CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

Midterm Review

Chris Samayoa

Week 9 – 1st Lecture
3/15/2022

Course Information

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- CECS 303
  - Networks and Network Security – 3.0 units
- Class meeting schedule
  - TuTH 5:00PM to 7:15PM
  - Lecture Room: VEC 402
  - Lab Room: ECS 413
- Class communication
  - chris.samayoa@csulb.edu
  - Cell: 562-706-2196
- Office hours
  - Thursdays 4pm-5pm (VEC-404)
  - Other times by appointment only

IEEE – Networking Specifications

- IEEE's Project 802
  - Effort to standardize physical and logical network elements
    - Frame types and addressing
    - Connectivity
    - Networking media
    - Error-checking algorithms
    - Encryption
    - Emerging technologies
- 802.3: Ethernet
- 802.11: Wireless

IEEE – Network Standards

CALIFORNIA STATE UNIVERSITY LONG BEACH College of Engineering

Standard	Name	Topic
802.1	Bridging and Management	Routing, bridging, and network-to-network communications
802.2	Logical Link Control	Error and flow control over data frames
802.3	Ethernet	All forms of Ethernet media and interfaces
802.5	Token Ring LAN	All forms of token ring media and interfaces
802.11	Wireless LANs	Standards for wireless networking for many different broadcast frequencies and usage techniques
802.15	Wireless PANs	The coexistence of wireless personal area networks with other wireless devices in unlicensed frequency bands
802.16	Broadband Wireless MANs	The atmospheric interface and related functions associated with broadband wireless connectivity; also known as WiMAX
802.17	Resilient Packet Rings	Access method, physical layer specifications, and management of shared packet-based transmission on resilient rings (such as SONET)
802.20	Mobile Broadband Wireless Access	Packet handling and other specifications for multivendor, mobile high-speed wireless transmission, nicknamed "mobile WiMAX"
802.22	Wireless Regional Area Networks	Wireless, broadcast-style network to operate in the UHF/VHF frequency bands formerly used for TV channels

Image: Course Technology / Cengage learning

IANA and ICANN

- IP (Internet Protocol) address
  - Address identifying computers in TCP/IP based (Internet) networks
  - Reliance on centralized management authorities
- History
  - Initially: IANA (Internet Assigned Numbers Authority)
  - 1997: Three RIRs (Regional Internet Registries)
    - ARIN (American Registry for Internet Numbers)
    - APNIC (Asia Pacific Network Information Centre)
    - RIPE (Réseaux IP Européens)

IANA and ICANN (cont'd)

- History (cont'd)
  - Late 1990s: ICANN (Internet Corporation for Assigned Names and Numbers)
    - Private nonprofit corporation
    - Remains responsible for IP addressing and domain name management (DNS)
    - IANA performs system administration
- ISPs (Internet Service Providers) are responsible for distributing IP addresses to users and businesses

OSI Model

- Model for understanding and developing network host-to-host communications
- Developed by ISO in the 1980s
  - Best looked at as a conceptual model at this point
- Divides network communications into seven layers
  - Physical, Data Link, Network, Transport, Session, Presentation, Application

OSI Model (cont'd)

- Protocol interaction
  - Stacked approach – interact with layers directly above and below
- Application layer protocols
  - Interact with software
- Physical layer protocols
  - Cables and connectors
- Theoretical representation describing network communication between two nodes

OSI Model - Data Flow

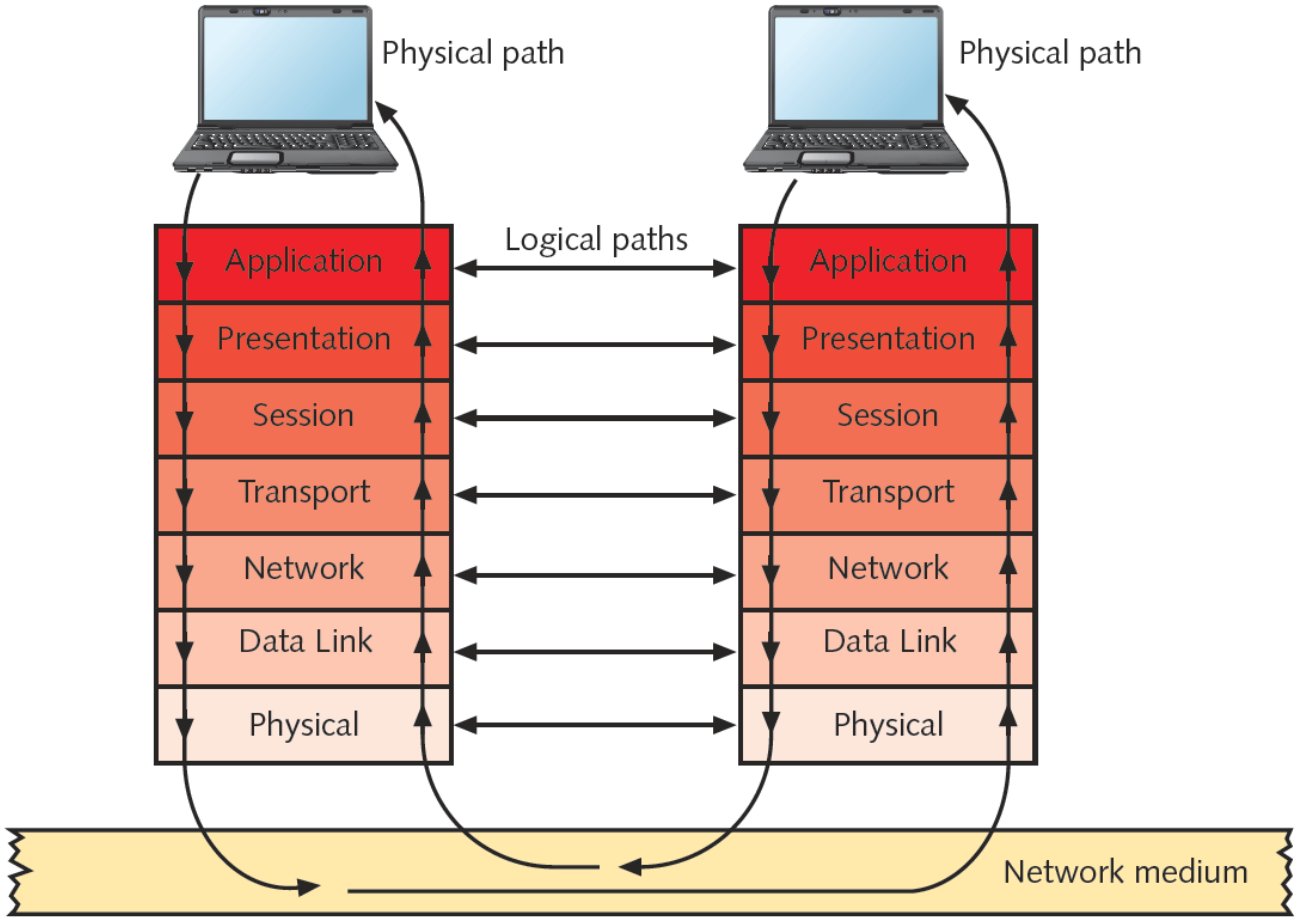


Image: Course Technology/Cengage Learning

Network Layer

- Protocol functions
  - Translate network addresses into physical counterparts
  - Decide how to route data from sender to receiver
- Addressing
  - System for assigning unique identification numbers to network devices
- Types of addresses
  - Network addresses (logical or virtual addresses)
  - Physical addresses

Network Layer

- Network address example: 192.168.1.4
- Physical address example: A6-2B-B5-AE-00-FB (48 bits)
- Factors used to determine path routing
  - Delivery priority
  - Network congestion
  - Quality of service
  - Cost of alternative routes
- Routers belong in the network layer

Network Layer (cont'd)

- Common Network Layer Protocol
  - IP (Internet Protocol)
- Fragmentation
  - Subdividing Transport layer segments
  - Performed at the Network layer
- Segmentation preferred over fragmentation for greater network efficiency

Network Layer (cont'd)


```
⊞ Frame 7: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
⊞ Ethernet II, Src: c2:01:0f:2c:00:00 (c2:01:0f:2c:00:00), Dst: c2:02:0c:0c:00:00 (c2:02:0c:0c:00:00)
⊟ Internet Protocol Version 4, Src: 10.0.12.1 (10.0.12.1), Dst: 10.0.12.2 (10.0.12.2)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 120
    Identification: 0x000b (11)
  ⊞ Flags: 0x00
    Fragment offset: 8880
    Time to live: 255
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x8b21 [validation disabled]
    Source: 10.0.12.1 (10.0.12.1)
    Destination: 10.0.12.2 (10.0.12.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ⊟ [7 IPv4 Fragments (8980 bytes): #1(1480), #2(1480), #3(1480), #4(1480), #5(1480), #6(1480), #7(100)]
      [Frame: 1, payload: 0-1479 (1480 bytes)]
      [Frame: 2, payload: 1480-2959 (1480 bytes)]
      [Frame: 3, payload: 2960-4439 (1480 bytes)]
      [Frame: 4, payload: 4440-5919 (1480 bytes)]
      [Frame: 5, payload: 5920-7399 (1480 bytes)]
      [Frame: 6, payload: 7400-8879 (1480 bytes)]
      [Frame: 7, payload: 8880-8979 (100 bytes)]
      [Fragment count: 7]
      [Reassembled IPv4 length: 8980]
      [Reassembled IPv4 data: 080025f10003000000000000000001eb30abcdabcdabcdabcd...]
⊞ Internet Control Message Protocol
```

Data Link Layer

- Protocol functions
  - Divide data received into distinct frames for transmission in Physical layer
- Frame
  - Structured package for moving data
  - Includes raw data (payload), sender's and receiver's network addresses, error checking and control information
- Communications Issues
  - Not all information received
  - Corrected by error checking

Data Link Layer (cont'd)

- Error checking methods
  - Frame check sequence
  - CRC (cyclic redundancy check)
- Frame
  - Structured package for moving data
  - Includes raw data (payload), sender's and receiver's network addresses, error checking and control information

Data Link Layer (cont'd)

- Two Data Link layer sublayers
  - LLC (Logical Link Control) sublayer
  - MAC (Media Access Control) sublayer
- MAC sublayer
  - Manages access to the physical medium
  - Appends physical address of destination computer onto data frame
- Physical Address
  - Fixed number associated with each device's network interface

OSI Model - Summary

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

OSI model layer	Function
Application (Layer 7)	Provides interface between software applications and a network for interpreting applications' requests and requirements
Presentation (Layer 6)	Allows hosts and applications to use a common language; performs data formatting, encryption, and compression
Session (Layer 5)	Establishes, maintains, and terminates user connections
Transport (Layer 4)	Ensures accurate delivery of data through flow control, segmentation and reassembly, error correction, and acknowledgment
Network (Layer 3)	Establishes network connections; translates network addresses into their physical counterparts and determines routing
Data Link (Layer 2)	Packages data in frames appropriate to network transmission method
Physical (Layer 1)	Manages signaling to and from physical network connections

Image: Course Technology / Cengage learning

Network Basics

- What is a computer network?
  - Group of interconnected computers and devices
    - Connected by transmission media
- Stand-alone computer
  - Not connected to other computers
  - Can only use local software and data
- Advantages of networks
  - Device and resource sharing by multiple users
    - Saves money and time
  - Central network management

LANs, MANs, and WANs

- LAN (local area network)
  - Network confined to relatively small location
  - Original simple peer-to-peer based networks
  - Currently used for large and complex client/server networks and peer-to-peer networks
- Original simple peer-to-peer based networks
  - Up to individuals if resources are shared (and which ones)
- MAN (metropolitan area network)
  - Connects clients and servers from multiple buildings

LANs, MANs, and WANs (cont'd)

- WAN (wide area network)
  - Connects two or more geographically separate LANs or MANs
  - Often interconnected via the internet and different internet service providers
  - Uses
    - Interconnect separate offices for same organization
    - Interconnect separate offices/networks for different organizations and client users

Mail Servers

- Host responsible for e-mail storage and transfer of messages
- Additional tasks of mail servers
  - Intercept spam
  - Handle objectionable content
  - Route messages according to rules
  - Provide Web-based client for checking e-mail
  - Notify administrators or users if certain events occur
  - Schedule e-mail transmission, retrieval, storage, maintenance
  - Communicate with mail servers on other networks
- Specialized software is needed in order to function as a mail server

TCP/IP Model

- Four Layers
  - Application layer
  - Transport layer
  - Internet layer
  - Network access layer (or Link layer)

TCP/IP Model (cont'd)

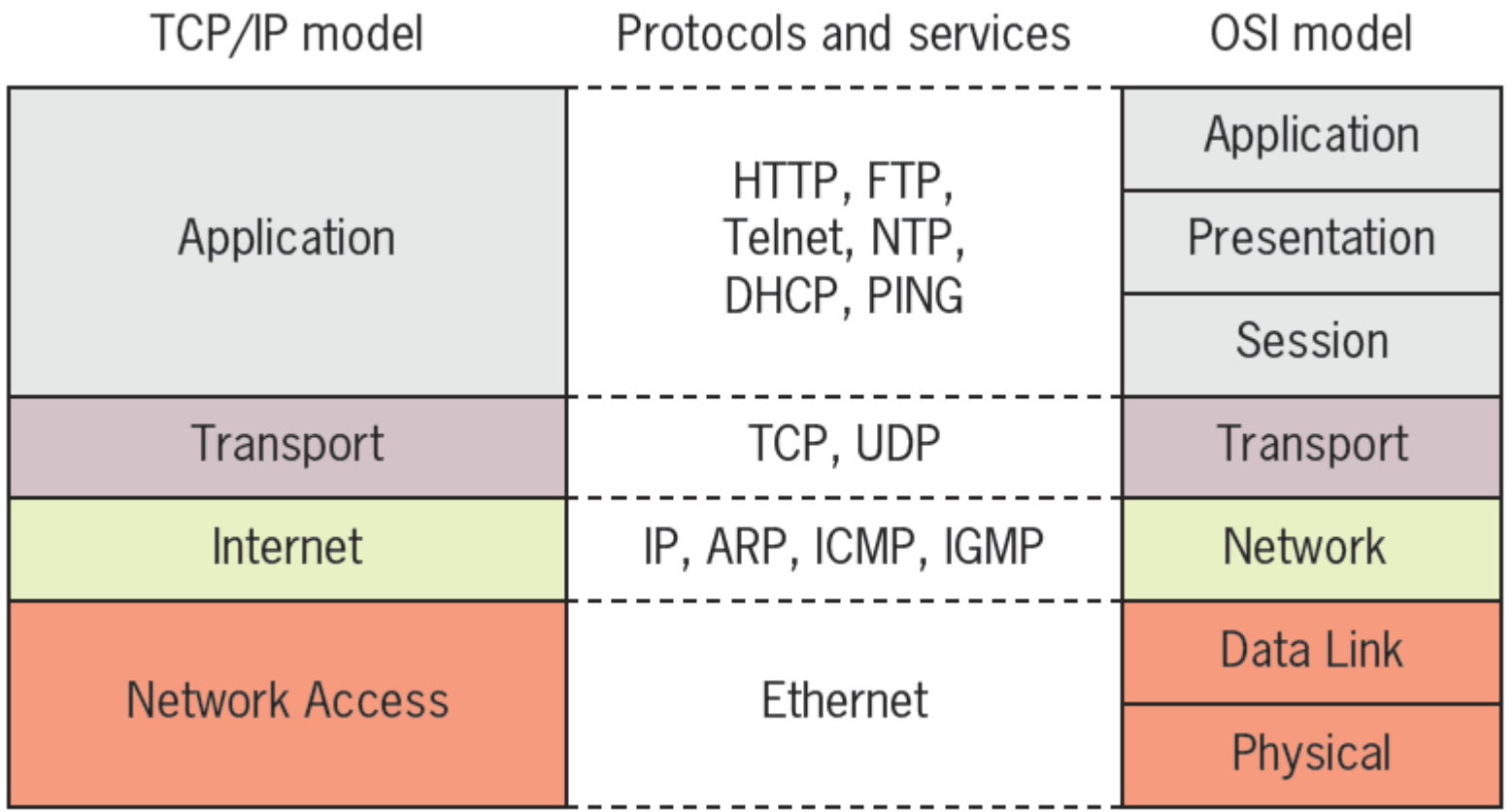


Image: Course Technology / Cengage learning

TCP/IP Overview

- TCP/IP = Transmission Control Protocol / Internet Protocol
- Protocol Suite
  - Commonly referred to as “IP” or “TCP/IP”
  - Subprotocols include TCP, IP, UDP, and ARP
  - Internet layer
  - Network access layer (or Link layer)
- Developed by US Department of Defense
  - Specifically DARPA (Defense Advanced Research Projects Agency)
  - ARPANET (developed in late 1960s) was precursor to TCP/IP protocol suite and internet as a whole

TCP/IP Core

- TCP/IP suite subprotocols
- Mainly operates in Transport or Network layers of OSI model
- Provide basic services to protocols in other layers
- Most significant protocols in TCP/IP suite
  - TCP
  - IP

TCP

- TCP = Transmission Control Protocol
  - Transport layer protocol
- Provides reliable data delivery services
  - Connection-oriented subprotocol
    - Establish connection before transmitting
- Uses sequencing and checksums
- Provides flow control
- TCP segment format
  - Encapsulated by IP packet in Network layer
    - Becomes IP packet's "data"

TCP 3-Way Handshake

- Three segments establish a connection
- Host A issues message to Host B
  - Sends segment with SYN bit set
    - SYN field: Random synchronize sequence number
- Host B receives message
  - Sends segment
    - ACK field: sequence number Host A sent plus 1
    - SYN field: Computer B random number
- Host A responds
  - Sends segment
    - ACK field: sequence number Host B sent plus 1
- FIN flag indicates transmission end

3-Way Handshake (cont'd)

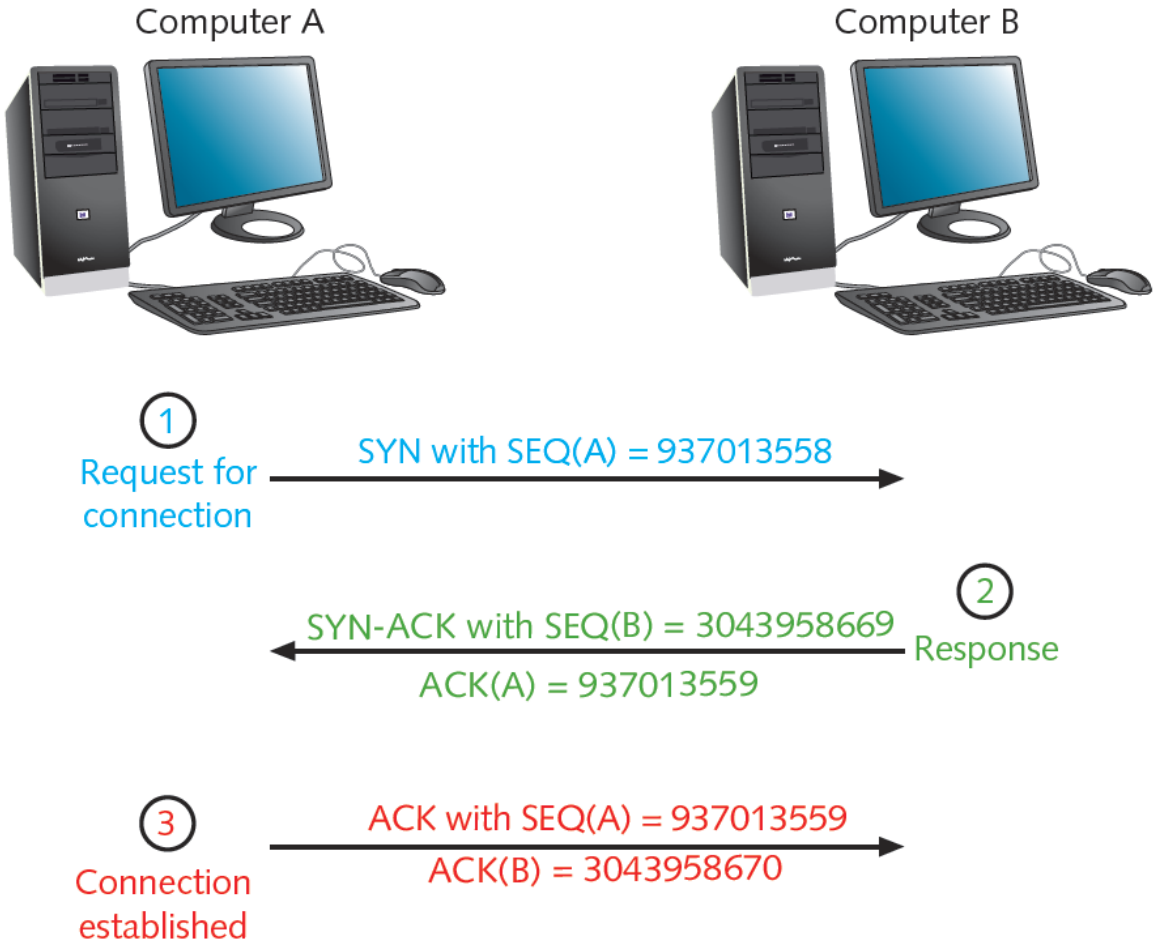


Image: Course Technology / Cengage learning

UDP

- UDP = User Datagram Protocol
  - Transport layer protocol
- Provides unreliable data delivery services
  - Connectionless transport service
  - No assurance packets received in correct sequence
  - No guarantee packets received at all
  - No error checking, sequencing
  - Lacks sophistication
    - More efficient than TCP
- Useful situations
  - Great volume of data transferred quickly

IP (Internet Protocol)

- Network layer protocol
  - How and where data delivered, including:
    - Data's source and destination addresses
- Enables TCP/IP to internetwork
  - Traverse more than one LAN segment
    - More than one network type through router
- Network layer data formed into packets
  - IP packet
    - Data envelope
    - Contains information for routers to transfer data between different LAN segments

IP (cont'd)

- Versions
  - IPv4: unreliable, connectionless protocol
  - IPv6: connectionless or connection-oriented
- "Newer" version of IP protocol
  - IP next generation
  - Released in 1998
- Advantages of IPv6
  - Provides trillions of additional IP addresses
  - Better security and prioritization provisions

IPv4 Packet

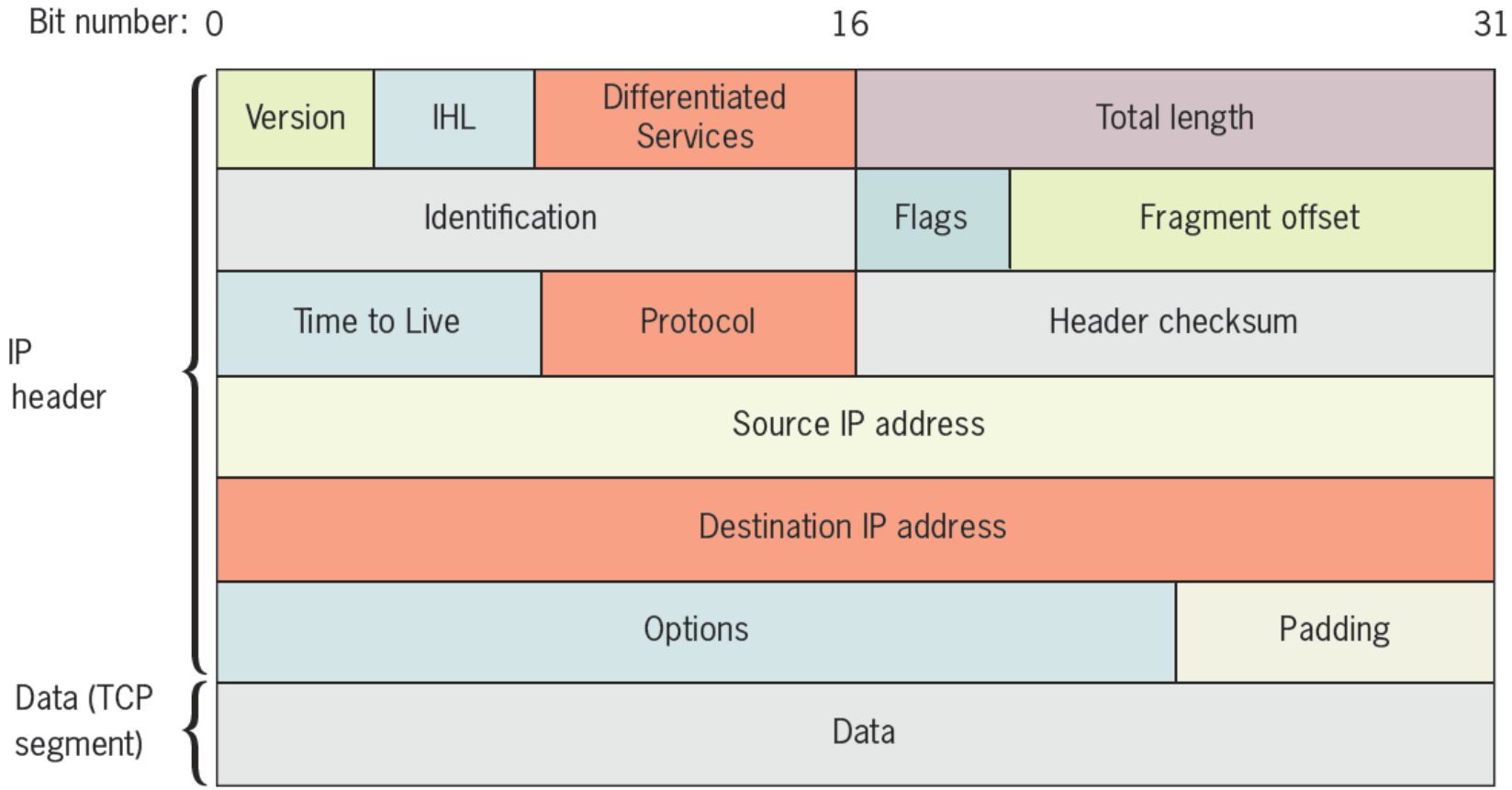


Image: Course Technology / Cengage learning

ARP

- ARP = Address Resolution Protocol
- Network layer protocol
- Used with IPv4
- Obtains MAC (physical) address of host or node
- Creates database that maps MAC to host's IP address
- ARP table
  - Table of recognized MAC-to-IP address mappings
  - Saved on network device's local storage (host, network switch, etc.)
  - Increases efficiency
  - Contains dynamic and static entries

ICMP

- ICMP = Internet Control Message Protocol
- Network layer protocol
  - Reports on data delivery success or failure
- Announces transmission failures to sender
  - Network congestion
  - Data fails to reach destination
  - Data discarded: TTL expired
- ICMP cannot correct errors
  - Provides critical network problem troubleshooting information
- ICMPv6 used with IPv6

IPv4 Addressing

- Networks recognize two addresses
  - Logical (Network layer)
  - Physical (MAC / hardware) addresses
- IP Protocol handles logical addressing
- Specific Parameters
  - Unique 32-bit number
    - Divided into four octets (sets of eight bits) separated by periods
    - Example: 192.168.1.1
  - Network class determined from first octet

Common IPv4 Classes

Network class	Beginning octet	Number of networks	Maximum addressable hosts per network
A	1–126	126	16,777,214
B	128–191	> 16,000	65,534
C	192–223	> 2,000,000	254

Image: Course Technology / Cengage learning

IPv4 Addressing (cont'd)

- Class D, Class E rarely used (never assign)
  - Class D: value between 224 and 239
    - Multicasting
  - Class E: value between 240 and 254
    - Experimental use
- Eight bits have 256 combinations
  - Networks use 1 through 254
  - 0: reserved as placeholder
  - 255: reserved for broadcast transmission

IPv4 Addressing (cont'd)

- Class A devices
  - Share same first octet (bits 0-7)
    - Network ID
  - Host: second through fourth octets (bits 8-31)
- Class B devices
  - Share same first two octet (bits 0-15)
  - Host: second through fourth octets (bits 16-31)
- Class C devices
  - Share same first three octet (bits 0-23)
  - Host: second through fourth octets (bits 24-31)

IPv4 Classes

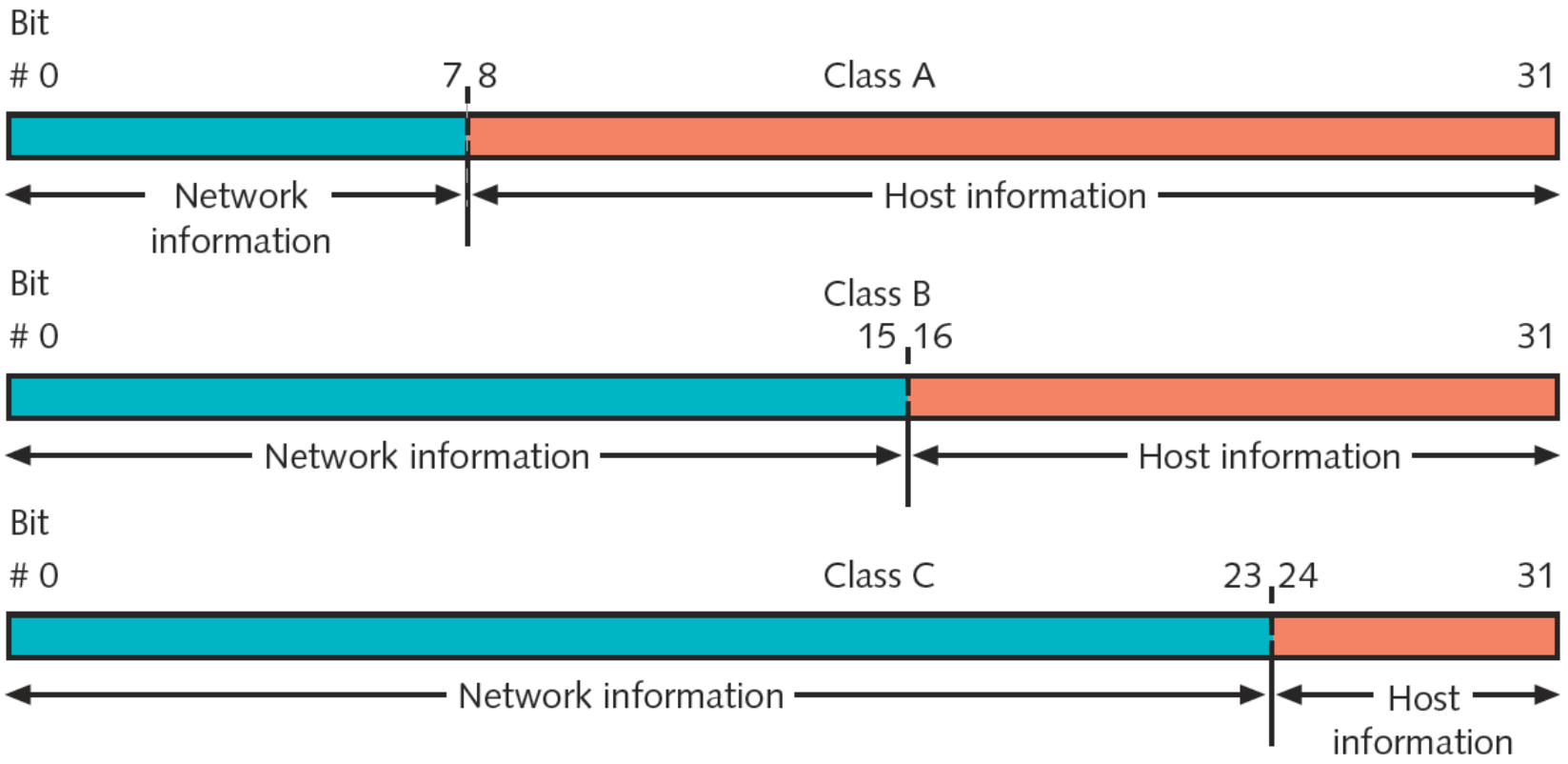


Image: Course Technology / Cengage learning

IPv4 Addressing (cont'd)

- Loopback address
  - First octet equals 127 (127.0.0.1)
- Loopback test
  - Attempting to connect to own machine
  - Useful for troubleshooting
- Windows
  - 'ipconfig' command
- Unix / Linux
  - 'ifconfig' command

Subnet Mask

- 32-bit number identifying a device's subnet
- Combines with device IP address
- Informs network about logical subdivision of IPs
- Four octets (32 bits)
  - Expressed in binary or dotted decimal notation
- Assigned same way as IP addresses
  - Manually or automatically (via DHCP)

Subnet Mask (cont'd)

Network class		Default subnet mask
A	1–126	255.0.0.0
B	128–191	255.255.0.0
C	192–223	255.255.255.0

Image: Course Technology / Cengage learning

Assigning IP Addresses

- Government-sponsored organizations
  - Distribute IP addresses
  - IANA, ICANN, RIRs (Regional Internet Registries)
    - ARIN (American Registry for Internet Numbers) responsible for serving the United States (and Antarctica, Canada, and various islands)
- Companies and individuals obtain IP addresses from ISPs (typically)
- Every network node must have a unique IP address
  - Otherwise network errors occur
  - Only one can exist in a router or switch's ARP table

Assigning IP Addresses (cont'd)

- Static IP address
  - Manually assigned
  - To change -> modify client workstation TCP/IP properties
  - Human error causes duplicates
- Dynamic IP address
  - Assigned automatically
  - Most common method
    - Dynamic Host Configuration Protocol (DHCP)

DHCP

- Automatically assigns device a unique IP address
- Application layer protocol
  - Uses lower layers, but functions as a service
  - Still some debate over whether it is an application or network layer protocol
- Reasons for implementing
  - Reduce time and planning for IP address management
  - Reduce potential for error in assigning IP addresses
  - Enable users to move workstations and printers
  - Make IP addressing transparent for mobile users

DHCP (cont'd)

- DHCP leasing process
  - Device borrows (leases) an IP address while attached to network
- Lease time
  - Determined when client obtains IP address at log on
  - User may force lease termination
- DHCP service configuration
  - Specify leased address range
  - Configure lease duration
  - Many additional options are configurable
- Several steps to negotiate client's first lease
  - DHCPDISCOVER
  - DHCPOFFER
  - DHCPREQUEST
  - DHCPACK

DHCP Leasing Process

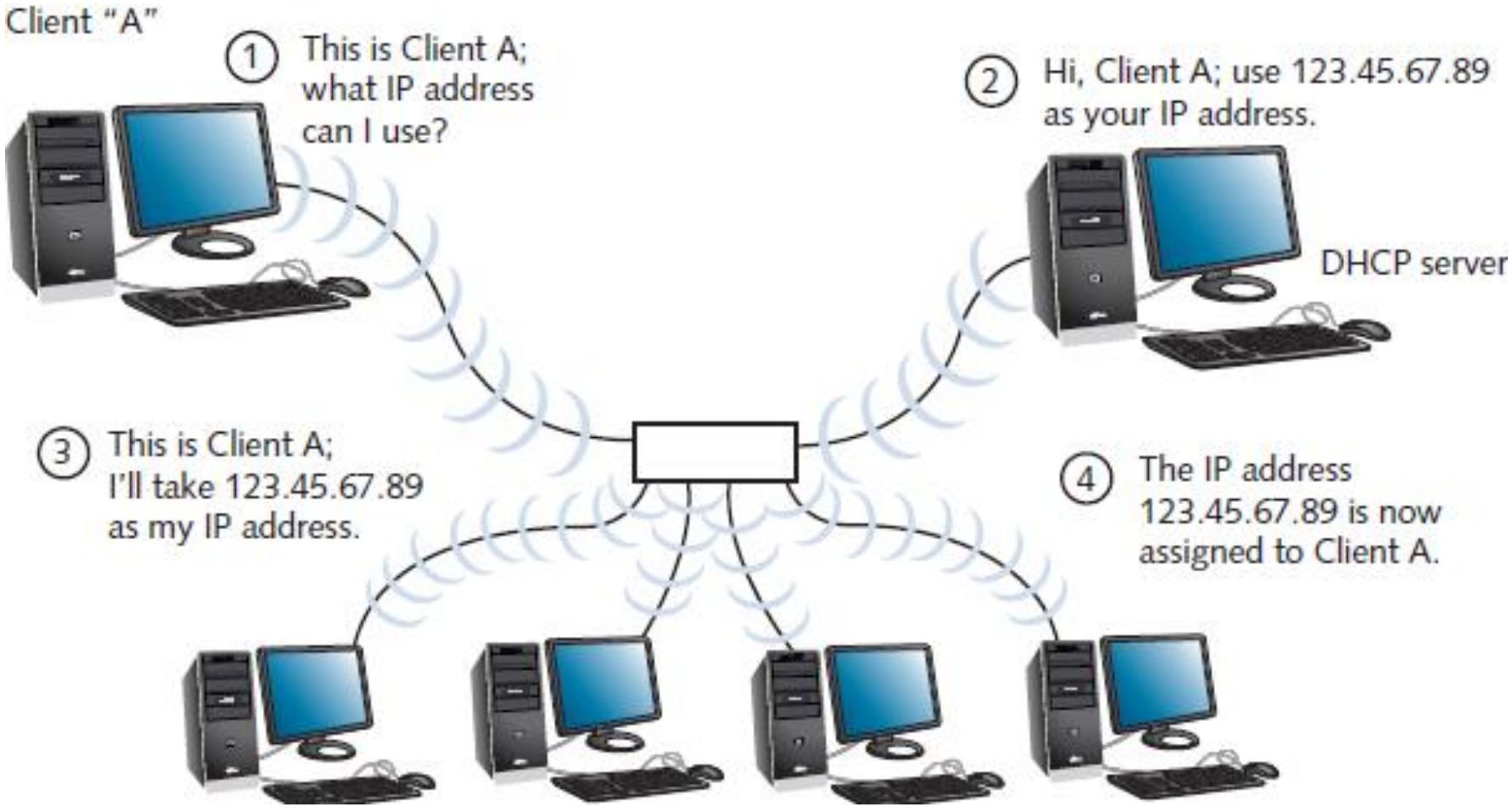


Image: Course Technology / Cengage learning

DHCP (cont'd)

- Terminating a DHCP Lease
  - Expire based on period established in server configuration
  - Manually terminated at any time
    - Client's TCP/IP configuration
    - Server's DHCP configuration
- Circumstances requiring lease termination
  - DHCP server fails and replaced
- DHCP services run on several server types
  - Installation and configurations vary

Private and Link-Local Addresses

- Private addresses
  - Allow hosts in organization to communicate across internal network
  - Cannot be routed on public network
- Specific IPv4 address ranges reserved for private addresses
  - Class A: 10.0.0.0 to 10.255.255.255
  - Class B: 172.16.0.0 to 172.31.255.255
  - Class C: 192.168.0.0 to 192.168.255.255
- Link-local address
  - Provisional address
  - Capable of data transfer only on local network segment

Sockets and Ports

- Processes assigned unique port numbers
- Process's socket
  - Port number plus host machine's IP address
- Port numbers
  - Simplify TCP/IP communications
  - Ensures data transmitted correctly
- Example
  - Telnet port number: 23
  - IPv4 host address: 192.168.1.28
  - Socket address: 192.168.1.28:23

Sockets and Ports (cont'd)

- Port number range: 0 to 65535
- Three types
  - Well known ports
    - Range: 0 to 1023
    - Operating system or administrator use
  - Registered ports
    - Range: 1024 to 49151
    - Assigned by IANA
    - Network users, processes with no special privileges
  - Dynamic and/or private ports
    - Range: 49152 to 65535
    - No restrictions; typically used by customized services or temporary purposes

Common Port Numbers

Port number	Process name	Protocol used	Description
20	FTP-DATA	TCP	File transfer—data
21	FTP	TCP	File transfer—control
22	SSH	TCP	Secure Shell
23	TELNET	TCP	Telnet
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP and UDP	Domain Name System
67 (client to server) and 68 (server to client)	DHCPv4	UDP	Dynamic Host Configuration Protocol version 4
69	TFTP	UDP	Trivial File Transfer Protocol
80	HTTP	TCP and UDP	Hypertext Transfer Protocol
110	POP3	TCP	Post Office Protocol 3
123	NTP	TCP	Network Time Protocol
143	IMAP	TCP	Internet Message Access Protocol
443	HTTPS	TCP	Secure implementation of HTTP
546 (client to server) and 547 (server to client)	DHCPv6	UDP	Dynamic Host Configuration Protocol version 6
3389	RDP	TCP	Remote Desktop Protocol

Image: Course Technology / Cengage learning

Host Files

- ARPAnet used hosts.txt file
  - Associated host names with IP addresses
  - Host matched by one line
    - Identifies host's name and IP address
    - Alias provides nickname
- UNIX-/Linux computer
  - Host file called hosts
  - Located in the /etc directory
- Windows computer
  - Host file called hosts
  - Located in Windows\system32\drivers\etc folder

Sample Hosts File

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
192.168.1.34           www.abc.com

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

Image: Course Technology / Cengage learning

DNS

- DNS = Domain Name Service
- Hierarchical
- Associate domain names with IP addresses
- DNS refers to:
  - Application layer service accomplishing association
  - Organized system of computers, databases making association possible
- DNS redundancy
  - Many computers across globe related in hierarchical manner
  - Root servers
    - 13 computers (ultimate authorities)

DNS (cont'd)

- Three components
  - Resolvers
    - Any hosts on Internet needing to look up domain name information
  - Name servers (DNS servers)
    - Databases of associated names and IP addresses
    - Provide information to resolvers on request
  - Namespace
    - Abstract database of Internet IP addresses and associated names
    - Describes how name servers of the world share DNS information

Domain Name Resolution

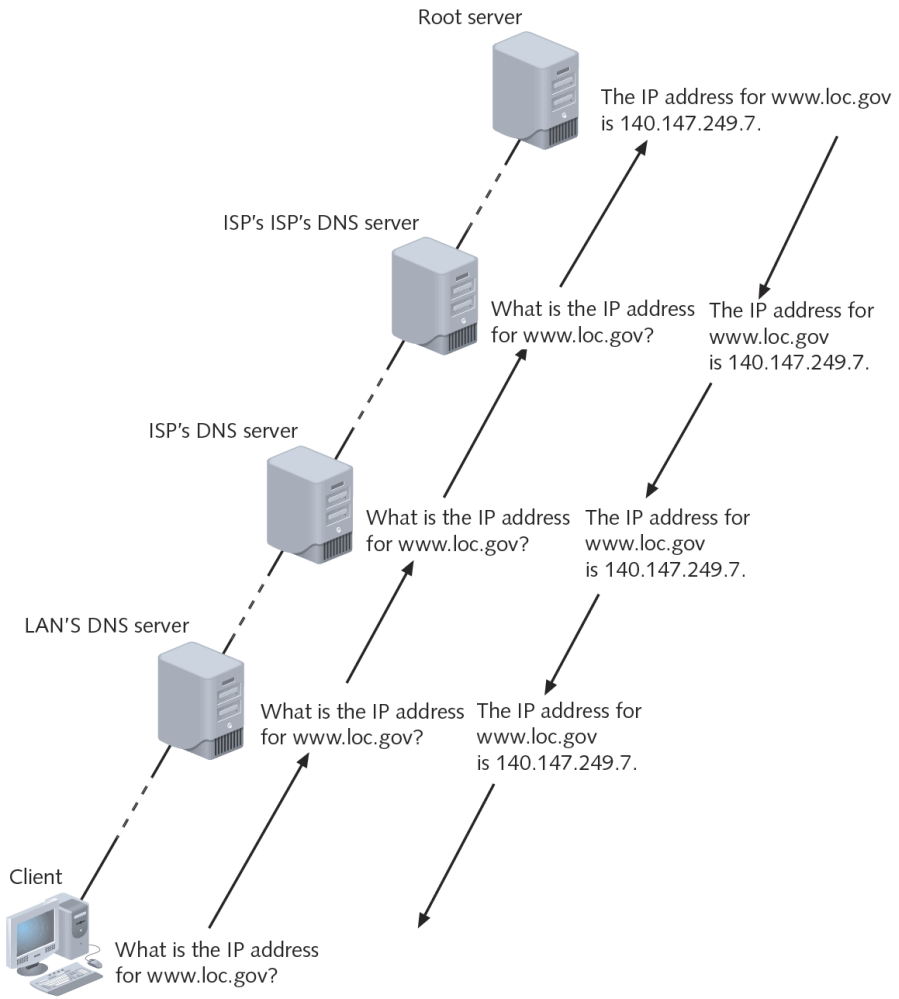


Image: Course Technology / Cengage learning

DNS (cont'd)

- Resource record
  - Describes one piece of DNS database information
  - Many different types
    - Dependent on function

Type	Name	Description
A	Address record	A host's IPv4 address
AAAA	Address record	A host's IPv6 address
CNAME	Canonical name record	Another name for the host
MX	Mail exchange record	Identifies a mail server
PTR	Pointer record	Points to a canonical name

DDNS

- DDNS (Dynamic DNS)
- Often used for website hosting by small businesses or private individuals
  - Manually changing DNS records unmanageable with dynamic external IP addresses
- Process
  - Service provider runs program on user's computer
    - Notifies service provider when IP address changes
  - Service provider's server launches routine to automatically update DNS record
    - Effective throughout Internet in minutes
- Larger organizations buy statically assigned IP address blocks

Three Aspects of Security

- Confidentiality
  - Keep data private
- Integrity
  - Keep data from being modified by unauthorized individuals/processes
- Availability
  - Keep the system running and reachable

Policy vs. Mechanism

- A **security policy** defines what is and is not allowed on a network or system
  - Needed for organizations of all sizes
- **Security mechanism** is a method or tool for enforcing security policy
  - Prevention
  - Detection
  - Response
- Types of mechanisms:
  - Identification
  - Authentication
  - Audit
  - Containment

Important Considerations

- Risk analysis and risk management
  - Impact of loss of data
  - Impact of disclosure
  - Legislation may play a role
- Human factors
  - The weakest link

Attacker Type: Published Attack Tools

- Attacker has specific tools
  - Casts the tool widely to see what can be caught.
  - Sometimes described as script-kiddies
    - Gets them into systems with specific vulnerabilities
    - Gets them account access to susceptible employees
  - They gather what they find, exfiltrate or modify, and stop there
- Strong security posture is effective
  - Sound security practices
  - Systems up to date
  - Least privilege

Attacker Type: Opportunistic

- Looks for a weak link
  - Uses tools to scan for vulnerabilities
  - Once in, repeats the process
    - This time starting with elevated access because of the system or user ID already compromised.
  - They gather what they find, exfiltrate or modify, and stop there
- Good containment architecture can be effective
  - Administrators need to be aware of what paths might be used to reach sensitive data

Attacker Type: Goal Oriented and Top Down

- Researches your organization and system
  - Goal is to compromise some component of your system or access specific data.
  - Learns precursor activities that must be achieved to meet that goal.
  - Often applies APT – Advanced Persistent Threat tactics
  - Will wait for threat vector to propagate
- Defense requires comprehensive strategy:
  - Strong security posture
  - Training of privileged employees
  - Containment Architecture
  - Strong defenses to subversion

Monetary Motivations

- Botnets
  - Controlled machines for sale
- “Protection” or “recovery” for sale
- Attack software for sale
- Stolen data for sale
- Intermediaries used to convert online balances to cash
  - These are the pawns and the ones that are most easily caught

Terminology

- Vulnerability
  - A weakness in a system, program, procedure, or configuration that could allow an adversary to violate the intended policies of a system
- Threat
  - Tools or knowledge (capabilities) that are capable of exploiting a vulnerability to violate the intended policies of a system
- Attack
  - An attempt to exploit a vulnerability to violate the intended policies of a system
- Compromise
  - The successful actions that violate the intended polices of a system

Terminology (cont'd)

- Penetration
  - A successful attack (intrusion) that exploits a vulnerability in the code base of a system or its configuration. The result will often be to install a subversion
- Denial of Service
  - An attack that prevents authorized access to a resource, by destroying a target or overwhelming it with undesired requests
- Subversion
  - An intentional change to the code base or configuration of a system that alters the proper enforcement of policy. This includes the installation of backdoors and other control channels in violation of the policy relevant to the system
- Subversion vectors
  - The methods by which subversions are introduced into a system. Often the vectors take the form of malicious code

Terminology (cont'd)

- Secure
  - A system is secure if it correctly enforces a correctly stated policy for a system. A system can only be secure with respect to a particular set of policies and under a set of stated assumptions. There is no system that is absolutely secure.
- Attack Surface
  - The accumulation of all parts of a system that are exposed to an adversary against which the adversary can try to find and exploit a vulnerability that will render the system insecure (i.e. violate the security policies of the system).

General Security Concerns

- Buggy code
- Protocol design failures
- Weak crypto
- Social engineering
- Insider threats
- Poor configuration
- Incorrect policy specification
- Stolen keys or identities
- Denial of service

Security Mechanisms

- Encryption
- Checksums
- Key management
- Authentication
- Authorization
- Audit logs
- Firewalls
- Virtual Private Nets (VPNs)
- Intrusion detection
- Intrusion response
- Development tools
- Virus Scanners
- Policy managers
- Trusted hardware

Identification vs Authentication

- Identification
  - Associating an identify with an individual, process, or request
- Authentication
  - Verification of a claimed identity
  - Ideally
    - Who you are
  - Practically
    - Something you know
    - Something you have
    - Something you are
- Often used in combination
  - e.g. Diffie-Hellman in TLS to exchange AES cipher

Something You Know

- Password or Algorithm
  - e.g. Encryption key derived from password
- Issues
  - How to keep it secret?
    - Find it, sniff it, social engineer it
  - You need to remember it
  - How is it stored and checked?
- Potential attacks
  - Brute force
  - Dictionary
  - Pre-computed Dictionary
  - Guessing
  - Finding elsewhere

Something You Have

- Cards
  - Mag stripe
  - Smart Card
  - USB Key
  - Time varying password
- Issues
  - How to validate?
    - Verifier can be compromised
  - Need special infrastructure
  - e.g. RSA SecureID (https://www.wired.com/2011/06/rsa-replaces-securid-tokens/)

Something You Are

- Biometrics
  - Iris scan
  - Fingerprint
  - Picture
  - Voice
- Issues
  - Need to prevent spoofing

Router Access Lists

- Control traffic through routers
- Router's main functions
  - Examine packets
  - Determine destination
    - Based on Network layer addressing information
- ACL (access control list)
  - aka. access list
  - Routers can decline to forward certain packets
- Stateless
  - Access lists look at packets independent of what traffic has come before

Router Access Lists (cont'd)

- ACL variables used to permit or deny traffic
  - Network layer protocol (IP, ICMP)
  - Transport layer protocol (TCP, UDP)
  - Source IP address
  - Source netmask
  - Destination IP address
  - Destination netmask
  - TCP or UDP port number

Router Access Lists (cont'd)

- Router receives packet, examines packet
  - Refers to ACL for permit / deny criteria
  - Drops packet if deny characteristics match
  - Forwards packet if permit characteristics match
- Access list statement examples
  - Deny all traffic from source address with netmask 255.255.255.255
  - Deny all traffic destined for TCP port 23
- Separate ACL's for:
  - Interfaces; inbound and outbound traffic

ACL Example

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

```
R1(config-ext-nacl)#do sh access-list OutBoundAccess
Extended IP access list OutBoundAccess
    10 permit ip 192.168.1.0 0.0.0.255 any
    11 deny tcp 192.168.2.0 0.0.0.127 any eq smtp
    12 deny tcp 192.168.2.0 0.0.0.127 any eq sunrpc
    13 deny tcp 192.168.2.0 0.0.0.127 any eq pop2
    14 deny tcp 192.168.2.0 0.0.0.127 any eq nntp
    15 deny tcp 192.168.2.0 0.0.0.127 any eq ftp
    16 deny tcp 192.168.2.0 0.0.0.127 any eq ftp-data
    17 deny tcp 192.168.2.0 0.0.0.127 any eq telnet
    18 deny tcp 192.168.2.0 0.0.0.127 any eq cmd
    19 deny tcp 192.168.2.0 0.0.0.127 any eq irc
    20 permit ip 192.168.2.0 0.0.0.255 any
    30 permit ip 192.168.3.0 0.0.0.255 any
    40 permit ip 192.168.4.0 0.0.0.255 any
    50 permit ip 192.168.5.0 0.0.0.255 any
R1(config-ext-nacl)#
```

Source: CCIE-or-Null.net

Firewalls

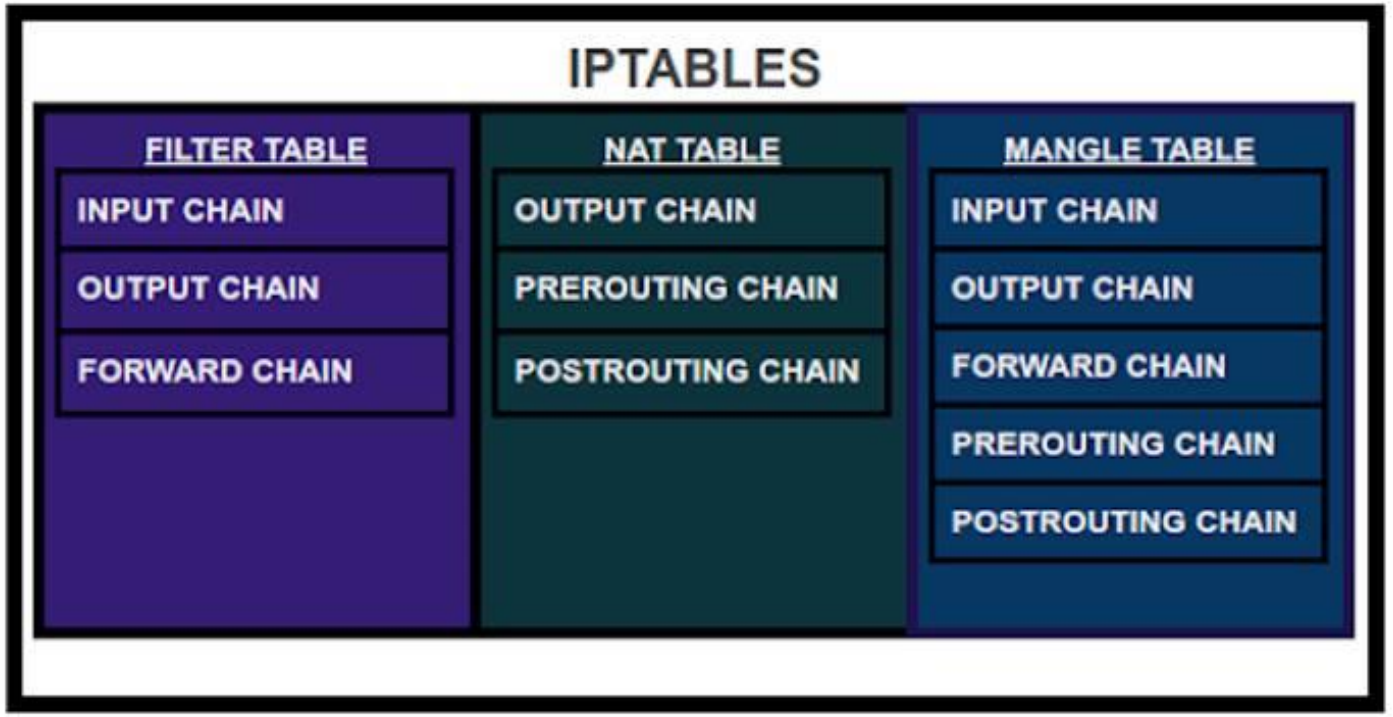
- Specialized device or computer installed with specialized software
  - Selectively filters and blocks traffic between networks
  - Involves hardware and software combination
  - Stateful
    - Decisions can be made based on previous traffic
    - e.g. Allowing return traffic from a web server
- Firewall locations
  - Between two interconnected private networks
  - Between private network and public network (network-based firewall)
  - Between two hosts (host based firewall)

iptables

- What is iptables
  - Firewall utility built for Linux operating systems
  - Stateful
    - But can be configured in a stateless manner
  - Uses policy chains to allow or block traffic
    - List based
- Types of chains
  - Input: used to control behavior for incoming connections
  - Forward: used for rerouting of traffic or NAT
  - Output: used to control behavior for outgoing connections
    - Need to consider return data as well

Iptables (cont'd)

- Filter table
  - Control flow of packets to and from the system
- NAT table
  - Redirect connections to other interfaces on network
- Mangle table
  - Modify packet headers



Source: linode.com

iptables (cont'd)

- Policy chain default behavior
  - What should iptables do if the connection doesn't match any existing rules?
    - ACCEPT
    - DROP (deny)
    - REJECT (deny)

```
user1@cecshost1:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
user1@cecshost1:~$
```

Address Translation

- Private Network
  - Access typically restricted
    - ➢ Clients and machines have proper authentication mechanisms
  - Hiding IP addresses
    - ➢ Provides more flexibility in assigning addresses
- NAT (Network Address Translation)
  - Gateway replaces client's private IP address with public (internet-recognized) IP address
    - ➢ Occurs in packet header
  - Separates private / public transmissions on TCP/IP network
- Reasons for using address translation
  - Overcome IPv4 address availability limitations
  - Add small level of security to private networks that need connectivity to public networks

NAT Types

- SNAT (Static Network Address Translation)
  - Client associated with one private IP address and one public IP address
  - Addresses never (rarely) change
  - Useful when running services such as a mail server
    - Helps to avoid IP blacklisting
- DNAT (Dynamic Network Address Translation)
  - Also called IP masquerading
  - Internet-valid IP address might be assigned to any client's outgoing transmission
- PAT (Port Address Translation)
  - Each client session with a server on the Internet is assigned a separate TCP port number
    - Client-server packets (headers) contain this port number
  - Internet server responds to packet's source address using same port

Private and Link-Local Addresses (review)

- Private addresses
  - Allow hosts in organization to communicate across internal network
  - Cannot be routed on public network
- Specific IPv4 address ranges reserved for private addresses
  - Class A: 10.0.0.0 to 10.255.255.255
  - Class B: 172.16.0.0 to 172.31.255.255
  - Class C: 192.168.0.0 to 192.168.255.255
- Link-local address
  - Provisional address
  - Capable of data transfer only on local network segment

CVE

- CVE = Common Vulnerabilities and Exposures
- List of publicly disclosed computer security flaws
  - Uses unique ID numbers to track separate vulnerabilities
- Overseen by MITRE corporation
  - Not-for-profit organization
  - Center for research for government and private instititutions
  - Received funding by CISA (Cybersecurity and infrastructure Security Agency) for maintaining CVE program
- Maintains list of vulnerabilities, but does not find them
  - Vulnerabilities are found by various organizations and individuals
- CVSS (Common Vulnerability Scoring System)
  - Open standard for assigning a value to a given vulnerability (0.0 – 10)
  - Higher numbers indicate a higher level of severity

CVE Criteria

- Independently fixable
  - Can be fixed independently of other vulnerabilities
- Acknowledged or documented
  - Affected vendor acknowledges that the finding is indeed a bug in their system
  - Reporter can alternatively share a vulnerability report that demonstrates negative impact to vendor and security policy violation
- Impacts one codebase
  - Each affected codebase or product gets a unique CVE
  - UNLESS there is shared code that cannot be used without it being vulnerable

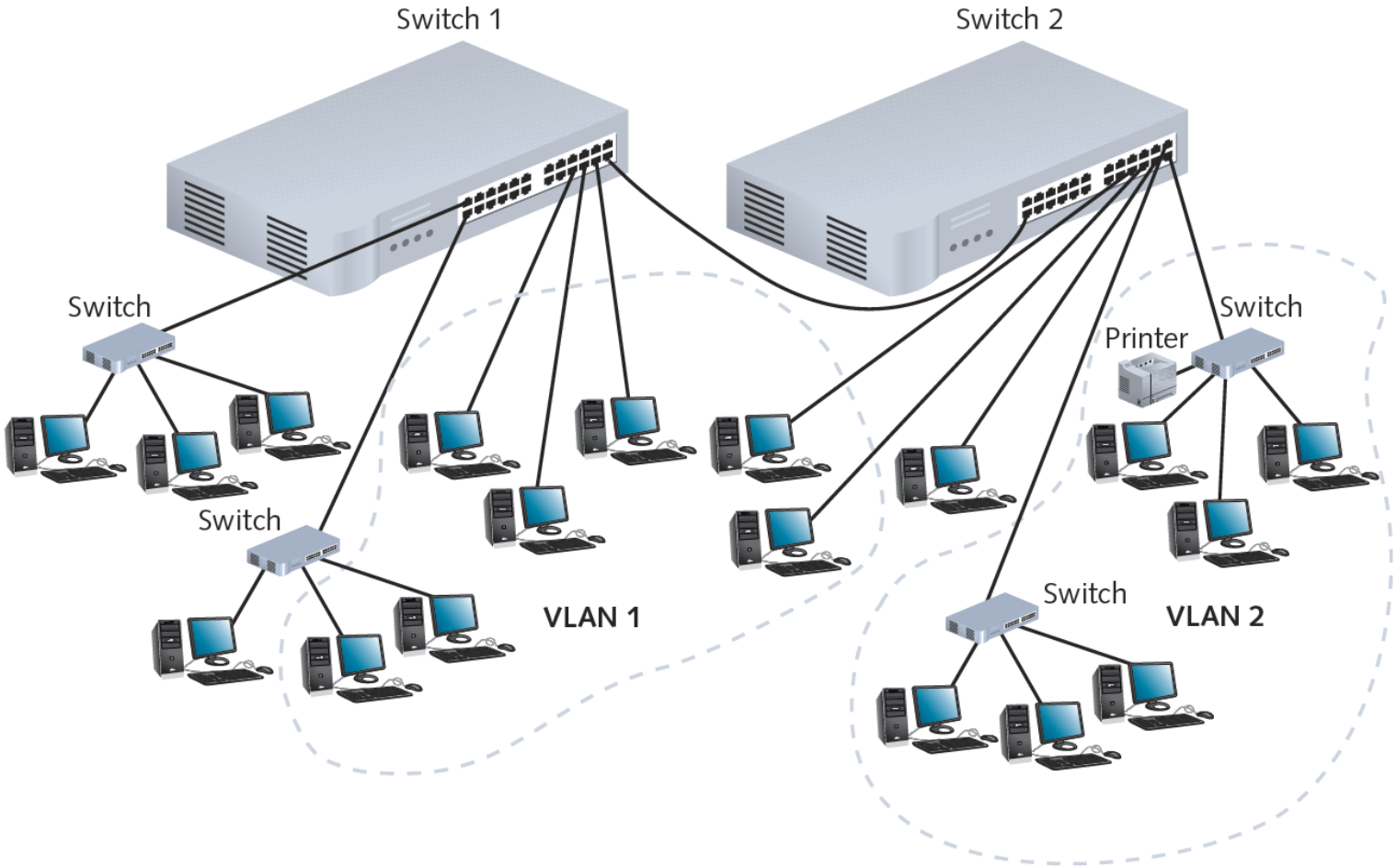
Switches

- Connectivity devices that subdivide a network
  - Segments
- Traditional switches
  - Operate at Data Link OSI model layer
- Modern switches
  - Can operate at Layer 3 or Layer 4
- Switches interpret MAC address information
- Common switch components
  - Internal processor, operating system, memory, ports

VLANs

- VLANs (virtual local area networks)
  - Logically separate networks within networks
    - Groups ports (physical) into broadcast domain
- Broadcast domain
  - Port combination making a Layer 2 segment
  - Ports rely on Layer 2 device to forward broadcast frames
- Collision domain
  - Ports in same broadcast domain could have collisions
  - Switches take care of this issue – each port is a separate collision domain

VLAN Example



Source: Course Technology / Cengage Learning

VLANs (cont'd)

- Advantages of VLANs
  - Flexible
    - Ports from multiple switches or segments
    - Use any end node type
  - Reasons for using VLANs
    - Separating user groups
    - Isolating connections
    - Identifying priority device groups
    - Grouping legacy protocol devices
    - Separating large network into smaller subnets

VLANs (cont'd)

- Typical switch pre-configuration
  - One default VLAN
  - Cannot be deleted or renamed
- Creation of additional VLANs
  - Indicate to which VLAN each port belongs
  - Additional specifications
    - Security parameters, filtering instructions, port performance requirements, network addressing and management options
- VLAN configurations are maintained using switch's software (OS)

VLANs and Trunking

- Potential problem
  - Group of nodes getting cut off from rest of network
    - Fix by using a router or Layer 3 switch
- Trunking
  - Switch's interface carries traffic of multiple VLANs
  - Typically used to interconnect multiple switches
- Trunk
  - Single physical connection between switches
- VLAN data separation
  - Frame contains VLAN identifier in header

Host Based Firewalls

- Each individual host has its own firewall
  - Closer to the data to be protected
  - Avoids the “chewy on the inside” problem in that you still have a boundary between each machine and even the local network
- Potential issues
  - More difficult to manage
  - Can be subverted by malicious applications (false sense of security)

Application Firewall (Proxy)

- No direct flow of traffic
  - Connection is made to proxy with application protocol
  - Proxy makes similar request to the server on the outside
- Advantage
  - Can’t hide attacks by disguising as different protocol
  - But can still encapsulate attack
- Disadvantage
  - Cannot support end-to-end encryption because packets must be interpreted by the proxy and recreated

Attack Vectors

- Trojan Horse
  - Extra code added manually to web page, program, plugin, etc.
- Viruses
  - Self-propagating (on execution)
  - Contains a malicious payload
- Worms
  - Self-propagating through process exploit.
  - Contains a malicious payload
- Penetration Tools (remote or local)
  - Exploits vulnerabilities to violate policy
  - Injection, Overrun, Logic, other
- Impersonation / Insider

General Actions - Payloads

- Modification of data
- Spying - exfiltration
- Stepping off point for further attacks
- Advertising – and tracking interests
- Self Preservation - Rootkits
- Subversion

Defenses to Malicious Code

- Detection
  - Virus scanning
  - Intrusion Detection
- Least Privilege
  - Don’t run as root
  - Separate users ID’s
- Isolation
  - Mandatory controls on information flow
- Sandboxing
  - Limit what the program can do
- Backup
  - Keep something stable to recover

Categorizing Malicious Code

- How does it propogate??
- Trojan Horses
  - Embedded in useful program that others will want to run.
  - Covert secondary effect
- Viruses
  - Tries to propagate itself when the program is started
- Worms
  - Exploits vulnerabilities (bugs) to infect running programs
  - Infection is immediate

Trojan Horses

- People use programs because of a desired and documented effect
- Malicious payload
  - An “undocumented” activity that might be counter to the interests of the user
- Examples: Some viruses; much spyware
- Issues: How do you get a user to run your program?
  - Software that doesn’t come from a reputable source may embed trojans
  - Program with same name as one commonly used can be inserted in search path
  - Depending on settings, visiting a web site or reading an email may cause a program to execute

Zombies / Bots

- Machines controlled remotely
  - Infected by virus, worm, or trojan
  - Can be contacted by master / control server
  - May make calls out so control is possible even through firewall
  - Often uses IRC for control

Spyware

- Infected machines collect data
  - Keystroke monitoring
  - Screen scraping
  - History of URL's visited
  - Scans disk for credit cards and passwords
  - Allows remote access to data
  - Sends data to third party
- Spyware can be local
  - Targeted ads
  - Revenue for referring victim to merchant
  - Might rewrite URL's to steal commissions

Malicious Code - Defenses

- Detection
  - Signature-based
  - Activity-based
- Prevention
  - Prevent certain actions in an environment
  - Take action based on detection
- Sandbox
  - Limits access of running program
  - Program doesn’t have full access or even user-level access
- Detect Modifications
  - Signed executables
  - Tripwire or similar

Root Kits - Subversion

- Hide traces of infection or control
  - Intercept systems calls
  - Return false information that hides the malicious code
  - Return false information to hide effect of malicious code.
  - Some root kits have countermeasures to attempts to detect the root kits
  - “Blue Pill”

Types of Hackers

- White Hat
  - Ethical hacker
  - Trained penetration testers
- Black Hat
  - Malicious attacker
  - “Script Kiddies”?
- Grey Hat
  - Violates laws and ethical standards, but no malicious intent

White Hat

- Permission to engage by organization or customer
  - Always discloses found vulnerabilities
- Techniques
  - Penetration Testing
  - Email Phishing
  - Denial-of-service (DoS) Attack
  - Social Engineering
  - Security Scanning
    - Vulnerability scanners (Nessus)
    - Web Application Vulnerability Scanners (Acunetix / Netsparker)
    - Nikto
    - Metasploit

Black Hat

- Has malicious intent
  - Does not request permission to find vulnerabilities
  - Does not disclose vulnerabilities when found
- Can be skilled hackers or “script kiddies”
  - Title has more to do with intent than ability
  - Traditionally Black Hat hackers referred to skilled malicious actors
- Use same techniques as White Hat hackers
- Often develop specialties
  - Command and control of remote assets
  - (spear)Phishing campains
  - Malicious software development

Black Hat - Organized

- Types of organizations
  - Criminal
  - Nation-state
- Resources
  - Training
  - Sales (partners / resellers / vendors)
  - Call centers
  - International
- Goals:
  - Data exfiltration
  - Extortion
  - Botnets (crypto-mining or DoS for hire)

Grey Hat

- Intent is “typically” not malicious
  - Does not request permission to find vulnerabilities
  - Sometimes discloses vulnerabilities when found
- Can be skilled hackers or “script kiddies”
- Use same techniques as White / Black Hat hackers
- Differences
  - Sometimes violates ethical standards, but without malicious intent
  - Could be attempting to collect a fee for patching vulnerabilities
    - Businesses can decide to seek prosecution
  - Exploitation of vulnerability could be for a “good” cause

Why Pen Test?

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- Compliance
  - Some industries have specific frameworks that they must adhere to legally
    - Payment card industry (PCI DSS)
    - North American utility companies (NERC CIP)
    - Medical Industry (HIPAA)
    - Department of Defense (CMMS [Cybersecurity Maturity Model Certification])
  - Other organizations may have a self imposed compliance requirement
    - Good publicity
    - ISO 27001
    - NIST-CSF
- Risk Management
  - Cybersecurity insurance will often require penetration testing
  - Acceptable risks can be calculated if needed
- Baselines
  - Regular penetration tests can serve as baselines for needed remediations
  - Set future architecture roadmaps
- Stay informed!

Penetration Testing Types

- White Box
  - Internal structure of network environment is known
  - Tester can view source code and have access to applications and systems
  - Test from developer's / administrators point of view
- Black Box
  - Internal structure is unknown for network environment
  - Little to no information provided to testers
  - Can most closely resemble external actors
    - Time restraints are different
- Grey Box
  - Combination of white box and black box
  - Tester can partially "see" inner working of a network environment
    - Allows for more of the network to be tested within a given time frame
    - Tester granted some permissions or internal access on the network
  - Typically where most penetration tests land

Penetration Testing Stages

- Planning (scoping)
- Reconnaissance
- Gaining Access (exploitation) – Lateral Movement
- Maintaining Access / Escalation
- Analysis / Reporting
- Remediation

Rules of Engagement

- Rules of Engagement (ROE)
  - Written document that specifies the scope and allowable actions during a penetration test
  - Specifies level of communication during engagement
- Type and scope of engagement
  - White box / black box / grey box
  - What attack surfaces can be tested
  - What methods are allowed?
    - Intrusive vs. non-intrusive
    - Physical vs remote engagements
- Client contact details
  - Who knows about the testing?
  - Who should be contacted and in what order?
  - Preferred methods of communication

Rules of Engagement

- IT Team Notifications
  - When should the IT team be engaged?
  - Establish levels of criticality
- Sensitive data
  - Special provisions for regulated data (e.g. HIPAA)
- Meetings and report
  - Pre-determined meeting dates and frequency
  - What types of reports are needed (e.g. technical, executive, sanitized)

Rules of Engagement

- Hours of engagement
  - 24/7
  - After-hours only
  - Who needs to know these?
- Handling of a sensitive / critical vulnerability
- Essential to legally protect penetration testers

Reconnaissance

- Goals
  - Discover attack surfaces (physical and network)
  - Discover overall cybersecurity environment
  - Gain information to assist with vulnerability exploitation
- Publicly available information
  - Company employee directories
  - Whois information
  - DNS information
  - ARIN
- Physical visits
  - What can be learned about the facilities?
  - Lobby officers?
  - Server room locations?
  - Access control?

Reconnaissance (cont'd)

- Social engineering
  - Tailgating
  - Phishing
  - Discover overall cybersecurity environment
  - Gain information to assist with vulnerability exploitation
- Social media or other employee profiles
  - Potential usernames
  - Potential passwords
  - Vacations
  - Insider information
  - Many of this information can help to impersonate individuals

NMAP

- GUI Available
  - Zenmap
- Options
  - Port Scanning
    - Default: Scans the most common 1,000 ports for each protocol
    - Fast flag: Scan the 100 most common
  - Ping Scanning
    - IP address ranges
    - Subnet masks
    - Single IPs
  - Host Scans
    - Sends ARP requests (MAC address collection)
    - DNS queries
    - Latency information
  - Output to files

NMAP (cont'd)

- Port scans
  - TCP SYN: TCP handshake is not completed (avoids suspicion)
  - TCP connect: TCP handshake is completed (more reliable)
  - UDP: Identify DNS, SNMP, and DHCP ports
    - Frequently targeted by hackers
- OS Scans
  - Uses TCP and UDP Ports
  - Compares responses to database of over 2500 operating systems
    - Can return information about OS and version for each host

Masscan

- Two types of port scanners
  - Synchronous (connection-oriented)
    - Send request to target port and waits for response or time-out
    - Slower
    - More accurate
  - Asynchronous (connectionless
    - Does not wait for response prior to sending out next port probe
    - Less accurate – can't detect dropped packets
- Masscan is incredibly fast (asynchronous scanner)
  - Can facilitate DoS attacks
  - Said to be able to scan the entire internet in 6 minutes
    - 10 million packets per second

Example Questions

Correctly order the layers of the TCP / IP Model (5 pts):

TCP / IP Model

Transport

Internet

Application

Network Access

Example Questions

A network that connects two states would commonly be known as a ____ network? (3 pts)

A) Wide Area
B) Hub Area
C) Metropolitan Area
D) Local Area

Which of the answers listed below refers to a secure replacement for Telnet? (2 pts)

A) TFTP
B) SSH
C) CHAP
D) SNMP

Which of the following is a system of mappings of domain names to various data, including numerical IP addresses? (2 pts)

A) TCP/IP
B) SQL
C) DNS
D) DHCP

Example Questions

What is the foundation for defining a secure system? (5 pts)

As the administrator of a mail server? What are some of the tasks you are responsible for configuring and discuss how one or more of these tasks is related to network security? (10 pts)

What layer of the OSI model does a network router function? (5 pts)