THOMSON COURSE TECHNOLOGY

Network+ Guide to Networks, Fourth Edition

Chapter 4
Network Protocols

Objectives

- Identify the characteristics of TCP/IP, IPX/SPX, NetBIOS, and AppleTalk
- Understand how network protocols correlate to layers of the OSI Model
- Identify the core protocols of the TCP/IP suite and describe their functions
- Identify the well-known ports for key TCP/IP services

Objectives (continued)

- Understand addressing schemes for TCP/IP, IPX/SPX, NetBEUI, and AppleTalk
- Describe the purpose and implementation of DNS (Domain Name System) and WINS (Windows Internet Naming Service)
- Install protocols on Windows XP clients

Introduction to Protocols

- Protocols vary according to purpose, speed, transmission efficiency, utilization of resources, ease of setup, compatibility, and ability to travel between different LANs
- Multiprotocol networks: networks running more than one protocol
- Most popular protocol suite is TCP/IP
  - Others: IPX/SPX, NetBIOS, and AppleTalk

TCP/IP (Transmission Control Protocol/Internet Protocol)

- Suite of specialized subprotocols
  - TCP, IP, UDP, ARP, and many others
- De facto standard on Internet
  - Protocol of choice for LANs and WANs
- Protocols able to span more than one LAN are routable
- Can run on virtually any combination of NOSs or network media
- TCP/IP core protocols operate in Transport or Network layers

The TCP/IP Core Protocols: TCP (Transmission Control Protocol)

- Provides reliable data delivery services
  - Operates in Transport layer
  - Connection-oriented
  - Ensures reliable data delivery through sequencing and checksums
  - Provides flow control
- Port hosts address where an application makes itself available to incoming or outgoing data

The TCP/IP Core Protocols: TCP (continued)

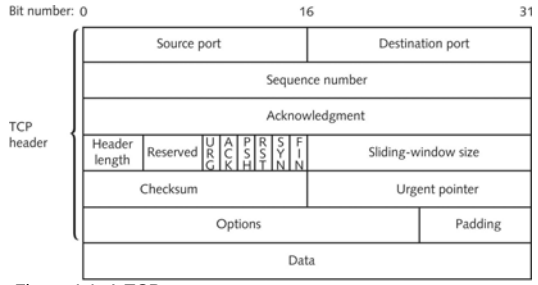

Figure 4-1: A TCP segment

The TCP/IP Core Protocols: TCP (continued)

```
Transmission Control Protocol, Src Port: http (80), Dst Port: 1958 (1958), Seq: 3043958669, Ack: 937013559, Len: 0
    Source port : http (80)
    Destination port: 1958 (1958)
    Sequence number: 3043958669
    Acknowledgment number: 937013559
    Header length: 24 bytes
⊞ Flags:_ 0xx0012 (SYN, ACK)
      0... .... = Congestion Window Reduced (CWR): Not set
      .0.. .... = ECN-Echo: Not set
      ..0. .... = Urgent: Not set
      ...1 .... = Acknowledgment: Set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..1. = Syn: Set
      .... ...0 = Fin: not set
    window size: 5840
    Checksum: 0x206a (correct)
⊞ Options: (4bytes)
    Maximum segment size: 1460 bytes
```

Figure 4-2: TCP segment data

The TCP/IP Core Protocols: TCP (continued)

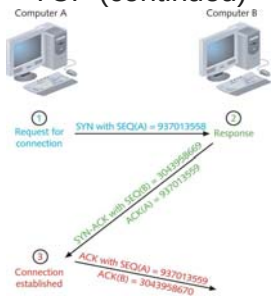

Figure 4-3: Establishing a TCP connection

UDP (User Datagram Protocol)

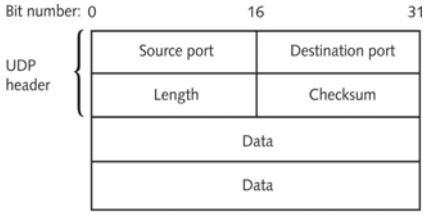

Figure 4-4: A UDP segment

IP (Internet Protocol)

- Provides information about how and where data should be delivered
  - Data's source and destination addresses
  - Network layer protocol
  - Enables TCP/IP to internetwork
  - Unreliable, connectionless protocol
- IP datagram: packet, in context of TCP/IP
  - Envelope for data

IP (continued)

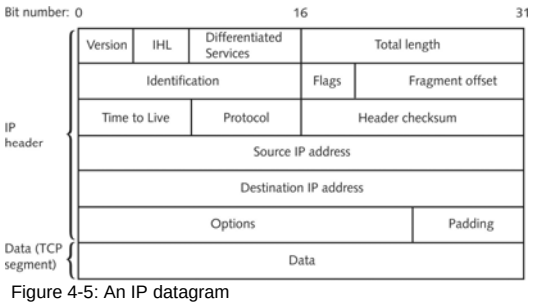

Figure 4-5: An IP datagram

IP (continued)

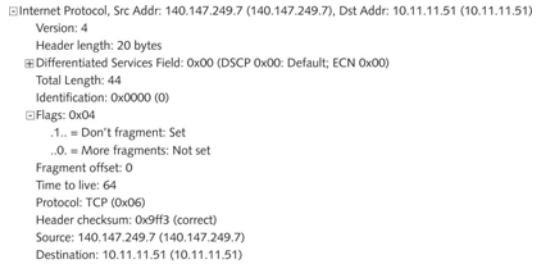

Figure 4-6: IP datagram data

ICMP (Internet Control Message Protocol)

- Network layer protocol that reports on success or failure of data delivery
  - Indicates when part of network congested
  - Indicates when data fails to reach destination
  - Indicates when data discarded because allotted time for delivery (TTL) expired
  - Cannot correct errors it detects

IGMP (Internet Group Management Protocol)

- Network layer protocol that manages multicasting
  - Transmission method allowing one node to send data to defined group of nodes
    - Point-to-multipoint method
    - Teleconferencing or videoconferencing over Internet
- Routers use IGMP to determine which nodes belong to multicast group and to transmit data to all nodes in that group

ARP (Address Resolution Protocol)

- Network layer protocol
  - Obtains MAC (physical) address of host
    - Creates database that maps MAC address to host's IP (logical) address
- ARP table or cache: local database containing recognized MAC-to-IP address mappings
  - Dynamic ARP table entries created when client makes ARP request that cannot be satisfied by data already in ARP table
  - Static ARP table entries entered manually using ARP utility

RARP (Reverse Address Resolution Protocol)

- Allows client to broadcast MAC address and receive IP address in reply
  - If device doesn't know own IP address, cannot use ARP
- RARP server maintains table of MAC addresses and associated IP addresses

Addressing in TCP/IP

- IP core protocol responsible for logical addressing
  - IP Address: unique 32-bit number
    - Divided into four octets separated by periods
    - 0 reserved as placeholder referring to entire group of computers on a network
    - 255 reserved for broadcast transmissions

Addressing in TCP/IP (continued)

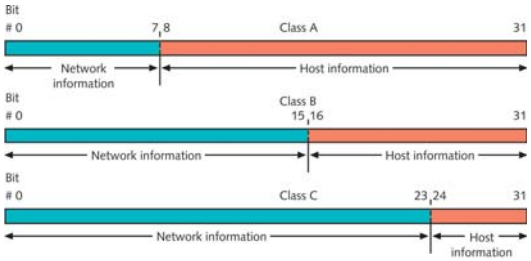

Figure 4-8: IP addresses and their classes

Addressing in TCP/IP (continued)

- Many Internet addresses go unused
  - Cannot be reassigned because they are reserved
  - IP version 6 (IPv6) will incorporate new addressing scheme
- Some IP addresses reserved for special functions
  - 127 reserved for a device communicating with itself
    - Loopback test
- ipconfig: Windows XP command to view IP information
  - ifconfig on Unix and Linux

Binary and Dotted Decimal Notation

- Most common way of expressing IP addresses
  - Decimal number between 0 and 255 represents each binary octet
  - Separated by period
- Each number in dotted decimal address has binary equivalent

Subnet Mask

- Every device on TCP/IP-based network identified by subnet mask
  - 32-bit number that, when combined with device's IP address, informs rest of network about segment or network to which a device is attached
- Subnetting: subdividing single class of networks into multiple, smaller logical networks or segments

Assigning IP Addresses

- Nodes on a network must have unique IP addresses
- Static IP address: manually assigned
  - Can easily result in duplication of addresses
- Most network administrators rely on network service to automatically assign IP addresses

BOOTP (Bootstrap Protocol)

- Uses central list of IP addresses and associated devices' MAC addresses to assign IP addresses to clients dynamically
  - Dynamic IP addresses
  - Application layer protocol
  - Client broadcasts MAC address, BOOTP server replies with:
    - Client's IP address
    - IP address of server
    - Host name of server
    - IP address of a default router

DHCP (Dynamic Host Configuration Protocol)

- Automated means of assigning unique IP address to every device on a network
  - Application layer protocol
  - Reduces time and planning spent on IP address management
  - Reduces potential for errors in assigning IP addresses
  - Enables users to move workstations and printers without having to change TCP/IP configuration
  - Makes IP addressing transparent for mobile users

DHCP (continued)

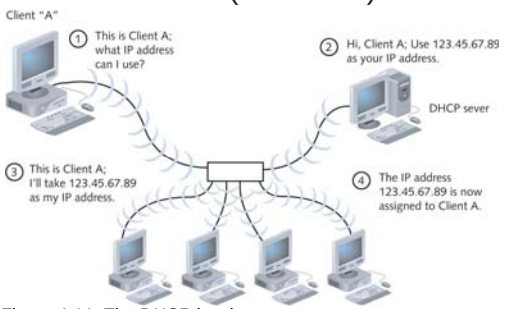

Figure 4-11: The DHCP leasing process

APIPA (Automatic Private IP Addressing)

- Provides computer with IP address automatically
  - For Windows 98, Me, 2000, XP client and Windows 2003 server
  - For situations where DHCP server unreachable
  - Assigns computer's network adapter IP address from predefined pool of addresses
    - 169.254.0.0 through 169.254.255.255
  - Computer can only communicate with other nodes using addresses in APIPA range

Sockets and Ports

- Every process on a machine assigned a port number 0 to 65535
- Process's port number plus host machine's IP address equals process's socket
  - Ensures data transmitted to correct application
- Well Known Ports: in range 0 to 1023
  - Assigned to processes that only the OS or system administrator can access

Sockets and Ports (continued)

- Registered Ports: in range 1024 to 49151
  - Accessible to network users and processes that do not have special administrative privileges
- Dynamic and/or Private Ports: in range 49152 through 65535
  - Open for use without restriction

Addressing in IPv6

- IPv6 slated to replace current IP protocol, IPv4
  - More efficient header, better security, better prioritization
  - Billions of additional IP addresses
- Differences:
  - Address size
  - Representation
  - Distinguishes among different types of network interfaces
  - Format Prefix

Host Names and DNS (Domain Name System): Domain Names

- Every host can take a host name
- Every host is member of a domain
  - Group of computers belonging to same organization and has part of their IP addresses in common
  - Domain name usually associated with company or other type of organization
- Fully qualified host name: local host name plus domain name
- Domain names must be registered with an Internet naming authority that works on behalf of ICANN

Host Files

- ASCII text file called HOSTS.TXT
  - Associate host names with IP addresses
  - Growth of Internet made this arrangement impossible to maintain

# IP address	host name	alias
132.55.78.109	bingo.games.com	bingo
132.55.78.110	parcheesi.games.com	parcheesi
132.55.78.111	checkers.games.com	checkers
132.55.78.112	darts.games.com	darts

Figure 4-13: Example host file

DNS (Domain Name System)

- Hierarchical method of associating domain names with IP addresses
  - Refers to Application layer service that accomplishes association and organized system of computers and databases making association possible
  - Relies on many computers around world
- Thirteen root servers
- Three components:
  - Resolvers
  - Name servers
  - Name space

DNS (continued)

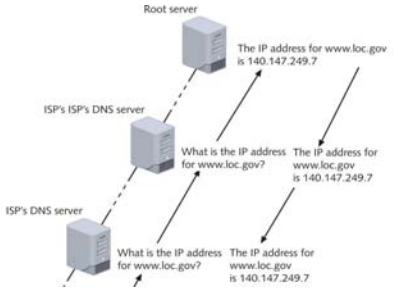

Figure 4-14: Domain name resolution

DNS (continued)

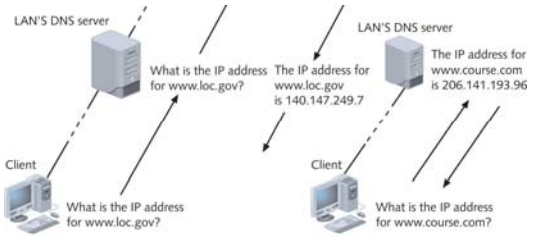

Figure 4-14 (continued): Domain name resolution

DDNS (Dynamic DNS)

- DNS is reliable as long as host's address is static
  - Many Internet users subscribe to type of Internet service in which IP address changes periodically
- In DDNS, service provider runs program on user's computer that notifies service provider when IP address changes
  - DNS record update effective throughout Internet in minutes

Zeroconf (Zero Configuration)

- Collection of protocols designed by IETF to simplify setup of nodes on TCP/IP networks
  - Assigns IP address
  - Resolves node's host name and IP address without requiring DNS server
  - Discovers available services
  - Enables directly connected workstations to communicate without relying on static IP addressing
  - IP addresses are assigned through IPv4LL (IP version 4 Link Local)

Some TCP/IP Application Layer Protocols

- Telnet: terminal emulation protocol used to log on to remote hosts using TCP/IP protocol suite
  - TCP connection established
  - Keystrokes on user's machine act like keystrokes on remotely connected machine
- FTP (File Transfer Protocol): Application layer protocol used to send and receive files via TCP/IP
  - Server and clients
  - FTP commands work from OS's command prompt
  - Anonymous logons

Some TCP/IP Application Layer Protocols (continued)

- Trivial File Transfer Protocol (TFTP): enables file transfers between computers
  - Simpler than FTP
  - Relies on UDP at Transport layer
    - Connectionless
- Network Time Protocol (NTP): Application layer protocol used to synchronize clocks of computers
- Network News Transfer Protocol (NNTP): facilitates exchange of newsgroup messages between multiple servers and users

Some TCP/IP Application Layer Protocols (continued)

- Packet Internet Groper (PING): utility that can verify that TCP/IP is installed, bound to the NIC, configured correctly, and communicating
- Pinging:
  - Echo request and echo reply
  - Can ping either an IP address or a host name
  - Pinging loopback address, 127.0.0.1, to determine whether workstation's TCP/IP services are running
  - Many useful switches
    - e.g., -?, -a, -n, -r

IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange)

- Required to ensure interoperability of LANs running NetWare versions 3.2 and lower
  - Replaced by TCP/IP on Netware 5.0 and higher

The IPX and SPX Protocols

- Internetwork Packet Exchange (IPX): provides logical addressing and internetworking services
  - Operates at Network layer
  - Similar to IP
  - Connectionless
- Sequenced Packet Exchange (SPX): Works with IPX to ensure data received whole, in sequence, and error free
  - Belongs to Transport layer
  - Connection-oriented

Addressing in IPX/SPX

- Each node on network must be assigned unique address
  - IPX address
    - Network address: chosen by network administrator
    - Node address: by default equal to network device's MAC address

NetBIOS and NetBEUI

- NetBIOS originally designed to provide Transport and Session layer services for applications running on small, homogenous networks
- Microsoft added standard Transport layer component called NetBEUI
  - Efficient on small networks
    - Consumes few network resources
    - Provides excellent error correction
  - Does not allow for good security
  - Few possible connections
  - Cannot be routed

Addressing in NetBEUI

- Network administrators must assign NetBIOS name to each workstation
- After NetBIOS has found workstation's NetBIOS name, it discovers workstation's MAC address
  - Uses this address in further communications

WINS (Windows Internet Naming Service)

- Provides means to resolve NetBIOS names to IP addresses
  - Used exclusively with systems using NetBIOS
    - Microsoft Windows
- Automated service that runs on a server
- Guarantees unique NetBIOS name used for each computer on network
- Clients do not have to broadcast NetBIOS names to rest of network
  - Improves network performance

AppleTalk

- Protocol suite originally designed to interconnect Macintosh computers
  - Can be routed between network segments and integrated with NetWare-, UNIX-, Linux-, or Microsoft-based networks
- AppleTalk network separated into logical groups of computers called AppleTalk zones
  - Enable users to share file and printer resources
- AppleTalk node ID: Unique 8- or 16-bit number that identifies computer on an AppleTalk network

Binding Protocols on a Windows XP Workstation

- Windows Internet Naming Service (WINS): process of assigning one network component to work with another
- Core Network and Transport layer protocols normally included with OS
  - When enabled, attempt to bind with network interfaces on computer
- For optimal network performance, bind only protocols absolutely needed
- Possible to bind multiple protocols to same network adapter

Summary

- Protocols define the standards for communication between nodes on a network
- TCP/IP is most popular protocol suite, because of its low cost, open nature, ability to communicate between dissimilar platforms, and routability
- TCP provides reliability through checksum, flow control, and sequencing information
- IP provides information about how and where data should be delivered
- Every IP address contains two types of information: network and host

Summary (continued)

- Subnetting is implemented to control network traffic and conserve a limited number of IP addresses
- Dynamic IP address assignment can be achieved using BOOTP or the more sophisticated DHCP
- A socket is a logical address assigned to a specific process running on a host
- IPv6 provides several other benefits over IPv4
- A domain is a group of hosts that share a domain name and have part of their IP addresses in common

Summary (continued)

- DNS is a hierarchical way of tracking domain names and their addresses
- IPX/SPX is a suite of protocols that reside at different layers of the OSI Model
- NetBEUI is a protocol that consumes few network resources, provides error correction, and requires little configuration
- WINS is a service used on Windows systems to map IP addresses to NetBIOS names
- AppleTalk is the protocol suite originally used to interconnect Macintosh computers