COMPUTER NETWORKS

CHAPTER 1

Topics :

- ○ **What is internet?**
- ○ **What is a protocol?**
- ○ **Network edge: hosts, access networks , physical media.**
- ○ **Network core: packet/ circuit switching, internet structure.**
- ○ **Performance: loss, delay, throughput**
- ○ **Security**
- ○ **Protocol layers, service models**
- ○ **History**

http://gaia.cs.umass.edu/kurose_ross/lectures.php

NETWORK EDGE:-

It is the outer boundary where end users device connects to a network. It is crucial because it is where data enters or exits the network, where interactions between end user and servers take place.

Key components:-

Hosts (clients and servers) :- any device connected to a network.

1. **Clients :** end user devices e.g. laptops , personal computers.
   Clients initiates request for data or services.
2. **Servers :** devices that store or provide services to clients. E.g. web server , email server etc. servers are often known as data centres. Data centres are centralized facilities equipped with robus infrastructure, including servers, storage , network equipment and security measures. Designed to handle large amounts of data, provide high speed connectivity and ensure availability and reliability of resources.

Access networks, physical media :-

Access networks and physical media are the parts that connects end users to the core networks.

1. **Wired communication :** involves physical cables e.g. fibre optics, copper wires etc.
2. **Wireless communication :** relies on electromagnetic waves e.g. wi-fi, cellular networks , satellite communications.
3. **Links :** pathways that enable communication between devices in a network. They can be wired or wireless.

Network core :-

1. **Interconnected routers:** high speed , interconnected backbone of routers that facilitate the seamless flow of data within a network of networks. It represents a **network of networks.**

How to connect?

End system -> edge routers.

a. Residential access networks
b. Institutional access networks (school , company)
c. Mobile access networks (4G/5G).

DSL and Cable internet access:

They use existing telephone and cable tv infrastructure, while fthh employs optical fibres offering high speed (GB/ sec) by directly connecting homes to central office.

DSL INTERNET ACCESS:-

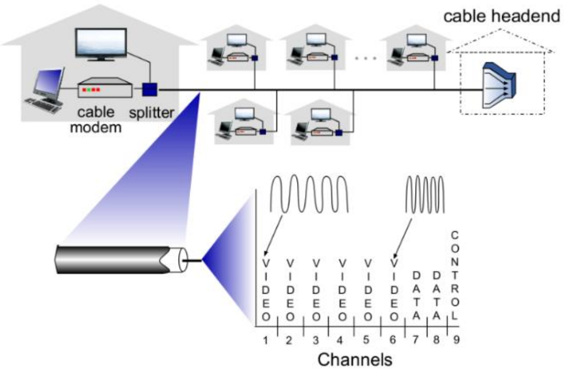
FIBRE TO HOME (FTTH):-

ACCESS NETWORKS :-

a. Cable based Access :-

Frequency division Multiplexing (FDM):

Cable based networks utilize coaxial cables to deliver internet service to homes. A modem connects the cable to a device, which a splitter divides the signal for multiple connections. Cable headend manages data transmission, employing FDM to send multiple channels over different frequencies simultaneously. Cable internet access requires special modems called "cable modems".



Hybrid Fibre Coax (HFC):

HFC (Hybrid Fiber Coax) networks combine fiber optic and coaxial cable technology to deliver internet and TV services. They offer asymmetric speeds, with **downstream rates ranging from 40 Mbps to 1.2 Gbps** and **upstream rates from 30 Mbps to 100 Mbps**.

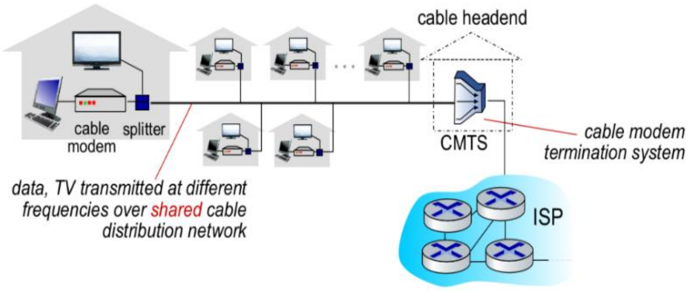
Homes connect to the ISP router via fiber, sharing the cable access network to the cable headend. Cable modems divide the network into downstream and upstream channels, allowing data and TV signals to be transmitted at different frequencies over the shared cable distribution network. The Cable Modem Termination System (CMTS) manages communication between cable modems and the ISP.

Downstream and upstream channels refer to the directions of data transmission in a communication system, such as in cable-based internet access networks like HFC (Hybrid Fiber Coax) systems:

Downstream Channel: This is the direction of data transmission from the service provider (e.g., the cable headend) to the end-user (e.g., the subscriber's home). Downstream channels carry data, such as internet content, TV programs, and other information, from the central source to the users.

Upstream Channel: Conversely, the upstream channel is the direction of data transmission from the end-user (e.g., the subscriber's home) to the service provider (e.g., the cable headend). Upstream channels are used for sending data, such as requests for web pages, uploads, and other user-generated content, back to the central source.

In cable internet access networks, such as those employing HFC technology, the cable modem divides the network into two separate channels—one for downstream communication and another for upstream communication. This division allows for efficient data transfer in both directions over the shared cable infrastructure.


cable headend
cable modem
splitter
CMTS
cable modem termination system
data, TV transmitted at different frequencies over shared cable distribution network
ISP

b. digital subscriber line (DSL):-

1. **<u>Central Office:</u>** The central office is the point **where the telephone network connects with the internet backbone.** It serves as a hub for routing communication signals between subscribers and the wider network.

2. **<u>Telephone Network:</u>** The telephone network **refers to the infrastructure of telephone lines and equipment used** for traditional landline phone services.

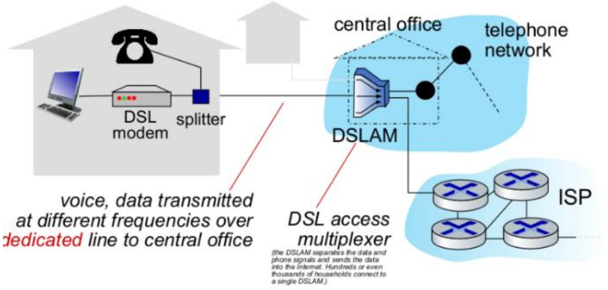
3. **<u>DSLAM (Digital Subscriber Line Access Multiplexer):</u>** The DSLAM is a **network device located in the central office that aggregates multiple DSL connections from subscribers and routes their data** onto the internet or other networks.

4. **<u>Voice and Data Transmission:</u>** DSL technology **allows for the simultaneous transmission of voice (telephone) and data signals over the same telephone line.** Voice and data are transmitted at different frequencies over the dedicated line to the central office.

5. **<u>Dedicated Line to Central Office:</u>** Each subscriber's **DSL service is delivered over a dedicated line that connects their premises to the central office.** This line allows for high-speed internet access without interfering with traditional telephone service.

6. **<u>Data and Voice Routing:</u>** Data transmitted over the DSL phone line is directed to the internet, providing access to online services and content. Voice signals, on the other hand, are routed to the telephone network, enabling traditional phone calls.

7. **<u>Transmission Rates:</u>** DSL **offers asymmetric transmission rates**, with dedicated **downstream rates typically ranging from 24 to 52 Mbps** and **upstream rates ranging from 3.5 to 16 Mbps**. This means that **downstream data** (from the internet to the subscriber) **can be transmitted at higher speeds than upstream data** (from the subscriber to the internet).


central office
telephone network
DSL modem
splitter
DSLAM
ISP
voice, data transmitted at different frequencies over dedicated line to central office
DSL access multiplexer
(the DSLAM separates the data and phone signals and sends the data into the Internet. Hundreds or even thousands of households connect to a single DSLAM.)

c. Home Networks:

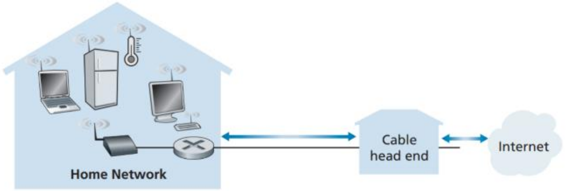
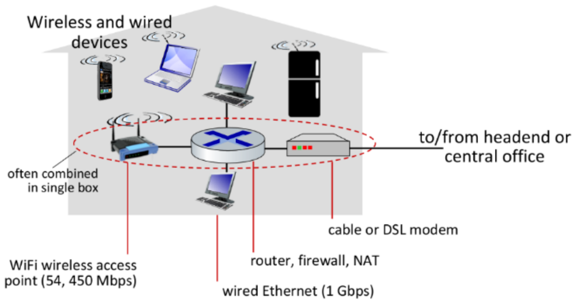
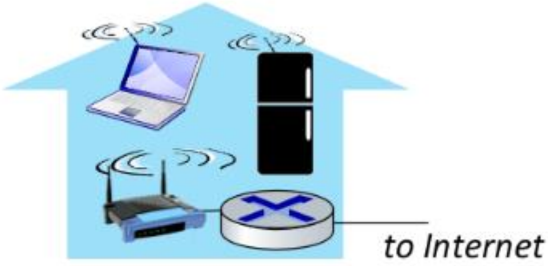
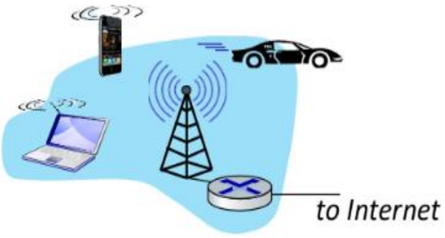


Figure 1.9 • A typical home network

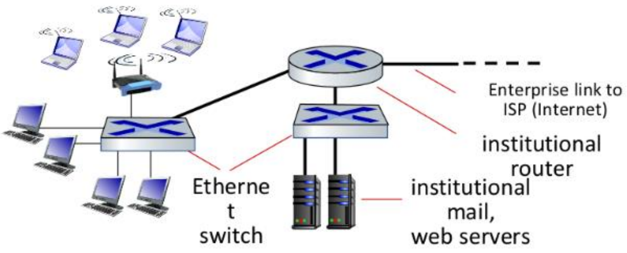

Wireless and wired devices
to/from headend or central office
often combined in single box
cable or DSL modem
WiFi wireless access point (54, 450 Mbps)
router, firewall, NAT
wired Ethernet (1 Gbps)

WIRELESS ACCESS NETWORKS:

Wireless access networks connect devices to the internet without the need for cables.

Wireless Local Area Networks (WLANs)	Wide Area Cellular Access Networks
Limited to small areas, typically within or around buildings, with a range of about 100 feet.	**Span larger geographic areas**, ranging from urban to rural regions, extending tens of kilometers or more.
Devices connect through a base station or access point, usually connected to a router.	**Devices connect to cellular networks via base stations or cell towers**, which are part of the cellular infrastructure.
Use Wi-Fi standards like 802.11b/g/n, providing **transmission rates ranging from 11 to 450 Mbps.**	**Offer varying transmission rates,** typically **ranging from tens of Mbps to several hundred Mbps, depending on network conditions** and technology generation (4G, 5G).
Commonly used for local connectivity within homes, offices, schools, and public places like cafes or airports.	**Provide mobile internet access, enabling users to stay connected** while on the move, whether in urban, rural areas, or during travel between locations.
Often owned and managed by the entity operating the premises where deployed (homeowner, business, organization).	**Owned and operated by mobile network operators,** providing subscription-based services for accessing their network infrastructure.
	

ENTERPRISE NETWORKS:-


Enterprise link to ISP (Internet)
institutional router
Etherne t switch
institutional mail, web servers

Enterprise networks are **used by organizations like companies and universities**, employing a **combination of wired and wireless technologies** to connect switches and routers. Wired **Ethernet connections offer speeds of 100Mbps, 1Gbps, or 10Gbps**, while **wireless Wi-Fi access points provide speeds ranging from 11 to 450 Mbps**.Understanding the speed capabilities of wired Ethernet and wireless Wi-Fi connections helps organizations design and implement their network infrastructure to meet the diverse needs of their users, whether they are accessing resources locally within the organization's premises or remotely via wireless connections.

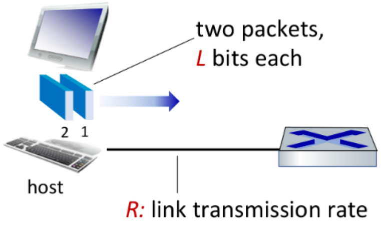
DATA CENTER NETWORKS:-

Data centre networks **are characterized by high-bandwidth links**, typically **ranging from tens to hundreds of gigabits per second (Gbps),** which **interconnect hundreds to thousands of servers within the data centre itself** and provide connectivity to the internet.

> Amazon Web Services (AWS) and Google Cloud Platform (GCP) have large scale data center networks that form the backbone of their cloud computing services. These networks consist of numerous interconnected servers and high-speed links, allowing them to provide various cloud services to users worldwide.

PROCESS OF SENDING DATA FROM HOSTS:-

1. The **host takes an application message and breaks it into smaller pieces called <u>packets</u>**, each consisting of a **<u>length of L bits</u>**.
2. These **packets are then transmitted into the access network at a transmission rate denoted by R**, which represents the **<u>link's transmission rate</u>** or **<u>bandwidth capacity</u>**.



3. Each **packet incurs a transmission delay**, which is the **time needed to transmit the L-bit packet into the link,** determined by **the ratio of the packet size (L bits) to the transmission rate (R bits per second).**

$$\text{packet transmission delay} = \text{time needed to transmit } L\text{-bit packet into link} = \frac{L \text{ (bits)}}{R \text{ (bits/sec)}}$$

LINKS: PHYSICAL MEDIA :-

In networks, links **represent the physical pathways through which data** (in the form of bits) **travels between transmitter and receiver pairs.** These links consist of physical media, which can be **categorized into guided and unguided media.**

Guided Media (Solid Media)	Unguided Media (Free Propagation)
Signals propagate through solid media, such as copper wires, fibre optic cables, or coaxial cables, providing a guided path for data transmission.	**Signals propagate freely through the air or space,** as in radio or wireless communication, without the need for a physical pathway.
Examples include twisted-pair cables, coaxial cables, and fiber optic cables, where data is transmitted along physical pathways.	**Examples** include radio waves, microwaves, and infrared signals, where data is transmitted through the air or space without the need for a physical pathway.
Guided media **offer higher reliability and lower susceptibility to external interference**, making them **suitable for wired communication** over relatively **short distances.**	Unguided **media allow for flexible and convenient wireless communication,** enabling mobility and **eliminating the need for physical connections,** though with **higher susceptibility to interference** and attenuation **over longer distances.**

Guided media are **commonly used in wired communication networks,** such as Ethernet LANs, fiber optic backbone networks, and cable television systems.	Unguided media are **used in wireless communication technologies, including Wi-Fi,** cellular networks, satellite communication, and Bluetooth.

Twisted Pair (TP)	**Coaxial Cable**	**Fiber Optic Cable**	**Wireless Radio**
Consists of two insulated copper wires twisted together, used for various applications including Ethernet.	Utilizes two concentric copper conductors, enabling bidirectional communication with multiple frequency channels and speeds up to hundreds of Mbps per channel.	Uses glass fibers to transmit light pulses, enabling high-speed transmission (10's-100's of Gbps) with low error rates and immunity to electromagnetic noise.	Relies on radio signals in the electromagnetic spectrum for communication without physical wires, experiencing environmental effects like reflection, obstruction, and interference.
Category 5 supports Ethernet speeds up to 100 Mbps and 1 Gbps, while Category 6 supports 10 Gbps Ethernet.	Offers broadband capabilities with multiple frequency channels and speeds in the hundreds of Mbps per channel.	Enables high-speed point-to-point transmission with low error rates, utilizing repeaters for long-distance communication.	Provides broadcast communication with varying bands in the electromagnetic spectrum, supporting half-duplex communication between sender and receiver.
Commonly used in Ethernet LANs for various applications.	Used in cable television systems and broadband internet connections.	Widely employed in high-speed data transmission for long-distance communication.	Utilized in various wireless communication technologies like Wi-Fi and cellular networks for mobility and flexibility.

RADIO LINKS USED IN NETWORKS:-

- **Wireless LAN (WiFi):** Offers **speeds ranging from 10 to hundreds of Mbps, covering distances of tens of meters.** Commonly **used for local wireless internet access in homes, offices, and public spaces.**

- **Wide-area (e.g., 4G cellular): Provides speeds in the 10 Mbps over distances of approximately 10 kilometers**. Utilized **for cellular communication, enabling mobile internet access** over large geographic areas.

- **Bluetooth:** Primarily s**erves as a cable replacement technology for short-range communication,** offering **limited data rates over short distances.**

- **Terrestrial Microwave: Point-to-point communication** method with **channels of 45 Mbps capacity.** Often **used for long-distance data transmission** between **fixed locations.**

- **<u>Satellite</u>:** Offers **channels with speeds up to 45 Mbps per channel**, with an **end-to-end delay of approximately 270 milliseconds**. Commonly used for long-distance communication where terrestrial infrastructure is impractical or unavailable.

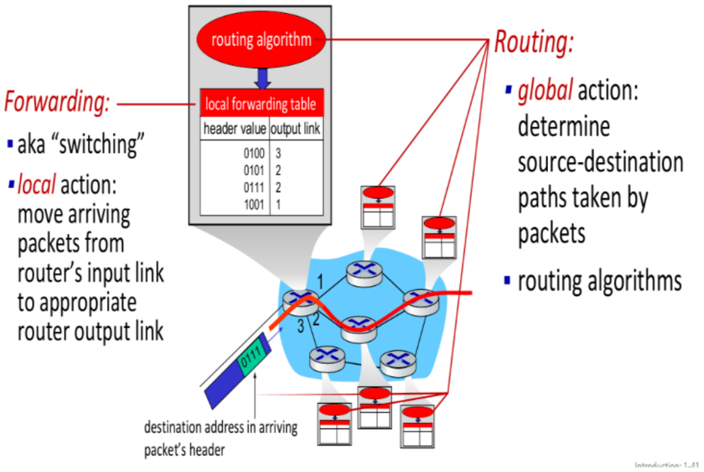
<u>NETWORK CORE:-</u>

The network core comprises **a mesh of interconnected routers**, facilitating packet-switching, where hosts divide messages into packets. **Routers forward packets across links to reach their destination, forming a path from the source to the target.**

TWO KEY NETWORK CORE FUNCTIONS:-

1. **FORWARDING:-** Think of it **like delivering mail within a building**. **When a packet arrives at a router, it checks the address on the packet and looks at its local forwarding table to see where to send it next**. Then, it **moves the packet to the right place for it to continue its journey.**

2. **ROUTING:-** This is like **planning the best route for a road trip**. Routing algorithms figure out the **best path for packets to travel from the sender to the receiver across the entire network,** considering factors like traffic and distance. It's about finding the most efficient way for data to get where it needs to go.



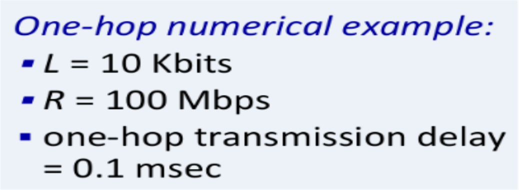
Forwarding:
- aka "switching"
- *local* action: move arriving packets from router's input link to appropriate router output link

Routing:
- *global* action: determine source-destination paths taken by packets
- routing algorithms

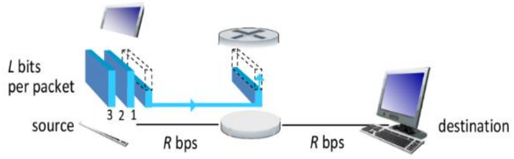
PACKET SWITCHING:-

a. Store and forward:-

Packet-switching uses **store-and-forward** means that **when a router receives a packet, it waits for the entire packet to arrive before sending it out on the next link.** The **transmission delay is the time it takes to push out a packet of length L bits onto a link with transmission rate R bps**. For example, with a packet size of 10 Kbits and a transmission rate of 100 Mbps, the one-hop transmission delay would be 0.1 milliseconds.

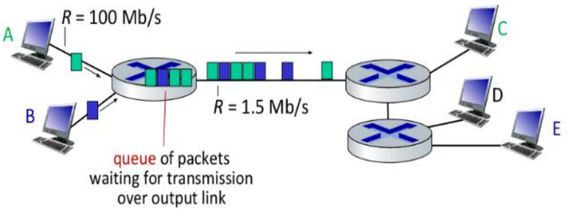


One-hop numerical example:
- L = 10 Kbits
- R = 100 Mbps
- one-hop transmission delay = 0.1 msec



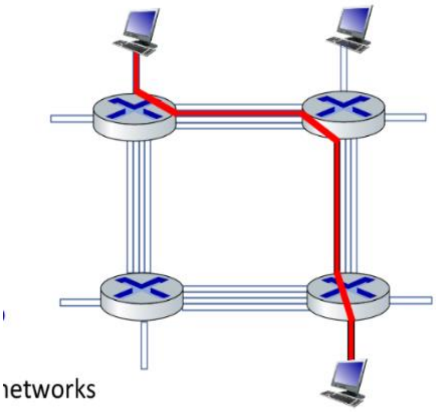
b. Queuing :-

When there are **more packets arriving at a link** than it can transmit, they **form a queue**, waiting for **their turn to be sent**. If this **continues for too long** or if the **router's memory becomes full**, packets **may be dropped**, meaning **they're lost** and **won't be transmitted**. This **helps manage network congestion** and **prevent overload on the router**.



CIRCUIT SWITCHING:- (ALTERNATE TO PACKET SWITCHING)

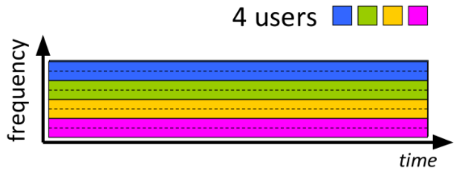
Circuit switching **is like reserving a dedicated path for a phone call between two people**. **Each link in the network has multiple circuits**, and when a **call is made**, it **gets its own circuit** on each link it travels through. These **resources are dedicated to the call** and **aren't shared with others**, providing guaranteed performance like traditional telephone networks. **If a circuit isn't being used, it stays idle, waiting for the call to use it.**



you're making a phone call. With circuit switching, it's like reserving a special road just for your call to travel from your phone to the person you're calling. This road is only for your call, and nobody else can use it while you're talking. It's like having your own private highway for your conversation, ensuring a smooth and reliable connection, similar to how traditional telephone networks operate.

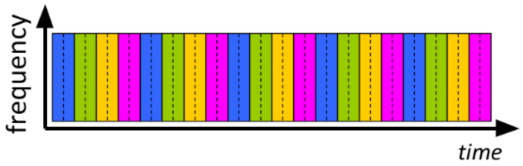
a. FREQUENCY DIVISION MULTIPLEXING:-

Think of FDM like a radio station. Just as **different stations use different frequencies to avoid interference**, FDM **divides the available frequency spectrum into narrow bands**. Each user gets their own band to transmit data, like tuning into a specific radio station.



b. TIME DIVISION MULTIPLEXING :-

With TDM, it's like sharing a single road at different times. Instead of dividing the frequency spectrum, **TDM divides time into slots. Each user gets their own time slot to transmit data, allowing them to use the entire frequency band during their allocated time**. It's like having your own lane on the road, but you can only use it at certain times.



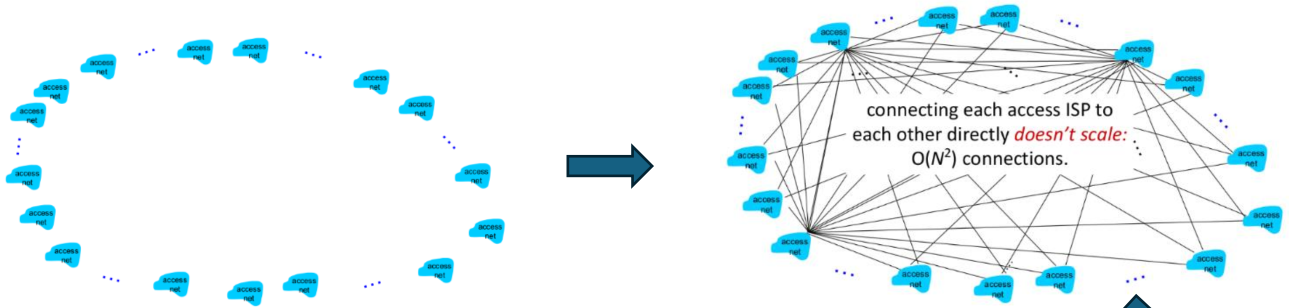
Circuit switching	**packet switching**
In circuit switching, **each user gets dedicated bandwidth for their entire call duration,** regardless of **whether they're actively using it or not**. With a 1 Gb/s link and each user needing 100 Mb/s when active, you can support 10 users, even if they're not always active.	In packet switching, **bandwidth is shared among users dynamically**. Since users are only active 10% of the time, you can support more users. With 35 users, the probability that more than 10 are active simultaneously is less than 0.0004, meaning it's highly unlikely that too many users will be active at the same time. This is due to the statistical nature of packet switching, where users share the link capacity based on their activity level.
A human analogy for circuit switching is like booking a private car for a trip, where you have exclusive access to the vehicle for the entire journey. On the other hand, packet switching is same to taking a public bus, where you share the ride with others and only use resources when needed.	Packet switching is like a flexible bus service where passengers get on and off as needed. It's **great for bursty data** because it efficiently shares resources among users, but it can lead to congestion and delays during busy times. To achieve circuit-like behavior, where users have dedicated resources, packet switching uses complex techniques like quality of service (QoS) and virtual circuits.

INTERNET STRCUTURE “NETWORK OF NETWROKS” :-

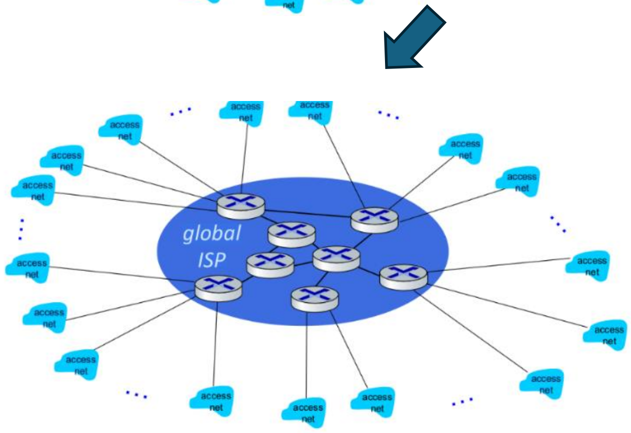
The Internet is like a massive web made up of smaller **networks**. When you **connect to the Internet through your ISP**, you're joining this network of networks. **ISPs are linked together** so that any two devices, no matter where they are, can communicate with each other by sending packets of data. The Internet's structure is complex and has evolved over time due to factors like economics and national policies.

Question: given millions of access ISPs, how to connect them together?

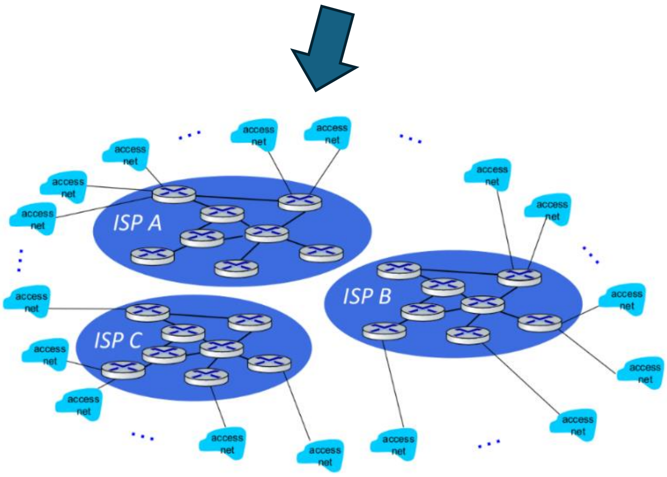
Connecting millions of access ISPs directly to each other would create an large number of connections, making it impractical. This approach doesn't scale because it requires O(N^2) connections, where N is the number of ISPs, leading to inefficiency and complexity.


access net
connecting each access ISP to each other directly doesn't scale: O(N^2) connections.

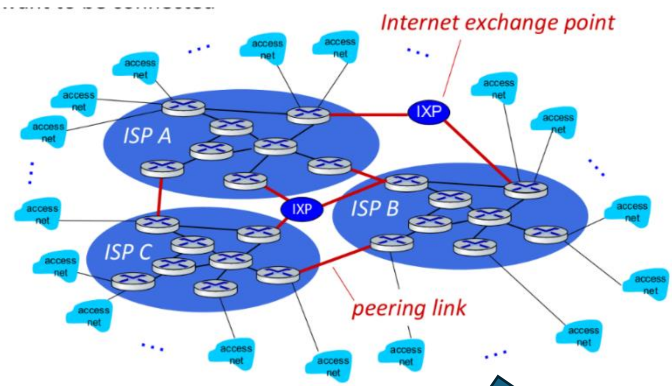
In this approach, each access ISP connects to a global transit ISP, which acts as a central hub for routing traffic between different access networks. Access ISPs pay the global ISP for access to the wider internet, creating an economic agreement. This simplifies the network structure and reduces the number of direct connections needed, making it more scalable and efficient.



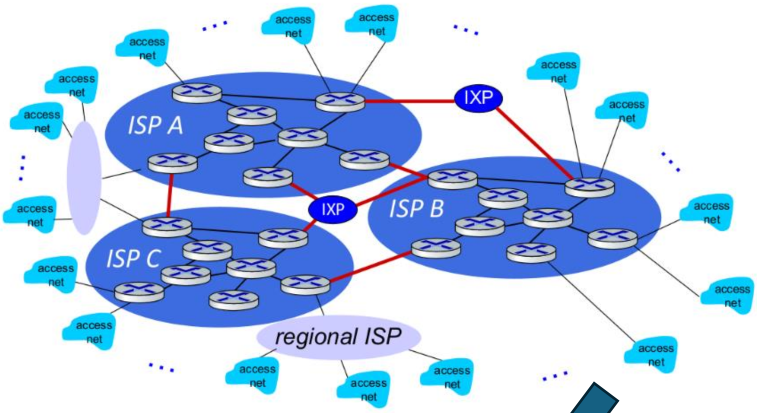
If one global ISP is successful, competitors are likely to emerge, leading to a competitive market for providing global transit services. This competition can benefit consumers by offering better services, pricing, and innovation in the network of networks.



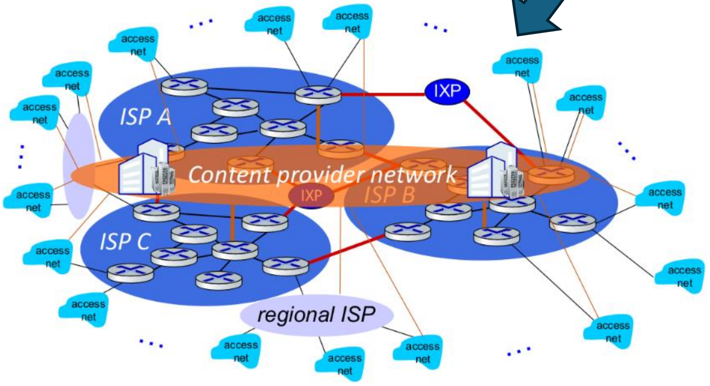
These competitors will seek to interconnect with other networks efficiently to expand their reach and offer competitive services. Internet Exchange Points (IXPs) serve as meeting points where multiple networks, including ISPs and content providers, can interconnect and exchange traffic directly, using peering links. This enables efficient and cost-effective data exchange between networks, fostering competition and innovation in the internet ecosystem.



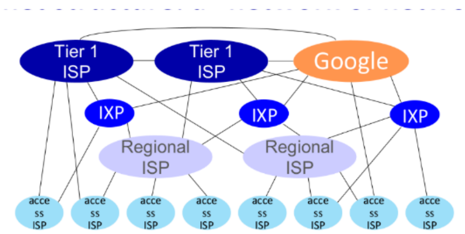
As the internet evolves, regional networks may emerge to connect local access networks to ISPs. These regional ISPs serve as intermediaries, connecting multiple local access networks to larger global networks through Internet Exchange Points (IXPs). This decentralized approach allows for efficient routing of traffic and enables access networks in different regions to connect to the broader internet infrastructure.



Content provider networks, such as those operated by Google, Microsoft, or Akamai, may deploy their own infrastructure to deliver services and content closer to end users. These networks often interconnect with regional ISPs and access networks through Internet Exchange Points (IXPs) to distribute content efficiently. By bringing their services closer to users, content providers can improve performance and reliability, reducing latency and enhancing the user experience.



Think of the internet as a big network made up of smaller networks. At the heart of this big network are a few really big networks called "tier-1" ISPs like AT&T or Sprint. They're like the superhighways of the internet, connecting everything together. Then there are companies like Google and Facebook that have their own private networks, kind of like secret tunnels that let them send data fast without going through the regular ISPs.



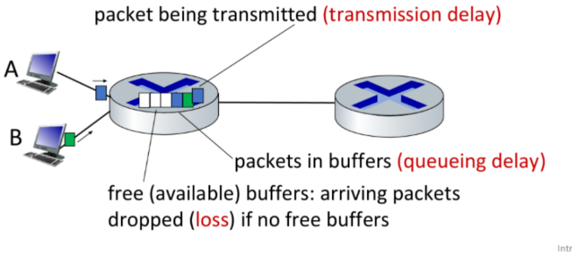
Performance: loss, delay, throughput:-

PACKET DELAY AND LOSS:-

how do they occur ?

Packet delay and loss happen **when routers get too busy.**

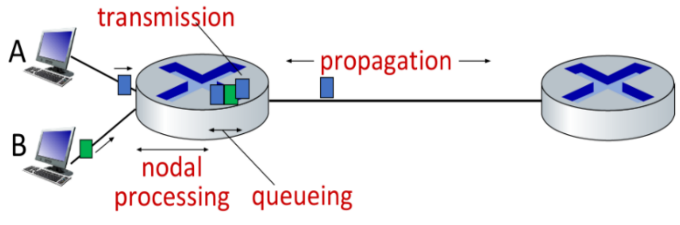
- **Delay** occurs **when packets line up in router buffers**, waiting their **turn to be sent**. This **happens** when the **arrival rate of packets temporarily exceeds** the **capacity of the output link.**
- **Loss** occurs **when there's no more room in the router's memory for queued packets**. **If** there are **no free buffers available**, incoming packets **get dropped or lost.**


packet being transmitted (transmission delay)
A
B
packets in buffers (queueing delay)
free (available) buffers: arriving packets dropped (loss) if no free buffers
Intr

Delays happen **because packets** have to **wait** in line, and **loss** happens when there's **no more space** to hold them.

4 sources of packet delay:-

1. **Nodal Processing (dproc):** The **time** it takes **for a router to process the packet**, including tasks like **error checking** and **determining the output link**. This is usually **very quick**, typically taking microseconds or less.
2. **Queueing Delay (dqueue):** The **time** the **packet spends waiting in a router's queue** for **transmission onto the output link.** This depends on how congested the router is.

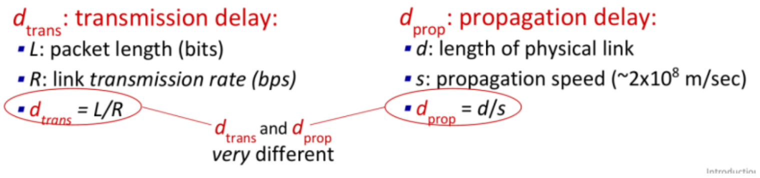


$$d_{\text{nodal}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$$

3. **Transmission Delay (dtrans):** The **time** it takes **to push the packet onto the link for transmission,** which depends on the packet's size and the link's transmission rate. It **depends on the length of the packet (L) and the transmission rate of the link (R).** So, if you have a big packet or a slow link, it will take longer to transmit the packet.
4. **Propagation Delay (dprop):** The **time** it takes for **the packet to travel from one router to the next** due to the physical distance between them. It depends on the physical distance between the routers (d) and the speed at which the signal propagates through the link (s). So, if the routers are far apart or the signal travels slowly, it will take longer for the packet to propagate.

Difference between dtrans and dprop:-

transmission delay is about **how fast you can push the packet onto the link**, while **propagation delay** is about **how long it takes for the packet to travel through the link**. They're **different because they're measuring different things**: one is about the speed of transmission, and the other is about the speed of travel.



d_{trans}: transmission delay:
- L: packet length (bits)
- R: link *transmission rate (bps)*
- $d_{trans} = L/R$

d_{prop}: propagation delay:
- d: length of physical link
- s: propagation speed (~2×10^8 m/sec)
- $d_{prop} = d/s$

d_{trans} and d_{prop} *very* different

CARAVAN ANOLOGY:-

In the caravan analogy, each **car represents a bit of data**, and the **toll booth represents the link transmission.**

- If the toll booth takes **12 seconds** to service each car (bit transmission time) and the cars propagate at **100 km/hr**, it takes **1 hour** (time = distance/speed => 100km/100 km/hr) for the last car to reach the second toll booth. So, the time for the entire caravan (packet) to push through the toll booth is **120 seconds.**(service time of each car * no. of cars=12*10)
- If the cars now propagate at **1000 km/hr** and the toll booth takes **one minute** to service a car, the **first car** will arrive at the second booth after **7 minutes**, while three cars are still at the first booth. This shows that with **faster propagation and quicker service**, the **cars arrive at the second booth** before all of them are serviced at the first booth.

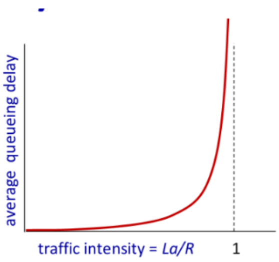
Packet queuing delay:-

$$\frac{L \cdot a}{R} : \frac{\text{arrival rate of bits}}{\text{service rate of bits}}$$ *"traffic intensity"*

a: average packet arrival rate

L: packet length (bits)

R: link bandwidth (bit transmission rate)



- When the **traffic intensity is low (La/R = 0),** the **average queueing delay is small** because the rate of arriving packets is much **lower** than the capacity of the link.
- When the **traffic intensity approaches 1 (La/R => 1),** the **average queueing delay becomes larger** because the rate of arriving packets is **closer** to the capacity of the link.
- When the **traffic intensity exceeds 1 (La/R > 1),** the **average queueing delay becomes infinite** because **more packets are arriving** than can be serviced, leading to **congestion**.

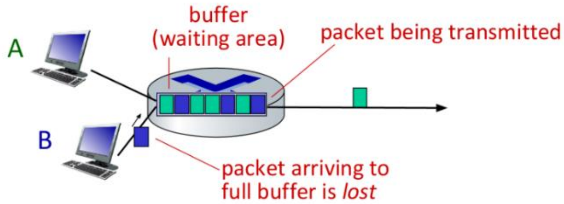
Traceroút Programs:-

Traceroute is a program that **measures delays along the internet path** from the **source to a router along the way to the destination**. It sends three packets to each router on the path, with a time-to-live value that corresponds to the router's position. The router returns the packets to the sender, and the sender measures the time between sending and receiving the packets to calculate the delay. This helps understand the real internet delays and routes.

Traceroute is like sending a message to someone, but along the way, you ask each person it passes through to send it back to you. You send three messages to each "stop" or router along the internet path to your destination. Each router sends your message back, and you measure how long it took for them to do that. This helps you see the delays and the path your message takes on the internet.

Packet loss:-

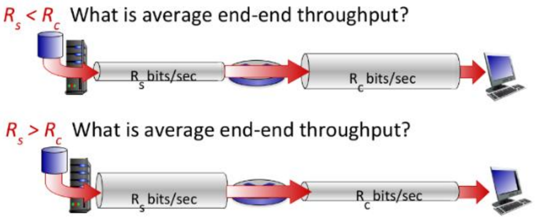
Packet loss happens when the queue (or buffer) preceding a link in the network has a limited capacity. If this buffer becomes full and a new packet arrives, there's no space to store it, so the packet is dropped or lost. This **lost packet may or may not be retransmitted by the previous node or the source end system**.



Throughput :-

Throughput is the rate at which bits are sent from a sender to a receiver.

- If the **sender's rate (Rs) is less than the receiver's rate (Rc)**, the average end-to-end throughput is **limited by the sender's rate.**
- If the **sender's rate is greater than the receiver's rate**, the average end-to-end throughput is **limited by the receiver's rate**.

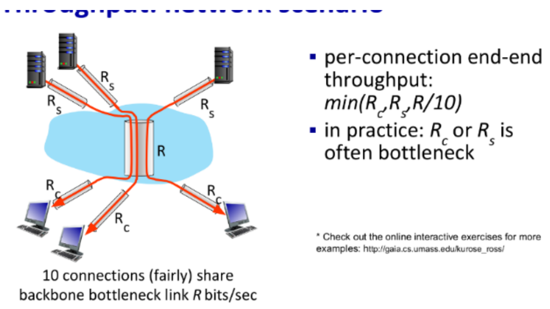

$R_s < R_c$ What is average end-end throughput?
R_s bits/sec
R_c bits/sec
$R_s > R_c$ What is average end-end throughput?
R_s bits/sec
R_c bits/sec

In a network scenario where multiple connections share a bottleneck link, the per-connection end-to-end throughput is limited by the minimum of the bottleneck link's capacity and the rates of the sender and receiver. In practice, either the sender's or the receiver's rate is often the bottleneck for throughput.

The bottleneck link is like a narrow part of the road in a traffic jam—it's the part that slows down the flow of data in the network.

Just like how a narrow road can only handle so much traffic at once, a bottleneck link can only carry a certain amount of data at a time. So, even if the sender and receiver have fast connections, if the data has to pass through this bottleneck link, it slows everything down to the speed of that link.

In simple terms, the bottleneck link is like the "slowest link in the chain" that determines how fast data can move through the network.



- per-connection end-end throughput: *min(R_c,R_s,R/10)*
- in practice: R_c or R_s is often bottleneck

10 connections (fairly) share backbone bottleneck link *R* bits/sec

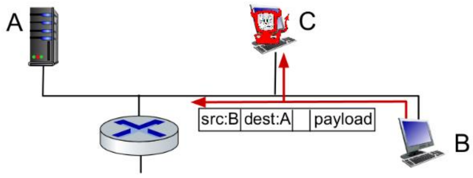
* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/

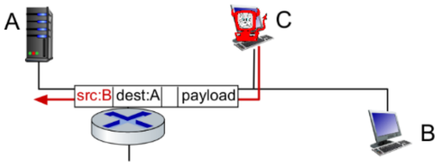
NETWORK SECURITY:-

Network security is essential as the **internet wasn't originally designed with much security** in mind.

1. how bad guys can attack computer networks
2. how we can defend networks against attacks
3. how to design architectures that are immune to attacks

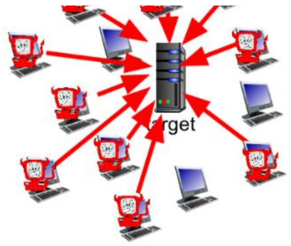
- **Packet interception(sniffing)** :-Attackers **silently listens on network traffic to capture sensitive information,** such as passwords or financial data, by using tools that intercept and analyze packets passing through the network.





- **Spoofing**:- Attackers forge the **source address of packets to disguise their identity or impersonate legitimate users**, potentially leading to unauthorized access or manipulation of data.

- **Denial of Service (DoS) attacks**:- Attackers **flood a network**, server, or service with a **high volume of traffic,** overwhelming its capacity and causing it to become unavailable to legitimate users, disrupting normal operations..



Lines of defence:-

To defend against these attacks, we use authentication, encryption, integrity checks, access restrictions, and firewalls. These measures help ensure the confidentiality, integrity, and availability of network resources.

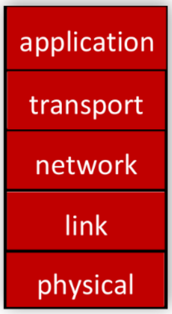
Protocol layers, service models:-

Why layering ?

Layering provides a structured way to understand complex systems by breaking them into manageable parts. It simplifies maintenance and updates, as changes in one layer don't disrupt the rest. This approach ensures clarity, ease of maintenance, and seamless adaptation to evolving requirements.

layering stack:-

- **Application layer:** Supports network applications like HTTP (web browsing), IMAP (email), SMTP (email sending), and DNS (domain name resolution).
- **Transport layer:** Manages process-to-process data transfer using protocols like TCP (reliable, connection-oriented) and UDP (unreliable, connectionless).
- **Network layer:** Handles routing of datagrams from source to destination using IP (Internet Protocol) and routing protocols. network-layer protocol encapsulates transport-layer segment [Ht | M] with network layer-layer header Hn to create a network-layer datagram Hn used by network layer protocol to implement its service



- **Link layer:** Facilitates data transfer between neighboring network elements, such as Ethernet, 802.11 (WiFi), and PPP.
- **Physical layer:** Deals with transmitting raw bits over the network medium.

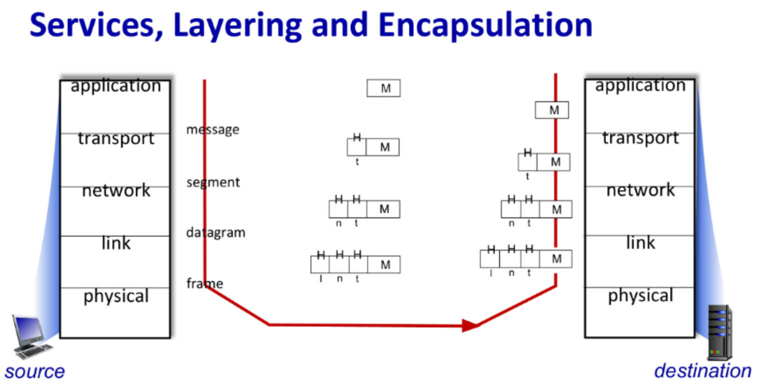
Each layer implements a specific service, relying on the services provided by the layer below it. This layered approach simplifies system design and maintenance, as changes in one layer's implementation don't affect the rest of the system.

ENCAPASULATION:-

Encapsulation is a key concept where each layer adds its own header to the data received from the layer above before passing it down to the next layer. This process continues until the data is transmitted over the physical medium.

a. **Sending a message:-**

1. Application layer will encapsulate the message and will attach the header of message that is H[m].
2. Transport layer will encapsulate the message and will attach the header of Transport layer and now it will become H[t]H[m].
3. Network layer will encapsulate the message and will attach the header of Network layer and now it will become H[n]H[t]H[m].
4. The link layer will check port number and IP configuration where to send the message.
5. Physical layer will transfer the message.



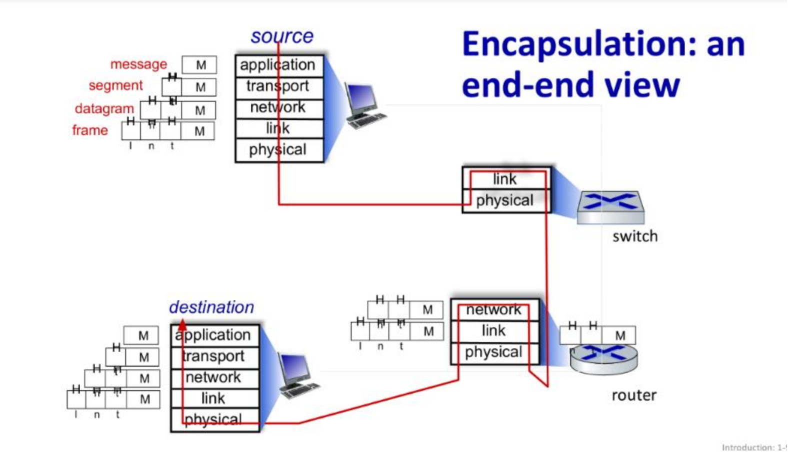
Services, Layering and Encapsulation

Now the message transferred in the form of H[n]H[t]H[m].

b. **Receiving a message: -**

On the receiving side it will be upside down process.

1. Physical layer will receive the message.
2. The link layer will check the port number and IP configuration.
   Network layer will decapsulate or decrypt the H[n] layer and now the message will become H[t]H[m] and will be transferred to transport layer.
3. Now the Transport layer will decapsulate or decrypt the H[t] layer and now the message will become H[m] and transferred to application layer.
4. Application layer will decapsulate or decrypt the message layer H[m] and the user can now see the message.



Encapsulation: an end-end view