# BLM6196 COMPUTER NETWORKS AND COMMUNICATION PROTOCOLS

Prof. Dr. Hasan Hüseyin BALIK

(3<sup>rd</sup> Week)

#### **3. The Internet Protocol**

## **3.Outline**

- Principles of Internetworking
- Internet Protocol Operation
- Internet Protocol
- IPv4 and IPv6
- Virtual Private Networks and IP Security

#### **Communication Network**

A facility that provides a data transfer service among devices attached to the network.

#### Internet

A collection of communication networks interconnected by bridges and/or routers.

#### Intranet

An internet used by a single organization that provides the key Internet applications, especially the World Wide Web. An intranet operates within the organization for internal purposes and can exist as an isolated, self-contained internet, or may have links to the Internet.

#### Subnetwork

Refers to a constituent network of an internet. This avoids ambiguity because the entire internet, from a user's point of view, is a single network.

#### End System (ES)

A device attached to one of the networks of an internet that is used to support enduser applications or services.

#### Intermediate System (IS)

A device used to connect two networks and permit communication between end systems attached to different networks.

#### Bridge

An IS used to connect two LANs that use similar LAN protocols. The bridge acts as an address filter, picking up packets from one LAN that are intended for a destination on another LAN and passing those packets on. The bridge does not modify the contents of the packets and does not add anything to the packet. The bridge operates at layer 2 of the OSI model.

#### Router

An IS used to connect two networks that may or may not be similar. The router employs an internet protocol present in each router and each end system of the network. The router operates at layer 3 of the OSI model.

### Internetworking Terms



Figure 14.1 TCP/IP Concepts

## **Connectionless Operation**

Internetworking involves connectionless operation at the level of the Internet Protocol (IP)



particular network



Figure 14.2 Example of Internet Protocol Operation

## **Connectionless Internetworking**

- Connectionless internet facility is flexible
  IP provides a connectionless service
  - between end systems
    - Advantages:
      - Is flexible
      - Can be made robust
      - Does not impose unnecessary overhead

# **IP Design Issues**

Routing
 Datagram lifetime
 Fragmentation and reassembly
 Error control
 Flow control





# Routing



 Can be static or dynamic

> ES / routers maintain routing tables

#### Source routing

- Source specifies route to be followed
- Can be useful for security and priority

 Each router appends its internet address to a list of addresses in the datagram

 Useful for testing and debugging purposes

#### Route recording

# **Datagram Lifetime**

- If dynamic or alternate routing is used the potential exists for a datagram to loop indefinitely
  - Consumes resources
  - Transport protocol may need upper bound on lifetime of a datagram
    - Can mark datagram with lifetime
    - When lifetime expires, datagram is discarded



# Fragmentation and Re-assembly

- Protocol exchanges data between two entities
- Lower-level protocols may need to break data up into smaller blocks, called fragmentation
- Reasons for fragmentation:
  - Network only accepts blocks of a certain size
  - More efficient error control and smaller retransmission units
  - Fairer access to shared facilities
  - Smaller buffers
- Disadvantages:
  - Smaller buffers
  - More interrupts and processing time



# **IP** Fragmentation

IP re-assembles at destination only
 Uses fields in header





Figure 14.4 Fragmentation Example

## **Error and Flow Control**

#### Error control

- Discarded datagram identification is needed
- Reasons for discarded datagrams include:
  - Lifetime expiration
  - Congestion
  - FCS error

#### Flow control

- Allows routers to limit the rate they receive data
- Send flow control packets requesting reduced data flow

### Internet Protocol (IP) v4

Defined in RFC 791
 Part of TCP/IP suite
 Two parts

Specification of interface with a higher layer Specification of actual protocol format and mechanisms

## **IP Services**

#### Primitives

- Specifies functions to be performed
- Form of primitive implementation dependent
- Send-request transmission of data unit
- Deliver-notify user of arrival of data unit

Parameters

Used to pass data and control information



## **IP Parameters**

- Source and destination addresses
- Protocol
- Type of Service
- Identification
- Don't fragment indicator
- Time to live
- Data length
- Option data
- > User data



## **IP** Options

#### Security

Route recording

Source routing

Stream identification

Timestamping



- Version (4 bits) Internet Header Length (IHL) (4 bits)
- DS (8 bits)
- ECN (2 bits)
- Total Length (16 bits)
- Identification (16 bits)
- Flags (3 bits)
- Fragment Offset (13 bits)
- Time to Live (8 bits)
- Protocol (8 bits): TCP = 6; UDP = 17; ICMP = 1
  - Header Checksum (16 bits)

0	Network (7 bits)	Host (24 bits)		Class A	
1	0 Netw	vork (14 bits)	Host (	16 bits)	Class B
1	1 0	Network (21 bits	5)	Host (8 bits)	Class C
1	1 1 1 0 Multicast				Class D
1	1 1 1 0	Fu	ture Use		Class E

Figure 14.6 IPv4 Address Formats



#### Start with binary 0

Network addresses with a first octet of 0 (binary 0000000) and 127 (binary 0111111) are reserved

> 126 potential Class A network numbers

> > Range 1 to 126

### IP Addresses Class B

Start with binary 10

Range 128 to 191(binary 10000000 to 1011111)

Second octet also included in network address

2<sup>14</sup> = 16,384 Class B addresses IP Addresses Class C

Start with binary 110

Range 192 to 223

Second and third octet also part of network address

2<sup>21</sup> = 2,097,152 addresses

Nearly all allocated •See IPv6

Class	Subuet Mask decimal	No. of Hosts per Network	No. of Networks	Start -End Address	
Α	255.0.0.0	16 Million	127	27 1.0.0.0 - 126.255.255.255	
B 255.255.0.0 65000 16000		16000	128.0.0.0 - 191.255.255.255		
С	255.255.255.0	254	2 Million	192.0.0.0 - 223.255.255.255	
D	D Reserved for multicast groups			224.0.0.0 - 239.255.255.255	
E	Reserved for future use, or Research and Development Purposes			240.0.0.0 - 254.255.255.254	

<u>Class</u>	<u>Address Range</u>	<u>Default Subnet Mask</u>
А	10.0.0.0 - 10.255.255.255	255.0.0.0
В	172.16.0.0 - 172.31.255.2	55 255.255.0.0
С	192.168.0.0 -	
	192.168.255.255	255.255.255.0

## **Subnets and Subnet Masks**

- Allows arbitrary complexity of internetworked LANs within organization
- Insulate overall internet from growth of network numbers and routing complexity
- Site looks to rest of internet like single network
- Each LAN assigned subnet number
- Host portion of address partitioned into subnet number and host number
- Local routers route within subnetted network
- Subnet mask indicates which bits are subnet number and which are host number

### **IPv4 Addresses and Subnet Masks**

	Binary Representation	Dotted Decimal
IP address	11000000.11100100.00010001.00111001	192.228.17.57
Subnet mask	11111111111111111111111111111100000	255.255.255.224
Bitwise AND of address and mask (resultant network/subnet number)	11000000.11100100.00010001.00100000	192.228.17.32
Subnet number	11000000.11100100.00010001.001	1
Host number	0000000.0000000.000 00000.00011001	25

(a) Dotted decimal and binary representations of IPv4 address and subnet masks

	Binary Representation	Dotted Decimal
Class A default mask	11111111.0000000.0000000.00000000	255.0.0.0
Example Class A mask	11111111.11000000.0000000.00000000	255.192.0.0
Class B default mask	11111111.1111111.00000000.00000000	255.255.0.0
Example Class B mask	111111111111111111111000.00000000	255.255.248.0
Class C default mask	1111111111111111111111111100000000	255. 255. 255.0
Example Class C mask	11111111.11111111.111111111111100	255. 255. 255.252

(b) Default subnet masks

# Internet Control Message Protocol (ICMP)

Provides a means for transferring messages from routers and other hosts to a host

### Provides feedback about problems

- Datagram cannot reach its destination
- Router does not have buffer capacity to forward
- Router can send traffic on a shorter route
- Encapsulated in IP datagram
  - Hence not reliable

# **Common ICMP Messages**

Destination unreachable Time exceeded > Parameter problem Source quench > Redirect Echo and echo reply Timestamp and timestamp reply > Address mask request and reply



# Address Resolution Protocol (ARP)

#### Need MAC address to send to LAN host

Manual Included in network address Use central directory Use address resolution protocol

#### ARP provides dynamic IP to Ethernet address mapping

Source broadcasts ARP request Destination replies with ARP response

### **IP Next Generation**

## Address space exhaustion:

- Two level addressing (network and host) wastes space
- Network addresses used even if not connected
- Growth of networks and the Internet
- Extended use of TCP/IP
- Single address per host

# Requirements for new types of service

- Address configuration routing flexibility
- Traffic support

## **IPv6 RFCs**

» RFC 1752 - Recommendations for the IP Next Generation Protocol

- Requirements
- PDU formats
- Addressing, routing security issues
- » RFC 2460 overall specification
- > RFC 4291 addressing structure

## **IPv6 Enhancements**

Expanded 128 bit address space

Improved option mechanism

- Most not examined by intermediate routes
- Dynamic address assignment
- Increased addressing flexibility
  - Anycast and multicast
- Support for resource allocation
  - Labeled packet flows



Figure 14.9 IPv6 Packet with Extension Headers (containing a TCP Segment)



Version (4 bits) > DS/ECN (8 bits): Flow Label (20) bits) Payload Length (16 bits) Next Header (8) bits) Hop Limit (8 bits)

# **IPv6 Flow Label**

- Related sequence of packets
- Special handling
- Identified by source and destination address plus flow label
- Router treats flow as sharing attributes
- May treat flows differently
- Alternative to including all information in every header
- Have requirements on flow label processing

### **IPv6 Addresses**

- > 128 bits long
- > Assigned to interface
- Single interface may have multiple unicast addresses

#### Three types of addresses:

- Unicast single interface address
- Anycast one of a set of interface addresses
- Multicast all of a set of interfaces

## **IPv6 Address Space Usage**

Address Type	Binary Prefix	IPv6 Notation	Fraction of address space
Embedded IPv4 address	001111 1111 1111 1111 (96 bits)	::FFFF/96	2-96
Loopback	001 (128 bits)	::1/128	2-128
Link-local unicast	1111 1110 10	FE80::/10	1/1024
Multicast	1111 1111	FF00::/8	2/256
Global unicast	Everything else		

# **Hop-by-Hop Options**

- Must be examined by every router
  - If unknown discard/forward handling is specified
- Next header
- Header extension length
- Options
  - Pad1
  - PadN
  - Jumbo payload
  - Router alert

## **Fragmentation Header**

Fragmentation only allowed at source

- No fragmentation at intermediate routers
- Node must perform path discovery to find smallest MTU of intermediate networks
- Set source fragments to match MTU
- Otherwise limit to 1280 octets

# **Routing Header**

Contains a list of one or more intermediate nodes to be visited on the way to a packet's destination

Header includes Next header

- Header extension length
- Routing type
- Segments left

### **Destination Options Header**

Carries optional information for destination node Format same as hop-by-hop header

# Virtual Private Network (VPN)

Set of computers interconnected using an unsecure network

• e.g. linking corporate LANs over Internet

- > Using encryption and special protocols
  - to provide security
    - Eavesdropping
    - Entry point for unauthorized users



Proprietary solutions are problematical

Development of IPSec standard

### **IPsec**

> RFC 1636 (1994) identified security need Encryption and authentication necessary security features in IPv6 Designed also for use with current IPv4



Electronic commerce security



## **Benefits of IPsec**

- Provides strong security for external traffic
- Resistant to bypass
- Below transport layer hence transparent to applications
- Can be transparent to end users
- Can provide security for individual users if needed

## **IPsec Functions**

Authentication header (AH)

For authentication only

Encapsulating Security Payload (ESP)

For combined authentication/encryption

A key exchange function

Manual or automated

VPNs usually need combined function