- **Describe the goals of network security (locate the slide for the question).**
    - Providing Secure Connectivity: The goal of network security is to provide secure connectivity. Network security used to emphasize blocking attackers from accessing corporate networks and inflicting damage. Now creating a secure connectivity with trusted users and their networks is the main goal.
    - Providing Nonrepudiation: Nonrepudiation is the capability to prevent a participant in an electronic transaction from denying that it performed an action.
    - Secure Remote Access: Providing secure remote access for travelling employees is a large security challenge. Now VPN's are recommended because they use authentication and encryption mechanisms.
    - Ensuring Privacy: Databases that contain personal information must be protected. Financial information is especially at risk. Educating those who interact with data is the best way to maintain its privacy.
    - Confidentiality: Confidentiality prevents intentional and unintentional disclosure of communications between the sender and the recipient.
    - Integrity: Integrity ensures the accuracy and consistency of information during its processing period.
    - Availability: Availability is the assurance that authorized users can access certain resources in a reliable and timely-manner.

- **Describe security risk in terms of threats and vulnerabilities.**
    - Threats: A threat is the potential for a violation of security. This exists when there is the capability, a circumstance, action, or event that could breach an organization's security and inflict harm. Objects, persons, and other entities present a danger to an asset.
    - Vulnerabilities: Vulnerabilities are flaws or weaknesses in a system's design. On top of this, the implementation, operation, and management of a system could be exploited to violate the system's security policy. Vulnerabilities can be classified as leaky, corrupted, unavailable, or slow.

- **Discuss how ICMPv6 replaces ARP and ICMPv4 Router Discovery.**
    - ICMPv6 replaces ARP and ICMPv4 Router Discovery with Neighbor Discovery (ND). It is a new protocol used by IPv6 to determine neighboring hosts. It has prefix detection, duplicate address detection, and automatic address configuration. It is a series of five ICMPv6 messages used to manage node-to-node communications on a link. The duplicate address detection has nodes that check when an address is already in use. The automatic address configuration performs stateless configuration of addresses.

- **Discuss the three drawbacks of IPv4 and how IPv6 overcomes those drawbacks.**
    1. Exponential internet growth and the soon-to-be exhaustion of available IPv4 addresses. There is also the lack of ability of Internet backbone routers to maintain large routing tables. IPv6 has a larger address space because it is 128 bits. Its backbone routing tables only need the entries of other routers that are directly connected to them.

2. There is a need for simpler configuration. IPv6 can determine its own settings based on stateful autoconfiguration or stateless autoconfiguration.
3. There is a requirement for security at the IP level. In IPv6, Network Address Translation (NAT) is unnecessary.
4. There is a need for better support for real-time delivery of data (Quality-of-Service or QoS). IPv6 has integrated support called IPsec.

- **Compare and contrast ping sweeping and port scanning.**
    - Ping Sweeping: Ping Sweeping is used by attackers to determine the location of a host. This is done by an attacker who sends ICMP echo request packets by a range of IP addresses. The actual ping sweep does not do any damage, but the IP addresses used in the ping sweep should be noted so they can be tracked if they are active again.
    - Port Scanning: Port Scanning is when there is an attempt to connect to a computer's ports to see if they are active. When an attacker finds one, they can exploit the known vulnerabilities associated with the service that runs on that port. A signature of a port scan typically includes a SYN packet that was sent to each port on an IP address.