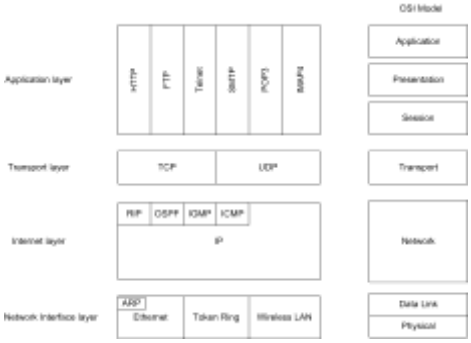
Network communication protocols

- Establish the rules and formats that are followed for communication between networks and nodes
- Formats data into packets
- Media access method sends packets

TCP/IP architecture



Network Interface layer protocols

Protocol	Description
802.3	Ethernet
802.5	Token Ring
802.11	Wireless LAN
802.15	Wireless personal area network

Address Resolution Protocol (ARP)

- Convert logical IP addresses to physical MAC addresses
- Reverse Address Resolution Protocol (RARP) converts physical MAC addresses to logical IP addresses
- Operate at the OSI Data Link layer

MAC address filter

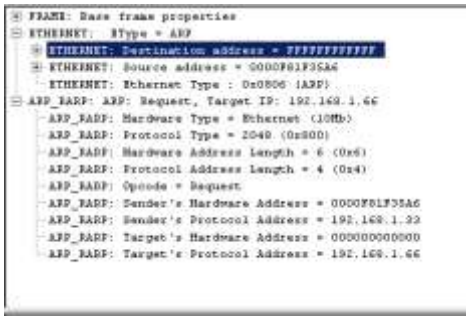
- NICs use a MAC address to filter irrelevant packets
- When a packet is received, the NIC verifies that the destination MAC address matches the MAC address of the network card or is a broadcast MAC address
- This process offloads analyzing packets from IP to NIC
- Reduces CPU utilization on the computer

Data packet addresses

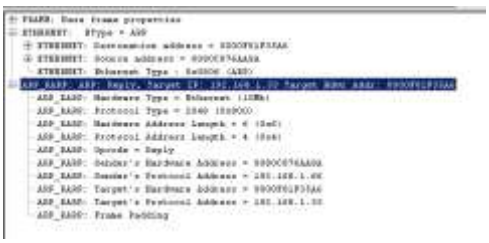
- Four addresses
  - Source IP address
  - Destination IP address
  - Source MAC address
  - Destination MAC address
- Uses ARP to find MAC address of destination
  - A two-packet process

ARP request and reply

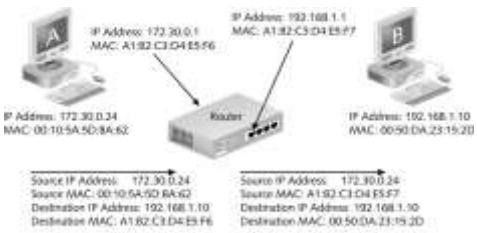
ARP Request packet structure



ARP Reply packet structure



Router forwarding



IPCONFIG

- Command-line utility
- Retrieves a computer's IP configuration
- Optional switches
  - /all
- Help
  - /?

Internet Layer protocols

- Responsible for all tasks related to logical addressing
- Each Internet layer protocol is very specialized
- Includes
  - IP
  - RIP
  - OSPF
  - ICMP
  - IGMP
  - SSH

Internet Protocol (IP)

- Unreliable connectionless protocol
- Functions at the OSI Network layer
- Sole function is to transmit TCP, UDP, and other higher-level protocols
- Responsible for the logical addressing of each outgoing packet
- Verifies incoming packets are addressed to computer
- Must have a Transport layer service to work with

RIP/RIPv2 and OSPF

- Routing Information Protocol (RIP)
- Newer version RIPv2
- Open Shortest Path First (OSPF)
- Routing protocols
- Responsible for defining how internetwork paths are chosen
- Define how routers can share network information
- Operate at the OSI Network Layer

ICMP/ICMPv6

- Internet Control Messaging Protocol (ICMP)
- Newer version ICMPv6
- Used to send IP error and control messages between routers and hosts
- Operates at OSI Network layer
- Most common use of ICMP is ping

IGMP

- Internet Group Management Protocol (IGMP)
- Used for the management of multicast groups
- Hosts and routers both use IGMP
- Operates at OSI Network layer

SSH

- Secure Shell (SSH)
- Exchanges data between two network nodes over a secure channel
- Operates at the OSI Network layer
- Designed as a replacement for Telnet and other insecure remote shells
- SSH encryption provides data confidentiality and integrity over an insecure network
- Primary use is on Linux and Unix systems to access shell accounts

Transport layer protocols

- Responsible for getting data ready to move across the network
- Breaks message down into smaller pieces called packets
- Two Transport layer protocols:
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
- Use port numbers
- Combination of IP address and port number is referred to as a socket

Service port numbers

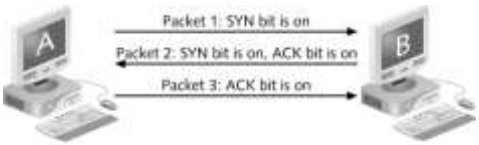
Service	Port
FTP	TCP 21, 20
SSH	TCP 22 UDP 22
Telnet	TCP 23
SMTP	TCP 25
DNS	TCP 53 UDP 53
BOOTP and DHCP	UDP 67, 68
Trivial FTP (TFTP)	UDP 69

Service	Port
HTTP	TCP 80
POP3	TCP 110
NNTP	TCP 119
NTP	UDP 123
IMAP	TCP 143 UDP 143
SNMP	TCP 161 UDP 161
Secure HTTP	TCP 443

TCP

- Standard protocol used to transmit information across the Internet
- Provides
  - Acknowledged, connection-oriented communications
  - Guaranteed delivery
  - Proper sequencing
  - Data integrity checks

TCP three-way handshake



Microsoft Network Monitor

- Simple, software-based protocol analyzer
- Available for download from Microsoft
- Capture and then analyze data

UDP

- User Datagram Protocol (UDP)
- Connectionless, unacknowledged communications
- Simply sends information
- Not as commonly used as TCP
- Operates at OSI Transport layer
- Using IP, adds information about the source and destination socket identifiers
- Used for streaming audio and video, online games

Application layer protocols

- Accepts information from applications on the computer
- Sends information to the requested service provider
- Only available on TCP/IP networks
- Each application layer protocol is associated with a client application and service

HTTP

- Hypertext Transfer Protocol (HTTP)
- Most common protocol used on the Internet
- Used by Web browsers and Web servers
- Defines the commands that Web browsers can send and how Web servers are capable of responding
- Can upload information using HTTP

HTTP, continued

- Mechanisms for passing data:
  - Common Gateway Interface (CGI)
  - Internet Server Application Programmer Interface (ISAPI)
  - Netscape Server Application Programmer Interface (NSAPI)
- HTTPS connections
  - Secure Web servers use SSL (Secure Sockets Layer)
  - Create an encrypted communication channel
  - SSL is a public-key/private-key encryption protocol
  - https:// instead of http://
  - Secure HTTP (S-HTTP) secures individual data packets

FTP

- File Transfer Protocol (FTP)
- Simple file-sharing protocol
- Includes commands for
  - Uploading files
  - Downloading files
  - Requesting directory listings
- Transfers binary files over the Internet without encoding and decoding
- Trivial File Transfer Protocol (Trivial FTP or TFTP)
  - Has fewer commands than FTP
  - Can be used only to send and receive files
  - Can be used for multicasting

Telnet

- Terminal emulation protocol
- Primarily used to remotely connect to UNIX and Linux Systems
- Specifies how telnet server and telnet clients communicate
- Telnet support only text-based interface

NTP

- Network Time Protocol (NTP)
- Time synchronization system for computer clocks through the Internet network
- Provides mechanisms to synchronize time and coordinate time distribution
- Operates at rates from mundane to light wave
- Uses a returnable time design

E-mail messaging protocols

- Simple Mail Transfer Protocol (SMTP)
  - Used to send and receive e-mail between e-mail servers
  - Also used by e-mail clients to send messages to the server
  - Never used to retrieve e-mail
- Post Office Protocol version 3 (POP3)
  - Most common protocol for retrieving e-mail messages
  - Has commands to download and delete messages from the mail server
  - Doesn't support sending messages

continued

E-mail protocols, continued

- Internet Message Access Protocol version 4 (IMAP4)
  - Used to retrieve e-mail messages
  - More features than POP3. Examples
    - Can choose which messages to download
    - Allows for multiple folders on the server side to store messages

Topic B

- Topic A: The TCP/IP protocol suite
- Topic B: TCP/IP
- Topic C: DHCP servers

IPv4

- Internet standard since September 1981
- Binary data – two states: on (1) off (0)
- Byte (or octet) – a string of eight bits
- IPv4 address – 32 bits divided into four octets
- Two notations for IPv4
  - Binary:
    11001010 00101101 11100001 00001111
  - Decimal: 208.206.88.56

continued

IPv4, continued

- Can uniquely identify up to 2^{32} addresses
- IP addresses composed of two parts
  - Network ID
  - Host ID
- No two computers on the same network can have the same host ID
- Two computers on different networks can have the same host ID

Classful IPv4 addresses

Class	Addresses	Description
A	1.0.0.0 to 126.0.0.0	First octet is network ID Last three octets are Host ID Default subnet mask is 255.0.0.0
B	128.0.0.0 to 191.255.0.0	First two octets are network ID Last three octets are Host ID Default subnet mask is 255.255.0.0
C	192.0.0.0 to 223.255.255.0	First three octets are network ID Last octet is Host ID Default subnet mask is 255.255.255.0
D	224.0.0.0 to 239.0.0.0	Multicasting addresses
E	240.0.0.0 to 255.0.0.0	Experimental use

Subnet masks

- Use to identify network ID and host ID portions of IP address

IP address	Subnet mask	Host ID	Network ID
192.168.100.33	255.255.255.0	192.168.100.0	0.0.0.33
172.16.43.207	255.255.0.0	172.16.0.0	0.0.43.207

Network IDs

- Always contiguous and start on the left

Valid subnet masks	Invalid subnet masks
255.0.0.0	0.255.255.255
255.255.0.0	255.0.255.0
255.255.255.0	255.255.0.255

Special addresses

- Reserved addresses ~ 18 million
- Multicast addresses ~ 16 million
- "This network" = 0.0.0.0
- Local loopback address = 127.0.0.1
- Broadcast address
  - Sends information to all machines on a subnet
  - Is the last address in the range belonging to the subnet
  - On a Class A, B, or C subnet, the broadcast address always ends in 255

CIDR

- Classless Inter-Domain Routing (CIDR)
- Implemented in 1993
- Alleviates problem of too few addresses
- Allows you to use variable-length subnet masking (VLSM) to create addresses beyond IPv4 classes
- Group addresses together in CIDR blocks

CIDR address

- Written in the standard 4-part dotted decimal
- Followed by /N
  - N is a number from 0 to 32
  - N is the prefix length
- Prefix is the number of bits (starting at the left of the address) that make up the shared initial bits

NAT

- Network Address Translation (NAT)
- Modifies network address information in the packets it transmits from an internal network onto the Internet
- Use a single public address
- Route all internal Internet traffic through single public IPv4 address
- All internal host have private IPv4 addresses
- Protection built-in: NAT-enabled firewalls

APIPA

- Private IP Addressing (APIPA)
- 169.254.0.0 network
- Windows OSes, Windows Server 2000 forward, autogenerate APIPA addresses

IPv6

- Internet Protocol version 6 (IPv6)
- Uses128-bit addresses
- Provides 2^{128} addresses
- Eight 6-bit fields
- Write as eight groups of four numbers in hexadecimal notation separated by colons
  - Replace group of all zeros by two colons
  - Only one :: can be used per address
  - Can drop leading zeros in a field
  - All fields require at least one number, except for the :: notation

continued

IPv6, continued

- Network portion indicated by a slash followed by the number of bits in the address that are assigned to the network portion
  - /48
  - /64
- Loopback address is a localhost address
- IPv6 loopback address can be written as ::/128
- fe80::/10 is equivalent to the IPv4 169.254.0.0

IPv6 address types

- Link-local
  - IPv6 version of IPv4's APIPA
  - Self-assigned using Neighbor Discovery process
  - Starts with fe80::
- Site-local
  - IPv6 version of IPv4 private address
  - Begins with FE
  - C to F for the third hex digit—FEC, FED, FEE, or FEF

continued

IPv6 address types, continued

- Global unicast
  - IPv6 version of an IPv4 public address
  - Identified for a single interface
  - Routable and reachable on the IPv6 Internet
  - First three bits are 001 in binary.
  - All global addresses start with the binary values 001 (2000::/3) through 111 (E000::/3)
  - Exception FF00::/8, reserved for multicasts
  - Following 48 bits designate global routing prefix
  - Next 16 bits designate the subnet ID
  - Last 64 bits identify the individual network node

continued

IPv6 address types, continued

- Multicast
  - Sends information or services to all interfaces that are defined as members of the multicast group
  - First 16 bits ff00n = multicast address
- Anycast
  - New, unique type of address in IPv6
  - Cross between unicast and multicast
  - Identifies a group of interfaces
  - Packets are delivered to the nearest interface as identified by the routing protocol distance measurement

IPv6 address scopes

- Define regions
- Also known as spans
- Unique identifiers of an interface
- Scopes include
  - Link local
  - Site network
  - Global network.
- A device usually has a link-local and either a site-local or global address
- Network address can be assigned to a scope zone
  - Zone index suffix follows %

Subnet masks

- Used to determine local or remote network communications

IPv4 custom subnets

- Borrow host bits to add to network bits
- Keep it simple – borrow in groups of eight
- Subnets with all 1s and 0s are discarded
- Complex subnetting takes less than a full octet from host bits
- Calculate the number of subnets using the formula 2^n-2

IPv6 subnets

- Follows similar rules as IPv4
- Subnet masks are denoted as fs
  If you had an IPv6 address of
  - fec0:0000:0000:0000:0220:edff:fe6a:0f76

  A subnet mask of
  - ffff:ffff:ffff:ffff:0000:0000:0000:0000

  You get a network address of
  - **fec0:0000:0000:0000**:0000:0000:0000:0000

  You get a host address of
  - 0000:0000:0000:0000:**0220:edff:fe6a:0f76**
- Designate subnet mask in CIDR format
  - *IPv6-Node-Address/Prefix-Length*

IPv6 custom subnets

- Subnet ID or Site-Level Aggregator 16-bit field allows you to configure up to 65,535 individual subnets
- All 16 bits to zero creates a single network
- Use all 16 bits to perform the equivalent of subnetting under IPv4, by assigning a different Subnet ID to each subnet, up to 65,536
- Use the 16 bits to create a multiple-level hierarchy of subnets
  - Similar to Variable Length Subnet Masking in IPv4

  For example
  - First two bits to create four subnets
  - Next three bits to create eight sub-subnets in some or all of the first four subnets
  - 11 more bits to create sub-sub-subnets

Default gateway

- Term for TCP/IP router
- Hosts use default gateway to deliver packets to remote networks
- Routers
  - Often dedicated hardware devices
  - Sometimes computer with multiple NICs
  - Supports IPv4, IPv6, or both
  - Move packets between networks
  - Has an IP address for every network it's attached to

Routing example

Address translation

- Port Address Translation (PAT)
  - Translates TCP or UDP communications between private network hosts and public network hosts
  - Allows a single public IP address to be used by many hosts on a private network
- Source network address translation (SNAT)
  - Process used by router or firewall
  - Rewrites source and destination addresses of IP packets as they pass through

DNS

- Domain Name System (DNS)
  - Resolves host names to IP addresses
  - Finds domain controllers
  - Locates resources on the Internet
- FQDN has two parts
  - Host name
  - Domain name

DNS namespace

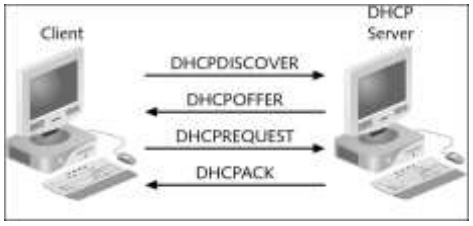
Static TCP/IP configuration

- Manually entered on each network device
- Pitfalls
  - Time consuming
  - Error-prone
  - Making changes is not an efficient process
- NETSH can be used to control TCP/IP parameters

DHCP and DHCPv6

- Dynamic Host Configuration Protocol (DHCP)
- Automated mechanism to assign IP addresses to clients
- Two versions
  - Original DHCP used for IPv4 addressing
  - Dynamic Host Configuration Protocol for IPv6 (DHCPv6) used for IPv6 addressing
- Can hand out IP addresses plus other TCP/IP configuration parameters
- Lease is on a time limit

IPv4 lease process



IPv6 lease process

- Network devices autoconfigure when connected to a routed IPv6 network
- Process
  1. Performs stateless address autoconfiguration
  2. Sends link-local multicast router solicitation request for configuration parameters
  3. Router responds with a router advertisement packet containing network configuration parameters flags

IPv6 router flags

- Managed Address Configuration Flag (M flag)
  - When set to 1, device should use DHCPv6 to obtain a stateful IPv6 address
- Other Stateful Configuration Flag (O flag)
  - When set to 1, device should use DHCPv6 to obtain other TCP/IP configuration settings

M and O flags

- Both M and O flags are 0
  - No DHCPv6 server
  - Device uses router advertisement to obtain a non-link-local address
  - Device uses other methods, such as manual configuration, to configure other IPv6 configuration parameters
- Both M and O flags are 1
  - Device should obtain both an IPv6 address and other configuration parameters from DHCPv6 server
  - DHCPv6 stateful addressing

continued

M and O flags, continued

- M flag is 0 and O flag is 1
  - Device should use its stateless autoconfiguration IPv6 address
  - Device should retrieve other configuration parameters from the DHCPv6 server
  - DHCPv6 stateless addressing
- M flag 1 and O flag is 0
  - Device should obtain an IPv6 address from a DHCPv6 server
  - Doesn't obtain other TCP/IP configuration parameters
  - Combination is rarely used

Topic C

- Topic A: The TCP/IP protocol suite
- Topic B: TCP/IP
- Topic C: DHCP servers

Installing a DHCP server

- Standard networking service included with Windows Server 2008
- Not installed by default
- Install manually using the Add Roles feature in Server Manager
- In domain environment must be authorized in Active Directory
- Non-authorized servers shut down and log an event error

IPv6 scopes

- Consecutive range of IPv6 addresses for DHCP server to lease
- Configure IPv6 scope after DHCP installation
- Configure using DHCP Administrative Tools utility
- Specify only subnet prefix
- DHCPv6 automatically creates IPv6 addresses within subnet

DATA COMMUNICATIONS AND COMPUTER NETWORKS

Unit summary

- Described the functions of the protocols in the TCP/IP protocol suite
- Configured TCP/IP
- Installed and configured DHCP and DHCPv6