Data Communication and Computer Networks

10. Link Layer
PART-C

Dr. Aiman Hanna
Department of Computer Science & Software Engineering
Concordia University, Montreal, Canada

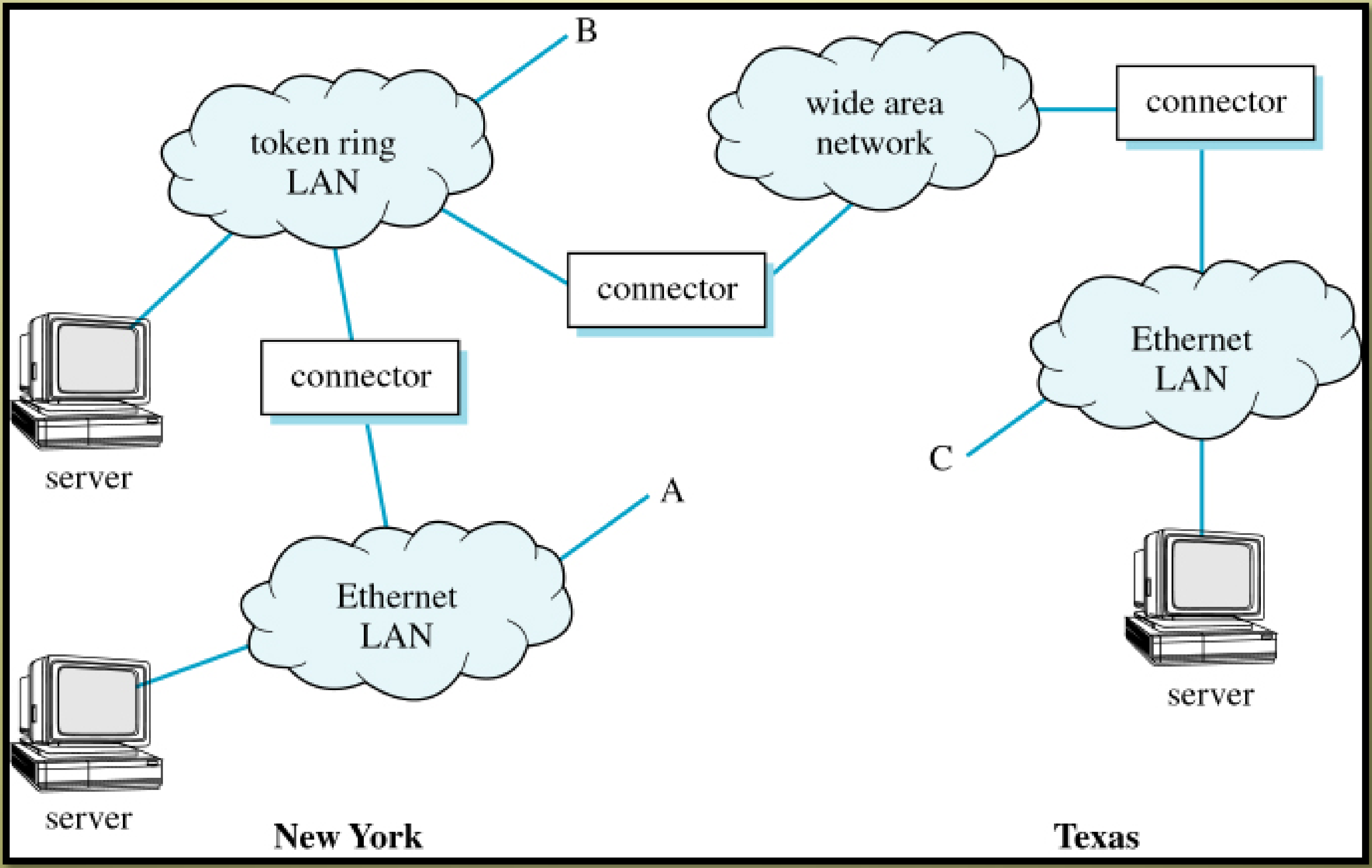
These slides have mainly been extracted, modified and updated from original slides of :
Computer Networking: A Top Down Approach, 6th edition Jim Kurose, Keith Ross
Addison-Wesley, 2013

Additional materials have been extracted, modified and updated from:
Understanding Communications and Networking, 3e by William A. Shay 2005

Connecting Networks

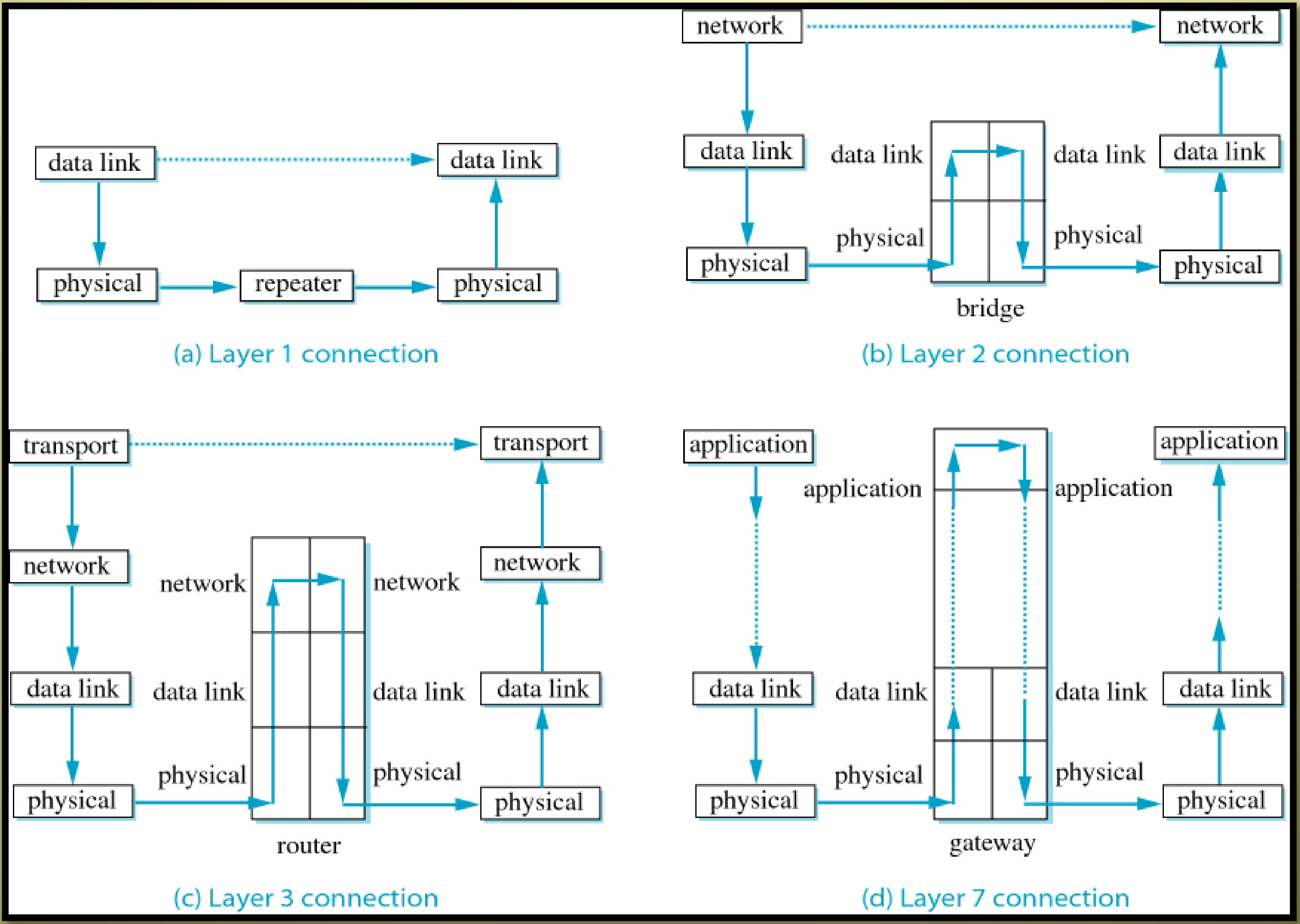
- the larger the number of devices in a single LAN, the higher the chances that the LAN performance degrades
- one possible solution is to separate devices into multiple LANs
- yet, these LANs need to be connected for the devices to communicate

Connecting Networks



Interconnecting Networks

Connecting Networks



OSI Connections

Connecting Networks

- **protocol converters** are used to connect different networks
- the most common protocol converters exist at layers 1, 2 & 3
- at layer 1: **hubs**, **repeaters**
- at layer 2: **bridges**, **switches**, …
- at layer 3: **routers**

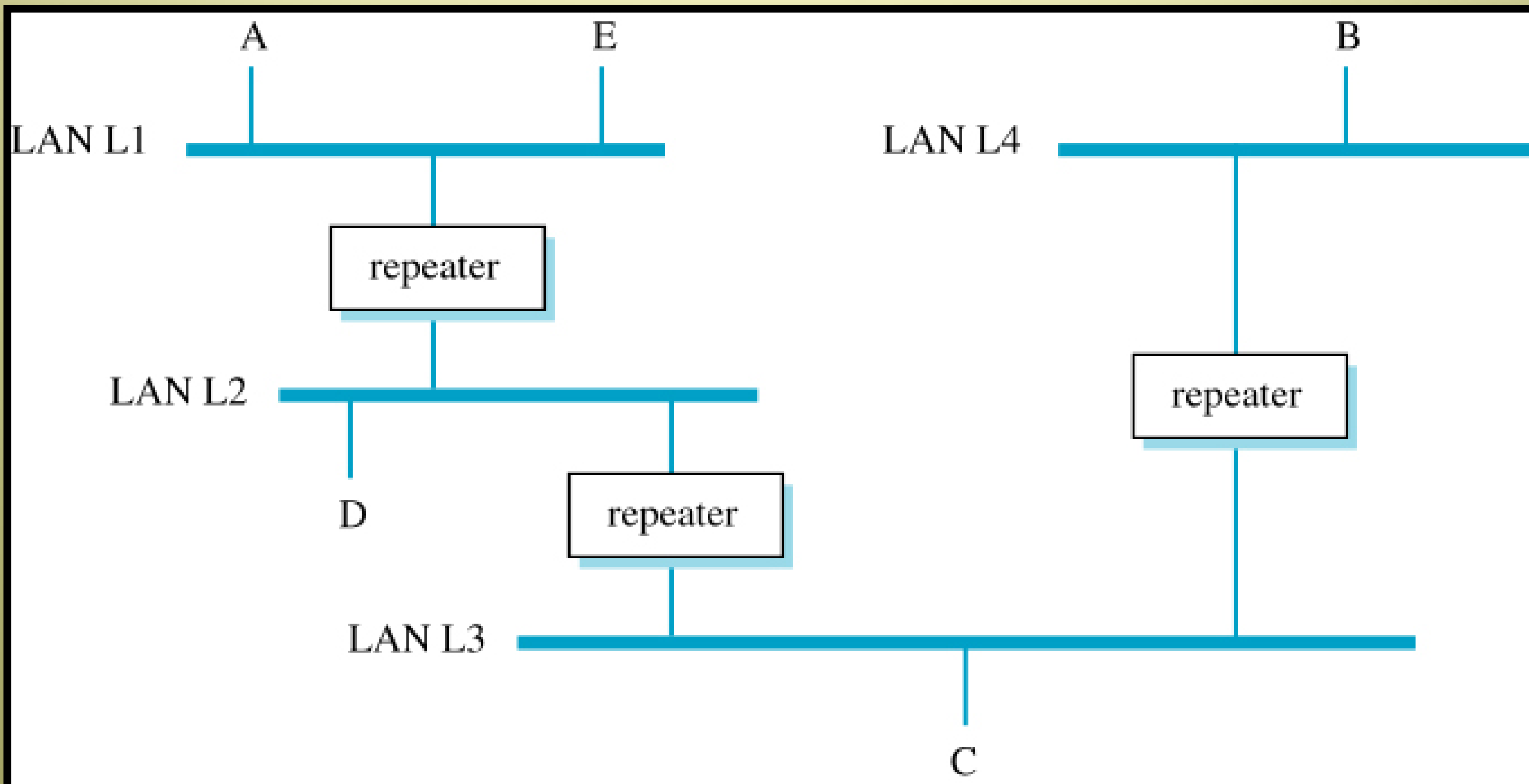
Layer 1 Connections

Repeaters

- operate at the physical layer (layer 1)
- connect LANs that are using the same protocol and frame format
- main function is to just regenerate signals then send them again, hence extend the distance covered by a LAN protocol

Layer 1 Connections

Repeaters



LANs Connected with a Repeater

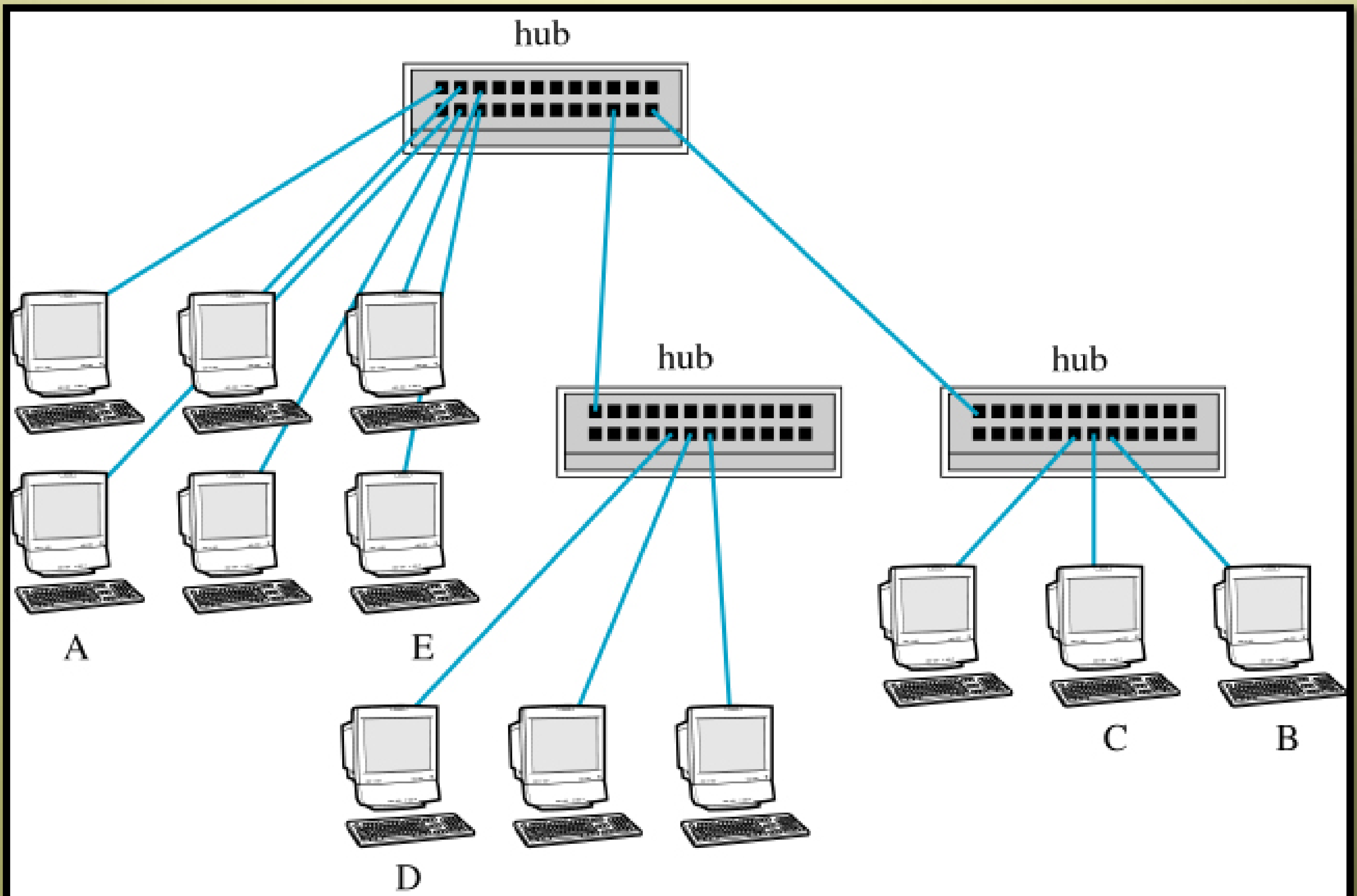
Layer 1 Connections

Hubs

- sometimes called multi-port repeaters
- the main difference between a hub and repeater is that a hub has multiple ports, hence many devices can directly be connected to it
- all devices connected to a hub are still in the same collision domain
- the more the devices connected to hubs, the more the chances that the network performance will degrade

Layer 1 Connections

Hubs



Making Connections Using Hubs

Layer 2 Connections

Bridges

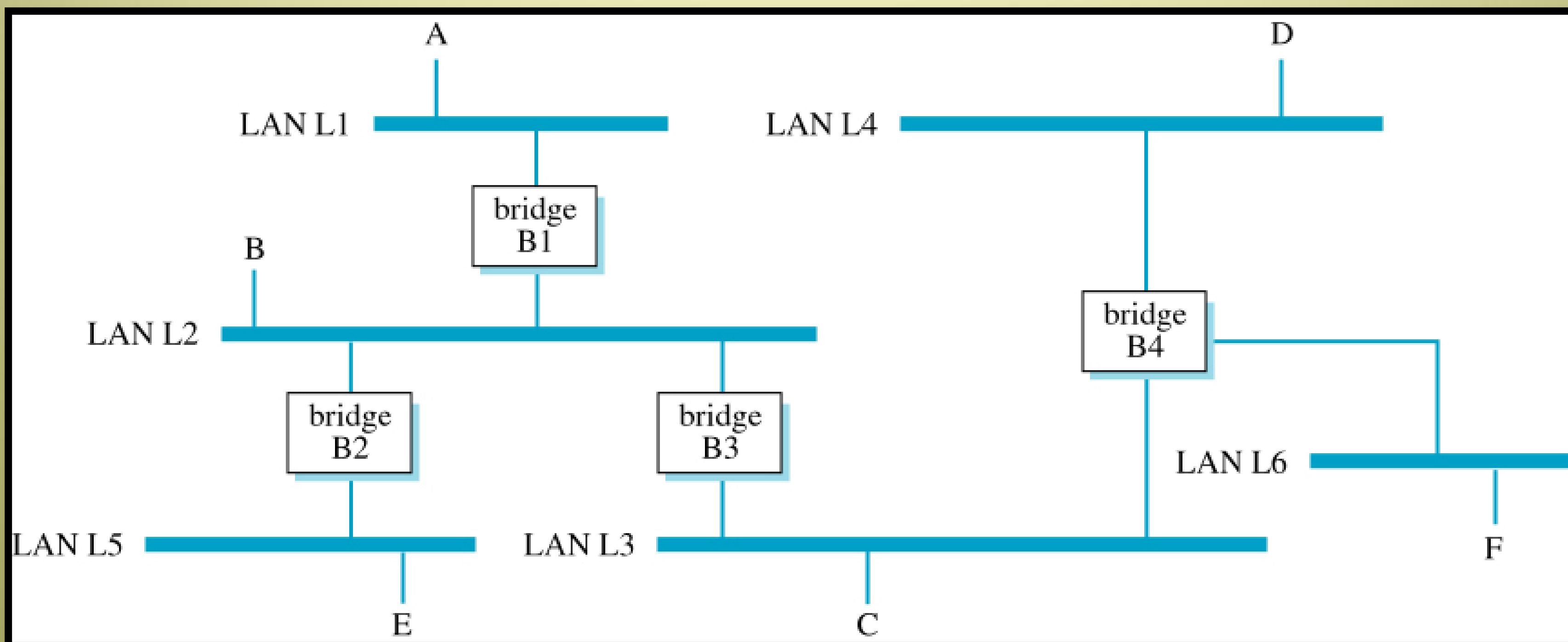
- a bridge connects two LANs

- operate at layer 2; so they are capable of:
  - Making decision about when to forward any frame they received
  - Performing data link function such as error detection, frame formatting, frame routing, …etc.

- a bridge examines an incoming frame and route it to its LAN only if it is destined to a device in that LAN

Layer 2 Connections

Bridges



LANs Connected through Bridges

** notice that there is an error in the above image. What is it?

Layer 2 Connections

Bridging different types of LANs

- a bridge may connects two LANs of different types
- this is more difficult however since many issues must be considered:
  - what if the two LANs operate on different speed
  - how about bridges delay; will they cost any further problems
  - what if the frame formats of the two network are different

Layer 2 Connections

Bridges - Routing

- how would a bridge know that a specific device is in its LAN
- worst, what if the device is not in the bridge's LAN but the frame must be passed by the bridge to another in order to deliver the frame
- what if a device is initially served (either directly or indirectly) by a bridge but then the device is moved
- the process of deciding which frames to accept/forward and where to forward them is called **bridge routing**

Layer 2 Connections

Bridges – Routing Tables

- routing decision are made based on a **routing table**
- each bridge has a routing table for each LAN it connects to

Routing Tables for Bridges in Previously Shown LANs

Source LAN L1		Source LAN L2	
Destination	Next LAN	Destination	Next LAN
A	—	A	L1
B	L2	B	—
C	L2	C	—
D	L2	D	—
E	L2	E	—
F	L2	F	—

(a) Bridge B1

Source LAN L2		Source LAN L5	
Destination	Next LAN	Destination	Next LAN
A	—	A	L2
B	—	B	L2
C	—	C	L2
D	—	D	L2
E	L5	E	—
F	—	F	L2

(b) Bridge B2

Source LAN L2		Source LAN L3	
Destination	Next LAN	Destination	Next LAN
A	—	A	L2
B	—	B	L2
C	L3	C	—
D	L3	D	—
E	—	E	L2
F	L3	F	—

(c) Bridge B3

Source LAN L3		Source LAN L4		Source LAN L6	
Destination	Next LAN	Destination	Next LAN	Destination	Next LAN
A	—	A	L3	A	L3
B	—	B	L3	B	L3
C	—	C	L3	C	L3
D	L4	D	—	D	L4
E	—	E	L3	E	L3
F	L6	F	L6	F	—

(d) Bridge B4

Layer 2 Connections

Bridges – Routing Tables

- how does a bridge defines it routing table?

- **fixed routing**: program the bridge with each device address and the LAN to which a frame should be forwarded to

- fixed routing however is not that feasible in reality since changes are always possible (remove device, add device, ..etc.)

- to accommodate more dynamic environment, either:
  - keep in changing the routing table whenever a change is done, or
  - determine some way for the bridges to update their routing tables automatically

  → the first alternative is not that viable in a more dynamic environment

  → bridges that are capable of creating and updating their routing tables automatically are referred to as ***transparent bridges***

Layer 2 Connections

Bridges - Transparent Bridges

- bridge that are capable of creating and updating their routing tables
- once plugged, they can immediately work regardless of the topology or device locations
- determine location of devices automatically then create/update the routing tables
- if devices move, the tables are also automatically updated (by the bridges)
- the capability to update routing tables automatically is referred to as ***route learning*** or ***address learning***

Layer 2 Connections

Bridges – Route Learning

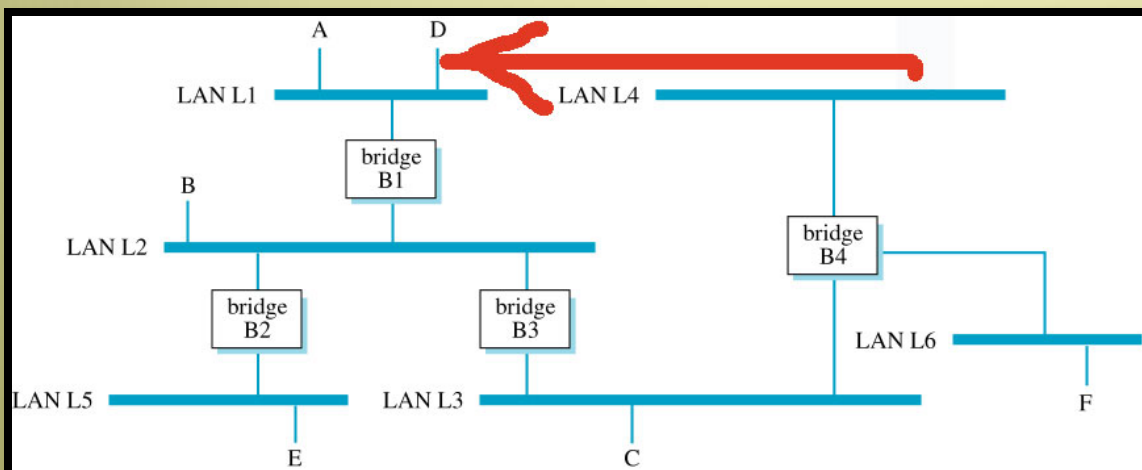
- bridge creates routing table by observing traffic
- when a frame is received, the bridge can know two things:
  - address of device
  - the LAN from which the frame came from
- the bridge then examines its routing table to confirm that this information matches the table entries for that device
- if not, the bridge updates the routing table to match the latest configuration

Layer 2 Connections

Bridges – Route Learning

Example:

→ device D moved from L4 to L1



Modified version of Previously Shown LANs
D moved from *L4* to *L1*

Source LAN L1		Source LAN L2	
Desti-nation	Next LAN	Desti-nation	Next LAN
A	—	A	L1
B	L2	B	—
C	L2	C	—
D	L2	D	—
E	L2	E	—
F	L2	F	—

(a) Bridge B1

OLD Routing Table of *B1* before moving *D* from *L4* to *L1*

Layer 2 Connections

Bridges – Route Learning

Example (continues…):

→ After moving, device D sent a frame to E

Source LAN L1		Source LAN L2	
Destination	Next LAN	Destination	Next LAN
A	--	A	L1
B	L2	B	--
C	L2	C	--
D	--	D	L1
E	L2	E	--
F	L2	F	--

Updated Routing Table for *B1*

Layer 2 Connections

Bridges – Route Learning

Questions:

- →*What if D never sent a frame?*
- →*What about the table of B4; is it updated!*

Another question: *What happens at startup when all tables are empty?*

Layer 2 Connections

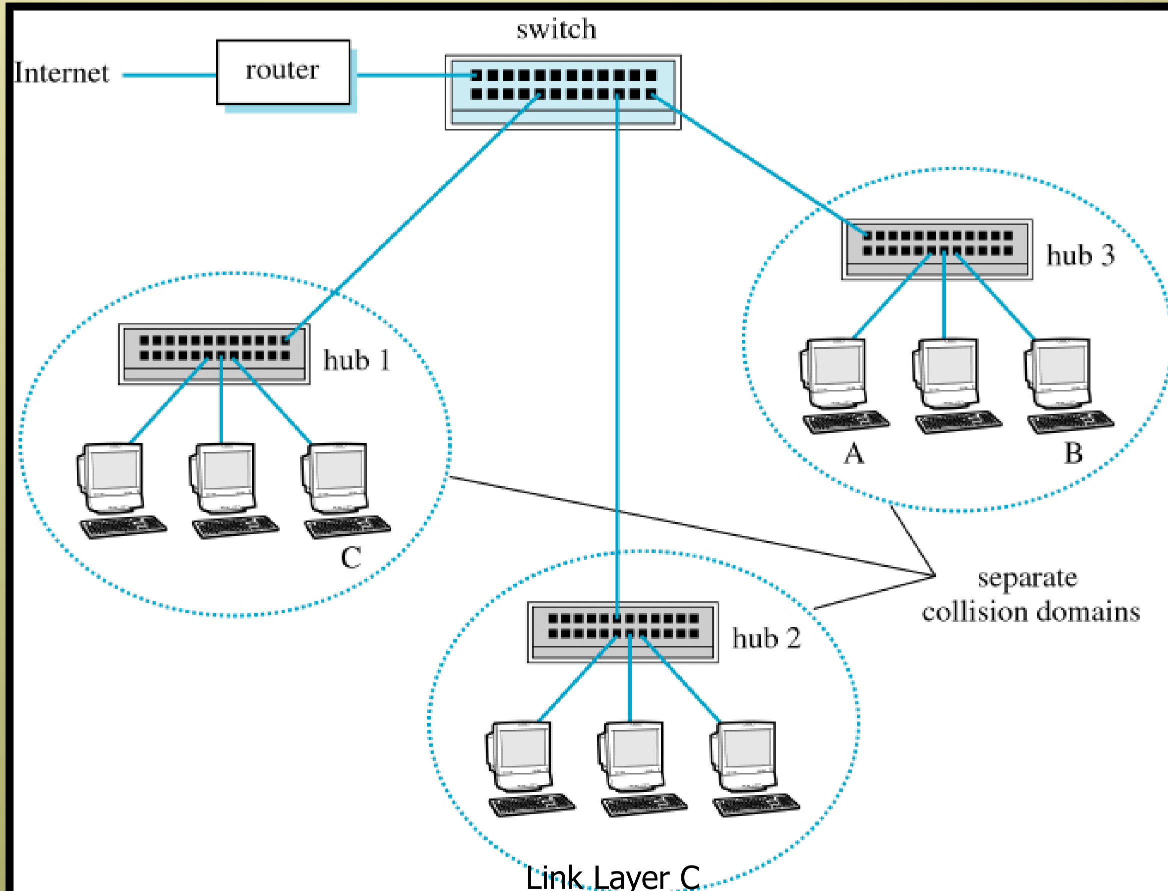
Bridges – Route Learning

- each bridge maintains a timer; once this timer expires, it purges its routing table
- this action makes the devices inaccessible
- however, once a bridge receives a frame for a device that has no entry in the routing table, it uses a **flooding algorithm**
- **spanning tree** is constructed for **controlled flooding**, in a similar fashion to what we discussed before

Switches & Switched Ethernet

- switches are similar to bridges, with one primary difference
- while a bridge can connect two LANs, a switch can connect multiple LANs through ports

Connections Using Hubs & Switches



Switches & Switched Ethernet

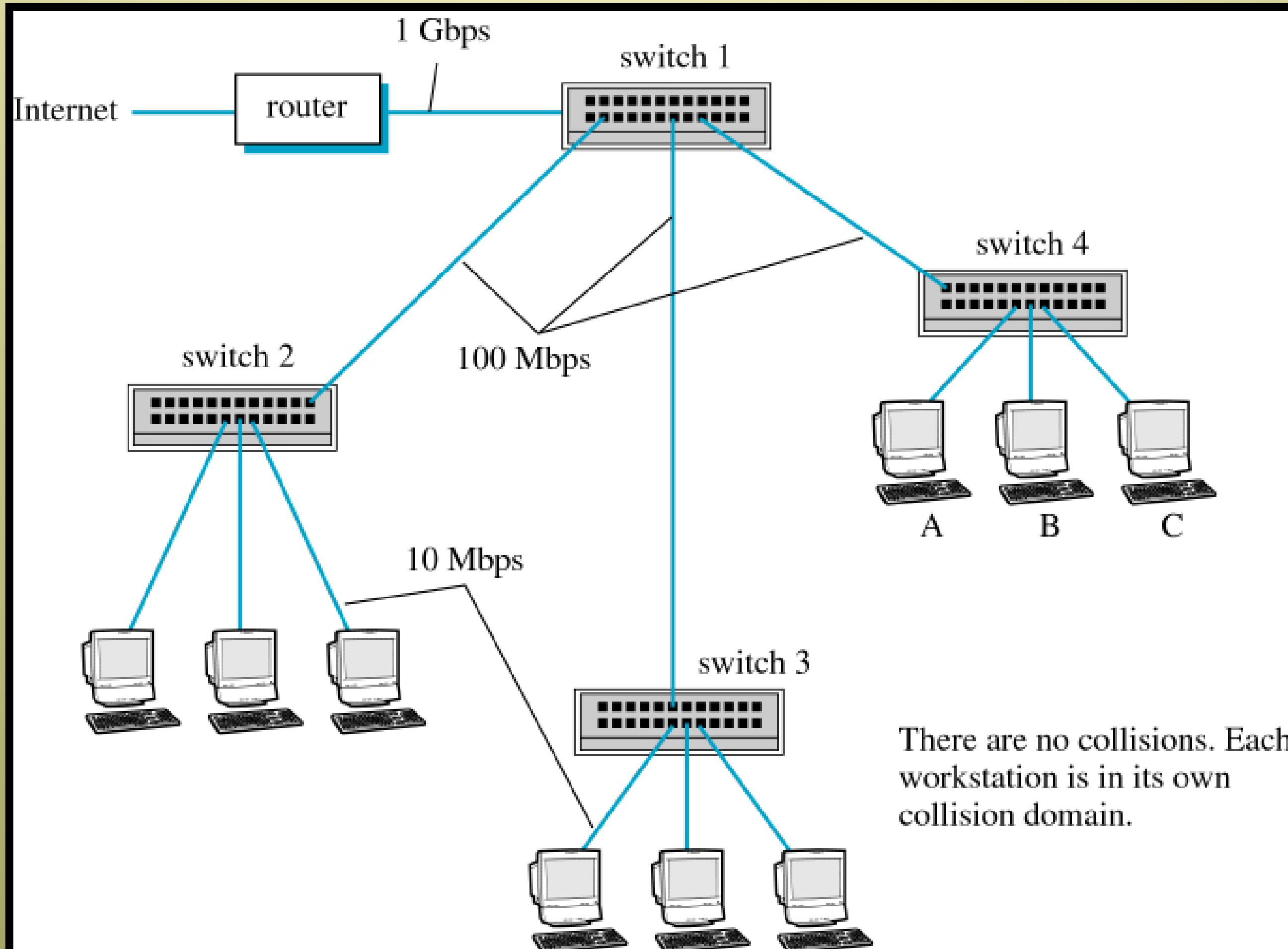
- although there may be many collision domains, a single **broadcast domain** can be defined
- the destination MAC address in an Ethernet frame can specify either a device address or a broadcast address
- a broadcast frame is forwarded over all ports and accepted by all devices
- effectively, collision is now possible in a topology that uses hubs and switches (as in previous figure)

Switches & Switched Ethernet

- a fully **Switched Ethernet** topology solves this collision problem
- with Switched Ethernet, all hubs are replaced by switches
- because switch ports lead to different collision domains, and each device is connected to a separate port, there is no more collision anywhere
- furthermore, if connection between the device and the switch operate in full-duplex mode, there is no more need for CSMA/CD
- each device is still capable of communicating with any other device, broadcast domain is also still there; there is just no more collision problems

Switches & Switched Ethernet

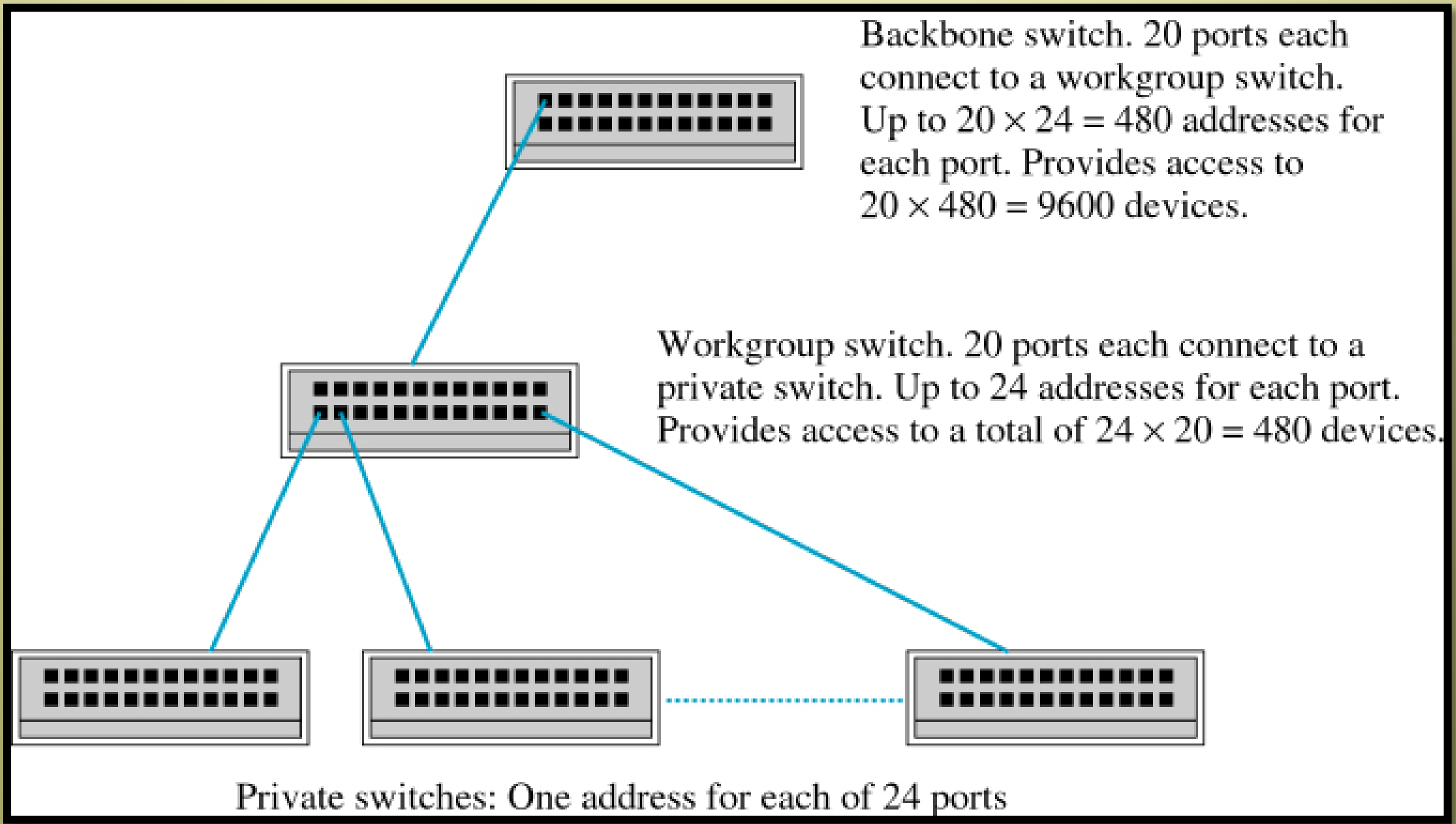
- another advantage of Switched Ethernet is that the bit rate for ports can vary



Connections Using Only Switches

Switches & Switched Ethernet

- Multiple layers of switches are also possible



Private, Workgroup & Backbone Switches

Data center networks

- 10's to 100's of thousands of hosts, often closely coupled, in close proximity:

Microsoft's data center in San Antonio, Texas

Data center networks

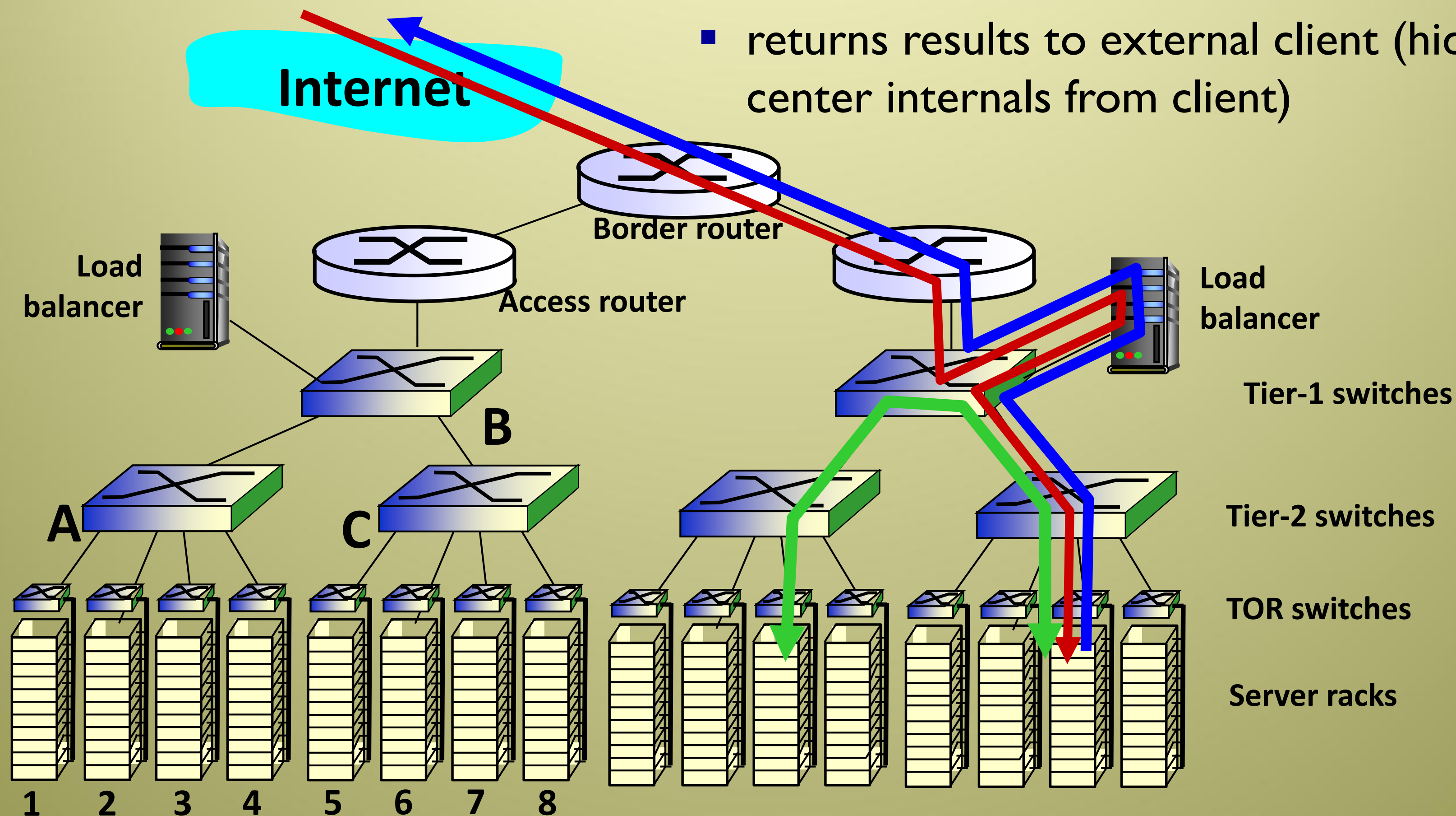
- Concurrently supporting many cloud applications:
  - e-business
  - content-servers
  - search engines, data mining
  - E-mail servers
  - …
- challenges:
  - multiple applications, each serving massive numbers of clients
  - managing/balancing load, avoiding processing, networking, data bottlenecks

Inside a 40-ft Microsoft container, Chicago data center

Data center networks

load balancer: application-layer routing

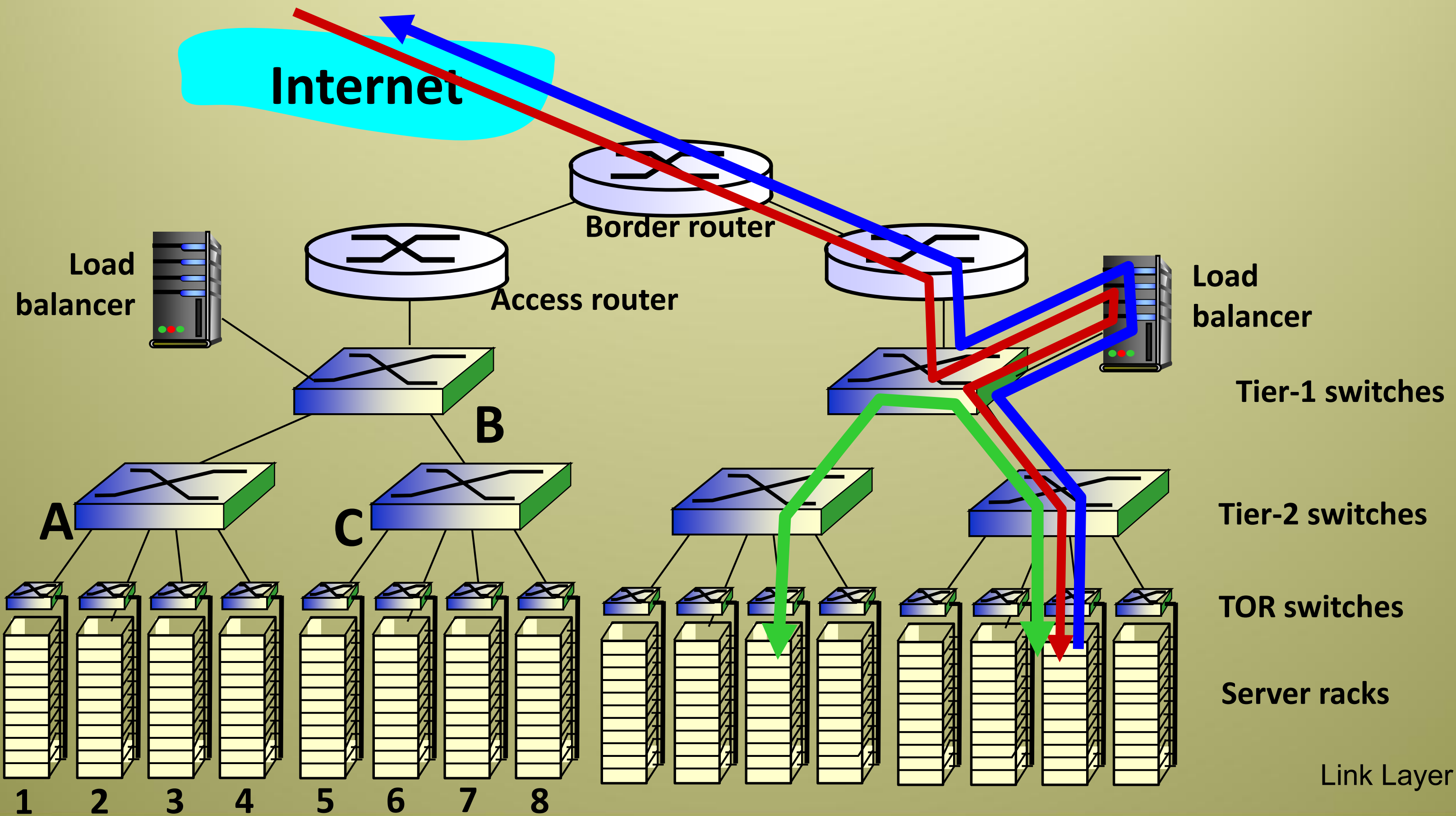
- receives external client requests
- directs workload within data center
- returns results to external client (hiding data center internals from client)



Data center networks

Problem: Limited host-to-host capacity!

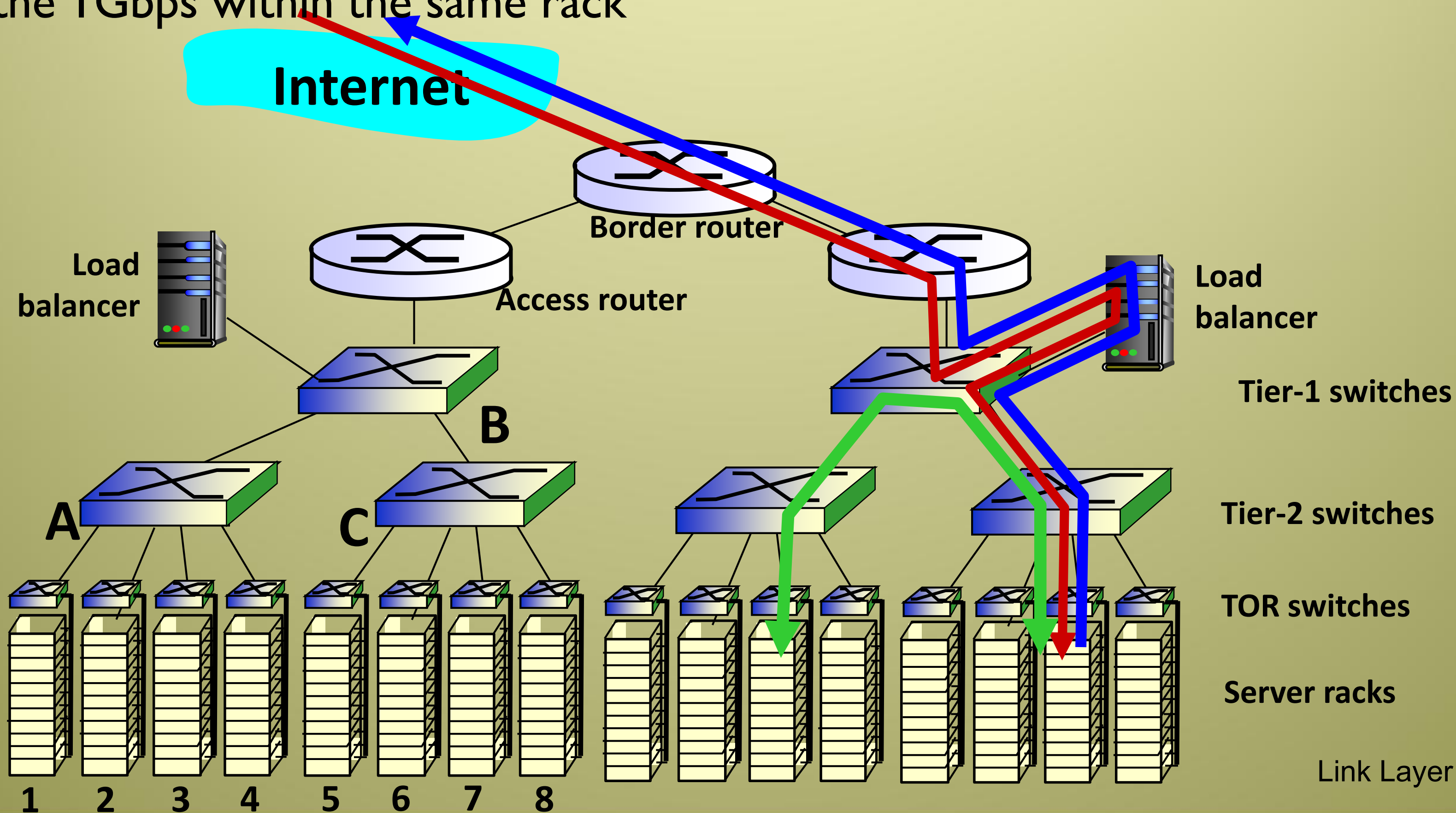
- suppose each host communicates with TOR with 1Gbps link, whereas links between switches are 10 Gbps
- Two hosts in same rack can communicate with 1Gbps, but what is the rate between hosts in different racks if many simultaneous flows are there?



Data center networks

Problem: Limited host-to-host capacity!

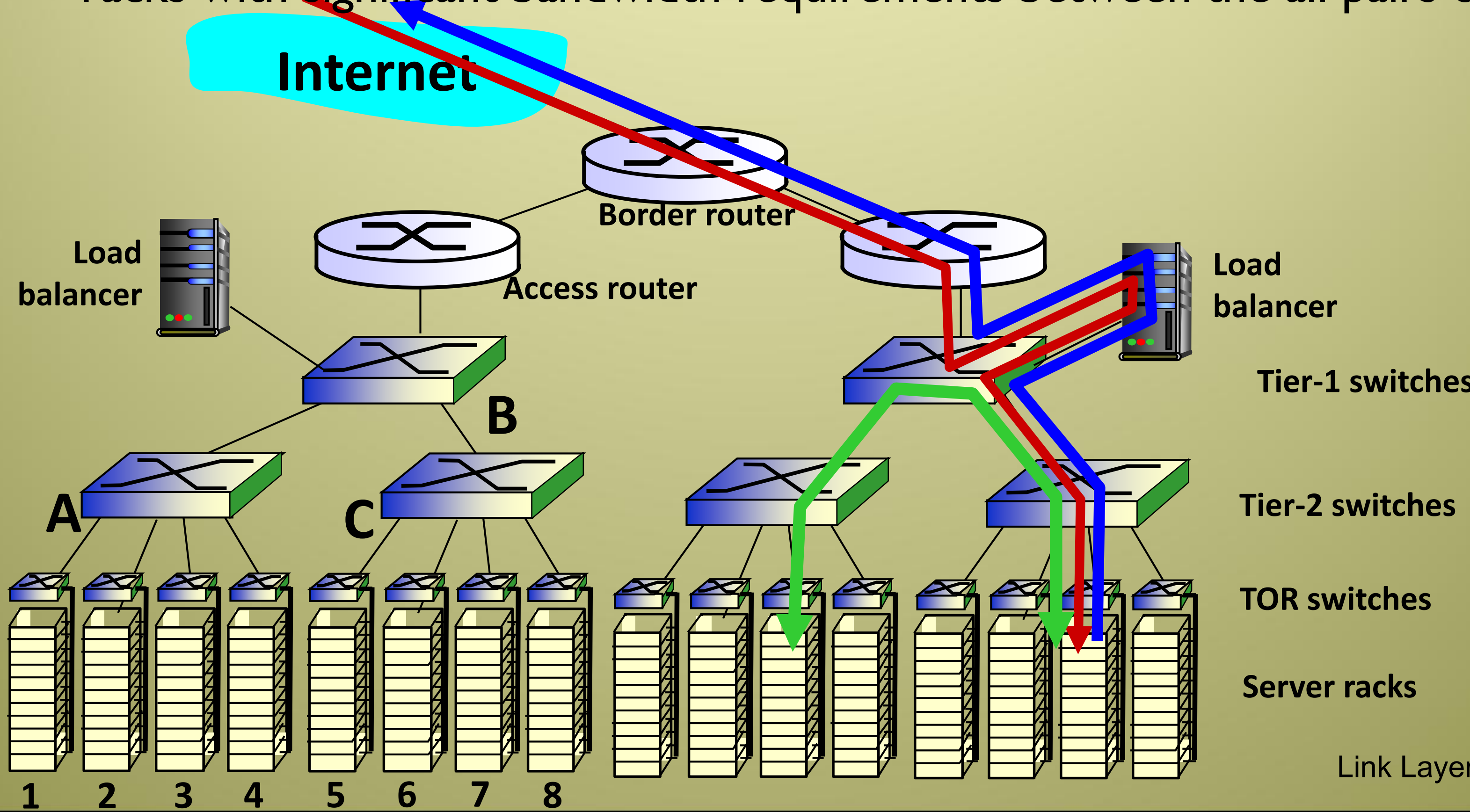
- assume each 10 hosts in rack 1 send to the 10 hosts of rack 5
- similarly assume hosts in rack 2, 3 and 4 send to 6, 7 and 8 respectively, so there is 40 simultaneous flows through links A-B and B-C
- each of these 4 flows will receive 10G/40 = 250 Mbps, which is much less than the 1Gbps within the same rack



Data center networks

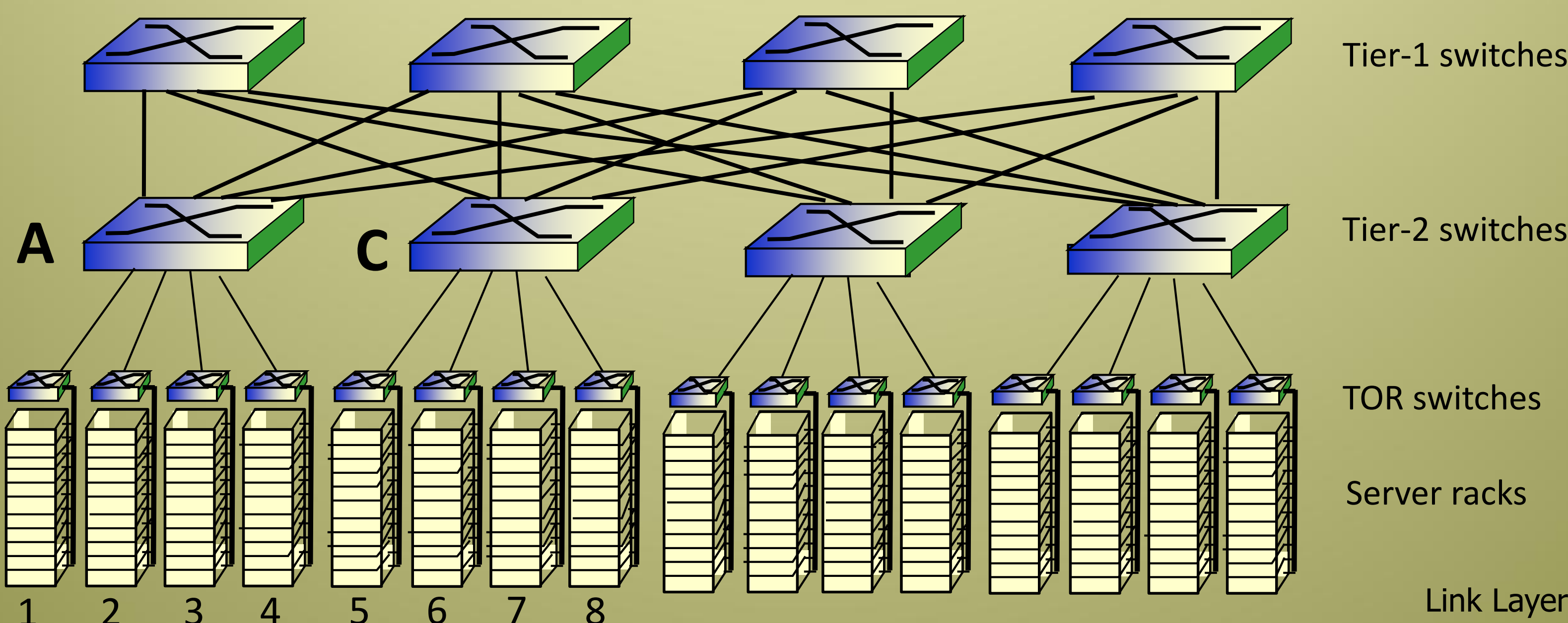
Problem: Limited host-to-host capacity!

- the problem become more acute for flows between hosts that need to travel higher up the hierarchy
- supporting high-bandwidth for host-to-host communication is important
  - i.e. a search engine may run on thousands of hosts spread across multiple racks with significant bandwidth requirements between the all pairs of hosts



Trends in data center networking

- **fully-connected topology**
  - Now, there are 4 distinct paths between A and C, providing an aggregate capacity of 40 Gbps
  - such design not only alleviates the host-to-host capacity limitations but also allows communication between hosts in any two racks, not connected to the same switch, to be logically equivalent, irrespective of their location in the data center



Trends in data center networking

- **shipping container-based modular data centers**
  - employ standard 12-meter shipping container as a mini data center
  - 1000s of hosts packed in racks closely to each other
  - at the data center, containers are interconnected to each other and the Internet
  - at the scale of few thousand hosts, it is possible to build a fully-connected network
  - however, interconnecting 100s to 1000s of containers while providing host-to-host bandwidth remains a challenge