Compare and contrast static and dynamic routing. Describe the two types of dynamic Routing Protocols (elaborate each to some extent).

- Static Routing: Can be used when an administrator needs to specify a route or adjust the traffic flow to improve and maximize efficiency, conserve bandwidth, and improve security and performance. Static routing is done manually and dynamic routing is not. They are both routing algorithms to find the lower cost path for a packet to travel. Static routing has fine-tuned controls for administrators which decreases resources being used. However, it takes a lot of time to configure these manual routes and routing tables need to be updated and managed when network topology changes. If an admin can make the static route more efficient than the dynamic route, the dynamic route can be eliminated.
- Dynamic Routing: Enables routers to communicate with each other and map the network, these are routing tables. Routing tables are updated when a route changes or at regular intervals. Dynamic routing is automatically populated by protocols and algorithms. This allows routes to be changed quickly with periodical updates in response to link cost changes. Dynamic routing uses distance-vector and link-state protocols. Distance-vectors are a decentralized algorithm that uses mathematical calculations to compare routes based on some measurement of distance like a hop. Link-state vectors require each router to maintain a partial network map. It is a global routing algorithm that utilizes link-state advertisements to broadcast changes. Routers monitor link state changes and updates are sent to neighboring routers to inform them of the change. The changes and network details/the topology are stores in routing tables.

Explain how digital signature can ensure message integrity and nonrepudiation. Explain each of the two mechanisms clearly.

- Digital signatures use hashing algorithms with asymmetric encryption to ensure message integrity. Hashing algorithms are processes that a computer runs to verify this message integrity by generating a hash value which is a string with a fixed-size representing the original input's contents. Once this hash value is created it can be compared to the original or expected hash value to display whether or not the message has been changed or retains its integrity. This is because a message with integrity is one that has not been changed from the original while being encrypted and decrypted. Asymmetric cryptography uses a message digest to double check the hash value to verify its status.
- Digital signatures also provide nonrepudiation with this asymmetric encryption. The message is encrypted using a private key. When an individual uses the private key, they are the only logical person to have encrypted that message. The public key is the only thing that can decrypt the message. This ensures the message came from the intended individual. Person A cannot deny they sent the message, and Person B cannot deny receiving it.

Explain three analog modulation methods.

1. The first example of an analog modulation method is amplitude modulation (AM). The height of the carrier wave is changed so a higher wave represents a 1 but and a lower wave represents a 0 bit.
2. The second is frequency modulation (FM). The number of waves representing one cycle is changed so the number representing 1 bit is greater than the number representing 0 bit.
3. The third is phase modulation (PM). The cycle's starting point is changed when the bit being transmitted changes

from 1 to 0. The wave oscillates from minimum to neutral and then back to minimum before returning to neutral and back to minimum instead of oscillating regularly from maximum to minimum when the bit changes.

Discuss 802.1X/EAP. Describe its purposes, authentication mechanisms, and the features of the authentication server.

- Purpose: The IEEE 802.1x standard was developed to provide port-based access control on Ethernet LANs and was further revised to work with wireless networks as well. It uses extensible authentication protocol (EAP) and encrypted tunnels for data exchanges. EAP is a group of extensible management protocols that stations use to request port access and includes a method of secure key exchange.
- Authentication Mechanisms: 802.1x authentication involves three main participants which are the supplicant, authenticator, and authentication server. The supplicant is the station that requests access through the authenticator which is usually an AP in wireless networks. The authenticator passes the request to the authentication server which stores the credentials of authorized users.
- Benefits: The supplicant never communicates directly with the authentication server. This reduces the chance of sensitive data on the server being compromised.