NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 6: IP Addressing and Routing (Part I)

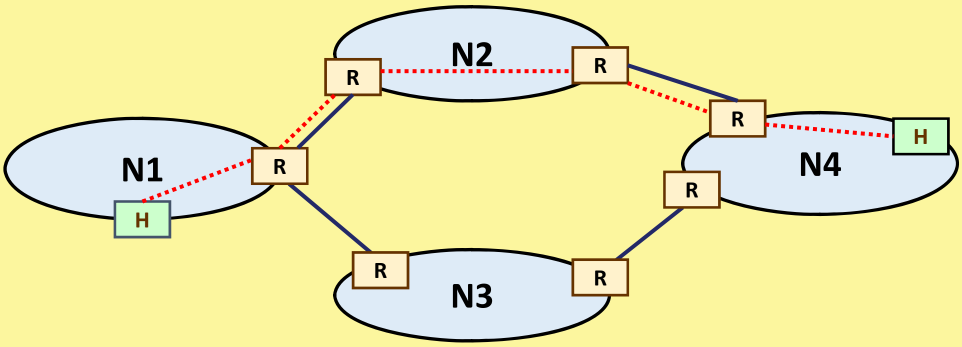
CONCEPTS COVERED

- IP packet fragmentation
- Transparent / non-transparent fragmentation

Fragmentation

- Why needed?
  - The IP layer injects a packet into the datalink layer.
    - Not responsible for the reliable transport of these packets.
  - Each layer imposes some maximum size of packets, due to various reasons.
    - Called ***Maximum Transfer Unit (MTU).***
  - Suppose a large packet travels through a network whose MTU is too small.
    - Fragmentation (and also reassembly) is required.
    - Each fragment is transmitted as a separate IP packet.
    - Fragmentation is typically done by routers.
- Fragments reassembled later: ***transparent*** or ***non-transparent***.

Interconnection of Networks

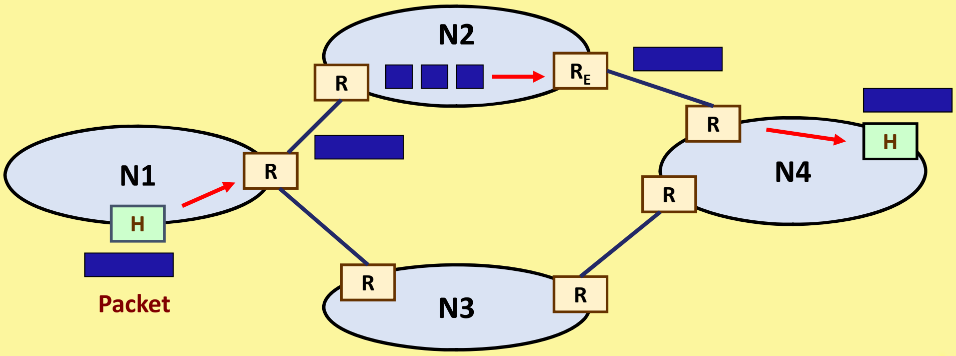


Transparent Fragmentation

- Fragmentation is *transparent* to subsequent networks, through which the packet pass.
- Basic concept:
  - An oversized packet reaches a router, which breaks it up into fragments.
  - All fragments sent to the same exit router (say, R_E).
  - R_E reassembles the fragments before forwarding to the next network.
- Why called transparent?
  - Subsequent networks are not even aware that fragmentation had occurred.
- A packet may get fragmented several times.

5

Transparent Fragmentation (contd.)



6

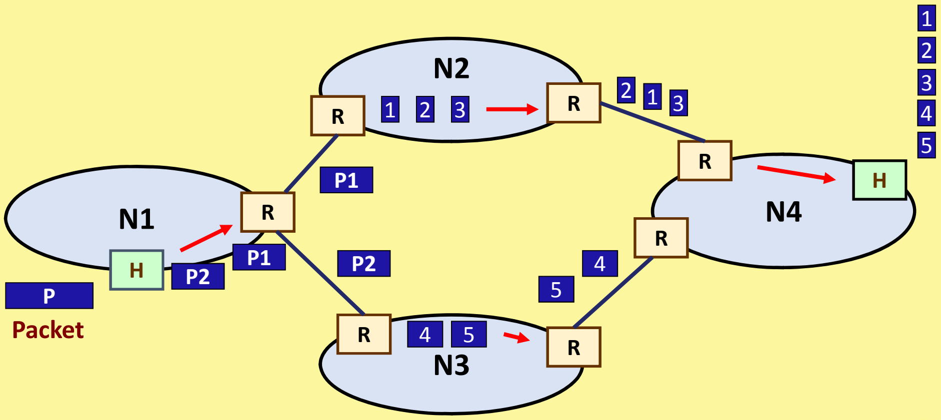
Transparent Fragmentation (contd.)

- Drawbacks:
  - All packets must be routed via the same exit router.
  - Exit router must know when all the pieces have been received.
    - Either a ***count*** field or ***end-of-packet*** field must be stored in each packet.
  - Lot of overhead.
    - A large packet may be fragmented and reassembled repeatedly.

Non-transparent Fragmentation

- Fragmentation is not transparent to subsequent networks.
- Basic concept:
  - Packet fragments are not reassembled at any intermediate router.
  - Each fragment is treated as an independent packet.
  - The fragments are reassembled at the final destination host.
- IP uses this philosophy.

Non-transparent Fragmentation (contd.)



Non-transparent Fragmentation (contd.)

- Advantage:
  - Multiple exit routers may be used.
  - Higher throughput.
- Drawback:
  - When a large packet is fragmented, overhead increases.
  - Each fragment must have a header (minimum 20 bytes).
- IP protocol uses non-transparent fragmentation.

IP Datagram

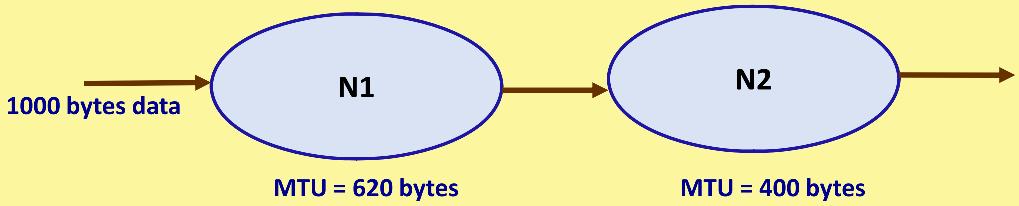
0	4	8	15 16	31
VER	HLEN	Service type	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
Options				
DATA				

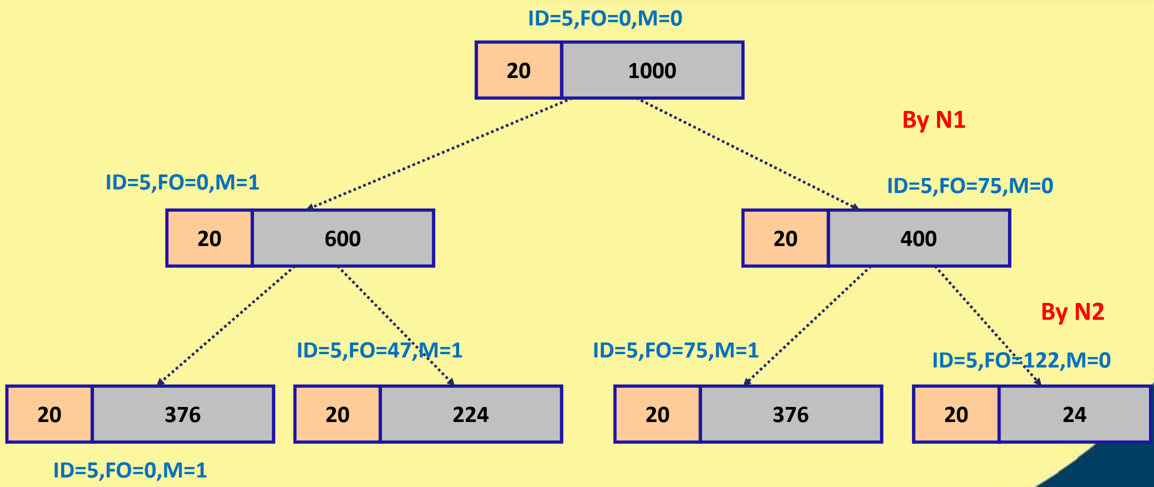
HEADER

What does IP do?

- To allow fragment reassembly at the final destination, IP uses the following fields in the header:
  - Identification (16 bits)
    - ❖ A datagram id set by the source.
  - Fragment offset (13 bits)
    - ❖ Indicates where in the original datagram this fragment belongs to.
    - ❖ Specified in multiple of 8 bytes.
  - Flags (3 bits) --- two flags are defined
    - D bit :: don't fragment; prevents fragmentation from taking place.
    - M bit :: more fragment; specifies if this fragment is the last one in the original packet or not.

Example :: IP Fragmentation





1020 bytes sent and 1080 bytes received


FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत
NPTEL ONLINE CERTIFICATION COURSES
Thank you!
15

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 7: IP Addressing and Routing (Part II)

CONCEPTS COVERED

- IP addressing
- IP address classes

Basic IP Addressing

- Each host connected to the Internet is identified by a unique IP address.
- An IP address is a 32-bit quantity.
  - Expressed as a dotted-decimal notation W.X.Y.Z, where dots are used to separate each of the four octets of the address.
  - Consists of two logical parts:
    a) A network number
    b) A host number
  - This partition defines the *IP address classes*.

Dotted Decimal Notation

IP address: 01000010 10001000 00110000 01111110

01000010	10001000	00110000	01111110
(66)	(134)	(48)	(126)

Dotted Decimal Notation: 66.134.48.126

Hierarchical Addressing

- A computer on the Internet is addressed using a two-tuple:
  - The network number
    - ❖ Assigned and managed by central authority.
  - The host number
    - ❖ Assigned and managed by local network administrator.
- When routing a packet to the destination network, only the network number is looked at.

IP Address Classes

- There are five defined IP address classes.
  - Class A UNICAST
  - Class B UNICAST
  - Class C UNICAST
  - Class D MULTICAST
  - Class E RESERVED
- Identified by the first few bits in the IP address.
- There also exists some special-purpose IP addresses.
- The class-based addressing is also known as the *classful model*.

Class A Address

0	Network	Host	Host	Host

- Network bits : 7
  - Number of networks = $2^7 - 1 = 127$
- Host bits: 24
  - Number of hosts = $2^{24} - 2 = 16,777,214$
- Address range:
  - 0.0.0.0 to 127.255.255.255

7

Class B Address

10	Network	Network	Host	Host

- Network bits : 14
  - Number of networks = $2^{14} - 1 = 16,383$
- Host bits: 16
  - Number of hosts = $2^{16} - 2 = 65,534$
- Address range:
  - 128.0.0.0 to 191.255.255.255

8

Class C Address

110	Network	Network	Network	Host

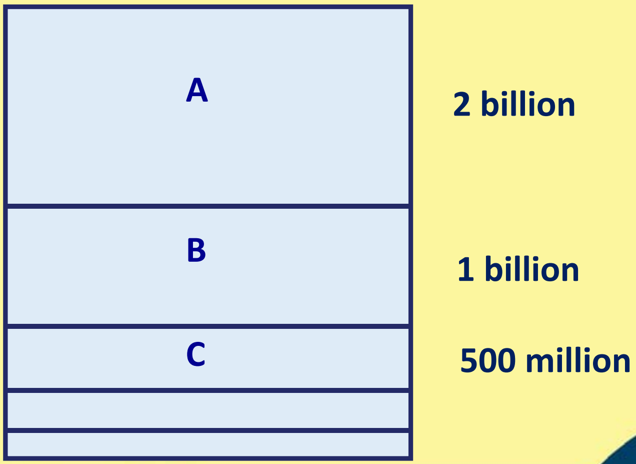
- Network bits : 21
  - Number of networks = $2^{21} - 1$ = 2,097,151
- Host bits: 8
  - Number of hosts = $2^{8} - 2$ = 254
- Address range:
  - 192.0.0.0 to 223.255.255.255

Class D Address

1110	Multicast Address

- Address range:
  - 224.0.0.0 to 239.255.255.255

Address Distribution



Special-purpose IP Addresses

- Reserved for private use
  - 10.x.x.x (Class A)
  - 172.16.x.x – 172.31.x.x (Class B)
  - 192.168.x.x (Class C)
- Loopback/local address
  - 127.0.0.0 – 127.255.255.255
- Default network
  - 0.0.0.0
- Limited broadcast
  - 255.255.255.255

Some Conventions

- Within a particular network (Class A, B or C), the first and last addresses serve special functions.
  - The first address represents the ***network number***.
    - ❖ For example, 118.0.0.0
  - The last address represents the directed ***broadcast address*** of the network.
    - ❖ For example, 118.255.255.255

13

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 8: TCP and UDP (Part I)

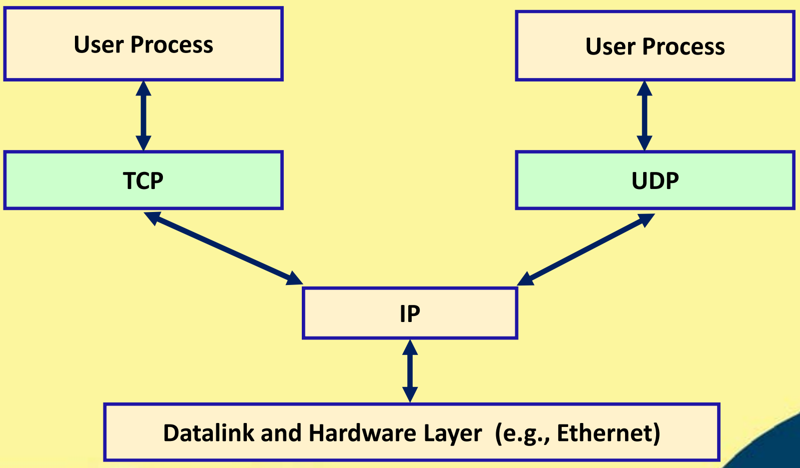
CONCEPTS COVERED

- TCP and UDP
- Port numbers

Introduction

- In TCP/IP, the transport layer consists of two different protocols.
  a) Transmission control protocol (TCP).
  b) User datagram protocol (UDP).
- Basic idea:
  - User processes (applications) interact with the TCP/IP protocol suite by sending/receiving TCP or UDP data.
  - Both TCP and UDP in turn uses the IP layer for delivery of packets.

TCP and UDP



Role of TCP

- Provides a connection-oriented, reliable, full-duplex, byte-stream service.
  - Underlying IP layer is unreliable and provides connectionless delivery service.
  - TCP provides end-to-end reliability using
    - ❖ Checksum
    - ❖ Positive acknowledgements
    - ❖ Timeouts
    - ❖ End-to-end flow control.
- TCP also handles
  - Establishment and termination of connections between processes.
  - Sequencing of data that might reach the destination in any arbitrary order.

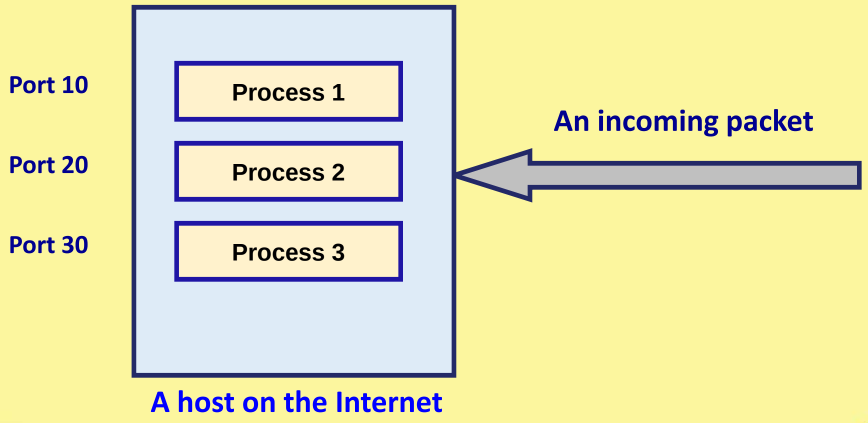
Role of UDP

- UDP provides a connectionless and unreliable datagram service.
  - Very similar to IP in this respect.
  - Provides two features that are not there in IP:
    - ❖ A checksum to verify the integrity of the UDP packet.
    - ❖ Port numbers to identify the processes at the two ends.

Port Numbers

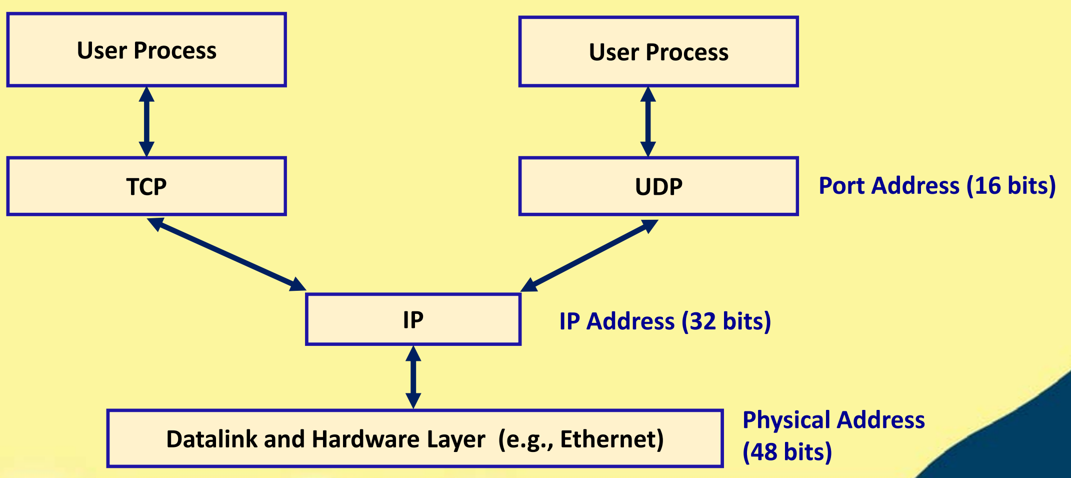
- Multiple user processes on a machine may use TCP or UDP at the same time.
- There is need for a mechanism to uniquely identify the data packets associated with each process.

Port Numbers (contd.)



Port Numbers (contd.)

- How this is done?
  - Both TCP and UDP uses 16-bit integer port numbers.
  - Different applications are identified by different port numbers.
  - Port numbers are stored in the headers of TCP or UDP packets.



Port Numbers (contd.)

- Client-server scenario
  - By knowing the 32-bit IP address of the server host, a client host can connect to the server.
  - To identify a particular process running on the server host, the client must also know the corresponding port number.
- Well-known port numbers
  - Predefined, and publicly known.
  - FTP uses port 21, SMTP uses port 25.

11

Port Numbers (contd.)

- Well-known port numbers are stored in a particular file on the host machine.
  - Unix:: `/etc/services`
  - Windows:: `C:\WINDOWS\system32\drivers\etc\services`
  - Each line has the format:

    `<service name> <port number>/<protocol> [aliases...] [#<comment>]`
- Few lines of the file are shown next.

12

services - Notepad

File Edit Format View Help

```
# Copyright (c) 1993-2004 Microsoft Corp.
#
# This file contains port numbers for well-known services defined by IANA
#
# Format:
#
# <service name>  <port number>/<protocol>  [aliases...]   [#<comment>]
#

echo                7/tcp
echo                7/udp
discard             9/tcp    sink null
discard             9/udp    sink null
systat             11/tcp    users                  #Active users
systat             11/udp    users                  #Active users
daytime            13/tcp
daytime            13/udp
qotd               17/tcp    quote                  #Quote of the day
qotd               17/udp    quote                  #Quote of the day
chargen            19/tcp    ttytst source          #Character generator
chargen            19/udp    ttytst source          #Character generator
ftp-data           20/tcp                           #FTP, data
ftp                21/tcp                           #FTP. control
ssh                22/tcp                           #SSH Remote Login Protocol
telnet             23/tcp
smtp               25/tcp    mail                   #Simple Mail Transfer Protocol
time               37/tcp    timserver
time               37/udp    timserver
rlp                39/udp    resource               #Resource Location Protocol
nameserver         42/tcp    name                   #Host Name Server
nameserver         42/udp    name                   #Host Name Server
nicname            43/tcp    whois
domain             53/tcp                           #Domain Name Server
domain             53/udp                           #Domain Name Server
bootps             67/udp    dhcps                  #Bootstrap Protocol Server
bootpc             68/udp    dhcpc                  #Bootstrap Protocol Client
tftp               69/udp                           #Trivial File Transfer
gopher             70/tcp
finger             79/tcp
```

13

Ephemeral Port Numbers

- A typical scenario:
  - A client process sends a message to a server process located on some host at port 1534.
  - How will the server know where to respond?
    - ❖ Client process requests an unused port number from the TCP/UDP module on its local host.
    - ❖ These are temporary port numbers, called *ephemeral port numbers*.
    - ❖ Send along with the TCP or UDP header.
- How are the port numbers assigned?
  - Port numbers from 1 to 1023 are reserved for well-known ports.
    - ❖ Has been extended to 4095.
  - Numbers beyond this and up to 65535 used as ephemeral port numbers.

14

Connection Establishment

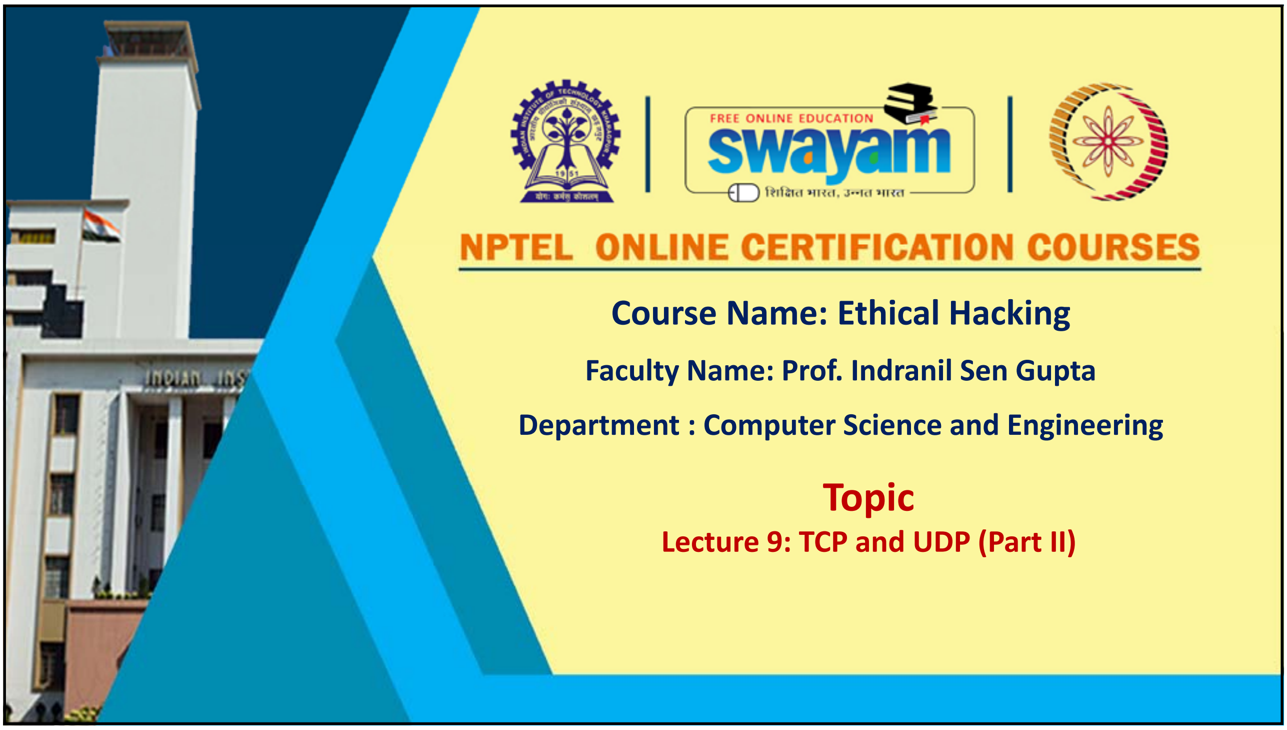
- A hierarchical addressing scheme is used to define a connection path between two hosts.
  - IP address
    - ❖ Identifies the communicating hosts.
  - Protocol identifier
    - ❖ Identifies the transport later protocol being used (TCP, UDP or anything else).
  - Port number
    - ❖ Identifies the communicating processes in the two hosts.

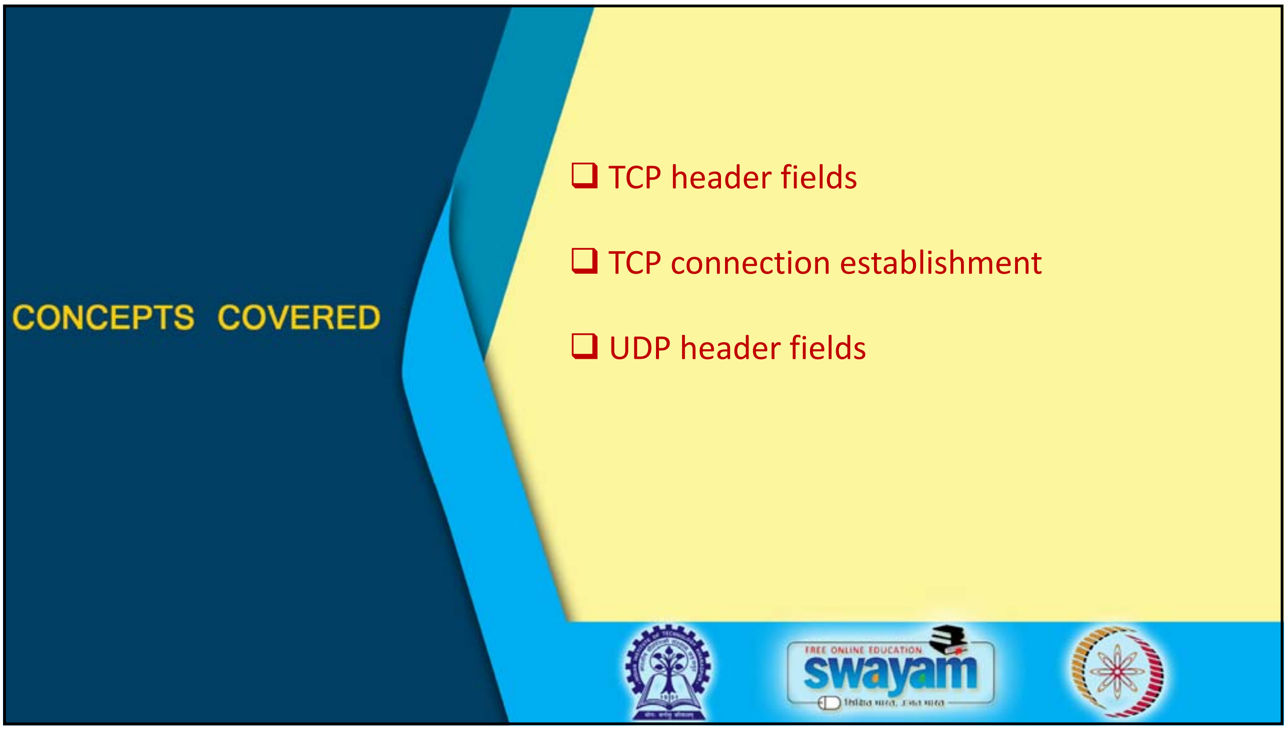
Association

- A set of five values that describe a unique process-to-process connection is called an *association*.
  - The protocol (TCP or UDP).
  - Local host IP address (32-bit value).
  - Local port number (16-bit value).
  - Remote host IP address (32-bit value).
  - Remote port number (16-bit value).
- Example of an association:

  {TCP, 144.16.192.5, 1785, 144.16.202.57,21}


FREE ONLINE EDUCATION
swayam
NPTEL ONLINE CERTIFICATION COURSES
Thank you!
17

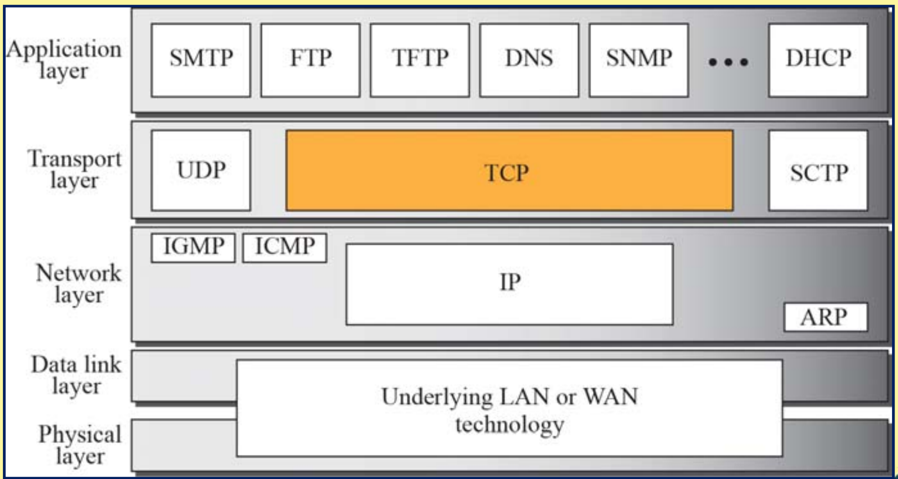

FREE ONLINE EDUCATION
swayam
NPTEL ONLINE CERTIFICATION COURSES
Course Name: Ethical Hacking
Faculty Name: Prof. Indranil Sen Gupta
Department : Computer Science and Engineering
Topic
Lecture 9: TCP and UDP (Part II)


CONCEPTS COVERED
TCP header fields
TCP connection establishment
UDP header fields
swayam

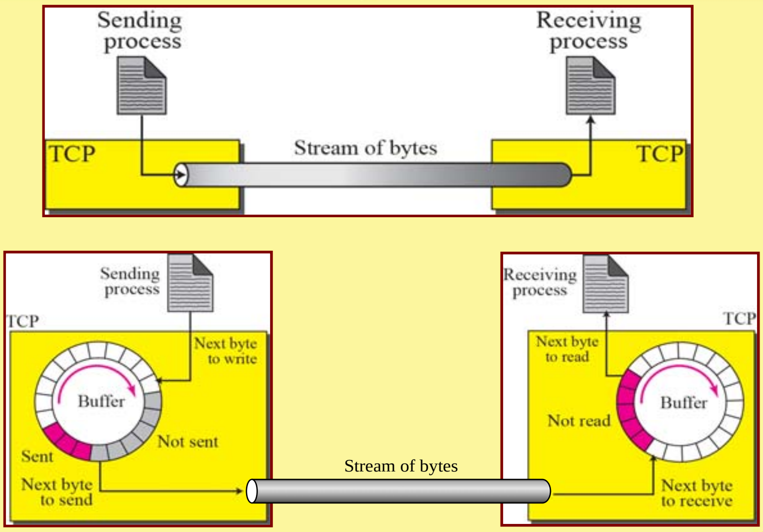
Transmission Control Protocol (TCP)

- TCP supports host-to-host communication with the following features:
  - Process-to-process communication
  - Stream delivery service
  - Full-duplex communication
  - Multiplexing and de-multiplexing
  - Connection-oriented reliable service

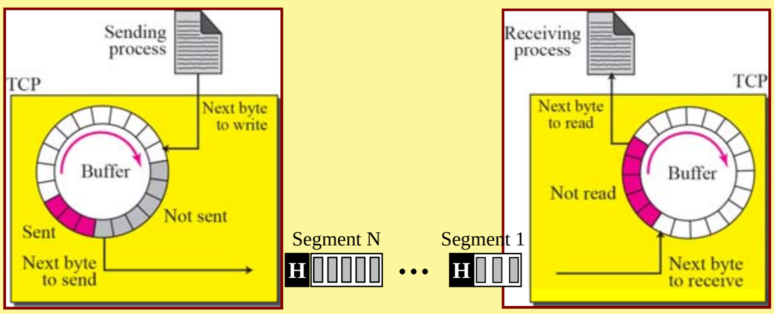
3



4


Sending process
Receiving process
TCP
Stream of bytes
TCP
Sending process
TCP
Next byte to write
Buffer
Not sent
Sent
Next byte to send
Stream of bytes
Receiving process
TCP
Next byte to read
Buffer
Not read
Next byte to receive

5


Sending process
TCP
Next byte to write
Buffer
Not sent
Sent
Next byte to send
Segment N
H
...
Segment 1
H
Receiving process
TCP
Next byte to read
Buffer
Not read
Next byte to receive

6

Format of TCP Segment (20-60 bytes of header)

0 16 31

Source Port			Destination Port
Sequence Number			
Acknowledgement Number			
HLEN	Reserved	Flags	Window
Checksum			Urgent Pointer
Options			
DATA			

TCP Header Fields

- Source port (16 bits)
  - Identifies the process at the local end.
- Destination port (16 bits)
  - Identifies the process at the remote end.
- Sequence number (32 bits)
  - Used for reliable delivery of message.
  - Each byte of message is assigned a 32-bit number that is incremented sequentially.
  - The field holds the number of the first byte in that TCP segment.

TCP Header Fields (contd.)

- Acknowledgement Number (32 bits)
  - Used by remote host to acknowledge receipt of data.
  - Contains the number of the next byte expected to be received.
- HLEN (4 bits)
  - Specifies the header length in number of 32-bit words.

TCP Header Fields

- Flags (6 bits)
  - There are six flags.
    - ❖ URG is set to 1 if the urgent pointer is in use.
    - ❖ A connection request is sent by making SYN=1 and ACK=0.
    - ❖ A connection is confirmed by sending SYN=1 and ACK=1.
    - ❖ When the sender has no more data, FIN=1 is sent to release the connection.
    - ❖ RST bit is used to reset a connection. It is also used to reject a connection attempt.
    - ❖ PSH bit indicates the push function. Used to indicate end of message.

TCP Header Fields (contd.)

- Window (16 bits)
  - Specifies how many bytes may be sent beyond the byte acknowledged.
  - This number, called *window advertisement*, can increase or decrease as needed.
  - A value of zero closes the window altogether.

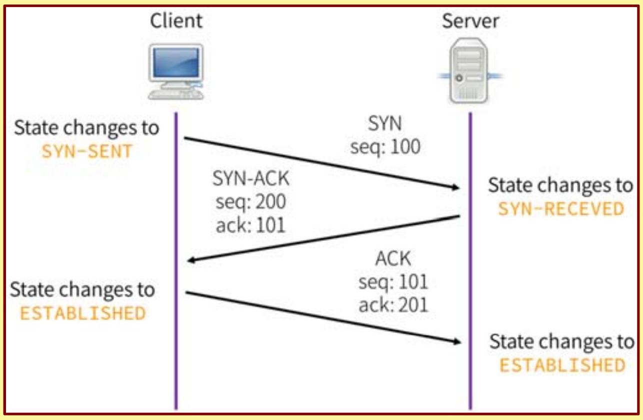
11

TCP Header Fields (contd.)

- Checksum (16 bits)
  - Applies to the entire segment and a pseudo-header.
  - The pseudo-header contains the following IP header fields:
    - ❖ Source IP address, destination IP address, protocol, segment length.
    - ❖ TCP protects itself from misdelivery by IP (delivered to wrong host).
  - Same algorithm as used in IP.

12

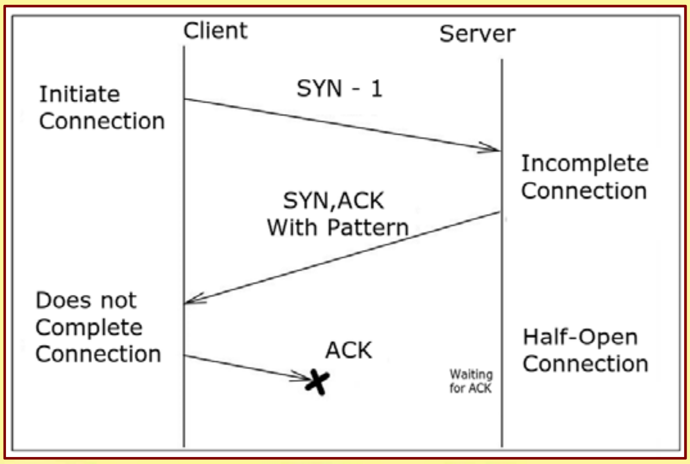
TCP Connection Establishment



3-way handshake

13

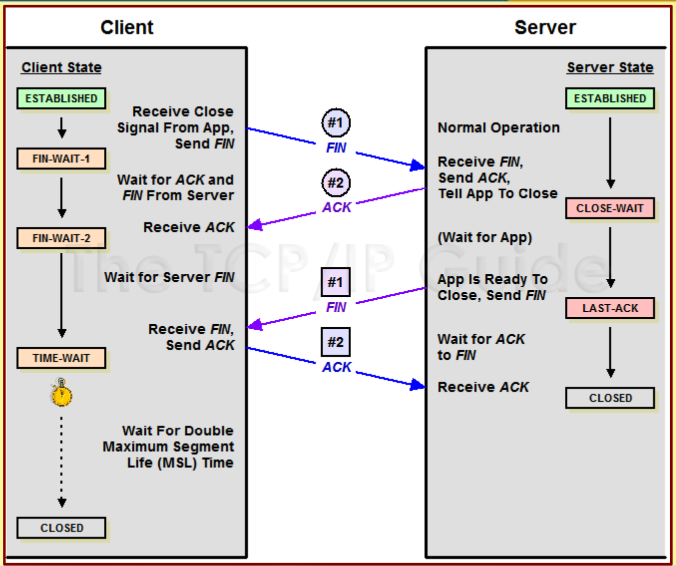
Half-open (Incomplete) Connection



Possible attack scenario:

- Create many half-open connections to target.
- Ignore SYN+ACK response
- Target connection table fills up, resulting in denial-of-service (DoS) attack.

14



TCP Connection Termination

Format of UDP Segment (8 bytes header)

0 16 31

Source Port	Destination Port
Message Length	Checksum
DATA	

UDP Header Fields

- Source port (16 bits)
  - Identifies the process at the local end.
- Destination port (16 bits)
  - Identifies the process at the remote end.
- Message length (16 bits)
  - Specifies the size of the datagram in bytes (UDP header plus data).
- Checksum (16 bits)
  - Computed in the same way as TCP.
  - This is optional; set to zero if not used.

17

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 10: IP Subnetting

CONCEPTS COVERED

- IP subnets and masks
- Variable length subnet mask (VLSM)
- Classless internet domain routing (CIDR)

IP Subnet

- A subnet is a subset of a class A, B or C network.
- IP addresses without subnets consists of a network portion, and a host portion.
  - Represents a static two-level hierarchical addressing model.
- IP subnets introduces a third level of hierarchy.
  - a) a network portion
  - b) a subnet portion
  - c) a host portion
- Allow more efficient (and structured) utilization of the addresses.
- Uses network masks.

Natural Masks

- Network mask 255.0.0.0 is applied to a class A network 10.0.0.0.
  - In binary, the mask is a series of contiguous 1's followed by a series of contiguous 0's.

11111111 00000000 00000000 00000000

Network portion (11111111) — **Host portion** (00000000 00000000 00000000)

Natural Masks (contd.)

- Provide a mechanism to split the IP address 10.0.0.20 into
  - a network portion of 10, and
  - a host portion of 20.

	Decimal	Binary
IP address:	10.0.0.20	00001010 00000000 00000000 00010100
Mask:	255.0.0.0	11111111 00000000 00000000 00000000
		Network Host

Natural Masks (contd.)

- Class A, B and C addresses
  - Have fixed division of network and host portions.
  - Can be expressed as masks.
    - Called ***natural masks***.
- Natural Masks
  - Class A :: 255.0.0.0
  - Class B :: 255.255.0.0
  - Class C :: 255.255.255.0

Creating Subnets using Masks

- Masks are very flexible.
  - Using masks, networks can be divided into smaller subnets.
  - By extending the network portion of the address into the host portion.
- Advantage:
  - We can create a large number of subnets from one network.
  - Can have less number of hosts per network.

7

Example: Subnets

- Network mask 255.255.0.0 is applied to a class A network 10.0.0.0.
  - This divides the IP address 10.5.0.20 into
    - a network portion of 10,
    - a subnet portion of 5, and
    - a host portion of 20.
- The 255.255.0.0 mask borrows a portion of the host space, and applies it to network space.

8

- What happens?
  - Initially it was a single large Class A network ($2^{24} – 2$ hosts).
  - We have now split the network into 256 subnets.
    - From 10.0.0.0 to 10.255.0.0.
    - The hosts pet subnet decreases to 65,534.

	Decimal	Binary
IP address:	10.5.0.20	00001010 00000101 00000000 00010100
Mask:	255.255.0.0	11111111 11111111 00000000 00000000
		Network Subnet Host

Default Mask and Subnet mask

Default Mask
255.255.0.0

IP Address
144.16.72.57

AND

Network Address
144.16.0.0

192: 1100 0000
72: 0100 1000

Subnet Mask
255.255.192.0

IP Address
144.16.72.57

AND

Network Address
144.16.64.0

Variable Length Subnet Masks (VLSM)

- Basic concept
  - The same network can be configured with different masks.
  - Can have subnets of different sizes.
  - Allows better utilization of available addresses.

Example: VLSM

- Suppose we are assigned a Class C network 192.203.17.0.
  - To be divided into three subnets.
    - ❖Corresponding to three departments.
    - ❖With 110, 45 and 50 hosts respectively.
- Available subnet options
  - The network mask will be the Class C natural mask 255.255.255.0
  - Subnet masks of the form 255.255.255.X
    - ❖Can be used to divide the network into more subnets.

D1
(110)

D2
(45)

D3
(50)

The Subnet Options

X	X (in binary)	No. of Subnets	No. of Hosts
128	1000 0000	2	128
192	1100 0000	4	64
224	1110 0000	8	32
240	1111 0000	16	16
248	1111 1000	32	8
252	1111 1100	64	4

Cannot satisfy the requirements.

The VLSM Option

- Basic concept:
  - Use the mask 255.255.255.128 to divide the network address into two subnets with 128 hosts each.
    - 192.203.17.0 (.0 to .127)
    - 192.203.17.0 (.128 to .255)
  - Next subnet the second .128 subnet using a mask of 255.255.255.192.
    (Creates two subnets, 64 hosts each)
    - 192.213.17.128 (.128 to .191)
    - 192.213.17.128 (.192 to .255)

The VLSM Option (contd.)

192.203.17.0

Mask: 255.255.255.128

192.203.17.0 (.0 to .127)

192.203.17.0 (.128 to .255)

Mask: 255.255.255.192

192.213.17.128 (.128 to .191)

192.213.17.128 (.192 to .255)

15

Classless Internet Domain Routing (CIDR)

- CIDR is a new concept to manage IP networks.
  - Classless Inter Domain Routing.
  - No concept of class A, B, C networks.
  - Reduces sizes of routing tables.
- An IP address is represented by a prefix, which is the IP address of the network.
- It is followed by a slash, followed by a number M.
  - M: number of leftmost contiguous bits to be used for the network mask.
  - Example: 144.16.192.57 / 18

16

CIDR: An Important Rule

- The number of addresses in each block must be a power of 2.
- The beginning address in each block must be divisible by the number of addresses in the block.
  - A block that contains 16 addresses cannot have beginning address as 144.16.223.36.
  - But the address 144.16.192.64 is possible.

17

Example: CIDR

- An organization is allotted a block with beginning address:

  144.16.192.24 / 29

  What is the range of the block?

Start addr: 10010000 00011000 11000000 00011000

End addr: 10010000 00011000 11000000 00011111

There are 8 addresses in the block.

18

Present Trend

- Use CIDR addressing.
  - Existing classful networks can also be represented using this notation.
    - Class A: W.X.Y.Z / 8
    - Class B: W.X.Y.Z / 16
    - Class C: W.X.Y.Z / 24
- All routers today support CIDR.

19