DFSC 1316: digital forensic and information assurance fundamentals I

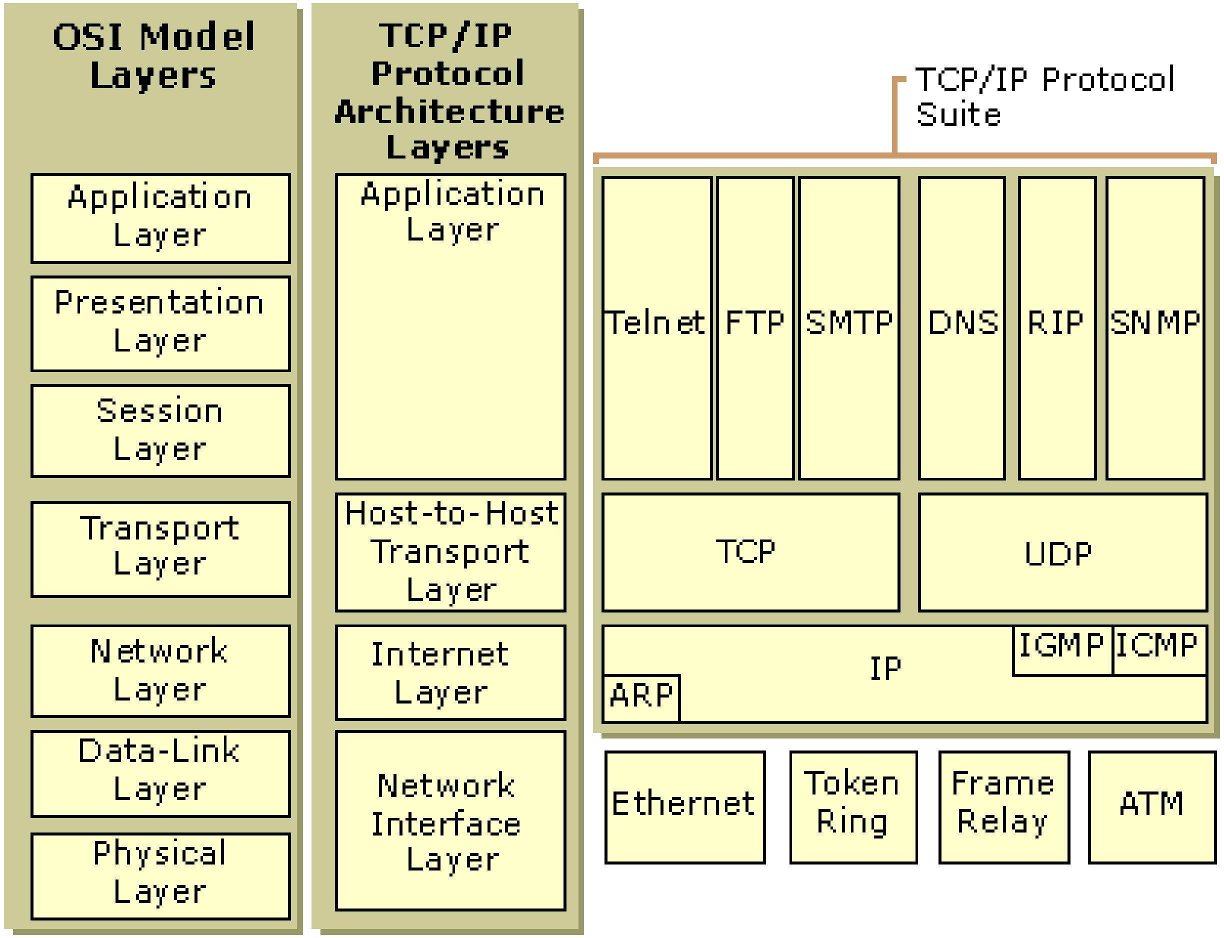
4. TCP/IP Suite

*Reference book: *TCP/IP Protocol Suite* by Behrouz A. Forouzan.

TCP/IP Protocol Suite

- The TCP/IP protocol suite was developed prior to the OSI model.
- The layers in the TCP/IP protocol suite do not match exactly with those in the OSI model.
- The TCP/IP protocol suite was defined as four software layers built upon the hardware.
  - Sometimes it is also considered to have 5 layers, with the Network-interface layer divided into physical and data-link layer.

Comparison between OSI and TCP/IP



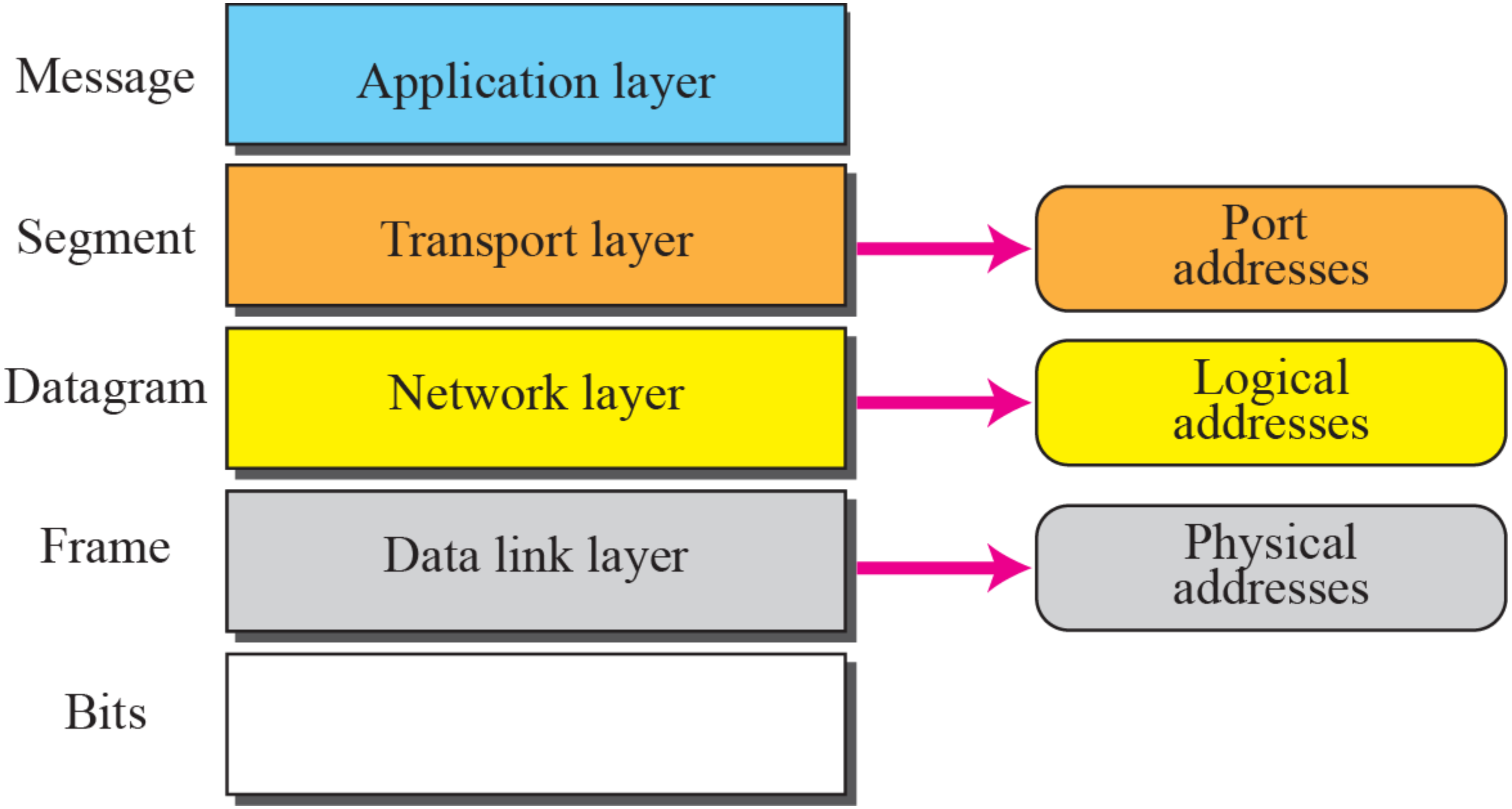
IP and TCP Protocol

- Internet Protocol (IP).
  - Network layer protocol.
  - Unreliable, connectionless, best-effort service.
  - Unit of communication is called *datagram*. Datagrams can travel different route and arrive at different order.
  - Provides basic transmission functions that can be added with more features when needed.
- Transmission Control Protocol (TCP).
  - Reliable, connection-oriented.
  - Unit of communication is segment.
  - Segments are numbered for reassembly.
  - Acknowledge is required for each segment received.

TCP/IP Addressing

- Three levels of addresses are used in an internet employing the TCP/IP protocols.
  - Physical address;
  - Logical address (Internet Address);
  - Port address;
- Each address is related to one layer in the TCP/IP architecture.

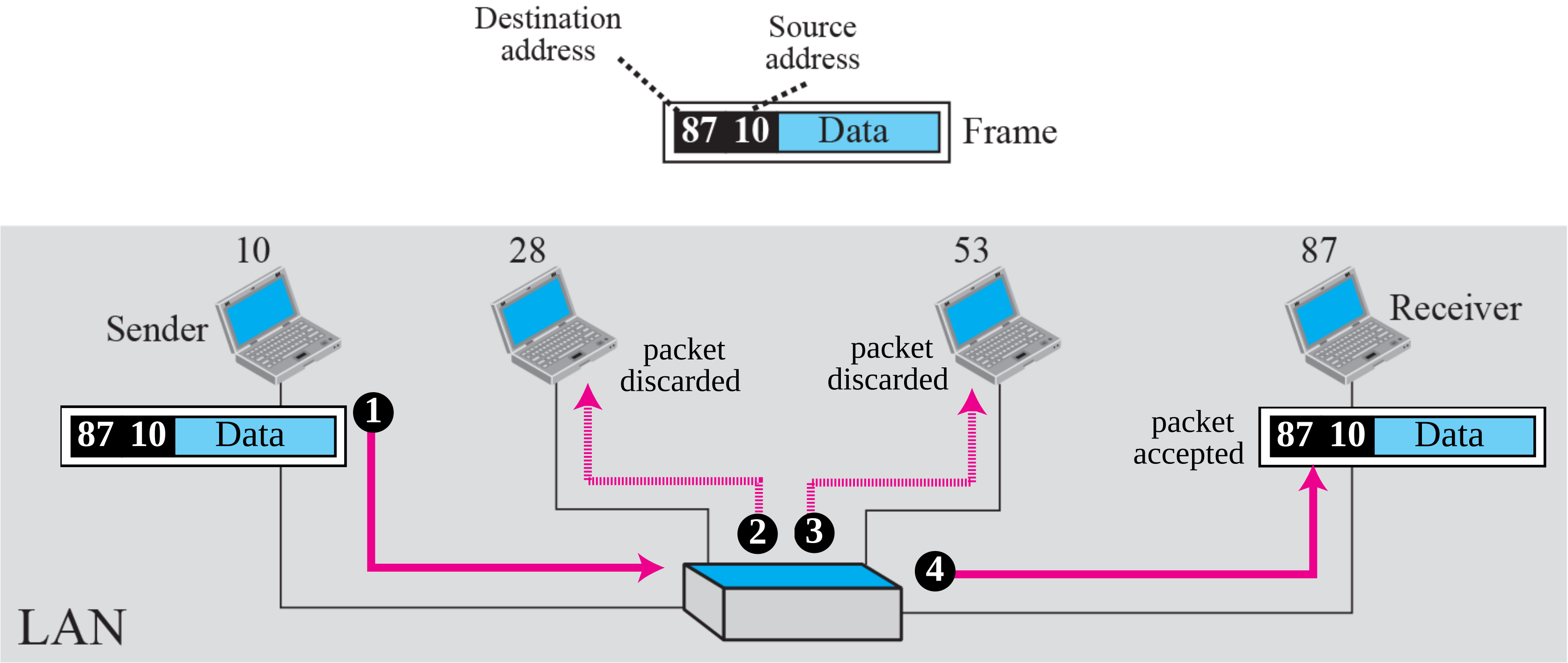
TCP/IP Addressing



Physical Address

- Also known as the link address, or the MAC address.
- It is included in the frame used by the data link layer.
- It is the lowest level address.
- In Ethernet, the physical address of a device is a 6-byte number.
  - Usually shown in Hexadecimal format.
  - A4-34-D9-3E-C0-F6
  - A4:34:D9:3E:C0:F6

Communication Example Using Physical Address

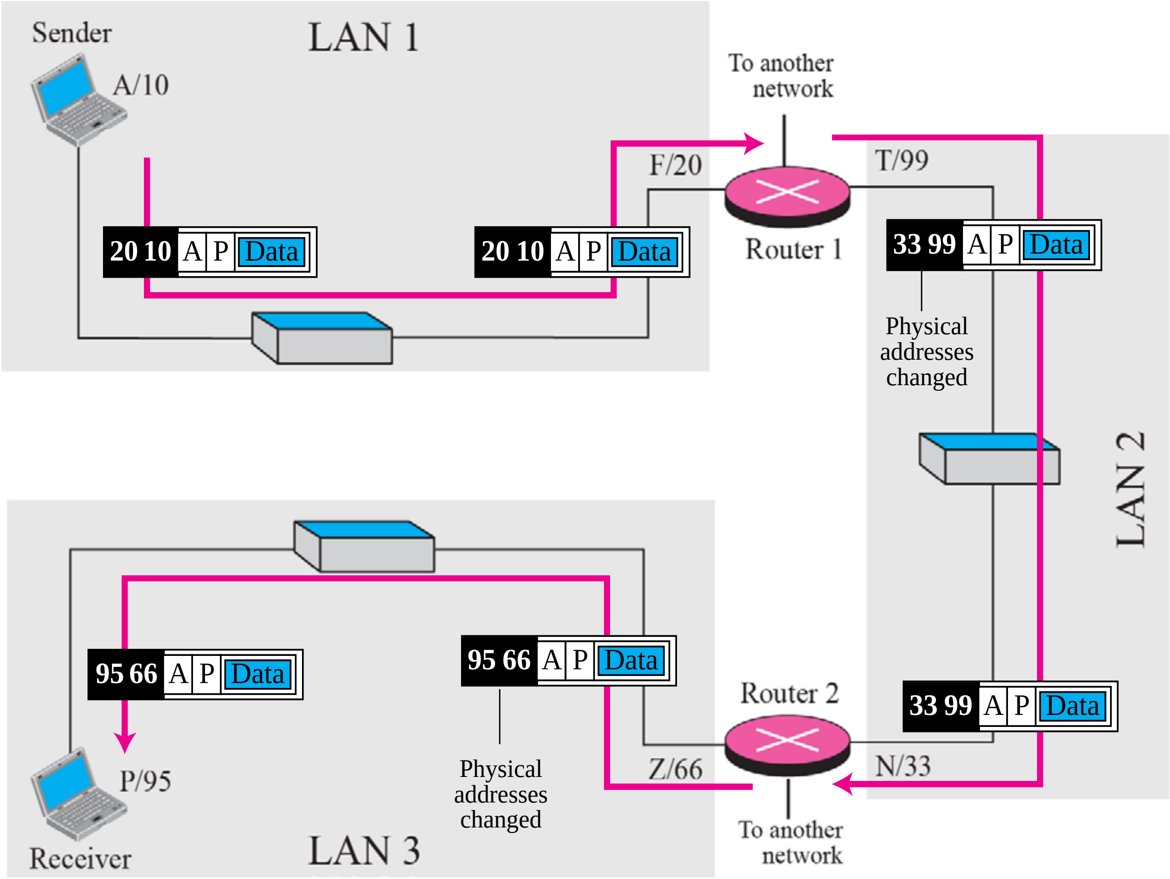


- 10 and 87 are connected by a link.
- Only physical address is needed for communication.

Logical Address (Internet Address)

- Necessary for universal communication that are independent of physical network.
  - Different network may have different physical address formats.
- Internet address
  - Also known as Internet Protocol (IP) address.
  - In IP version 4, the IP address is a 4-byte number.
    - Usually shown in Decimal format.
    - 192.168.10.1

Communication Example Using Internet Address



- A/10 and P/95 are not in the same network.
- A and P are network address, 10 and 75 are physical.
- Network address will not change during routing, while physical will.

Exercise: A real world analogy

- Each person has to identifiers
  - MAC – name
  - IP – home-address
- A person knows:
  - The name of his neighbor
  - The home-address of any other person
- A person does not know:
  - The name of non-neighbor
- A person can send letter to anyone, but can only pass the letter through his neighbor.
- How would a pizza be ordered, and delivered?

IPv4 and IPv6

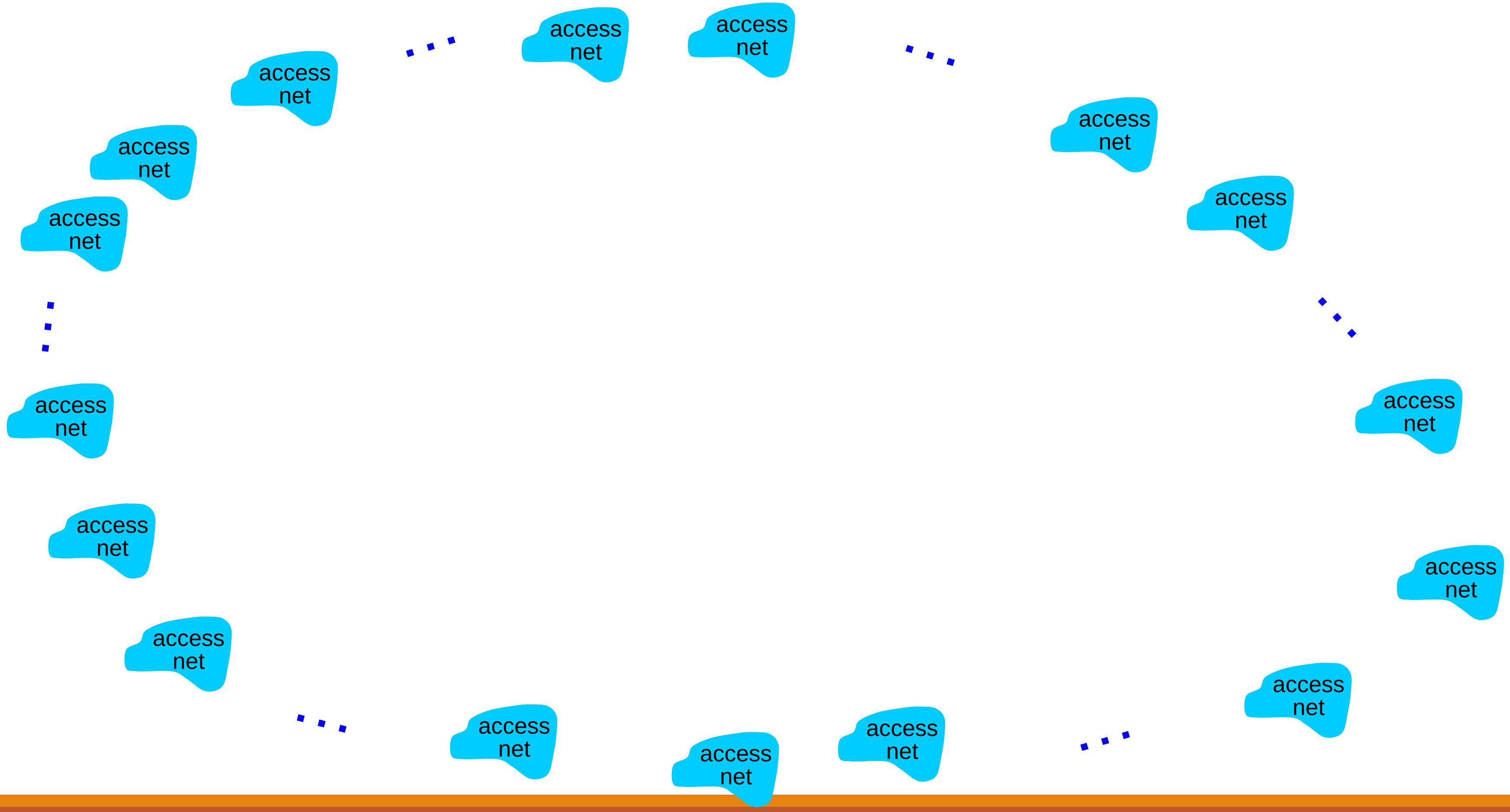
- IP version 4
  - Still widely used.
  - Facing the problem that all available address will be used up.
    - Only have 32 bits in total.
    - More and more devices requires Internet access.
- IP version 6
  - Only changes the network layer.
  - Use 128 bits addressing, compared to 32 bits in IPv4.
  - Other benefits such as security.

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

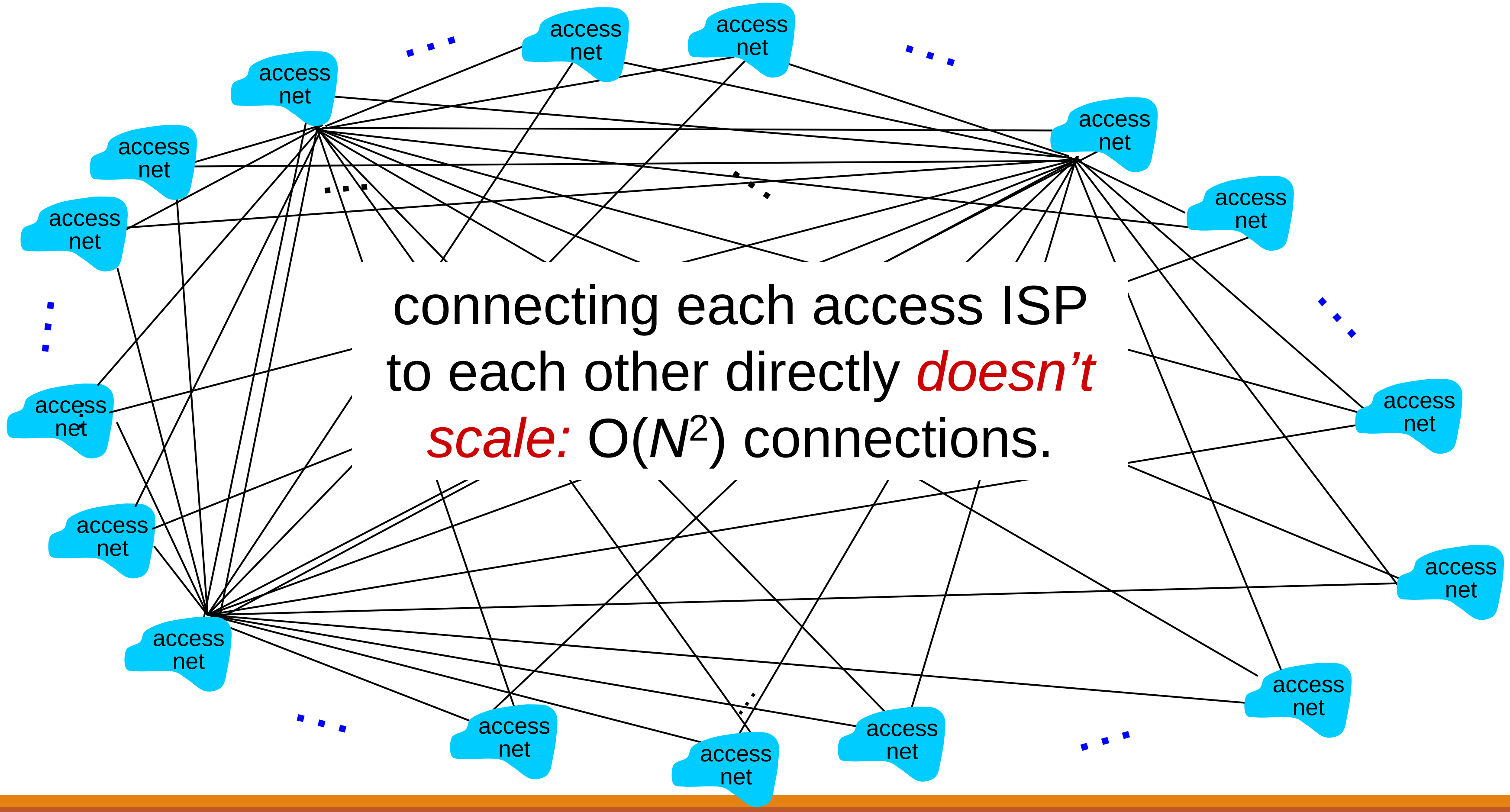
Internet structure: network of networks

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



Internet structure: network of networks

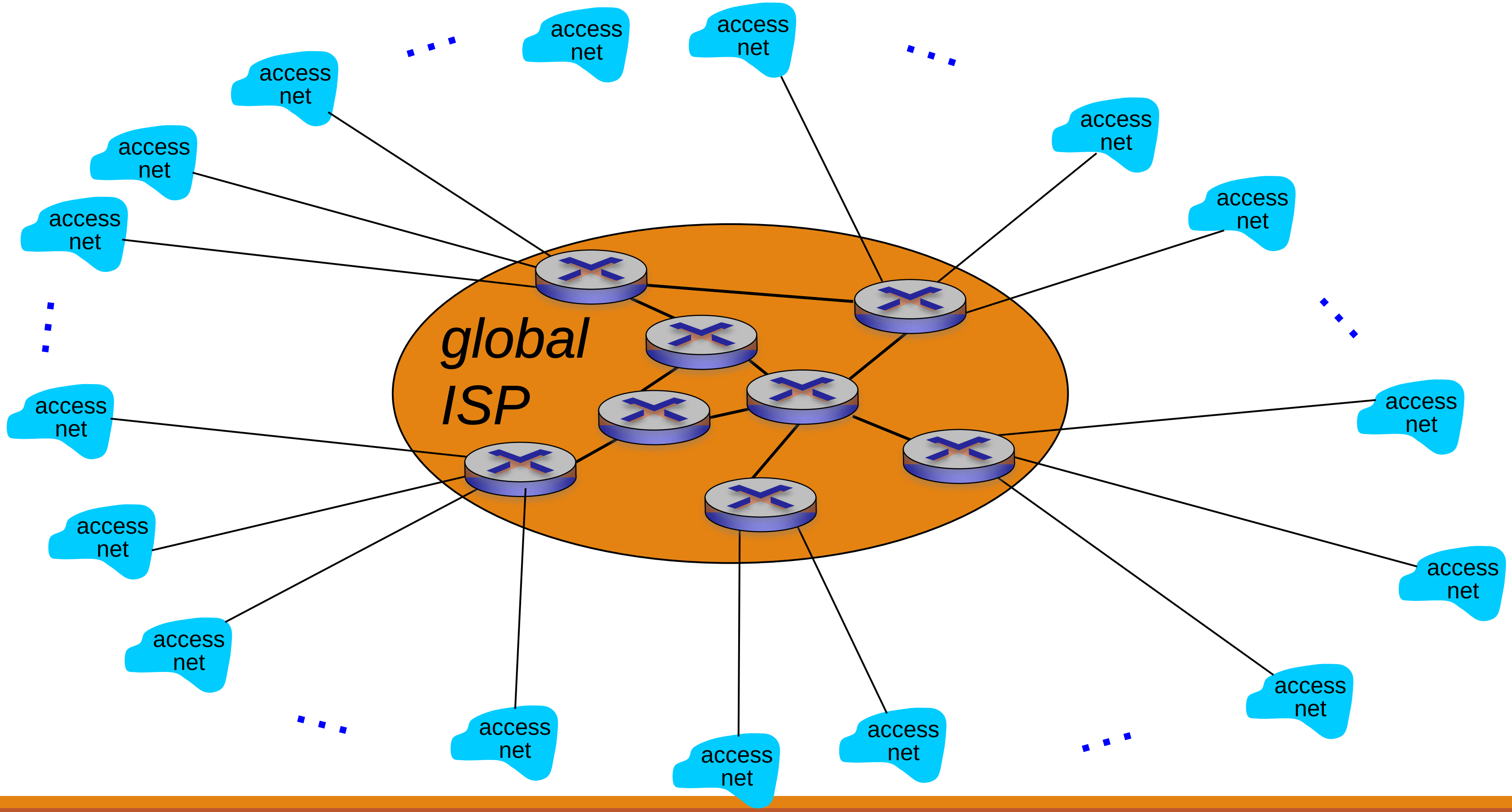
- Option: connect each access ISP to every other access ISP?



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

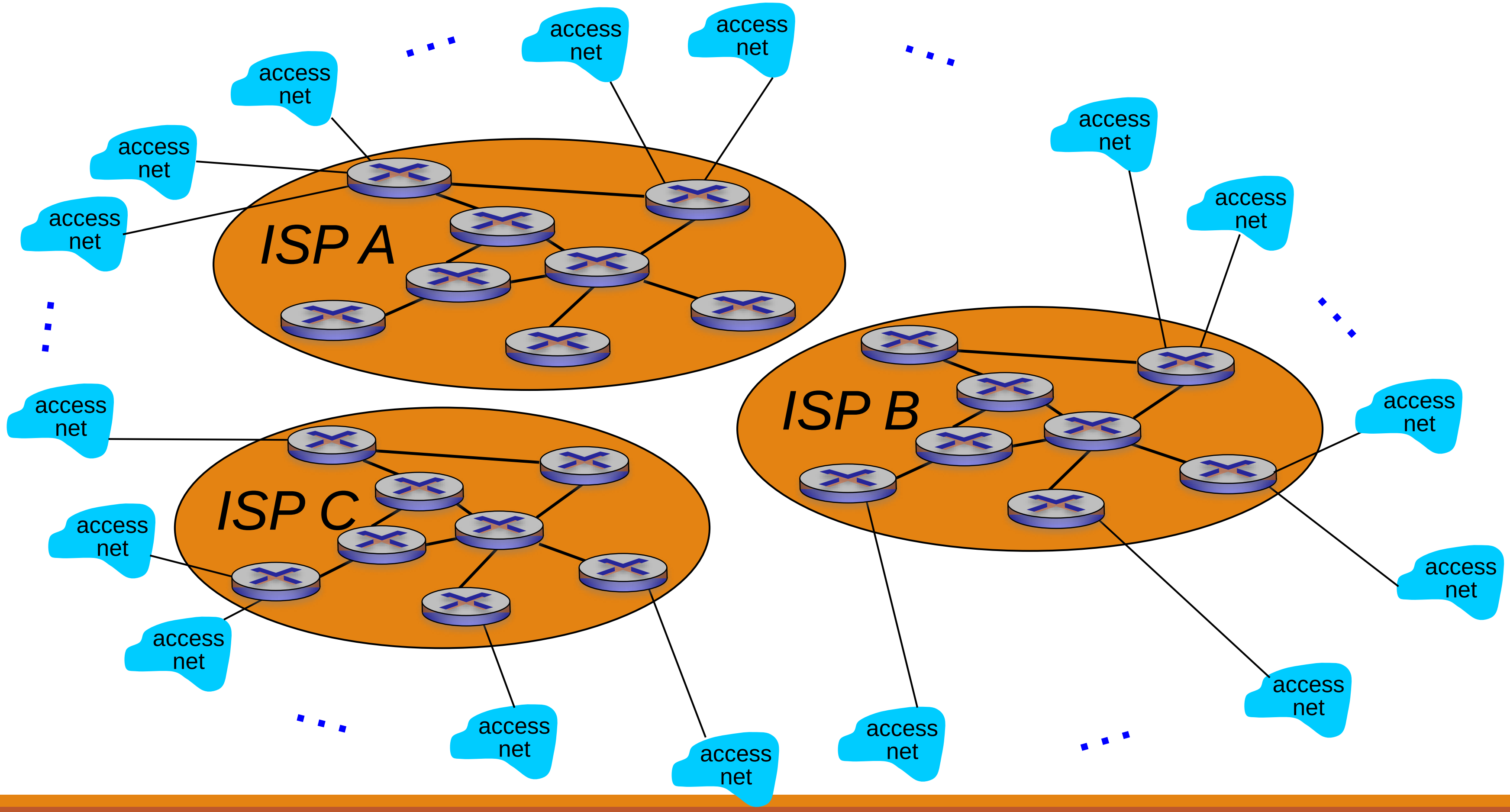
Internet structure: network of networks

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



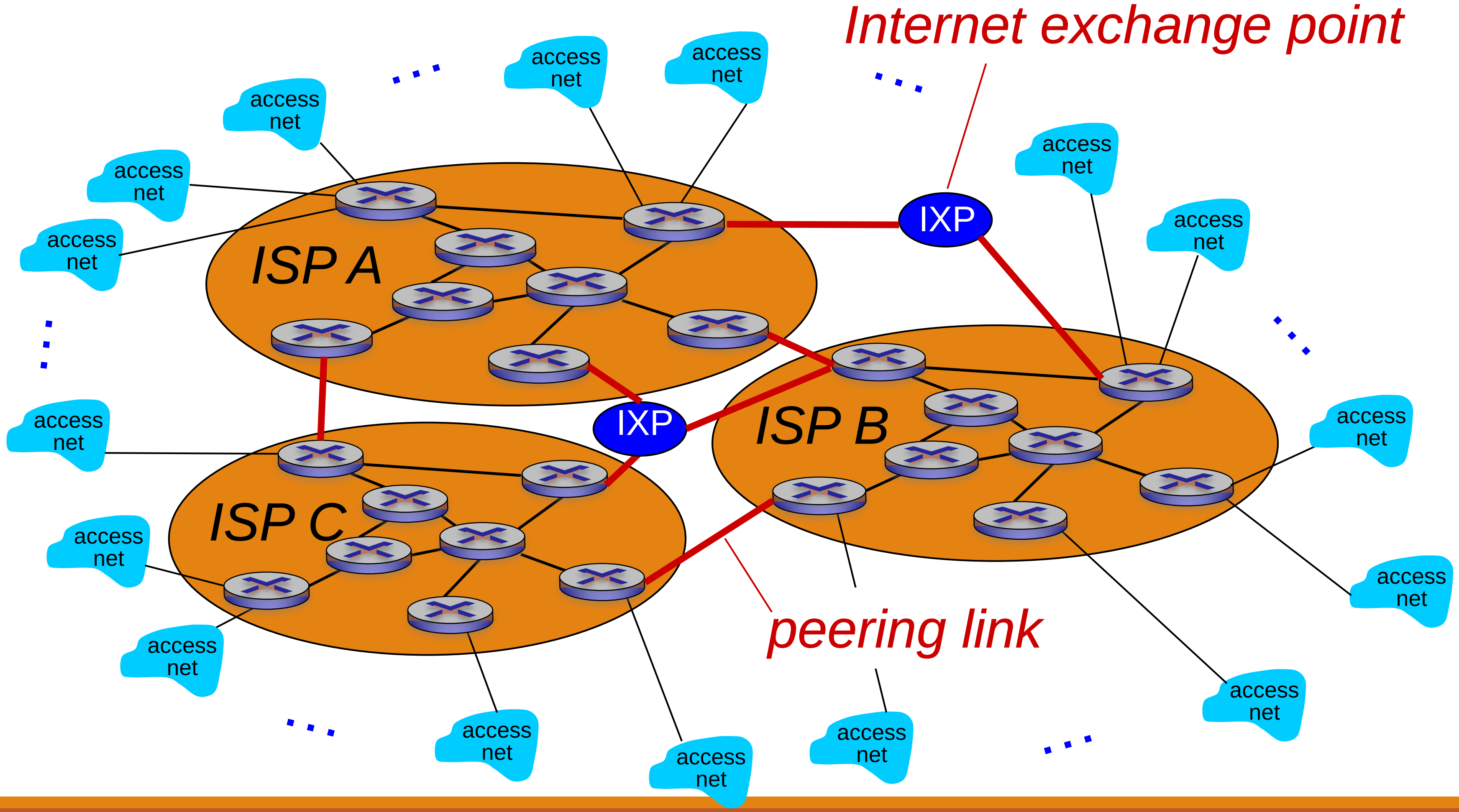
Internet structure: network of networks

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



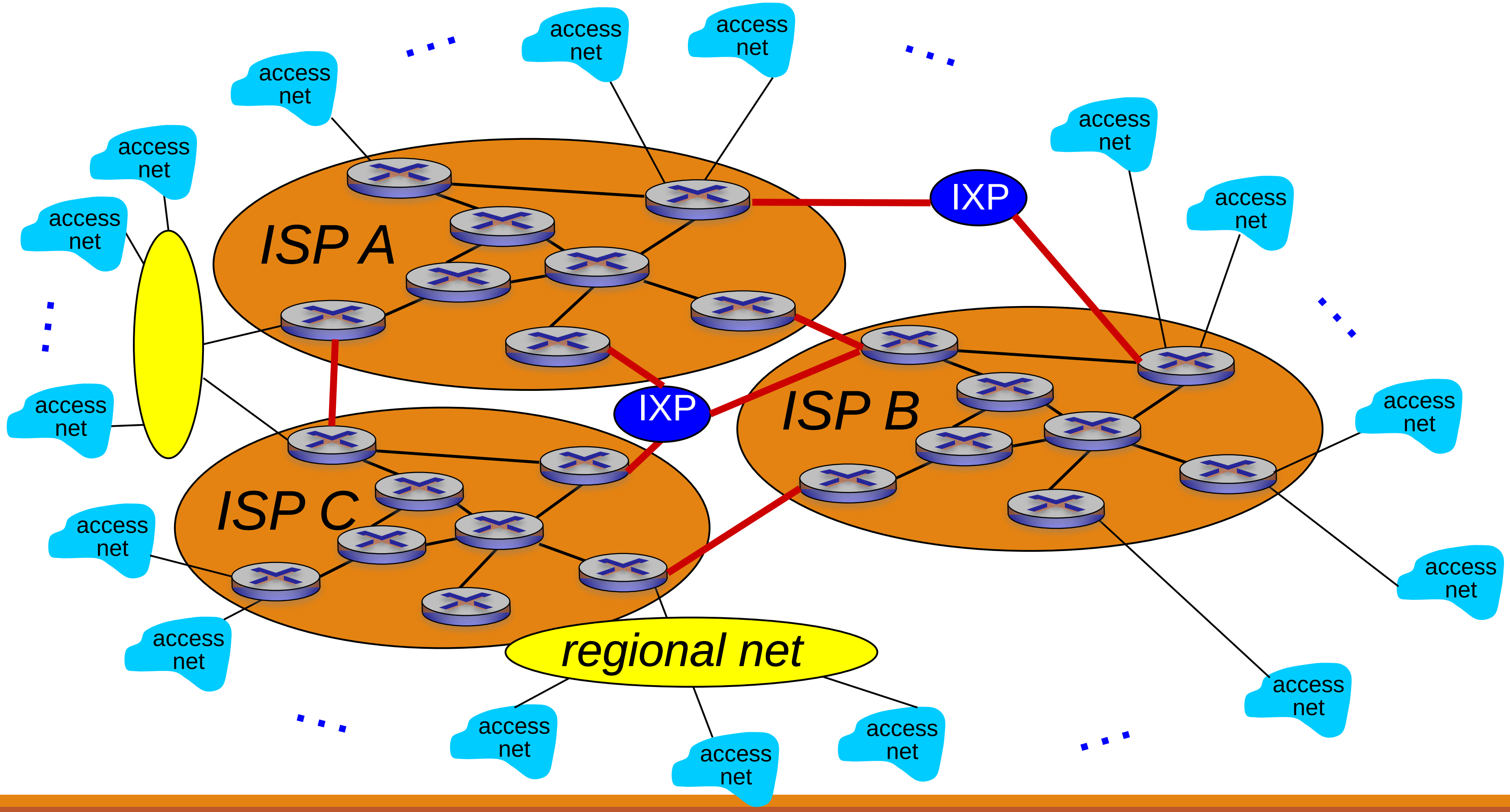
Internet structure: network of networks

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



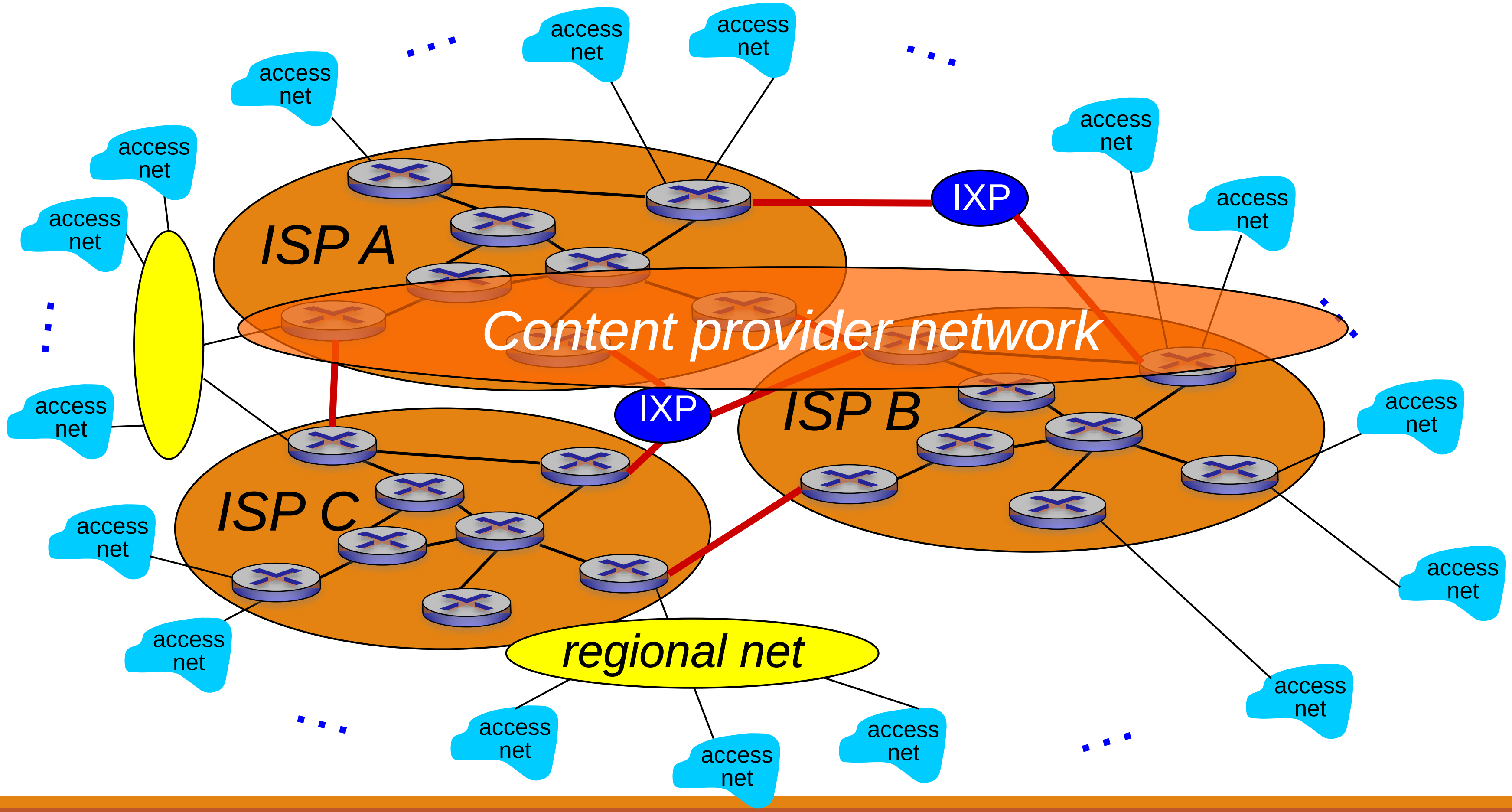
Internet structure: network of networks

- … and regional networks may arise to connect access nets to ISPs

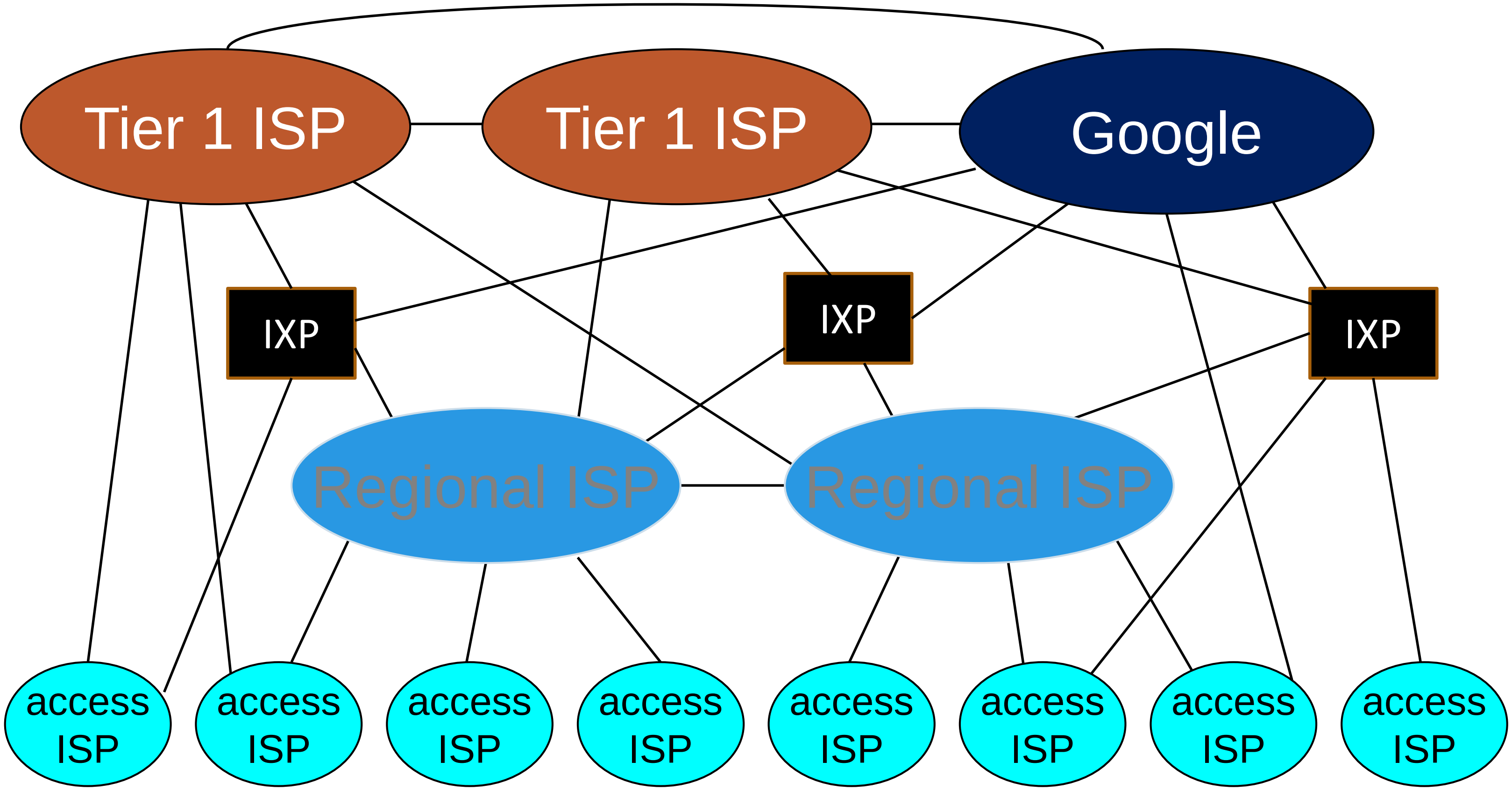


Internet structure: network of networks

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

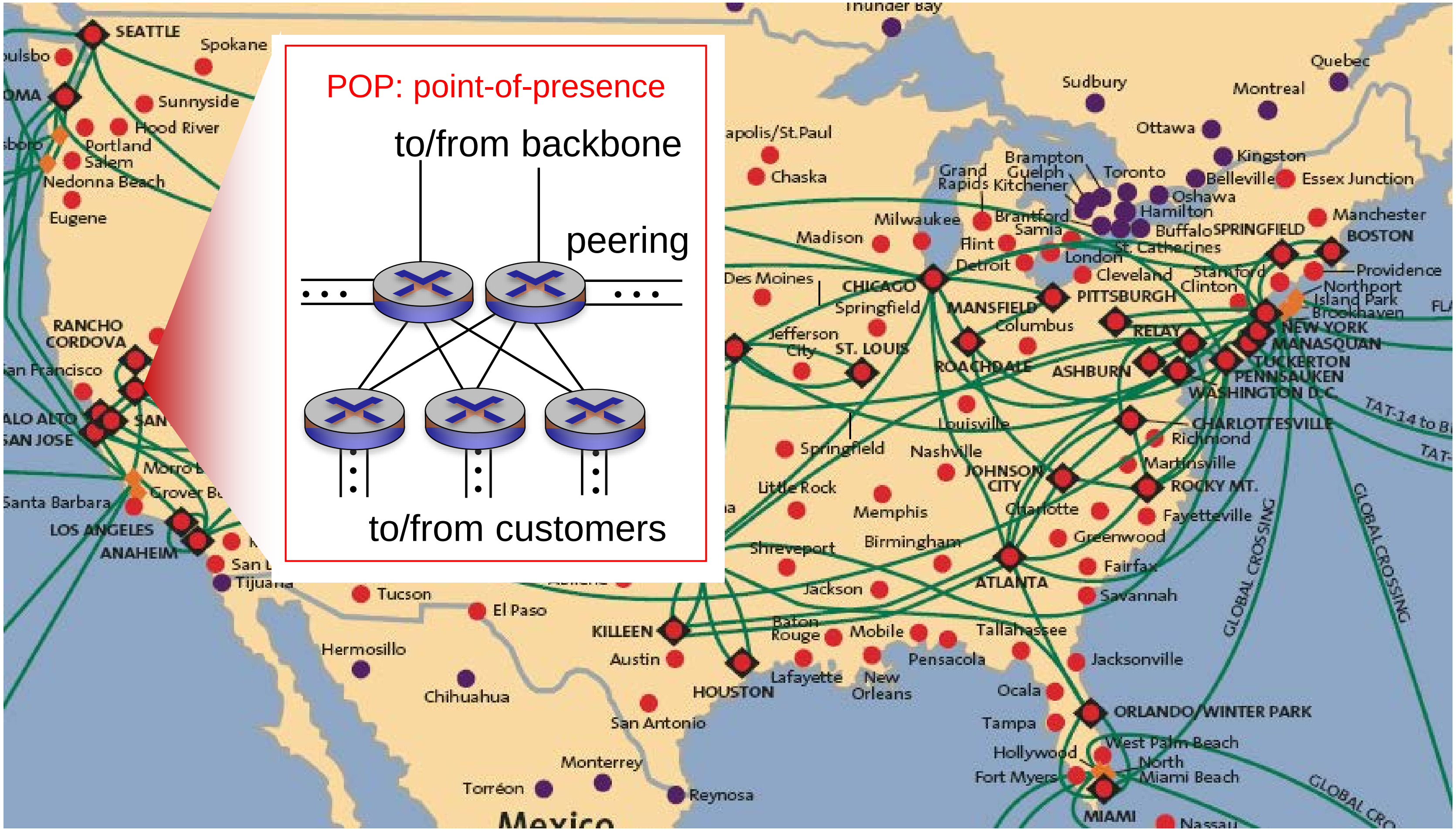


Internet structure: network of networks



- “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

Tier-1 ISP: e.g., Sprint



POP: point-of-presence

to/from backbone

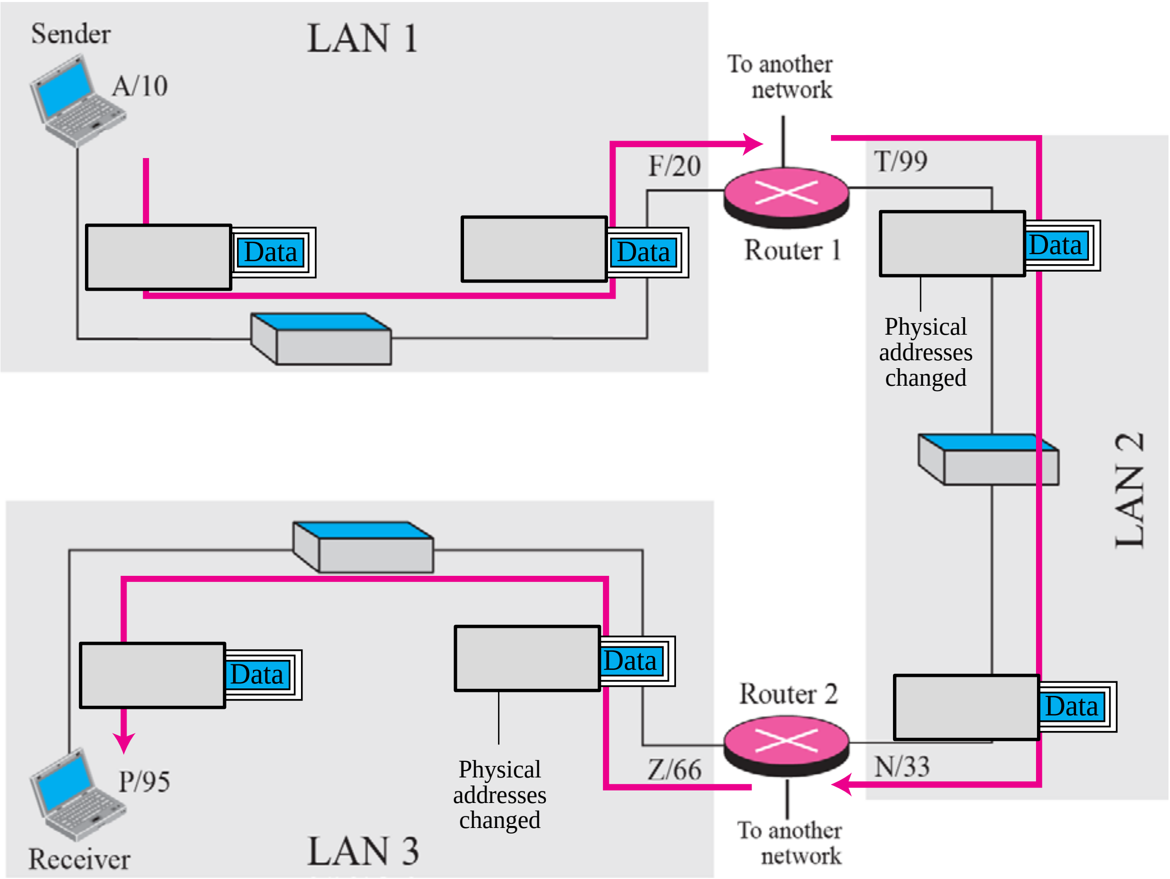
peering

to/from customers

http://www.telecomramblings.com/network-maps/usa-fiber-backbone-map-resources/

Exercise

- Reconstruct the content of packets



Sender
A/10
LAN 1
To another network
F/20
T/99
Router 1
Data
Data
Data
Physical addresses changed
LAN 2
Data
Data
Data
Router 2
Physical addresses changed
Z/66
N/33
P/95
Receiver
LAN 3
To another network