Networks COMP30650

Maria Leech 19210540

Maria.leech@ucdconnect.ie

Contents

Question 3

MTU is Maximum Transmission Unit, and it is the largest size of packet that can be sent across the network. The size that can be sent varies depending for example on whether it is being sent across WIFI MTU of 2300bytes or ethernet MTU of 1500bytes.

This obstacle necessitates Fragmentation and MTU discovery which we are going to look at in this question. Routers do the fragmentation but do not reassemble them, only the receiver reassembles them. A few of the flags that help the receiver do this are:

1. ID= Is the ID number that each fragment belongs to.
2. MF=stands for more fragments and it signals to the receiver that more fragments are on the way if it is set above 0.
3. DF=Do not Fragment meaning the message cannot be fragmented. If it is too big it is dropped and an ICMP is sent to the sender telling them it has been dropped.
4. Fragment Offset is the order in which the fragments were sent and should be reassembled.
5. Source Address is the senders IP address.
6. Destination address id the receivers IP address.

IPV header Fields

i. IPv4 Header **(A) MTU=1600**

   a. **Identification=0x128**
   b. **MF=0**
   c. **DF=0**
   d. **Fragment Offset=0**
   e. **Source Address=Node A's IP address**
   f. **Destination Address=Node B's IP address**

IPv4 Header **(B) MTU=800**
Splits into two messages
Message 1

   a. **Identification=0x128**
   b. **MF=1**
   c. **DF=0**
   d. **Fragment Offset=0**
   e. **Source Address= Node A's IP address**
   f. **Destination Address=Node B's IP address**

Message 2

   a. **Identification=0x128**
   b. **MF=0**
   c. **DF=0**
   d. **Fragment Offset=800**
   e. **Source Address= Node A's IP address**
   f. **Destination Address=Node B's IP address**

IPv4 Header **(C) MTU=1200**

Message 1

a. **Identification=0x128**
b. **MF=1**
c. **DF=0**
d. **Fragment Offset=0**
e. **Source Address= Node A's IP address**
f. **Destination Address=Node B's IP address**

Message 2

a. **Identification=0x128**
b. **MF=0**
c. **DF=0**
d. **Fragment Offset=800**
e. **Source Address= Node A's IP address**
f. **Destination Address=Node B's IP address**

IPv4 Header **(D) MTU=1600**

a. **Identification=0x128**
b. **MF=1**
c. **DF=0**
d. **Fragment Offset=0**
e. **Source Address= Node A's IP address**
f. **Destination Address=Node B's IP address**

Message 2

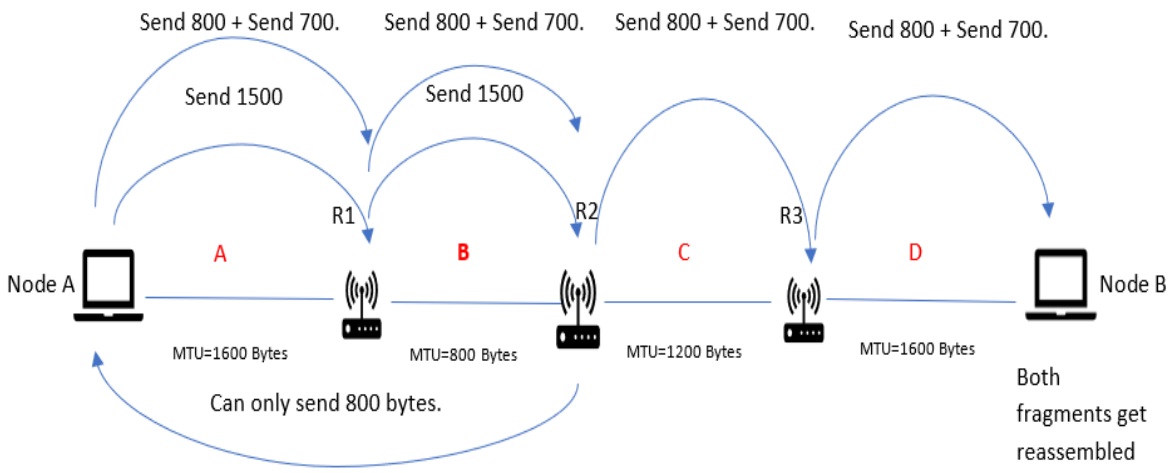
a. **Identification=0x128**
b. **MF=0**
c. **DF=0**
d. **Fragment Offset=800**
e. **Source Address= Node A's IP address**
f. **Destination Address=Node B's IP address**

Weaknesses of Fragmentation

Fragmentation creates more work for routers and hosts as routers fragment the packets and then they must be reassembled on the receiver's side. Routers do not reassemble as they are not equipped to hold on to all the packets because their main job is to transmit as quickly as possible, and the fragments may take different routes and not end up at the same router.
It can magnify loss rate because more messages are being sent increasing the risk that some will get lost along the route.
Firewalls can have trouble processing fragmented messages for instance if they arrive out of sequence a packet may get dropped if its not the first fragment as it does not contain all the necessary information to match the packet filter.

Alternative approach

Path maximum transmission unit discovery used today by IP.



1. Node A will try to send 1500 and the first connection can handle that.
2. R1 will try to send 1500 to R2.
    a. R2 will send back to Node A try 800.
    b. Node A will send one 800 byte and one 700-byte message to R1.
3. R1 will forward the two messages to R2.
4. R2 will try to send 800 bytes the connection can handle it, so it sends the 700-byte message to.
5. R3 will do the same as R2 and when the fragmented message reaches the destination at Node B it will be reconstructed once all fragments have arrived.

Question 4

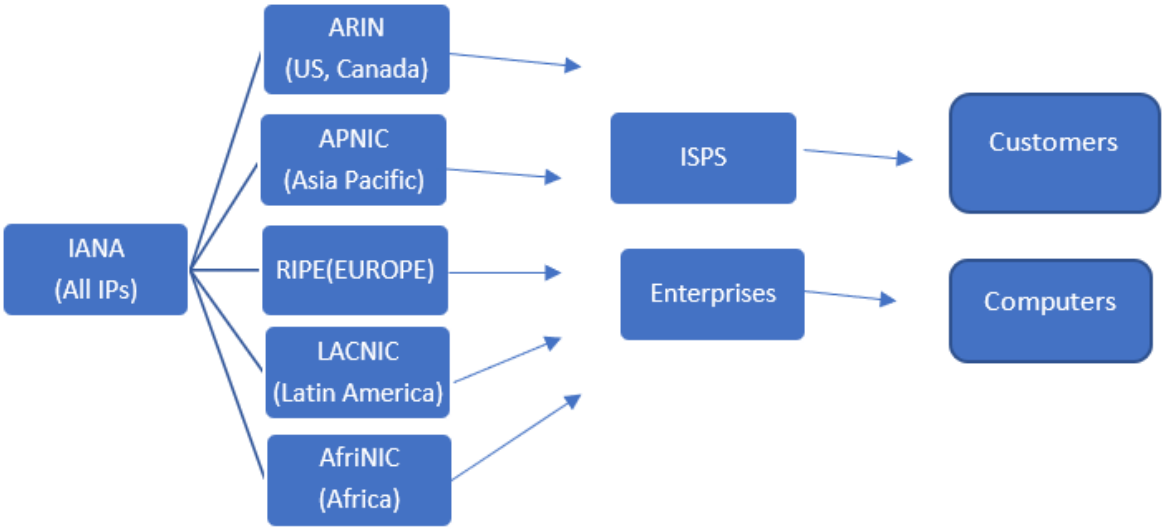
To compare MAC addresses and IP addresses I will examine certain characteristics for both address types.

1. The layer they used in.
2. How they are used.
3. How they are assigned and the protocols that do this.
4. How they are used together.

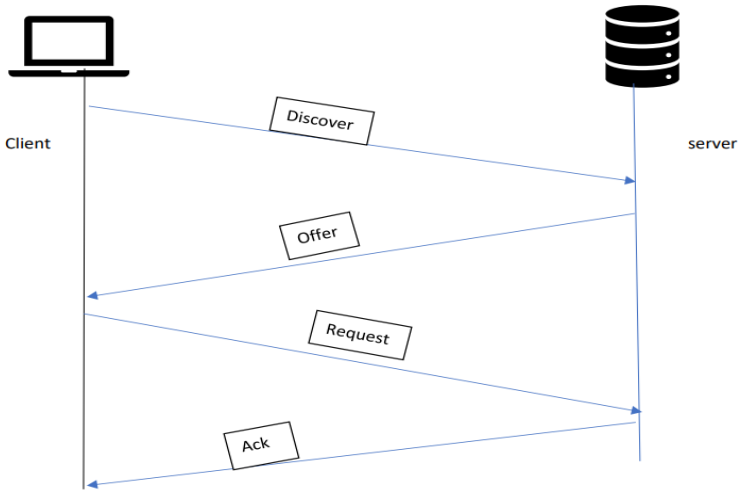
IP addresses

IP addresses are dealt with in the Network layer and are used by applications to communicate with one another. IP is a Datagram, or connectionless service. There is a public and private IP associated with different devices on the network. Private IP addresses can be used freely with a private network, but they need a public IP and Network Address Translation(NAT) to access other networks like the Internet. Public IP addresses are generally leased and therefore the public IP may change unlike a MAC address. IP addresses two types IPv4 32bit, which are mostly exhausted, so we are migrating to the newer IPv6 128bit. As IPv6 is still growing in adoption IPv6 headers still need to be wrapped in IPv4 headers to make them compatible and allow messages to be transmitted between the two different IP protocols.

IP addresses follow a hierarchal process in how they are assigned. The Internet Assigned Numbers Authority(IANA) control the distribution of IP addresses they provide IP ranges to Regional Internet Registries (RIR) who then pass along ranges of IPs to Internet Service providers (ISPs).



IP addresses are assigned by DHCP to individual customer nodes. An example of DORA with sample IP and ethernet addresses:



Discover

First the client does not have an IP address it is set to source: 0.0.0.0 ethernet 76:70:6d:70:33:a0. A

message is broadcast to the whole network destination Ip 255.255.255.255 ethernet ff:ff:ff:ff:ff:ff.

This is a broadcast message.

Offer

In the offer stage the source IP is the network IP :address 192.168.122.1 ethernet 4a:6c:34:ff:25:06. It returns a message to the destination IP address 192.168.122.163 ethernet 76:70:6d:70:33:a0. This IP

is offered to the client as their leased IP address. This is unicast.

Request

A request is sent from source 0.0.0.0 ethernet 76:70:6d:70:33:a0 to destination 255.255.255.255

ethernet ff:ff:ff:ff:ff:ff asking to be assigned IP 192.168.122.163. This message is broadcast.

Ack

Source IP address 192.168.122.1 ethernet 4a:6c:34:ff:25:06 destination IP 192.168.122.163 ethernet

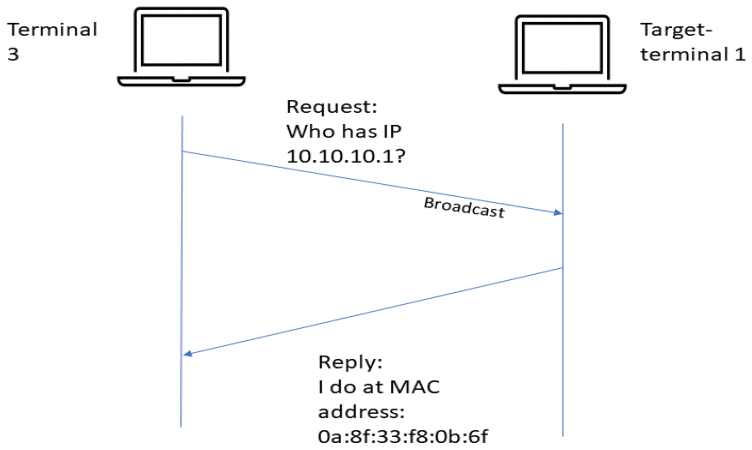
76:70:6d:70:33:a0. This message in unicast. The server has now acknowledged the request committing to the IP lease.

MAC Address

MAC addresses are used in the link layer. MAC addresses are assigned at the time of manufacture. They are the physical address of a node and are unique to that device. MAC addresses are 48bits. The first 24 bits are assigned to the manufacturer by the Internet Standards Body and the last 24 bits are the serial number assigned to the device by the manufacturer.

To send a message to the correct destination the IP address must be converted into the corresponding MAC address. This is done through a process called Address Resolution Protocol (ARP). ARP builds a table which maps remote IP addresses to the physical MAC address of a router.

An example of diagram of how ARP works converting an IP address to the required MAC address of the next hop. This shows an internal network ARP request but works also for external network communication. Instead of the broadcast going to another terminal it will go to the router who can decide how best to send the message and what the next hop is to get the message off the network.



Question 5

Hub

A hub is one of the most basic network devices it is not as sophisticated as a switch or router. It operates on the physical layer of the network. Hosts connect through wires to the hub ports and the information gets broadcast through all ports.

Advantages

Cheap

Disadvantages

100Mbps for the whole hub. Its not scalable the bandwidth is shared across all ports on the device.

Poses a security risk with the messages broadcast to all ports.

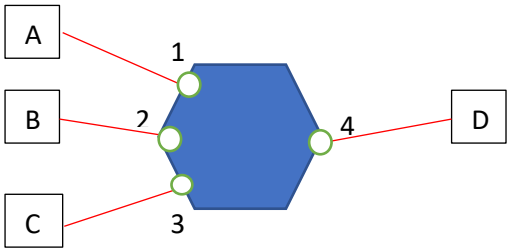
Switches

Switches work on the Link layer of the network and are more sophisticated than hubs. They can be wired or wireless. A switch can direct a message using frame addresses to the right port where the destination device is located, it builds a lookup table through backwards learning to know which device is at which port. A switch has an internal fabric that directs the message this allows for simultaneously sending of messages. The ports are both input and output or full duplex ports. Each port has sole use of the port i.e., there is no multiple access protocol. Switches can have buffers which can help mitigate against varying speeds of transmission or many to one transmits. A buffer allows short term storage to help with overloading where messages can be lost if the message cannot be stored. If the buffer reaches capacity, no more frames can be stored and will be discarded and must be retransmitted.

Backwards learning

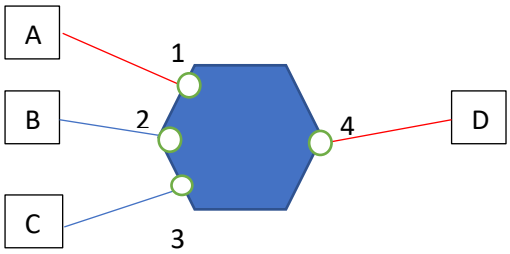
How does the switch find the correct output port for the destination node? Hosts readily able to be moved around. Backwards learning is used to help overcome these issues. A look up table that the switch creates stores the source address of input frames it sends to port if known otherwise it broadcasts to all ports.

In this topology A is sending to D it starts by broadcasting a message to all nodes broadcasting will be red lines. The switch takes MAC address A message and looks at its port and updates the lookup table.



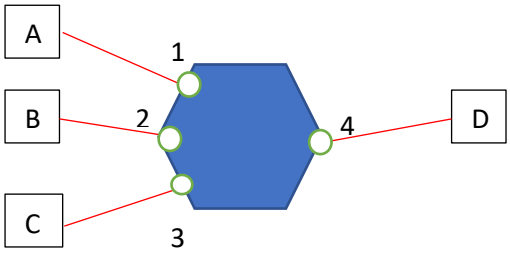
Address	Port
A	1
B	
C	
D	

D then replies to A and the switch store the port for MAC address D. As the switch now knows what port A and D are on messages can be sent directly and not broadcast.



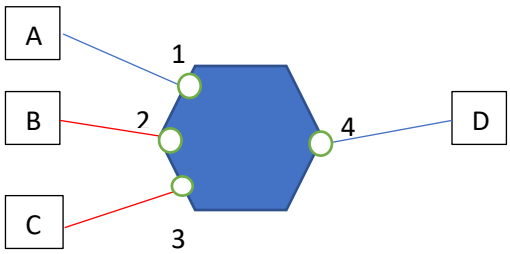
Address	Port
A	1
B	
C	
D	4

If the node with MAC address B was sending to the node with MAC address C the message would first have to be broadcast. The switch would look at the source address which is B and add that port to the lookup table.



Address	Port
A	1
B	2
C	
D	4

Once C responds to B the switch will then add C's port number to the lookup table. And it will continue to check to make sure the table is up to date, and all ports remain correct and connected to the device the switch thinks it is.



Address	Port
A	1
B	2
C	3
D	4

Spanning Tree

A spanning tree is a subset of links that reaches all switches it removes any loops, and each route is a tree structure. It is useful where there is redundancy built into the topology and helps to overcome loops as without this broadcast messages can end up in a continual loop. The spanning Algorithm Runs all the time and searches for the best solutions.

Benefits of the spanning tree method of routing messages are it can be applied to any topology and does not require any configuration. It is also able to adapt to link switch failures which ensures reliability and robustness within the network even if some nodes or connections fail.

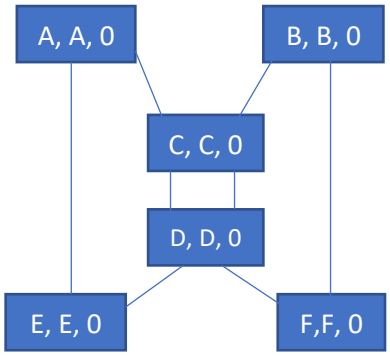
Algorithm

1. Elect the root node, the node with the lowest address.

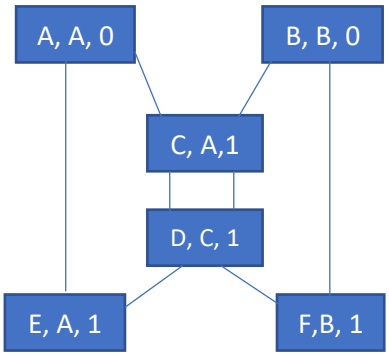
2. Use the shortest distance when growing the tree and in the case of a tie use the lowest address.
3. Turn off the ports if they are not on the spanning tree.

- Each node think they are root in the beginning.
- Each switch sends a message to its neighbours with:
    - Their Address
    - Address of root
    - Distance in hops to root.
- Ports with the shortest distance to the root node are favoured.

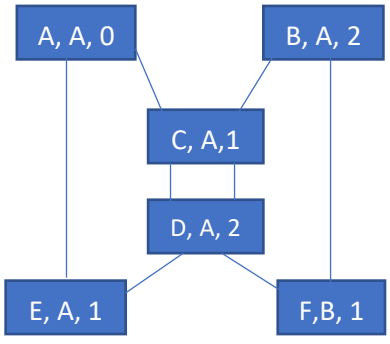
All nodes believe they are root. And they broadcast this to all other nodes.



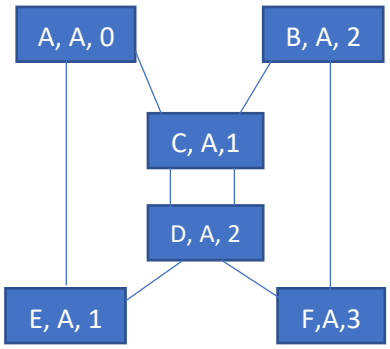
After the initial broadcast has been sent the nodes update the root node with the lowest address from their neighbours

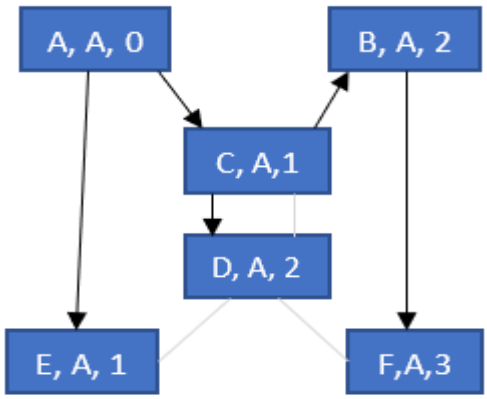


On the second round of sharing information the switches update accordingly



And finally, they all know that A is the root node and how many hops it is away from them.





An example of how the spanning tree might look and the nodes will favour the shortest route when building the paths and switch off the other ports if they are not in the spanning tree. Updates all the time, if a new switch is added it updates, if a node or link fails it updates.

Advantages of switches

A centralised area to run cabling to is more convenient.

It is more reliable than a traditional bus topology where a damaged wire will disrupt the entire network one node failing is not going to affect the other nodes in the network.

Scalable performance, for example 100Mbps per port each device gets access to the same bandwidth through their port they do not have to share bandwidth resources.

Limitations

Switches do not scale well to large networks.

They only work across one link layer.

They do not provide much traffic control as we saw with the spanning tree it may not be the most efficient route.

The spanning tree overcomes a lot of the issues, but it may not be the most efficient route to send the message in the network.

Router

A router works between the Network and Link layer with IP addresses. It is a very sophisticated device that does a lot of work in delivering our data to the correct location. The routers' main function is to join networks together. It uses the datagram model it is given the destination address and each router uses it to forward the packet to the next router who is on one of the paths for the destination address. The router uses ARP to get the MAC address to do the physical sending of the message across the link. A home router is usually a switch and router combined.

Routers provide two key services on the network.

1. Routing

This is computational expensive for the router; it decides which way messages should be sent.

It builds a lookup table from the routing process so it can then just forward message as quickly as possible. It knows where to send messages that do not belong to the same network.

2. Forwarding

Uses the lookup table the routing services built to send the packets in the correct direction.

Forwarding uses the longest matching prefix rule to send the message to the most specific IP address it has for that destination address.

Routing algorithms

Routing algorithm play an important role in our routers. We will take a closer look at Dijkstra's algorithm but there are other ones.

A routing algorithm should be decentralised meaning it should be automatic and not need any human input. The nodes only know information that neighbouring nodes share.

It expands on the spanning tree idea of the switch and builds routes that are most efficient.

There are five properties that we desire when we talk about routing.

1. Correctness finds paths that deliver the right messages to the right node.
2. Efficient paths utilise bandwidth efficiently.
3. Fair paths no nodes are cut off or starved.
4. Fast convergence adapts quickly to changes.
5. Scalability continues to operate effectively even as the network expands.

A Sink tree is the shortest path from every other node in the network to a particular node.

A Source tree is the shortest path from a particular node to every other node in the network.

Dijkstra's Algorithm

Make all nodes tentative set distances from source to 0 and ∞ infinity for all other nodes.

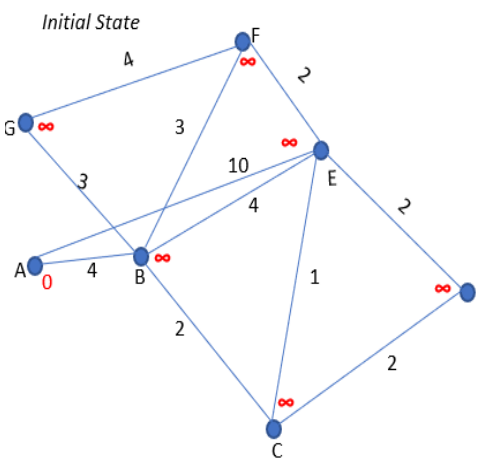
While a tentative node remains:

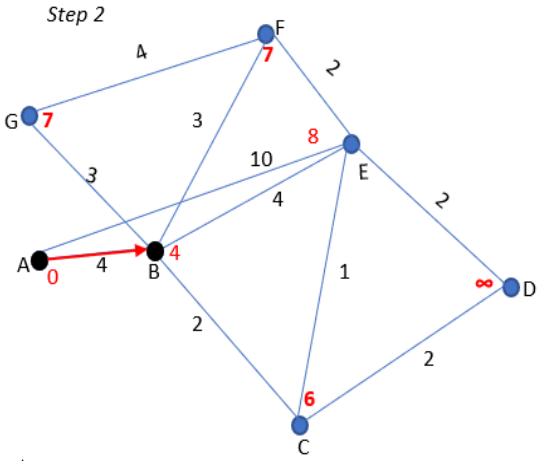
Extract N, a node with the lowest distance

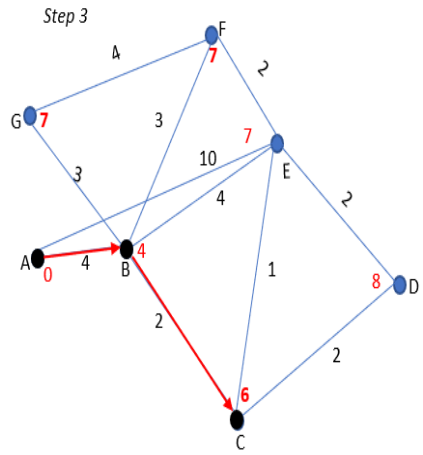
Add link to N to the shortest tree path.

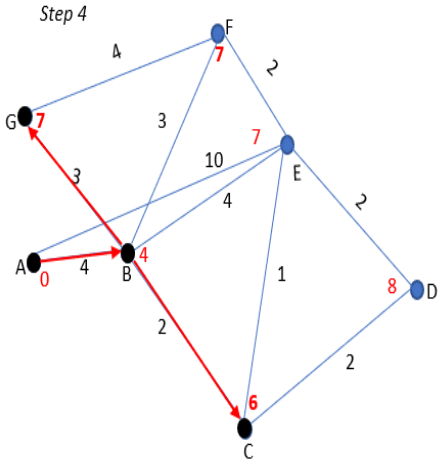
Relax the distances of neighbours of N by lowering any better distance estimates. If the distance works out higher leave as is.

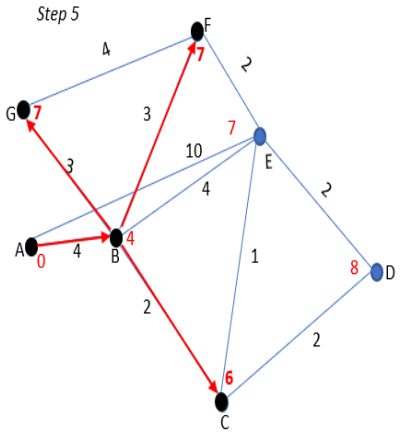
Example of Dijkstra's Algorithm

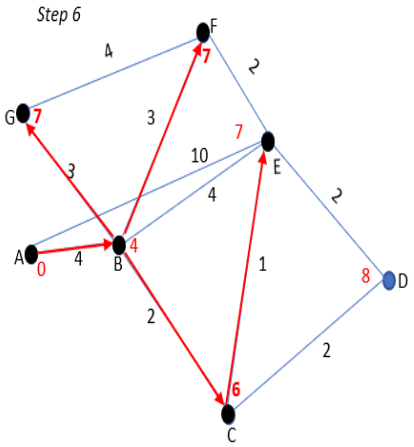


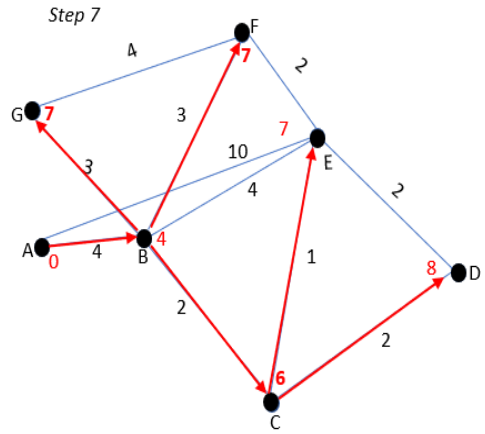












Notes to remember about Dijkstra's algorithm are:

- Sub paths are also shortest paths.
- Gives complete source and sink trees more than is needed for forwarding.
- It requires the complete network topology to work, which we will discuss next.

Link state Routing

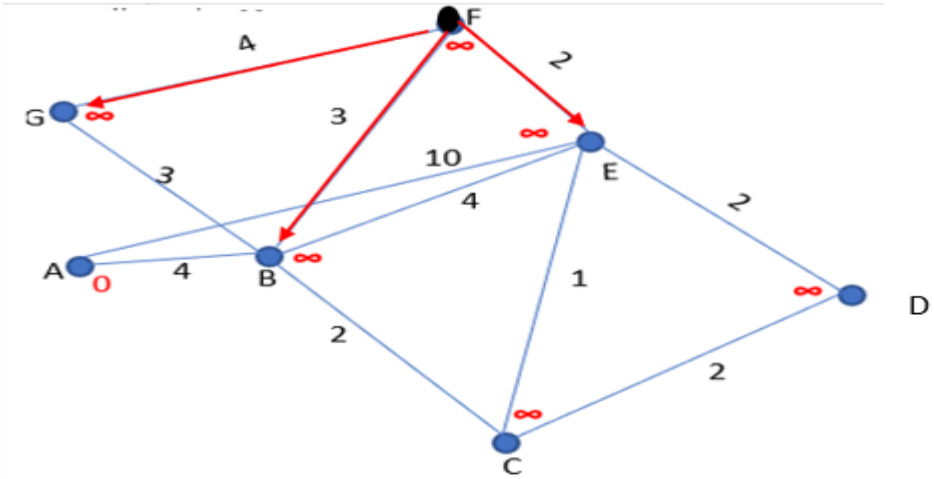
Link State routing is how routers find the full network topology.

Examples are OSPF(Open Shortest Path First used for IP networks

IS-IS Intermediate System to Intermediate System. It is neutral for which type of network addresses it can route for.

Routers need to build a full picture of the network topology, run Dijkstra's algorithm, and build a forwarding table from it.

To build the picture of the network the routers use flood messages which they forward to every other router they are connected to. The Flood message is in the firm of a Link State packet. It describes that nodes portion of the network. The Link state packet has a sequence number, so each node knows which is the most up to date packet it has.



Once E,B,G receive this message they will then forward it onto their neighbours like so until all nodes have received the message.

SEQ. # Node F	
E	2
B	3
G	4

SEQ. # Node E	
A	10
B	4
C	1
D	2
F	2

SEQ. # Node B	
A	4
C	2
E	4
G	3
F	3

SEQ. # Node G	
B	3
F	4

Each node then has the full network topology from combining the information from all the Link State packets it has received it can then run Dijkstra's algorithm and construct the forwarding table from the sink source tree. Updated constantly in case of node failure in the network. If a change happens LSPs get updated, and the routes are recomputed.

F's forwarding table	
To	Next
A	B
B	B
C	E
D	E
E	E
F	----------
G	G

Multipath routing as there can be more than one shortest path the router can choose one to use randomly it includes redundancy in case of node failure and it can improve performance by distributing the routes the messages are sent on as opposed to the same path each time.

Issues with scalability with routing.

Routing computation gets more complex and takes longer.

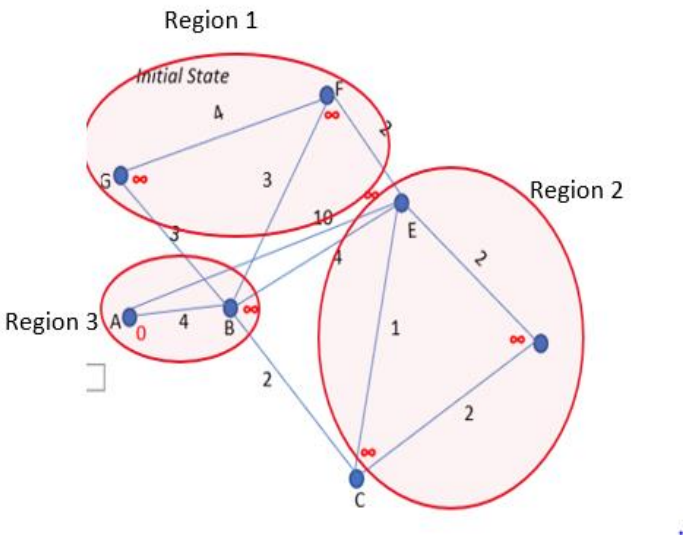
Looking up the next hop will take longer as there is more and more IP addresses added to the lookup table.

Routing messages grow more link state packets need to be sent to keep the network up to date with the full topology.

There are two methods to prevent the lookup table from becoming unmanageable are using IP prefixes and sending messages to blocks of IP's as opposed to a single IP or to route to a region. We can use a larger IP prefix and leave it to the routers in that region to forward the message appropriately.

Example of routing by region:

F's forwarding table	
To	Next
A	B
B	B
C	E
D	E
E	E
F	----------
G	G



F's forwarding table by region		
To	Next	Hops
G	G	1
Region 2	E	1
Region 3	B	1

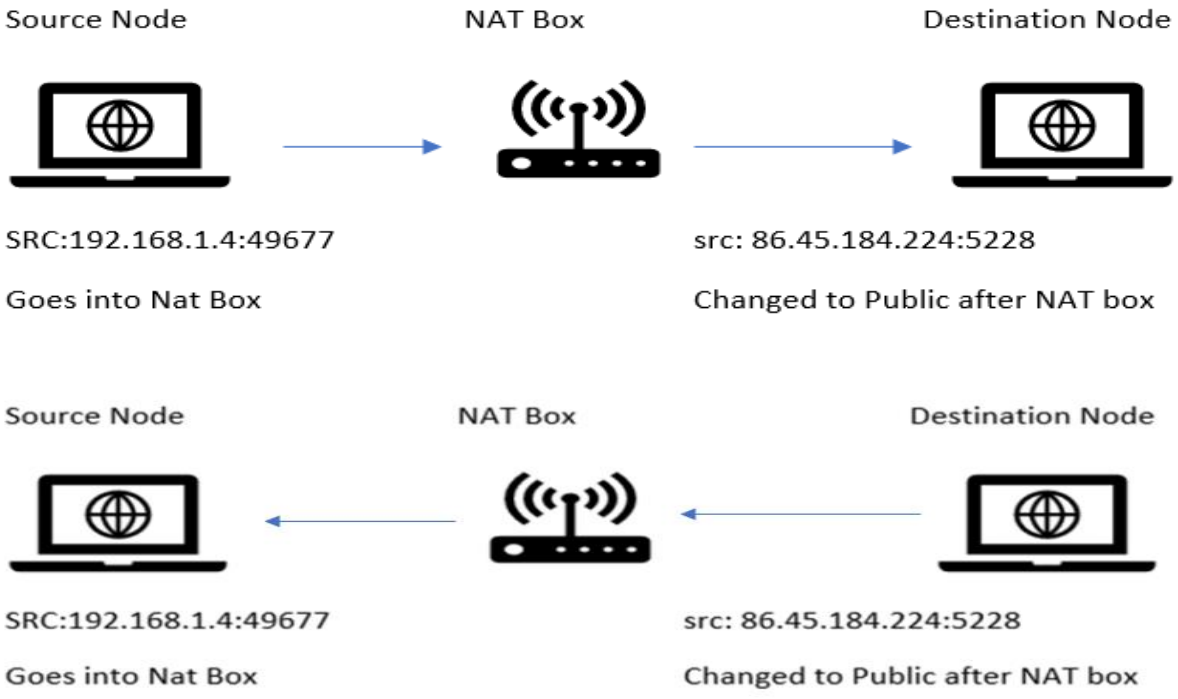
Question 6.

Network Address Translation or NAT works at the network layer with IP addresses.

NAT operates on the fringes of a network and a NAT box is widely used to connect local private networks to an external network. It is needed due to the scarcity of IP addresses. With the use of a NAT box, we can use just a few IP addresses in an internal network to connect the nodes in that network together and these IP addresses can be used in multiple internal networks as they can only communicate through a public IP so many devices on an internal network look like one device to the external networks. The NAT box translate these private IP address into a Public IP address that allows the internal network to interact with an external network like the Internet. The home router contains the NAT box.

NAT works by creating a table made up of the private IP addresses and the device TCP ports and maps them to the Single public IP address with a unique port so that each device has a 1-1 mapping to the external IP.

	Internal IP: port	External IP: port
My Laptop	192.168.1.4:49677	86.45.184.224:5228
Second laptop	192.168.1.3:33060	86.45.184.224:5357
Phone	192.168.1.1:49669	86.45.184.224:9308



The table is created when there is an outgoing message. It maps the outgoing IP address and port number of the computer to the external IP address and port number in the router.

Advantages

The use of NAT relieves pressure on the dwindling supply of IPv4 addresses.

It is easy to deploy your router provides the NAT service automatically, it does not need external configuration.

Firewalls help with privacy. It works because outside contacts can not connect to you unless an outgoing connection has been made first. A single public IP helps with privacy also as it can represent multiple users and devices.

Disadvantages

An external node cannot contact an internal node unless the internal node has made contact first, in particular with servers.