A network’s connection structure is known as its *network topology*.

- **Host nodes** – source and destination of messages
- **Communication nodes** – where messages pass through; can be routers/hubs/switches, etc.
- **LAN** – home, school, etc.
- **WAN** – internet
- **AS** – clusters of routers within a WAN that is controlled by a single entity.
Circuit switching is one method for transmitting data within a network.

- Used in the phone networks.
- When a node of a network wishes to communicate with another node, a route that goes through a sequence of hardware devices is established between the two.
- Data is then sent along this route.
- The route is maintained until communication ends.
A more modern method is *packet switching*.

- Used in the Internet.
- Data is split into *packets*.
- Packets are transported independently through the network.
- In *connectionless* packet switching, packets sent from one node to another need not follow the same routes.

In *virtual circuit switching*, packet switching mimics circuit switching.
Packets and Encapsulation

A packet typically consists of

- a *header*: contains control info like source and destination addresses
- sometimes a *footer*: for checksums, etc.
- *payload*: data

Additionally, a packet can be *encapsulated* within another packet.
The architecture of the Internet is modeled conceptually as consisting of *layers*. Each layer has *addresses* to identify the source and destination of the packets and *protocols* which describe how the packets should be routed.

We shall use the TCP/IP model which has 5 layers. The OSI model has 7 layers.
Physical layer
- deals with the type of physical connection used: copper wires, fiber-optic cables or wireless radio, etc.

Link layer
- transmits packets across LANs
- uses 48-bit media access control (MAC) addresses
- Ethernet: deals with the logical aspects of sending info across a network link
- ARP: determines routes
Network layer / Internet layer

- used for Internet-wide communication
- main protocol: Internet Protocol (IP)
  - in IPv4: each host has a 32-bit address
  - in IPv6: each host has a 128-bit address
- packets are routed on a best effort basis

Transport layer

- support communication and connections between applications based on IP addresses and ports, which are 16-bit addresses
- has two kinds of protocols:
  - Transmission Control Protocol (TCP): connection-oriented
  - User Datagram Protocol (UDP): connectionless-oriented
Application layer

- provide protocols that support useful functions based on services provided by the transport layer
  - HTTP: uses TCP and supports web browsing
  - SMTP and IMAP: uses TCP and support e-mail
  - VoIP: uses UDP and supports Internet phone messaging
Encapsulating application layer packets

Application Packet

TCP Header

TCP Data

Application Layer

Transport Layer

IP Header

IP Data

Network Layer

Frame Header

Frame Data

Frame Footer

Link Layer

Computer Networks I
Figure 5.3: Connections and communication needed to send data from a host through two routers to another host.
Network Security Issues

The Internet was built with the assumption that users are not malicious. With its current usage, however, the assumption no longer holds.

For each of these security goals, extra work must be done at the application layer or lower-level protocols must be revised:

- Confidentiality
- Integrity
- Availability
- Assurance
- Authenticity
- Anonymity
The Link Layer
Network Interfaces

- Network interfaces are devices used to connect a computer to a network – e.g. Ethernet cards, WiFi adaptors.
- At the link layer, packets are called *frames*.
- Frames are transmitted between network interfaces.
- In *regular mode*, a network interface only processes frames addressed to it.
- In *promiscuous mode*, a network interface reads *all frames* that go through it.
Most network interfaces come with a predefined MAC address.

A MAC address is a 48-bit number usually represented in hex e.g., 00-1A-92-D4-BF-86

MAC addresses are intended to be unique to facilitate routing of frames.

Nonetheless, they can be reconfigured by network interface driver software. (Trouble!)
Hubs and switches are used to connect multiple devices together.

- **Hubs** typically forward all frames to all attached devices.
- **Switches** learns the addresses of the machines that are connected to its various ports. It will forward frames along links connected to the destination computer.
A **MAC spoofing attack** impersonates another machine:

- Find out MAC address of target machine.
- Reconfigure MAC address of rogue machine.
- Turn off or unplug target machine.
MAC Spoofing Attack

A **MAC spoofing attack** impersonates another machine:

- Find out MAC address of target machine.
- Reconfigure MAC address of rogue machine.
- Turn off or unplug target machine.

**Countermeasures:**

- Check for multiple occurrences of the same MAC address.
- Disable one or both machines.
The address resolution protocol (ARP) connects the network layer to the data layer by converting IP addresses to MAC addresses.

**ARP works by broadcasting requests and caching responses for future use:**
The address resolution protocol (ARP) connects the network layer to the data layer by converting IP addresses to MAC addresses.

ARP works by broadcasting requests and caching responses for future use:

- The protocol begins with a computer broadcasting a message of the form
  
  `who has <IP address1> tell <IP address2>`

- When the machine with `<IP address1>` or an ARP server receives this message, it broadcasts the response
  
  `<IP address1> is <MAC address>`

The requestor's IP address `<IP address2>` is contained in the link header.
Once the requestor receives the ARP reply, it stores the IP-MAC address pair in a table called its **ARP cache**.

An example of an ARP table:

<table>
<thead>
<tr>
<th>Internet Address</th>
<th>MAC Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.148.31.1</td>
<td>00-00-0c-07-ac-00</td>
<td>dynamic</td>
</tr>
<tr>
<td>128.148.31.15</td>
<td>00-0c-76-b2-d7-1d</td>
<td>dynamic</td>
</tr>
<tr>
<td>128.148.31.71</td>
<td>00-0c-76-b2-d0-d2</td>
<td>dynamic</td>
</tr>
</tbody>
</table>

Finally, it sends its data to the destination.
ARP Poisoning

- An ARP cache updates every time that it receives an ARP reply 
  *even if it did not send any ARP request!*
- It is possible to poison an ARP cache by sending *gratuitous* ARP replies!

**MAIN ISSUE: Lack of identity verification**
In the previous slide, Eve is basically doing a **man-in-the-middle-attack**. She can see all traffic between Alice and Bob. She can sniff passwords and/or modify the data.
In the previous slide, Eve is basically doing a **man-in-the-middle-attack**. She can see all traffic between Alice and Bob. She can sniff passwords and/or modify the data.

**Countermeasures:**

- Use static ARP tables only. (Too strict and hard to manage!)
- Use software solutions that inspect all ARP packets and compare their contents with stored records of ARP entries. Examples include programs like anti-arpspoof, XArp, Arpwatch, etc.