Computer Networking

谢 逸
中山大学 • 计算机学院

2024. Fall

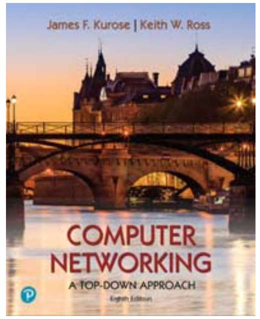
Chapter 1 Introduction

A note on the use of these PowerPoint slides:
We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

For a revision history, see the slide note for this page.

Thanks and enjoy! JFK/KWR



Computer Networking: A Top-Down Approach
8th edition
Jim Kurose, Keith Ross
Pearson, 2020

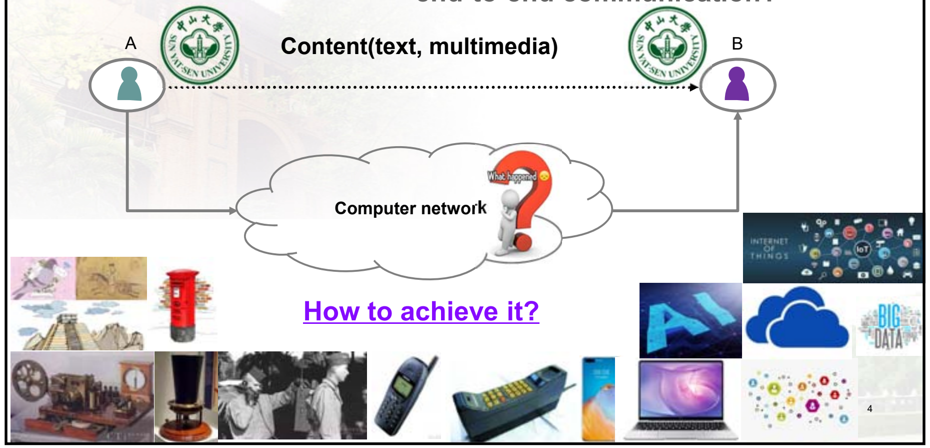
1-2

Computer Network is different from other fields:

- Computer networks are artificial systems, not natural products, , which leads to the existence of a large number of artificial concepts；
- The network is large, complex, and time-varying, making it difficult to describe using general mathematical models；
- It involves low-level physical networks, middle-level data analysis, and high-level behavior understanding；
- Data-driven analysis is only a part of it, while physical mechanisms and principles are more important。
- Only by mastering the underlying core technology can one gain the right to speak。

3

The first question: What happens to the network in end-to-end communication?



4

Assignments:

- Ch1(ver7, CN/EN): 6, 7, 8, 9, 10, 13, 14, 20, 25, 27, 29, 31, 33
- Ch1(ver8, CN/EN): 6, 7, 8, 9, 10, 13, 14, 20, 25, 27, 29, 31, 33
- Practice: 18, 19

下横杠题目为必做题

- Keywords : protocol, network edge, access network, Packet Switching, Circuit Switching, delay, Encapsulation

Chapter 1: introduction

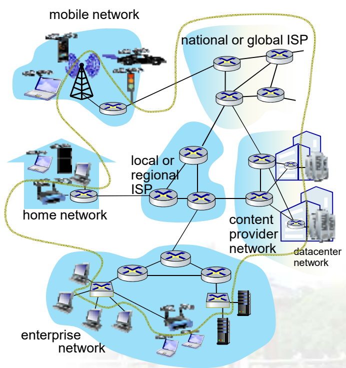
The Internet: a "nuts and bolts" view

Billions of connected computing *devices*:
- *hosts* = *end systems*
- running *network apps* at Internet's "edge"

Packet switches: forward packets (chunks of data)
- *routers*, *switches*

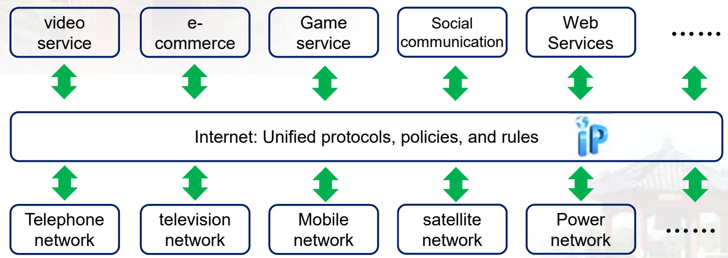
Communication links
- fiber, copper, radio, satellite
- transmission rate: *bandwidth*

Networks
- collection of devices, routers, links: managed by an organization



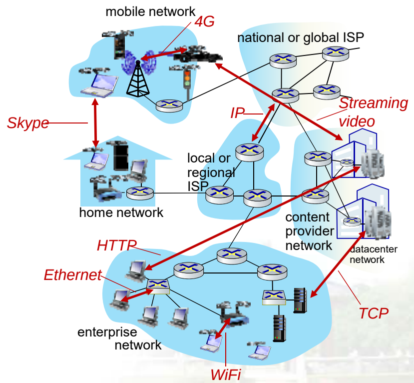
The Internet: a "nuts and bolts" view

- ***Internet: "network of networks"***
  - Interconnected ISPs



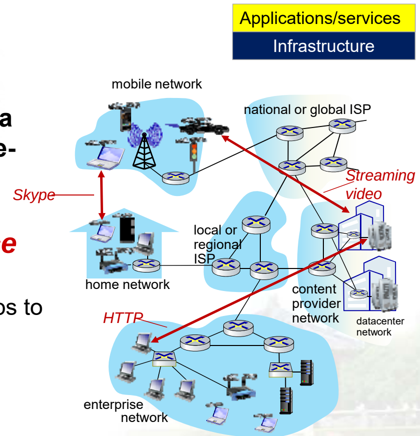
The Internet: a “nuts and bolts” view

- ***protocols are everywhere***
  - control sending, receiving of messages
  - e.g., HTTP (Web), streaming video, Skype, TCP, IP, WiFi, 4G, Ethernet
- ***Internet standards***
  - RFC: Request for Comments
  - IETF: Internet Engineering Task Force



The Internet: a “services” view

- ***Infrastructure*** **that provides services to applications:**
  - **Web, streaming video, multimedia teleconferencing, email, games, e-commerce, social media, inter-connected appliances, …**
- ***provides programming interface to distributed applications:***
  - “hooks” allowing sending/receiving apps to “connect” to, use Internet transport service
  - provides service options, analogous to postal service



What’s a protocol?

human protocols:

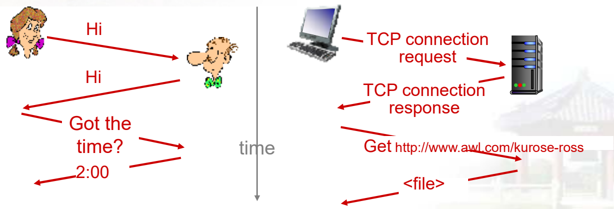
- **“what’s the time?”**
- **“I have a question”**
- **introductions**

specific **msgs** sent
specific **actions** taken when msgs received, or other events

network protocols:

- **machines rather than humans**
- **all communication activity in Internet governed by protocols**

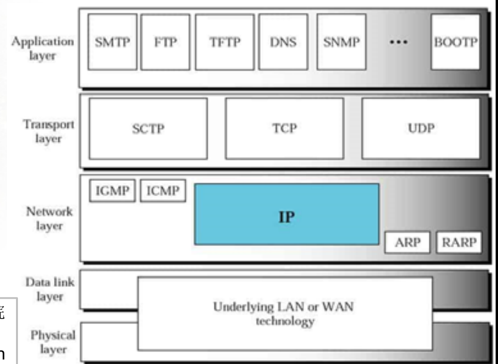
a human protocol **and** **a computer network protocol:**



What’s a protocol?

network protocols:

protocols define format, order of msgs sent and received among network entities, and actions taken on msg transmission, receipt



例如: 中国广东省广州市大学城中山大学计算机学院

School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou Higher Education Mega Center, China

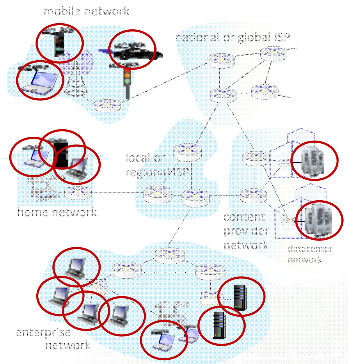
计算机大学城广州市中国学院中山大学广东省

Chapter 1: introduction

- 1.1 what *is* the Internet?
- 1.2 network edge
  - end systems, access networks, links
- 1.3 network core
  - packet switching, circuit switching, network structure
- 1.4 delay, loss, throughput in networks
- 1.5 protocol layers, service models
- 1.6 networks under attack: security
- 1.7 history

A closer look at Internet structure

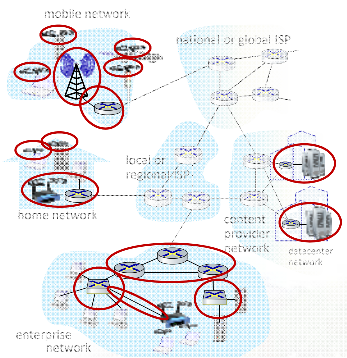
Network edge:
- hosts: clients and servers
- servers often in data centers



A closer look at Internet structure

Network edge:
- hosts: clients and servers
- servers often in data centers

Access networks, physical media:
- wired, wireless communication links

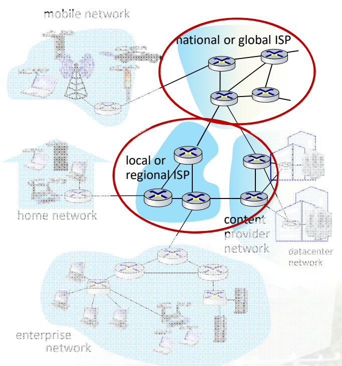


A closer look at Internet structure

Network edge:
- hosts: clients and servers
- servers often in data centers

Access networks, physical media:
- wired, wireless communication links

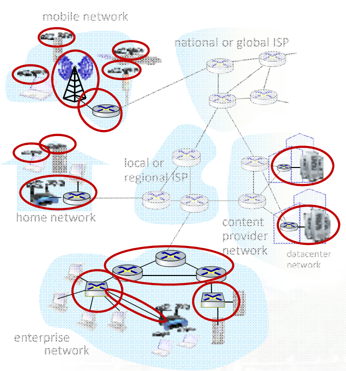
Network core:
- interconnected routers
- network of networks



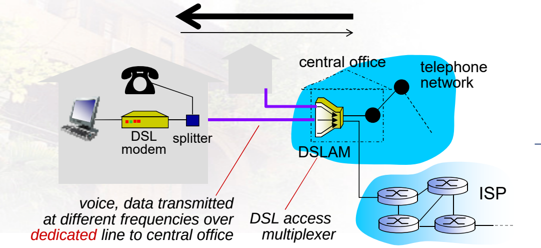
Access networks and physical media

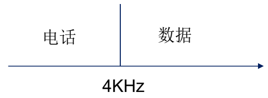
Q: How to connect end systems to edge router?

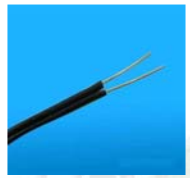
- **residential access nets**
- **institutional access networks (school, company)**
- **mobile access networks (WiFi, 4G/5G)**



Access net: digital subscriber line (DSL)

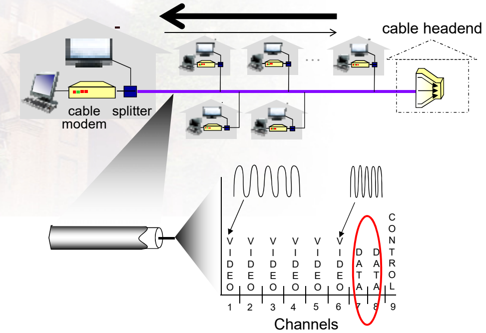






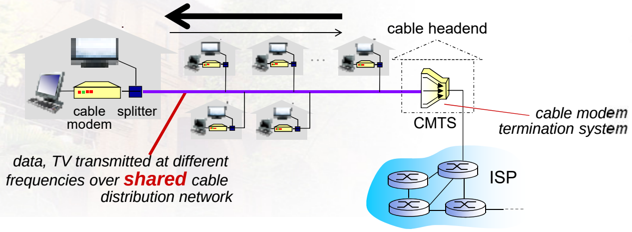
- use *existing* telephone line to central office DSLAM
  - data over DSL phone line goes to Internet
  - voice over DSL phone line goes to telephone net
- < 2.5 Mbps upstream transmission rate (typically < 1 Mbps)
- < 24 Mbps downstream transmission rate (typically < 10 Mbps)

Access net: cable network



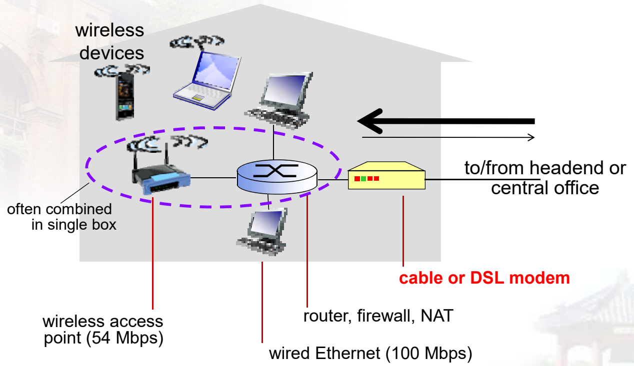
frequency division multiplexing: different channels transmitted in different frequency bands

Access net: cable network

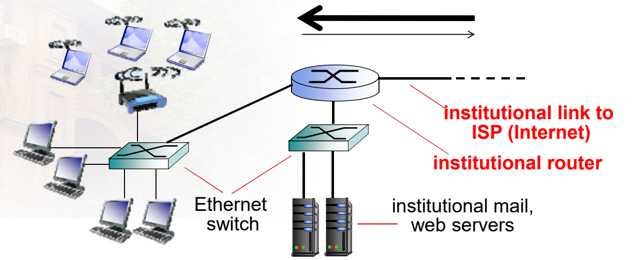


- HFC: hybrid fiber coax
  - asymmetric: up to 30Mbps downstream transmission rate, 2 Mbps upstream transmission rate
- network of cable, fiber attaches homes to ISP router
  - homes ***share access network*** to cable headend
  - unlike DSL, which has dedicated access to central office

Access net: home network



Enterprise access networks (Ethernet)



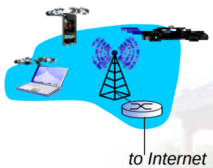
- typically used in companies, universities, etc
- 10 Mbps, 100Mbps, 1Gbps, 10Gbps transmission rates
- today, end systems typically connect into Ethernet switch

Wireless access networks

- shared *wireless* access network connects end system to router
  - via base station aka "access point"

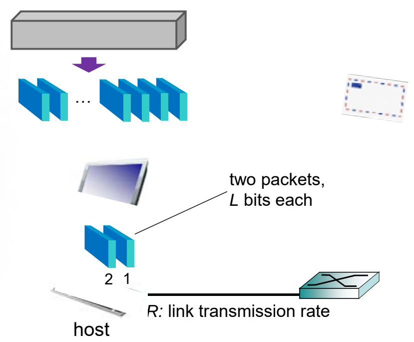
wireless LANs:
- within building (100 ft)
- 802.11b/g (WiFi): 11, 54 Mbps transmission rate

wide-area wireless access
- provided by telco (cellular) operator, 10's km
- between 1 and 10 Mbps
- 3G, 4G, 5G



Host: sends *packets* of data

host sending function:
- takes application message
- breaks into smaller chunks, known as ***packets***, of length ***L*** bits
- transmits packet into access network at ***transmission rate R***
  - link transmission rate, aka link ***capacity, aka link bandwidth***



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

Physical media

- **bit:** propagates between transmitter/receiver pairs
- **physical link:** what lies between transmitter & receiver
- **guided media:**
  - signals propagate in solid media: copper, fiber, coax
- **unguided media:**
  - signals propagate freely, e.g., radio

twisted pair (TP)
- **two insulated copper wires**
  - **Category 5: 100 Mbps, 1 Gpbs Ethernet**
  - **Category 6: 10Gbps**



1-25

Physical media: coax, fiber

coaxial cable:
- **two concentric copper conductors**
- **bidirectional**
- **broadband:**
  - **multiple channels on cable**
  - **HFC**

fiber optic cable:
- glass fiber carrying light pulses, each pulse a bit
- high-speed operation:
  - high-speed point-to-point transmission (e.g., 10’s-100’s Gpbs transmission rate)
- low error rate:
  - repeaters spaced far apart
  - immune to electromagnetic noise

1-26

Links: physical media

Wireless radio
- signal carried in various “bands” in electromagnetic spectrum
- no physical “wire”
- broadcast, “half-duplex” (sender to receiver)
- propagation environment effects:
  - reflection
  - obstruction by objects
  - Interference/noise

Radio link types:
- Wireless LAN (WiFi)
  - 10-100’s Mbps; 10’s of meters
- wide-area (e.g., 4G cellular)
  - 10’s Mbps over ~10 Km
- Bluetooth: cable replacement
  - short distances, limited rates
- terrestrial microwave
  - point-to-point; 45 Mbps channels
- satellite
  - up to 45 Mbps per channel
  - 270 msec end-end delay

Introduction: 1-27

Chapter 1: Introduction

1.1 what *is* the Internet?
1.2 network edge
- **end systems, access networks, links**

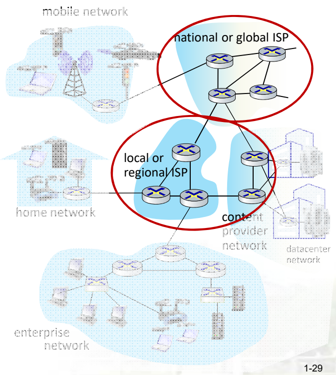
1.3 network core
- **packet switching, circuit switching, network structure**

1.4 delay, loss, throughput in networks
1.5 protocol layers, service models
1.6 networks under attack: security
1.7 history

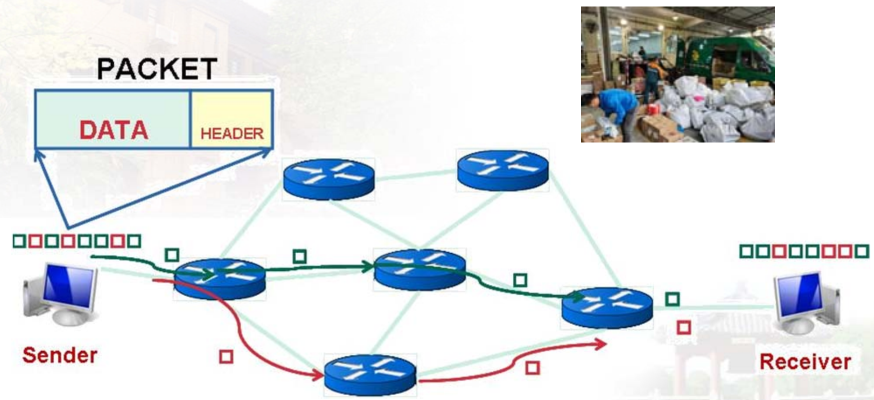
1-28

The network core

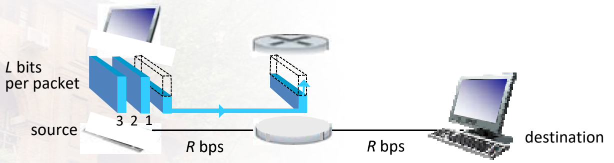
- mesh of interconnected routers
- packet-switching: hosts break application-layer messages into *packets*
  - forward packets from one router to the next, across links on path from source to destination
  - each packet transmitted at full link capacity



Packet-switching: store-and-forward



Packet-switching: store-and-forward



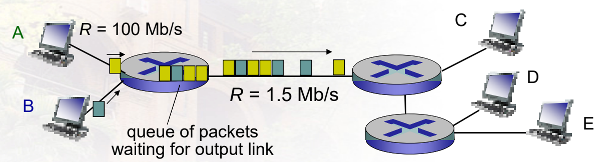
- takes L/R seconds to transmit (push out) L-bit packet into link at R bps
- *store and forward:* entire packet must arrive at router before it can be transmitted on next link

one-hop numerical example:
- L = 7.5 Mbits
- R = 1.5 Mbps
- one-hop transmission delay = 5 sec

- end-end delay = $2L/R$ (assuming zero propagation delay)

more on delay shortly …

Packet Switching: queueing delay, loss



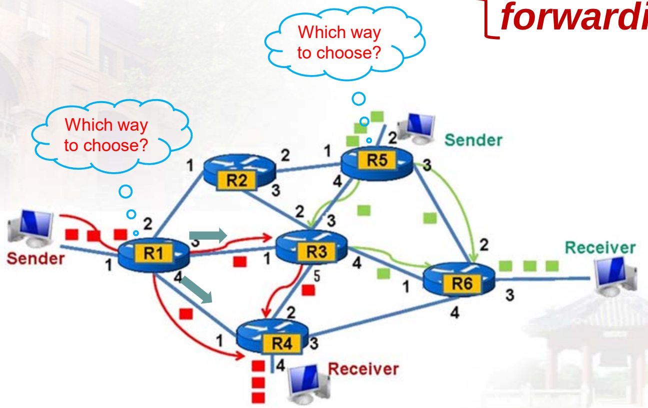
queuing and loss:
- If arrival rate (in bits) to link exceeds transmission rate of link for a period of time:
  - packets will queue, wait to be transmitted on link
  - packets can be dropped (lost) if memory (buffer) fills up

Queueing occurs when work arrives faster than it can be serviced:

2023.8.30

Two key network-core functions

routing
forwarding



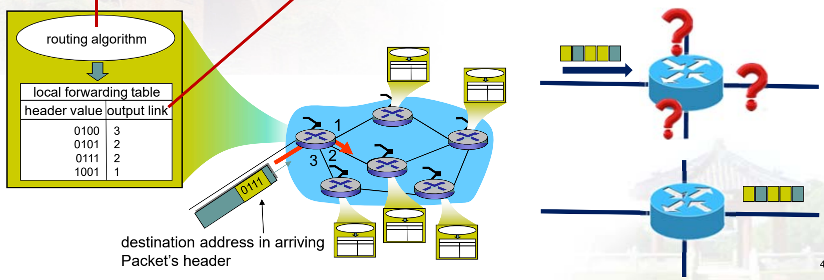
33

Two key network-core functions

routing: **determines** source-destination **route** taken by packets
- *routing algorithms*

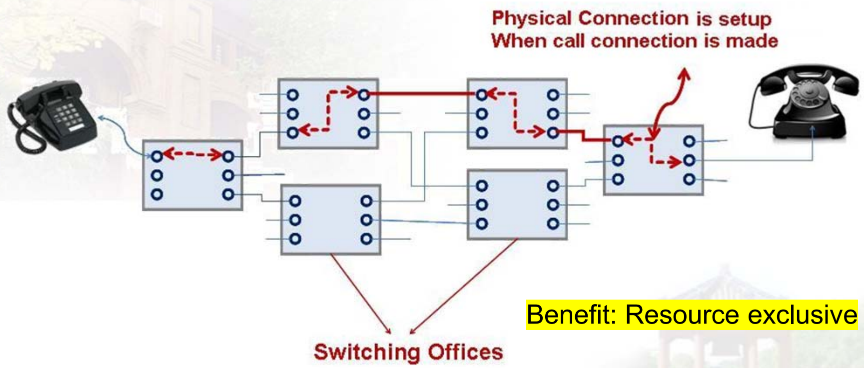
forwarding: **move** packets from router's input to appropriate router **output**

Benefit: Resource sharing



4-34

Alternative core: circuit switching



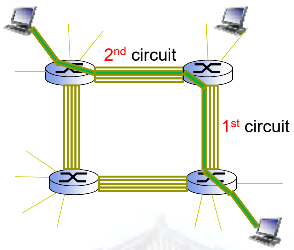
Benefit: Resource exclusive

1-35

Alternative core: circuit switching

end-end resources allocated to, reserved for "call" between source & dest:

- **In diagram, each link has four circuits.**
  - **call gets 2nd circuit in top link and 1st circuit in right link.**
- **dedicated resources: no sharing**
  - **circuit-like (guaranteed) performance**
- **circuit segment idle if not used by call (*no sharing*)**
- **Commonly used in traditional telephone networks**



Q: How does circuit switching support multiple users?

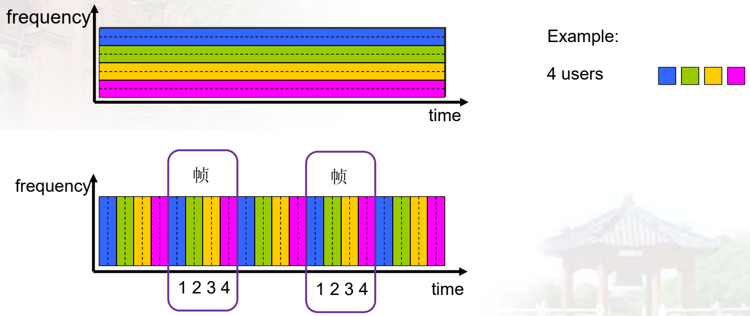
1-36

Circuit switching: FDM versus TDM

How to allocate channels and circuits

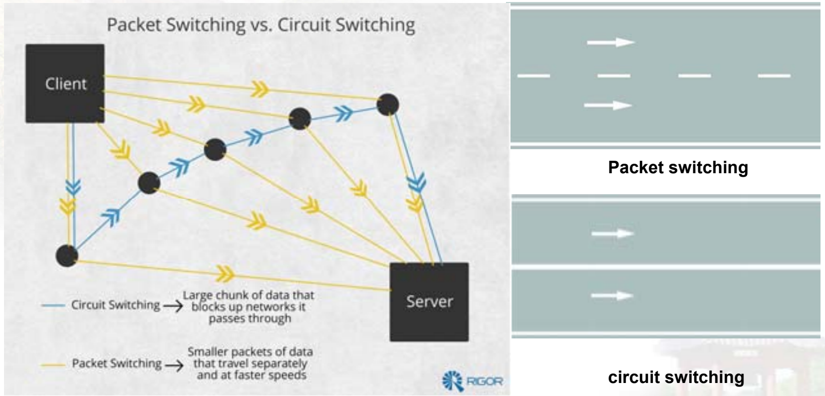
FDM

TDM



1-37

Packet switching versus circuit switching



Circuit switching: send data after the path is determined
Packet switching: send data while routing

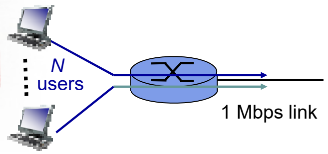
38

Packet switching versus circuit switching

packet switching allows more users to use network!

example:

- **1 Mb/s link**
- **each user:**
  - **100 kb/s when "active"**
  - **active 10% of time**



- ***circuit-switching:***
  - **10 users 10*100kb/s=1Mb**
- ***packet switching:***
  - **with 35 users, probability > 10 active at same time is less than .0004 ***

Q: how did we get value 0.0004?

(binomial distribution) $P(X=k)=C_n^k p^k (1-p)^{n-k}$

Q: what happens if > 35 users ?

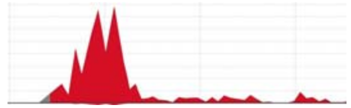
1-39

* Check out the online interactive exercises for more examples

Packet switching versus circuit switching

is packet switching a "slam dunk winner?"

- **great for bursty data**
  - **resource sharing**
  - **simpler, no call setup**



- **excessive congestion possible: packet delay and loss**
  - **protocols needed for reliable data transfer, congestion control**
- ***Q:* How to provide circuit-like behavior?**
  - **bandwidth guarantees needed for audio/video apps**
  - **still an unsolved problem**

Q: human analogies of reserved resources (circuit switching) versus on-demand allocation (packet-switching)?

1-40

Internet structure: network of networks

- End systems connect to Internet via access ISPs (Internet Service Providers)
  - Residential, company and university ISPs
- Access ISPs in turn must be interconnected.
  - So that any two hosts can send packets to each other
- Resulting network of networks is very complex
  - Evolution was driven by economics and national policies
- Let's take a stepwise approach to describe current Internet structure

41

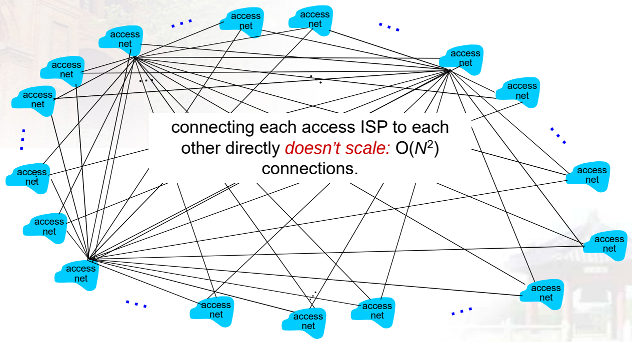
Internet structure: network of networks

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

42

Internet structure: network of networks

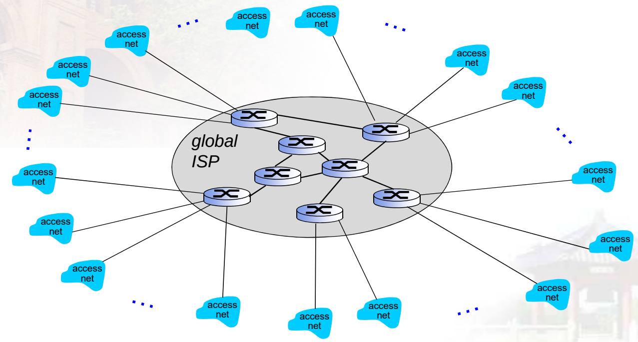
***Option:* connect each access ISP to every other access ISP?**



43

Internet structure: network of networks

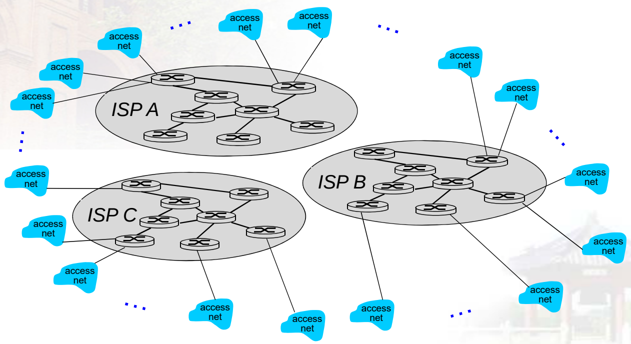
Option: connect each access ISP to a global transit ISP? Customer and provider ISPs have economic agreement.



44

Internet structure: network of networks

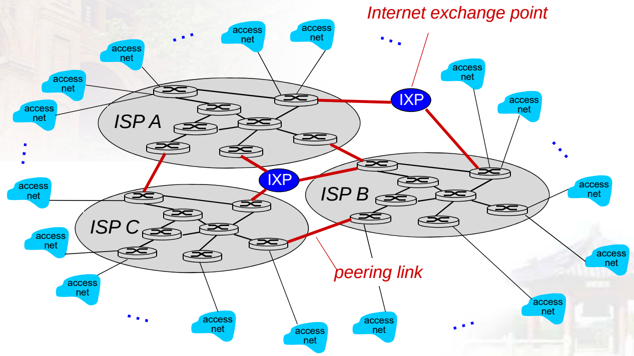
But if one global ISP is viable business, there will be competitors ….



45

Internet structure: network of networks

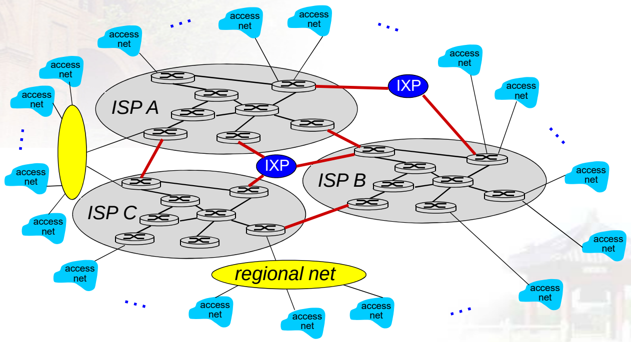
But if one global ISP is viable business, there will be competitors …. which must be interconnected



46

Internet structure: network of networks

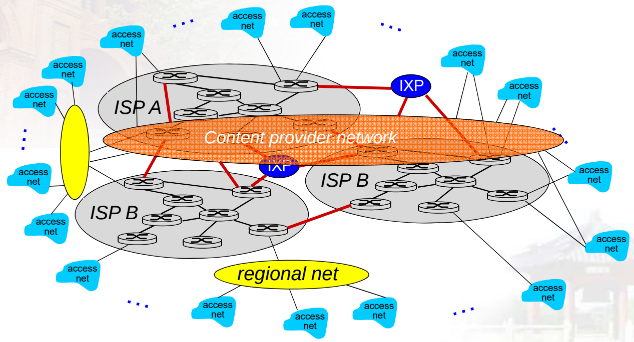
… and regional networks may arise to connect access nets to ISPS



47

Internet structure: network of networks

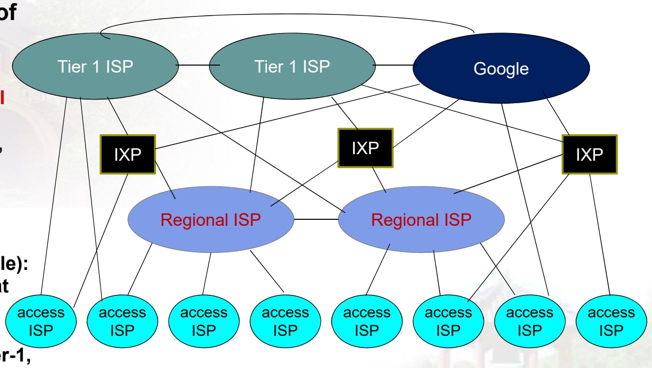
… and content provider networks (e.g., Google, Microsoft, Akamai) may run their own network, to bring services, content close to end users



48

Internet structure: network of networks

- at center: small # of well-connected large networks
  - "tier-1" commercial ISPs (e.g., Level 3, Sprint, AT&T, NTT), national & international coverage
  - content provider network (e.g, Google): private network that connects it data centers to Internet, often bypassing tier-1, regional ISPs



1-49

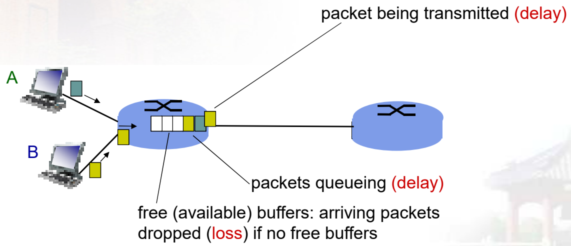
Chapter 1: introduction

1-51

How do loss and delay occur?

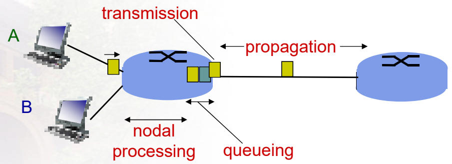
packets *queue* in router buffers

- packet arrival rate to link (temporarily) exceeds output link capacity
- packets queue, wait for turn



1-52

Four sources of packet delay



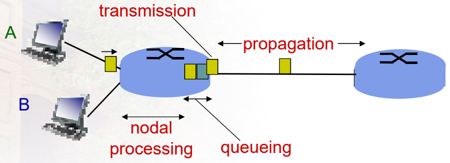
$$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$$

d_{proc}: nodal processing
- check bit errors
- determine output link
- typically < msec

d_{queue}: queueing delay
- time waiting at output link for transmission
- depends on congestion level of router

1-53

Four sources of packet delay



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

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

d_{prop}: propagation delay:
- d: length of physical link
- s: propagation speed in medium (~2x10^8 m/sec)
- $d_{prop} = d/s$

d_{trans} and d_{prop}
Very Very different

* Check out the Java applet for an interactive animation on trans vs. prop delay

1-54

Caravan analogy

相当于网卡，传输时延:12s

传播时延：1hr

传播时延>>传输时延

- **cars "propagate" at 100 km/hr**
- **toll booth takes 12 sec to service car (bit transmission time)**
- **car~bit; caravan ~ packet**
- ***Q:* How long until caravan is lined up before 2nd toll booth?**

- **time to "push" entire caravan through toll booth onto highway = 12*10 = 120 sec**
- **time for last car to propagate from 1st to 2nd toll both: 100km/(100km/hr)= 1 hr**
- ***A:* about 62 minutes**

1-55

Caravan analogy (more)

传输时延:1m

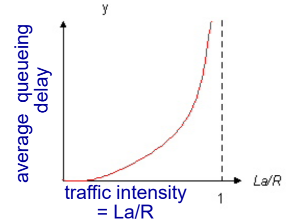
传播时延：6m

- **suppose cars now "propagate" at 1000 km/hr**
- **and suppose toll booth now takes one min to service a car**
- ***Q:* Will cars arrive to 2nd booth before all cars serviced at first booth?**
  - ***A: Yes!* after 7 min, 1st car arrives at second booth; three cars still at 1st booth.**

1-56

Queuing delay (revisited)

- ***R:* link bandwidth (bps)**
- ***L:* packet length (bits)**
- **a: average packet arrival rate**



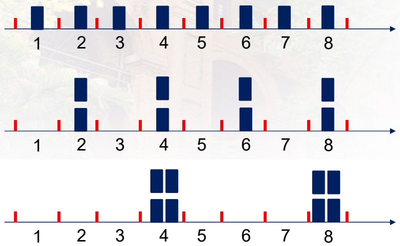
- ***La/R* ~ 0: avg. queuing delay small**
- ***La/R* → 1: avg. queuing delay large**
- ***La/R* > 1: more "work" arriving than can be serviced, average delay infinite!**

* Check out the Java applet for an interactive animation on queuing and loss

1-57

- *La/R* → 1: avg. queuing delay large
- *La/R* > 1: more “work” arriving than can be serviced, average delay infinite!

Why?



恒定速率λ到达，LaR=1，满负荷，没有排队

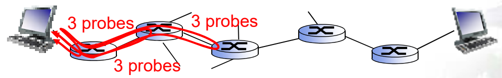
平均速率依然为λ，但是{2，4，6，8}时刻出现排队，各有1次排队

平均速率依然为λ，但是{4，8}时刻出现排队，各有3次排队

原因：分组到达不是恒定速率，具有随机突发性！
理论分析参阅排队论

“Real” Internet delays and routes（DIY）

- what do “real” Internet delay & loss look like?
- `Traceroute(win: tracert)` program: provides delay measurement from source to router along end-end Internet path towards destination. For all *i:*
  - sends three UDP packets that will reach router *i* on path towards destination
  - router *i* will return packets to sender
  - sender times interval between transmission and reply.



“Real” Internet delays, routes

traceroute: gaia.cs.umass.edu to www.eurecom.fr

3 delay measurements from gaia.cs.umass.edu to cs-gw.cs.umass.edu

```
1  cs-gw (128.119.240.254)  1 ms  1 ms  2 ms
2  border1-rt-fa5-1-0.gw.umass.edu (128.119.3.145)  1 ms  1 ms  2 ms
3  cht-vbns.gw.umass.edu (128.119.3.130)  6 ms 5 ms 5 ms
4  jn1-at1-0-0-19.wor.vbns.net (204.147.132.129)  16 ms 11 ms 13 ms
5  jn1-so7-0-0-0.wae.vbns.net (204.147.136.136)  21 ms 18 ms 18 ms
6  abilene-vbns.abilene.ucaid.edu (198.32.11.9)  22 ms  18 ms  22 ms
7  nycm-wash.abilene.ucaid.edu (198.32.8.46)  22 ms  22 ms  22 ms
8  62.40.103.253 (62.40.103.253)  104 ms 109 ms 106 ms
9  de2-1.de1.de.geant.net (62.40.96.129)  109 ms 102 ms 104 ms
10  de.fr1.fr.geant.net (62.40.96.50)  113 ms 121 ms 114 ms
11  renater-gw.fr1.fr.geant.net (62.40.103.54)  112 ms  114 ms  112 ms
12  nio-n2.cssi.renater.fr (193.51.206.13)  111 ms  114 ms  116 ms
13  nice.cssi.renater.fr (195.220.98.102)  123 ms  125 ms  124 ms
14  r3t2-nice.cssi.renater.fr (195.220.98.110)  126 ms  126 ms  124 ms
15  eurecom-valbonne.r3t2.ft.net (193.48.50.54)  135 ms  128 ms  133 ms
16  194.214.211.25 (194.214.211.25)  126 ms  128 ms  126 ms
17  * * *
18  * * *
19  fantasia.eurecom.fr (193.55.113.142)  132 ms  128 ms  136 ms
```

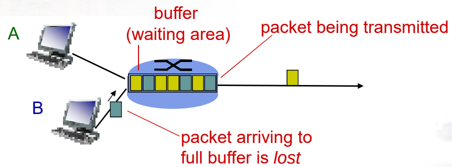
trans-oceanic link

* means no response (probe lost, router not replying)

* Do some traceroutes from exotic countries at www.traceroute.org

Packet loss

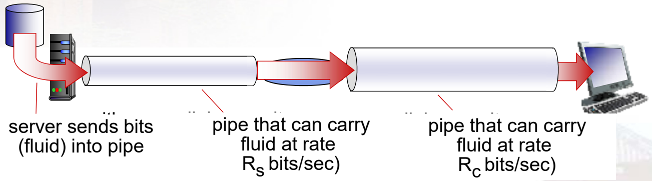
- queue (aka buffer) preceding link in buffer has finite capacity
- packet arriving to full queue dropped (aka lost)
- lost packet may be retransmitted by previous node, by source end system, or not at all



* Check out the Java applet for an interactive animation on queuing and loss

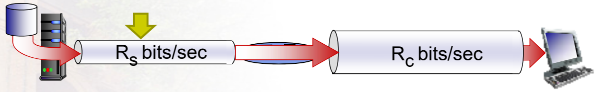
Throughput

- ***throughput:*** **rate (bits/time unit) at which bits transferred between sender/receiver**
  - ***instantaneous:*** **rate at given point in time**
  - ***average:*** **rate over longer period of time**

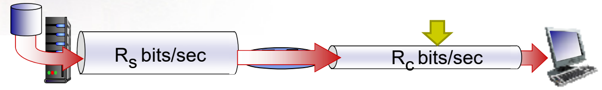


Throughput (more)

- ***$R_s < R_c$*** **What is average end-end throughput?**



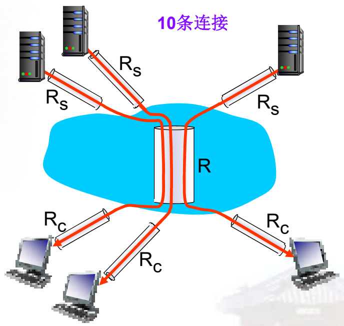
- *$R_s > R_c$* What is average end-end throughput?



bottleneck link
link on end-end path that constrains end-end throughput

Throughput: Internet scenario

- **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

Chapter 1: introduction

1.1 what *is* the Internet?
1.2 network edge
- **end systems, access networks, links**

1.3 network core
- **packet switching, circuit switching, network structure**

1.4 delay, loss, throughput in networks
1.5 protocol layers, service models
1.6 networks under attack: security
1.7 history

Protocol "layers"

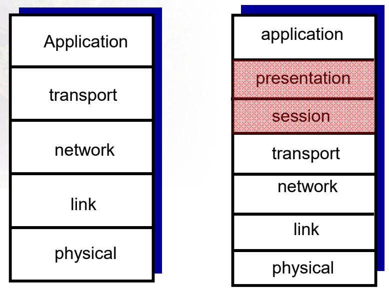
Networks are complex, with many "pieces":
- hosts
- routers
- links of various media
- applications
- protocols
- hardware, software

Question:
is there any hope of *organizing* structure of network?

…. or at least our discussion of networks?

1-66

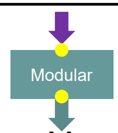
Protocol "layers"



Internet protocol stack   ISO/OSI reference model

67

Why layering?

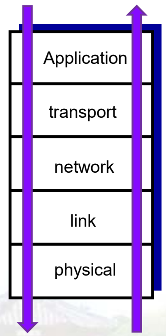


dealing with complex systems:
- explicit structure allows identification, relationship of complex system's pieces
  - layered *reference model* for discussion
- modularization eases maintenance, updating of system
  - change of implementation of layer's service transparent to rest of system
  - e.g., change in gate procedure doesn't affect rest of system
- layering considered harmful?

1-68

Internet protocol stack

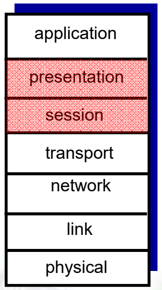
- *application:* supporting network applications
  - FTP, SMTP, HTTP
- *transport:* process-process data transfer
  - TCP, UDP
- *network:* routing of datagrams from source to destination
  - IP, routing protocols
- *link:* data transfer between neighboring network elements
  - Ethernet, 802.111 (WiFi), PPP
- *physical:* bits "on the wire"



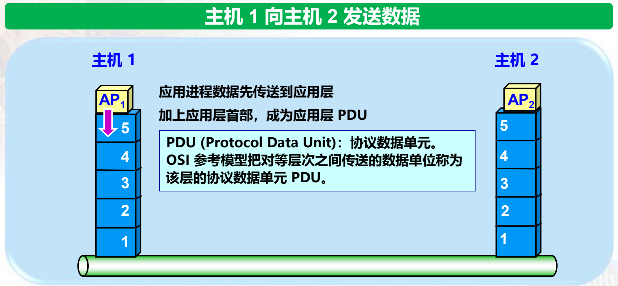
1-69

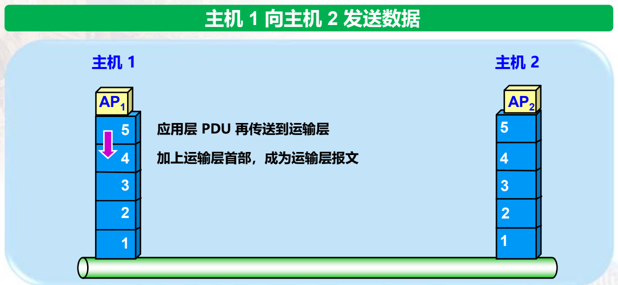
ISO/OSI reference model

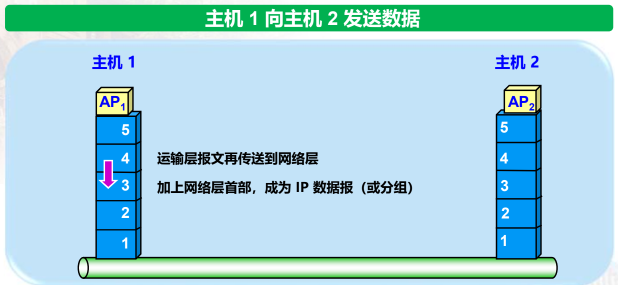
- ***presentation:*** allow applications to interpret meaning of data, e.g., **encryption, compression**, machine-specific conventions
- ***session:*** synchronization, check pointing, recovery of data exchange
- **Internet stack "missing" these layers!**
  - these services, *if needed,* must be implemented in application
  - needed?



2023.9.4

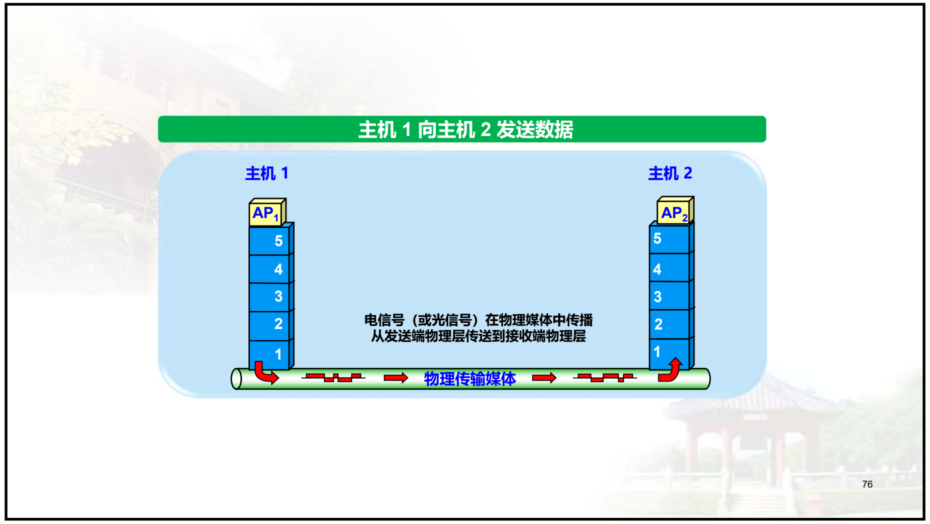







主机 1 向主机 2 发送数据
主机 1
主机 2
IP 数据报再传送到数据链路层
加上链路层首部和尾部，成为数据链路层帧
74


主机 1 向主机 2 发送数据
主机 1
主机 2
数据链路层帧再传送到物理层
最下面的物理层把比特流传送到物理媒体
75


主机 1 向主机 2 发送数据
主机 1
主机 2
电信号（或光信号）在物理媒体中传播
从发送端物理层传送到接收端物理层
物理传输媒体
76


主机 1 向主机 2 发送数据
主机 1
主机 2
物理层接收到比特流，上交给数据链路层
77


主机 1 向主机 2 发送数据
主机 1
主机 2
AP1
AP2
5
4
3
2
1
数据链路层剥去帧首部和帧尾部
取出数据部分，上交给网络层
78


主机 1 向主机 2 发送数据
主机 1
主机 2
AP1
AP2
5
4
3
2
1
网络层剥去首部，
取出数据部分上交给运输层
79


主机 1 向主机 2 发送数据
主机 1
主机 2
AP1
AP2
5
4
3
2
1
运输层剥去首部，
取出数据部分上交给应用层
80


主机 1 向主机 2 发送数据
主机 1
主机 2
AP1
AP2
5
4
3
2
1
应用层剥去首部，
取出应用程序数据上交给应用进程
81


主机 1 向主机 2 发送数据
主机 1
主机 2
我收到了 AP1 发来的
应用程序数据！
AP1
AP2
5
4
3
2
1
82


主机 1 向主机 2 发送数据
注意观察加入或剥去首部（尾部）的层次
主机 1
主机 2
应用层首部
运输层首部
网络层首部
链路层首部
链路层尾部
应 用 程 序 数 据
H5
H4
H3
H2
T2
10100110100101 比 特 流 110101110101
83


主机 1 向主机 2 发送数据
主机 1
主机 2
主机 2 的物理层收到比特流后
交给数据链路层
H2 H3 H4 H5 应 用 程 序 数 据 T2
10100110100101 比 特 流 110101110101
84


主机 1 向主机 2 发送数据
主机 1
主机 2
数据链路层剥去帧首部和帧尾部后
把帧的数据部分交给网络层
H3 H4 H5 应 用 程 序 数 据
H2 H3 H4 H5 应 用 程 序 数 据 T2
85

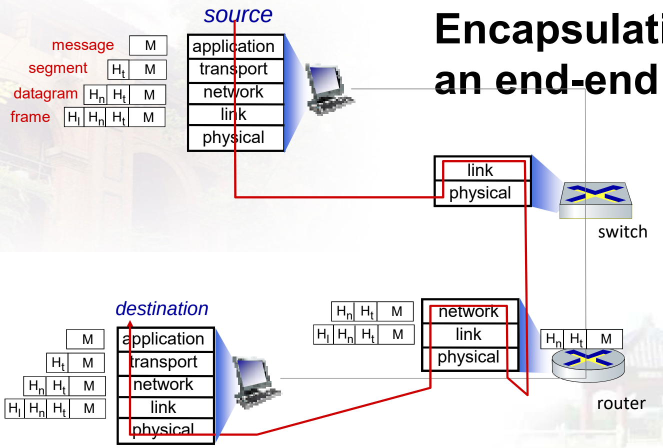

主机 1 向主机 2 发送数据
主机 1
主机 2
AP_1
AP_2
网络层剥去分组首部后
把分组的数据部分交给运输层
H_4 H_5 应用程序数据
H_3 H_4 H_5 应用程序数据
86


主机 1 向主机 2 发送数据
主机 1
主机 2
AP_1
AP_2
运输层剥去报文首部后
把报文的数据部分交给应用层
H_5 应用程序数据
H_4 H_5 应用程序数据
87


主机 1 向主机 2 发送数据
主机 1
主机 2
AP_1
AP_2
应用程序数据
H_5 应用程序数据
应用层剥去应用层 PDU 首部后
把应用程序数据交给应用进程
88


主机 1 向主机 2 发送数据
主机 1
主机 2
AP_1
AP_2
我收到了 AP_1 发来的
应用程序数据！
89

Encapsulation: an end-end view



Chapter 1: introduction

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:*** a small program written to alter the way a computer operates, without the permission or knowledge of the user. A virus must meet two criteria:
    - It must execute itself.
    - It must replicate itself.
  - ***worm:*** self-replicating infection by **passively** receiving object that gets itself executed
  - ***What is the difference between virus and worm?***
    - Virus: Effect host's behavior
    - Worm: travel from computer to computer

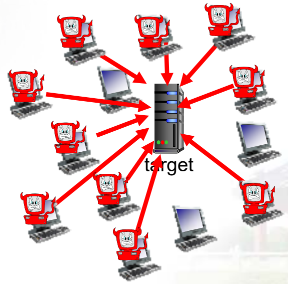
Bad guys: put malware into hosts via Internet

- **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**

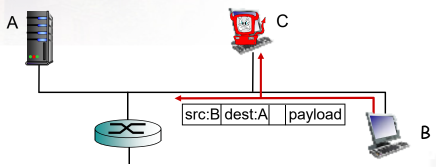
1. select target
2. break into hosts around the network (see botnet)
3. send packets to target from compromised hosts



Bad guys can sniff packets

packet "sniffing":

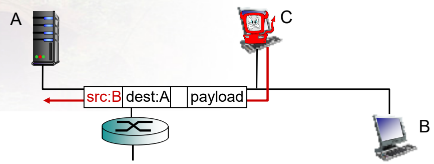
- **broadcast media (shared ethernet, wireless)**
- **promiscuous network interface reads/records all packets (e.g., including passwords!) passing by**



- 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**



… lots more on security (throughout, Chapter 8)

Lines of defense:

- authentication: proving you are who you say you are
  - cellular networks provides hardware identity via SIM card; no such hardware assist in traditional Internet
- confidentiality: via encryption
- integrity checks: digital signatures prevent/detect tampering
- access restrictions: password-protected VPNs
- firewalls: specialized "middleboxes" in access and core networks:
  - off-by-default: filter incoming packets to restrict senders, receivers, applications
  - detecting/reacting to DOS attacks

… lots more on security (throughout, Chapter 8)

Introduction: 1-98

Chapter 1: introduction

- **1.1 what *is* the Internet?**
- **1.2 network edge**
  - end systems, access networks, links
- **1.3 network core**
  - packet switching, circuit switching, network structure
- **1.4 delay, loss, throughput in networks**
- **1.5 protocol layers, service models**
- **1.6 networks under attack: security**
- **1.7 history (read after class)**

1-99

Introduction: summary

covered a "ton" of material!

- Internet overview
- what's a protocol?
- network edge, core, access network
  - packet-switching versus circuit-switching
  - Internet structure
- performance: loss, delay, throughput
- layering, service models
- security
- history

you now have:

- context, overview, "feel" of networking
- more depth, detail *to follow!*

The End of Chapter 1

Thanks

Q & A

Email: xieyi5@mail.sysu.edu.cn
https://cse.sysu.edu.cn/content/2462