Principles of computer networks

ASSIGN BUSTER

In this assignment I am going to describe the types of networks available and how they relate to particular network standards and protocols and I am also going to describe, using examples, why different network standards and protocols are necessaryLANThis is type of network which covers a small office, home or a school network. A LAN uses either wired Ethernet or wireless RF technology. Using a LAN can be much easier when there is a printer available or sharing a file throughout the network.

Updating software is much easier because updating software will automatically update all the other software's. LAN has much higher transmission rates because it is wired connection rather than wireless. Ethernet and Wi-Fi as most widely used technologies, however many others such as token rings have been used before. This relates to standard IEEE 802. 2.

This standard allows two connectionless and one connection orientated operational mode: Type 1 which allows frames to be sent to a single destination or multiple destinations on the same network is a connectionless mode. Type 2 is the oriented operational connection mode. In this mode it uses something called sequence numbering which makes sure that when the data is send it gets to the destination in the correct order and not a single frame has been lost. Type 3 which is also a connectionless service, but only support point to point communication. Infrared is related to this service because in computer infrared network it can receive and transmit data either through the side of the device or the rear side of the device. When connections are made using Microsoft Windows Infrared the same method used for LAN connections can be used.

Infrared technology has been extended to allow more than two computers to be connected semi permanent networks. The advantage of a LAN is that the same physical communication path can be shared by multiple devices. For example it there is a printer, a computer and the internet connection the LAN will allow connections to the printer and it will also allow connections to the internet. If a software is loaded onto the file server that all the computers on the network can use it. There are quite a few drawbacks of a LAN network. For example security measures need to be taken so that users cannot access unauthorised areas.

It is quite hard to setup the network. Skilled technicians are needed to maintain the network. Yet the biggest disadvantage is that if the file server goes down than all the other computers on thenetworkare affected as well. WANThis type of network covers a wider area.

It is used over high speed, long distance communications such as computers in two different areas. A WAN can also be shared. For example two occupants in two buildings can share the wireless connection to a third person, or a business or anyone or anything they wish to do so. Data is safe, secure and quick when it is transmitted between two computers. WAN can also be used to connect different types of networks together for example a WAN network connected to a LAN networks.

The reason behind this is that it is AppleTalk. It is a cheap LAN architecture which is a standard model built for all Apple Macintosh computers and laser printers. It also supports Apple LocalTalk cabling scheme as well as Ethernet and IBM token ring. AppleTalk can connect to standard computers which do

not have AppleTalk. This all relates to FDDI standard which stands for Fibre Distributed Data Interface. It is a backbone of a wide area network.

It uses fibre optic cable to transmit data up to supported rate of 100 Mbps. An advantage of a WAN it allows secure and fast transmission between two computers. Data transmission is inexpensive and reliable. Sharing a connection is easy as well because it allows direct connectivity. A WAN also allows sharing of software and resources to other workstations connected on the network.

Disadvantage of a WAN network is that the signal strong all the time so anyone trying to hitchhike a connection can use the WAN connection it is not protected. WAN are slow and expensive to set-up. They also need a good firewall to stop intruders using the connection. Client/Server NetworkThe client is a application on a workstation dependent upon a server to do the operations.

For example an e-mail client such as Outlook Express, it sends and receives mail. Another example is a web server; it is a client program at the user’s computer which can access information at any server in the world. If both the client and sever are running on the same computer or the location than this is known single seat set-up. Advantage of a client/server network is they can be more secure because there is only one administrator and he control the network so he can put passwords on or do whatever he wants. Client/server’s are flexible so new technology can be integrated into the system. Network runs faster because data is handled by a machine.

Data security and files are controlled through the server. Troubleshooting is easy because the fault would normally be found on the server because it has all the setting and configurations and not the individual machines. It one computer has a firewall than the rest of the connected computer have a firewall. Disadvantages of a client/server networks is that they are expensive and difficult to set-up initially. It the client/server fails than everything every else fails. Older OS such as Windows NT cannot are not compatible.

Major drawback is that it can cause network congestion which then results in network performance, the speed and many other things. Peer-to-Peer NetworkIn a Peer-to-peer network a couple of computers are connected together without the use of a server and they share the resources. A ADHOC connection can be categorized as a peer-to-peer network. Computers connected together in an office or a school classroom using wires can also be classed as a peer-to-peer network. These are physical peer-to-peer networks.

Network protocols and applications which set-up connections with other user through the use of a internet are called peer-to-peer applications. Advantage of a pee-to-peer network is that the individual has rights rather than the administrator. You can control the machine and define what it is used for. Peer-to-peer networks are lot easier to set-up because only the OS need configuration.

It also works out cheaper and a administrator is not required either. Also in a peer-to-peer network any workstation can be a server or a user workstation. There are also drawbacks of this type of a network. They are a lot less secure.

They take a lot of time to maintain the software on an individual workstation. Network performance can be a issue because peer-to-peer is designed for a small network when to a bigger network of let’s say 10 or more computers than the network speed will decrease making it difficult to expand. PANIt stands for Personal Area Network and used for communication between computer devices which include telephone and also PDA’s. As well as using to communicate with PDA’s it can also be used for connecting to next level up in the next hierarchy and connecting to the Internet. PAN could be wired with a USB pen or even a wireless PAN can be setup using technologies such as IRDA, Bluetooth and zigbee.

Bluetooth standard is related to PAN because it is a wireless protocol which exchanges data over short distances from fixed and mobile devices which make up the PAN. Benefit of using Bluetooth is that it can overcome the problem of synchronization. Bluetooth in other words is a standard and communication protocol which has been designed for low power and cost transceiver microchips in every device. Another benefit of using Bluetooth is that as long as the transmission device has enough power it can be as far apart and no bee in sight of each other they can still transmit or communicate.

VANVAN which stands for value added network is a private network setup that’s been tweaked and value has been added to basic communication which has been available to well known carriers and has the ability to lest the user get access to email and video conferencing. VAN is attractive and also good for companies who use telecommunication but want to reduce the costs. VAN transmits the data in EDI format but can also transmit using XML

and Binary formats. A VAN can also be defined as a extra services excluding internet which ISP providers provide to its customer. Frame RelayThis is a type of data transmission technique used to send digital information. In frame relay packets are called frame and they are passed through one or more start point to one ore more destinations through a sequence of nodes.

Network providers use frame relay as a encapsulation technique when voice or data is transmitted between a LAN over WAN. Encapsulation in simple words is making it compatible. For example when the internet is based upon a TCP/IP model and most of the applications either use UDP or TCP. The data is encapsulated in a UPD datagram to allow communication with other application on other host by even more encapsulation into IP to allow internet working to remote sites. After the encapsulation take place in frame relay for voice and data.

Every user gets leased line to a frame relay node. TCP/IP stands for Transmission Control Protocol over Internet Protocol. This relates to frame relay when it uses encapsulation to give abstractions of protocol and services. An application uses a given set of protocols and services and sends the data down to the layer so the data can be further encapsulated.

ISDNISDN which stands for Integrated Service Digital Network is the successor to dial-up narrowband services. An ISDN adapter would be needed in-order to access broadband service. It also gives access to packet switched networks. They are designed to allow digital transmission of voice and data over copper telephone wires. This gives better voice quality than an analogue phone. ISDN connection gives bandwidth of around 128 Kbps.

Due to the mass availability of cheap DSL and cable services in the UK IDSN has been superseded. ATMAsynchronous Transfer Mode (ATM) is a dedicated connection switching technology standard worldwide. There has to been a connection made between the node transmitting the data and requesting the data before the data is received. All the digital data transmitted between the source node and the destination node is organized by ATM into fixed length of 53 byte cell units. Bus Topology – In a bus network the clients are connected via a shared communication line which is known as a bus.

It is one of the easiest way of connect multiple clients. This topology consists of a main cable which either can be a twisted pair, coaxial or a fibre optic cable running through the network with a connector at each end of the cable. When two devices are transmitting at the same time results in collision on the network. When data is transmitted between two devices on the network it will also be broadcasted to other devices on the network virtually simultaneously. Advantages* Easy to implement and extend, because it consist of a long cable running through the network.* It is cheap to build because it requires a lot less cable to implement the topology.

It is also good for temporary networks which need to be set up in a hurry.* Transmission rate are relatively high compared to other network. The cable faults can also be easily identified. Disadvantages* The data is transmitted to every computer when the data is just to be sent and received between two computers.

Even though it is has a relatively high transmission rate it does not cope well with eavy traffic rates.* There is a limited amount of cable and workstations

that can be used and connected.* If the network is cable is broken it can cripple the whole network, the computer will be functioning but cannot communicate with each other.* Maintenance of the network in long period may be high, and also long term running more computers are added to the network the performance will drop.

Star Topology – Star topology is a central node with outlying nodes. In a star topology the messages are transmitted via a switch, hub or even a computer. The chance of being hit by a Network failure is quite low because all the computer systems are connected to the central node. Each of the devices connected have their own connection. The connections are made by network cable running from the central node directly to the device. Advantages* Performance is a lot better because the data packets that are sent and goes through unnecessary node the star topology will block this from happening.

Even if the central node has very high network utilization it will only affect the computer it is communicating with.* Each device connected to the network is isolated; this prevents any non-centralized failure to affect other devices on the network.* Expanding the network is very easy because of centralization. It can also analyze traffic and determine whether suspicious behaviour.* This topology overall is very easy to understand, design and navigate.

This topology discards the need of complex routing/message forwarding protocolsDisadvantages* There are setbacks of this type of topology because the network is dependent on the system functioning of the central hubs, If

there is a problem with the central hub then the whole network will stop working.* The whole network will also depend on the performance and capabilities of the central hub. The performance will depend on the number of connection that can be made simultaneously to the server.* Centralization can be a drawback if it there is high utilizing of the network because it will result in performance drop in the traffic on the network. Mesh Topology – In this type of topology each of the nodes are connected with each other. This means that the internet is the largest type of mesh topology.

When the data is transmitted it will automatically know where the data is to be sent and it will take the shortest route. Advantages* Even if there is a fault in the cable the traffic will still be sent because all the nodes on the network are joined together. The node can automatically reroute itself if the cable is broken because there is not gateway computer. Disadvantages* Takes a long time to set up beach each node needs to be connected to each other, so data can flow around without problems.

* It requires a lot more cable than other types of topologies because all the node are connected, so the more nodes that are connected the more cable is needed.* It can workout to be quite expensive to setup. Ring Topology – The node are interconnected with each other like mesh but each node is exactly connected to two other node, which result in a pathway for signal that are transmitted. The data which is transmitted is handled by each node on the network and then sent back with an acknowledgement of receipt. When the node transmitting the data receives the receipt it destroys the token ring. Either a token ring or a small packet is continuously passed around the

network so when a device needs to send something it will reserve the token ring.

Advantages* Network is not dependent on a centralized node because each of the nodes on the network can support the transmission rates around the network. Each of the nodes has the ability to take control of the transmission rate.* Extremely high transmission rate can be achieved. Typically speed of transmission is around 10 Mbps which is quite quick.

For e. g. it will take around 2 minutes to send a 100MB file which is pretty quick.* Compared to a star topology it performs a lot better under heavy load.* Network server is not required to manage the network.

Token PassingToken passing is the method used by nodes to send and receive data in a network. In token passing a node takes possession of a small frame called a token and attaches the data, control information and the specified target. Then the sending node will send it off, if a computer not targeted receives the token it will simply forward it off and when the target receives the data it opens the frame and reads the data and then send of the receipt of acknowledgement to the computer then transmitted the data and the token is destroyed and a new free token is created. CSMA/CDCarrier Sense Multiple Access/Collision Detection is a network control protocol where the transmitting data station detects that another station is transmitting signal that the first station will transmit a jam signal. Jam signal is used to request other transmission station that it needs to stop transmitting it does this by carrying a 32 bit binary pattern. 232 bits is the maximum diameter for a Ethernet cable which allows it to make a trip-time of 464 bits.

Slot time for a Ethernet cable is 512 and the difference between slot time and RTD is only 48 bits which not a lot. This is the maximum jam-time. Since the time a data station transmits a jam signal it has to wait before it can send that frame again. CSMA performance is increase by using Collision Detection. When a collision is detected Collision detection will terminate the transmission and this will also stop the probability of second collision on retry. The standard 802.

3 can be related to this topic because CSMA/CD monitors traffic on the line at transmitting stations. If there is no transmission then simply the station wanting to transmit will transmit and if there is a second station transmitting as well then this causes a collision and this is detected by all the station wanting to transmit. So after a random interval it will retransmit and then if there a collision again the transmission stop and retransmits at the random waiting time by there are increased every time. CSMA/CACarrier Sense Multiple Access/Collision Avoidance is used to improve the performance of CSMA, by being less hungry on the channel. Similar to the CDMA/CD if the channel is busy then it will stop for a random amount of time and then retransmit which reduces the possibility of another collision. CSMA/CA will send a requesting signal which needs to be acknowledged by other nodes before transmission takes place.

The 802. 11 standard is based of the CSMA/CA protocol which also includes the random waiting interval time. A station must be connected or linked to a access point when it establishes a connections which allows it to send packets. DHCPDynamic Host Configuration Protocol is used to get the parameters obligatory for functions in an internet protocol network. New

device can be added to the network without the need for a lot of configuration because the work load for the system administrator is reduced by this protocol.

DHCP is a really important protocol because it automatically retrieval of default gateway’s, IP addresses, subnet masks and other required IP parameters. When a client configured by DHCP connects to the network it automatically sends a broadcast query asking for the required information to the DHCP server. The IP address and information about the client configuration such as the gateway, domain name & etc, is all managed by the DHCP server. FTPFile Transfer Protocol is used to transfer data from one computer to another via a network similar to the internet.

FTP is quite an insecure way of transferring data because there is not straightforward way of transferring data which is encrypted. It works at the application layer. When the FTP protocol is in active mode the FTP client will release a dynamic port which will send the FTP server the dynamic port number which is used to listen over the control stream and waits for the connection from the FTP server. HTTPHTTP stands for Hyper Text Transfer Protocol. HTTP client initiates and send requests and start a transmission control protocol (TCP) connection to a unique port on a host.

The HTTP listening server will wait till it receives the request message. When it receives the message then it will send back a status or a replay saying HTTP/2. 1 300 OK and it will also send its own message with the status reply. SMTPSMTP protocol which stands for Simple Mail Transfer Protocol.

SMTP is an internet standard for electronic mail transfer across IP addresses. This is also a text based protocol. In text based one or more recipients can be added and other encoded subjects can also be attached and transfer. When the mail is transferred it will first go to a remote server using different commands of quires and responses between the server itself and the client.

DNSDNS which stands for Domain Name System is a naming system for computers, services, or any other resource in the Internet. It will translate the human text to binary indentifies associated, this allows network equipment to locate and addresses these devices world-wide. Often the concept of a phonebook is applied to make someone understand the theory of DNS, It acts as a phonebook for the Internet by translating the human text to IP addresses. For example www. google.

co. uk is translated to 74. 125. 76. 104.

TCP/IPIt stands for Transmission Control Protocol /Internet Protocol. There are obliviously two different parts to this. TCP controls and allows hosts to make connections and exchange data while the IP deals with packets. TCP guarantees the delivery of the data and also guarantees that the packets will not change the order in which they were sent in and will reach the destination in the exact order sent in. AppleTalkA cheap LAN architecture made by Apple that was built and used for Macintosh computers/printers.

AppleTalk supports Apple’s local talk cabling scheme as well as Ethernet and IBM’s token ring. Using AppleTalk Mac computer can be connected to printers and PC’s if the special software for hardware and software is provided. UDPStands for User Datagram Protocol, this an internet protocol

used for datagram services. This protocol allows computers on a network to send short messages to one another which is also known as datagram. Opposite to TCP/IP it does not guarantee the reliability and delivery of the message and packets the order they are sent in.

This means that the message can come out of order it can also be corrupted or sections missing from the message without you knowing or noticing. UDP works at the transport layer. This protocol is as important as other protocols because the upper layer protocol has no guarantee from UDP that the message has been successfully delivery. Sender of a UDP does not assure the state of UDP message once. If any kind of reliability is needed for the message transmission than it is all implemented in upper layers. IEEE 802Institute of Electrical and Electronics Engineers 802 is the standard which looks after LAN and metropolitan area networks.

It is restricted to networks which are carrying variable-size packets. It works with to lower layer of the OSI model. The data link layer and the physical layer. It further splits the data link layer into Logical Link Control and Media Access Control. IEEE 802. 2Standard which defines Logic Link Control (LLC).

According to this standard it is the upper sub layer of the OSI Data Link Layer. A uniform interface of the data link service is presented to the user. This standard give two connectionless and one connection oriented operational does. Type 1 is an unacknowledged connectionless mode which allows frames to be sent o signal destination also known as point-to-point or unicast transfer. It allows multiple nodes on the same network known as

multicast and finally allows sending it to all nodes on the network known as broadcast. Type 2 is a connection-oriented operational mode.

It uses sequence numbering similar to the TCP/IP guarantee it guarantees that the order they are sent in is the order they receive it in and no frames are lost. Finally Type 3 is an acknowledged connectionless service which only supports communication to single destination or point-to-point communication. IEEE 802. 3This standard defines the MAC layer for bus network using CSMA/CD. It is considered as a LAN technology and uses very few WAN applications.

Connections between node and infrastructure are made using various fibre cable connecting switches and hubs together. IEEE 802. 5Also known as token ring local area network is a LAN protocol which uses special 3 byte frame called a token which travel around a network ring. Nodes on a token ring LAN are organized into a ring topology. The ring goes around and station wanting to transmit data will take control of it and send it to the destination and when the transmission is completed than the token ring is destroyed and new one is created. IEEE 802.

11Set of standards which put into operation WLAN communication in the 2. 4, 3. 6 and 5 GHz spectrum band. Original version of this standard that was created is now out of date.

It specified two net bit rates of 1 or 2 Mbps. Since higher rates can now be achieved there are sub-standard under 802. 11 which run from 802. 11a to 802. 11z. For example 802.

11a uses the same data link layer protocol and frame format as the original standard but it works in the 5 GHz ban and has a maximum net data rate of 54 Mbps. IEEE 802. 11This is the standard which handles Wi-Fi connections. Current it is they method used for deploying portable broadband internet to devices.

You would normally find Wi-Fi connections in hotels, cafes ; airports. People have started to use it at home as well. Nearly all personal computer operating systems, game consoles, laptops, smart phones, printer and other peripherals support Wi-Fi. IEEE 802. 16It is known as the Broadband Wireless Access.

This is the standard for the upcoming WiMax system. It stands for Worldwide Interoperability for Microwave Access. It is a telecommunication technology which uses wireless transmission to deploy broadband to anywhere. It uses 75 Mbps broadband speed without the need for cables. FDDIIt stands for Fibre Distributed Data Interface. A protocol which allows digital data to be sent over fibre optic cable.

FDDI networks are also token passing networks but support speeds up to 100 Mbps. There is also an extension to FDDI called FDDI2 which supports voice and video transmission as well as data transmission. InfraredSimilar to Bluetooth but has not got as good transmission or sending range but it’s a technology which allows devices to communicate at short range using wireless signals. Computers equipped with infrared can transfer digital data bidirectionally.

As mentioned before infrared communications have very short distances. Unlike Bluetooth it can’t penetrate thought walls and only works in direct line of sight. Infrared technology exists in three formsIrDA-SIR (slow speed) infrared supporting data rates up to 115 Kbps. IrDA-MIR (medium speed) infrared supporting data rates up to 1.

15 Mbps. IrDA-FIR (fast speed) infrared supporting data rates up to 4 Mbps. BluetoothA wireless transmission protocol which has been around for a lot of years but recently been used more than ever. It is a short distance data exchanging over short distances fixed and mobile devices which make up PAN’s. Benefit of using Bluetooth is that it can overcome the problem of synchronization.

Bluetooth in other words is a standard and communication protocol which has been designed for low power and cost transceiver microchips in every device. Another benefit of using Bluetooth is that as long as the transmission device has enough power it can be as far apart and no bee in sight of each other they can still transmit or communicate. ConclusionOnly one standard or various standards cannot be used for different things, this would result in things not working properly and not compatible with different devices.