TCP/IP for Programmers

Eli the Computer Guy

Why TCP/IP Matters to Coders…???

- Architecture… Architecture… Architecture…

Logical vs. Physical

- Logical Devices are the Specific Service - Firewall, Router, Modem, Access Point
  - These were, and can still be dedicated devices, but are generally built into a single device such as a SOHO Router that has a Router, Switch, Access Point, Firewall and even VPN built in.
- Physical Devices are the actual objects you plug into the network.
- Design/ Whiteboard based on Logic
- Build based on Physical

BEWARE of CACHEING

- Systems “cache” data and store it locally so that they can respond to clients more quickly.
- When you make a change the system you are connecting to may still respond with cached data.
- Either wait for caches to clear, or force a cache to be “flushed”
- “Replication” times are how long it takes for changes to be copied to all relevant systems

What is a Protocol

- Language for computers to talk to each other
- Network Protocols, Storage Protocols, Communication Protocols
- TCP/IP
- FTP
- SIP
- RTMP
- iSCSI

TCP/IP v6 ???

- Tomorrow… is always a day away…
- We’ll run out of v4 addresses the day after tomorrow…
- “Legacy” systems have a nasty habit of not dying properly…

Ethernet Standard

- Star Typology
- RJ45 Connectors
- MAC addresses
- CSMA/CD - Collision Domains

MAC Address?

- Universally Unique Identifier
- Part is the Vendor ID, Part is the Serial Number
- Connection has a MAC Address
- REST API to Find Info Based on MAC Address
  - https://www.macvendorlookup.com/api

Layer 2 Networking

- Cross Over Cables
- Hubs
- Bridges
- Switches
  - MAC address table
- Broadcast Storms

Layer 3 Networking

- Connecting Multiple Networks Together
- LAN, WAN, CAN, MAN, Internet
- Routers
- Routable Protocols - TCP/IP v4, TCP/IP v6, IPX/SPX

TCP/IP v4 - Routable Protocol Suite

- Protocol Suite
- TCP - Transmission Protocol
- IP - Addressing Protocol
- ICMP - Ping

TCP/IP Address and Subnet Mask

- 192.168.1.1
- 192.166.1.1/24
- An IP Address contains the address for the Network and the Host
- Subnet Mask divides IP Address Into Network and Host Addresses
- A, B and C Subnets
- Scribble stuff on whiteboard about octets to impress students…
- Octet Value - 2 for number of hosts
  - Lower Number is Subnet, Higher is Broadcast

Private IP Address Blocks

Non Internet Routable

Private IPv4 addresses [edit]

The Internet Engineering Task Force (IETF) has directed the Internet Assigned Numbers Authority (IANA) to reserve the following IPv4 address ranges for private networks:[1]:4

RFC 1918 name	IP address range	Number of addresses	Largest CIDR block (subnet mask)	Host ID size	Mask bits	*Classful* description[Note 1]
24-bit block	10.0.0.0 – 10.255.255.255	16 777 216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits	single class A network
20-bit block	172.16.0.0 – 172.31.255.255	1 048 576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits	16 contiguous class B networks
16-bit block	192.168.0.0 – 192.168.255.255	65 536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits	256 contiguous class C networks

Switches and ARP

- Switches are layer 2 networking
- Switches contain MAC Address Tables
- ARP - Address Resolution Protocol - Resolves MAC address to IP Address
- Example - Run: arp -a

TCP Ports

- 192.168.1.1:8080
- Every Protocol uses a TCP Port.
- These are generally preconfigured, but can be manually set.
- SMTP - 25
- HTTP - 80
- HTTPS - 443
- FTP - 20
- SSH - 22

Routers and Default Gateways

- Routers Connect Networks Together
- The Default Gateway is the Router a Host communicates with is a computer cannot be found on the LAN

Modems

- Modems Change Network Types
- Cable Modem -> Ethernet
- Fiber Optic Modem -> Ethernet

NAT and Port Forwarding

Network Address Translation

- NAT Killed IPv6…
- Numerous Connected Devices can share the same External IP Address. The NAT Enabled Router will automatically route traffic to appropriate Hosts.
- Port Forwarding forwards inbound TCP Port Traffic to Specific Hosts
- BEWARE - Carrier NAT…

Internet Facing Static IP Addresses

- Server is “directly” connected to the Internet
- No need for Port Forwarding
- May cost extra money
- May be limited or not available from vendor
  - Many ISP’s will sell no, or limited static IP Addresses to customers

Firewalls

- Block TCP Ports
- Inbound/ Outbound
- Hardware / Software
- Servers should be configured so only specific Hosts can connect on specific TCP Ports
- BE CAREFUL configuring Software Firewalls on test systems…
  - Verify your setup works BEFORE implementing firewalls

DNS

Domain Name Service

- Resolves Fully Qualified Domain Names (FQDN’s) to IP Addresses
- SERVER -> 192.168.1.10
- cnn.com -> 151.101.3.5
- Resolution Order
  - Hosts File
  - Local DNS
  - Remote DNS (ISP, CloudFlare, Google)
- Reverse DNS resolves IP Addresses to FQDN’s to Prevent Spoofing

DHCP

Dynamic Host Configuration Protocol

- Dynamic IP Addresses
- Scope - Pool of IP Addresses that DHCP can assign from
- Lease Length - How long before Lease Expires
- Reserved Addresses /Static Addresses - Addresses reserved for devices that will have IP Addresses that will not change. For networking equipment, possibly printers, infrastructure servers…
- DHCP and DNS servers should talk to each other, generally they will be the same server.
- Use FQDN's where possible in code so that if the Server IP changes it will be seamless with a DNS update.

VPN

Virtual Private Network

- Creates a Tunnel from a computer External to a LAN to make it logically appear on the LAN.
  - Allows you to use local file servers, networked printers, etc.
  - Creates major vulnerabilities if VPN account is compromised
  - Flaky ISP Connections can cause major issues
- Generally used to bypass geo restrictions to access restricted content on Netflix.
- In your project if you collect IP Address information what you receive will be from VPN provider, not the actual users external address.

Command Line Tools

- ping
- arp -a
- traceroute
- ifconfig /ipconfig/ ip address

Labs

- lab-mac.py
  - Uses REST API to find Vendor of MAC Address
- lab-mac-arp.py
  - Grabs response from “arp -a” for a list of MAC addresses and then uses REST API to show vendors for all of them
- lab-ping.py
  - Uses OS module to Ping IP Addresses in List and Print Results
- lab-ping-loop.py
  - Pings a list of IP Addresses and shows latency in a continuous loop