

WAN Technologies

- ❑ Dial-up modem connections
 - Cheap
 - Slow
 - A phone line, a modem at each end

WAN Technologies

- ❑ Integrated Services Digital network (ISDN)
 - Higher cost
 - Faster
 - A special phone line
 - Interface standards
 - Basic Rate Interface (BRI)
 - Uses three separate channels
 - » Two bearer channels of 64Kbps carrying the voice/data
 - » A delta channel of 16Kbps for signaling
 - Primary Rate Interface (PRI)
 - Uses 23 bearer channels of 64kbps for data/voice
 - Uses one 64kbps delta channel for signaling

WAN Technologies

□ T-carrier lines

- High-speed lines
- Can be leased from telephone companies
- Are often used to create private networks
- Four types
 - T1
 - Offers speed of 1.544Mbps
 - Connects LANS
 - T2
 - Offers speed of 6.312Mbps
 - Uses 96 64Kbps B channels
 - T3
 - Offers speed of 44.736Mbps
 - Uses 672 64Kbps B channels
 - T4
 - Offers speed of 274.176Mbps
 - Uses 4,032 64Kbps B channels
 - T5
 - Offers speed of 400.352Mbps
 - Uses 5,760 64Kbps B channels

WAN Technologies

❑ Fiber Distributed Data Interface (FDDI)

- Uses fiber-optic cable
 - Resistance to EMI
 - Can use copper cable too
- Uses token-passing media access
 - Dual-ring for redundancy and fault tolerance
- Reaches 100Mbps at distance of two kilometers
- Hard to implement and high cost

WAN Technologies

❑ X.25

- old
- Packet-switching
 - Each packet is likely to take a different route to reach its destination during a single communication session.
- Only 56Kbps - was fast in 1970's

WAN Technologies

❑ Asynchronous transfer Mode (ATM)

- For voice, data and video
- Packet-switching technology
 - Use fixed-length packets of 53bytes (5+48)
- Provides speeds from 1.544Mbps to 622Mbps
- Circuit-based network technology
 - Switched virtual circuits (SVCs)
 - Permanent virtual circuits (PVCs)
- Expensive hardware to disassemble and assemble cells
- High overhead (due to fixed cell with padding)
- Still good to not so high speed connection

❑ Ip Over ATM

- Atmarp server

❑ LAN Emulation with ATM

- Broadcast and multicast support mechanism

WAN Technologies

❑ Frame relay

- Packet-switching technology
- Uses variable-length packets
- Offers speeds starting at 56kbps
- Using PVC

WAN Technologies

❑ SONET/OC-x levels

- Bell Communication Research developed SONET (Synchronous Optical Network)
 - Physical layer network technology to carry large volumes of traffic over relatively long distances on fiber optic cabling
 - Internet backbone
 - Point-to-point lease lines
- Optical Carrier (OC) levels
 - OC-1 51.84Mbps
 - OC-3 155.52Mbps
 - OC-12 622.08Mbps
 - OC-24 1.244Gbps
 - OC-48 2.488Gbps
 - OC-192 9.953Gbps
 - OC-768 40Gbps

Security protocols - SSL

- ❑ Secure Sockets layer (SSL)
 - Server authentication
 - Client authentication
 - Encrypted connections
 - Above the network layer
 - Only for applications that can use SSL
 - Web browsers

Security protocols - IPSec

❑ IP Security (IPSec)

- Created by IETF
- Works on both IPv4 and IPv6
- Provides three key security services
 - Integrity
 - hash algorithm applied to key + IP datagram
 - Confidentiality
 - Standard symmetric encryption algorithms
 - Private transactions, again denial of service attack
 - Sliding window and sequence number

Security protocols - IPSec

- Operates at the network layer
 - Can secure practically all TCP/IP related communications
- Two modes:
 - Transportation
 - | IP | AH | TCP | DATA |
 - Tunnel
 - | New IP | AH | IP | TCP | DATA |
- Protocols
 - Authentication Header (AH)
 - Encapsulated Security Payload (ESP)
 - Internet key exchange (IKE) protocol
 - Authentication of the peers and the exchange of the symmetric keys.

Security protocols

- ❑ Point to point Tunneling protocol (PPTP)
 - Creates a secure transmission tunnel between two points on a network
 - Creates multi-protocol Virtual Private Network(VPNs)
 - Requires to establish a PPTP session using port 1723
- ❑ Layer 2 Forwarding (L2F)
 - Developed by Cisco
 - Allows tunneling to be utilized
- ❑ Layer 2 Tunneling Protocol (L2TP)
 - Is a combination of PPTP and Cisco's L2F technology
 - Authenticates the client in two-phase process
 - Computer
 - User
 - Operates at the data-link layer

Security protocols

- ❑ The advantages of PPTP and L2TP
 - PPTP
 - More interoperability
 - Easier to configure
 - Less overhead
 - L2TP
 - greater security
 - common public key infrastructure technology
 - header compression

Security protocols

□ Kerberos

- Network authentication protocol
- Ensure the authentication data is encrypted
- Default authentication method for Windows 2000 and Windows XP

Configuring remote connectivity

❑ Physical connections

- Public switched telephone network (PSTN)
 - A modem
 - The plain old telephone system (POTS)
- Integrated Services Digital Network (ISDN)
 - Digital signals
- Cable
 - Broadband internet access over TV cable
- DSL
 - Broadband offering from telecom companies
- Satellite

Remote access protocols

- ❑ Remote Access Service (RAS)
 - Is a Windows Solution
 - Any client with dial-in protocols can connect to RAS
 - Uses SLIP and PPP as underlying technologies
- ❑ SLIP
- ❑ PPP
- ❑ Point to point Tunneling protocol (PPTP)

Configuring remote connectivity

□ Protocols

- Data link layer
 - PPP
 - SLIP
 - PPPoE
- Network-layer and transport-layer protocols
 - TCP/IP
 - IPX/SPX

VPN

- ❑ What is a virtual private network (VPN)?
 - Allows two or more private networks to be connected over a publicly accessed network.
 - Can be build over ATM, frame relay, X.25, IP-based network, etc.
 - Have save security and encryption features as a private network.
 - Encryption
 - Authentication
 - Network tunneling
 - IPSec, PPTP, L2TP

VPN

❑ How to choose a VPN?

- Leased line?
- Managed VPN?
 - Implement your own VPN?
 - Outsource?
- Check the service provided vs. required?
 - Service level agreement can be tricky
 - 99.999% connectivity
 - No guarantee once the packet crosses over to another ISP
 - Encryption level
 - Site to site VPN
 - Performance, security and manageability
 - Remote user to LAN
 - Easy of use

VPN

- ❑ How a virtual private network works
 - Traffic reach the network backbone using
 - T1, frame relay, ISDN, ATM, dial-up
 - Reach a tunnel initiating device, which communicate with a VPN terminator to agree on an encryption scheme.
 - The tunnel initiator then encrypt the package before transmitting to the terminator
 - Terminator decrypts the packet and delivers it to the appropriate destination on the network.

VPN

❑ The advantage of a VPN

○ Cost savings

- No longer to purchase expensive leased lines
- Flexibility for growth
- Reduce long-distance telephone charges
 - Call local number of server provider's access point
- Reduce support burden
- Equipment costs - modem, remote access server, wan equipment, etc
- Switch to another provider for a better price

○ Secure

○ Quick to implement