COMPUTER NETWORKS 1B: ASSIGNMENT 1

Student Number: ST10467645
Full Name: Kandyce Jade Smit

Lecturer: Farshida Wania
Module Code: CONE5112

Table of Contents

Question 1 2
Question 2 4
Question 3 6
Question 4 9
Question 5 12
References 13

Question 1

1.1) Queuing delay occurs when the packet is waiting in the buffer of a router or switch before being forwarded because of network congestion or heavy traffic load. For example, if many students join a live lecture session at the same time peak usage, then packets are waiting to be processed and will get queued, which causes the buffering or lag in video playback. This isn't ideal because it slows down the video delivery and creates a poor experience for students in the e-learning platform. (GeeksForGeeks, 2025).

Packet loss happens when packets don't arrive at the intended recipient's destinations - in many situations this is caused be routers being overloaded and cannot handle the overload to prevent dropped packets. Common causes for packet loss in networks are network congestion, failing hardware, and channel interference. In an e-learning platform, dropped packets can result in choppy video, video and/or audio that are missing during live sessions, and force resends for assignments during upload, which adds delay and can be frustrating for the student. (IR, 2025; NSRC, 2019).

1.2) End-to-end delay is the time it takes for a data packet to be sent from the sender (for example, the user's device such as a laptop or smart phone) to the end-receiver (for example, the e-learning server), while experiencing the delays of any remote and intermediate systems that are part of the path. The end-to-end packet delay has four main components of delay:

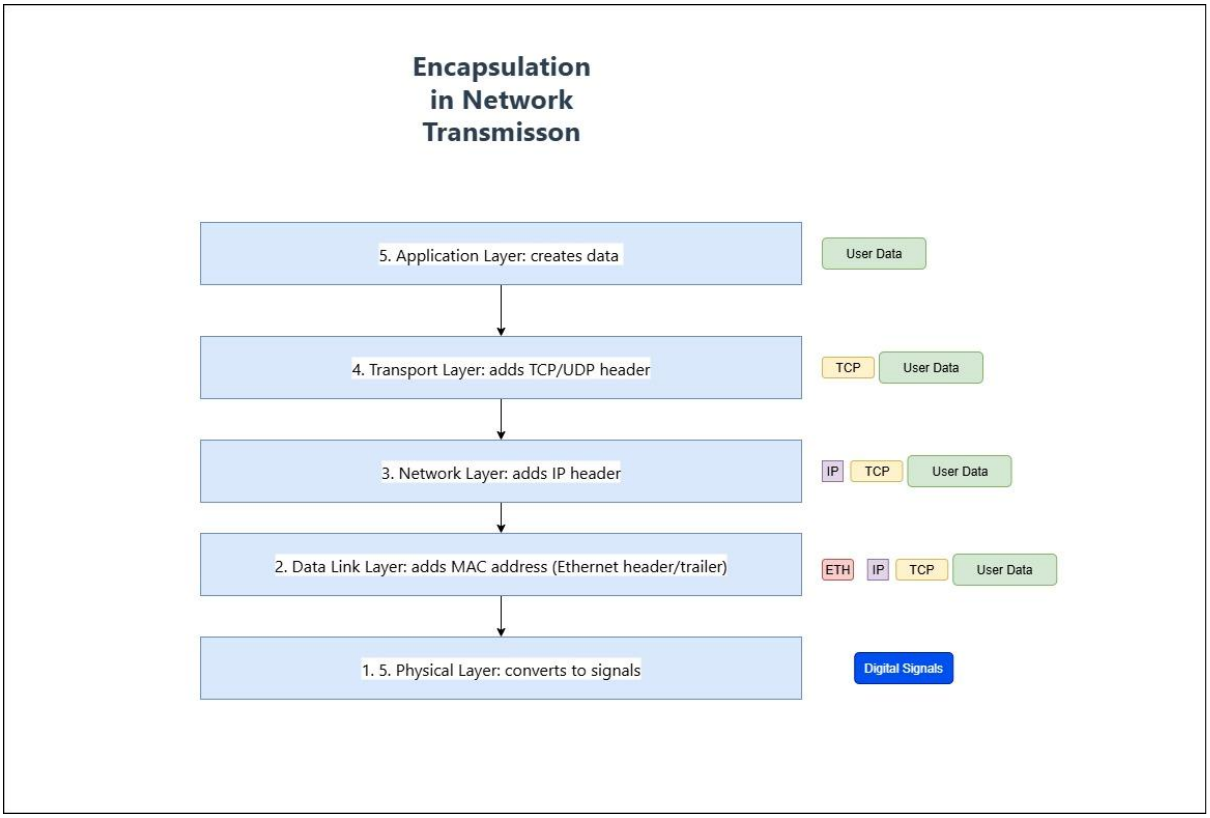
- Processing delay: the time it takes the routers to examine header information and check for errors (NSRC, 2019).
- Transmission delay: the amount of time it takes to push all of the bits of the packet onto the communication link, and this is determined by the packet size and the available bandwidth of the communication link (NSRC, 2019).
- Propagation delay – the time a signal takes to get to the destination and is determined by the physical distance of the links, and the time it takes the signals to propagate through the medium (NSRC, 2019).
- Queuing delay – the amount of time a packet spends waiting in a router's buffers when devices are causing network congestion (NSRC, 2019).

For example, when many users are streaming a lecture at the same time, the packets might sit in queues longer, which means an overall higher end-to-end delay will be witnessed, and students will experience video buffering or lag in the e-learning platform.

1.3) Encapsulation occurs when data from an application, such as a student submission or live streaming video, is wrapped with headers at every layer of the network to ensure correct delivery (GeeksForGeeks, 2025). Each layer adds its own information, such as IP addresses or port numbers to provide routers and switches with as much information as possible about where that data needs to go to enable delivery (JumpCloud, 2025).

An encapsulation example would be when a student uploads an assignment, the data is encapsulated step by step. Routers read only the headers they need, which makes delivery faster and more reliable, even if many students submit at once. (GeeksForGeeks, 2025).

<u>An illustrated example of the process of encapsulation in data transmission:</u>



My encapsulation illustration was created using draw.io. (Draw.io, n.d.).

Question 2

2.1) The architecture for 4G LTE has three major components: User Equipment (UE), E UTRAN, and Evolved Packet Core (EPC). UE consists of devices such as a smartphone or IoT devices, such as in Metrotech, where a traffic camera is streaming live video to the city traffic center (Mobile Packet Core, n.d.). The E UTRAN is the radio network consisting of eNodeBs (base stations) which control wireless communication and attach each device to the core network to ensure the camera feed continues without interruption (Tutorialspoint, 2025).

The EPC oversees data routing and session-management. The components of EPC consist of MME (device authentication and handles mobility), SGW (data routing throughout handover), PGW (connects device to the internet), and HSS (holds subscriber information) (Mobile Packet Core, n.d.). LTE is all-IP and uses OFDM and MIMO for efficient spectrum use and higher data rates, as well as provides seamless handovers, so if the traffic camera is moved, it would connect to the other eNodeB and continue feeding live video footage without any interruptions (Tutorialspoint, 2025).

2.2) The enhancements from 5G to 4G networks are significant, especially in speed, latency, and reliability as the main performance metrics for implementation and applications in smart cities like Metrotech:

- Speed: 5G offers peak download speeds up to 20 Gbps, enabling rapid data transfer essential for applications such as high-definition video streaming and real-time traffic monitoring in smart city infrastructure, allowing cameras and sensors in Metrotech to send live data without delay (Qualcomm, n.d.).
- Latency: The peak download speeds of 5G reach up to 20 Gbps, allowing for efficient and speedy data transfer. This is significant for applications such as HD video streaming and real-time monitoring of video-based sources, for example, traffic monitoring in smart city infrastructure. In Metrotech, camera and sensor data can be transmitted immediately without any obvious latency (Qualcomm, n.d.).
- Reliability: Reliability in 5G networks is improved with new technologies such as Ultra-Reliable Low Latency Communications (URLLC) that guarantee near real-time delivery of data flows. Critical applications such as public safety systems or industrial automation benefit from the reliability of networks, so emergency alerts and control signals in Metrotech would be delivered without interruption (Qualcomm, n.d.).

2.3) 5G technology facilitates advancements in smart cities through improvements in massive capacity for device connection, high-speed data transfer, and ultra-low latency needed for urban infrastructure improvements in cities like Metrotech:

- IoT Applications: 5G will enable real time monitoring of urban conditions including traffic, air quality, and energy usage. Smart pay parking or traffic lights will connect and adjust with real time data provided by sensors and cameras in Metrotech, improving congestion and commute times (Reply, 2025).
- Autonomous Vehicles: With low latency, cars can communicate instantaneously with infrastructure and other cars, improving road safety and efficiencies in Metrotech (Reply, 2025).
- Smart Utilities: Can connect water and electricity meters and alerts will be instantaneous to notify of a leak or overuse, reducing waste and operational costs in Metrotech (Reply, 2025).
- Public Safety: The reliability and high-speed connection allow emergency service data flows the ability to access live video sources from drone feeds or security cameras. This allows for instantaneous responses to incidents, and ultimately, improved safety of citizens in Metrotech (Reply, 2025).

Question 3

3.1) Routing is the process of determining the best path for packets to take from the source to the destination across a network. Routing is conducted using routing protocols (OSPF or BGP, for example) that update routing tables with path information and adapt to network changes (Educative, 2025). For example, if one of TechConnect's branch office links goes down, routers will automatically run OSPF, recalculate the best route, and update their routing tables.

Forwarding, on the other hand, is what routers do once routing has determined a path. A router simply looks at the destination address in the packet, checks the forwarding table that was built based on the routing table and sends the packet to the right output interface without recalculating the entire path (Han, n.d.). In TechConnect's case, once the OSPF update has taken place, every packet moving from headquarters to that branch office is quickly forwarded hop-by-hop along the new route based on the updated forwarding table entries.

Therefore, routing is the control plane, the decision-making process that finds and maintains the path, while forwarding is the data plane, the fast, physical step of moving each packet along the given path. Together they are what makes TechConnect's enterprise network reliable and efficient. (Educative, 2025; Han, n.d.)

3.2) Traditional routing protocols are meant to enable routing devices to share information and make decisions about the best path for forwarding packets across a network. Traditional routing protocols use routing tables, metrics, and algorithms to help determine the selected paths forward:

- RIP (Routing Information Protocol): RIP is one of the original distance-vector protocols. RIP uses hop count as its metric, which means packets take the route with the least number of routers as a metric. For instance, in TechConnect's network, RIP could route traffic between two different branch offices with a path that has two hops even if a faster path may exist (GeeksforGeeks, 2025).
- OSPF (Open Shortest Path First): OSPF is a link-state protocol that makes use of Dijkstra's algorithm to determine the shortest path. OSPF determines a path based on the metric (packet traversal through links) while taking into consideration parameters such as bandwidth (the interface's speed) as a part of its decision-making process. This makes OSPF more efficient than RIP. For example, if TechConnect must manage and plan for video conferencing often this will result in requiring a higher quality of service on links with greater bandwidth. OSPF will automatically prioritise a link of a higher bandwidth, or higher quality of service (QoS) (Cisco, 2012).
- BGP (Border Gateway Protocol): BGP is primarily used for routing between different organisations or ISPs. BGP reaches a forwarding decision utilising policies and following the path attributes as opposed to distance. For

example, if TechConnect develops a connection with its cloud provider, BGP allows the organisation to route the traffic it sends through the external connection with the most reliability, available bandwidth or lower cost rather than simply taking the shortest path(Cloudflare, 2025).

3.3) Traditional control plane architectures have key drawbacks simply due to the distributed nature of the control plane. Each router makes its decision independently, which can result in sluggish resolutions to changes in the network, complex configuration, and limited flexibility in managing traffic. To help alleviate the burden of traditional control planes, Software-Defined Networking (SDN) centralises the control plane, adds programmability, and improves network scalability and security in the process:

- Slow Response to Changes (limitation): In traditional networks, if a link unexpectedly fails, it takes time (and may cause temporary packet loss) for each router to share in the updates and recalibrate routes. For example, if TechConnect's enterprise links at a remote branch were failed, the impact to video conferencing services could be delayed while each of the network routers converged again. (Cisco, n.d.).
  SDN solution: The SDN approach centralises the control plane at a controller. Therefore, once a failure is detected, the SDN controller can deploy route rules across the network. When traffic is rerouted, operations such as live training can be uninterrupted. (Cisco, n.d.).
- Complex Configuration (limitation): Traditional routers can be configured manually using OSPF or BGP which adds to the administrative overhead of managing a traditional architecture. The impact of this complexity, in TechConnect's model will make it difficult to scale additional remote branches as branch numbers can scale exponentially. (Open Networking Foundation, 2025)
  SDN solution: SDN allows for simple programmable APIs that allow network administrators to configure policies from a single point of administration and/or initial configuration from a single dashboard view. For example, if TechConnect needed to prioritise VoIP calls over regular data traffic, the SDN controller could simply apply this policy network-wide, rather than requiring the configuration of every device in the TechConnect enterprise network.(Open Networking Foundation, 2025).
- Limited Flexibility in Managed Traffic (limitation): Traditional control planes are still based on mostly static routing decisions, where the routes/routes taken do not adapt to the operational load of routes. For example, a traditional routing decision on TechConnect may simply fail to redirect the congestion on a high-usage link.(Open Networking Foundation, 2025).
  SDN solution: SDN has at its core flexible routing that can be automatically adjusted for a dynamic load balancing across multiple designated paths for critical applications such as remote healthcare consultations or very large data loading, SDN movement can be performed. (Open Networking Foundation, 2025).

As a result, traditional control plane designs struggle with speed, complexity and flexibility, while SDN addresses these challenges through centralised intelligence, programmability and adaptability. Thus, SDN is a good fit for enterprises such as TechConnect that are seeking to build scalable, secure and efficient networks.

Question 4

4.1) The control plane is essentially the brains of a networking device where it decides how to direct network packets. It will create and maintain the routing table and inform the data plane how to navigate through the real traffic of packets. For example, if XYZ Corp has two branches linked together and an outage were to occur, the control plane would allow XYZ Corp to recover from the outage. The control plane would use a routing protocol such as OSPF to find a new path. Then the routing table would update regardless of a manual configuration, while providing traffic to continue using the unaffected path. (Cloudflare, 2025).

Another key role of the control plane is the efficiency of the organisation and how it allocates its resources which generally comes through the control plane implementing policies. This includes rules for routing, security policies, and a measure of Quality of Service (QoS). If the company determining its policy wanted to ensure that Microsoft Teams calls continue to receive priority even during a heavy traffic peak, the control plane will pass that rule into the hardware and the delivery of voice packets should run smoothly, even if the network is full. (Cloudflare, 2025; Juniper, 2023)

Therefore, the control plane controls all the decision (route calculation, implementing policies, updating on-going routing tables) and mitigation, which is beneficial for an enterprise trying to overcome slow convergence and inefficient routing such as XYZ Corporation. (Cloudflare, n.d.; Juniper, n.d.).

4.2) Distance-vector routing is an approach in which each router periodically communicates its routing table to its directly connected neighbours. This communication, called route advertisement, allows all routers to converge on the best routes, where each router determines a distance to a destination, usually hop count, and chooses the lowest one. (GeeksforGeeks, 2024).

For example, if Branch A of the XYZ Corporation wishes to send data to Branch C, the router at Branch A will receive router updates from its directly connected neighbour routers at Branch B and Branch D, and determine which paths have the least hops, and will route that advertisement to its neighbouring routers. This cycle repeats indefinitely, allowing all routers to eventually converge to the best paths.

Unfortunately, distance-vector protocol architectures like Routing Information Protocol (RIP) have a tendency for slow convergence. With link failure, it can take several update cycles before a router even notices a link has failed and update its routing table. It is this slow failure notification time of the router that could lead to incorrect routing tables and possible routing loops causing packet loss (GeeksforGeeks, 2024). This slow convergence may help to explain why they are experiencing latency and inefficiencies in inter-branch communications while using traditional distance-vector routing techniques within the XYZ Corporation.

4.3) OSPF (Open Shortest Path First) is a link-state routing protocol that operates differently than distance-vector protocols. Each router in OSPF generates a map of the network by exchanging Link-State Advertisements (LSAs) with all other routers in the area, resulting in an overall router map of the network, unlike distance-vector routing where the original router only shared its hop counts with its neighbouring routers (CCNA, 2025). OSPF allows each router to create a complete topology and use the Dijkstra algorithm for calculating the shortest path to every network.

In OSPF, the routers in the network become designated routers (DRs) and backup designated routers (BDRs) depending on the network formation and topology. This serves a useful purpose in a multi-access network by preventing an overwhelming amount of LSA traffic, as all the other routers now only send LSA's updates to the DR/BDR. As an example, at XYZ Corporation if Branch A's routers detect a new link to a remote branch, it will generate an LSA and send it to the DR/BDR. Each of the routers will recalculate the shortest path upon receiving notification of the new branch, which ultimately results in routing the data packets through the strongest path. (CCNA, 2025).

The speed of converging any OSPF topologies is related to the avoidance of routing loops, which is ultimately the reason XYZ Corp can implement OSPF routing for a faster, more reliable router communication system between branch offices than traditional distance-vector routing protocols. Ultimately, the control plane will update its routing table following the identified shortest paths while the data plane will route the traffic along the shortest paths that were calculated by the control plane. (CCNA, 2025).

4.4) Routing policies determine how routers will use network topology to decide the actions they will take regarding which path to use to send data, the level of traffic to allow based off predetermined metrics and which paths not to use strictly based off predetermined security concerns of the network. Routing policies help network administrators allow or deny specific classified traffic, determine if a specific route is unsafe or blocked by policy and manipulate what routes are included based of predefined metric determined by the organisation. (Huawei, n.d.).

For example, routing policy configurations at XYZ Corporation can be used by the IT team to prioritise all traffic to and from their headquarters and main data center location. These will allow zoom, people working, database calls, and other critical applications to work without interruption while any other branch is being congested due to an increase in file sharing, email, downloads, etc. for large file sharing. It also permits traffic engineering to allow the same data to flow across multiple paths to stop the same bottleneck traffic wherever possible and to keep from using any path deemed" unsecured" method of transit for security reasons within the organisation. (Juniper, 2024).

By applying routing, they allow the control plane to make better decisions for routing, while the data plane is more efficient in forwarding packets. The routing policies keep transit longer, improve terminal and overall network performance, lower the routing path as it decreases latency, and ensure redundancy and reliability for all operating branches.

Question 5

A. Introduction:
This assignment was broken down into answering scenario-based questions of networking to explore, routing, software defined networking, control planes, OSPF, and encapsulation. To complete this assignment, I broke down the questions into smaller parts, used reliable sources to research each question, and used my own understanding to write the responses. The most difficult part for me was discovering and understanding resources that explained some of the topics in less technical language, but I enjoyed being able to relate the theories to real-world examples of smart cities and enterprise networks.

B. List of hard skills that I learned:
I learnt how to describe networking concepts, like encapsulation, routing protocols, software defined networking, and routing policies in a structured way.

C. List of soft skills that I learned:
I developed my time management and problem-solving skills while planning and researching to properly answer each question.

D. List of technologies and software that I used:

- Microsoft Word: to type up my assignment.
- Draw.io: for my encapsulation illustration.
- Microsoft Edge: to do research.
- Asus Vivobook laptop: to do my whole assignment and use all the software.

E. Conclusion:
This assignment helped me to relate networking theories to practical applications. Even though trying to find valid references was difficult and somewhat frustrating, I was comfortable with being able research and clearly explain things at the end of it.

References

CCNA, 2025. *OSPF Routing Protocol Overview.* [Online]
Available at: https://study-ccna.com/ospf-overview/
[Accessed 04 September 2025].

Cisco, 2012. *Routing Protocols.* [Online]
Available at: https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/network/3-8/reference/guide/routpro.html
[Accessed 03 September 2025].

Cisco, n.d. *Software-Defined Networking.* [Online]
Available at: https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html
[Accessed 03 September 2025].

Cloudflare, 2025. *What is BGP? | BGP routing explained.* [Online]
Available at: https://www.cloudflare.com/en-gb/learning/security/glossary/what-is-bgp/
[Accessed 03 September 2025].

Cloudflare, 2025. *What is the control plane? | Control plane vs. data plane.* [Online]
Available at: https://www.cloudflare.com/en-gb/learning/network-layer/what-is-the-control-plane/
[Accessed 04 September 2025].

Draw.io, n.d. *Draw.io online diagram editor.* [Online]
Available at: https://app.diagrams.net/?src=about
[Accessed 19 August 2025].

Educative, 2025. *What is the difference between routing and forwarding?.* [Online]
Available at: https://how.dev/answers/what-is-the-difference-between-routing-and-forwarding
[Accessed 03 September 2025].

GeeksforGeeks, 2024. *Distance Vector Routing (DVR) Protocol.* [Online]
Available at: https://www.geeksforgeeks.org/computer-networks/distance-vector-routing-dvr-protocol/
[Accessed 04 September 2025].

GeeksForGeeks, 2025. *how data encapsulation and de-encapsulation works?.* [Online]
Available at: https://www.geeksforgeeks.org/computer-networks/how-data-encapsulation-de-encapsulation-works/
[Accessed 02 September 2025].

GeeksForGeeks, 2025. *Packet switching and delays in computer network.* [Online]
Available at: https://www.geeksforgeeks.org/computer-networks/packet-switching-and-delays-in-computer-network/
[Accessed 02 September 2025].

GeeksforGeeks, 2025. *Routing Information Protocol (RIP).* [Online]
Available at: https://www.geeksforgeeks.org/computer-networks/routing-information-protocol-rip/
[Accessed 03 September 2025].

Han, M., n.d. *Lecture 07-01: Network layer forwarding and routing (PDF)*. [Online]
Available at: https://www.cs.utexas.edu/~mhan/courses/cs356r/sp23/lecture_notes/CS356R-07-01-Network-Intro-Forwarding-and-Routing.pdf
[Accessed 03 September 2025].

Huawei, n.d. *Overview of routing policies*. [Online]
Available at:
https://info.support.huawei.com/hedex/api/pages/EDOC1100277644/AEM10221/03/resources/vrp/dc_vrp_route-policy_cfg_0001.html
[Accessed 04 September 2025].

IR, 2025. *What Is Network Packet Loss?*. [Online]
Available at: https://www.ir.com/guides/what-is-network-packet-loss?
[Accessed 02 September 2025].

JumpCloud, 2025. *Understanding encapsulation in networking*. [Online]
Available at: https://jumpcloud.com/it-index/understanding-encapsulation-in-networking
[Accessed 02 September 2025].

Juniper, 2023. *Junos OS architecture overview*. [Online]
Available at: https://www.juniper.net/documentation//us/en/software/junos/junos-overview/topics/concept/junos-software-architecture.html
[Accessed 04 September 2025].

Juniper, 2024. *Configuring OSPF routing policy*. [Online]
Available at: https://www.juniper.net/documentation//us/en/software/junos/ospf/topics/topic-map/configuring-ospf-routing-policy.html
[Accessed 04 September 2025].

Mobile Packet Core, n.d. *LTE (4G) network architecture*. [Online]
Available at: https://mobilepacketcore.com/lte-4g-network-architecture/
[Accessed 02 September 2025].

NSRC, 2019. *Network management & monitoring (PDF)*. [Online]
Available at: https://nsrc.org/workshops/2019/ubuntunet-nren-noc/netmgmt/en/smokeping/types-of-delay.pdf?
[Accessed 02 September 2025].

Open Networking Foundation, 2025. *Software-Defined Networking (SDN) definition*. [Online]
Available at: https://opennetworking.org/sdn-definition/
[Accessed 03 September 2025].

Qualcomm, n.d. *Everything you need to know about 5G.*. [Online]
Available at: https://www.qualcomm.com/5g/what-is-5g
[Accessed 02 September 2025].

Reply, 2025. *5G and smart cities: smarter solutions for a hyperconnected future*. [Online]
Available at: https://www.reply.com/en/telco-and-media/5g-smart-cities
[Accessed 02 September 2025].

Tutorialspoint, 2025. *LTE network architecture*. [Online]
Available at: https://www.tutorialspoint.com/lte/lte_network_architecture.htm
[Accessed 02 September 2025].