Chapter 5 - Fundamentals of IP Addressing and Routing

Routing: is the processing of forwarding the packet (L3 PDU)

Logical addressing: address that can be used regardless of the physical network used, providing each device at least one address, logical address enables rotting processing identify a packet's source and destination.

Routing Protocol: a protocol that aids routers by dynamically learning about the group of addresses in the network, which in turn allows the routing process to work well.

Other utilities: DNS, DHCP, ARP, Ping

Path Selection :- Routing Protocol, some time refer to Routing (forwarding) processes

IP is a connectionless protocol, does not require overhead agreements or messages before sending a packet.

Routing (Forwarding) , Network Layer Interaction with Datalink Layer

Routing table contains network layer address groupings.

Network layer use data-link layer to send data over a physical network, packet encapsulated as frames.

Routing process forwards only the packet, end-to-end through the network, discarding data-link header and trailer along the way, and re-encapsulating as per the data link protocol used.

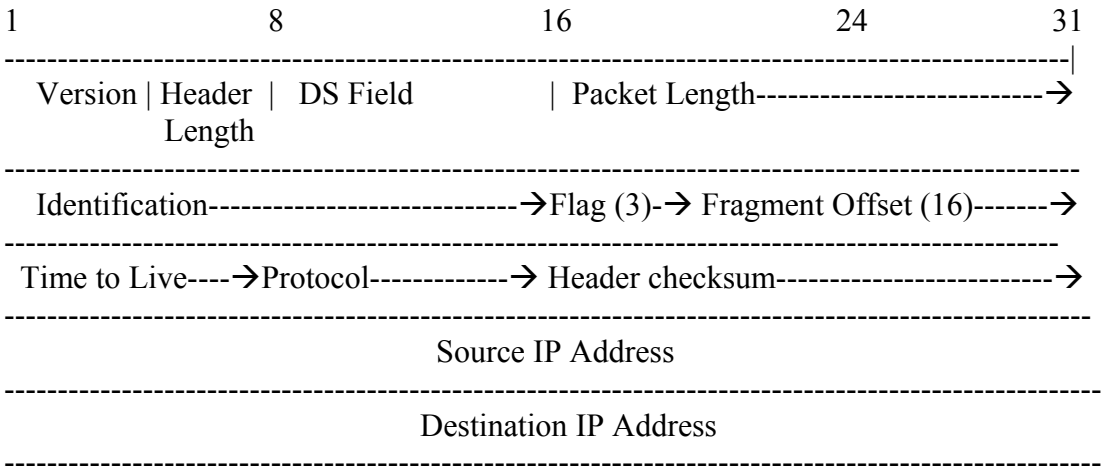
Address Resolution Protocol (ARP) is used to dynamically learn about the data-link address of a IP host connected to a LAN.

Process of routing forwards Layer 3 packets, L3 PDU, based on the destination layer 3 address in the packet.

Routing process uses data-link layer to encapsulates the layer 3 packet into layer 2 frames for transmission across each successive data link.

IP Packets and IP Header

IPv4 header in a packet is 20 bytes long and key fields are



Version : Version of IP Protocol – most networks use IPV4 today

Header Length : IP Header length, defines IP header length including optional fields

DS Field : Differentiated services field. It is used for marking packets for the purpose of applying different Quality-of-service QoS levels to different packets.

Packet Length : Identified entire length of the packet including data.

Identification : Used by IP packet fragmentation process, all fragments of the original packets contain same identifier.

Flag : 3 bit flag used by IP fragmentation process

Fragment Offset : A number used to help hosts reassemble fragmented packets into the original large packet

TTL (1 Byte) – time to live, value used to prevent routing loops

Protocol (1 Byte) – idetnfity contents of data portion of the IP packet, Protocol 6 implies that a TCP header is the first thing in the IP Packet data field

Header checksum for FCS

Source IP Address (4 Bytes) : 32 bits IP Address of the sender of the packet

Destination IP Address (4 Bytes) : 32 bit IP address of the intended recipient of the packet

Network Layer (Layer 3) Addressing

Layer 3 addresses are designed to allow logical grouping of addresses.

A network or subnet is represented by a ip address which implies a group of ip addresses.

The end goal for a routing protocol is to fill the routing table with all know destination groups and with the best route to reach each group.

Routers build their routing table entries dynamically using a routing protocol.

Routing protocol learns the locations of the groups and advertise the group so the routers can fill their routing table.
A **routing protocol** learns the route and put those routes in a routing table.
Routed protocol defines the type of packet forwarded or routed through a network.

IP packets are routed in a network, so IP would be the routed protocol, If the routers used the Routing Information Protocol to learn about the routes then RIP would be the Routing protocol.

IP is a routed protocol, and RIP- routing information protocol is routing protocol.

IP Addressing
Any device that can send and receive IP packets is called an **IP host**.

32 bit IP address is represented in dotted decimal, and has 4 octets.
Each octect has a range 0 – 255 inclusive

IP address not of the PC but of the NIC.

IP Address Groups – IP Networks :
(two statements about how ip expects ip addresses to be grouped into networks or subnets)

- All IP addresses in the same group must not be separated by a router.
- IP address separated by a router must be in different groups

IP routing relies IP addresses in the same group (network, subnet) to be in the same general location.

Classes of IP networks

IP defines three different network classes of addresses used by individual host – addresses called unicast addresses , Class A, B and C, TCP/IP uses Class D for multicast and class E for experimental addresses.

Size of Network and Host part of the IP addresses with no subnetting

Network class	Network bytes	Host bytes	Number of addresses
A	1 (8 bits)	3 (24 bits)	2 (raised 24) - 2
B	2 (16 bits)	2 (16 bits)	2 (raised 16) – 2
C	3 (24 bits)	1 (8 bits)	2 (raised 8) – 2

Network number (group address) has all binary zeros in the host part of the number. A network number with all binary 1s in the host part is called network **broadcast or direct broadcast address**, any packet send to this address will be forwarded to all devices in that network.

Internet corporation for assigned network number (ICANN) is in charge of universal ip address assignment formally was done by IANA, the internet assigned numbers authority.

All possible valid network numbers

class	First octet range	Valid network numbers	total number for this class of networks	Total number of hosts per network
A	1 -126	1.0.0.0 to 126.0.0.0	2 (raised 7) – 2 (126)	2 (raised 24) -2 16, 777, 214
B	128 - 191	128.0.0.0 to 191.255.0.0	2 (raised 14) 16,384	2 (raised 16) – 2 65, 534
C	192 – 223	192.0.0.0 to 223.255.255.0	2 (raised 21) 2, 097, 152	2 (raised 8) – 2 254

List of all possible valid network numbers….reference table for the number of network, size of the network part, size of the host part, for Class A,B and C ip networks.

	Class A	Class B	Class C
First Octect range	1 to 126	128 - 191	192 – 223
Valid Network Numbers	1.0.0.0 to 126.0.0.0	128.0.0.0 191.255.0.0	192.0.0.0 to 223.255.255.0
Number of networks in this Class	2 ^ 7 – 2 = 128	2 ^ 14 = 16,384	2 ^ 21= 2,097,152
Number of hosts per network	2 ^ 24 – 2 = 16,777,214	2 ^ 16 – 2 = 65,534	2 ^ 8 – 2 = 254
Size of network part of the address (bytes)	1	2	3

Size of hosts part of the address (bytes)	3	2	1

^ *raised to*

(why it is 7,14, and 21 network bits on CLASS A,B and C networks : explained)

CLASS A (7 Network Bits)

0	N	N	N	N	N	N	N	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8

CLASS B (6 + 8 = 14 Network Bits)

1	0	N	N	N	N	N	N	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8

CLASS C (5 + 16 = 21 Network Bits)

1	1	0	N	N	N	N	N	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8

Class A , B and C network, network and host parts and default mask

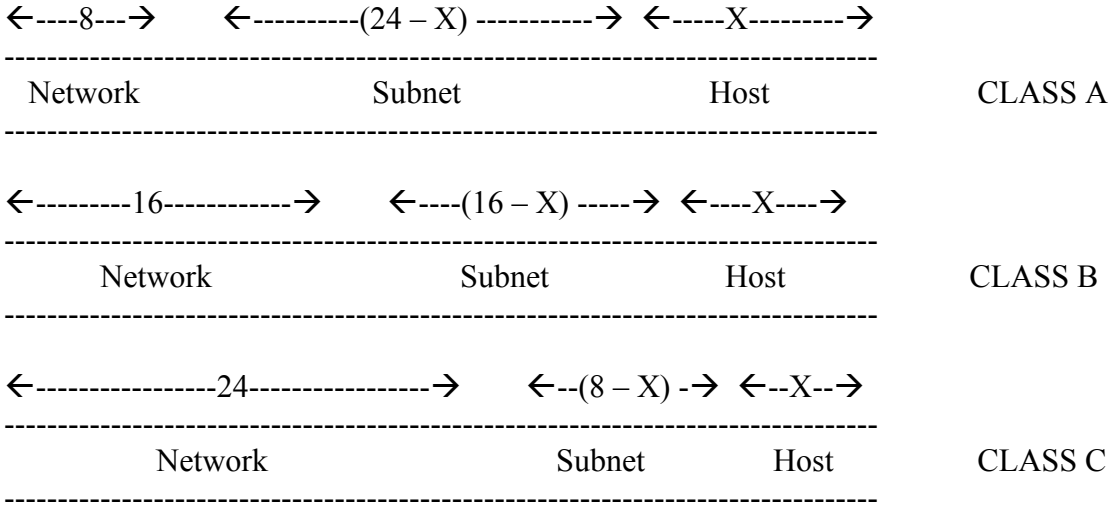
Class of Address	Size of network part of address in bits	Size of host part of address in bits	Default mask for each class of network
A	8	24	255.0.0.0.
B	16	16	255.255.0.0
C	24	8	255.255.255.0

Subnets

Subnetting: the process of sub dividing the class A, B or C network into smaller groups is called subnetting.

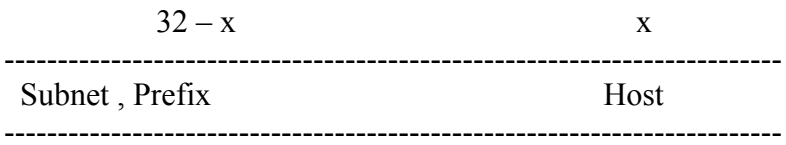
When subnetting a third part of an IP address appears between the network and host parts of the ip address – namely the subnet part of the ip address. This part is created by stealing or borrowing bits from the host part of the ip address. The size of the network part of the address never shrinks.

Adders format when Subnetting is used. (Classful)



Classful addressing : refers to ip address with three parts, network part (confirming to the Class A, B and C) rules, subnet part and a host part.

Classless Addressing : Instead of three parts as in classful addressing, a classless address has two parts , the part on which routing is based, and the host part. The part on which routing is based is the combination of network and subnet parts from the classful addressing view, the first part is often called subnet part or sometimes the prefix.



IP Routing

Host Routing : Hosts uses the following two step logic when choosing where to send a packet;
(two step process of how hosts route packets)

If the destination ip address is in the same subnet as the host, it send the packet directly to the destination host.

If the destination ip address is not in the same subnet as the host, sends the packet to the default gateway (a routers Ethernet interface on the subnet).

A Routers uses the following logic when receiving a data link frame – a Frame that has an IP packet encapsulated in it.

(four step process of how hosts route packets)

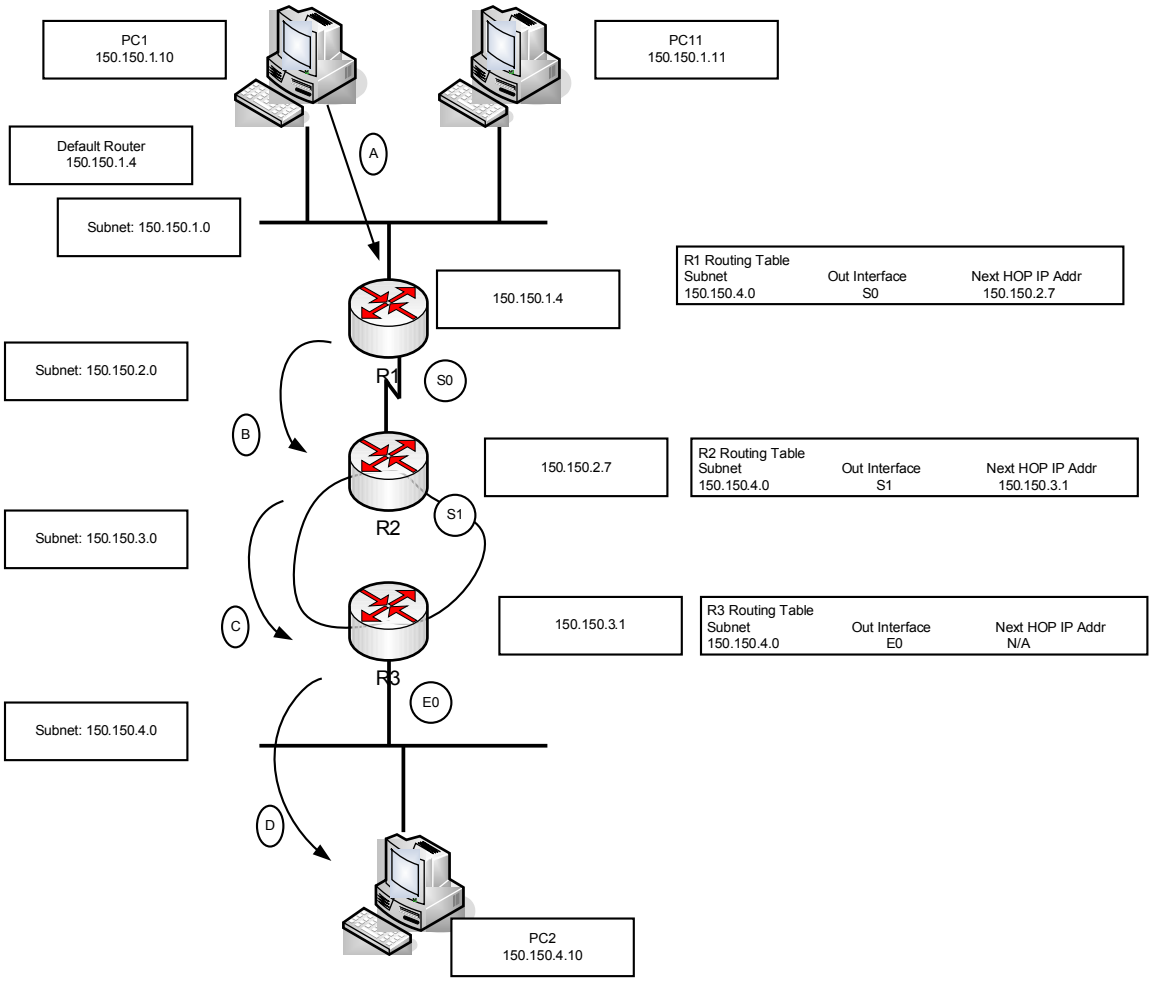
Step 1 : Use the data link FCS field to ensure that the frame had no errors, if errors occurred discard the frame

Step 2 : Assuming the frame was not discarded in step 1, discard the old data link header and trailer leaving the IP Packet

Step 3 : Compare the IP packets destination IP address to the routing table and determine the route that matches the destination address. This route identifies the outgoing interface of the router and possibility the next hop router.

Step 4 : Encapsulate the IP packet in new data link header and trailer appropriate for the outgoing interface and forward the frame.

With these steps each router forwards the packet until it reaches its destination.



Step A : PC1 sends a packet to its default gateway. PC1 builds an IP Packet with PC2's ip address (150.150.4.10). PC1 needs to send the packet to R1 (PC1's default gateway) because the destination address is on a different subnet. PC1 send the ip packet as Ethernet frame to R1's MAC address over the Ethernet.

Step B : R1 processes the incoming frame and forwards to R2. R1 copies the frame of the Ethernet, checks the frame's FCS and no errors have occurred. Discards the Ethernet header and trailer, R1 compares the destination address and finds a matching route (S0) from the routing table. R1 forwards the packet to outgoing interface S0 to next hop router R2, after encapsulating the packet in an HDLC frame.

Step C : R2 processes the incoming frame and forwards the packet to R3.
R2 does the same steps as that of R1, checks the FCS of the HDLC frame, finds no errors, discards the HDLC header and trailer, finds a match from the routing table and determines the outgoing route as S1 and sends it to next hop address 150.150.3.1 (R3) after encapsulating the packet in a frame relay header.

Step D : R3 process the frame and forward the packet to PC2
Like R1 and R2, R3 checks the FCS and finds no errors, discards the old data link header and trailer, R3's routing table entry shows that the destination ip address is in the same

subnet as R3, and outgoing interface is R3's Ethernet interface. R3 encapsulates the packet in Ethernet frame and forwards the frame to PC2's to MAC address over Ethernet.

IP Routing Protocol

IP Routing protocols fills the routing table with valid, loop-free routes.

Goals of Routing Protocol…

- To dynamically learn and fill the routing table with routes to all the subnets in the network
- If more than one route to a subnet is available, place the best route in the routing table
- To notice when the routes in the routing table are no longer valid and remove them from the routing table
- If a route is removed from the routing table, and another route through another neighbouring router is available, add the route to the routing table
- To add new routes, and replace lost routes, with best currently available route as soon as possible. The time between loosing a route and finding a working replacement route is called **convergence** time
- To prevent routing loops

Routing protocols follow three general steps in advertising routes in a network…

Step 1 : Each router adds a route to its routing table for subnets directly connected to the router

Step 2 : Each router tells its neighbours about all the routes in its routing table, including directly connected routes and routes learned from other routers

Step 3 : After learning a new route from a neighbour, the router adds a route to its routing table, with the next hop router typically being the neighbour from which the route was learned

How each router learns its route to 150.150.4.0 (PC2's subnet) From the above figure…..

Step A. R3 learns a route that refers to its own E0 interface because subnet 150.150.4.0 is directly connected

Step B. R3 sends a routing protocol message called a **routing update** to R2, causing R2 to learn about the subnet 150.150.4.0

Step C. R2 sends similar routing protocol message called a **routing update** to R1, causing R1 to learn about the subnet 150.150.4.0

Step D. R1's route to 150.150.4.0 lists R2's IP address as the next hop address, because R1 learned about the route from R2. The route also lists R1's outgoing interface as S0 because R1 learned about the route from the update came through the interface S0.

Network Layer Utilities
ARP – Address Resolution Protocol – used to learn MAC address of other computers in the same LAN subnet.
DNS – Domain Name System – used to learn IP address

DNS Name resolution : A pc learns IP address of the DNS server, either pre-configured or via DHCP, and sends a DNS request to resolve the name of the computer to communicate to its IP Address, and DNS server returns the IP address.

The ARP Process : Sending pc issues an ARP broadcast, an ARP broadcast is sent to an Ethernet broadcast address, so everyone on the LAN receives it, the host in the same LAN subnet with the IP address as in the ARP broadcast, will respond with its MAC address.

If both sending and destination hosts are in the subnet then ARP will be used to learn the MAC address of the destination host, other wise will be used to learn the MAC address of the default router where the IP packet will be forwarded by the host.

Any device that uses IP should retain, or cache, the information learned with ARP, placing the information in its ARP cache. Each time a host wants to send a packet encapsulated in Ethernet frame it checks its ARP cache, and uses the MAC address found there. If the correct information is not listed in the ARP cache, then the host uses ARP to discover the MAC address used by the particular IP address. Also a host learns ARP information when it receives an ARP as well.

Address Assignment and DHCP

DHCP defines the protocol used to allow computers to request a lease of an IP address. DHCP uses a server, with the server keeping a list of pools of IP addresses available on each subnet. DHCP clients can send DHCP server a message asking to borrow or lease an IP address. The server then suggests an IP address, if accepted the server notes that the address is no longer available for assignment to any other hosts.

DHCP supplies IP addresses to client, and it also supplies other information. For example hosts need to know their IP address, plus subnet mask to use, plus default gateway to use, as well as IP address of any DNS servers. In most networks today DHCP supplies all these facts to a typical end user host.

Typically a PC used as DHCP server in an enterprise network. Routers can also provider DHCP server functions, dynamically assigning IP addresses to host in a small or home

office environment, use DHCP client functions (router can act as DHCP clients as well) to dynamically lease IP address from an ISP.

4 typical DHCP messages to acquire an IP address

1. DHCP discover message (LAN Broadcast) (from DHCP Client)
2. DHCP offer message directed to client (From DHCP Server to broadcasting Client)
3. DHCP request message directed to server
4. DHCP acknowledgment with information (IP Address, Mask, Default Gateway etc) directed to client

ICMP Echo and Ping command

Ping – (Packet Internet Groper) a tool for network connectivity testing, uses Internet Control Message Protocol (ICMP), sending a message called ICMP echo request to another ip address, the computer with that ip address replies with an ICMP echo reply.

ICMP just tests the IP connectivity, layer 1,2 and 3 of the OSI network model.

ARP : Address resolution protocol – an internet protocol used to map an ip address to a MAC address, defined in RFC 826.

Default Gateway/Default Router: On an IP host, the IP address of some router to which the host sends packets when the packets destination ip address is on a subnet other than the host's local subnet.

DHCP : Dynamic Host Configuration Protocol. A protocol used by hosts to dynamically discover and lease an ip address, and learn the correct subnet mask, default gateway, DNS server ip address.

DNS : Domain Name System. An application layer protocol used throughout the internet for translating host names into their associated IP addresses.

Host part : a term used to describe part of an IPV4 address that is used to uniquely identify a host inside a subnet. Host part is identified by bits of value 0 in the subnet mask.

IP Address : In IP Version 4 (IPv4), a 32 bit address assigned to host using TCP/IP. Each address consists of a network number, optional subnetwork number, and host number. Network number and subnetwork number together are used for routing, and the host number is used to address an individual host within a network or subnetwork.

Logical Address : A generic reference to addresses as defined by layer 3 protocols, which do not have to be concerned with the physical details of the underlying physical media. Used mainly in contrast with the data link addresses which are physical addresses based on the physical medium used.

Network broadcast address : In IPv4 an a special address in each classful network that can be used to broadcast a packet to all hosts in the same classful network. Numerically the address has the same value as the network number in the network part and a value of 255 in all the host part.

Network Number / Network Address : A number that uses the same decimal notation as that of the IP address, but the number itself represents all the hosts in a single class A,B or C ip network.

Network Part : The portion of an IPv4 address, 1,2 or 3 octect/bytes long based on whether the address is in a Class A,B or C network.

Routing Table : A list of routes in a router, with each route listing the destination subnet and mask, router interface out which to forward the packets destined to that subnet, and as needed, the next hop routers IP address.

Subnet broadcast address : A special address in each subnet, specifically the largest numeric address in the subnet, designed so that the packets send to this address should be delivered to all hosts in that subnet.

Subnet number / Subnet Address : In IPv4 a dotted decimal number that represents all addresses in a single subnet. Numerically the smallest value in the range of number in a subnet, reserved so that it cannot be used as a unicast address by a host.

Subnet Part : In a subnetted IPv4 address, interpreted with classful addressing rules, one of the three parts of the structure of an IP address, with the subnet part uniquely identifying different subnets of a classful IP network.

Please go to ……Do I know this Already –QUIZ. – Chapter 5. :- Page 94.