Communication technologies assignment

This is a rudimentary diagram representing the basic network that is employed in the Boston College Rockford Campus. This section represents a room, or department within the campus, showing how the Nodes are all connected to a multi-port switch using straight-through cables (Used to connect non-similar devices, such as a PC and a switch). The diagram on the left is a bog standard star topology, whereby a switch is connected to multiple nodes via an RAJA straight-through cable, thus allowing the transfer of packets to and from the devices on the sub-network; I.

E. PC to printer, or laptop o PC and so on. By the connecting the switch to the router(s) at the centre of the college network, you are allowing the sub network above to communicate with other departments and devices around the campus. Such as the Student file server, and the email server, (Which are used for the storage and retrieval of files, and the sending and storing of emails.) both of which are connected to the entire network, allowing access from around the campus, regardless of what device a user chooses to try and access them.

The college has also incorporated a server which is used to host the website, and the various services (DNS, ADDS, DDCD) squired for students and staff alike to access the internet whilst in college. This method is a very effective way of creating and maintaining a functioning multi- user network. It’s cost effective, and in terms of labor and parts required very simple to set up (Apart from the cable management) Another advantage of this type of network is that if one component breaks, as long as it’s not something crucial like a switch, then the network will continue to function for other users in the areas that have working components.

As a broad explanation, Networks communicate by passing packets from one end device to another, along a rise of cables, like straight-through and crossover cables, which connect the end devices to one another, and to devices that deal with the direction and contents of each and every packet that is sent. The router is by far one of the most important devices in promoting efficient transfer of data, and it operates by following a specific protocol, usually the TCP/IP protocol, or sometimes UDP. Task 2. UP. : Describe the following communication protocols and why they are important -Bluetooth: Bluetooth is one of the most common short range methods of wireless communication between one or more device. Signals are reanimated by Bluetooth equipped devices using a short-wave UHF radio wave which is located in the ISM bandwidth transmitting at 2. 4-2. 485 GHZ from both fixed devices and mobile devices, such as a mobile phone, or a TV sound system. Bluetooth was originally designed by the electronics company Ericson in 1994 as a replacement for a data transfer cable known as RSI-232.

One of the main advantages of Bluetooth is that it can connect multiple devices at any one time, and remain connected indefinitely, providing that the devices all remain within range. Bluetooth is still incredibly important in modern technology, and is still en of the prevalent protocols used for short-range wireless connections, it can be used to connect mobile phones to hands-free sets in cars, or AMP players to computers to allow transfer of files; or even used to play Deeds Midnight Runners through a surround sound system whilst a teenager types up their computing assignment on their day off. Wife: Wife itself is not actually a protocol; in fact it is a synonym for a Wireless Local Area Network based upon the IEEE 802 family of standards,

and is a play on the term Hi-If (High Fidelity). As stated previously, Wife is simply a trade name for a Wireless LANA, which means that rather than neglecting to a network via the traditional methods, I. E using an Ethernet cable; users can connect wirelessly. Routers transmit and receive packets to and from user devices (laptops, phones, tablets etc. Using radio waves at the frequency 2. GHz and even at GHz in some newer and more expensive routers, however that is still being phased in and is not yet in full use. As with and cable based CAN, all of the networking and traffic must be transmitted and received in accordance with a set of standards, which is where the IEEE 802 family comes into play. Wireless networks are specified as running on the 802. 11 branch of he family, however this in itself has more protocols that define the speed etc. Of the network: 802. La: This is the GHz strand, and is one of the fastest that is currently available for use, boasting data transfer speeds of up to megabits per second thanks to the use of orthogonal frequency-division multiplexing (FOOD) which splits the signal into lots of little sub-signals before it reaches the receiver, thus reducing interference. 802. Bib: This is the slowest and formerly most popular standard allowing speeds up to 1 1 megabits per second on the 2. GHz frequency, however the decreasing costs of faster standards means that his former leviathan is now rarely used. 02. 1 leg: This also transmits at 2. GHz much like ‘ b’, however it uses the same type of coding as ‘ a’ (FOOD) allowing the signal to be transmitted with far less interference and greater speeds, hitting megabits per second. 802. 1 In: The most popular of standards and the most widely available. This standard allows for the transmitting of four streams of data, each one scrambled by FOOD, meaning that xx the amount of data can be transmitted compared to the other

standards, each stream holding the potential to transmit at up to megabits per second.

However most routers only allow for the receipt of 2-3 streams at anyone time, meaning it’s not as fast as it could be. 802. 1 lace: This is the newest of the standards, and is still technically in the development stage, however devices are being released that have the capability to transmit and receive signals in accordance with ‘ AC’. This works much the same as ‘ n’ however it transmits at both 2. GHz and GHz, with 4 streams on each. Meaning that it has the potential to broadcast a maximum of 8 streams, each at 450 megabits per second.

Considerably faster than any of it’s predecessors. The importance of Wife is fairly self-explanatory, however I’ll explain it anyway, just in case you’re still stuck in the mid 199(Yes. For years people have been plugging their PC’s into the back of a plastic box somewhere near the household telephone with a long yellow wire that never seems to untangle properly. As you can imagine this would’ve been an issue if say, you wanted to move the PC, or you wanted more than one device to connect at any one time, or you didn’t fancy running a cable all the way through the house.

But along came Wife (and routers which do literally everything, but that’s a different ball game) and hanged everything. It allows more than one user (Providing the device they use has wireless capabilities) to connect to the router at any time, and then gives them free reign to move around as much as they want within the wireless range, because they don’t have to remain plugged in permanently much like their predecessors.

By introducing Wife into our homes and workplaces, we have paved the way for portable wireless devices, such as phones and laptops and tablets, all of which mean that we can remain connected, regardless of where we are. As I type, my laptop is connected to the router wirelessly, meaning I can antique to listen to terrible Us rock music anywhere in the house. Whether it’s from the comfort of the armchair, or the equal comfort of the upstairs toilet. Quite simply, Wife has overhauled the way we access a network, and made it a hell of a lot easier and less time consuming. Radar: Radar stands for Infrared Data Association, which is the name of the company that first introduced infrared signals as a way of exchanging data between devices. It works by sending beams of infrared light to a receiver, which then interprets the patterns and translates them into a piece of data. Radar is most common in smaller devices, such as bile phones and was first introduced in 1 993 when it was very popular for wireless data transfer, and it remained the first choice for the transfer of data without cables for about a year, when Ericson then released Bluetooth.

Radar is still however used by a few devices like cameras and medical equipment where it remains popular given its high level of security and the fact that errors aren’t common when exchanging bits. Radar works on a Line of Sight basis, meaning that in order for 2 devices to remain connected, there can be no physical obstacles in the way, such as a wall, or a person. This means that although limited by range and movement, the connection is stable and secure, and that there is very little packet loss.

Radar, although on the whole massively out-dated by technologies such as Bluetooth, does remain an important means of wireless transmission

between devices. It remains important mostly in the private sector, rather than in the hands of the public because of it’s aforementioned high level of security and stability when maintaining a connection, boasting the same level of security and stability as a wired cable connection, something that Bluetooth and ‘ Wife’ cannot. -Cellular Radio:

A cellular network is a Wide Area Wireless network, which is divided into smaller land areas known as cells (short for cellular). Each of these cells is serviced by one or more Fixed Location Radio Transceivers, which transmit/boost wireless signals to devices on that network, as well as relay the signals that are sent back. In a cellular network, each transceiver operates on a different set of frequencies to avoid any interference with the other cells in the network.

By linking loads of these cells together, a network can be created that can cover hundreds of thousands of miles of land and can be accessed by anyone at anytime providing hey have a device that is connected to said network, Egg. A mobile phone or a laptop with USB dongle. This sort of Network is very important in modern society and is by far the most used type of Network protocol. Without it I wouldn’t be able to pick up my mobile telephone and order a pizza, or the local taxi company wouldn’t be able to communicate with the driver that needs to go and pick somebody up.

It’s networks like these that are the backbone of society. -GSM/ COMETS: GSM and NUTS are both standards developed by the European Telecommunications Standards Institute to define a set of protocols for the charity of cellular mobile phones to run on and abide by. GSM is the 2nd

generation of standards developed, and is an improvement on the 1st generation of standards that was an analogue based set of protocols and didn’t allow for data packets to be passed to devices.

GSM, on the other hand is a works on a digital signal, which allowed for the expansion of the networks to encompass data packet transfer via GAPS (General Packet Radio Services) and more recently EDGE which is a refined version of GAPS allowing for faster rates of packet transfer. Most of the world’s mobile phones still run on the GSM protocol, with approximately 700 service providers in 200 country’s use it as their main means of providing a network to their users. GSM operates in the mezzo and 1. GHz bands in Europe, and can offer speeds of up to 9. Kbps of data packet transfer, which although very very very slow, is still better than nothing at all. NUTS is the name of the 3rd generation of protocols, and is a direct development of GSM. NUTS stands for Universal Mobile Telecommunications system, which as previously stated is a generational improvement of GSM, and uses wideband code division multiple access to provide a more expansive, and faster network o allow users more instant access to the data services provided by their Mobile Phone Network, be it web browsing, or watching a TV show, or even just sending a simple email.

Because of the way NUTS works, users have access to all of their Internet services at far higher speeds than GSM, in keeping with the progression in mobile phones and Pad’s, most of which now have the capability to access the Internet at the tap of a screen. The key difference is the speed; NUTS can boast speeds of up to 14 megabits per second, which is quick by most standards. Whereas GSM, running at Kbps is appallingly slow by comparison.

Both of these protocols are incredibly important, as they have allowed for the introduction and improvement of mobile wireless Internet connectivity and network access.

The development of these two standards, in the order that they came, helped the world to move on from just being able to make a phone call, and allowed them to send a text, and eventually access the internet from the tiny thing in our pockets. The development of these two protocols really had paved the way for the digital era. -WAP: Wireless Application Protocol, this basically means that you can access the Internet from your phone or tablet. It is compatible cross all mobile operating systems, and all microbreweries used by phones and tablets operate based upon this protocol.

Crucially, WAP is supported by GSM and NUTS, meaning that it is basically the template on which mobile Internet access is based. Essentially, what WAP does is allow users to view PC based web applications on their smaller screen devices that commonly utilities a touch screen. It converts the standard HTML web file into a mobile internet compatible WOMB file, allowing users to view and navigate on web pages and applications from their hand held device. As I have just explained, but shall repeat anyway;

WAP is incredibly important in modern day use, as it allows users of mobile devices running on either a GSM or NUTS or even LET network to access HTML web addresses and applications. It converts the HTML files into a WOMB file, which is specifically tailored for handheld mobile devices, making the screen size and resolution adaptable, allowing it to change to suit multiple platforms. It also converts the navigation methods on the page, so

that the user can navigate the page using a thumb or finger, rather than the mouse and keyboard associated with a PC or laptop.

WOMB: I mentioned this briefly the previous communication retool; as it is the protocol that allows users to access web sites and other Internet based applications from a small handheld device, such as a mobile phone, or a touch screen tablet. It stands for Wireless Markup Language, and up until recently was the main way of getting HTML web page to operate as you would like on a mobile device. WOMB was first invented because of the limitations of their handheld devices, processing power and the size of the memory in a phone was often too little to deal with some demanding web pages and applications, due to the sheer size of file.

So WOMB came along with the IM of converting the large HTML files into far smaller WOMB files that a phone or tablet could deal with without putting a lot of strain on the hardware of the device. WOMB also had the purpose of altering the basic amenities that you would expect from a website, things like navigation, resolution and size of screen. It allows users to navigate using their thumb, or a finger, as well as adapting the web page’s screen size and resolution to fit that of the device being used.

As times move on, and mobile phones and tablets progress, WOMB is less necessary because of the prated hardware that modern phones have; however the replica implications of WOMB are still heavily relied upon for ease of use. For these reasons WOMB is incredibly important, and will almost certainly be in use for the foreseeable future, as it allows users easy access to web applications, and combined with GSM/NUTS/LET, means that it can be

done from almost anywhere in the known world (and even space allegedly), making it one of the most important, and unlimitedly useful protocols in current use. 02. 11 standards: The . 11 strand of the IEEE 802 family of standards is the one that is used by the majority of wireless networks in the world. The . 1 strand of the family is the one that defines the parameters that all Weans run on, be it a small office set up, or a multi-chain supermarket with free Wife (k that never happens, but we live in hope) they all utilities the protocols defined by the IEEE 802. 11 standard(s). 802. La: This is the GHz strand, and is one of the fastest that is currently available for use, boasting data transfer speeds of up to megabits per second thanks to the use of orthogonal frequency-division multiplexing (FOOD) which splits the signal into lots of little sub-signals before it reaches the receiver, thus reducing interference. 02. Bib: This is the slowest and formerly most popular standard allowing speeds up to 1 1 megabits per second on the 2. GHz frequency, however the decreasing costs of faster standards means that this former leviathan is now rarely used. 02. 1 leg: This also transmits at 2. GHz much like ‘ b’, however it uses the same type of coding as ‘ a’ (FOOD) allowing the signal to be transmitted with far less interference and greater speeds, hitting megabits per second. 802. 11 n: The most popular of standards and the most widely available. This standard allows for the transmitting of four streams of data, ACH one scrambled by FOOD, meaning that xx the amount of data can be importance of the development of the . 11 family of standards is unprecedented.

It was brought in in the late toys in an attempt to basically standardize the way in which wireless networks operate all across the world, it allowed

companies to mass produce the equipment that allows us to access the internet. The introduction of theses standards meant that ordinary people would have access to web services in the comfort of their own homes, and that it wasn’t simply reserved for large companies and government agencies like it had been for o long. It most certainly helped to pave the way for the Internet age.

TCP/IP: Transmission control protocol/lenient protocol; as the name suggests, these protocols define the way in which we access the Internet on an everyday basis. The protocol defines how data is transferred from user to user; both in a LANA and an internet based WAN. This protocol is based around 4 layers: Source of photo: Unknown. (Unknown). Communication Over the Network. Available: http://www. Heighten. Net/EN/Communicating/Communicating _over_the_Network. HTML. Last accessed 9. 10. 14. The main job of the TCP/IP del is to format data into a transportable package that can be transferred across a network, or even multiple networks.

The TCP/IP model defines how data is transported around the Internet, and is essential for all networks to be standardized worldwide. Just in case you don’t know why standardization of protocols could be beneficial and very important, I shall explain. By standardizing and making SUre all networks utilities the same protocol, we can ensure that every network around the world can communicate flawlessly and in theory without delay; purely and simply because they are all signing from the same hymn heed and there is no fifing about trying to convert from one thing to another.

Wireless Security Protocols: Wireless security protocols were developed primarily to protect home and work wireless networks, and there are 3 main types of Security Protocol. Wired Equivalency Protocol (WEEP): WEEP was the first security protocol brought into wireless networks, and as the name suggests, is meant to provide similar levels of security as that of a wired network by restricting access and encrypting data. However there were a few easily traceable and exploitable flaws with WEEP, which has made it increasingly unpopular.

Wife-Protected Access (WAP): This was first brought in as a temporary security protocol whilst the 802. Iii security protocol was being developed with the intention of rolling it in across all wireless networks. Most WAP systems utilities a ASK (pre-shared key), which is basically a fancy name for a password. Which blocks unauthorized access by asking users to enter the correct password upon connection to the wireless router. This system is also sometimes referred to as WAP-Personal because the password can be changed to something personalized in order to make it more memorable.

Wife- Protected Access 2 (WAP-2): This is mostly the same as WAP-I however it is based more on the finalized 802. Iii security standard, but still shares the ASK feature with its predecessor. The main difference between the two is the addition of the Advanced Encryption Standard (AES) Which as the name suggests, is an advanced method of encrypting data, and is approved for use by the United States Government for protecting top secret files, so it’s pretty good. The importance of these protocols is pretty obvious in all honesty; they protect the network, and all of the users on it.

There are thousands of people out there who an learn all sorts of information about you just by accessing the network that you are connected to. By protecting the access to the network, you are making the accessing of your personal information considerably more difficult than with an insecure network. Put simply, it makes the network safer for all users. UP. 2 TCP/IP model: Transmission control protocol/lenient protocol; as the name suggests, these protocols define the way in which we access the Internet on an everyday basis.

The protocol defines how data is transferred from user to user; both in a LANA and an Internet based WAN. This protocol is based around 4 areas: _over_the_Network. HTML. Last accessed 9. 10. 14. Application Layer: This is the top layer of the TCP/IP protocol model, it includes protocols and applications that use the protocols from the transport layer to deliver the data to the destination device and user. The application layer has a few protocols and applications in its arsenal that allow it to communicate effectively with the transport layer and to perform correctly.

Applications like HTTP (Hypertext transfer protocol) and ESMTP (Simple mail transfer protocol). Both of these are essentially ways of the user performing different tasks on their devices. Transport Layer: This is the main layer that controls the data flow between two hosts. The layer receives data from the Application layer, which has just been covered above. Like the application layer, the transport layer has numerous protocols for its purpose, however the 2 most commonly used are TCP and UDP.

TCP is used when a stable and reliable connection is required by the user, say when viewing a website, or your Internet banking site. Once a packet is sent, it awaits a receipt from the destination user before sending another packet, and visa versa. Thus ensuring that all packets are levered correctly and to the right destination before sending any more. This means that in theory, no information is lost during transfer, or if it is, no more data is sent. Significantly reducing packet loss.

JODI is the unstable version of TCP and is comparatively simpler than it’s sister protocol. It sends packets from one host to another, in much the same way, however it is used primarily for the transfer of media based data, such as a video that is being streamed, or the all important music that’s keeping you going whilst typing up an incredibly dreary and long winded assignment (not that I would know how that feels of course). Essentially, rather than waiting for an acknowledgement of receipt of a packet, it just keeps sending them to ensure smooth streaming.

After all there is nothing worse than missing out on Pedigree’s BRB fist simply because your computer wanted to make sure you were receiving everything k. Network Layer: This layer is also often called the Internet layer, mainly because it’s purpose is to handle the movement of data on a network. Basically, it makes sure it goes to the right place by reading the destination IP and Mac addresses and sending it in the right direction. The main protocol used is simply called IP.

Data Link Layer: This layer also gets called the Network Interface Layer, and normally consists of the device drivers in the SO and the NICE that’s in the

system. Both of these devices control the communication details with the media being used to transfer the data over a network; usually this comes in the form of cables. Some of the more common protocols used in this particular layer are Address Resolution Protocols (ARP) and the Point-to-Point Protocol (APP). The OSI model: PLEASE DO NOT THROW SAUSAGE PIZZA AWAY is by far the best way to remember the order of the OSI model: Physical, Data, Network, Transport,

Session, Presentation and finally Application. Although this is the correct numerical order for the model, in reality it does kind of work the other way round, starting with application. Layer 7: Application. This is the layer that does all of the interaction with the user via the PC’s operating system or whatever application is being used when the user wants to transfer a file (or files). Or perform other network related activities, like searching for cures to deadly diseases, or catching up with friends on a social network of your choosing.

Layer 6: The Presentation Layer. This takes the data room the application layer and essentially converts it into a standard format. So it would potentially convert an ASCII message into binary ready for transport, or visa versa. This is also the layer at which the encryption and decryption of data occurs, again, making it safe and ready for transport later in the stack. Layer 5: Session. The session layer has a simple job, it establishes and maintains a connection with the next step in the transportation step, so normally with a router or a switch.

Letting said device know that a packet is going to be sent their way. Layer 4: Transport. The Transport layer is responsible for the error checking of bits of data, and also maintains the flow control when in transit. In essence this means that the layer has a look to see if the data is coming from more than one application at any one time, and then integrates applications data into a single stream of data. Layer 3: Network. The network layer is responsible solely for the forwarding of the packets to the correct ‘ next step’ so in most cases, the next device in the chain of delivery.

For example, from your PC to the router, the entirety of the OSI process is repeated once again at the next step in the process. Layer 2: Data Link. This layer deals with the assignment of the appropriate protocols to bits of data, so for example, you send an email with a picture of you riding a camel on holiday in Azerbaijan to your Nan, the Data Link layer would assign this packet with the ESMTP protocol (Simple mail transfer protocol) and send it along the chain to the final layer. Layer 1: Physical. This is the level that deals with the actual PC hardware.

Quite simply, this layer defines the characteristics of a network, and details the connections to the network. As well as things like voltage levels and timing of the system. Comparison of the two: Similarities: Both models share a similar architecture, as they are both defined with layers that have similar purposes. They both have a common layer, the application layer, however the similarities end at the shared name. Both layers have different purposes. Both of the models do pretty much the same thing; they both serve the same purpose. The analysis and transfer of packets throughout a network.

Both models have a Transport and Network layer that share similar jobs, the transport layer of the TCP/IP model performs pretty much the same function as what happens between the presentation and network layer of the OSI. We need both models in networking, they both have great significance when it comes to networking, however everything is done automatically now, so professionals rarely use it anymore. But knowledge of it is essential. Both models make the assumption that packets are switched, meaning that individual packets can take different paths in an attempt to reach the same destination.

Differences: The protocols in the TCP/IP model are broadly considered to be the generic standards around which the internet has been developed, and is recognized as the main way of defining the way in which data is turned into packets and touted to the next step. Whereas the OSI is considered a generic protocol, that uses independent standards. TCP/IP combines presentation and session layers of the OSI model and makes it one simplified layer, called the application layer. This makes the explanation of it considerably easier, and makes the use of it considerably simpler as well.

The Data link and Physical layers of the OSI models are also compressed into one broad layer of the TCP/IP model, the data link layer. Which deals with the same thing as the OSI equivalents, but in one step rather than 2 The TCP/IP is generally considered to be a simpler model because of the mailer number of layers, however I have to say, having studied both, I do prefer the OSI model because it clearly separates each process into one step, rather than 2 or 3 in the same layer, much like the TCP/IP.

The TCP/IP is also considered more credible, simply because it is the protocol stack around which the Internet as we know it was developed. Where as the OSI stack is rarely used to set up a network, other than by Cisco, who seem to love it and use it constantly. However it is mostly used in theory as a guidance tool, unlike the TCP/IP, which is actually used in real networks. The OSI has 7 layers, where as the TCP/IP has only 4 (had o be mentioned, sorry!) The transport layer in the OSI model guarantees the delivery of packets, unlike the TCP/IP model, which does not.

The OSI model is a general model, where as the TCP/IP is very specific to the internet, and can’t really be used in other applications, unless heavily adapted first. The OSI model has the issue of struggling to fit the protocols into the model itself, where as the TCP/IP does not actually fit any protocol and creates it’s own. Protocols in the OSI model are hidden, and are easily replaced, whereas protocols are very difficult to replace in the TCP/IP model. UP: 6 Types of Communication Devices

First, a brief overview of a communication device: A communication device is defined as a device that possesses the capability to transmit an analogue or digital signal either wired or wirelessly (whatever form that may take). 1. Mobile Telephone: Also called a cellular phone is a small (unless you have a 198(Yes Dynamic) portable handheld device capable of transmitting and receiving signals via a Cellular Radio Network, which provides network coverage over a large geographical area (See UP. For an in depth explanation) It makes use of protocols such as GSM and MUTE to transmit and receive digital signals across the network o other communication devices, such as a server for a social networking site. 2. Ethernet Hub: An

Ethernet hub is a device that connects multiple devices together via a series of Ethernet RAJA cables and makes them work together as a single network segment. It has multiple 1/0 ports on the device itself, usually 44, which are used to connect the devices in the segment.

The Hub is part of the physical layer of the OSI model, and the repeater version of a Hub can also take part in collision detection of packets. Which is useful in basic networks. 3. Router: A router is another networking device used in almost every network round the globe. It’s purpose is to forward data packets between networks, so say I wanted to send this assignment in an email to the poor sod that has to read it; The router would receive the packet, and then send it from my home network to the next hop address, where it would eventually wind up at the router of the lucky chaps home network, and would then appear in his inbox. . Switch: Not too dish-similar from a Hub, a switch also connects multiple devices together to create a miniature sub-network that can be independent, even when connected to other switches. It uses a similar form of packet switching to that of a router, ND does essentially the same job, but on a far smaller scale, and without the ability to send a packet to an unconnected network.

The main difference between a switch and hub is that a switch can be port specific, and will send a packet to the intended port, rather than all of it’s ports, much like a hub. 5. PC (personal computer): A personal computer is a general purpose computer that is generally just useful to people. The personal computer is designed to be as simple as possible so that any old idiot can use it courtesy of a combination of graphic user interfaces, rather

than having to be trained to use command line interface, which is nigh on impossible to master.

Computers have the potential to host many many applications, ranging from a basic graphical calculator, all the way up to a piece of code-breaking software that could hack into the most secure banks in the world (assuming YOU’Ve kitted it out to be a beast). However a literal definition would be; a group of hardware components connected into a motherboard that is controlled by a processing chip and the PC’s Random Access memory. 6. Pager: A pager is a wireless telecommunication device that has the capability to receive digital signals and convert them into a text-based message,