SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Lec1 – Introduction

50.012 Networks

Jit Biswas

(based on earlier version co-developed with Nils Tippenhauer)

Cohort 1: TT7&8 (1.409-10)

Cohort 2: TT24&25 (2.503-4)

About 50.012 - Admin

- Course Lead and Instructor: Jit Biswas
  - Office hours: Thurs 3-5pm (1.502.25)
- TA for Cohort 1: Tok Yee Ching
  - Office hours: Tues 3-5 - Graduate Studies Cluster (GSC) 7 (1.417)
- TA for Cohort 2: John H. Castellanos Alvarado
  - Office hours: Wed 3-5 (2.716 – Grad Student Center 6)
- Part of ISTD Security and Communications Track
- Accompanying materials (slides / exercises) on eDimension
  - You should all be subscribed to the class already
- Lectures
  - Cohort 1: Mon 11:00am &Tue 10:30 am in TT7&8
  - Cohort 2: Mon 3pm &Tues 1:30 pm in TT24&25
- Labs (LEET lab 1.612)
  - Cohort 1: Wed 8:30am
  - Cohort 2: Fri 9am
- Make-up for public holiday on Deepavali
  - Cohort 1: Wed 7th Nov - 2:30pm
  - Cohort 2: Wed 7th Nov - 4pm

About 50.012 – Grades

- Grade: 40% lab exercises including project, 10% in-class activities and homework, 22% midterm, 28% final
- Lab exercise submission and grading via eDimension
- Lab late policy – total of four days of late submission (see details on Slide 5).
- Activities and Homeworks – equal weightage – best 20 out of (approx) 25 will be counted. There is no late policy for activities and homeworks.

About 50.012 – Exams

- Exams are closed book, pen & paper
- Midterm Exam: Wed 17 Oct, 2:30 pm, 90 minutes
- Midterm Venue: – Coh1-TT11&12, Coh2-TT24&25

  (Cohort 1 please note venue)
- Final Exam: Thurs 13 Dec, 3:00 pm, 120 minutes
- Final venue: TBA
- Lab grades tend to be better, exam grades tend to be harder

Notes: Lab exercises, class activities and homework

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

- Unless otherwise specified, all work is to be submitted via eDimension.
- Three of the weekly lab exercises will be substituted by a project. The project is to be completed in groups of four students.
- To cover any contingencies, students will have an allowance of four late days (**total** for the semester) for submitting their labs. Once an allowance is used up, any late submissions will not be graded or earn credit.
- In-class activities and written homeworks (*excluding* labs and project) will be assessed for the attempt made. You should show a **real attempt** in answering the questions, and you must submit your answers by the deadline to get credit. By default, in-class activities are due within class time. To cover any contingencies, the best 20 activities and homeworks will be counted, from among the total number of (approx) 25 assigned activities and homeworks.
- No makeups will be given for missed activities or homeworks

Academic Honesty

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

- **Important**. Policy of **academic honesty will be strictly adhered to**. In particular, everything (including texts and code) that you submit **must be originally authored by you** (or your group in the case of group assignments), except that you can use content from the official course textbooks (but not any solution manuals). **If you copy, quote, or paraphrase any other sources** (including but not limited to friends, classmates, work by previous students in the course, sample solutions given previously by instructors of the course, solution manuals of any textbooks, textbooks other than the official ones listed in Sec. IV below, and any internet or public resources), **you must *explicitly* reference the sources.** Borrowing liberally or unnecessarily from third-party sources will reduce your credit, but proper citation will exonerate you from academic dishonesty. We will use automated tools to check for plagiarism of writing or programs.

About 50.012 – Content

- First half of term: Discussion of individual network layers
- Second half of term: Discussion of cross-layer topics
- Main contents:
  - Internet as service platform
    - HTTP/RESTful APIs, streaming, balancing
  - Nuts and Bolts of TCP/IP and Internet
- TCP, routing protocols, network devices
  - Other networks (industrial, buses, etc.)
    - Datacenter networks, software-defined networks
- Any other topics of interest? Please let us know!

Content Plan

Roughly six bi-weekly segments:

- Weeks 1&2 - Intro, The Internet, Application layer and Web APIs
- Weeks 3&4 - Transport layer, TCP, Network Layer, Routing
- Weeks 5&6 - Link Layer, Encapsulation, Physical Layer, IPv6 and IOT
- Weeks 7&8 - Wireless, Mesh Networks and Industrial Control Networks
- Weeks 9&10 - Aggregated networks and their management, the separation of planes
- Weeks 11&12 - Special topics (Privacy, Enterprise Networks, Overlay networks)

Recommended texts

- The lectures are loosely based on “Computer Networks: A top-down Approach” 6th edition, Kurose & Ross
- Reference foils, as appropriate, are available at:

`http://www-net.cs.umass.edu/kurose-ross-ppt-6e/`

- Other recommended books (both available in e-book form, subscribed by our library)
  - Tanenbaum and Wetherall, “Computer Networks”, 5th Edition, 2011. `http://proquestcombo.safaribooksonline.com.library.sutd.edu.sg:2048/book/networking/9780133485936`
  - Peterson and Davie, "Computer Networks: A Systems Approach“, 5th Edition. `http://proquestcombo.safaribooksonline.com.library.sutd.edu.sg:2048/book/networking/9780123850591`

Informal Goals

- Give you detailed understanding of the structure of the Internet
- Understand most important protocols you use daily
- Understand servers + cloud, how to set up their networking
- Understand web APIs
- Understand local area networks, how to set them up
- Understand networking options for embedded devices/ IoT

Learning Objectives

1. Explain fundamental network protocols
2. Paraphrase the organization of computer networks, and list factors influencing computer network development and the reasons for having variety of different types of networks
3. Solve standard problems in interconnections between autonomous networks
4. Model the Internet structure and derive operational parameters
5. Design optimized network topology for given problem settings
6. Judge and evaluate a provided network setup
7. Design and implement a server-client architecture based on sockets

Measurable Outcomes

1. Describe the essential features of different networking protocols, such as UDP, TCP, IP, DNS, and ARP [LO1]
2. Design of a computer network based on a set of provided operational requirements [LO2+LO5]
3. Apply routing algorithms to determine the shortest path in a network, modeled as a weighted graph [LO3]
4. Model and analyze the Internet as a network of autonomous systems [LO4]
5. Analyze a real network setup and critique the design decisions [LO6]
6. Design and implement a client-server application program using sockets. [LO7]

Introduction to Networks

Overview of today's lecture

- What are networks?
- How to approach the Internet?
- (Re-) introduce five network layers
- Use the layers to structure networks
- There will be some overlap with CSE content

What are networks?

- In your own words, what are networks?
- Why are they important?
- What types of networks are you familiar with?
- How have you used networks?
- What is fundamental to all networks?
- How are they different?
- What are common components in networks?

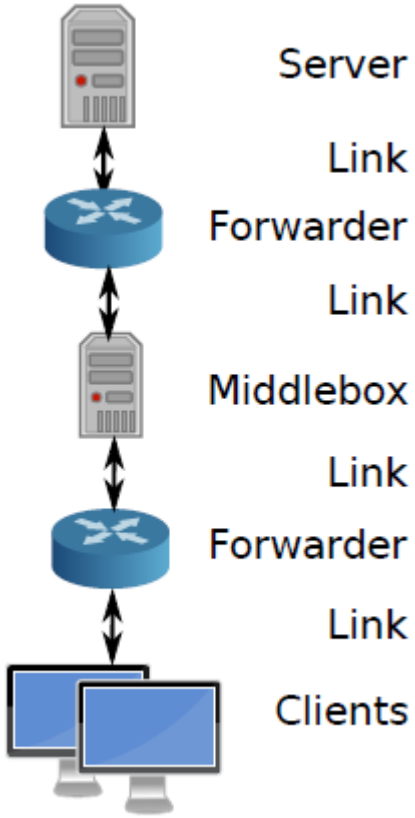
SUTD network: how do you see it?

Warm-up discussion: your view of the SUTD network

- What does it provide for you?
- How do you think it is organized?
- How could it be improved?
- What could you use it for?

Common components in networks

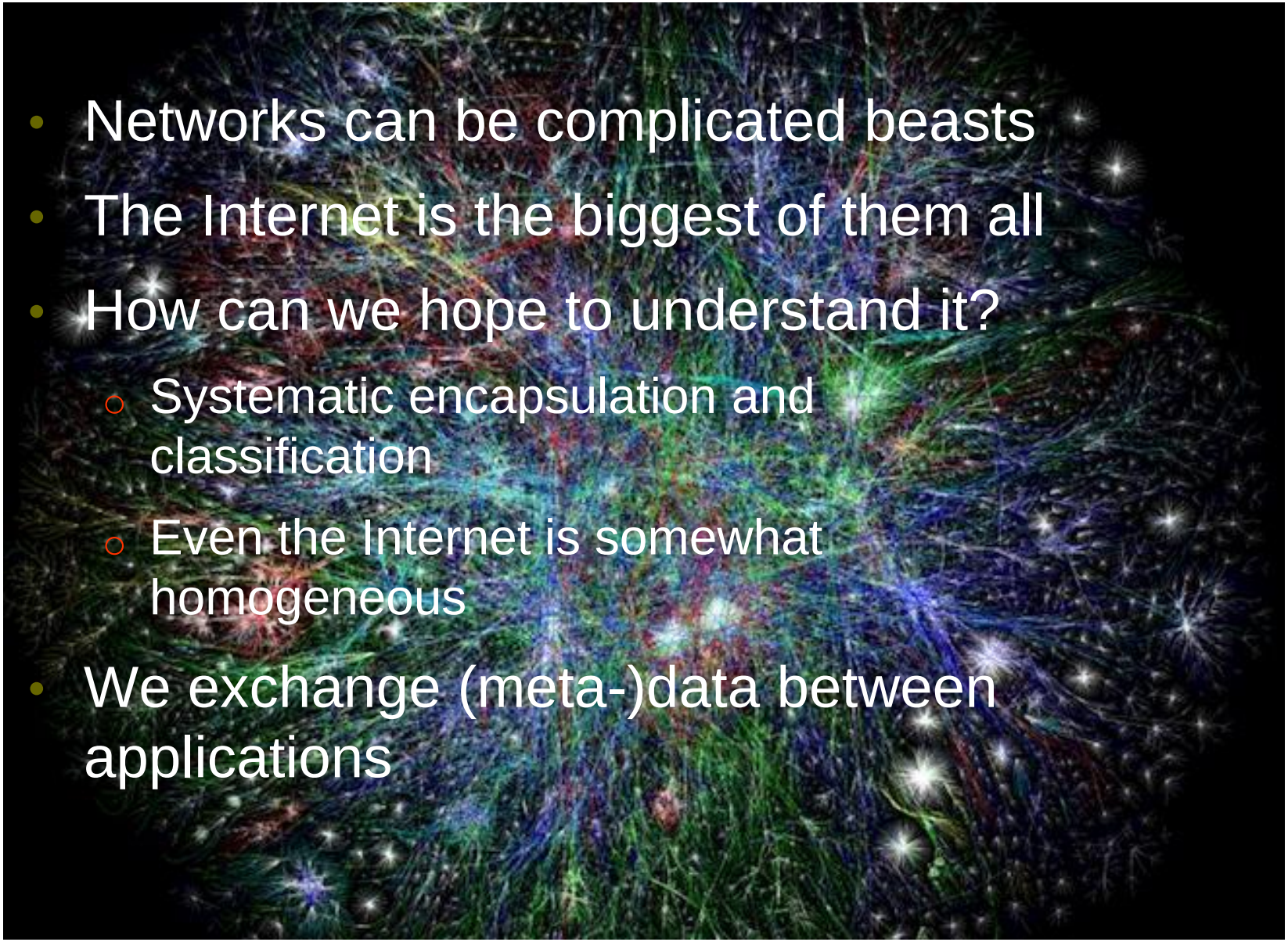
- Servers:
  - Always available
  - Provide service for users
- Links (connecting devices)
- Forwarder (Router, switches)
- Middlebox (inspecting and changing traffic: firewall, proxy, NAT)
- Clients:
  - Starting and stopping dynamically
  - Actively initiating connection to server



Networking as a fundamental service

- In this class, we focus on the Internet
- But networking does not stop there
  - Mobile phone networks
  - Local bus between CPU and memory
  - Automotive and airplane networks
- In general: any data exchange between systems

How to approach the Internet?



- Networks can be complicated beasts
- The Internet is the biggest of them all
- How can we hope to understand it?
  - Systematic encapsulation and classification
  - Even the Internet is somewhat homogeneous
- We exchange (meta-)data between applications

 A map of the internet, circa 2005. *Image:* The Opte Project

Different views of a network

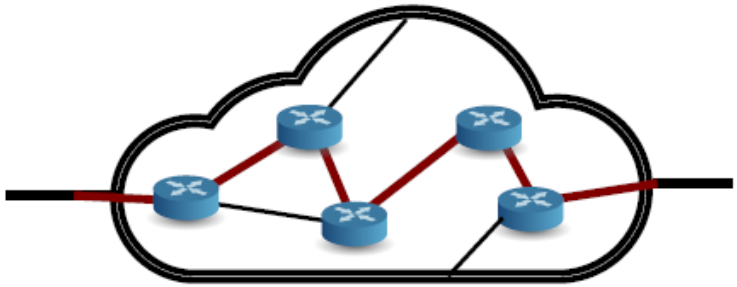
- Networks (like any system) can be viewed from multiple perspectives:
- High-level perspective:
  - How do I use the network?
  - What can I do using the network?
  - Focusing on the edge of the system
- Medium-level perspective:
  - How can we connect different systems?
  - Which services are required in the background?
  - Focusing on the core of the network
- Low-level perspective:
  - How can two computers transmit data via a wire?
  - How can multiple transceivers share a common medium?
  - Focusing on the *signals* exchanged

High level view of the Internet

- Websites: type in keyword at google, visit websites to get info, order things, share pictures, collaborate in a teleconference
- Email: configure your phone, it gets your email for you
- Gaming: online activation, online matchmaking etc.
- Synchronization: Dropbox, GIT, Bittorrent
- Ideally, all of this happens magically
- Internet as a "black box"

Medium level view of the Internet

- Data is exchanged in nested data structures (like envelopes in envelopes)
- Internet is a large exchange of internet protocol (IP) packets
  - Need to be forwarded towards target (routing & forwarding)
  - The payload does not matter much for routing
- IP packets are passed along *route* from source to destination



Low level view of the Internet

- IP packets can be transported in many different ways
  - Ethernet
  - WiFi
  - Pigeons (see RFC 1149)

- Communication standards define
  - The communication channel/medium
  - The modulation
  - Low-layer medium access control and similar

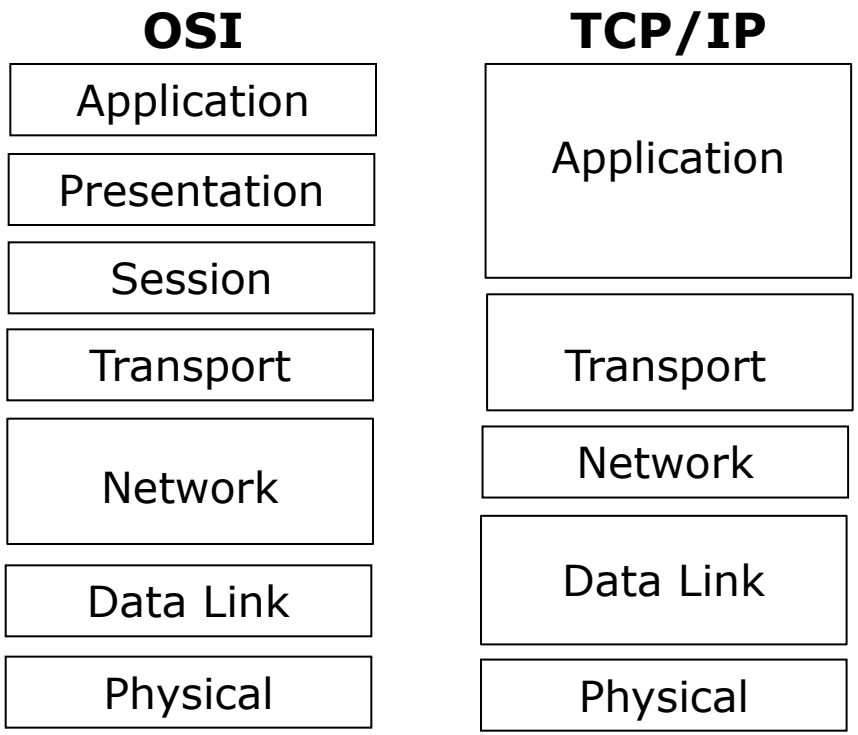
Protocol – definition

A **protocol** defines the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event.

Protocol models:

- OSI
- TCP / IP

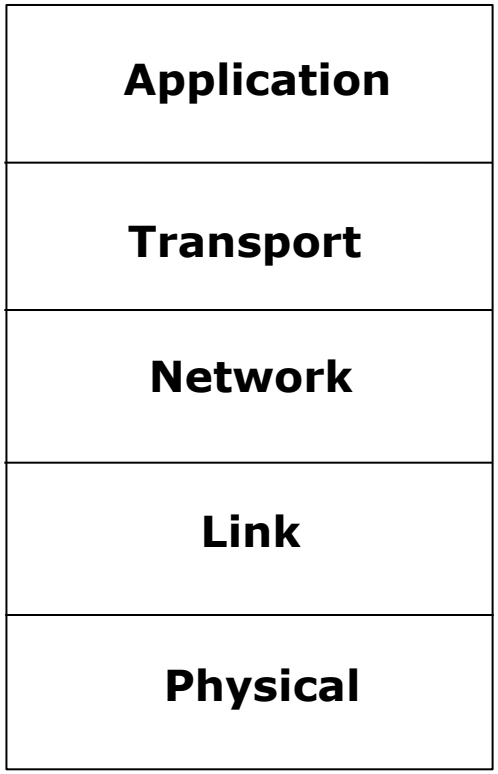
Open Systems Interconnection (OSI) and TCP/IP stacks



- The seven-layer OSI **Open Systems Interconnection** model is often used as a reference
- Did not gain popularity
- Only X.400, X.500, and IS-IS have achieved lasting impact
- The goal has been met by the Internet protocol suite

Protocol Layers

- We can map these different views on different layers
- Here, we use a layer model with 5 layers
- Layers only "see" the neighboring layer
- Reduces complexity in design of system
  - Similar to encapsulation in programming
  - Allows isolated changes to part of system



Applying layers to our views

- "High level" view described is the application layer
  - Protocols such as HTTP, SMTP, SIP
  - Only view needed for most programmers
- "Medium level" view is the Internet layer
  - How to route IP packets, queuing and forwarding
  - Only view needed for most sysadmins
- "Low level" view is physical layer
  - Which voltage denotes a logical One, frequency division of channel, etc.
  - Only view needed for (electrical) engineers

Data processed in each layer

Each layer adds further data, we use different terms to refer to data in each layer:

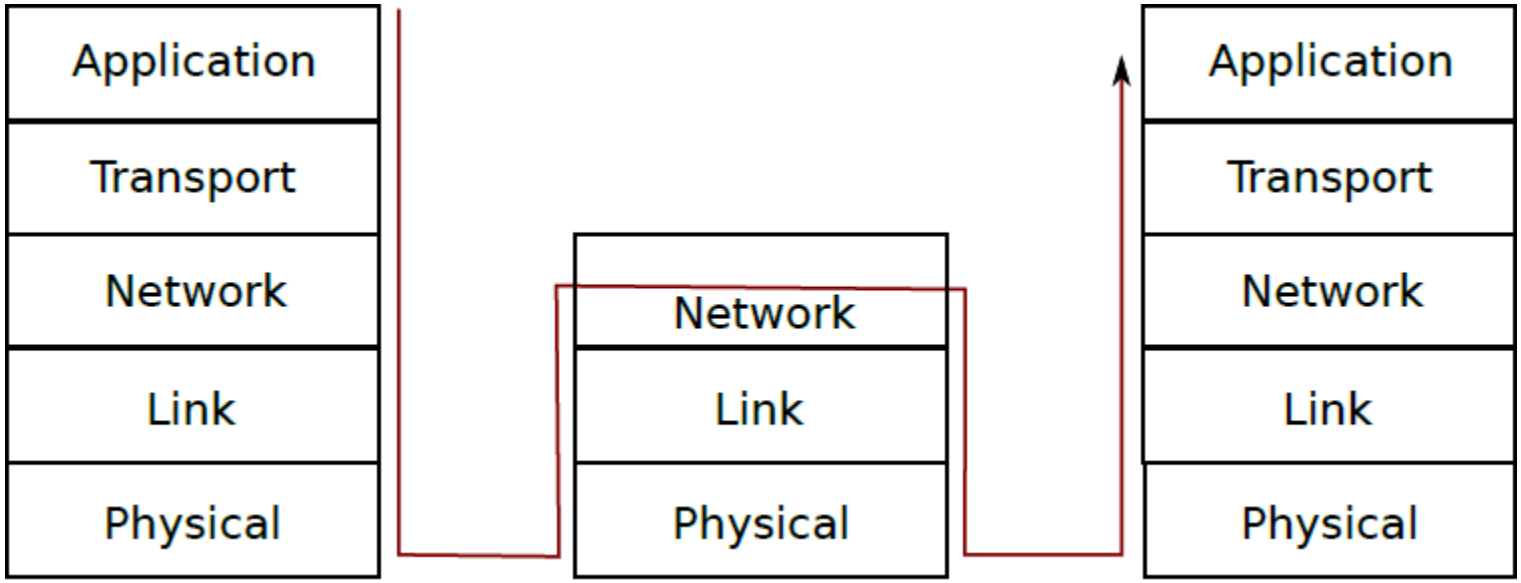
- Application layer: messages
  - Data, in format understandable by app (e.g. JSON)
- Transport layer: segment
  - Added data: port numbers, flow control, integrity checks
- Network layer: datagram
  - Added data: IP addresses
- Link layer: frame
  - Added data: MAC address, checksums, channel access data
- Physical layer: symbols
  - More like translation of data into analog representations

Key functions at layers

- Segmentation and reassembly
- Multiplexing and de-multiplexing
- Connection setup
- Error handling
- Flow control

More on layers

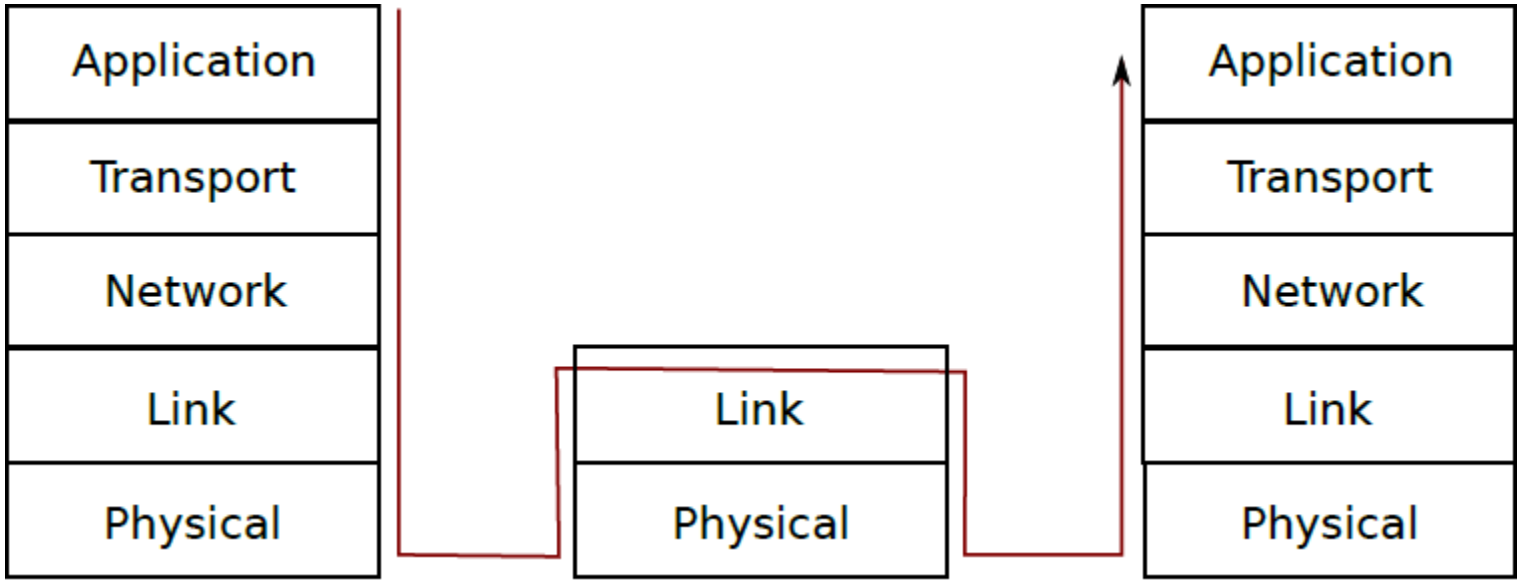
- Network core usually only required lowest three layers
  - Intermediate links could even have only two layers
- Only the network edge has all the complexity, i.e. all five layers



Transport through L3 router

More on layers

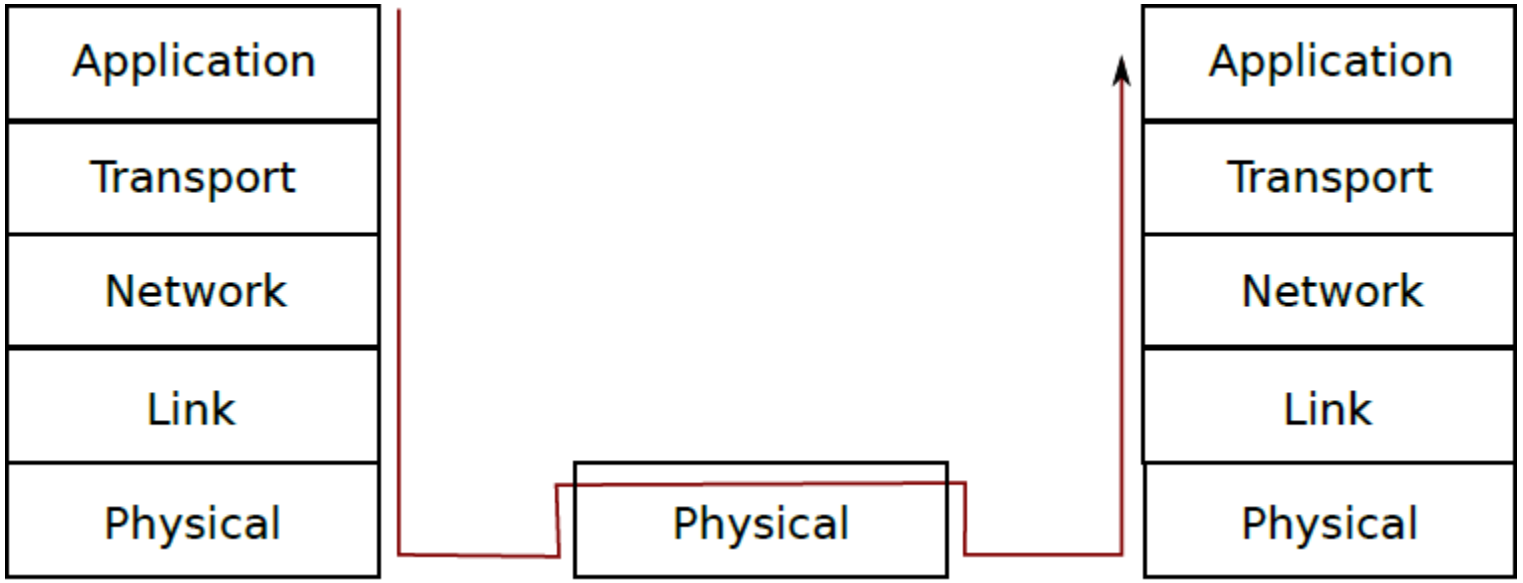
- Network core usually only required lowest three layers
  - Intermediate links could even have only two layers
- Only the network edge has all the complexity, i.e. all five layers



Transport through L2 switch

More on layers

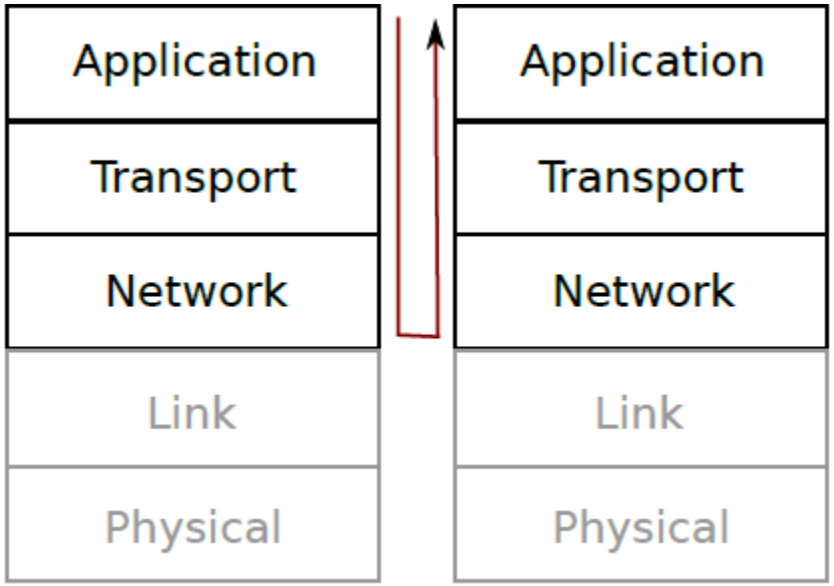
- Network core usually only required lowest three layers
  - Intermediate links could even have only two layers
- Only the network edge has all the complexity, i.e. all five layers



Transport through L1 repeater / hub

More on layers

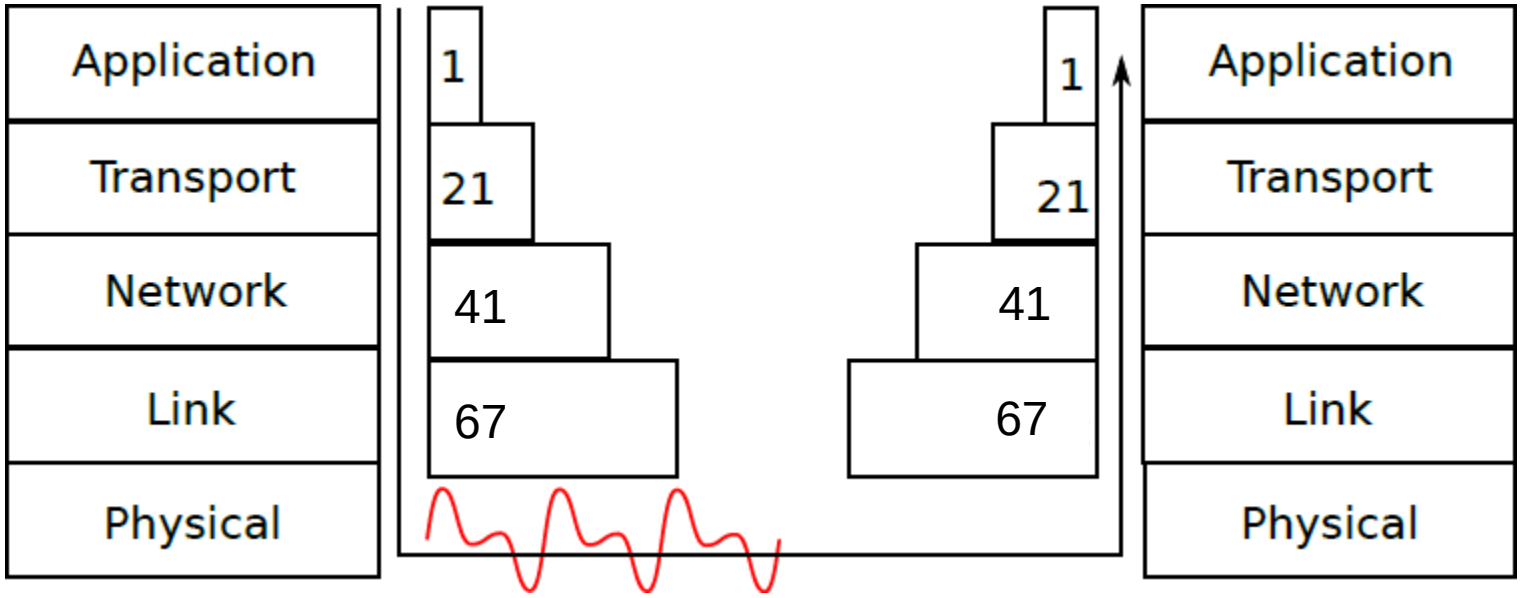
- Network core usually only required lowest three layers
  - Intermediate links could even have only two layers
- Only the network edge has all the complexity, i.e. all five layers
- Communication between applications on the same machine might skip link layer and lower



Local Transport through Loopback interface

Overhead through layers

- Messages sent from one application to another:
  - Descend the layers to physical layer at sender
  - Ascend the layers to application layer at receiver
- With each layer descent, additional information is added
  - A 1 Byte application layer message can be inflated to 67 Bytes (TCP+IP+ETH)



Key challenges

Key challenges faced by networks:

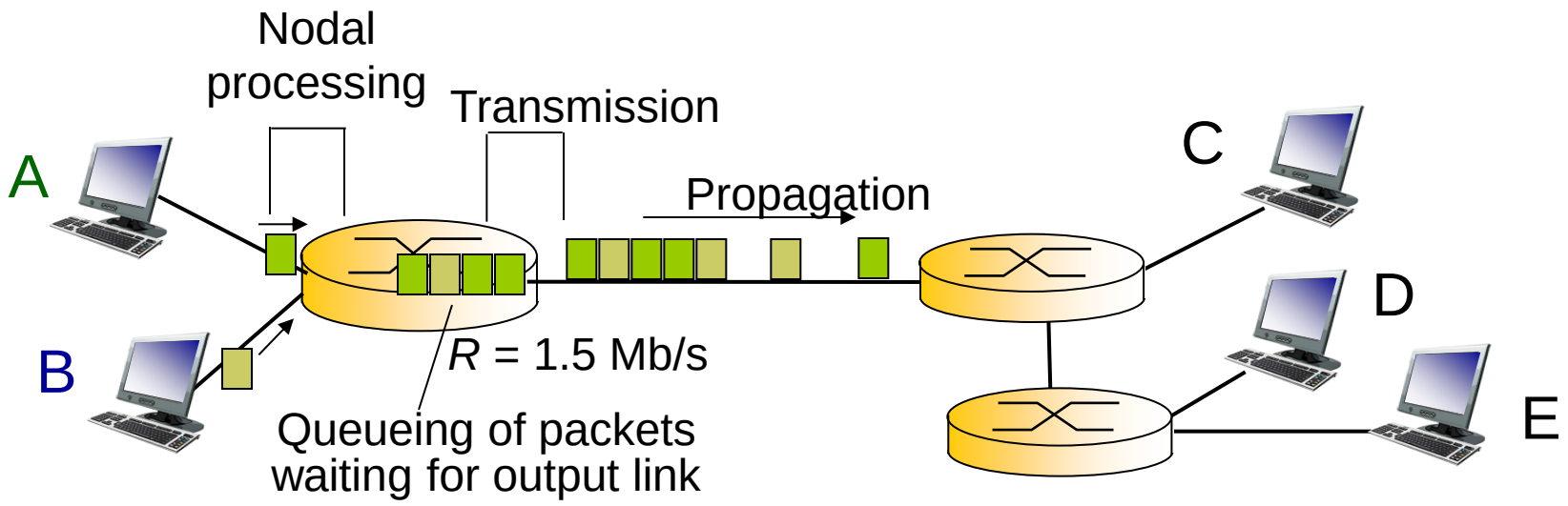
- Reliability (loss, link failure)
- Scalability (rapid increase of users)
- Interoperability (new applications/protocols vs legacy)
- Efficiency (efficient use of bandwidth/resources)
- Security (confidentiality, integrity, availability)

Throughput, Latency, Loss

What are the performance characteristics of networks?

- Throughput: How much data can be transmitted per time unit
- Per node delays:
  - Transmission delay: Time taken by transceiver to send out the packet
  - Propagation delay: How long does the message travel
  - Processing delay: Time taken for processing incoming packet
  - Queuing delay: How long does the message wait in node buffer
- Latency: Time taken for a packet to travel from one point in a network to another
- Loss / reliability: Will all packets be delivered, or will some be lost?

Packet Switching: Delays and loss

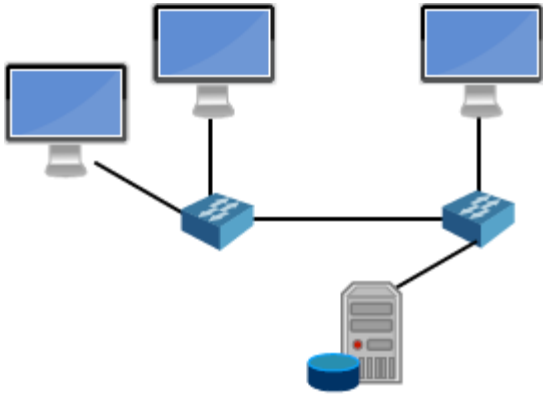


queuing and loss:

- 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

Packet Switching vs Circuit Switching

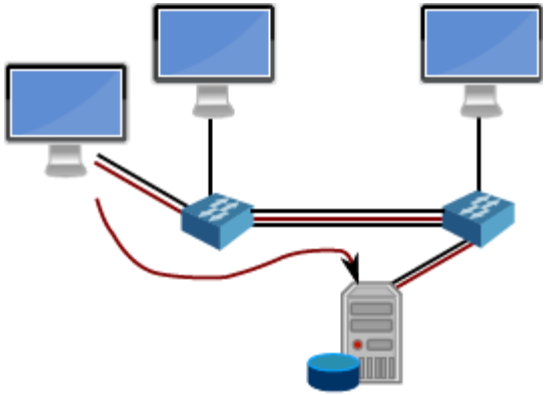
- How are packets transmitted end-to-end?
- Circuit Switching: each link can have multiple circuits
  - Prior to transmission, a sequence of circuits is reserved
  - These circuits are then exclusively used to transmit message
  - While reserved, circuits are only used by message
- Packet Switching: message is split into packets
  - Each packet is routed individually
  - Links are shared with other transmissions
  - No guarantees on max delay, higher throughput



Example Network

Packet Switching vs Circuit Switching

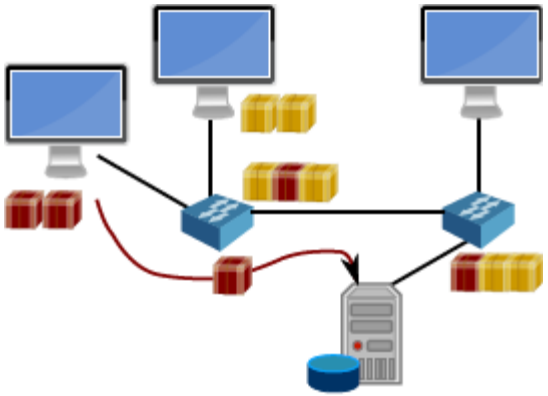
- How are packets transmitted end-to-end?
- Circuit Switching: each link can have multiple circuits
  - Prior to transmission, a sequence of circuits is reserved
  - These circuits are then exclusively used to transmit message
  - While reserved, circuits are only used by message
- Packet Switching: message is split into packets
  - Each packet is routed individually
  - Links are shared with other transmissions
  - No guarantees on max delay, higher throughput



Circuit-switching: Path of circuits reserved for transmission

Packet Switching vs Circuit Switching

- How are packets transmitted end-to-end?
- Circuit Switching: each link can have multiple circuits
  - Prior to transmission, a sequence of circuits is reserved
  - These circuits are then exclusively used to transmit message
  - While reserved, circuits are only used by message
- Packet Switching: message is split into packets
  - Each packet is routed individually
  - Links are shared with other transmissions
  - No guarantees on max delay, higher throughput



Packet-switching: Transmissions as packets through shared links

Packet vs Circuit Switching II

- Circuit switching is the traditional telephone network approach
  - Guaranteed capacity for high quality calls
  - Pricing is based on time, not volume
- Packet switching is key concept of Internet and computer networks
  - Best effort transmission of packets
  - Much better capacity use
  - Great for bursty data
  - Simpler, no call setup
  - Traffic-based billing (higher yield for operator)
  - No transmission guarantees, e.g. queuing loss
- Downside - excessive congestion possible: packet delay and loss
  - protocols needed for reliable data transfer, congestion control

Performance comparison packet vs circuit switching

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

- Example: 100 Mb/s link
- Each user requires 10 Mb/s when active
  - Users are only active 10% of the time
- Performance of circuit switching:
  - 10 users are assigned 10 Mb/s each
- Performance of packet switching ?

Performance comparison packet vs circuit switching

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

- Example: 100 Mb/s link
- Each user requires 10 Mb/s when active
  - Users are only active 10% of the time
- Performance of circuit switching:
  - 10 users are assigned 10 Mb/s each
- Performance of packet switching ?

- Binomial distribution yields probability of overload ($>$ 10 users)
- For error threshold of 0.05%, 35 users can share link

$$P(X \leq 10) = \sum_{i=0}^{10} \binom{35}{i} (0.1)^i (0.9)^{35-i} = 0.99957$$

$$P(X > 10) = 1 - P(X \leq 10) = 0.00042..$$

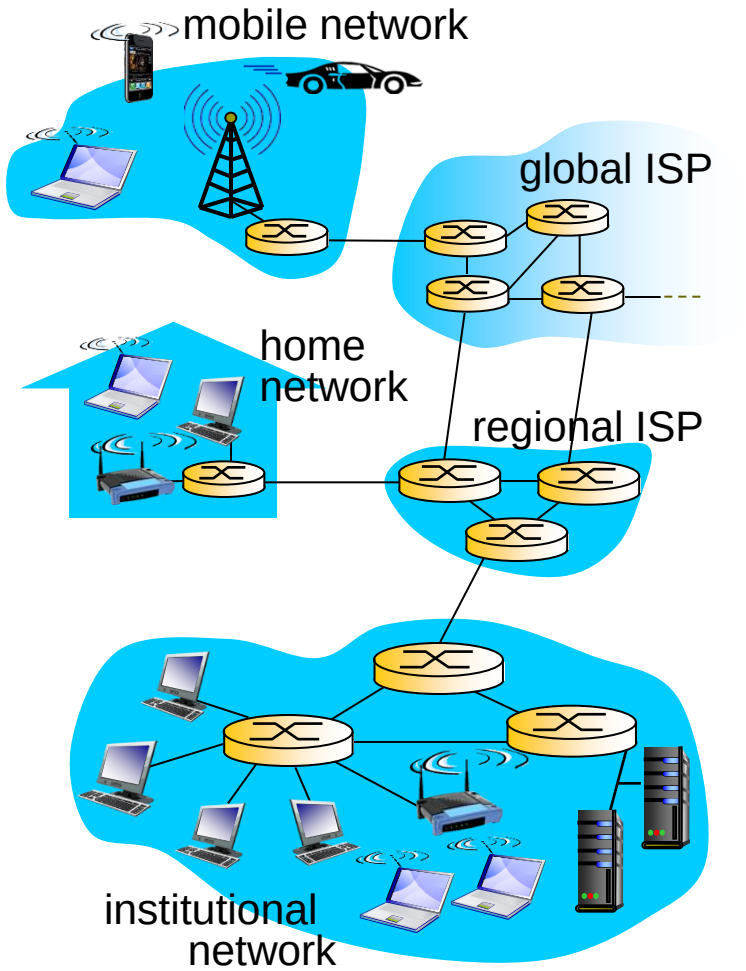
- Packet switching: 35 users instead of 10

Best effort vs. Guarantees

- We saw that for average conditions, packet-switching allows better performance
- Unfortunately, we sacrifice guarantees for this:
  - What if the link bandwidth is exceeded?
    - In practice, we fill buffers, which might overflow
    - We will start to lose packets
- This is a fundamental design decision:
  - The internet (and IP) is a best-effort solution

A closer look at network structure:

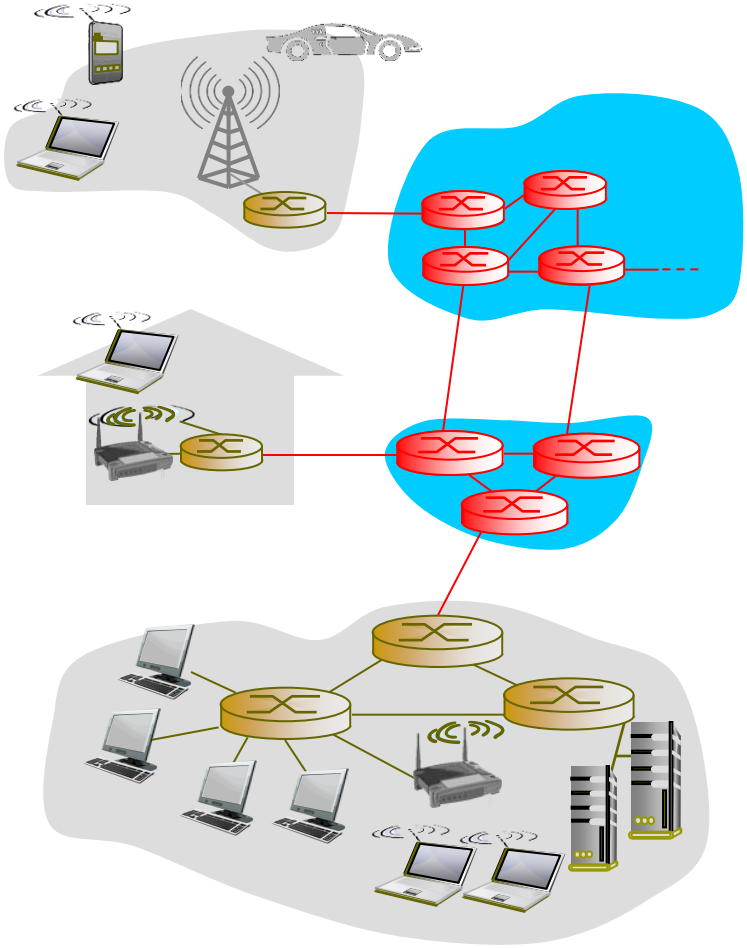
- *network edge:*
  - hosts: clients and servers
  - servers often in data centers
- *access networks, physical media:* wired, wireless communication links
- *network core:*
  - interconnected routers
  - network of networks



Source: Kurose & Ross Chapter 1 slide set

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



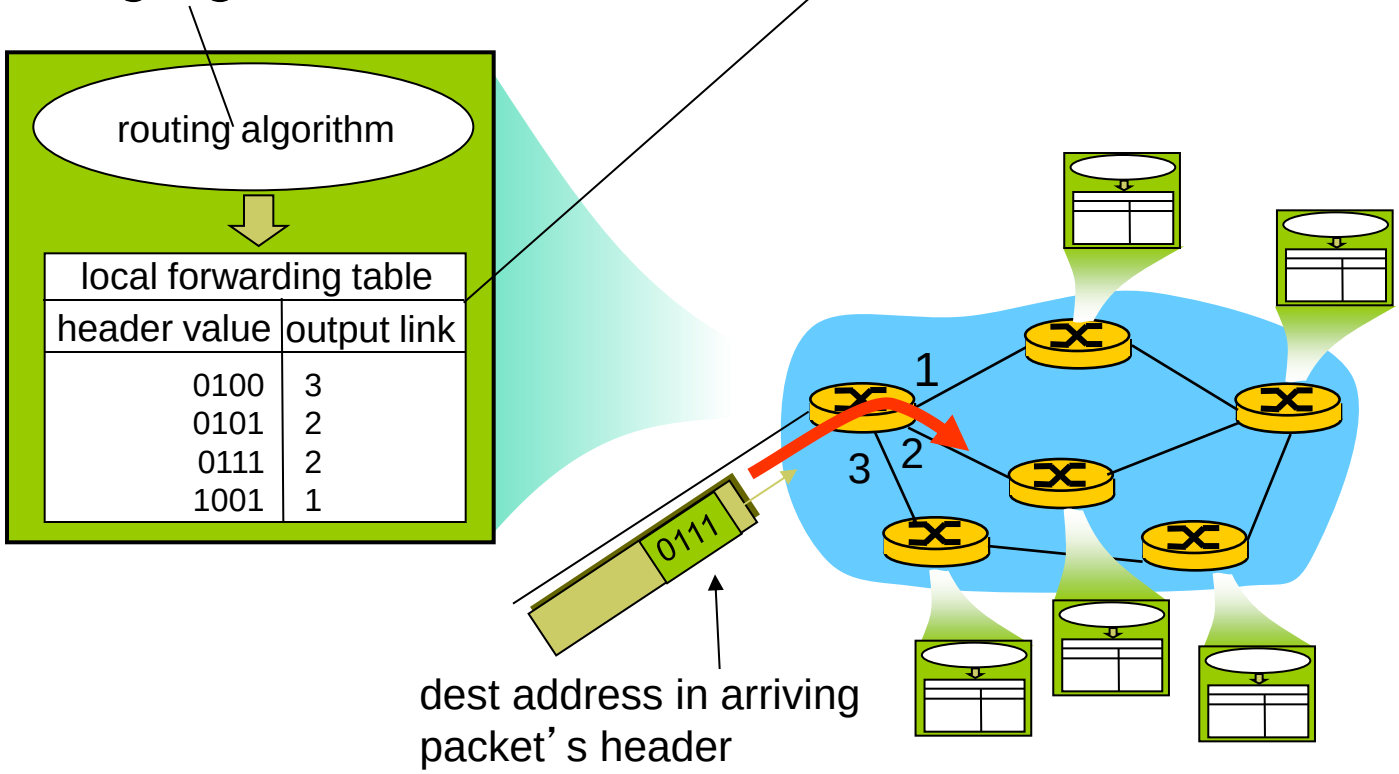
Source: Kurose & Ross Chapter 1 slide set

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



Source: Kurose & Ross Chapter 4 slide set

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

Network security – a brief reminder

DPM: Delinking PCs from Net would have disrupted attack

Privacy watchdog looking into possible security lapses; COI members named

Irene Tham
Senior Tech Correspondent

Cutting off Internet access on public healthcare computers could have disrupted the cyber attack that led to the most serious data breach in Singapore's history, Deputy Prime Minister Teo Chee Hean said yesterday.

"We could and should have implemented Internet surfing separation on public healthcare systems just as we have done on our public sector systems," said DPM Teo, who was the minister-in-charge of the civil service when the computers were delinked from the Internet.

"This would have disrupted the cyber kill-chain for the hacker and reduced the surface area exposed to the attack. This has now been done," he said at the Public Service Engineering Conference 2018.

He disclosed that the attackers had gained entry into the SingHealth system through one of the front-end computers connected to the Internet used by "thousands of users in the medical and academic community".

The incident had exposed weaknesses in the end-user workstations of the public health sector, he added.

The attack, which led to the data leak involving 1.5 million SingHealth patients, including Prime Minister Lee Hsien Loong, took place between June 27 and July 4. It was made public last Friday.

Yesterday, more details of widening investigations into the breach came to light.

The privacy watchdog, the Personal Data Protection Commission (PDPC), is looking into whether there were security lapses in healthcare group SingHealth and the Integrated Health Information Systems (IHiS), the technology outsourcing arm of public hospitals.

The PDPC will assess if SingHealth and IHiS had properly secured patients' personal data and whether they are liable for a fine of up to $1 million under the Personal Data Protection Act.

The commission will take into account the report of the Committee of Inquiry (COI), which will be headed by former chief district judge and current Public Service Commission member Richard Magnus.

In convening the COI, whose members were named yesterday, Minister-in-charge of Cyber Secu-

Source: Straits Times – July 25th 2018

Network security

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

- 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!

Source: Kurose & Ross Chapter 1 slide set

Bad guys: put malware into hosts via Internet

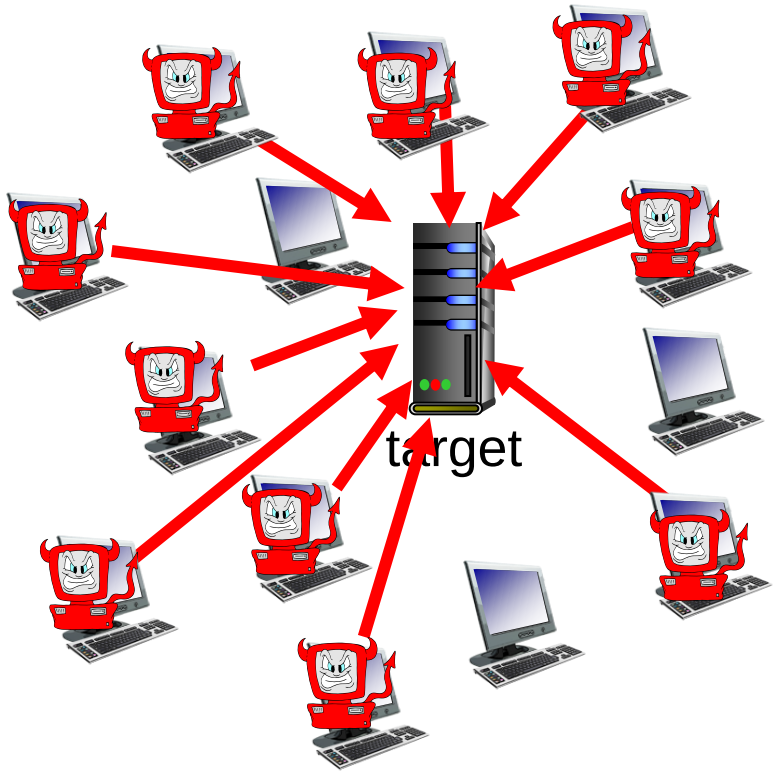
- malware can get in host from:
  - *virus:* self-replicating infection by receiving/executing object (e.g., e-mail attachment)
  - *worm:* self-replicating infection by passively receiving object that gets itself executed
- spyware malware can record keystrokes, web sites visited, upload info to collection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

Source: Kurose & Ross Chapter 1 slide set

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

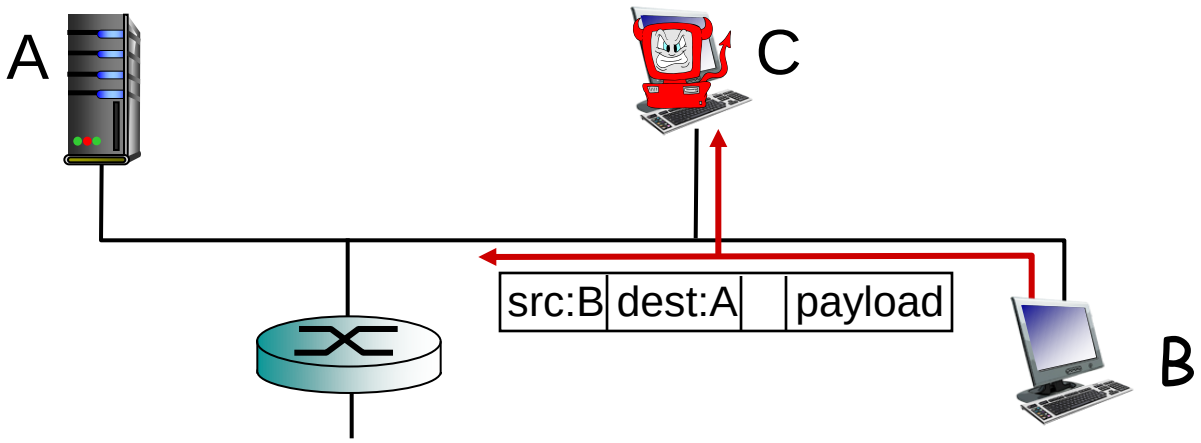


Source: Kurose & Ross Chapter 1 slide set

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

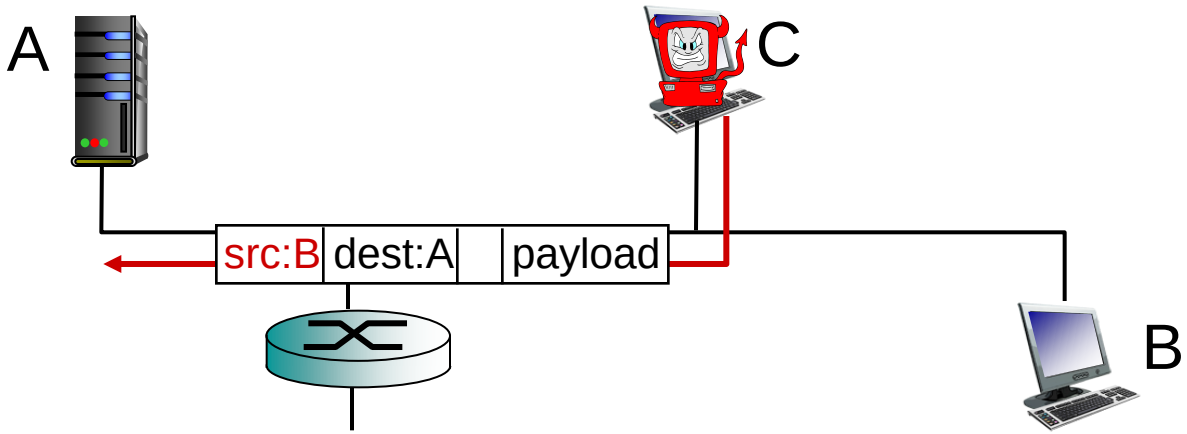


- wireshark software is a (free) packet-sniffer

Source: Kurose & Ross Chapter 1 slide set

Bad guys can use fake addresses

IP spoofing: send packet with false source address



Source: Kurose & Ross Chapter 1 slide set

Homework 1: Learning from ping and ICMP

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

- Q1. What are two advantages and two disadvantages of having international standards for network protocols?

- Q2a. Assume a host sends out a ping request using ICMP. The ICMP default payload size is 32 bytes. Assume an ICMP header of 8 bytes and an IP header of 20bytes and an Ethernet header of size 14 bytes, What is the size of a frame transmitted on the wire?
- Q2b. Assume that with additional ping arguments the ICMP payload becomes the maximum MTU size at IP layer (1500bytes), What is the ICMP payload size? What is the size of the frame transmitted on the wire?
- Q2c. Try to verify your calculations using wireshark.

Ref: http://www.hackingarticles.in/understanding-guide-icmp-protocol-wireshark/

Conclusion

Today we presented a high level overview of networks

- what's a network?
- The Internet is packet-switched and best-effort
  - no guarantees on delivery, but good performance on average
  - packet-switching versus circuit-switching
- Internet structure
- Important quality metrics of links: loss, delay, throughput
- Layering helps to classify and understand complex networks
- Security

More in depth in the remaining lectures