Name: Lum Chee Xiang Michael (Lan Zhixiang)
Student ID: 111102750
Assignment 3

Module: Introduction to Computing and the Internet
Module number: CO1110-01

University of London International Programmes
BSc in Computing and Informations: Introduction to Computing and the Internet
Module number: CO1110-01
Assignment 3

Name: Lum Chee Xiang Michael (Lan Zhixiang) Module: Introduction to Computing and the Internet
Student ID: 111102750 Module number: CO1110-01
Assignment 3

Introduction

As this module is is known as 'Introduction to Computing and the Internet', it is understood that the study material can be broadly classified into two parts, namely the computer science portion which focuses on the technicalities of computing such as the hardware used to make up a complete computer system (like the processor and memory), and the software component which consists of the operating system that is responsible for serving as the 'middleman' between the machine's hardware and the end-user. Along the line, we also learnt how data is represented in computers, and that understanding was tested in the recently-submitted Coursework 2.

Now that we are well into the second half of the semester, we are ready to leave the computer science section of the module and proceed to part two of the course material, which covers networking technologies. Based on the questions set by the University of London for this coursework, it can be determined that the focus of study in the networking portion of this module is on network topologies and the TCP/IP stack, with the latter being especially important due to it being the fundamental tool that makes communication over the Internet possible today.

In short, the requirements for the questions set in Coursework 3 are as follow:

Question 1 – This question is particularly straightforward with its requirements: it asks that the candidate provide a detailed description of the network topologies as listed within, as well as an explanation of the advantages and disadvantages that are associated with the particular topology, all of which should be accompanied with a well-labelled diagram to illustrate the schema of said topologies.

Of particular note is 1D, in which the candidate is alerted to the fact that there exists two commonly-used bus topologies, namely backbone or multipoint. That the word '**or**' is used implies that the candidate only needs to select one of the bus topology variants for use in his answer, and not to provide both.

Question 2 – This question is a test on a candidate's understanding on the aspects of the TCP/IP stack, or more specifically, how the use of headers are essential in helping networked machines establish a connection under the TCP/IP model. Also required in this question is the candidate's ability to describe and explain the procedure in which this connection can be established with the use of headers in the TCP/IP stack, as well as any prerequisites that both machines may need to meet before actually doing so.

Lastly, the question also states that it is fine for candidates to make logical assumptions in the description of the procedure; this suggests that the candidate is allowed to choose a suitable scenario to illustrate his understanding of how the connection could be established in a particular context.

Question 3 – Like Question 2 before it, this question is also aimed at testing the candidate's understanding of the TCP/IP stack, except that the emphasis now is on the IP part instead. Specifically, the candidate is required to know how to identify various types or classes of networks based on the nature of their IP addresses, and to also be capable of deriving the addresses of the subnet mask in both binary and decimal formats.

Finally, the question ends by asking the candidate to not only explain how network addresses can be used to identify the different network classes they belong to, but to also be capable of describing in some detail the advantages and disadvantages of the class-based approach in IP addressing. As there is no mention within the question about having the candidate propose measures or workarounds to mitigate the shortcomings of the class-based approach, it can be assumed that there is no real need to do so.

Name: Lum Chee Xiang Michael (Lan Zhixiang) Module: Introduction to Computing and the Internet
Student ID: 111102750 Module number: CO1110-01
Assignment 3

Question 1

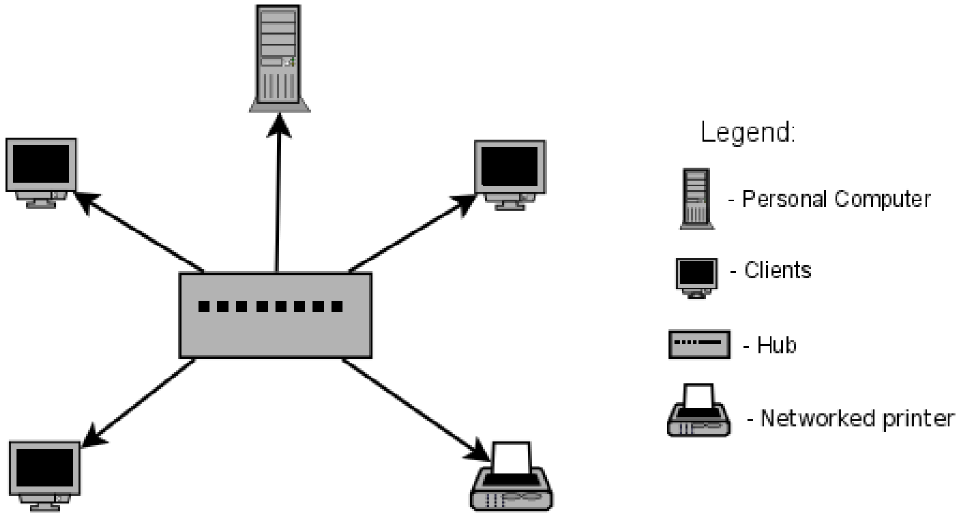
Describe concisely each of the standard network structures below. Draw a topology diagram to show your understanding of each structure, including as many types of the network nodes as possible, for example, (i) Station, (ii) Repeater, (iii) Hub, (iv) Tap, and (v) End Cable. Discuss the advantages and disadvantages for each network structure

(a) Star
(b) Ring
(c) Mesh
(d) Bus (backbone or multipoint link)

Answer (Star topology)

The **star topology** is but one of many different ways in which the connections between different computers or systems on a network can be structured, and, according to certain sources, is claimed to be the most commonly utilized topology when used in the context of modern-day network implementations (Ciccarelli et al, 2008, p. 112). To understand why this particular topology can come to enjoy such status today, we will need to take a look at its defining characteristics and implementation.

In its simplest form, the star topology can be illustrated in a diagram as shown below:



By looking at the diagram, it is readily apparent that the single defining characteristic of the star topology lies in the presence of a single **central hub or switch** (Lowe, 2005, p. 16) which is responsible for facilitating communications between **all** the devices (henceforth referred to as 'clients' or nodes') that are connected to it (Comer, 2009, p. 230). If we are to use our diagram above as an example, a client which wants to send a document to the networked printer will perform the following steps:

1) Establish a connection with the central hub or switch
2) Send the message to the central hub or switch
3) which will in turn deliver the message to the networked printer for printing.

Because data and information sent from one client to another are delivered to the receiving party almost directly without going through any intermediate nodes (save for the central hub or switch), each node appears to be directly connected to each other (logically, that is) as if they were “immediate neighbours” (Dumas & Schwartz, 2009, p. 132)

Lastly, the diagram also provides a hint as to why this particular topology is known as a 'star' topology; since every single connection in the star topology eventually ends at a single point (the central hub or switch), the outcome bears a slight semblance to the skeletal view of a star or the “spokes in a bicycle wheel”, hence its name (Ciccarelli et al, 2008, p. 112).

Advantages

Logically speaking, there must be something which the star topology has got to be doing right if it is able to claim the status of being the world's most commonly used network structure in today's “modern network implementations” (Ciccarelli et al, 2008, p. 112). This would imply that the star topology boasts several characteristics which would be seen as being advantageous or desirable to both end users and network administrators.

The list of advantages associated with the star topology are described in the following subsections.

Potentially lower data access and transfer times

Using the diagram and the example in the preceding paragraphs, it was shown that, regardless of the number of nodes or client machines that are connected to the central hub or switch, data that is sent from one client to another only needs to travel through two links (Duck & Read, 2003, p. 30); one from the sender to the central hub or switch, and one from the hub or switch to the receiver.

Barring extreme or worse-case situations where the load on the central hub or switch may be so great that it effectively ends up bottlenecking the rate of data transfer between the connected clients, the fact that data only needs to travel a maximum of two 'hops' to reach its eventual destination (Dumas & Schwartz, 2009, p. 132) means that is potentially capable of providing a network with “higher throughput and performance”, of which the implementation of Fast Ethernet is an example of such an advantage being realized (Kasera, Narang & Narang, 2005, p. 60).

Isolation of nodes with broken connections

Because the nodes or clients in a star topology are logically connected to one another via a physical connection to the central hub or switch, it can be inferred that a broken connection between one node to the central hub or switch will not have any adverse effects on the entire network as whole. This is because a broken connection will only sever the affected node from the network while all the other nodes or clients will still remain connected to the network and can thus proceed with data transmission as though nothing has happened (Kasera, Narang & Narang, 2005, p. 60).

In other words, as long as the central hub or switch remains online, a network-wide failure will never take place.

Administration and management ease

As stated earlier, all connectivity in a star topology is facilitated by a central hub of switch, by which must all clients in the network must be physically connected to (either by copper cables or wireless technology) in order to gain access to the network. This centralized connection means that it is extremely easy for a network administrator to hook up and administrator terminal to the network and actively manage the network as required, since it is possible to keep track of any machine that is currently connected to the central hub or switch. This in turn makes it easier to seek out nodes with broken connections (Ciccarelli et al, 2008, p. 112).

Similarly, the star topology makes it easier for a network administrator to add new devices to the network. If we assume that all connections to the central hub or switch are done by copper cables, adding a new device to the network is just a matter of simply wiring the device to the hub or switch with a capable and letting the hub or switch's built-in intelligence automatically handle the connection on its own, while removing a device from the network is done in a similar manner (Ciccarelli et al, 2008, p. 112). More importantly, all this is done without any form of interruption or downtime to the network.

Lastly, the presence of the central hub or switch also greatly simplifies the task of upgrading the network to take advantage of faster data transmission speeds, as the network administrator only needs to replace the central hub or switch with a newer one and connectivity can be re-established with all the devices (Ciccarelli et al, 2008, p. 112). In some cases, the upgrade can even done by simply flashing the firmware installed on the hub or switch; this method has the added benefit of eliminating any network downtime as opposed to the previous method where some downtime is inevitable due to the network administrator having to take the network offline for a period of time to manually install the new hub or switch before re-establishing connectivity.

Cost-effective

The fact that the star topology is claimed to be the most widely used network structure today implies that much of the networking hardware available in the market are built or designed to support the star network topology as a standard feature (Ciccarelli et al, 2008, p. 112). This would mean that there are an abundance of compatible products available for such a topology, which would in turn suggest that infrastructure costs for setting up a network based on the star topology would be considerably low.

Disadvantages

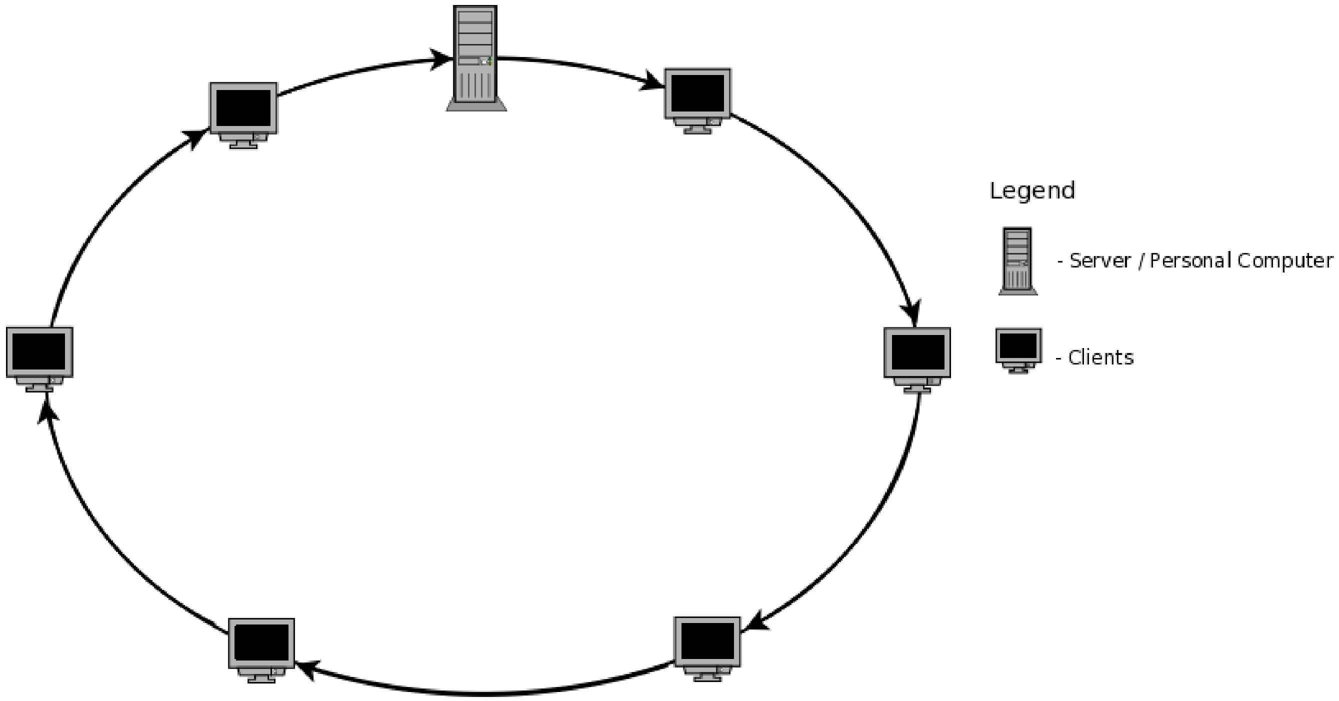
One minor disadvantage about a network based off the star topology lies in the need to invest in a central hub or switch (Ciccarelli et al, 2008, p. 112). While we have mentioned earlier that the costs of setting up such a network is considerably low due to the variety of equipment available for it and the ease of management involved, it does not change the fact that the presence of the central hub or switch implies an added expense which network administrators may need to take into account when setting up a network structure.

Ironically, the advantages brought about by the central hub or switch end up emphasizing its single major flaw; because every single device in a star network is connected to one another **via** it, its failure will cause a disruption in the entire network (Kasera, Narang & Narang, 2005, p. 60). This can be seen in our earlier diagram: if we were to remove the block that represents the central hub or switch in the diagram, all connection paths between the different devices are immediately severed. This implies a **single point of failure**, which can be said to the star topology's biggest and most severe disadvantage.

Answer (Ring topology)

The ring topology is another one of the four basic topologies upon which built and structured upon; it is claimed by some sources (Ciccarelli et al, 2008, p. 112) that this particular topology was originally designed by IBM for use with its own networking equipment, and that it was once a very popular choice of topology in the early days of networking (Lowe, 2005, p. 18).

In its simplest form, the ring topology can be illustrated in a diagram as shown below:

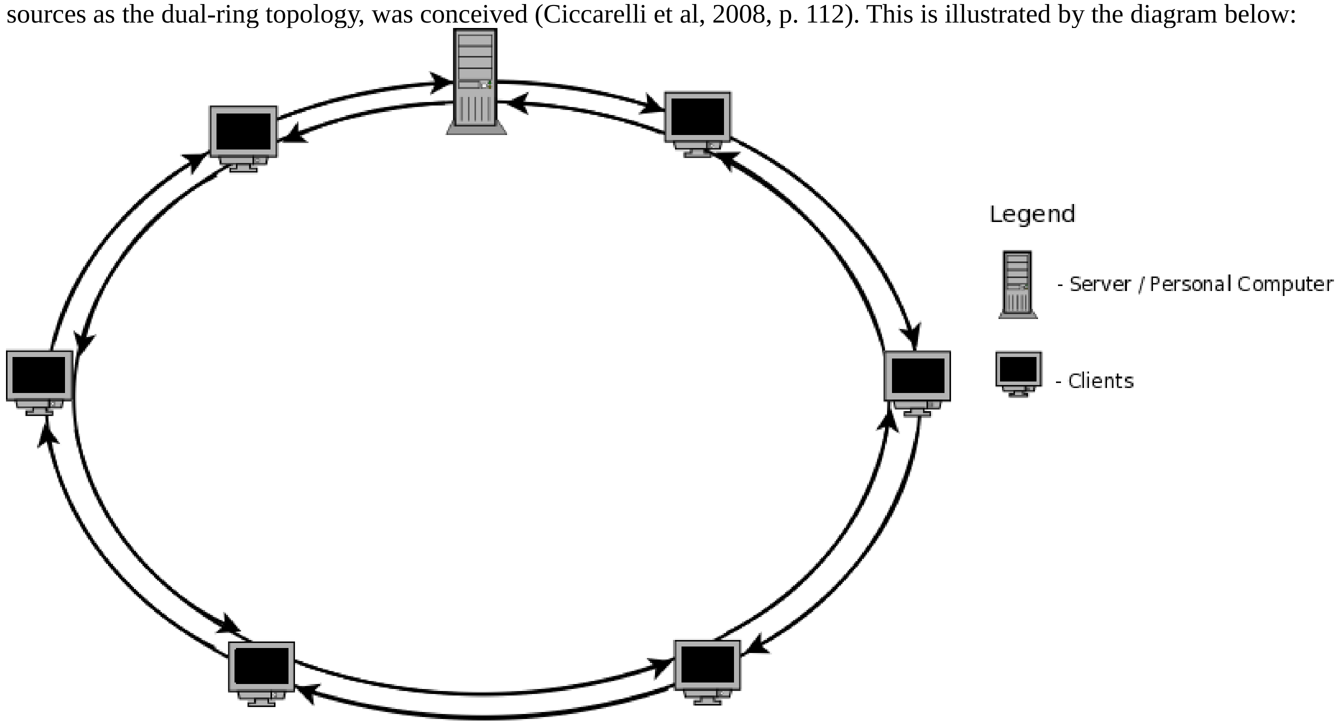


As illustrated by the diagram above, it can be seen that the key feature of a ring topology lies in the way each device is connected to one another. While the star topology had each individual device connected to a central hub or switch which was responsible for facilitating and controlling connectivity and data transfer between them almost directly, the ring topology works by connecting each device directly to its **immediate neighbours only** (Dumas & Schwartz, 2009, p. 132), and each subsequent device that is to be hooked up to said network will be connected in such a manner until an unbroken loop has been formed.

At this point, the network is considered to be complete and operational, and data can be transferred from one node to another node. How this is done can be described in a sequence of steps as shown below. For simplicity, we will make use of a uni-directional ring topology (i.e, data is sent in only one direction) as illustrated in our diagram.

1) A device that needs to send out data or information to another designated device on the network prepares the info and transmits it to the device that is directly connected to it (Kasera, Narang & Narang, 2005, p. 60). In our illustration's case, it will be the device on its right, as that is the direction of our data flow.
2) If the device that receives the data is not the intended recipient, it is not allowed to accept the message, and is required to retransmit the data to the next connected device on its right (Lowe, 2005, p. 18).
3) The process continues until the data is received by the intended recipient, upon which an acknowledge is sent to the original sender and the sequence halts.

As network technology advanced, a newer and more efficient implementation of the ring topology, described by some sources as the dual-ring topology, was conceived (Ciccarelli et al, 2008, p. 112). This is illustrated by the diagram below:



In the case of the dual-ring topology, data is still transmitted between devices in the same manner as previously described in the uni-directional ring network; the main difference is that the dual-ring network supports the transmission of data in both directions. This development would have various effects on the network, which we will discuss in the next section.

Advantages

The list of advantages associated with the ring topology are described in the following subsections.

Reliability

Only one device on the network is allowed to transmit data or information at any point of time (Ciccarelli et al, 2008, p. 110 - 111); if a device A wants to send a message while a device C is currently doing so, device A must wait for device C to finish its task and for the recipient to send an acknowledgement is sent back to the original sender before it can transmit its data. Because of this, packet collision is non-existent, which in turn improves communication reliability. This applies to both uni-directional and dual-ring (bi-directional) ring topologies.

Redundancy (Dual-ring / bi-directional only)

In the event that a node is forced offline due to cable faults, the presence of an additional ring allows for the network to automatically bypass the faulty links in order to ensure that transmitted data will still manage to reach its intended recipient, unless the recipient was already forced offline due to dead hardware (Ciccarelli et al, 2008, p. 110 – 111). This built-in redundancy (Kasera, Narang & Narang, 2005, p. 60) prevents a single break in the loop from shutting the entire network down.

Disadvantages

The list of disadvantages associated with the ring topology are described in the following subsections.

Potential downtime

The 'loop-based' nature of a ring topology has its own downside: while it is effective in eliminating packet collision by ensuring that only one device on the network is allowed to transmit data at any given time, it also means that a break in the loop at one section caused by either faulty hardware, faulty cables or a combination of both will force the entire network offline, even if all the other sections are still operational (Kasera, Narang & Narang, 2005, p. 60). This can be somewhat prevented by employing a bi-directional implementation of the topology, but in the rare even that **both** rings suffer a single break in the loop, the network will still be taken offline until the network hole is patched.

In addition, the diagrams that have been used for illustrating the ring topologies in the preceding sections also highlight another flaw, this time in the design of the network itself; there is no way the network can be expanded or scaled down without forcing it offline for a period of time (Ciccarelli et al, 2008, p. 112). This is because any change to the physical network requires that the closed loop be first 'broken' before the installation or removal of any hardware can be performed; this translates to the aforementioned downtime until the physical hardware is ready to be rejoined with the rest of the network.

Potentially higher data access times

Because data is not sent directly from one device to another, but indirectly via a series of connected devices until it finally reaches its destination, it means that data needs to travel a much longer distance in order to reach the intended recipient. This is even more prevalent in uni-directional ring networks: the intended recipient may be directly connected to the left of the sender, but if the data flow in the network runs clockwise, the data needs to traverse almost the entire length of the ring before finally reaching the recipient.

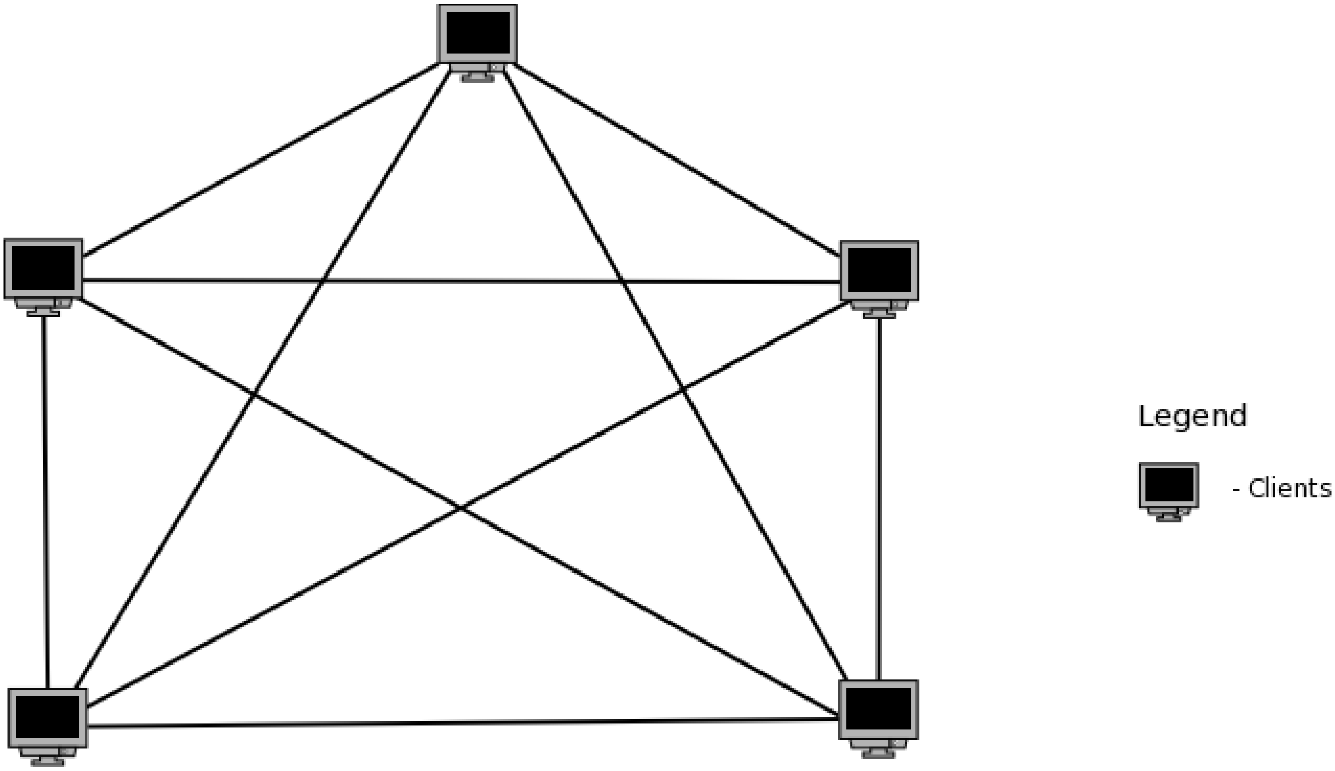
Cost

As stated earlier, the ring topology is a fairly old network structure that was originally developed by IBM for use with their own hardware (Ciccarelli et al, 2008, p. 112). Given its age, it would be logical to deduce that specialized equipment for supporting a ring network are not as readily available as those for a star network, and that those are are still being produced and sold will probably be costlier than the latter. This translates to additional costs that must be borne by users, which may be a deciding factor in certain situations.

Answer (Mesh topology)

Before we start, it is important to note that there exists at least two different kinds of topologies that can be classified under the term 'Mesh topology', namely a **partial mesh topology** and a **full mesh topology** (“Mesh topology network”, n.d., paras 2 – 3) http://www.buzzle.com/articles/mesh-topology.html**.** For simplicity and consistency, we will assume that the question is asking for an explanation on the characteristics of a **full mesh topology.**

In its simplest form, the layout for a network structured under the full mesh topology (henceforth referred to as simply 'mesh topology) can be visualized in the following diagram:



As can be seen, the key characteristic of a mesh network lies in each node having access to a direct path of connection with every other single node in the network. This means that there exists multiple ways data can be transmitted from one node to another, and that the transmitted data is almost guaranteed to eventually reach its destination, as the only way for the transmission to fail will be for the entire network to be forced offline.

Due to the presence of interconnected web of paths for transmitting data from one node to another, a mesh network typically features some form of built-in intelligence which allows it determine the most effective route for getting the message across to the intended recipient. Logically, the direct route is often considered to be the fastest possible route, but in the event that this route is either experience abnormal spikes in network activity or is downright broken due to connection failure, the network needs to be capable of automatically determining the next best possible route to the receiver in order to reduce data access and waiting times. This process is done in the background and is typically not visible to the user.

For this reason, the mesh topology is widely considered to be the most complicated topology (“Mesh topology network”, n.d., para 6) http://www.buzzle.com/articles/mesh-topology.html to be used in the modern-day networking context.

Advantages

The list of advantages associated with the mesh topology are described in the following subsections.

Full redundancy

As stated previously, the key property of a full mesh topology lies in the presence of direct connection routes from one node to another; all these routes, when combined together, form a highly complex web of possible routes in which data could possible be transmitted from one node to another.

If one were to trace all the possible routes that the transmitted data could take to reach its destination in the diagram above, he or she would eventually come to the conclusion that there is virtually no way a packet can fail to reach a receiver unless a) the entire network is forced offline or b) the particular receiver is physically unavailable due to faulty hardware or other reasons. For the most part, Case B is not a valid cause as a node which does not exist in the network physically would be logically incapable of being identified as a receiver, and such such should not be even able to receive data from any other connected device in the network in the first place.

This just leaves Case A as the only plausible way data can fail to reach its destination in a mesh network, which is also extremely unlikely to happen considering how the number of connections (let us assume that each line of connection between two nodes represents a single copper cable) correspond to the formula of **[n x (n – 1)] / 2**, where n is the number of nodes present in the network. In our earlier diagram, our network had 5 nodes; this translates to 10 discreet paths available for data to travel from one node to another. In a real world implementation where the number of connected nodes can be quite large, a fully connected mesh will have so many discreet paths available that it is virtually impossible for all the connections to fail abruptly without warning.

The extent of this redundancy makes a mesh network highly desirable for use in critical operations where network downtime cannot be allowed to happen under any circumstances.

Intelligent routing

Because of the complexity involved in navigating the interconnected web of discreet paths available in a full mesh network, the network needs to feature some form of built-in intelligence that will allow it to determine the most efficient path transmitted data should take in order to ensure that it reaches its destination in the least amount of time.

An example of how this can be accomplished would be to consider a situation where the direct path between two nodes is not accessible either because of a faulty cable or that the particular path is experience a sudden spike in network traffic that renders it incapable of accepting any more data. In such a case, the network's built-in intelligence will allow it to quickly determine the presence of the next best alternative path that will result in the required data being transmitted to the receiver by passing it through an intermediate node.

Disadvantages

The list of disadvantages associated with the mesh topology are described in the following subsections.

Design complexity

Designing and constructing a proper mesh network is an extremely challenging task that is typically considered to be beyond the capabilities of most skilled network designers and administrators. Because of its complex nature, a poorly designed mesh network may end up being not only physically messy to set up, but can also cause management nightmares for personnel as it will complicate the already difficult job of administering and monitoring the network.

Also, it is possible (albeit quite unlikely) that the full redundancy nature of the network may result in connection failures along certain direct routes being able to slip by unnoticed by network administrators because of the network's capability to automatically route data through alternative paths in the background on the fly. At best, this may cause a very slight anomaly in terms of a minor spike in network traffic along the re-routed path which may not be significant enough to capture an administrator's attention, and thus the faulty cable may never be detected at all unless a through network audit is carried out.

As such, networks of such a nature are usually only considered for implementation after consultations with experts or external consultants have been held.

High operational and setup costs

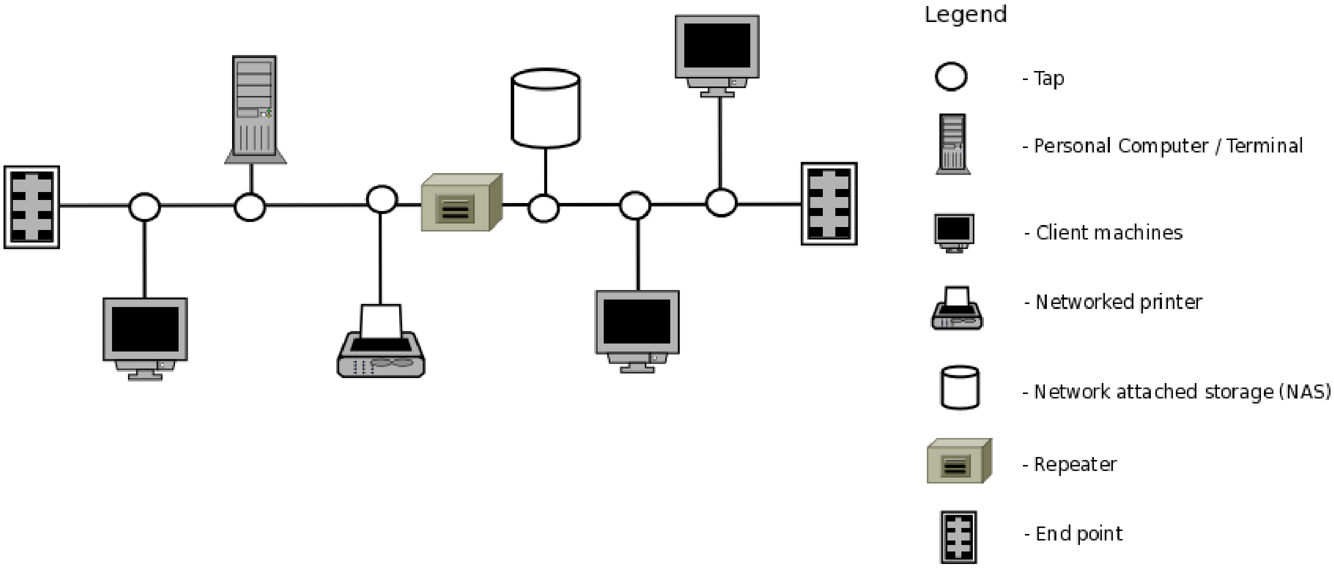
Like the star topology concept discussed earlier, the full mesh topology's single biggest flaw has its roots in its biggest advantage; its full redundancy quality. Because so many cables are needed to establish the foundation for the infrastructure of a mesh network, “a large number of I/O ports are needed” to facilitate its implementation. This implies that a mesh network requires much more physical hardware to be present in order for it to even work in the first place.

In addition, hardware capable of supporting such demanding needs in a mesh network are typically sold at a premium, and are usually difficult to install as well. This combination of tangible and intangible costs, combined with the sheer complexity of the network and the difficulties involved in maintaining and administering it, makes the mesh topology extremely expensive to implement, operate and maintain. This in turn makes the mesh topology extremely impractical for use in large networks, as it is expected that the aforementioned costs will only increase exponentially with respect to the desired size of the network, thus effectively limiting its usefulness to much smaller networks only.

Answer (Bus topology – Backbone)

The last network topology we are going to look at for this question is the **bus topology,** or more specifically, one of its implementations commonly known as the **backbone.** According to some sources, this particular topology can be most commonly found in LAN setups (Lowe, 2005, p. ???).

In its simplest form, the bus topology and its backbone implementation can be illustrated in a diagram as shown below:



To understand the bus topology's key features and its modus operandi, we will need to visualize the network as consisting of one single long cable (usually coaxial), with each node being connected to this extremely long cable via a tap which allows it to intercept data that is being transmitted along it (Lowe, 2005, p. ???). In a way, it can be said to share some similarities with the ring topology that was discussed earlier, in which all data is communicated via a single path with each node poised to intercept said data as and when needed.

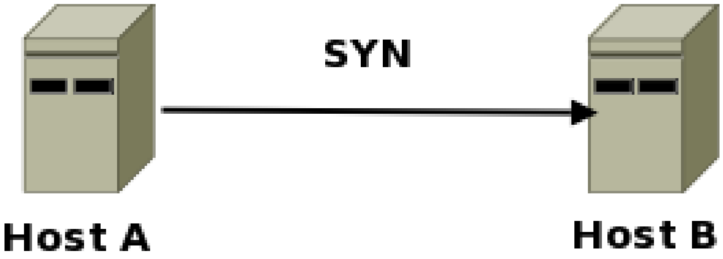
In order to transmit data in a bus topology, an uninterupted signal path from one end of the cable must passed through to the other end, but

Question 2

Explain, with a suitable diagram, the use of headers in routing protocols under the TCP/IP model. Give an example where two computers A and B wish to establish a communication. What essential steps do they need to take under the TCP/IP model? Show step by step how headers can be implemented and useful for routing. Add details of assumptions in your discussion if necessary.

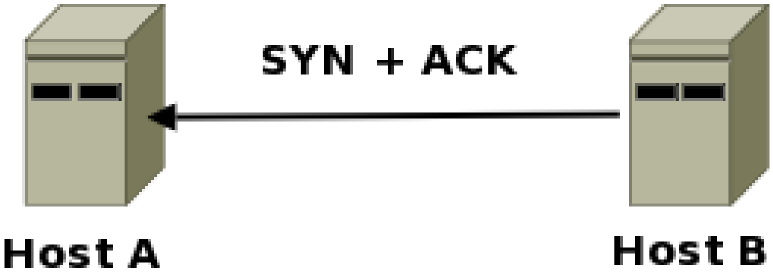
In order for two computers to start sharing information between each other, they will first need to establish a connection under the TCP / IP model. In most cases, this initial connection is done using the **three-way handshake**, in which a very simplified description of the process can be illustrated with the following diagrams shown below:

Step one: Sending the request



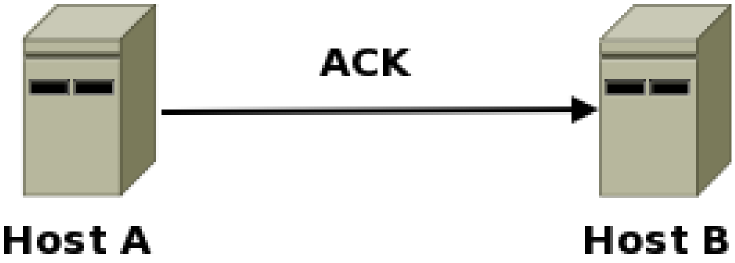
We will assume that Computer A, also known as Host A, is the machine which wants to establish a connection with Host B under the TCP model. To do so, Host A will need to send a special packet known as a TCP **syn**chronize packet to Host B first, as illustrated in the diagram above.

Step 2: Acknowledging the request



If Host B receives the SYN packet and decides to accept the connection with Host A, it will have to send back another packet containing both an SYN bit and an **ACK**nowledgement bit to Host A to acknowledge that it had received the request to establish a connection.

Step 3: Acknowledging the acknowledgement



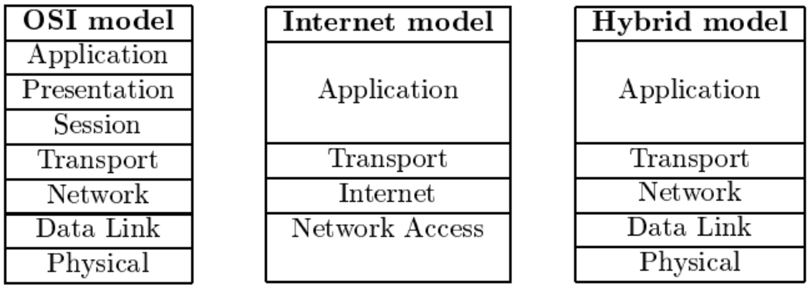
If A receives B's SYN + ACK packet it will now have confirmation that there exists a usable route between itself and Host B. However, this is not enough to establish a connection yet, as Host B needs a confirmation from A that the latter has received its acknowledgement and is aware of a possible connection path between them. To fulfil this need, Host A needs to send out one last ACK bit to complete the process, as shown in the illustration above.

Step 4: Connection Established

Connection Established
Host A
Host B

With that done, a connection is finally established between Hosts A and B via the Three-Way Handshake process under the TCP model.

With the connection established, Host A is now able to start sharing data between itself and Host B. According to the study guide provided by the University (Kibble, 2006), the TCP /IP model consists of four main layers, namely the Network layer, Internet layer, Transport layer and lastly, the Application layer, as shown in the diagram below (pp. 12 – 13):

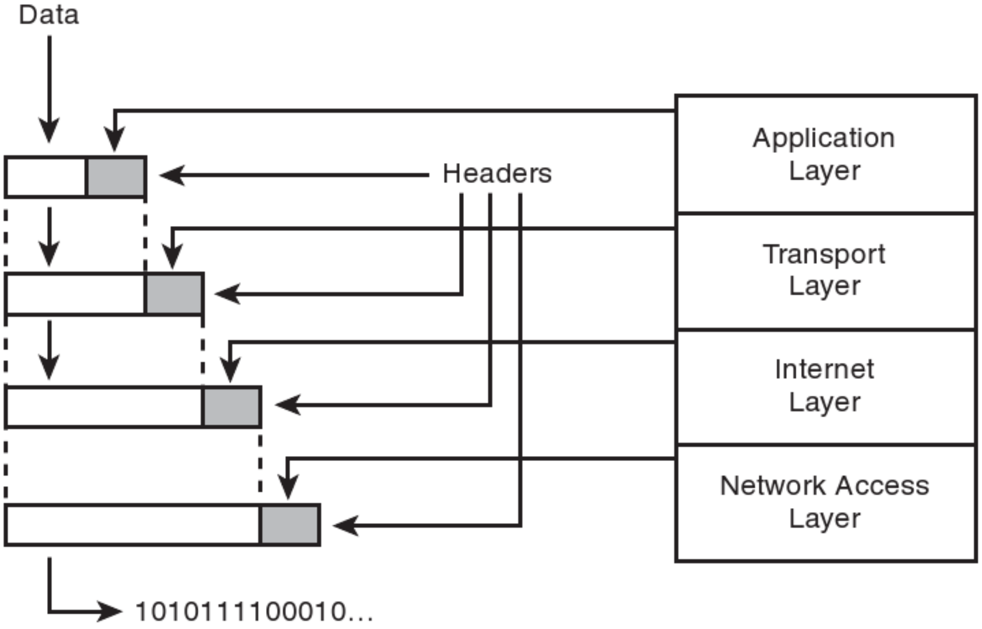


OSI model
Application
Presentation
Session
Transport
Network
Data Link
Physical

Internet model
Application
Transport
Internet
Network Access

Hybrid model
Application
Transport
Network
Data Link
Physical

The study guide also mentions that communication is achieved by “dividing packets into header and data sections”, and that data which passes from one layer to has a header “containing information for software at the corresponding layer on the receiving system” attached to it (Kibble, 2006, p. 15). Exactly how this works can be explained via a diagram, as shown below (Casad, 2009, p. 27):



The steps in which this is done are as follow:

1. Host A establishes a connection with Host B via the Three-way Handshake procedure as described earlier.

2. The **data** that Host A is supposed to send to Host B is prepared; since the data resides in the Application layer of the TCP / IP model, a header containing information about the data at the application level is added to it.

3. The data with its application-layer header is then passed down to the next layer, the Transport layer, whose role is to “facilitate end-to-end communication over the internetwork” and “allowing logical connections to be made between devices” so that data can be sent from host to host either reliably or unreliably (Kozierok, 2005, p. 130). Regardless of the reliability of the transmission, it needs to ensure that the transmitted data is 'aware' of its eventual destination. A header containing this information is affixed to the message, thus creating a data segment.

4. The segment is then sent down to the next layer, which is known as the Internet layer. It is in this layer that the segment is prepared for transmission over the network to its eventual destination by providing information about the receiver's IP address, as well as the types of **routing protocols** that are to be used in the transmission process, such as RIP, OSFP and BGP, among many others. All this information is supplied in the form of a header which is attached to the segment to form a datagram.

5. The datagram is finally passed down to the lowest-level layer, the Network Access layer. In this layer, information about the best possible route the data can take while travelling from Host A to Host B based from consultations with **routing tables** are added to the datagram in the form of an additional header. At this point, the datagram becomes a frame and it is subsequently transmitted to Host B via the optimal route as specified in the Network Access header.

6. When the frame reaches Host B at the Network Access layer, the corresponding header is stripped from the frame, with the latter subsequently being passed on to the nest higher layer, the Internet layer.

7. When the data reaches the Internet layer, the header containing the receiver's IP address and the routing protocol used is discarded, and the remaining segment is subsequently passed on to the next higher-level layer, the Transport layer.

8. Upon reaching the Transport layer, the corresponding header on the transmitted data is discarded; based on whether the data was intended to be sent reliably or not, Host B may send an acknowledgement to Host A to confirm the integrity of the received data before subsequently passing the data up to the highest-level layer, the Application layer.

9. The relevant application (a web browser in most cases) displays the data that was sent from Host A to Host B, and the process ends.

Question 3

Consider the class-based IP addressing scheme. Explain how the following network addresses can be used to identify a particular network. Discuss the advantages and disadvantages of the class-based IP addressing.

(a) 112.32.7.28:80;
(b) 38.34.2.1:21.

Your solutions should include all your work, and certain details, further assumptions and related topics if appropriate, such as the binary version of address and mask, boolean AND mask/address, address class or network address, subnet address, host, and application.

Answer (a)

The first step in using a network address to identify its network involves converting each segment of its numerical address into its binary equivalent. Therefore, each numerical block in the address 112.32.7.28 will need to be expressed in binary, with the results being as follow:

112 / 2 = 56 R 0
56 / 2 = 28 R 0
28 / 2 = 14 R 0
14 / 2 = 7 R 0
7 / 2 = 3 R 1
3 / 2 = 1 R 1
1 / 2 = 0 R 1

Reading remainders from bottom up, we get 111 0000, therefore $(112)_{10} = (0111\ 0000)_2$

32 / 2 = 16 R 0
16 / 2 = 8 R 0
8 / 2 = 4 R 0
4 / 2 = 2 R 0
2 / 2 = 1 R 0
1 / 2 = 0 R 1

Reading the remainders from bottom up, we get 10 0000, therefore $(32)_{10} = (0010\ 0000)_2$

7 / 2 = 3 R 1
3 / 2 = 1 R 1
1 / 2 = 0 R 1

Reading the remainders from bottom up, we get 111, therefore $(7)_{10} = (0000\ 0111)_2$

28 / 2 = 14 R 0
14 / 2 = 7 R 0
7 / 2 = 3 R 1
3 / 2 = 1 R 1
1 / 2 = 0 R 1

Reading the remainders from bottom up, we get 1 1100, therefore $(28)_{10}$ = $(0001\ 1100)_2$

Putting the above answers together will return the provided network address of 112.32.7.28 in binary format, as shown in the table below:

Network address (decimal)	112	**.**	32	**.**	7	**.**	28
Network address (binary)	0111 0000	**.**	0010 0000	**.**	0000 0111	**.**	0001 1100

Based on the first three digits of the network address, it can be determined that this network address is part of a Class A network. Assuming that this network is a public network, the subnet mask for this particular network will be **255.0.0.0**, which we will need to convert into binary to determine its network ID and host ID. We can make this assumption based on the following grounds:

- Private IP addresses always start with either:
  - 10.x.x.x for Class A networks,
  - 172.16.x.x for Class B networks, and
  - 192.168.x.x for Class C networks. (Lim, 2011, paras 5 – 6) - http://vcoutonalim.org/2011/01/05/how-to-determine-public-vs-private-ip-addresses/

Since the first octet of our network address has the decimal value of 112 and not 10, it can be deduced that the network address of 112. 32.7.28 is an IP address from a public network.

The next step in determining the network and host IDs from this network address will be to convert the Class A subnet mask address of 255.0.0.0 into its binary equivalent:

255 / 2 = 127 R 1
127 / 2 = 63 R 1
63 / 2 = 31 R 1
31 / 2 = 15 R 1
15 / 2 = 7 R 1
7 / 2 = 3 R 1
3 / 2 = 1 R 1
1 / 2 = 0 R 1

Reading the remainders from bottom up, we get 1111 1111, therefore $(255)_{10}$ = $(1111\ 1111)_2$. Therefore, the binary equivalent of the subnet mask address $(255.0.0.0)_{10}$ = $(1111\ 1111\ .\ 0000\ 0000\ .\ 0000\ 0000\ .\ 0000\ 0000)_2$.

With this we are now able to obtain the network ID of the provided address by performing an AND operation with the binary equivalents of both the network address and the subnet mask address, with the results being as such:

Network address (Binary)	0111 0000	**.**	0010 0000	**.**	0000 0111	**.**	0001 1100
Subnet mask address (binary)	1111 1111	**.**	0000 0000	**.**	0000 0000	**.**	0000 0000
Network ID (binary)	0111 0000	**.**	0000 0000	**.**	0000 0000	**.**	0000 0000

Finally, we convert the binary value of the network ID into its decimal equivalent, which returns the following result:

$$\begin{aligned}(0111\ 0000)2 &= (1 \text{ x } 2^4)_{10} + (1 \text{ x } 2^5)_{10} + (1 \text{ x } 2^6)_{10} \\ &= (16)_{10} + (32)_{10} + (64)_{10} \\ &= (112)_{10}\end{aligned}$$

Therefore, the network ID of the address is 112.0.0.0.

Lastly, to determine the network's Host ID, we take the binary equivalent of the subnet mask and subtract it from the binary equivalent of the network address, like so:

Network address (Binary)	0111 0000	**.**	0010 0000	**.**	0000 0111	**.**	0001 1100
Network ID (binary)	0111 0000	**.**	0000 0000	**.**	0000 0000	**.**	0000 0000
Host address (binary)	0000 0000	**.**	0010 0000	**.**	0000 0111	**.**	0001 1100

This gives us a host address of $(0000\ 0000\ .\ 0010\ 0000\ .\ 0000\ 0111\ .\ 0001\ 1100)_2$ in binary, which we need to convert to its decimal equivalent:

$$(0000\ 0000)_{2\text{ -}} = (0)_{10}$$

$$\begin{aligned}(0010\ 0000)_2 &= 1 \text{ x } 2^5 \\ &= (32)_{10}\end{aligned}$$

$$\begin{aligned}(0000\ 0111)_2 &= 1 \text{ x } 2^2 + 1 \text{ x } 2^1 + 1 \text{ x } 2^0 \\ &=(4)_{10} + (2)_{10} + (1)_{10} \\ &= (7)_{10}\end{aligned}$$

$$\begin{aligned}(0001\ 1100)_2 &= 1 \text{ x } 2^4 + 1 \text{ x } 2^3 + 1 \text{ x } 2^2 \\ &= (16)_{10} + (8)_{10} + (4)_{10} \\ &= (28)_{10}\end{aligned}$$

This gives us a value of 0. 32.7.28. Therefore, the network's specifications are as follow:

Name: Lum Chee Xiang Michael (Lan Zhixiang)
Student ID: 111102750
Assignment 3

Module: Introduction to Computing and the Internet
Module number: CO1110-01

IP address = 112.32.7.28
Type: public Class A network
Network address: 112.0.0.0
Host address: 0.32.7.28
Subnet mask: 255.0.0.0
Port: 80

Finally, port 80 is the port used to facilitate data transfer over the Internet via the HTTP protocol, which suggests that the sender is sending information that will most likely be viewed at the receiver's end via a web browser.

Answer (b)

As was the case with the previous section, the first step in using a network address to identify its network involves converting each segment of its numerical address into its binary equivalent. Therefore, each numerical block in the address 38.34.2.1 will need to be expressed in binary, with the results being as follow:

38 / 2 = 19 R 0
19 / 2 = 9 R 1
9 / 2 = 4 R 1
4 / 2 = 2 R 0
2 / 2 = 1 R 0
1 / 2 = 0 R 1

Reading remainders from bottom up, we get 10 0110, therefore $(38)_{10}$ = $(0010\ 0110)_2$

34 / 2 = 17 R 0
17 / 2 = 8 R 1
8 / 2 = 4 R 0
4 / 2 = 2 R 0
2 / 2 = 1 R 0
1 / 2 = 0 R 1

Reading the remainders from bottom up, we get 10 0010, therefore $(34)_{10}$ = $(0010\ 0010)_2$

2 / 2 = 1 R 0
1 / 2 = 0 R 1

Reading the remainders from bottom up, we get 10, therefore $(2)_{10}$ = $(0000\ 0010)_2$

1 / 2 = 0 R 1

Reading the remainders from bottom up, we get 1, therefore $(1)_{10}$ = $(0000\ 0001)_2$

Putting the above answers together will return the provided network address of 38.34.2.1 in binary format, as shown in the table below:

Network address (decimal)	38	**.**	34	**.**	2	**.**	1
Network address (binary)	0010 0110	**.**	0010 0010	**.**	0000 0010	**.**	0000 0001

Based on the first three digits of the network address, it can be determined that this network address is part of a Class A network. Assuming that this network is a public network, the subnet mask for this particular network will be **255.0.0.0**, which we will need to convert into binary to determine its network ID and host ID. Once again, we can make this assumption based on the following grounds:

- Private IP addresses always start with either:
  - 10.x.x.x for Class A networks,
  - 172.16.x.x for Class B networks, and
  - 192.168.x.x for Class C networks. (Lim, 2011, paras 5 – 6) - http://vcoutonalim.org/2011/01/05/how-to-determine-public-vs-private-ip-addresses/

Since the first octet of our network address has the decimal value of 38 and not 10, it can be deduced that the network address of 38.34.2.1 is an IP address from a public network.

The next step in determining the network and host IDs from this network address will be to convert the Class A subnet mask address of 255.0.0.0 into its binary equivalent:

255 / 2 = 127 R 1
127 / 2 = 63 R 1
63 / 2 = 31 R 1
31 / 2 = 15 R 1
15 / 2 = 7 R 1
7 / 2 = 3 R 1
3 / 2 = 1 R 1
1 / 2 = 0 R 1

Reading the remainders from bottom up, we get 1111 1111, therefore $(255)_{10} = (1111\ 1111)_2$. Therefore, the binary equivalent of the subnet mask address $(255.0.0.0)_{10} = (1111\ 1111\ .\ 0000\ 0000\ .\ 0000\ 0000\ .\ 0000\ 0000)_2$.

With this we are now able to obtain the network ID of the provided address by performing an AND operation with the binary equivalents of both the network address and the subnet mask address, with the results being as such:

Network address (Binary)	0010 0110	**.**	0010 0010	**.**	0000 0010	**.**	0000 0001
Subnet mask address (binary)	1111 1111	**.**	0000 0000	**.**	0000 0000	**.**	0000 0000
Network ID (binary)	0010 0110	**.**	0000 0000	**.**	0000 0000	**.**	0000 0000

Finally, we convert the binary value of the network ID into its decimal equivalent, which returns the following result:

$$\begin{aligned}(0010\ 0110)_2 &= (1 \text{ x } 2^5)_{10} + (1 \text{ x } 2^2)_{10} + (1 \text{ x } 2^1)_{10} \\ &= (32)_{10} + (4)_{10} + (2)_{10} \\ &= (38)_{10}\end{aligned}$$

Therefore, the network ID of the address is 38.0.0.0.

Lastly, to determine the network's Host ID, we take the binary equivalent of the subnet mask and subtract it from the binary equivalent of the network address, like so:

Network address (Binary)	0010 0110	**.**	0010 0010	**.**	0000 0010	**.**	0000 0001
Network ID (binary)	0010 0110	**.**	0000 0000	**.**	0000 0000	**.**	0000 0000
Host address (binary)	0000 0000	**.**	0010 0010	**.**	0000 0010	**.**	0000 0001

This gives us a host address of $(0000\ 0000\ .\ 0010\ 0000\ .\ 0000\ 0111\ .\ 0001\ 1100)_2$ in binary, which we need to convert to its decimal equivalent:

$$(0000\ 0000)_{2\ -} = (0)_{10}$$

$$(0010\ 0010)_2 = 1 \text{ x } 2^5 + 1 \text{ x } 2$$
$$= (34)_{10}$$

$$(0000\ 0010)_2 = 1 \text{ x } 2$$
$$= (2)_{10}$$

$$(0000\ 0001)_2 = 1 \text{ x } 2^0$$
$$= (1)_{10}$$

This gives us a value of 0. 34.2.1. Therefore, the network's specifications are as follow:

IP address = 38.34.2.1
Type: public Class A network
Network address: 38.0.0.0
Host address: 0.34.2.1
Subnet mask: 255.0.0.0
Port: 21

Finally, port 21 is the port used to facilitate data transfer over the Internet via the FTP protocol, which suggests that the sender and receiver are most likely to be communicating with each other via an FTP client, and that some form of file sharing is currently taking place between the machines.

Advantages and Disadvantages of the class-based IP addressing scheme

Before we describe any advantages or disadvantages pertaining to any scheme or implementation, it is important that we are able to understand why the said scheme was even thought up of, or implemented in the first place. Therefore, we will attempt to determine the rationale behind the implementation of the class-based IP addressing scheme first before proceeding to explain the advantages and disadvantages of such a scheme.

Apparently, the class-based IP addressing scheme, which is also known as the first and original IP addressing system used to facilitate the transport of data on the internetwork, was conceived due to the developers of the IP syststem recognizing that organizations come in various sizes and would subsequently have different needs for IP addresses to establish a presence on the Internet (“IP 'Classful' Addressing Overview and Address Classes”, n.d, paras 1 – 3, http://www.tcpipguide.com/free/t_IPClassfulAddressingOverviewandAddressClasses.htm). To solve this issue, it was decided that all the available addresses were divided and grouped into classes in which each class would host a subset of the total number of addresses available based on the current addressing scheme (“Function Description:, 1981, paras 1 – 6, http://tools.ietf.org/html/rfc791#section-2.2); the goal was to ensure that organizations of varying sizes would always have enough IP addresses to support varying numbers of connected hosts based on the class type network allocated to them; this can be illustrated in a table as shown below (Wilder, 1998, p. 135)

Class	Valid network IDs	Valid Host IDs
A	1 – 126	1 – 255.255.254
B	128.1 – 192.254	1 – 255.254
C	192.0.1 – 223.255.254	1 – 254
D	224.0.0.1 – 239.255.255.255	Not applicable
E	240 – 255.255.255.255	Reserved

Having done that, we are now in a better position to understand the advantages of the class-based IP addressing scheme as proposed by the Information Sciences Institute for the Defense Advanced Research Projects Agency (DARPA), and what are some of the scheme's disadvantages that became apparent when Internet usage and the subsequent demand for IP addresses grew exponentially.

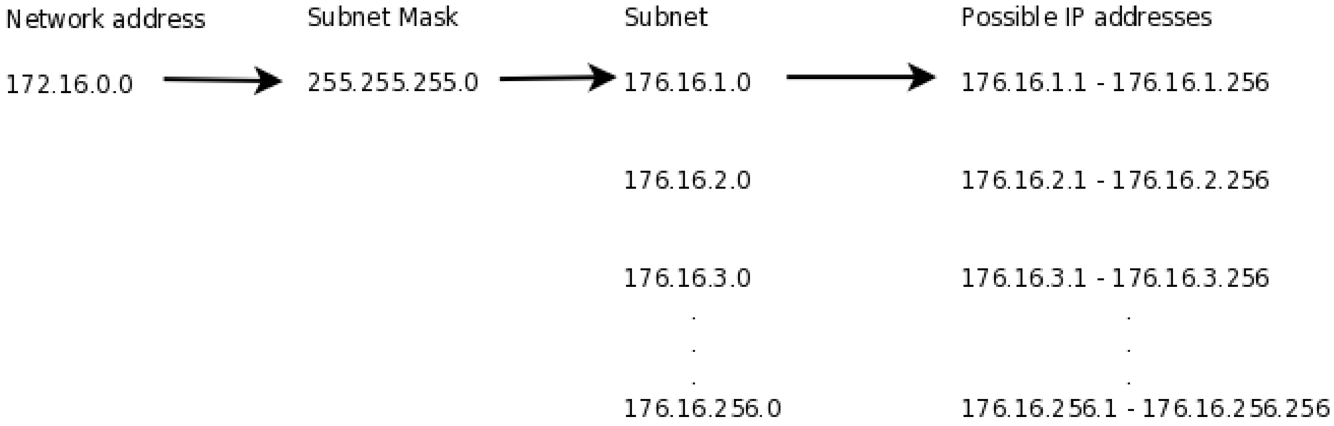
Advantages

One of the biggest advantages in the class-based addressing scheme is centred around the concept of subnetting, which, as described by Tanenbaum (2011), is a technique designed to grant organizations the flexibility to “assign blocks of addresses” within itself (p. 468).

To understand how this flexibility is made possible, we need to look at how a specific class's subnet mask can be used on a different class's address. For example, we know that a standard Class B network, when utilized with a standard Class B subnetmask, is capable of supporting up to 16,382 networks, with each network further supporting up to 65,536 hosts, disregarding forbidden values (Tittel, 2002, p. 158 – 159). For example, if an organization which purchased the 172.16.x.x block of network addresses were to randomly assign network and host IDs / addresses to a large number of devices that are being connected to the network (eg: Device 1 gets 172.16.1.2, Device 2 gets 172.16.200.200, and so on), the difficulty involved in managing and subsequently administering or troubleshooting increases exponentially as there is no systematic procedure in place to manage the allocation of addresses to the devices.

This makes it difficult (but not impossible) for a network administrator to keep track of the addresses of devices that are currently connected to the network, akin to hunting down pieces of a jigsaw puzzle that have been hidden in different rooms across different houses along a street.

However, when a Class C subnet mask is applied onto said Class B network, it suddenly becomes possible for a network administrator to 'divide' the aforementioned network block of 176.16.x.x into a combination of 256 subnets, which are in turn capable of supporting up to 256 hosts, disregarding forbidden values. This can be illustrated in the diagram below:



Network address		Subnet Mask		Subnet		Possible IP addresses
172.16.0.0	→	255.255.255.0	→	176.16.1.0	→	176.16.1.1 - 176.16.1.256
				176.16.2.0		176.16.2.1 - 176.16.2.256
				176.16.3.0		176.16.3.1 - 176.16.3.256
				.		.
				.		.
				.		.
				176.16.256.0		176.16.256.1 - 176.16.256.256

(adapted from “Subnetting IPv4 networks with standard subnet masks”, *Schaum's Outlines – Computer Networking*, Titel, 2002, p. 160)

With this, some semblance of order starts to surface: instead of allocating network-connected devices an address randomly, a network administrator can now take advantage of subnetting by allocating each device with an address from a specific subnet. For example, it is now possible for an organization to configure four subnets (176.16.1.x, 176,16.2.x, 176.16.3.x and 176.16.4.x) and explicitly specify that networked printers be allocated to the 176.16.1.x subnet, desktop PCs be assigned to the 176.16.2.x subnet and so on. This leads to the aforementioned advantage of flexibility (able to designate specific subnets for specific purposes), which in turns translates to simplicity in both implementation and management (Dumas & Schwartz, 2009, p. 285).

Lastly, another advantage of subnetting, as described by Dumas & Schwartz (2009) is that it allows an organization to establish a connection to the Internet using only a single IP address as opposed to the alternative of having to perform the same task for every single subnetwork, thus providing said organizations with the means of using their network addresses more efficiently. (p. 285).

Disadvantages

Probably the single major flaw present in the class-based addressing scheme lies in the decision made by the Internet's designers in determining the maximum size of each network class (i.e, defective by design). As have been discussed earlier, the scheme was born out of the realization that different organizations have different needs for IP addresses due to their varying sizes (“IP 'Classful' Addressing Overview and Address Classes”, n.d, paras 1 – 3, http://www.tcpipguide.com/free/t_IPClassfulAddressingOverviewandAddressClasses.htm). That a Class A network address block would support up to 16,777,214 connected hosts for an astronomical total of 2,147,483,648 individual addresses (“Class A network”, n.d, paras 2 – 3) meant that it was way too big all except the largest organizations to consider using.

In contrast, a Class C network block sits on the other extreme end of the scale with support for only 256 hosts, which would be considered as too small or limiting for most organizations today, as they will have to purchase and manage additional network network blocks if their networking needs exceed the 256 hosts limit (Dumas & Schwartz, 2009, p. 283). This resulted in most organizations opting for the next best option: to purchase a single Class B network block that was capable of supporting a maximum number of 65,536 hosts, which was (and probably still is) deemed as “just right” to meet its needs as well as provide a reasonable buffer for eventual expansion even if it meant that most of the available addresses would never be allocated for a very long time or at all, especially if the claim of a majority of Class B network holders having no more than 50 connected hosts is to be believed (Tanenbaum & Wetherall, 2011, p. 468).

This fact translates into large scale wastage of network addresses, which has been singled out as one of the major reasons for the exhaustion of IPv4 addresses, a problem that the world is facing today (cite study guide). If we were to use the study mentioned above as an example, this would mean that, out of the 65,536 hosts that have been allocated to an organization, at least 65,488 addresses would never be used. Similarly, a large learning institute may have purchased a Class A network block capable of supporting more than 16 million hosts, but it is extremely unlikely that said institute would ever be able to utilize a majority of these allocated hosts. Such wastage, when compounded across multiple organizations all over the world, results in an enormous loss of potential addresses (Dumas & Schwartz, 2009, p. 283).

This wastage also hurts the effectiveness of subnetting; while we have mentioned earlier that the advantages of the class-based networking scheme are centred around subnetting, its capabilities are heavily limited if that much address wastage is present in the network. Even though subnetting makes network management much more orderly, easier, flexible and efficient, it is incapable of arresting the wastage of addresses.

For example, an organization which has 50 hosts under a Class B network of 176.10.x.x may be capable of allocating subnetworks and its corresponding host addresses efficiently (eg: 176.10.1.x for one department, 176.10.2 for another department and so on), but it does not change the fact that 65,488 addresses remain unallocated.

In short, regardless of how one wants to see it, efficient wastage is still wastage.

References

Computer Networks - Fifth Edition (International Edition)
Andrew S. Tanenbaum, David J. Wetherall
Published 2011, Boston, Massachusetts, Pearson Education Inc., Prentice Hall.

Day 3: How to determine Public vs Private IP addresses
Videoconferencing Out on a Lim
Published January 5, 2011, Janine Lim
http://vcoutonalim.org/2011/01/05/how-to-determine-public-vs-private-ip-addresses/
Date: 16 Feb 2012

Internet Protocol Classes - Network and Host ID
Firewall.CX: The site for networking professionals
Published May 17, 2011, no author
http://www.firewall.cx/networking-topics/protocols/protocols-ip/165-protocols-ip-network-id.html
Date: 16 Feb 2012

The TCP/IP companion: A guide for the common user
Matin R. Arick, Anura Guruge
Published 1993, Massachusetts, John Wiley and Sons, Inc.

Network Analysis, Architecture, and DEsign (3rd Edition)
James D. McCabe
Published 2007, Massachusetts, Elsevier Inc, Morgan Kaufmann Publishers

Schaum's Outlines: Computer Networking
Ed Tittel
Published 2002, USA, The McGraw-Hill Companies, Inc.

Principles of Computer Networks and Communications
M. Barry Dumas, Morris Schwartz
PUblished 2009, New Jersey, Pearson Prentice Hall Inc

A guide to the TCP/IP protocol suite
Floyd Wilder
Published 1998, Boston, Artech House Publishers

Communication Networks - Principles and Practice
Sumit Kasera, Nashit Naring, Sumit Narang
Published 2005, India, McGraw-Hill Communications

Computer Networks and Internets Fifth Edition
Douglas E. Comer
Published 2009, New Jersey, Pearson Prentice Hall

Data Communications and Computer Networks for Computer Scientists and Engineers - Second Edition
Michael Duck, Richard Read
PUblished 2003, London, Pearson Prentice Hall

Wiley Pathways - Networking Basics
Patrick Ciccarelli, Christina Faulkner, Jerry FitzGerald, Alan Dennis, David Groth, Tony Skandier, Frank Miller

Published 2008, Massachusetts, John Wiley and Sons, Inc.