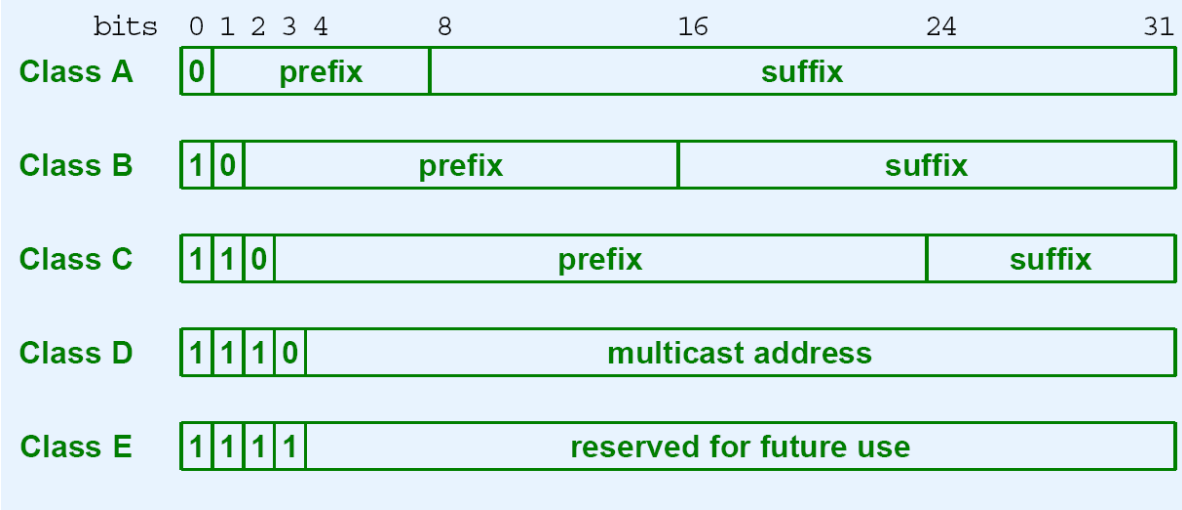
IP Address Assignment

An IP address does not identify a specific computer. Instead, each IP address identifies a connection between a computer and a network. A computer with multiple network connections (e.g., a router) must be assigned one IP address for each connection.

IP Address Details

- Divided into two parts
  - Prefix identifies network
  - Suffix identifies host
- Global authority assigns unique prefix to network
- Local administrator assigns unique suffix to host

Original Classes Of Addresses



- Initial bits determine class
- Class determines boundary between prefix and suffix

Dotted Decimal Notation

- Shorthand for IP address
- Allows humans to avoid binary
- Represents each octet in decimal separated by dots
- NOT the same as names like www.somewhere.com

Example Of Dotted Decimal Notation

32-bit Binary Number	Equivalent Dotted Decimal
10000001 00110100 00000110 00000000	129 . 52 . 6 . 0
11000000 00000101 00110000 00000011	192 . 5 . 48 . 3
00001010 00000010 00000000 00100101	10 . 2 . 0 . 37
10000000 00001010 00000010 00000011	128 . 10 . 2 . 3
10000000 10000000 11111111 00000000	128 . 128 . 255 . 0

- Four decimal values per 32-bit address
- Each decimal number
  - Represents eight bits
  - Is between 0 and 255

Classful Addresses And Network Sizes

Address Class	Prefix Bits	Max Nets	Suffix Bits	Max Hosts Per Net
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

- Maximum network size determined by class of address
- Class A large
- Class B medium
- Class C small

Addressing Example

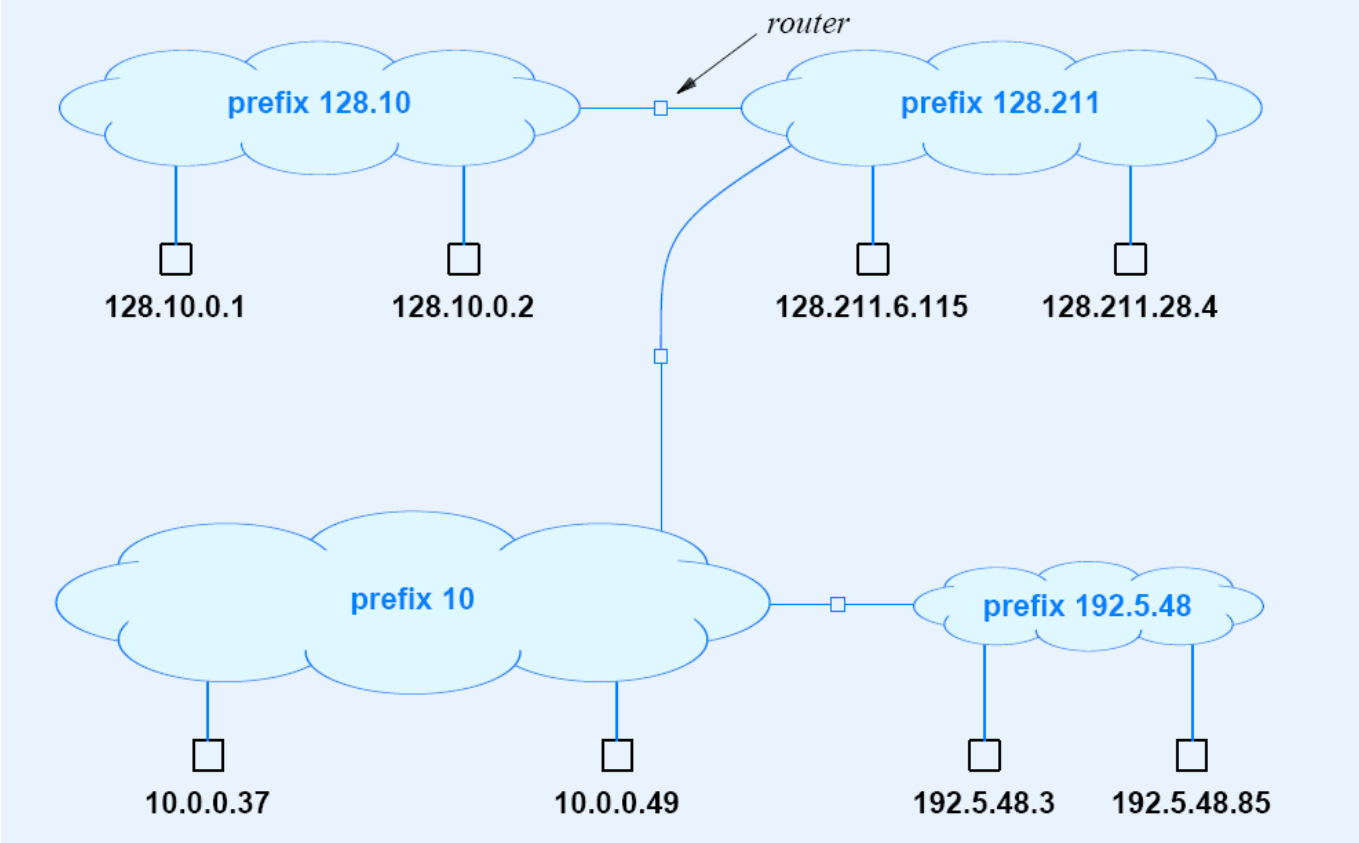
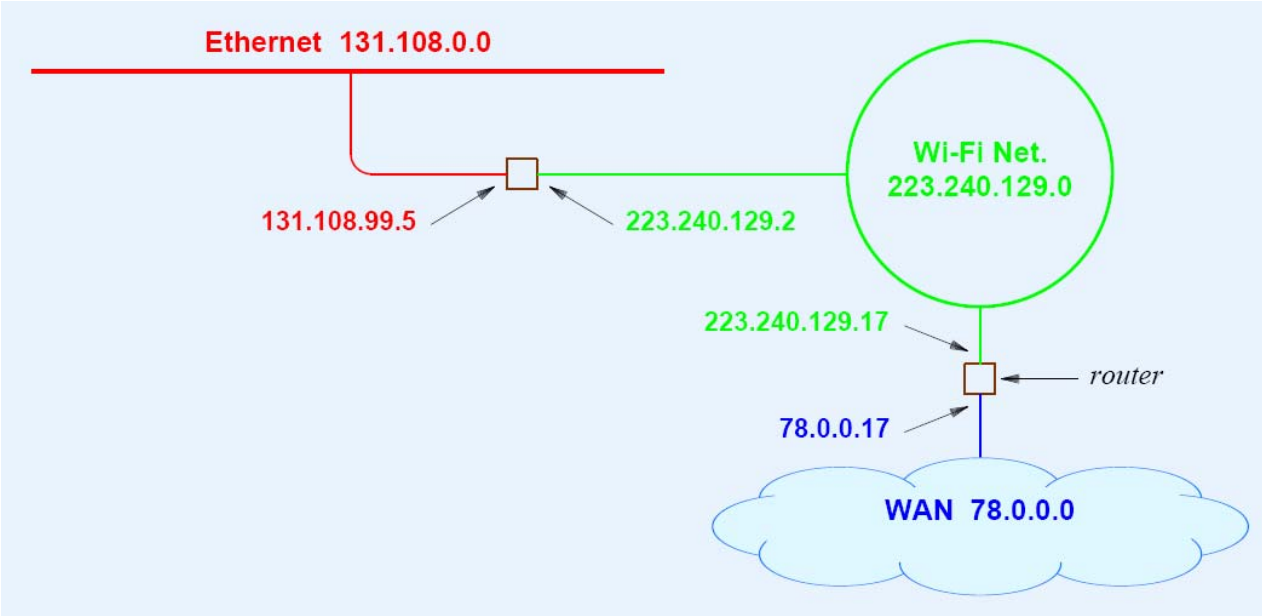


Illustration Of Router Addresses



- Address prefix identifies network
- Need one router address per connection

Special Addresses

Prefix	Suffix	Address Type	Purpose
all-0s	all-0s	this computer	bootstrap
network	all-0s	network	network ID
network	all-1s	directed bcast	bcast on specified net
all-1s	all-1s	limited bcast	bcast on local net
127	any	loopback	testing

- Network address not used in packets
- Loopback never leaves local computer

Subnet And Classless Addressing

- Not part of original scheme
- Invented to prevent address exhaustion
- Allow boundary between prefix and suffix to occur on arbitrary bit boundary
- Require auxiliary information to identify boundary

Address Mask

- Accompanies IP address
- 32 bit binary value
- Specifies prefix / suffix boundary
  - 1 bits cover prefix
  - 0 bits cover suffix
- Example: class B mask is

255 . 255 . 0 . 0

Subnet Addressing

- Goal: extend address space
- Invented in 1980s
- Works within a site
- Technique
  - Assign single network prefix to site
  - Divide suffix into two parts: network at site and host
- Typical use: divide class B address

Example Of Subnet Addressing

- Single Class B number such as 128.10.0.0 assigned to site
- Site chooses subnet boundary such as 24 bits
- Routers and hosts configured with corresponding subnet mask

  M = 255.255.255.0

- Given destination address, D, extract prefix with “logical and” operation

  D & M

Classless Addressing

- Goal: extend address space
- Invented in 1990s
- Works throughout Internet
- Accommodates
  - Original classful addresses
  - Subnet addresses
  - Other forms

Classless Addressing (continued)

- Technique
  - Allow arbitrary prefix size
  - Represent network address as pair (address , mask_size)
- Known as Classless Inter-Domain Routing (CIDR)

CIDR

- Uses slash notation
- Example

  128.211.0.0/17

  means that the boundary between prefix and suffix occurs after the first 17 bits.
- Each network can be as large or small as needed (power of two)

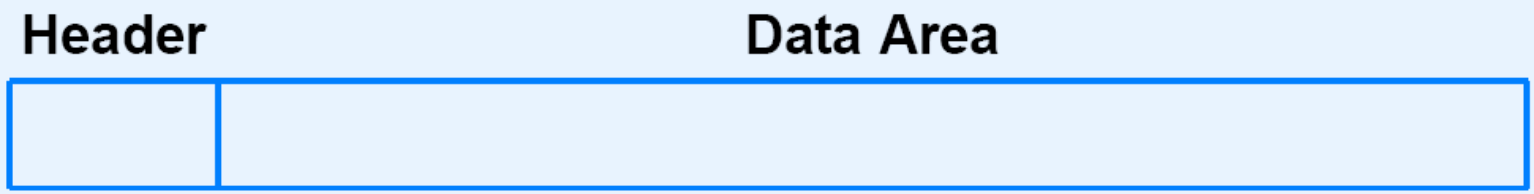
Motivation For IP Packets

Because it can connect heterogeneous networks, a router cannot transmit a copy of a frame that arrives on one network across another. To accommodate heterogeneity, an internet must define a hardware-independent packet format.

Internet Packets

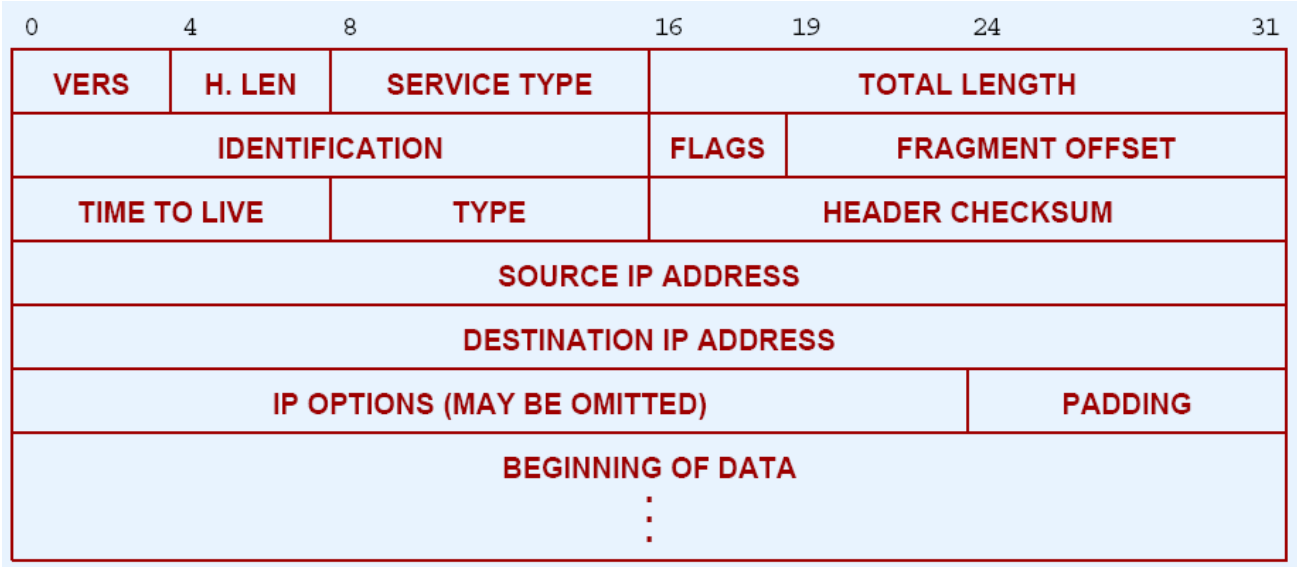
- Abstraction
- Created and understood only by software
- Contains sender and destination addresses
- Size depends on data being carried
- Called IP datagram

The Two Parts Of An IP Datagram



- Header
  - Contains destination address
  - Fixed-size fields
- Payload
  - Variable size up to 64K
  - No minimum size

Datagram Header

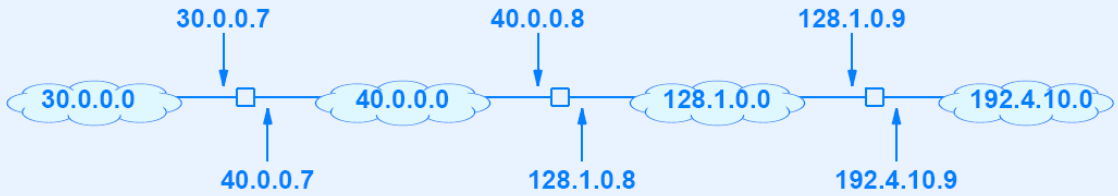


- Three key fields
  - Source IP address
  - Destination IP address
  - Type (contents)

IP Datagram Forwarding

- Performed by routers
- Similar to WAN forwarding
  - Table-driven
  - Entry specifies next hop
- Unlike WAN forwarding
  - Uses IP addresses
  - Next-hop is router or destination

Example Of An IP Routing Table



(a)

Destination	Mask	Next Hop
30.0.0.0	255.0.0.0	40.0.0.7
40.0.0.0	255.0.0.0	deliver direct
128.1.0.0	255.255.0.0	deliver direct
192.4.10.0	255.255.255.0	128.1.0.9

(b)

Table (b) is for center router in part (a)

Routing Table Size

Because each destination in a routing table corresponds to a network, the number of entries in a routing table is proportional to the number of networks in an internet.

Datagram Forwarding

- Given a datagram
- Extract destination address field, D
- Look up D in routing table
- Find next-hop address, N
- Send datagram to N

Key Concept

The destination address in a datagram header always refers to the ultimate destination. When a router forwards the datagram to another router, the address of the next hop does not appear in the datagram header.

IP Semantics

- IP is connectionless
  - Datagram contains identity of destination
  - Each datagram sent/handled independently
- Routes can change at any time

IP Semantics (continued)

- IP allows datagrams to be
  - Delayed
  - Duplicated
  - Delivered out of order
  - Lost
- Called best effort delivery
- Motivation: accommodate all possible networks

PART XII

Internetworking Part 4

(Transport Protocols, UDP and TCP, Protocol Port Numbers)

Transport Protocol

- Separate layer of protocol stack
- Conceptually between
  - Applications
  - IP

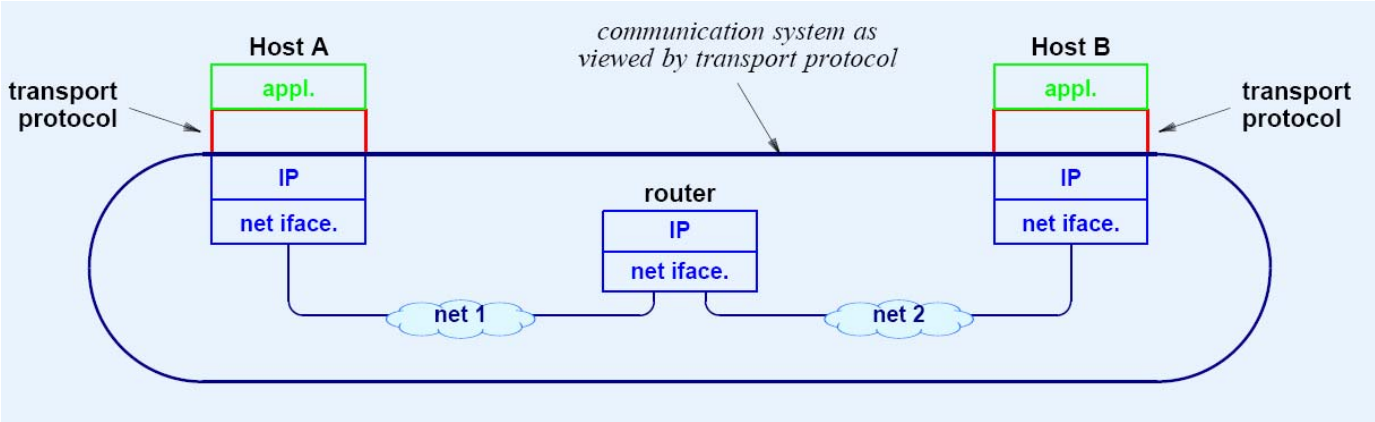
Terminology

- IP
  - Provides computer-to-computer communication
  - Source and destination addresses are computers
  - Called machine-to-machine
- Transport protocols
  - Provide application-to-application communication
  - Need extended addressing mechanism to identify applications
  - Called end-to-end

Transport Protocol Functionality

- Identify sending and receiving applications
- Optionally provide
  - Reliability
  - Flow control
  - Congestion control
- Note: not all transport protocols provide above facilities

Relationship Between Transport Protocols And Other Protocols



- Transport protocols are end-to-end
- Transport protocol on one computer uses IP to communicate with transport protocol on another computer

Two Transport Protocols Available

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Major differences
  - Interface provided to applications
  - Underlying functionality

User Datagram Protocol

- Lightweight transport
- Becoming more popular (IP telephony)
- Best-effort delivery

UDP Features

- Connectionless service
- Arbitrary interaction
- Message-oriented interface
- Best-effort semantics
- Each message encapsulated in IP datagram
- Uses protocol ports to identify applications

UDP Details

- Accepts and delivers messages
  - Message received is exactly same as message sent
  - Boundaries preserved
- Maximum message size approximately 64K octets Efficient
  - No connection overhead
  - No state information maintained

UDP Semantics

- Same best-effort semantics as IP (i.e., unreliable transfer)
- Message can be
  - Lost
  - Duplicated
  - Delayed
  - Delivered out of order
- Works best in LAN applications

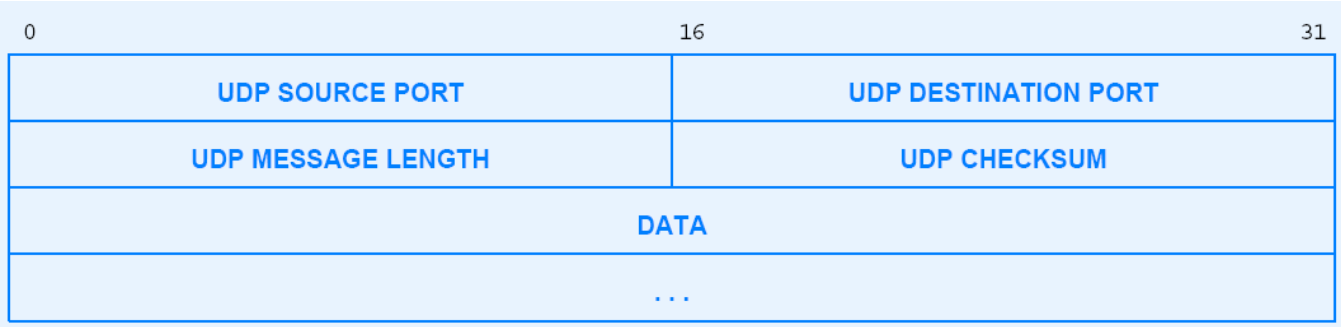
Interaction With UDP

- UDP allows communication that is
  - 1-to-1
  - 1-to-many
  - Many-to-1
  - Many-to-many
- Application programmer chooses

Packet Delivery

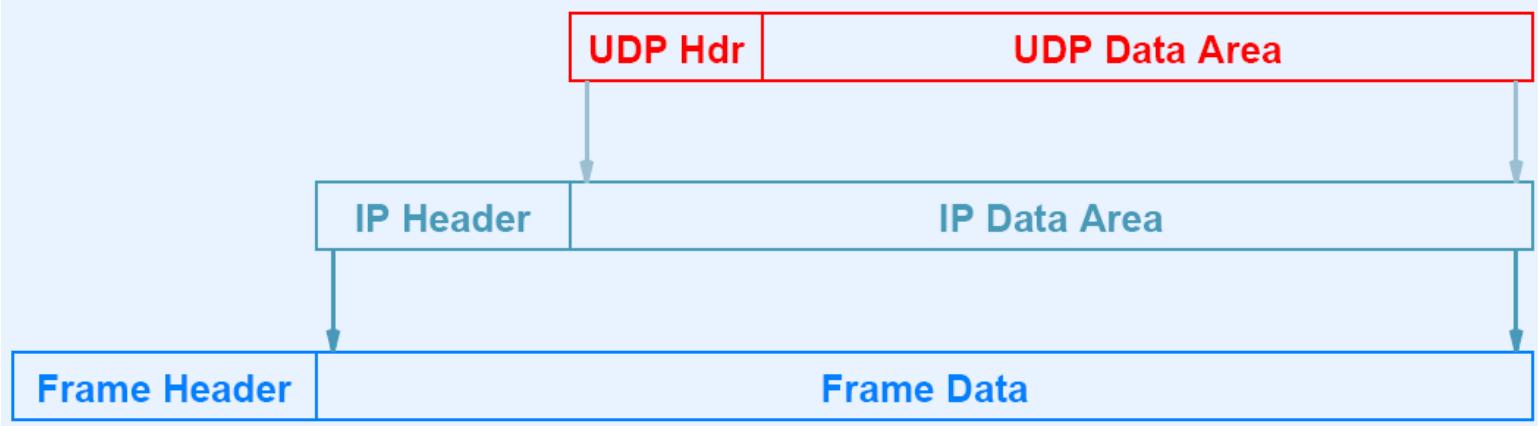
- UDP can support
  - Unicast
  - Multicast
  - Broadcast

User Datagram Format



- Extremely small header (called thin layer)
- Checksum optional

UDP Encapsulation



- Two levels of encapsulation
- UDP datagram size cannot exceed maximum IP payload

Identifying An Application

- Cannot extend IP address
  - No unused bits
- Cannot use OS-dependent quantity
  - Process ID
  - Task number
  - Job name
- Must work on all computer systems

Identifying An Application (continued)

- Invent new abstraction
  - Called protocol port number
  - Used to identify sending or receiving application unambiguously
  - Independent of underlying operating system
  - Used only with TCP/IP protocols

Protocol Port Numbers

- Server
  - Follows standard
  - Always uses same port number
  - Uses low port numbers
- Client
  - Obtains unused port from protocol software
  - Uses high port numbers

Protocol Port Example

- Domain name server application is assigned port 53
- Application using DNS obtains port 28900
- UDP datagram sent from application to DNS server has
  - Source port number 28900
  - Destination port number 53
- When DNS server replies, UDP datagram has
  - Source port number 53
  - Destination port number 28900

Transmission Control Protocol (TCP)

- Major transport protocol used in Internet
- Heavily used
- Completely reliable transfer

TCP Features

- Connection-oriented service
- Point-to-point
- Full-duplex communication
- Stream interface
- Stream divided into segments for transmission
- Each segment encapsulated in IP datagram
- Uses protocol ports to identify applications

TCP Feature Summary

TCP provides a completely reliable (no data duplication or loss), connection-oriented, full-duplex stream transport service that allows two application programs to form a connection, send data in either direction, and then terminate the connection.

Apparent Contradiction

- IP offers best-effort (unreliable) delivery
- TCP uses IP
- TCP provides completely reliable transfer
- How is this possible?

Achieving Reliability

- Reliable connection startup
- Reliable data transmission
- Graceful connection shutdown