Network Re-design for Vita Pharma

(Ishwarya Rajendrababu, Mansi Patel, Aditya Rajmane, Rohan Deshmukh, Samira Sawant, Janhavi Bagwe, Utkarsha Shetye)

Abstract

We reviewed Vita Pharma's current network architecture and designed new improved version of the network architecture for Vita Pharma. The newly designed network architecture mainly focuses on the complaints which were there in the previous network architecture such as slow access to files, e-mail delivery, poor voice quality and various application crashing due to poorly designed network.

I. Introduction

Vita Pharma is a global company. The current network architecture of Vita Pharma is undergoing some issues which include slow access to files, e-mail delivery, poor voice quality and crashing of various applications because of poorly designed network. Network reengineering for Vita Pharma encompasses redesigning of global network that is development of new IP addressing schema for each and every office location, Redesigning of all local LANs and Re-architecting global voice and data networks etc.

II. High Level Network

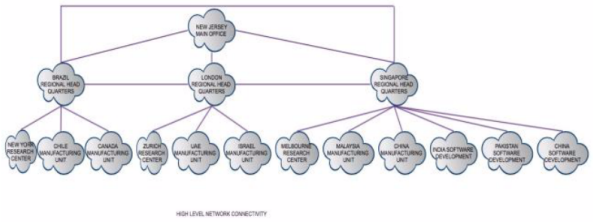

Fig.1 Global network

The global network of the Vita Pharma organisation is given above where the organization's presence is grouped on a region basis. We have three regions here Americas, Europe and Middle East, Asia Pacific

The individual departments located at different countries in the region will be connected to the corresponding Regional Headquarters (RHQ) in the region such as Sao Paulo Brazil, London and Singapore and the RHQ's connect with each other in turn. The RHQ's altogether connecting to the Main Office at New Brunswick, New Jersey.

III. IP Addressing Schema

The New Jersey main office:

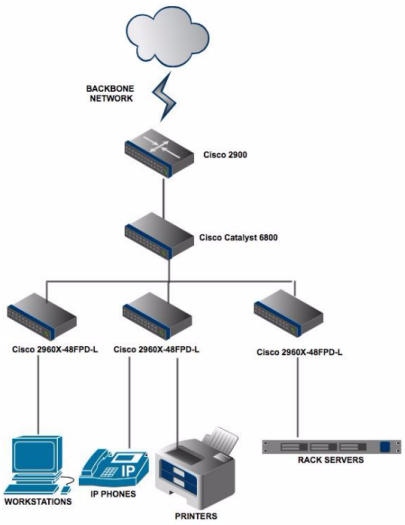

Fig.2 Network diagram for new Jersey main office

We have assumed that the number of the employees in the New Jersey Main office is around 200. And hence IP allocated for the workstations, VoIP phones, printers and the servers.

The CIDR addressing scheme is used to allocate the IP address.

The main office at the New Brunswick, NJ is allocated the 10.6.0.0 network.

The network 10.6.0.0/24 is allocated for the workstation subnet.

The network 10.6.1.0/24 is allocated for the IP phones and printer subnet.

The network 10.6.2.0/28 is allocated for the server's subnet.

The servers include the LDAP server, the DHCP server, mail server etc. The voice network here is connected to the individual RHQs via VPN since it is the head office and requires critical information communicated without delay.

In this network, a total of 528 IP's are allocated and it has enough IP's unused that can be used when the network is scaled.

The workstations that belong to the same department are grouped into VLAN's.

Verizon is the leading Internet Service Provider in NJ and hence we connect to Verizon.

INTERMEDIATE SWITCH

Cisco® Catalyst® 2960-X Series Switches are fixed-configuration, stackable Gigabit Ethernet switches that provide enterprise-class access for campus and branch applications.
24 or 48 Gigabit Ethernet ports with line-rate forwarding performance
● Gigabit Small Form-Factor Pluggable (SFP) or 10G SFP+ uplinks
● FlexStackPlus for stacking of up to 8 switches with 80 Gbps of stack throughput.
It is also cost effective to use this switch as it is available for $ 2000(approx).
So we will use the following switch, this is stackable so based on the number of connections per workstations , per VOIP and per server in the server farm we can increase the number of blades in the rack. This is usually located on a per floor basis in all the buildings in a geographical location.

CORE SWITCH

Cisco Catalyst 6800 series switches are programmable campus backbone switches optimized for 10/40/100 Gigabit Ethernet services. These switches offer converged wired, wireless, and VPN security. Cisco Catalyst 6880-X Switches provide scalability with eighty 10 or twenty 40 Gigabit Ethernet ports.

CORE ROUTERS :
CISCO ASR 1002X Router:
CISCO ASR 1006 Router

The Cisco ASR 1000 Series Aggregation Services Routers transform the service provider and enterprise network edge by delivering industry-leading performance, instant-on service capabilities, and high availability in a compact form factor. The Cisco ASR 1000 Series Routers deliver:

- Highly secure, high-performance, and integrated software-enabled services
- A new price class for high-performance edge routers
- High resiliency with convenient and cost-saving, in-service software upgrades
- Software redundancy on non-redundant hardware

For service providers, the Cisco ASR 1000 Series facilitates more flexible, efficient, and cost-effective delivery of complex consumer and business services. And for enterprises, it delivers a highly reliable, high-performance WAN edge solution where information, communication, collaboration, and commerce converge.

REGIONAL HEADQUARTERS' IP SCHEMA: BRAZIL

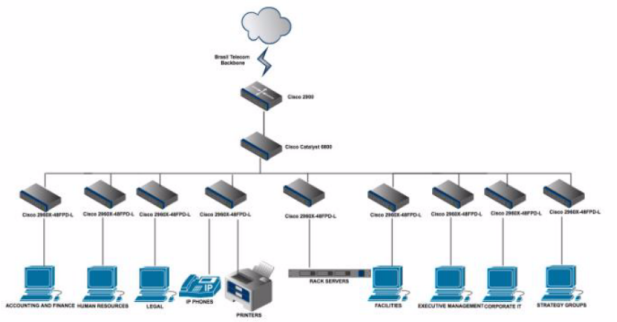

Fig.3 IP Schema for Brasil

The Brasil telecom is the leading Internet service provider in Brasil and hence it is chosen.
The switches and the routers used here are same as the ones used in the main office.
The network 10.1.0.0/22 is allocated here with 1024 IP's using CIDR, out of which 976 are allocated for the existing employees. We have few IP's left unused for scalability purposes.

CORPORATE IT	10.1.2.192/26 - 10.1.2.255/26
FACILITIES	10.1.3.0/26 – 10.1.3.63/26
EXECUTIVE MANAGEMENT	10.1.3.64/26 – 10.1.3.127/26
STRATEGY GROUPS	10.1.3.128/26 – 10.1.3.191/26
SERVERS	10.1.3.192/28 – 10.1.3.207/28

REGIONAL HEADQUARTERS' IP SCHEMA: LONDON

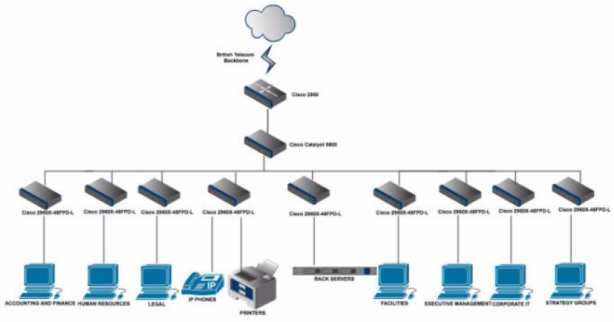

Fig.4 IP Schema for London

The British telecom is the leading Internet service provider in London and hence it is chosen.

The switches and the routers used here are same as the ones used in the main office.
The network 10.2.0.0/22 is allocated here with 1024 IP's using CIDR, out of which 976 are allocated for the existing employees. We have few IP's left unused for scalability purposes.

Subnet	IP Allocation
Voice	10.2.1.1/23 – 10.2.1.255/23
Accounting and Finance	10.2.2.0/26 – 10.2.2.63/26
Human Resources	10.2.2.64/26 – 10.2.2.127/26
Legal	10.2.2.128/26– 10.2.2.191/26
Corporate IT	10.2.2.192/26– 10.2.2.255/26
Facilities	10.2.3.0/26 – 10.2.3.63/26
Executive Management	10.2.3.64/26 – 10.2.3.127/26
Strategy groups	10.2.3.128/26– 10.2.3.191/26
Servers	10.2.3.192/28– 10.2.3.207/28

REGIONAL HEADQUARTERS' IP SCHEMA: SINGAPORE

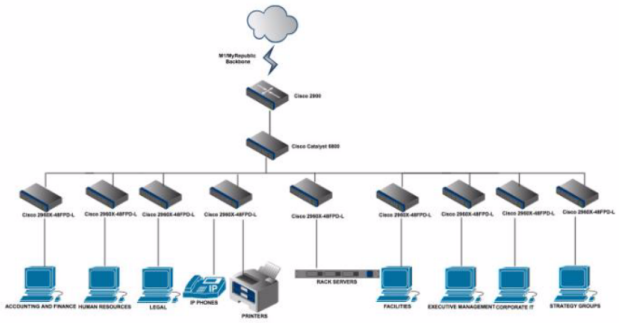

Fig.5 IP Schema for Singapore

The M1/MyRepublic is the leading Internet service provider in Singapore and hence it is chosen.
The switches and the routers used here are same as the ones used in the main office.
The network 10.3.0.0/22 is allocated here with 1024 IP's using CIDR, out of which 976 are allocated for the existing employees. We have few IP's left unused for scalability purposes.

Subnet	IP Allocation
Voice	10.3.1.1/23 – 10.3.1.255/23
Accounting and Finance	10.3.2.0/26 – 10.3.2.63/26
Human Resources	10.3.2.64/26 – 10.3.2.127/26
Legal	10.3.2.128/26– 10.3.2.191/26
Corporate IT	10.3.2.192/26– 10.3.2.255/26
Facilities	10.3.3.0/26 – 10.3.3.63/26
Executive Management	10.3.3.64/26 – 10.3.3.127/26
Strategy groups	10.3.3.128/26 – 0.3.3.191/26
Server	10.3.3.192/28 – 0.3.3.207/28

RESEARCH CENTRE IP SCHEMA: NEW YORK

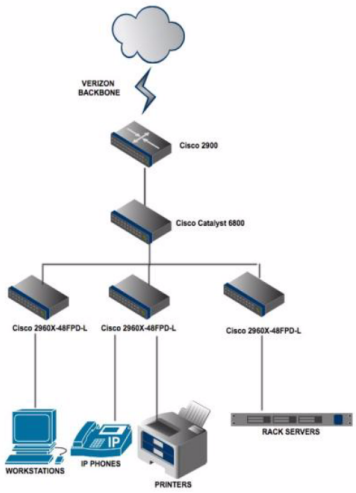

Fig.6 IP Schema for New York

Verizon is the leading Internet service provider in Singapore and hence it is chosen.
The switches and the routers used here are same as the ones used in the main office.
The network 10.1.4.0/23 is allocated here with 512 IP's using CIDR, out of which 272 are allocated for the existing employees and the network elements. We have few IP's left unused (240) for scalability purposes.

Subnet	IP Allocation
Workstations	10.1.4.1/25 – 10.1.4.127/25
Voice	10.1.4.128/25 – 0.1.4.255/25
Servers	10.1.5.0/28 – 10.1.5.15/28

RESEARCH CENTRE IP SCHEMA: ZURICH

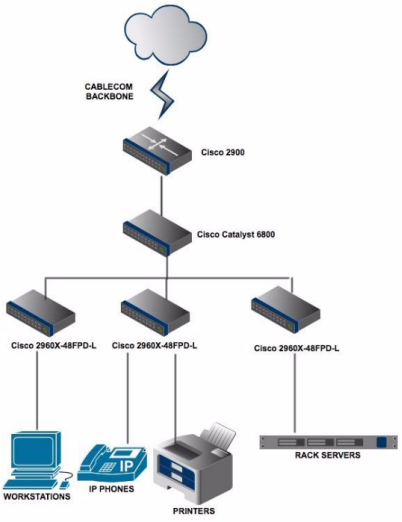

Fig.7 IP Schema for Zurich

Cablecom is the leading Internet service provider in Singapore and hence it is chosen.
The switches and the routers used here are same as the ones used in the main office.
The network 10.2.4.0/23 is allocated here with 512 IP's using CIDR, out of which 272 are allocated for the existing employees and the network elements. We have few IP's left unused (240) for scalability purposes.

Subnet	IP Allocation
Workstations	10.2.4.1/25 – 10.2.4.127/25
Voice	10.2.4.128/25 – 0.2.4.255/25
Servers	10.2.5.0/28 – 10.2.5.15/28

RESEARCH CENTRE IP SCHEMA: MELBOURNE

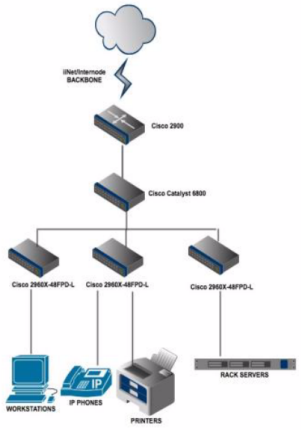

Fig.8 IP Schema for Melbourne

iiNet/Internode is the leading Internet service provider in Singapore and hence it is chosen.
The switches and the routers used here are same as the ones used in the main office.
The network 10.3.4.0/23 is allocated here with 512 IP's using CIDR, out of which 272 are allocated for the existing employees and the network elements. We have few IP's left unused(240) for scalability purposes.

Subnet	IP Allocation
Workstations	10.3.4.1/25 - 10.3.4.127/25
Voice	10.3.4.128/25 - 10.3.4.255/25
Servers	10.3.5.0/28 - 10.3.5.15/28

MANUFACTURING AND DISTRIBUTION CENTRE IP SCHEMA:

There are 2 manufacturing and distribution centers under each geographical region. A total of 6 such facilities are spread across the Americas, Europe and Middle East and Asia Pacific.

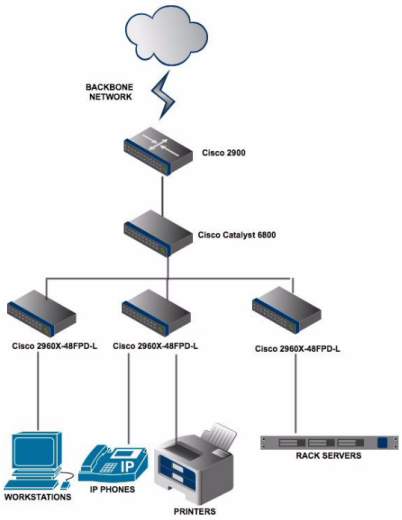

Fig.8 IP Schema for Manufacturing and Distribution

The facilities are located at Chile, Canada, UAE, Israel, China and Malaysia. They have the similar network as above with a different service provider according to the location.
The leading ISP's in these countries are used as the backbone network. Each facility is allocated with 2048 IP's where 1008 IP's are left unused.
The switches and the routers used here are same as the ones used in the main office.

IP SCHEMA: CHILE

Network : 10.1.6.0/21

Subnet	IP Allocation
Workstations	10.1.6.1/23 – 10.1.7.255/23
Voice	10.1.8.0/23 – 10.1.9.255/23
Servers	10.1.10.0/28 – 10.1.10.15/28

IP SCHEMA: CANADA

Network : 10.1.14.0/21

Subnet	IP Allocation
Workstations	10.1.14.1/23 – 0.1.15.255/23
Voice	10.1.16.0/23 – 0.1.17.255/23
Servers	10.1.18.0/28 -10.1.18.15/28

IP SCHEMA: UAE

Network : 10.2.6.0/21

Subnet	IP Allocation
Workstations	10.2.6.1/23 -10.2.7.255/23
Voice	10.2.8.0/23 - 10.2.9.255/23
Servers	10.2.10.0/28-10.2.10.15/28

IP SCHEMA: ISRAEL

Network : 10.2.14.0/21

Subnet	IP Allocation
Workstations	10.2.14.1/23- 10.2.15.255/23
Voice	10.2.16.0/23 - 10.2.17.255/23
Servers	10.2.18.0/28 - 10.2.18.15/28

IP SCHEMA: CHINA

Network : 10.3.6.0/21

Subnet	IP Allocation
Workstations	10.3.6.1/23 - 10.3.7.255/23
Voice	10.3.8.0/23 - 10.3.9.255/23
Servers	10.3.10.0/28 - 10.3.10.15/28

IP SCHEMA: MALAYSIA

Network : 10.3.14.0/21

Subnet	IP Allocation
Workstations	10.3.14.1/23 - 10.3.15.255/23
Voice	10.3.16.0/23 - 10.3.17.255/23
Servers	10.3.18.0/28 - 10.3.18.15/28

SALES OFFICE: IP SCHEMA

There are 20 sales office(small and medium size) distributed across the each geographical region such as the Americas, Europe and Middle and Asia Pacific.
So in our design we have split it as 5 medium sized and 15 small sized offices in each region.
The total number of employees are distributed across these 20 offices.
The IP schema allocation is 256 IP's are allocated for the medium sized office and 128 IP's are allocated for the small size office. The IP's are allocated in such a way that few of them are left unused for the network to be scalable in the future.
The employees who are mobile will obtain the IP address using the DHCP protocol

IP SCHEMA IN A MEDIUM SIZED SALES OFFICE: AMERICAS

MEDIUM SIZED SALE OFFICE 1:
Network : 10.1.22.0/24

Subnet	IP Allocation
Workstations	10.1.22.1/26 - 10.1.22.63/26
Voice	10.1.22.64/26- 0.1.22.127/26
Servers	10.1.22.128/28- 10.1.22.143/28

Similarly the same kind of allocation is done for the remaining 4 medium sized office in Americas with the following IP distribution.
The individual IP distribution for the workstations, voice and the servers are same as above but the network prefix alone changes as it is given below.

MEDIUM SIZED SALE OFFICE 2:
Network : 10.1.23.0/24
MEDIUM SIZED SALE OFFICE 3:
Network : 10.1.24.0/24
MEDIUM SIZED SALE OFFICE 4:
Network : 10.1.25.0/24
MEDIUM SIZED SALE OFFICE 5:
Network : 10.1.26.0/24

IP SCHEMA IN A SMALL SIZED SALES OFFICE: AMERICAS
SMALL SIZED SALE OFFICE 1:
Network : 10.1.27.0/25

Subnet	IP Allocation
Workstations	10.1.27.1/27 - 10.1.27.31/27
Voice	10.1.27.32/27 - 10.1.27.63/27
Servers	10.1.27.64/28 - 10.1.27.87/28

Similarly the same kind of allocation is done for the remaining 14 small sized office in Americas with the following IP distribution.
The individual IP distribution for the workstations, voice and the servers are same as above but the network prefix alone changes as it is given below.

SMALL SIZED SALE OFFICE 2:
Network : 10.1.28.0/25
SMALL SIZED SALE OFFICE 3:
Network : 10.1.29.0/25
SMALL SIZED SALE OFFICE 4:
Network : 10.1.30.0/25
SMALL SIZED SALE OFFICE 5:
Network : 10.1.31.0/25
SMALL SIZED SALE OFFICE 6:
Network : 10.1.32.0/25
SMALL SIZED SALE OFFICE 7:
Network : 10.1.33.0/25

SMALL SIZED SALE OFFICE 8:
Network : 10.1.34.0/25
SMALL SIZED SALE OFFICE 9:
Network : 10.1.35.0/25
SMALL SIZED SALE OFFICE 10:
Network : 10.1.36.0/25
SMALL SIZED SALE OFFICE 11:
Network : 10.1.37.0/25
SMALL SIZED SALE OFFICE 12:
Network : 10.1.38.0/25
SMALL SIZED SALE OFFICE 13:
Network : 10.1.39.0/25
SMALL SIZED SALE OFFICE 14:
Network : 10.1.40.0/25
SMALL SIZED SALE OFFICE 15:
Network : 10.1.41.0/25

IP SCHEMA IN A MEDIUM SIZED SALES OFFICE: EUROPE AND MIDDLE EAST
MEDIUM SIZED SALE OFFICE 1:
Network : 10.2.22.0/24

Subnet	IP Allocation
Workstations	10.2.22.1/26 - 10.2.22.63/26
Voice	10.2.22.64/26-10.2.22.127/26
Servers	10.2.22.128/28- 10.2.22.143/28

Similarly the same kind of allocation is done for the remaining 4 medium sized office in Americas with the following IP distribution.

The individual IP distribution for the workstations, voice and the servers are same as above but the network prefix alone changes as it is given below.

MEDIUM SIZED SALE OFFICE 2:
Network : 10.2.23.0/24
MEDIUM SIZED SALE OFFICE 3:
Network : 10.2.24.0/24
MEDIUM SIZED SALE OFFICE 4:
Network : 10.2.25.0/24
MEDIUM SIZED SALE OFFICE 5:
Network : 10.2.26.0/24

IP SCHEMA IN A SMALL SIZED SALES OFFICE: EUROPE AND MIDDLE EAST
SMALL SIZED SALE OFFICE 1:
Network : 10.2.27.0/25

Subnet	IP Allocation
Workstations	10.2.27.1/27 - 10.2.27.31/27
Voice	10.2.27.32/27 - 10.2.27.63/27
Servers	10.2.27.64/28 - 10.2.27.87/28

Similarly the same kind of allocation is done for the remaining 14 small sized office in Americas with the following IP distribution.
The individual IP distribution for the workstations, voice and the servers are same as above but the network prefix alone changes as it is given below.

SMALL SIZED SALE OFFICE 2:
Network : 10.2.28.0/25
SMALL SIZED SALE OFFICE 3:
Network : 10.2.29.0/25
SMALL SIZED SALE OFFICE 4:
Network : 10.2.30.0/25
SMALL SIZED SALE OFFICE 5:
Network : 10.2.31.0/25
SMALL SIZED SALE OFFICE 6:
Network : 10.2.32.0/25
SMALL SIZED SALE OFFICE 7:
Network : 10.2.33.0/25
SMALL SIZED SALE OFFICE 8:
Network : 10.2.34.0/25
SMALL SIZED SALE OFFICE 9:
Network : 10.2.35.0/25
SMALL SIZED SALE OFFICE 10:
Network : 10.2.36.0/25
SMALL SIZED SALE OFFICE 11:
Network : 10.2.37.0/25
SMALL SIZED SALE OFFICE 12:
Network : 10.2.38.0/25
SMALL SIZED SALE OFFICE 13:
Network : 10.2.39.0/25
SMALL SIZED SALE OFFICE 14:
Network : 10.2.40.0/25
SMALL SIZED SALE OFFICE 15:
Network : 10.2.41.0/25

IP SCHEMA IN A MEDIUM SIZED SALES OFFICE: ASIA PACIFIC
MEDIUM SIZED SALE OFFICE 1:
Network : 10.3.22.0/24

Subnet	IP Allocation
Workstations	10.3.22.1/26 - 10.3.22.63/26
Voice	10.3.22.64/26- 0.3.22.127/26
Servers	10.3.22.128/28-0.3.22.143/28

Similarly the same kind of allocation is done for the remaining 4 medium sized office in Americas with the following IP distribution.
The individual IP distribution for the workstations, voice and the servers are same as above but the network prefix alone changes as it is given below.

MEDIUM SIZED SALE OFFICE 2:
Network : 10.3.23.0/24

MEDIUM SIZED SALE OFFICE 3:
Network : 10.3.24.0/24
MEDIUM SIZED SALE OFFICE 4:
Network : 10.3.25.0/24
MEDIUM SIZED SALE OFFICE 5:
Network : 10.3.26.0/24

IP SCHEMA IN A SMALL SIZED SALES OFFICE: EUROPE AND MIDDLE EAST
SMALL SIZED SALE OFFICE 1:
Network : 10.3.27.0/25

Subnet	IP Allocation
Workstations	10.3.27.1/27 - 10.3.27.31/27
Voice	10.3.27.32/27 - 10.3.27.63/27
Servers	10.3.27.64/28 - 10.3.27.87/28

Similarly the same kind of allocation is done for the remaining 14 small sized office in Americas with the following IP distribution.
The individual IP distribution for the workstations, voice and the servers are same as above but the network prefix alone changes as it is given below.

SMALL SIZED SALE OFFICE 2:
Network : 10.3.28.0/25
SMALL SIZED SALE OFFICE 3:
Network : 10.3.29.0/25
SMALL SIZED SALE OFFICE 4:
Network : 10.3.30.0/25
SMALL SIZED SALE OFFICE 5:
Network : 10.3.31.0/25
SMALL SIZED SALE OFFICE 6:
Network : 10.3.32.0/25
SMALL SIZED SALE OFFICE 7:
Network : 10.3.33.0/25
SMALL SIZED SALE OFFICE 8:
Network : 10.3.34.0/25
SMALL SIZED SALE OFFICE 9:
Network : 10.3.35.0/25
SMALL SIZED SALE OFFICE 10:
Network : 10.3.36.0/25
SMALL SIZED SALE OFFICE 11:
Network : 10.3.37.0/25
SMALL SIZED SALE OFFICE 12:
Network : 10.3.38.0/25
SMALL SIZED SALE OFFICE 13:
Network : 10.3.39.0/25
SMALL SIZED SALE OFFICE 14:
Network : 10.3.40.0/25
SMALL SIZED SALE OFFICE 15:
Network : 10.3.41.0/25

SOFTWARE DEVELOPMENT CENTER: IP SCHEMA

The software development centers are available in the Asia Pacific region of India, Pakistan and Russia.
A total of 512 IP's are assigned to each location. The unused IP's are used for the purpose of scalability in the future.

IP SCHEMA IN A SOFTWARE DEVELOPMENT CENTER: INDIA
Network : 10.3.42.0/23

Subnet	IP Allocation
Workstations	10.3.42.1/25 - 10.3.42.127/25
Voice	10.3.42.128/25- 10.3.42.255/25
Servers	10.3.43.0/28 - 10.3.43.15/28

IP SCHEMA IN A SOFTWARE DEVELOPMENT CENTER: PAKISTAN
Network : 10.3.44.0/23

Subnet	IP Allocation
Workstations	10.3.46.1/25 - 10.3.46.127/25
Voice	10.3.46.128/25- 10.3.46.255/25
Servers	10.3.46.0/28 - 10.3.46.15/28

DATA CENTER 1:
Network : 10.1.42.0/25

Subnet	IP Allocation
Workstations	10.1.42.1/27 - 10.1.42.32/27
Voice	10.1.42.33/27 - 10.1.42.64/27
Servers	10.1.42.65/28 - 10.1.42.80/28

DATA CENTER 2:
Network : 10.2.42.0/25

Subnet	IP Allocation
Workstations	10.2.42.1/27 - 10.2.42.32/27
Voice	10.2.42.33/27 - 10.2.42.64/27
Servers	10.2.42.65/28 - 10.2.42.80/28

DATA CENTER 3:
Network : 10.3.47.0/25

Subnet	IP Allocation
Workstations	10.3.47.1/27 - 10.3.47.32/27
Voice	10.3.47.33/27 - 10.3.47.64/27
Servers	10.3.47.65/28 - 10.3.47.80/28

DATA CENTER 1(MPLS LINK):
Network : 10.4.0.0/25

Subnet	IP Allocation
Servers	10.4.0.1/27 - 10.4.0.31/27

DATA CENTER 2 (MPLS LINK):
Network : 10.4.1.0/25

Subnet	IP Allocation
Servers	10.4.1.1/27- 10.4.1.31/27

DATA CENTER 3 (MPLS LINK) :
Network : 10.4.2.0/25

Subnet	IP Allocation
Servers	10.4.2.1/27 - 10.4.2.31/27

IV. Internet Service Provider (ISP) edge:

Every location which has the enterprise network is backed up with an extra ISP. The network diagrams above have shown a single ISP. The network diagram with duplicate ISP:

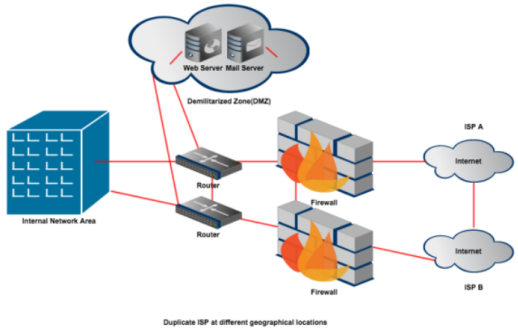

Fig.10 ISP

The list of duplicate ISP for every location is as follows:

Location	Internet Service Providers
New Jersey	Verizon, Comcast
London	British telecom, Virgin Media
Singapore	M1/MyRepublic, SingTel
New York	Verizon, Comcast
Zurich	Cablecom, Swisscom
Melbourne	iiNet/Internode, ADSLplus

V. Virtual LAN (VLAN) and Virtual Private Network (VPN)

In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a **virtual local area network**, **virtual LAN** or **VLAN**.

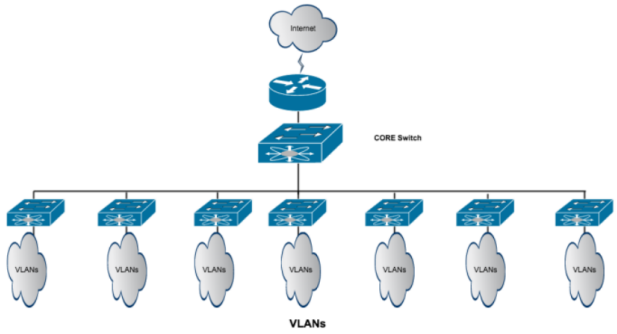

Fig.11 VLAN

VPN (Virtual Private Network)

Technically, all of these technologies are virtual private networks, but when we say VPN I mean a wide area network created by using encrypted "tunnels" over the public Internet. Your VPN is created using Internet Protocol (IP) and will be set up by your IT department, IT consultant, or managed firewall service provider.

Advantages

- A VPN keeps data safe as it crosses the public Internet by using encryption such as IP-Sec, PPP, or SSL, and is secure if properly configured, although perhaps not quite as secure as the other technologies.
- VPN's are carrier agnostic and work seamlessly across multiple networks. All you need is a working business broadband Internet connection with a publicly routed IP address.
- Because it uses your existing Internet connection, a VPN tunnel is cheapest to set up and configure and coverage includes anyplace you can get a broadband Internet connection.

Disadvantages

- Because VPN's use the Internet to get data from location to location it is subject to network congestion and other issues that can slow your connection down.
- You can configure your premise router to provide QoS prioritization to protect voice and video service quality, and you can pass that QoS marking on to your ISP. However there is no guarantee that your ISP will honor those QoS markings, and many of the largest providers do not.

VI. Protocols and LAN Technologies

Protocols:

Ethernet is a family of computer networking technologies for local area (LAN) and larger networks. It was commercially introduced in 1980 while it was first standardized in 1983 as IEEE 802.3 and has since been refined to support higher bit rates and longer link distances. Over time, Ethernet has largely replaced competing wired LAN technologies such as token ring, FDDI, and ARCNET. The primary alternative for

contemporary LANs is not a wired standard, but instead a wireless LAN standardized as IEEE 802.11 and also known as Wi-Fi.

Point-to-Point Protocol (**PPP**) is a data link protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption (using ECP, RFC1968), and compression.

Multiprotocol Label Switching (**MPLS**) is a mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (*paths*) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols.

Internet Protocol (**IP**) is the principal communications protocol in the Internet protocol suite for relaying datagram across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

Transmission Control Protocol (**TCP**) is one of the core protocols of the Internet protocol suite (IP), and is so common that the entire suite is often called *TCP/IP*. TCP provides reliable, ordered and error-checked delivery of a stream of octets between programs running on computers connected to a local area network, intranet or the public Internet. It resides at the transport layer.

The **User Datagram Protocol** (**UDP**) is one of the core members of the Internet protocol suite. UDP uses a simple connectionless transmission model with a minimum of protocol mechanism.

Domain Name System (**DNS**) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates domain names, which can be easily memorized by humans, to the numerical IP addresses needed for the purpose of computer services and devices worldwide. The Domain Name System is an essential component of the functionality of most Internet services.

Hypertext Transfer Protocol Secure (**HTTPS**) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications. The main motivation for HTTPS is to prevent wiretapping and man-in-the-middle attacks.

BGP and OSPF

Diagram below depicts the overall WAN scenario which the company should utilize. We have bifurcated the AS (Autonomous systems) according to geographical locations which are talking with each other using OSPF protocol. The continental geographic locations (namely, Americas, Europe and Asia-pacific) use BGP.

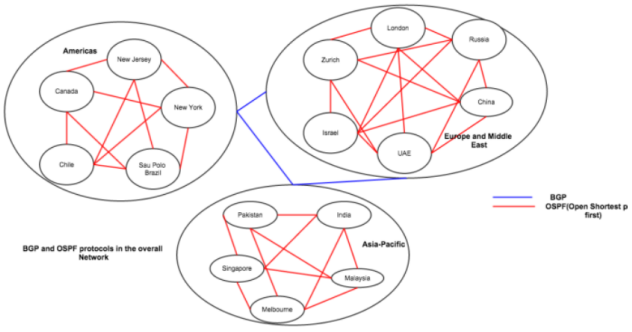

Fig.12 Overall global Network

LAN Technologies:

1. Ethernet - IEEE 802.3

10BASE-T-uses Coaxial cable or Cat-5 Twisted Pair cable with RJ-5 connector

2. Fast Ethernet-IEEE 803.2

100BASE-T - using Cat-5 Twisted pair cable

100BASE-FX - Ethernet over Fibre can be extended up to 100 meters in half-duplex mode and can reach maximum of 2000 meters in full-duplex over multimode fibres.

3. Giga Ethernet (Copper) -IEEE802.3ab

1000BT-standardize Giga-Ethernet over UTP using Cat-5, Cat-5e and Cat-6 cables.

4. Giga Ethernet (Fiber)-IEEE802.3ah 1000SX-defines Giga-Ethernet over Fiber.

5. VLANs - IEEE 802.1Q is the networking standard that supports virtual LANs (VLANs) on an Ethernet network.

6. Link Aggregation Protocol (LAG)-IEEE 802.3ad- for port level protection.

7. Ethernet Automatic Protection Switching- G.8031- used for service level protection per VLAN.Ethernet Automatic Protection Switching (EAPS) is used to create a fault tolerant topology by configuring a primary and secondary path for each VLAN.

8.10 G Ethernet - 802.3ae 10GBASE-LR. 10 G over fiber single mode fibre cable.

VII. Data Centres

There are three data centres according to the new Network architecture. One is located at USA for the region of Americas one is located at Germany for the region of Europe and middle east and the last one is located at Malaysia for the region of Asia Pacific.

Factors that are considered while selecting the location for Data centres are as follows:

Availability and Cost of Electric Power:

Data centers use a large amount of electricity to run equipment. It is important for a company to select a site which provides multiple sources of power and has the current and future capacity to meet the company's needs. In addition, it is important to choose a location with affordable and predictable electric rates, on a comparative basis, to ensure the long-term viability of the prospective location

Natural Disasters/Weather Events:

Generally speaking, companies determining the best location for new data center facilities carefully analyze the potential risk for natural disasters or disruptive weather events. Natural disasters/weather events such as hurricanes, floods, tornados and earthquakes create a lot of concern for data centers. These types of weather events can interrupt data center operations for a lengthy period of time, beyond what is addressed through contingency plans.

Tax Rates:

i. Property Tax Rates**:** Data centres are capital intensive, and it is important to understand the impact of property taxes on the company's on-going operating costs. Property taxes can impact both real estate improvements and equipment investment, depending on the geography under consideration. We use the tax rates history to select the site.

ii. Corporate Income Tax Rates**:** Depending on a state's income tax apportionment structure, a data centre can have a material impact on a company's corporate income tax liability. A number of states have moved to a single sales factor apportionment structure for corporate income taxes. These states have an advantage when it comes to data centres. States that continue to use a property, people and sales apportionment tax structure hit data centre projects harder due to the fact that they are capital intensive.

iii.Sales Taxes**:** States that have high sales tax rates and/or sales taxes that apply to several types of purchases can materially impact a capital intensive project such as a data centre. As a result of sales taxes being charged at the time of transaction, projects are typically impacted well before they are in operation.

Labour Availability/Quality:

It is critical for companies considering where to locate data centre facilities to carefully analyze the availability and quality of labour in the different geographic areas under consideration for the project. Even though data centres typically do not require a large number of employees, a company must have confidence in its ability to secure a workforce capable of helping the company be successful in its operations.

Construction Costs/Quality:

Due to the costs associated with the construction of data centre facilities, companies must understand construction costs in the different geographic areas under consideration. The costs and quality of construction labour has a material impact on data centre projects. .

Telecommunications Infrastructure Availability:

It is vital for companies locating new data centre facilities to have confidence in the ability to be served by redundant telecommunications infrastructure. Access to multiple points of presence, telecommunications "trunk" lines and national carriers is vital to any company operating a data centre.

Quality of Life Amenities:

Vita Pharma data centres need to employ highly skilled workers. Highly skilled workers want to live and work in an environment where they can enjoy quality of life amenities. Data centre workers typically enjoy many types of pursuits during leisure time, but outdoor recreational, music, museums, sports and culturally diverse amenities typically rate high on the list.

Data centres connectivity:

Data centres are connected to each other by using MPLS protocol.

What is MPLS?

Multiprotocol Label Switching (MPLS) is a mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols. MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay, and DSL.

MPLS is a scalable, protocol-independent transport. In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end-to-end circuits across any type of transport. medium, using any protocol.

The primary benefit is to eliminate dependence on a particular OSI model data link layer technology.

MPLS operates at a layer that is generally considered to lie between traditional definitions of layer 2 (data link layer) and layer 3 (network layer), and thus is often referred to as a "layer 2.5" protocol

WHY MPLS?

If you operate a multi-location business, you're usually faced with the challenge of moving data from office to office quickly and securely in some form of Wide Area Network (WAN). Also, in today's environment of converged voice, data and video networks, most IT managers must design their networks to provide Quality of Service (QoS) so that calls are clear and video is skip-free.

Like VPN Tunneling, MPLS uses a router-based protocol to transport data from location to location. Although many operators run their MPLS network on a completely separate network from regular Internet traffic, others may be running their regular Internet network over MPLS. Your IT department or consultant will set up your an MPLS network by first selecting, then coordinating with a carrier that supports MPLS.

Advantages

- MPLS networks offer improved performance vs. VPN tunneling because when you split your data into different categories such as real time traffic, priority traffic, low priority traffic and so on, your carrier will

honor these priorities across its entire network, providing quality of service from end to end.

- MPLS is highly secure, because traffic is segmented from other users on the carrier's network.
- Because MPLS typically involves only one carrier's network, you or your IT vendor has greater ability to troubleshoot issues of network congestion, packet loss, and other performance issues than you do with a VPN. This is sometimes negated when multiple networks must be used in a WAN.

Disadvantages

- There are differences in the design and configuration of MPLS from carrier to carrier, and no one carrier offers ubiquitous coverage for MPLS in Maine. You may run into interoperability issues or pay for long, expensive point to point circuits to connect remote offices.

Metro Ethernet

Unlike VPN's and MPLS networks, Metro Ethernet is not a router based technology. Ethernet operates at the more fundamental transport layer, and creates point to point or point to multi-point paths using switches rather than routers. This means that in an Ethernet WAN, your carrier is essentially handing you a really long network cable, and your IT department, IT consultant, or Managed Router provider builds your own IP network on top of that.

Advantages

- Metro Ethernet networks switch based architecture typically offers lower latency than router-based protocols like MPLS or VPN's, and makers of Metro Ethernet equipment engineer their solutions to support the stringent latency requirements of the Metro Ethernet Forum. This can be very important in real time applications and other areas where milliseconds count.
- Because its underlying architecture is point to point, Ethernet is highly secure and completely segregated from the Internet.
- Metro Ethernet networks offer dedicated bandwidth, giving you the specified data rate from end to end, and allowing you to run your own custom QoS routing scheme without the need to comply with a carrier's MPLS product design. Most carriers can also help by creating discrete VLAN's within your Ethernet network, dedicating a set amount of bandwidth to a set task.

Disadvantages

- Metro Ethernet coverage is not ubiquitous yet, and you may need to use other solutions to connect offices in remote areas. (Today, GWI's Metro Ethernet Network stretches from New York City to Bangor, although other Ethernet products are offered as far north as Madawaska.)
- As with MPLS networks, Metro Ethernet networks can offer interoperability challenges between carriers.

From the analysis above, we conclude to use MPLS as the best option for our project as:

- MPLS provides better performance than VPN.
- MPLS provides high security and troubleshooting requirements for vita Pharma
- Metro Ethernet is not ubiquitous and can cause interoperability issues with the existing structures in the network.

Inter-connections and Links:

Data-centers need high data transfer rate to and from the headquarter's server to the data centers. So, we need high reliability and fast links interconnecting the data centers. For Vita Pharma, links between all data centers (Germany to USA, USA to Malaysia and Malaysia to Germany) will use MPLS (Multi-Protocol Label Switching). Thus we have 3 MPLS links in the network.

Point-to-Point Protocol is used for the links between an employee's workstation of regional headquarters, main office or sales office to the respective switch. Also, from the switches to the servers of the respective regions.

The data is transferred between the Main office server to regional headquarters server and between sales office server to regional headquarter server via the internet.

Operations over MPLS:

When an office personnel wants to fetch information from a data centre of the same region:

- 'Request data' query is send to the switch.
- Switch forwards it to the headquarters' server.
- Server sends this query over the MPLS link to the database's server.
- Server forwards this to the regional

VIII. Bandwidth and Delay

Bandwidth:

Data Usage per workstation(employee) based on the average statistical data report

Heavy Web Browsing: 2 GB/month Online Banking, Reading, etc

Downloads/ Uploads: 1 GB/month Documentation, logs, etc

Software Upgrades: 5 GB/month Up-gradation of software version, etc

Email: Without Attachments-4500/per month (30KB per text message) 135MB/month

With Attachments-10/month (3MB per attachment) 30 MB/month

VoIP: G.711 Codec Bandwidth Requirement-128 kbps

8.165 GB/month per workstation

Delay:
Sum of Processing Delay and Queueing Delay together add up to a very small fraction of the total delay.
It is visible from the statistics collected throughout the globe:

So we assume the average possible value for a single router as the sum of processing delay and queuing delay, that is: 0.51ms + 1.64ms = 2.15ms
For 5 servers : 2.15 * 5 = 10.75ms

Suppose we have

Example:
Propagation speed is in range of 2*10^8 to 3*10^8 > Assume 3*10^8
Distance between London and New York

Delay for Europe(London) to USA(New York)
Propagation delay = D/s = 5576.5*10^3m/3*10Gbps=185ms
Transmission delay = L/R = 1GB*8/100Gbps=80ms
Processing + Queueing delay = 10.75ms
Total delay = 275.85

IX. Security

Security in the whole infrastructure is provided in 2 broad areas:

Data at rest
For the security of static data "Disc Encryption" is applied. Since at the enterprise level we are using Microsoft Windows all the systems will be regularly patched for Microsoft's application "Bit locker Drive Encryption". Bit Locker helps keep everything from documents to passwords safer by encrypting the entire drive that Windows and the data reside on. Once Bit Locker is turned on, any file we save on that drive is encrypted automatically. It can also be used to encrypt the data of removable drives.
Bit locker installed in the systems uses 256-bit AES(symmetric key algorithm). The key used to encrypt data is stored in the Bit Locker metadata on the protected volume. This key is encrypted using another key, namely the Volume Master Key (VMK). Several copies of the VMK are also stored in the metadata. Each copy of the VMK is encrypted using another key, also known as key-protector key. In our machines key-protector key will be the username password of the user. These usernames and passwords are stored in the Active directories present in the network.
Bit locker is installed in the machines which store highly sophisticated data. Such as the machines used by Researchers, Company heads and mobile Sales employees.
Bit locker is most helpful for security of mobile machines which can be compromised in case of losing or theft.

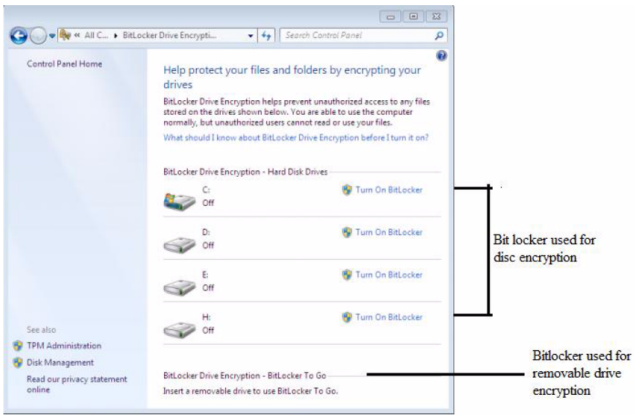

Fig.13 Bitlocker

Data in transit - For the sophisticated data in transit, many measures have been taken throughout the network. For secure transmission of inter-network data transmission following measures has been taken.

Virtual Private Network (VPNs):
VPNs are made for the transfer of sophisticated data in the enterprise. Since, Research Department and Finance department will have the most sophisticated data in transit so these departments will communicate through VPNs.

For Finance and Research departments IPSec VPN is configured in the Cisco Catalyst 6800 series(as mentioned in the network details). IPSec VPN will provide employees who are distributed around the world, a secure and "always on" connectivity that will enable them to access all of the corporate resources they need to achieve over VPN. IPSec works on layer 3 and provides authentication, encryption and confidentiality.

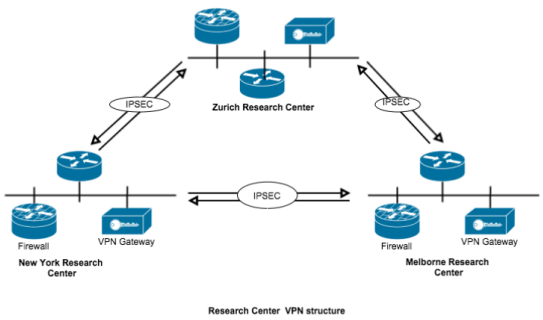

Fig.14 Research centre VPN Structure

A similar plan is configured for the finance department.

Network Perimeter Security:

- The perimeter starts with border part of Internet edge infrastructure which consists of routers that interface

directly to the Internet. Internet-facing border routers peer directly to the Internet SP (service provider).

- For an enterprise safe and secure network is essential. Thus **stateful firewalls** are configured for network security. These firewalls are configured with iptable rules to restrict the ingress and egress traffic in accordance to access control list of the employees. Outer IPs will not have access to the internal Corporate network.
    - IPTable Filter rules are configured for dropping network packets coming from foreign network trying SSH or ICMP PING.
    - When network monitoring(using NAGIOS) detects repeated attacks from a particular IP address, that IP address can be blocked by IPTable configuration.
- Public facing applications are placed in the **Demilitarized zone(DMZ)**. DMZ acts as the middle stage between Internet and enterprise network. This structure helps protecting the internal server and resources from being exposed.
    - Web server and email server is placed in the DMZ.

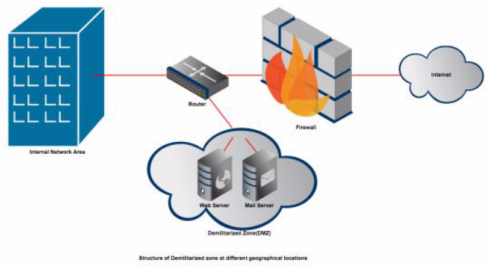

Fig.15 Structure of Demilitarised zone at different geographical locations

Wireless environment security:
Wi-Fi protected Access-2(WPA2), IEEE 802.11i is used in the Wireless environments of the enterprise. It has strongest encryption to date and uses AES(256-bit), which is a very strong block cipher. It includes 4-way handshake between STA(host) and AP(Access Point).Both AP and STA are authenticated.

Using HTTPS for the HR application and Company's website:
HTTPS is HTTP on the top of TLS/SSL protocol.
The HR application will contain very sensitive data such as employee's personal information(social security numbers, names and addresses). Due to this fact the storage and transit of this sophisticated information in plaintext is not advisable. HTTPS would provide authentication while communicating with the HR Departments present at various geographical locations. It will protect against man-in-the-middle attack. HTTPS provides bidirectional encryption which will protect against eavesdropping and tampering.
Similarly, the company website will be protected against man-in-middle attack and eavesdropping by using HTTPS. It will also help to provide the safe payment transactions which are delegated to third-party.

Safe Browsing (Using Citrix Farm VMs):

While network partitioning and firewall rules protect us from direct attacks targeting our servers and network infrastructure, we still need to address another class of attack – the client side attacks.
We provide a secure browsing environment where employees who regularly have to download files or open links from untrusted sources can do so in a manner where we don't expose our CORP workstations to client side attacks. The setup consists of a couple of isolated Citrix farm on an isolated network outside CORP. Employees are trained (mandated in some departments) to open any external/potential risky URLs and files using this external browser. The employee clicks an icon on this computer to invoke the Citrix receiver and gets a browser window on the remote Citrix VM. During the browsing session, if the machine gets infected by a malware, it's the Citrix VM on the isolated network which gets infected and not the CORP workstation. The VM reverts back to a known clean snapshot after the user ends the browser session.

REFERENCES

[1] http://www.cisco.com/c/en/us/support/docs/voice/voice-quality/7934-bwidth-consume.html
[2] http://www.cisco.com/c/en/us/support/docs/voice/voice-quality/7934-bwidth-consume.html
[3] http://www.voip-info.org/wiki/view/Codecs