Kevin Chen

11/24/16

IP Addressing Notes

Numbering Systems

* 1101 is a decimal number, 0x1101 indicates a hexadecimal number, and ob1011 indicates a binary number

Understanding Addressing

* Physical Addressing
  + The actual physical address assigned to a device. It is set at the factory. Often referred to as MAC address. MAC address is esp. relevant to Ethernet.
  + Basic MAC addressing: hexadecimal, 48-bits long. 2 parts: first part is the Organizationally Unique Identifier (OUI) (24 bits long, specific to the manufacturer of the device. Needs to be registered by manufacturers) and second part is the host portion (24 bits long, changes for each MAC address made. No two devices on same network cannot share same MAC address).
  + Variations on Basic MAC Address: EUI-60 (MAC address is 60 bits long – OUI is 24 bits long, host portion is 36 bits long), EUI-64 (MAC address is 64 bits long – OUI is 24 bits long, host portion is 40 bits long. It is able to work with IPv6 to create IPv6 addresses).
  + Routers and computers have MAC address, but switches don’t (they take the MAC address of whatever device it is connected to).
  + Segments can be formed: one switch connecting computers to a router’s interface. Two routers connected directly to each other also form a switch. Segments can also be formed between just switches without a router being involved.
* Logical Addressing
  + All devices on a network need a unique logical address
  + Logical address is determined by the Network Layer Protocol being used. Almost all modern networks use TCP/IP so logical address often is an IP address.
  + IP addresses can be entered manually or automatically. Manually = static IP addresses. Two methods to dynamically assign IP addresses: Dynamic Host Control Protocol (DHCP) (requires a server to use) and Automatic Private Internet Protocol Addressing (APIPA) (only usable by MSFT OS. Most MSFT OS failover to APIPA if no other addressing is available. Many routers and switches intended for home users use APIPA as a default setting.)
  + The zero at the end of an IP Address indicates the IP Address is a Network Address. When you assign a Network Address to a segment, that segment becomes a network or subnetwork. Then you can assign unique host IP addresses to each interface within the segment.
* How Logical and Physical Addresses Work Together
  + One computer (A) wants to send a packet to another computer (B) on the network, but it doesn’t know how to get there. But it knows the source and destination IP addresses because the DNS server on the network told it those things. Computer A sends its packet to its default router/gateway by setting the source physical address to its own physical address and the destination physical address to the router’s physical address. Then sets source logical address to its own IP address, and sets the destination logical address to the logical address of the destination computer. Then releases the packet to the router, resulting in a hop. The router then analyzes the packet. If the destination IP address is not directly connected to the router, then it looks at the routing table to find out which router it needs to send it to to get the packet closer. The source physical address is then set to the interface the router received the packet from and the destination physical address is set to the interface the next router/device will receive the packet from. Logical address is not changed. Packet is sent, resulting in a hop. Process is repeated until Computer B receives the packet.
* Unicast/broadcast/multicast: ways that a computer can send out signals across a network
  + Unicast: One device sends a packet to only one other device. One-to-one communications. When switches are used, most network traffic is unicast.
  + Broadcast: One device sends a packet to all available devices on the network at the same time. One-to-everyone communications. Network-wide alerts sent out this way. When a system is first trying to find an IP address with DHCP, it uses this type of signal. When using hubs, most transmissions are of this type.
  + Multicast: one device sends a packet to a group of devices. One-to-many communications. Used to send out information only to the devices that need it. Video conferencing uses this type of communications.
* Broadcast Domains vs. Collision Domains
  + Broadcast Domains: all devices are able to receive a signal sent by another computer in the network. To be part of broadcast domain, the signal cannot have passed through a switch, router, or similar device.
  + Collision Domains: this happens when two or more devices are able to cause their signals to interfere with each other. When signals interfere with each other, it is called a collision. Devices connected in a bus topology create collision domains. They are not as much of an issue anymore because switches do not allow collisions to take place, and modern networks use different pair of wires for sending and receiving.

IPv4 Addressing

* Why IPV4 and the IPv4 Addressing Structure
  + Why IPV4: Even though there is IPv6, IPv4 is still widely used for local area networks. APIPA only works with IPv4.
  + IPv4 Address structure: address is 32-bits long, address broken into four 8-bit segments called octets. Each 8-bit octet is represented by its decimal equivalent value. Each octet is separated by a decimal point. w.x.y.z notation is used to represent each section of the IPv4 address, where w, x, y, and z are octets.
* IPv4 Classful Addresses
  + Originally IPv4 addresses separated into classes, but no longer use classful IP addressing. Classes: A, B, C, D, and E. A and B and C for general use, D for multicast use, E for experimental use.
  + Class A: Bits defining class: 0. (IP Address begins with a 0.) 8 bits for Network IDs. (Network w & Host x.y.z). Actual subnet mask: 255.0.0.0. network IDs available, Host IDs available. IP Address range: 0.0.0.0 to 127.255.255.255.
  + Class B: Bits defining class: 10. 16 bits defining subnet mask (Network w.x & Host y.z). Actual subnet mask: 255.255.0.0. 16536 network IDs available, host IDs available. IP Address range: 128.0.0.0 to 191.255.255.255.
  + Class C: Bits defining class: 110. 24 bits defining subnet mask (Nework w.x.y & Host z). Actual subnet mask: 255.255.255.0. network IDs available, host IDs available. IP address range: 192.0.0.0 to 223.255.255.255.
  + Class D: Bits defining class: 1110. Bits defining subnet mask, actual subnet mask, Network and Host IDs available are all undefined because they were never intended for general public use. IP Address range: 224.0.0.0 to 239.255.255.255
  + Class E: Bits defining class: 1111. Many things undefined just like Class D. IP Address range: 240.0.0.0 to 255.255.255.255
* IPv4 Classless Addressing
  + Type of IP addressing currently used. Network portion of address determined by subnet mask. Use CIDR notation to show subnet.
  + CIDR-Based Addressing: Stands for Classless Inter-Domain Routing. Generally starts with 24-bits for the network address prefix and 8 bits for the host ID. Looks like w.x.y.z/a where a is the prefix length or # of bits used for network ID.
* Reserved IP Address Ranges and Loopback.
  + Reserved IP addresses set aside by ICANN for specific uses. Loopback IP addresses are a set of reserved IP addresses that serve a specific function. They allow an interface to send a signal back to itself, which is useful for testing and setting up an interface that is not actually present but can be addressed.
  + Reserved IP Address Ranges. 0.\*, 10.\* (Class A Private Address Block), 127.0.0.1 to 127.255.255.255 (Loopback Address Range), 128.0.\*, 169.254.\* (Microsoft APIPA Reserved Range), 172.16-31.\* (Class B Private Address Block), 191.255.\*, 192.0.0.\*, 192.168.\* (Class C Private Address Block), 223.255.255.0 to 225.255.255.255.
* Private vs. Public Addressing and APIPA
  + Public addressing: any interface that needs direct Internet access is required to use a public address. Need to be registered with ICANN. Only registered public addresses are allowed direct access to the Internet. If an interface does not need direct access to the Internet, then a public IP address is not required. Can use Private IP address instead.
  + Private Addressing: only used inside a network that does not directly access the Internet. Certain ranges of IP address are predefined as private addresses by ICANN. Cannot be used to access Internet. Defined in RFC 1918. ICANN will never assign these IP addresses for public use. When building a private network, use one of the ranges defined as Private IP addresses.
  + APIPA: Created by MSFT for Windows 9x and higher. Uses IP address range 169.255.0.0/16. Uses subnet mask 255.255.\*. Used when Windows computer is set to automatically find an IP address and DHCP is not available.
* Subnetting with IPv4
  + What is subnetting: the process of breaking a larger network into smaller, more manageable networks. Can be done by breaking up a larger IP address range into smaller address ranges, which can be used in networks with smaller number of computers. Prevents wasting IP addresses when using small number of computers in a network.
  + Some Basic rules: cannot use first IP address in a range for a computer because it is the network address used to identify a specific network. Cannot use last IP address in a range for a computer because it is the broadcast address used to send a message that is intended for all devices on that particular network. When breaking up a larger IP address range into smaller ranges, cannot use the first and last IP ranges because first range is confused by the computer with network addresses and the last range is confused by the computer with broadcast addresses. If subnets are needed, it is usually the system admin’s job to determine what subnet ranges should be used.
* Default Routes and Gateway Settings
  + Default Routes: it is not practical to define all possible routes a computer could take to find resources on the Internet. It is more practical to define one route (the default route) that summarizes all the locations not on the local subnet, which is used gateway of last resort. Offloads responsibility of knowing all possible locations from the local computer to a router. IP address used by local computer to connect to the router is called the default route or gateway.
  + Default Gateway Settings: provides “next hop” destination for all destinations not located on the local network segment. If using DHCP, default gateway is configured on DHCP server and sent automatically. Can be configured manually.
* Subnet Mask and Subnet Mask Setting
  + Subnet mask: a special IP address used by the computer to determine what part of an IP address is for the network and what part is for the host.
  + Subnet mask setting: a setting in the network configuration that tells the computer what subnet mask to use for the interface.

IPv6

* Introducing IPv6
  + IPv4 is limited to 32-bit address system, so limited to total addresses, which is too small of an address space.
  + IPv6 has 128-bit address system, so total addresses.
  + Design advantages of IPv6 address space: designed for efficient address allocation, designed to reflect topology of the modern Internet, designed to accommodate 64-bit MAC addresses, allows flexibility in designing hierarchical addressing, allows flexibility in designing hierarchical routing
  + IPv6 described in RFC 3516.
* IPv6 Addressing Structure
  + 128-bit address divided in 16-bit boundaries or sections. Each section represented by a 4-digit hexadecimal number. Each adjacent block separated by a colon.
  + IPv6 addresses can be simplified under certain conditions. Example: if a boundary has more than 1 leading zero, then the zeros can be removed, but there still needs to be one digit left.
* Subnetting in IPv6.
  + IPv6 addresses normally have a minimum of a /48 prefix, so the first 48-bits of IP address is used for Network ID and remaining 80 bits are used for host IDs. RFC 4291 recommends using at least a /64 prefix. Only exception is loopback, which uses a /128 prefix.
  + Common to use the first 16-bits of IPv6 address after ISP prefix as site or network ID. ( possible IDs). It also changes the prefix to /80 if IPv6 address from ISP follows RFC 4291 recommendation of a /64 prefix.