Mississippi State UNIVERSITY

J. A. "Drew" Hamilton, Jr., Ph.D.

Director, Distributed Analytics & Security Institute
Director, Center for Cyber Innovation
Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Outline (Designing and Protecting Network Security) 14%

- Secure network architecture design (e.g. IP & non-IP protocols, segmentation)
- Secure network components
- Secure communication channels
- Network attacks

Secure network architecture design (e.g. IP & non-IP protocols, segmentation)

Dr. Patrick Pape, MSU

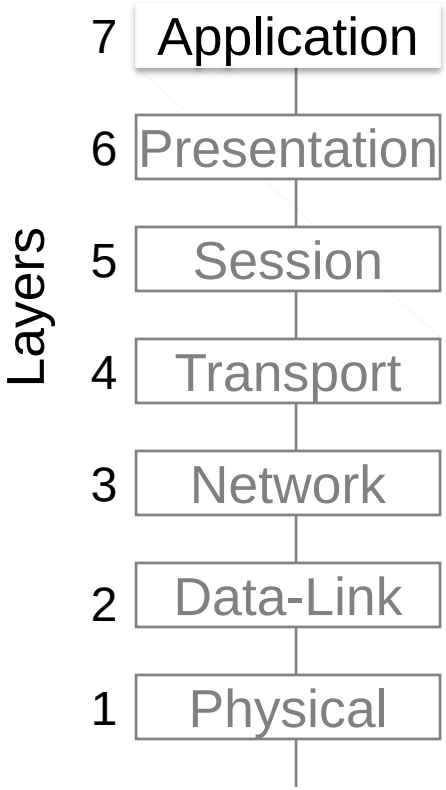
Dr. Chris Harrison, Sandia Labs

Shon Harris

Overview

- The OSI Model
- TCP/IP
- Media Access Technologies
- Cabling Types
- Data Transmission Types
- Network Topology
- Network Devices
- Media Access Protocols
- Firewalls
- Networking Services
- MANs and WANs
- Remote Access

OSI Model - Application Layer



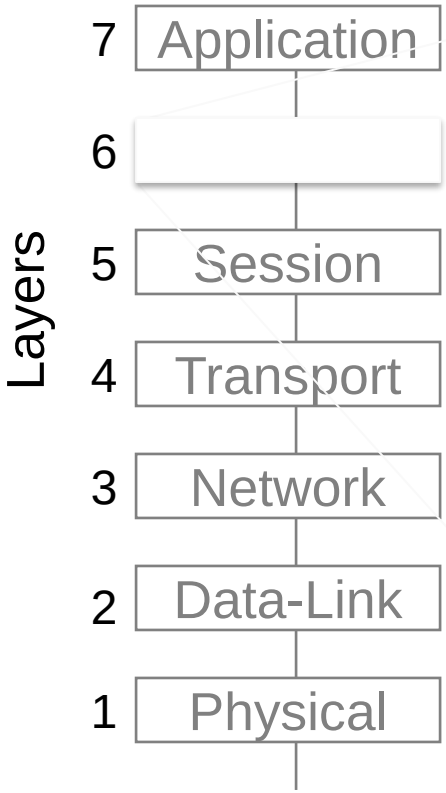
Application Layer

- User-to-Process Interface
  - Database Access
  - E-Mail
  - File Transfer
- Remote Connection
  - e.g. X.400

Protocols

- **FTP**
- **HTTP**
- **TFTP**
- **SNMP**
- **Telnet**
- **SMTP**

OSI Model - Presentation Layer



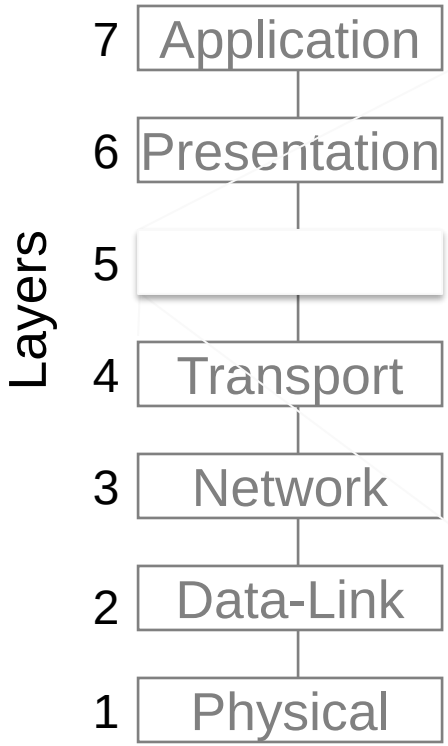
Presentation Layer

- Process-to-Session Interface
  - Protocol Conversion
  - Data Translation
  - Compression/Encryption
  - Character Set Conversion
  - Graphics Command Interpretation
- Redirectors
  - File System
  - Printers
  - Networks

Standards

- **ASCII**
- **EBCDIC**
- **TIFF**
- **JPEG**
- **MPEG**
- **MIDI**

OSI Model – Session Layer



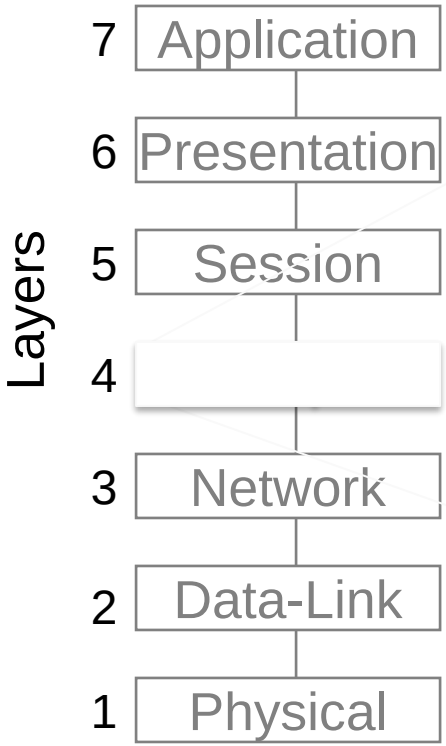
Session Layer

- Process-to-Process
- Establishes comm-link between processes
- Controls Dialog: transmit/receive
- Synchronization: Keeps track of long messages
- Modes:
  - Simplex
  - Half-Duplex
  - Full-Duplex

Protocols

- **NetBios**
- **NFS**
- **SQL**
- **RPC**

OSI Model - Transport Layer



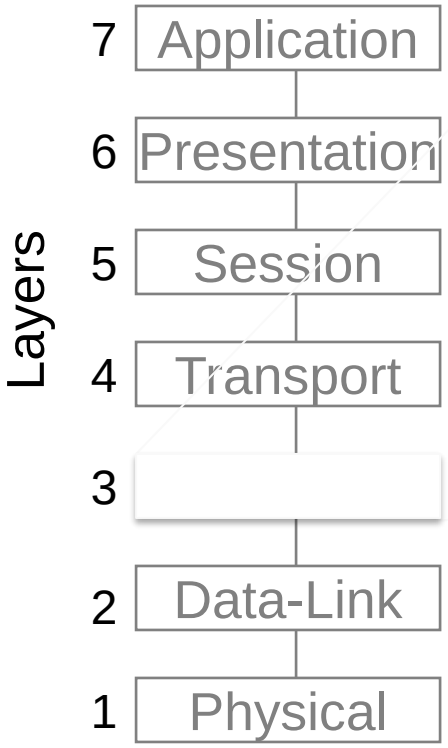
Transport Layer

- Session-to-Network Interface
- Packetizes Session Messages
- Ensures Reliable Connection
- Transmits ACK

Protocols

- **TCP**
- **UDP**
- **SPX**
- **TLS**

OSI Model - Network Layer



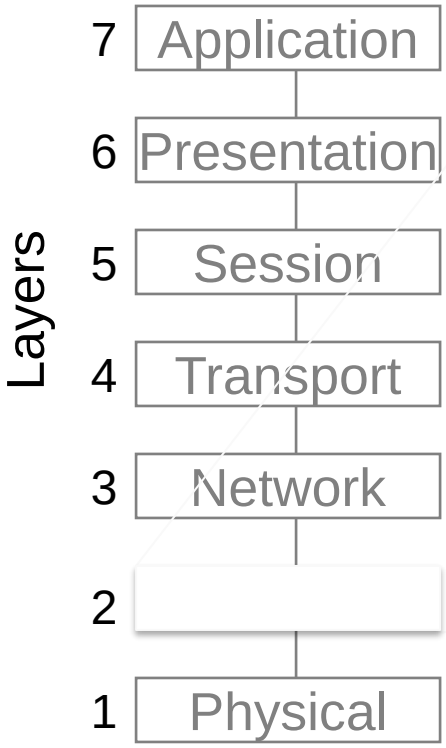
Network Layer

- Network-to-Network
- Packet Transmission
- Routing Decisions
- Load Adaptation

Protocols

- **IP**
- **ICMP**
- **RIP**
- **OSPF**
- **IPX**

OSI Model - Data Link Layer

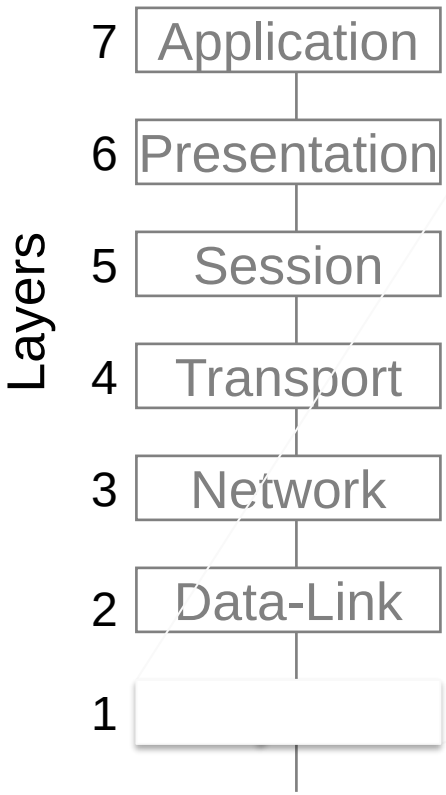


Data Link Layer

- Machine-to-Machine
- Frame Creation
- Error Detection
- Error Correction
- Frame Sequence
- Checksums

- **Protocols**
  - **SLIP**
  - **PPP**
  - **ARP**
  - **RARP**

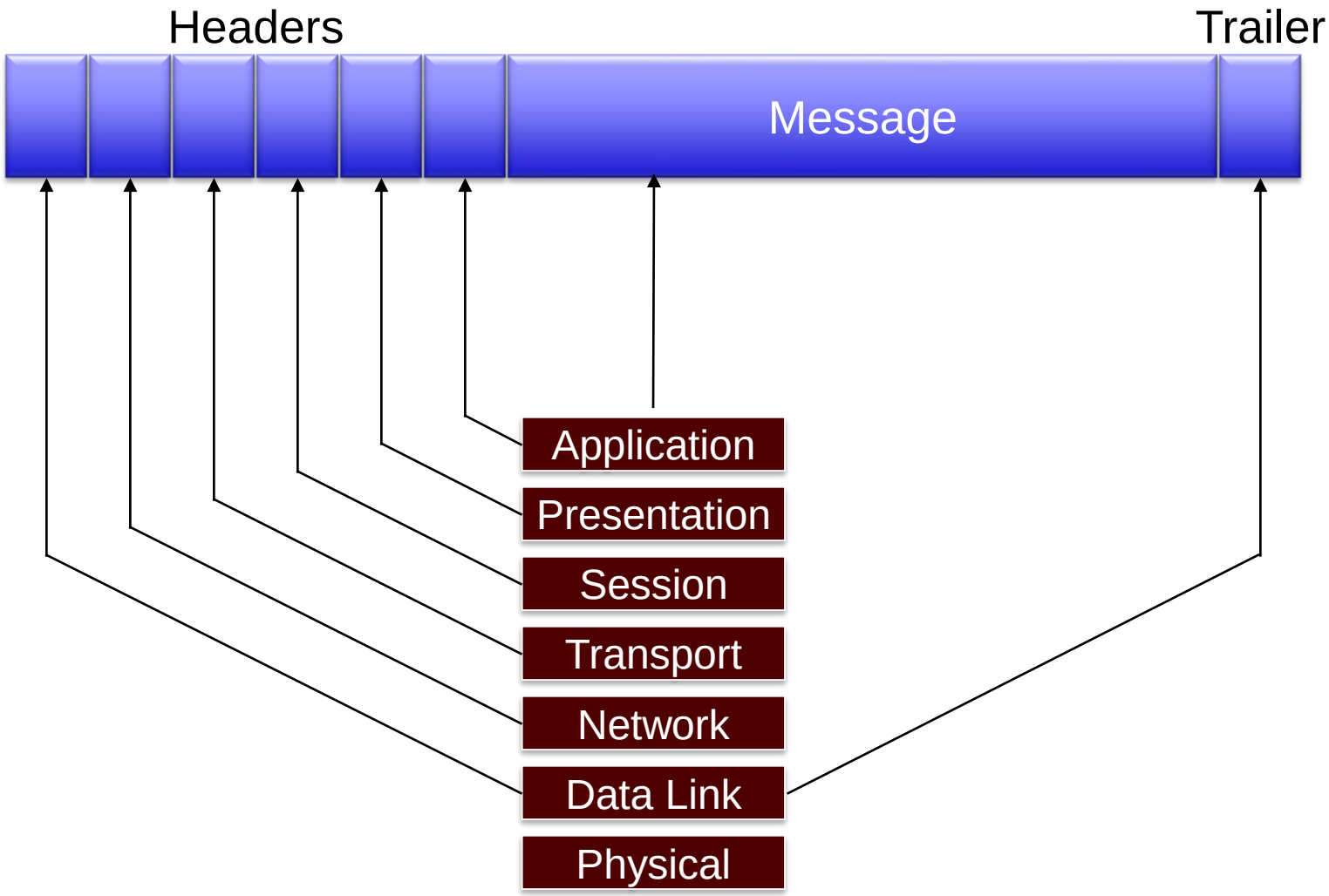
OSI Model - Physical Layer



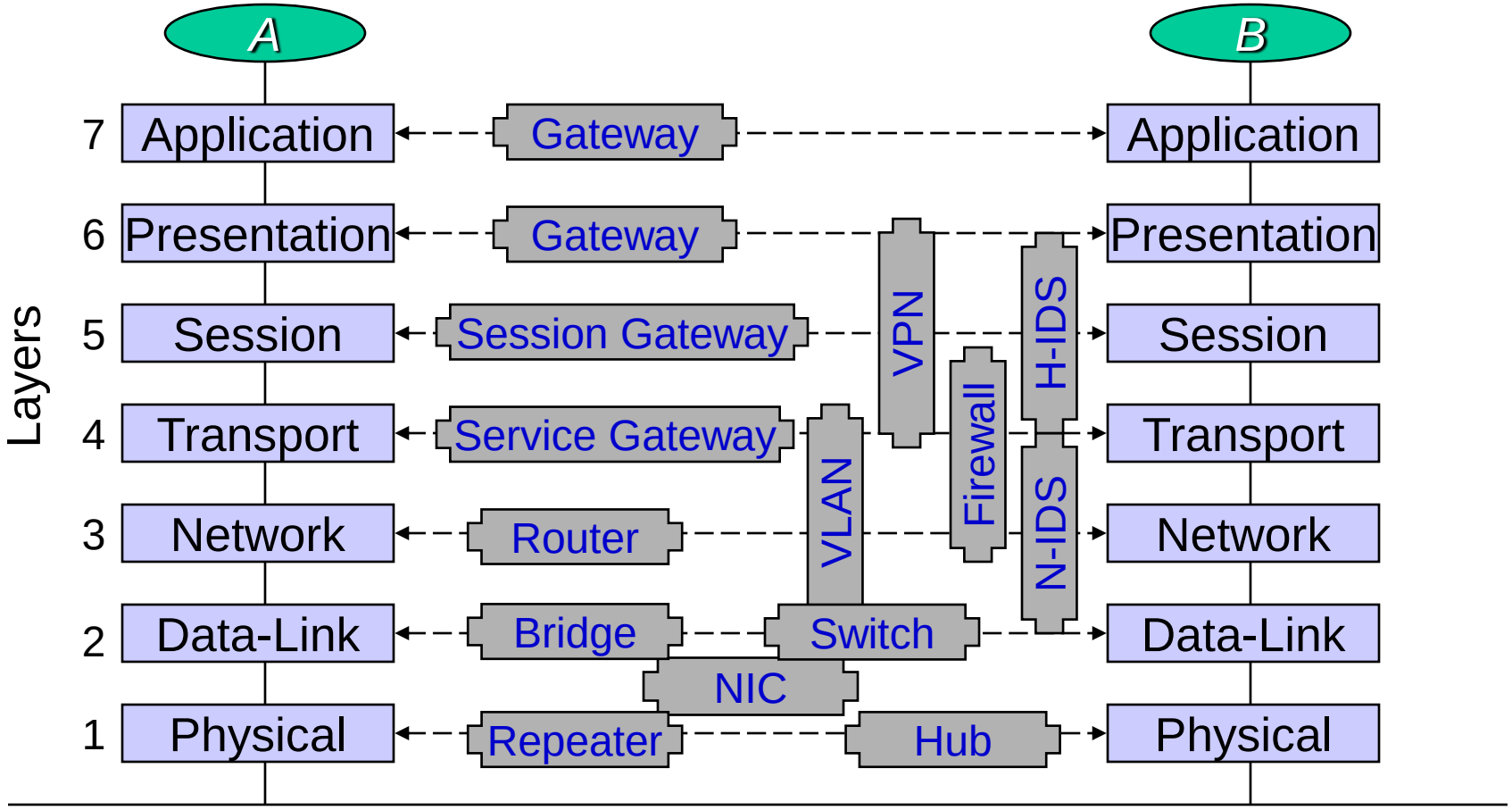
Physical Layer
- •Adapter-to-Adapter
- •Transmission of Bits
- •Voltage Levels
- •Bits per Second
- •Connector Dimensions
- •Adapter Interrupts

Std. Interfaces
- **•RS-232**
- **•HSSI**
- **•X.21**
- **•USB**

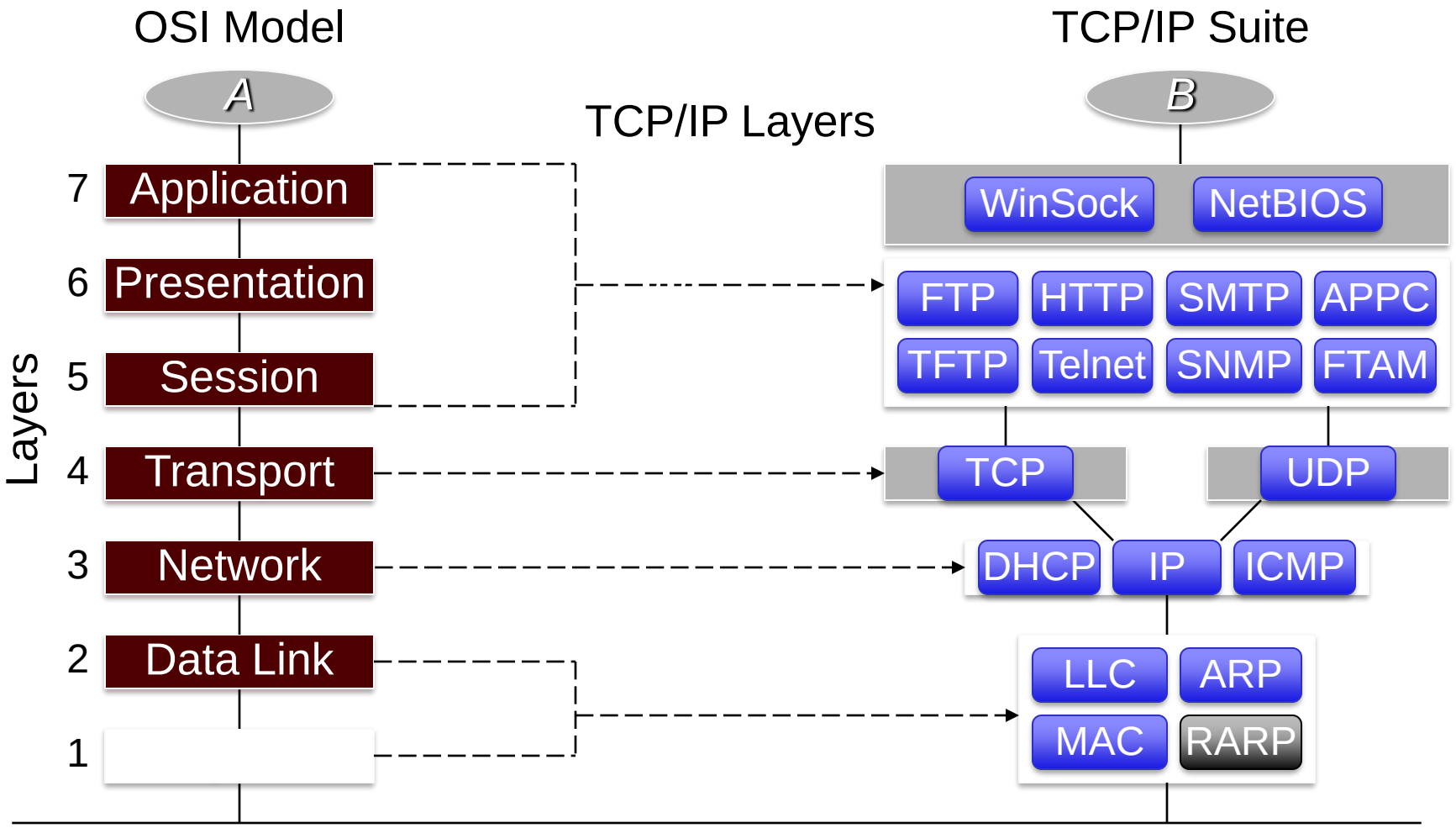
OSI Model - Encapsulation



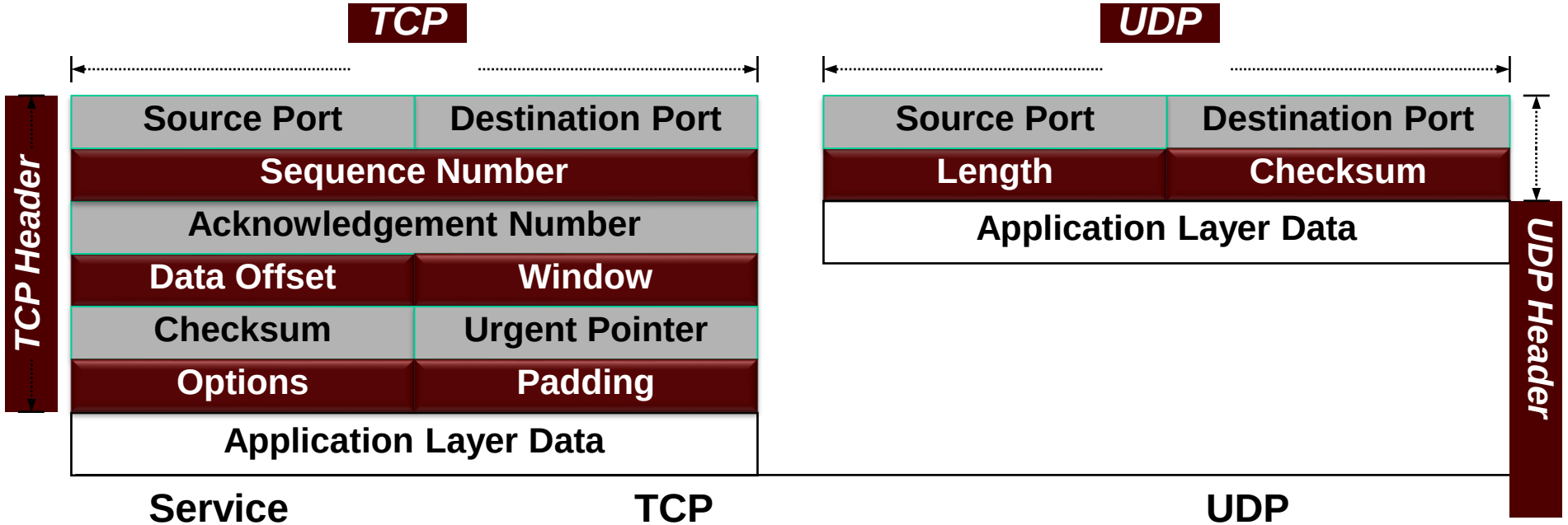
Hardware in the OSI Model



TCP/IP using the OSI model



TCP/IP - Packet Structures and Differences

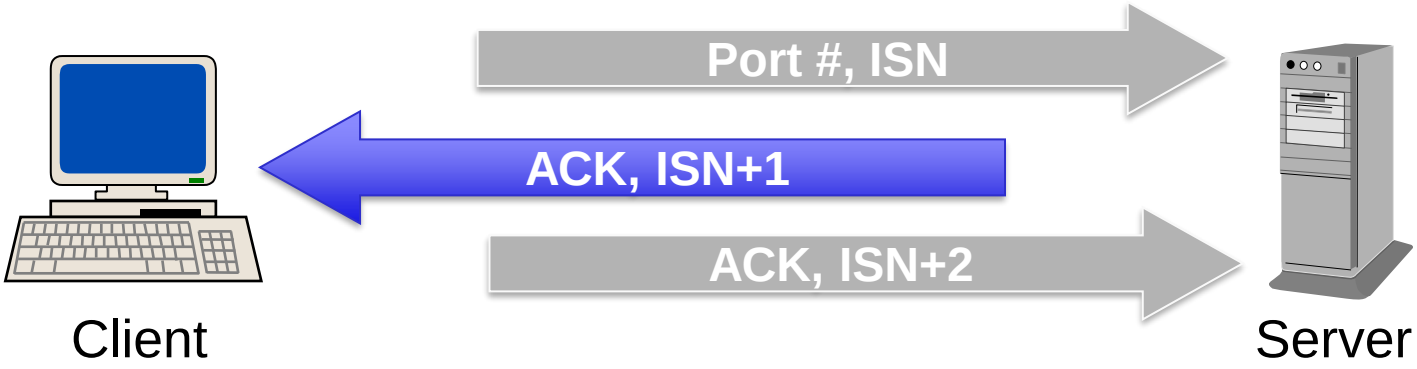


Service	TCP	UDP
Reliability	Returns ACKs when packets are received	Does not guarantee packet arrival
Connection	Connection-oriented; performs handshaking.	Connectionless
Packet Sequence	Uses sequence numbers	None
Congestion Controls	Can slow transmission to alleviate congestion.	No flow control
Speed/Overhead	Slower and more resource intensive	Fast and Light

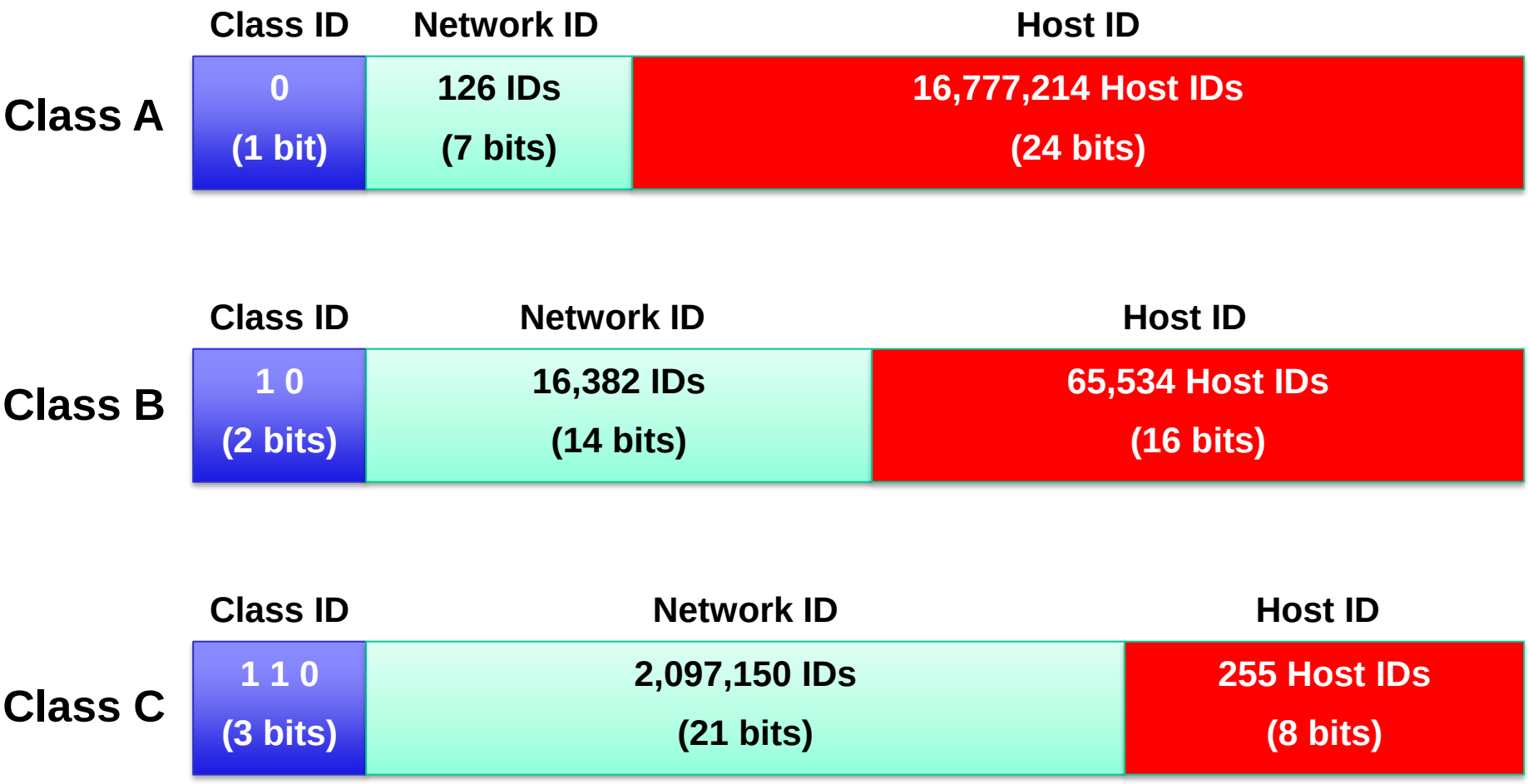
TCP/IP - TCP "Three-Way" Handshake

Initial Sequence Number

- Picked at random
- Controls packet sequence

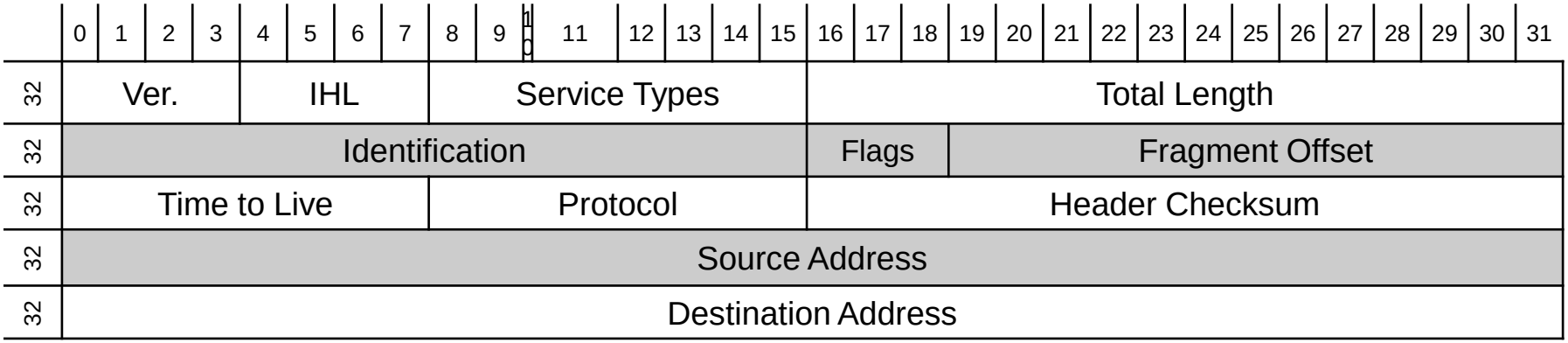


TCP/IP - IPv4 Address Classes

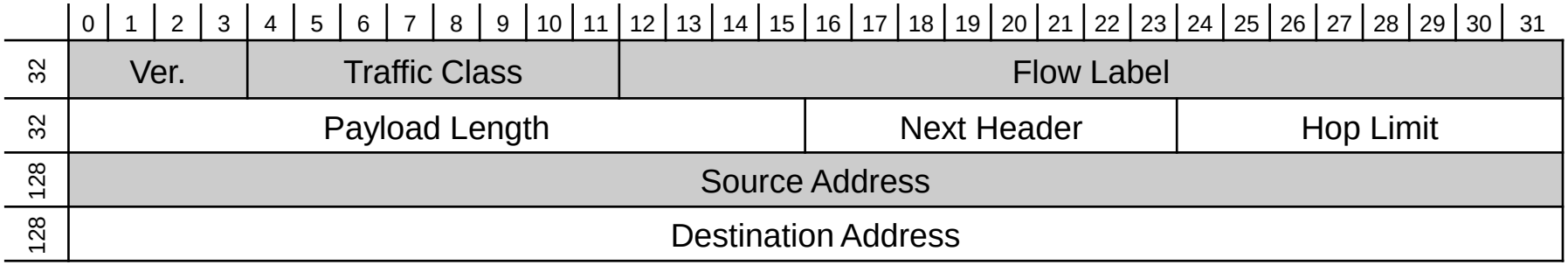


TCP/IP – Differences between IPv4/IPv6

IPv4 Packet

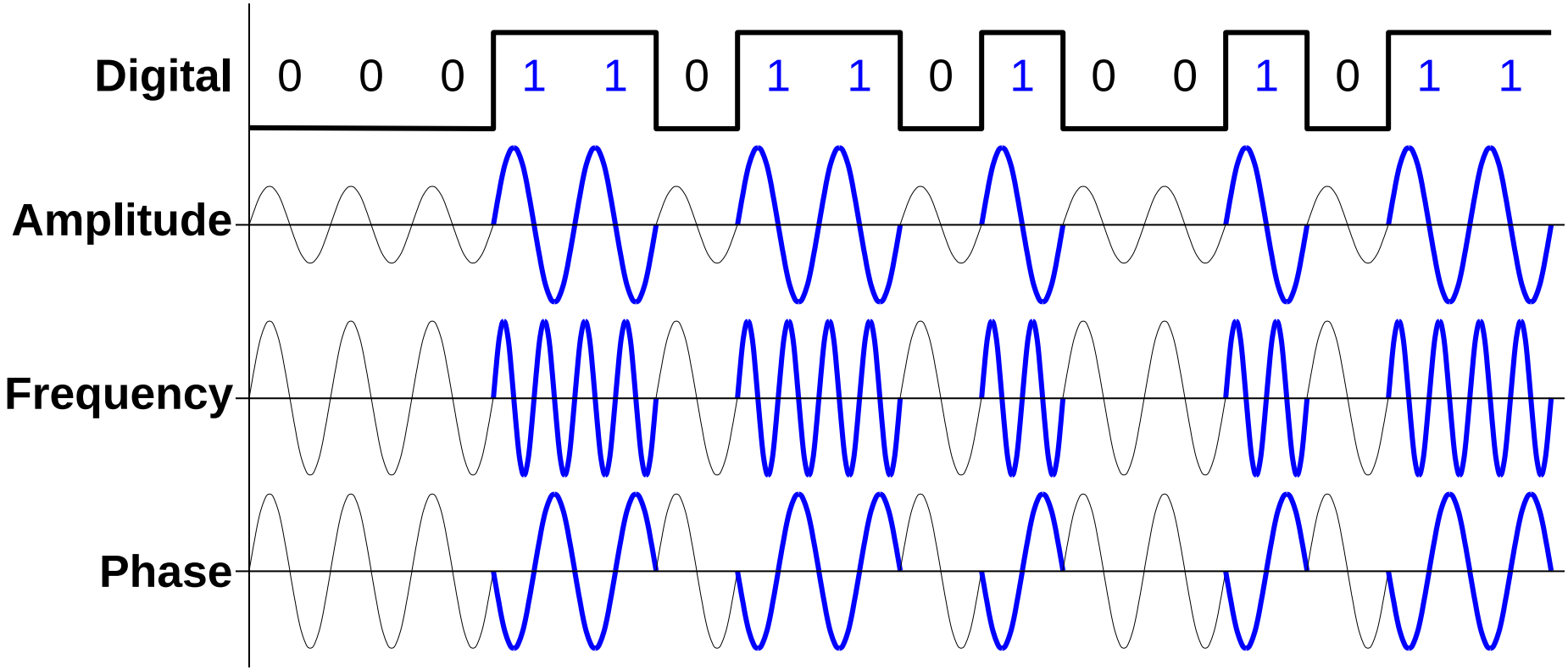


IPv6 Packet

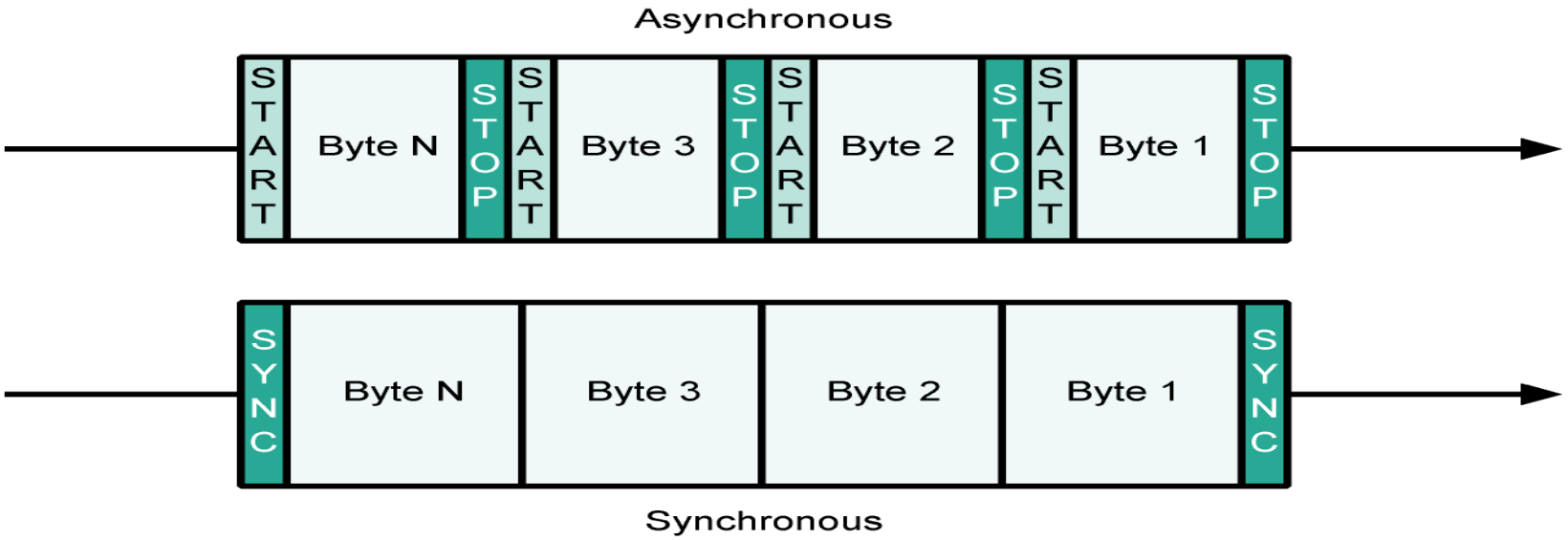


- **Multicasting is globally routable.**
- **Stateless address autoconfiguration (SLAAC)**
- **Added Labeling of Traffic Flow for improved QoS.**
- **Jumbogram increase (64KO to 4GO)**
- **Added extension support for authentication, data integrity, and data confidentiality.**

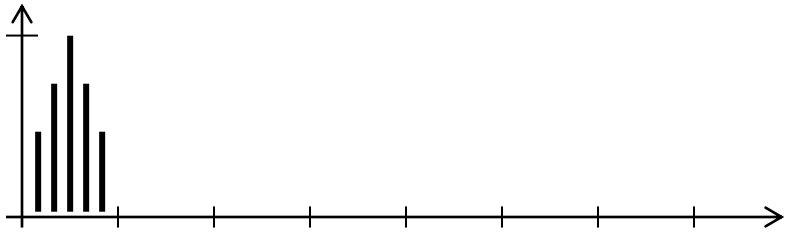
Data Transmission - Digital versus Analog



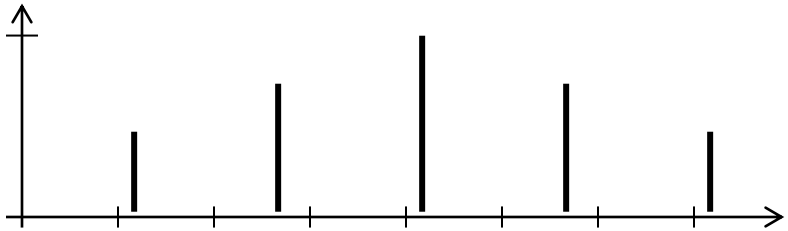
Data Transmission - Asynchronous vs Synchronous



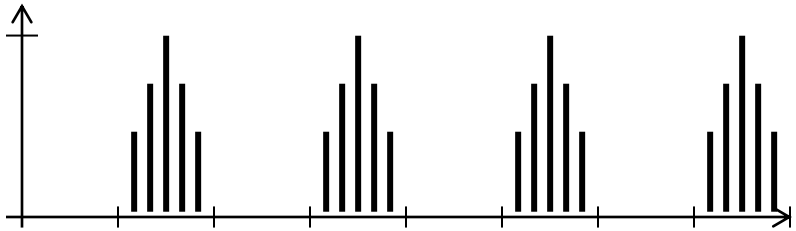
Data Transmission - Broadband versus Baseband



- *Narrowband*
  - Single channel
  - telephone, modem

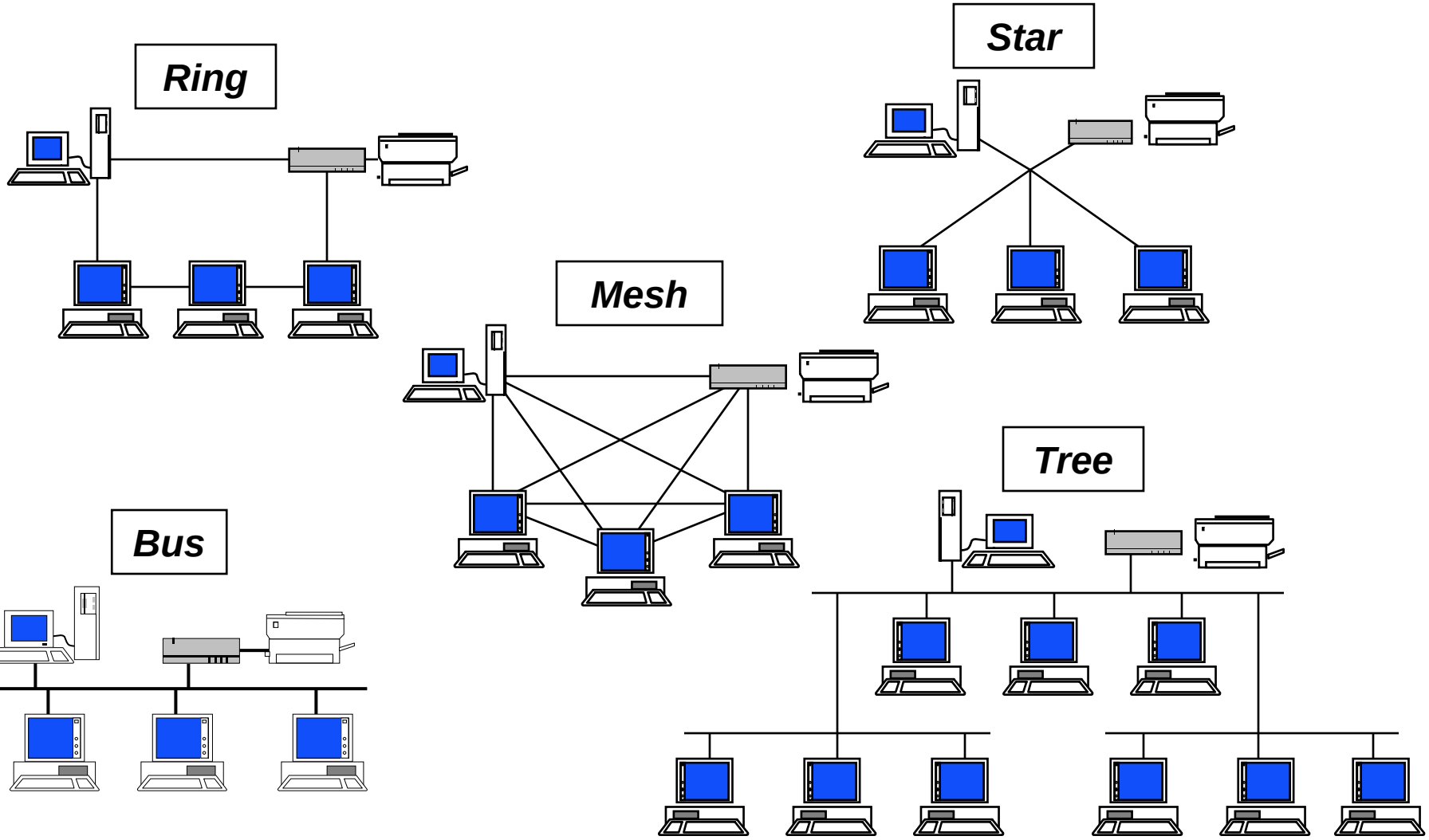


- *Baseband*
  - Comprises entire bandwidth
  - Radar, TV



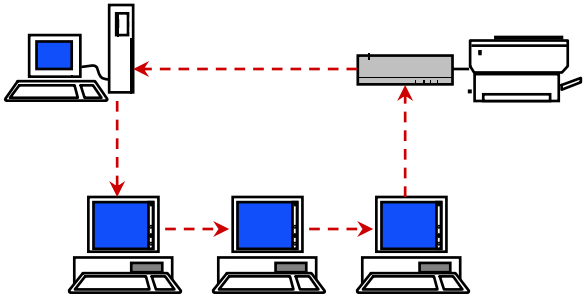
- *Broadband*
  - Splits bandwidth into channels
  - DSL, T1

Network – LAN - Physical Topology



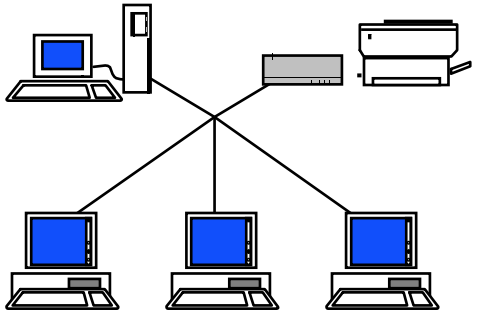
Network – Token Ring and Ethernet

Token Ring (802.5)



- *Token-Passing*
  - Token: 24-bit control frame
    - *Passed sequentially*
  - Process
    - *Source machine receives token*
      - Adds data & addressing
      - *Destination machine copies data*
      - Returns token to Source
      - Source removes data
- *Multi-Station Access Unit* (hub)
- Active Monitor: *handles undeliverable tokens*
- Beaconing: *Locates & mitigates failures*
- Advantage: No collisions

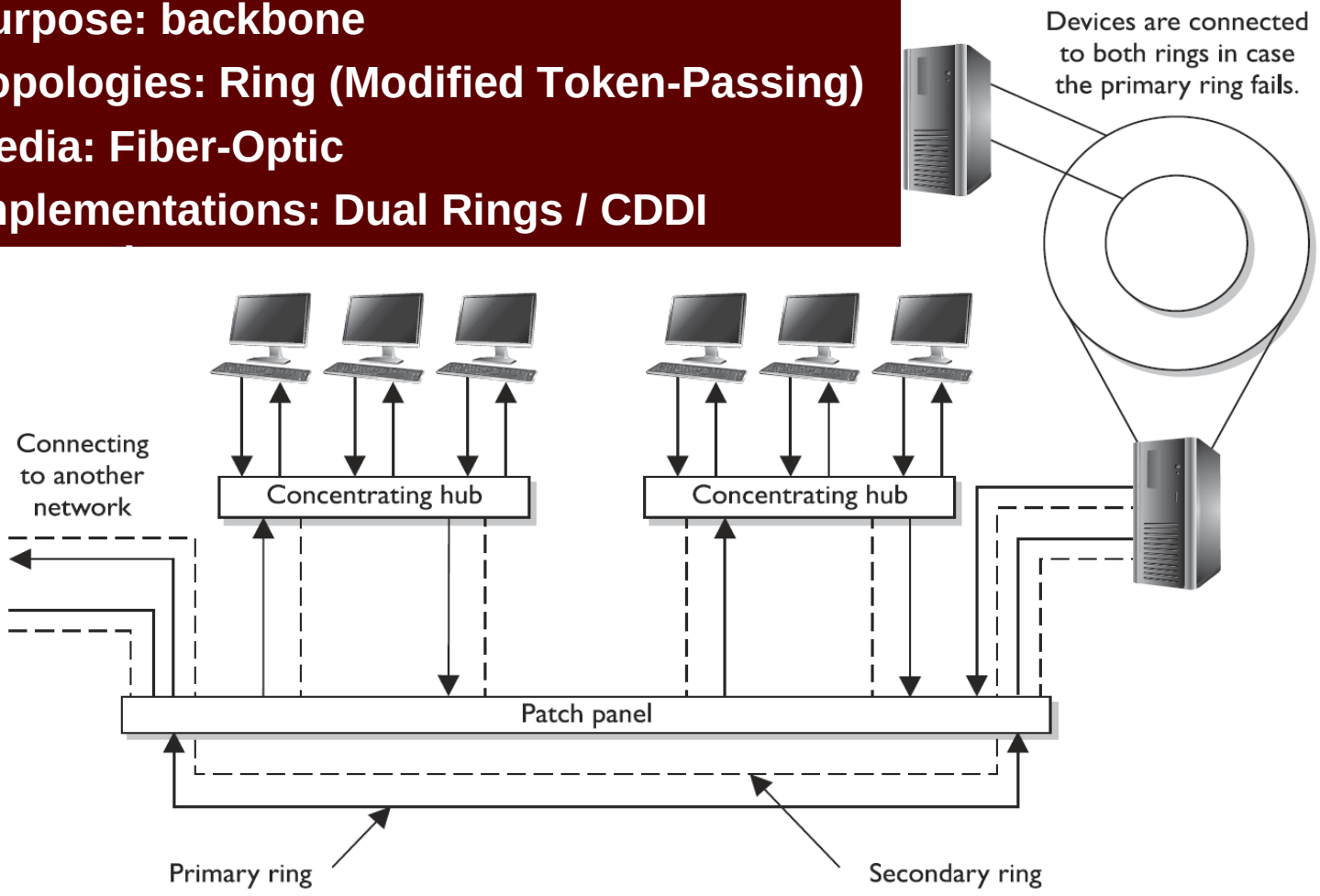
Ethernet (802.3)



- *CSMA/CD*
  - Carrier: A machine is transmitting
    - *Contention: Compete for access*
    - *Collision: Simultaneous transmits*
  - Process
    - *Source listens for carrier*
      - If no carrier, transmit; else, wait.
    - *Destination receives packet*
      - If no collision, acknowledge; else, request retransmission
    - *Source receives request*
      - Wait random time; then retransmit
  - Advantage: Fast at low traffic loads

Network – Fiber Distributed Data Interface (802.8)

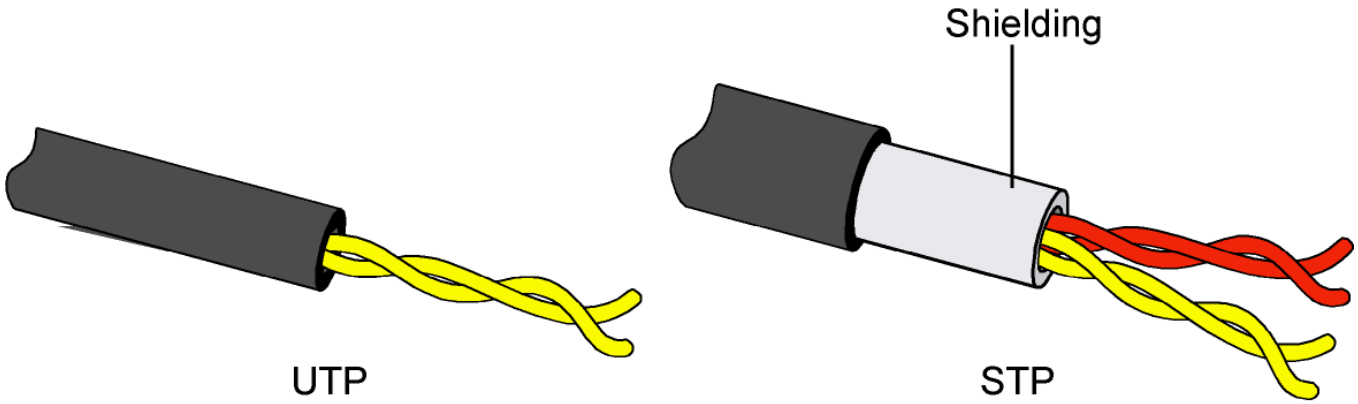
- Purpose: backbone
- Topologies: Ring (Modified Token-Passing)
- Media: Fiber-Optic
- Implementations: Dual Rings / CDDI



Cabling

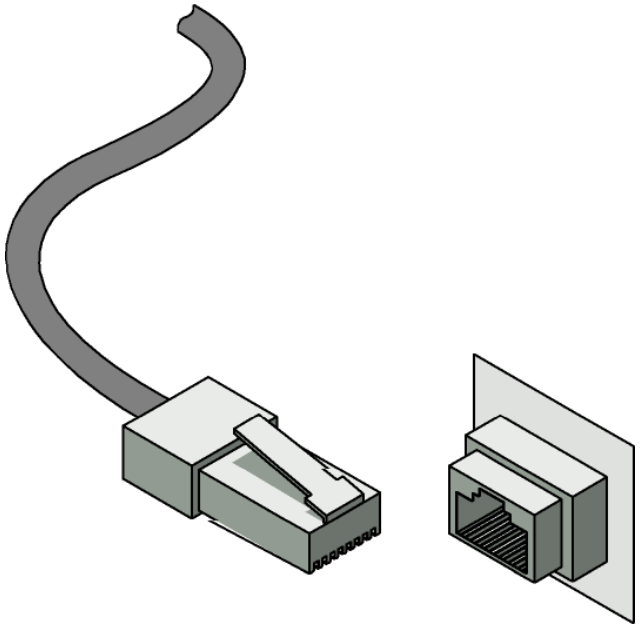
- **Characteristics:**
  - **Bandwidth: *Highest frequency (Hz)***
  - **Data Rate: *Throughput (bps)***
- **Issues**
  - **Noise**
    - **EMI: Electromagnetic Interference**
    - **RFI: Radio Frequency Interference**
  - **Attenuation**
  - **Crosstalk**
  - **Fire Rating:**
    - **Plenum Space: Gap in false ceilings and raised floors**
    - **Plenum Cables: Fluoro-polymer covering**
    - **Conduits: Metal is fire resistant and physical protection**

Cabling - Twisted-Pair



- Least expensive
- Choice of ratings

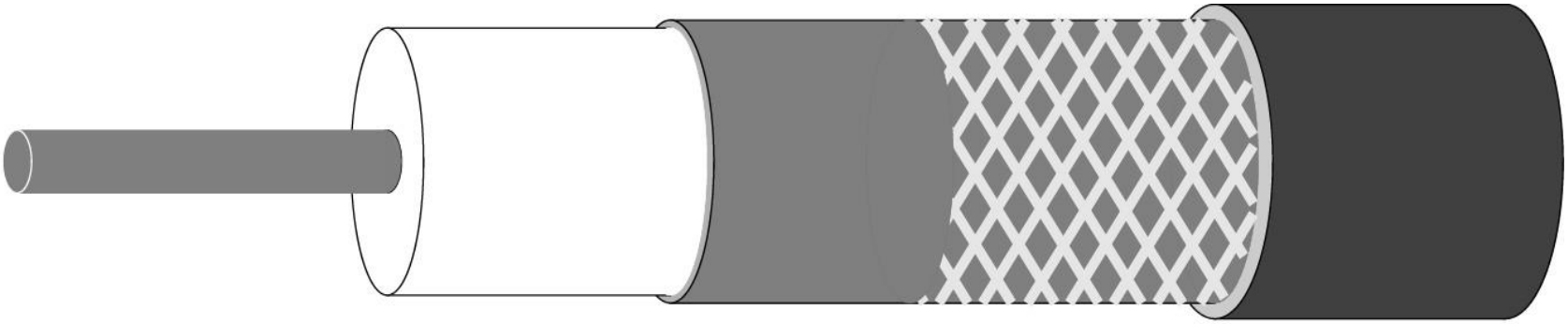
- Least interference resist.
- High attenuation
- Easily tapped



Cabling - UTP Category Ratings

UTP Category	Characteristics	Usage
Category 1	Voice-grade telephone cable	Not recommended for network use, but modems can communicate over it.
Category 2	Data transmission up to 4 Mbps	Used in mainframe and minicomputer terminal connections, but not recommended for high-speed networking.
Category 3	10 Mbps for Ethernet and 4 Mbps for Token Ring	Used in 10Base-T network installations.
Category 4	16 Mbps	Usually used in Token Ring networks.
Category 5	100 Mbps for 100Base-TX and CDDI networks; has high twisting and thus low crosstalk	Used in 100Base-TX, CDDI, Ethernet, and ATM installations; most widely used in new network installations.
Category 6	10 Gbps	Used in new network installations requiring high-speed transmission. Standard for Gigabit Ethernet.
Category 7	10 Gbps	Used in new network installations requiring higher-speed transmission.

Cabling - Coaxial Cable



Solid metal inner core

Plastic insulator - usually white

Foil shield

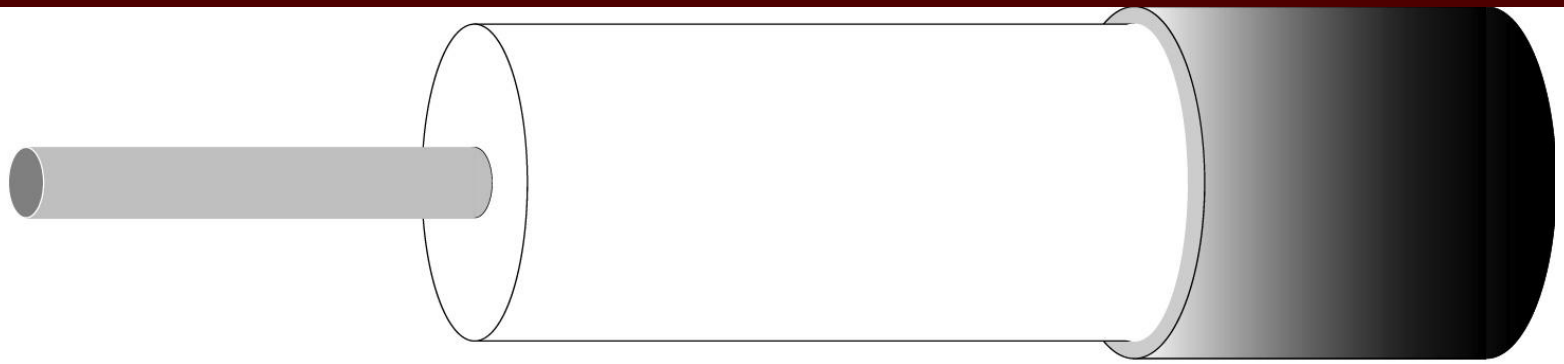
Braided shield/outer conductor

Plastic or vinyl jacket

- **High EMI resistance**
- **Greater Bandwidth than UTP**
- **Less Attenuation than UTP**

- **Expensive**
- **Difficult to install**

Cabling Types - Fiber Optic Cable



	Glass core		Glass cladding
diameters	50 microns 62 microns 100 microns	Multimode	125 microns 125 microns 140 microns
	2-8 microns	Singlemode	

Plastic or vinyl jacket

Note: A micron is a millionth of a meter

- **No EMI/RFI**
- **Highest Bandwidth**
- **Least Attenuation**
- **Hardest to tap**

- **Most Expensive**
- **Difficult to work with**

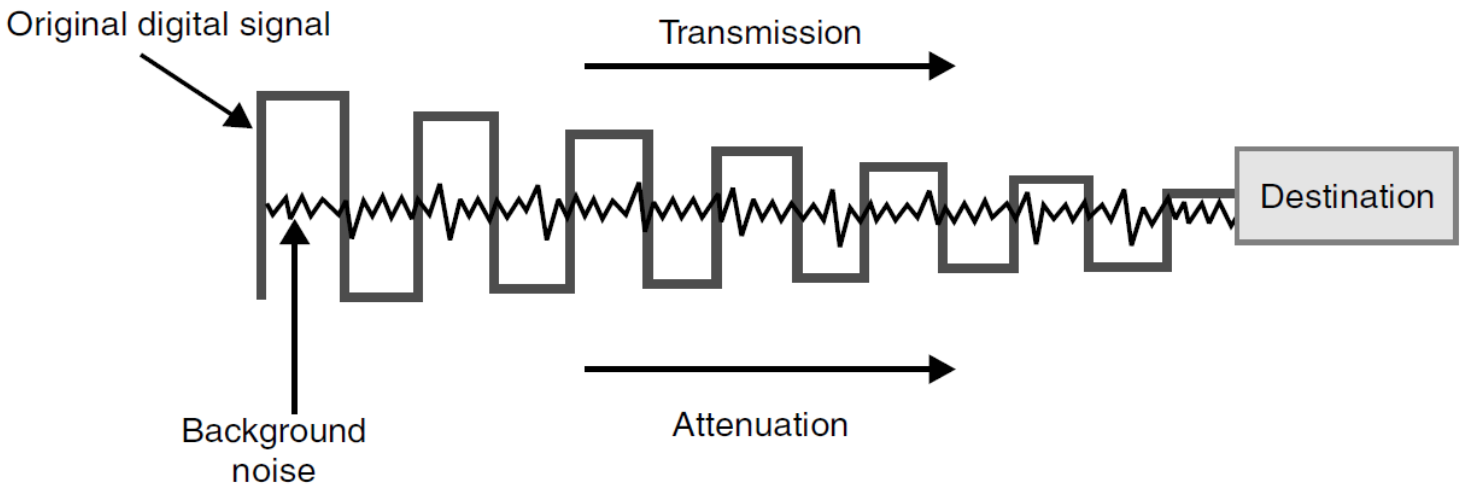
Transmission - Methods

- **Unicast: One-to-One**
  - **Use: *Standard Internet interaction***
- **Multicast: One-to-Many (Class D)**
  - **Use: *Multimedia, real-time video, voice clips***
- **Broadcast: One-to-All (on subnet)**
  - **Use: *Administrator notifications, Network mapping***

Media Access Protocols

- **Addresses**
  - **MAC Address: *Unique physical address of NIC***
    Initial MAC in ROM: 24 bit manufacturer code + 24 bit S/N
  - **IP Address: *Unique logical address on network***
    Static: Assigned by administrator
    Dynamic: Assigned by DHCP server
- **Address Resolution Protocol (ARP) – IP/MAC**
  Stored in ARP table – susceptible to poisoning
- **Reverse ARP (RARP) – MAC/IP**
  - **Boot Protocol (BOOTP): *returns own IP address, name server address and gateway address***
- **Internet Control Message Protocol (ICMP)**
  - **Delivers messages, reports errors & routing info.**
  - **Replies when testing connectivity & problems**
    "Ping" - Echo frame, Reply frame

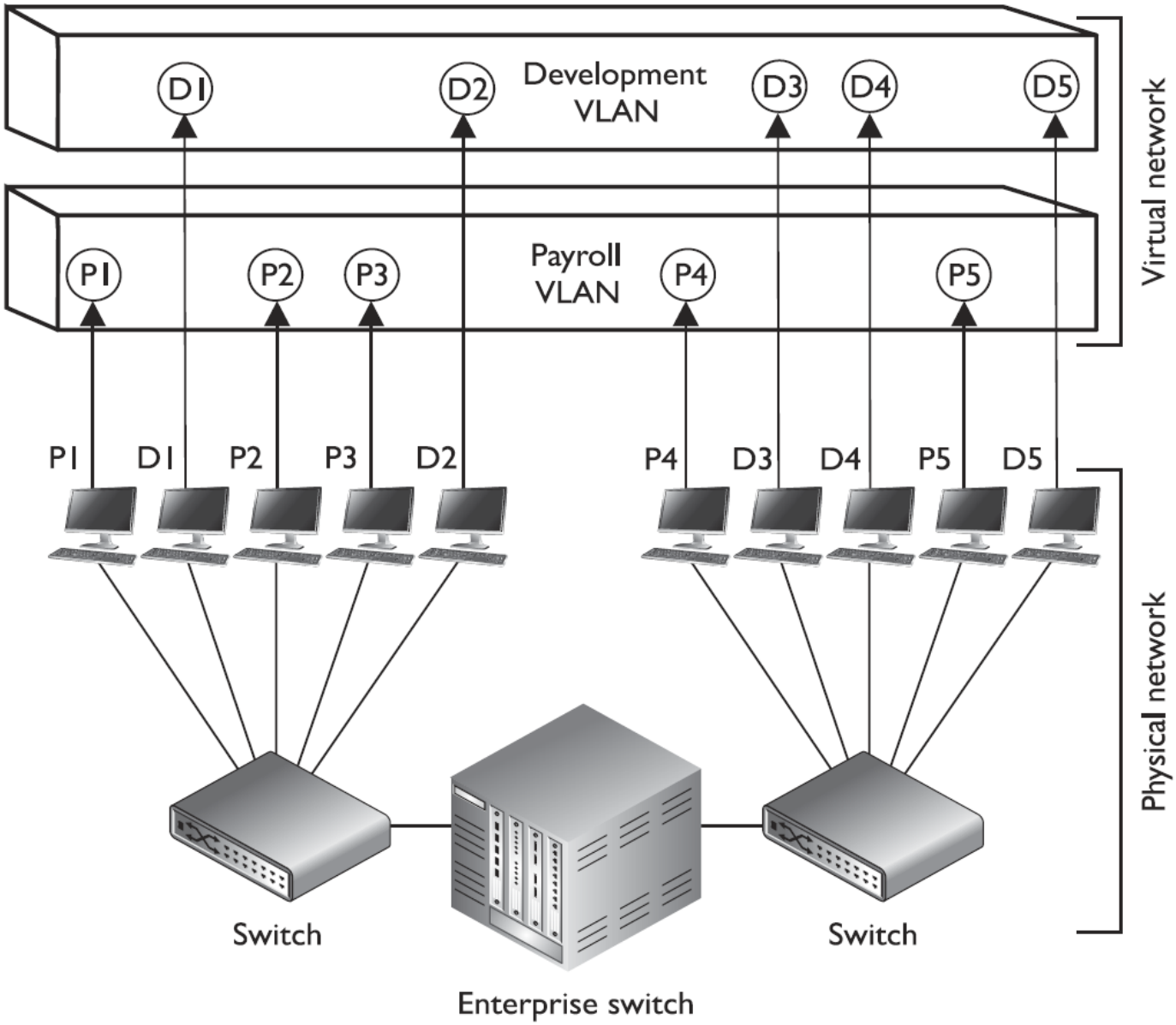
Network Devices – Repeater & Regenerator



Network Segregation & Isolation

- **Purpose**
  - Users do not need full access to all assets
  - Limiting access also reduces network traffic
- **Physical Segregation**
  - Devices: *Locked in wiring closets*
  - Servers: *Kept in controlled room*
  - Workstations: *Separated by organization function*
- **Logical Segregation**
  - Architecture: *Clearly thought-out, fully documented*
  - Routers: *Block broadcast & collision domain information*
  - Users: *Limit number who can connect to critical assets*
  - ACLs

Network Devices – Switch and VLAN



Network Devices – Bridge v. Router

Bridge	Router
Reads header information, but does not alter it	Creates a new header for each frame
Builds forwarding tables based on MAC addresses	Builds routing tables based on IP addresses
Uses the same network address for all ports	Assigns a different network address per port
Filters traffic based on MAC addresses	Filters traffic based on IP addresses
Forwards broadcast packets	Does not forward broadcast packets
Forwards traffic if a destination address is unknown to the bridge	Does not forward traffic that contains a destination address unknown to the router

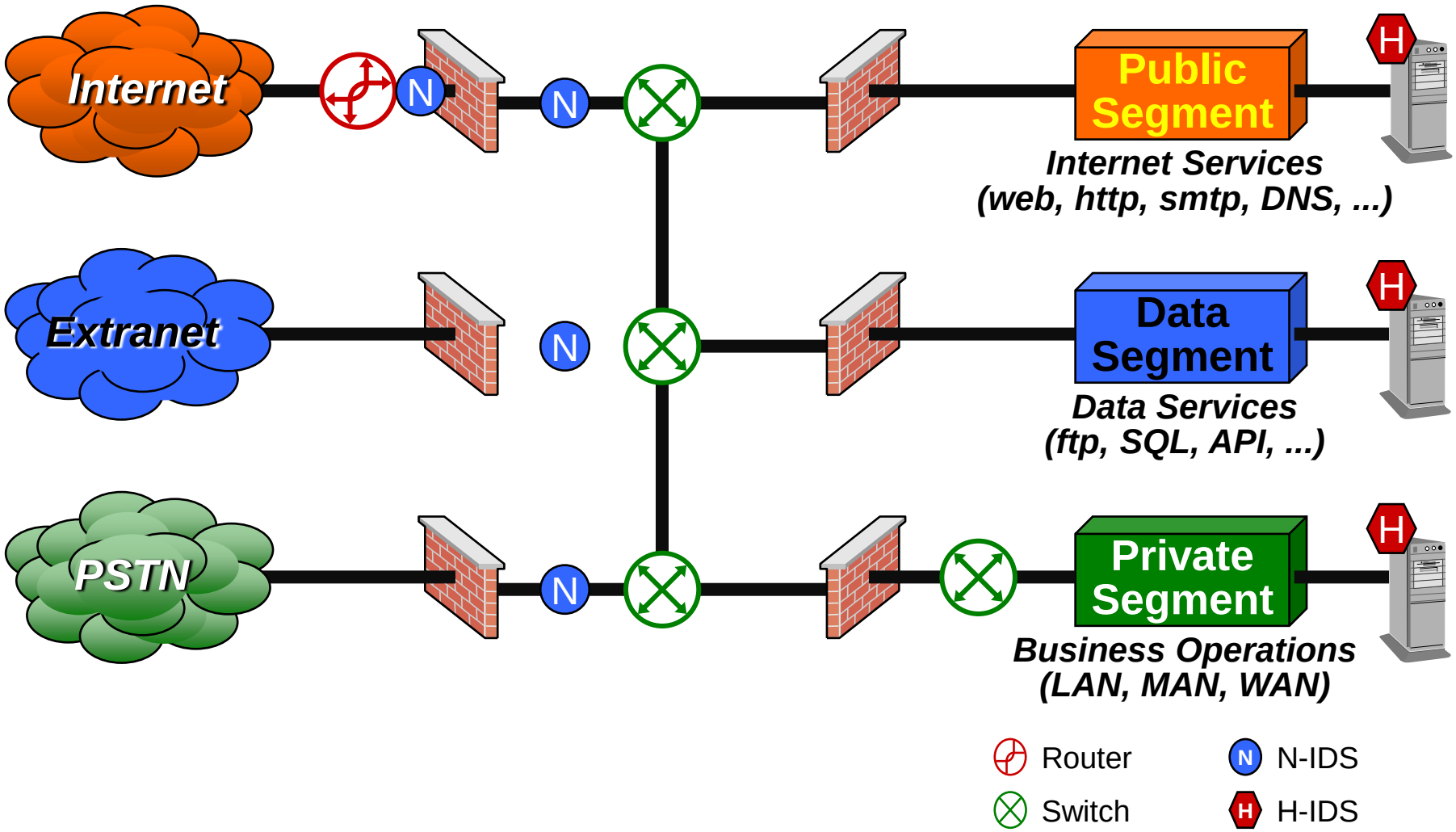
Network Devices - Summary

Device	OSI Layer	Functionality
Repeater	Physical	Amplifies the signal and extends networks.
Bridge	Data Link	Forwards packets and filters based on MAC addresses; forwards broadcast traffic, but not collision traffic.
Router	Network	Separates and connects LANs creating internetworks; routers filter based on IP addresses.
Switch	Data Link	Provides a private virtual link between communicating devices; allows for VLANs; reduces collisions; impedes network sniffing.
Gateway	Application	Connects different types of networks; performs protocol and format translations.

Firewalls

- **Purpose**
  - **Enforce security policy**
    - Acceptable & unacceptable actions
    - Allowable TCP ports & services
    - IP address range restrictions
- **Function**
  - **Monitors & filters packets based on**
    - IP address, TCP port, packet type, protocol, etc.

Demilitarized Zone (DMZ) "Screened Subnet"



Filtering Firewalls

- **Packet Filtering - First Generation**
  - Inspect packet header: *IP address & TCP port*
    Use ACL rules to allow or disallow
  - Pros: *Scalable, Fast, Application independent*
  - Cons: *Header data only, Does not track state*
- **Proxy Firewalls - Second Generation**
  - Makes connection: *hides private network addresses*
    Handles all messages: copies, inspects, repackages
  - Pros: *Application aware, Filters at all layers*
  - Cons: *Not scalable, very slow, limited to defined apps*
- **Stateful Packet Filtering - Third Generation**
  - Tracks connections to completion
  - State Table: *Pairs inbound & outbound packets*
    States: Outbound request is waiting for inbound reply
    Rules: Disallow inbound requests, but allow inbound replies
  - Pros: *Scalable, Fast, Transparent, Stateful*
  - Cons: *Denial of Service attacks*

Firewall - Proxies

- **Dual-Homed Host Firewalls**
  - **Two interfaces, Two NICs - *inward & outward***
    - **No packet-forwarding: would allow uncontrolled access**
    - **Proxy software handles packet transfers**

- **Proxy Types**
  - **Application-Level: *Inspects packet content***
    - **Access decided based on content of packet**
      - **Service, Protocol, Command: *FTP Get vs. FTP Put***
    - **Pro: High level of granularity**
    - **Con: Must have one App-Level proxy per service, Slow**
  - **Circuit-Level: *Monitors client to server connection***
    - **Access based on source & destination IP addresses**
    - **Pro: Handles many protocols**
    - **Con: Not as granular as App-level**
  - **SOCKS Servers: *Circuit-level proxy gateway***
    - **Usage: Outbound Internet & pseudo VPN functionality**
      - **Provides authentication & encryption**

Firewall Architecture

- **Bastion Host - The Firewall**
  - Exposed to the Internet: *existence is known*
  - Locked down: *Lose all protection if compromised*
- **Screened Host**
  - Bastion behind a border router
    - Border router filters out irrelevant Internet traffic
    - Only the firewall talks to the border router
- **Honeypots**
  - Purpose: *Entice attackers*
  - Setup: *Unprotected computer in the DMZ*
  - Concept: *Loss of honeypot is not critical*
    - Can provide warning before attack to critical systems
    - Can support evidence of attack against other systems

Firewall Best Practices

- **Blacklist**
- **Rules:**
  - **Spoofing - *Inbound packet has internal source address***
  - **Zombies - *Outbound packet has external source address***
  - **Fragments - *May be malicious when reassembled***
  - **Source-routing - *Helps outsiders map internal networks***
- **Minimize Attack Vectors**
  - **No unnecessary services**
  - **Disable unused subsystems**
  - **Patch known vulnerabilities**
  - **Disable unused user accounts**
  - **Close unneeded TCP ports**

Network Services - Domain Name System (DNS)

- **Purpose**
  - Resolves URL to IP addr. (ICANN)
- **Architecture**
  - Root Domain Server: *Managed by Network Solutions, Inc.*
  - TLD Server (*Top-Level Domain)*: .com, .net, .mil
  - DNS Server: Fault Tolerant, backup servers
  - Authoritative Name Server: *DNS for internal "zone"*
    - Zone: DNS services for organizational subgroups
      - May encompass one or more domains
- **Name Resolution Process**
  - URL entered
  - Client sends URL to DNS to resolve
    - If not in Records, pass to next level up
  - Server returns IP address

Networking Services - Directory Services

- **Purpose**
  - **Central repository of important network info.**
- **Components**
  - **Class based Hierarchical database**
    - **X.500: model for database structure**

    Entities: Instances of objects
    - **Types: *users, computers, peripherals, other resources***
    - **Attributes: *name, location, resources, profiles***
    - **Information: *peripherals, e-commerce, network services***
    - **Controls: *ACLs, audits, resource limits, firewall rules, VPN, QoS***
  - **Schema: *Structure of the directory, object relationships***
  - **LDAP: *Lightweight Directory Access Protocol***
  - **Meta-directory: *Allows for communication between directories***
- **Examples**
  - **Microsoft Active Directory, Novell Directory Services (NDS)**

Metropolitan Area Network (MAN)

- **Purpose: Business backbone**
  - **Connect to Internet, WAN or other business**
- **Implementations**
  - **FDDI**
  - **SONET: *Synchronous Optical Network***
    - **Telecom over fiber standard: self-healing, redundant paths**
    - **Content: Digitized voice, Variable frame size**
    - **Carriers: T-1, Fractional T1, T-3**

Wide Area Network (WAN)

- Multiplexing: *Combine multiple channels onto one path*
- TDM: *Time-Division Multiplexing* -- shared by timeslot
  - T-1 = 24 channels, T-3 = 28 T-1 channels
- Fiber-optics: *Large bandwidth, long-distance, high quality*
- Optical Carrier: *Packetized TDM over Fiber* -- e.g. SONET
- ATM: *Asynchronous Transfer Mode*
  - Fixed-length frames, called "cells", over SONET
- Dedicated Links
  - Lease or "point-to-point": *Fast, but expensive*
    - Pro: Only destination points can use it to communicate
    - Con: Connected even during periods of non-use
- T-Carriers
  - Dedicate lines carry voice & data over trunks
    - T-1 = 1.544 Mbps, T-3 = 45 Mbps

WAN (2)

- Switching
  - Circuit-Switching: Connects a channel from end to end
  - Packet-Switching: Packets use multiple paths to the destination
- Virtual Circuits
  - Permanent Virtual Circuit (PVC): Programmed in advance
- Switched Virtual Circuit (SVC): Built up on demand
- S/WAN: Secure WAN
  - Firewall-to-Firewall connection
    - Based on VPNs created with IPSec
    - Strong encryption (incl. header), Public-Key authentication
  - Initiative of RSA Security

WAN Protocols

WAN Technology	Characteristics
Dedicated line	- Dedicated, leased line that connects two locations - Expensive compared to other WAN options - Secure because only two locations are using the same media
Frame relay	- High-performance WAN protocol that uses packet-switching technology, which works over public networks - Shared media among companies - Uses SVCs and PVCs - Fee based on bandwidth used
X.25	- First packet-switching technology developed to work over public networks - Shared media among companies - Lower speed than frame relay because of its extra overhead - International standard and used more in countries other than the U.S. - Uses SVCs and PVCs
SMDS	- High-speed swtiching technology used over public network
ATM	- High-speed bandwidth switching and multiplexing technology that has a low delay - Uses 53-byte fixed-size cells - Very fast because of the low overhead
SDLC	- Enables mainframes to communicate with remote offices - Provides polling mechanism to allow primary and secondary stations to communicate
HDLC	- New and improved SDLC protocol - A data encapsulation method for synchronous serial links - Point-to-point and multipoint communication
HSSI	- DTE/DCE interface to enable high-speed communication over WAN links
VoIP	- Combines voice and data over the same IP network media and protocol - Reduces the costs of implementing and maintaining two different networks

Remote Access

- **Dial-up and RAS**
  - **Analog, point-to-point, circuit-switched**
    - **Modem provides 56 Kbps**
  - **Network Access Server: *PPP session***
  - **Remote Access Service: *Microsoft***
  - **RADIUS Server**
- **ISDN: Integrated Services Digital Network**
  - **Digital, point-to-point, circuit-switched**
    - **Basic (B) channel: 64 Kbps -- voice or data**
    - **Data (D) channel: 16 Kbps -- signaling**
  - **Basic Rate Interface (BRI): *144 Kbps***
  - **Primary Rate Interface (PRI): *1.544 Mbps***
  - **Broadband-ISDN: *backbone***

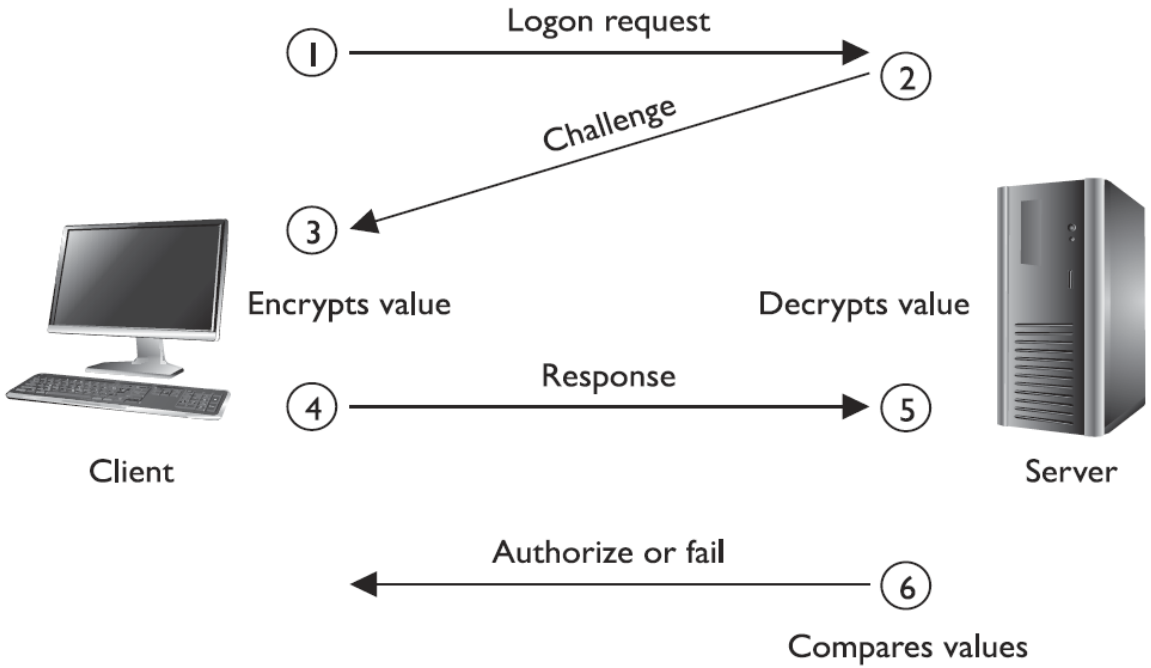
Remote Access (2)

- **DSL: Digital Subscriber Line**
  - **Digital, high-speed, broadband -- *up to 52 Mbps***
    - **Rate depends on distance from central office**
    - **Symmetric or asymmetric**
- **Cable Modems**
  - **Digital, high-speed, broadband -- *up to 50 Mbps***
    - **Rate depends on number of subscribers**
- **VPN: Virtual Private Network**
  - **Secure, private connection via public networks**
    - **Encryption/tunneling ensure privacy -- PPTP, IPSec, L2TP**
  - **Usage**
    - **Dial-up to ISP to Company**
    - **User-to-User: Requires VPN**
    - **Gateway-to-Gateway: VPN between routers**
    - **Firewall-to-Firewall: VPN between firewalls -- Extranet**

Remote Access - Tunneling Protocols

- **Tunneling Protocols**
  - **Tunnel: *Virtual path across networks***
    Allows connection of non-routable protocols -- NetBEUI
  - **PPP: *Point-to-Point Protocol* -- Internet dial-up *-- replaced SLIP***
    Encapsulate messages & transmit over serial line
  - **PPTP: *Point-to-Point Tunneling Protocol***
    Encrypts & encapsulates PPP packets
  - **L2F: *Layer Two Forwarding* -- provides mutual authentication**
  - **L2TP: *Layer Two Tunneling Protocol* -- PPTP + L2F**
    Tunnels many types of networks, but is not encrypted

Remote Access – Authentication Protocols



- Authentication Protocols
  - Negotiation order: *EAP, CHAP, PAP*
  - PAP: *Password Authentication Protocol* -- Cleartext
    - Vulnerable to sniffing, replay and MiM attacks
  - CHAP: *Challenge-Handshake Authentication Protocol*
    - Encrypt & compare random value
  - EAP: *Extensible Authentication Protocol* -- framework
    - Allows tokens, biometrics, etc.

Remote Access – Best Practices

- **Modems**
  - **Caller ID: *Blacklist (answer approved calls only)***
  - **Call-Back: *Use prearranged phone number***

    Compromised with Call-Forwarding
  - **Wardialing: *Disable unprotected modems, Answer after fourth ring, Dial-out only***

- **"Always-on" Modems**
  - **Vulnerable to sniffing, scanning, probing, hacking, DoS, etc.**
  - **Solution: *Personal firewalls***

- **Other**
  - **Identify & audit users: *Disable unneeded accounts***
  - **Two-factor authentication: *RADIUS or TACACS+***

Secure network components

Pascal Meunier, Ph.D., M.Sc., CISSP

Routing Outline

- Distance vector algorithms
  - RIP
    - Intra-domain routing
- Path vector protocols
  - BGP
    - Inter-domain routing
- Link State protocols
  - OSPF

Definitions

- A router connects two or more networks and forwards packets at the network layer (IP)
  - Where to is based on "routes"
  - Routes can be static, or calculated by using a routing protocol
- Router and gateway are synonyms
- Autonomous System
  - "A set of routers under a single technical administration, using an interior gateway protocol and common metrics to route packets within the AS, and using an exterior gateway protocol to route packets to other ASs"
  - Encapsulates a set of networks as a single entity, regardless of what happens inside

Secure Routing Requirements

- **Routing information must have:**
  - **Integrity**
  - **Authenticity**
  - **Authorization**
  - **Timeliness**
    - **Resist replay attacks**

Source Routing

- IP option to specify the routes a packet should take
  - In the IP header
    - Data controlled by sender
- Options:
  - Strict Source Route
    - Exact sequence of routers to use
  - Loose Source Route
    - Specify some routers packets should go through
  - Record Route
    - Figure out which routes a packet takes
- Return route must be saved and used on all further communications (e.g., TCP segments)

Source Routing Attacks

- An attacker can send a packet specifying the return route
  - The attacker may control one of the "routers" on the return route
  - Attacker needs to send a single valid packet for that new route to be used for the entire TCP connection
    - Initial sequence number just has to be guessed correctly once
      - TCP session sniffing
      - Man-in-the-middle attack
        - » On-the-fly packet modification
        - » Dropping packets selectively, or all packets
  - TCP IP spoofing
    - Three-way handshake possible because the attacker gets the replies through the specified router

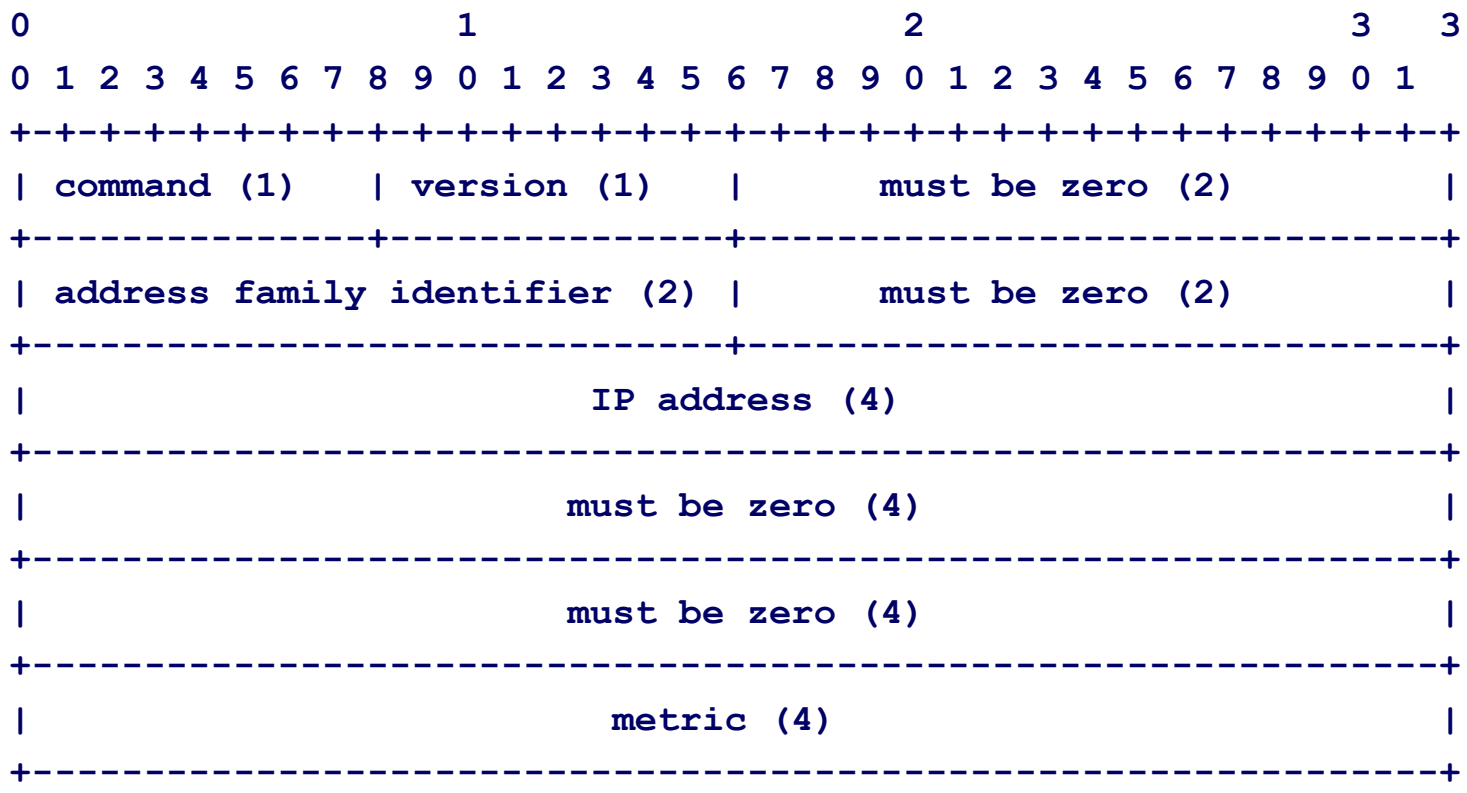
ICMP Router Discovery Protocol

- "Trust me, I'm a gateway" messages
  - No form of authentication
  - Enabled by default on DHCP clients running Microsoft
    - Windows 95, 98, 98 SE, 2000 machines
  - By spoofing IRDP Router Advertisements, an attacker can remotely add default route entries to a remote system
    - The default route entry added by the attacker will be preferred over the default route obtained from the DHCP server.
    - Windows 2000 is less vulnerable as it is impossible to give it a route that is preferred over the default route obtained via DHCP

Distance Vector Protocols

- Routers exchange distance information
- Routers keep the least expensive routes, and share that information
- Problems:
  - Trust and robustness issue:
    - pre-processed second-hand information is accepted
  - Distance-vector algorithms are not robust vs. unreliable (noisy) or malicious information.
- a.k.a. Routing by rumor
- Routers are advertising routes they are not directly connected to
- Slow convergence
- Does not scale well

RIP: Routing Information Protocol

- **RFC 1058 (version 1)**
- **UDP Port 520**
- 

Attacks on Distance-Vector Algorithms

- **Malicious router can:**
  - **Advertise 0-cost to some networks but do not forward**
    - **DoS for some routes**
- **Mallory can create fake messages with UDP spoofing**
  - **Create loops**
  - **Send all traffic to one router**
  - **Make counting to infinity (16) take infinity by resetting the count every so often...**
  - **Send messages saying that router A is unable to reach its own networks, to other routers...**

MIM Routing Attack

- Send a message to all gateways, saying the gateway to network A has made network A unreachable
- Send another message advertising that you can reach network A cheaply
  - You will start receiving all traffic for network A
- Forward the traffic to the original gateway, after doing whatever you want to do with it

FIRP Attack

- "Faulty Intermediate Router Problem"
- In distance vector algorithms, a node sends aggregated and processes information from other nodes, which subsequent nodes have to trust
- Router makes faulty calculations, by accident or on purpose
- How much a single FIRP can affect the routing?
  - Devastating to distance-vector algorithms

RIP V. 2

- RFC 2453
- Adds authentication via a shared password
  - 16 octets
  - plain text (can be sniffed)
- Weakest point of failure still brings down the protocol (black hole routing, FIRP problem)
- Access control recommended but not specified

BGP: Border Gateway Protocol

- Inter-Autonomous System routing protocol
- Uses TCP (or any reliable transport mechanism)
  - Port 179
- RFC 1771 (BGP-4)
  - Optional authentication field
    - Various authentication options
  - Authentication is only in the "OPEN" message
    - Connection can be hijacked afterwards
      - TCP session hijacking

BGP Connections

- **Once a connection to another BGP router has been established, it is expected to remain open and stable**
  - **If it closes:**
    - **All resources for that BGP connection are deallocated.**
    - **Routing table entries associated with the remote peer are marked as invalid.**
    - **The fact that the routes have become invalid is passed to other BGP peers before the routes are deleted from the system.**
- **TCP RST attacks can be very damaging!**
  - **Cause routing instabilities**
  - **Must use the TCP MD5 signature option (RFC 2385)**
    - **Or IPSEC, etc...**

BGP Limitations

- BGP (Border Gateway Protocol) has all the issues of Distance Vector algorithms
- New issues due to unsafe policies
  - Reference: "Policy Disputes in Path-Vector Protocols" Timothy G. Griffin, F. Bruce Shepherd, and Gordon Wilfong
- Works well in practice
  - Popular
- Quite vulnerable in theory

Link State Protocols

- Each router is responsible for meeting neighbors and learning their names
- Each router constructs a packet called a Link State Advertisement (LSA)
- List of neighbors
- Cost of link
- LSAs are reliably "flooded" to all routers; everyone gets the same consistent information, so there is no "counting to infinity" or memory.
- Each router computes the best routes on its own -- no need to trust your neighbor's calculations.

OSPF: Open Shortest Path First

- It's an authenticated link state protocol (RFC 2328) running directly on top of IP (proto 89) and using multicasts instead of broadcasts
  - Alternative to RIP
- Each node advertises only the information it knows first-hand (no hearsay)
- Every node calculates the paths independently, requiring matching information from both sides of a link to validate it! A single rogue router can't claim inexistent links.

"Fight Back" Phenomenon

- Because LSAs (Link State Advertisements) are flooded, an LSA produced by a malicious router is sent to all
- A router that knows better will respond and try to correct a tainted LSA
- Malicious router has to keep attacking: "persistent" attack is needed
- More costly to attacker, and less stealthy
- Better route integrity

Authentication in OSPF

- **Methods:**
  - **1. Password (plain text), vulnerable to sniffers**
  - **2. Keyed MD5 (a.k.a. HMAC-MD5)**
    - **K is a shared secret key (padded with zeros)**
    - **T is the message**
    - **H() is a hash function like MD5**
    - **F(K, T) is a function that pre-mixes T and K**
    - **Idea: Along with message, send also H(F(K,T)). Routers that know K can verify the integrity of T, as well as authenticate the message.**
    - **See RFC 1828**
    - **Similar to TCP MD5 signature option (RFC 2385)**

OSPF in IPSEC and IPv6

- No authentication at the OSPF level
- Uses IPSEC/IPv6 to provide security
- Does not protect against the faulty intermediate router problem (FIRP)
  - Intermediate router is man-in-the-middle
    - MIM protection judged too expensive
  - Must ultimately rely on intrusion detection

IGRP

- Interior Gateway Routing Protocol
  - also used externally in practice
- Cisco protocol (1980's)
- Distance vector algorithm
- Metric is weighted formula using internetwork delay, bandwidth, reliability, and load
- Has a "holddown" period for keeping bad routes down and increasing routing information consistency
  - Useful for route stability and against race conditions between routing updates

EIGRP

- Enhanced IGRP (1990's)
- Distance vector algorithm
- Uses "Diffusing Update Algorithm (DUAL)" to prevent loops
  - State machine
  - Timers
  - More complex

Secure communication channels

Dr. Drew Hamilton

IP Security Overview

- **IP Packets have no inherent security**
  - **Relatively easy to**
    - **forge contents of IP packets**
    - **modify contents of IP packets**
    - **inspect the contents of IP packets in transit**
- **Therefore, there is no guarantee that IP datagrams received:**
  - **are from the claimed sender (source address in the IP header)**
  - **contain the original data that the sender placed in them**
  - **were not inspected by a third party while the packet was being sent from source to destination**

IPSec is a means to limit the spoofing of routers

Virtual Private Networks

- A VPN is a way to simulate a private network over a public network, such as the Internet
  - "Virtual" because it depends on the use of virtual connections
  - temporary connections that have no real physical presence, but consist of packets routed over various machines on the Internet on an ad hoc basis
  - secure virtual connections are created between machines and networks as follows:
    - two machines
    - a machine and a network
    - two networks

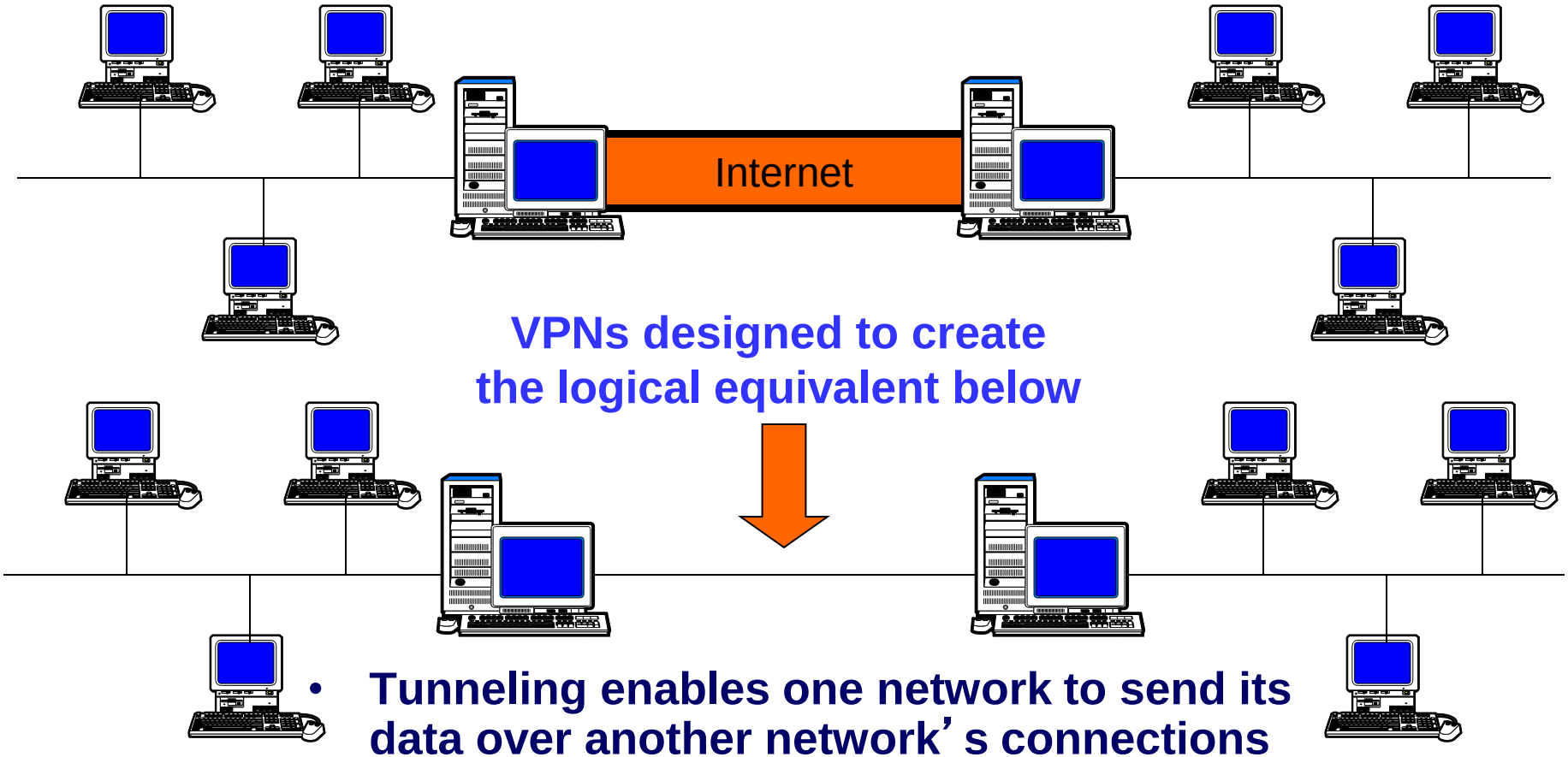
Origins of VPNs

- WANs
  - T1/T3
  - ATM
  - Frame Relay
  - ISDN
  - X.25
- Forerunner of VPNs was the idea of a virtual circuit
  - A virtual circuit creates a logical path from the source to the destination

Virtual Circuits

- In packet switched networks, the network makes dynamic decisions concerning the pathway each packet will take
- To improve reliability, a decision could be made prior to any data being sent
  - In this manner, a single static path could be set up between two communicating parties and used exclusively between them
  - This pathway is known as a virtual circuit
- When creating a virtual circuit, sender and receiver agree on which path will be used and on packet size.
  - During communications, acknowledgements are sent, including flow control info and error control info

Tunneling



- Tunneling enables one network to send its data over another network's connections
- Tunneling creates circuit-like connections across the packet-oriented Internet

VPNs versus long haul connections

- **Long Haul connections**
  - **leased line**
  - **frame relay network**
  - **ISDN**
  - **.....**
- **For two remote offices, much cheaper to each get an ISP POP (point of presence)**
  - **Then deploy an VPN between the two routers at the two offices over the Internet**

How VPNs Solve Internet Security Issues

- **Firewalls**
  - **discussed next lecture**
- **authentication**
  - **multiple means including IPSec**
  - **Challenge Handshaking Authentication Protocol (CHAP)**
  - **RSA**
- **encryption**
  - **multiple means including IPSec**
  - **private key encryption**
  - **public key encryption**

IP Spoofing

- An attacker compromises the routing packets to redirect a file or transmission to a different destination
  - most routing information is not encrypted
    - easy to modify source data or change destination
  - also used to mask attacker's identity
- Best solutions
  - screen packets at router and firewall, reject any that appear to come from an internal address
  - encryption to safeguard the payloads of the packets
  - authentication to verify sender

IPSec

- IPSec is a method of protecting IP datagrams.
- This protection takes the form of
  - data origin authentication
  - connectionless data integrity authentication
  - data content confidentiality
  - anti-replay protection
  - limited traffic flow confidentiality
- Protection via Encapsulating Security Payload (ESP) or Authentication Header (AH)
  - Ultimate security dependent upon the cryptographic algorithm applied
  - Symmetric key cryptography used – why?

What is Tunneling?

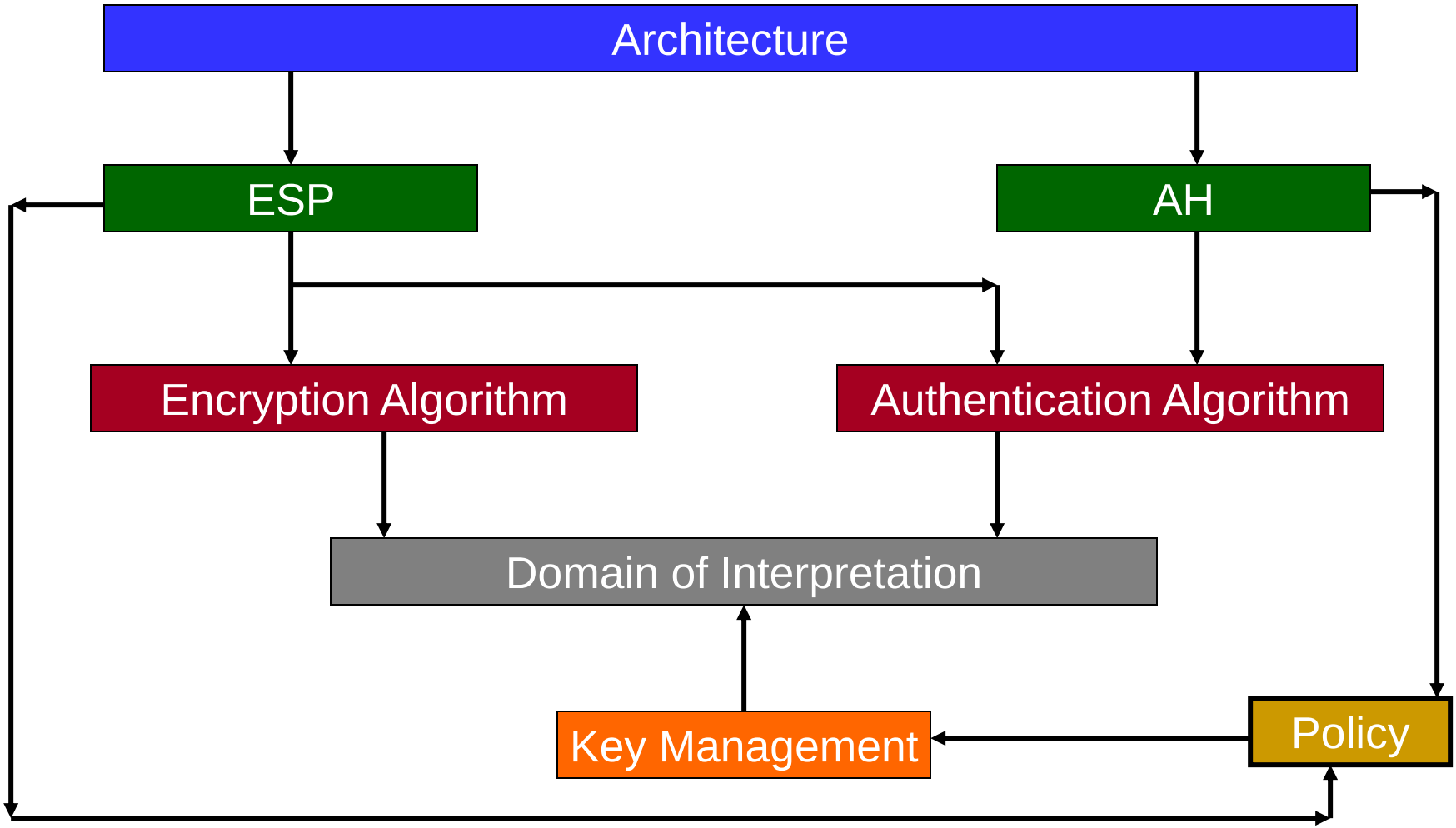
- Tunneling encloses one type of data packet into the packet of another protocol
  - Protocol of the encapsulating packet is understood by the network and by the network entry and exit points
- Before encapsulation takes place, packets are encrypted so that the payloads are unreadable during transit
- Tunneling involves three different protocols
  - Carrier protocol – used by the network that the information is traveling over – usually TCP/IP
  - Encapsulation protocol – protocol that the original data is packaged in such as GRE, IPSec, L2F, PPTP or L2TP
  - Passenger protocol – original or native data that is being carried from the network where the originating host resides such as IPX, AppleTalk, IP

Tunneling Protocols

- **Layer 2 tunneling protocols**
  - **Layer 2 protocols correspond to the Data Link layer and use frames as their unit of exchange. PPTP, L2TP and L2F are Layer 2 tunneling protocols. These protocols encapsulate the data in a Point-to-point Protocol (PPP) frame to send across an internetwork***

    ***an internet with a lower case i, is any collection of networks that are networked or connected together over a common infrastructure.**
- **Layer 3 tunneling protocols**
  - **Layer 3 protocols correspond to the network layer and use packets. IP over IP and IPSec Tunnel Mode are examples of Layer 3 tunneling protocols. These protocols encapsulate IP packets in an additional IP header before sending them across an IP internetwork.**

IPSec Overview



IPSec Roadmap, Doraswamy and Harkins

IPSec Architecture Revisited

- Defined by RFC 2401
- Mandatory in IPv6
- Internet Key Exchange (IKE)
  - Symmetric key cryptography is used for efficiency
  - To exchange keys securely, a negotiation protocol is used that allows users to agree on authentication methods, encryption methods and the keys to use.
  - It also specifies how long keys can be used before changing and how to accomplish key exchange
- The IPSec protocols, AH and ESP can be used to protect an entire IP payload or the upper layer protocols of an IP payload.
  - AH used for authentication
  - ESP used for encryption
- Two different modes of IPSec
  - Transport mode to protect upper-layer protocols
  - Tunnel mode to protect entire IP datagrams

Internet Key Exchange (IKE)

- **Compliant IKEs require adherence to three documents**
  - **ISAKMP specification (RFC 2408) (Internet Security Association and Key Management Protocol)**
  - **Domain of Interpretation for (DOI) for for IPSec (RFC 2407)**
  - **IKE specification (RFC 2409)**
- **Security Associations (SAs) are used with IPSec to define the processing done on a specific IP packet.**
- **IKEs establish shared security parameters and authenticated keys – SAs- between IPSec peers**
- **IKE is a generic protocol with application beyond IPSec**
  - **ex. RIPv2 or OSPF**

Transforms

- Transformation applied to the data to secure it.
  - includes algorithm, key sizes, derivations
  - specific information required in order for different implementations to interoperate
- IKE – Internet Key Exchange
  - establishes shared security parameters and authenticated keys
    - i.e. security associations (SAs) between IPSec peers
  - Actual negotiated parameters come up in the Domain of Interpretation (DOI)
- Policy
  - Necessary but not sufficient for interoperability
  - Determines transforms, representations and implementation

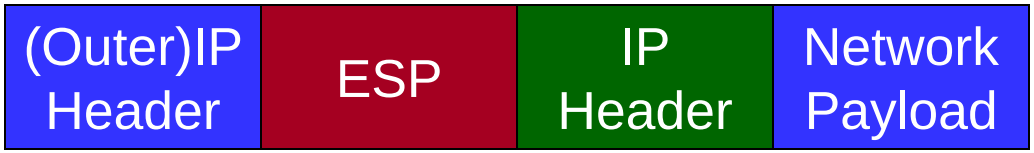
Overview of ISAKMP

- AH Transform Identifiers
  - AH_MD5
  - AH_SHA
  - AH_DES
  - AH_SHA2-256 (256 bit message digest)
  - AH_SHA2-384
  - AH_SHA2-512
  - AH_RIPEMD
- Certificate Types
  - PGP certificates
  - DNS signed key
  - x.509 cert – signature
  - x.509 cert – key exchange
  - Kerberos tokens
  - CRL (Cert Revocation List)
  - ARL (Auth Revocation List)
  - SPKI cewrt
  - x.509 cert - Attribute
- ESP Transform Identifiers
  - ESP_DES_IV64 (DES in CBC mode with a 64 bit IV)
  - ESP_DES (DES in CBC mode)
  - ESP_3DES
  - ESP_RC5
  - ESP_IDEA
  - ESP_CAST
  - ESP_Blowfish
  - ESP_3IDEA
  - ESP_DES_IV32 (DES in CBC mode with a 32-bit IV)
  - ESP_RC4
  - ESP_NULL (NONE)
  - ESP_AES

Security Associations

- SAs form the basis for IPSec
  - contract between two communicating entities
  - determine the protocols used for securing packets
- SAs are one-way, i.e. simplex
  - If two hosts are communicating, host A will have an SAout and an SAin
- SAs are protocol specific
  - Each host builds a separate SA for AH and ESP
- Security policy database
  - Works in conjunction with the security association database
- Security Parameter Index
  - 32-bit entity that is used to uniquely identify an SA at the receiver
  - SPI passed to AH and ESP headers using a tuple <spi,dst,protocol>

IPSec in Tunnel Mode

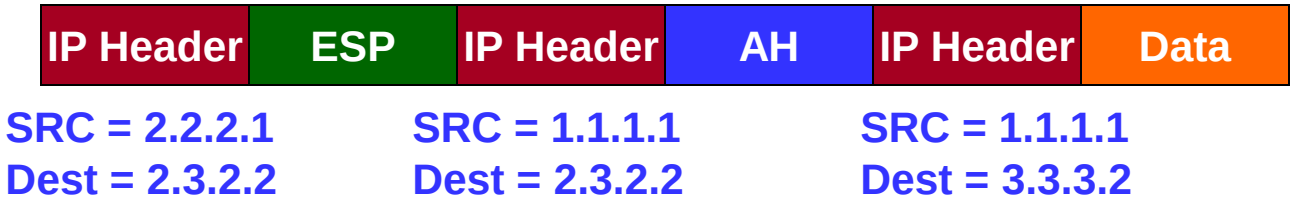


IPSec tunneled mode packet format

- **An IPSec tunnel mode packet has two headers – inner and outer**
  - **Inner header constructed by the host**
  - **Outer header is added by the device providing security services**

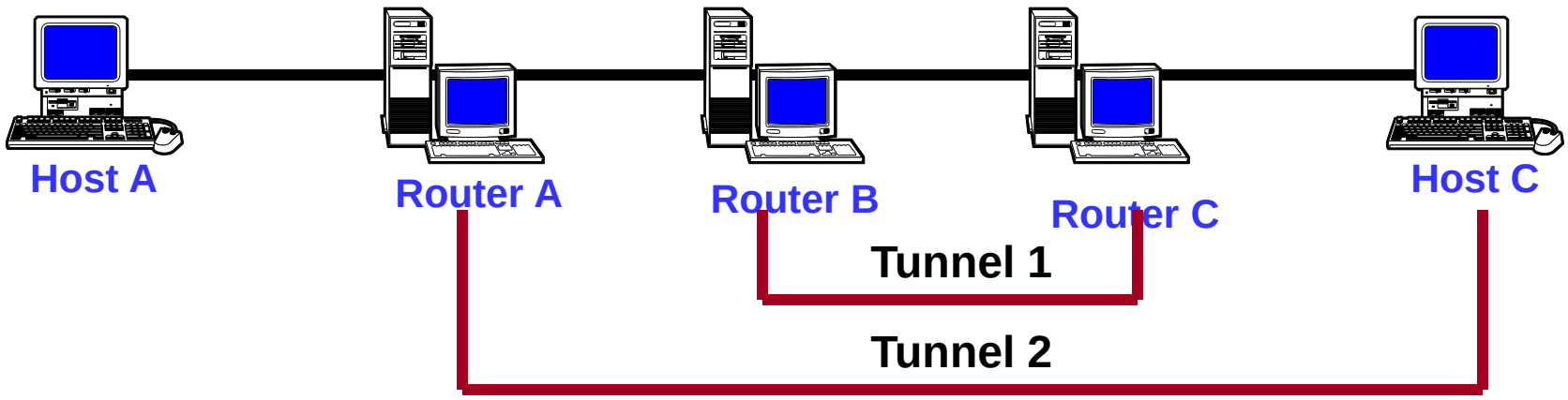
Nested Tunnels

Nested Packet Format

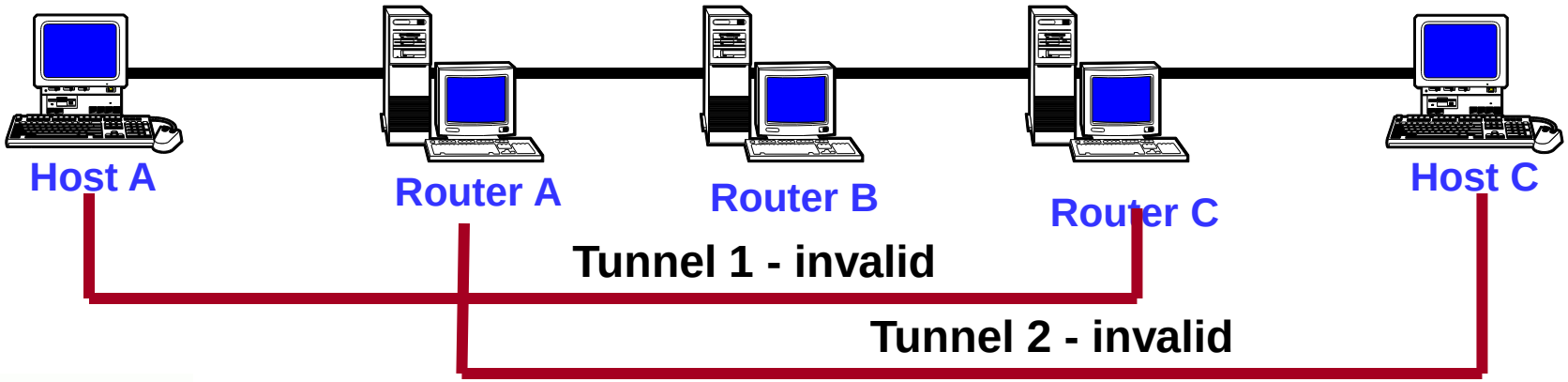


- IPSec defines tunnel mode for both ESP and AH
- In the nested tunnel example above, host A is sending a packet to host B.
  - Policy requires authentication to router B
  - VPN between the two networks bounded by router A and router B

Valid and Invalid Nested Tunnels

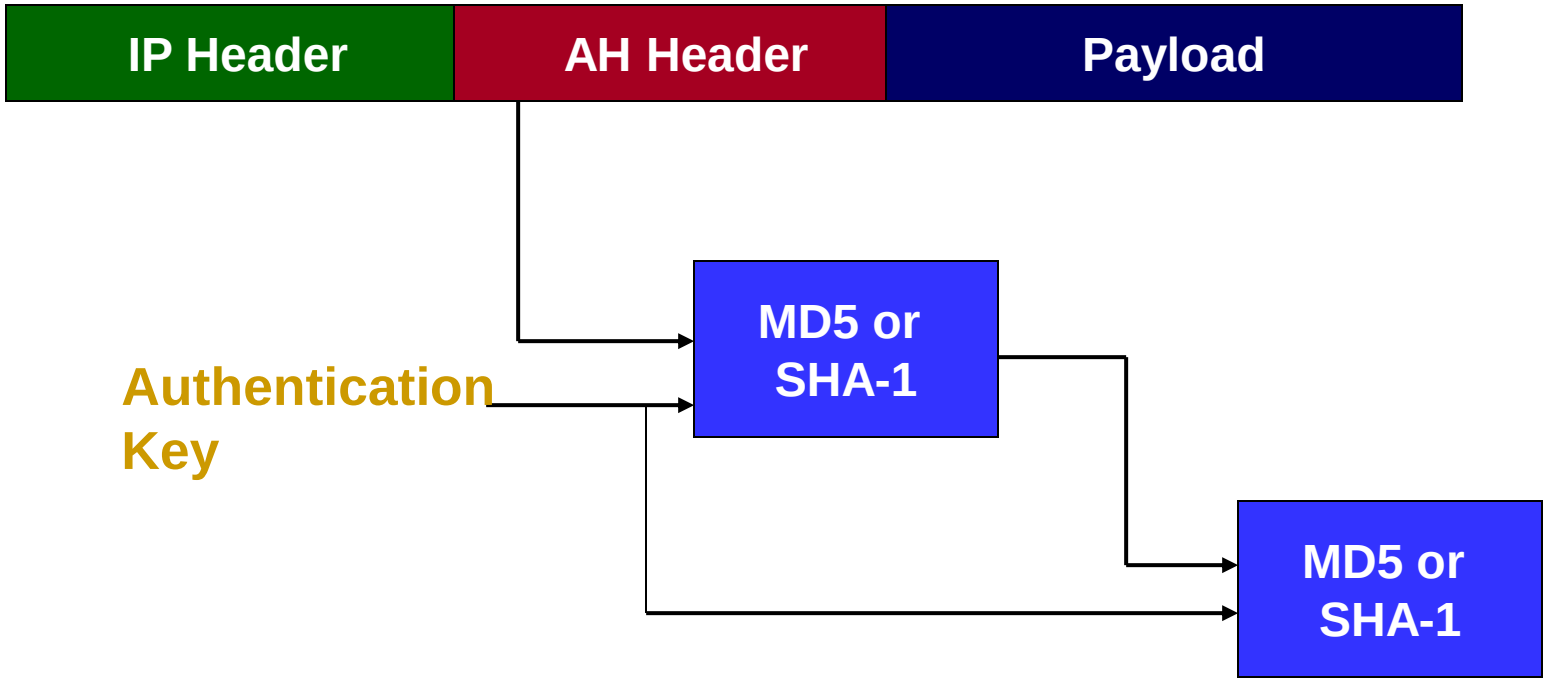


- **The requirement for the tunnel is that the inner header must be completely encompassed by the outer header.**



Authentication Header

1st 96 bits of second hash becomes Integrity Check Value (ICV)

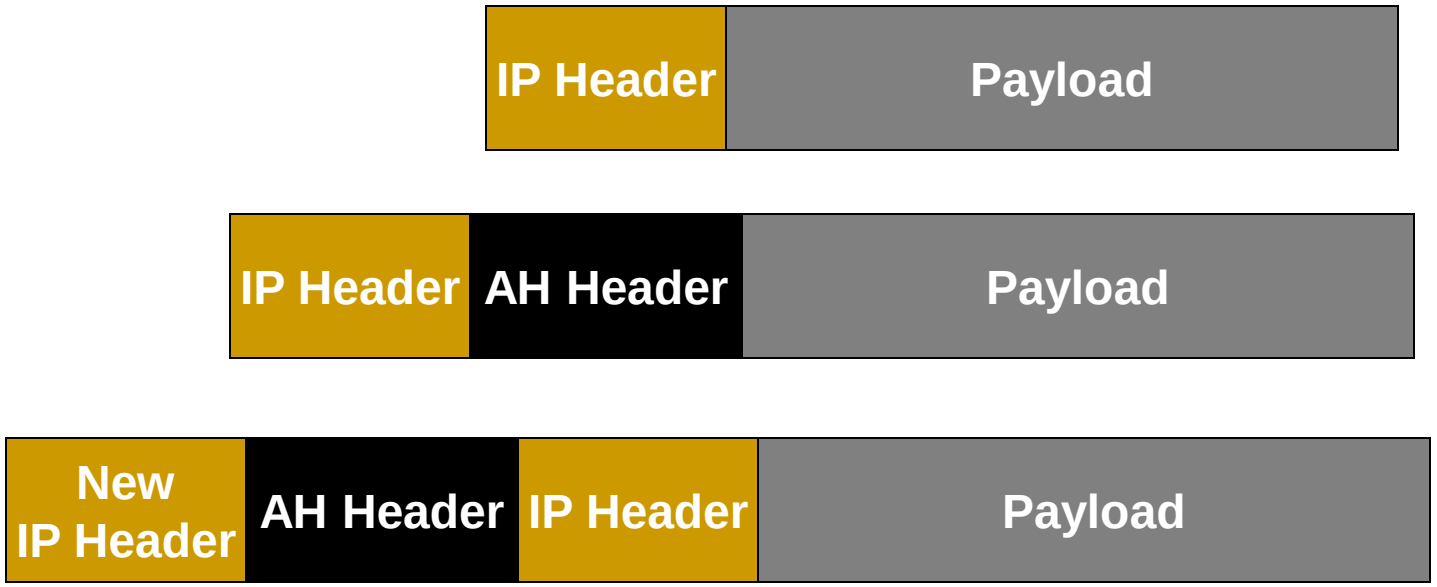


- 96 bits is selected to maintain compatibility with original IPSec spec
- Replay protection is provided by using the Sequence Number field within the AH header whose value is covered by the authentication procedure

Mutable IPv4 fields that cannot be protected by AH

- Mutable IPv4 fields that cannot be protected by AH
  - Type of Service (TOS)
  - Flags
  - Fragment Offset
  - Time to Live (TTL)
  - Header Checksum
- When protection of these fields is required, tunneling should be used
- Payloads of an IP packet are considered immutable and therefore always protected by AH
- An IP packet with AH applied can be fragmented **but** AH cannot be applied to a fragmented packet

AH Transport and Tunnel Modes



- In transport mode, the original datagram's IP header is the outermost IP header
- In tunnel mode, a new IP header is generated for use as the outer IP header of the resulting datagram
  - Source and destination address of the new header will generally differ – i.e. the destination address of the new IP header may be a corporate firewall.

Encapsulating Security Payload (ESP)

- ESP adds approximately 24 bytes per packet
- For interoperability purposes, mandatory to implement algorithms has been defined for ESP
  - The must-implemented cipher is DES-CBC with an explicit IV (RFC 2405)
  - The must-implement authenticators are HMAC-MD5-96 and HMAC-SHA-96 (RFCs 2403 AND 2404)
- Published prior to development of “deep crack”
- RFCs updated to indicate deprecated nature of DES and suggesting stronger cipher algorithms

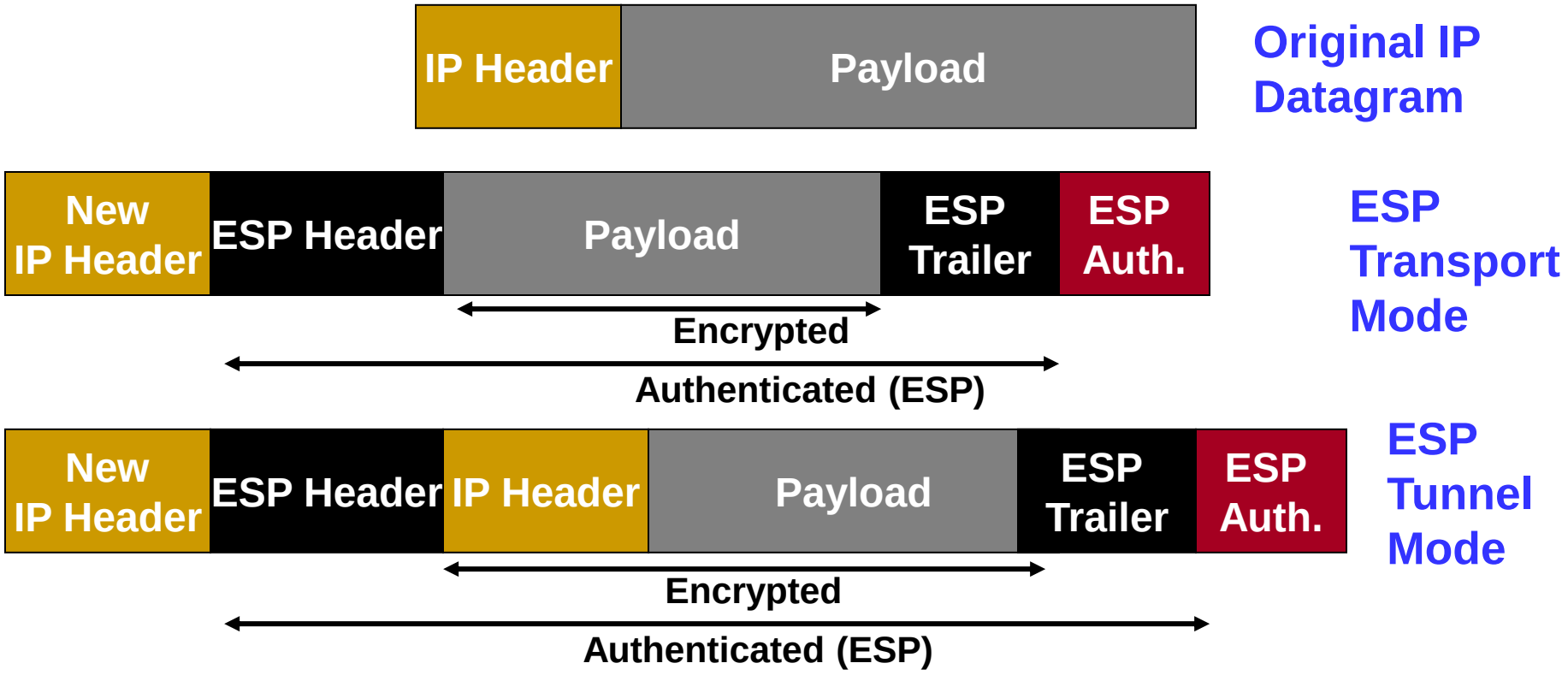
Outbound ESP Processing

- Insert header (similar for both IPv4 and IPv6)
- Encrypt packet from beginning of the payload to the next header field in the trailer using appropriate cipher specified in the SA (policy check)
- Authenticate packet from ESP header through the ciphertext to the ESP trailer.
  - Insert result in the authentication data field of the ESP trailer
- Recompute checksum of the IP header that precedes the ESP header

Inbound ESP Processing

- SA determines what the incoming packet **should** be.
  - No way to tell until packet is decrypted
  - Makes unauthorized traffic analysis harder
  - If no valid SA exists – drop the packet
- Next, authenticate by checking the message digest
  - pass appropriate key to authentication algorithm from the SA
- Decrypt the packet -- from the beginning of the payload data to the next header field
  - decrypted using the key and cipher algorithm from the SA
  - check decryption by checking the padding
    - padding is completely deterministic
    - verifies whether packet was successfully decrypted.

ESP Transport and Tunnel Modes



- ESP in transport mode provides neither authentication nor encryption for the IP header.
- In tunnel mode, the new IP header is not encrypted – everything else is

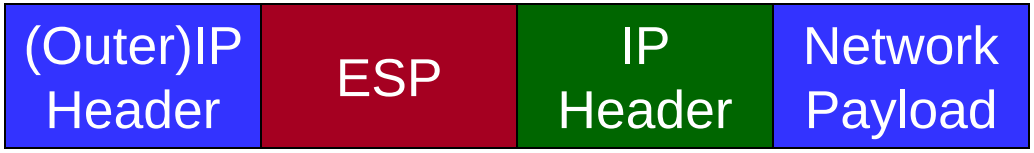
Transport Mode

- **AH and ESP intercept the packets moving from the transport layer into the network layer.**
  - **When security is NOT enabled, TCP and UDP flow into IP which adds an IP header**
  - **When security is enabled, TCP / UDP flow into the IPSec component**
  - **When both AH and ESP are used, ESP is applied first – why?**

Packet format with AH and ESP

Tunnel Mode

- **IPSec in Tunnel mode is normally used when the ultimate destination of the packet is different from the security termination point.**
  - **ex. security termination point may be a router rather than a host.**
  - **also used when a router provides security services for packets it is forwarding**
  - **In the case of tunnel mode, IPSec encapsulates an IP packet with IPSec headers and adds an outer IP header**



IPSec tunneled mode packet format

Conclusion: IPSec Implementation

- Can be implemented in end hosts, gateways / routers or both
- Advantages of OS-level integration
  - Efficiency: IPSec can use network services in the OS such as user context (sockets)
  - Ease of Implementation: Network connections, HTTP connections – all can be configured from the host
  - All IPSec modes are supported
- BUMP-in-the-Stack (BITS) network level integration
  - Supports multiple OSs
  - Duplicated functionality causing unnecessary complications
  - Allows firewall vendors to integrate with their products

Network attacks

Debabrata Dash

Outline

- Security Vulnerabilities
- DoS and D-DoS
- Firewalls
- Intrusion Detection Systems

Security Vulnerabilities

- **Security Problems in the TCP/IP Protocol Suite – Steve Bellovin - 89**
- **Attacks on Different Layers**
  - **IP Attacks**
  - **ICMP Attacks**
  - **Routing Attacks**
  - **TCP Attacks**
  - **Application Layer Attacks**

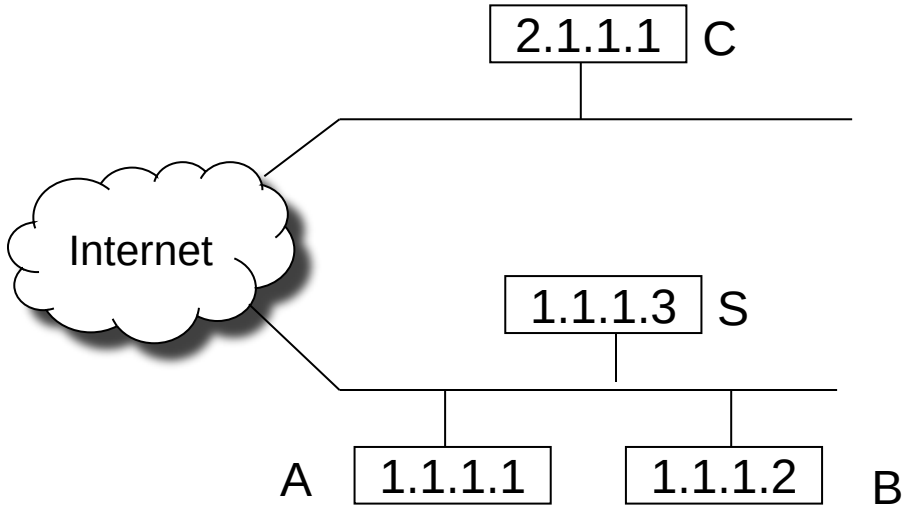
Why?

- TCP/IP was designed for connectivity
  - Assumed to have lots of trust

- Host implementation vulnerabilities
  - Software "had/have/will have" bugs
  - Some elements in the specification were left to the implementers

Security Flaws in IP

- **The IP addresses are filled in by the originating host**
  - **Address spoofing**
- **Using source address for authentication**
  - **r-utilities (rlogin, rsh, rhosts etc..)**



•Can A claim it is B to the server S?

•ARP Spoofing

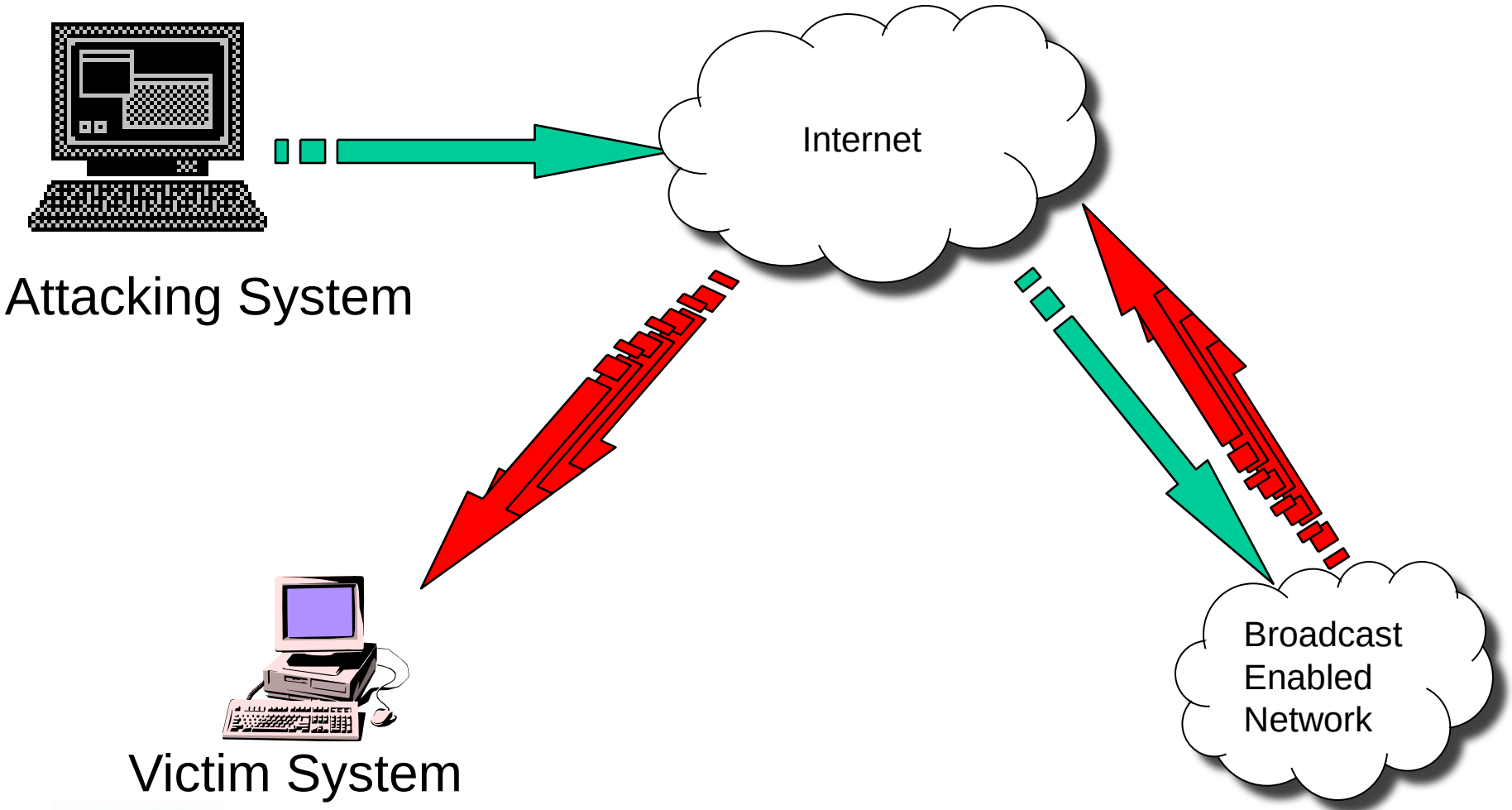
•Can C claim it is B to the server S?

•Source Routing

Security Flaws in IP

- IP fragmentation attack
  - End hosts need to keep the fragments until all the fragments arrive
- Traffic amplification attack
  - IP allows broadcast destination
  - Problems?

Ping Flood


Internet
Attacking System
Victim System
Broadcast
Enabled
Network

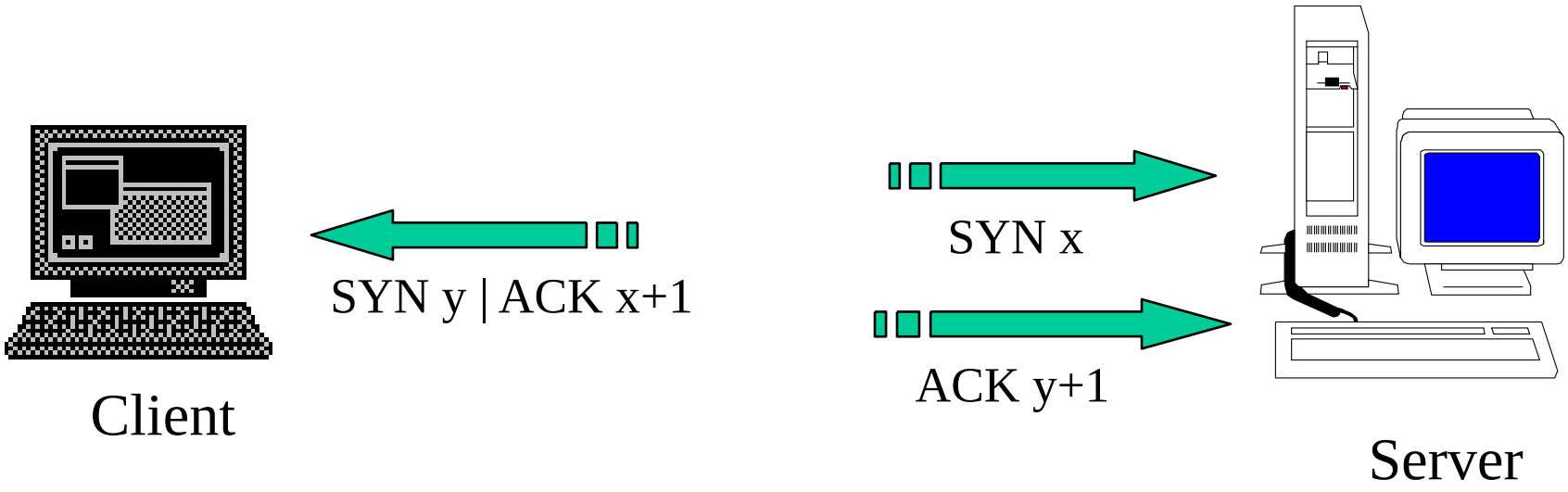
ICMP Attacks

- No authentication
- ICMP redirect message
  - Can cause the host to switch gateways
  - Benefit of doing this?
    - Man in the middle attack, sniffing
- ICMP destination unreachable
  - Can cause the host to drop connection
- ICMP echo request/reply
- Many more…
  - http://www.sans.org/rr/whitepapers/threats/477.php

Routing Attacks

- Distance Vector Routing
  - Announce 0 distance to all other nodes
    - Blackhole traffic
    - Eavesdrop
- Link State Routing
  - Can drop links randomly
  - Can claim direct link to any other routers
  - A bit harder to attack than DV
- BGP
  - ASes can announce arbitrary prefix
  - ASes can alter path

TCP Attacks



Issues?

- Server needs to keep waiting for ACK y+1
- Server recognizes Client based on IP address/port and y+1

TCP Layer Attacks

- **TCP SYN Flooding**
  - **Exploit state allocated at server after initial SYN packet**
  - **Send a SYN and don't reply with ACK**
  - **Server will wait for 511 seconds for ACK**
  - **Finite queue size for incomplete connections (1024)**
  - **Once the queue is full it doesn't accept requests**

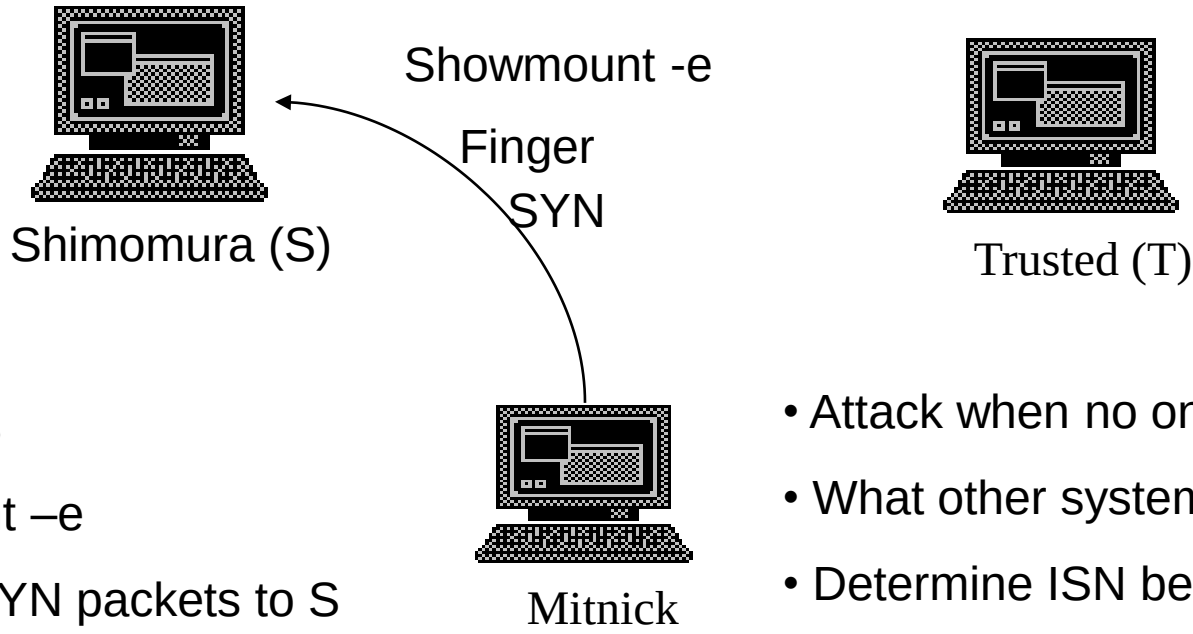
TCP Layer Attacks

- **TCP Session Hijack**
  - **When is a TCP packet valid?**
    - **Address/Port/Sequence Number in window**
  - **How to get sequence number?**
    - **Sniff traffic**
    - **Guess it**
      - **Many earlier systems had predictable ISN**
  - **Inject arbitrary data to the connection**
- **TCP Session Poisoning**
  - **Send RST packet**
    - **Will tear down connection**
  - **Do you have to guess the exact sequence number?**
    - **Anywhere in window is fine**
    - **For 64k window it takes 64k packets to reset**
    - **About 15 seconds for a T1**

Application Layer Attacks

- Applications don't authenticate properly
- Authentication information in clear
  - FTP, Telnet, POP
- DNS insecurity
  - DNS poisoning
  - DNS zone transfer

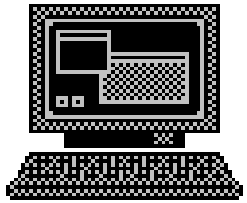
An Example



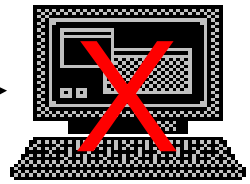
- Finger @S
- showmount –e
- Send 20 SYN packets to S

- Attack when no one is around
- What other systems it trusts?
- Determine ISN behavior

An Example

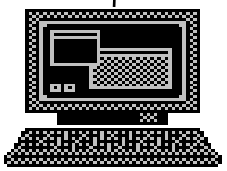


Shimomura (S)



Trusted(T)

Syn flood

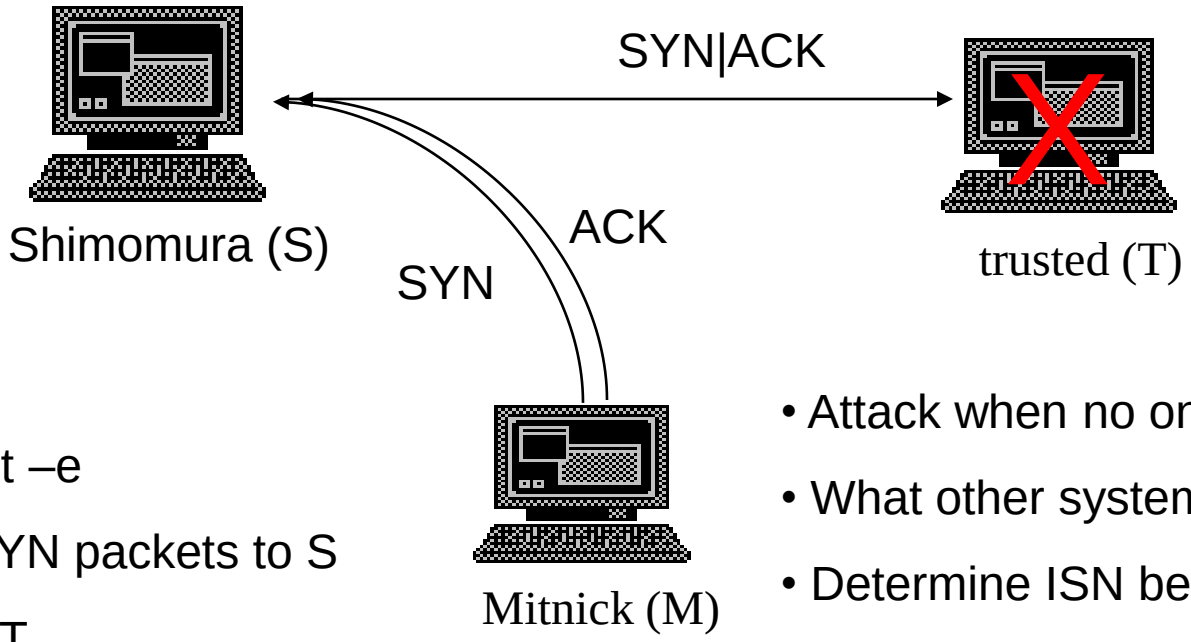


Mitnick

- Finger @S
- showmount –e
- Send 20 SYN packets to S
- SYN flood T

- Attack when no one is around
- What other systems it trusts?
- Determine ISN behavior
- T won't respond to packets

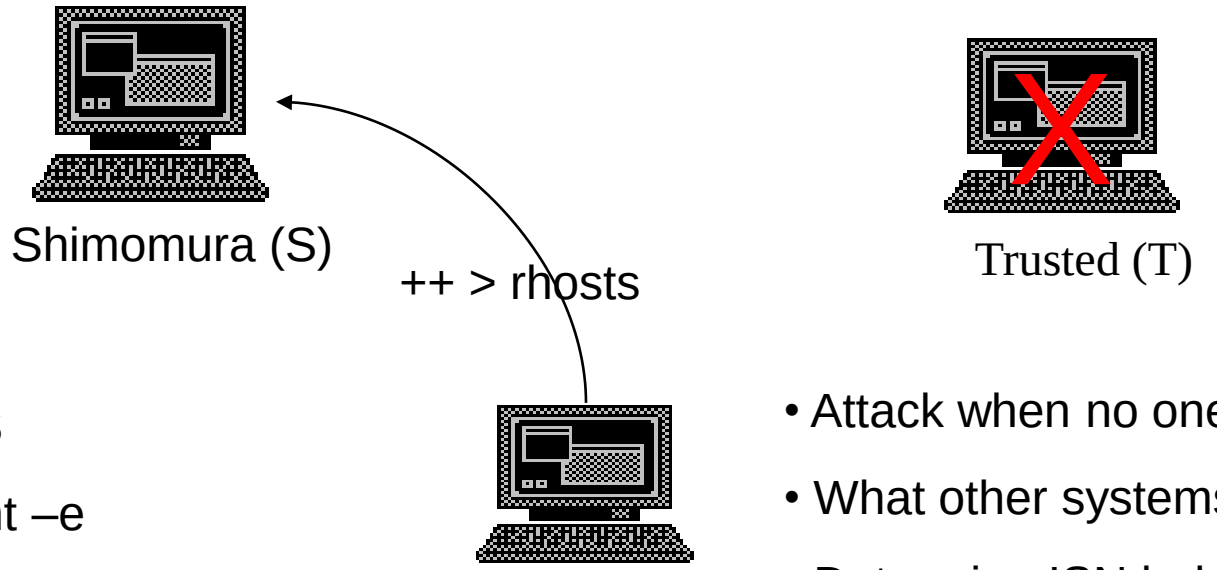
An Example



- Finger @S
- showmount –e
- Send 20 SYN packets to S
- SYN flood T
- Send SYN to S spoofing as T
- Send ACK to S with a guessed number

- Attack when no one is around
- What other systems it trusts?
- Determine ISN behavior
- T won't respond to packets
- S assumes that it has a session with T

An Example



- Finger @S
- showmount –e
- Send 20 SYN packets to S
- SYN flood T
- Send SYN to S spoofing as T
- Send ACK to S with a guessed number
- Send "echo + + > ~/.rhosts"

- Attack when no one is around
- What other systems it trusts?
- Determine ISN behavior
- T won't respond to packets
- S assumes that it has a session with T
- Give permission to anyone from anywhere

Denial of Service

- **Objective → make a service unusable, usually by overloading the server or network**

- **Consume host resources**
  - **TCP SYN floods**
  - **ICMP ECHO (ping) floods**

- **Consume bandwidth**
  - **UDP floods**
  - **ICMP floods**

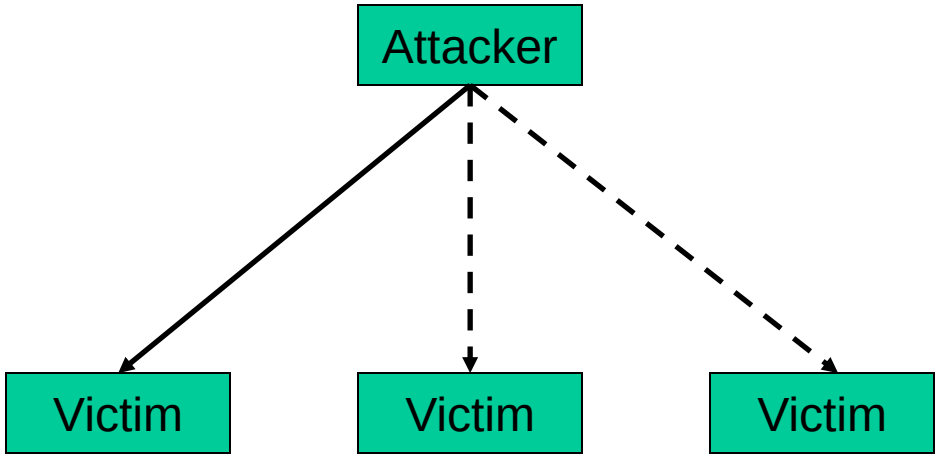
Denial of Service

- **Crashing the victim**
  - **Ping-of-Death**
  - **TCP options (unused, or used incorrectly)**
- **Forcing more computation**
  - **Taking long path in processing of packets**

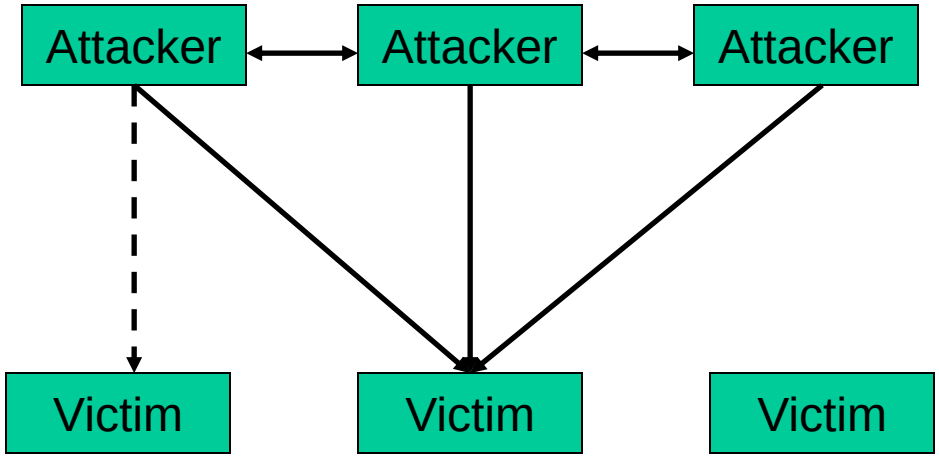
Simple DoS

The Attacker usually spoofed source address to hide origin

Easy to block

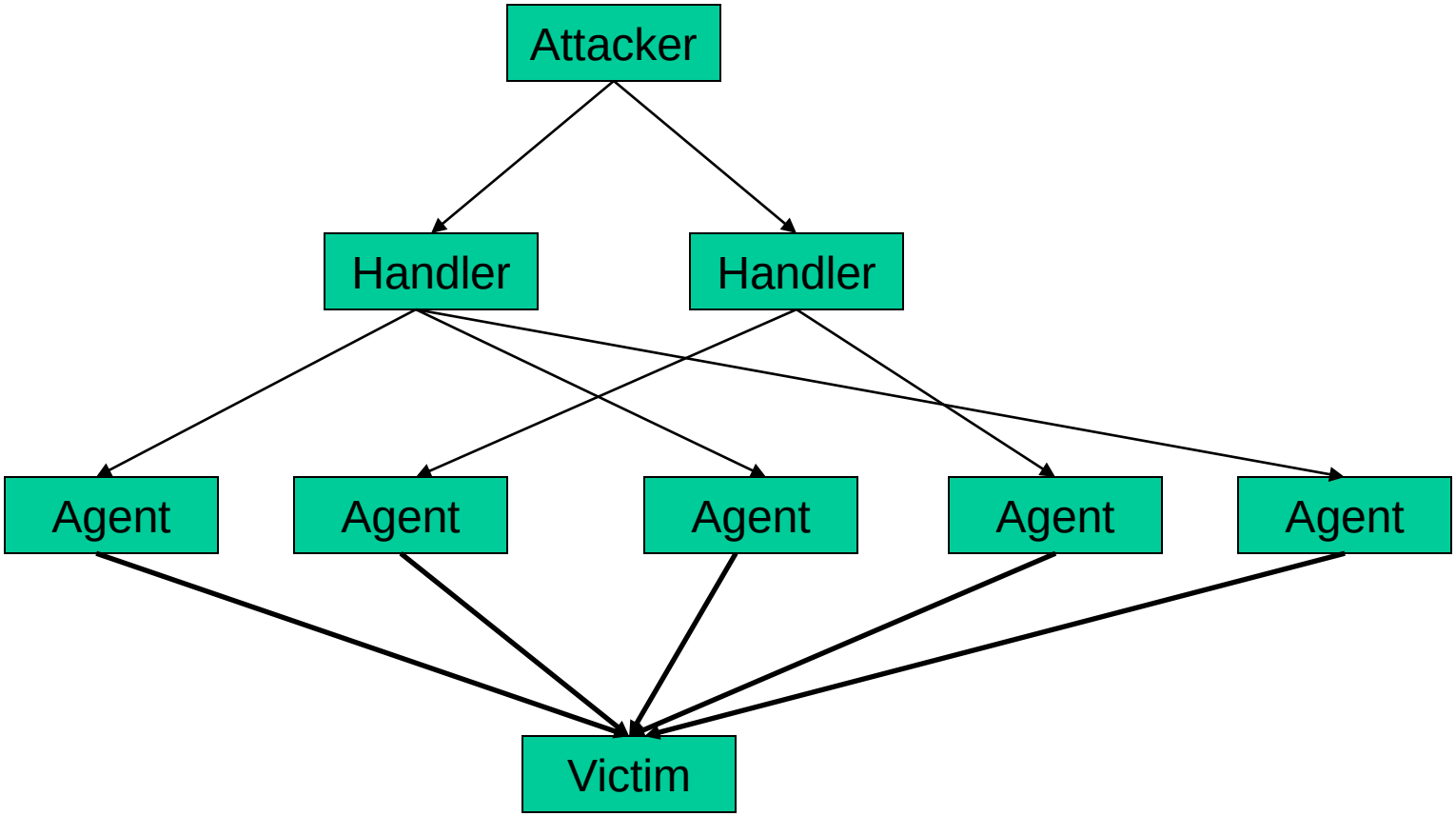


Coordinated DoS



- The first attacker attacks a different victim to cover up the real attack
- The Attacker usually spoofed source address to hide origin
- Harder to deal with

Distributed DoS



Distributed DoS

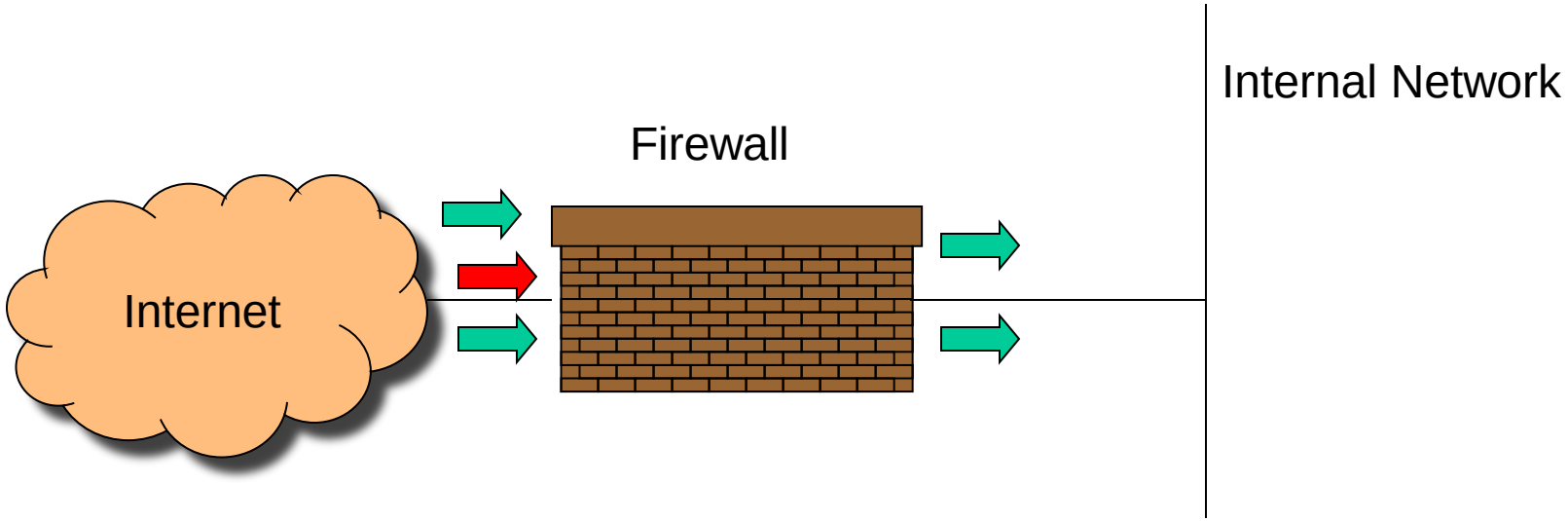
- The handlers are usually very high volume servers
  - Easy to hide the attack packets
- The agents are usually home users with DSL/Cable
  - Already infected and the agent installed
- Very difficult to track down the attacker
- How to differentiate between DDoS and Flash Crowd?
  - Flash Crowd → Many clients using a service legitimately
    - Slashdot Effect
    - NBA Finals Stream
  - Generally the flash crowd disappears when the network is flooded
  - Sources in flash crowd are clustered

Firewalls

- Lots of vulnerabilities on hosts in network
- Users don't keep systems up to date
  - Lots of patches
  - Lots of exploits in wild (no patch for them)
- Solution?
  - Limit access to the network
  - Put firewalls across the perimeter of the network

Firewalls (contd…)

- Firewall inspects traffic through it
- Allows traffic specified in the policy
- Drops everything else
- Two Types
  - Packet Filters, Proxies



Packet Filters

- Packet filter selectively passes packets from one network interface to another
- Usually done within a router between external and internal networks
  - screening router
- Can be done by a dedicated network element
  - packet filtering bridge
  - harder to detect and attack than screening routers

Packet Filters Contd.

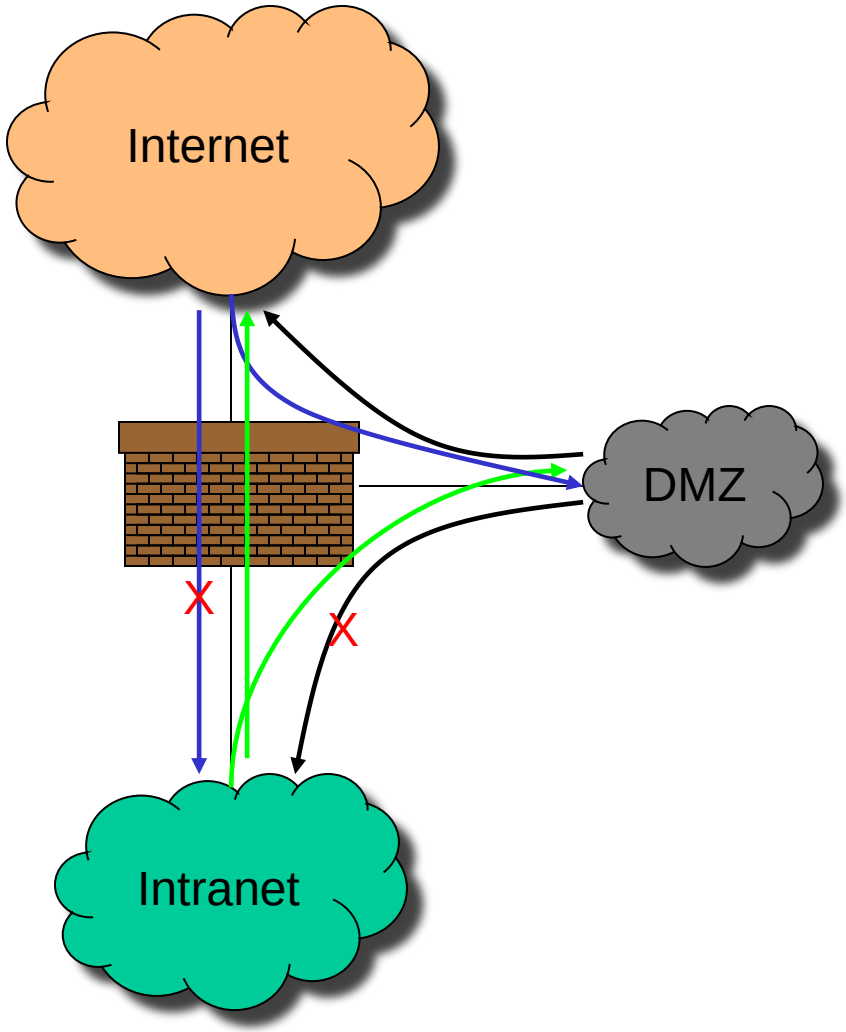
- **Data Available**
  - IP source and destination addresses
  - Transport protocol (TCP, UDP, or ICMP)
  - TCP/UDP source and destination ports
  - ICMP message type
  - Packet options (Fragment Size etc.)
- **Actions Available**
  - Allow the packet to go through
  - Drop the packet (Notify Sender/Drop Silently)
  - Alter the packet (NAT?)
  - Log information about the packet

Packet Filters Contd.

- **Example filters**
  - **Block all packets from outside except for SMTP servers**
  - **Block all traffic to a list of domains**
  - **Block all connections from a specified domain**

Typical Firewall Configuration

- Internal hosts can access DMZ and Internet
- External hosts can access DMZ only, not Intranet
- DMZ hosts can access Internet only
- Advantages?
  - If a service gets compromised in DMZ it cannot affect internal hosts

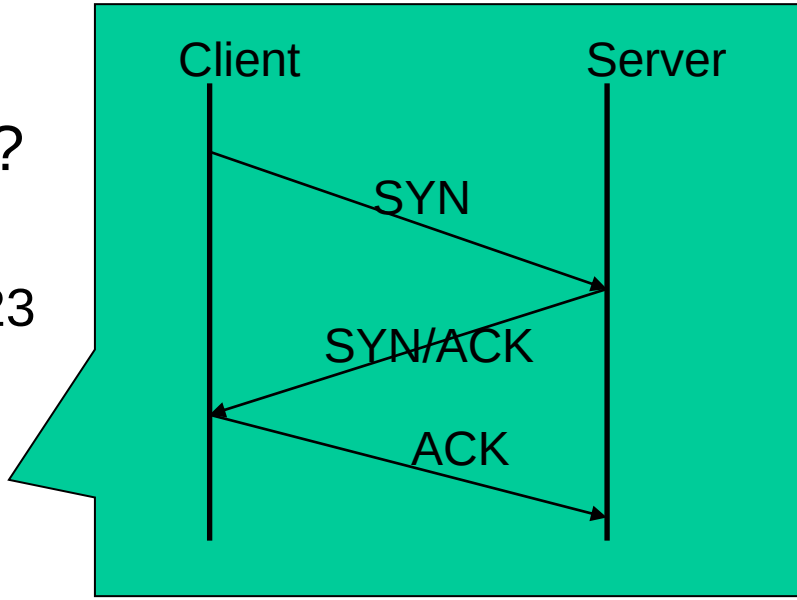


Example Firewall Rules

- Stateless packet filtering firewall
- Rule → (Condition, Action)
- Rules are processed in top-down order
  - If a condition satisfied – action is taken

Sample Firewall Rule

- Allow SSH from external hosts to internal hosts
  - Two rules
    - Inbound and outbound
  - How to know a packet is for SSH?
    - Inbound: src-port>1023, dst-port=22
    - Outbound: src-port=22, dst-port>1023
    - Protocol=TCP



Rule	Dir	Src Addr	Src Port	Dst Addr	Dst Port	Proto	Ack Set?	Action
SSH-1	In	Ext	> 1023	Int	22	TCP	Any	Allow
SSH-2	Out	Int	22	Ext	> 1023	TCP	Yes	Alow

Default Firewall Rules

- **Egress Filtering**
  - **Outbound traffic from external address → Drop**
  - **Benefits?**
- **Ingress Filtering**
  - **Inbound Traffic from internal address → Drop**
  - **Benefits?**
- **Default Deny**
  - **Why?**

Rule	Dir	Src Addr	Src Port	Dst Addr	Dst Port	Proto	Ack Set?	Action
Egress	Out	Ext	Any	Ext	Any	Any	Any	Deny
Ingress	In	Int	Any	Int	Any	Any	Any	Deny
Default	Any	Any	Any	Any	Any	Any	Any	Deny

Packet Filters

- **Advantages**
  - **Transparent to application/user**
  - **Simple packet filters can be efficient**
- **Disadvantages**
  - **Very hard to configure the rules**
  - **Doesn't have enough information to take actions**
    - **Who is the user accessing the SSH?**

Alternatives

- **Stateful packet filters**
  - **Keep the connection states**
  - **Easier to specify rules**
  - **More popular**
  - **Problems?**
    - **State explosion**
    - **State for UDP/ICMP?**

Alternatives

- **Proxy Firewalls**
  - **Two connections instead of one**
  - **Either at transport level**
    - **SOCKS proxy**
  - **Or at application level**
    - **HTTP proxy**
- **Requires applications (or dynamically linked libraries) to be modified to use the proxy**

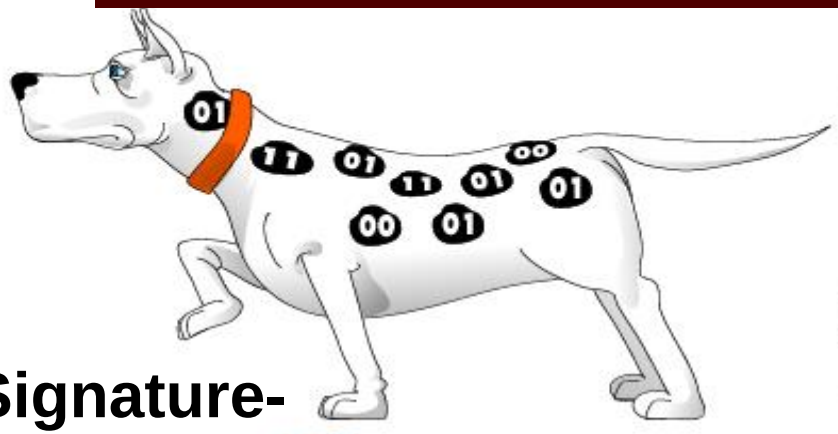
Proxy Firewall

- **Data Available**
  - **Application level information**
  - **User information**
- **Advantages?**
  - **Better policy enforcement**
  - **Better logging**
- **Disadvantages?**
  - **One proxy for each application**

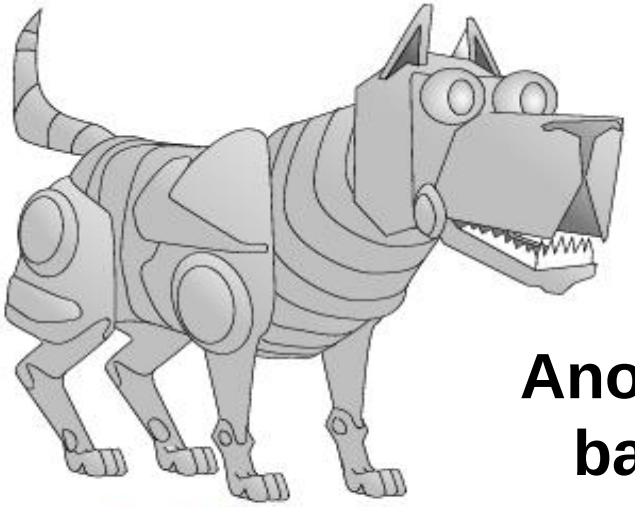
Intrusion Detection Systems

- Firewalls allow traffic only to legitimate hosts and services
- Traffic to the legitimate hosts/services can have attacks
- Solution?
  - Intrusion Detection Systems
  - Monitor data and behavior
  - Report when identify attacks

Types of IDS



Signature-based



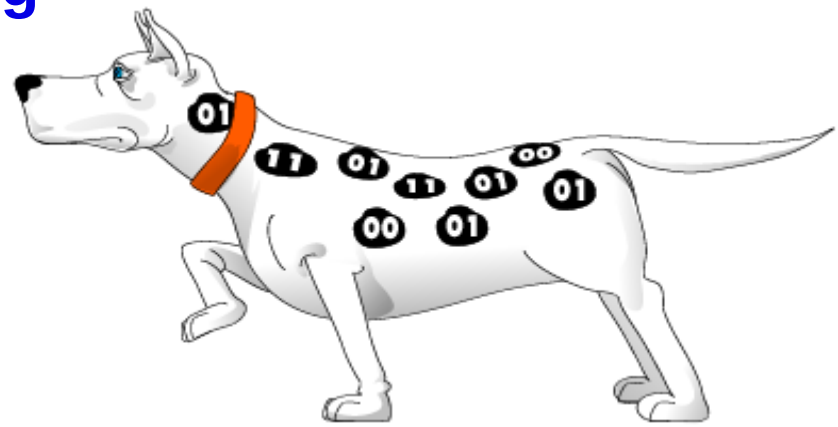
Anomaly-based

Host-based

Network-based

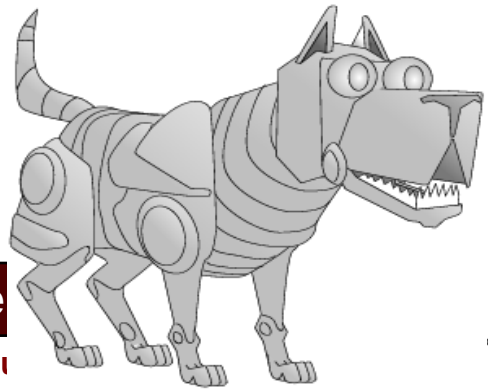
Signature-based IDS

- **Characteristics**
  - **Uses known pattern matching to signify attack**
- **Advantages?**
  - **Widely available**
  - **Fairly fast**
  - **Easy to implement**
  - **Easy to update**
- **Disadvantages?**
  - **Cannot detect attacks for which it has no signature**



Anomaly-based IDS

- **Characteristics**
  - Uses statistical model or machine learning engine to characterize normal usage behaviors
  - Recognizes departures from normal as potential intrusions
- **Advantages?**
  - Can detect attempts to exploit new and unforeseen vulnerabilities
  - Can recognize authorized usage that falls outside the normal pattern
- **Disadvantages?**
  - Generally slower, more resource intensive compared to signature-based IDS
  - Greater complexity, difficult to configure
  - Higher percentages of false alerts

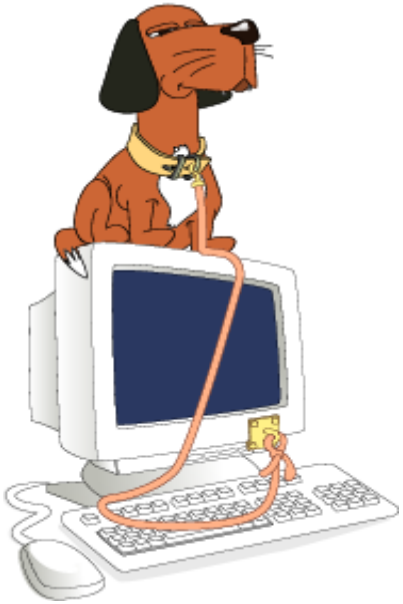


Network-based IDS

- **Characteristics**
  - NIDS examine raw packets in the network passively and triggers alerts
- **Advantages?**
  - Easy deployment
  - Unobtrusive
  - Difficult to evade if done at low level of network operation
- **Disadvantages?**
  - Different hosts process packets differently
  - NIDS needs to create traffic seen at the end host
  - Need to have the complete network topology and complete host behavior

Host-based IDS

- **Characteristics**
  - Runs on single host
  - Can analyze audit-trails, logs, integrity of files and directories, etc.
- **Advantages**
  - More accurate than NIDS
  - Less volume of traffic so less overhead
- **Disadvantages**
  - Deployment is expensive
  - What happens when host get compromised?



Summary

- TCP/IP security vulnerabilities
  - Spoofing
  - Flooding attacks
  - TCP session poisoning
- DOS and D-DOS
- Firewalls
  - Packet Filters
  - Proxy
- IDS
  - Signature and Anomaly IDS
  - NIDS and HIDS