NYU | TANDON SCHOOL OF ENGINEERING

CS-GY 6834: Computer Networking

VITA PHARMA-NETWORK REDESIGN

Fall 2017, December 17, 2017

Under the Guidance of:

Professor Rafael Portnoy

By:

Akshat Tyagi	(at3761)
Avaiyang Garg	(ag6026)
Binal Modi	(bjm470)
Rajeev Joshi	(rj1234)
Shrey Gupta	(sg5085)

TABLE OF CONTENTS

Chapter 1
INTRODUCTION

Every minute counts in a company and reliable networks are a powerful tool for boosting productivity and encouraging information sharing. The success of a company is measured by its ability to retain and expand its client base by providing fast seamless and reliable delivery of its services.

Today a company is not restricted to just one place or country but are expanding their offices in major cities around the globe, and for this a reliable and secure network foundation is of paramount importance. This not only helps in the interoperability of the work but also helps in saving money and time and brings the services closer to the client.

The pervasive nature of Internet has forced large companies to design and implement a robust scalable and reliable network to cater to the needs of the consumers all around the world. To implement a new network we need to understand and evaluate the scope of the network design. This can be done by creating a network diagram which would then serve as a blueprint to actually implement the network.

The network design includes:

- Designing a logical map of the network.
- Developing an IP addressing schema.
- Defining the security mechanism for protecting the data.
- Determining the type, quantity and location of various network devices.
- Determining the throughput and required bandwidth according to the office needs.

Chapter 2
STATUS QUO OF THE COMPANY

Vita Pharma is a global pharmaceutical company, and has its main office in New Brunswick, New Jersey. It also has three regional Headquarters in London UK, Sao Paulo Brazil and Singapore. There are seven different departments at each of these locations that help in maintaining the company's logistics. The departments are:

- Accounting/ Finance
- Human Resources
- Legal
- Corporate IT
- Facilities Management
- Executive Management
- Strategy Groups

The company develops its own medicine at three different research centers located at Zurich, New York, and Melbourne. The manufacturing of its products take place in six different locations; these include Canada, Chile, United Arab Emirates, Israel, China, and Malaysia. The sales organisation of Vita Pharma are highly distributed among all the major geographical areas (Americas, Europe/Middle East and Asia Pacific). In addition to all those, it has three software development centers in Russia, India and Pakistan where the employees are working on multiple client-server and web-based software projects to support global operations, supply chain, drug research and development management and many others.

Chapter 3
GOAL OF THE NETWORK REDESIGN

The main aim is to redesign Vita Pharma's network to meet the company's future goals. This includes a significant expansion and better service for their users. Vita Pharma also plans to decrease the time-to market for their products and their increase global workforce.

3.1 Problem

These are the ongoing complaints in the Vita-Pharma:

- Slow access to files
- Slow email delivery
- Poor voice quality
- Application crashing

3.2 Objective

The following are the objectives for network redesign:

- Redesign the global network.
- Develop a protocol stack.
- Analyse the bandwidth requirements.
- Develop a new IP addressing schema.
- LAN design, which includes the local LANs.
- Identify the number of data centers, location and functionalities.
- Identify the types of servers and their relevance with respect to the firm.
- Design a secure system which provides security for the on site systems, data centers, servers and communication link.

3.3 Analysis

3.3.1. Main Office and Regional Headquarters:

- Seven departments.
- 1 Main Headquarter, 3 Regional Headquarters.
- Total Number of employees: 500
- Specifications:
    - HR applications are used to manage resources, which contain personally identifiable information; this means that the HR departments have to be secured.
    - Finance and Accounting use Financial Management System, which contains specific financial data for the entire organization; this means that the Finance and Accounting departments have to be secured.

- Treasury Sub-department requires access to trading markets to invest some of the profits in OTC commodities and stocks. This means that the Treasury sub-departments have to be secured and have to be supplied with a fast and reliable network.

3.3.2. Global Research Centers:

- 3 Research Centers
- Total Number of Scientists: 200
- Specifications:
  - R&D uses special analytics and product development software, which is highly confidential. This means that the Research and Development Departments have to be secured.

3.3.3. Manufacturing and distribution Facilities:

- Total Number of offices: 6
- Total Number of employees: 2000

3.3.4. Sales Organizations:

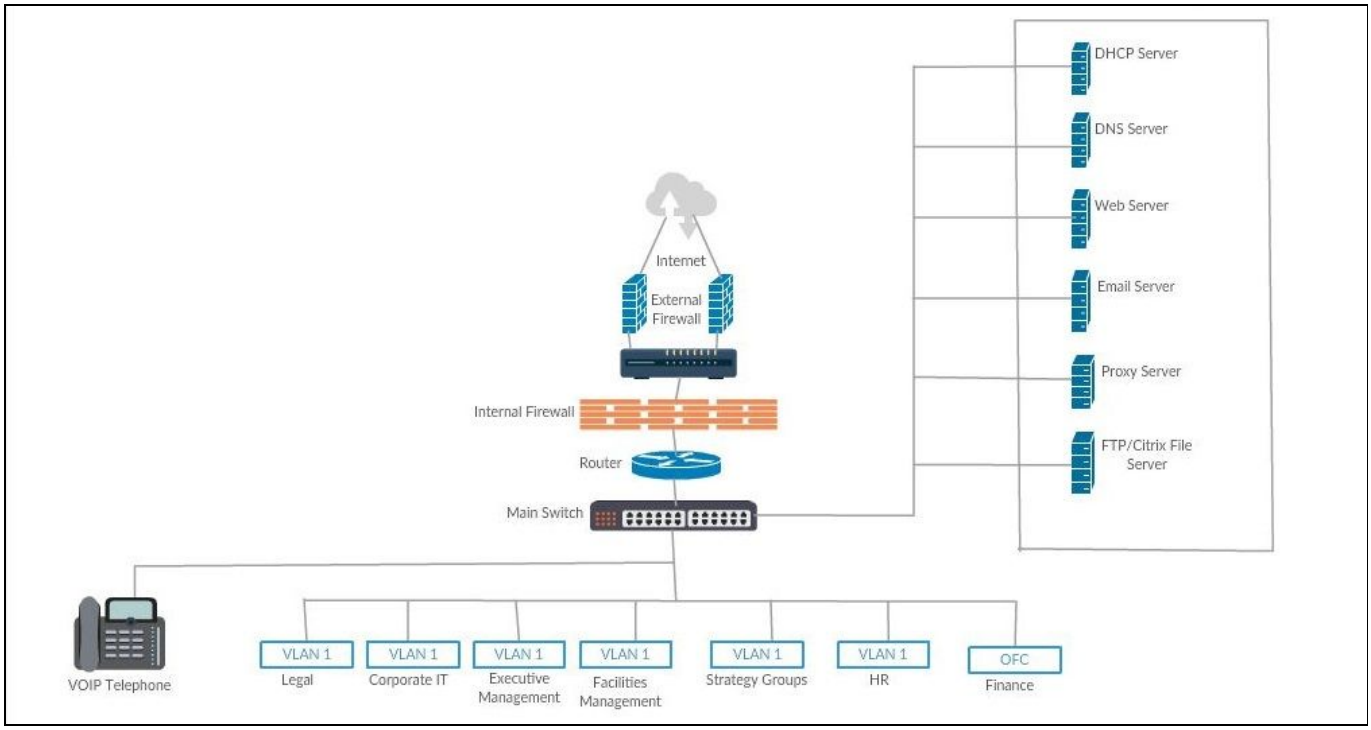
- Total Number of offices: 60 (20 in each of America, Europe/Middle East and Asia-Pacific)
- Total Number of employees: 1000
- Specifications:
  - The sale offices are highly distributed
  - Most the employees within sale are mobile.
  - Sales and Marketing is managed through a suite of applications, which contain customer specific data. This means that the Sales Organizations have to secure.

3.3.5. Software Development Centers:

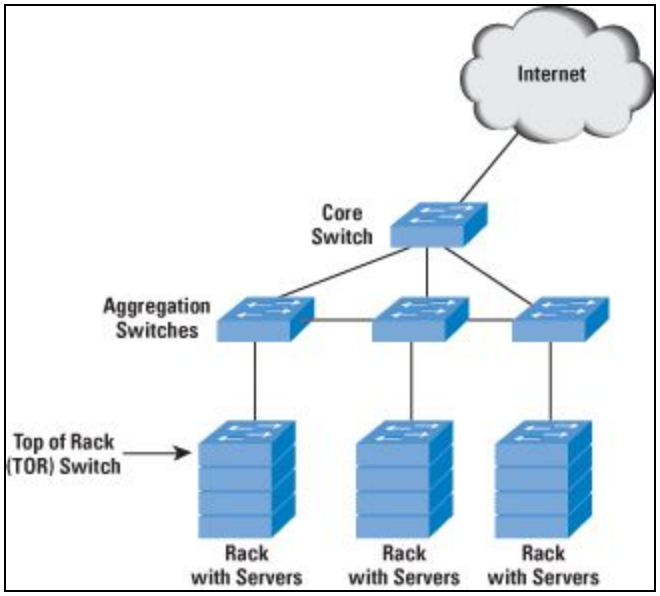
- Total Number of offices: 3
- Total Number of employees: 300
- Specifications:
  - Work on multiple client-server and web-based software projects to support global operations, supply chain, drug research and development management and many others. Since we are using VDI Citrix all the software updates and patching will done in the data centers. This means that the software development organizations have to be connected to the other data centers.

Chapter 4
PROPOSED SYSTEM DESIGN

4.1 Diagrams



Main Office: LAN Design



Data Center Architecture

4.2 Private Networks

We will assign private network to all the offices in Vita Pharma. Also, the number of employees are assumed to be increasing every year since the company is likely to be expanding, so keeping this in mind we will design our private network. Let us assume that there is increase in the number of employees by at least 80% of the present value in 4-5 years, whereby each year the employees increase by 15%. With the help of DHCP, we will assign the IP addresses to each user dynamically. Moreover, we will provide a dedicated subnet to printers, faxes, voice over IP telephone and other devices in-order to minimize the interference by these devices.

4.2.1. Main Office and Headquarters:

- Total number of employees: 500
- Assuming a Growth Rate of 15% per year, total number of employees after 5 years (80% growth)= 500 + 400 = 900
- Number of employees per office: 900/4 = 225. (Assuming equal employees in all offices)

Assuming 125 employees initially and 15% increase every year accounting to a total of 225 in 4-5 years, if we use /23 subnet mask, it will provide us with a total of 512 IP addresses out of which 225 can be used for office employees and remaining 285 addresses can be used for office devices like printers, scanner, voIP, faxes etc. The first and last IP in each subnet will be used for subnet address and broadcast address respectively. Here we are assuming that each person uses a telephone and one in ten people use a printer and scanner.

We will use the address range for:

Locations	**IP Address Range**	
Main Office in New Jersey, USA	172.20.0.1	172.20.1.254
Head-Quarter in London, UK	172.20.2.1	172.20.3.254
Head-Quarter in Sao Paulo Brazil	172.20.4.1	172.20.5.254
Head-Quarter in Singapore	172.20.6.1	172.20.7.254

4.2.2. Global Research Centers:

- Number of employees: 200
- Assuming a Growth Rate of 15% per year, total number of employees after 5 years (80% growth) = 200+160 = 360
- Number of employees per office: 360/3 = 120. (Assuming equal employees in all offices)

Assuming 67 employees initially and 15% increase every year accounting to a total of 120 in 4-5 years, if we use /24 subnet mask, it will provide us with a total of 256 IP addresses out of which 120 can be used for office employees and remaining 134 addresses can be used by the devices like printers, voIP, faxes etc. The first and last IP in each subnet will be used for subnet address and broadcast address respectively.

We will use the address range for Research center in :

Locations	**IP Address Range**	
Zurich	172.20.8.1	172.20.8.254
New York	172.20.9.1	172.20.9.254
Melbourne	172.20.10.1	172.20.10.254

4.2.3. Manufacturing and Distribution:

- Number of employees: 2000
- Assuming a Growth Rate of 15% per year, total number of employees after 5 years (80% growth) = 2000+1600 = 3600
- Number of employees per office: 3600/6 = 600 (Assuming equal employees in all offices)

Assuming 334 employees initially and 15% increase every year accounting to a total of 600 in 4-5 years, if we use /22 subnet mask, it will provide us with a total of 1024 IP addresses out of which 600 can be used for office employees and remaining 422 addresses can be used by the devices like printers, voIP, faxes etc. The first and last IP in each subnet will be used for subnet address and broadcast address respectively.

We will use the address range for Manufacturing and Distribution in:

Locations	**IP Address Range**	
China	172.20.11.1	172.20.14.254
Israel	172.20.15.1	172.20.18.254
Chile	172.20.19.1	172.20.22.254
Canada	172.20.23.1	172.20.26.254
UAE	172.20.27.1	172.20.30.254
Malaysia	172.20.31.1	172.20.34.254

4.2.4. Sales Organization:

- Number of employees: 1000
- Assuming a Growth Rate of 15% per year, total number of employees after 5 years (80% growth) = 1000 + 800 = 1800
- Number of employees per office: 1800/60 = 30 (Assuming equal employees in all offices)

Assuming 17 employees initially and 15% increase every year accounting to a total of 30 in 4-5 years, if we use /26 subnet mask, it will provide us with a total of 64 IP addresses out of which 30 can be used for office employees and remaining 32 addresses can be used by the devices like printers, voIP, faxes etc. The first and last IP in each subnet will be used for subnet address and broadcast address respectively.
We will use the address range for all 20 offices of Sales Organization in :

Locations	**IP Address Range**	
America	172.20.35.1	172.20.39.254
Europe/Middle East	172.20.40.1	172.20.44.254
Asia Pacific	172.20.45.1	172.20.49.254

4.2.5. Software Development Centers:

- Number of employees: 300
- Assuming a Growth Rate of 15% per year, total number of employees after 5 years (80% growth) = 300 + 240 = 540
- Number of employees per office: 540/3 = 180 (Assuming equal employees in all offices)

Assuming 100 employees initially and 15% increase every year accounting to a total of 180 in 4-5 years, if we use /23 subnet mask, it will provide us with a total of 512 IP addresses out of which 180 can be used for office employees and remaining 310 addresses can be used by the devices like printers, voIP, faxes etc. We are taking 310 additional addresses because many more extra devices will be used for the development purposes.
We will use the address range for Software Development Center in:

Locations	**IP Address Range**	
India	172.20.50.1	172.20.51.254
Pakistan	172.20.52.1	172.20.53.254
Russia	172.20.54.1	172.20.55.254

4.3 Public Networks

Public network is a type of network where anyone can connect to some other network, in contrast to the private network, there is generally very few or no restrictions applied to public networks. We use static addressing to connect to the public networks. Total number of routers in each office depends on the employee to router ratio. To keep a balance between the congestion on a router and total resources consumed we take router to employee ratio as 1:40.

4.3.1. Main Office and Headquarters:

We have assumed that for every 40 employees there is 1 router.
We have a total of 500 employees initially which will be increased upto 900 employees in Main office and 3 Headquarters. Since, each office comprise of 225 employees, so we will use 6 routers in each of these offices.

We will use public address range for:

Locations	**IP Address Range**	
Main Office, New Jersey	156.1.1.1	156.1.1.6
Head-Quarter in London	156.1.1.7	156.1.1.12
Head-Quarter in Brazil	156.1.1.13	156.1.1.18
Head-Quarter in Singapore	156.1.1.19	156.1.1.24

4.3.2. Global Research Centers:

We assume that for every 40 employees there is 1 router.
We have a total of 200 employees initially which will be increased upto 360 employees in 3 office locations.. Since, each office comprise of 120 employees, so we will use 3 routers in each of these offices.

We will use public address range for Research Center in:

Locations	**IP Address Range**	
Zurich	156.1.1.25	156.1.1.27
New York	156.1.1.28	156.1.1.30
Melbourne	156.1.1.31	156.1.1.33

4.3.3. Manufacturing and Distribution:

We assume that for every 40 employees there is 1 router.

We have a total of 2000 employees initially which will be increased upto 3600 employees in 6 office locations. Since, each office comprise of 600 employees, so we will use 15 routers in each of these offices.

We will use public address range for Manufacturing and Distribution in:

Locations	IP Address Range	
China	156.1.1.34	156.1.1.48
Israel	156.1.1.49	156.1.1.63
Chile	156.1.1.64	156.1.1.78
Canada	156.1.1.79	156.1.1.93
UAE	156.1.1.94	156.1.1.108
Malaysia	156.1.1.109	156.1.1.123

4.3.4. Sales Organization:

We have assumed that for every 40 employees there is 1 router.

We have a total of 1000 employees initially which will be increased upto 1800 employees in 60 offices, 20 each in 3 locations. Since, each office comprise of 30 employees, so we will use 1 router in each of these offices.

We will use public address range for Sales office in:

Locations	IP Address Range	
America	156.1.1.124	156.1.1.143
Europe/Middle East	156.1.1.144	156.1.1.163
Asia Pacific	156.1.1.164	156.1.1.183

4.3.5. Software Development Centers:

We assume that for every 40 employees there is 1 router.

We have a total of 300 employees initially which will be increased upto 540 employees in 3 office locations. Since, each office comprise of 180 employees, so we will use 5 routers in each of these offices.

We will use public address range for Software Development Centers in:

Locations	IP Address Range	
India	156.1.1.184	156.1.1.188
Pakistan	156.1.1.189	156.1.1.193
Russia	156.1.1.194	156.1.1.198

4.4 Data Center

A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls and various security devices.

We kept the following factors in mind while selecting the locations for our data centres:

1. The IT staff should be able to easily access the data centres, so it should be in the proximity of the company's location.
2. It should be in a geographical stable place, and risk free from natural environmental disasters.
3. It should have reliable and easy access to power grid.
4. Data centres involves high construction costs, and is different in different geographical regions depending on the regions tax and labour costs and other factors.
5. The data centres should have access only to limited staff and authorized personnels and should have secure checkpoints and monitoring systems.

We chose the following locations for our data centers for various location, environmental and infrastructure based advantages:

1. Netherlands

Beyond being the most wired country in Europe and having the continent's fastest connection speeds. Provides strong, clean power infrastructure. It also directly links continental Europe to North America. Plus, Netherlands' mild climate and robust renewable energy cluster provides sustainable and affordable options for data center energy efficiency needs—from power production to cooling.

2. Iowa

Iowa's electricity rates are relatively lower than many other states. Iowa also doesn't apply sales tax to power use. Tax breaks for industrial use of land.

3. Singapore

Singapore has world class infrastructure, with Singapore Government allocating extensive resources to fund R&D initiatives. Many of Singapore's data centers are housed across multiple floors. Having more storage space in a single data center facility also makes it easier for data center operators to better manage overall power efficiency.

Moreover, establishment of submarine cable systems has proven to be a pivotal factor in determining Singapore's pole position in the data center landscape – offers customers scalable, low-cost and low-latency connectivity – a desirable advantage for multi-national companies and startups with global expansion plans

Figure: Location of the Data Centers

Chapter 5
PROTOCOLS

For the network redesigning of the Vita Pharma, we would be using the following protocols which will help us in the achieving the overall requirements for the company.

Layer	Protocols
Application	● HTTP ● HTTPS ● DNS ● SMTP ● DHCP ● IMAP ● SNMP ● Citrix/VDI ● SSH
Transport	● TCP ● UDP
Network	● IP ● IPSEC ● ICMP ● OSPF ● BGP
Data Link Layer	● MAC ● VPN ● ARP ● Ethernet

Chapter 6
LAYERS

We are using a top-down approach while defining the layers.

6.1 Application Layer

There are wide variety of protocols available for the application layer, from which we have chosen the following protocols for our network redesigning.

1. **HTTP**
   It functions as a request-response protocol in a client-server computing model. The client submits an HTTP request message to the server, and in return server provides resources such as HTML files and other data-content as a response message to the client. The response contains completion status information about the request and may also contain requested content in its message body. For our network redesign for Vita Pharma, the browser applications make use of HTTP and HTTPs.

2. **DNS**
   The Domain Name System assigns domain names and maps those names to Internet resources by designating authoritative name servers for each domain. Also, with the help of DNS we will resolve the public domain names used.

3. **SMTP-IMAP**
   These mechanisms are used for sending and receiving email and very vital for handling the email for the Vita Pharma. SMTP is used for the sending of the emails to the intended destination, while IMAP is used for managing and retrieving the emails from the server.

4. **DHCP (Dynamic Host Configuration Protocol)**
   A DHCP is a network management protocol which can manage TCP/IP settings for devices on a network, by dynamically assigning Internet Protocol (IP) addresses to any device, or node, so that they can communicate with each other using this IP. Most residential network routers receive a globally unique IP address within the provider network. Within a local network, a DHCP server assigns a local IP address to each device connected to the network. In the Vita Pharma, we will use it for assigning the IPs to all the departments and the systems so they are able to communicate with each other, moreover with the use of DHCP servers, they are able to communicate with the departments in the other regional offices as well.

5. **CITRIX**
   With the advancement in the technology, where the data needs to be accessed from anywhere around the corner of the world, it is not feasible to get access to the data physically, hence we are now storing the data on the cloud which can be accessed at any instance of time. Moreover, it also provides securing the data by the encryption key facility, making the data secure. Thus, this is very important for the Vita Pharma network to upgrade their system of file sharing.

6. **SSH**
   It is used for operating network services securely over an unsecured network, mainly for the purpose of remote access of the company resources. SSH uses an encryption which is intended to provide integrity and confidentiality of data, thus making it comparatively more secure. SSH over VPDN can be used for remote login. This will accommodate not only Sales persons who are mobile to access company's network but also enables users to work remotely from any place, thus making the interaction with the client and customers more available and friendly.

6.2 Transport Layer

The transport layer is responsible for end-to-end communication over a network. It provides logical communication between application processes running on different hosts within a layered architecture of protocols and other network components. The transport layer is also responsible for the management of error correction, providing quality and reliability to the end user.

The transport layer can provide some or all of the following services:

- **Connection-Oriented Communication**: The devices of a network communication establish a three way handshake protocol to ensure a connection is robust before data is exchanged. It is only in the case of TCP.
- **In Order Delivery**: It ensures that packets are always delivered in sequential order.
- **Data Integrity**: With the use of checksums, it guarantees that there is no modification in the data in between the sending and the receiving end, thus ensuring the data integrity.
- **Flow Control**: It helps in controlling the data throughput, i.e., the speed at which data can be sent so that the receiver can receive it without any congestion and breakdown in the communication.
- **Multiplexing**: The transmission of multiple packet streams from unrelated applications or other sources (multiplexing) across a network requires some very dedicated control mechanisms, which are found in the transport layer. This multiplexing allows the use of simultaneous applications over a network such as when different internet browsers are

opened on the same computer. In the OSI model, multiplexing is handled in the service layer.

The transport layer uses TCP and UDP protocols for the transmission on the data. The significant difference between TCP and UDP is that TCP is reliable and ensures guarantee of delivery of the data to the end system, while UDP ensures fast delivery of data. In our case, we will use TCP for the finance department, since it requires the data to be received correctly without any loss. Also, we require the data to be sent through secure means for which we will use SSL/TSL which will help in increasing the security, for transmitting and accessing confidential data.

6.3 Network Layer

The network layer is considered to be the mainstay of our model. Network layer protocol exists in every host and router, and it selects and manages the best logical path for the packet to be shared between the host and destination. The router looks through the header field of the IP packet and then pass to the next hop along the destination.

There are two main functions of the network layer:

1. **Forwarding:** The function of this is to move the packet when it arrives at the router's input link to the appropriate output link.
2. **Routing:** The network layer determines the path/ route taken by the packets as they move from the source to the destination.

In our network redesigning:

- We will be using, IPv4, IPSec technologies and ICMP, OSPF, BGP protocols for routing.
- There are total 79 offices for the Vita Pharma, hence for each office we need to assign a public static IP address.
- We use IP for the regular routing and IPSec for routing over VPN in this layer. IPSec and Secure Socket Layer (SSL)/ Transport Layer Security (TLS) are two most common choices for secure VPN.
- IPSec provides us with two types of security features; Authentication Header protocol which helps in providing source authentication and data integrity, and Encapsulation Security protocol which not only provides data integrity and source authentication but also provides confidentiality.
- For the communication between different offices and departments, we will be using routers, bridges, and switches.
- ICMP will be used for error reporting and is used by hosts and routers to communicate network-layer information to each other.

- To communicate between different departments and system within the same office, we will make use of OSPF, while to communicate between office located different locations/regions we will make use of BGP.
- OSPF stands for Open-Shortest path First. Its a Link State Routing protocol, hence it calculates the shortest distance from the source to the destination using Dijkstra's algorithm. OSPF is advantageous here because it has the complete knowledge of the network topology, thus allowing it's routers to calculate appropriate routes.
- To speed up our response time of the network, instead of requesting data from the main server we will install cache servers for every regional offices. So, when the request is made it will first check the cache server and if it is not present there it will call from the main server, thus reducing the response time of the request.

6.4 Data Link Layer

We adopt a hybrid topology to incorporate the best of all available topologies namely Bus , Ring, Mesh and Star. Due to the highly distributed nature of the company this allows for choosing the optimal option for a particular use-case.

Different protocols used in the data link layer include:

- **ARP**: The address resolution protocol is a protocol used by the Internet Protocol (IP) [RFC 826], specifically IPv4, to map IP network addresses to the physical addresses used by a data link protocol
- **MAC**: Carrier Sense Multiple Access (CSMA) is a media access control (MAC) protocol in which a node verifies the absence of other traffic before communicating on a shared medium.
- **Virtual LANs** are used to re-partition the physical LAN in order to improve the traffic management. The traffic between devices split across two or more physical networks ordinarily needs to be handled by a network's core routers, but with a VLAN that traffic can be handled more efficiently by network switches instead.
- **Virtual Private Networks** extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
  Types of VPNs
  - VPDN Virtual Private Dial-Up Network is a network that extends remote access to a private network using a shared infrastructure. Since most of the sales employees are mobile they may use this service to connect to the vita-pharma’s LAN.
  - Intranet VPN It provides a secure LAN to LAN connection, this can be used to connect geographically separated offices at vita-pharma.

- Extranet VPN it provides a secure connection from vita-pharma LAN to network of Business partners, Vendors etc.

6.5 Physical Layer

This is the bottom most layer in the network, and it deals with the bit level transmission between different devices rather than logical data packets. As the name suggests, it deals with the network's physical connection which may involve wireless transmission, cabling and wired connections. We will make use of the wired connections to connect to the workstations, and will use wireless connection for VOIP, Printers, faxes, and other devices.

- For the wired connections, we will use twisted pair of copper wires, connecting all the workstations in all departments, except the Treasury department.

6.5.1 Access Technologies

The ability of any individual or organization to connect to the internet though the means of terminals, computers or other devices, and access services such as mail, or world wide web is termed as internet access.

We employ following access technologies in our network:

- **DSL (Digital Subscriber Line)**
  It is an access technology that uses local telephone lines to provide access to the internet.This can be used by mobile sales force organization for working while staying at their residence. It uses a dsl modem and a splitter to filter and differentiate between the data and voice signals. It offers data rates ranging from 128 Kbps to 3 Mbps.

- **Twisted Pair Cable (Cat 6_a 10GBASE-T Ethernet)**
  This is the least expensive and most commonly used access technology. It can provide data rates from 10 Mbps to 10 Gbps. This can be used to access internet for all the departments, namely HR, strategy, legal, corporate IT, facilities management, executive management

- **Fibre Optic**
  For the Treasury department, we will make use of the fibre optics, since it needs to be secure and fast as it is dealing with trading. The plus point of using Optical fibre is it helps in avoiding latency and electromagnetic interference.

- **WiFi (Ethernet 802.11)**
  It is used to provide Internet access to devices which are within the range of a wireless network that is connected to the Internet. The coverage of one or more interconnected access points (hotspots) depends upon the type of device used, and can extend from an area as small as a few meters to as large as many square kilometres. This form of access technology will mostly be used by offices within different divisions of the company.

Chapter 7
SECURITY

Due to the presence of highly sensitive data - personally identifiable information like social security numbers, customer specification data, financial data for the organisation and confidential analytics product development softwares used by R&D, Security is one of the top priority and network should be designed keeping in mind the security needs.

7.1 Network Perimeter Security

This is the first layer of defence in the network. It secures the perimeter of an internal private and locally managed and owned side of network and the public side, usually provider managed side of network.

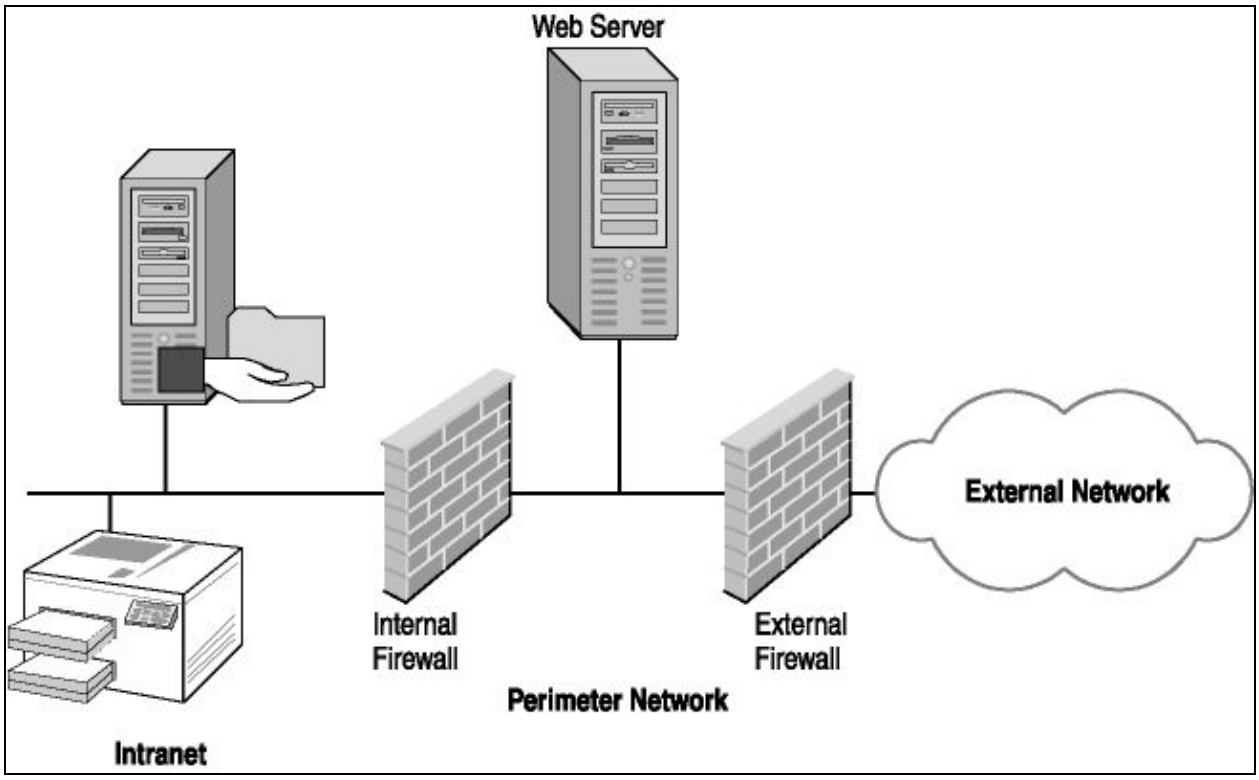


Figure: Network Perimeter Security

7.2 Firewalls

We use stateful firewalls. It keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it, while filtering it. Using the restrictive policy, only packets matching a known active connection will be allowed by the firewall, while others will be rejected.

Implementing stateful firewalls would secure the internal network as -

- The IPtables in access control list will only allow employees to get through, it will block packets coming from unknown network sources.
- Since, stateful firewalls keep track of state of network connections, it can detect the IP addresses which have reported with repetitive attacks and block those IP addresses.

7.3 Demilitarized Zone

If firewalls and routers are the guards, gate, walls of a castle, then the DMZ is like the courtyard once inside the castle. It functions as an isolated network positioned between the external network and the enterprise network, where the external network can only access resources in DMZ, while the local network is firewalled.

To protect the internal servers and resources from being exposed to the untrusted network, we put web and mail servers in the DMZ zone.

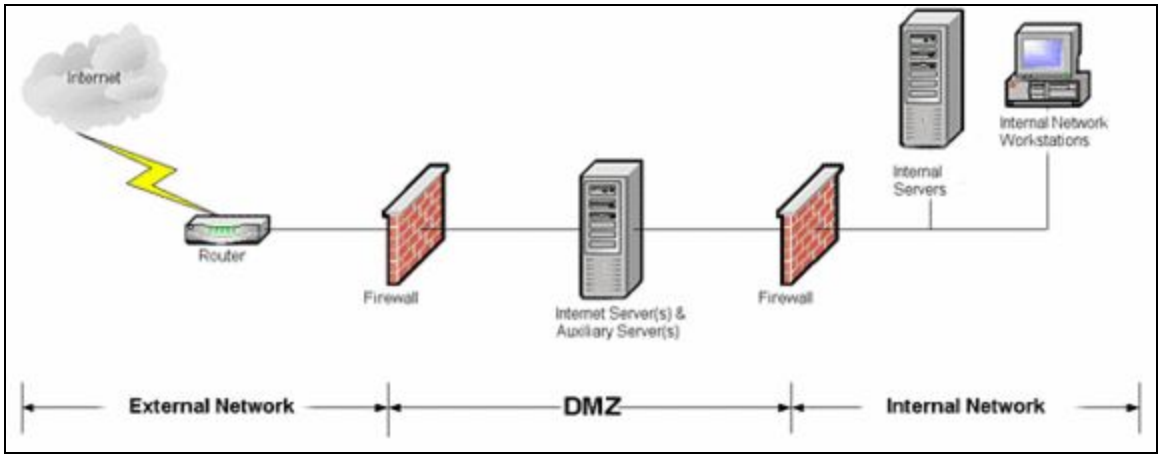


Figure: Demilitarized Zone

7.4 Virtual Private Network

VPN allows users to securely access a private network and share data remotely through public networks. IPsec VPN utilizes tunnel mode for creating VPN tunnels and provides enhanced level of security on VPN connections by default by providing authentication, encryption and compression services.

Finance & Accounting, Treasury and R&D department have high security needs, employing IPsec VPNs will provide them with secure and always on network connectivity.

7.5 Secure Socket Layer

SSL is a cryptographic protocol that provides communications security over a network. It establishes an encrypted link between a server and a client, thus avoiding eavesdropping and tampering of information. Using HTTPS over SSL/TLS will ensure privacy, integrity and authentication.

7.6 Data Security

For data security and data transmission security we employ encryption techniques such as AES and RSA. This will ensure confidentiality of data. We also add S/MIME (Secure/Multipurpose Internet Mail Extensions) protocol in communicating end systems, for sending digitally signed and encrypted messages.

7.7 Wireless Security

WPA2 (Wi-fi Protected Access-2) will be used for ensuring wireless security. It uses AES, which is a very strong block cipher. Has 4 way handshake between the host and access point, thus providing strong authentication. It also allows connections to be modified or revoked by administrators at anytime.

Chapter 8
CALCULATIONS

Throughput is the key measure for the network performance. It tells us the amount of successful data that can be transferred through the network per unit of time over a communication channel. Throughput is essential for various application types, like real time big data services, VoIP, video-streaming, etc.

8.1 Acceptable Delay

Office	Acceptable Delay
Headquarter	≤ 1000 ms
Finance	≤ 100 ms
Software and Development	≤ 800 ms
Sales	≤ 1500 ms
Manufacturing and Distribution	≤ 2000 ms
Global Research Centre	≤ 500 ms

8.2 Bandwidth Calculation

8.2.1 Headquarter

- Maximum acceptable delay = 1000 ms
- Total number of employees in each headquarter (with a 15% growth rate / year) = 900/4 = 225
- Average bandwidth available for each employee = Bandwidth / 225 Mbps
- To send or receive a file of size 1 MB by each employee,

For 1s delay $= \frac{1024 \times 225}{Bandwidth}$ s

Bandwidth $= \frac{230400}{1}$ bps

$= 230.4$ Mbps $\simeq$ 231 Mbps

The Minimum Required Bandwidth = 231 Mbps

Recommended acceptable delay = 500 ms

For 0.5 s delay $= \frac{1024 \times 225}{Bandwidth}$ s

Bandwidth $= \frac{230400}{0.5}$ bps

$= 460.8$ Mbps $\simeq$ 461 Mbps

Therefore, Recommended Required Bandwidth = 461 Mbps

These bandwidths will be required by each department, except for the finance department. Since it deals with the treasury and financial transactions, hence we require a small delay, for which we calculate the bandwidth as shown below.

8.2.1.1 Finance

- Maximum acceptable delay = 100 ms
- Total number of employees in each headquarter (with a 15% growth rate / year) = 225/7 = 33
- Average bandwidth available for each employee = Bandwidth / 33 Mbps
- To send or receive a file of size 1 MB by each employee,

For 0.1s delay $= \frac{1024 \times 33}{Bandwidth}$ s

Bandwidth $= \frac{33792}{0.1}$ bps

$= 337.92$ Mbps $\simeq$ 338 Mbps

Therefore, Minimum Required Bandwidth = 310 Mbps

Recommended acceptable delay = 50 ms

For 0.05 s delay $= \frac{1024 \times 33}{Bandwidth}$ s

Bandwidth $= \frac{33792}{0.05}$ bps

$= 675.8$ Mbps $\simeq$ 680 Mbps

Therefore, Recommended Required Bandwidth = 680 Mbps

8.2.2 Software and Development

- Maximum acceptable delay = 800 ms
- Total number of employees in each office (with a 15% growth rate / year) = 540/3 = 180
- Average bandwidth available for each employee = Bandwidth / 180 Mbps
- To send or receive a file of size 1 MB by each employee,

For 0.8 s delay = $\frac{1024 \times 180}{Bandwidth}$ s

Bandwidth = $\frac{184320}{0.8}$ bps

= 230.4 Mbps ≃ 231 Mbps

Therefore, Minimum Required Bandwidth = 231 Mbps

Recommended acceptable delay = 400 ms

For 0.4 s delay = $\frac{1024 \times 180}{Bandwidth}$ s

Bandwidth = $\frac{184320}{0.4}$ bps

= 460.8 Mbps ≃ 461 Mbps

Therefore, Recommended Required Bandwidth = 461 Mbps

8.2.3 Sales

- Maximum acceptable delay = 1500 ms
- Total number of employees in each office (with a 15% growth rate / year) = 1800/60 = 30
- Average bandwidth available for each employee = Bandwidth / 30 Mbps
- To send or receive a file of size 1 MB by each employee,

For 1.5s delay = $\frac{1024 \times 30}{Bandwidth}$ s

Bandwidth = $\frac{30720}{1.5}$ bps

= 20.48 Mbps ≃ 21 Mbps

Therefore, Minimum Required Bandwidth = 21 Mbps

Recommended acceptable delay = 800 ms

For 0.8 s delay = $\frac{1024 \times 30}{Bandwidth}$ s

Bandwidth = $\frac{30720}{0.8}$ bps

= 38.4 Mbps ≃ 40 Mbps

Therefore, Recommended Required Bandwidth = 40 Mbps

8.2.4 Manufacturing and Distribution

- Maximum acceptable delay = 2000 ms
- Total number of employees in each office (with a 15% growth rate / year) = 3600/6 = 600

- Average bandwidth available for each employee = Bandwidth / 600 Mbps
- To send or receive a file of size 1 MB by each employee,

For 2s delay $= \frac{1024 \times 600}{Bandwidth}$ s

Bandwidth $= \frac{614400}{2}$ bps

$= 307.2$ Mbps $\simeq$ 310 Mbps

Therefore, Minimum Required Bandwidth = 310 Mbps

Recommended acceptable delay = 1000 ms

For 1 s delay $= \frac{1024 \times 600}{Bandwidth}$ s

Bandwidth $= \frac{614400}{1}$ bps

$= 614.4$ Mbps $\simeq$ 615 Mbps

Therefore, Recommended Required Bandwidth = 615 Mbps

8.2.5 Global Research Center

- Maximum acceptable delay = 500 ms
- Total number of employees in each headquarter (with a 15% growth rate / year) = 360/3 = 120
- Average bandwidth available for each employee = Bandwidth / 120 Mbps
- To send or receive a file of size 1 MB by each employee,

For 0.5s delay $= \frac{1024 \times 120}{Bandwidth}$ s

Bandwidth $= \frac{122880}{0.5}$ bps

$= 245.76$ Mbps $\simeq$ 246 Mbps

Therefore, Minimum Required Bandwidth = 246 Mbps

Recommended acceptable delay = 50 ms

For 0.2 s delay $= \frac{1024 \times 120}{Bandwidth}$ s

Bandwidth $= \frac{122880}{0.2}$ bps

$= 614.4$ Mbps $\simeq$ 615 Mbps

Therefore, Recommended Required Bandwidth = 615 Mbps

Office	Minimum Bandwidth	Recommended Bandwidth
Headquarter	231 Mbps	461 Mbps
Finance	338 Mbps	680 Mbps
Software and Development	231 Mbps	461 Mbps
Sales	21 Mbps	40 Mbps
Manufacturing and Distribution	310 Mbps	615 Mbps
Global Research Centre	246 Mbps	615 Mbps

Although the throughput efficiency of the network varies greatly and it is an ideal case to assume 1 Mbps Bandwidth available for each user at any time, but due to the fact that the probability of every user using the network bandwidth at the same time is very low our assumption can be considered practical.

REFERENCES

[1.] https://www.paessler.com/it-explained/ip-address
[2.] https://en.wikipedia.org/wiki/Reserved_IP_addresses
[3.] https://www.techopedia.com/definition/26424/public-network
[4.] https://docs.oracle.com/cd/E19455-01/806-0916/6ja85398r/index.html
[5.] http://www.pearsonitcertification.com/articles/article.aspx?p=1843889
[6.] http://www.datacenterjournal.com/factors-choosing-data-center-colocation-provider/
[7.]http://www.areadevelopment.com/siteSelection/April2012/data-center-location-decision-criteria-26255554.shtml
[8.] https://www.techopedia.com/definition/8866/physical-layer
[9.] https://www.lifewire.com/virtual-local-area-network-817357
[10.]https://www.cisco.com/c/en/us/tech/dial-access/virtual-private-dialup-network-vpdn/index.html
[11.] https://www.zeemaps.com/map?group=2799577
[12.]https://www.theatlantic.com/technology/archive/2015/12/why-are-so-many-data-centers-built-in-iowa/418005/
[13.]https://www.enterpriseinnovation.net/article/secret-behind-singapores-data-center-success-1926059439
[14.] https://en.wikipedia.org/wiki/Throughput
[15.] https://learningnetwork.cisco.com/docs/DOC-5876
[16.]https://en.wikipedia.org/wiki/Internet_access
[17.]https://en.wikipedia.org/wiki/Wi-Fi#IEEE_802.11_standard