- # Chapter 2 The Internet Address Architecture
- ## 2.1 Introduction
  - Every device connected to the internet has at least one IP address
  - devices used in private networks based on TCP/IP protocols also require IP addresses
  - when devices are attached to the global internet they are assigned addresses that must be coordinated so as to not duplicate other addresses in use on the network
  - for private networks, the IP addresses being used must be coordinated to avoid similar overlaps within the private networks
  - Groups of IP addresses are allocated to users and organizations
  - The recipients of the allocated addresses then assign addresses to devices
  - Internet service providers (ISPs) - provide both the addresses and the promise of routing traffic in exchange for a fee
- ## 2.2 Expressing IP Addresses
  - IPv4 -
    - most popular type addresses are often represented in so-called dotted-quad or dotted decimal notation
    - 32 bits long
  - IPv6 -
    - 128 bits long
    - a series of four hexadecimal numbers called blocks or fields separated by colons
    - IPv6 agreed upon standards
      - leading zeros of a block need not be written
      - blocks of all zeros can be omitted and replaced by the notation ::. This is can only be used once.
      - embedded IPv4 addresses represented in the IPv6 format can use a form of hybrid notation in which the block preceding the IPv4 portion of the address have the value ffff and the remaining part of the address is formatted dotted-quad
      - A conventional notation is adopted in which the low-order 32 bits of the IPv6 address can be written using dotted-quad notation. The IPv6 address ::0102:f001 is therefore equivalent to the address ::1.2.2401
    - can use brackets characters, [and], are used to surround the IPv6 address.
      - URL = IPv6 address -> Port number
    - RFC5952
      - imposes some rules to narrow the ranges of options while remaining compatible
        - Leading zeros must be suppressed
        - The :: construct must be used to its maximum possible effect (most zeros suppressed) If multiple blocks contain equal light runs of zeros, the first is replaced with ::.
        - The hexadecimal digits a through f should be represented in lowercase
- ## 2.3 Basic IP Address Structure
  - Due to large number of addresses it is convenient to divide the address space into chunks
  - IP addresses are grouped by type and size
  - IPv4
    - unicast addresses - chunks subdivided down to a single address and used to identify a single network interface of a computer attached to the Internet or to some private intranet
    - most of the IPv4 address space is unicast space
  - IPv6
    - most of the address space is not being used

- ## 2.3.1 Classful Addressing
  - Unicast
    - when Internet address structure was originally defined
      - every unicast IP address has a network portion, to identify the network on which the interface using the IP address was to be found
      - host portion, used to identify the particular host on the network given in the network portion
      - net number - some number of contiguous bits in the address
      - host number - the remaining bits after the net number in the address
  - Different networks might have different number of hosts and that each host requires a unique IP address
    - partitioning of the address space involved five classes
    - each class represented a different trade-off in the number of bits of a 32 bit IPv4 address devoted to the network
  - class structure (sometimes called glassful addressing structure)
    - used primary as a way of allocating unicast address blocks of different sizes to users
    - the partitioning into classes induces a trade-off between the number of available network numbers of a given size and the number of hosts that can be assigned to the given network
- ## 2.3.2 Subnet Addressing
  - subnet addressing - using subnet addressing a site is allocated a class A, B, or C network number, leaving some number of remaining host bits to be fourth allocated and assigned within a site
    - this site may further divide the host bit to be further allocated and assigned within a site
    - the site may further divide the host portion of its base address allocation into a subnetwork (subnet) number and a host number
    - subnet addressing adds one additional field to the IP address structure, but without adding any bits to its length
    - as a result a site administrator is able to trade off the number of subnetworks verus the number of hosts expected to be on each subnetwork without having to coordinate with other sites
  - Example
    - class B address might be “subnetted” a site in the Internet has been allocated a class B network number. The first 16 bits of every address the site will use are fixed at some particular number because these its have been allocated by a central authority
      - The last 16 bits can now be divided by the site network administrator as needs may dictate. In this example 8 bits have been chosen for the subnet number leaving 8 bits for the host number.
      - This particular configuration allows the site to support 256 subnetworks and each subnetwork may contain up 254 hosts
        - the first and last addresses for each subnetwork are not available
  - subnetwork structure is known only by hosts and routers where the subnetting is taking place
    - the remainder of the Internet still treats any address associated with the site just as it did prior to the advent of subnet addressing
- Subnet Masks
  - is an assignment of bits used by a host or router to determine how the network and subnetwork information is partitioned from the host information in a corresponding IP address

- subnet masks for IP are the same length as the corresponding IP addresses
- They are typically configured into a host or router in the same way as IP addresses either statically (typical for routers) or using a dynamic system such as Dynamic Host Configuration Protocol
- prefix length - the most common format for expressing masks that simply gives the number of contiguous 1 bits in the mask (starting from the left)
- masks are used by routers and hosts to determine where the network/subnetwork portion of an IP address ends and the host part begins
- Each bit in the mask is ANDed with each corresponding bit in the subnet mask
  - this is precisely the information required by the border router to determine to which subnetwork a datagram destined for the system with address 128.32.1.14 should be forwarded
  - Note again that the rest of the Internet routing system does not require knowledge of the subnet mask because routers outside the site making routing decisions based only on the network number portion of an address and not the combined network/subnetwork or host portions

- 2.3.4 Variable-Length Subnet Masks (VLSM)

- possible to use a different-length subnet mask applied to the same network number in different portions of the same site
- although doing this complicates address configuration management, it adds flexibility to the subnet structure because different subnetworks may be set up with different number of hosts
- VLSM
  - can be used to partition a network number into subnetworks with differing number of hosts on each subnet
  - example
    - three different subnet masks are used within the site to subnet the network
      - doing so provides for a different number of hosts on each subnet
    - the number of hosts is constrained by the number of bits remaining in the IP address that are not used by the network/subnet number
      - IPv4 /24 prefix allows 32 - 24 = 8 bits (256 hosts) /26 (64 hosts)
    - each interface on each and router depicted is now given both an IP address and a subnet mask, but the mask differs across the network topology

- 2.3.5 Broadcast Addresses

- IPv4 subnetwork a special address is reserved to be the subnet broadcast address
  - formed by setting the network/subnetwork portion of an IPv4 address to the appropriate value and all the bits in the Host field to 1
  - formed by Oring the complement of the subnet mask with the IPv4 address
- directed broadcast - A datagram using this type of address as its destination
  - such a broadcast can, at least theoretically, be routed through the internet as a single datagram until reaching the target subnetwork, at which point it becomes a collection of broadcast datagrams that are delivered to all hosts on the subnetwork
- special use address 255.255.255.255 is reserved as the local net broadcast also called limited broadcast which is never forwarded by routers
- broadcasts addresses are typically used with protocols such as UDP/IP or ICMP because these protocols do not involve two-party conversations as in TCP/IP

- 2.3.6 IPv6 Addresses and Interface Identifiers

- IPv6 addresses also have additional structure in additional to be longer than IPv4 addresses

- special prefixes indicate the scope of an address
  - the scope of an address refers to the portion of the network where it can be used
- node-local - the address can be used only for communication on the same computer
- link-local - used only among nodes on the same network link or IPv6 prefix
- global - internet wide
- IPv6 - most nodes have more than one address in use, often on the same network interface
  - not as common for IPv4
- Interface identifiers (IIDs) -
  - used a basis for unicast IPv6 assignment
  - used as the low-order bits of an IPv6 address in all cases except where the address begins with the binary value 000, and as such they must be unique within the same network prefix
  - ordinarily 64 bits long and are formed wither directly from the underlying link layer MAC address of a network interface using EUI-64 format, or by another process that randomizes the vale in hopes of providing some degree of privacy against address tracking
- Extended unique identifier (IEEE standards) - 24-bit Organizationally unique identifier followed by a 40-bit extension identifier assigned by the organization, which is identified by the first 24 bits.
- EUIs may be “universally administered” or “locally administered”
- OUI - 24 bits long and occupies the first 3 bytes of both EUI-48 and EUI-64 addresses
  - the low-order 2 bits of the first bytes of these addresses are designated the u and g bits, respectively
    - u bit - when set indicates that the address is locally administered
    - g bit - when set indicates that the address is group or multicast-type address
- EUI-64 from EUI-48
  - can be formed by copying the 24-bit OUI value from the EUI-48 address to the EUI-64 address, placing the value (hex FFFE) in the fourth and fifth bytes of the EUI-64 address, and then copying the remaining organization-assigned bits
  - this mapping is the first step used by IPv6 in constructing its IIDs when EUI-48 are address are available
  - modified EUI-64 used to form IIDs for IPv6 addresses simply inverts the u bit
- When an IPv6 IID is needed for a type of interface that does not have EUI-48-bit
  - the underlying address is left-padded with zeros to form the IID
  - IIDs created for interfaces that lack any form of other identifier may be derived from some other interface on the same node or from some identifier associated with the node.
  - Lacking any other options,, manual assignment is a last resort
- Tunnel endpoint - which is used to carry IPv6 traffic through networks that otherwise support IPv4
  - example
    - physical address is the hexadecimal encoding of IPv4 address
    - OUI used is the one assigned to IANA
    - Combination of IANA with the hex value fe (indicating an embedded IPv4 address) this combination is then combined with the standard link-local prefix fe80::/10
- Zone ID - windows indicates the interface index number on the computer corresponding to the IPv6 address

- 2.4 CIDR and Aggregation

- Scaling problems

- 1. 1994 over half of all the class B addresses had already been allocated
- 2. 32-bit IPv4 address was thought to be inadequate to handle the size of the Internet anticipated
- 3.Number of entries in the global routing table was growing and routing performance would suffer

- 2.4.1 Prefixes

- availability of IPv4 addresses
  - to help relieve the pressure classful addressing scheme was generalized using CIDR
  - Classless Inter-Domain Routing - provided a way to conveniently allocate contiguous address ranges that contained more than 255 hosts but fewer than 65,536
    - any address range is not predefined as being part of a class but instead requires a mask similar to a subnet mask, sometimes called CIDR mask
    - CIDR masks are not limited to a site but instead are visible to the global routing system
    - The core Internet routers must be able tot interpret and process masks in addition to network numbers
      - This combination of numbers, called a network prefix, is used for both IPv4 and IPv6 address management
- eliminating the predefined separation of network and host number within an IP address makes finer-grain allocation of IP address ranges possible
- dividing the address spaces into chunks is most easily achieved by grouping numerically contiguous addresses for use as a type or for some particular purpose
  - groupings now expressed using a n-bit prefix for the first n bits of an address
  - IPv4 n is in range 0-32
  - IPv6 n is in range 0-128
  - smaller prefix length corresponds to a larger number of possible addresses
- example
  - without prefix
    - 128.0.0.0
  - with prefix
    - 128.0.0.0/1

- 2.4.2 Aggregation

- routing table entry tells the router where to send traffic
- essentially
  - the router inspects the destination IP address in an arriving datagram, finds a matching routing table entry, and from the entry extracts the “next hop” for the datagram
- Network with a tree topology (Left (Random (location independent) addressing) \ Right (Topology Sensitive (location dependent) addressing))
  - addresses can be assigned in a special way so as to limit the amount of routing information (“state”) that needs to be stored in a router
  - if addresses are not assigned in this way (left side), shortest path routes cannot be guaranteed without storing an amount of state proportional to the number of nodes to be reached
  - while assigning addresses in a way that sensitive to the tree topology saves state
  - if the network topology changes, a reassignment of addresses is generally required
- Hierarchical routing - idea can be used in a specific way to reduce the number of Internet routing entries that would be required otherwise
- route aggregation - works by joining multiple numerically adjacent IP prefixes into a single shorter prefix that covers more address space

2.5 Special-Use Addresses

- IPv4 and IPv6 address spaces include a few address ranges that are used for special purposes
  - therefore they are not used in assigning unicast addresses
- For both if address ranges not designed as special, multicast, or reserved are available to be assigned for unicast use
  - some unicast address space is reserved for building private networks
- nonroutable addresses - that is, they will not be routed by the public Internet
- IPv4 private addresses
  - very common in home networks and for the internal networks of moderately sized and large enterprises
    - frequently used in combination with NAT
  - network address translation (NAT) - which rewrites IP addresses inside IP datagrams as they enter the Internet

2.5.1 Addressing IPv4/IPv6 Translators

- some networks it may be attractive to perform translation between IPv4 and IPv6
- framework has been developed for unicast translations, and one is currently underdevelopment for multicast translations
  - basic functions to provide automatic algorithmic translation
  - the scheme makes use of a specialized address format called an UPv4-embedded IPv6 address
    - contains the IPv4 address inside of the IPv6 address
    - encodes using one of the six formats, based on the length of the IPv6 prefix
    - the prefix is either well-known prefix or a prefix unique to the organization deploying translators
- method to produce a translation to produce IPv4-embedded IPv6 address
  - concatenate the IPv6 prefix with the 32-bit IPv4 address, ensuring that the bits 63-71 are set to 0 (inserting if necessary)
  - append the suffix as 0 bits until a 128-bit address is produced.

2.5.2 Multicast addresses

- supported by IPv4 and IPv6
- IP multicast address - called a group or group address
  - identifies a group of host interfaces, rather than a single one
  - the group can span the entire Internet
- scope - the portion of the network that a single group covers
  - node-local - same computer
  - link-local - same subnet
  - site local - applicable to some site
  - global - entire Internet
  - administrative - may be used in an area that has been manually configured into routers
    - admin-scope boundaries - meaning that multicast traffic of the associated group is not forwarded past the router
  - site-local and administrative scopes are available for use only with multicast addressing
- software control
  - the protocol stack in each Internet host is able to join or leave a multicast group
  - when a host sends something to a group, it creates a datagram using one of its own (unicast) IP addresses as the source address and a multicast IP address as the destination
  - all hosts that have joined the group should receive any datagrams sent to the group

- the sender is not generally aware of the hosts receiving/ how many are receiving the datagram unless they explicitly reply
- any-source multicast (ASM)
  - any sender may send to any group
  - a receiver joins the group by specifying only the group address
- source-specific multicast (SSM)
  - uses only a single sender per group
  - when joining a group a host specifies the address of a channel, which comprises both a group address and a source IP address

- 2.5.3 IPv4 Multicast Addresses

- class D space reserved for supporting multicast
  - 28 bits free supports 2^28 hosts
- the blocks of addresses up to 224.255.255.255 are allocated for the exclusive use of certain application protocols or organizations
- the local network control block
  - is limited to the local network of the sender; datagrams sent to those addresses are never forwarded by the multicast routers
- internetwork control block
  - similar to the local network control range but is intended for control traffic that needs to be routed off the local link
    - ex. Network Time Protocol (NTP)
- first ad hoc block was constructed to hold addresses that did not fall into either the local or internetwork control blocks
  - most of the allocations in this range are for commercial services, some which do not (or never will) require global address allocations; they eventually be returned in favor of GLOP addressing
  - SDP/SAP block contains addresses used by applications such as the session directory tool (SDR) that send multicast session announcements using Session Announcement Protocol (SAP)
  - Session Description Protocol (SDP) is now used not only with IP multicast but also with other mechanisms to describe multimedia sessions
- SSM block is used by applications employing SSM in combination with their own unicast source IP address in forming SSM channels
- GLOP block multicast addresses are based on the autonomous system (AS) number of the host on which the application allocating the address resides
  - addresses are generated by placing a 16 bit AS number in the second and third bytes of the IPv4 multicast address
  - leaving room for 1 byte to represent the possible multicast addresses
- unicast-prefix-based (UBM) - the most recent of the IPv4 multicast address allocation mechanisms associates a number of multicast addresses with an IPv4 unicast address prefix
  - a unicast address allocation with a /24 or shorter prefix may make use of UBM addresses
    - allocations with fewer addresses must use some other mechanism
  - UBM addresses are constructed as a concatenation of the 234/8 prefix, the allocated unicast prefix, and the multicast group ID
- The IPv4 UBM address format. For unicast address allocations of /24 or shorter, associated multicast addresses are allocated based on a concatenation of the prefix 234/8, the

assigned unicast prefix, and the multicast group ID. Allocations with shorter unicast prefixes therefore contain more unicast and multicast addresses

- It is possible to determine the owner of a multicast address by simply “left shifting” the multicast address by 8 bit positions
- advantages
  - they do not carry the 16-bit restriction for AS numbers used by GLOP addressing
  - they are allocated as a consequence of already-existing unicast address space allocations
- Large sites sometimes subdivide administratively scoped multicast addresses to cover specific useful scopes (e.g. work group, division, and geographical area)

- 2.5.4 IPv6 Multicast Addressees

- more aggressive in its use of multicast
- the prefix ff00::/8 has been reserved for multicast addresses
- 112 bits are available for holding the group number, providing the possibility of 2^112 groups
- multicast format
  - includes 4 flag bits
    - 0
    - reserved R contains rendezvous point;
    - P, uses unicast prefix
    - T is transient
  - 4-bit Scope ID field in the second nibble
    - used to indicate a limit on the distribution of datagrams addressed to certain multicast addresses
  - The group ID is encoded in the low-order 112 bits
  - If P or R bit is set, an alternative format is used
- many IPv6 multicast addresses allocated by the IANA for permanent use intentionally span multiple scopes
  - each of these is defined with a certain offset relative to every scope
    - called scope-relative or variable-scope
- format given in figure 2 is used when the P and R bit fields are set to 0
- when P is set to 1, two alternative methods exist for multicast addresses that do not require global agreement on a per-group basis
  - unicast-prefix-based - multicast address assignment, a unicast prefix allocation provided by an ISP or address allocation authority also effectively allocates a collection of multicast addresses, thereby limiting the amount of global coordination required for avoiding duplicates
  - link-scoped IPv6 multicast - IIDs are used and multicast addresses are based on a host IID
- T bit field when set indicates that the included group address is temporary or dynamically allocated
- P bit field is set to 1, the T bit must also be set to 1
  - when this happens a special format of IPv6 multicast addresses based on unicast address prefixes is enabled
  - changes the format of the multicast address to include space for a unicast prefix and its length, plus a smaller (32-bit) group ID
  - purpose of this scheme is to provide a way of allocating globally unique IPv6 multicast addresses without requiring a new global mechanism for doing so

- IPv6 unicast addresses are already allocated globally in units of prefixes it is possible to use bits of this prefix in multicast addresses, thereby leveraging the existing method of unicast address allocation for multicast use

- IPv6 link-scoped multicast address format
  - applicable only to link- (or smaller) scoped addresses, the multicast address can be formed by combining an IPv6 interface ID and a group ID. The mapping is straightforward, and all such addresses use prefixes of the form ff3x:001/32 where x is the scope ID and is less than 3
  - similar to the previous figure address
    - changes
      - prefix length field is set to 255, and instead of a prefix being carried in the subsequent field, an IPv6 IID is instead
      - the advantage over the previous structure is that no prefix need to be supplied in forming a multicast address
- In ad hoc networks where no routers may be available an individual machine can form unique multicast addresses based on its own IID without having to engage in a complex agreement protocol
  - this format works only for link- or node-local multicast scoping
  - when larger scopes are required, either unicast-prefix-based addressing or a permanent multicast addresses are used
- R bit - used when unicasting prefix-based multicast addressing is used (the P bit is set) along with a multicast routing protocol that requires knowledge of a rendezvous point
- rendezvous point (RP) is the IP address of a router set up to handle multicast routing for one or more multicast groups.
  - RPs are used by the PIM-SM protocol to help senders and receivers participating in the same multicast group to find each other.
  - One of the problems encountered in deploying Internetwide multicast has been locating rendezvous points. This scheme overloads the IPv6 multicast to include an RP address. Therefore, it is simple to find an RP from a group address by just selecting the appropriate subset of bits.
- The unicast IPv6 address of a RP can be embedded inside of an IPv6 multicast address. Doing so makes it straightforward to find an RP associated with an address for routing purposes. An RP is used by the multicast routing system in order to coordinate multicast senders with receivers when they are not on the same network.
- As with IPv4, there are a number of reserved IPv6 multicast addresses. These addresses are grouped by scope, except for the variable-scope addresses mentioned before

- 2.5.5 Anycast Addresses

- anycast address is a unicast IPv4 or IPv6 address that identifies a different host depending on where in the network it is used
  - this is accomplished by configuring Internet routers to advertise the same unicast routes from multiple locations in the Internet routers to advertise the same unicast routes from multiple locations in the Internet

- 2.6 Allocation

- IP address space is allocated usually in large chunks, by a collection of hierarchically organized authorities
- Top of hierarchy is the IANA - which has wide-ranging responsibility of allocating IP addresses and other types of numbers used in the Internet protocols

- 2.6.1 Unicast

- provider-aggregatable (PA) - addresses because they consist of one ore more prefixes that can be aggregated with other prefixes the ISP owns. Such addresses are also sometimes called non-portable addresses.
- switching providers typically requires customers to change IP prefixes on all computers and routers they have that are attached to the Internet (called renumbering)
- provider-independent (PI)
  - allocated directly to the user and may be used with any ISP
  - not aggregatable

- Multicast
  - IPv4 and IPv6 multicast addresses can be described based on their scope, the way they are determined (statically, dynamically by agreement, or algorithmically), and whether they are used for ASM or SSM
  - guidelines have been constructed for allocation of these groups
  - groups that are not of global scope can be used in various parts of the Internet and are either configured by a network administrator out of an administratively scoped address block or selected automatically by end hosts
  - Globally scoped addresses that are statically allocated are generally fixed and may be hard-coded into applications
  - algorithmically determined globally scoped addresses can be created based on AS numbers, as in GLOP, or an associated unicast prefix location
    - SSM can use globally scoped addresses, administratively scoped addresses, or unicast-prefix based IPv6 addresses where the prefix is effectively zero

- 2.7 Unicast Address Assignment

- once a site has been allocated a range of IP addresses, typically from its ISP, the site or network administrator must determine how to assign addresses in the address range to each network interface and how to set up the subnet structure
- single physical network process is relatively straightforward (e.g. private homes)
- Larger enterprises receiving service from multiple ISPs and that use multiple physical network segments distributed over a large geographical area, this process can be complicated

- 2.7.1 Single Provider/No Network/Single Address

- simplest type of Internet service that can obtained today is to receive a single IP address from an ISP to be used with a single computer
- DSL
  - single address might be assigned as the end of a point-to-point link and might be temporary
  - example
    - computer connects to Internet using DSL, it might be assigned the address … on a particular day
    - any send carries the source IPv4 address
    - Host this simple has other active IP addresses as well. These include the local “loopback” address and some multicast addresses, including, at a minimum, the All Hosts multicast address
    - If the host is running IPv6 at a minimum it is using the All Nodes IPv6 multicast address (ff02::1)

- 2.7.2 Single Provider/Single Network/Single Address

- router forwards packets from the home network to the ISP and also performs NAT by rewriting the IP addresses in packets being exchanged with customer’s ISP
  - from the ISP point of view only a single IP address has been used

- The routers provide automatic address assignment to the home clients using DHCP
- They also handle address assignment for the link set up with the ISP if necessary

- 2.7.3 Single Provider/Multiple Networks/Multiple Addresses

- a site has been allocated the prefix 128.32.2.64/26 providing up to 64 (minus 2) routable IPv4 addresses.
- The “DMZ” network (“demilitarized zone” network, outside the primary firewall) is used to attach servers that can be accessed by users on the Internet. Such computers typically provide Web access, login servers, and other services.
- These servers are assigned IP addresses from a small subset of the prefix range; many sites have only a few public servers. The remaining addresses from the site prefix are given to the NAT router for the basis for “NAT pool”
- The router can rewrite datagrams entering and leaving the internal network using any of the addresses in its pool.
- Figure description
  - A typical small to medium-size enterprise network. The site has been allocated 64 public (routable) IPv4 addresses in the range …/26. A “DMZ” network holds servers that are visible to the Internet. The internal router provides Internet access for computers internal to the enterprise using NAT

- 2.7.4 Multiple Providers/Multiple Networks/Multiple Addresses (Multihoming) ?

- Some organizations that depend on Internet access for their continued operations attach to the Internet using more than one provider (called multihoming) in order to provide redundancy in case of failure, or for other reasons.
- Example
  - Site S has two ISPs, P1 and P2
  - If it uses PA address space from P1’s block (12.46.129.0/25), it advertises this prefix at points C and D to P1 and P2, respectively. The prefix can be aggregated by P1 into its 12/8 block in advertisements to the rest of the Internet at point A, but P2 is not able to aggregate it at point B because it is not numerically adjacent to its own prefix
  - In addition from the point of view of some host in the other parts of the Internet, traffic for 12.46.129.0/25 tends to go through ISP P2 rather than ISP P1 because the prefix for site S is longer than when it goes through P1
  - This is a consequence longest matching prefix algorithm works for Internet routing
  - In essence, a host in the other parts of the Internet could reach the address … via either a matching prefix matches, the one with the larger or longer mask is preferred which in this case is P2

- Attacks Involving IP Addresses
  - IP addresses are essentially numbers, few network attacks involve only them
  - Generally attacks can be carried out when sending “spoofed” datagrams or with other related activities
  - IP addresses are being used to identify individuals that are suspected of undesirable activities
    - Can be misleading for several reasons
      - IP addresses are only temporary
      - attach to the internet through some open source

- 2.9 Summary

- IP address is used to identify and locate network interfaces on devices throughout the Internet System (unicast addresses)

- May also be used for identifying more than once such interface (multicast, broadcast, or anycast addresses)
- Each interface has a minimum of one 32-bit IPv4 address and usually has several 128-bit addresses if using IPv6
- Unicast addresses are allocated in blocks by hierarchically structured set of administrative entities
- Prefixes allocated by such entities represent a chunk of unicast IP address space typically given to ISPs that in turn provide addresses to their users
- Numerically adjacent address prefixes (PA addresses) can be aggregated to save routing table space and improve scalability of the Internet
  - approach arose when the Internet's "classful" network structure consisting of class A, B, and C network numbers was abandoned in favor of classless inter-domain routing (CIDR).
  - CIDR - allows for different sizes of address blocks to be assigned to organizations with different needs for address space; essentially CIRD enables more efficient allocation of address space
- Anycast addresses are unicast addresses that refer to different hosts depending on where the sender is located; such addresses are often used for discovering network services that may be present in multiple locations.
- IPv6 addresses have a scope concept, for both unicast and multicast addresses an indicates where an address is valid
  - node-local
  - link-local - are often created based on a standard prefix in combination with an IID that can be based on addresses provided by lower-layer protocols (such as hardware/MAC addresses) or random values
  - global
- Both IPv4 and IPv6 support addressing formats that refer to more than one network interface at a time
- Broadcast and multicast supported in IPv4, but multicast only in IPv6
- Broadcast allows for one-to-all communication
- multicast allows for one-to-many communication
- Senders send to multicast groups (IP addresses) that act somewhat like television channels
  - sender has no direct knowledge of the recipients of its traffic or how many receivers there are on a channel
- Global multicast in the Internet has evolved over more than a decade and involves many protocols—some for routing, some for address allocation and coordination, and some for signaling that host wishes to join or leave a group
- Many types of IP multicast addresses, both in IPv4 and IPv6
  - variants of the IPv6 multicast address format provide ways for allocating groups based on unicast prefixes embedding routing information (RP addresses) in groups, and creating multicast addresses based on IIDs