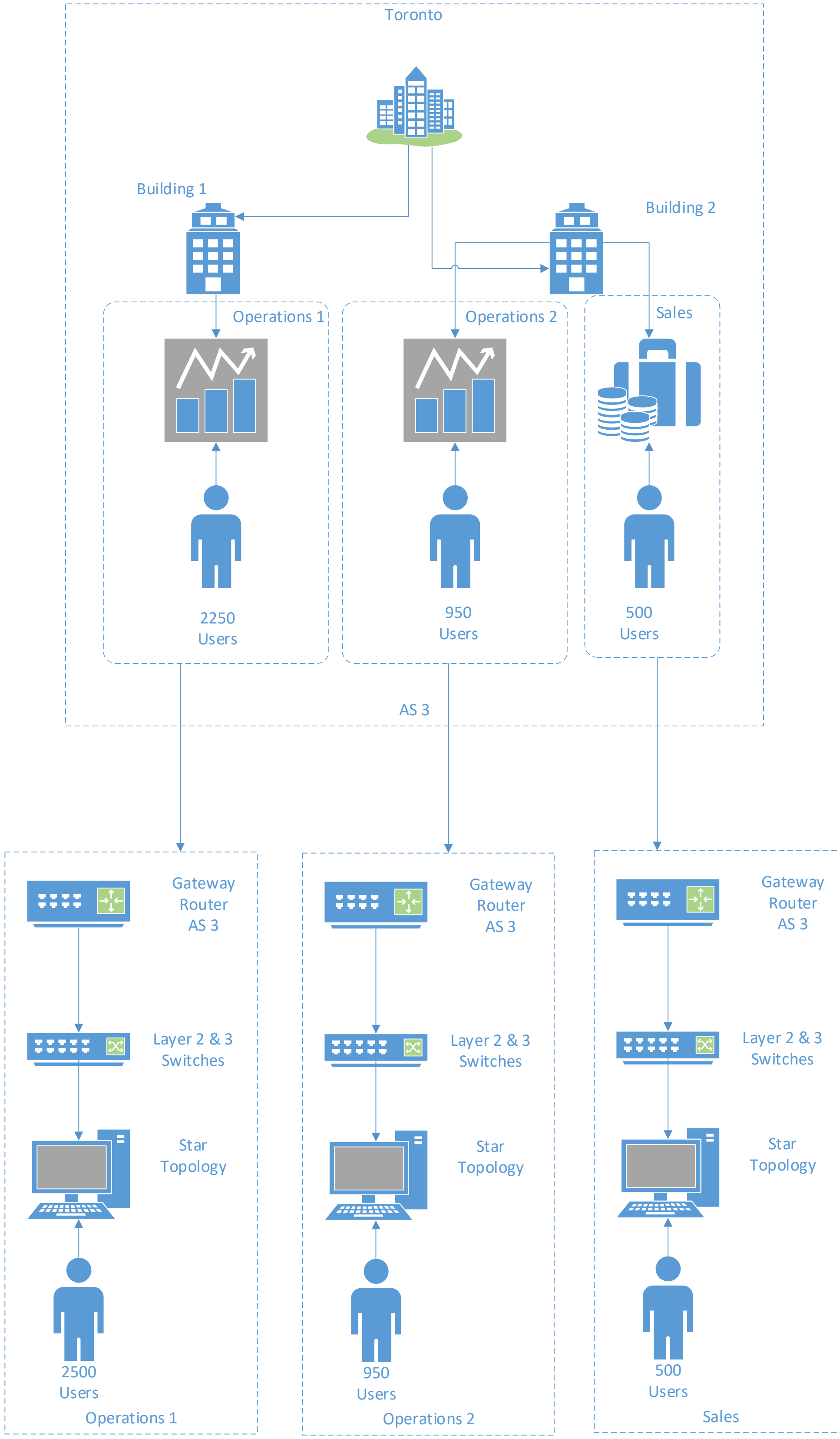


Figure. Autonomous System 3

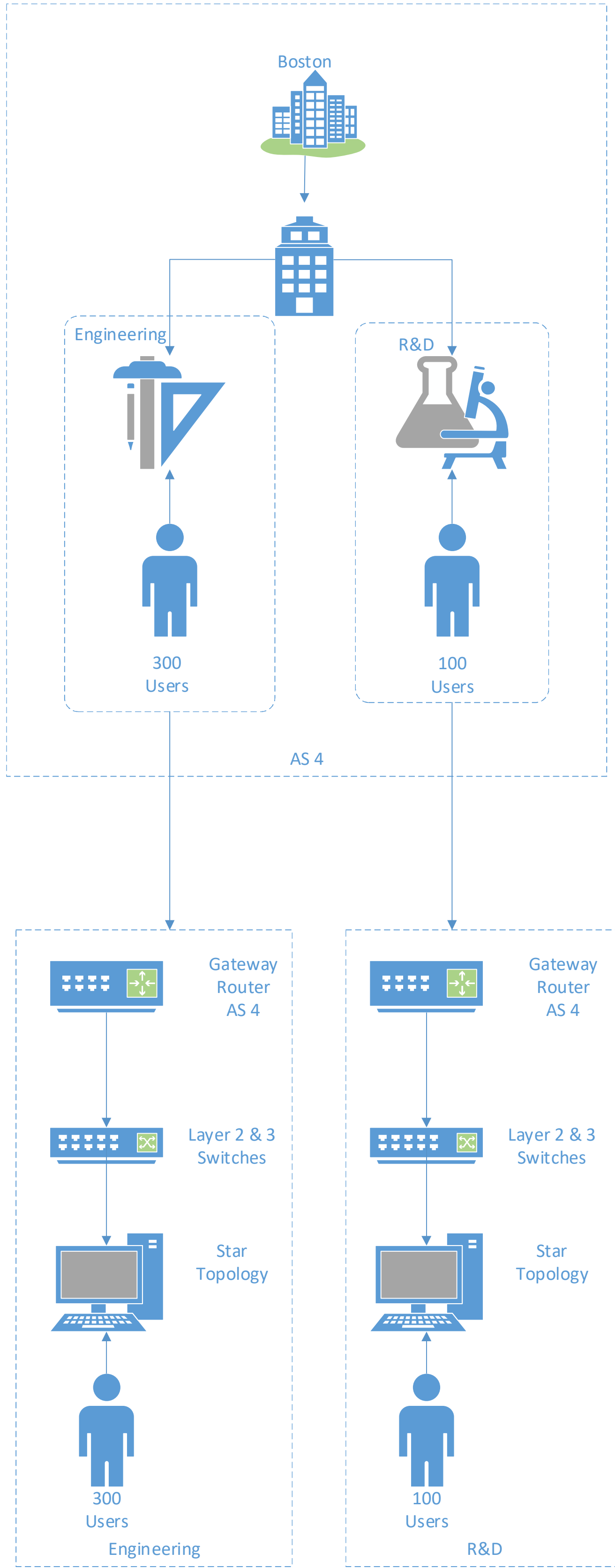


Figure. Autonomous System 4

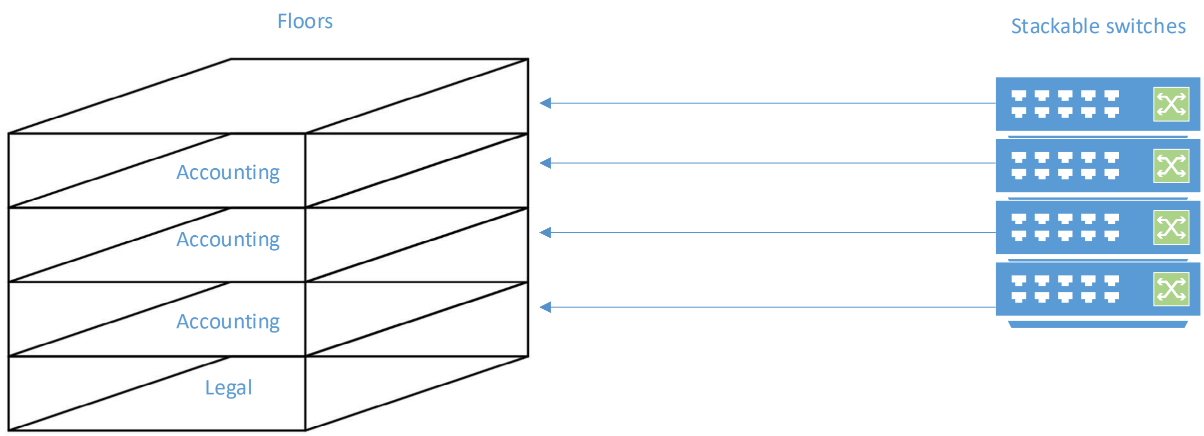


Figure. Vancouver Building Stacked Switches

*Note: We can use this stacking implementation to connect floors together for the rest of the buildings. We would also separate the stacks of a building depending on the department. This allows for subnetting to be done per department instead of grouping all connections under one subnet.

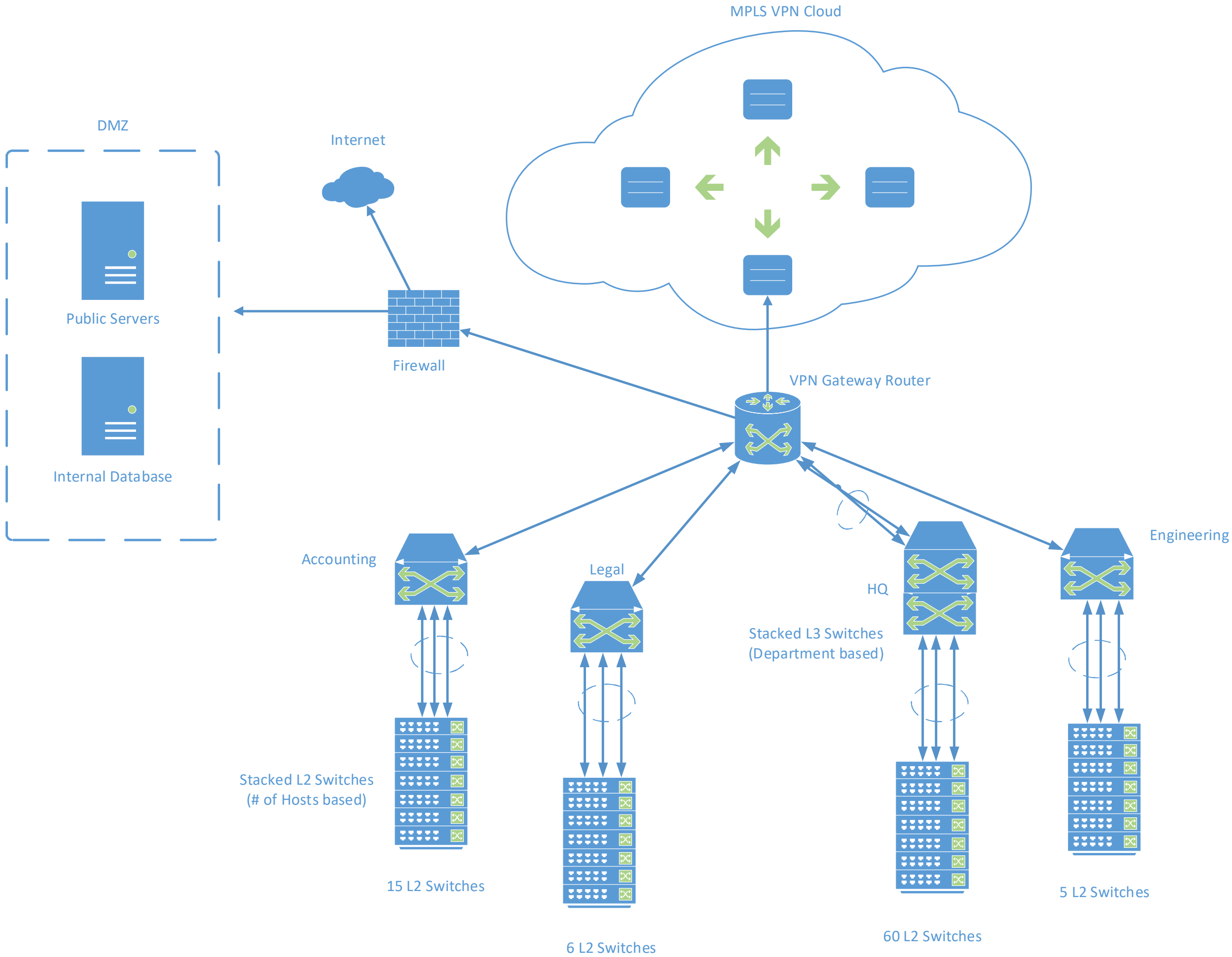


Figure. Logical Diagram for AS1

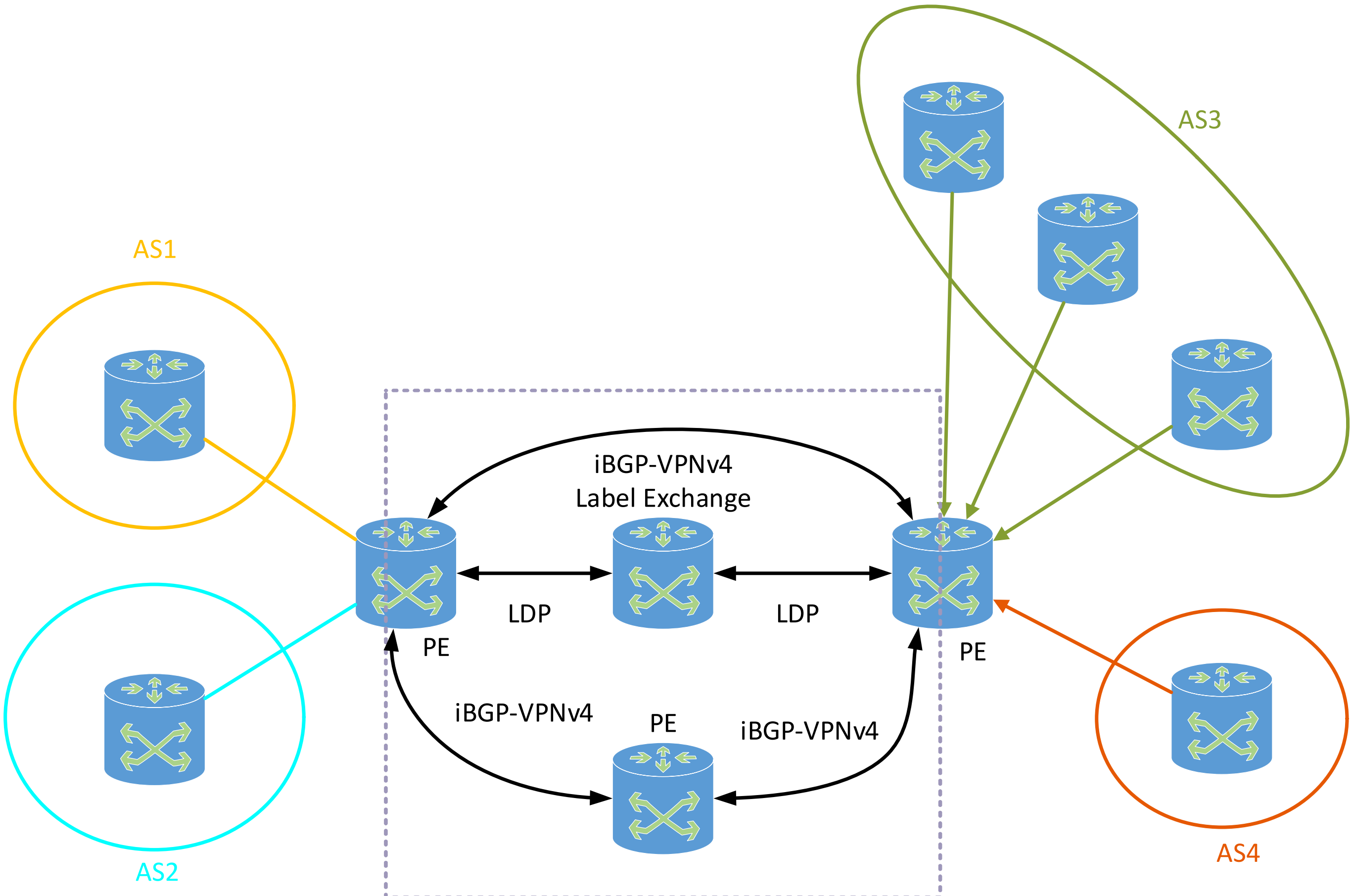
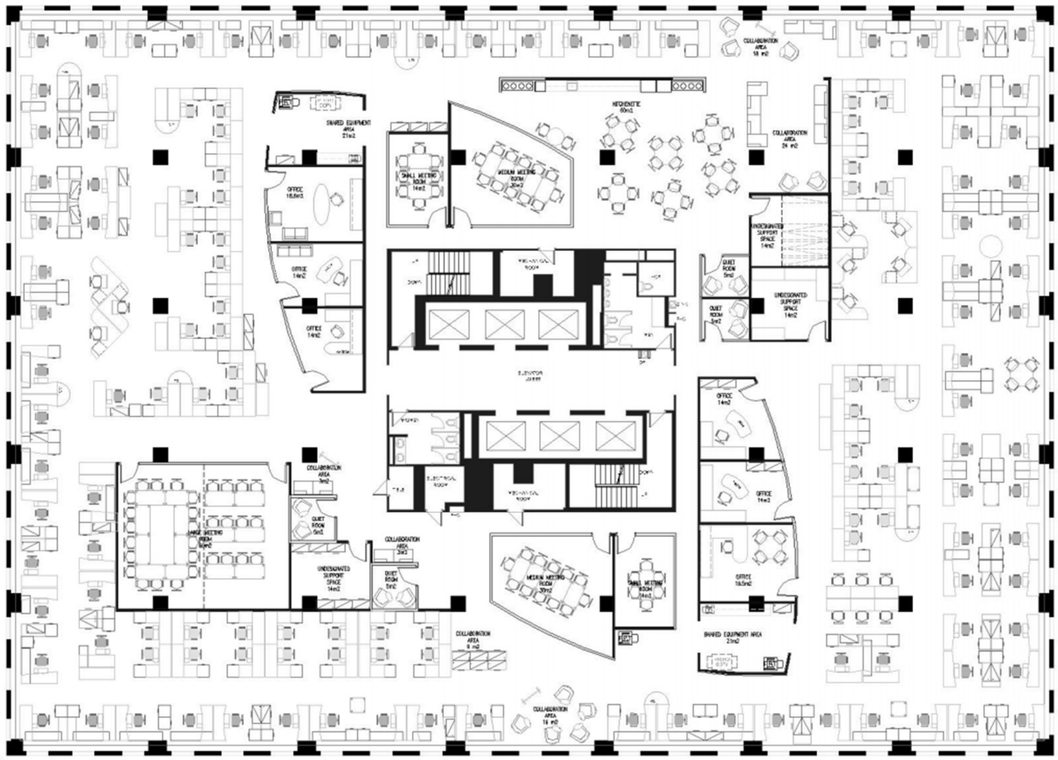


Figure. VPN Layout
Referred to: https://www.cisco.com/c/dam/global/fr_ca/training-events/pdfs/Intro_to_mpls.pdf

Floor Plan

The floor plan shown below will be used as a basis for the network infrastructure, where 152 hosts can be given connections on each floor.



Workplace 2.0 Fit-up Standards, Government of Canada. “PL1 Diagram.” *Buyandsell.gc.ca*, Government of Canada, Apr. 2012, buyandsell.gc.ca/cds/public/2013/07/24/eca34fffc77113b8f3f89360169bfa75/workplace_2_0_manual.pdf.

Building Plan

As we use the maximum hosts per floor in reference to the floor plan above, we can obtain the number of floors per building for each department.

Vancouver Building 1:

- 3 floors for Accounting
- 1 floor for Legal

Vancouver Building 2:

- 10 floors for HQ
- 1 floor for the Engineering

Los Angeles Building:

- 1 floor for Sales

London Building

- 1 floor for Sales

Montreal Building
- 1 floor for Sales

Toronto Building 1:
- 15 floors for Operations 1

Toronto Building 2:
- 7 floors for Operations 2
- 4 floors for Sales

Boston Building:
- 2 floors for Engineering
- 1 floor for R&D

Regulations

As an engineer, I would need to regulate my entire network according to the IEEE 802 standards and any other legal standards that are present. One of the active standards that should be considered would be *P802.15.12 - Upper Layer Interface (ULI) for IEEE 802.15.4 Low-Rate Wireless Networks*, and many other through the IEEE SA website. Due to time constraints, it is difficult to show the various regulations and steps I would take to completely regulate the current design such as 802.3 is for ethernet regulations, etc. Logging each device connection to various systems and networks would be an essential part for creating this network infrastructure. Referred to: https://standards.ieee.org/standard/8802-15-6-2017.html

Concerns & Security

In regards to security, we would look at the cyber security for our network. By using a DMZ area, we are eliminating a majority of public/external threats to the network. The same goes with using the MPLS VPN which privatized the entirety of the network. Access to the network should be done the encrypted passwords/two-factor authentication for an extra security measure and maybe use an anti-virus software. As for the resources and budget concerns, going the extra mile for VLANs would definitely improve resource usage and possibly reduce the number of switches that are currently being used. VLANs help with eliminating broadcasts, where high levels of traffic collision occur. Without VLANs, the network will be slower as seen from the ENEL 492 labs.

Summary

Overall, we were able to create a network from the ground up with reference to the client statement and external resources. Since we have such a simplistic and clean approach, the network components and sub-networks can be easily replicated for expansion and re-workability. By using stacked switches, we would need to consider the IEEE standards for the number of switches per cabinet/area and other network factors are needed to be considered. To make the system more redundant, VLANs would be a great alternative. Instead of have a personal database server, using 3rd party utilities seem more reliable but at the cost of an increased budget. The over design was implemented with a large consideration going into future expansion, where they may be more departments, more hosts, or additional autonomous systems. A few improvements would be to create simulations showing how the network acts with in different situations such as high traffic or heavy external traffic via the internet.