CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

Common Ports and DNS

Chris Samayoa

Week 4 – 1st Lecture
2/8/2022

Course Information

- 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
  - Other times by appointment only

Objectives

- Review well-known ports for key TCP/IP services
- Describe the purpose and implementation of DNS (Domain Name System)

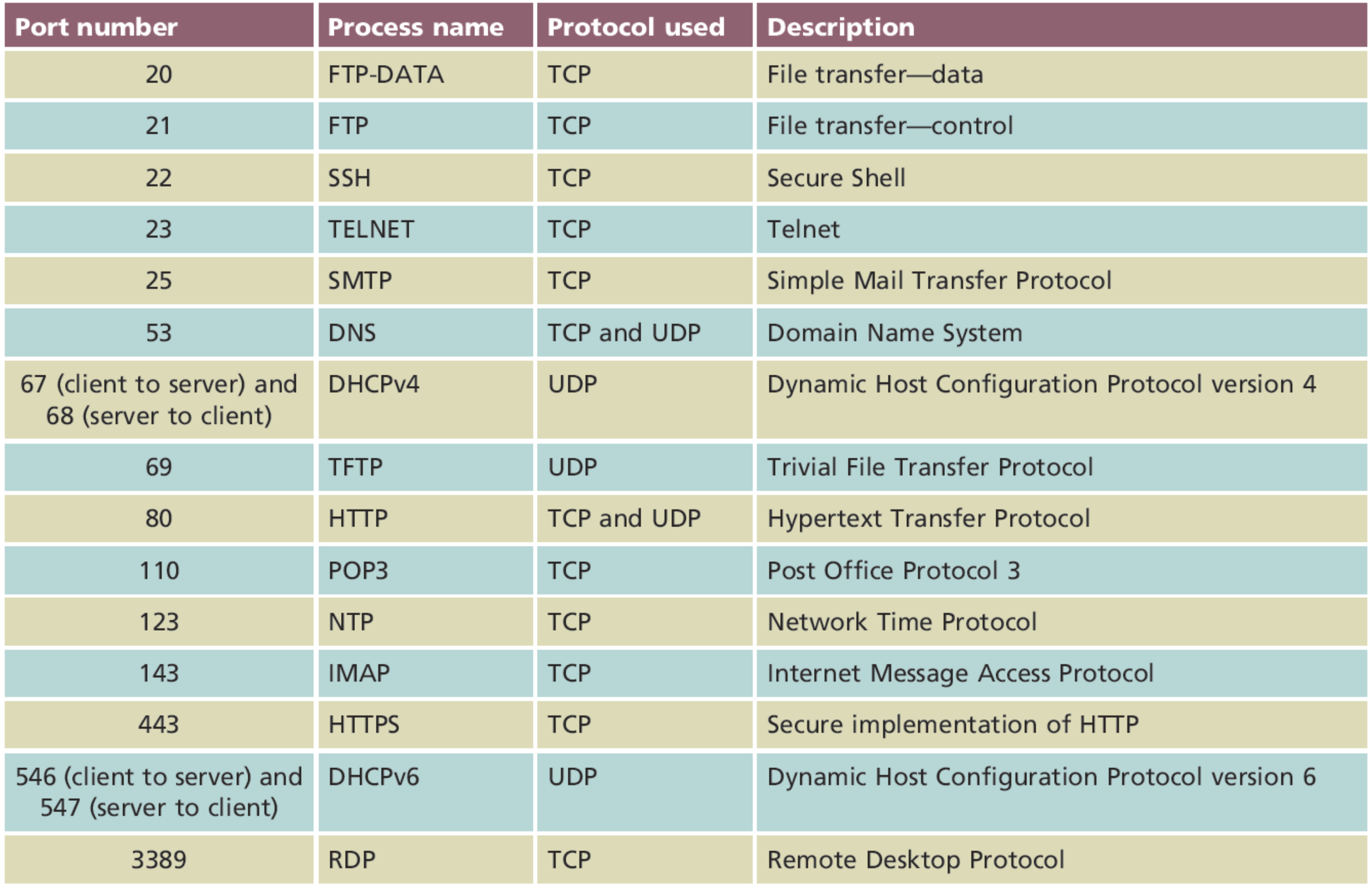
Sockets and Ports

- 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 Names and DNS

- IP addressing
  - Long, complicated numbers
  - Good for computers
- Easier for people to use words
  - Internet authorities established internet node naming system
- Host
  - Networked device
- Host name
  - Name describing device

Domain Names

- Domain
  - Group of computers belonging to the same organization
- Domain name
  - Identifies domain (e.g. abc.com)
  - Associated with company, university, government organization
  - Can be local/private or public
- Fully qualified domain name (FQDN)
  - Local host name + domain name
  - e.g. host1.abc.com

Domain Names (cont’d)

- Label (character string)
  - Separated by dots
  - Represents level in domain naming hierarchy
- Example: www.google.com
  - Top-level domain (TLD): com
  - Second-level domain: google
  - Third-level domain (aka. sub-domain): www
- May contain multiple third-level domains
- ICANN established domain naming conventions

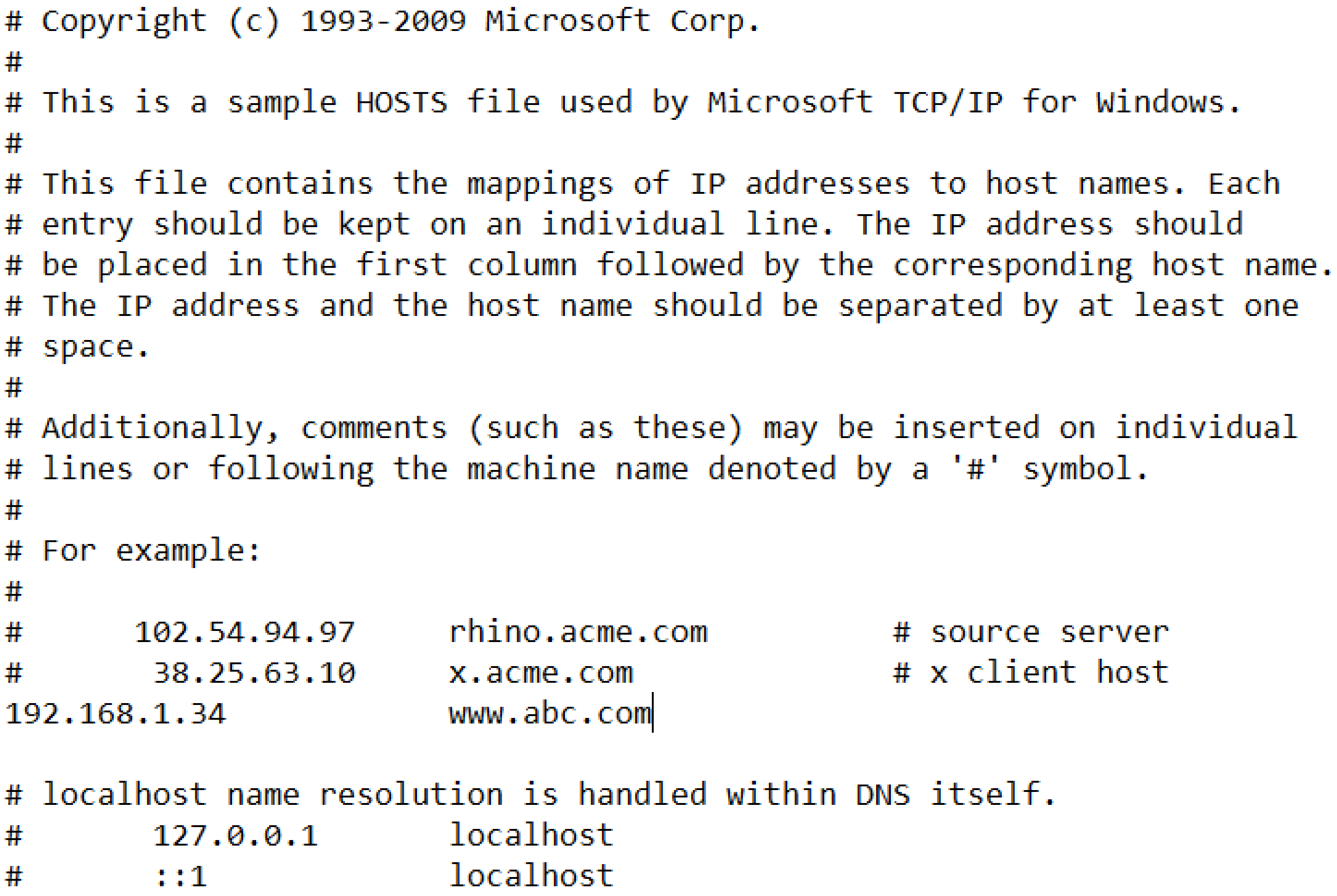
Domain Names (cont'd)

- ICANN has approved 255 country codes
- Host and domain names restrictions
    - Any alphanumeric combination up to 253 characters
    - Include hyphens, underscores, periods in name
    - No other special characters

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



```
# 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

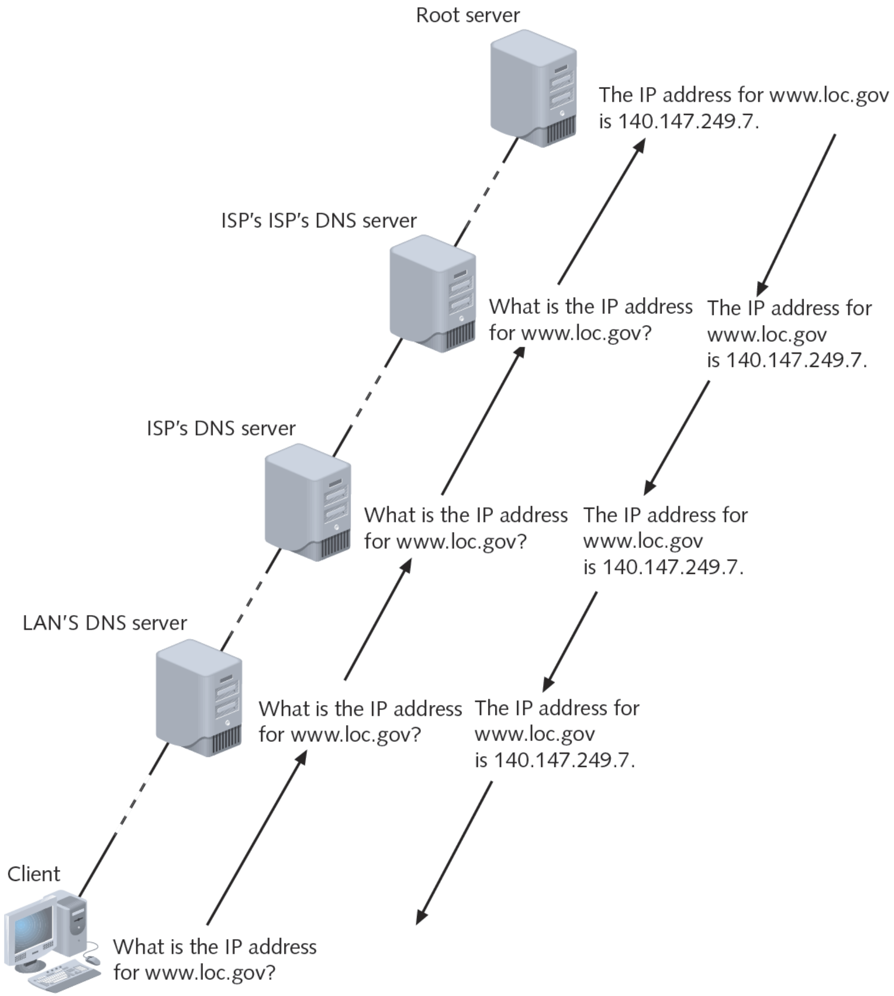
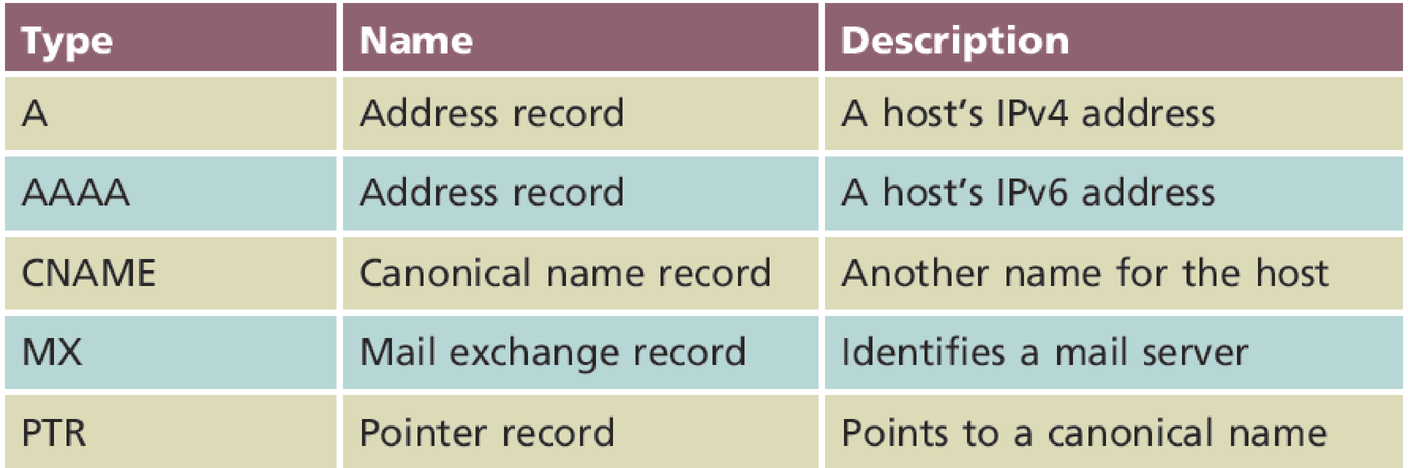

Root server
The IP address for www.loc.gov is 140.147.249.7.
ISP's ISP's DNS server
What is the IP address for www.loc.gov?
The IP address for www.loc.gov is 140.147.249.7.
ISP's DNS server
What is the IP address for www.loc.gov?
The IP address for www.loc.gov is 140.147.249.7.
LAN'S DNS server
What is the IP address for www.loc.gov?
The IP address for www.loc.gov is 140.147.249.7.
Client
What is the IP address for www.loc.gov?

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

Configuring DNS

- Large organizations
  - Often maintain multiple name servers
    - Primary and secondary designations
  - Ensures internet availability of translation
- DHCP service assigns clients appropriate addresses
- Manual configuration is also possible
  - Static often used for publically available DNS
  - Private networks often rely on a combination of manual (static) and automatic configurations

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

Summary

- Knowledge of common TCP/IP ports is essential for understanding network security
- DNS tracks domain names and their respective IP addresses

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

Network Security Principles

Chris Samayoa

Week 4 – 1st Lecture
2/8/2022

Objectives

- Overview of Network Security fundamentals
- Attacker motivations and types

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

Attackers

- Motivation(s)
  - Bragging Rights
  - Revenge / to inflict damage
  - Terrorism and extortion
  - Financial / criminal enterprises
  - Nation State objectives
- Risk to attacker
  - Organizations can play defensive roles
  - Effective attribution

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

Summary

- Security Triad = Confidentiality, Integrity, and Availability (CIA)
- Security policy defines acceptable use of system
- Security mechanisms enforce the policy
- Attackers have various different motivations