IP, TCP, UDP

ALTRAN

IP, TCP, UDP

Computer Networks
May 16,2011

TOC

- Internet Protocol (IP)
- What IP Does not provide?
- Relation of IP To other Protocol
- IPV4 Datagram format
- IP Fragmentation and reassembly
- IP Routing
- Routing and Forwarding
- The Routing Table

Internet Protocol(IP)

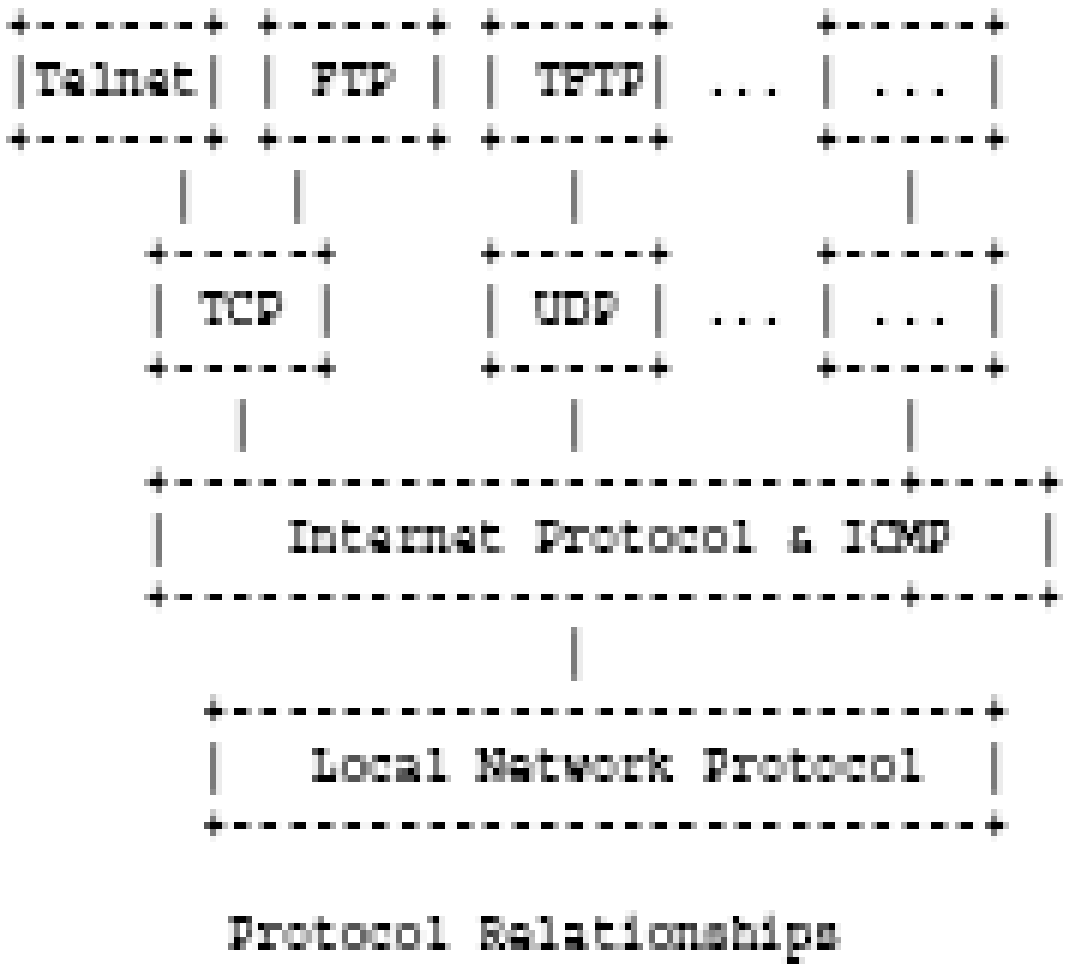
- Internet Protocol
  - ✓ Is a network Layer Protocol
  - ✓ Transmits blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses (IP Addresses) .

What IP does not provide ?

IP does not provide a reliable communication facility

- No acknowledgement either end to end or hop-by-hop.
- No error control for data, only a header checksum
- No retransmission
- No flow control

Relation of IP to other protocols



Protocol Relationships

IPv4 Datagram format

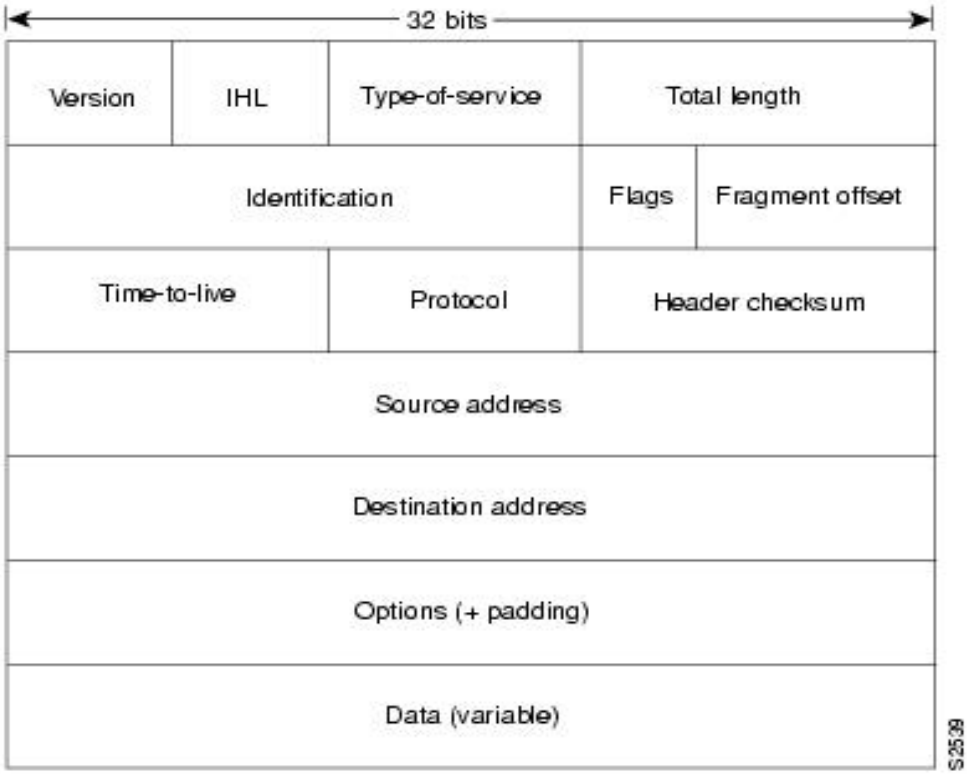
An IPv4 datagram consists of

IP Header (20 bytes)

data (variable length)

Transmitted in big endian format

IPV4 Datagram format



Fragmentation and Reassembly

Fragmentation of an Internet datagram is necessary when it originates in a local network that allows a large packet size and must traverse a local network that limits packets to a smaller size to reach its destination.

- ✓An internet datagram can be marked “don’t fragment“. Any internet datagram so marked is not to be internet fragmented under any circumstances.
- ✓If internet datagram marked “don’t fragment” cannot be delivered to its destination without fragmenting it, it is to be discarded.

Fragmentation and Reassembly – Identification Field

The Internet Identification field is used to distinguish the fragments of one datagram from those of another.

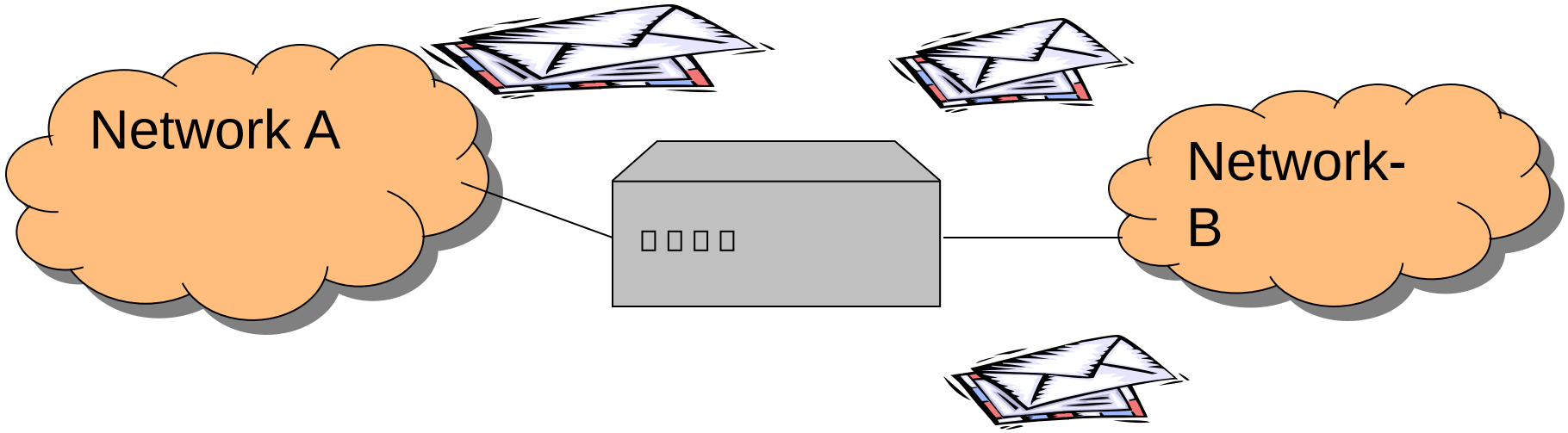
The originating protocol module of an internet datagram sets the identification field to a value that must be unique for that source destination pair and protocol for the time the datagram will be active in the internet system.

Fragmentation and Reassembly – Flags and Fragmentation offset

Note the Flags field and Fragmentation Offset Field in the IP Header.

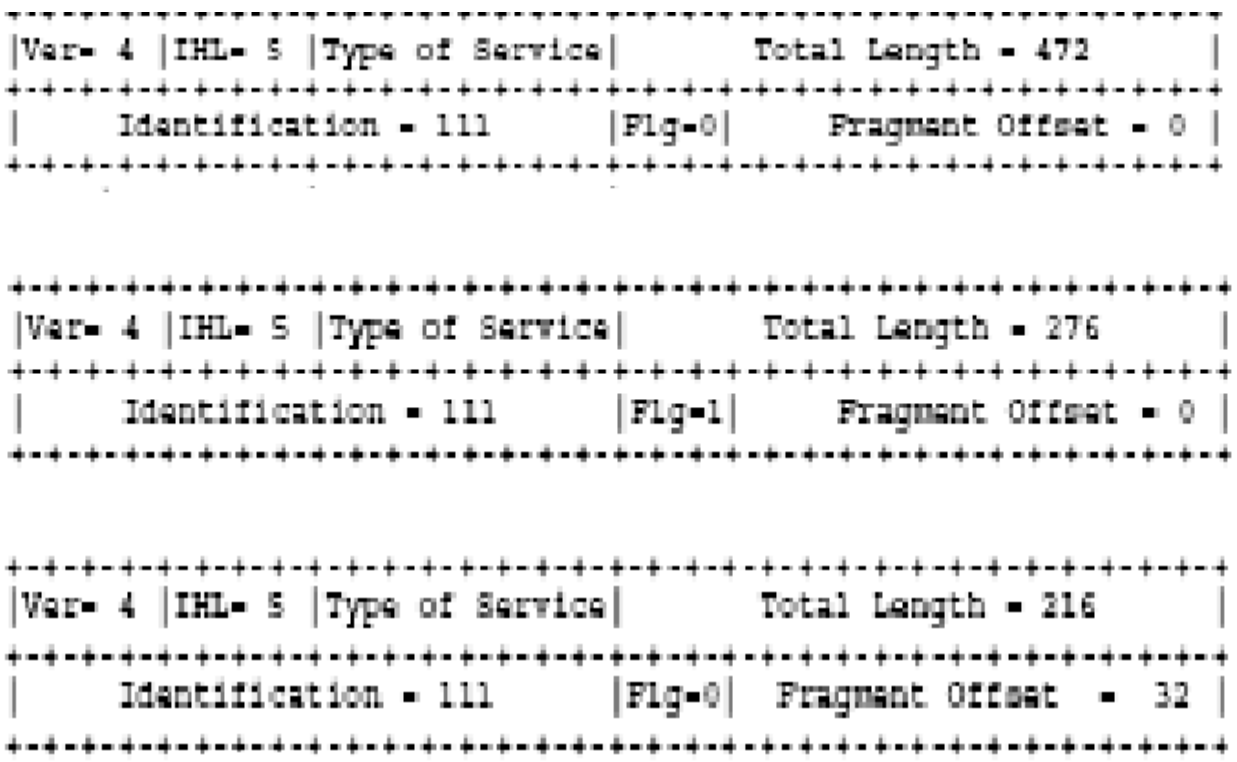
- Flags : 3 bits (0, DF, MF)
  - First Bit = 0
  - DF = 0 (May Fragment), 1 (Don’t Fragment)
  - MF = 0 (Last Fragment), 1 (More Fragment)
- Fragmentation Offset (13 bits)
  - Identifies the fragment location relative to the beginning of the original unfragmented datagram. Fragments are counted in units of 8 Bytes.

An Example of Fragmentation



Consider a moderate size IP datagram of 452 bytes of data originating in Network A. Maximum size of transmission allowed in Network B is 280 Bytes. How can you fragment the datagram ?

An Example of Fragmentation contd…



Original

Fragment-1

Fragment-2

Reassembly Process

To assemble the fragments of an Internet datagram , an IP module combines internet datagrams that all have the same value for the following four fields:

(identification , source , destination ,protocol)

Data portion of the datagram is placed in the correct position from the fragmentation offset field.

First fragment is identified by fragmentation offset = 0 and the last fragment by MF bit = 0.

Routing

Routing is the process of choosing a path over which to send packets.

Router is a computer that makes the choice of path for routing.

IP routing algorithm has to choose how to send a datagram across multiple physical networks.

Routing and Forwarding

Forwarding is used in network routing to find the proper interface to which the input interface should send a packet to be transmitted by the router. Forwarding tables are built by the routing process.

Routing table consists of the IP address of the next hop (router) which should be used to route a packet destined for a specific network address.

Routing table

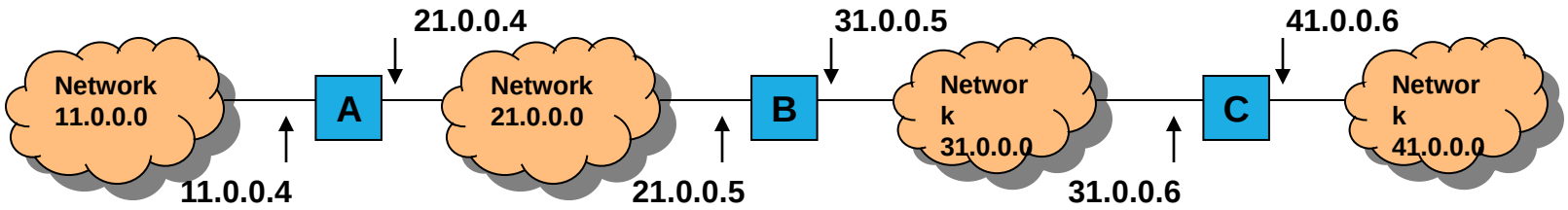
NetworkNum	NextHop
10	171.69.245.10

vs.

Forwarding table

NetworkNum	Iface	MAC addr
10	eth0	8:0:2:e4:b:1:2

The Routing Table



The above figure shows 4 IP networks interconnected with 3 routers. Each of the routers has 2 interfaces, and is connected to 2 other networks.

The table below shows the entries in the routing table maintained at the router ‘B’.

21.0.0.0	Direct Delivery
11.0.0.0	21.0.0.4
31.0.0.0	Direct Delivery
41.0.0.0	31.0.0.6

Transmission Control Protocol (TCP)

Computer Networks
May 16,2011

TOC

- The TCP
- TCP operation
- Relation with other protocols
- TCP segment format
- Connection Establishment (3 Way Handshake)
- Connection Termination (4 Way Handshake)
- TCP State diagram
- Window and Acknowledgement strategy in TCP

The TCP

➢TCP is a Transport Layer protocol whose primary purpose is to provide reliable and secure connection service between pairs of processes.

➢To provide this service on top of less reliable internet communication system, it requires facilities in the following areas -

- Basic data transfer
- Reliability
- Flow Control
- Multiplexing
- Connections

TCP Operation - Basic Data Transfer

- TCP is able to transfer a **continuous stream of bytes** in each direction between its users.

- It does so by packaging some number of bytes into segments for transmission through the internet system.

- In general, the TCP decides when to block and forward data at their own convenience.

TCP Operation - Reliability

- The TCP must recover from data that is damaged, lost, duplicated, or delivered out of order by the internet communication system.

- Sequence number - This is assigned a sequence number to each octet transmitted.

- The receiving process must send a positive acknowledgment (ACK) for the received octet. If the ACK is not received within a timeout interval, the data is retransmitted.
- At the receiver, the sequence numbers are used to correctly order segments that may be received out of order and to eliminate duplicates.

- Checksum – Corrupted segments are handled by adding a checksum to each segment transmitted, checking it at the receiver, and discarding damaged segments.

TCP Operation – Flow Control

TCP provides flow control by providing a means for the receiver to govern the amount of data sent by the sender.

- This is achieved by returning a "window" with every ACK indicating a range of acceptable sequence numbers beyond the last segment successfully received.

- The window indicates an allowed number of bytes that the sender may transmit before receiving further permission.

This communication between processes to synchronize the bytes in the window is controlled by the Sliding Window protocol.

TCP Operation - Multiplexing

- TCP allows multiple application programs on a given machine to communicate concurrently using the TCP services.
- TCP also demultiplexes incoming TCP traffic among application programs. It uses protocol port numbers to identify the ultimate destination within a machine.
- Port numbers, concatenated with the network and host addresses from the internet communication layer, form a socket. A pair of sockets uniquely identifies each connection.
- A socket may be simultaneously used in multiple connections.

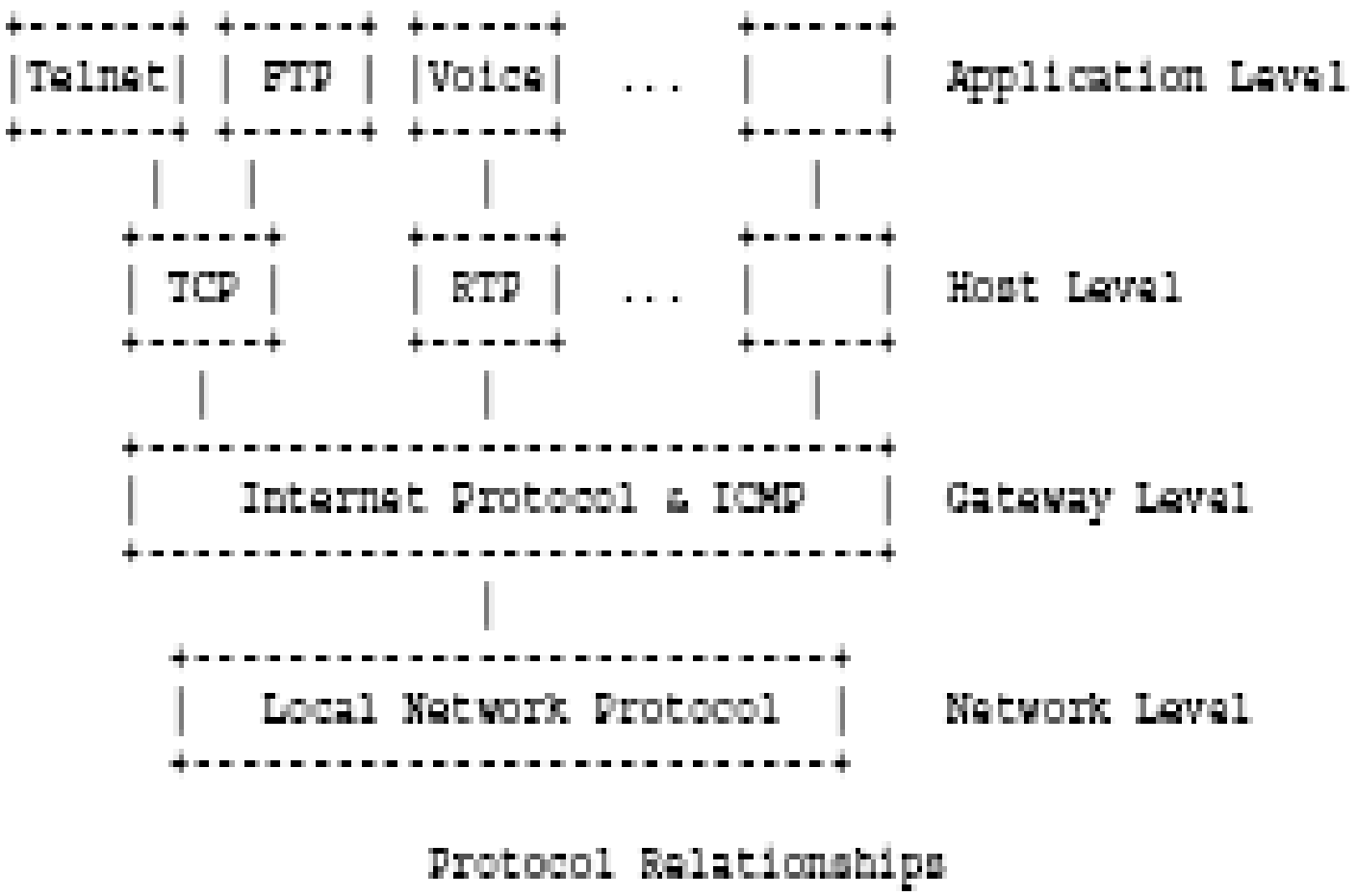
TCP Operation - Connections

- The reliability and flow control mechanisms require that TCP initializes and maintains certain status information for each data stream.

- The combination of this information, including sockets, sequence numbers, and window sizes, is called a connection.

- Each connection is uniquely specified by a pair of sockets identifying its two sides.

Relation with Other protocols



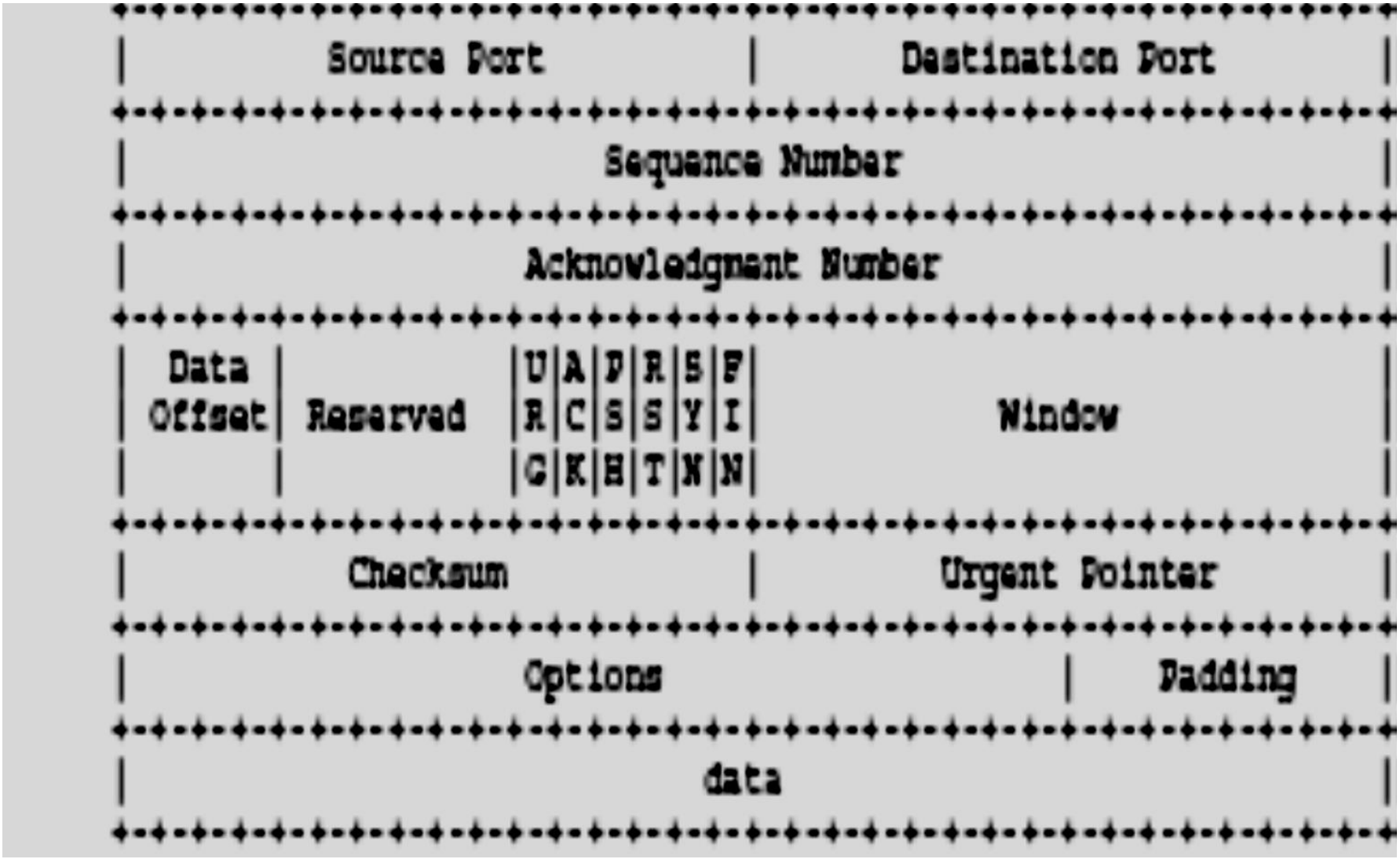
Protocol Relationships

Connection Oriented Transmission

➢TCP Connection oriented transmission requires three phases :

- Connection Establishment
- Data Transfer
- Connection Termination

TCP Segment Format



TCP Segment Format (contd…)

- Source port – Source port Number (16 bit)
- Destination Port – Destination port Number (16 bit)
- Sequence No – Sequence number of the first data byte in this segment (except when SYN is present) (32 bit)
- ✓Note: (Seq No refers to bytes flowing in the same direction as the segment and Ack no refers to bytes flowing in the opposite direction from the segment)

- Acknowledgement Number – Byte number that the source expects to receive next (32 bit)
- Data offset - Length of the segment Header measured in 4 byte words (4 bit)
- Control Bits - (URG,ACK,PSH,RST,SYN,FIN)

Connection Establishment

- Suppose host A wishes to establish a connection with host B
- Each side sends its own initial sequence Number and also receives a confirmation from the other side.

  1)A→B (SYN , my sequence Number is X)

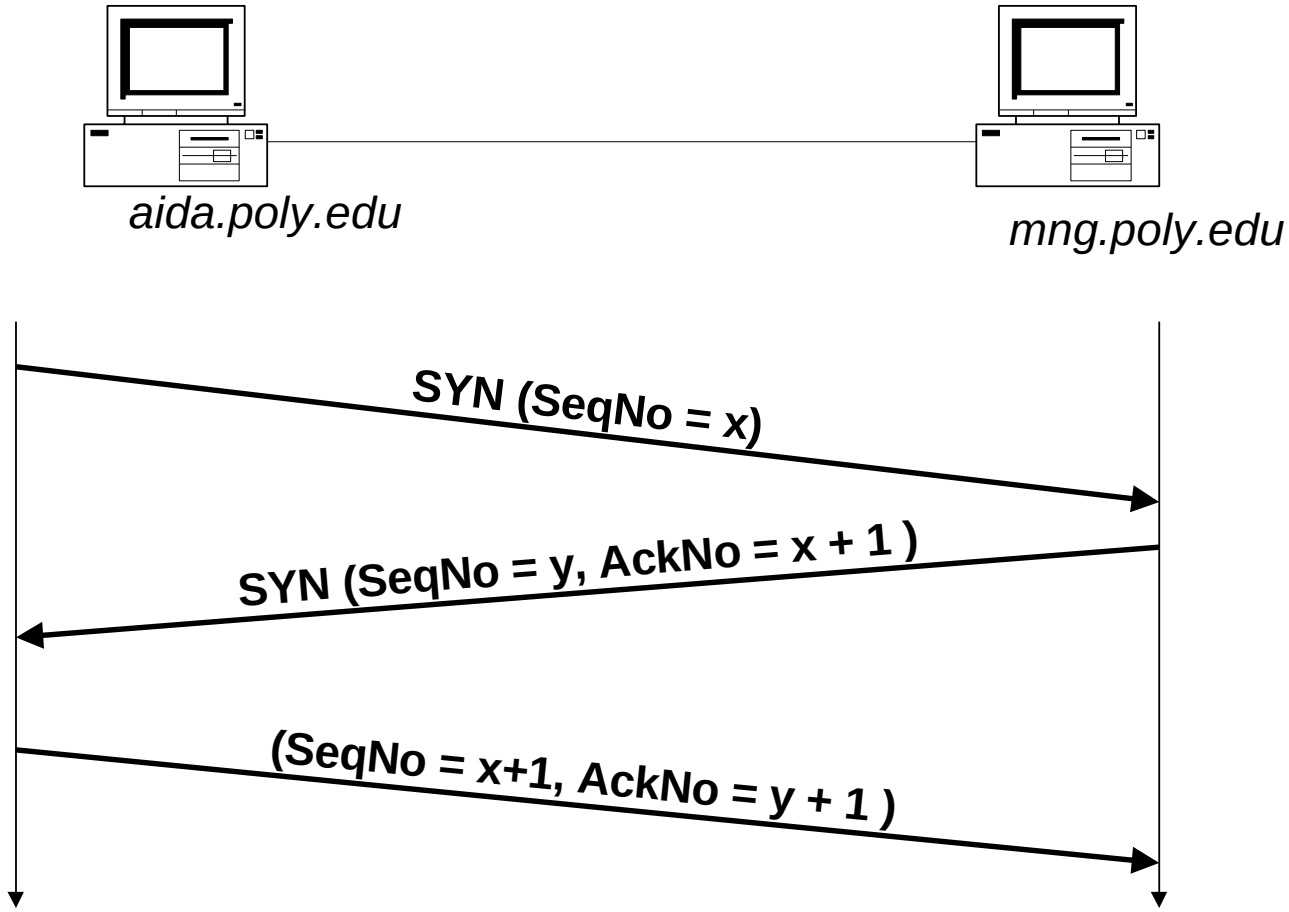
  2)A←B(ACK , your sequence Number is X)

  3) A←B(SYN , my sequence Number is Y)

  4) A→B(ACK , your sequence Number is Y)

- Steps 2 & 3 can be combined in a single message , so this procedure is called Three way Handshake

Connection Establishment contd…



An Example of 3 way Handshake

TCP A	TCP B
1.closed	Listen
2.SYN-SENT(Seq=100,syn) =>	SYN-RECV
3.Established <=(Seq=300,Ack=101,syn,ack)	SYN-RECV
4.Established(Seq=101,Ack=301,ack)=>	Established
5.Established (Seq=101,Ack=301,ack,data)=>	Established

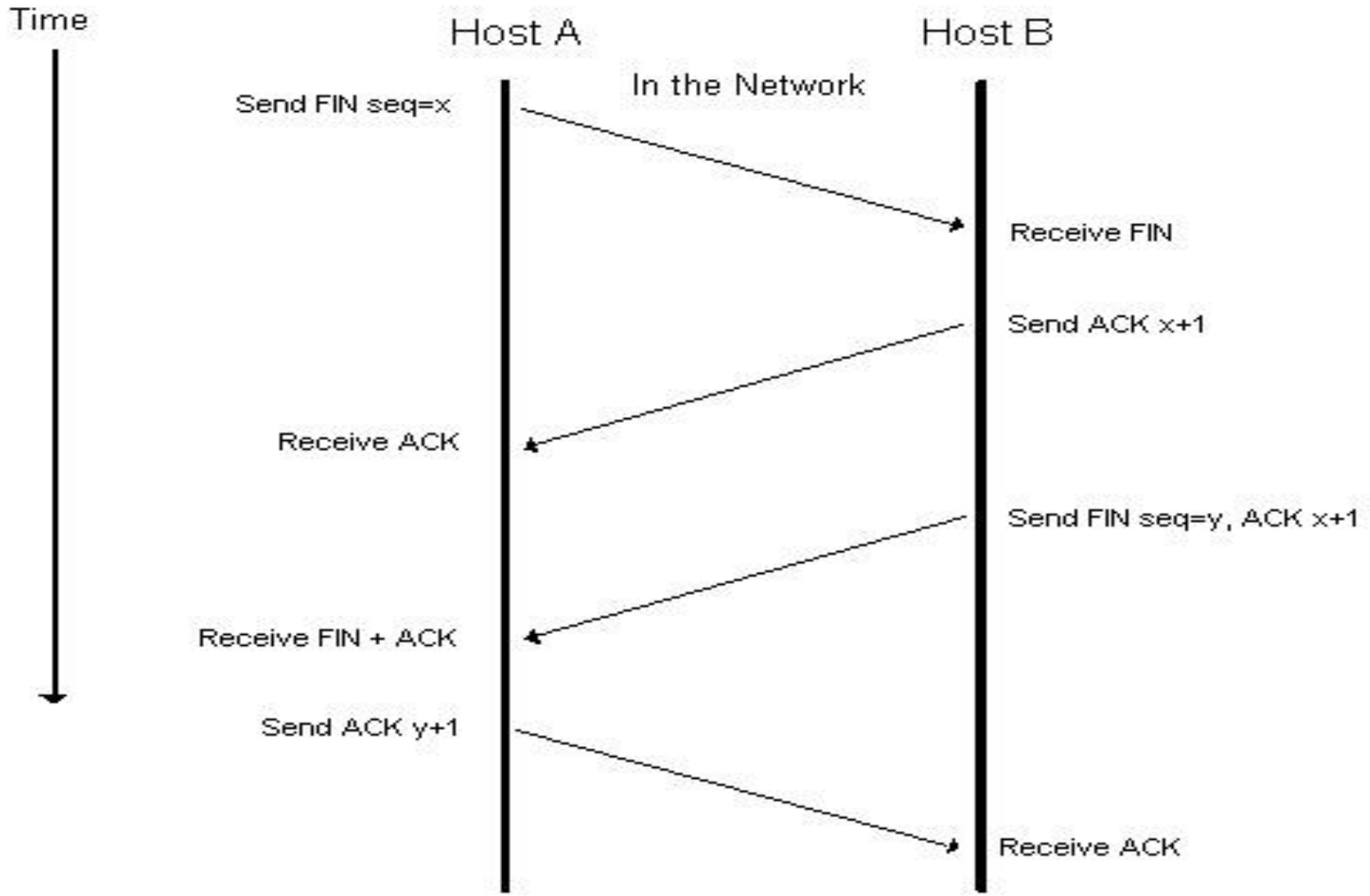
- Note : Seq No of the segment in line 5 is same as in line 4 because ACK does not occupy sequence Number space.

Necessity of 3 way Handshake

- Sequence Numbers are not tied to a global clock in the network and TCP's may have different mechanisms for choosing the initial sequence Number (ISN).

- The receiver of the first SYN has no way of knowing whether the segment was an old delayed one or not .So it must ask the sender to verify the SYN.

Connection Termination



Connection Termination

- In the previous slide Host A performs active close (TCP sends a FIN segment , which means it has finished sending data)

- The other end (Host B) that receives the FIN performs the passive close .FIN is being Acknowledged (FIN occupies one Byte in seq no space)The receipt of FIN is also passed to the application as an end-of-file.

- The application (in Host B) that received the end of file will close its socket.This causes TCP to send a FIN.

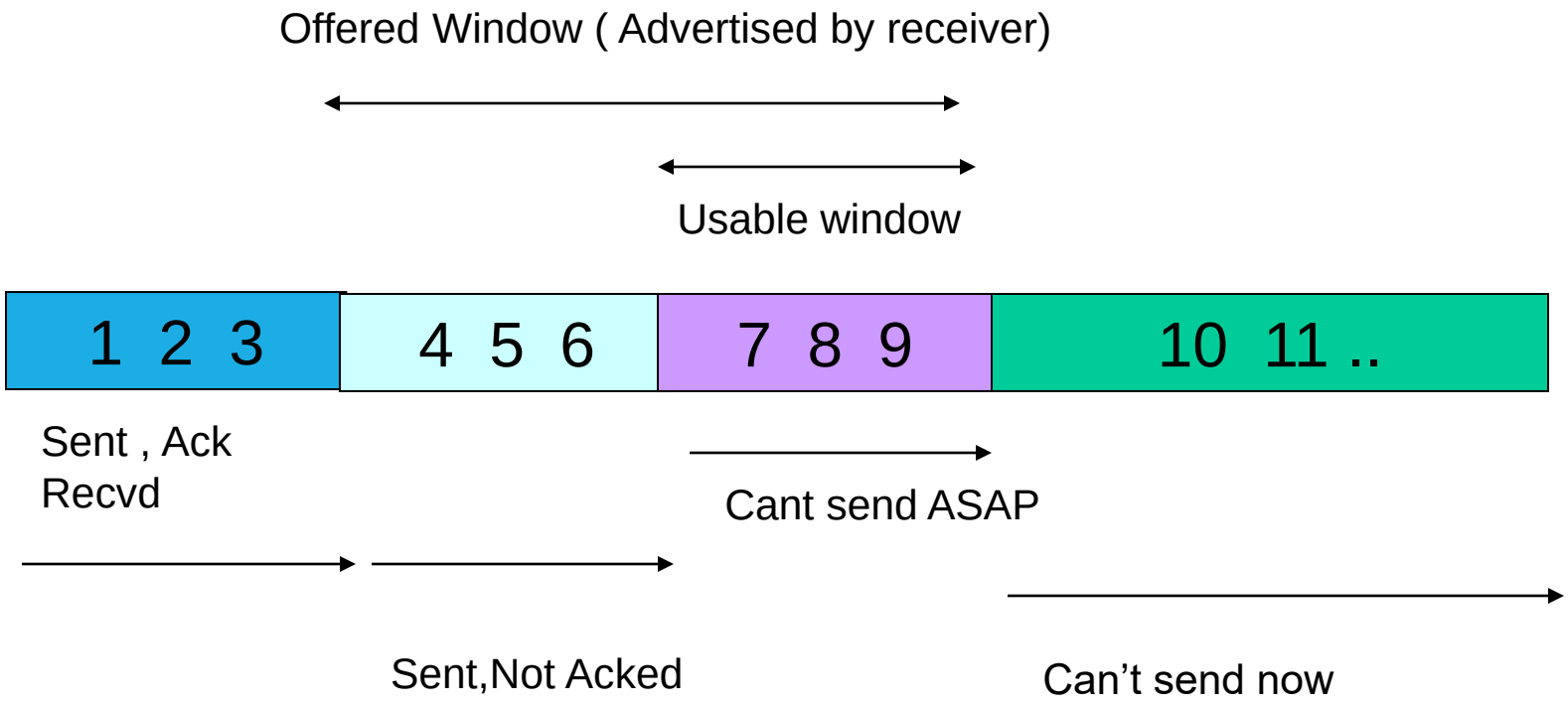
- The TCP on the system that receives this Final FIN (the end that did the active close) acknowledges the FIN.

Necessity of 4 way Handshake

- To implement TCP’S full duplex connection termination reliably.

- To allow old duplicate segments to expire in the network.

TCP – Sliding Window



A sliding window protocol allows a sender to transmit multiple packets before it stops and waits for an acknowledgement.This leads to faster data transfer, since the sender does not have to stop and wait for an acknowledgement each time a packet is sent

Acknowledgement strategy in TCP

- When data arrives at the receiver, the protocol specifies that it send back an acknowledgement of this data
  - Bytes of data are sequentially numbered so the receiver can acknowledge data by naming the highest numbered byte of data it has received , which also acknowledges the previous bytes (actually it identifies the first byte of data which it has not yet received)
  - So the acknowledgement mechanism is cumulative.

User Datagram Protocol (UDP)

Computer Networks
May 16,2011

TOC

User Datagram Protocol

- The User Datagram Protocol is defined to make available a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. This protocol assumes that the Internet Protocol (IP) is used as the underlying protocol.

- Each output operation in a process produces exactly one UDP datagram, which causes one IP datagram to be sent .

✓This is different from TCP where the amount of data written by an application may have little relationship to what actually gets sent in a single IP datagram .

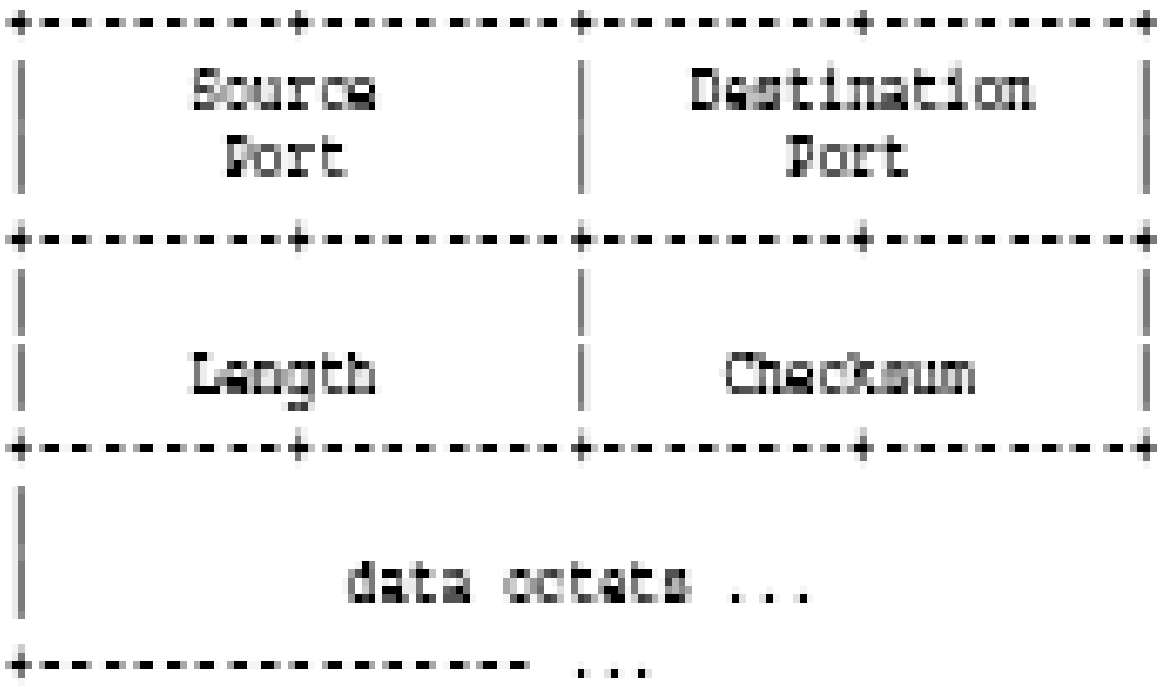
UDP -Features

- This protocol provides a procedure for application programs to send messages to other programs with a minimum of protocol mechanism.

- The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed.

- Applications requiring ordered reliable delivery of streams of data should use the Transmission Control Protocol (TCP) .

UDP Datagram Header Format



References

Computer networks ,Andrew S. Tanenbaum

Computer networking ,James F. Kurose, Keith W. Rose

Disclaimer

Altran Group makes no representations or warranties with respect to contents of these slides and the same are being provided "as is". The content/materials in the slides are of a general nature and are not intended to address the specific circumstances of any particular individual or entity. The material may provide links to internet sites (for the convenience of users) over which Altran Group has no control and for which Altran Group assumes no responsibility for the availability or content of these external sites. While the attempt has been to acknowledge sources of materials wherever traceable to an individual or an institution; any materials not specifically acknowledged is purely unintentional

Any Questions?

Thanks


ALTRAN