NYU

TANDON
SCHOOL OF
ENGINEERING

Vita Pharma

Network Architecture

The **Global Tech** ® Team:
Mamadou Lamine Dianko(md1864)
Monil Shah(mds747)
Vatsal Gopani(vbg221)
Prashant Patel(pnp249)
Jatri Dave(jad752)

Executive Summary

Global Tech is a IT consulting firm. Vita pharma a global mid-size level Pharmaceutical company has discovered issues with its current network architecture. Also, the company is planning significant expansion into the new markets by decreasing time-to-market for their core set of products and increasing the global workforce hiring. Due to above reasons, VitaPharma has decided to redesign its network architecture for better performance. As Global Tech is an IT consulting firm, Vita Pharma has signed a contract with Global tech, to redesign their Network Architecture. We are team of network engineers at Global tech , working on this report to analyze the current complaints and redesign the network architecture for the firm. In this report we will try to solve the ongoing issues, provide new IP schema, network architecture and Security essentials required for the betterment of firm growth.

Background

Vita Pharma is a global company.

- Main office is in New Brunswick, New Jersey, USA.
- Regional headquarters are in (500 employees total) :
    - London, UK
    - Sao Paulo, Brazil
    - Singapore
- Each regional HQ has departments:
    - accounting/finance
    - human resources
    - legal
    - corporate IT
    - facilities management
    - executive management
    - strategy groups.
- Global research centers are in(200 scientist total approx) :
    - Zurich, Switzerland
    - New York, USA
    - Melbourne, Australia
- There are manufacturing and distribution facilities in(2000 people total approx):
    - China
    - Israel
    - Chile
    - Canada
    - United Arab Emirates
    - Malaysia

- Sales organization is highly distributed(1000 employees total)
    - approximately 20 small and medium size offices in each of the major geographical areas (Americas, Europe/Middle East and Asia Pacific) to a total of 1000 employees.
    - Most of the sales employees are mobile.
- Software Development centers in:
    - Pakistan
    - India
    - Russia
    - Total of 300 employees working on multiple client-server and web-based software projects to support global operations, supply chain, drug research and development management and many others.
- The company uses HR application to manage resources, which contains personally identifiable information, such as social security numbers, names and addresses.
- Finance and Accounting use Financial Management System, which contains specific financial data for the entire organization. Treasury department, which is a part of Finance organization, requires access to trading markets to invest some of the profits in OTC commodities and stocks.
- Sales and Marketing is managed through a suite of applications, which contain customer specific data.
- R&D uses special analytics and product development software, which is highly confidential.
- All apps are developed using Microsoft ASP.NET (i.e. inside the browser) technology. Citrix/VDI is used to access files and folders on the network.

Project Goal

Vita Pharma is a mid size global Pharmaceutical company. The company is planning significant expansion into the new markets by decreasing time-to-market for their core set of products and increasing the global workforce hiring. There are ongoing complaints about slow access to files, email delivery, poor voice quality and various applications crashing due to poorly designed network. The recent complains and new addition are solved in this project by :

- Redesign global network
- Develop new IP addressing schema for each and every office and location.
- Redesign all local LANs.
- Re-architect global voice and data networks.
- Identify and select global data center locations for major functions.

- Identify relevant protocols, which facilitate any and all forms of communications.
- Identify all access technologies.
- Developing application profiles(protocols, security, throughput), acceptable delays and identify and document minimum and recommended bandwidth requirements for each location.
- Showing analysis, draw diagrams and document calculation.

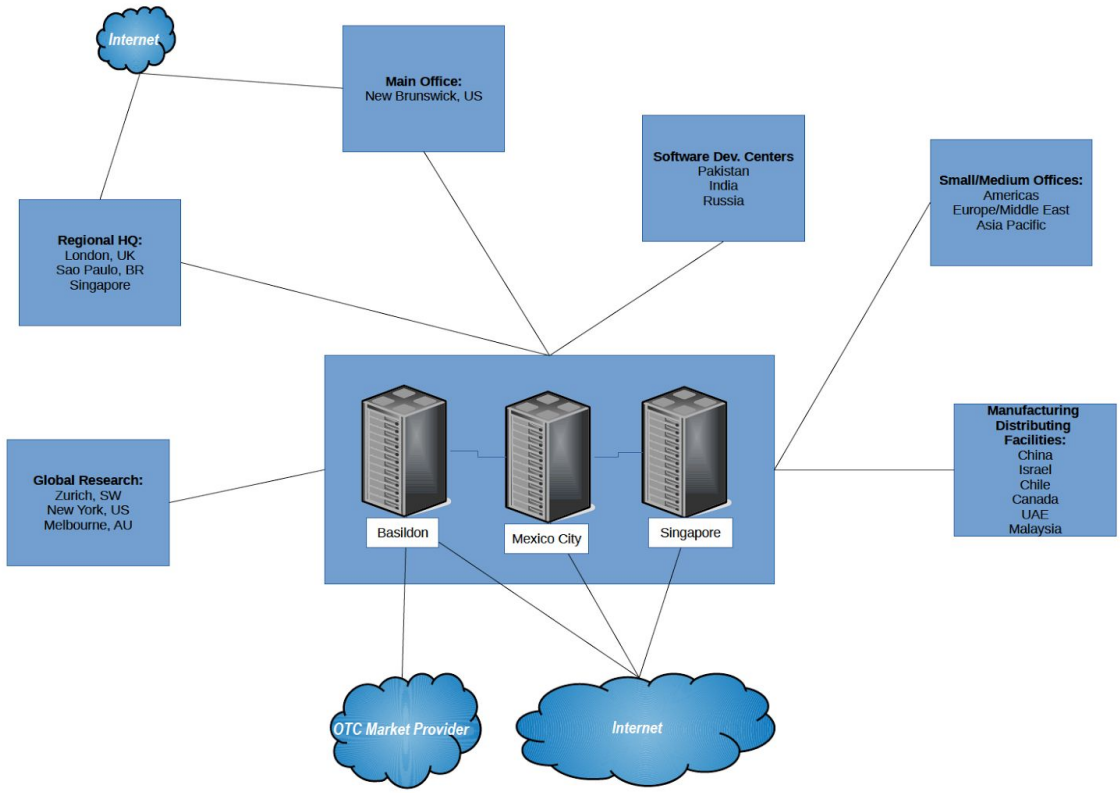
Methodology

In addition to the current complaints noted in the initial analysis of the problem, Vita Pharma also operates in a very competitive environment which is subject to lots of industrial spying. The methodology used here is very security focused. We wanted to design a network which had inherent security built-in. This facilitates the safeguard of trade secrets for instance.

The design also accounted for cost as we choose a hybrid model for internet access meaning some locations had a direct line to the internet while most connected via the data centers. We believe this model scales very well in the event the company grows even bigger in the future.

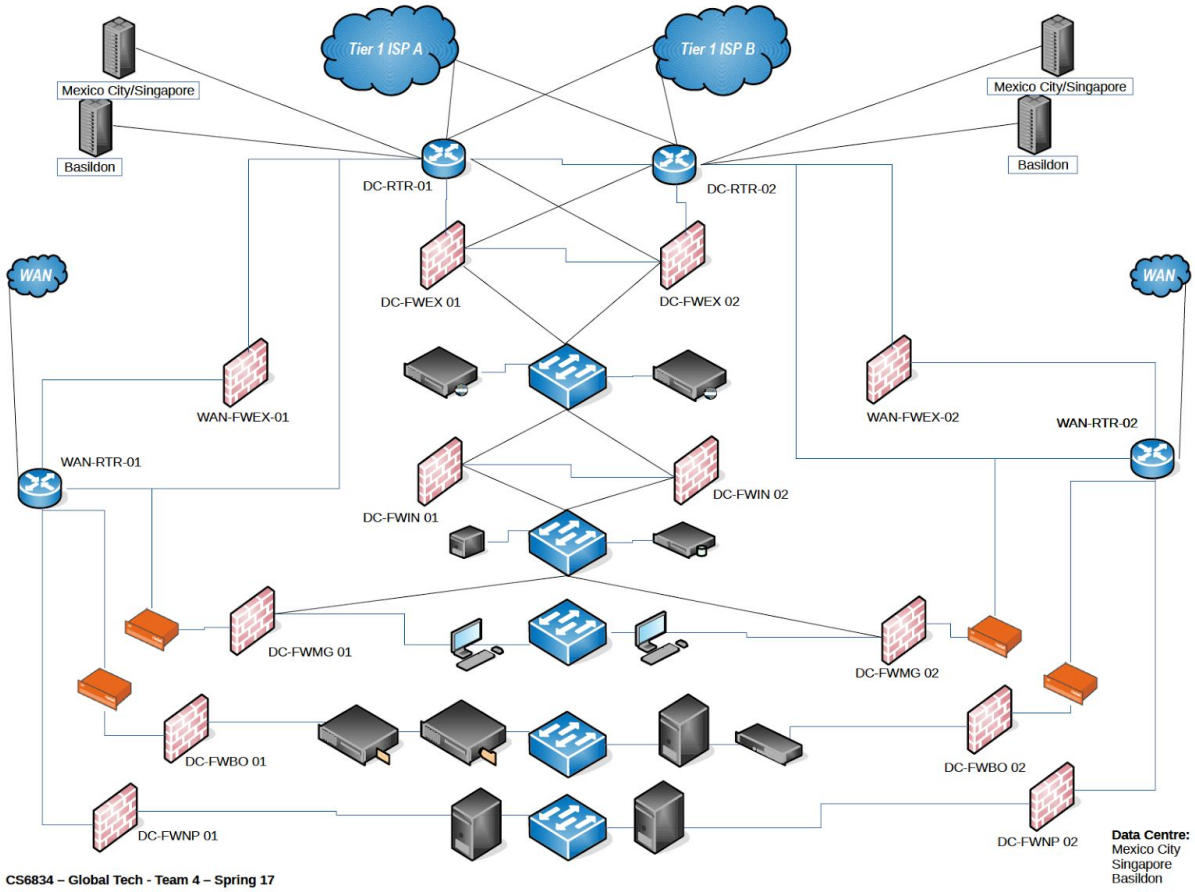
We focused our architecture on centralizing core functions such as email, DNS, file share etc.. To resolve some of the issues such as the poor voice quality, we chose to distribute the voice infrastructure to each location. The poor network design which caused application crashes was also addressed as we designed the data centers to allow easy and controlled communication between silos.

Network Architecture
High Level Overview



The architecture consists of a star like design. Besides the main offices and regional HQs, the only way to access internet from a remote location is via the Data centers. Basildon DC gets a dedicated line to an OTC market provider in order to provide trading capability to the London Trading floor located in the London Regional HQ.

Data Centre



The data centers are designed to provide redundancy and reliable upkeep of the production services. These include:

- Internet access
- file share
- DNS
- VoiP
- E-mail
- Database
- Applications
- Web services

The design allows for Offices/Research centers, Dev centers and Manufacturing facilities to all connect to the data center via the WAN routers (WAN-RTR-01/02). Those links are GRE over IPSec.

The data center comprises five silos which are:

- DMZ
- Internal
- Management
- Back Office
- Non-prod (DEV/QA)

Each silo plays a specific function in order to support operations at Vita Pharma.

DMZ
This silo contains the web servers and the VPN concentrator which allows employees to connect remotely via an IPSec tunnel or SSL VPN.

Internal
The internal silo houses the application servers and the databases which contains the data store of applications used company wide such as the HR application. This silo is very important as it contains servers with sensitive information. This warranted the decision to perform VLAN segmentation across all the internal segments. There are ACLs in the internal switches which prevent lateral movement (e.g from one internal VLAN to another).

Management
A Citrix/VDI farm and management terminal servers are located in this silo. This is meant to house any management function carried out by operational teams. Citrix/VDIs farm gives the ability to start SSH sessions for connectivity to production database, application or web servers server. Back Office file shares are also accessed from the Citrix/VDI farm in management.

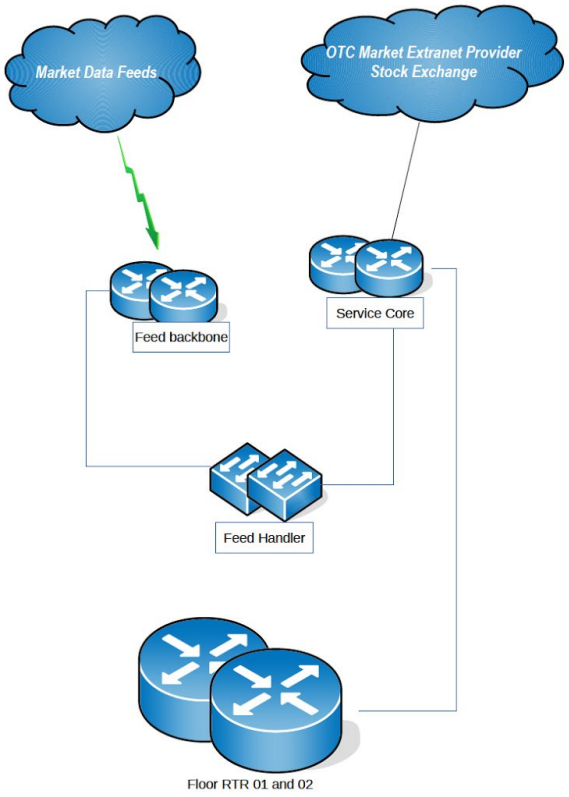
Back Office
All of the back office functions are carried out in this silo. The DNS servers are located in this segment along with the File shares, E-mail and the data center call managers. Having DNS servers in back office and not in the remote locations makes it easier to management and protect. This silo's goal is to host a centralized environment where any major function is easily controllable.

Non-prod (DEV/QA)
This is the QA/DEV environment, we allocated this silo in the data center exclusively to any non-production activity. It is heavily segregated from the rest of the environment as well using firewall rules on DC-FWNP-01/02.

Each data center has the following access technologies:

Appliance	DMZ	Internal	Management	Back Office	Non-prod
Next Gent Firewall	4	2	2	2	2
Core Switch	2	2	2	2	2
Router	2	0	2	0	0

The Trading Environment (Basildon only)



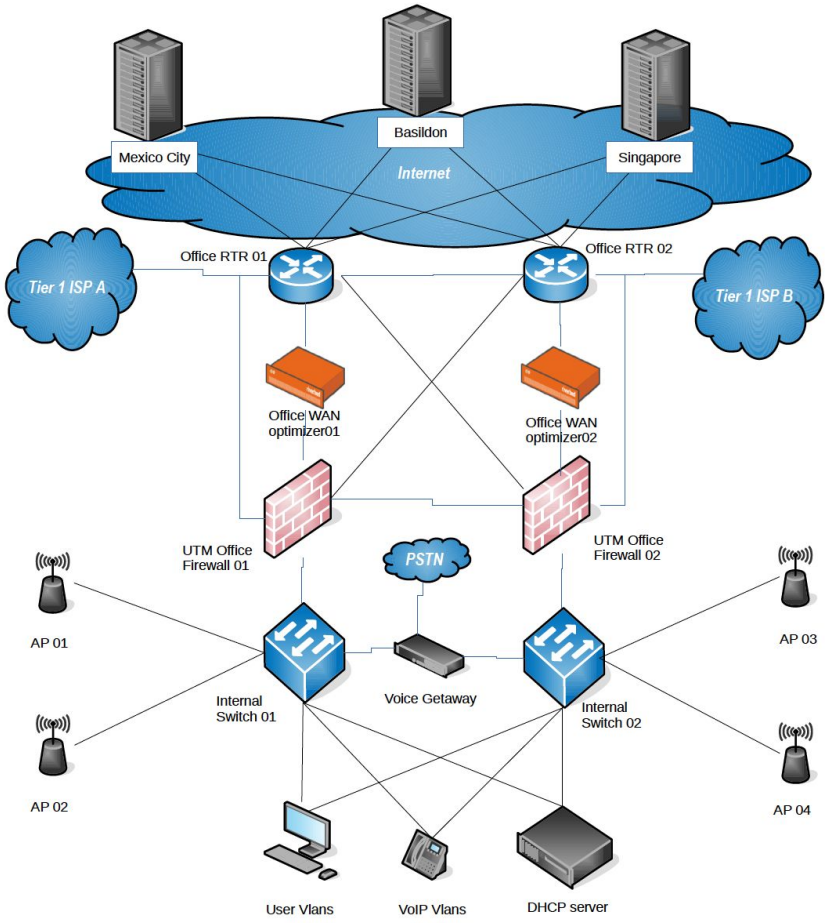
Basildon:
Trading Floor

In the Basildon data center, we built a trading silo which is exclusive to the London office. We did this with the idea that the London office was the closest physically to the Basildon data center which is a known trading hub. There are two specific traffic which make up a standard trading environment:

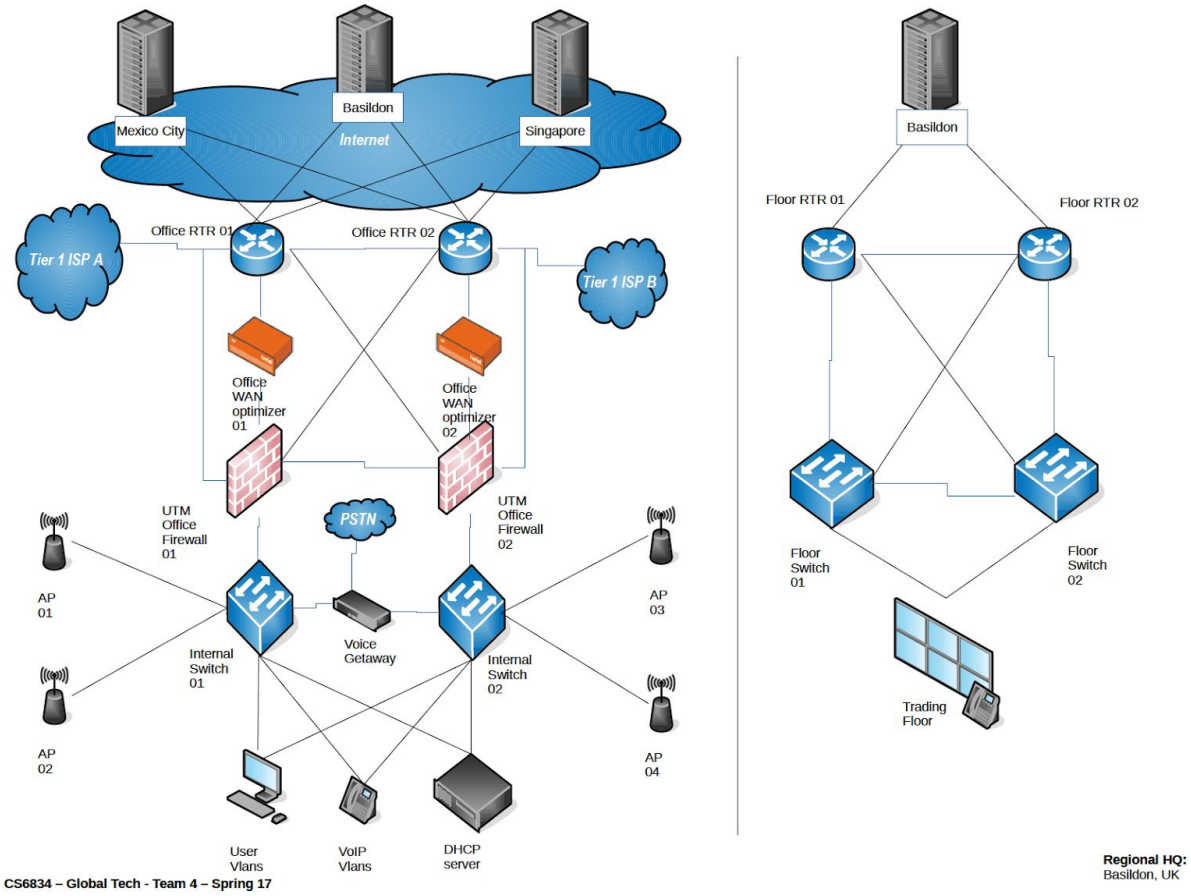
- Market Data
- Market Orders

In Basildon, feed backbone receives the market data from the providers (e.g Reuters or Bloomberg) which then sends the traffic to the feed handlers. The next and final hop is the service core which also handles the market orders directly from the Trading Floor in the London office. Because this is all taking place on dedicated networks which are segregated from the rest of the data center networks, there is a lot to gain in terms of security and speed.

Main Office/Regional Headquarters

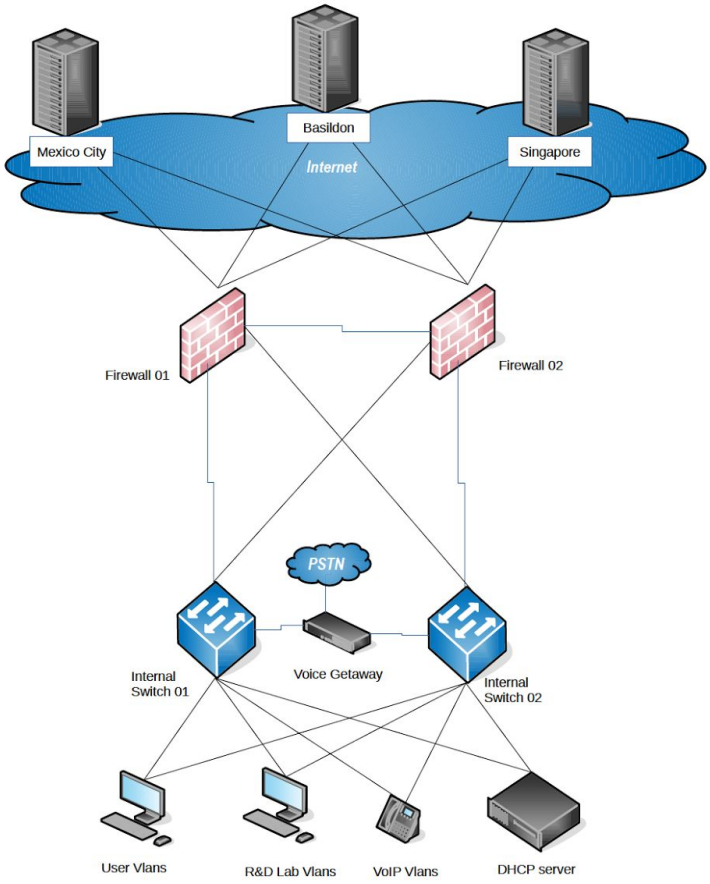


The main office and regional HQ architecture is comprised of two routers, two firewalls, two WAN optimizers, two internal switches. The design aims for redundancy of the circuits. The routers at the edge provide direct internet connectivity as well as Datacenter connectivity via GRE over IPsec tunnels. There is a Voice gateway connected to a PSTN in each office as well to route the Voice calls efficiently. The VoiP systems have dedicated Vlans. Wifi access is available locally as well as a local DHCP server.



Since the Treasury department has a requirement to access trading networks in order to invest Vita Pharma's profit into OTC commodities, we decided to logically separate the London office into two parts. The London office still gets the same stack as the other HQs but on top of that, it also houses a Trading Floor. London is geographically the closest to Basildon which is one of the major Data centers for trading. We therefore assumed that any Treasury staff who engages in Trading will need to be based out of London. The trading floor has a direct link to the Basildon Datacenter from where access to the OTC market is implemented.

Global Research

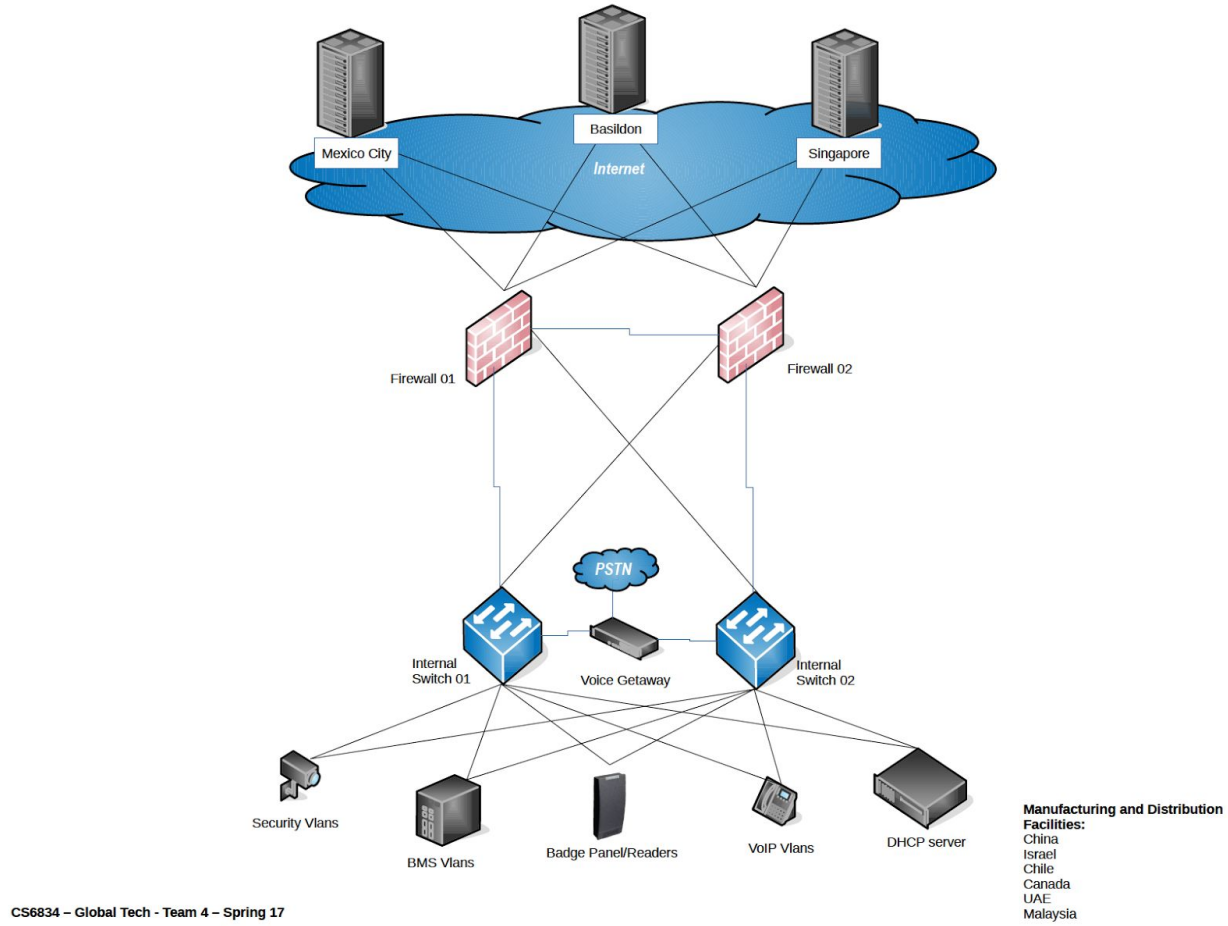


CS6834 – Global Tech - Team 4 – Spring 17

Global Research Centers:
Zurich, CHE
New York, US
Melbourne, AU

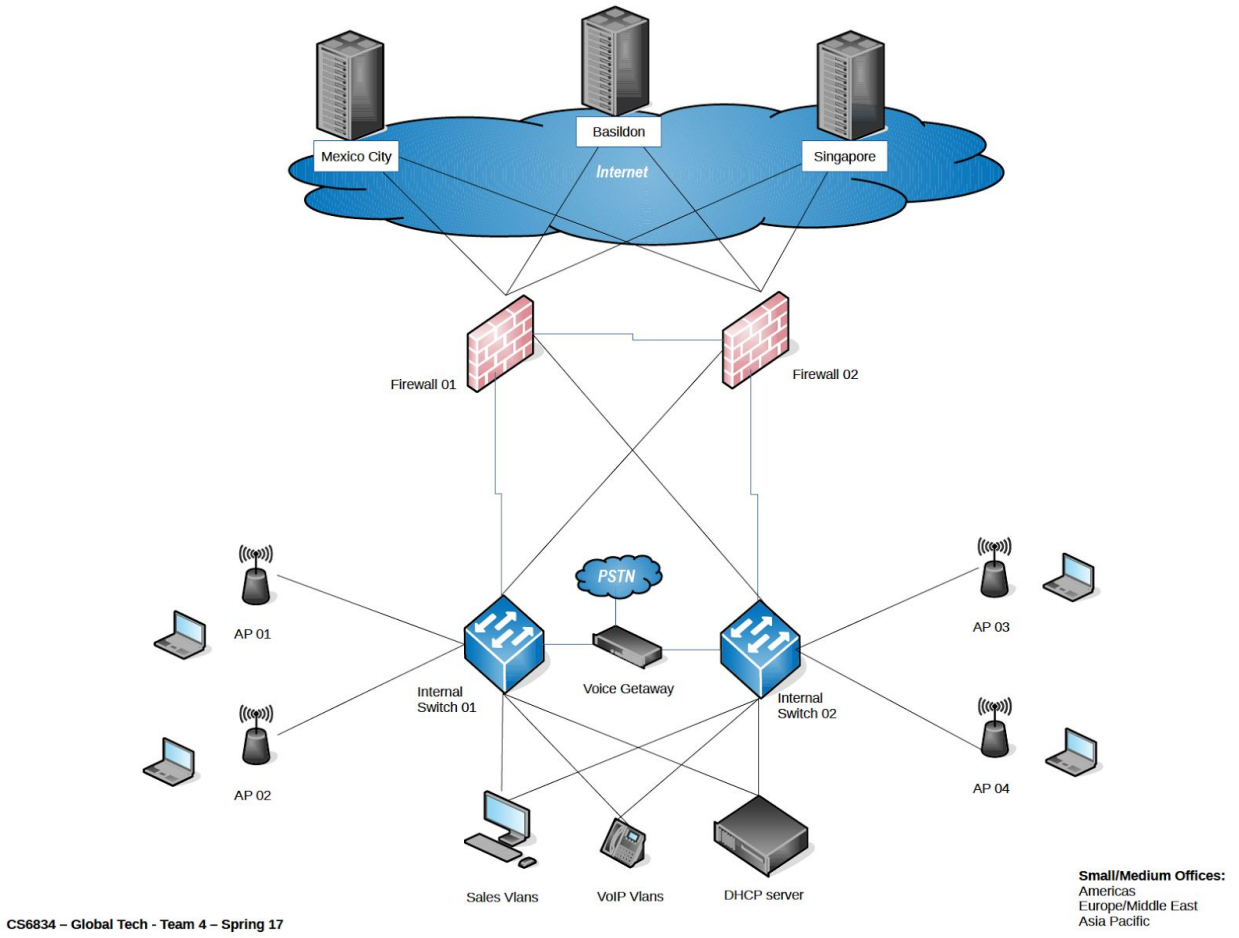
These research centers are extremely important for the company as they drive innovation and essentially help the company stay relevant. It is therefore crucial the network design facilitates the goal which is to help innovate and safeguard the trade secrets. That being said, these research centers will have R&D Labs which will NOT have access to internet and will be isolated from anything else. Access to and from those R&D Lab Vlans will be strictly controlled via Firewall rules. The idea is for researchers to not be able to access the internet from R&D hence avoiding the exposure to cyber threats (phishing, spying etc..). We still included a small user VLANs to allow staff to perform basic functions such as emails and safe internet browsing.

Manufacturing Distributing Facilities



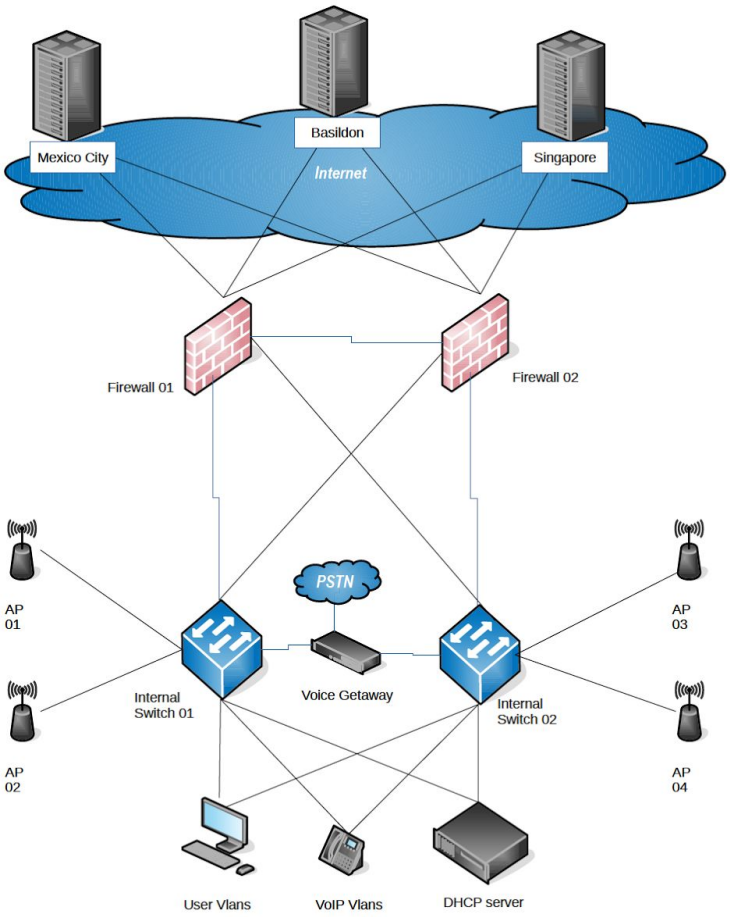
The manufacturing facilities were designed to NOT have internet access. These are treated as factories and as such, there is also an emphasis on security. There is a dedicated security VLANs for cameras and CCTV. Badge readers and badge panels used by employees for access also gets a dedicated VLAN. We have decided to include a Building Management System (BMS) technology to monitor building related systems. A VoiP VLAN is also deployed similarly to the other locations. All VLANs are terminated on the firewall which is where internet access is restricted.

Small/Medium(Sales) Offices



Because employees in Sales are mostly mobile in small/medium offices, we focused on a WiFi oriented design in this office. There is a small sales Vlan which contains teleconference rooms in the event that sales employees needed to bring clients for presentation sessions of the product sets. Each sales employee gets a work laptop with a company image installed. They are expected to use the Office WiFi to connect to the VPN concentrator located at the data centre. That image will contain a VoiP soft phone which enables them to communicate using the VoIP infrastructure located at the datacenter.

Software Development Centers



The software development centers inherits a similar architecture to the Small/Medium offices. Internet access is through the data centers. The main difference here is the presence of a bigger user VLAN to accommodate the employees working on dev projects as they are going to spend more time at the office than the sales employees. As per the other locations, all VLANs are terminated on the office firewall cluster which is the primary control point. There is a dedicated VoiP network here as well to allow voice communication. Lastly, WiFi is available locally. The employees in these offices perform most of their tasks at the data centers where the non-prod networks are located.

IP Schema

Main Office

New Brunswick, US	Network	Hosts	Gateway
accounting/finance	10.10.100.0/24	254	10.10.100.1
human resources	10.10.101.0/24	254	10.10.101.1
legal	10.10.102.0/24	254	10.10.102.1
corporate IT	10.10.103.0/24	254	10.10.103.1
facilities management	10.10.104.0/24	254	10.10.104.1
executive management	10.10.105.0/24	254	10.10.105.1
strategy groups	10.10.106.0/24	254	10.10.106.1
VoiP	10.10.10.0/24	254	10.10.10.1
WiFi	10.10.3.0/24	254	10.10.3.1

Regional HQ

London, UK	Network	Hosts	Gateway
accounting/finance	10.30.100.0/24	254	10.30.100.1
human resources	10.30.101.0/24	254	10.30.101.1
legal	10.30.102.0/24	254	10.30.102.1
corporate IT	10.30.103.0/24	254	10.30.103.1
facilities management	10.30.104.0/24	254	10.30.104.1
executive management	10.30.105.0/24	254	10.30.105.1
strategy groups	10.30.106.0/24	254	10.30.106.1
VoiP	10.30.10.0/24	254	10.30.10.1
WiFi	10.30.3.0/24	254	10.30.3.1
Trading Floor	172.26.100.0/24	254	172.26.100.1

Sao Paulo, BR	Network	Hosts	Gateway
accounting/finance	10.40.100.0/24	254	10.40.100.1
human resources	10.40.101.0/24	254	10.40.101.1
legal	10.40.102.0/24	254	10.40.102.1
corporate IT	10.40.103.0/24	254	10.40.103.1
facilities management	10.40.104.0/24	254	10.40.104.1
executive management	10.40.105.0/24	254	10.40.105.1
strategy groups	10.40.106.0/24	254	10.40.106.1
VoiP	10.40.10.0/24	254	10.40.10.1
WiFi	10.40.3.0/24	254	10.40.3.1

Singapore	Network	Hosts	Gateway
accounting/finance	10.50.100.0/24	254	10.50.100.1
human resources	10.50.101.0/24	254	10.50.101.1
legal	10.50.102.0/24	254	10.50.102.1
corporate IT	10.50.103.0/24	254	10.50.103.1
facilities management	10.50.104.0/24	254	10.50.104.1
executive management	10.50.105.0/24	254	10.50.105.1
strategy groups	10.50.106.0/24	254	10.50.106.1
VoiP	10.50.10.0/24	254	10.50.10.1
WiFi	10.50.3.0/24	254	10.50.3.1

Global Research

Zurich, SW	Network	Hosts	Gateway
R&D Lab	172.16.10.0/24	254	172.16.10.1
User	10.60.100.0/25	126	10.60.100.1
VoiP	10.60.10.0/25	126	10.60.10.1

New York, NY	Network	Hosts	Gateway
R&D Lab	172.16.20.0/24	254	172.16.20.1
User	10.70.100.0/25	126	10.70.100.1
VoiP	10.70.10.0/25	126	10.70.10.1

Melbourne, AU	Network	Hosts	Gateway
R&D Lab	172.16.30.0/24	254	172.16.30.1
User	10.80.100.0/25	126	10.80.100.1
VoiP	10.80.10.0/25	126	10.80.10.1

Manufacturing and Distribution Facilities

China	Network	Hosts	Gateway
Security	172.20.100.0/26	62	172.20.100.1
BMS	172.20.101.0/26	62	172.20.101.1
VoiP	10.90.10.0/27	30	10.90.10.1
Badge System	172.20.102.0/26	62	172.20.102.1

Israel	Network	Hosts	Gateway
Security	172.21.200.0/26	62	172.21.100.1
BMS	172.21.201.0/26	62	172.21.101.1
VoiP	10.100.10.0/27	30	10.100.10.1

Badge System	172.21.102.0/26	62	172.21.102.1

Chile	Network	Hosts	Gateway
Security	172.22.200.0/26	62	172.22.100.1
BMS	172.22.201.0/26	62	172.22.101.1
VoiP	10.110.10.0/27	30	10.110.10.1
Badge System	172.22.102.0/26	62	172.22.102.1

Canada	Network	Hosts	Gateway
Security	172.23.200.0/26	62	172.23.100.1
BMS	172.23.201.0/26	62	172.23.101.1
VoiP	10.120.10.0/27	30	10.120.10.1
Badge System	172.23.102.0/26	62	172.23.102.1

UAE	Network	Hosts	Gateway
Security	172.24.200.0/26	62	172.24.100.1
BMS	172.24.201.0/26	62	172.24.101.1
VoiP	10.130.10.0/27	30	10.130.10.1
Badge System	172.24.102.0/26	62	172.24.102.1

Malaysia	Network	Hosts	Gateway
Security	172.25.200.0/26	62	172.25.100.1
BMS	172.25.201.0/26	62	172.25.101.1
VoiP	10.140.10.0/27	30	10.140.10.1
Badge System	172.25.102.0/26	62	172.25.102.1

Small/Medium Offices

Americas	Network	Hosts	Gateway
Sales Vlan	10.100.100.0/26	62	10.100.100.1
VoiP	10.100.10.0/26	62	10.100.10.1
WiFi	10.100.3.0/24	254	10.100.3.1

Europe/Middle East	Network	Hosts	Gateway
Sales Vlan	10.x.x.x/26	62	10.x.x.1
VoiP	10.x.x.x/26	62	10.x.x.1
WiFi	10.x.x.x/24	254	10.x.x.1

Asia Pacific	Network	Hosts	Gateway
Sales Vlan	10.x.x.x/26	62	10.x.x.1
VoiP	10.x.x.x/26	62	10.x.x.1
WiFi	10.x.x.x/24	254	10.x.x.1

Software Development Centers

Pakistan	Network	Hosts	Gateway
WiFi	10.210.3.0/24	254	10.210.3.1
User	10.210.100.0/24	254	10.210.100.1
VoiP	10.210.10.0/24	254	10.210.10.1

India	Network	Hosts	Gateway
WiFi	10.230.3.0/24	254	10.230.3.1
User	10.230.100.0/24	254	10.230.100.1
VoiP	10.230.10.0/24	254	10.230.10.1

Russia	Network	Hosts	Gateway
WiFi	10.240.3.0/24	254	10.240.3.1
User	10.240.100.0/24	254	10.240.100.1
VoiP	10.240.10.0/24	254	10.240.10.1

Data Centres

Mexico City	Network	Hosts	Gateway
DMZ	10.5.40-44.0/24	254 each.	10.5.40-44.1
Internal	10.5.45-55.0/24	254 each.	10.5.45-55.1
Management	10.5.56-60.0/24	254 each.	10.5.56-60.1
Back Office	10.5.61-65.0/24	254 each.	10.5.61-65.1
Non-prod	10.5.66-70.0/24	254 each.	10.5.66-70.1

Basildon	Network	Hosts	Gateway
DMZ	10.6.40-44.0/24	254 each.	10.6.40-44.1
Internal	10.6.45-55.0/24	254 each.	10.6.45-55.1
Management	10.6.56-60.0/24	254 each.	10.6.56-60.1
Back Office	10.6.61-65.0/24	254 each.	10.6.61-65.1
Non-prod	10.6.66-70.0/24	254 each.	10.6.66-70.1

Singapore	Network	Hosts	Gateway
DMZ	10.7.40-44.0/24	254 each.	10.7.40-44.1
Internal	10.7.45-55.0/24	254 each.	10.7.45-55.1
Management	10.7.56-60.0/24	254 each.	10.7.56-60.1
Back Office	10.7.61-65.0/24	254 each.	10.7.61-65.1
Non-prod	10.7.66-70.0/24	254 each.	10.7.66-70.1

Application Profiles

Applications are the vital for an online business to succeed. Vita Pharma being mid-cap organization with resources spread throughout the globe needs highly structured application stack. For example, employees use the Citrix to access the virtual client and do the filesharing, the traffic between the Citrix and the application server is primarily driven by use of the Citrix only. Though the actual traffic generated by business application is contained within the datacenter which has the direct access to the internet, and it exist between the Citrix Server and the application server hosting all those services as well as applications. Below is a list of applications and the description regarding the throughput.

Application / Services	Description	Protocols Used	Bandwidth Needed
Email	Electronic mail. Email gateways .POP3 Connections to Third Party Email Providers	• SMTP • TCP • TLS • HTTPS	Low- Medium
Citrix Desktop	Citrix Desktop interface, which is accessible from the ICA protocol.	• ICA • HTTPS	Medium-High
VoIP	Voice over Internet Protocol	• SIP • SRTP • IPSEC(If we need secure encrypted connection)	Medium-High
HR Application	HR application for staffing, recruiting and other HR related works. Web app/SaaS.	• HTTPS • TCP	Low-Medium
VitaR&D	R&D application, web / native for the research and development. Since R&D is not connected with the internet local webapp/native app will be used instead	• HTTP • TCP	No bandwidth needed from the datacenter.
SalesApp	Web/native application used by the Sales team for order booking,invoicing, order processing etc.	• HTTPS • TCP • RDP	Medium-High
Marketing App	Web/native application used by the marketing team to	• HTTPS • TCP	Low-Medium

	manage the marketing, pricing strategy, communications ,promotions etc		
TradingApp	Web/native application for the trading purpose of OTC commodities,items	• HTTPS • TCP	Medium-High (Real Time Processing)
Network Storage/File Sharing/Citrix	File sharing, using Citrix	• SMB • TCP • HTTPS	Medium-High (Real Time)

Calculation of Bandwidth, Throughput and Delay:

We are considering the below issues:

- Bandwidth Considerations
- Bandwidth delay product
- Throughput

- **Main office:** The main office needs to communicate and monitor the work in regional headquarters spread across the world. These communication happen through VOIP or video conferencing. Because of which, the main office requires high bandwidth. As we have assumed 500 people in the main office, we assign a Bandwidth of 2000-3000Mbps.

    - Bandwidth Range : Assuming all the employees work using the internet at the same time in the office, hence the bandwidth required here would be high. Considering usage in the terms of email with attachment as 50kb per user and video calling , VoIP in the main HQ, a fast connection with a speed range of 2-3Gbps i.e. 2000-3000Mbps is sufficient range for daily usage.

- **Regional Headquarters:** The Headquarters have to communicate with Main office as well as other offices in their respective regions. Total number of Employees across all the headquarters is 500. So it is around 150 people in each of the three headquarters.

    - Bandwidth Range: Considering Regional Headquarter is constantly connected to main HQ via email or voice call, considering 150 employees for each of the three headquarter. Summing up the bandwidth required for each department, Vita Pharma needs to allocate 2000-3000 Mbps of

bandwidth overall for the usage of three headquarters on basis of daily usage. Hence,

- London HQ : 660 - 1000 Mbps Bandwidth Range
- Brazil HQ : 660 - 1000 Mbps Bandwidth Range
- Singapore HQ : 660 - 1000 Mbps Bandwidth Range

- Sub-Allocation of Bandwidth between Departments in Regional Headquarters:
- Finance Department: This department deals with a lot of data hence we allocate maximum amount of bandwidth to this department which is 100 Mbps
- Human Resource: We allocate 50 Mbps
- All other Departments: 50 Mbps

- **Global Research Center:** Global Research centres don't require a high bandwidth as most of the work at the research centers doesn't involve net connectivity. Vita Pharma has three research centers across the world and has 200 scientists. So each Center has around 70 scientists and we allocate 100-150 Mbps daily.

    - Zurich : 100-150 Mbps
    - New york: 100-150 Mbps
    - Melbourne: 100-150 Mbps

- **Manufacturing and Distribution:** Since it is Pharmaceutical company, manufacturing and distribution unit will not need too much of bandwidth. This department has 2000 people spread over 6 offices with approximately 340 employees in each centre.

    - Bandwidth Range: As per our design we have mentioned not to provide a heavy usage internet connection to the Manufacturing and Distribution department. Considering the usage for Security vlans , building management and related stuff the bandwidth can be allocated as below on daily usage basis:
        - China : 100-150 Mbps
        - Israel : 100-150 Mbps
        - Chile : 100-150 Mbps
        - UAE : 100-150 Mbps
        - Canada : 100-150 Mbps
        - Malaysia : 100-150 Mbps

- **Software Development Department:** This department will make use of cloud applications and needs video conferencing and internet telephony. The software development offices are located at 3 locations in India, Pakistan, Russia.

    - Bandwidth Range: This are the Software Development Departments and are directly connected to the servers in the HQ, where there is a need of softwares. Hence, this departments have heavy usage of cloud services. Requiring a total bandwidth of 2000-3000 Mbps i.e 660-1000 Mbps each on daily usage basis.
        - India : 660-1000 Mbps
        - Pakistan : 660-1000 Mbps
        - Russia : 660-1000 Mbps

- **Sales:** There are 60 offices all over the world with 1000 employees including all.

    - Bandwidth Range: Assuming that there are 15 medium size with 30 employees and 45 small size with 12 employees each. Offices. Most of the sales employees have field work and do not use much of the office network. Hence we allocate a bandwidth on daily usage basis of 15-20 Mbps for medium size and 6-10 Mbps to small size companies
        - Small Company size: 6-10 Mbps
        - Medium company size: 10-15 Mbps

Bandwidth Delay Product:

Consider a default MSS(TCP packet Size) 536 bytes (20 for IP header) (20 for TCP header)
Avg min RTT is 20ms and max RTT is 60 ms
Bandwidth delay product = bandwidth*RTT

- Main Office : 3000*0.02 | 3000*0.06 = 60|180 ms
- Regional HeadQuarters(Each): 1000*0.02 | 1000*0.06 = 20 | 60 ms
- Global Research Center(Each) : 150*0.02 | 150*0.06 = 3 | 9 ms
- Manufacturing and Distribution : 150*0.02 | 150*0.06 = 3 | 9 ms
- Software Development Department(Each) : 1000*0.02 | 1000*0.06 = 20 | 60 ms
- Sales(Small Company) : 10*0.02 | 10*0.06 = 0.2|0.6 ms
- Sales(Medium Company): 15*0.02 | 15*0.06 = 0.3|0.9 ms

Throughput:

Throughput = Receive Window Size / RTT
Receive Window Size = 536 bytes
Throughput = 536/0.02 | 536/0.06 = 26.8kb/s | 8.93Kb/s

- Main Office : 3000/500 = 6 Mbps
- Regional HeadQuarters(Each): 1000/150 = 6.66 Mbps
- Global Research Center(Each) : 150/70 = 2.14 Mbps
- Manufacturing and Distribution : 150/340 = 0.44 Mbps
- Software Development Department(Each) : 1000/100 = 10 Mbps