Networking

DSC340
Mike Pangburn

Networking: Computers on the Internet

- 1969 - 4
- 1971 - 15
- 1984 - 1000
- 1987 - 10,000
- 1989 - 100,000
- 1992 - 1,000,000
- 1996 - 10,000,000
- 2001 - 100,000,000
- By 2005... billions

Typical LAN “Local Area Network”

Client/Server Networks

Network Hardware

- The most essential networking hardware devices for us to learn about are:
  - Cables
  - NICs
  - Hubs
  - Switches
  - Routers

Wire Media
Media Bandwidth

<table>
<thead>
<tr>
<th>Line Type</th>
<th>Use</th>
<th>Maximum Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone line (twisted pair copper lines)</td>
<td>Dial-up modem</td>
<td>56 Kbps</td>
</tr>
<tr>
<td></td>
<td>DSL modem</td>
<td>1.544 Mbps</td>
</tr>
<tr>
<td></td>
<td>WAN—T1— using a pair of telephone lines</td>
<td>1.544 Mbps</td>
</tr>
<tr>
<td>Coaxial cable</td>
<td>Cable modem</td>
<td>Upto 20 Mbps</td>
</tr>
<tr>
<td>Unshielded twisted pair (UTP)</td>
<td>LAN</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>Optical fiber cable</td>
<td>LAN and WAN—T3, OC-708, etc.</td>
<td>40 Gbps or more</td>
</tr>
<tr>
<td>Switch</td>
<td>LAN—OC-708, etc.</td>
<td>40 Gbps or more</td>
</tr>
</tbody>
</table>

NIC — a “Network Interface Card”

- Every networked device must have a NIC
- Most laptops today have both a wired NIC and a wireless NIC
- Each NIC has an IP address (it’s “logical address”) and a physical address called a MAC address.
- Each NIC is given an address at the factory that is the device’s physical address or MAC address.
- No two NIC devices will ever have the same MAC address.
- MAC Addresses are used within a LAN
  - IP addresses allow routers to route a message across different networks
  - when a message reaches the correct destination network, the correct NIC is identified via its MAC address.

Hubs

- A “hub” is a networking component that into which you can plug in multiple network devices
- Connect computers, printers, scanners, etc.
- Anytime a connected device sends a network message, the hub forwards the message to all other connected devices (not just the intended recipient!!)
- Unintended recipients should ignore bogus network traffic (akin to “screening” telephone calls)
- Creates opportunities for deviant “packet sniffers”
- Hub can only deal with one message at a time, since it is broadcast over all connections

Switches

- A switch is a network device which directs traffic only to its intended destination(s) rather than to all devices on the network.
  - sometimes referred to as an “intelligent hub”
- Provide a dedicated connection between individual devices
  - multiple devices can send data at once

Consider packing sniffing software threat for people who share a hub and have not activated network encryption
- Data sent “in the clear” means it has not been encrypted, and therefore is vulnerable to eavesdropping via a hub
- As the prices for switches have dropped tremendously over time, most companies have replaced hubs with switches
  - Switch protects from eavesdropping by sending data on the LAN only to the intended recipient
**Routers**

Different networks connect via routers (not switches or hubs).

Routers even connect networks based on different protocols, which is important since not all networks use the same protocol.

**Gateway router**

- When your computer needs to contact a computer that is not within the immediate network (i.e., your LAN), then your computer’s networking software is configured to send the request to a particular router called a:
  - Default Gateway
  - Gateway router

- For each of us, the most noteworthy role of the gateway router is to connect your computer’s LAN to your ISP’s larger network so that your computer accesses the Internet.

- Therefore, a gateway router is your computer’s onramp to the Internet.

**Standard networking protocols (communications standards)**

- The committee that addresses LAN standards is called the IEEE 802 Committee.
- Thus, IEEE LAN protocols always start with the number 802.
- “Ethernet” is a particular protocol published by this committee as their “802.3” protocol.
- Ethernet (802.3) is the world’s #1 standard wired-LAN protocol.
- There are other protocols besides Ethernet, but it is dominant.
- Most PCs’ NICs support 10/100/1000 Mbps Ethernet.

**Packet switching**

- The Ethernet (IEEE 802.3) standard transmits data in little chunks called packets.
- Break long messages into short “packets”
  - Keeps one user from hogging a line.
  - Each packet is tagged with where it’s going.
- Route each packet separately
  - Each packet often takes a different route.
  - Packets often arrive out of order.
  - Receiver must reconstruct original message.

**TCP/IP**

- Transmission Control Protocol/Internet Protocol (TCP/IP) provides the technical foundation for the public internet as well as for large numbers of private network. It is defined in terms of layers.
- Do you use TCP/IP?
  - If you are on the Internet, yes, you are using TCP/IP.
- TCP/IP layers (at left, with particular implementations at right)

**A TCP/IP network packet**

- Here is the basic structure of any one of trillions of packets traversing the Internet at this moment.
Tying this back to Switches and Routers

- **Routers** operate between networks (at the “internet” layer of TCP/IP) and use IP addresses to direct network traffic.

- **Switches** work within a single network (at the “network interface” layer of TCP/IP) and use hardware MAC addresses we discussed earlier.

### Wireless networking

- Wireless fidelity (wi-fi) – a means of linking computers into a wireless local area network (WLAN)
- Also referred to as 802.11
- Wi-Fi has evolved through various standards, the most common of which have been:
  - 802.11b, with 11 Mbps bandwidth
  - 802.11g, with 54 Mbps bandwidth
  - 802.11n, with 100 - 200 Mbps bandwidth

### Basic web networking scenario

Not secure. You and your BFF are exposed and relying on your ISPs to provide all security (from hacker attacks, viruses, worms).

- IP's are public accessible.

Better: add router (a “firewall”)

Better. You buy a router that connects to your ISP. The router assigns your PC a private IP address.

Recall Private IP addresses

- Is anyone here using this IP address at home? 192.168.0.1
- How can many people use the same IP address?
  - “I thought each computer on the internet required a different IP address?”
- Recall: the IT industry decided that the following ranges of IP addresses would be non-routable (i.e., a router will not pass along packets with such destinations to another network):
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255
Private IP address requires your router’s NAT (Network Address Translation)

Your router’s NAT feature modifies your outgoing packets such that their source IP becomes 24.48.0.1. Your BFF’s chat program thus sends its response to 24.48.0.1. Your router’s NAT function also changes the destination IP on the response packets it later receives from your BFF to 192.168.0.1.

Hiding multiple servers behind one public IP address: Port Mapping

- Port mapping is what allows companies to have multiple servers accessible via one IP and corresponding DNS address.
- Common example: company wish to run both an FTP and Web server from its domain name, asite.com
  - ftp://www.asite.com
    - Note: this is equivalent to typing ftp://www.asite.com:21 because port 21 is the default for ftp
    - The firm’s router with Port Mapping will send port 21 traffic to the FTP server
  - http://www.asite.com
    - Note: this is equivalent to typing http://www.asite.com:80 because port 80 is the default for http
    - The firm’s router with Port Mapping will send port 80 traffic to the web server

Hiding multiple servers behind one IP address: Port Mapping

- Need to direct incoming packets to the appropriate server
- Corporate Router with Port Mapping and NAT activated
  - FTP server 224.60.32.1:21
  - Web server 224.60.32.1:80

- 24.48.0.1
  - You 192.168.0.1
  - Corporate Router with Port Mapping and NAT activated
  - FTP server 224.60.32.1:21
  - Web server 224.60.32.1:80