IP Datagram Format

There are 20 (or more with options) bytes in the header, giving a 20-byte overhead on any IP datagram, no matter the size.

- The first field a router reads is the version number, so it can tell how to read the rest of the header.
- Uses the header length field to tell if there are options in use.
- The "type of service" field tells whether the packet is important and should be given priority
- TTL is used to prevent packets going in loops – routers decrement the value every time, once it gets to 0 the packet gets dropped.
  - Can be used to restrict scope of packets (how far they go)
- IP addresses limited to 2^32 because of size of fields
  - Source address can be used for *ingress filtering* – suppressing packets that claim they're coming from somewhere that doesn't make sense

Fragmentation / Reassembly

Fragmentation is a feature of IPv4 that accounts for link layer protocols supporting smaller message sizes. Link layer protocols may be heterogeneous, which is why we need to account for this.

Packets are broken up into multiple packets to get them down to the right size, and reassembled at the destination.

Each packet gets a new header, with the same ID as the large packet that's being broken up. The packets are also given an offset value, to show the order they go in. The offset is measured in 8-byte chunks (185 = 1480 bytes).

In IPv6, there's a minimum MTU that every link has to be above, and there's a way to check the minimum MTU between a source and destination – this saves the 32 bits in the header related to fragmentation.

IP Addressing

Intro

An IP address identifies a particular subnetwork, and a device on that network (e.g. UCC and then a specific machine).

Structured addresses like this have a few benefits:

- Working with the numbers is easier (e.g. UCC can be responsible for allocating numbers within their subnet)
  - Without a structure allocation would require a single authority that everyone would need to contact.
  - Finding particular IPs would require flooding the network by asking every device if they know where the IP is.

Technically different network interfaces have different IP addresses, so one machine can have multiple addresses (e.g. routers).

Subnets

All devices on a subnet share an IP prefix. A subnet is where devices can communicate directly, rather than through a router.

One interface of a router connecting some subnets sits on each subnet.

Class-Based Addressing

- need to know why it was abandoned
  - difficulty with efficiency of allocating addresses

CIDR (Classless InterDomain Routing)

The subnet portion of an IP address is no longer a fixed length – the length is specified along with the IP.

Getting an IP Address

In the past, addresses were manually hardcoded, and provided by network admins according to which ones they knew were free.

Nowadays, DHCP is used, which is where devices dynamically get addresses from the server.

DHCP

Devices lease addresses from the server, so the server can reclaim addresses over time if they're no longer used.

DHCP protocol contains 4 types of message:

- DHCP discover (optional)
  - "Is there a DHCP server out there?"
- DHCP offer (optional)
  - "You can use this address"
- DHCP request
  - "I would like to use this address"
- DHCP ack
  - "Confirmed. The address is yours"

Sidebar: Broadcasting

You can deliver a message to a special address which means the message should be delivered to every interface on the local network.

They can be used for finding the DHCP server.

Other DHCP Info

DHCP server also tells a client the IP of the first-hop router on the path out of the network, as well as the name and IP of the local DNS nameserver, and the network mask, which tells which portion of the IPs is for the local network.

DHCP is application layer and nearly always runs on UDP.

DHCP must also do access control – decide whether it'll give a computer access to the network.