Subnets, NAT, and Routing

Josh Wilcox (jw14g24@soton.ac.uk)

April 12, 2025

Contents

1 Subnets

1.1 Available Addresses in an IPv4 subnet

- Not all addresses are usable
  - First address is reserved
  - Last address is the broadcast address
  - One address is required for the router
- For example: 152.78.70.0/24 will have **253** available addresses
  - 152.78.70.0 will be reserved
  - 152.78.70.255 will be used as the broadcast address
  - Another will be used for the router

1.2 Example

- Allocation: 152.78.70.0/23
- Requirement: Three subnets
  - One subnet with 200 devices
  - Two subnets with 100 devices each
- Calculation:
  - For 200 devices, a /24 subnet is needed (254 addresses)
  - For 100 devices, a /25 subnet is needed (126 addresses)
- Subnet Allocation:
  - 152.78.70.0/24 for 200 devices
  - 152.78.71.0/25 for 100 devices
  - 152.78.71.128/25 for 100 devices

1.3 RFC1918

- RFC 1918 *private addresses* can be used for private networks and are not globally routable
  - 10.0.0.0/8, 16 million addresses
  - 172.16.0.0/12, 1 million addresses
  - 192.168.0.0/16, 65k addresses
- These addresses are commonly used in home, office, and enterprise networks
- Devices using private addresses communicate with the internet through a NAT (Network Address Translation) device
- Benefits of using private addresses:
  - Conserves global address space
  - Enhances security by hiding internal network structure
- Limitations:
  - Cannot be used for direct communication over the internet
  - Requires NAT for internet access

2 Network Address Translation

- NAT is primarily used for IPv4, not needed for IPv6 due to the larger address space
- It works by sharing a global IPv4 address among multiple hosts
- The source address of outgoing packets is modified based on the NAT configuration
- NAT modifies the source IP address of outgoing packets and the destination IP address of incoming packets
- Types of NAT:
  - **Static NAT**: One-to-one mapping between local and global addresses
  - **Dynamic NAT**: Maps a local address to a global address from a pool of available addresses
  - **PAT (Port Address Translation)**: Also known as *NAT overload*, it maps multiple local addresses to a single global address using different ports
- Benefits of NAT:
  - Conserves the number of public IP addresses needed
  - Adds a layer of security by hiding internal IP addresses
- Limitations of NAT:
  - Can complicate protocols that embed IP addresses in the payload
  - May introduce latency due to address translation

3 Routing

How does a network know how to get packets between two hosts in different networks?

3.1 Netmasks

- Addresses that fall outside of the same netmasks requires a router to talk b etween them

3.2 IP Routing

- Occurs when there is a *change* in IP address space
- A router has an IP address in each address space it **handles routing**
- There can be many routers between hosts
  - Jumping between multiple routers are known as hops
  - Parts of the IP header are rewritten at each hop

3.3 View from a Host

- From the POV of a host, it just needs to know where to send a packet
  - Can be direct sending on a local subnet - will never go near a router
  - Or it will forward it to a router
- Hosts are uually unaware of routers beyond their own subnet
- Hosts can have multiple possible routers

3.4 Routing Tables

- Every host on the network will have a routing table
- May be built from DHCP or IPv6 Router Advertising
- Very small for most hosts - including:
  - Contains destination IP prefixes and the interface or next hop to use
  - The local subnet that the host is connected to
  - A catchall **default route**
- Uses a set of rules that matches routes to destinations
- The most specific matching route is picked first
  - E.g. the route with the longest prefix
- Metric - Determines the best path for sending network traffic when multiple routes to the same destination exist.
  - **Choose Lower Metrics on the table**

3.5 Prefix Aggregation

- In principle, all routers would need to know the presence of every subnet on the Internet
  - Very expensive and nasty
- In practice, this is not needed
  - A subnet's prefix can be aggregated with other adjacent subnets
    * 192.168.10.0/24 and 192.168.11.0/24 can be aggregated to 192.168.10.0/23
- Allows organisations to only advertise one route for its entire address space

3.6 Beyond the default router

- IP packets not delivered locally are sent via the default router
- This router needs to know where to send the packet next
  - Could be very large and subject to frequent changes
  - Manual configuration may not be feasible
- Manually configuring these tables would be a nightmare

4 Autonomous Systems

- An AS is a large network or group of networks that has a **unified routing policy**
- The internet is made of interconnected Autonomous Systems
- Each AS is assigned an Autonomous System Number (ASN) by the same bodies that allocate IPs

5 Routing Protocols

- Allows routers to build and exchange routing information automatically
- Different protocols are used for different systems

5.1 Interior Gateway Protocol

- Used within an AS
- Uses **Distance Vectors**
  - Talks only to directly neighbouring routers
  - Exchange best routes based on distance for any know prefixes
- **Link State**
  - Talks to all routers to establish full knowledge of the routers on a site

5.2 Routing Information Protocol (RIP)

- Router sends its whole routing table periodically to directly connected routers
- Desitnation network (prefix) and distance (cost) are included
- Receiving routers update their view of the best route to a given network
- Every router gets a view of how to get everywhere else

5.2.1 Limitations

- Updates only sent around every 30 seconds
- Updates are not acknowledged (it is UDP)
- Metrics are simple hop count values and have a max value of 15
  - Could be a satellite link or have massive packet loss and they would never know
- Routers don't have knowledge of network topology

5.3 Link State Routing

1. Discover neighbours and determine cost metric
2. Flood message with this information to all routers
3. Use received messages to build topology
   - Compute shortest paths for prefixes serverd by any router

- Messages are sent periodically, or any time a change in connectivity is detected
- Both ends of a link must agree for it to be valid
- All routers learn the full network topology
- Discovering neighbours is more streamlined than RIP

6 Routign Between Sites - Exterior Routing Protocols

- Advertise network prefixes to neighbouring *networks*
- May or may not offer transit to other networks
- *Policy* is often more important thatn path costs

6.1 Border Gateway Protocol

- BGP is used to exchange routing information between different Autonomous Systems (AS).
- In configuration, specify the IP of a neighbor and its AS, e.g., on Cisco:

```
neighbor FE80::1234:BFF:FE0E:A471% remote-as 64600
```

- BGP establishes a peering session over TCP (port 179).
- At session start, the full routing table is sent, with later sessions using incremental UPDATE messages.
- Advertised routes include:
  - Network prefix and prefix length
  - AS path and next hop
- Filtering is applied on both advertised and received routes; neighbors choose which routes to accept.
- The AS path attribute enables loop detection by verifying that a route does not include the local AS.

6.2 Downsides of BGP

- BGP relies heavily on trust between peers; a malicious or misconfigured peer can propagate erroneous routing information, leading to network instability.
- BGP convergence is slow:
  - Updating BGP routing tables takes significant effort, partly due to the default KEEPALIVE period of 60 seconds and a HOLDDOWN timer of 180 seconds.
  - Rapid link fluctuations can cause route flapping, further destabilizing the network.
- Routers have limited BGP routing table capacities:
  - Older hardware may only support around 1 million IPv4 routes and approximately 128k IPv6 routes.
  - The expansion of the Internet and the constraints imposed by IPv4 exhaustion are pushing these limits.