OCW: Unit 4

UNIT 4 - Week 2

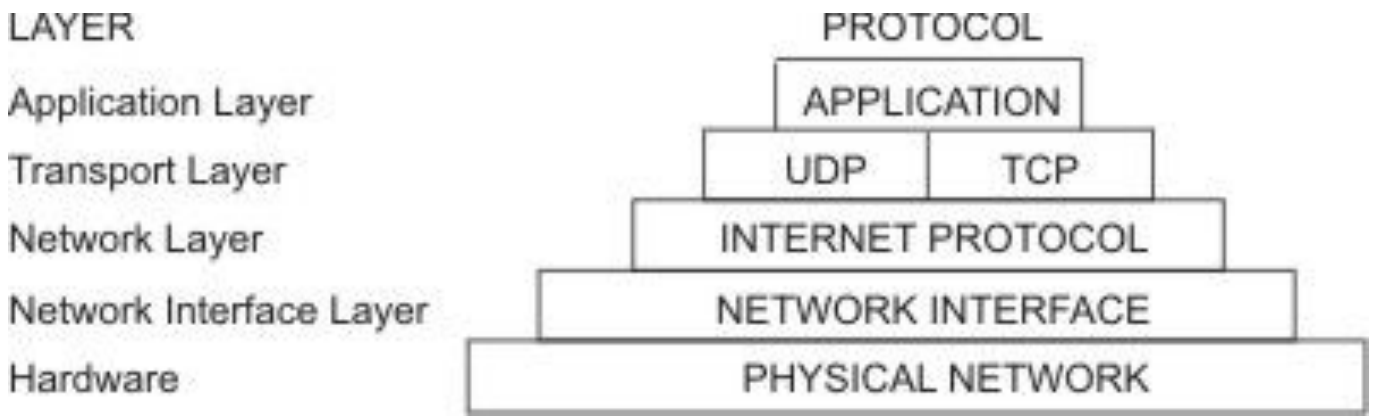
Topics to be covered:

Session 1: TCP/IP, IP Address and significance,

Session 2: Internet and its Protocols (http, https, ftp) - Security related topics

TCP/IP protocol

- Set of rules for message formats and procedures that allow machines and application programs to exchange information.
- defines carefully how the information moves from sender to receiver.
- layers of the **TCP/IP** protocol



TCP/IP protocol

application programs send messages or streams of data to one of the Internet Transport Layer Protocols, either the

User Datagram Protocol (**UDP**) or

Transmission Control Protocol (**TCP**).

Data will be divided into packets and destination address will be added.

Then the packets will be passed to next layer, the internet network layer.

TCP Protocol

TCP sends data in a form that appears to be transmitted in a character-by-character fashion, rather than as discrete packets. This transmission consists of a starting point, which opens the connection, the entire transmission in byte order, and an ending point, which closes the connection.

TCP attaches a header onto the transmitted data. This header contains a large number of parameters that help processes on the sending machine connect to peer processes on the receiving machine.

TCP confirms that a packet has reached its destination by establishing an end-to-end connection between sending and receiving hosts. TCP is therefore considered a "reliable, connection-oriented" protocol.

UDP Protocol

The other transport layer protocol, provides datagram delivery service.

It does not provide any means of verifying that connection was ever achieved between receiving and sending hosts.

Because UDP eliminates the processes of establishing and verifying connections, applications that send small amounts of data use it rather than TCP.

Internet Protocol (IP)

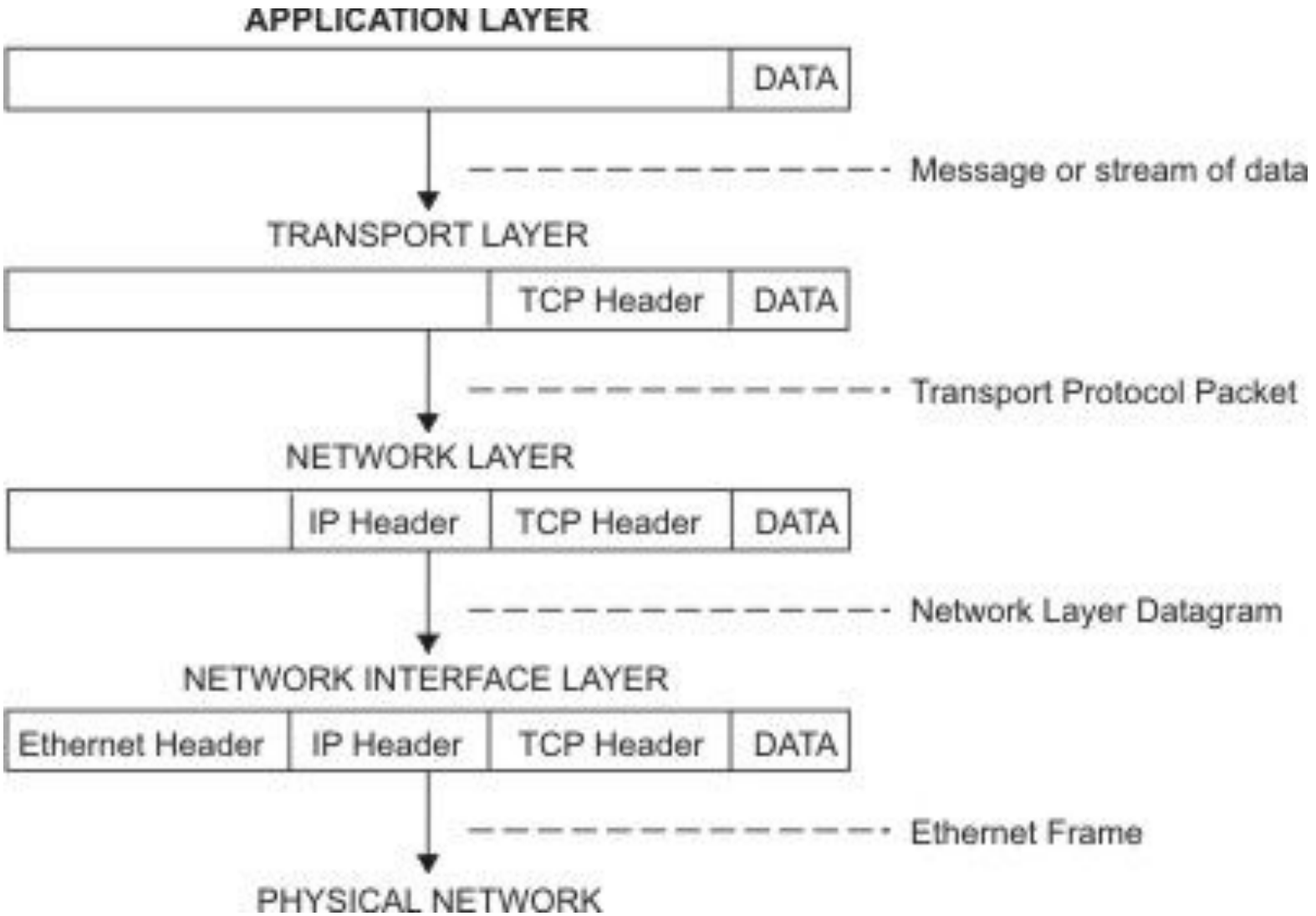
The Internet Network layer encloses the packet in an **Internet Protocol** (**IP**) datagram,

puts in the datagram header and trailer, decides where to send the datagram and

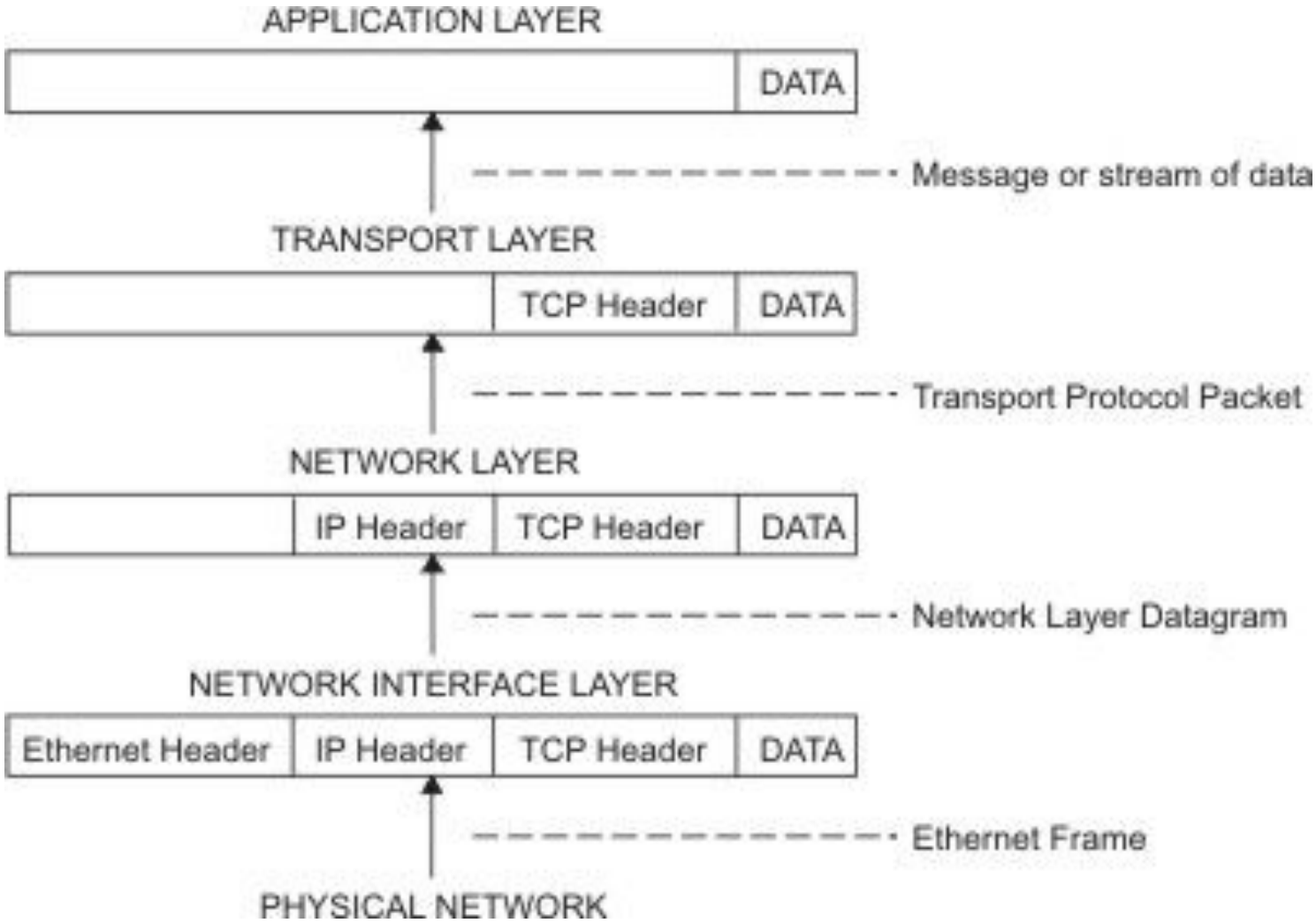
passes the datagram on to the Network Interface layer.

The Network Interface layer accepts **IP** datagrams and transmits them as *frames* over a specific network hardware, such as Ethernet

Flow of information “down” the TCP/IP protocol layers



flow of information “up” the **TCP/IP** protocol layers



TCP/IP Addressing

allows users and applications to identify a specific network or host with which to communicate.

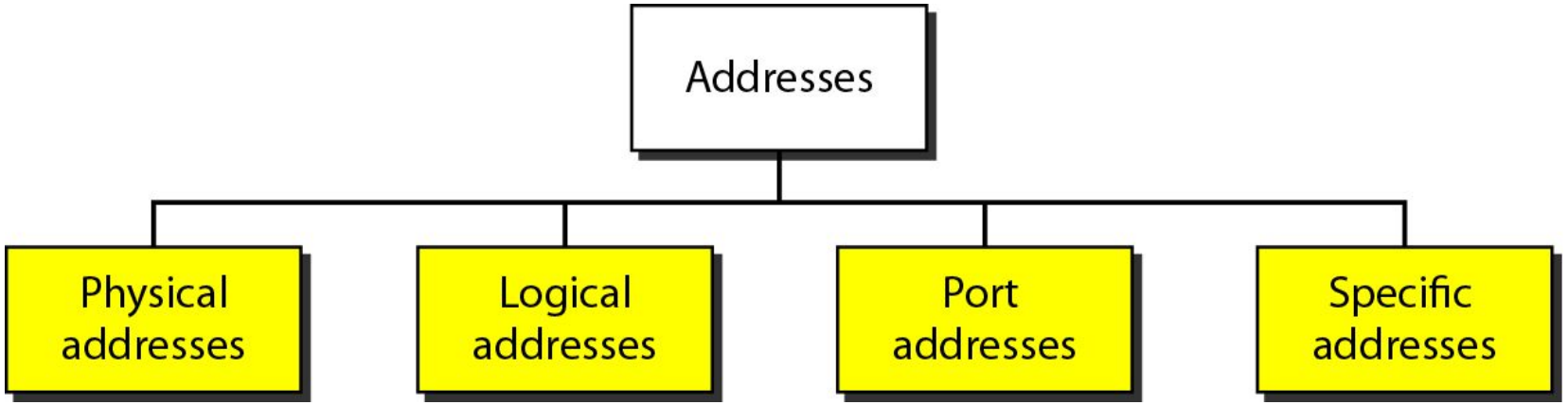
TCP/IP provides standards for assigning addresses to networks, subnetworks, hosts, and sockets, and for using special addresses for broadcasts and local loopback.

Internet addresses are made up of a network address and a host (or local) address.

This two-part address allows a sender to specify the network as well as a specific host on the network.

A unique, official network address is assigned to each network when it connects to other Internet networks.

Addresses in TCP/IP



Basic Structure of an IP Address

- 32 bit number (4 octet number):
  (e.g. 133.27.162.125)
- Decimal Representation:

133	27	162	125

- Binary Representation:

10000101	00011011	10100010	01111101

- Hexadecimal Representation:

85	1B	A2	7D

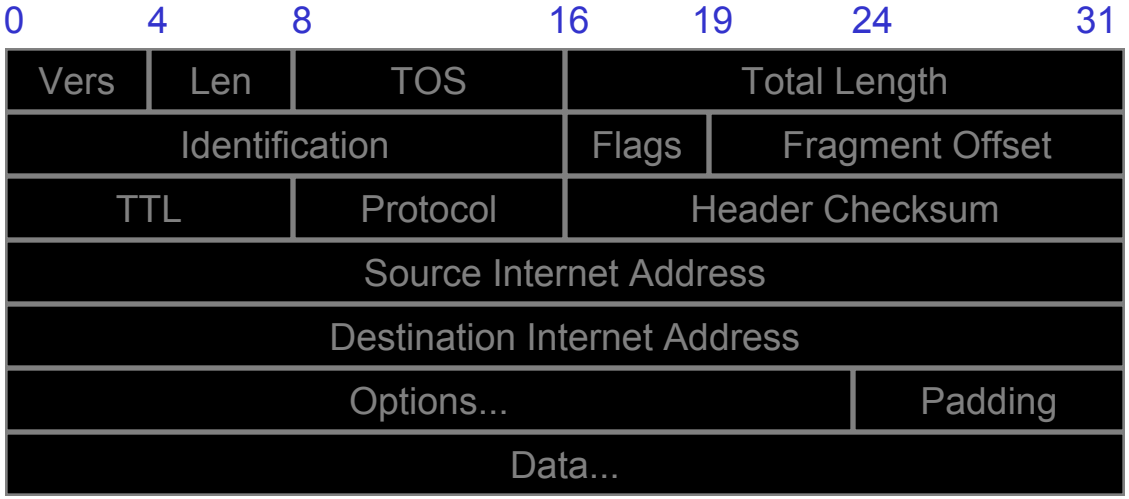
IP Address Classes

- Class A - 168.212.226.204
- supports 16 million hosts on each of 127 networks
- Class B - 168.212.226.204
- supports 65,000 hosts on each of 16,000 networks
- Class C - 168.212.226.204
- supports 254 hosts on each of 2 million networks

IP

- Responsible for end to end transmission
- Sends data in individual packets
- Maximum size of packet is determined by the networks
  - Fragmented if too large
- Unreliable
  - Packets might be lost, corrupted, duplicated, delivered out of order

IP Datagram



Field	**Purpose**
Vers	IP version number
Len	Length of IP header (4 octet units)
TOS	Type of Service
T. Length	Length of entire datagram (octets)
Ident.	IP datagram ID (for frag/reassembly)
Flags	Don't/More fragments
Frag Off	Fragment Offset

Field	**Purpose**
TTL	Time To Live - Max # of hops
Protocol	Higher level protocol (1=ICMP, 6=TCP, 17=UDP)
Checksum	Checksum for the IP header
Source IA	Originator's Internet Address
Dest. IA	Final Destination Internet Address
Options	Source route, time stamp, etc.
Data...	Higher level protocol data

You just need to know the IP addresses, TTL and protocol #

IPv4 vs. IPv6

- IPv4
  - 32 bits used for address
  - Addresses not assigned by geographic region
- IPv6
  - 128 bits used for address
  - Addresses will be assigned by geographic region

IPv4 vs. IPv6

- IPv4 addresses written as four octets (8 bits) separated by periods.
  - 134.129.67.235
- IPv6 address written as eight 4-digit (16-bit) hexadecimal numbers separated by colons.
  - 1080:0:0:0:0:800:0:417A

Allocation of addresses

- Controlled centrally by ICANN
  - Fairly strict rules on further delegation to avoid wastage
    - Have to demonstrate actual need for them
- Organizations that got in early have bigger allocations than they really need

•***I**nternet **C**orporation for **A**ssigned **N**ames and **N**umbers*

Purpose of an IP address

Unique Identification of

–Source

Sometimes used for security or policy-based filtering of data

–Destination

So the networks know where to send the data

Network Independent Format

–IP over anything

Network security

- field of network security:
  - how bad guys can attack computer networks
  - how we can defend networks against attacks
  - how to design architectures that are immune to attacks
- Internet not originally designed with (much) security in mind
  - *original vision:* "a group of mutually trusting users attached to a transparent network" ☺
  - Internet protocol designers playing "catch-up"
  - security considerations in all layers!

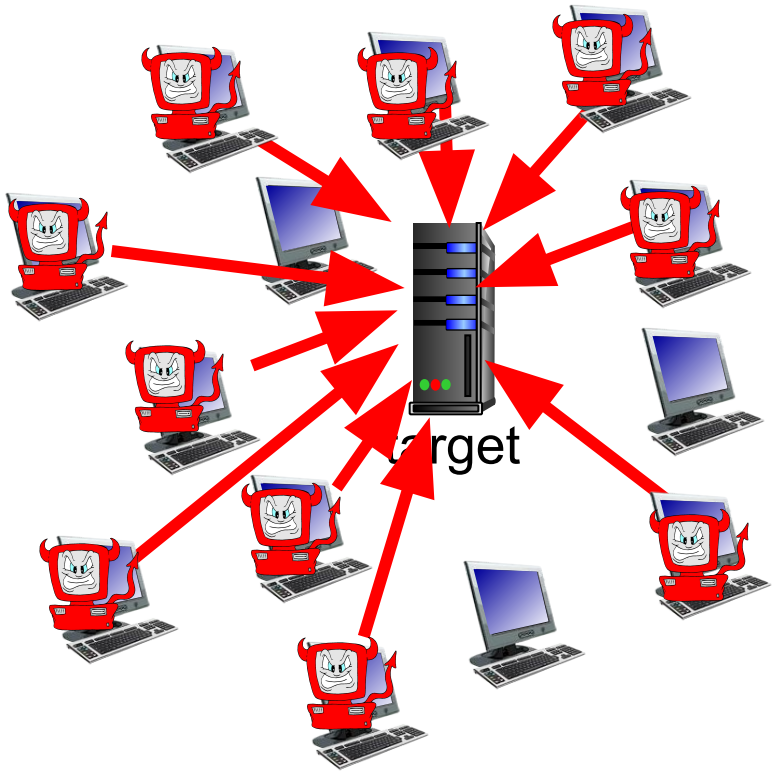
Bad guys: put malware into hosts via Internet

- malware can get in host from:
  - *virus:* self-replicating infection by receiving/executing object (e.g., e-mail attachment)
  - *worm:* self-replicating infection by passively receiving object that gets itself executed
- spyware malware can record keystrokes, web sites visited, upload info to collection site
- infected host can be enrolled in botnet, used for spam. DDoS attacks

Bad guys: attack server, network infrastructure

Denial of Service (DoS): attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

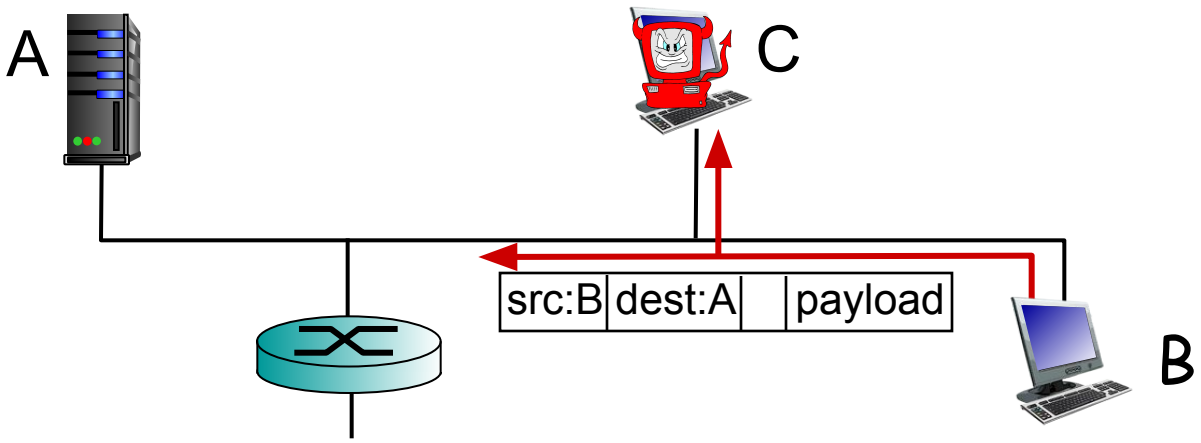
1. select target
2. break into hosts around the network (see botnet)
3. send packets to target from compromised hosts



Bad guys can sniff packets

packet "sniffing":

- broadcast media (shared ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



- wireshark software used for end-of-chapter labs is a (free) packet-sniffer

Bad guys can use fake addresses

IP spoofing: send packet with false source address