

Group members: Cameron Kerley

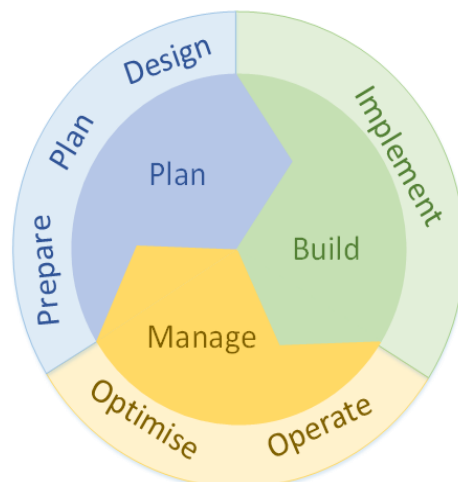
Professor: Dr. Barbara Stoops

IST-260

Coolco. design philosophy and Foundation:

Our project team has been tasked with drafting the design philosophy and core foundation of the network for a new R&D division located in Columbia, South Carolina. With that in mind our design must account for the vast geological distance between our other physical corporate locations in Amsterdam and Singapore, which will need reliable accesses to & from this new planned location. This geological separation also requires some other consideration, Singapore and frequently in countries currently evolving nationwide network infrastructures with new/currently available technologies so assessing the current state of our enterprise network will be required for many reasons.

Without question this task will require careful planning at all phases, from each team member, with that in mind we chose to employ a design methodology that focuses on a well-considered, scope oriented plan; Cisco PBM (Plan, Build, and Manage). However, we will need to adapt some of these concepts to achieve our network's primary goal.



Cisco PBM plan phase, each process followed by this team's approach:

- **Plan phase analysis:**

- Strategy and Analysis process*

- Identify employee/corporate needs and the requirements of the network.

- Outline expectations for new network functionality

- Assessment process*

- Outline critical components of the existing network, considering required services, new network functionality, consistent availability, and security.

- This will serve as the scope of our design.

- Design process*

- design the topology and implement solutions within the scope of this plan we have created, if an issue is identified in the design, start the assessment over, no short-cuts.

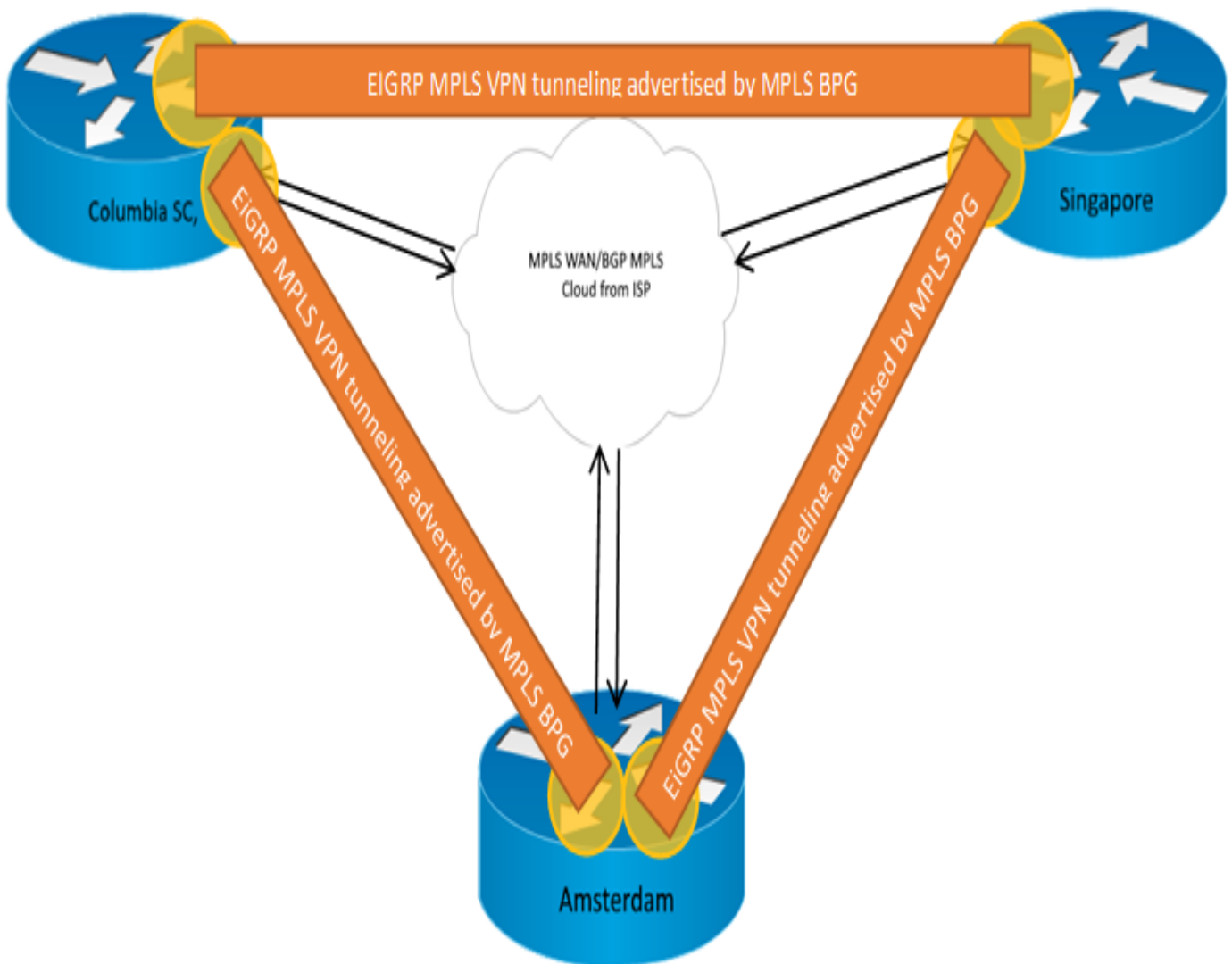
Identifying the scope of network requirements necessitates a preliminary audit of the network; its current capability's, max capacity, and ultimately the shortcomings that already exist. This assessment will prove not only vital in creating a life cycle plan for the new Colombia location, but identify areas in our current infrastructure that could benefit from upgrading, via the implementation of life cycle policy. When properly implanted a network lifecycle can help more accurately predict costs of maintaining and updating our equipment. Without question having more powerful hardware in the proper locations is a major benefit for, availability of services, increasing the network speed, and efficient allocation of monetary resources.

High level network topology:

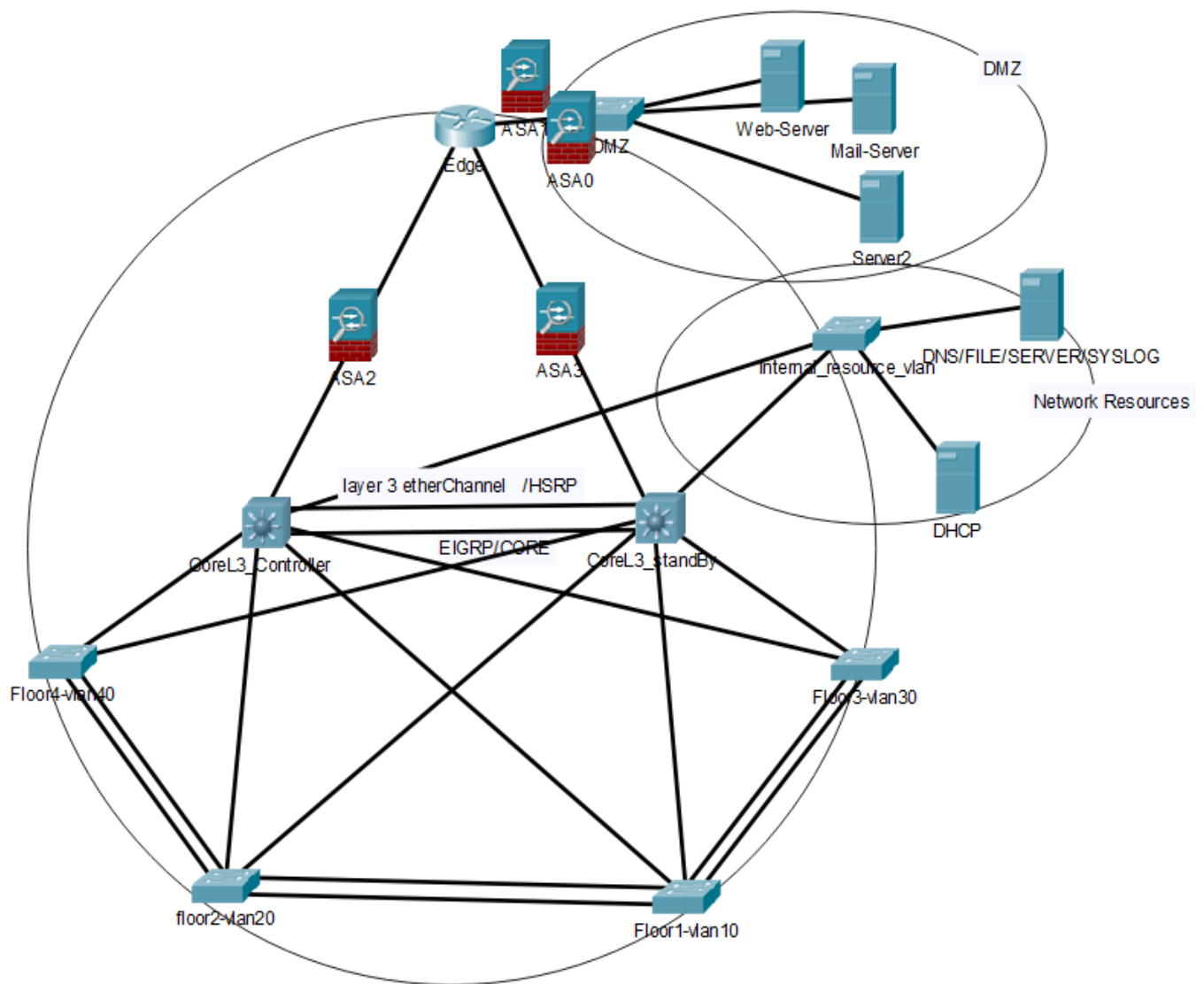
The goal when designing this campus network was to allow for a decent level of redundancy and fail over while attempting to minimize cost and maximize speed and security. With these objectives in mind our team chose a Small Enterprise campus, with a collapsed core partial mesh design. Full mesh topology is simply too expensive, even with the almost total redundancy it can provide, partial mesh provides full redundancy in critical areas at the sacrifice of full redundancy of non-critical infrastructure but at similar fault tolerance. Other issues arise when considering the need for either 48 port or likely bigger access switches just for redundant links estimated \$75,000 as compared to a partial mesh statement \$35,000. A partial mesh topology is fully capable of providing adequate levels of redundancy with the proper considerations, for a more reasonable price.

Maintaining network availability and the security of data requires extra considerations. One ASA system will check all incoming intranet to the core and one will check all internet data. Another ASA system will monitor DMZ traffic inbound to the edge router and one will monitor traffic outbound from the edge router to the DMZ. Operating these ASA's as one-way filters will greatly decrease the impact on network performance, while providing highly configurable security filters. Which can conform to each data streams individual restrictions and requirements. In conjunction with strict access control lists no packet should ever be out of place or unscanned.

What considerations are necessary for adequate redundancy in a partial mesh topology? First recognize that full mesh concepts can be applied at specific layers in our design to ensure constant availability to vital network resources, services, and company data. The distribution layer will be full mesh and take priority for the fastest links available. Use MPLS for WAN primary and back up with EIGRP MPLS, advertised and propagated through BPG MPLS.

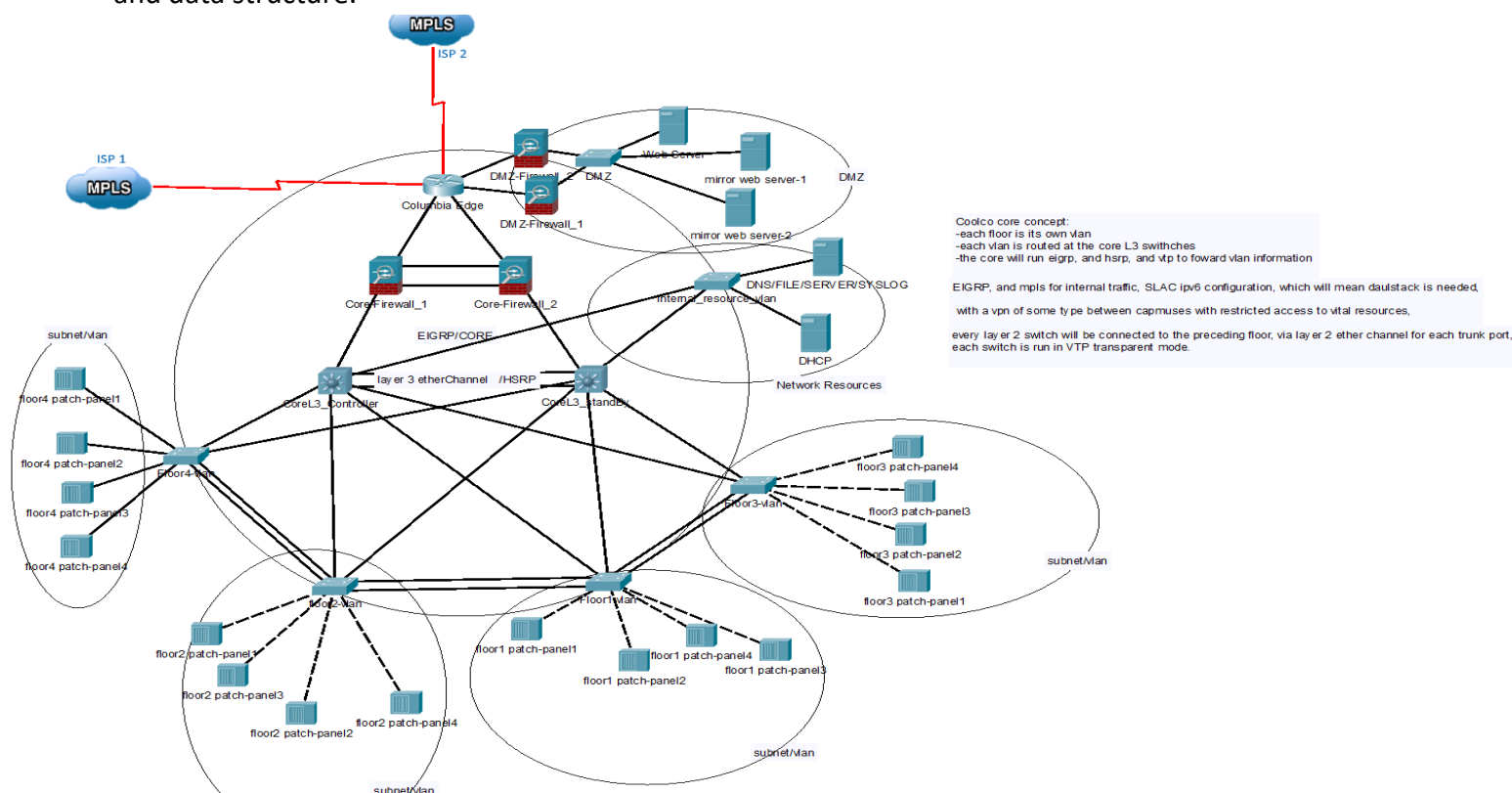


Partial mesh is implanted at the access layer, each floor is a network cluster with an associated VLAN, each VLAN also serves as a subnet with all layer 3 routing occurring at the 2-core layer 3 switches SVI's. The layer 3 switches are responsible for access layer and inter VLAN routing with EIGRP. HSRP will be used on a layer 3 ether-channel the virtual router will serve as the default gateway for our SVI's. Each access switch will have at least one link to each core L3 switch, and a layer two trunk ether-channel between each descending floor from the data center.



All the switches will operate in VTP transparent mode receiving basic VLAN configurations from the core. The internal_resources_vlan has been segmented from other portions of the network for security reasons. This VLAN houses vital network resources such as DNS and DHCP services, resources commonly targeted by AVT's for man in the middle attacks, DHCP blackholes, DNS spoofing etc. which will require a higher level of control, by restricting its accessibility with ACL's.

There is one last major design choice we can make to ensure uptime and redundancy at the same time. The Columbia location will have 2 separate fiber lines from different service providers. Also known as a multihomed network, even if our primary providers link goes down, we can still communicate with and host services for our internal network, through BGP MPLS, which will be configured on both ISP links. The following image represents the logical topology and data structure.



Recommended equipment/hardware:

L2 Switches:

We decided to use Cisco Catalyst 2960-X 48 GigE PoE 370W switches. These can be configured to run as L2 with dual stack enabled and will provide power over ethernet to IP phones. We are using the fiber SFP ports for connections between switches, and to the Edge Router. These switches will set us back about \$1410 per switch.



L3 Switches:

For layer 3 We decided to use Cisco Catalyst 9200 C9200L-48P-4G Layer 3 Switches. Two of these devices will serve as our core, running EIGRP and HSRP to load balance and provide failover in case of device or interface failure. We will prioritize using the fiber links to each switch except for the internal resources VLAN. These switches will not require PoE as our access layer switches are all PoE capable, drastically reducing the price of this series of switch. Each of these will cost us \$3,000 - \$4,000.









For Public Access Point:



For Public access, we will use a single UniFi Enterprise Wifi AP, located in the entry lobby. Devices that connect to this will be restricted to only acceptable internet sites and must sign off on AUP portal before use. This can be bought on Amazon for as low as \$80.

For Firewall:

We chose to use clustered Cisco ASA's as our firewall solution. We have decided to be extremely security aware and use four total firewall devices. While it can be hard to justify such an investment, nothing is more costly than losing or leaking vital company, employee, or customer data.

Solutions Ranging from SMB to Large Enterprise					
	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550
					
Target Market	Teleworker / Branch Office / SMB	SMB and SME	Enterprise	Medium Enterprise	Large Enterprise
List Price (CDN\$)	Starting at \$702	Starting at \$4,124	Starting at \$9,434	Starting at \$20,054	Starting at \$23,594
Performance Max Firewall Max Firewall + IPS Max IPSec VPN Max IPSec/SSL VPN Peers	150 Mbps Future 100 Mbps 25/25	300 Mbps 300 Mbps 170 Mbps 250/250	450 Mbps 375 Mbps 225 Mbps 750/750	650 Mbps 450 Mbps 325 Mbps 5000/2500	1.2 Gbps N/A 425 Mbps 5000/5000
Platform Capabilities Max Firewall Conns Max Conns/Second Packets/Second (64 byte) Base I/O VLANs Supported HA Supported	10,000/25,000 3,000 85,000 8-port FE switch 3/20 (trunk) Stateless A/S (Sec Plus)	50,000/130,000 6,000 190,000 5 FE 50/100 A/A and A/S (Sec Plus)	280,000 9,000 320,000 4 GE + 1 FE 150 A/A and A/S	400,000 20,000 500,000 4 GE + 1 FE 200 A/A and A/S	650,000 28,000 600,000 8 GE + 1 FE 250 A/A and A/S

Presentation_ID: © 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

13

Overall Network security:

To protect our network physically and virtually, we have implemented several layers of security. For virtual protection we are utilizing four ASAs with half clustered at the DMZ and the other half clustered at the Edge. We will actively have all of the ASAs running in the respective inbound and out bound configuration, each will maintain a copy of the other filter configuration for redundancy. To protect our data center physically from any intrusions or security breaches we will utilize cameras, hardware locks on doors, keypad entry to sensitive areas, and a mantrap in the datacenter. The cameras will be set to back up their video onto the security servers which will keep the video from floors one-three stored for 30 days and data center for 90 days.

Since no firewall is perfect the ACLs inside our network either blocks or permits traffic depending on what ports, protocols, and IP addresses are in the packet. For example, traffic originating outside the network will be blocked by both the firewall and our ACLs so that it cannot access our core or distribution layer and remains quarantined in our DMZ. First, support the ASA's by controlling the logical flow of data, so it remains in and outbound with ACL's. Second, the configuration of vlans, protect our network by segmenting our broadcast domains so that if there is an intrusion or error in the network it has isolated effect on the other 11 vlans and possible critical infrastructure. Finally, logging events in our network monitoring tool, SolarWinds, we can look for patterns or errors in the data stream before they impact the network. Conveniently, it also serves as a network baseline, used as a control for comparison showing any activity outside of this "baseline". To facilitate this, use SNMP traps for each switch, router, and firewall then send the data to SolarWinds, to be logged and analyzed.

Website, web conferencing, and email:

Our choice of web server to host our website is a NGINX web server. We chose this web server over the leading Apache web servers due to the security gaps present in almost all Apache based web servers due to SQL and MySQL. NGINX servers can take on many different roles such as being a reverse proxy server for the HTTP, HTTPS, SMTP, POP3, and IMAP protocols, a load balancer and an HTTP cache, our web server will be running HTTPS protocols so that our data is encrypted even on company intranet. We also gain the capacity to host our intranet from the data center. Allowing all 3 campuses, network folder sharing, and remote host capabilities given the proper credentials from the CIA philosophy.

As for our email and web conferencing we made the decision to use office365. By using Office365 we do not have to worry about hosting or securing email servers. However, using outlook comes with inherent risk. The possibility of someone copying or spoofing your outlook domain is astronomically higher. The chance of whaling and phishing increase drastically, security breaches server side are not under your control. However not hosting an email server prevents us from being targeted by the most common security threats and source of breaches, like improperly formatted SQL queries that happen to return username and password tables from the database. One less public facing device that requires the highest level threat monitoring.

IP Addressing scheme:

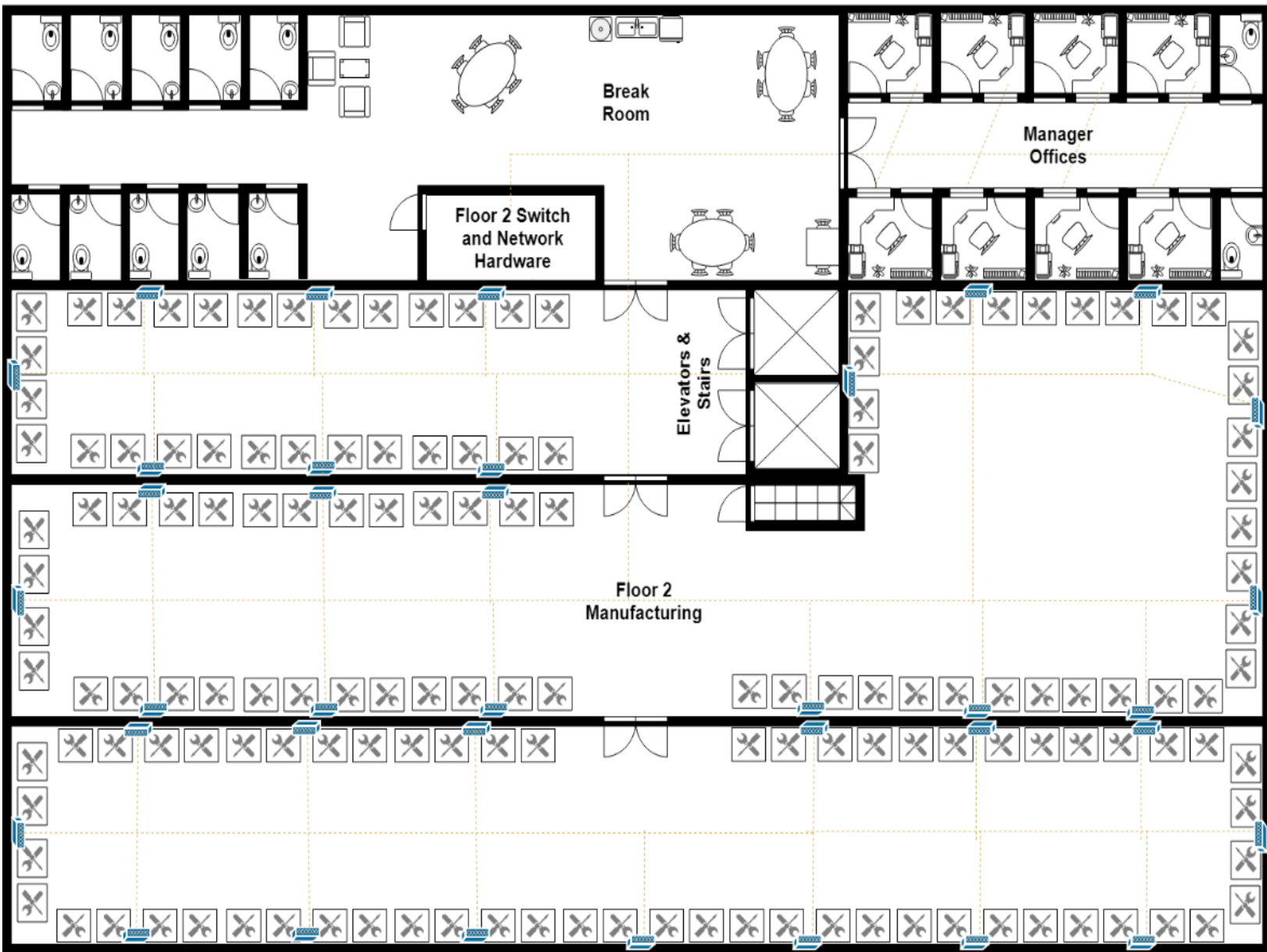
Addressing Table				
Equipment/ Location	Interface	IP Address/Prefix	Default Gateway	IPv6 Address/Prefix
Cisco / COLUMBIA (From PE)	S0/0/0	203.125.28.50/29	203.125.28.49/29	
		STATIC NAT ASSIGNED TO DMZ EQUIPMENT		
Cisco / COLUMBIA (To DMZ)	G0/1	172.16.1.1/24	N/A	2001:db8::ac10:101/96
WEB SERVER	NIC	172.16.1.11/24 (203.125.28.57)	172.16.1.1/24	2001:db8::ac10:10b/96
OFFICE 365 SERVER	NIC	172.16.1.12/24 (203.125.28.58)	172.16.1.1/24	2001:db8::ac10:10c/96
DHCP Server	NIC	172.16.1.13/24 (203.125.28.59)	172.16.1.1/24	2001:db8::ac10:10d/96
DNS Server	NIC	172.16.1.14/24 (203.125.28.60)	172.16.1.1/24	2001:db8::ac10:10e/96
COLUMBIA - 1ST FLOOR	VLAN 101	10.100.1.0/24	10.100.1.1/24	2001:db8::a64:101/96
COLUMBIA - 2ND FLOOR	VLAN 102	10.100.2.0/24	10.100.2.1/24	2001:db8::a64:200/96
COLUMBIA - 3RD FLOOR	VLAN 103	10.100.3.0/24	10.100.3.1/24	2001:db8::a64:300/96
COLUMBIA - 4TH FLOOR	VLAN 104	10.100.4.0/24	10.100.4.1/24	2001:db8::a64:400/96
COLUMBIA - VOIP	VLAN 105	10.100.5.0/24	10.100.5.1/24	2001:db8::a64:500/96
COLUMBIA - MARKETING	VLAN 106	10.100.6.0/24	10.100.6.1/24	2001:db8::a64:600/96
COLUMBIA - FINANCE	VLAN 107	10.100.7.0/24	10.100.7.1/24	2001:db8::a64:700/96
COLUMBIA - HR	VLAN 108	10.100.8.0/24	10.100.8.1/24	2001:db8::a64:800/96
COLUMBIA - GUEST WIFI	VLAN 109	10.100.9.0/24	10.100.9.1/24	2001:db8::a64:900/96
COLUMBIA - SECURITY	VLAN 110	10.100.10.0/24	10.100.10.1/24	2001:db8::a64:a00/96
COLUMBIA - IT (MANAGEMENT)	VLAN 199	10.100.11.0/24	10.100.11.1/24	2001:db8::a64:b00/96

Wiring Scheme and floor plan:

-Floor 1-



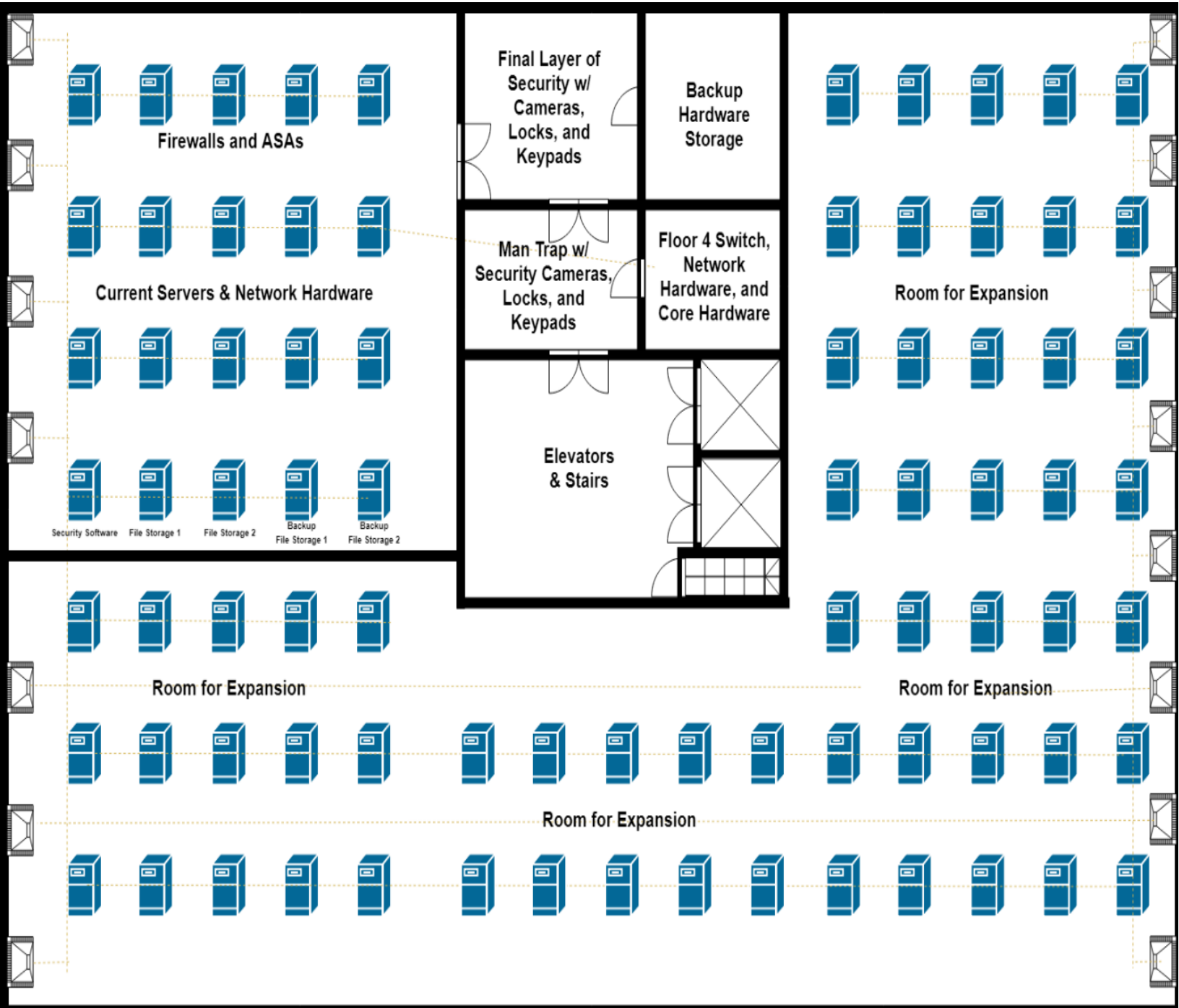
-Floor 2-



-Floor 3-



-Data Center-



Conclusion; benefits, drawbacks and future:

Opening this new office space will be a massive undertaking, but such an expansion is an exciting business venture for Coolco. As the current plan stands this new branch will employ 300 people on startup, with plans for growth. This location will also house vital confidential employee data, like payroll/health care, and will be the host for our corporate website both internally and over the web. This requires us to be extremely mindful of our network reliability/uptime, resilience to failure/loss of data, and strong security policy's.

In order to accomplish these goals our team employed ideas from the Cisco Plan Build manage design philosophy. However, our team realized these methods were simply concepts or guidelines requiring more detail to help our network achieve its goals. With design philosophy in place the team worked to assemble a detailed plan with clear objectives and well-defined scopes of responsibility for each portion of the network. After resolving any foreseeable design flaws, we start constructing the data flow for the network alongside basic structure. Finally, when the logical topology was complete, we could begin to identify the network equipment and software capable of providing the infrastructure the design requires.

In conclusion our design attempts to deliver an extremely secure network, that is always available, at a consistent speed. Our decision to primarily use Cisco network equipment is not the most cost effective, however Cisco makes quality products that can be up graded and customized with modules to suit your needs. EIGRP is a Cisco proprietary protocol and will be essential to our network by providing a wide variety of k metrics or weights that can be configured to fully control the flow of data through our network on a per link bases when

necessary. We decided security was a top priority at a higher cost bases; because ensuring the integrity of our infrastructure and data is vital. Maintaining a CIA protocol is paramount for securing data and maintaining trust of both customers and employees. Since we plan to expand our data center as company needs grow, its only logical to attempt at providing robust security day one. There is no sugar coating it, the starting investment our network will require is relatively high but not without purpose or consideration of each alternative. Guaranteed confidentiality, availability and expandability of this network creates a dedicated line between us, our customers, and a shared reliable network between our international campuses.