

Chapter 2: TCP/IP Concepts Review

Objectives

Describe the TCP/IP protocol stack
 Explain the basic concepts of IP addressing
 Explain the binary, octal, and hexadecimal numbering system

Overview of TCP/IP

Protocol

- Common language used by computers for speaking

Transmission Control Protocol/Internet Protocol (TCP/IP)

- Most widely used protocol

TCP/IP stack

- Contains four different layers
 - Network
 - Internet
 - Transport
 - Application

The Application Layer

Front end to the lower-layer protocols

What you can see and touch – closest to the user at the keyboard
 HTTP, FTP, SMTP, SNMP, SSH, IRC and TELNET all operate in the Application Layer

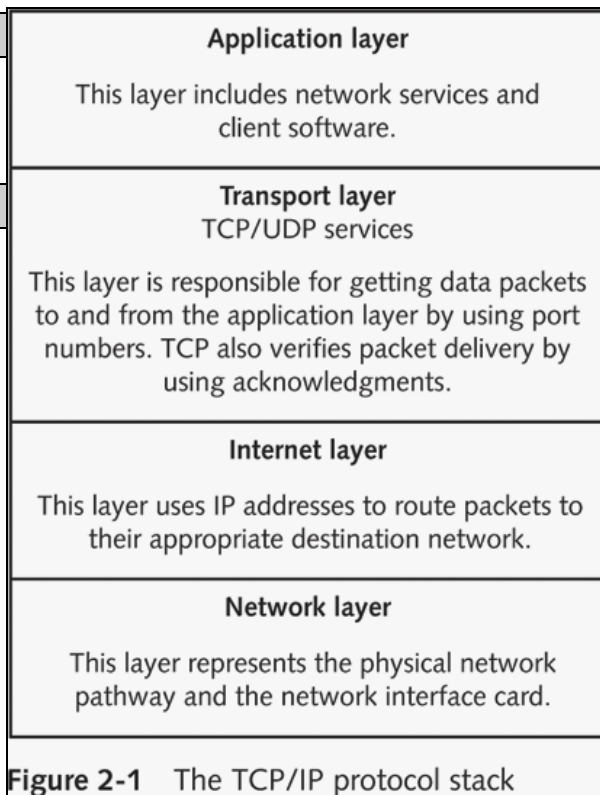


Figure 2-1 The TCP/IP protocol stack

Table 2-1 Application layer programs

Application	Description
Hypertext Transfer Protocol (HTTP)	The primary protocol used to communicate over the World Wide Web (see RFC-2616 at www.ietf.org for details)
File Transfer Protocol (FTP)	Allows different operating systems to transfer files between one another
Simple Mail Transfer Protocol (SMTP)	The main protocol for transmitting e-mail messages across the Internet
Simple Network Management Protocol (SNMP)	Primarily used to monitor devices on a network, such as remotely monitoring a router's state
Secure Shell (SSH)	Enables a remote user to log on to a server and issue commands
Internet Relay Chat (IRC)	Enables multiple users to communicate over the Internet in discussion forums
Telnet	Enables users to remotely log on to a server

The Transport Layer

Encapsulates data into segments

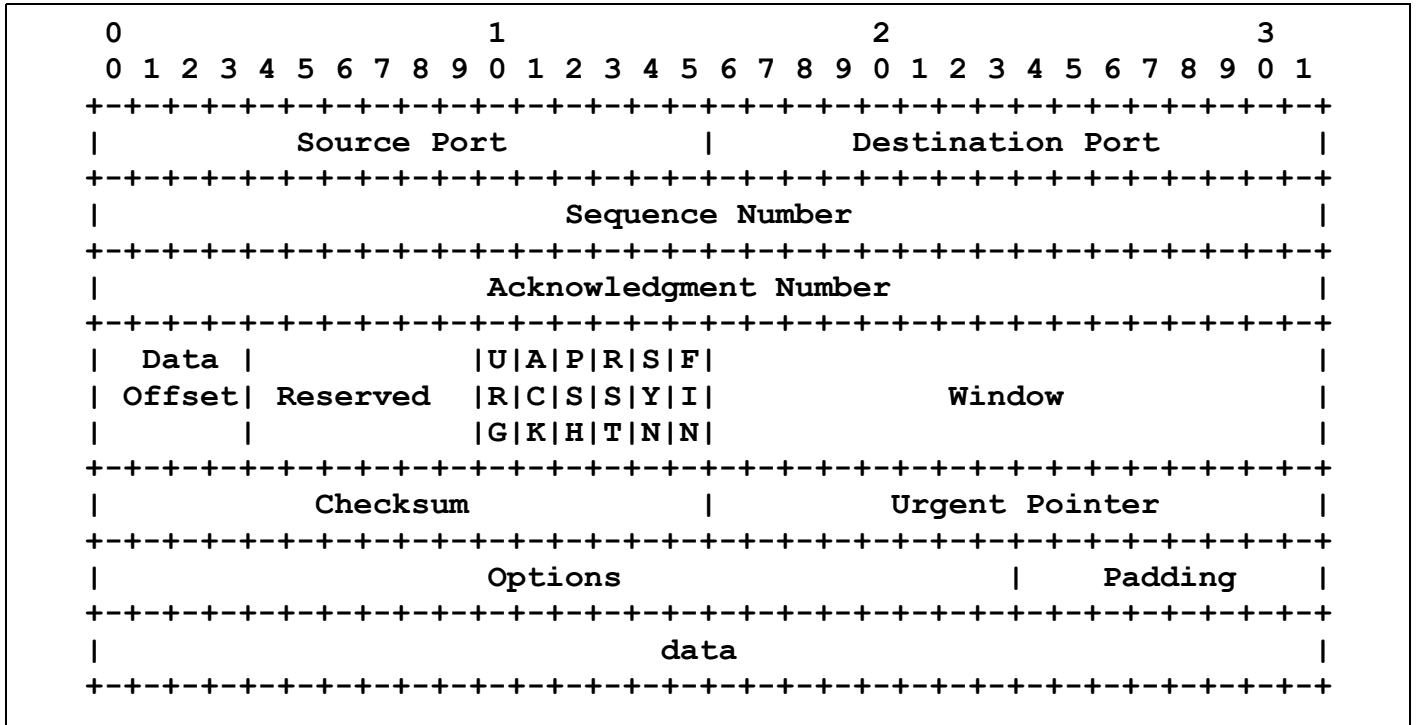
Segments can use TCP or UDP to reach a destination host

- TCP is a connection-oriented protocol

TCP three-way handshake

- Computer A sends a SYN packet
- Computer B replies with a SYN-ACK packet
- Computer A replies with an ACK packet

TCP Header Format



TCP Segment Headers

Critical components:

- TCP flags
- Initial Sequence Number (ISN)
- Source and destination port

Abused by hackers finding vulnerabilities

TCP Flags

Each flag occupies one bit

Can be set to 0 (off) or 1 (on)

Six flags

- SYN: synchronize, (not synthesis) flag
- ACK: acknowledge flag
- PSH: push flag
- URG: urgent flag
- RST: reset flag
- FIN: finish flag
- Error in textbook on page 22: SYNchronize, not SYNthesis (link Ch 2a, RFC 793)

Initial Sequence Number (ISN)

32-bit number

Tracks packets received

Enables reassembly of large packets

Sent on steps 1 and 2 of the TCP three-way handshake

- By guessing ISN values, a hacker can hijack a TCP session, gaining access to a server without logging in

Chapter 2: TCP/IP Concepts Review

TCP Ports

Port

- Logical, not physical, component of a TCP connection
- Identifies the service that is running
- Example: HTTP uses port 80

A 16-bit number – 65,536 ports

Each TCP packet has a source and destination port

Blocking Ports

Helps you stop or disable services that are not needed

- Open ports are an invitation for an attack

You can't block all the ports

- That would stop all networking
- At a minimum, ports 25 and 80 are usually open on a server, so it can send out Email and Web pages

Only the first 1023 ports are considered well-known

List of well-known ports

- Available at the Internet Assigned Numbers Authority (IANA) Web site (www.iana.org)

Ports 20 and 21

- File Transfer Protocol (FTP)
- Use for sharing files over the Internet
- Requires a logon name and password
- More secure than Trivial File Transfer Protocol (TFTP)

Port 25

- Simple Mail Transfer Protocol (SMTP)
- E-mail servers listen on this port

Port 53

- Domain Name Service (DNS)
- Helps users connect to Web sites using URLs instead of IP addresses

Port 69

- Trivial File Transfer Protocol
- Used for transferring router configurations

Port 80

- Hypertext Transfer Protocol (HTTP)
- Used when connecting to a Web server

Port 110

- Post Office Protocol 3 (POP3)
- Used for retrieving e-mail

Port 119

- Network News Transfer Protocol
- For use with newsgroups

Port 135

- Remote Procedure Call (RPC)
- Critical for the operation of Microsoft Exchange Server and Active Directory

Port 139

- NetBIOS
- Used by Microsoft's NetBIOS Session Service
- File and printer sharing

Port 143

- Internet Message Access Protocol 4 (IMAP4)
- Used for retrieving e-mail
- More features than POP3

Chapter 2: TCP/IP Concepts Review

Demonstration

Telnet to hills.ccsf.edu and netstat to see the connections

- Port 23 (usual Telnet)
- Port 25 blocked off campus, but 110 connects
- Port 21 works, but needs a username and password

```
C:\ Command Prompt
E:\Documents and Settings\Sam>telnet hills.ccsf.edu 110
```

```
C:\ Command Prompt
E:\Documents and Settings\Sam>netstat -n

Active Connections

Proto Local Address           Foreign Address         State
TCP   127.0.0.1:1047          127.0.0.1:1048        ESTABLISHED
TCP   127.0.0.1:1048          127.0.0.1:1047        ESTABLISHED
TCP   192.168.2.14:1129      72.5.124.55:80        CLOSE_WAIT
TCP   192.168.2.14:1130      208.59.201.18:80      CLOSE_WAIT
TCP   192.168.2.14:1175      147.144.1.2:110       ESTABLISHED
```

Demonstration

Wireshark Packet Sniffer

- TCP Handshake: SYN, SYN/ACK, ACK
 - TCP Ports
 - TCP Status
- Flags

o	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.14	82.165.134.55	TCP	1157 > http [SYN] Seq=0
2	0.100187	82.165.134.55	192.168.2.14	TCP	http > 1157 [SYN, ACK]
3	0.100281	192.168.2.14	82.165.134.55	TCP	1157 > http [ACK] Seq=1
4	0.100656	192.168.2.14	82.165.134.55	HTTP	GET /235/s214.html HTTP
5	0.214045	82.165.134.55	192.168.2.14	TCP	http > 1157 [ACK] Seq=1
6	0.218748	82.165.134.55	192.168.2.14	TCP	[TCP segment of a reass
7	0.220002	82.165.134.55	192.168.2.14	TCP	[TCP segment of a reass

⊕	Frame 1 (62 bytes on wire, 62 bytes captured)
⊕	Ethernet II, Src: AcctonTe_0e:5c:8a (00:10:b5:0e:5c:8a), Dst: BelkinCo_02
⊕	Internet Protocol, Src: 192.168.2.14 (192.168.2.14), Dst: 82.165.134.55 (
⊖	Transmission Control Protocol, Src Port: 1157 (1157), Dst Port: http (80)
	Source port: 1157 (1157)
	Destination port: http (80)
	Sequence number: 0 (relative sequence number)
	Header length: 28 bytes
⊖	Flags: 0x02 (SYN)
	0... .. = Congestion window Reduced (CWR): Not set
	.0.. .. = ECN-Echo: Not set
	..0. = Urgent: Not set
	...0 = Acknowledgment: Not set
 0... = Push: Not set
0.. = Reset: Not set
1. = Syn: Set
0 = Fin: Not set
	window size: 16384
	checksum: 0x6033 [correct]
⊕	Options: (8 bytes)

Chapter 2: TCP/IP Concepts Review

User Datagram Protocol (UDP)

Fast but unreliable protocol

Operates on transport layer

Does not need to verify whether the receiver is listening

Higher layers of the TCP/IP stack handle reliability problems

Connectionless protocol

The Internet Layer

Responsible for routing packets to their destination address

Uses a logical address, called an IP address

IP addressing packet delivery is connectionless

Internet Control Message Protocol (ICMP)

Operates in the Internet layer of the TCP/IP stack

Used to send messages related to network operations

Helps in troubleshooting a network

Some commands include

- Ping
- Traceroute

Table 2-2 ICMP type codes

ICMP Type Code	Description
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
8	Echo
9	Router Advertisement
10	Router Solicitation

Wireshark Capture of a PING

Warriors of the Net

Network+ Movie

Warriorsofthe.net (link Ch 2d)

No.	Time	Source	Destination	Protocol	Info
1	0.00	192.168.2.14	192.168.2.30	ICMP	Echo (ping) request
2	0.00	192.168.2.30	192.168.2.14	ICMP	Echo (ping) reply

⊕	Frame 1 (74 bytes on wire, 74 bytes captured)
⊕	Ethernet II, Src: AcctonTe_0e:5c:8a (00:10:b5:0e:5c:8a), Dst: Trigem
⊕	Internet Protocol, Src: 192.168.2.14 (192.168.2.14), Dst: 192.168.2.
⊖	Internet Control Message Protocol
	Type: 8 (Echo (ping) request)
	Code: 0
	Checksum: 0x405c [correct]
	Identifier: 0x0400
	Sequence number: 0x0900
	Data (32 bytes)

IP Addressing

Consists of four bytes, like 147.144.20.1

Two components

- Network address
- Host address
- Neither portion may be all 1s or all 0s

Classes

- Class A
- Class B
- Class C

Table 2-3 TCP/IP address classes

Address Class	Range	Address Bytes	Number of Networks	Host Bytes	Number of Hosts
Class A	1-127	1	127	3	16,777,214
Class B	128-191	2	16,128	2	65,534
Class C	192-223	3	2,097,152	1	254

Chapter 2: TCP/IP Concepts Review

Class A

- First byte is reserved for network address
- Last three bytes are for host address
- Supports more than 16 million host computers
- Limited number of Class A networks
- Reserved for large corporations and governments (see link Ch 2b)
- Format: *network.node.node.node*

Class B

- First two bytes are reserved for network address
- Last two bytes are for host address
- Supports more than 65,000 host computers
- Assigned to large corporations and Internet Service Providers (ISPs)
- Format: *network.network.node.node*
 - CCSF has 147.144.0.0 – 147.144.255.255

Class C

- First three bytes are reserved for network address
- Last byte is for host address
- Supports up to 254 host computers
- Usually available for small business and home networks
- Format: *network.network.network.node*

Subnetting

- Each network can be assigned a subnet mask
- Helps identify the network address bits from the host address bits

Class A uses a subnet mask of 255.0.0.0

- Also called /8

Class B uses a subnet mask of 255.255.0.0

- Also called /16

Class C uses a subnet mask of 255.255.255.0

- Also called /24

Planning IP Address Assignments

Each network segment must have a unique network address

Address cannot contain all 0s or all 1s

To access computers on other networks

- Each computer needs IP address of **gateway**

TCP/IP uses subnet mask to determine if the destination computer is on the same network or a different network

- If destination is on a different network, it relays packet to gateway
- Gateway forwards packet to its next destination (routing)
- Packet eventually reaches destination

Overview of Numbering Systems

Binary

Octal

Hexadecimal

Reviewing the Binary Numbering System

Uses the number 2 as its base

Binary digits (bits): 0 and 1

Byte

- Group of 8 bits
- Can represent $2^8 = 256$ different values

UNIX and Linux Permissions

UNIX and Linux File permissions are represented with bits

Chapter 2: TCP/IP Concepts Review

- 0 means removing the permission
- 1 means granting the permission
- 111 (rwx) means all permissions apply

Examples of Determining Binary Values

Each position represents a power of 2 value

- Usually the bit on the right is the less significant bit

Converting 1011 to decimal

- $1 \times 2^0 = 1$
- $1 \times 2^1 = 2$
- $0 \times 2^2 = 0$
- $1 \times 2^3 = 8$
- $1 + 2 + 8 = 11$ (decimal value)

Understanding Nibbles

Half a byte or four bits

Helps with reading the number by separating the byte

- 1111 1010

Components

- High-order nibble (left side)
- Low-order nibble (right side)

Understanding Nibbles (continued)

Converting 1010 1010 to decimal

- Low-order nibble
 - $1010 = 10$ (base 10)
- Multiply high-order nibble by 16
 - $1010 = 10 \times 16 = 160$ (base 10)
- $160 + 10 = 170$ (base 10)

Reviewing the Octal Numbering System

Uses 8 as its base

- Supports digits from 0 to 7

Octal digits can be represented with three bits

Permissions on UNIX

- Owner permissions (rwx)
- Group permissions (rwx)
- Other permissions (rwx)
- Example: 111 101 001
 - Octal representation 751

Reviewing the Hexadecimal Numbering System

Uses 16 as its base

- Support numbers from 0 to 15

Hex number consists of two characters

- Each character represents a nibble
- Value contains alphabetic letters (A ... F)
 - A representing 10 and F representing 15

Sometimes expressed with "0x" in front

If you want more about binary, see Link Ch 2c