VIRTUAL PRIVATE NETWORK
-As a popularity of internet grew, business turned into as a means of extending their own network.
-First came Intranet where using password-protected websites designed for use only by company employees.
-Now company creates their own VPN to accommodate the need of remote employees and distant offices.
Introduction

- VPN: A computer network in which some of the links between nodes are carried by virtual circuit in larger network like internet instead of physical wires.

- The link-layer protocols of the virtual network are said to be tunneled through the larger network when this is the case.

- VPN can be used to separate the traffic of different user communities over an underlying network with strong security features.
Benefits of VPN

- Extend geographic connectivity
- Improve security
- Reduce operational costs versus traditional WAN
- Reduce transit time and transportation costs for remote users
- Improve productivity
- Simplify network topology
- Provide global networking opportunities
- Provide telecommuter support
- Provide broadband networking compatibility
- Provide faster ROI (return on investment) than traditional WAN
Essential features in VPN

- Security
- Reliability
- Scalability
- Network management
- Policy management
Characteristics of secure VPN

- Data confidentiality
- Data integrity
- Authentication
Data confidentiality

Tunneling

• Transmission of data through a public network so that routing nodes in the public network are unaware that the transmission is part of a private network.

• It allows the use of public networks to carry data on behalf of users as though the users had access to a private network.

• It is the process of placing an entire packet within another packet and sending the new, composite packet over a network.
Tunneling
Tunneling

The three different protocols that tunneling uses are as follows:

- **Carrier protocol**: The protocol the information is traveling over (Frame-Relay, ATM, MPLS).

- **Encapsulating protocol**: The protocol (GRE, IPsec, L2F, PPTP, L2TP) that is wrapped around the original data.

- **Passenger protocol**: The original data (IPX, AppleTalk, IPv4, IPv6).

  E.g.: postcard delivery
Encryption

• Definition:
Encryption is the process of taking all the data that one computer is sending to another computer and encoding the data into a form that only the intended destination computer will be able to decode.

• Strength based on key

• More secure when key is exchanged frequently
Encryption

Primary methods of encryption:

- Symmetric Key Encryption.
- Asymmetric Encryption.
Symmetric Key Encryption

- Secret Key Encryption: Requires to know secret key to the receiving node.

- A secret Key (code) is used to encrypt the data. Sending computer encrypts data using this key.

- Example: Secret key is "Shift by 2"

- Drawback: Involves exchanging secret keys across the very insecure Internet.
Asymmetric Encryption

- Uses combination of private key and public key.

- Private key is known to dedicated computer only.

- To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key.
TYPES OF VPN
Types Of VPN

- Remote Access VPN.
- Site-to-Site VPN.
Remote Access VPN

Client-Initiated Remote Access VPNs

Main Office

VPN Cloud (internet, IP)

VPN Router

IPSec/PPTP/L2TP

Tunnel

Tunnel

1.2TP/L2F

NAS

PSTN

NAS-Initiated Tunnel

Client-Initiated Tunnel
Remote Access VPN

- Also called as Virtual Private Dial-up Network (VPDN).
- It is a user-to-LAN connection: For connecting private network from remote location.
- To setup Remote Access, VPN is outsourced by Enterprise service provider (ESP).
- ESP sets up network access server (NAS) and provides to remote user with desktop client software for their users.
- Toll free number used to reach to NAS.
- Provides secure encrypted connection between company's private network and users by third party service provider.
Site-to-Site VPN: Intranet
Site-to-Site VPN: Extranet
Site-to-Site VPN

- Through the use of dedicated equipments and large scale encryption, company can connect more fixed sites over a public network like internet.

- Intranet-Based: if a company has branches at remote location to connect them company can use intranet-based VPN to connect LAN to LAN.

- Extranet-Based: if a company has close relationship with their suppliers, partners, clients company can use extranet VPN to connect LAN to LAN, and allow companies to work in a shared environment.
Mobile VPN

- Host Identity Protocol (HIP) supports mobile VPN
- Designed for mobile and wireless users.
- They integrate standards-based authentication and encryption technologies to secure data transmissions to and from devices and to protect networks from unauthorized users.
- Mobile VPNs allow users to roam seamlessly across IP-based networks and in and out of wireless coverage areas without losing application sessions or dropping the secure VPN session
**MPLS-VPN**

- **Problem:**
  - Layer 2 VPN technology does not scale well.
  - It is also difficult to provide traffic engineering using a Layer 2 VPN approach.

- **Solution:**
  - A border gateway protocol/multiprotocol label switching (BGP/MPLS) VPN standard is now being adopted to provide Layer 3 VPN solutions using BGP to carry route information over a MPLS core.
  - This Layer 3 MPLS-VPN solution achieves all of the security of the Layer 2 approach, while adding enhanced scalability inherent in the use of Layer 3 routing technology.
Tunneling: Site-to-Site

- General Routing Encapsulation (GRE) is the encapsulation protocol.
- Provides framework for how to package the passenger protocol over the carrier protocol which is typically IP based.
- Includes information what type of packet and information about the client and server.
- Instead of GRE, IPSec in tunnel mode is used as a encapsulating protocol.
Tunneling: Remote-Access

- Relies on Point to point (PPP) protocol.

- Protocol based on PPP
  - L2F (Layer2 Forwarding)
  - PPTP (Point to Point Tunneling Protocol)
  - L2TP (Layer2 Tunneling Protocol)
Protocols in VPN

PPTP and L2TP:

- **PPTP: Point to Point Tunneling Protocol**
  - Popular and easy to configure, first VPN protocol that was supported by Microsoft Dial-up Networking.
  - Relies on the protocol being tunneled to provide privacy.
  - Does not provide confidentiality or encryption.
  - Has been made obsolete by Layer 2 Tunneling Protocol (L2TP) and IPSec.

- **L2TP: Layer 2 Tunneling Protocol**
  - At the time of setup of L2TP connection, many control packets are exchanged between server and client to establish tunnel and session for each direction.
  - Then using this tunnel and session id, data packets are exchanged with the compressed PPP frames as payload.
  - The entire L2TP packet, including payload and L2TP header, is sent within a UDP datagram
Protocols in VPN

**IPSec:**
- A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
- An end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite.
- Used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

**L2F:** Layer 2 Forwarding
- Proprietary Cisco tunneling protocol
- Uses any authentication supported by PPP, but does not support encryption.
General security risks

- User-credential-related risks
- Spread of viruses, worms, and Trojans from remote computers to the internal network
- Split tunneling
- Lack of required host security software on public machines
- Physical access to shared machines
- Keystroke loggers
- Endpoints—loss of sensitive information and intellectual property
- Man-in-the-middle attacks
- Hardware limitation
• **Username Enumeration Vulnerabilities**  
  Allow valid usernames to be guessed through a dictionary attack

• **Offline password cracking**  
  A valid password is obtained using IKE Aggressive Mode

• **VPNs are an attractive target to hackers**  
  VPNs often allow full access to the internal network, while VPN traffic is usually invisible to IDS monitoring.

• **Security practices**  
  The majorities of VPN vendors still allow their implementations to leak information
Risk mitigation

- Security policies and secure access through strong user authentication
- Host identity verification
- Secure desktop
- Cache cleaning
- Keystroke logger detection
- Configuration consideration
VPN GLOBAL SCENARIO
## Global Providers and their services

<table>
<thead>
<tr>
<th>Provider</th>
<th>International site-to-site MPLS VPN services</th>
<th>International site-to-site Layer 2 MPLS VPN (Ethernet services)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT&amp;T</td>
<td>AVPN (AT&amp;T VPN) EVPN (Enhanced VPN)</td>
<td>OPT-E-WAN (VPLS)</td>
</tr>
<tr>
<td>BT Global Services</td>
<td>iVPN (Intelligent VPN) MPLS 6COS (BT) IP VPN Secure (BT Infonet) AC VPN (BT Infonet)</td>
<td>Global Etherflow EPL Global Etherflow EVPL EVLAN (VPLS, planned in 2010)</td>
</tr>
<tr>
<td>Cable &amp; Wireless</td>
<td>IPVPN</td>
<td>Ethernet Wireline (VPWS) Ethernet VPN (VPLS)</td>
</tr>
<tr>
<td>NTT Communications</td>
<td>Arcstar Global IP-VPN</td>
<td>Vlink (E-Line) Global eVLAN (E-LAN)</td>
</tr>
<tr>
<td>Orange Business Services</td>
<td>MPLS IP VPN</td>
<td>International Ethernet Link (E-Line) International Ethernet Link (VPLS E-LAN) (by end of 2009)</td>
</tr>
<tr>
<td>Sprint</td>
<td>Global MPLS VPN</td>
<td>SprintLink V-LAN (over L2TPv3)</td>
</tr>
<tr>
<td>T-Systems</td>
<td>Intraselect IP VPN</td>
<td>Ethernet VPN (E-Line) Ethernet VPN (E-LAN) (by end of 2009)</td>
</tr>
<tr>
<td>Verizon Business</td>
<td>Private IP VPN (PIP)</td>
<td>Ethernet Virtual Private Line (select countries) Ethernet VPLS (select countries by end of 2009)</td>
</tr>
</tbody>
</table>
Global Scenario

- The Leaders include AT&T, BT Global Services, Orange Business Services, and Verizon Business.
- AT&T had the highest scores in both strategy and market presence, while Orange had the highest score in current offering.
- T-Systems gained considerable ground since our last evaluation, especially in strategy and market presence.
- Sprint, Cable & Wireless, and NTT Communications regressed somewhat as global players, facing very tough competition in a now mature market.
• There are other providers, such as
  • Virtela, which sells end-to-end managed global MPLS services in the US market
  • Macquarie, which does the same in Australia
  • the global virtual network operator Vanco (now a unit of the new Indian-based global telecom player, Reliance Globalcom, which also acquired US Ethernet provider, Yipes!)
  • another Indian newcomer, Tata Communications (a sister company of IT outsourcer Tata Consulting Services)
  • Experienced global network integration specialists like Dimension Data,
SCENARIO IN EUROPEAN COUNTRIES

• The Leaders were AT&T, BT Global Services, Colt, Orange Business Services, and Verizon Business. Verizon Business led with the best overall combination of current offering, strategy, and market presence.

• Easynet, Global Crossing, Interoute, KPN, Reliance Globalcom, Telefónica, and T-Systems were ranked as Strong Performers.
<table>
<thead>
<tr>
<th>Vendor</th>
<th>Ranking</th>
<th>Best suited for</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>European former national carriers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BT Global Services</td>
<td>Leader</td>
<td>European-based MNCs looking a strong all-around provider for telecoms and IT</td>
</tr>
<tr>
<td>KPN International</td>
<td>Strong Performer</td>
<td>Benelux firms looking to procure converged Ethernet and IP networks</td>
</tr>
<tr>
<td>Orange Business Services</td>
<td>Leader</td>
<td>European firms looking for the widest geographic coverage in Europe and beyond</td>
</tr>
<tr>
<td>Telefónica</td>
<td>Strong Performer</td>
<td>European firms with a major requirement for mobile services</td>
</tr>
<tr>
<td>T-Systems</td>
<td>Strong Performer</td>
<td>European firms looking to outsource telecoms and IT to one supplier</td>
</tr>
<tr>
<td><strong>US-based carriers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>Leader</td>
<td>European firms looking for European and US coverage with strong SLAs</td>
</tr>
<tr>
<td>Global Crossing</td>
<td>Strong Performer</td>
<td>UK-centric firms looking for network-based services like VoIP</td>
</tr>
<tr>
<td>Verizon Business</td>
<td>Leader</td>
<td>European firms looking for converged services with aggressive SLAs</td>
</tr>
<tr>
<td><strong>European alternative carriers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Colt</td>
<td>Leader</td>
<td>European firms looking for aggressive Ethernet performance and best prices</td>
</tr>
<tr>
<td>Easynet</td>
<td>Strong Performer</td>
<td>European firms with large branch networks looking to lower their network costs</td>
</tr>
<tr>
<td>Interoute</td>
<td>Strong Performer</td>
<td>European firms looking for an innovative alternative supplier with keen prices</td>
</tr>
<tr>
<td><strong>Asian-based carrier</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reliance Globalcom</td>
<td>Strong Performer</td>
<td>European firms looking for connectivity to Asia with keen prices</td>
</tr>
</tbody>
</table>
IMPLEMENTATION OF VPN STATUS IN INDIA
The Indian Scenario

In India MNCs have been the first adopters of VPN technology as they can connect seamlessly into the networks of their parent organizations for global efficiencies.

Following Industries are using VPN Technology:-

- IT Industry
- Banking and e-commerce.
- FMCG vertical
- Healthcare segment
- Retail industry
Major VPN Players in India

1. Tulip Connect
2. NTT Communications (NTT Com)
3. Railtel Corporation of India
4. Bharti Airtel
5. Sify Limited
6. BSNL
7. Reliance
8. HCL Infinet
Tulip Connect

Tulip is India’s largest MPLS VPN player and has been the front-runner in provisioning and managing multi location wide area networks for various industry verticals.

Tulip Telecom has won the Frost & Sullivan Growth Leadership Award for Enterprise Data Services (MPLS VPN) 2009, the 3rd time in a row

It is the only network in the country offering MPLS VPN services to over 2000 locations in India.

The Core network of Tulip consists of high speed interconnects between the twelve major cities in India.
NTT Communications

NTT Com has worked with Tata Communications, a telecommunications carrier in India since May 2004, to establish POP facilities in Bangalore, Mumbai and New Delhi.

In December 2009, NTT Communications launched an international IP-VPN service POP in Chennai, a major city in southern India, for its Arcstar™ Global IP-VPN.

In April 2009, the 5th branch office for NTT Communications India Private Ltd. (Head office: New Delhi, further referred to as NTT Com India) was opened in Neemrana, Rajasthan.
Railtel Corporation of India

- Railtel Corporation of India is a Government of India enterprise focusing on providing broadband and VPN services.
- IP services are extended through carrier Ethernet networks at all the locations, interconnected to MPLS –IP CORE network at the 36 important cities.
Sify Limited

- Sify is the first MPLS-enabled network service provider in India.

- The different VPN services that Sify provides include IP-VPN services, Dedicated Internet Access services, and VoIP services.

- Sify offers *ExpressConnect, ExpressTalk*

- Sify Wins the Frost & Sullivan Market Leadership Award for IP VPN Services; Continues Leadership of the IP VPN Market in India for Second Consecutive Year.

BSNL

- BSNL has introduced unlimited and concessional VPN packages between BSNL fixed and BSNL cellular service with effect from 1st May 2007.
MARKET OUTLOOK
VPN Business Segment in India

- The data services market was estimated to be around Rs. 6,051 crore in FY’ 09 and is estimated to reach Rs. 16,779 crore by FY’ 14 with a CAGR of 22.6%

- The growth of data market is driven by MPLS/VPN market which is expected to be about 58% of the overall enterprise data services market by FY’ 14

- IT/ITeS, BPOs, KPOs, Retail, Govt. establishments, etc. have been the main growth areas for the VPN technology in India

<table>
<thead>
<tr>
<th>Company</th>
<th>Share (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2008*</td>
</tr>
<tr>
<td>Tulip Telecom</td>
<td>27.2</td>
</tr>
<tr>
<td>Sify</td>
<td>15</td>
</tr>
<tr>
<td>Reliance</td>
<td>17.5</td>
</tr>
<tr>
<td>Bharti</td>
<td>8.1</td>
</tr>
<tr>
<td>VSNL</td>
<td>7.1</td>
</tr>
<tr>
<td>BSNL</td>
<td>12.4</td>
</tr>
<tr>
<td>Others</td>
<td>12.7</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
</tr>
</tbody>
</table>

Source : Frost & Sullivan
## VPN Business segment globally

<table>
<thead>
<tr>
<th>Provider</th>
<th>Countries with own MPLS</th>
<th>Countries with Ethernet access</th>
<th>Market capitalization (of group) on March 31, 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT&amp;T</td>
<td>163</td>
<td>37</td>
<td>$149 billion</td>
</tr>
<tr>
<td>BT Global Services</td>
<td>65</td>
<td>37</td>
<td>£6.1 billion (£8.67 billion)</td>
</tr>
<tr>
<td>Cable &amp; Wireless</td>
<td>34</td>
<td>43</td>
<td>£4.83 billion (£6.87 billion)</td>
</tr>
<tr>
<td>Global Crossing</td>
<td>45</td>
<td>26 (55 with NNI1s)</td>
<td>$605 million</td>
</tr>
<tr>
<td>NTT Communications</td>
<td>21</td>
<td>33</td>
<td>$60.2 billion (equivalent)</td>
</tr>
<tr>
<td>Orange Business Services</td>
<td>197</td>
<td>32</td>
<td>€44.84 billion (£59.23 billion)</td>
</tr>
<tr>
<td>Sprint</td>
<td>34</td>
<td>31</td>
<td>$10.2 billion</td>
</tr>
<tr>
<td>T-Systems</td>
<td>47</td>
<td>26</td>
<td>€40.78 billion (£53.9 billion)</td>
</tr>
<tr>
<td>Verizon Business</td>
<td>155</td>
<td>43</td>
<td>$85.78 billion</td>
</tr>
</tbody>
</table>
Positioning of global VPN players (Forrester Research)
Gartner’s Magic Quadrant for SSL VPN (Dec-2010)
Future of VPN: Enterprise Mobility

- Cisco Anyconnect secure mobility solution
  - Provides a comprehensive, highly secure enterprise mobility solution
  - Combines Cisco web security with next-generation remote access technology
  - Users can choose the devices to access the network (laptops, handhelds, smartphones, etc.)
  - Anyconnect solution can be downloaded from Cisco’s website or as an application from the App store for smartphones and handhelds
  - Automatically select the optimal network access point
  - Adapt its tunneling protocol to the most efficient method
  - Helps enable built-in web security and malware threat defense
Conclusion (1/2)

Enterprise networks are moving away from traditional TDM based private network to MPLS based IP VPN network.

![Enterprise Data Services Market in India](chart.png)
Conclusion (2/2)

- VPN as a reliable substitute to security problems on the internet.

- Generating immediate cost-reduction opportunities in long distance charges, leased line fees and network support requirements.

- Indian companies are looking to build regional or global networks with the help of IP-VPN technology as they expand their operations overseas.

- VPN networks are robust, secure, scalable, flexible, cost-effective and easier to maintain in the long run.

- With a VPN, organizations can see immediate cost-reduction opportunities in their long distance charges, leased line fees, equipment inventories (like large bank of modems) and network support requirements.

- VPNs represent the next generation in terms of communications networks, and will power the future of business and governance with the convergence of voice, video and data services over IP networks.
Thank You