NETWORKING

Overview

NETWORKING?

- Connecting machines and resources for purposes of sharing and communication
- Handled on many different levels, from the physical mediums doing the connecting to the lofty application layer providing a service to the end user

NETWORK SANDWICH

- If you crack a networking book, they talk about the 7 layer OSI model. Then immediately tell you to toss that out the window, because the predominant networking systems of today don't really follow the model. :)

- The layers we really care about in this class include:

  - Physical - cabled, fiber, wireless
  - Link - Ethernet, 802.11
  - Network - IP
  - Transport - TCP/UDP
  - Application - HTTP, FTP, SSH, DNS, SMTP, POP3, IMAP, etc, etc, etc

PHYSICAL LAYER

- The physical layer specifically defines access to the communication medium. Generally one of:
  - Copper (wires) - voltages
  - Plastic/Glass (fiber) - light pulses
  - Air (radio waves) - modulated waves

LINK LAYER

- The link layer defines access to the physical media, spelling out procedures for communication, collision handling and more.
- Examples include: Ethernet, Token Ring, FDDI, WiFi
- Protocols running at this layer include: ARP, RARP, PPP, SLIP

LINK LAYER

- Ethernet is by far the most common link layer protocol in use today.
  - Uses CSMA/CD (Carrier Sense, Multiple Access with Collision Detection) for media access
- Wi-Fi (802.11) is rapidly expanding in popularity and use
  - Uses CSMA/CA (Carrier Sense, Multiple Access with Collision Avoidance) for media access

LINK LAYER

- The link layer generally defines a physical-level address, known as the MAC (Media Access Control) address.
  - Normally hard coded by manufacturer
  - Guaranteed unique
  - Allows basic communication at the physical level, on local networks. To expand into other networks, though, a virtualized address must be used, which is handled by the...

NETWORK LAYER

- The network layer provides inter-networking capabilities, bridging multiple LANs.
- Most popular protocol is the Internet Protocol (IP), which provides the virtualized addresses and basic network communication support.
- Supporting protocols include: ICMP, BGP, IGMP, OSPF, RIP
- Does not guarantee delivery of messages
- Does not track order of message deliveries

TRANSPORT LAYER

- Most common: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) - provides finer grained addressing with ports
- TCP - Establishes and manages connections between nodes on a network.
  - Guarantees delivery of messages
  - Guarantees order of delivered messages
  - Throttles traffic (flow control)
- UDP - Connectionless
  - Best effort delivery; low overhead

PORTS

- A port is an address component in TCP and UDP messages which identifies the service that should receive the message within the addressed system.
- Number from 1-65535
- Hundreds of “well-known” ports and corresponding services defined in `/etc/services`
- Examples:
  - HTTP: 80, SMTP: 25, POP3: 110, SSH: 22

APPLICATION LAYER

- Finally, the application layer is the ‘user’ of the networking services - leveraging TCP and UDP protocols to shuttle information around the room or the globe.

- Common application layer protocols include:
  - HTTP (web)
  - SMTP (sending mail)
  - POP (reading mail)
  - SSH (secure shells)
  - And many, **many** more

END TO END

- Each layer wraps on top of the next, so a message starts at the application layer as data specific to the application
- This data gets wrapped with information for TCP/UDP and IP layers, providing addressing and transport ability
- Wrapped again by Ethernet, providing physical access
- Wrapped one more time by physical layer, getting sent out
- When received at other end, each layer is unwound as the message travels “up” the stack on the receiving system

TCP/IP

- TCP and IP work hand in hand to run most of the world's network communications.
- While there isn't much else to TCP or UDP for this discussion, there is more to IP
- Specifically, addresses...

IP ADDRESSES

- The IP address provides the user-configured, routable virtual address used for communication in and between LAN's
- There are two versions of the IP protocol: version 4 and version 6.
- IPv4 is the old guard, developed decades ago and still in use nearly everywhere. Fairly simple set of features and a 32 bit address. Will be focus of this discussion.
- IPv6 was recently (~10 years ago) ratified to address some of the shortcomings of IPv4, including security features and a lack of address space. IPv6 addresses are 64 bits.

IP ADDRESSES

- 32 bit value (32 1's and 0's)
- Not easily represented as 32 digits (too much typing!)
- Instead, broken into four groups of 8 bits
- 8 bits can be represented in decimal as 0-255
- Hence, the dotted quad is born:
- 192.168.1.100

THAT'S NOT ALL!

- When IPv4 was designed, it included a subnetting ability.
- Subnetting allows for grouping and organizing networks within the IPv4 address space.
- The first part of every IP address is designated as the network address, identifying the subnet to which the IP address belongs.
- The remaining portion of the IP address is known as the host address and uniquely identifies the addressed node within the subnet.

SUBNET MASK

- Identifying the two components of an IP address is the job of the subnet mask

- A mask is a special number which is compared to another number using mathematical functions (usually boolean algebra's AND operation) to extract information.

- A subnet mask is a 32 bit number with a special definition: where the mask is a 1, it corresponds to the network address within an IP address, and where it's a 0, the host address.

- Since there are only two components to an IP address, subnet masks are always start as a series of ones, then switch to zero's

SUBNET MASKS

- Subnet masks are also written as dotted quads. But since they're just a series of 1's, then 0's, they usually look something like:
  - `255.255.255.0` or `255.255.192.0`
- An easier way to express a subnet is to use CIDR notation. CIDR stands for Classless Inter-Domain Routing, and was created to address a shortcoming of the IPv4 standard design - subnet classes.

SUBNET CLASSES

- The original IPv4 spec created set network sizes and named them “classes”.
  - Class A: 8 bit network address
  - Class B: 16 bit network address
  - Class C: 24 bit network address
  - Class D and Class E: special purpose networks
- This was done to define the overall layout of the 32 bit address space. It quickly became insufficient to support the networks being created, and CIDR was implemented.

CIDR

- CIDR breaks away from class-based subnets and allows for the creation of arbitrary subnet sizes (still within the overall layout of the 32 bit address space)
- CIDR notation is simpler than dotted quad for subnet masks
- A slash, followed by the number of the last bit of the network address. Example:
  - /24 - class C - 255.255.255.0
- Usually combined with the IP address to form a complete address:
  - 192.168.1.100/24

SAY WHAT?

- Networking is a huge and complex topic. Subnetting alone gets pretty hairy to understand without a lot of background material.

- We can't get into a long discussion of subnetting, but suffice it to say that an IP address alone is not enough to define a machine's access to the local network. A subnet mask must also be provided.

- For more information, see a google

```
slideshow.end();
```