Communication & Network Security

MIS-5903

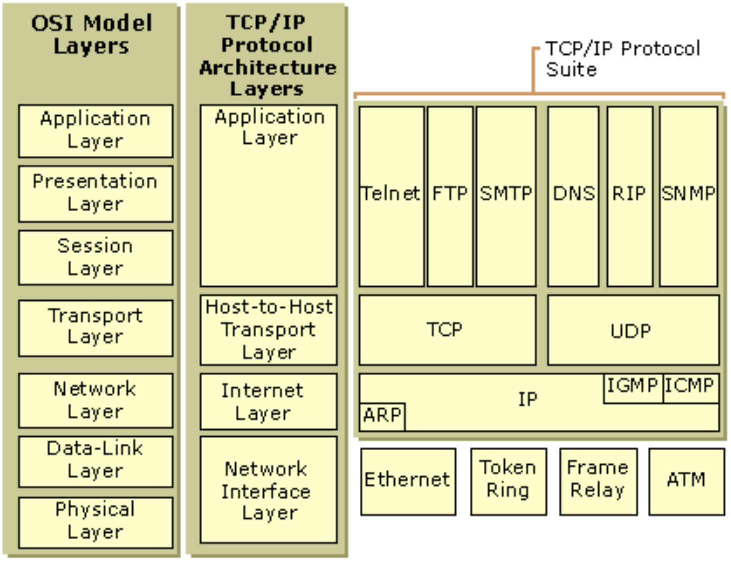
Week Five – Domain 4

http://community.mis.temple.edu/mis5903sec711summer2022/

1

OSI vs. TCP/IP Model

- TCP/IP
  - DOD
  - ARPANet
- OSI
  - Expanded into 7 layers
- Data-Link Sub-Layers per IEEE 802
  - Media Access Control
  - Logical Link Layer



OSI Model Layers

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data-Link Layer

Physical Layer

TCP/IP Protocol Architecture Layers

Application Layer

Host-to-Host Transport Layer

Internet Layer

Network Interface Layer

TCP/IP Protocol Suite

Telnet FTP SMTP DNS RIP SNMP

TCP UDP

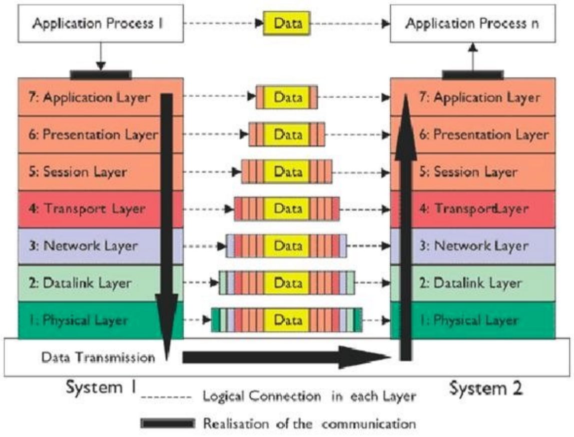
IP IGMP ICMP ARP

Ethernet Token Ring Frame Relay ATM

2

Encapsulation

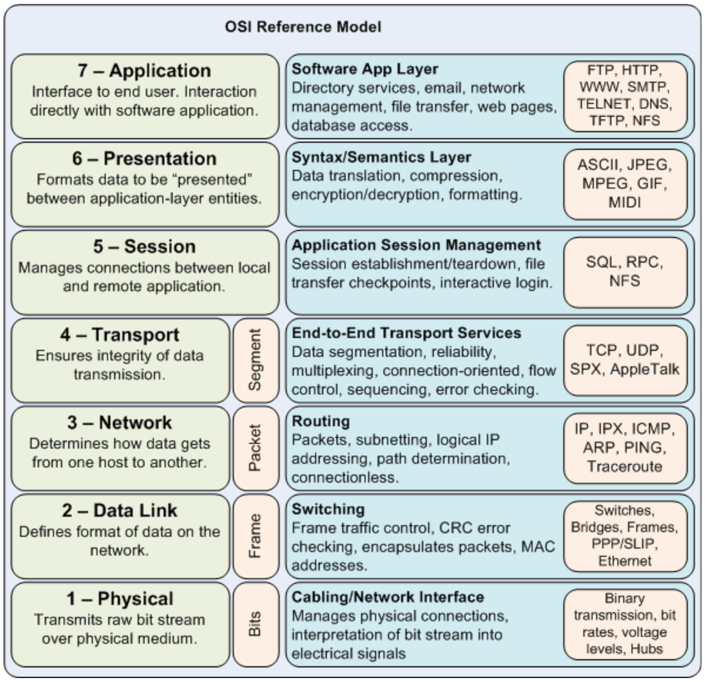
- System 1 is a “subject” (client)
- System 2 has the “object” (server)



OSI Reference

Notice:

- Segments
- Packets (Datagrams)
- Frames
- Bits



OSI Reference Model

7 – Application Interface to end user. Interaction directly with software application.		**Software App Layer** Directory services, email, network management, file transfer, web pages, database access.	FTP, HTTP, WWW, SMTP, TELNET, DNS, TFTP, NFS
6 – Presentation Formats data to be "presented" between application-layer entities.		**Syntax/Semantics Layer** Data translation, compression, encryption/decryption, formatting.	ASCII, JPEG, MPEG, GIF, MIDI
5 – Session Manages connections between local and remote application.		**Application Session Management** Session establishment/teardown, file transfer checkpoints, interactive login.	SQL, RPC, NFS
4 – Transport Ensures integrity of data transmission.	Segment	**End-to-End Transport Services** Data segmentation, reliability, multiplexing, connection-oriented, flow control, sequencing, error checking.	TCP, UDP, SPX, AppleTalk
3 – Network Determines how data gets from one host to another.	Packet	**Routing** Packets, subnetting, logical IP addressing, path determination, connectionless.	IP, IPX, ICMP, ARP, PING, Traceroute
2 – Data Link Defines format of data on the network.	Frame	**Switching** Frame traffic control, CRC error checking, encapsulates packets, MAC addresses.	Switches, Bridges, Frames, PPP/SLIP, Ethernet
1 – Physical Transmits raw bit stream over physical medium.	Bits	**Cabling/Network Interface** Manages physical connections, interpretation of bit stream into electrical signals	Binary transmission, bit rates, voltage levels, Hubs

Well known ports

Protocol	TCP/UDP	Port Number
File Transfer Protocol (FTP) (RFC 959)	TCP	20/21
Secure Shell (SSH) (RFC 4250-4256)	TCP	22
Telnet (RFC 854)	TCP	23
Simple Mail Transfer Protocol (SMTP) (RFC 5321)	TCP	25
Domain Name System (DNS) (RFC 1034-1035)	TCP/UDP	53
Dynamic Host Configuration Protocol (DHCP) (RFC 2131)	UDP	67/68
Trivial File Transfer Protocol (TFTP) (RFC 1350)	UDP	69
Hypertext Transfer Protocol (HTTP) (RFC 2616)	TCP	80
Post Office Protocol (POP) version 3 (RFC 1939)	TCP	110
Network Time Protocol (NTP) (RFC 5905)	UDP	123
NetBIOS (RFC 1001-1002)	TCP/UDP	137/138/139

5

Well known ports

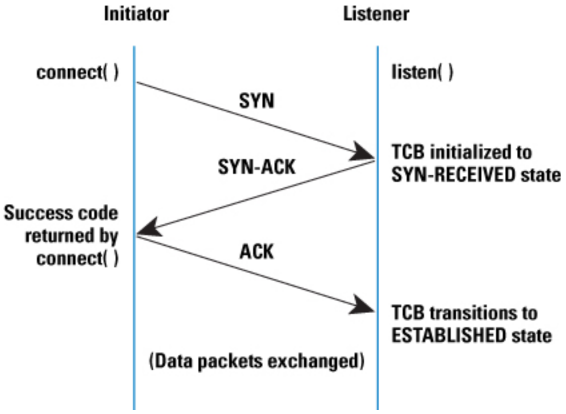
Protocol	TCP/UDP	Port Number
Internet Message Access Protocol (IMAP) (RFC 3501)	TCP	143
Simple Network Management Protocol (SNMP) (RFC 1901-1908, 3411-3418)	TCP/UDP	161/162
Border Gateway Protocol (BGP) (RFC 4271)	TCP	179
Lightweight Directory Access Protocol (LDAP) (RFC 4510)	TCP/UDP	389
Hypertext Transfer Protocol over SSL/TLS (HTTPS) (RFC 2818)	TCP	443
Lightweight Directory Access Protocol over TLS/SSL (LDAPS) (RFC 4513)	TCP/UDP	636
FTP over TLS/SSL (RFC 4217)	TCP	989/990

- http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml.

6

TCP – Three Way Handshake

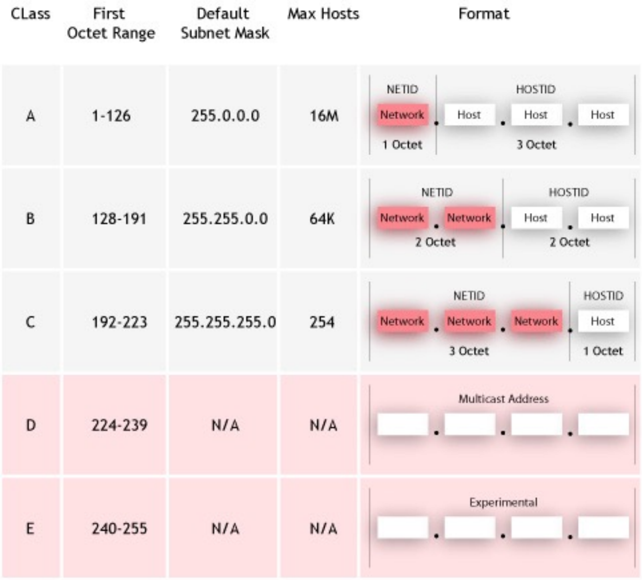
- Reliability
- Connection
- Sequencing
- Congestion
- Usage
- Reliability rather than Real-Time
- Speed is not of the essence.


Initiator
Listener
connect( )
listen( )
SYN
TCB initialized to SYN-RECEIVED state
SYN-ACK
Success code returned by connect( )
ACK
TCB transitions to ESTABLISHED state
(Data packets exchanged)

7

IPv4 Classes 32-bit

- Subnet
- Subnet Mask
- Classful (groups of 8)
- Classless Interdomain Routing (e.g. /23)
  aka supernetting

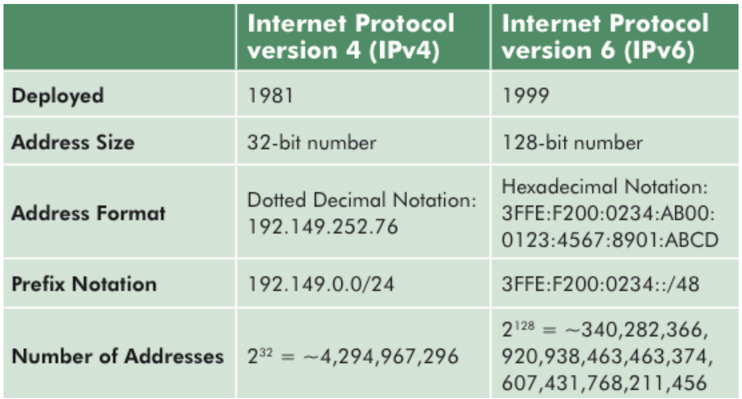


CLass	First Octet Range	Default Subnet Mask	Max Hosts	Format
A	1-126	255.0.0.0	16M	NETID: Network (1 Octet) HOSTID: Host . Host . Host (3 Octet)
B	128-191	255.255.0.0	64K	NETID: Network . Network (2 Octet) HOSTID: Host . Host (2 Octet)
C	192-223	255.255.255.0	254	NETID: Network . Network . Network (3 Octet) HOSTID: Host (1 Octet)
D	224-239	N/A	N/A	Multicast Address
E	240-255	N/A	N/A	Experimental

8

IPv6 128-bit

- Intersite:
  - 6to4
  - Teredo
- Intrasite:
  - ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)



	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	2^{32} = ~4,294,967,296	2^{128} = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456

9

Network Address Translation (RFC1918)

- Private addresses for internal use, Not routed on Internet
- Communicate transparently on Intranet to Internet (via router)
- A: 10.x.y.z
- B: 172.16.x.y – 172.31.x.y
- C: 192.168.x.y
- Static mapping – pool of public addresses (used for same public address at all times)
- Dynamic mapping – pool that is allocated on first-come, first-served
- Port Address Translation – owns only one public IP address for all systems – modifies source port

10

Layer 2 Security

- 802.1AE – IEEE Mac Security Standard (MACSec)
- 802.1AF – key agreement
- 802.1AR – unique per-device identifiers (DevID)
- “sticky mac” port security

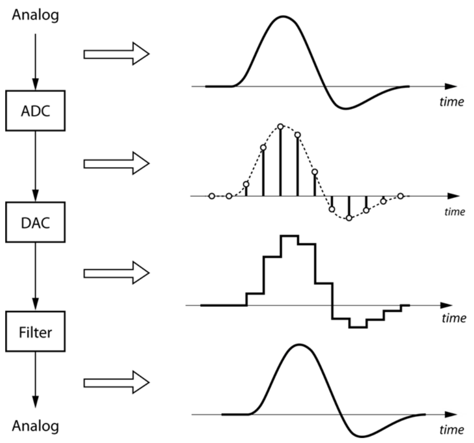
11

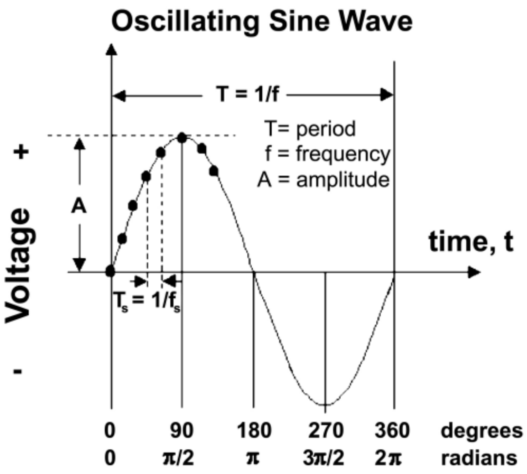
Converged Protocols

- Fiber Channel over Ethernet (FCoE) – some SANs
- Multiprotocol Label Switching (MPLS) – create VPN
- Internet Small Computer System Interface (iSCSI)
- Voice over Internet Protocol

12

Transmission – Analog/Digital





13

Micro-Segmentation

- Software Defined Network (SDN)
- Virtual eXtensible Local Area Network (VXLAN)
- Encapsultation
- Software Defined Wide Area Network (SDWAN)

14

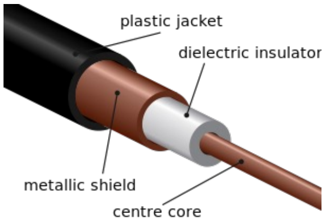
Asynchronous & Synchronous

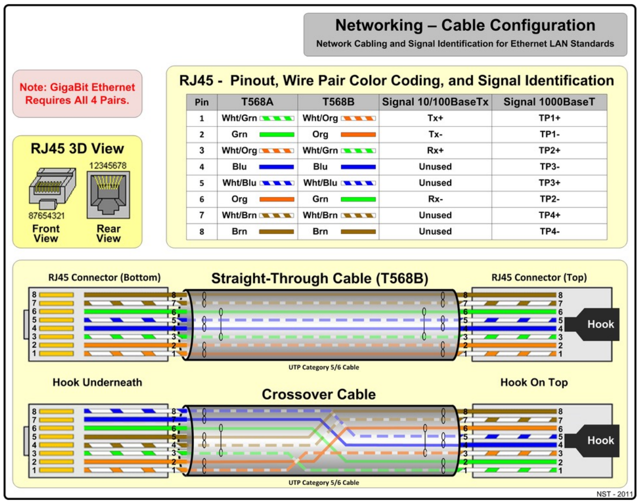
- Asynchronous
  - No timing component
  - Surrounds each byte with processing bits
  - Parity bit used for error control
  - Each byte required three bits of instruction
    - Start, stop, parity
- Synchronous:
  - Timing component for data transmission
  - Robust error-checking (CRC)
  - Used for high-speed, high-volume transmissions
  - Minimal overhead compared to asynchronous communications

15

Transmission Methods:

- Baseband uses the entire communication channel
- Broadband divides the channel into individual and independent channels





Networking – Cable Configuration

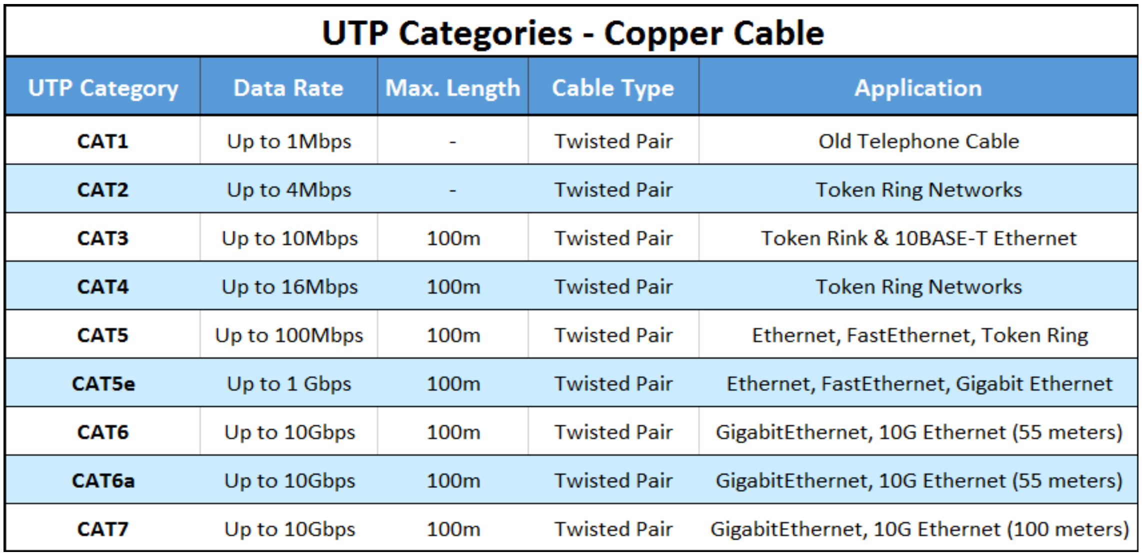
Network Cabling and Signal Identification for Ethernet LAN Standards

Note: GigaBit Ethernet Requires All 4 Pairs.

RJ45 - Pinout, Wire Pair Color Coding, and Signal Identification

Pin	T568A	T568B	Signal 10/100BaseTx	Signal 1000BaseT
1	Wht/Grn	Wht/Org	Tx+	TP1+
2	Grn	Org	Tx-	TP1-
3	Wht/Org	Wht/Grn	Rx+	TP2+
4	Blu	Blu	Unused	TP3-
5	Wht/Blu	Wht/Blu	Unused	TP3+
6	Org	Grn	Rx-	TP2-
7	Wht/Brn	Wht/Brn	Unused	TP4+
8	Brn	Brn	Unused	TP4-

16



UTP Categories - Copper Cable

UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

Fiber Optic Cables

- Source: Light Emitting Diodes (LEDs) or Diode lasers
- Single Mode: small glass core,
  - high speed
  - less susceptible to attenuation
- Multimode – large glass cores
  - Carry mode data
  - Best for shorter distance
  - Higher attenuation

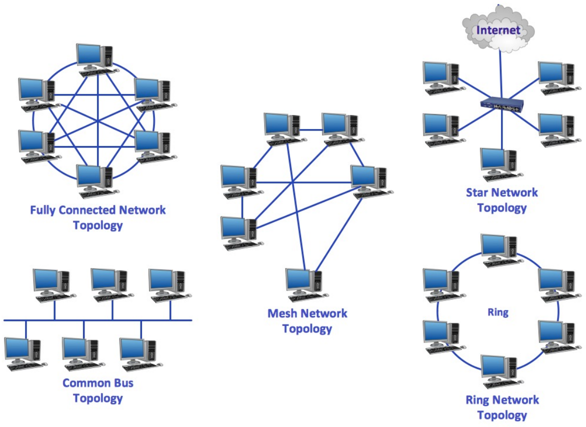
Cabling Issues

- Noise – interference
    - EMI
    - RFI
- Attenuation – loss of signal over distance
- Crosstalk – interference from nearby wires (consider STP over UTP)
- Fire Ratings:
    - Plenum areas
    - PVC cables in non-plenum areas
    - Pressurized conduits include alarms in secured areas

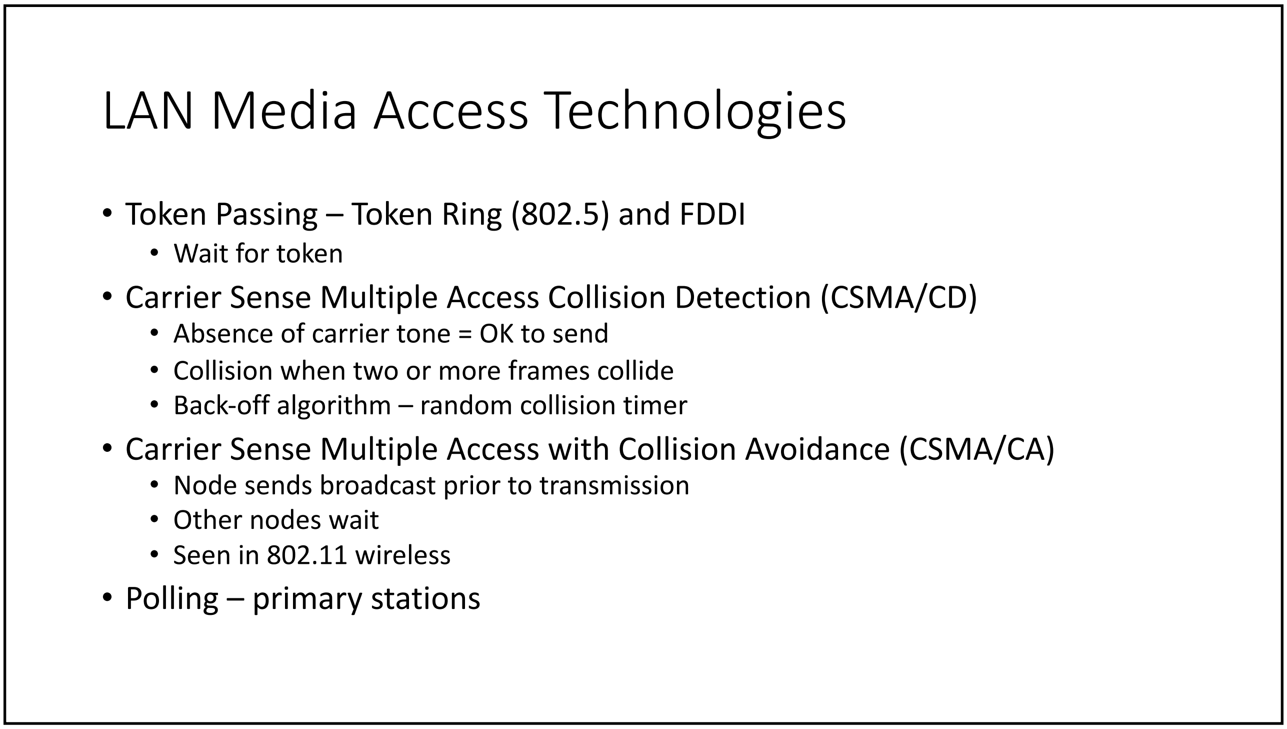
19

Topology

- Also Tree: bus topology with branches off of the main cable. There are multiple single points of failure



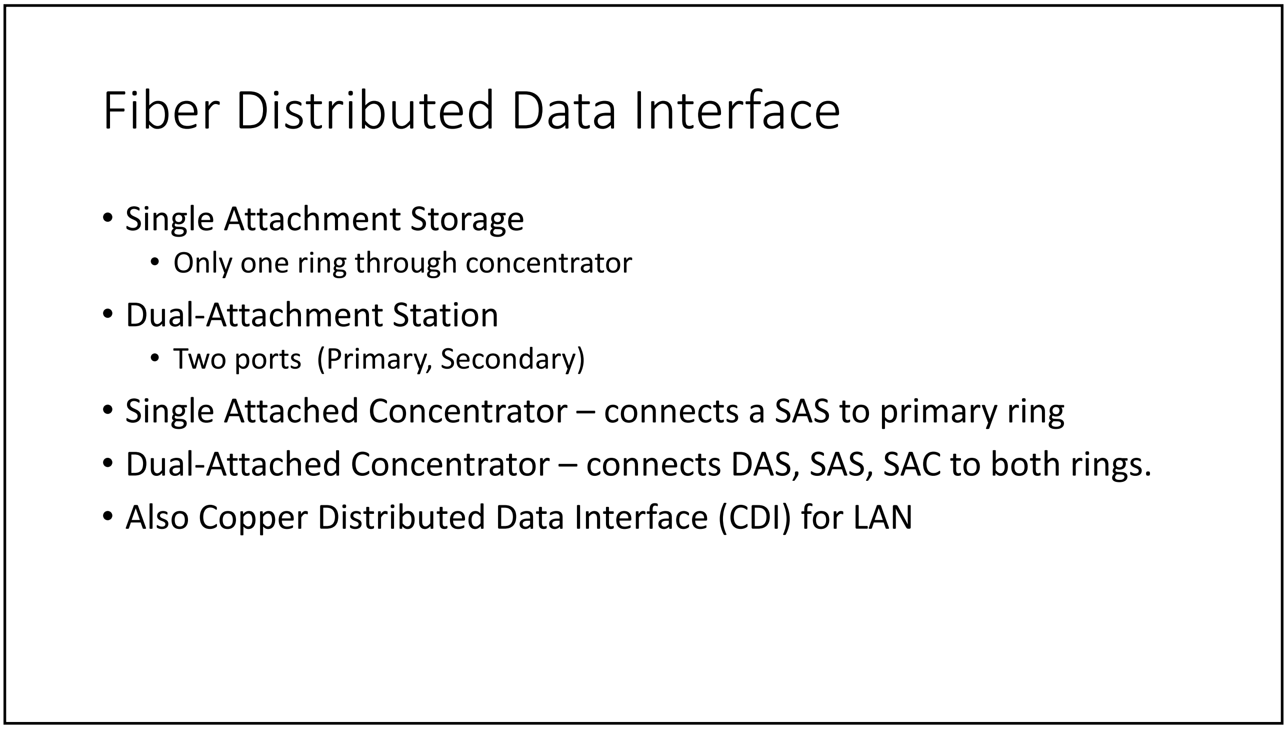
20



LAN Media Access Technologies

- Token Passing – Token Ring (802.5) and FDDI
  - Wait for token
- Carrier Sense Multiple Access Collision Detection (CSMA/CD)
  - Absence of carrier tone = OK to send
  - Collision when two or more frames collide
  - Back-off algorithm – random collision timer
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - Node sends broadcast prior to transmission
  - Other nodes wait
  - Seen in 802.11 wireless
- Polling – primary stations

21



Fiber Distributed Data Interface

- Single Attachment Storage
  - Only one ring through concentrator
- Dual-Attachment Station
  - Two ports (Primary, Secondary)
- Single Attached Concentrator – connects a SAS to primary ring
- Dual-Attached Concentrator – connects DAS, SAS, SAC to both rings.
- Also Copper Distributed Data Interface (CDI) for LAN

22

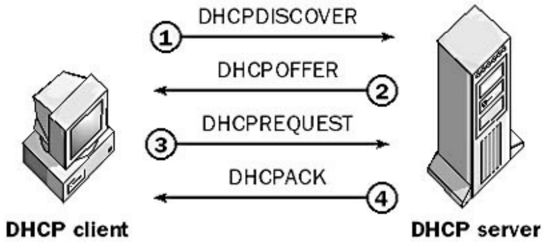
Address Resolution Protocol

- NIC has a Media Access Control (MAC) address
- ARP resolves MAC for a specific IP
- Stored in ARP cache
- ARP poisoning – respond with malicious MAC
- Broadcast traffic
- Broadcasts separated by routers, but not bridges

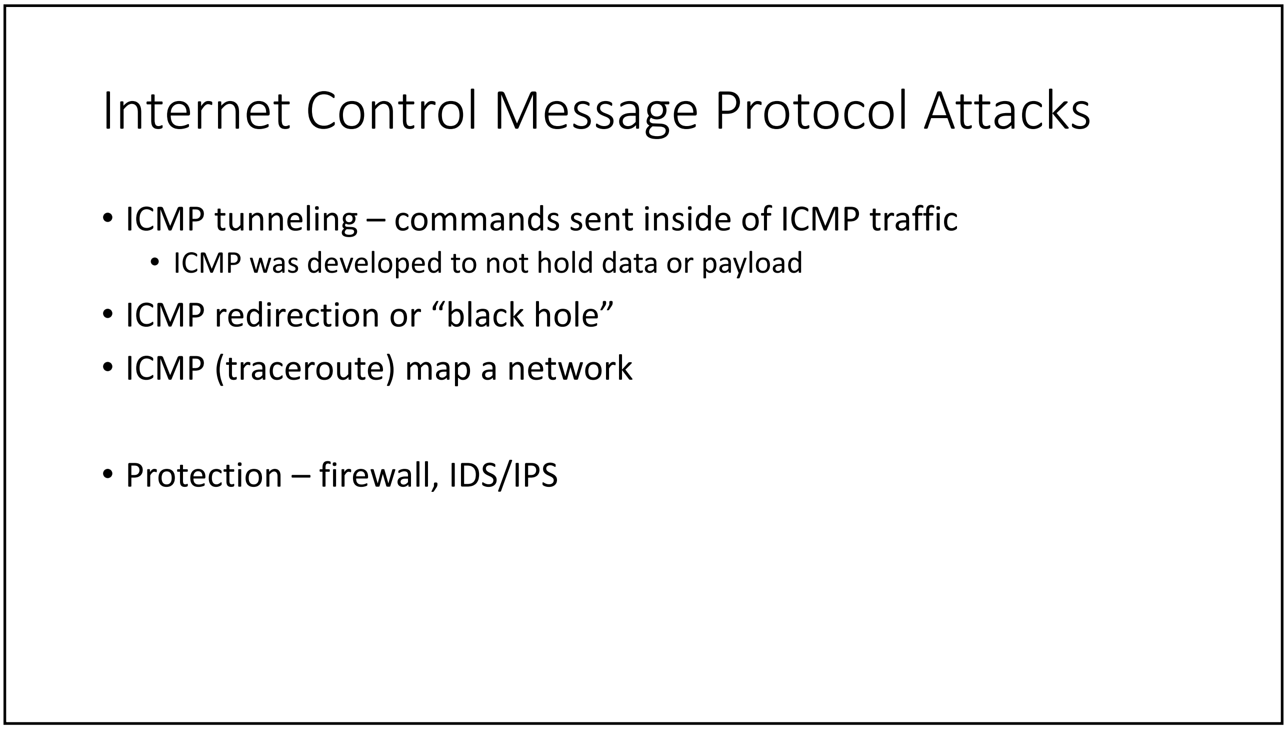
23

Dynamic Host Configuration Protocol

- Broadcast request
- DHCP reservation is not the same as static configuration
- Previous versions:
  - Reverse Address Resolution Protocol
    IP address configuration
  - Bootstrap Protocol (BOOTP) adds name server, default gateway



24

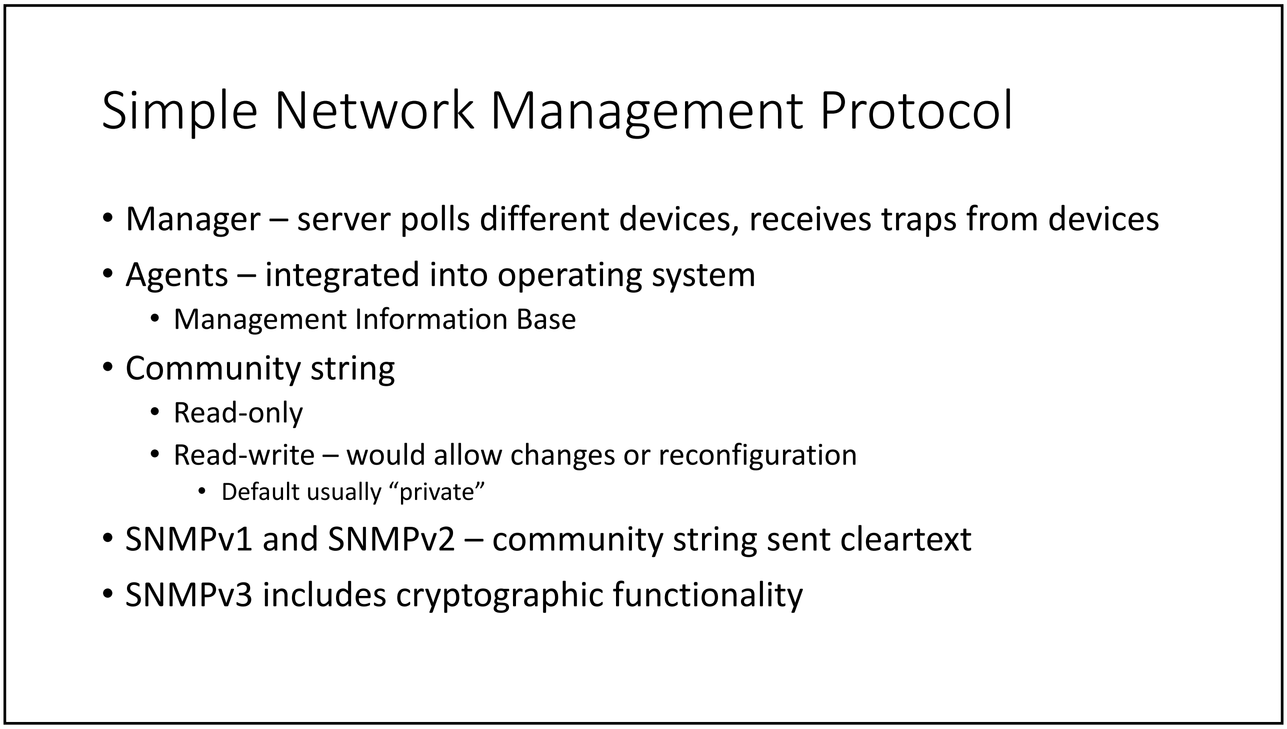


Internet Control Message Protocol Attacks

- ICMP tunneling – commands sent inside of ICMP traffic
  - ICMP was developed to not hold data or payload
- ICMP redirection or “black hole”
- ICMP (traceroute) map a network

- Protection – firewall, IDS/IPS

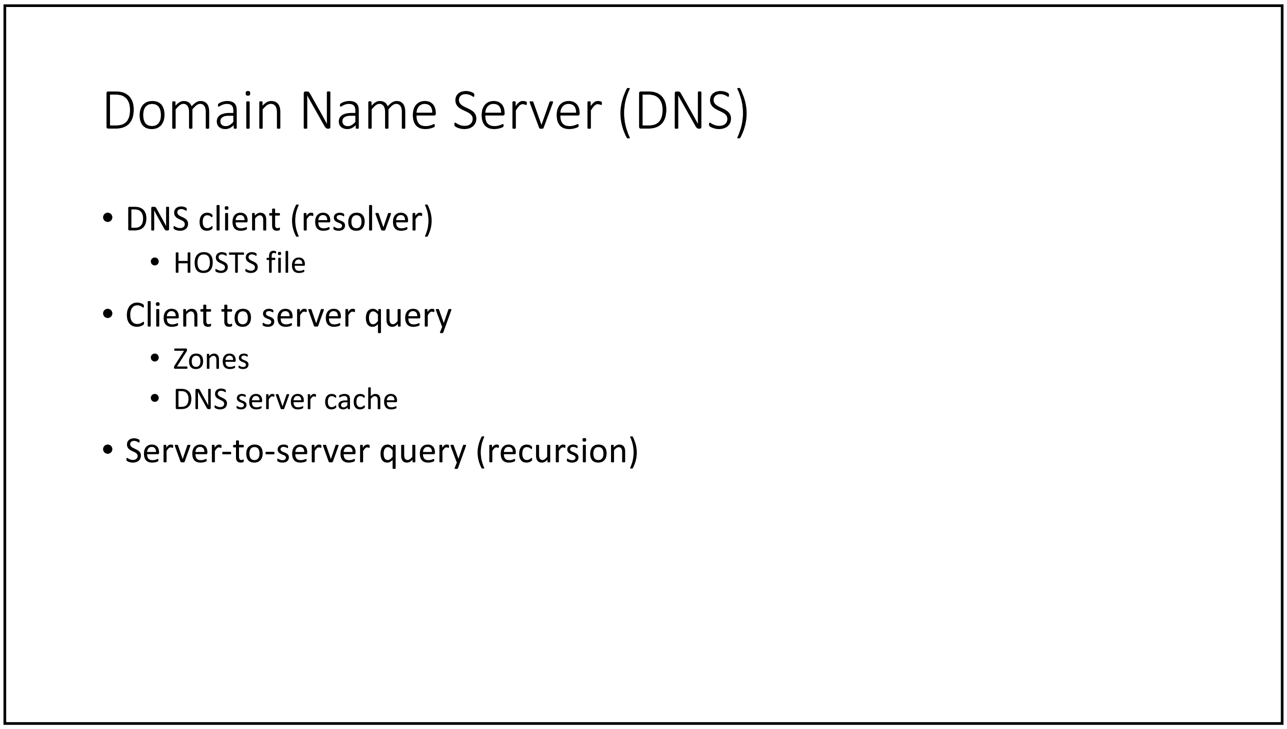
25



Simple Network Management Protocol

- Manager – server polls different devices, receives traps from devices
- Agents – integrated into operating system
  - Management Information Base
- Community string
  - Read-only
  - Read-write – would allow changes or reconfiguration
    - Default usually “private”
- SNMPv1 and SNMPv2 – community string sent cleartext
- SNMPv3 includes cryptographic functionality

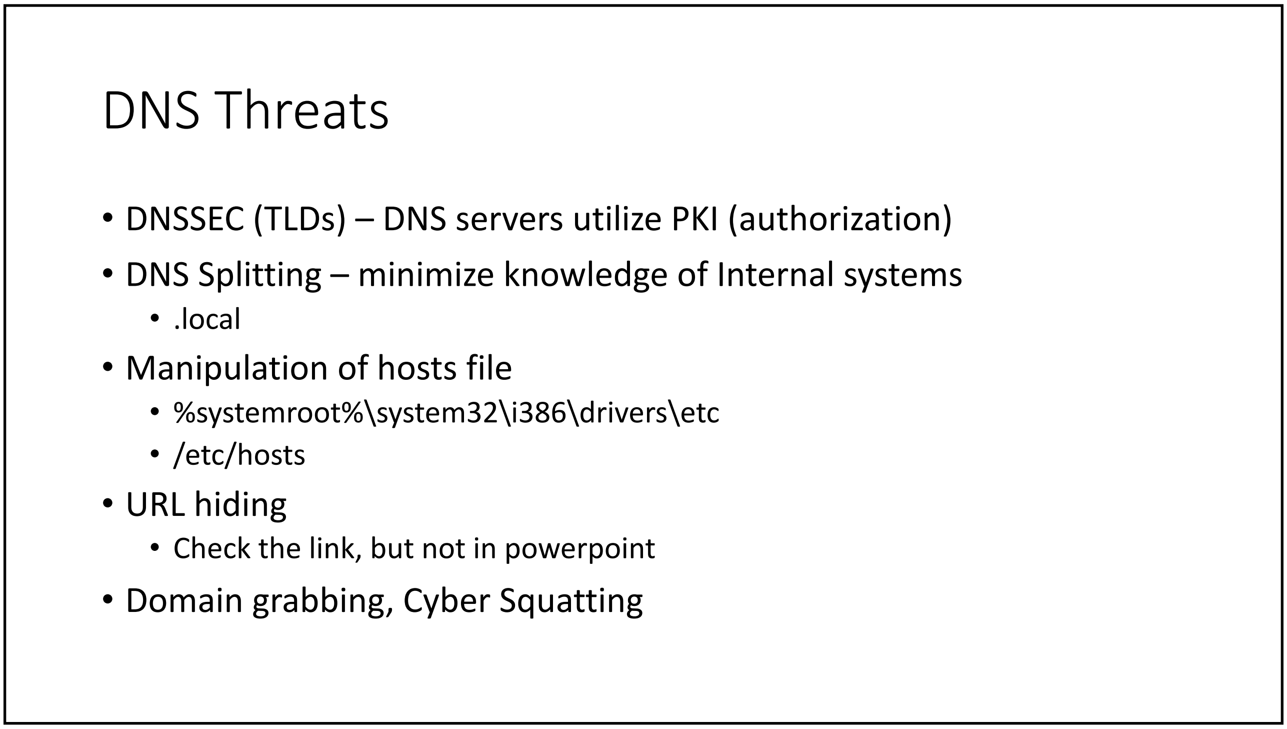
26



Domain Name Server (DNS)

- DNS client (resolver)
  - HOSTS file
- Client to server query
  - Zones
  - DNS server cache
- Server-to-server query (recursion)

27



DNS Threats

- DNSSEC (TLDs) – DNS servers utilize PKI (authorization)
- DNS Splitting – minimize knowledge of Internal systems
  - .local
- Manipulation of hosts file
  - %systemroot%\system32\i386\drivers\etc
  - /etc/hosts
- URL hiding
  - Check the link, but not in powerpoint
- Domain grabbing, Cyber Squatting

28

E-Mail Threats

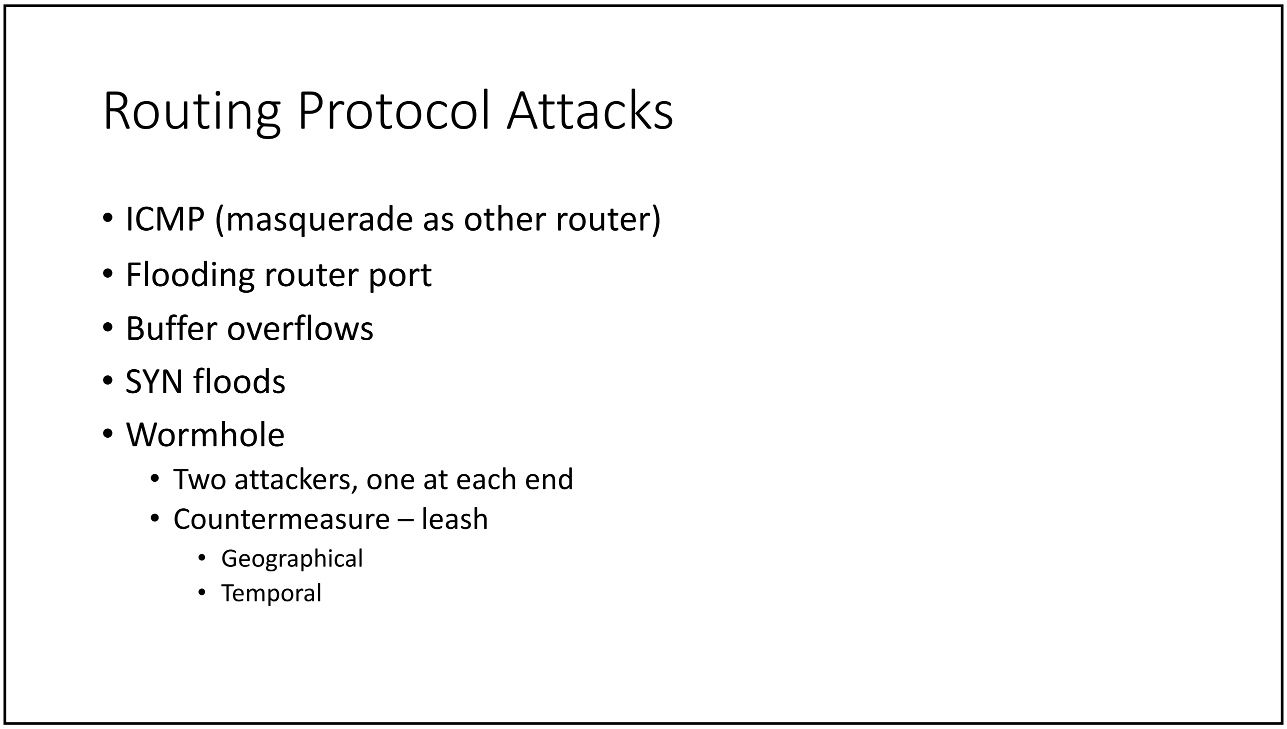
- Spoofing (forged e-mail)
- SMTP Authentication (SMTP-AUTH)
- Sender Policy Framework (verify sender’s IP address, confirm with DNS)
- DomainKeys Identified Mail
  - RFC6376
  - Utilizes Public Key Infrastructure (PKI) to validate origin and integrity
- Domain-Based Message Authentication (DMARC)
  - Combines SPF and DKIM
- Phishing
- Spear phishing – specific people
- Whaling – “big fish”

29

Routing Protocols

- Individual networks on Internet = Autonomous Systems (AS)
  - Administered by single entity
  - Common Interior Gateway Protocol (IGP)
- Dynamic vs. Static
- Route flapping
  - Notification that a link is down prevents “black hole”
- Distance-Vector (RIP) vs. Link-State
  - Interior: OSPF, IGRP, EIGRP (Cisco), VRRP, IS-IS
  - Exterior: BGP

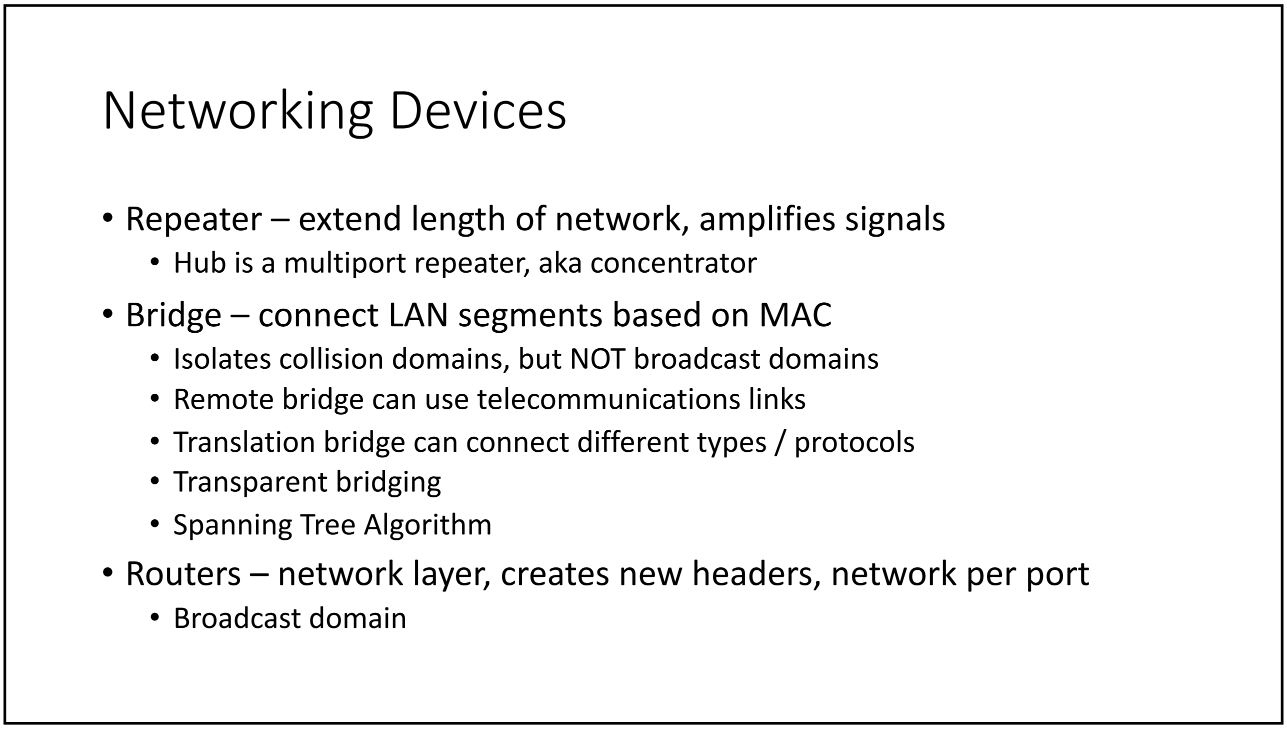
30



Routing Protocol Attacks

- ICMP (masquerade as other router)
- Flooding router port
- Buffer overflows
- SYN floods
- Wormhole
  - Two attackers, one at each end
  - Countermeasure – leash
    - Geographical
    - Temporal

31



Networking Devices

- Repeater – extend length of network, amplifies signals
  - Hub is a multiport repeater, aka concentrator
- Bridge – connect LAN segments based on MAC
  - Isolates collision domains, but NOT broadcast domains
  - Remote bridge can use telecommunications links
  - Translation bridge can connect different types / protocols
  - Transparent bridging
  - Spanning Tree Algorithm
- Routers – network layer, creates new headers, network per port
  - Broadcast domain

32

Switches

- Basic switches operate at layer 2
- Multilayered switches (3, 4)
- Multiprotocol Label Switching for time-sensitive traffic
- Virtual LANs (VLANs)
  - Hopping – access to traffic in various VLAN segments
  - Switch spoofing attack – insert between other VLAN devices
  - Double tagging attack – insert VLAN tags

- Gateway – at application layer, software running on a device (e.g. mail gateway)
- Private Branch Exchange (PBX) – phone, analog, data; phreakers

33

Firewall Types

Type	OSI Layer	Characteristics
Packet filtering	Network	Source/Destination address, ports, services. Access Control Lists
Stateful	Network	State and context of packets. State table tracks each conversation.
Application-Level proxy	Application	Granular access control decisions; requires one proxy per protocol.
Circuit-Level proxy	Session	Evaluates only header packet information
Dynamic Packet filtering	Network	Allows permitted outbound and only responses inbound
Kernel proxy	Application	Processing is faster, performed oin the kernel. One network stack for each packet.
Next-Generation	Multiple layers	Built-in IPS, Able to connect to external services such as Active Directory.

34

Firewall Architecture

- Dual-Homed / Multihomed
  - Single point of failure
- Screened Host – Firewall connects to screening device
- Screened Subnet – Creates distinct DMZ

35

Shoulds of Firewalls

- #1 implicitly deny any packets not explicitly allowed
  - Masquerading or spoofing of internal addresses, for example
  - Zombies send outbound traffic with external source addresses (DDoS)
- Reassemble fragments before forwarding
  - Fragmentation and reassembly flaws
  - Teardrop – malformed fragments created to cause victim to become unstable.
  - Overlapping – subvert filters that do not reassemble before inspection (overwrites approved fragments)

36

Firewall rules

- Silent – drop “noisy” without logging it.
- Stealth – disallows access to firewall software from unauthorized systems
- Cleanup – last rule drops and logs any traffic that does not meet preceding rules.
- Negate – rather than “any”, specifies what system can be accessed and how.

37

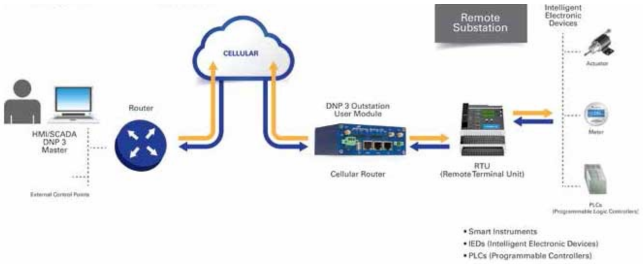
Proxy

- Forwarding proxy allows the client to specify the server
- Open proxy is open for anyone to use
- Anonymous open proxy conceals IP address
- Reverse proxy appears as the original server

38

Multilayer Protocols

- Distributed Network Protocol 3 (DNP3)
  - Designed for use in SCADA Systems
  - Does not incorporate routing functionality
  - Devices Connected to Remote Terminal Units
  - SCADA Master includes Human-Machine Interface (HMI)
  - 3-layer Enhanced Performance Architecture (EPA)
    - Corresponds to OSI layers 2, 4, and 7
- Controller Area Network Bus (CANBUS)
  - Autonomous automobiles
- ModBus - PLCs


HMI/SCADA DNP 3 Master
External Control Points
Router
CELLULAR
DNP 3 Outstation User Module
Cellular Router
RTU (Remote Terminal Unit)
Remote Substation
Intelligent Electronic Devices
Actuator
Meter
PLCs (Programmable Logic Controllers)
• Smart Instruments
• IEDs (Intelligent Electronic Devices)
• PLCs (Programmable Controllers)

39

Other technologies

- Unified Threat Management (UTM) appliances
- Content Distribution Networks – multiple servers distributed over a region. (e.g. Netflix)
- Software Defined Networking
  - Control plane – routing decisions are made (congestion)
  - Forwarding plane – forwarding decisions are made
  - Open, API (CISCO), Overlays
- Value Added Network (VAN)
  - EDI infrastructure maintained by service bureau. (merchandise replenishment)

40

Metropolitan Area Networks

- Synchronous Optical Networks (SONETs) or FDDI
  - Self-healing
- Sites connect to rings via T1, fractional T1, or T3
- Metro Ethernet
  - Can be pure Ethernet or integrated with Multiprotocol Label Switching (MPLS)

41

Telecommunications History

- Copper lines (56+8k)
- T1 – up to 24 (x64k) – Time Division Multiplexing
  - E1 – 32 * 64k E0 channels (2.048 Mbps)
- T3 – up to 28 T1
  - E3 – 34.368 Mbps
- Fiber Optic / SONET (e.g. OC-1 51.84Mbps)
- ATM (53-byte) cells over SONET

42

WAN Technologies

- Channel Service Unit / Data Service Unit
  - CSU – connects network to service provider’s line
  - DSU – converts digital signals from routers, switches, multiplexers to signals that can be transmitted over service provider’s lines.
  - Provides interface for:
    - Data Circuit-terminating Equipment (DCE) = carrier’s switch
    - Data Terminal Equipment (DTE)
- Circuit-Switched (e.g. telephone calls, ISDN) – voice, predictable
- Packet Switched – variable, bursty, dynamic paths, data
- Frame Relay
  - Committed Information Rate (CIR)

43

Other WAN Technologies

- Virtual Circuits
  - Frame Relay and X.25 forward frames
  - Permanent Virtual Circuit (PVC) – guaranteed bandwidth
  - Switched Virtual Circuits (SVC) – temporary connections
  - X.25 uses 128-byte HDLC frames (High-Level Data Link Control)

44

Asynchronous Transfer Mode

- Fixed-rate 53-byte cells
- Types of Data:
  - Constant Bit Rate (time-sensitive applications)
  - Variable Bit Rate (VBR) connection-oriented channel ; delay-insensitive applications / uneven throughput
  - Unspecified Bit Rate – connectionless; no control over traffic rate
  - Available Bit Rate – connection-oriented channel that allows speed to be adjusted
    - Bandwidth that remains after guaranteed service rate has been met

45

QoS Service Levels

- Best-effort service – no guarantee of throughput, delay, or delivery
- Differentiated service – assigned classification for more bandwidth, shorter delays, fewer dropped frames
- Guaranteed service – time-sensitive traffic guaranteed a minimum speed

46

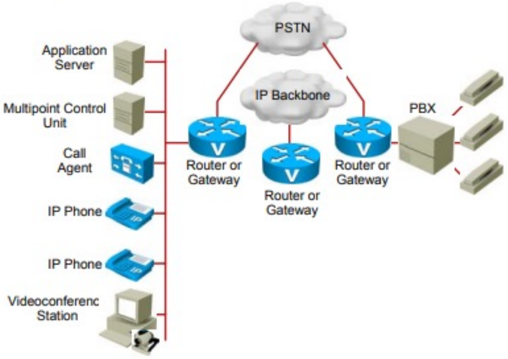
More WAN Technologies

- Synchronous Data Link Control (SDLC) – communication within SNA.
- High-Level Data Link Control – serial device to device WAN communication.
  - Extension of SDLC
- Point to Point Protocol (PPP)- encapsulation of Ethernet protocol over telecommunication equipment
- High-Speed Serial Interface – connect multiplexers and routers to ATM, frame relay, up to 52Mbps.

47

Multiservice Access Technologies

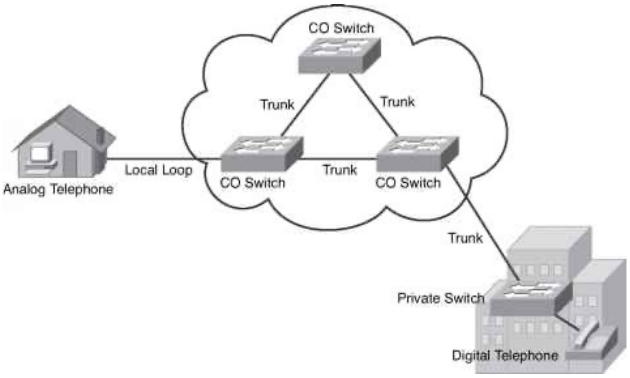
- PSTN – circuit switched phone uses Signaling System 7 (SS7)
- H.323 Gateways – video, real-time audio, data packet-based transmissions
- VoIP uses Session Initiation Protocol (SIP)
  - VOIP refers to services (caller ID, QoS, voicemail)
  - IP Telephony includes all real-time applications over IP (Voice over IM, Videoconferencing)



48

Remote Connectivity – Dial-Up

- PSTN modems using PPP
- War-dialing
- Unknown Back-Doors
- Countermeasures:
  - Call-Back
  - Disable or Remove modems
  - Consolidate and manage centrally
  - Implement two-factor authentication, VPNs, personal firewalls



49

Remote Connectivitiy – ISDN

- Integrated Services Digital Network
- Data, voice, other traffic all transferred in digital format
- Basic Rate Interface (BRI) – copper lines, 2B + 1D (64+64+16) = 144Kb
- Primary Rate Interface (PRI) – equivalent to T1 / 1.544 Mbps
  - 23 x 64K B + 64K D
- Broadband ISDN (BISDN)
  - Mainly used within telecommunications carrier backbones
  - ATM commonly employed to encapsulate data at data link layer into cells, which travel over a SONET network.

50

Remote Connectivity – Digital Subscriber Line (DSL)

- Up to 52 Mbps
- Must be within 2.5 mile radius of service provider’s equipment
- Distance = reduced speed
- Symmetric – same rate upstream and downstream
- Asymmetric – Data travels faster downstream (residential) – 768k/384k
- High-Bit-Rate (HDSL) T1 speeds over copper wires
  - Requires two twisted pairs of wires
- Very High-Data-Rate Digital Subscriber Line (VDSL) – 13M/2M
- Rate Adaptive Digital Subscriber Line – adjusts to match quality and length of line.

51

Remote Connectivity

- Cable Modems – use Data Over Cable Service Interface Specifications (DOCSIS)
  - Always-On
  - Baseline Privacy Interface/Security (BPI/SEC) encrypts data
- FIOS
- Satellite

52

Virtual Private Network (VPN)

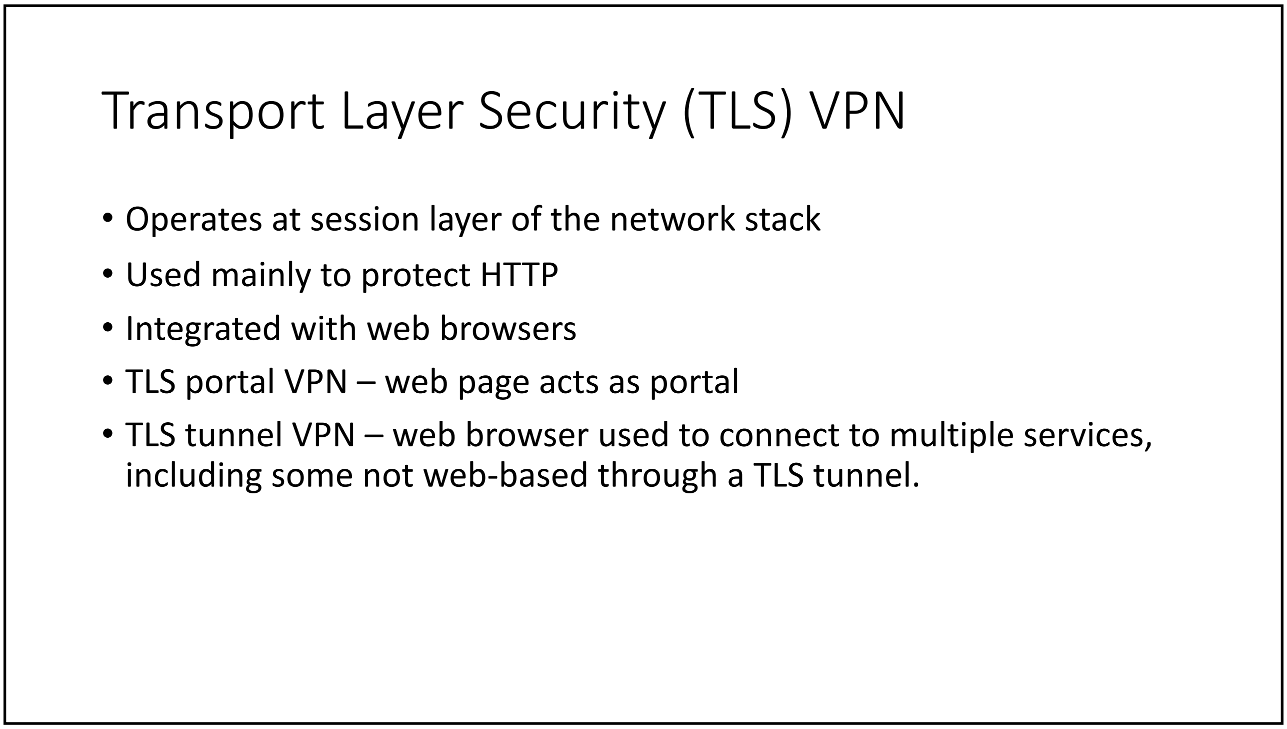
- Point-to-Point Tunneling Protocol (PPTP) included with Windows
  - Authenticated using PAP, CHAP, MS-CHAP, or EAP-TLS
  - Payload encrypted using Microsoft Point-to-Point Encryption (MPPE)
- Layer 2 Tunneling Protocol
  - Combines features of PPTP and Cisco’s Layer 2 Forwarding (L2F)
  - Not restricted to just IP
  - Inherits PPP authentication and integrates with IPSec

53

Internet Protocol Security (IPSec)

- Authentication Header (AH) – Provides integrity, origin authentication, protection from replay
- Encapsulating Security Payload (ESP) – provides confidentiality, origin authentication, data integrity
- Internet Security Associate and Key Management Protocol (ISAKMP)
  - Framework for security association, key exchange
- Internet Key Exchange – provides authenticated keying material for use with ISAKMP
- Supports only IP networks, on network layer

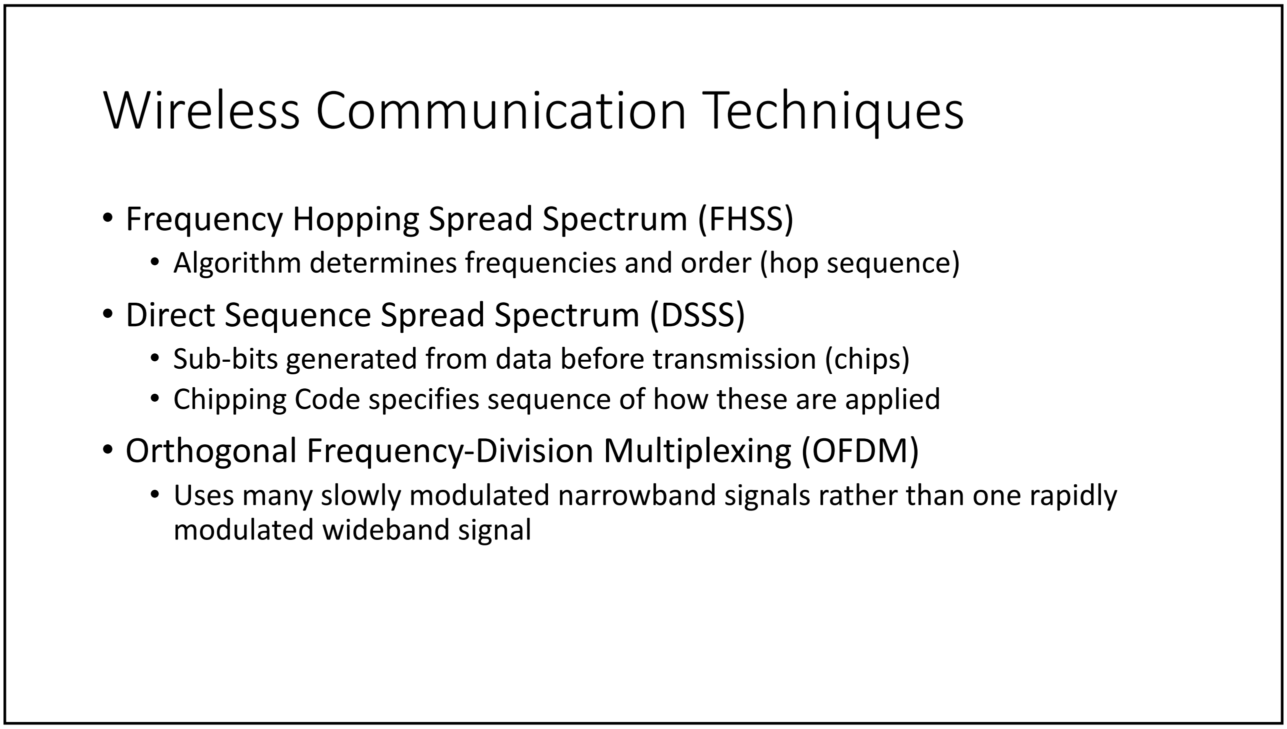
54



Transport Layer Security (TLS) VPN

- Operates at session layer of the network stack
- Used mainly to protect HTTP
- Integrated with web browsers
- TLS portal VPN – web page acts as portal
- TLS tunnel VPN – web browser used to connect to multiple services, including some not web-based through a TLS tunnel.

55



Wireless Communication Techniques

- Frequency Hopping Spread Spectrum (FHSS)
  - Algorithm determines frequencies and order (hop sequence)
- Direct Sequence Spread Spectrum (DSSS)
  - Sub-bits generated from data before transmission (chips)
  - Chipping Code specifies sequence of how these are applied
- Orthogonal Frequency-Division Multiplexing (OFDM)
  - Uses many slowly modulated narrowband signals rather than one rapidly modulated wideband signal

56

WLAN Components

- Access Point
  - Infrastructure mode – connect ot existing wired network
- Ad-Hoc Mode
  - No access points; devices connect to each other directly
- Service Set ID (SSID)
  - In Infrastructure mode, the group is a Basic Service Set (BSS)
- Channel – devices communicate over same channel

57

Wireless Standards (802.11)

GET IEEE 802 IEEE Standards

1. 802.11b – 2.4 Ghz, 11 Mbps
2. 802.11a – 5 Ghz, 54 Mbps
3. 802.11g – 2.4 Ghz, 54 Mbps
4. 802.11n – 2.4 + 5 Ghz, 100 Mbps
5. 802.11ac – extension of 802.11n, up to 1.3 Gbps
6. 802.11ax – efficiency – multiuser OFDM, doubles MU-MIMO streams

58

Wireless Standards (802.11)

GET IEEE 802 IEEE Standards

- 802.11e – Quality of Service
- 802.11f – Mobility between Aps
- 802.11h – European modification
- 802.11j – Interoperability worldwide

59

WLAN Security

- 802.11 – Wired Equivalent Privacy (WEP)
  - Intruder can intercept traffic
- 802.11i – Wi-Fi-Protected Access II (WPA2)
  - “draft 802.11i” (aka WPA) re-used some elements of WEP
  - Temporal Key Integrity Protocol (TKIP) – new key for every frame transmitted (key mixing)
  - Aka Robust Security Network
  - Enterprise – integrates 802.1X port authentication and Extensible Authentication Protocol (EAP)
- 802.11w – adds Management Frame Protection (MFP)
- WPA3
  - Personal – uses Simultaneous Authentication of Euals (802.11s)
  - Enterprise – restricted to 192-bit keys
- 802.1x
  - Not a wireless protocol, but an access control protocol to be used on wired and wireless networks.
- Cannot make full connection without authentication

60

Other Wireless

- 802.16 (WiMax) broadband wireless access for Metropolitan Area Networks
- 802.15.4 – Wireless Personal Area Network (WPAN)
  - 2.4 Ghz (Industrial, Scientific and Medical (ISM) Band – unlicensed)
  - Short distance, no more than 100 meters
  - ZigBee supports 250 kbps w/128-bit symmetric key encryption
- Bluetooth – 1, 10, or 100 meters; 2.4 Ghz
  - Bluejacking – unsolicited message to device
  - Bluesnarfing – unauthorized access to device
- 802.15.7 – Visible Light Communications
  - LiFi
- 802.15.8 – Wireless Peer Aware Networking (WPAN)

61

Wireless Security Best Practices

- Change default SSID
- Implement WPA2 and 802.1X to use centralized user authentication (RADIUS, Kerberos)
- Separate VLANs for class of user
- Deploy a Wireless Intrusion Detection System (WIDS)
- AP Placement – center of building
- Connect AP to a DMZ segment; inspect prior to connecting to LAN
- Implement VPN for wireless devices
- Configure AP to only allow known MAC addresses (still in cleartext)
- Conduct penetration tests on the WLAN

62

Network Encryption

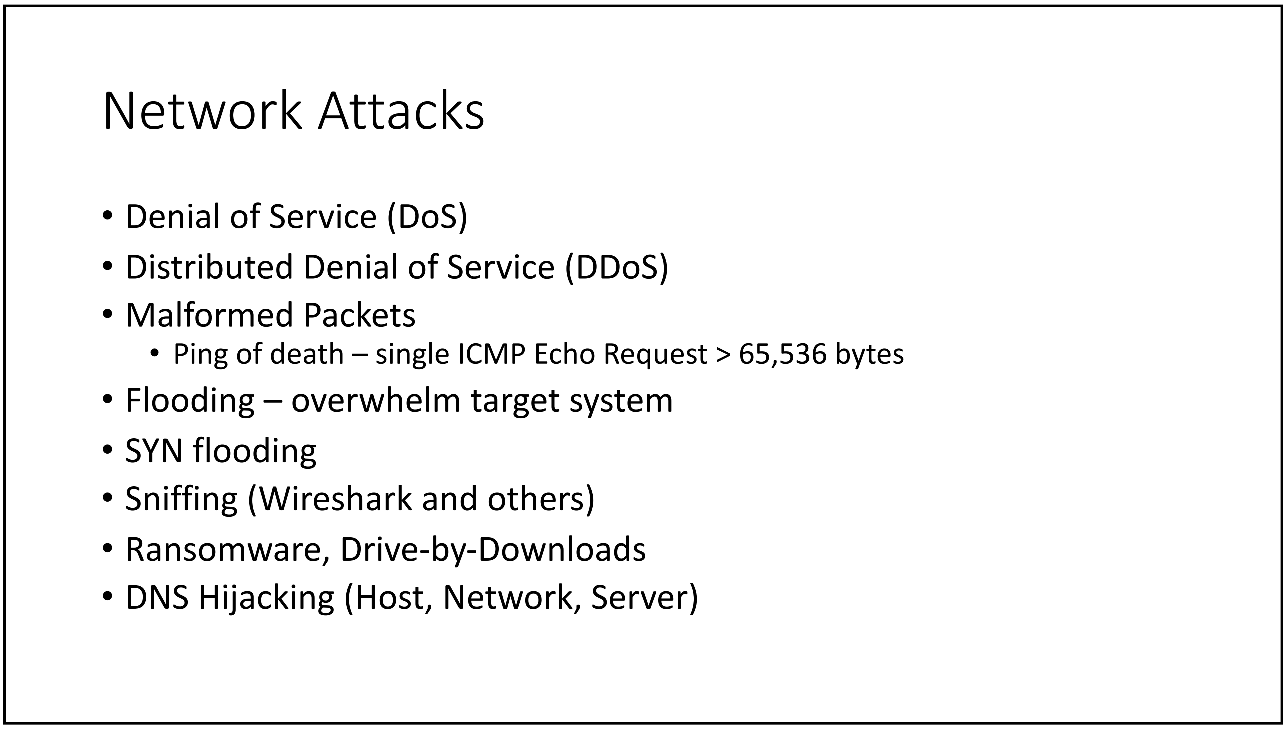
- Link encryption – all data along the specified communication path
  - Except data link control messaging
  - Called online encryption
- End-to-End encryption – headers, addresses, routing information, trailer information not encrypted
  - Requested by the user

63

Internet Security

- Secure Multipurpose Internet Mail Extensions (S/MIME) encrypt e-mail and attachments
- Pretty Good Privacy (PGP) – uses a key ring, open source, de facto standard
- HTTP Secure (HTTPS) – HTTP over SSL or TLS
- Limit cookies
- Secure Shell

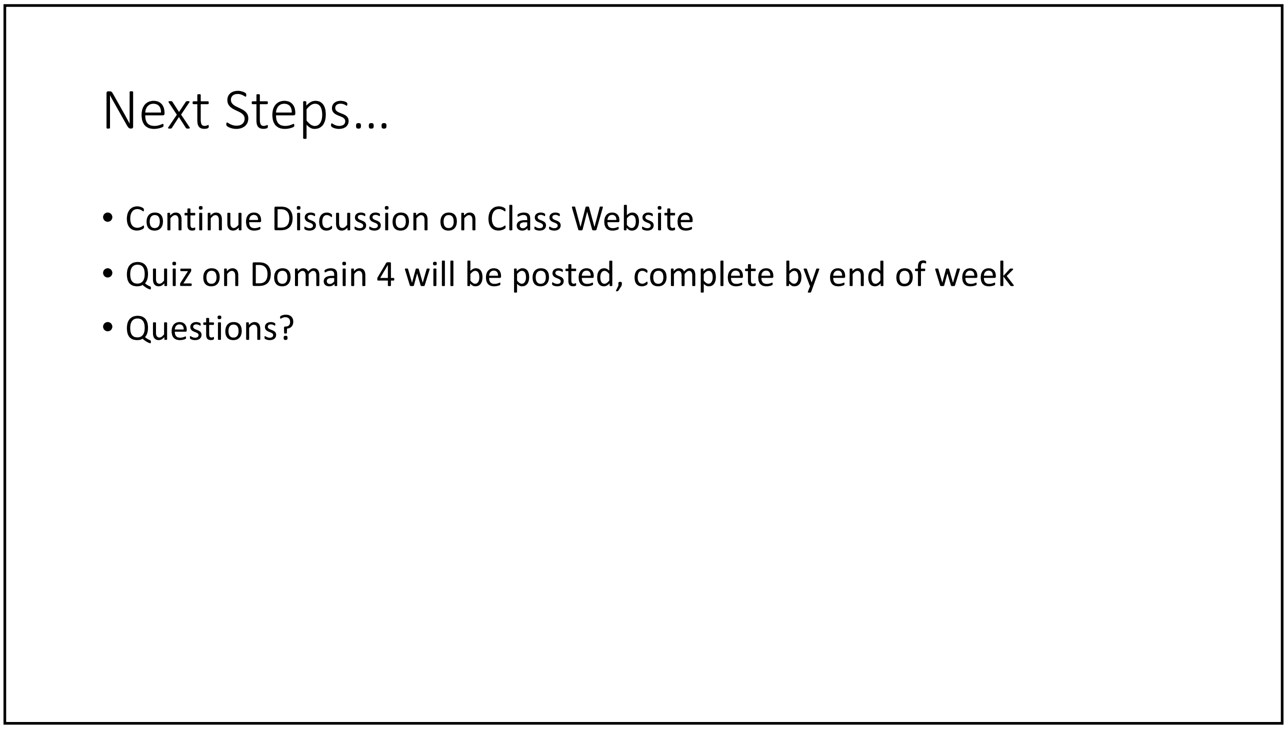
64



Network Attacks

- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Malformed Packets
  - Ping of death – single ICMP Echo Request > 65,536 bytes
- Flooding – overwhelm target system
- SYN flooding
- Sniffing (Wireshark and others)
- Ransomware, Drive-by-Downloads
- DNS Hijacking (Host, Network, Server)

65



Next Steps…

- Continue Discussion on Class Website
- Quiz on Domain 4 will be posted, complete by end of week
- Questions?

66