Computer Networks

-Wide Area Networks, Cable networks-

College of Information Science and Engineering
Ritsumeikan University

RITSUMEIKAN UNIVERSITY

W9 short test (1)

- The data link layer takes the packets it gets from the network layer and encapsulates them into frames for transmission.
- List the three main types of Data Link layer services to the Network layer!
  - Unacknowledged connectionless service, Acknowledged connectionless service, Acknowledged connection-oriented service
- What is the problem with using just byte count to break up the bit stream into discrete frames?
  - If a transmission error happens, the receiver won't be able to locate the correct start of the next frame (even if it knows that it is incorrect).
- Why escape bytes are needed for byte stuffing?
  - Byte stuffing uses a flag byte to indicate the start and the end of each frame. However, these bytes might occur in the data itself, so a special escape byte is used before these accidental flag bytes.

W9 short test (2)

- What is the main difference between Error correction and Error detection?
  - Error-correcting codes include enough redundant information to enable the receiver to deduce what the transmitted data must have been.
    Error-detecting codes include only enough redundancy to allow the receiver to deduce that an error has occurred (but not which error) and have it request a retransmission.
- In what situation error-detecting codes would be preferred over error-correcting codes?
  - When the error-rate is low (and the connection is fast), detecting errors and retransmission is more efficient than dealing with an occasional error and correcting it (e.g., fiber).
- What is the main characteristic of PPP?
  - Establishing a direct connection between two nodes without any host or any other networking device in between.

W9 recap (1)

- LAN is a private network that operates within and nearby a single building
- Many link layer protocols rely on a broadcast communication medium to transmit data
- In any broadcast network, they key issue involves determining who gets to use the channel when there is "competition" for it
- The protocols used to determine who goes next on a multiaccess channel belong to a sublayer of the data link layer called MAC
- Allocate a single broadcast channel among users: static vs. dynamic allocation
- Many solutions for allocating multiple access channels exist; CSMA/CD
- Classic vs. Switched Ethernet to deal with the increased load
- Switches only output frames to the ports for which those frames are destined: when a switch port receives an Ethernet frame from a station, the switch checks the Ethernet addresses to see which port the frame is destined for

W9 recap (2)

- Fast, Gigabit, 10+ Gigabit Ethernet standards
- Many organizations have multiple LANs and connect them with bridges (switches)
- Different devices in different layers: repeater, hub, bridge, switch, router, transport gateway, application gateway
- The Ethernet header was changed to contain a VLAN tag, for logically configured LANs
- Which VLANs are accessible via which ports: configuration tables have to be set up in the bridges

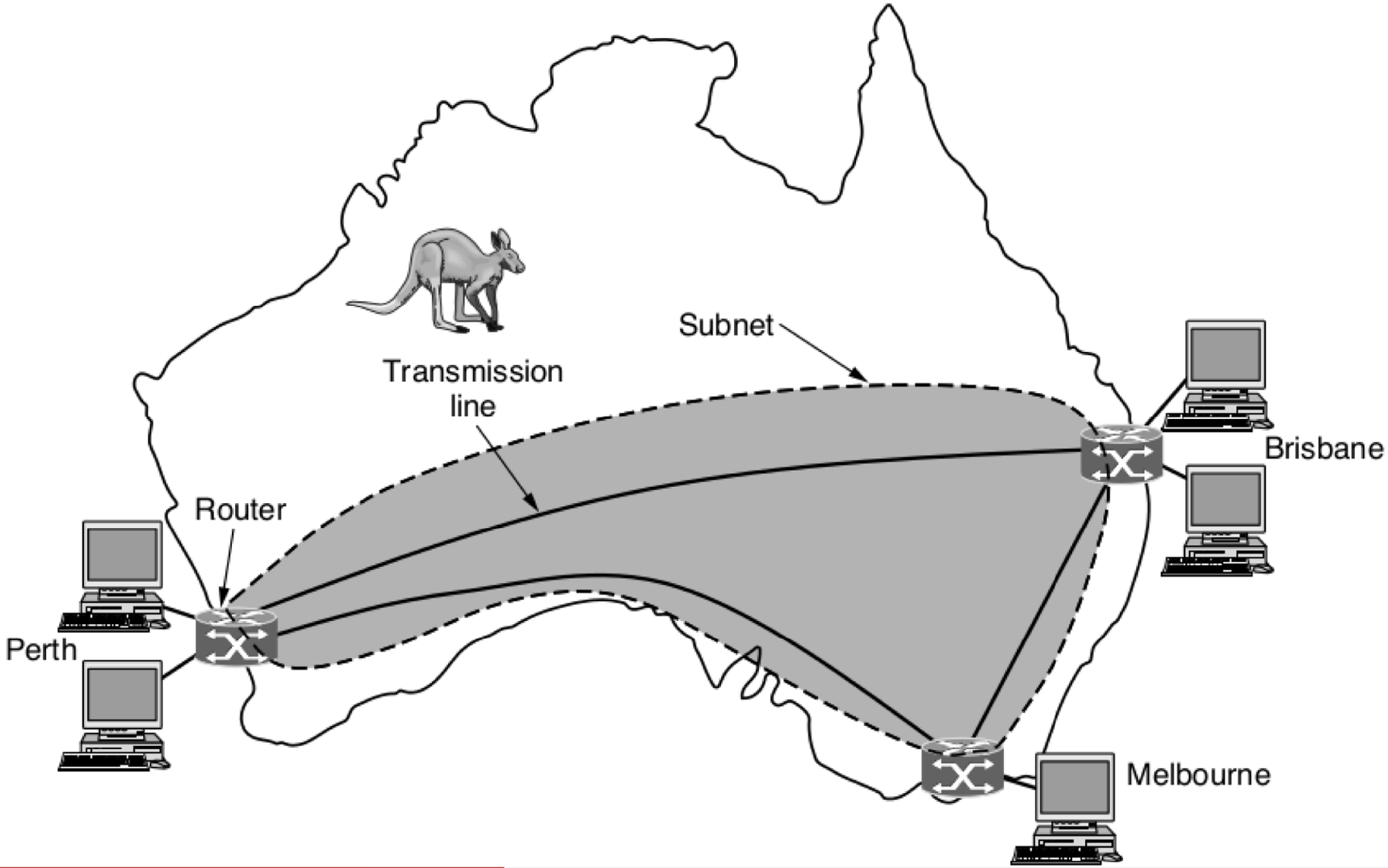
Agenda

- WAN recap
- The public switched telephone network
- Cable Networks
- Comparing access networks
- Communication security
- Summary

WAN (1)

- In simple terms, access networks connect subscribers to service providers
- A WAN (Wide Area Network) spans a large geographical area
  - e.g., a WAN that connects multiple offices of the same company where computers, hosts are running applications
  - the rest of the network that connects these hosts are the subnet
- Most companies use switches/routers to connect multiple transmission lines
  - when data arrive on an incoming line, a router chooses an outgoing line to forward it
- How the network makes a decision which path to use is called a routing algorithm
- How each router makes the decision where to send the information

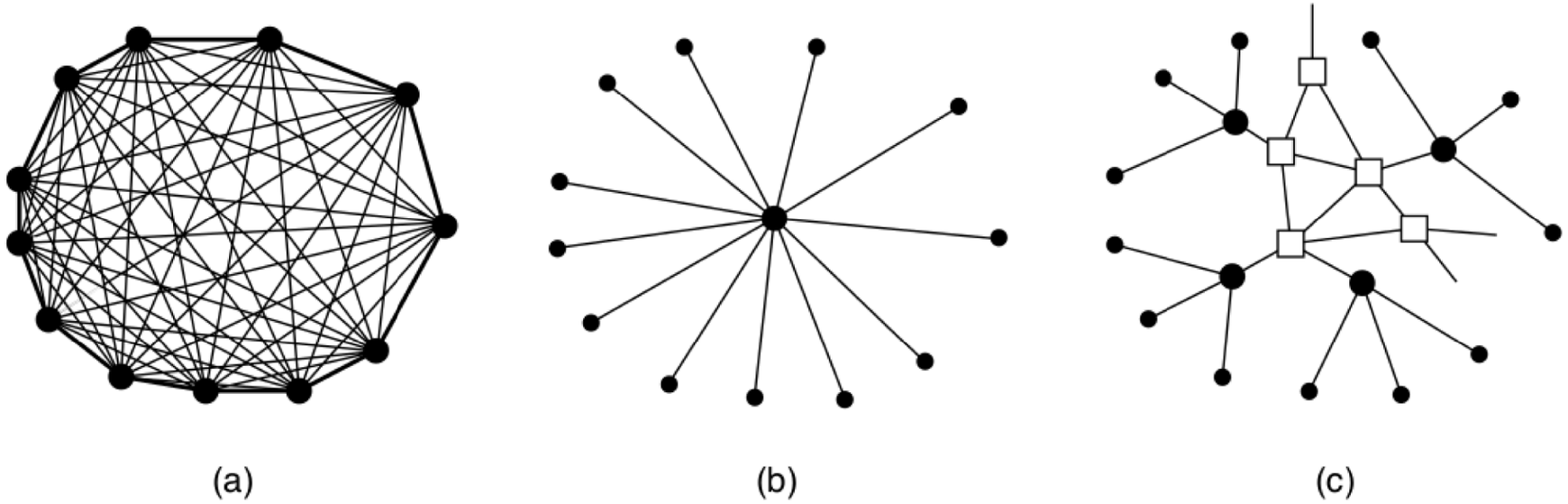
WAN (2)


Subnet
Transmission line
Router
Perth
Brisbane
Melbourne

PSTN

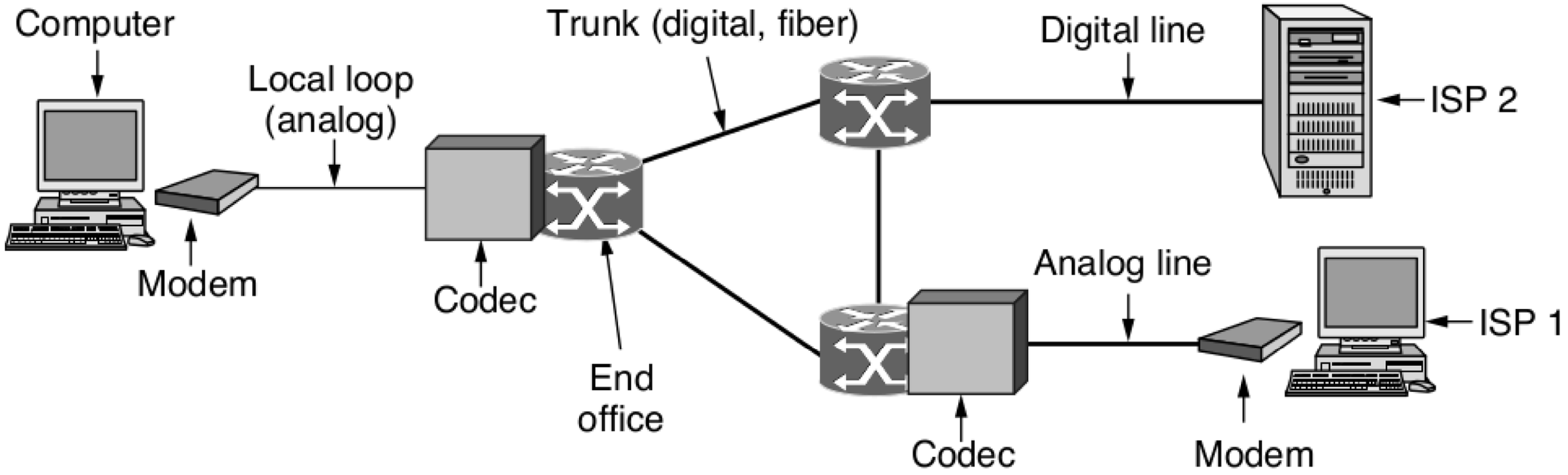
- When distances are large or there are many computers, the costs of running private cables can be too high (or even illegal)
  - network designers must rely on the existing telecommunication facilities (e.g., telephone network, cellular network, cable TV network)
  - engineering the existing physical infrastructure to increase transmission speeds is less expensive than using new fiber cables
- The **PSTN** (Public Switched Telephone Network) was designed many years ago
  - early DSL (Digital Subscriber Line) technologies could do only a few Mbps, now modern versions achieve rates $\sim$ 1 Gbps
- Three major components in the telephone system
  - local loops (analog twisted pairs between end offices and local houses)
  - trunks (very high-bandwidth digital fiber-optic links connecting switching offices)
  - switching offices (where calls are moved from one trunk to another)

Telephones, End offices, Toll offices



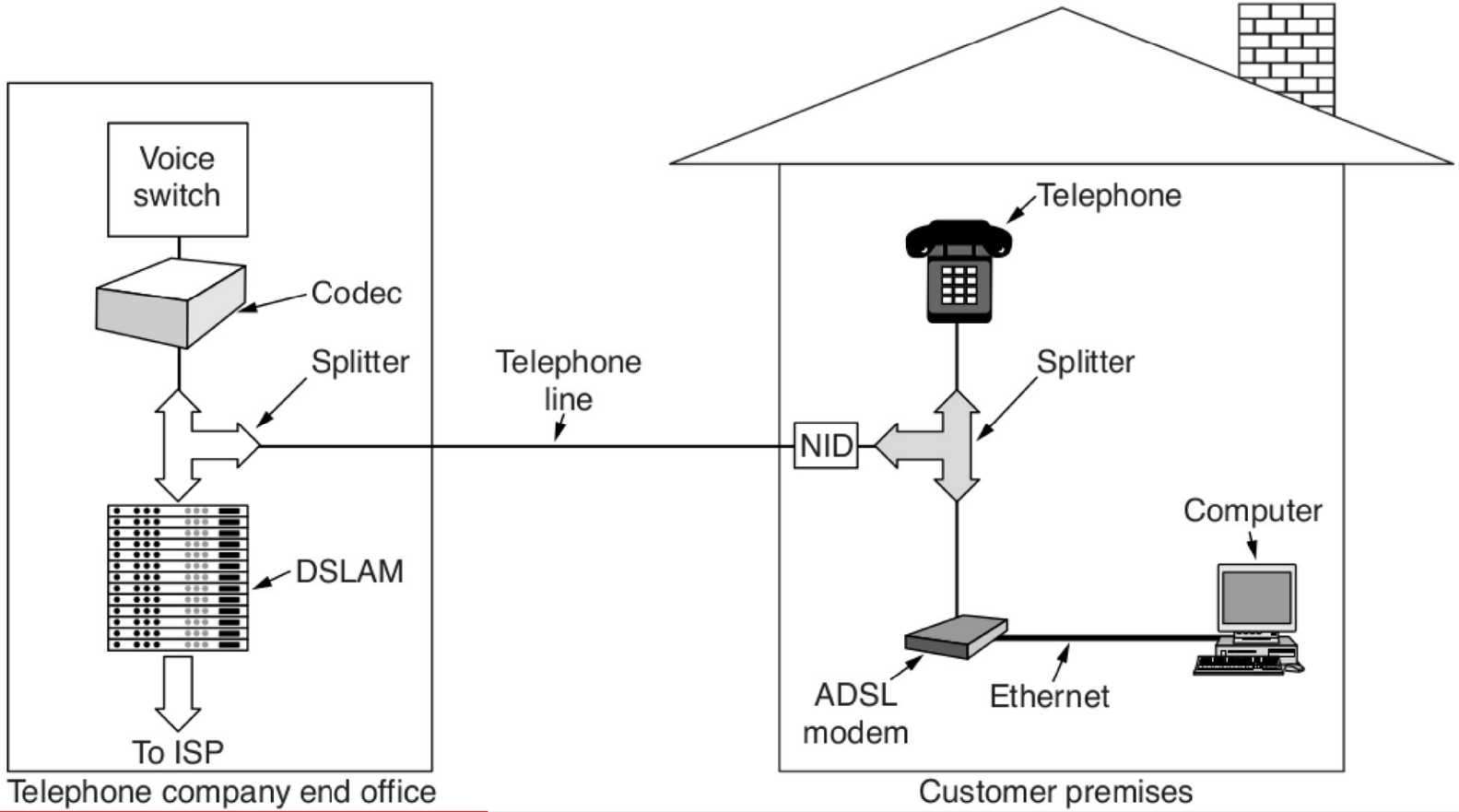
Telephone modems

- Telephone modems send digital data between computers over the narrow channel the telephone network uses for voice call
  - narrow bandwidth, signal distortion, susceptibility to electrical noise



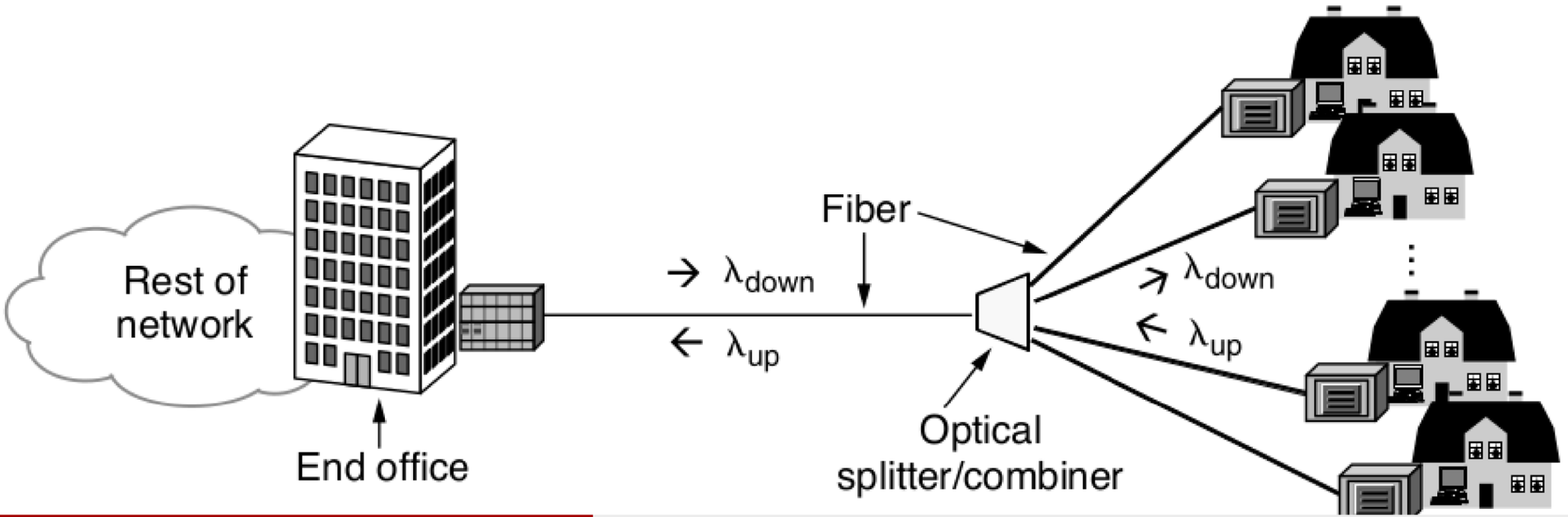
DSL

- The cable TV industry was offering higher speeds, so telephone companies needed a more competitive product
  - various **DSL** (Digital Subscriber Line) *broadband* services, e.g., **ADSL**:



FTTX

- The speed of last-mile networks is often constrained by the copper cables used in conventional telephone networks (cannot transmit data at high rates over as long distance as fiber)
  - variations of **FTTX**: **FTTH** (Fiber to the Home), or FTTN (Fiber to the Node)

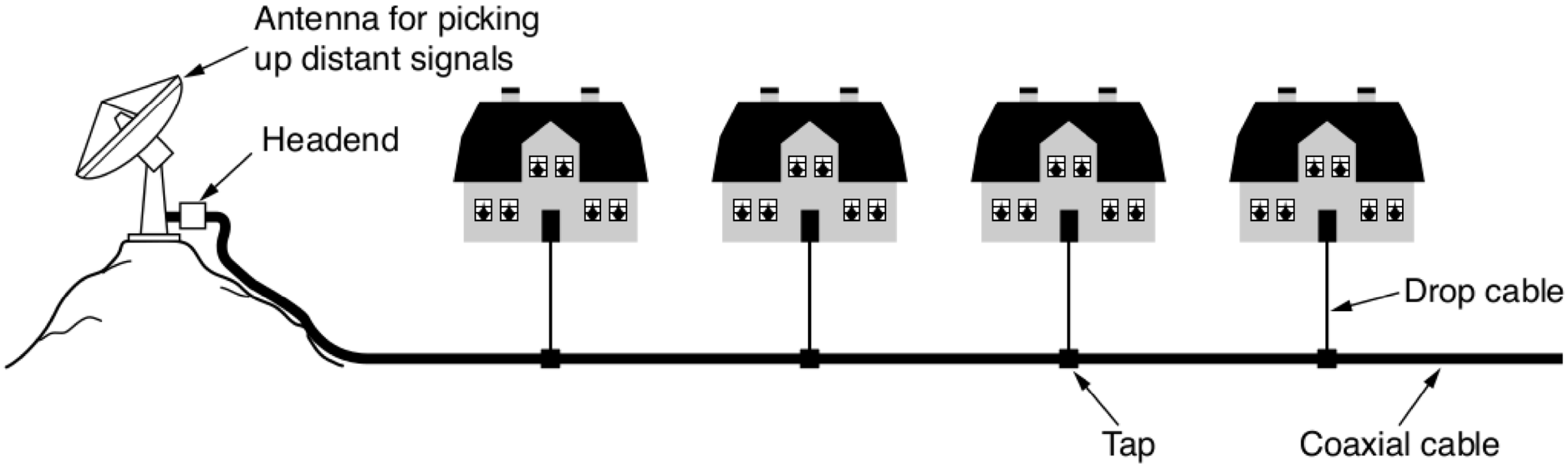


SONET/SDH

- **SONET** (Synchronous Optical Network) and **SDH** (Synchronous Digital Hierarchy) are similar standards used to transmit multiple digital bit streams synchronously over large distances with fiber optics
- Involves **multiplexing**/demultiplexing, and using repeaters
- High data rate/large bandwidth

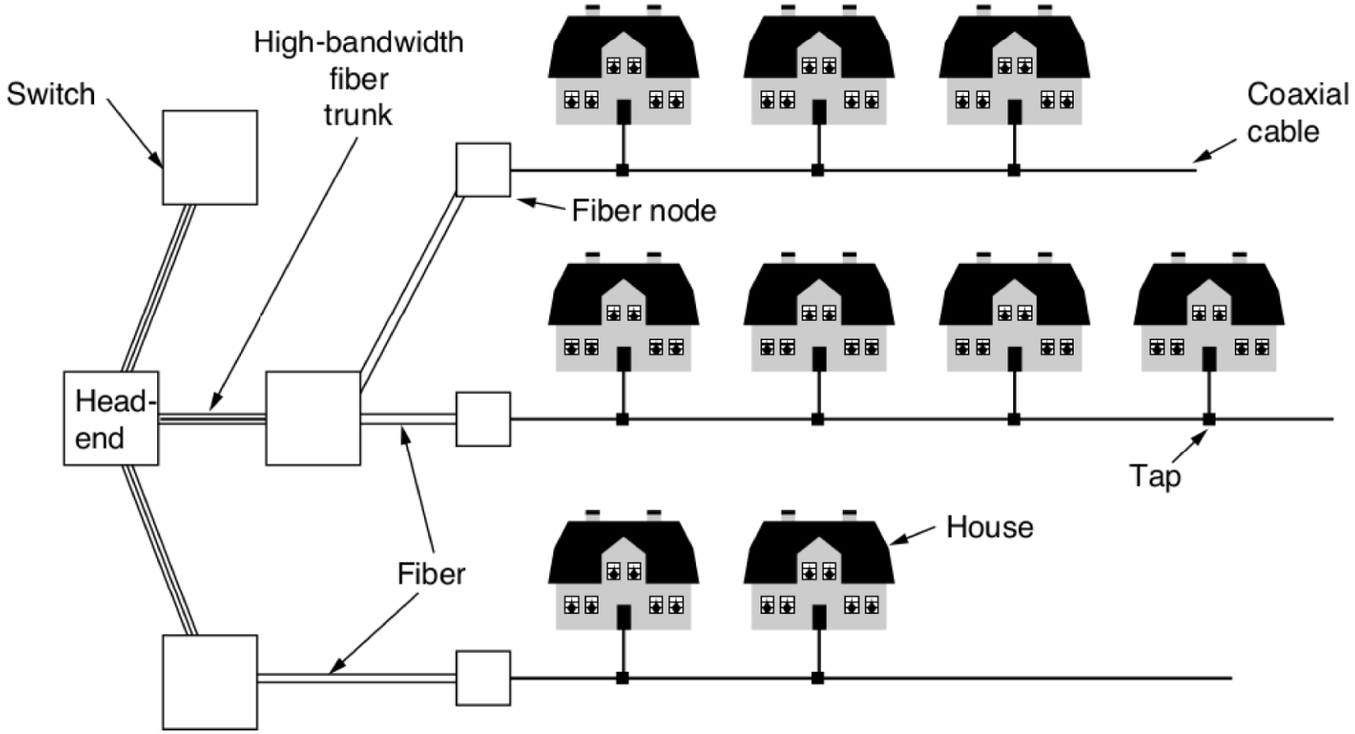
CATV

- Many people nowadays get their television, telephone, and Internet service "over cable"
- In the early years, cable television was called **CATV** (Communication Antenna Television):



Broadband Internet Access Over Cable: HFC

- Over time, cables between cities were replaced by high-bandwidth fiber
- A system with fiber for the long-hauls and coaxial cable to the houses is an **HFC** (Hybrid Fiber Coax), where a single fiber node can feed multiple coaxial cables
  - same trend as with telephone networks: moving fiber closer to the subscriber home



DOCSIS

- Cable companies operate networks that include HFC technology for last-mile connectivity, and also fiber and wireless last-mile connections
- The HFC part usually use the **DOCSIS** (Data Over Cable Service Interface Specification) standards
  - latest is the 3.1 version: over 1 Gbps of downstream capacity per home
  - multiple extensions to reduce latency
- Cable Internet subscribers require a DOCSIS cable modem to serve as the interface between the home network and the ISP network
  - the modem-to-home network interface is usually an Ethernet connection
  - sometimes ISPs provide a single hardware that combines the cable modem and the wireless access point
- The interface between the cable modem and the rest of the ISP network involves coordinating resource sharing among many cable subscribers who are connected to the same headend

Similarities

- Comparable service and comparable prices between cable, fiber, and ADSL
- All access network technologies now use fiber in the backbone
- Fiber and ADSL providers tend to deliver more consistent bandwidth (each user has dedicated capacity)
- The availability of high-speed Internet access still depends on the deployment of fiver or cable to homes
  - even ADSL requires some kind of fiber buildout at the edge

Differences

- They differ on the last-mile access technology
- Cable subscribers share the capacity of a single node (users may experience congestion)
- The maximum speeds a cable subscriber can achieve are limited by the capacity of the coaxial cable
  - the number of homes per node decrease as the cable ISPs continue to build fiver closer to the edge of the network
- Because ADSL is point-to-point, it is more secure than cable (although encrypted)

IPsec (1)

- **IPsec** (IP security) is a network protocol suite that authenticates and encrypts the packets of data sent over a network (network layer)
  - multiple services since not everyone wants all the security services all the time (also application dependent)
- IPsec itself is algorithm independent
  - algorithm that is secure now can be broken in the future, and switching algorithms are easier than changing a framework
- Although it is about IP, IPsec is connection oriented
  - to have security, a key must be established and used for some period of time
  - the connection in IPsec between two endpoints having a security identifier is a **SA** (Security Association)
  - SAs are carried in packets traveling on the secure connections, and used to look up keys, etc, when a secure packet arrives

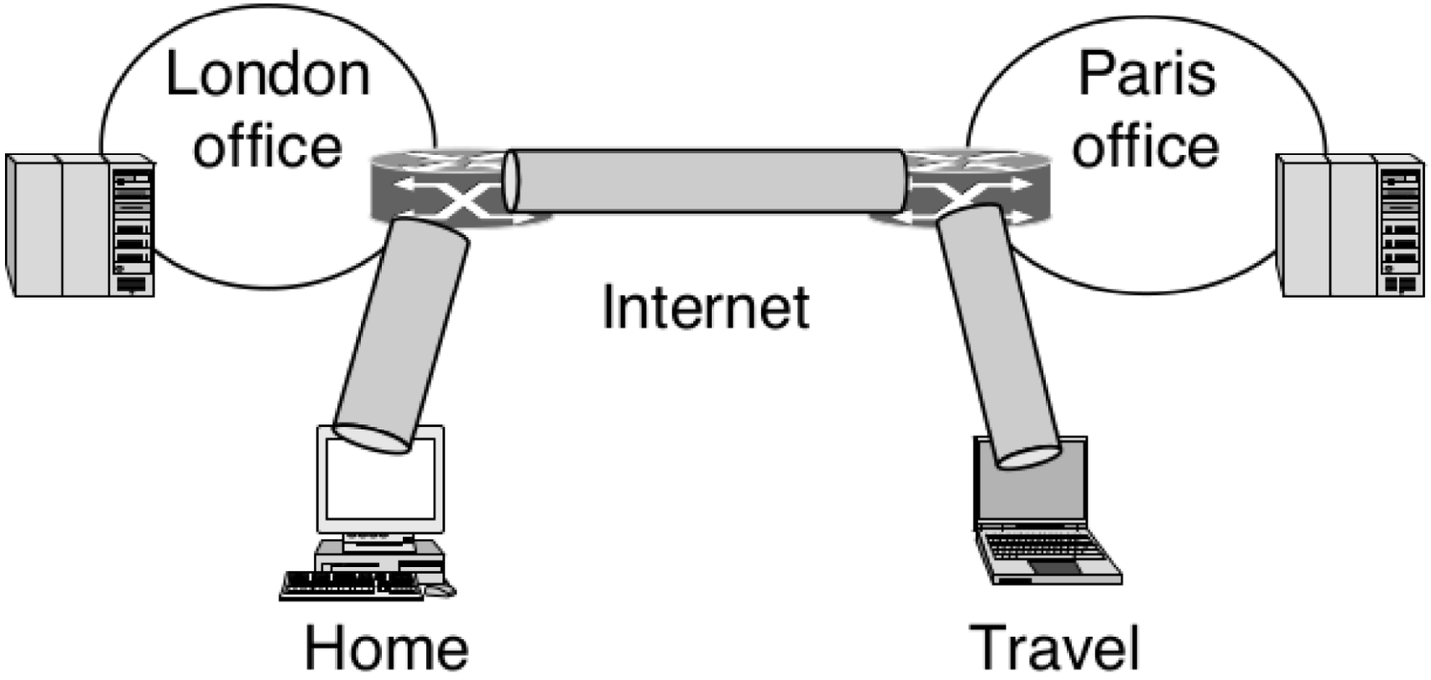
IPsec (2)

- IPsec has two main parts
  1. Two new headers that can be added to packets to carry the security identifier, etc.
  2. ISAKMP (Internet Security Association and Key Management Protocol) deals with establishing keys
- In **transport mode**, the IPsec header (having the SA identifier) is inserted after the IP header, and the Protocol field is changed to indicate that an IPsec header follows the normal IP header (before the TCP header)
- In **tunnel mode**, the entire IP packet is encapsulated in the body of a new IP packet with a new IP header (affects packet size substantially)
  - the end of the tunnel can be a security gateway machine: in a VPN, it encapsulates and decapsulates packets as they pass through it

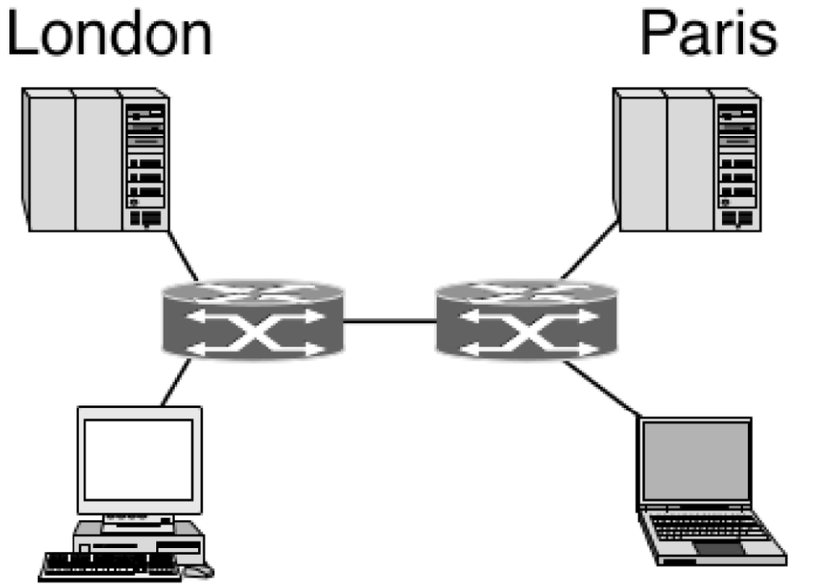
Virtual Private Networks (1)

- A network built up from company computers and leased telephone lines is called a *private network*
  - leasing dedicated lines between two points is expensive
- Moving to the "public" network but without giving up the security advantages: **VPN**s (Virtual Private Networks)
  - overlay networks on top of public networks with most of the properties of private networks
- The most popular approach is to build a VPN over the Internet
  - equip each office with firewall and create tunnels through the Internet between all pairs of offices
  - when the system is brought up, each pair of firewalls has to negotiate the parameters of its SA, including services, algorithms, keys

Virtual Private Networks (2)



(a)



(b)

Virtual Private Networks (3)

- If IPsec is used for tunneling, it is possible to aggregate all traffic between any two pairs of offices onto a single authenticated and encrypted SA
- Many firewalls have VPN capabilities already built in
- Once the SAs has been established, to a router within the Internet, a packet traveling along a VPN tunnel is just an ordinary packet (with an IPsec header)
- ISPs can set up VPNs using MPLS (MultiProtocol Label Switching), where paths for the VPN traffic can be set up across the ISP network between company offices
  - traffic is separate from other Internet traffic and guaranteed a certain amount of bandwidth

W10 Summary (1)

- Access networks connect subscribers to service providers, and a WAN spans a large geographical area
- When distances are large, network designers must rely on the existing telecommunication facilities
- Three major components in the telephone system: local loops, trunks, and switching offices
- Although limited, telephone modems send digital data between computers over the narrow channel the telephone network uses for voice call
- Early DSL technologies over the PSTN were slow, but modern broadband services such as ADSL are high bandwidth
    - involves an ADSL modem, splitters, codec, DSLAM
- Common to use variations of FTTX, because he speed of last-mile networks is often constrained by the copper cables used in conventional telephone networks

W10 Summary (2)

- SONET and SDH are standards used to transmit data over large distances with fiber optics
- Many people nowadays get their television, telephone, and Internet service "over cable"
- A system with fiber for the long-hauls and coaxial cable to the houses is an HFC (Hybrid Fiber Coax), where a single fiber node can feed multiple coaxial cables
  - uses the DOCSIS standards, where a dedicated cable modem is needed (often combined with a wireless access point)
- Same trend with cable and telephone networks: moving fiber closer to the subscriber home, and all access network technologies now use fiber in the backbone
- Although they differ on the last-mile access technology, comparable services and prices
  - fiber and ADSL providers tend to deliver more consistent bandwidth

W10 Summary (3)

- IPsec is a network protocol suite that authenticates and encrypts the packets of data sent over a network
  - the connection in IPsec between two endpoints having a security identifier is a SA
  - in transport mode, the IPsec header is inserted after the IP header
  - in tunnel mode, the entire IP packet is encapsulated in the body of a new IP packet
- VPNs are usually built over the Internet, but without giving up most of the security advantages of a real private network
  - if IPsec is used for tunneling, it is possible to aggregate all traffic between any two pars of offices onto a single authenticated and encrypted SA
  - as the SAs has been established, a packet traveling along a VPN tunnel is just an ordinary packet