EP2120 Internetworking
IK2218 Protocols and Principles of the Internet

Homework Assignment 1
(Solutions due 19:00, Mon., 11 Sept. 2023)
(Review due 19:00, Wed., 13 Sept. 2023)

1. IPv4 Addressing (30/100)
   a) What is the best fit netmask (i.e., resulting in as few host addresses as possible) for a network with 62 hosts in it? (5p)
   Ans:
   Given that for a network with 62 hosts, we need 62 IP addresses for the hosts and additionally one for network address and directed broadcast address making it **64 addresses** in total. Although we might need one more IP address for router but only if it isn't the part of hosts.

   Now, we need to know the smallest power of 2 greater than or equal to 64 and in notation form it can be said as "2^h >= 64".

   Starting with h = 6, we get 2^6 = 64
   We now need minimum of 6 host bits leaving us with 32-6= 26 bits

   After constructing a subnet mask, we have:
   11111111.11111111.11111111.11000000 (Binary form)

   Converting it into decimal we have: 255.255.255.192

   Therefore, we can say that the best fit netmask for a network with 62 hosts is 255.255.255.192 or /26

   b) What is the maximum number of hosts you can have in a /24 network? (5p)
   Ans:
   So, for /24 network, to know the maximum number of hosts, we have 32-24= 8 bits which is 2 to the power of 8 (2^8) = 256 host addresses. But out of these 256 addresses we need to subtract 1 network address and 1 directed broadcast address. Therefore a /24 network can have up to **254 hosts**.

   c) Split up the network 172.20.16.0/24 into five networks, three /26 networks and two /27 networks. Provide the resulting subnets in binary and in dotted decimal notation including the prefix length. (5p)
   Ans:

Given the network 172.20.16.0/24 and we need to split them into 5 networks in which 3 of them are /26 networks and two are /27 networks.

a) For creating /26 subnets, 2 bits need to be borrowed from host part of/24 network giving us 4 subnets that is 2*2=4. But we need just three of them, so we'll be using the first three.
   Subnet mask: 255.255.255.192 (11111111.11111111.11111111.11000000)
   1) Subnet: **172.20.16.0/26**
      Binary conversion: 10101100.00010100.00010000.00000000
   2) Subnet: **172.20.16.64/26**
      Binary conversion: 10101100.00010100.00010000.01000000
   3) Subnet: **172.20.16.128/26**
      Binary conversion: 10101100.00010100.00010000.10000000
b) For creating /27 subnets, 3 bits need to be borrowed from host part of /24 network giving us 8 subnets that is 2*3=4. But we need just two of them.
   Subnet mask: 255.255.255.224 (11111111.11111111.11111111.11100000)
   1) Subnet: **172.20.16.192/27**
      Binary conversion: 10101100.00010100.00010000.11000000
   2) Subnet: **172.20.16.224/27**
      Binary conversion: 10101100.00010100.00010000.11100000

d) What is the directed broadcast address of the network 37.156.192.0/20? (5p)

Ans:

The address used to send a broadcast packet to all hosts in the subnet is called as DBA. In order to find out the DBA of the given network 37.156.192.0/20 we need to know the subnet mask of /20 network which is 255.255.240.0.

So, we now have the following details:

Network: 37.156.192.0/20

Binary conversion of given network: 00100101.10011100.11000000.00000000

Subnet mask: 255.255.240.0

Binary conversion of given subnet: 11111111.11111111.11110000.00000000

Inverted Subnet mask: 00000000.00000000.00001111.11111111

After performing bitwise or operation we get our DBA as

00100101.10011100.11001111.11111111

Therefore, after converting the above binary address to decimal, we get our DBA for 37.156.192.0/20 network as "**37.156.207.255**".

e) Assume that the address of a host in a network is 172.20.17.193 and the directed broadcast address of the network is 172.20.17.255. What is the network address of the largest and smallest subnet that the device may belong to? Provide the results in dotted decimal notation including the prefix length. (5p)

Ans:
Given,
Host address in a network: 172.20.17.193
Binary form: 10101100.00010100.00010001.11000001

Directed broadcast address: 172.20.17.255
Binary form: 10101100.00010100.00010001.11111111

Largest subnet: 10101100.00010100.00010000.00000000/23
Decimal form: 172.20.16.0/23

Smallest subnet: 10101100.00010100.00010001.11000000/26
Decimal form: 172.20.17.192/26

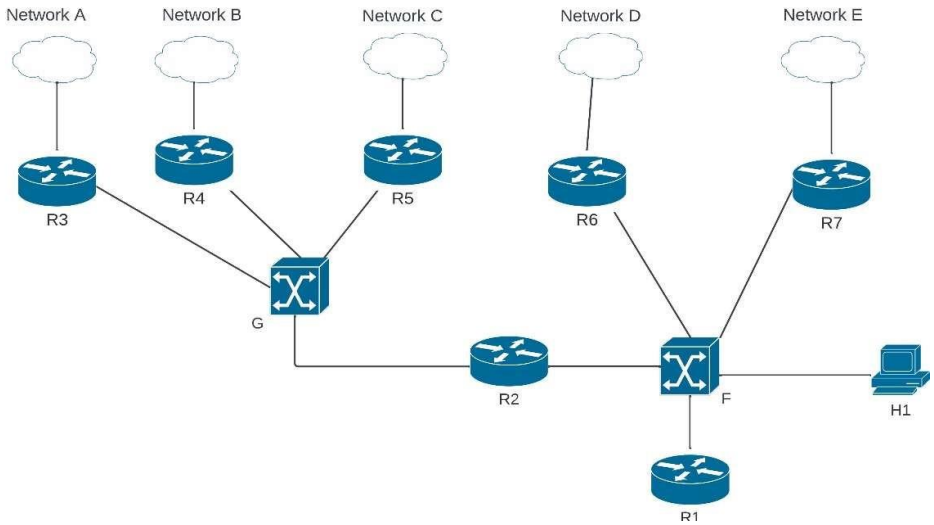
f) Use the services of IANA and a regional registry to figure out to whom the IP address block 37.156.192.0/24 belongs. Provide the name of the organization and the AS number. (5p)

Ans: Acc to RIPE database:

Name of the organization: **Vetenskapsradet / SUNET**

AS number: **AS1653**

2. Address allocation (30/100)



Consider the network above, a routed network in an organization's enterprise network. The organization built a core network (network F) connected to a central router (R1), which provides access to the rest of the Internet. Router (R2) connects network F to the switched Ethernet network G. The access routers (R3 to R7) are connected to a set of local offices (networks A to E). The host H1, connected to network F, performs various traffic monitoring tasks. All networks use Ethernet on the link layer.

The organization wants to make an address allocation by assigning an address block to networks A to G in the following way:

i. Network A requires 500 hosts, networks B and C require 200 hosts each, and networks D and E require 100 hosts each. The lowest address should be assigned to network A.
ii. There are no unnumbered point-to-point links: all Ethernet networks are IP subnets and all nodes (routers and hosts) have an IP address on all their network interfaces. All nodes need to be reachable from any other host.
iii. The address allocation should be such that the subnets can be aggregated.
iv. Each subnet should not be larger than necessary in order to accommodate all nodes (host or router interfaces) in the subnet.

a) Assume that the allocated address block is 152.68.208.0/22. Is it possible to have an address allocation that satisfies the above requirements? Justify your answer. (4p)

Ans:

Given address 152.68.208.0/22
If we do the calculations 32-22=10
And 2^10 = 1024
Now, 1024- Net address- DBA= 1022 addresses

The above notation shows that 1022 addresses can have 1022 hosts at maximum limit. Given the conditions, the number of hosts required for A, B, C, D, & E exceeds the limit of 1022 hosts. Therefore, it is not practically possible to have an address allocation that satisfies the requirements.

b) Now, assume that the enterprise allocated prefix 152.68.208.0/21 for its internal addresses. Make an address allocation as described in (i-iv). Based on your address allocation, provide the network addresses of networks A to G, and the required entries of the forwarding table of router R1. Choose appropriate IP addresses for the router interfaces that appear as next hop in the forwarding table. Give a sketch of your reasoning to support your solution. (26p)

Ans: Given address: 152.68.208.0/21

1) Network A:
   Network A requires 500 hosts, so it has to have subnet with at least 512 (2^9) addresses.

   500+ Net address+ DBA <= 512 (2^9) addresses (32-9= 23)

   Network address: **152.68.208.0/23**

2) Network B: it requires 200 hosts, so it has to have at least 256(2^8) addresses.

   200+Net address+ DBA<= 256 (2^8) addresses (32-8= 24)

   Network address: **152.68.210.0/24**

3) Network C: it also requires 200 hosts, so it has to have at least 256(2^8) addresses.

   200+Net address+ DBA<= 256 (2^8) addresses (32-8= 24)

   Network address: **152.68.211.0/24**

4) Network D:
It requires 100 hosts, so it has to have at least 128 (2^7) addresses (32-7=25).

100+ net address + DBA <= 128 (2^7)

Network address: **152.68.212.0/25**

5) Network E:
It also requires 100 hosts, so it has to have at least 128 (2^7) addresses (32-7= 25).

100+ net address + DBA <= 128 (2^7)

Network address: **152.68.212.128/25**

6) Network F:
5+Network address+ DBA<= 8 (2^3) addresses

Network address: **152.68.213.128/29**

7) Network G:
Network address: **152.68.213.0/29**

Destination	Next hop	Flags	Interface

3. IPv4 forwarding (20/100)

A router has the forwarding table shown below. Determine the next-hop address and the outgoing interface for the packets arriving to the router with destination addresses as given in points (a)-(e).

Destination	Next hop	Flags	Interface
80.5.0.0/16	-	U	m2
129.40.160.0/20	-	U	m1
201.50.1.0/25	-	U	m0
91.0.0.96/27	80.5.0.100	UG	m2
147.17.0.0/16	201.50.1.44	UG	m0
129.40.128.0/17	201.50.1.2	UG	m0
0.0.0.0/0	80.5.0.1	UG	m2

a) 201.50.1.63 (4p)

Ans:
Next hop: 80.5.0.1
Flag: indirect delivery/ default route
Interface: m2

b) 91.0.0.140 (4p)

Ans:
Next hop: 80.5.0.100
Flag: indirect delivery
Interface: m2

c) 129.40.255.48 (4p)
Ans:
Next hop: 201.50.1.2
Flag: indirect delivery
Interface: m0

d) 201.40.195.2 (4p)
Ans:
Next hop: 80.5.0.1
Flag: indirect delivery/ default route
Interface: m2

e) 147.17.224.224 (4p)
Ans:

Next hop: 201.50.1.44

Flag: Indirect delivery

Interface: m0

4. IPv4 and IPv6 datagram formats (20/100)

a. What is the purpose of TTL in the IPv4 header and in the IPv6 header? Please explain what could happen if the TTL field did not exist. (5p)
   Ans:

TTL stands for “Time to live” field and it plays a very important role in IPv4 and IPv6 headers. The main purpose of TTL is to prevent the packets to circulate/transmit indefinitely in the network and to prevent infinite looping in the routes.

1) In **IPv4 header** the TTL field(8-bit) is used to set limit to the packet’s lifespan. Normally it is started with the value set by the sender and decreases by one every time the packet has been forwarded by the router. When the TTL field reduces to 0, the packet is discarded by the router. The main purpose of TTL field in IPv4 header is to avoid routing loops and prevent packet aging.

2) In **IPv6 header** the TTL field is replaced by concept called “Hop Limit” which is equivalent to TTL. It is of the size of 8 bits and functions similarly to TTL. It sets a limit on the maximum number of network hops a packet can make and decreases by one with each router hop.

The consequences if TTL field did not exist includes:

1) Infinite looping of packets in the network due to endless circulation, which results in increase of network traffic and bandwidth usage.
2) The presence of old packets in the network could lead to network congestion and errors among routers resulting in delivery of irrelevant data.
3) Absence of TTL field can also cause network stability issues.

b. How is error checking done in IPv4? What is the purpose? (5p)
Ans:
In IPv4 there is a function to detect bit errors in the header which only covers the header only and not the payload. This function is called as “**Header Checksum** “. This plays an important role in ensuring the IP header’s integrity by allowing the receiving hosts and routers to detect errors occurred while the packet’s transmission. The header checksum is calculated upon every hop of the packet. The router or host recalculates the Header Checksum based on the received header when it receives an IPv4 packet, then compares the result to the value in the Header Checksum field. If there is a header error and the calculated and received checksums do not match, the packet may be removed.

The main purpose of the error checking in IPv4 includes:

1) Ensuring that routers and hosts make the right routing decisions and correctly interpret packet information is made possible by finding errors in the IP header.
2) It helps in checking the header integrity by ensuring that the packet has not been tampered during transmission.
3) For routers to make correct routing decisions it is necessary for the headers to be error free.
4) Overall, error checking enhances the reliability of IPv4 by knowing and operating errors occurred during packet transmission.

c. In the IPv4 header, the 'Flags' field consists of 3 bits, of which the 'DF' (Don't Fragment) and 'MF' (More Fragments) flags are used. Explain a scenario where these flags would

be relevant, how they are set, and the implications for packet fragmentation and reassembly. (5p)

Ans:

Yes, in IPv4 header, the "FLAGS" field consists of 3 bits known as RF (Reserved fragment), DF (Don't Fragment), and MF (More Fragments).

1) DF flag is mainly used to indicate that the packet is not to be fragmented during its transmission through the network. Usually set by the sender when the network path has small MTUs and wants to avoid fragmentation as it could lead to loss of packets. In a IPv4 header the DF flag is a single bit, if its set to "1" the packet must not be fragmented and if set to "0" then it can be fragmented. When a DF flag is set and if router's path encounters a link with smaller MTU, then the packet cannot be fragmented and is discarded by the router. The sender is notified about this and has options to change the size of the packet for fragmentation.

2) MF Flag is mainly used for fragmentation as the name suggests. When more fragments are needed for reassembly, this flag is used as an indication. MF flag is also a single bit IPv4 header. It is mostly set to "1" for all fragments of a packet except the last one which is set to "0" when fragmenting an IPv4 packet. The MF flag is used by the receiving host to check whether the fragmentation is done on the packet. And finally, when host has received the last fragment, the reassembly is done.

d. What is Explicit Congestion Notification (ECN)? How is it used? (5p)

Ans:

ECN is mainly a functionality that allows routers to signal about the congestion in the network before the packets get dropped. It is of 2 bits and has four values to it.

1. If the value of the bits is "00", then the datagram doesn't support ECN.
2. If the value of the bits is "01 or 10", the datagram supports ECN and is called ECT (ECN capable transport).
3. And to know if the network is experiencing congestion the "11" bits are used and is known as CE (congestion Experienced).