FIT9137 Applied Week 9

Topics

- Network Layer:
  - Routing
  - Static Routing
  - Dynamic Routing
- Transport Layer
  - Reliable Communication

Covered Learning Outcomes:

- Analyse and formulate the functions of communication architectures of local area networks, wide area networks and the Internet.
- Examine networks using the underlying fundamental theories, models, and protocols for data transmission.

Instructions

- One of the main purposes of an applied session is to build the learning community, create connections and include the learners. The other goal is to give and receive feedback from your peers and or your tutors.
- Form groups of 2 students (peers) to work through the exercises. If met a problem, try to solve it by asking direct questions to your peer. If the issue was not solved within peers, ask your tutor. If did not get a chance to solve the problem during your applied session with your peer or tutor, jump into one of many consultation hours and ask any of the tutors to help you. Please visit the "Teaching Team and Unit Resources" tile in the FIT9137 Moodle site.

Network & Transport Layer

1. Discuss what is a router, routing, and routing protocol?

A router is a layer 3 device, operates at the network layer, routers connect dissimilar networks. It is the most important piece of Internet infrastructure. Routers require one IP address per interface, i.e., typically per subnet the interface is connected to. Clients send packets to routers if destination is outside their own subnet. Routers use IP address to determine where the packet is sent next

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. ... Packet forwarding is the transit of network packets from one network interface to another. Intermediate nodes are typically network hardware devices such as routers, gateways, firewalls, or switches.

A routing protocol specifies how routers communicate with each other to distribute information that enables them to select routes between nodes on a computer network. Routers perform the traffic directing functions on the Internet; data packets are forwarded through the networks of the internet from router to router until they reach their destination computer. Routing algorithms determine the specific choice of route. Each router has a prior knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network.

2. **Discuss briefly the three components of routing protocol?**

Three components:

- **The routing protocol**: how to find the best route between a sender and a receiver through the network
- **The routing table:** the best routes currently known are stored in a lookup table for fast access
- **The routing decisions**: deciding for each incoming packet where it is sent next

3. **Discuss the Types of decentralized Routing:**

- **Static Routing:** Network manager prepares fixed routing tables Manually updated when the network changes Used in simple networks that don't change a lot.
- **Dynamic Routing:** Routers exchange information to build routing tables dynamically. Initial tables can be set up by network managers

4. **Compare and contrast Distance Vector and Link state Routing protocol? Give an example of Distance Vector and Link state Routing protocols**

   Distance Vector Routing: In distance vector routing, a router need not know the entire path to every network segment; it only requires knowing the direction or vector in which to send the packet. The technique determines the direction (vector) and distance (hop count) to any network in the internetwork.

   Distance vector routing algorithms periodically send all or parts of their routing table to their adjacent neighbors. The routers running a distance vector routing protocol will automatically send periodic updates even if there are no changes in the network.

   A router can verify all the known routes and alters its local routing table based on the updated information received from neighboring routing. RIP, IGRP and EIGRP are the commonly used distance vector protocol that uses hop counts or its routing metrics.

Example: Routing Information Protocol (RIP) is a **protocol** that **routers** can use to exchange network topology **information**. **Routing Information Protocol** (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network.

- **It** is characterized as an interior gateway **protocol.**
- **Typically** used in small to medium-sized networks.
- **Routes** are specified by **IP destination network** and **hop count**.
- The **maximum hop count** allowed for RIP is **15** and hop count of 16 is considered as network unreachable.
- Updates of the network are exchanged periodically.

- Updates (routing information) are always broadcast every **30** seconds
- Full routing tables are sent in updates.
- Routers always trust on routing information received from neighbor routers. This is also known as ***Routing on rumors.***
- **Routers will flush the entry** if the route does not respond in **240** seconds.

Link State Routing: In link-state routing, each router attempts to construct its own internal map of the network topology. At the initial stage of start-up, when a router becomes active, it sends the messages into the network and collects the information from the immediate routers to which it is directly connected. It also provides information about whether the link to reach the router is active or not. This information is used by other routers to build a map of network topology. Then the router uses the map to choose the best path.

The link state routing protocols respond swiftly to the network changes. It sends triggered updates when a network change occurs and sends periodic updates at long time intervals such as 30 minutes. If the link alters state, the device detected the alteration generates and propagate an update message regarding that link to all routers. Then each router takes a copy of the update message and update its routing table and forwards the message to all neighboring routers. This flooding of the update message is needed to ensure that all routers update their database before creating an update routing table that reflects on all routers. OSPF protocol is the example link state routing.

Example: OSPF stands for Open Shortest Path First which uses link-state routing algorithm. Using the link state information, which is available in routers, it constructs the topology in which the topology determines the routing table for routing decisions. It supports both variable-length subnet masking and classless inter-domain routing addressing models. Since it uses Dijkstra's algorithm, it computes the shortest path tree for each route. The main advantages of the OSPF (Open Shortest Path first) are that it handles the error detection by itself, and it uses multicast addressing for routing in a broadcast domain.

OSPF works on Dijkstra algorithm. It is a link state protocol, and it analyzes different sources like the link speed, cost and path congestion while identifying the shortest path. It is basically use for larger size organization in the network. There is no such restriction on the hop count. It is a more intelligent routing protocol than RIP. The networks are classified as areas, sub areas, autonomous systems, and backbone areas. It calculates the metric in terms of bandwidth.

Identify the transport layer protocol that provides connection-less service, List and explain the two strategies used by this connection-less protocol to achieve Quality of services?

5. **Identify the transport layer protocol that provides connection-less service, List and explain the two strategies used by this connection-less protocol to achieve Quality of services?**

   UDP is a connectionless protocol. No connection needs to be established between the source and destination before you transmit data.

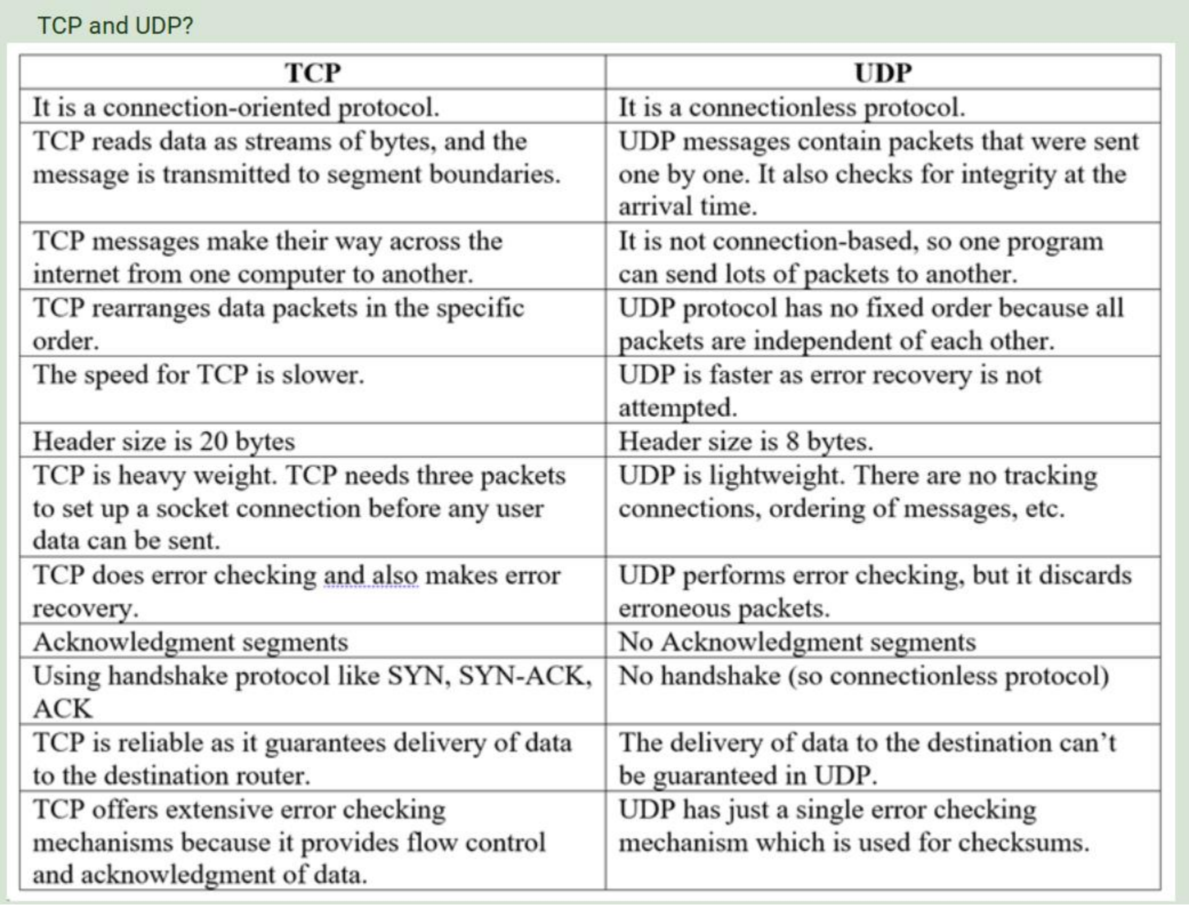
Two strategies:

- **Integrated Services** where applications request a channel with certain guarantees, Implemented by Resource Reservation Protocol (RSVP) on top of UDP.
- **Differentiated Services** where each individual packet requests a certain service class, which is given corresponding priority, implemented using special field in IP packet header

6. **Explain briefly how the transport layer uses sequence numbers and acknowledgement numbers.**

Sequence numbers are used for error correction / ARQ. Sequence/Ack numbers indicate the number of bytes transmitted / received. When a sender receives an ack number, it can determine whether all transmitted bytes have been received correctly, and if not, re-transmit.

7. **Compare and contrast at least four characteristics of the transport layer protocols TCP and UDP?**



TCP and UDP?

TCP	UDP
It is a connection-oriented protocol.	It is a connectionless protocol.
TCP reads data as streams of bytes, and the message is transmitted to segment boundaries.	UDP messages contain packets that were sent one by one. It also checks for integrity at the arrival time.
TCP messages make their way across the internet from one computer to another.	It is not connection-based, so one program can send lots of packets to another.
TCP rearranges data packets in the specific order.	UDP protocol has no fixed order because all packets are independent of each other.
The speed for TCP is slower.	UDP is faster as error recovery is not attempted.
Header size is 20 bytes	Header size is 8 bytes.
TCP is heavy weight. TCP needs three packets to set up a socket connection before any user data can be sent.	UDP is lightweight. There are no tracking connections, ordering of messages, etc.
TCP does error checking and also makes error recovery.	UDP performs error checking, but it discards erroneous packets.
Acknowledgment segments	No Acknowledgment segments
Using handshake protocol like SYN, SYN-ACK, ACK	No handshake (so connectionless protocol)
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination can't be guaranteed in UDP.
TCP offers extensive error checking mechanisms because it provides flow control and acknowledgment of data.	UDP has just a single error checking mechanism which is used for checksums.