
Telecommunications and Network Security

Ed Crowley
Fall '05

1

Objectives

- Define communication models including:
 - ISO/OSI
 - TCP/IP
- Identify major telecommunication and network components
- Draw three basic LAN topologies
- Explain packet orientated communications
- Analyze TCP/IP
- Explain basic protocol analysis with TCP/IP
- Compare and contrast routing and routed protocols
- Define firewall architectures
- List communication related security issues
- List major attacks types

2

Topics

- OSI Model
- TCP/IP Model
- LAN topologies
- Networking & Internetworking
 - Hardware
 - Bridging and routing
 - Routed protocols
- WANs
- IP configuration
- Routing Protocols
- Remote Access
- Virtual Private Networks (VPNs)

3

Standard Organizations

ISO

- International Standards Organization developed OSI model.

IETF

- Internet Engineering Task Force (IETF) (Internet Society subgroup) developed TCP/IP.

4

Other Standard Groups

- IEEE
 - Institute of Electrical and Electronics Engineers
 - NIST
 - National Institute for Standards and Technology
 - ANSI
 - American National Standards Institute
 - ITU/CCITT
 - International Telegraph and Telephone Consultative Committee
-

5

OSI Model

- Facilitates understanding of packet data flow
 - Physical and logical
 - Facilitates troubleshooting
 - Useful for understanding specific protocols

 - OSI is a model not an implementation.
 - Protocols are implementations.
-

6

LAN TOPOLOGIES

- Physical or logical arrangement of network resources including:
 - Computers
 - Cables
 - Other physical components.

 - Impacts network's speed, functionality, and scalability.
-

7

Standard Topologies

- Bus
 - Single linear cable segment.
 - Star
 - Central connection point.
 - Ring
 - Electrically connects in a loop.
-

8

Bus Topology

- Ethernet Classic.
 - Passive/broadcast methodology.
 - Only one computer, at any specific time, transmits. All computers receive all packets .
 - All machines read the packet header but only the receiving machine reads the entire message. (in theory.)
 - Each machine just listens to the wire.
 - Requires cable termination.
-

9

Bus Vulnerabilities

- Signal Bounce
 - Standing wave
 - Cable Breaks
 - Media can no longer propagate the signal
 - Effectively, your backbone runs too and from each computer.
-

10

Star Topology

- Computers connect to a central hub.
 - Solves Bus Topologies major vulnerability
 - Each device is on its own cable segment.
 - With the exception of the hub, cable failure affects only a single machine.
-

11

Star Topology

- Passive/broadcast technology.
 - Virtual Bus
 - Only addressee reads the entire broadcast.
 - Relative to bus, requires more cable.
 - Requires another component, a hub.
 - In newer networks, a switch is likely to be used in place of a hub.
-

12

Ring Topology

- Computers logically connect directly to the next computer in line, forming a loop.
 - Signals travel in only one direction.
 - Active topology as each computer either acts on or regenerates the signal.
 - Utilizes Token passing access methodology
-

13

Token Passing

- Active technology.
 - Devices either send or receive.
 - Deterministic resource sharing method.
 - Provides equitable access for all units.
 - Used by Token Ring, FDDI, and ArcNet.
-

14

Other Topologies

- Mesh -- Each network device connects to every other device.
 - Cable failures have no impact. (Fault Tolerant.)
- Star bus or distributed star
 - AKA star.
- Star wired ring
 - Another name for ring topology.
 - Physically a star, logically a ring.

15

Topology Summary

Advantages

Bus

- Simple

Star

- Scalable with isolation.

Ring

- Equitable access, scaleable.

Disadvantages

- Vulnerable backbone

- Requires more cable.
- Most Economical, Hub centric

- Requires more cable.
- Hub centric, Expensive.

16

LAN Access Methods

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
 - Listen before talk
- Token Passing
 - Only the device that holds the token can talk.

17

LAN Signaling Types

- Baseband
 - Single digital signal, single carrier
- Broadband
 - Analog signal
 - Multiple signals on a single carrier
 - Cable TV technology

18

Primary LAN Technologies

- Distinguished by access methodology.
 - Ethernet
 - CSMA/CD
 - Token Ring
 - Token passing, single token
 - FDDI
 - Token passing, multiple tokens
-

19

Ethernet

- CSMA/CD
 - Originally, a bus based broadcast topology
 - Transmission stops at terminators
 - Baseband
 - Most common network type
 - IEEE 802.3
-

20

Token Ring

- Token Passing
 - Logical Ring, physical star topology
 - Unidirectional Flow
 - Each node regenerates signal
 - Single token
 - 4 or 16 or higher Mbps
- IEEE 802.5

21

Fiber Distributed Data Interface (FDDI)

- Can utilize dual counter rotating rings
 - Devices attached to one, or both rings
 - Token passing access methodology
 - Logically and physically a ring
- ANSI X3T12

22

WANs

- Wide Area Networks connect geographically separated Local Area Networks
 - Utilize an exterior leased media
 - Links may come from Regional Bell Operating Companies (RBOCs) or Post, or other like companies
- MAN - Metropolitan Area Network

23

DTE/DCE

- On user side, Wan link contains Data Terminal Equipment (DTE).
- On WAN provider's side, contains Data Circuit Equipment (DCE)

24

Model Layers

OSI

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

TCP/IP

- Application
- Transport
- Internetwork
- Network Interface

25

Physical Layer

- Specifies electrical, mechanical, procedural, and functional requirements for activating, maintaining, and deactivating physical links between end systems

Physical link attributes:

- voltage levels
- data rates
- maximum transmission distances
- connectors

26

Physical Layer

- Media
 - 10baseT -- twisted pair
 - 10base2 – thin coax
 - 10base5 – thick coax
 - 10baseF -- fiber
 - Transceivers
 - Hubs
-

27

Twisted Pair

- 10BaseT (10 Mbps, 100 meter run)
 - Unshielded or shielded (UTP most common)
 - Two wires per pair, four pair standard, twisted in spiral
 - Noise immunity improved by shielding
 - Cat 5, Cat 5e ...
 - Bandwidth 1 to 10 Mbps, 100Mbps, or 1000Mbps
-

28

Coaxial

- 10Base2 (10 Mbps, 200 m max run)
 - ThinEthernet or Thinnet or Thin Coax
 - Terminator: 50 ohms
 - Relatively good noise immunity
 - RG 58

29

Thin Coax

- “T” connectors
- 50 ohm terminators
 - Each segment has 2 terminators
- Segments may be connected with repeaters, hubs, or switches, or like devices

30

Standard Ethernet

- 10Base5, Thick Ethernet
 - Max of 100 taps per segment
 - Nonintrusive taps available (vampire tap)
 - AUI (Attachment Unit Interface)
 - RG 8

31

Fiber-Optic Cable

- Outer jacket, cladding, and glass core
 - Fast
 - Requires relatively more care in planning and installation
 - Immune to EMF and RFI
 - Difficult to tap conventionally

32

Transceivers

- Physical devices allowing connection of different media
 - May include Signal Quality Error (SQE) or “heartbeat” to test collision detection mechanism on each transmission
 - May include “link light”

33

Hub

- Physical layer device that connects other devices
- Depending on context, may be referred to as a :
 - concentrator
 - multiport repeater,
 - multi-station access unit (MAU)

34

Data Link Layer

- Provides data transport across a physical link
 - Handles:
 - Physical addressing
 - Network topology
 - Line discipline
 - Error notification
 - Orderly delivery of frames
 - Optional flow control
 - Bridges are level two devices
 - Originally, switches were also level two devices
-

35

Data Link Sublayers

IEEE views Data Link Layer as having two sublayers.

- Logical Link Control (LLC)
 - Refers upward to higher layer software functions
 - IEEE 802.2
 - Media Access Control (MAC)
 - Refers downward to lower layer hardware functions
-

36

Media Access Control

- MAC address is “physical address”, unique for LAN interface card
 - Aka hardware or link-layer address
 - Burned into the Read Only Memory (ROM)
 - 48 bit address, normally represented by 12 hexadecimal digits
 - 1st six hex characters identify vendor aka OUI
 - 2nd six hex characters are unique, provided by vendor
-

37

Logical Link Control

- Presents a uniform interface between upper and lower layers
 - Provides upper layer independence from media access
 - Upper layers use network addresses rather than MAC addresses
 - Provide optional connection, flow control, and sequencing services
 - IEEE 802.2
-

38

Bridges

- Forwards frames between data link layers associated with separate cable segments
 - Utilizes Self Learning table with source and destination mac addresses
 - When bridge receives a frame, it attempts to find the destination address in its table
 - If found, frame is forwarded out appropriate port
 - If not found, frame is broadcast on all external ports
-

39

Bridges

- Limited filtering
 - Makes decisions based on source and destination mac address
 - Security or network management filtering
 - Can limit bandwidth hogs
 - Can prevent sensitive data from leaving
 - Bridges can be for local or remote networks
 - Remote has “half” at each end of WAN link
-

40

Network Layer

- Logical Addressing and Routing
 - Help determine packets route through a network
- Routers use routing protocols
 - Create and maintain routes

41

Network Layer

- Logical Address – ip address
- Route - how to get there
 - Depends on source
- Network layer services determine:
 - Path of data
 - Device addressing
 - Tracks device location.

42

Network Layer

- Only two devices directly connected by the same “wire” can directly interact
- Devices not on the same network must communicate via intermediate system i.e. must use routed info
- Routers are intermediate systems

43

Bridge vs. Router

- Bridges extend (only) a single network
 - All devices appear to be on same “wire”
 - Limited Scalability
 - Routers can connect bridged subnetworks
- Routed networks scale well

44

Network Layer

- May require Flow control
- Must handle specific features such as mapping between data link layer and network layer addresses
 - ARP
 - ICMP

45

Circuit-Oriented vs. Connectionless

- Circuit-Oriented
 - Provides a Virtual, not necessarily a private, Circuit (VC) between two end systems
 - 3 phases:
 - Call setup
 - Data exchange
 - Call close (teardown)
 - X.25, IBM SNA
 - Ideal for terminal-host networks of finite size aka mainframes

46

Circuit-Oriented vs. Connectionless

- Connectionless (CL)
 - Each data unit is independently routed
 - aka “datagram”
 - Each data unit must carry addressing info
 - Basis of current LAN/WAN operations
 - TCP/IP, IPX/SPX
 - Well suited to client/server and other distributed system networks
-

47

Connection-Oriented vs. Connectionless

- Market has decided on CL networking
 - All mainstream developments on CL
 - Majority of networks now built CL
 - Easier to extend LAN based networks using CL WANs
 - Netheads vs. Bellheads
-

48

Network switching

- Circuit-switched
 - Transparent path between devices
 - Dedicated circuit
 - Phone call
- Packet-switched
 - Data is segmented, buffered, & recombined

49

Network Layer Addressing

- Utilizes logical (level three) address rather than data link, physical (level two) addresses
 - Hierarchical
 - Routers only need to know regions (domains), not individual computers
 - The network address identifies the network and the host

50

Network Layer Addressing

- Network Address - used by router
- Host Address - specific device

51

Network Layer Addressing

- IP addresses are logical addresses
 - Networks are hierarchically divided into subnets called domains
 - Domains are assigned IP addresses and names
 - Domains are represented by the network portion of the address

52

IP Addresses

- IP addresses and Domains were originally issued by InterNIC (cooperative activity between the National Science Foundation, Network Solutions, Inc. and AT&T)
 - Now controlled by ICANN

53

Network Layer Addressing

- IP uses a 4 byte (32 bit) network address
- Network and host address portions can vary in size
- Originally, networks were assigned a class according to the network size
 - Class A uses 1 octet for the network
 - Class B uses 2 octets for the network
 - Class C uses 3 octets for the network
 - Class D is used for multicast addresses

54

IP Address Conventions

- A host address of all ones is a broadcast
- A host address of zero refers to the network
- Certain host addresses are reserved
 - Private IP addresses
 - Loop Back Address

55

Routed vs. Routing Protocols

Routed Protocol

- Used by packets to find their way across routers to reach destination

Routing Protocol

- Used by routers to share and maintain routing information

56

Routed Protocols

- IP
 - IPX
 - SMB
 - Appletalk
 - DEC/LAT
-

57

Routing Protocol Types

- Distance-Vector
 - Utilizes a list of destination networks with direction and distance in hops
 - Link-state routing
 - Utilizes a topology map of network identifies all routers and subnetworks
 - Route is an optimization of the shortest path to destination
 - Static or dynamic
-

58

Routing Internet

Management Domains

- Core of Internet uses Gateway-Gateway Protocol (GGP)
- Exterior Gateway Protocol (EGP) is used to exchange routing data with core and other autonomous systems
- Interior Gateway Protocol (IGP) is used within autonomous systems

59

Static Routing

- Static routes
 - Entered manually
 - Define a path to a network or subnet
 - Most secure
 - Most labor intensive

60

RIP

- Distance Vector
- Interior Gateway Protocol
- Verbose, not very efficient
 - Broadcast routes every 30 seconds
 - Lowest cost route always best
 - A cost of 16 is unreachable
- No authentication, anyone can pretend to be a router

61

OSPF

- Link-state
- Interior Gateway Protocol
 - Routers elect “Designated Router”
 - All routers establish a topology database using DR as gateway between areas
- Along with IGRP, a replacement for RIP

62

BGP

- Border Gateway Protocol is an EGP
 - Can support multiple paths between autonomous systems
 - Can detect and suppress routing loops
- Lacks security
- Internet can be downed because of incorrectly configured BGP on ISP router

63

Source Routing

- Source (packet sender) specifies route a packet uses to traverse network
 - Two types, strict and loose
 - Allows IP spoofing attacks
- Rarely allowed across Internet

64

Transport Layer

- TCP
- UDP

- IPX Service Advertising Protocol (SAP)

65

Session Layer

- Establishes, manages and terminates sessions between applications
 - Coordinates service requests and responses that occur when applications communicate between different hosts
- Examples include: NFS, RPC, X Window System, AppleTalk Session Protocol

66

Presentation Layer

- Provides code formatting and conversion
 - For example, translates between differing text and data character representations such as EBCDIC and ASCII
 - Also includes data encryption
 - JPEG, GIF, MPEG, MIDI
-

67

Firewall Terms

- Network address translation (NAT)
 - Internal addresses unreachable from external network
 - DMZ - De-Militarized Zone
 - Hosts that are directly reachable from untrusted networks
 - ACL - Access Control List
 - Applies to routers or firewalls
-

68

Firewall Terms

- Choke, Choke router
 - A router with packet filtering rules (ACLs) enabled
 - Gate, Bastion host, Dual Homed Host
 - A hardened server that provides packet filtering and/or proxy services
 - Proxy server
 - A server that provides application proxies
-

69

Firewall types

- Packet-filtering router (first gen)
 - Access Control Lists (ACL)
 - Filters on protocol header info including port, service, or source/destination address
 - Screened host (second gen)
 - Packet-filtering and Bastion host
 - Application layer proxies
 - Screened subnet (DMZ)
 - 2 packet filtering routers and bastion host(s)
 - Most secure
-

70

Firewall mechanisms

- Proxy servers (third generation)
 - Intermediary
 - Think of bank teller
- Stateful Inspection
 - State and context analyzed on every packet in connection

71

Intrusion Detection (IDS)

- Host or networkcentric
- Context and content monitoring
- Positioned at network boundaries
- Utilizes a sniffer engine augmented with the capability to detect known attack patterns (signatures)

72

Web Security

- Secure sockets Layer (SSL)
 - Transport layer security (TCP based)
 - Widely used for web based applications
 - by convention, https
 - Secure Hypertext Transfer Protocol (S-HTTP)
 - Less popular than SSL
 - Used for individual messages rather than sessions
-

73

Web Security

- Secure Electronic Transactions (SET)
 - PKI
 - Financial data
 - Supported by VISA, MasterCard, Microsoft, Netscape
-

74

IPSEC

- IP Security
 - IETF developed
 - Standard used to implement VPNs
 - Two modes
 - Transport Mode
 - encrypted payload (data), clear text header
 - Tunnel Mode
 - encrypted payload and header
 - IPSEC requires shared public key

75

Common Hacker Attacks

- Recognize the name and basic premise
 - Should also be able to name defense
- Including:
- Spoofing
 - Sniffing
 - Session Hijacking
 - IP Fragmenting
 - Syn Floods

76

Spoofing

- TCP
 - Sequence number prediction
 - UDP
 - Trivial to spoof (connection less)
 - DNS
 - Spoof/manipulate IP/hostname pairings
 - Source Routing
-

77

Sniffing

- Passive attack
 - Monitor the “wire” for all traffic - most effective in shared media networks
 - Sniffers originally “hardware”, evolved into software tools
-

78

Session Hijacking

- Uses sniffer to detect sessions, get pertinent session info
 - Sequence numbers
 - IP addresses
 - Actively injects packets, spoofing the client side of the connection, taking over session with server
 - Bypasses I&A controls
 - Encryption is a countermeasure, stateful inspection can be a countermeasure
-

79

IP Fragmentation

- Use fragmentation options in the IP header to force data in the packet to be overwritten upon reassembly
 - Header may use a negative offset
 - Circumvents packet filters
-

80

IDS Attacks

- Insertion Attacks
 - Insert information to confuse pattern matching
- Evasion Attacks
 - Trick the IDS into not detecting traffic
 - Example - Send a TCP RST with a TTL setting such that the packet expires prior to reaching its destination

81

Syn Floods

- TCP handshake
 - Syn, Syn-Ack, Ack
 - Send a lot of Syn
 - Don't send Acks
- Target has a lot of open connections, can't accept any more incoming connections
- Denial of Service

82

Telecom/Remote Access Security

- Dial up lines are favorite hacker target
 - War dialing
 - Social engineering
- PBX is a favorite phreaker target
 - blue box, gold box, etc.
 - Voice mail

83

WANs

- A network that spans a large geographical area typically using a leased line to connect separate areas.
 - Allow each segment or section of a network to be situated in a different building, city, state, or country.
- WANs are connected by a variety of communication links.

84

Communication Links

- WANs are often constructed by linking individual LANs. Links include:
 - Packet switching networks
 - Fiber optic cable
 - Microwave transmitters
 - Satellite links
 - Cable television coax systems

85

Link Technologies

- Analog
- Digital
- Packet Switching

86

Analog Connectivity

- Public switched telephone service (PSTN)
 - AKA Plain old telephone service (POTS)
 - Slow and inconsistent
 - A step up from POTS is a leased (or dedicated) line.
 - Due to conditioning, a leased line is more consistent.
 - A leased line is not switched.
-

87

Digital Connectivity

- Digital Data Services (DDS) lines are direct or point to point synchronous communication links with various bandwidths.
 - All digital lines require a CSU/DSU (Channel Service Unit/Data Service Unit) between the network connection device and the outside line.
-

88

T1 Lines

- Full duplex, max rate 1.544 Mbps.
 - Because 24 individual channels, 64 Kbps each, make up a T-1 line, fractional T-1 is usually available.
 - Transmits DS-1 formatted data at 1.544 MBs through a phone switched network
 - T3 Transmits DS-3 formatted data at 44.736 MBps through a phone switched network
-

89

Packet Switching Networks

- Fast, efficient, and highly reliable.
 - Data delivery does not depend on any single pathway between the origin and the destination.
 - Frame relay is an advanced fast packet variable length, digital, packet switching technology.
 - Provides bandwidth as needed.
 - Utilizes a PVC.
-

90

Virtual Circuits

- Virtual circuits provide temporary dedicated pathways between two points on a digital network.
 - Switched virtual circuits
 - Permanent virtual circuits
 - Virtual private networks represent temporary or permanent connections across a public network.
 - Point to Point Tunneling Protocol (PPTP)
-

91

Advanced WAN Technologies

- X.25 provides an interface between public packet switching networks and their customers.
 - Utilizes LAPB Link Access Procedure Balanced which defines frame types, as well as detecting out of sequence frames.
 - ISDN Integrated Services Digital Network
 - Cost effective nondedicated link.
-

92

Advanced WAN Technologies

- Frame Relay, a point to point PVC technology, offers WAN communications over a fast, reliable, digital packet switching network.
 - Uses variable length packets.
 - ATM Asynchronous Transfer Mode uses a 53 byte fixed length cell for transmission rates up to 622Mbps.
 - Ideal for bursty traffic
-

93

Other WAN Technologies

- SDLC
 - HDLC
 - HSSI
-

94

SONET

- Synchronous Optical Network uses fiber optic media to transmit voice, data, and video at speeds in multiples of 51.84 Mbps.

95

Remote Access Security

- SLIP
 - Serial Line Internet Protocol (DL)
- PPP
 - Point to Point Protocol (DL)
- SLIP/PPP about the same, PPP adds error checking, SLIP obsolete
- PAP
 - Password authentication protocol
 - clear text password
- CHAP
 - Challenge Handshake Auth. Prot.
 - Encrypted password

96

Remote Access Security

- TACACS, TACACS+
 - Terminal Access Controller Access Control System
 - Network devices query TACACS server to verify passwords
 - “+” adds ability for two-factor (dynamic) passwords
 - Radius
 - Remote Auth. Dial-In User Service
-

97

Virtual Private Networks

- PPTP - Point to Point Tunneling Protocol
 - Microsoft standard
 - Creates VPN for dial-up users to access intranet
 - SSH - Secure Shell
 - Allows encrypted sessions, file transfers
 - Can be used as a VPN
-

98

Questions?