# Networks, Security, and Privacy

## 158.235



A/  ard

Massey Uni

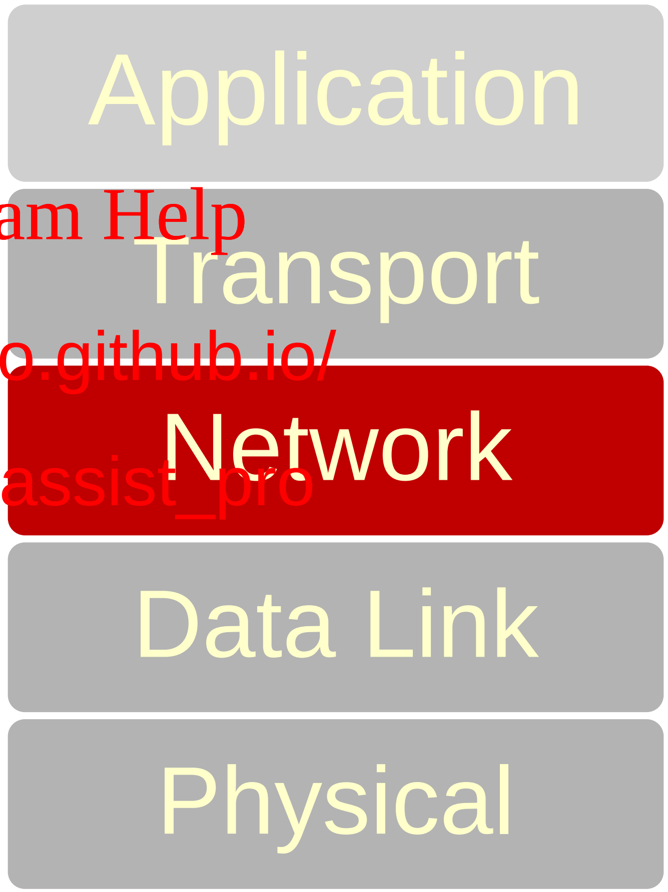
# Lay

*Reading: Chapter 5 in the prescribed textbook*

# Network Layer

- **Layer 3 in the Internet model**
  - **Responsible for moving messages from a source computer destinatio**
- **Main function:**
  - **IP fragmentation**
  - **Addressing**
  - **Routing**

**Internet Model**



# Network Layer Protocols

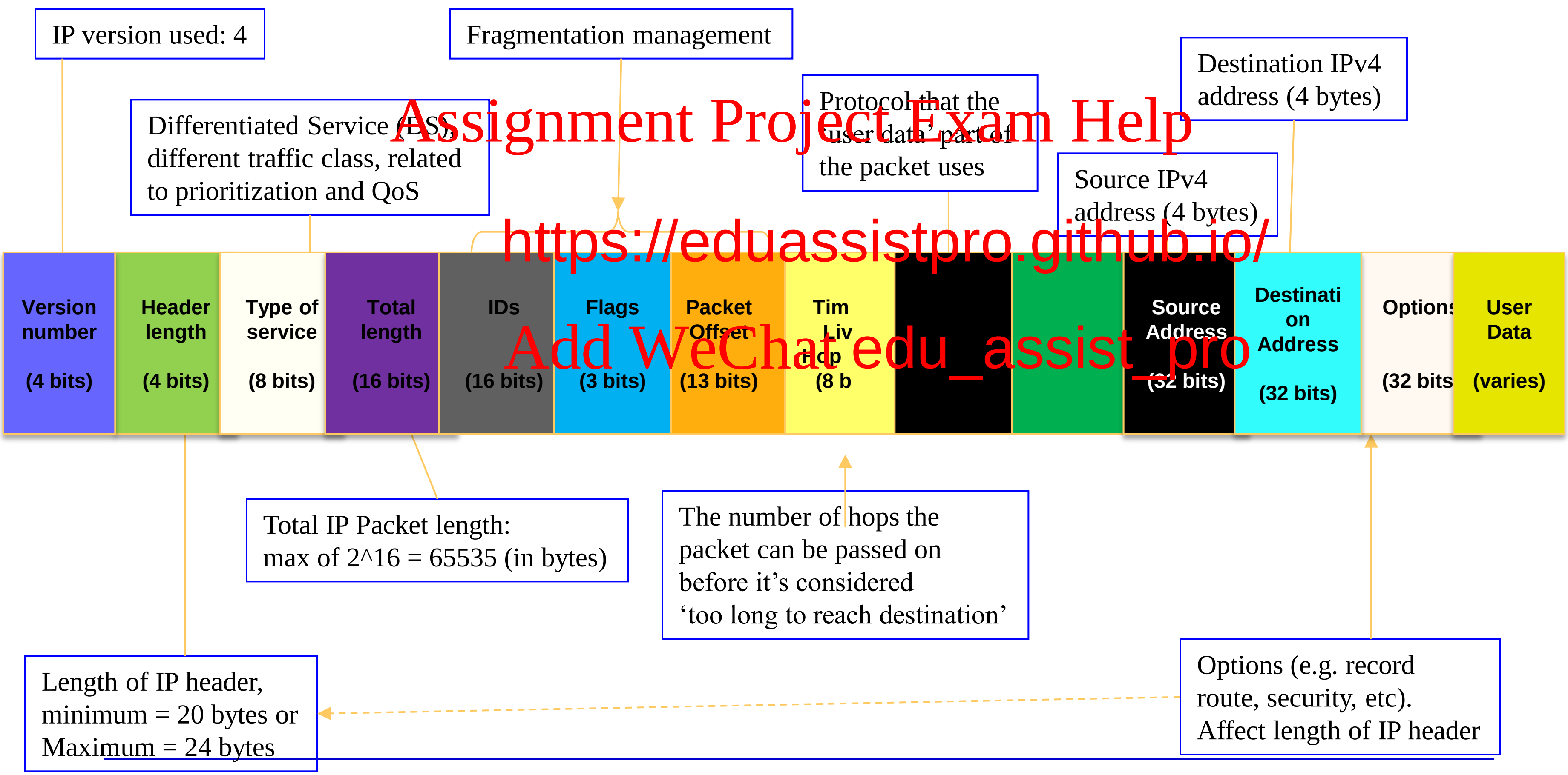
- Internet Protocol (IP)
  - IP version 4 (IPv4)
    - Most common version of IP used
    - 32-bit billion possib
    - Exhaustion of addre



| Version number | Header length | Type of service | Total length | IDs | Flags | Packet Offset | Time to Live / Hop Limit | Protocol | CRC-16 | Source Address | Destination Address | Options | User Data |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (4 bits) | (4 bits) | (8 bits) | (16 bits) | (16 bits) | (3 bits) | (13 bits) | (8 bits) | (8 bits) | (16 bits) | (32 bits) | (32 bits) | (32 bits) | (varies) |

# IP Packet Formats

## IPv4 Header: 192 bits (24 bytes)



# Network Layer Protocols

– IP version 6 (IPv6)

- 128-bit addresses ($2^{128}$ or ~$3.4 \times 10^{38}$ possible)

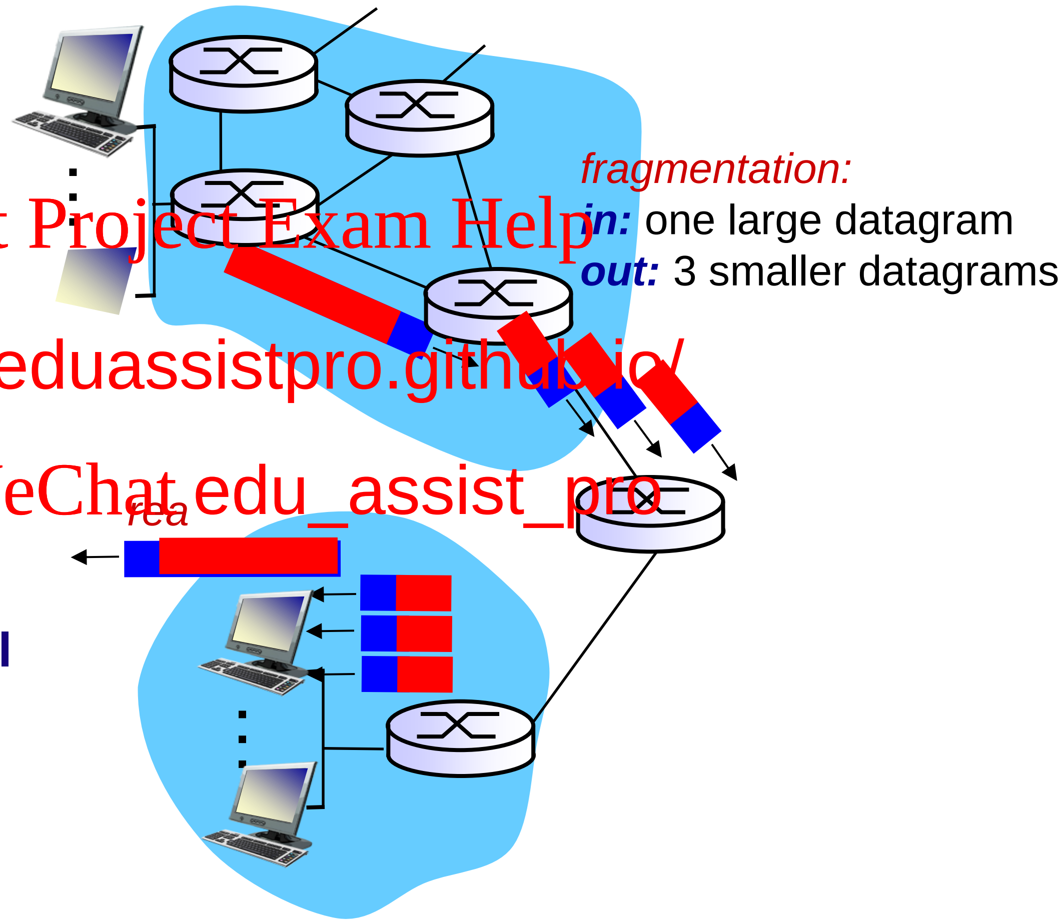
- Slowly IPv4 exhau

# Network Link Layer

- **IP fragmentation**
- **Addr**
- **Routing**

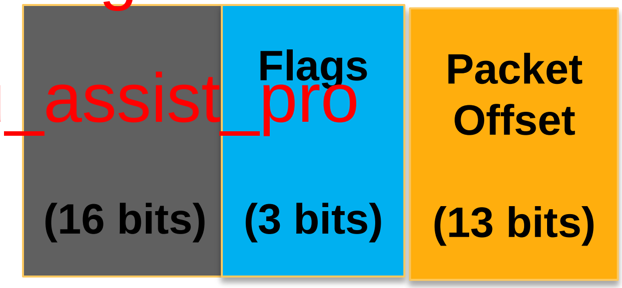
# IP Fragmentation

- **network links have MTU (max.transfer size) - largest possible link-level frame**
  - ✓**different link types, different MTUs**
- **large IP datagram ("fragmented") within net**
  - ✓**one datagram becomes several datagrams**
  - ✓**"reassembled" only at final destination**
  - ✓**IP header bits used to identify, order related fragments**



# IP Fragmentation

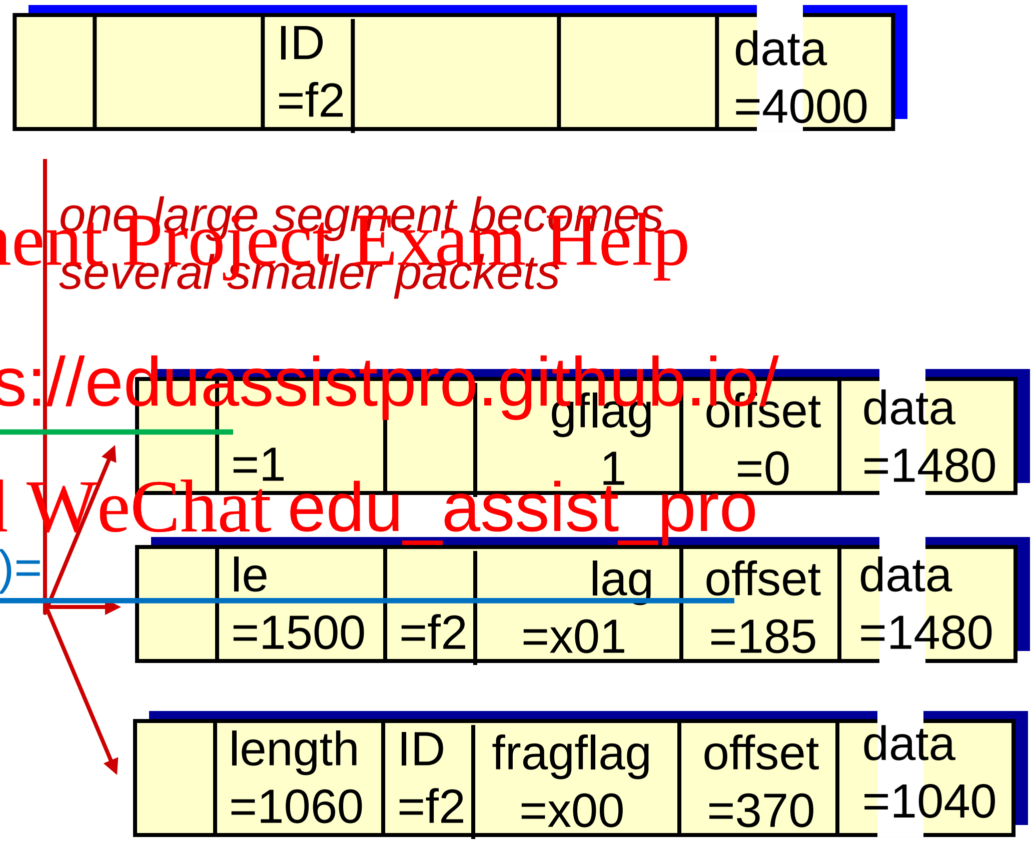
- Fragmentation management fields:
  - *identification* (16 bits): unique identification for *all packets* related to the same upper-layer datagram
  - *flags* (3 bits): fragment-ability management
    - 0xx : n
    - x0x : f
    - x1x : do not fragment
    - xx0 : the last fragment
    - xx1 : more fragments
  - *offset* (13 bits): starting sequence number for the packet (measured in the unit of 8 byte blocks)
    - ***To keep track of order of packets***



# IP Fragmentation

*example:*

- 4000 byte segment
- MTU = 1500 bytes




IP overhead (20 byte) + data (1480 byte) = 1500

offset (measured in octet)= 1480/8

# Network Link Layer

- IP fragmentation
- Addr
- Routing

# IP Addressing

- 4 byte (32 bit) addresses
  - Strings of 32 binary bits
- Dotted decimal notation
  - Used to ier to understa
  - Breaks the address int s and writes the digital equivalent for each byte
- Example: 128.192.56.1

| 1 0 0 0 0 0 0 0 | 1 1 0 0 0 0 0 0 | 0 0 1 1 1 0 0 0 | 0 0 0 0 0 0 0 1 |
| --- | --- | --- | --- |

# IP Addressing

- A portion of an IP address represents **the network** and the rest identifies **the host**
- Classful addressing
  - Uses the f mber of hosts
  - Discontin till used)
- Classless Inter-Domain CIDR)
  - No fixed subnet part and host parts
  - Flexible way to decide

# Classful Addressing

**Class A**

| | 7 bits | 24 bits |
|---|---|---|
| 0 | Net ID | Host ID |

0 -127

2^7 → 128 networks
2^24 → over 16 millions hosts per network
2^31 → over 2 Billion addresses in total



**Class B**

| | 14 bits | 16 bits |
|---|---|---|
| 1 0 | Net ID | |

128 -191



4 → over 16K networks
6 → over 65K hosts per network
0 → over 1 Billion addresses in total



**Class C**

| | 21 bits | 8 |
|---|---|---|
| 1 1 0 | Net ID | Host ID |

192 -223

→ over 2 million networks
2^8 → 255 hosts per network
2^29 → 536 Million addresses

**Class D**

| | |
|---|---|
| 1 1 1 0 | |

Multicast address
2^28 = 268 Million addresses

**Class E**

| | |
|---|---|
| 1 1 1 1 | |

Reserved
2^28 = 268 Million addresses

# Classless Inter-Domain Routing

- **Subnet portion of address of arbitrary length**
- **address format: a.b.c.d/x, where x is # bits in subne**



subnet part

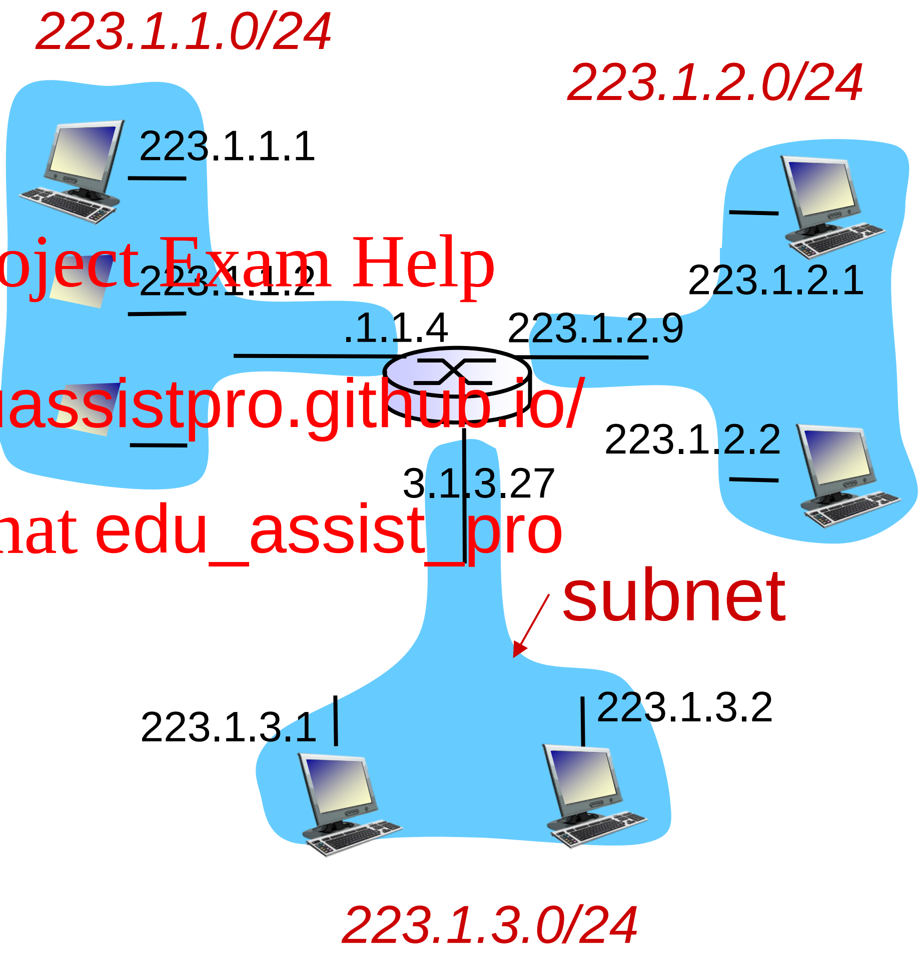
host part

11001000 00010111 00010000 00000000

200.23.16.0/23

# Subnets

- Group of computers **on the same LAN with IP address sharing *the same***
- Can physi
reach each other **without intervening router**



# IP Assignment

**Q: How does a *host* get IP address?**

- **hard-coded by system admin in a file**
  - Windows: control-panel->network->configuration->tcp/ip->properties
  - UNIX: /etc/rc.
- **DHCP: Dynamic Host Configuration Protocol:**
  - Plug and play

# DHCP

***Goal*** **allow host to *dynamically* obtain its IP address from network server when it joins network**

- can renew its lease on address in use



- allows reuse of addresses (only hold address while connected/



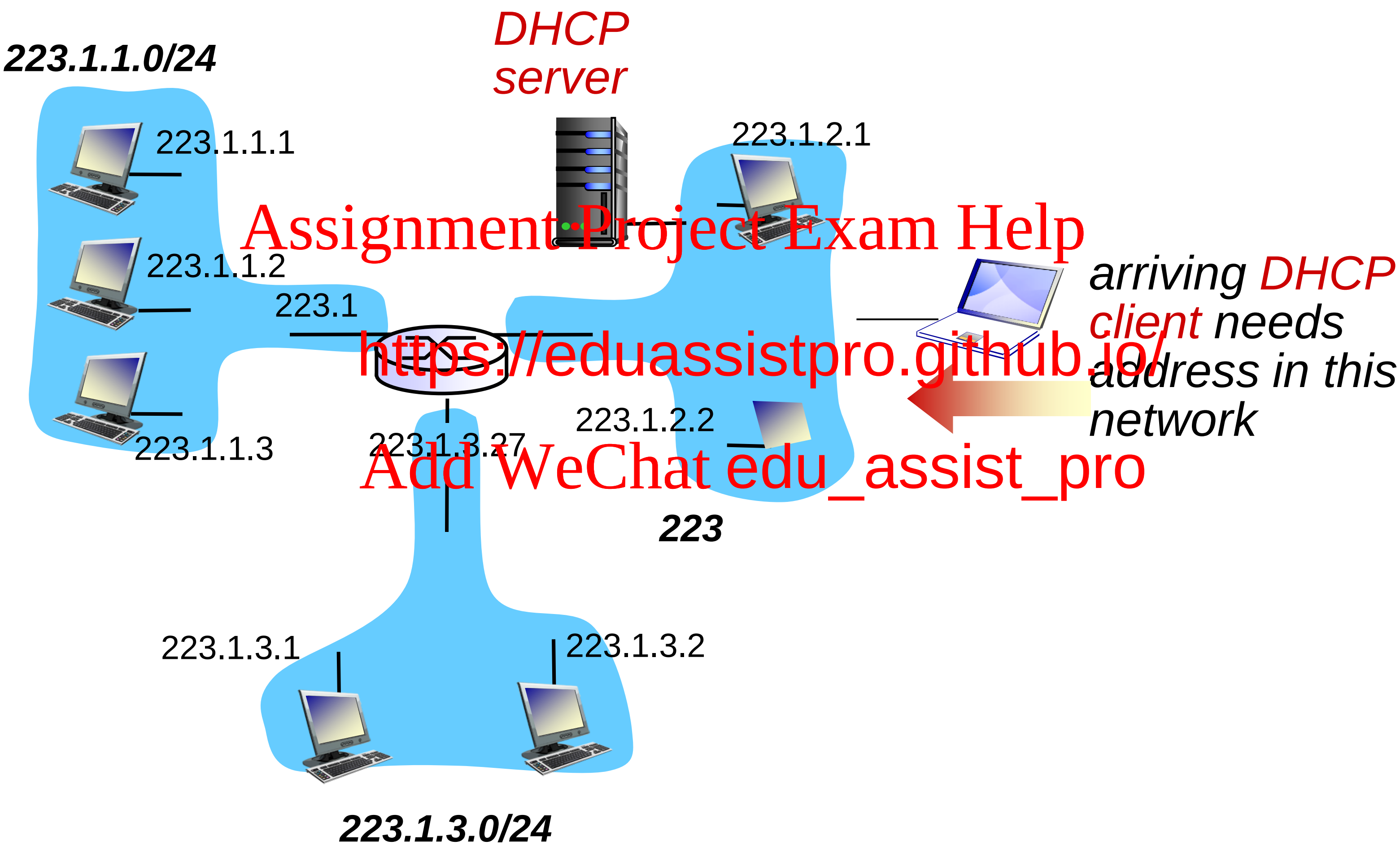
- support for to join network

***How it works:***

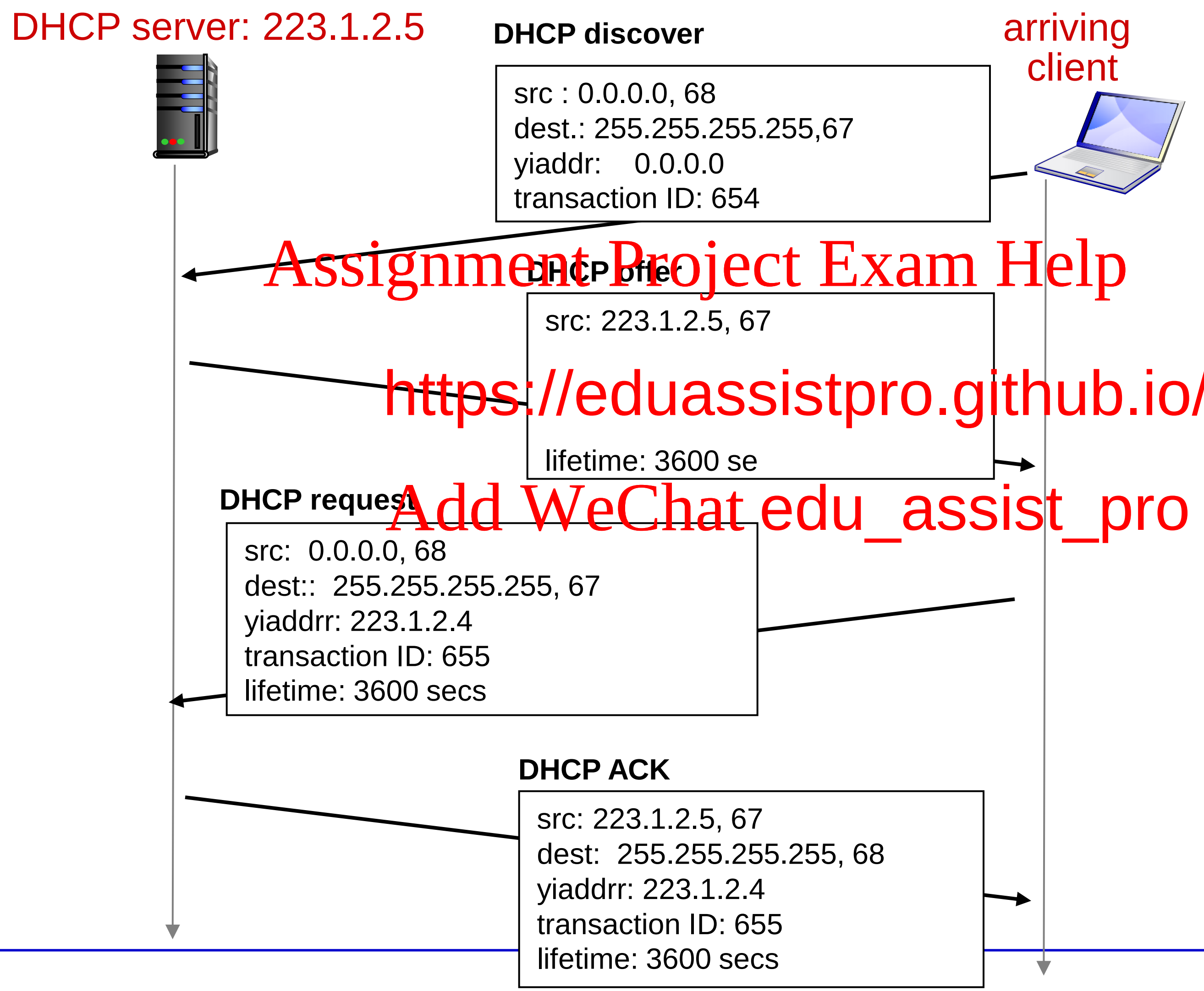


- host broadcasts "DHCP discover" msg
- DHCP server responds with "DHCP offer" msg
- host requests IP address: "DHCP request" msg
- DHCP server sends address: "DHCP ack" msg

# DHCP Scenario



# DHCP Scenario



# Address Resolution

- **Addresses exist at different layers**

| Address Type | Example | Example Address |
|---|---|---|
| Application layer | Web address (URL) | www.indiana.edu |
| Network layer | I | 9.79.78.193 (4 bytes) |
| Data link layer | | -6F-65-F8-33-8A (6 bytes) |



- **Addresses may be tra esolved) from one layer to another**

# Address Resolution

- **Server Name Resolution**
  - Translating destination host's domain name to its corresponding IP address
  - www.yahoo.com is resolved to → 204.71.200.74
  - Uses one e Service (DNS) servers t
- **Data Link Layer Addre ution**
  - Identifying the MAC address of the next node (that packet must be forwarded)
  - Uses Address Resolution Protocol (ARP)

# DNS: domain name system

***Domain Name System:***

- **hostname to IP address translation**
- ***distributed database*** **implemented in hierarchy of many** ***name***

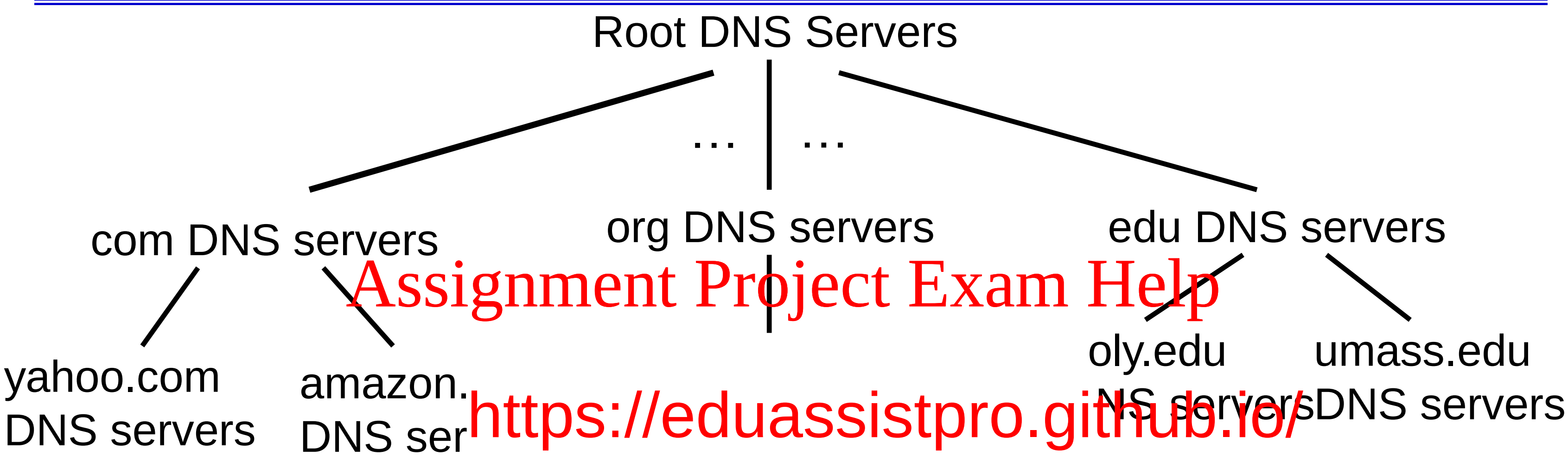
- ***application-***  **name servers communicate to** ***resolve***  **ress/name translation)**

***why not centralize DNS?***

- **single point of failure**
- **traffic volume**
- **distant centralized database**
- **maintenance**

*doesn't scale!*

# DNS: domain name system






***client wants IP for www.amaz st approx:***

- **client queries root server to find com DNS server**
- **client queries .com DNS server to get amazon.com DNS server**
- **client queries amazon.com DNS server to get IP address for www.amazon.com**

# DNS: root name servers

- contacted by local name server that can not resolve name
- root name server:
  - –contacts authoritative name server if name mapping not known
  - –gets mapping
  - –returns mapping t




*13 root name "servers" worldwide*

# TLD, authoritative servers

***top-level domain (TLD) servers:***

- responsible for com, org, net, edu, aero, jobs, museums, and all top-level country domains, e.g.: uk, fr, ca, jp

- Network S rs for .com TLD
- Education f


***authoritative DNS server***


- organization's own DNS server(s), providing authoritative hostname to IP mappings for organization's named hosts
- can be maintained by organization or service provider

# Local DNS name server

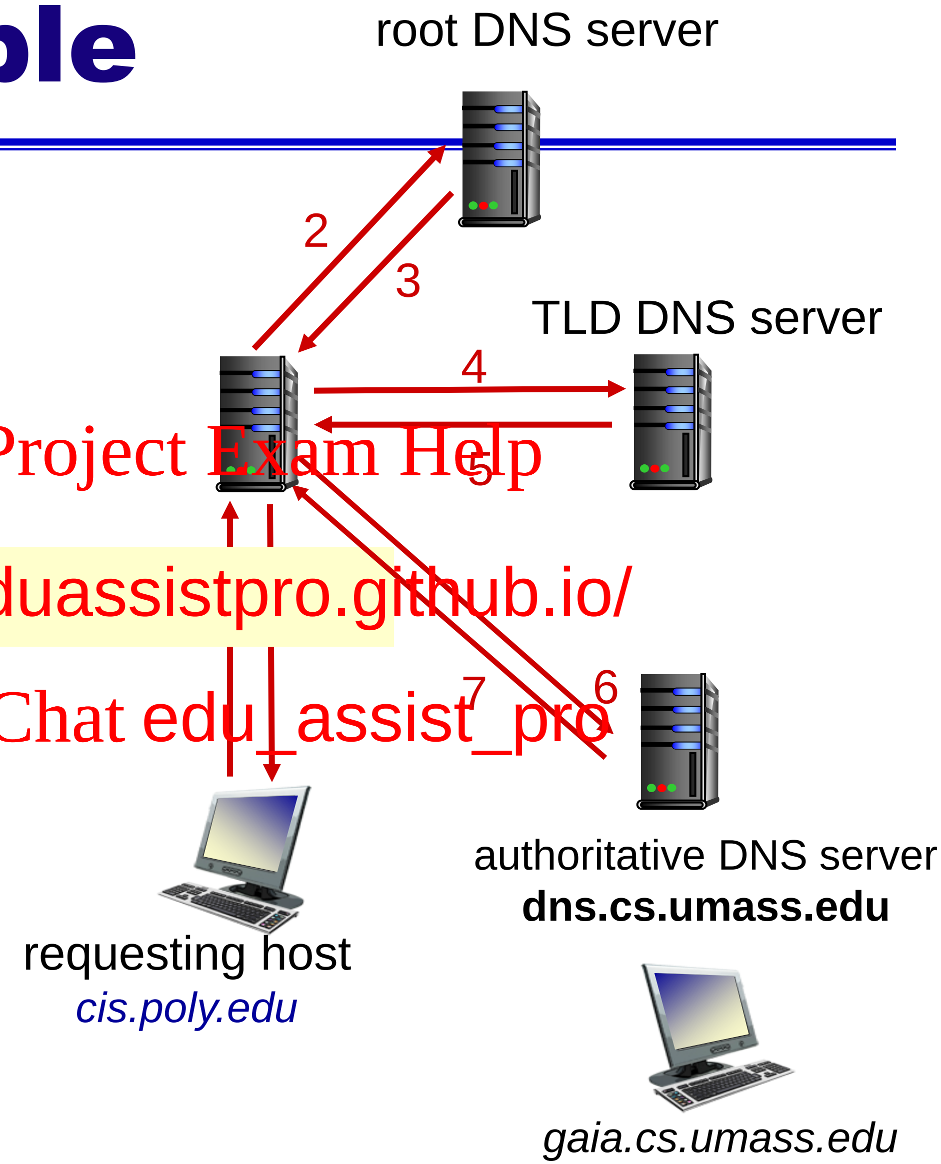
- does not strictly belong to hierarchy
- each ISP (residential ISP, company, university) has one
  - also calle r”
- when host query is sent to its local DNS s
  - has local cache of recent name-to-address translation pairs (but may be out of date!)
  - acts as proxy, forwards query into hierarchy

# DNS example

- **host at cis.poly.edu wants IP address for gaia.cs.umass.edu**

*iterated query:*

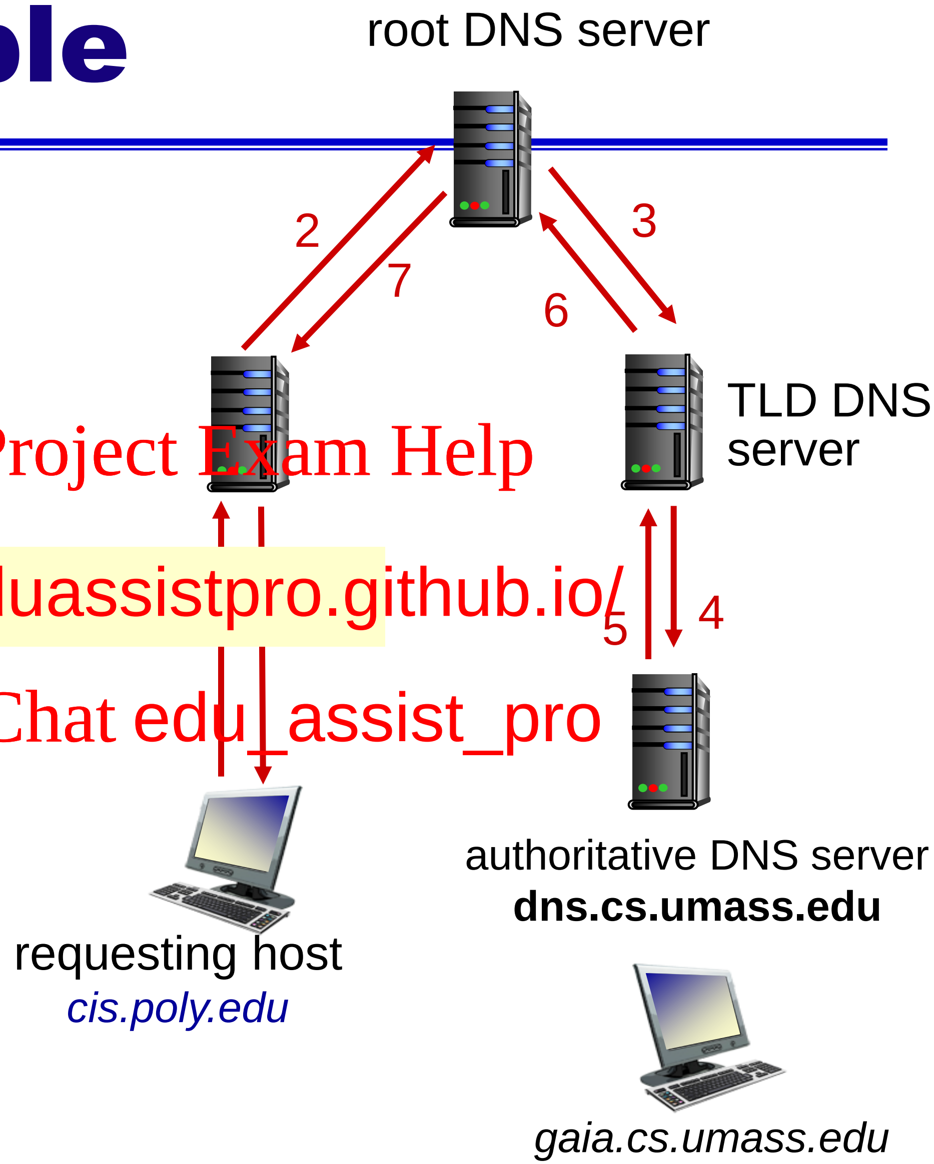
- contacted server replies with name of server to contact
- “I don’t know this name, but ask this server”



# DNS example

*recursive query:*

- puts burden of name resolution on contacted name server
- heavy load at upper levels of hierarchy?



# ARP name resolution

- Identifying the MAC address by IP address
- Operation
  - Broadcast an ARP message to all nodes on a LAN asking which node has a certain IP address
  - Host with that IP address then responds by sending back its MAC addres
  - Store this M le
  - Send the me

# MAC addresses and ARP

- **32-bit IP address:**
  - ***network-layer* address for interface**
  - **used for layer 3 (network layer) forwarding**



- **MAC (or LA hernet) address:**





  - **function: *used "locally"* *e from one interface to another physically-connected interface (same network, in IP-addressing sense)***
  - **48 bit MAC address (for most LANs) burned in NIC ROM, also sometimes software settable**
  - **e.g.: 1A-2F-BB-76-09-AD**

hexadecimal (base 16) notation
(each "number" represents 4 bits)

# LAN addresses (more)

- MAC address allocation administered by IEEE
- manufacturer buys portion of MAC address s



queness)

- analogy:



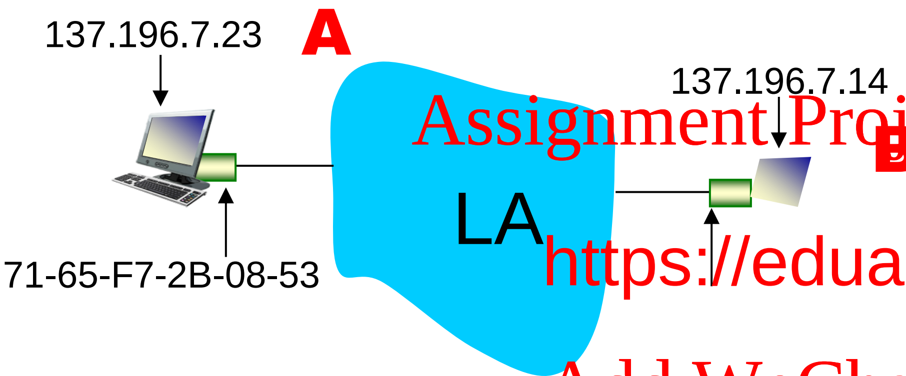
  - MAC address: like Soc Number
  - IP address: like postal



- MAC flat address ➜ portability
  - can move LAN card from one LAN to another
- IP hierarchical address *not* portable
  - address depends on IP subnet to which node is attached

# ARP

*Question:* how to determine a MAC address knowing its IP address?






- A broadcasts ARP query packet, containing B's IP address
  - MAC address = FF-FF-FF-FF
  - s on LAN receive ARP query (broadcast)
- B receives ARP packet, replies to A with its (B's) MAC address
  - frame sent to A's MAC address (unicast)

| | ARP query | ARP reply |
|---|---|---|
| Src IP address | 137.196.7.23 | 137.196.7.14 |
| Dest IP address | 137.196.7.14 | 137.196.7.23 |
| Src MAC address | 71-65-F7-2B-08-53 | 58-23-D7-FA-20-B0 |
| Dest MAC address | FF-FF-FF-FF-FF-FF | 71-65-F7-2B-08-53 |

# Network Link Layer

- IP fragmentation
- Addr
- Routing

# Routing

- **Process of determining the route (or path) a message will travel from the sending computer to the receiving computer**
- **Routers**
  - Special purp  routing decisions on the Internet
  - Maintain their own routing tab



- **Routing Tables**
  - Shows which path to send packets on to reach a given destination
  - Kept by computers making routing decisions

# Routing

- **Unicast - one computer to another computer**
- **Broadcast - one computer to all computers in the network**
- **Multicast - one computer to a group of computers ce)**
  - Same data ceivers and avoid transmitting it once for eac
    - Particularly useful if acc bandwidth limitations
    - Many implementations at different layers
    - In IP multicast, hosts dynamically join and leave multicast groups using Internet Group Management Protocol (IGMP)

# Routing

# Types of Routing

- **Centralized routing**
  - Decisions made by one central computer
  - Used on small, mainframe-based networks
  
  - Not common anymore
- **Decentrali** 
  - Decisions made by each endently of one another
  
  - Information needs to be exchanged to prepare routing tables
  - Used by the Internet

# Statc vs. Dynamic

- **Static routing:**
  - Fixed routing tables
  - Manually configured by network administrator
  - Used on relatively simple networks with few routing op



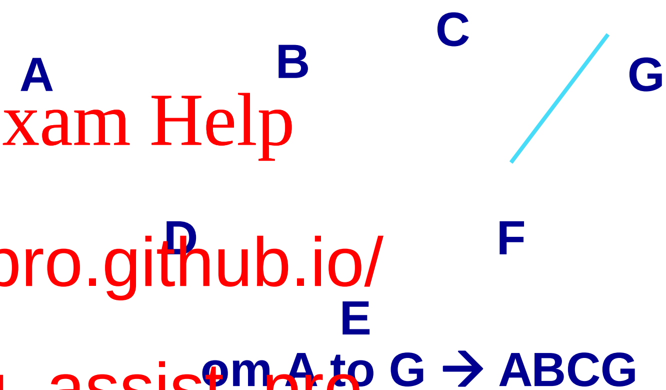


- **Dynamic ro**
  - Routing tables updated
  - Routers exchange information using protocols to update tables

# Dynamic Routing Algorithms

- **Distance Vector**
  - Uses the least number of hops to decide how to route a packet






- **Link State**
  - Uses a variety of informa to decide how to route a packet (more sophisticated)
    - e.g., number of hops, congestion, speed of circuit
  - Provides more reliable, up to date paths to destinations

# Routing Protocols

- **Used to exchange info among nodes for building and maintaining routing tables**
- **Types of Routing Protocols**
  
  - Interior routing protocols (RIP, OSPF, EIGRP, ICMP)
    - Operate 
    - Provide detailed info abou and paths
  
  - Exterior routing protocols (BG
    - Operate between networks (autonomous systems)

# Routing Information Protocol (RIP)

- **Dynamic distance vector protocol used for interior routing**
- **Operations:**



  - Commonly
  - Network ma  uting table
  - When a new node added, RI ber of hops between computers and upda  bles
  - Routing table status are broadcasted periodically (every minute or so) by all nodes

# Open Shortest Path First (OSPF)

- **A *dynamic hybrid (distance vector + link state)* interior routing protocol**
  - More reliable paths: Incorporates traffic and error rate meas
  - Most wide rotocol on large enterprise networks, pref CP/IP
  - Less burdensome to the
    - Only the updates sent (not entire routing tables) and only to other routers (no broadcasting)

# Other Interior Routing Protocols

- **Enhanced Interior Gateway Routing Protocol (EIGRP)**
  - A *dynamic hybrid interior* protocol (developed by Cisco)
  - Records transmission capacity, delay time, reliability and load for all p
  - Keeps the r s and uses this information i ll
- **Internet Control Message ICMP)**
  - Simplest and most basic: checks the reachability of a certain nodes and paths (e.g., Ping)
  - An error reporting protocol (report routing errors to message senders)

# Exterior Routing Protocols

- **Border Gateway Protocol (BGP)**
  - Used to exchange routing info between autonomous systems
  - Based on a *dynamic distance vector* algorithm
  - Far more uting protocols
  - Provide routing info only routes (e.g., preferred or best route)
    - Too many routes; can't maintain tables of every single route

# Internet Routing using GP, OSPF and RIP