RECAP/

IPv4 Unicast, Broadcastm and Multicast

Unicast

**One-to-one communications**

Unicast packet has   
 destination IP address that is a unicast address which goes to a single recipient

Source IP address can only be a unicast address bcs the packet can only originate from a single source

The IPv4 unicast addresses are in the range of 1.1.1.1 to 223.255.255.255

Broadcast

**One-to-all communications**

Broadcast packet has

Destination IP address with all ones (1s) in host partition, or 32 one (1) bits

This packet must be processed by all devices in the same broadcast domain

It may be **directed**

Is sent to all hosts on a specific network

or

**limited**

Is sent to 255.255.255.255

Multicast

Reduces traffic by allowing a host to send a single packet to a selected set of hosts that subscribe to a multicast group

Multicast packet has

Destination IP address that is a multicast group  
 (IPv4 has reserved the 224.0.0.0 to 249.255.255.255 for this)

When an IPv4 host subscribes to a multicast group, the host processes packets addressed to this multicast address, and packets addressed to its uniquely allocated unicast address

Types of IPv4 addresses

Public IPv4

Addresses which are globally routed between ISP routers  
 BUT NOT ALL ADDRESSES CAN BE USED

Private addresses   
 they are blocks of addresses that are used by most organiztions to assign IPv4 addresses to internal hosts

**They are not globally routable   
 before ISP can forward this packet, it must translate the source IPv4 address, which is a private address, to a public IPv4 address using NAT**

**Loopback addresses 127.0.0.0/8 or 127.0.0.1 to 127.255.255.254**

Are commonly identified as only **127.0.0.1**

These special addresses are used by host to direct traffic to itself

**Link-local addresses (169.254.0.0/16 or 169.254.0.1 to 169.254.255.254)**

Commonly known as the **Automatic Private IP addressing (APIPA) addresses**

Used by windows DHCP client to self-configure in the event that there are no DHCP

1981, RFC 790

Class A (0.0.0.0/8 to 127.0.0.0/8)

Extremely large network (16Mil and smt)

Class B (128.0.0.0/16 to 191.255.0.0/16)

Moderate to large size networks (about 65k hosts)

Class C (192.0.0.0/24 to 223.255.255.0/24)

Small networks with maximum of 254 hosts

Public IPv4 addresses are addresses which are globally routed over the internet.

Public IPv4 addresses must be unique.

Both IPv4 and IPv6 addresses are managed by the IANA.

The IANA manages and allocates blocks of IP addresses to the RIRs.

RIRs are responsible for allocating IP addresses to ISPs who provide IPv4 address blocks to organizations and smaller ISPs. Organizations can also get their addresses directly from an RIR.

Network segments

In an Ethernet LAN, devices use broadcasts and ARP to locate other devices.

ARP sends Layer 2 broadcasts to a known IPv4 address on the local network to discover the associated MAC address.

Devices on Ethernet LANs also locate other devices using services.

A host typically acquires its IPv4 address configuration using DHCP which sends broadcasts on the local network to locate a DHCP server.

Switches propagate broadcasts out all interfaces except the interface on which it was received.

A large broadcast domain is

a network that connects many hosts.

A problem with a large broadcast domain is

that these hosts can generate excessive broadcasts and negatively affect the network.

The solution is

to reduce the size of the network to create smaller broadcast domains in a process called subnetting.

These smaller network spaces are called subnets.

The basis of subnetting is to use host bits to create additional subnets.

Subnetting reduces overall network traffic and improves network performance. It helps administrators to implement security policies such as which subnets are allowed or not allowed to communicate together.

It reduces the number of devices affected by abnormal broadcast traffic due to misconfigurations, hardware/software problems, or malicious intent.