1. **Which of the following is true when describing an anycast address? (3 points)**

    a. Packets addressed to an anycast address are delivered to a single interface.
    b. Packets are delivered to all interfaces identified by the address. This is also called a one-to-many address.
    c. This address identifies multiple interfaces and the anycast packet is only delivered to one device. This address can also be used one-to-one-of-many.
    d. These addresses are meant for non-routing purposes, but they are almost globally unique, so it is unlikely they will have an address overlap.

2. **Which of the following correctly describe characteristics of IPv6 addressing? (Choose all correct answers) – 4 points**

    a. Global addresses start with 2000::/3
    b. Link-local addresses start with FF00::/10
    c. Link-local addresses start with FE80::/10
    d. There is only one loopback address, and it is ::1

3. **Invert the 7th bit of each of the following EUI-64 addresses. For all 5 examples, use the prefix of 2001:db8:1:1/64 (10 points)**

    a. Convert the following MAC address into an EUI-64 address: 0b0c:abcd:1234

    b. Convert the following MAC address into an EUI-64 address: 060c:32f1:a4d2

    c. Convert the following MAC address into an EUI-64 address: 10bc:abcd:1234

    d. Convert the following MAC address into an EUI-64 address: 0d01:3a2f:1234

    e. Convert the following MAC address into an EUI-64 address: 0a0c:abac:caba

Answer: I'll convert each MAC address to an EUI-64 address by:

- Splitting the 48-bit MAC address into two 24-bit halves
- Inserting FFFE between them
- Inverting the 7th bit (universal/local bit)
- Adding the prefix 2001:db8:1:1/64

a. MAC address: 0b0c:abcd:1234

Step 1: Split into 0b0c and cd:1234

Step 2: Insert FFFE: 0b0c:ab:FFFE:cd:1234

Step 3: Invert 7th bit (bit position in first byte):

- 0b in binary: 00001011
- Inverting 7th bit: 00001011 → 00001001 = 09
- Result: 090c:ab:FFFE:cd:1234

IPv6 address: 2001:db8:1:1:090c:abFF:FEcd:1234

b. MAC address: 060c:32f1

Step 1: Split into 060c:32 and f1

Step 2: Insert FFFE: 060c:32:FFFE:f1

Step 3: Invert 7th bit:

- 06 in binary: 00000110
- Inverting 7th bit: 00000110 → 00000100 = 04
- Result: 040c:32:FFFE:f1

IPv6 address: 2001:db8:1:1:040c:32FF:FEf1

c. MAC address: 10bc:abcd:1234

Step 1: Split into 10bc

and cd:1234 Step 2: Insert FFFE: 10bc:ab:FFFE:cd:1234 Step 3: Invert 7th bit:

- 10 in binary: 00010000
- Inverting 7th bit: 00010000 → 00010010 = 12
- Result: 12bc:ab:FFFE:cd:1234

IPv6 address: 2001:db8:1:1:12bc:abFF:FEcd:1234

d. MAC address: 0d01:3a2f:1234

Step 1: Split into 0d01:3a and 2f:1234 Step 2: Insert FFFE: 0d01:3a:FFFE:2f:1234 Step 3: Invert 7th bit:

- 0d in binary: 00001101
- Inverting 7th bit: 00001101 → 00001111 = 0f
- Result: 0f01:3a:FFFE:2f:1234

IPv6 address: 2001:db8:1:1:0f01:3aFF:FE2f:1234

e. MAC address: 0a0c:abac

Step 1: Split into 0a0c

and ac

Step 2: Insert FFFE: 0a0c:ab:FFFE:ac

Step 3: Invert 7th bit:

- 0a in binary: 00001010
- Inverting 7th bit: 00001010 → 00001000 = 08
- Result: 080c:ab:FFFE:ac

IPv6 address: 2001:db8:1:1:080c:abFF:FEac

4. **Which technology is designed to allow an ipv4-only LAN to communicate with an ipv6-only LAN? (2 points)**
   Answer: ISATAP is designed to enable IPv6 communication over an IPv4-only LAN. It allows IPv6-capable hosts within an IPv4 intranet to communicate with each other, even when the network infrastructure only supports IPv4.
   ISATAP treats the IPv4 network as a virtual IPv6 link, and it embeds the IPv4 address into the IPv6 address for routing purposes.

5. **You want to create a test ipv6 network in your organization. You want the test network to include three (3) subnets. What type of ipv6 address do you need? How did you arrive at this conclusion? (4 points).**

   Answer: To create a test IPv6 network with three subnets, I would use a Unique Local Address (ULA) range — specifically, addresses starting with FD00::/8.

   The reason is that ULAs are designed for private use within an organization, similar to private IPv4 ranges like 192.168.x.x. Since this is a test environment, we don't need globally routable addresses. ULAs are not advertised on the public Internet, which makes them ideal for internal testing and development.

   Also, using a /48 ULA prefix (like fd12:3456:789a::/48) would give me plenty of space to create multiple subnets. I can easily break that into subnets like:

- fd12:3456:789a:0001::/64
- fd12:3456:789a:0002::/64
- fd12:3456:789a:0003::/64

So, my conclusion is based on the fact that:

- ULA is intended for internal use.

- It supports subnetting.
- It avoids conflicts with public IPs.
- It’s perfect for testing and lab setups.

6. **Explain why deploying 6to4 might not be as attractive as Teredo, in the real world. (4 points)**

   Answer: In the real world, deploying 6to4 isn’t as attractive as Teredo mainly because 6to4 relies on having a public IPv4 address, and that’s not always available today. Many users, especially those behind NAT (like in homes or small offices) don’t have direct access to a public IPv4 address, which makes 6to4 fail or perform poorly.
   On the other hand, Teredo was specifically designed to work through NAT. It can tunnel IPv6 traffic over UDP even when the device is behind a NAT router. That makes Teredo more reliable in NAT-heavy environments, which are common in real-world networks.
   Another issue is that 6to4 routers must be correctly configured, and when they’re not (which often happens), it leads to broken connectivity or black holes. Teredo is generally more adaptable and self-configuring.

7. **Describe why you do not need to migrate all your devices to ipv6, when converting from ipv4 to ipv6. (5 points)**
   Answer: I don’t need to migrate all my devices to IPv6 right away because IPv4 and IPv6 can run together during the transition. This is called dual stack, where devices support both protocols at the same time, so they can talk to either IPv4 or IPv6 networks depending on what’s needed.

   Also, there are transition technologies like Teredo, 6to4, and NAT64 that allow IPv4-only and IPv6-only systems to communicate. These tools help me upgrade my network step-by-step, without breaking compatibility or causing service issues.

   So instead of doing a full migration all at once, I can move gradually, keeping everything running smoothly as I go.

8. **Your ISP does not yet offer ipv6 services. Your company does need to migrate to ipv6. Describe what option do you have to function in this environment? (3 points)**

   Answer: If my ISP doesn’t support IPv6 yet, but my company still needs to migrate, I can use IPv6 transition technologies to make it work. The best option in this case would be to use a tunneling protocol, like 6to4 or Teredo. These allow me to send IPv6 traffic over the existing IPv4 infrastructure, so I don’t have to wait for the ISP to support native IPv6.

   Another option is to set up a dual stack network internally this way, our devices can use IPv6 inside the company and fall back to IPv4 when connecting to the outside world.

These solutions let me start using IPv6 right now, even if my ISP isn't ready.

9. **Your ISP has given you the IPv6 address 2001:FE12:A231::/48: (8 points**)

   a. How many /64 subnets are available with this address?

      Answer: With a /48 IPv6 address, I can create 2^(64−48) = 2^16 = 65,536 unique /64 subnets. That's because I have 16 bits (from bit position 49 to 64) available for subnetting.

   b. List the first six /64 subnets?

      Answer: To list the first six, I'll just increment the subnet ID from 0000 to 0005 in hexadecimal:

      1. 2001:FE12:A231:0000::/64
      2. 2001:FE12:A231:0001::/64
      3. 2001:FE12:A231:0002::/64
      4. 2001:FE12:A231:0003::/64
      5. 2001:FE12:A231:0004::/64
      6. 2001:FE12:A231:0005::/64

10. **Explain how QoS optimizes voice traffic? (5 points)**

    Answer: Quality of Service (QoS) helps optimize voice traffic by giving it priority over other types of data on the network. Voice calls are sensitive to delay, jitter, and packet loss, so QoS makes sure those packets are sent faster and more reliably.

    QoS does this by:

    - Tagging voice traffic with a higher priority level.
    - Reserving bandwidth for voice so it doesn't get delayed by things like large file downloads.
    - Queuing voice packets first to reduce lag and improve call quality.

    In simple terms, QoS makes sure voice data always gets the "fast lane," so conversations stay clear and smooth even when the network is busy.

11. **A network engineer must configure the router R1 GigabitEthernet 1/1 interface to connect to the router R2 GigabitEthernet 1/1 interface. For the configuration to be applied, the engineer must compress the address 2001:db8:0000:0000:0500:000a:400F:583B. What complete Cisco IOS command must the engineer issue on the interface? (5 points)**

    Answer: First, I'll compress the IPv6 address using standard rules:

    - Remove leading zeros in each group.
    - Replace the longest consecutive block of zeros with : :

    So the full address: 2001:db8:0000:0000:0500:000a:400F:583B
    Becomes: 2001:db8::500:a:400F:583B

    Now, the complete Cisco IOS command to assign this address to interface GigabitEthernet1/1 is:
    ipv6 address 2001:db8::500:a:400F:583B/64

12. **What is the IPv6 prefix of the address 2001:00cb:1562:0dc3:5400:0001:24a0:0014 if the prefix length is /56? (5 points)**
    Answer: To find the IPv6 prefix of this address with a /56 prefix length, I need to keep only the first 56 bits, and zero out the rest.
    The full address is: 2001:00cb:1562:0dc3:5400:0001:24a0:0014
    IPv6 is grouped in 16-bit blocks (each group of 4 hex digits).
    - A /56 means the first 3 full blocks (48 bits) plus 8 bits (2 hex digits) from the fourth block are part of the network prefix.

    Let's break it down:
    - First block: 2001
    - Second block: 00cb
    - Third block: 1562
    - Fourth block (partial): 0d (first 2 hex digits of 0dc3)

    So the /56 prefix is: 2001:00cb:1562:0d00::/56
    We zero out the remaining bits to clean up the host portion.

13. **Describe, in your own words, what is the security threat against ipv6 Router Discovery process (8 points).**

    Answer: The IPv6 Router Discovery (RD) process (part of Neighbor Discovery Protocol, NDP) is vulnerable to several attacks because it relies on unauthenticated ICMPv6 messages. Here are the major threats:

    Rogue Router Advertisement (RA) Attacks

    - A malicious actor sends fake Router Advertisements (RAs), pretending to be a legitimate router.
    - This can redirect traffic to an attacker-controlled device (man-in-the-middle).

    Malicious Default Gateway Spoofing

    - Attackers can override the legitimate default gateway by sending fake RAs.

- Traffic is then intercepted or dropped, causing a DoS or eavesdropping.

Fake Prefix Advertisement (Network Hijacking)

- A rogue router advertises incorrect IPv6 prefixes, leading hosts to use invalid addresses.
- This can isolate hosts or redirect traffic to malicious networks.

Denial-of-Service (DoS) via Flood of Ras

- Attackers flood the network with bogus RAs, causing:
    - Excessive address changes (hosts constantly reconfiguring).
    - CPU exhaustion on routers and hosts.

Neighbor Cache Poisoning (via Fake Redirects)

- Attackers send fake ICMPv6 Redirect messages, tricking hosts into sending traffic to the wrong destination.

Address Resolution (NDP) Spoofing

- Since NDP lacks authentication, attackers can spoof Neighbor Solicitation/Advertisement messages to poison ARP caches (similar to IPv4 ARP spoofing).

SLAAC Exploitation (Stateless Address Autoconfiguration)

- Attackers manipulate RA flags to force hosts into using unsecured SLAAC (instead of DHCPv6), making them vulnerable to address spoofing.

Lack of Encryption & Authentication (NDP Weakness)

- NDP was originally designed without encryption or strong authentication, making it easy to spoof messages.
- SEcure Neighbor Discovery (SEND) was introduced to fix this, but adoption is still limited.

The IPv6 Router Discovery process is inherently insecure due to its reliance on unauthenticated ICMPv6 messages, making it vulnerable to spoofing, MITM attacks, and DoS. Proper hardening (RA Guard, SEND, monitoring) is essential for secure deployment.

14. Describe, in your own words, what is the security threat against ipv6 auto-configuration (10 points)

Answer: IPv6 auto-configuration, especially Stateless Address Auto-Configuration (SLAAC), is one of the key features that makes IPv6 attractive. It allows devices to configure their own IPv6 addresses automatically, without needing manual setup or a dedicated DHCP server. While this makes network management easier, it also opens up serious security vulnerabilities if the network is not properly protected.

The primary security threat lies in the trust-based nature of how SLAAC works. When a device connects to a network, it listens for Router Advertisement (RA) messages from local routers to learn about the network prefix and default gateway. The problem is — any device on the same local network can send these RA messages. This means that an attacker can spoof a RA message, making it look like it's coming from a legitimate router. If a victim's device accepts this spoofed RA, it will set the attacker's device as the default gateway, allowing the attacker to intercept, monitor, or manipulate all of the victim's internet traffic. This is the basis of a man-in-the-middle (MITM) attack.

Another issue is rogue router injection. An attacker can introduce a fake router into the network that advertises invalid or malicious routes. This can lead to:

- Traffic redirection to external or malicious sites,
- Traffic blackholing, where legitimate traffic never reaches its destination,
- or even network instability, as devices repeatedly reconfigure themselves based on conflicting RA messages.

Furthermore, denial-of-service (DoS) attacks are also possible through SLAAC. An attacker can flood the network with fake or constantly changing RA messages, causing devices to repeatedly reset their IP configurations, leading to degraded network performance or complete loss of connectivity.

Another threat is the use of rogue DHCPv6 servers in networks that use stateful auto-configuration. If an unauthorized device responds to DHCPv6 requests faster than the legitimate server, it can provide incorrect IP addresses, DNS servers, or other network parameters — redirecting traffic for the attacker's benefit.

All of this happens because there is no built-in authentication in SLAAC or DHCPv6. Devices will trust any router or DHCP message they receive, as long as it's formatted correctly and arrives quickly. This makes IPv6 networks especially vulnerable during the auto-configuration phase.

To mitigate these threats, network administrators must implement security measures like:

- RA Guard, which blocks unauthorized or rogue RA messages at the switch level,
- SEND (Secure Neighbor Discovery), which adds cryptographic authentication to NDP and RA messages,
- First-hop security features in enterprise-grade switches,
- and port-based access controls to restrict which devices can send router advertisements or act as DHCP servers.

15. **Identify the reverse lookup domain corresponding to the address 2001:db8:2:3:4:5:678:90ab (3 points)**
Answer: Expand the address: 2001:0db8:0002:0003:0004:0005:0678:90ab

Convert to a single string: 20010db80002000300040005067890ab
Reverse by nibble: b.a.0.9.8.7.6.0.5.0.0.0.4.0.0.0.3.0.0.0.2.0.0.0.8.b.d.0.1.0.0.2
Add .ip6.arpa:
Final PTR domain:
b.a.0.9.8.7.6.0.5.0.0.0.4.0.0.0.3.0.0.0.2.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa

16. **Describe whether deploying ipv6 enhances or reduces network security. Be specific and provide examples (10 points)**
Answer: Deploying IPv6 can both enhance and challenge network security, depending on how it's implemented. It introduces modern features that support stronger security, but also brings new risks if not properly managed.

How IPv6 Enhances Security:

Built-in IPsec support: IPv6 was designed with IPsec as a standard feature, allowing encryption and authentication for data at the IP layer. This provides better protection for sensitive data, especially in environments where secure tunnels or VPNs are used.

No reliance on NAT (Network Address Translation): In IPv4, many networks use NAT as a basic layer of security by hiding internal IP addresses. IPv6 doesn't use NAT — instead, every device has a unique global IP. While this might sound risky, it actually simplifies security policies and makes end-to-end encryption and communication easier, without having to deal with NAT-related complications.

Multicast and No Broadcast: IPv6 removes the need for broadcast traffic (which is often exploited in IPv4 attacks like ARP poisoning) and instead uses multicast, which is more efficient and reduces unnecessary exposure to the whole network.

Larger address space = harder scanning: With 128-bit addresses, IPv6 has a massive address space, making it extremely difficult for attackers to scan a subnet for active devices, unlike in IPv4 where scanning a /24 network is easy and quick.

But IPv6 Also Introduces New Risks:
Rogue Router Advertisements (RA): Devices use RA messages to automatically learn network info. If an attacker sends a fake RA, devices may treat them as a default router — which could lead to man-in-the middle attacks or redirected traffic. This is a real risk in public Wi-Fi or LAN environments.

Dual stack increases the attack surface: Most networks run both IPv4 and IPv6 during the transition (called dual stack). This doubles the number of potential vulnerabilities. For example, a firewall might be strict for IPv4 traffic but ignore IPv6, allowing attackers to sneak through.

Complexity and misconfiguration: Since IPv6 is still new for many admins, it's easy to misconfigure ACLs, firewalls, or router settings. Lack of experience can lead to open ports, exposed devices, or unmonitored tunnels.

Example: A company enables IPv6 on their LAN but doesn't configure RA Guard or monitor ICMPv6 traffic. An attacker plugs into the network and sends spoofed Router Advertisement messages, making their device appear as the default router. Other computers on the network accept the rogue RA, sending their internet-bound traffic through the attacker's system. This allows the attacker to capture sensitive data, redirect users to malicious websites, or launch man-in-the-middle attacks, all because the auto-configuration process was left unprotected.

17. **What is the correct abbreviated prefix for IPv6 address 0880:BB80:AAAA:00F0:0770:0010:0000:0113, assuming a mask of /36? (4 points)**
Answer: To determine the correct abbreviated prefix for the given IPv6 address using a /36 prefix length, we follow these steps:
Step 1: Understand the /36 prefix length

- IPv6 addresses are 128 bits long.
- Each hexadecimal character represents 4 bits.
- A /36 prefix means the first 36 bits define the network prefix.

Step 2: Convert the address to binary for the first 36 bits

- The address in hex groups: 0880 : BB80 : AAAA : 00F0 : 0770 : 0010 : 0000 : 0113
- Each group is 16 bits (4 hex digits × 4 bits).
- The first two groups (0880 and BB80) = 32 bits.
- We need 4 more bits from the third group (AAAA) to reach 36 bits.

Step 3: Extract the prefix

- First two groups: 0880:BB80
- Third group: AAAA
  - Hex 'A' = 1010 in binary
  - We only take the first 4 bits (one hex digit) from AAAA, which is 'A' (1010).
- So the prefix covers: 0880:BB80:A000::/36

Step 4: Write the abbreviated prefix

- The third group after taking only the first hex digit is 'A', and the rest are zeros because bits beyond the 36th are host bits.
- So the abbreviated prefix is: 0880:BB80:A000::/36

The correct abbreviated IPv6 prefix for the address 0880:BB80:AAAA:00F0:0770:0010:0000:0113 with a /36 mask is: 0880:BB80:A000::/36
This means the network portion includes the first 36 bits (two full 16-bit blocks and 4 bits of the third block), and the rest are zeroed out for the prefix.

18. **NSA recommends assigning addresses to hosts via what protocol to mitigate the SLAAC privacy issue? (3 points)**

    Answer: The NSA (National Security Agency) recommends using DHCPv6 (Dynamic Host Configuration Protocol for IPv6) to assign addresses to hosts.
    This is because SLAAC (Stateless Address Auto-Configuration) can expose device-specific identifiers, such as the MAC address, when generating IPv6 addresses using EUI-64 format. This may lead to privacy concerns or device tracking.
    By using DHCPv6, organizations gain more centralized control, consistent address assignment, and better privacy since host identifiers are not directly derived from hardware.

19. **What is the issue with Dual Stack? (4 points)**
    Answer: The main issue with Dual Stack is that it increases the network attack surface by running both IPv4 and IPv6 simultaneously. This means that every device and service must be secured and monitored on two different protocols, effectively doubling the potential entry points for attackers.
    Many organizations secure their IPv4 traffic properly but neglect IPv6, often leaving it unfiltered or misconfigured, which attackers can exploit. If IPv6 is enabled but not fully secured, attackers might bypass firewalls, intrusion detection systems, or access control lists that are only watching IPv4.
    Additionally, managing two stacks increases administrative complexity, requiring more resources, training, and configuration efforts.

20. **Given the following route information returned from the show ipv6 route command, what type of route is described? (5 points)**

    C 2001:DB8:1111:5::/64 [0/0]
    via Serial0/0/1, directly connected

    Answer: The route described in the show ipv6 route output is a directly connected route.

    Here's why:

    - **C (Connected):** The route code C at the beginning of the line explicitly indicates a directly connected interface. This means the router has an IPv6 address configured on the Serial0/0/1 interface that belongs to the 2001:DB8:1111:5::/64 subnet.
    - **via Serial0/0/1, directly connected:** This part of the output confirms that the destination network (2001:DB8:1111:5::/64) is directly attached to the Serial0/0/1 interface of the router. There are no intermediate hops or other routers involved in reaching this network. The router knows how to reach any device within this subnet because they are on the same physical link.

- **[0/0]:** The [administrative distance/metric] value of [0/0] further supports this. A directly connected route has an administrative distance of 0 (the most preferred) and a metric of 0 (no cost to reach).

In summary, the router has an interface (Serial0/0/1) that is configured with an IPv6 address within the 2001:DB8:1111:5::/64 network, making this network directly reachable through that interface.