NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 1: Introduction to Ethical Hacking

CONCEPTS COVERED

- What is ethical hacking?
- Penetration testing
- Role of the ethical hacker

What is Ethical Hacking?

- It refers to the act of locating weaknesses and vulnerabilities of computer and information systems by replicating the intent and actions of malicious hackers.
- It is also known as *penetration testing*, *intrusion testing* or *red teaming*.

Introduction to Ethical Hacking

- **Ethical Hackers**
  - Employed by companies to perform penetration test.
- **Penetration Test**
  - Legal attempt to break into the company's network to find the weak links.
  - Tester only report findings, does not provide solutions.
- **Security Test**
  - Also includes analyzing company's security policy and procedures.
  - Tester offers solutions to secure or protect the network.

Some Terminologies

- **Hacking** - showing computer expertise.
- **Cracking** - breaching security on software or systems.
- **Spoofing** - faking the originating IP address in a datagram.
- **Denial of Service (DoS)** - flooding a host with sufficient network traffic so that it cannot respond anymore.
- **Port Scanning** - searching for vulnerabilities.

Gaining access

- **Front door**
  - Password guessing
  - Password/key stealing
- **Back doors**
  - Often left by original developers as debug and/or diagnostic tools.
- **Trojan Horses**
  - Usually hidden inside of software that we download and install from the net.
  - Many install backdoors.

- **Software vulnerability exploitation**
  - Often advertised on the OEMs web site along with security patches.
  - Fertile ground for script kiddies looking for something to do.

Once inside, the hacker can...

- Modify logs
  - To cover their tracks.
- Steal files
  - Sometimes destroy after stealing.
  - An expert hacker would steal and cover their tracks to remain undetected.
- Modify files
  - To let you know they were there.
  - To cause mischief.
- Install back doors
  - So they can get in again.
- Attack other systems

The Role of Security and Penetration Testers

- Script kiddies or packet monkeys
  - Young or inexperienced hackers.
  - Copy codes and techniques from knowledgeable hackers.
- Experienced penetration testers write programs or scripts using
  - Perl, C, C++, Python, JavaScript, Visual Basic, SQL, and many others.

Penetration-Testing Methodologies

- **Tiger box**
  - Collection of OSs and hacking tools.
  - Usually on a laptop.
  - Helps penetration testers and security testers conduct vulnerabilities assessments and attacks.
- **White box model**
  - Tester is told everything about the network topology and technology.
  - Tester is authorized to interview IT personnel and company employees.
  - Makes tester's job a little easier.

- **Black box model**
  - Tester is not given details about the network.
  - Burden is on the tester to find the details.
- **Gray box model**
  - Hybrid of the white and black box models.
  - Company gives tester partial information.

What You Can Do Legally

- Laws involving technology change as rapidly as technology itself.
- Find what is legal for you locally.
  - Laws change from place to place.
- Be aware of what is allowed and what is not allowed.

Laws of the Land

- Tools on your computer might be illegal to possess.
- Contact local law enforcement agencies before installing hacking tools.
- Written words are open to interpretation.
- Governments are getting more serious about punishment for cybercrimes.

What You Cannot Do Legally

- Accessing a computer without permission is illegal.
- Other illegal actions:
  - Installing worms or viruses
  - Denial of Service attacks
  - Denying users access to network resources
- Be careful your actions do not prevent customers from doing their jobs.

Ethical Hacking in a Nutshell

- What it takes to be a security tester?
  - Knowledge of network and computer technology.
  - Ability to communicate with management and IT personnel.
  - Understanding of the laws.
  - Ability to use necessary tools.

In this course, we shall cover:

- Relevant networking technologies
- Basic cryptographic concepts
- Case studies of secure applications
- Unconventional attacks
- Tools demonstration

FREE ONLINE EDUCATION

swayam

शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

Thank you!

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 2: Basic Concepts of Networking (Part I)

CONCEPTS COVERED

- Types of computer networks
- Circuit switching and packet switching
- Virtual circuits

Networking: Basic Concepts

- Computer Network
  - A communication system for connecting computers / hosts
- Why?
  - Better connectivity
  - Better communication
  - Better sharing of resources
  - Bring people together

Types of Computer Networks

- **Local Area Network (LAN)**
  - Connects hosts within a relatively small geographical area
    - ❖ Same room
    - ❖ Same building
    - ❖ Same campus
- **Wide Area Network (WAN)**
  - Hosts may be widely dispersed
    - ❖ Across campuses
    - ❖ Across cities / countries/ continents

Faster

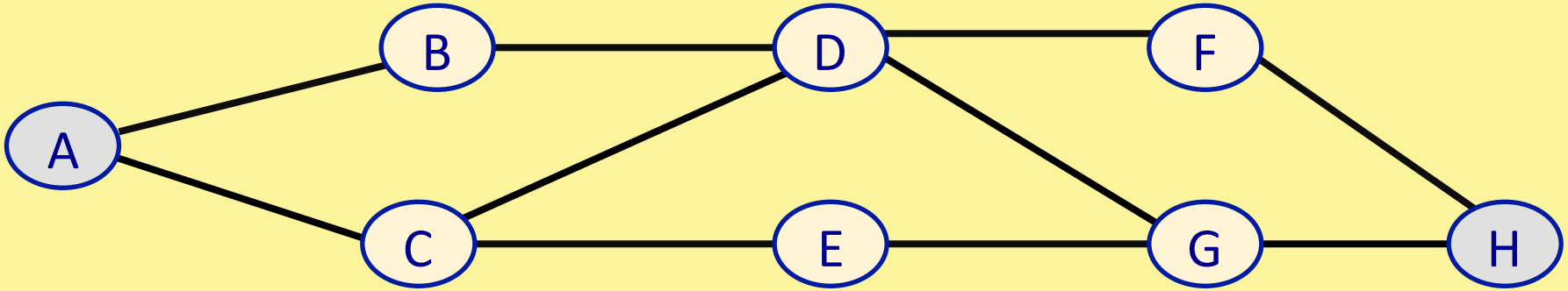
Cheaper

Slower

Expensive

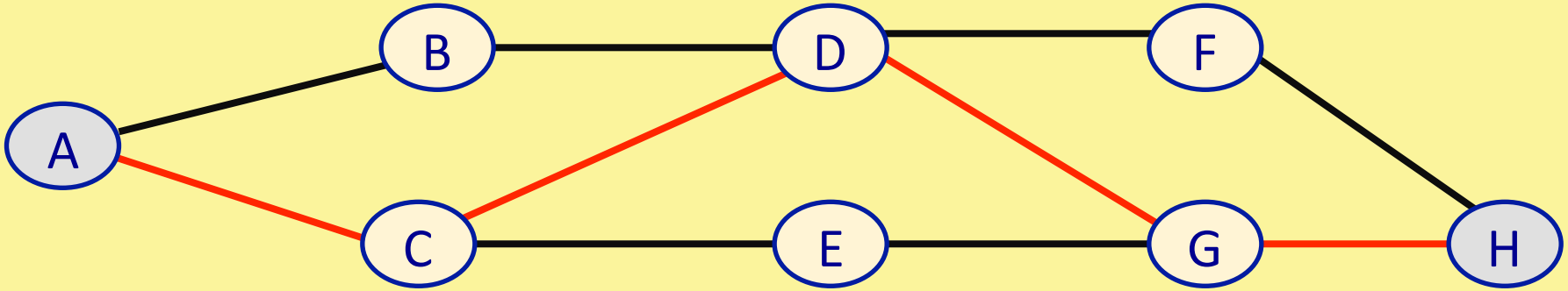
Data Communication over a Network

- Broadly two approaches:
  a) Circuit switching
  b) Packet switching



Circuit Switching

- A dedicated communication path is established between two stations.
  - The path follows a fixed sequence of intermediate links.
  - A logical channel gets defined on each physical link.
    - ❖ Dedicated to the connection.



Circuit Switching (contd.)

- Three steps are required for communication:

  a) **Connection establishment**
     - Required before data transmission.

  b) **Data transfer**
     - Can proceed at maximum speed.

  c) **Connection termination**
     - Required after data transmission is over.
     - For deallocation of network resources.

Circuit Switching (contd.)

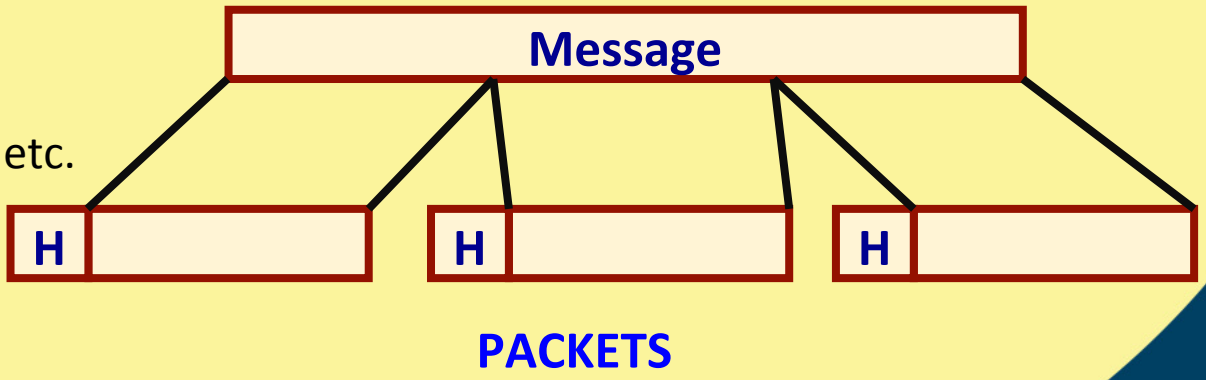
- Drawbacks:
  - Channel capacity is dedicated during the entire duration of communication.
    - ❖ Acceptable for voice communication.
    - ❖ Very inefficient for bursty traffic like data.
  - There is an initial delay.
    - ❖ For connection establishment.

Packet Switching

- Modern form of long-distance data communication.
  - Network resources are not dedicated.
  - A link can be shared.
- The basic technology has evolved over time.
  - Basic concept has remained the same.

Packet Switching (contd.)

- Data are transmitted in short packets (~ Kbytes).
  - A longer message is broken up into smaller *chunks*.
  - The chunks are called *packets*.
  - Every packet contains a *header*.
    - ❖ Relevant information for routing, etc.



Packet Switching (contd.)

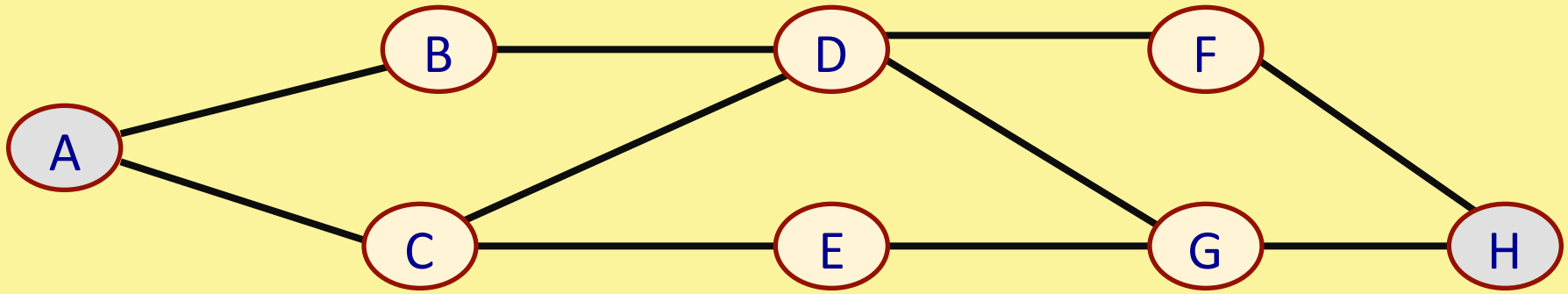
- Packet switching is based on store-and-forward concept.
  - Each intermediate network node receives a whole packet.
  - Decides the route.
  - Forwards the packet along the selected route.
- Each intermediate node (router) maintains a *routing table*.

Packet Switching (contd.)

- Advantages:
  - Links can be shared; so link utilization is better.
  - Suitable for computer-generated (bursty) traffic.
  - Buffering and data rate conversion can be performed easily.
  - Some packets may be given priority over others, if desired.

Packet Switching (contd.)

- How are packets transmitted?
  - Two alternative approaches:
    a) Virtual Circuits
    b) Datagram
- The abstract network model:



(a) Virtual Circuit Approach

- Similar in concept to circuit switching.
  - A route is established before packet transmission starts.
  - All packets follow the same path.
  - The links comprising the path are not dedicated.
    - ❖ Different from circuit switching in this respect.
- Analogy:
  - Telephone system.

(a) Virtual Circuit Approach (contd.)

- How it works?
  - Route is established a priori.
  - Packet forwarded from one node to the next using store-and-forward scheme.
  - Only the virtual circuit number need to be carried by a packet.
    - ❖ Each intermediate node maintains a table.
    - ❖ Created during route establishment.
    - ❖ Used for packet forwarding.
  - No dynamic routing decision is taken by the intermediate nodes.

FREE ONLINE EDUCATION

swayam

शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

Thank you!

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 3: Basic Concepts of Networking (Part II)

CONCEPTS COVERED

- Datagrams
- Layered network architecture

(b) Datagram Approach

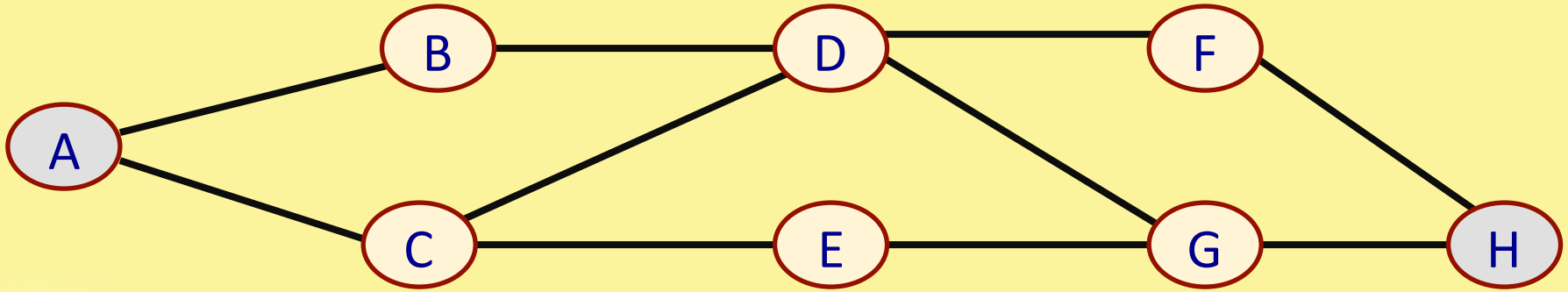
- Basic concept:
  - No route is established beforehand.
  - Each packet is transmitted as an independent entity.
  - Does not maintain any history.
- Analogy:
  - Postal system.

Datagram Approach (contd.)

- Every intermediate node has to take routing decisions dynamically.
  - Makes use of a *routing table*.
  - Every packet must contain *source and destination addresses*.
- Problems:
  - Packets may be delivered out of order.
  - If a node crashes momentarily, all of its queued packets are lost.
  - Duplicate packets may also be generated.

Datagram Approach (contd.)

- Advantages:
  - Faster than virtual circuit for smaller number of packets.
    - ❖ No route establishment and termination.
  - More flexible.
  - Packets between two hosts may follow different paths.
    - ❖ Can handle congestion/failed link.



Comparative Study

- Three types of delays must be considered:
  a) Propagation Delay
     - Time taken by a data signal to propagate from one node to the next.
  b) Transmission Time
     - Time taken to send out a packet by the transmitter.
  c) Processing Delay
     - Time taken by a node to process a packet.

Circuit Switching

- After initial circuit establishment, data bits sent continuously without any delay.

Virtual Circuit Packet Switching

- The *Call Request* packet sent from source to destination.
- The *Call Accept* packet returns back.
- Packets sent sequentially in a pipelined fashion.
  - Store-and-forward approach.

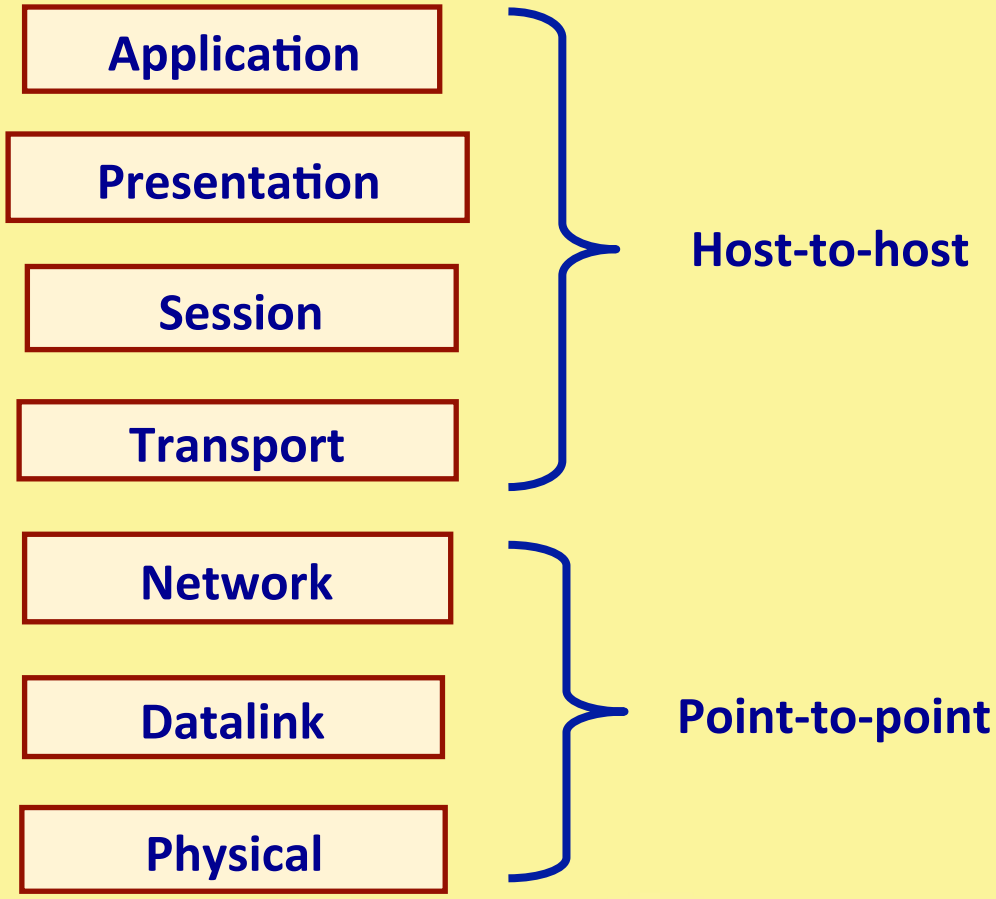
Datagram Packet Switching

- No initial delay.
- The packets are sent out independently.
  - May follow different paths.
  - Also follows store-and-forward approach.

Layered Network Architecture

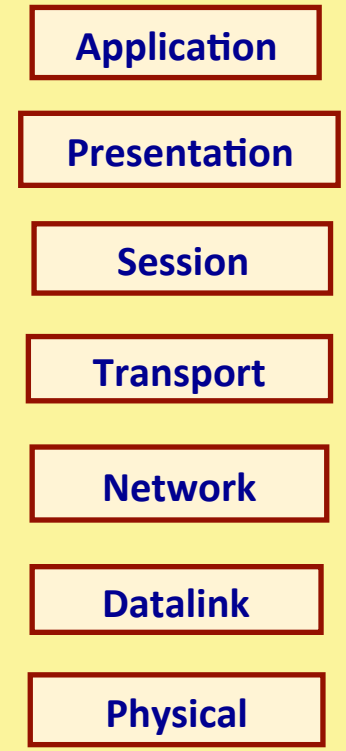
- Open systems interconnection (OSI) reference model.
  - Seven layer model.
  - Communication functions are partitioned into a hierarchical set of layers.
- Objective:
  - Systematic approach to design.
  - Changes in one layer should not require changes in other layers.

The 7-layer OSI Model



Layer Functions

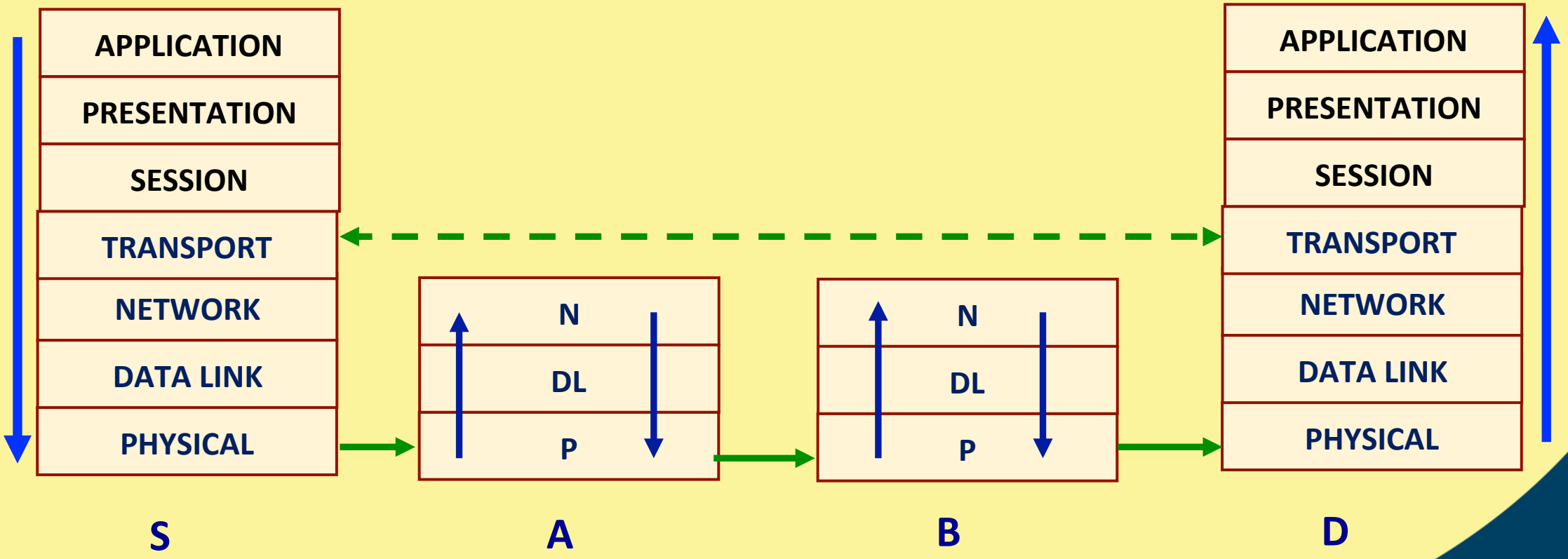
- **Physical**
  - Transmit raw bit stream over a physical medium.
- **Data Link**
  - Reliable transfer of frames over a point-to-point link (flow control, error control).
- **Network**
  - Establishing, maintaining and terminating connections.
  - Routes packets through point-to-point links.



Layer Functions (contd.)

- **Transport**
  - End-to-end reliable data transfer, with error recovery and flow control.
- **Session**
  - Manages sessions.
- **Presentation**
  - Provides data independence.
- **Application**
  - Interface point for user applications.

How Data Flows



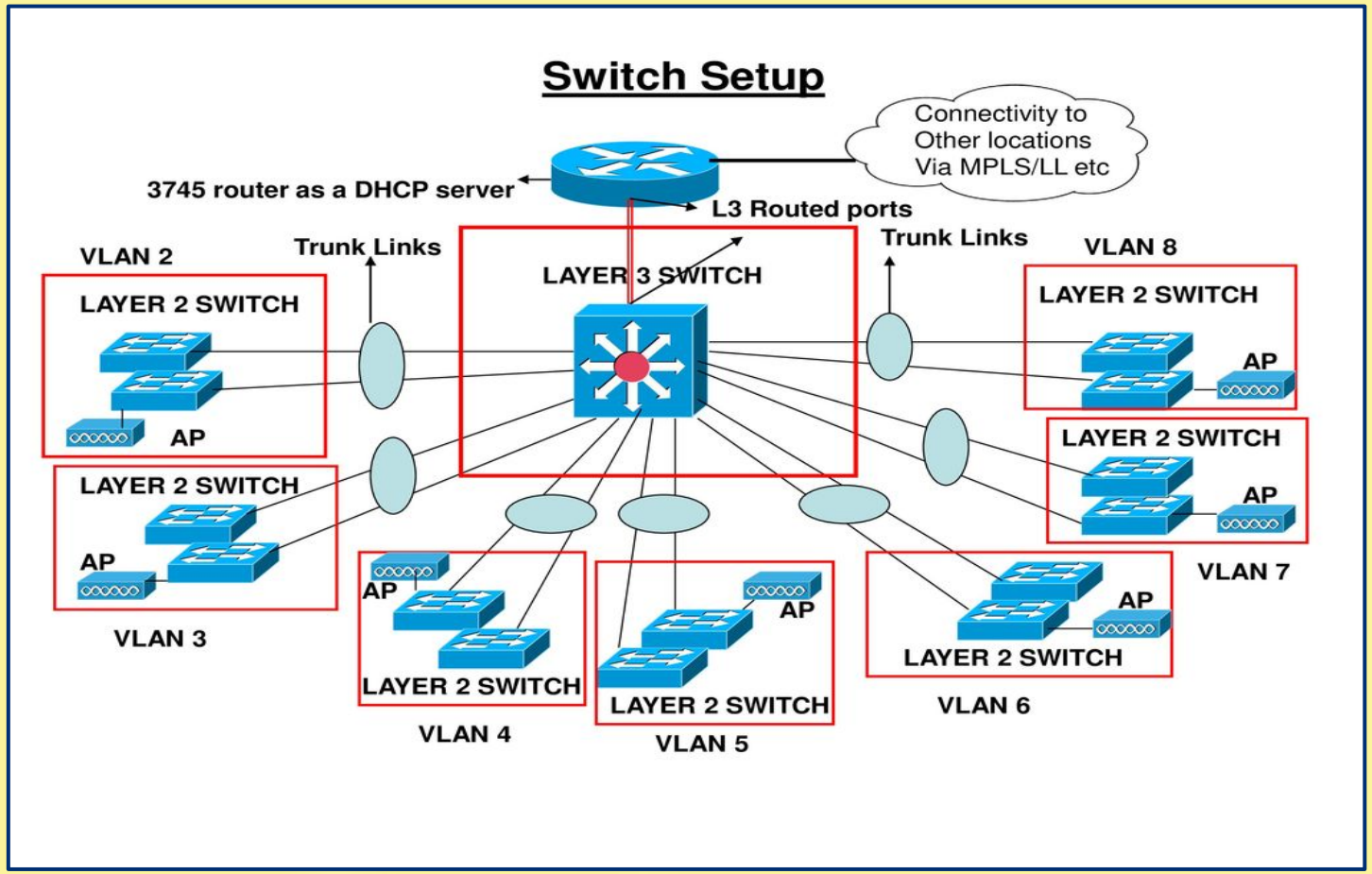
Internetworking Devices

- **Hub**
  - Extends the span of a single LAN.

- **Bridge / Layer-2 Switch**
  - Connects two or more LANs together.
  - Works at data link layer level.

- **Router / Layer-3 Switch**
  - Connects any combination of LANs and WANs.
  - Works at network layer level.

Typical Internetworking Structure



FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

Thank you!

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 4: TCP/IP Protocol Stack (Part I)

CONCEPTS COVERED

- TCP/IP protocol stack
- Basic functions of TCP, UDP and IP
- Data encapsulation

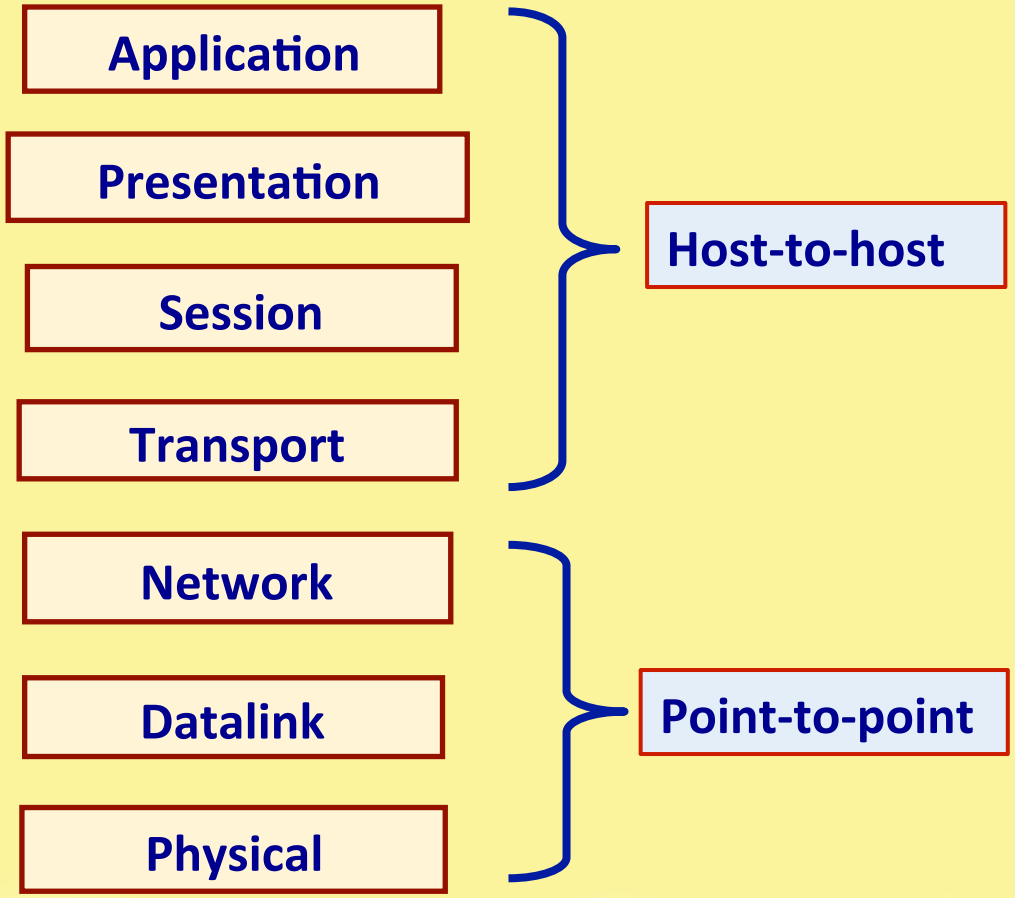
Introduction

- TCP/IP is the most fundamental protocol used in the Internet.
  - Allows computers to communicate / share resources.
  - Used as a standard.
  - To bridge the gap between non-compatible platforms.
- Work on TCP/IP started in the 1970s.
  - Funded by US Military.
  - Advanced Research Project Agency (ARPA).

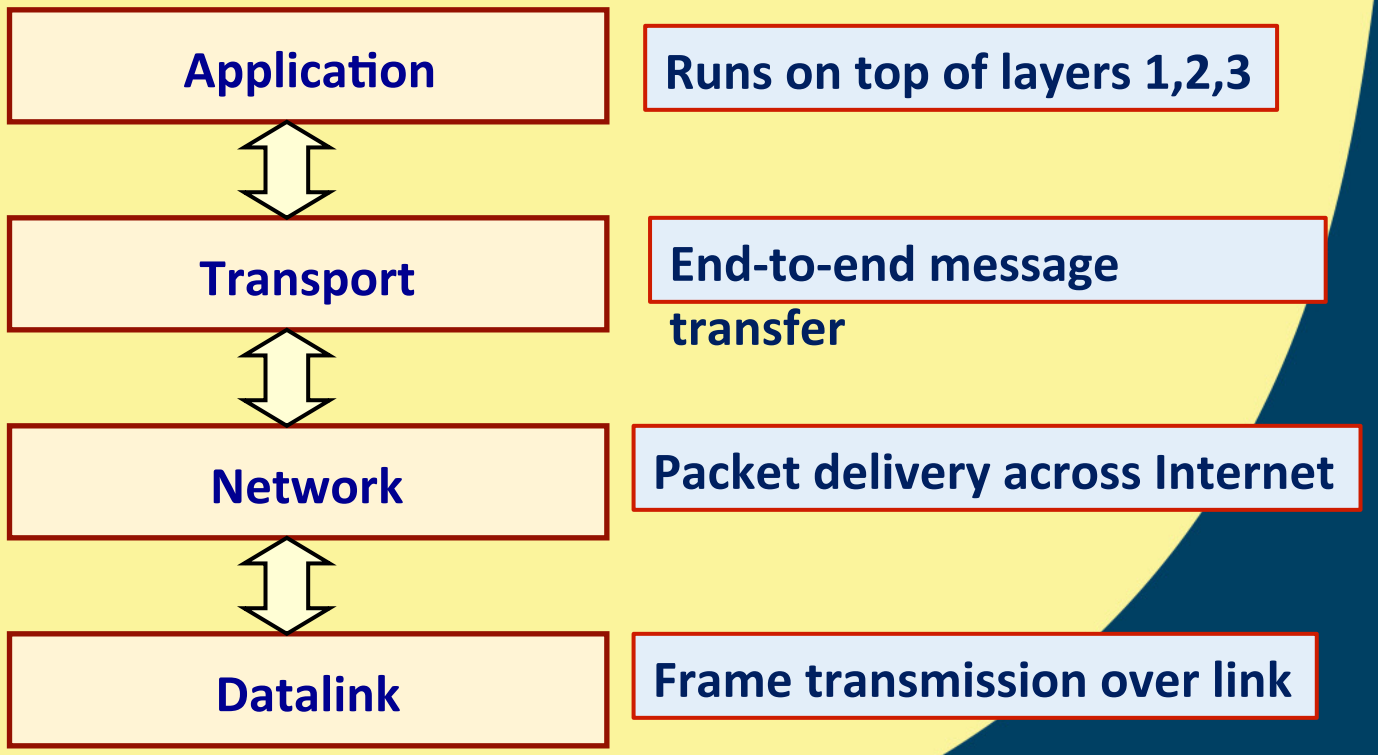
Network Layering in TCP/IP

- In 1978, International Standards Organization (ISO) proposed the 7-layer OSI reference model for network services and protocols.
  - TCP/IP does not strictly follow the OSI model.
  - It follows a simplified 4-layer model.

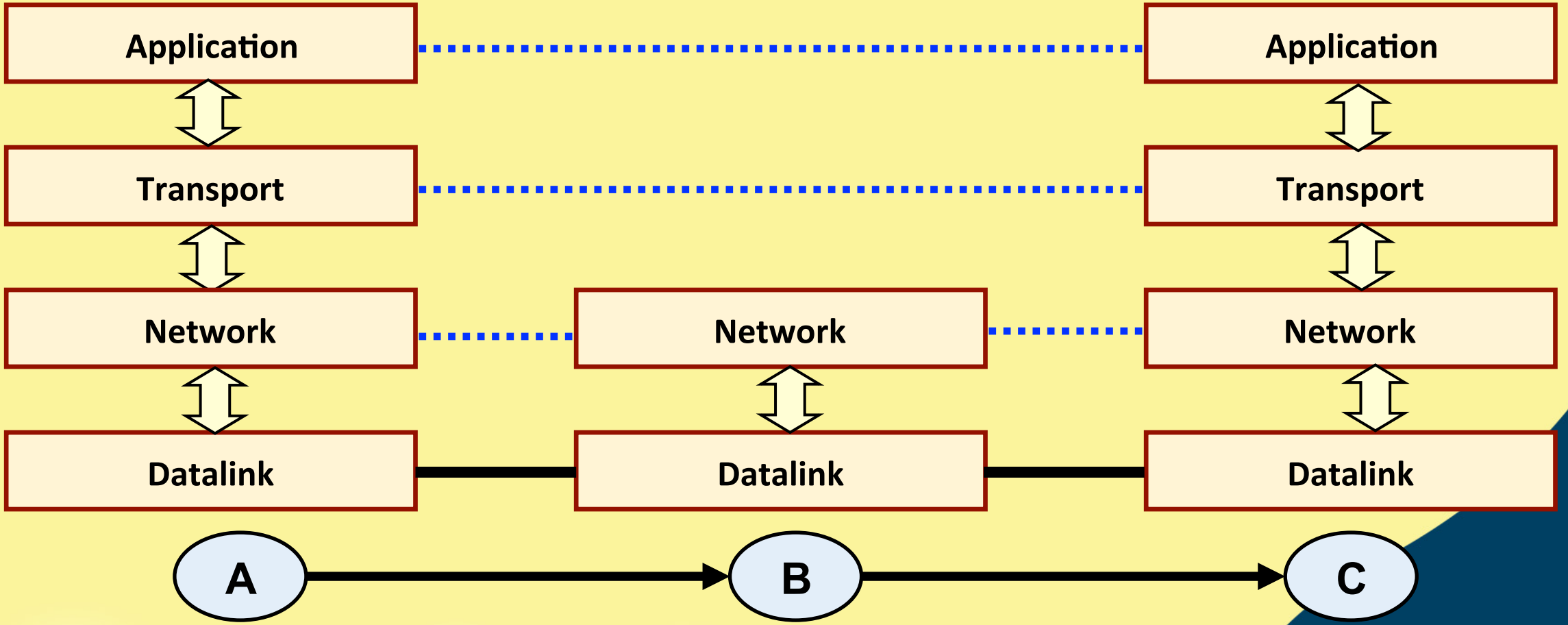
The 7-layer OSI Model



The 4-layer TCP/IP Model



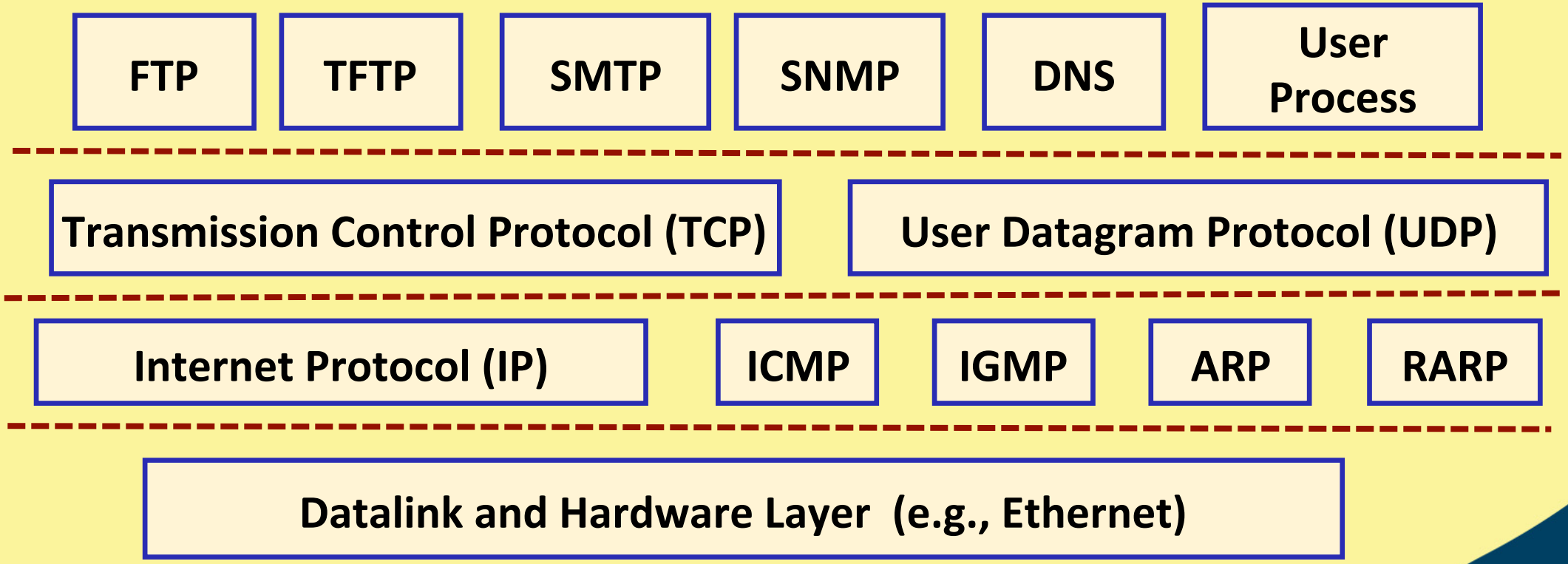
Data Flow in 4-layer Model



TCP/IP Protocol Suite

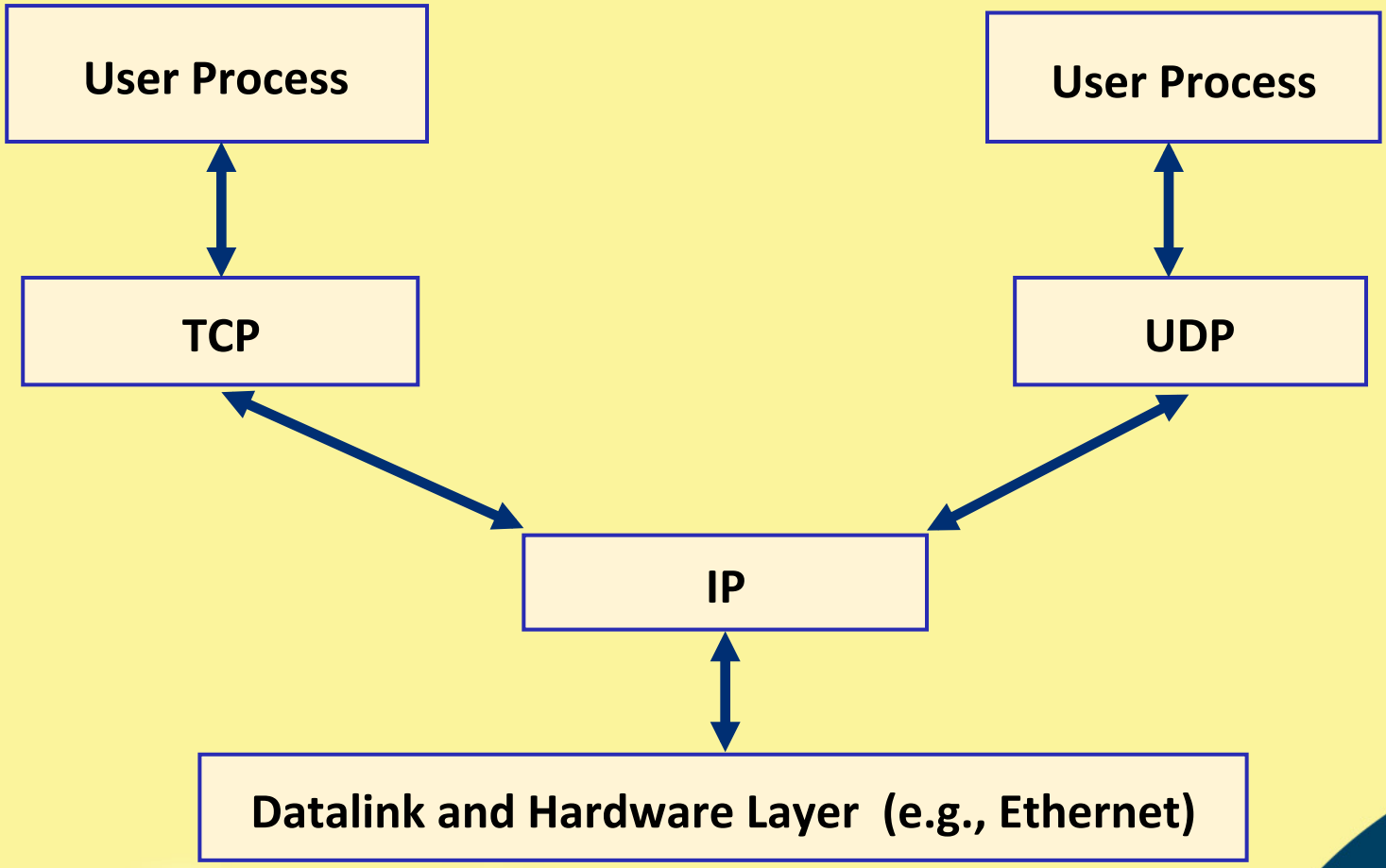
- Refers to a family of protocols.
- The protocols are built on top of connectionless technology (*datagrams*).
  - Data sent from one node to another as a sequence of datagrams.
  - Each datagram is sent independently.
  - The datagrams corresponding to the same message may follow different routes.
    - ❖ Variable delay, arrival order at destination.

TCP/IP Family Members (Partial List)



- **Address Resolution Protocol (ARP)**
  - Map IP addresses to hardware (MAC) addresses.
- **Reverse Address Resolution Protocol (RARP)**
  - Map hardware addresses to IP addresses.
- **Internet Control Message Protocol (ICMP)**
  - A network device can send error messages and other information.
- **Internet Group Management Protocol (IGMP)**
  - A node can send its multicast group membership to adjacent routers.

Typical Scenario



What does IP do?

- IP transports datagrams (packets) from a source node to a destination node.
  - Responsible for routing the packets.
  - Breaks a packet into smaller packets, if required.
  - Unreliable service.
    - ❖ A packet may be lost in transit.
    - ❖ Packets may arrive out of order.
    - ❖ Duplicate packets may be generated.

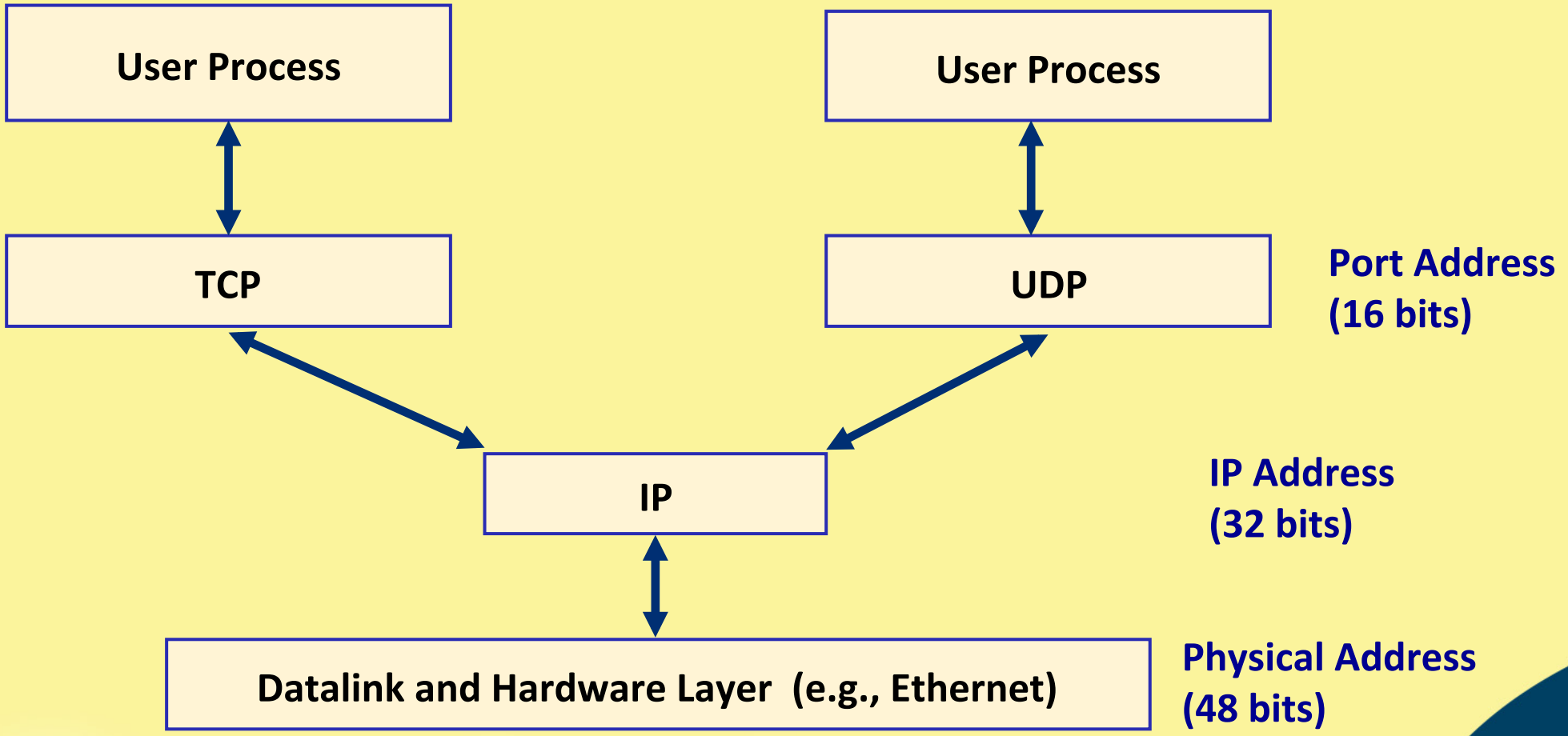
What does TCP do?

- TCP provides a connection-oriented, reliable service for sending messages.
  - Split a message into packets.
  - Reassemble packets at destination.
  - Resend packets that were lost in transit.
- Interface with IP:
  - Each packet forwarded to IP for delivery.
  - Error control is done by TCP.

What does UDP do?

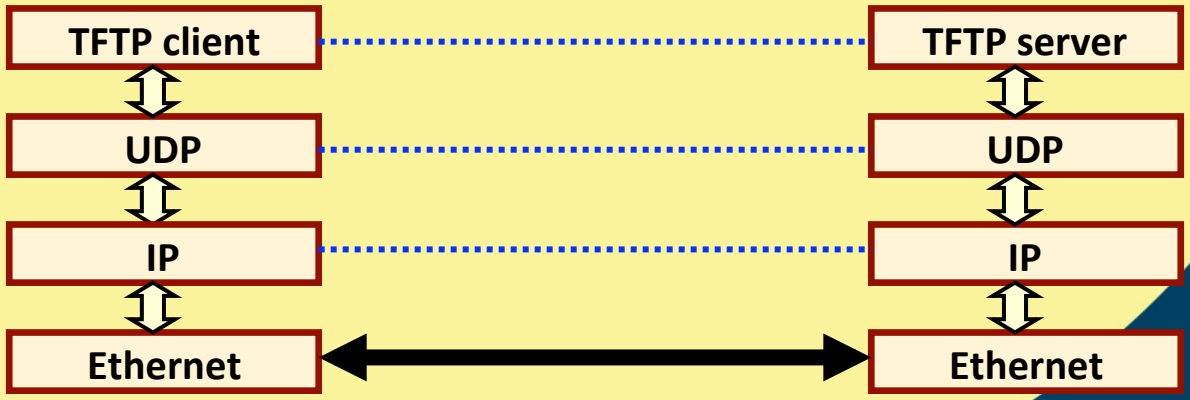
- UDP provides a connectionless, unreliable service for sending datagrams (packets).
  - Messages small enough to fit in a packet (e.g., DNS query).
  - Simpler (and faster) than TCP.
  - Never split data into multiple packets.
  - Does not care about error control.
- Interface with IP:
  - Each UDP packet sent to IP for delivery.

Addresses in TCP/IP

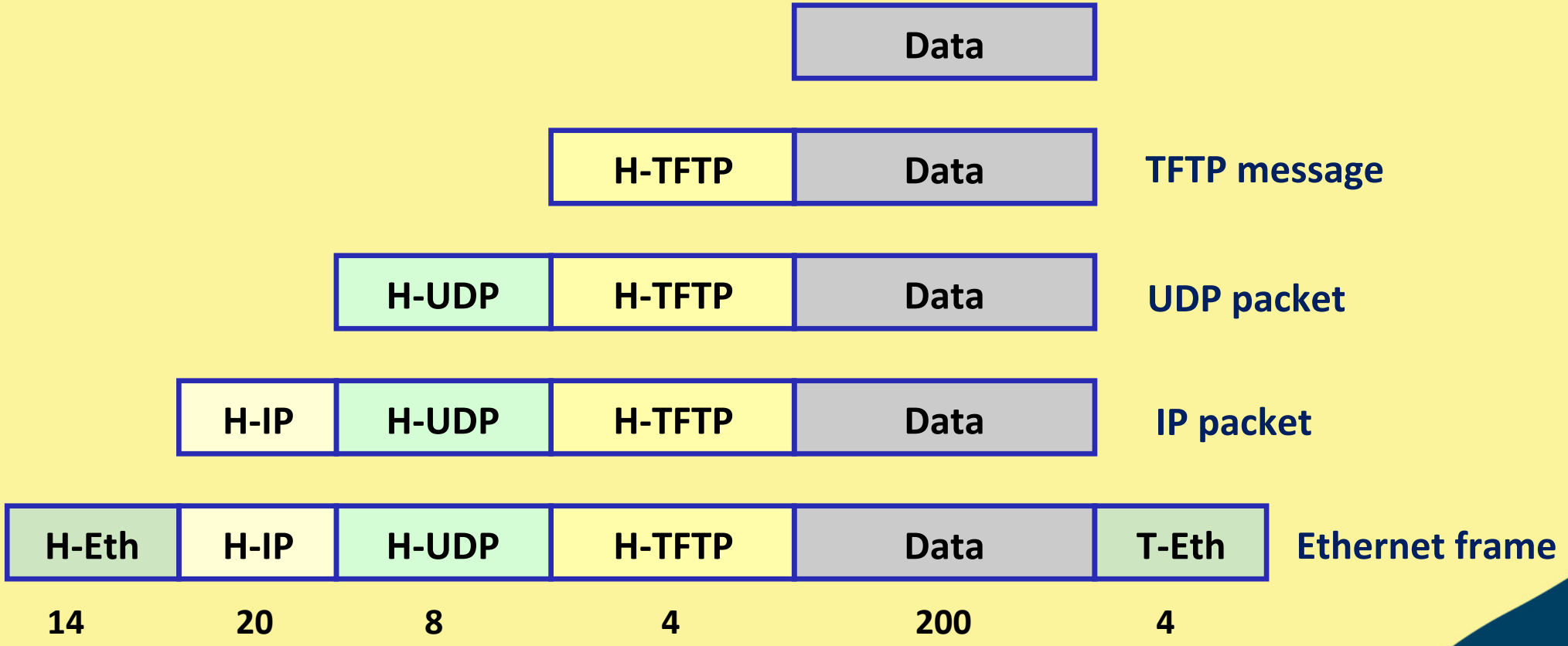


Encapsulation

- Basic concept:
  - As data flows down the protocol hierarchy, headers (and trailers) get appended to it.
  - As data moves up the hierarchy, headers (and trailers) get stripped off.
- An example to illustrate:
  - Trivial file transfer protocol (TFTP).
  - TFTP client transfers 200 bytes of data.
  - 4 bytes of TFTP header gets added.



Encapsulation in TFTP



FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

Thank you!

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 5: TCP/IP Protocol Stack (Part II)

CONCEPTS COVERED

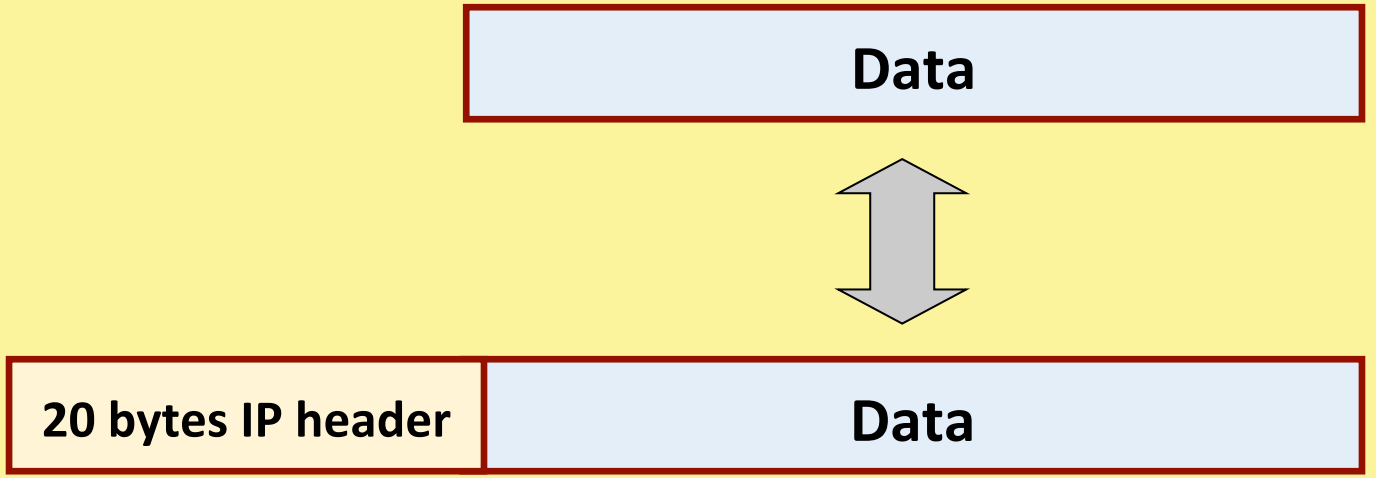
- IP Datagrams
- IP Header fields

IP Datagrams

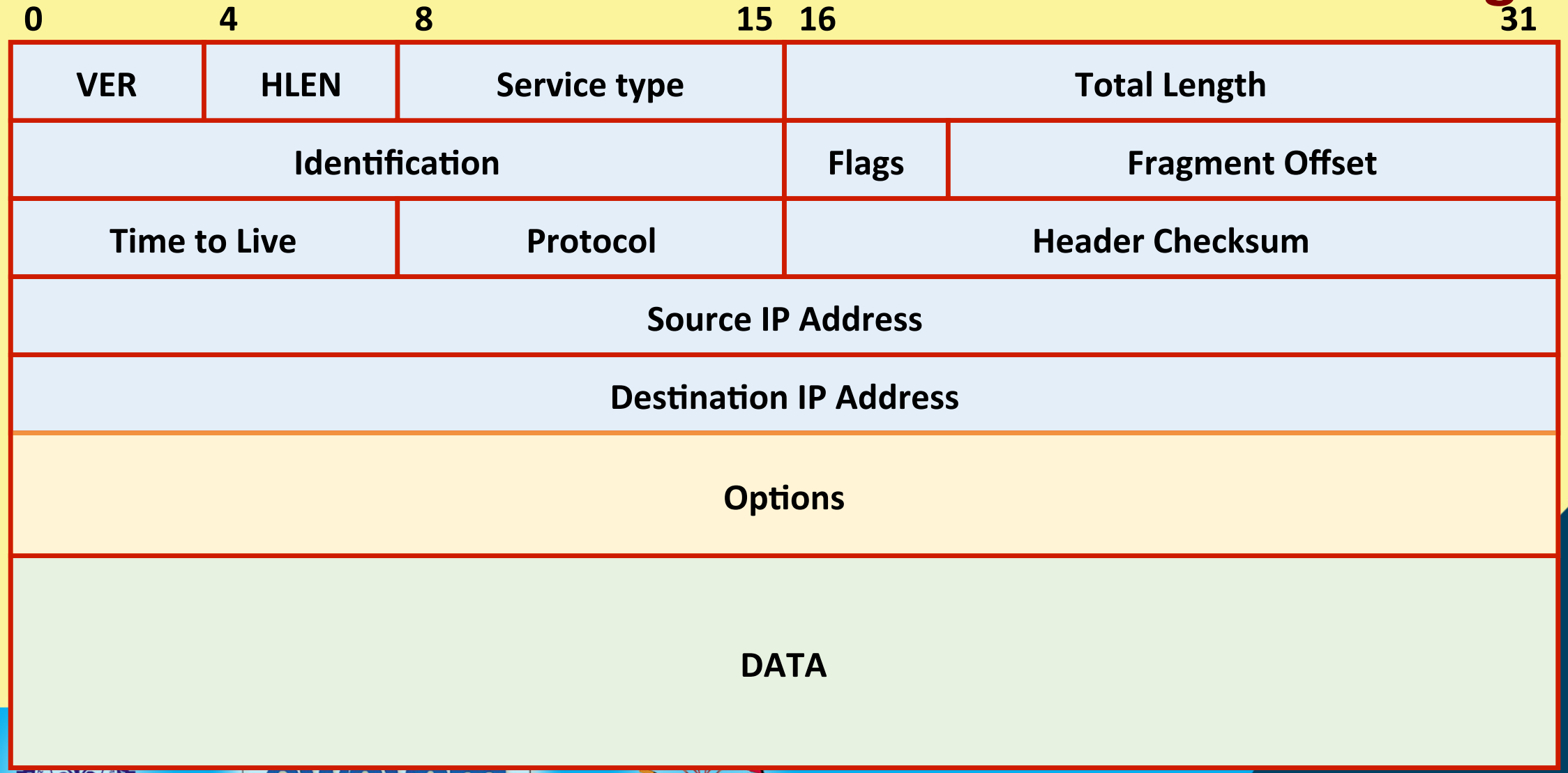
The IP Layer

- IP layer provides a connectionless, unreliable delivery system for packets.
- Each packet is independent of one another.
  - IP layer need not maintain any history.
  - Each IP packet must contain the source and destination addresses.
  - IP layer does not guarantee delivery of packets.
- IP layer encapsulation
  - Receives a data chunk from the higher layer (TCP or UDP).
  - Prepends a header of minimum 20 bytes.
    - ❖ Containing relevant information for handling routing and flow control.

Illustration



Format of IP Datagram



IP Header Fields

- **VER (4 bits)**
  - Version of the IP protocol in use (typically 4).
- **HLEN (4 bits)**
  - Length of the header, expressed as the number of 32-bit words.
  - Minimum size is 5, and maximum 15.
- **Total Length (16 bits)**
  - Length in bytes of the datagram, including headers.
  - Maximum datagram size :: 2^{16} = 65536 bytes.

IP Header Fields (contd.)

- **Service Type (8 bits)**
  - Allows packet to be assigned a priority.
  - Router can use this field to route packets.
- **Time to Live (8 bits)**
  - Prevents a packet from traveling in a loop.
  - Senders sets a value, that is decremented at each hop. If it reaches zero, packet is discarded.
- **Protocol (8 bits)**
  - Identifies the higher layer protocol being used.

IP Header Fields (contd.)

- **Source IP address (32 bits)**
  - Internet address of the sender.
- **Destination IP address (32 bits)**
  - Internet address of the destination.
- **Identification, Flags, Fragment Offset**
  - Used for handling fragmentation.
- **Options (variable width)**
  - Can be given provided router supports.
  - Source routing, for example.

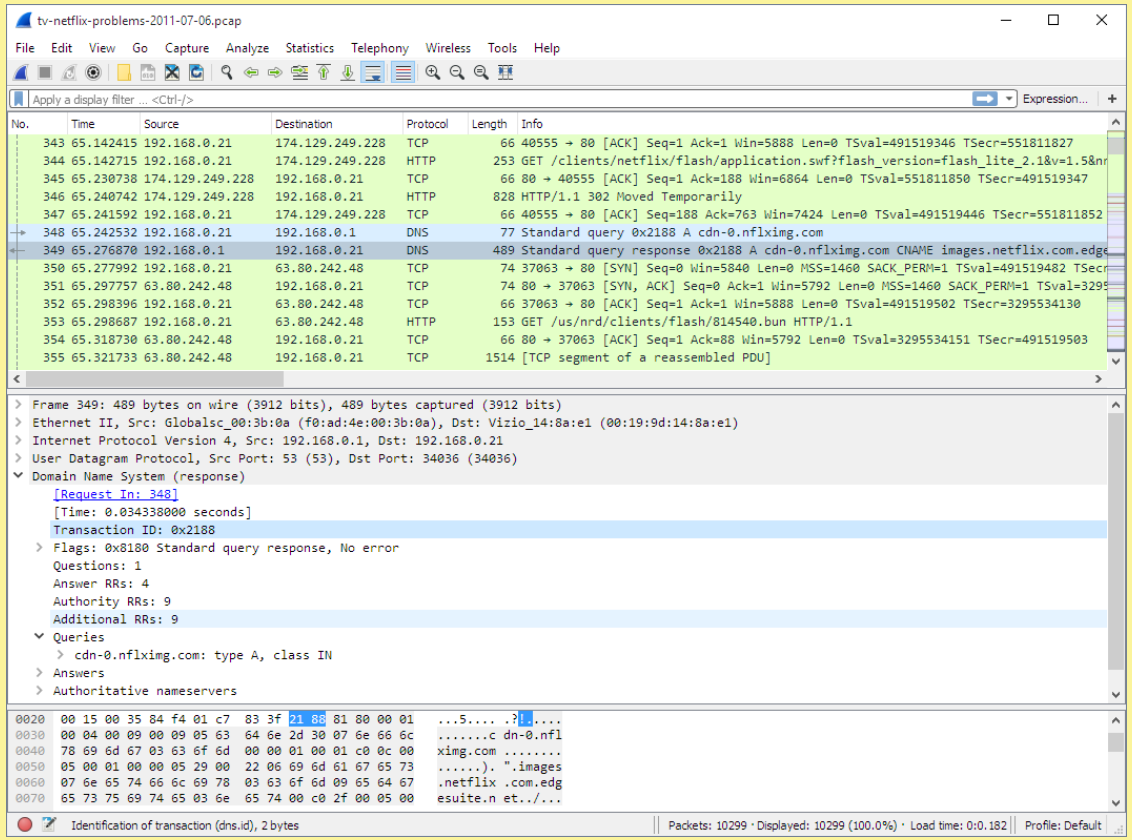
IP Header Fields (contd.)

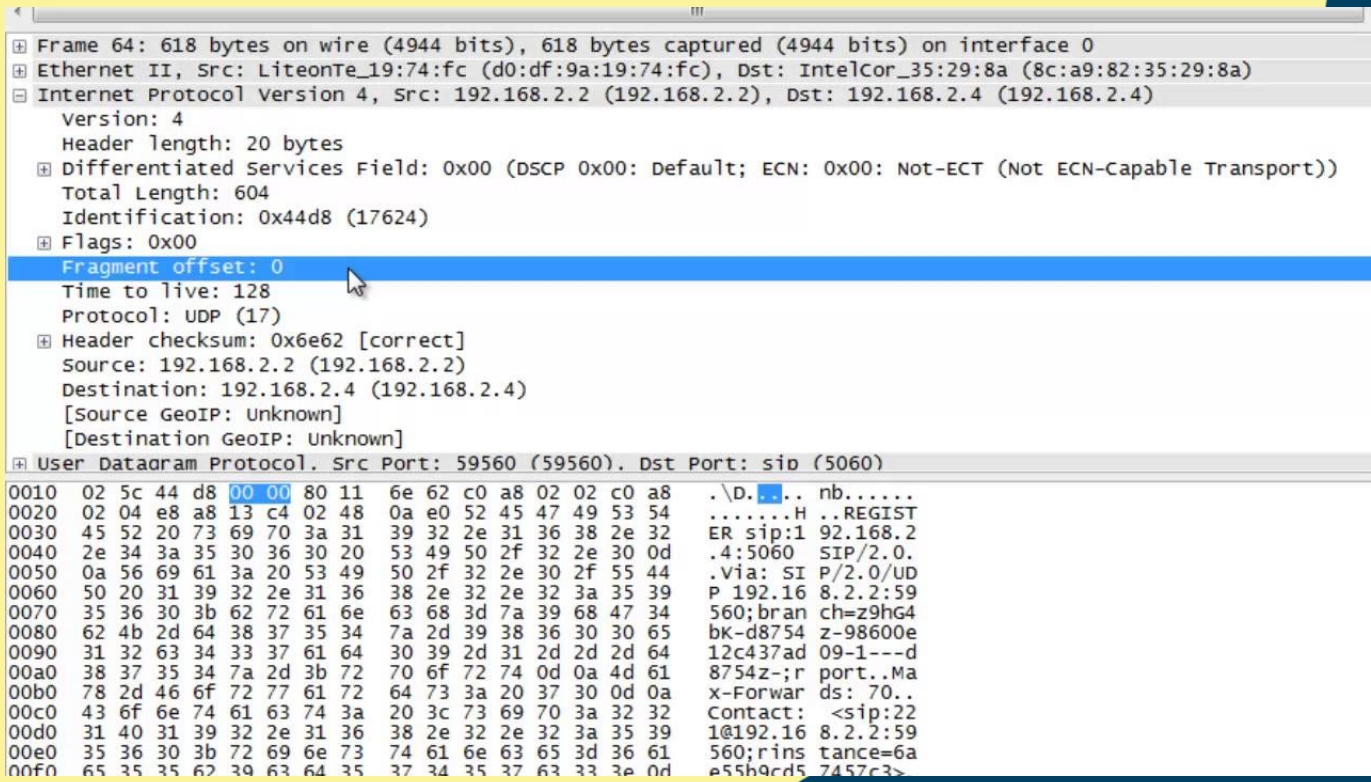
- **Header Checksum (16 bits)**
  - Covers only the IP header.
  - How computed?
    - ❖ Header treated as a sequence of 16-bit integers.
    - ❖ The integers are all added using ones complement arithmetic.
    - ❖ Ones complement of the final sum is taken as the checksum.
  - A mismatch in checksum causes the datagram to be discarded.

Viewing IP Packets

- We can use ***packet sniffers*** to view IP packets.
- Some popular packet sniffers:
  - Wireshark
  - Windump
  - tcpdump
  - Tshark
  - SolarWinds
  - …. and many more

Wireshark …


tv-netflix-problems-2011-07-06.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
343 65.142415 192.168.0.21 174.129.249.228 TCP 66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344 65.142715 192.168.0.21 174.129.249.228 HTTP 253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&n
345 65.230738 174.129.249.228 192.168.0.21 TCP 66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346 65.240742 174.129.249.228 192.168.0.21 HTTP 828 HTTP/1.1 302 Moved Temporarily
347 65.241592 192.168.0.21 174.129.249.228 TCP 66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348 65.242532 192.168.0.21 192.168.0.1 DNS 77 Standard query 0x2188 A cdn-0.nflximg.com
349 65.276870 192.168.0.1 192.168.0.21 DNS 489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
350 65.277992 192.168.0.21 63.80.242.48 TCP 74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
351 65.297757 63.80.242.48 192.168.0.21 TCP 74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
352 65.298396 192.168.0.21 63.80.242.48 TCP 66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353 65.298687 192.168.0.21 63.80.242.48 HTTP 153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354 65.318730 63.80.242.48 192.168.0.21 TCP 66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355 65.321733 63.80.242.48 192.168.0.21 TCP 1514 [TCP segment of a reassembled PDU]
Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
Domain Name System (response)
[Request In: 348]
[Time: 0.034338000 seconds]
Transaction ID: 0x2188
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 4
Authority RRs: 9
Additional RRs: 9
Queries
cdn-0.nflximg.com: type A, class IN
Answers
Authoritative nameservers
0020 00 15 00 35 84 f4 01 c7 83 3f 21 88 81 80 00 01 ...5.... .?!.....
0030 00 04 00 09 00 09 05 63 64 6e 2d 30 07 6e 66 6c ....c dn-0.nfl
0040 78 69 6d 67 03 63 6f 6d 00 00 01 00 01 c0 0c 00 ximg.com ....
0050 05 00 01 00 00 05 29 00 22 06 69 6d 61 67 65 73 ......). ".images
0060 07 6e 65 74 66 6c 69 78 03 63 6f 6d 09 65 64 67 .netflix .com.edg
0070 65 73 75 69 74 65 03 6e 65 74 00 c0 2f 00 05 00 esuite.n et../...
Identification of transaction (dns.id), 2 bytes
Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182
Profile: Default


Frame 64: 618 bytes on wire (4944 bits), 618 bytes captured (4944 bits) on interface 0
Ethernet II, Src: LiteonTe_19:74:fc (d0:df:9a:19:74:fc), Dst: IntelCor_35:29:8a (8c:a9:82:35:29:8a)
Internet Protocol Version 4, Src: 192.168.2.2 (192.168.2.2), Dst: 192.168.2.4 (192.168.2.4)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 604
Identification: 0x44d8 (17624)
Flags: 0x00
Fragment offset: 0
Time to live: 128
Protocol: UDP (17)
Header checksum: 0x6e62 [correct]
Source: 192.168.2.2 (192.168.2.2)
Destination: 192.168.2.4 (192.168.2.4)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 59560 (59560), Dst Port: sip (5060)
0010 02 5c 44 d8 00 00 80 11 6e 62 c0 a8 02 02 c0 a8 .\D..... nb......
0020 02 04 e8 a8 13 c4 02 48 0a e0 52 45 47 49 53 54 ....H ..REGIST
0030 45 52 20 73 69 70 3a 31 39 32 2e 31 36 38 2e 32 ER sip:1 92.168.2
0040 2e 34 3a 35 30 36 30 20 53 49 50 2f 32 2e 30 0d .4:5060 SIP/2.0.
0050 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f 55 44 .Via: SI P/2.0/UD
0060 50 20 31 39 32 2e 31 36 38 2e 32 2e 32 3a 35 39 P 192.16 8.2.2:59
0070 35 36 30 3b 62 72 61 6e 63 68 3d 7a 39 68 47 34 560;bran ch=z9hG4
0080 62 4b 2d 64 38 37 35 34 7a 2d 39 38 36 30 30 65 bK-d8754 z-98600e
0090 31 32 63 34 33 37 61 64 30 39 2d 31 2d 2d 2d 64 12c437ad 09-1---d
00a0 38 37 35 34 7a 2d 3b 72 70 6f 72 74 0d 0a 4d 61 8754z-;r port..Ma
00b0 78 2d 46 6f 72 77 61 72 64 73 3a 20 37 30 0d 0a x-Forwar ds: 70..
00c0 43 6f 6e 74 61 63 74 3a 20 3c 73 69 70 3a 32 32 Contact: <sip:22
00d0 31 40 31 39 32 2e 31 36 38 2e 32 2e 32 3a 35 39 1@192.16 8.2.2:59
00e0 35 36 30 3b 72 69 6e 73 74 61 6e 63 65 3d 36 61 560;rins tance=6a

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

Thank you!