THE INTERNET PROTOCOL (IP)

One of the fundamental concepts in the Network Layer of TCP/IP model is the format of the IP packet. It has a header part, at most 60 bytes long, out of which the first 20 bytes are required and have predefined fields. Remaining 40 bytes are optional. Theses bytes must be used in multiples of 4 bytes. The header is followed by a data part (payload). The total length of the header + data must not exceed 65535 (216 – 1) bytes. Whenever an IP packet is fragmented (because it is too large for lower layers), the fragments created use the same format as a standard IP packet.

Required Fields:

Version (Contains Protocol Version IPv4, IPv6) : 4 bits

IHL (IP Header Length) : 4 bits (0 to 15 bytes)

Service Type (Accuracy or Speed driven data

transfer desired) : 6 bits

Total Packet (or, Fragment) Length (Number of

bytes including header & data) : 16 bits

Packet Id (unique Number assigned to each packet

; enables its constituent fragments to be identified) : 16 bits

Dont-Fragment Bit (Fragmentation disallowed if

set) : 1 bit

More-Fragments Bit (Set on all fragments except

last one) : 1 bit

Fragment Offset (indicates position of fragment

within original packet) : 13 bits (0-8191)

Time-To-Live (Down-counts the number of

router-hops encountered so far by the packet,

i.e. 255 → 0) : 8 bits

Protocol (Upper Layer Transport Protocol to

which this packet must be handed over e.g.

TCP/UDP) : 8 bits

Header Checksum (Used to detect erroneous

headers, its value is adjusted at each hop such

that the checksum of all header bytes including

this field is zero) : 16 bits

Source (IP Address of sending host) : 32 bits

Destination (IP Address of receiving host) : 32 bits

Options (Fields related to Security, Routing advice,

Routing path history, Debugging) : 32 bits/field (usually)

Note: In practice a fragment is never less than 20 bytes long and must always be a multiple of 8 bytes, except for the last fragment.

IP ADDRESS SCHEME

Routing of IP packets is made possible by the fact that every machine on the Internet can be uniquely identified by its IP address. Hosts (connected to just one network-interface) have only one address. Routers (connected to multiple network interfaces) have multiple addresses, one per interface.

An IP address, a 32-bit number, consisting of some network id bits and some host id bits, is used to identify the source and destination of an IP packet.

The allocation of bits to host id and network id has traditionally been done by identifying 4 classes of IP addresses (a scheme now called the Classful IP Address Scheme, to distinguish it from a newer scheme (CIDR) which does not categorize addresses into classes). These 4 classes are:

Class A:

24-bit host id

7-bit network id

0

Allows 27 – 1 networks with 224 – 1 hosts/network.

Class B:

14-bit network id

0

1

16-bit host id

Allows 214 – 1 networks with 216 – 1 hosts/network.

Class C:

8-bit host id

21-bit network id

0

1

1

Allows 221 – 1 networks with 28 – 1 hosts/network.

Class D:

28-bit Multicast Group id

0

1

1

1

A special class D address allows an IP packet to be transmitted to multiple receivers identified by a group Id.

For convenience, an IP address belonging to any of the above classes is written as a sequence of 4 decimal numbers, separated by dots, i.e. B1.B2.B3.B4 where Bi is the decimal value of the ith byte and ranges from 0 to 255.

Certain predefined IP addresses have special interpretations and behavior.

SUBNETTING SCHEME

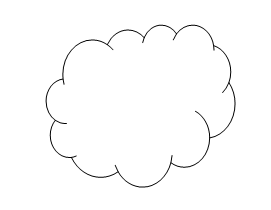
Since most traditional datalink layer protocols e.g. Ethernet have physical limits on the distance that they can cover (4 repeaters at 500 meters apart ≈ 2000 meters) it is impossible to build a single LAN which includes hundreds of hosts, since these hosts would usually not reside within these distance limits. For example, a class B network-id assigned to a company with 64,000 employees would limit it to a single Ethernet LAN spanning about 2000m. a solution is needed to enable hosts sharing the same network address to be grouped into clusters, each cluster attached to a small LAN, which may be separate and located far away from the other clusters. This is done by using some of the leading bits in the host-id (e.g. 8-bits in our example) as the subnet-id. The specific LAN to which a host belongs can de deciphered by the main router by simple removing the remaining host-id bits (last 8 bits in our case) following the subnet-id bits and routing the IP packet to the subordinate router (connected to this LAN) based on the composite network-id/subnet-id pair.

This subnetting technique requires the main and subordinates routers to know exactly the number of (trailing) bits used by the host-id part of the address. For this reason a subnet mask consisting of all 1’s for network-id and subnet-id bits and all 0’s for host-id bits is provided to the main routers (to handle incoming packets) as well as subordinate routers (to handle intersubnet packets). The subnet mask for our example is 255.255.255.0. Subnetting does not in any way modify the interface provided by the main router to external routers; it only establishes an internal interpretation of the IP addresses of its hosts so that they can be grouped into several subordinate routers connected to separate LANs, while providing flexibility for addition of new LANs. (read pp 443-440 self study)

AUTONOMOUS SYSTEMS & INTERNETWORK ROUTING

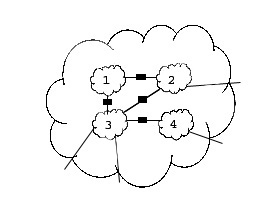
An internetwork, or briefly internet, is a collection of cooperative, interconnected physical networks. In this context, any communication system capable of transferring packets counts as a single physical network, independent of its delay, maximum packet size, throughput characteristics or geographic scale. The TCP/IP protocols treat all such networks equally, i.e. a LAN like Ethernet, a WAN used as a backbone or a point-to-point link between two computers, are each treated as a network. This results in a User’s view of a TCP/IP internet in which each computer appears to attach to a single large network, and, a Structural view in which a number of networks and routers provide interconnection.

Internet



Hosts

User View



Hosts

Internet

Router

Physical Network

Structural View

IP routers, which are specialized computers whose only job is to interconnect two networks and pass packets from one to the other were traditionally called IP gateways (somewhat misleading since gateways function at application layer). In the simplest case, an IP-router interfaces between and knows about just two networks.

internetcloud1 internetcloud1

Network

2

Network

1

R

In an actual internet that includes many routers and networks. Each router needs to know about the topology of the internet beyond the networks to which it connects.

internetcloud1 internetcloud1 internetcloud1

Network

1

R2

R1

Network

3

Network

2

However, routers use the destination network as target, not the destination host, when forwarding a packet; otherwise, they would need excessive storage capacity to know about every host in the internet to which they are connected.

The architecture of a simple internet is best viewed as a single organization, with multiple networks and routers under its control, wherein a single administrative authority can guarantee that internal routes remain consistent and viable. In addition, this authority can choose one of its routers to perform the function of informing the outside world of networks within the organization. Such a group of networks and routers controlled by a single administrative authority is called an Autonomous System (AS). Routers within an AS may choose their own internal mechanism for discovering, propagating, validating and checking the consistency of routes. The Internet, as we know it, is a collection of such ASes, connected to a backbone network via specialized routers that provide routing capability across ASes.

Backbone Network

R3

R2

R1

(For a more realistic example of an internet consisting of several interconnected ASes, see fig 5-49)-\*-. The above architecture requires two levels of routing mechanisms: one within an AS (an interior gateway protocol) and another across ASes (an exterior gateway protocol).