Here are the answers to your questions, based on the provided document:

1. **Benefits of VLANs:** VLANs offer several advantages:
   * **Improved network performance:** By segmenting broadcast domains, VLANs reduce unnecessary traffic and improve overall network efficiency.
   * **Enhanced security:** VLANs isolate sensitive data and prevent unauthorized access to specific network resources.
   * **Cost reduction:** VLANs can reduce the need for expensive routing equipment by allowing logical segmentation within a single switch.
   * **Simplified network management:** VLANs make it easier to add, move, and change network devices and users without reconfiguring the physical infrastructure.
   * **Increased flexibility and scalability:** VLANs allow for easy network expansion and reorganization without major hardware changes.
2. **How VLANs improve network performance and security:**
   * **Network Performance:** VLANs improve network performance by breaking large broadcast domains into smaller ones. This reduces the amount of broadcast traffic that each device has to process, leading to less network congestion and improved overall efficiency.
   * **Security:** VLANs enhance security by isolating traffic between different groups of users or devices. This means that if a security breach occurs in one VLAN, it is less likely to affect other VLANs. It also prevents unauthorized access to sensitive data and resources by keeping them on a separate VLAN.
3. **Types of passwords used to secure a Cisco router:**
   * **Console password:** Secures direct access to the router via the console port.
   * **Auxiliary password:** Secures access via the auxiliary port (e.g., for modem connections).
   * **Telnet/SSH password (VTY password):** Secures remote access to the router via Telnet or SSH.
   * **Enable password/secret:** Secures access to privileged EXEC mode. enable secret is preferred over enable password because it stores the password in an encrypted format.
4. **Difference between Physical Topology and Logical Topology:**
   * **Physical Topology:** Describes the physical arrangement of devices and cables in a network. It shows how devices are interconnected physically.
   * **Logical Topology:** Describes how data flows through the network, independent of the physical arrangement. It shows the logical connections between devices and how they communicate.
5. **Difference between switch, hub, and router:**
   * **Hub:** A basic networking device that connects multiple Ethernet devices together, making them act as a single network segment. It operates at the physical layer (Layer 1) of the OSI model and simply broadcasts all incoming data to all connected devices.
   * **Switch:** A more advanced networking device that connects multiple devices on a local area network (LAN). It operates at the data link layer (Layer 2) of the OSI model and learns the MAC addresses of connected devices. It forwards data only to the intended recipient, improving network efficiency and reducing collisions.
   * **Router:** A network device that forwards data packets between different computer networks. It operates at the network layer (Layer 3) of the OSI model and uses IP addresses to determine the best path for data to travel. Routers connect different networks (e.g., a home network to the internet) and enable communication between them.
6. **EIGRP protocol metrics:** The EIGRP metric is a composite value calculated using bandwidth, delay, reliability, and load. By default, EIGRP uses only bandwidth and delay for metric calculation. The formula is: Metric=256×(256−LoadK1×Bandwidth+K2×Bandwidth​+K3×Delay) Where K1, K2, K3, K4, and K5 are configurable constants. By default, K1=1, K2=0, K3=1, K4=0, K5=0.
7. **Difference between TCP and UDP:**
   * **TCP (Transmission Control Protocol):**
     + Connection-oriented: Establishes a connection before transmitting data.
     + Reliable: Guarantees delivery of data, retransmits lost packets, and provides flow control and error checking.
     + Ordered delivery: Ensures data arrives in the correct sequence.
     + Slower: Due to overhead for reliability.
     + Used for applications requiring high reliability, such as web Browse (HTTP), email (SMTP), and file transfer (FTP).
   * **UDP (User Datagram Protocol):**
     + Connectionless: Does not establish a connection before sending data.
     + Unreliable: Does not guarantee delivery, retransmission, or ordering.
     + Faster: Less overhead due to lack of reliability mechanisms.
     + Used for applications where speed is more critical than guaranteed delivery, such as streaming video/audio, online gaming, and DNS lookups.
8. **How to configure deny 192.168.1.0/28 and then allow 192.168.1.0/24 in EIGRP:** To achieve this, you would typically use an access control list (ACL) and then apply it to EIGRP using a distribute-list. The more specific route (192.168.1.0/28) needs to be denied before the less specific route (192.168.1.0/24) is permitted.
9. access-list 10 deny 192.168.1.0 0.0.0.15 // Deny 192.168.1.0/28
10. access-list 10 permit 192.168.1.0 0.0.0.255 // Permit 192.168.1.0/24
11. !
12. router eigrp [AS\_number]
13. distribute-list 10 in [interface\_type interface\_number] // To filter incoming updates
14. distribute-list 10 out [interface\_type interface\_number] // To filter outgoing updates

Alternatively, using a prefix-list (which is generally preferred for route filtering):

ip prefix-list DENY\_28\_ALLOW\_24 seq 5 deny 192.168.1.0/28

ip prefix-list DENY\_28\_ALLOW\_24 seq 10 permit 192.168.1.0/24

!

router eigrp [AS\_number]

distribute-list prefix DENY\_28\_ALLOW\_24 in [interface\_type interface\_number]

distribute-list prefix DENY\_28\_ALLOW\_24 out [interface\_type interface\_number]

1. **EIGRP Tables:** EIGRP maintains three tables:
   * **Neighbor Table:** Stores information about directly connected EIGRP neighbors, such as their IP addresses and interface information.
   * **Topology Table:** Stores all learned routes from EIGRP neighbors, including feasible successors and successor routes. It contains all destinations advertised by neighbors, along with their metric.
   * **Routing Table:** Contains the best paths to all known destinations, selected from the topology table. These are the routes that the router will use to forward traffic.
2. **EIGRP summary route and EIGRP external route:**
   * **EIGRP Summary Route:** A summarized route represents multiple more specific routes as a single, less specific route. This helps to reduce the size of routing tables and routing update traffic. For example, 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24 could be summarized as 192.168.0.0/22.
   * **EIGRP External Route:** An external route is a route that was learned by EIGRP from another routing protocol (e.g., OSPF, RIP, BGP) and then redistributed into EIGRP. These routes are marked with an external flag and have an administrative distance of 170 by default, indicating they are less preferred than internal EIGRP routes.
3. **How to redistribute an IPv6 default route in EIGRP:** To redistribute an IPv6 default route into EIGRP, you would typically use the redistribute static command (assuming the default route is a static route) or redistribute ospf etc., along with the default-information originate command if you want the router to advertise a default route into EIGRP.

First, ensure you have an IPv6 default route configured on the router:

ipv6 route ::/0 [next-hop-ipv6-address or exit-interface]

Then, within the EIGRP IPv6 router configuration:

ipv6 router eigrp [AS\_number]

redistribute static

default-information originate

1. **Loading routing tables in OSPF and the command:** In OSPF, the routing table is populated based on the Link-State Database (LSDB). The LSDB contains all the Link State Advertisements (LSAs) flooded throughout an area. OSPF routers use Dijkstra's Shortest Path First (SPF) algorithm to calculate the best paths to all destinations from the LSDB and then populate the routing table.

To view the OSPF routing table (i.e., the OSPF routes that are installed in the IP routing table), you can use the command:

show ip route ospf

To view the OSPF database (LSDB), which is used to build the routing table:

show ip ospf database

1. **Steps needed to change Neighborship to adjacency (OSPF):** The transition from OSPF neighborship to full adjacency involves several states, where routers exchange more detailed link-state information to build a complete topological map. The key steps/states for full adjacency are:
   * **Down:** No Hellos have been received from the neighbor.
   * **Init:** Hellos received, but router's own Router ID not in neighbor's Hello.
   * **2-Way:** Hellos received with mutual Router IDs (router's Router ID is in neighbor's Hello). This is where DR/BDR election occurs on multi-access networks.
   * **Exstart:** Routers establish a master-slave relationship and exchange DBD (Database Description) packets to describe their LSDBs.
   * **Exchange:** Routers exchange the actual DBD packets.
   * **Loading:** Routers send Link State Request (LSR) packets for missing LSAs and receive Link State Update (LSU) packets.
   * **Full:** LSDBs are synchronized, and routers are fully adjacent.
2. **OSPF timers:** OSPF uses timers to maintain neighbor relationships and ensure network stability:
   * **Hello Interval:** The frequency (in seconds) at which an OSPF router sends Hello packets out of an interface. The default is 10 seconds on broadcast and point-to-point networks, and 30 seconds on non-broadcast multi-access (NBMA) networks.
   * **Dead Interval:** The amount of time (in seconds) that a router waits to receive a Hello packet from a neighbor before declaring that neighbor down. The default is 4 times the Hello interval (40 seconds for broadcast/point-to-point, 120 seconds for NBMA).
   * **Wait Timer:** Used in the DR/BDR election process, this timer is equal to the Dead Interval.
   * **LSA Max Age Timer:** The maximum age an LSA can stay in the LSDB (3600 seconds or 1 hour). If an LSA reaches its max age, it is flushed from the database unless it is refreshed.
3. **Configure default and static route of IPv6 as shown in the figure (page 1):** To configure PC0 to recognize PC1 and PC1 to recognize PC0, you need to configure IPv6 addressing and routing on all routers (Router0, Router1, Router2, Router3) and the PCs. You'll need to set up static routes for connectivity between the subnets, and then a default route on the edge routers (Router0 and Router3) pointing towards the core.

**Router0 Configuration (Partial example for interfaces and default route):**

ipv6 unicast-routing

!

interface Gig0/0/0

ipv6 address 2001:B77:EF01:2002::1/64

no shutdown

!

interface Gig0/0/1

ipv6 address 2001:B77:EF01:002::1/64

no shutdown

!

ipv6 route ::/0 2001:B77:EF01:2002::2 // Default route pointing to Router1

**Router1 Configuration (Partial example for interfaces and static routes):**

ipv6 unicast-routing

!

interface Gig0/0/0

ipv6 address 2001:B77:EF01:2002::2/64

no shutdown

!

interface Gig0/0/1

ipv6 address 2001:B77:EF01:222::1/64

no shutdown

!

ipv6 route 2001:B77:EF01:1002::/64 2001:B77:EF01:222::2 // Static route to Router2's subnet

ipv6 route 2001:B77:EF01:100::/64 2001:B77:EF01:222::2 // Static route to PC1's subnet

ipv6 route 2001:B77:EF01:002::/64 Null0 // Static route for connected network (or redistribute connected)

**Router2 Configuration (Partial example for interfaces and static routes):**

ipv6 unicast-routing

!

interface Gig0/0/0

ipv6 address 2001:B77:EF01:222::2/64

no shutdown

!

interface Gig0/0/1

ipv6 address 2001:B77:EF01:1002::1/64

no shutdown

!

ipv6 route 2001:B77:EF01:002::/64 2001:B77:EF01:222::1 // Static route to PC0's subnet

ipv6 route 2001:B77:EF01:100::/64 2001:B77:EF01:1002::2 // Static route to PC1's subnet

**Router3 Configuration (Partial example for interfaces and default route):**

ipv6 unicast-routing

!

interface Gig0/0/0

ipv6 address 2001:B77:EF01:1002::2/64

no shutdown

!

interface Gig0/0/1

ipv6 address 2001:B77:EF01:100::1/64

no shutdown

!

ipv6 route ::/0 2001:B77:EF01:1002::1 // Default route pointing to Router2

**PC0 Configuration (IPv6 Address and Gateway):**

IPv6 Address: 2001:B77:EF01:002::100

Default Gateway: 2001:B77:EF01:002::1

**PC1 Configuration (IPv6 Address and Gateway):**

IPv6 Address: 2001:B77:EF01:100::100

Default Gateway: 2001:B77:EF01:100::1

1. **Write the full form of IPv6 and fill in the table (global routing, subnet ID, Interface ID):**

| Full Form of IPv6 Address | Global ID | Subnet ID | Interface ID | | :-------------------------------- | :-------------------------- | :----------- | :------------------- | | 2001:0BD8:0AA1:0BBA:0000:0000:0000:00A1 | 2001:BD8:0AA1:BBA | 0000 (implied) | 0000:0000:0000:00A1 | | 2001:0BD7:0B11:00BA:0006:0000:010A:00AA | 2001:BD7:0B11 | 00BA | 0006:0000:010A:00AA | | 2001:BBAB:0768:00EA:01F4:0000:0000:0000 | 2001:BBAB:768 | 00EA | 01F4:0000:0000:0000 |

*Note: The "Global ID" typically refers to the global routing prefix (first 48 bits, or first 3 hextets in typical assignment). The "Subnet ID" is the next 16 bits, and the "Interface ID" is the last 64 bits.*

1. **Configure DHCP and Static/EIGRP IP route on Router1, Router2, and Router3 for NET 200, NET 201, and NET 202 and ensure all computers can communicate:**

**Part A: Configure DHCP**

**Router1 (for NET 200)**

ip dhcp excluded-address 192.168.200.1 192.168.200.99

ip dhcp excluded-address 192.168.200.254

ip dhcp pool NET200\_POOL

network 192.168.200.0 255.255.255.0

default-router 192.168.200.254

**Router2 (for NET 201)**

ip dhcp excluded-address 192.168.201.1 192.168.201.99

ip dhcp excluded-address 192.168.201.254

ip dhcp pool NET201\_POOL

network 192.168.201.0 255.255.255.0

default-router 192.168.201.254

**Router3 (for NET 202)**

ip dhcp excluded-address 192.168.202.1 192.168.202.99

ip dhcp excluded-address 192.168.202.254

ip dhcp pool NET202\_POOL

network 192.168.202.0 255.255.255.0

default-router 192.168.202.254

**Part B: Configure Static and EIGRP IP routes** *Note: For all computers to recognize each other, you'll need both static routes for direct connections between routers, and EIGRP to dynamically learn routes to other networks.*

**Router1**

! Interface configurations based on the diagram

interface GigabitEthernet0/0

ip address 192.168.200.254 255.255.255.0

no shutdown

interface Serial0/0/0

ip address 192.168.111.254 255.255.255.252

no shutdown

!

ip route 192.168.112.0 255.255.255.252 192.168.111.253 // Static route to NET 112 via Router2

ip route 192.168.201.0 255.255.255.0 192.168.111.253 // Static route to NET 201 via Router2

ip route 192.168.202.0 255.255.255.0 192.168.111.253 // Static route to NET 202 via Router2

!

router eigrp 100 // Example AS number

network 192.168.200.0 0.0.0.255

network 192.168.111.0 0.0.0.3

no auto-summary

**Router2**

! Interface configurations based on the diagram

interface GigabitEthernet0/0

ip address 192.168.201.254 255.255.255.0

no shutdown

interface Serial0/0/0

ip address 192.168.111.253 255.255.255.252

no shutdown

interface Serial0/0/1

ip address 192.168.112.254 255.255.255.252

no shutdown

!

ip route 192.168.200.0 255.255.255.0 192.168.111.254 // Static route to NET 200 via Router1

ip route 192.168.202.0 255.255.255.0 192.168.112.253 // Static route to NET 202 via Router3

!

router eigrp 100

network 192.168.201.0 0.0.0.255

network 192.168.111.0 0.0.0.3

network 192.168.112.0 0.0.0.3

no auto-summary

**Router3**

! Interface configurations based on the diagram

interface GigabitEthernet0/0

ip address 192.168.202.254 255.255.255.0

no shutdown

interface Serial0/0/0

ip address 192.168.112.253 255.255.255.252

no shutdown

!

ip route 192.168.111.0 255.255.255.252 192.168.112.254 // Static route to NET 111 via Router2

ip route 192.168.200.0 255.255.255.0 192.168.112.254 // Static route to NET 200 via Router2

ip route 192.168.201.0 255.255.255.0 192.168.112.254 // Static route to NET 201 via Router2

!

router eigrp 100

network 192.168.202.0 0.0.0.255

network 192.168.112.0 0.0.0.3

no auto-summary

1. **Multicast addresses used in OSPF:** OSPF uses specific multicast addresses to communicate with other OSPF routers:
   * **224.0.0.5 (All OSPF Routers):** This address is used by OSPF routers to send Hello packets and Link State Updates (LSUs) to all OSPF routers on a segment.
   * **224.0.0.6 (All Designated Routers - DRs and BDRs):** This address is used by OSPF Designated Routers (DRs) and Backup Designated Routers (BDRs) to send LSUs to all other OSPF routers on a multi-access segment. Non-DR/BDR routers also send their LSUs to this address.
2. **Static Route and command line example:**
   * **Static Route:** A manually configured route in a router's routing table that specifies a fixed path for network traffic to reach a particular destination. Unlike dynamic routes, static routes do not automatically adapt to network changes.
   * **Example command line:**
   * ip route [destination-network] [subnet-mask] [next-hop-ip-address | exit-interface] [administrative-distance]

Example:

ip route 192.168.10.0 255.255.255.0 10.0.0.1

This command tells the router that to reach the 192.168.10.0/24 network, it should forward packets to the next-hop IP address 10.0.0.1.

1. **Default Route and command line example:**
   * **Default Route:** A route that specifies the path for all traffic for which there is no more specific route in the routing table. It's often referred to as the "gateway of last resort" and is commonly used to direct traffic to the internet or to a core router in a stub network.
   * **Example command line:**
   * ip route 0.0.0.0 0.0.0.0 [next-hop-ip-address | exit-interface]

Example:

ip route 0.0.0.0 0.0.0.0 203.0.113.1

This command sends all traffic not explicitly routed to the next-hop IP address 203.0.113.1.

1. **Routing Information Protocol (RIP) and command line example:**
   * **Routing Information Protocol (RIP):** A distance-vector routing protocol that uses hop count as its metric. It is one of the oldest routing protocols. RIP is typically used in small to medium-sized networks due to its simplicity, but it has limitations such as a maximum hop count of 15 (16 is infinite/unreachable) and slow convergence.
   * **Example command line (RIPv2):**
   * router rip
   * version 2
   * network 192.168.1.0
   * network 10.0.0.0
   * no auto-summary
2. **User EXEC mode:** User EXEC mode is the first level of access a user gets when logging into a Cisco device. It provides a very limited set of commands, primarily for basic monitoring and connectivity tests (e.g., ping, traceroute). The prompt typically ends with >. You cannot make any configuration changes in this mode.
3. **Privileged EXEC mode:** Privileged EXEC mode (also known as enable mode) provides access to all router commands, including those for viewing system information, debugging, and testing. It is accessed from User EXEC mode by typing enable and entering the enable password/secret. The prompt typically ends with #. From this mode, you can enter global configuration mode.
4. **Global configuration mode:** Global configuration mode is where you make changes that affect the entire router's operation. You enter this mode from privileged EXEC mode by typing configure terminal. The prompt changes to (config)#. From global configuration mode, you can access various sub-configuration modes (e.g., interface configuration mode, router configuration mode).
5. **IPv6 and its general characteristics:**
   * **IPv6 (Internet Protocol version 6):** The latest version of the Internet Protocol, designed to replace IPv4. It addresses the depletion of IPv4 addresses and introduces several improvements.
   * **General Characteristics:**
     + **Larger Address Space:** Uses 128-bit addresses, providing an astronomically larger number of unique addresses compared to IPv4's 32-bit addresses.
     + **Simplified Header:** Has a simpler and more efficient header format, which can improve routing efficiency.
     + **No Broadcasts:** Replaces broadcast with multicast and anycast, reducing network traffic.
     + **Improved Security:** IPSec is natively built into IPv6, providing end-to-end security (authentication and encryption).
     + **Stateless Autoconfiguration (SLAAC):** Allows devices to automatically configure their IPv6 addresses without a DHCP server.
     + **Better Support for Mobile IP:** Designed with mobility in mind.
     + **Enhanced QoS:** Improved support for Quality of Service through Flow Label field.
6. **OSPF Router ID:** The OSPF Router ID (RID) is a 32-bit value (formatted like an IPv4 address) that uniquely identifies an OSPF router within an OSPF autonomous system. It is used in the OSPF Hello packets and in the Link State Advertisements (LSAs) to identify the originating router. The Router ID is determined in the following order of preference:
   * Manually configured using the router-id command under OSPF router configuration mode.
   * The highest IP address of any loopback interface that is up/up.
   * The highest IP address of any active physical interface that is up/up.
7. **RIP routing protocol and command line example:**
   * **RIP (Routing Information Protocol):** (Already covered in question 21).
   * **Example command line (RIPv2):** (Already covered in question 21).
8. **OSPF Routing protocol:** OSPF (Open Shortest Path First) is a link-state routing protocol that is widely used in large enterprise networks. It uses Dijkstra's algorithm to calculate the shortest path to each destination based on a "cost" metric assigned to links. OSPF is known for its fast convergence, support for hierarchical design (areas), and scalability.
9. **Characteristics of OSPF:** Some characteristics of OSPF include:
   * **Link-State Protocol:** OSPF routers exchange link-state advertisements (LSAs) to build a complete topological map of the network.
   * **Hierarchical Design (Areas):** Supports the division of a large network into smaller, more manageable areas, which improves scalability and reduces routing table size.
   * **Fast Convergence:** Quickly adapts to network changes by using triggered updates and the SPF algorithm.
   * **Cost-Based Metric:** Uses a cost metric (bandwidth by default) to determine the best path.
   * **Classless:** Supports Variable Length Subnet Masks (VLSM) and Classless Inter-Domain Routing (CIDR).
   * **Multicast Updates:** Uses multicast addresses (224.0.0.5 and 224.0.0.6) for updates.
   * **Authentication:** Supports clear-text and MD5 authentication for secure routing updates.
10. **Requirements for dividing an autonomous system into different areas (OSPF):** The primary requirement for dividing an OSPF autonomous system into areas is to improve scalability, reduce routing table size on non-backbone routers, limit the impact of network instability (link flaps), and reduce the frequency of SPF calculations. Each area must have a router connected to the backbone area (Area 0), known as an Area Border Router (ABR). All non-backbone areas must be directly connected to the backbone area.
11. **Benefits of dividing the entire network into areas (OSPF):** The benefits of dividing a network into OSPF areas include:
    * **Reduced SPF Calculations:** Link-state changes within an area do not trigger SPF recalculations in other areas, localizing the impact of topology changes.
    * **Smaller Routing Tables:** Routers in non-backbone areas only need detailed information about their own area and summary routes for other areas, reducing memory consumption.
    * **Reduced LSA Flooding:** LSAs are confined to their respective areas, reducing the amount of routing traffic.
    * **Improved Scalability:** Allows OSPF to scale to very large networks.
    * **Easier Troubleshooting:** Network issues can be isolated to specific areas, simplifying troubleshooting.
12. **Backbone Area (OSPF):** The Backbone Area, also known as Area 0 (or Area 0.0.0.0), is the central and most important area in an OSPF hierarchical design. All other non-backbone areas must connect to the backbone area. The backbone's primary role is to provide a logical and physical distribution path for inter-area routing information.
13. **Parameters that must match for two OSPF routers to become neighbors:** For two OSPF routers to become neighbors (and eventually achieve full adjacency), the following parameters must match on their shared segment:
    * **Hello Interval:** The frequency at which Hello packets are sent.
    * **Dead Interval:** The time a router waits before declaring a neighbor down.
    * **Area ID:** The OSPF area that the interface belongs to.
    * **Authentication Type and Password (if configured):** If authentication is enabled, the type (e.g., clear text, MD5) and password must match.
    * **Stub Area Flag (if configured):** If the area is configured as a stub area, this flag must match.
    * **Subnet Mask (on broadcast/non-broadcast links):** For point-to-point links, the subnet mask does not necessarily need to match, but for multi-access segments, they must match for IP connectivity and neighbor discovery.
14. **OSPF states:** (Already covered in question 13 regarding steps to adjacency).
15. **OSPF LSA, LSU, and LSR:**
    * **LSA (Link State Advertisement):** A small packet of routing information that describes the state of a router's links (interfaces) and their associated networks. LSAs are generated by OSPF routers and flooded throughout an area to build the Link-State Database (LSDB). There are several types of LSAs (e.g., Router LSA, Network LSA, Summary LSA).
    * **LSU (Link State Update):** A packet that contains one or more LSAs. LSUs are used to reliably flood LSAs throughout the OSPF area. When a router receives an LSU, it acknowledges it and updates its LSDB.
    * **LSR (Link State Request):** A packet sent by an OSPF router when it discovers that parts of its LSDB are outdated or incomplete compared to a neighbor's. The LSR requests specific LSAs from the neighbor to synchronize the LSDBs.
16. **Steps needed to change Neighborship to adjacency:** (Already covered in question 13).
17. **Default Hello Interval (OSPF):** The default Hello Interval for OSPF is:
    * **10 seconds:** On broadcast multi-access networks (like Ethernet) and point-to-point links.
    * **30 seconds:** On non-broadcast multi-access (NBMA) networks (like Frame Relay, ATM).
18. **Default Dead Interval (OSPF):** The default Dead Interval for OSPF is typically four times the Hello Interval:
    * **40 seconds:** On broadcast multi-access networks and point-to-point links.
    * **120 seconds:** On non-broadcast multi-access (NBMA) networks.
19. **OSPF LSA types:** There are several types of OSPF LSAs, each carrying specific routing information:
    * **Type 1 - Router LSA (Router Link Advertisements):** Generated by every router within an area, describing the state of its links (interfaces) to other routers and networks in the same area. Flooded only within its area.
    * **Type 2 - Network LSA (Network Link Advertisements):** Generated by the Designated Router (DR) on multi-access networks, describing the routers connected to that segment. Flooded only within its area.
    * **Type 3 - Summary LSA (Inter-Area Link Advertisements):** Generated by Area Border Routers (ABRs) to advertise routes from one area into another. Used for inter-area routing.
    * **Type 4 - ASBR Summary LSA:** Generated by ABRs to advertise the location of an Autonomous System Boundary Router (ASBR) to other areas.
    * **Type 5 - External LSA (AS External Link Advertisements):** Generated by ASBRs to advertise routes learned from other routing protocols (external routes) into OSPF. Flooded throughout all areas (except stub/NSSA areas).
    * **Type 7 - NSSA External LSA:** Generated by an ASBR in a Not So Stubby Area (NSSA) to advertise external routes into the NSSA. These Type 7 LSAs are converted to Type 5 LSAs by the NSSA ABR when forwarded to other areas.
20. **How to configure OSPF Routing Protocol:** Basic OSPF configuration involves enabling the OSPF process, defining the networks to be advertised, and assigning them to an area.
21. router ospf [process-id]
22. router-id [x.x.x.x] // (Optional, but recommended)
23. network [network-address] [wildcard-mask] area [area-id]
24. // Example: network 192.168.1.0 0.0.0.255 area 0
25. // Example: network 10.0.0.0 0.255.255.255 area 1
26. passive-interface [interface-type interface-number] // (Optional, to suppress OSPF on an interface)
27. **Does EIGRP need "ip default-network" command to operate a default route?** No, EIGRP generally does not need the ip default-network command to advertise a default route. While ip default-network was used in older IGRP/EIGRP implementations, the preferred method to inject a default route into EIGRP is using the redistribute static command (if a static default route exists) or ip summary-address eigrp [AS\_number] 0.0.0.0 0.0.0.0 on an interface. The default-information originate command can also be used, especially when redistributing from another protocol or creating a default route based on an external source.
28. **Should I use "eigrp log-neighbor-changes command" when I install EIGRP?** The eigrp log-neighbor-changes command enables logging of EIGRP neighbor state changes (e.g., a neighbor going up or down). It's generally recommended to use this command, especially during initial setup and in production environments. It provides valuable troubleshooting information by indicating when neighbor adjacencies are formed or lost, which can help diagnose connectivity issues or unstable links.
29. **Does EIGRP support secondary addresses?** Yes, EIGRP does support secondary IP addresses. If an interface has a secondary IP address configured, EIGRP will advertise the network associated with that secondary address. This can be useful in scenarios where you need multiple IP subnets on a single physical interface.
30. **What debugging capabilities does EIGRP have?** EIGRP provides several debugging commands to monitor its operations and troubleshoot issues. Some common EIGRP debugging commands include:
    * debug eigrp packets: Shows EIGRP packet activity (Hello, Update, Query, Reply, Ack).
    * debug eigrp neighbor: Displays information about EIGRP neighbor state changes.
    * debug ip eigrp: A more general debug command that can include various EIGRP events.
    * debug eigrp internal: Provides details about internal EIGRP processes.
    * debug eigrp event: Shows significant EIGRP events.
    * debug eigrp summary: Provides a summary of EIGRP activities.
    * show ip eigrp traffic: Shows statistics on EIGRP packets sent and received.
31. **Does EIGRP support aggregation and variable-length subnet masks?** Yes, EIGRP fully supports both aggregation (route summarization) and Variable Length Subnet Masks (VLSM).
    * **Aggregation (Summarization):** EIGRP allows manual route summarization on interface boundaries using the ip summary-address eigrp command. This helps reduce the size of routing tables and limit query floods.
    * **VLSM:** EIGRP is a classless routing protocol, meaning it includes subnet mask information in its routing updates. This allows for the use of VLSM, which enables efficient use of IP address space by allowing different subnet mask lengths within the same major network.
32. **Can I configure more than one EIGRP autonomous system on a single router?** Yes, you can configure more than one EIGRP autonomous system (AS) on a single Cisco router. This is achieved by running multiple EIGRP processes, each with a different AS number. This can be useful in scenarios where a router needs to participate in different EIGRP domains, for instance, during network mergers or when interconnecting separate EIGRP networks.
33. **What are the key differences between IPv4 and IPv6?** | Feature | IPv4 | IPv6 | | :----------------- | :------------------------------------ | :------------------------------------- | | **Address Length** | 32-bit | 128-bit | | **Address Format** | Dotted decimal (e.g., 192.168.1.1) | Hexadecimal with colons (e.g., 2001:db8::1) | | **Address Space** | Limited (~4.3 billion unique addresses) | Vast (2^128 unique addresses) | | **Header** | Larger, more complex | Simpler, fixed size, more efficient | | **Checksum** | Present in header | Not present in header | | **Fragmentation** | Handled by routers | Handled only by sending host | | **Broadcast** | Supports broadcast addresses | Replaced by multicast and anycast | | **IPSec** | Optional | Built-in (native) | | **Mobility** | Mobile IP added later | Better inherent support | | **Configuration** | Manual, DHCP | Manual, DHCPv6, SLAAC | | **DNS Records** | A records | AAAA records |
34. **Explain the purpose of subnetting in networking:** The purpose of subnetting in networking is to divide a large network into smaller, more manageable subnetworks (subnets). This offers several benefits:
    * **Improved Efficiency:** Reduces the size of broadcast domains, leading to less broadcast traffic and improved network performance.
    * **Better Security:** Allows for the isolation of network segments, preventing unauthorized access to sensitive areas and containing security breaches.
    * **Enhanced Network Management:** Makes it easier to manage and troubleshoot network issues by localizing problems to specific subnets.
    * **Optimized IP Address Utilization:** Allows for more efficient allocation of IP addresses, especially with Variable Length Subnet Masking (VLSM), by using only the necessary number of hosts per subnet.
    * **Hierarchical Design:** Enables a more structured and hierarchical network design, which is crucial for large-scale networks.
35. **How does ARP (Address Resolution Protocol) work in an internetworking environment?** ARP (Address Resolution Protocol) is a Layer 2 protocol used to resolve an IPv4 address to a MAC address (Layer 2 physical address) within a local network segment. It works as follows:
    * **ARP Request:** When a device (e.g., PC1) wants to send data to another device (e.g., PC2) on the same local network segment, and it only knows PC2's IP address but not its MAC address, PC1 sends an ARP request. This request is a broadcast message (sent to all devices on the segment) containing PC2's IP address and PC1's own MAC and IP address.
    * **ARP Reply:** All devices on the segment receive the ARP request. Only the device that owns the requested IP address (PC2 in this case) responds with an ARP reply. The ARP reply contains PC2's MAC address and is sent as a unicast message directly to PC1.
    * **ARP Cache:** PC1 receives the ARP reply and stores the IP-to-MAC address mapping in its ARP cache for future use. This avoids sending an ARP request for every packet.
    * **Inter-Network Communication:** If the destination IP address is on a different network, the sending device sends the packet to its default gateway (router). The router then performs its own ARP process to determine the MAC address of the next-hop router or destination device on the subsequent network segment.
36. **Explain how OSPF (Open Shortest Path First) routing protocol works:** OSPF is a link-state routing protocol that operates by each router independently computing the shortest path to all known destinations. Here's how it generally works:
    * **Neighbor Discovery:** OSPF routers send Hello packets out of their OSPF-enabled interfaces to discover and establish neighbor relationships.
    * **Adjacency Formation:** Once neighbor relationships are established (2-way state), routers exchange Database Description (DBD) packets to share summaries of their Link-State Databases (LSDBs). If a router finds that it is missing LSAs from a neighbor, it sends Link State Request (LSR) packets to request the missing information. The neighbor then sends Link State Update (LSU) packets containing the requested LSAs.
    * **LSDB Synchronization:** Through this exchange, all routers within an OSPF area build an identical Link-State Database (LSDB), which is a complete topological map of that area.
    * **SPF Algorithm (Dijkstra):** Each router then uses Dijkstra's Shortest Path First (SPF) algorithm to calculate the shortest path tree to all known destinations, with itself as the root. The "cost" of a link (interface) is used as the metric for this calculation (default is based on bandwidth).
    * **Routing Table Population:** The best paths identified by the SPF algorithm are then installed into the router's IP routing table.
    * **Updates:** When a change occurs in the network topology (e.g., a link goes down, a new link comes up), the affected router generates a new LSA, floods it within its area, and other routers update their LSDBs and re-run the SPF algorithm to converge quickly.
37. **What is BGP (Border Gateway Protocol) and why is it important in the Internet?**
    * **BGP (Border Gateway Protocol):** BGP is the de facto standard exterior gateway protocol (EGP) used for routing between autonomous systems (AS) on the internet. Unlike interior gateway protocols (IGPs) like OSPF or EIGRP, which route within an AS, BGP routes between different ASes. It is a path-vector routing protocol.
    * **Importance in the Internet:**
      + **Interconnects Autonomous Systems:** BGP is fundamental to the internet's structure as it enables the exchange of routing information between the tens of thousands of independent networks (ASes) that make up the internet.
      + **Scalability:** It is designed to handle the massive scale of the internet's routing table, carrying hundreds of thousands of routes.
      + **Policy-Based Routing:** BGP allows network administrators to implement complex routing policies based on various attributes (e.g., AS Path, Local Preference, MED) to control how traffic enters and exits their AS. This is crucial for traffic engineering and meeting business objectives.
      + **Stability and Control:** BGP is designed for stability and provides mechanisms to prevent routing loops and ensure the integrity of routing information across the internet.
38. **Describe the Verification Commands in BGP routing protocol:** To verify BGP operations, you can use several show commands:
    * show ip bgp summary: Provides a concise overview of BGP neighbor relationships, including their state, messages exchanged, and prefix counts.
    * show ip bgp: Displays the contents of the BGP routing table, including prefixes, next-hop information, and BGP attributes.
    * show ip bgp neighbors: Shows detailed information about BGP neighbors, including their configuration, capabilities, and session statistics.
    * show ip bgp [network-address]: Displays BGP information for a specific network.
    * show ip bgp regexp [regular-expression]: Filters BGP routes using a regular expression.
    * show ip bgp longer-prefixes [network-address]: Shows more specific routes for a given network.
    * show ip protocols: Includes information about BGP routing protocol.
39. **How does NAT help in saving IP Addresses?** NAT (Network Address Translation) helps in saving IP addresses by allowing multiple devices within a private network to share a single or a few public IP addresses when accessing the internet.
    * **Many-to-One Mapping:** Typically, an entire private network can communicate with the outside world using just one or a small pool of public IP addresses. This means that instead of each internal device requiring its own unique public IP address, they all use a translated public IP.
    * **Private Address Space:** NAT leverages the use of private IP address ranges (e.g., 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), which are not routable on the internet. Devices within a private network use these addresses, and the NAT router translates them to public, globally routable addresses only when communication is initiated to the internet.
    * **Conservation:** This significantly conserves the limited IPv4 public address space, as organizations only need to acquire a few public IP addresses from their ISP, rather than one for every device.
40. **Describe the process of DHCP (Dynamic Host Configuration Protocol):** DHCP (Dynamic Host Configuration Protocol) is a network protocol that enables a server to automatically assign IP addresses and other communication parameters (like subnet mask, default gateway, DNS servers) to devices connected to a network. The process typically involves four main steps, often remembered as DORA (Discover, Offer, Request, Acknowledge):
    * **DHCP Discover:** When a client device (e.g., a PC) boots up or connects to a network, it broadcasts a DHCP Discover message (to destination IP 255.255.255.255 and MAC address FF:FF:FF:FF:FF:FF) to find any available DHCP servers.
    * **DHCP Offer:** Any DHCP server that receives the Discover message and has an available IP address broadcasts a DHCP Offer message. This message includes a proposed IP address for the client, subnet mask, default gateway, DNS server addresses, and the lease duration.
    * **DHCP Request:** The client receives one or more DHCP Offer messages. It selects one offer (usually the first one it receives) and broadcasts a DHCP Request message to formally accept the offered IP address and parameters. This broadcast ensures that other DHCP servers know their offers were not accepted.
    * **DHCP Acknowledge (ACK):** The selected DHCP server receives the Request message and sends a DHCP ACK (Acknowledgment) message to the client. This message confirms the IP address lease and all configuration parameters. The client then configures its network interface with the received information and can begin communicating on the network.
41. **Compare TCP and UDP in terms of reliability and use cases:** (Already covered in question 7).
42. **What is the configuration neighbor statement in EIGRP?** The neighbor statement in EIGRP is used for configuring static EIGRP neighbors. Unlike OSPF or BGP, EIGRP typically uses multicast Hellos (224.0.0.10) for neighbor discovery, so explicitly configuring neighbors is usually not required in broadcast multi-access environments. However, the neighbor command is essential in non-broadcast multi-access (NBMA) networks (like Frame Relay, ATM, or sometimes VPNs) where multicast is not supported or desired.
    * **Syntax:**
    * neighbor [ip-address] [interface-type interface-number]
      + ip-address: The IP address of the EIGRP neighbor.
      + interface-type interface-number: The local interface through which the neighbor is reachable.
    * **Usage:** When you configure a neighbor statement, the router will send unicast EIGRP Hellos to that specific IP address, rather than relying on multicast discovery. This forces a neighbor relationship with the specified router.
43. **What does the word "serno" mean at the end of EIGRP topology by typing "show ip eigrp topology" command?** When you see "Serno" (or "sequence number") at the end of an EIGRP topology entry (e.g., show ip eigrp topology), it refers to the **sequence number of the update packet** that carried the information for that specific route. EIGRP uses sequence numbers for reliable transport (RTP) of update packets. Every EIGRP update sent has a sequence number. When a router receives an update, it acknowledges it with the corresponding sequence number. The "Serno" in the topology table indicates the sequence number of the update from the successor (or feasible successor) that advertised that particular route. It's a troubleshooting aid to track the freshness and origin of routing information.
44. **What is VPN IPSEC Tunnel?** A **VPN (Virtual Private Network) IPSec Tunnel** is a secure, encrypted connection (a "tunnel") established over an insecure network (like the internet) to provide private communication between two or more endpoints. IPSec (Internet Protocol Security) is a suite of protocols that provides security for IP communications by authenticating and encrypting each IP packet.
    * **VPN:** Creates a logical "private" network over a public infrastructure, allowing remote users or branch offices to securely access a central network as if they were directly connected.
    * **IPSec:** Provides the cryptographic services (encryption, authentication, integrity) that secure the VPN tunnel. It operates at the network layer (Layer 3) and can encrypt the entire IP packet (tunnel mode) or just the payload (transport mode).
    * **Tunnel:** Refers to the encapsulation of original IP packets within new IP packets, which are then encrypted and sent across the public network. At the other end, the outer headers are removed, the packet is decrypted, and the original packet is delivered.
45. **Given the image for configuring VPN IPSEC (Page 5), fill in the blanks:**

**A-On router PP1**

crypto isakmp policy 1

encr aes 256

authentication pre-share

group 2

!

crypto isakmp key [YOUR\_PRESHARED\_KEY] address [TK1\_Public\_IP\_Address] // Pre-shared key for TK1

!

crypto isakmp identity [local-id | hostname] // Often omitted if using pre-shared key by IP

!

crypto ipsec transform-set TS\_PP1\_TK1 esp-aes 256 esp-sha-hmac // Define transform set

!

crypto map CMAP\_PP1 1 ipsec-isakmp

set peer [TK1\_Public\_IP\_Address]

set transform-set TS\_PP1\_TK1

match address 101 // Assuming access-list 101 defines interesting traffic

!

interface [Interface\_Facing\_ISP] // e.g., GigabitEthernet0/1

crypto map CMAP\_PP1

!

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255 // Interesting traffic

**B-On router TK1**

crypto isakmp policy 1

encr aes 256

authentication pre-share

group 2

!

crypto isakmp key [YOUR\_PRESHARED\_KEY] address [PP1\_Public\_IP\_Address] // Pre-shared key for PP1

!

crypto isakmp identity [local-id | hostname] // Often omitted if using pre-shared key by IP

!

crypto ipsec transform-set TS\_TK1\_PP1 esp-aes 256 esp-sha-hmac // Define transform set

!

crypto map CMAP\_TK1 1 ipsec-isakmp

set peer [PP1\_Public\_IP\_Address]

set transform-set TS\_TK1\_PP1

match address 101 // Assuming access-list 101 defines interesting traffic

!

interface [Interface\_Facing\_ISP] // e.g., GigabitEthernet0/1

crypto map CMAP\_TK1

!

access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255 // Interesting traffic (reverse of PP1)

*Note: Replace [YOUR\_PRESHARED\_KEY], [TK1\_Public\_IP\_Address], [PP1\_Public\_IP\_Address], and [Interface\_Facing\_ISP] with your actual values.*

1. **How do multiple IPSec VPN destinations connect to Cisco?** Multiple IPSec VPN tunnels to different destinations on Cisco routers can be configured in several ways:
   * **Multiple Crypto Maps:** For site-to-site VPNs, you can configure multiple crypto map entries (with different sequence numbers) under a single crypto map set. Each entry can point to a different peer and define different interesting traffic for that tunnel.
   * crypto map MY\_MAP 10 ipsec-isakmp
   * set peer [Peer\_IP\_1]
   * match address 101
   * crypto map MY\_MAP 20 ipsec-isakmp
   * set peer [Peer\_IP\_2]
   * match address 102
   * interface [ISP\_Facing\_Interface]
   * crypto map MY\_MAP
   * **DMVPN (Dynamic Multipoint VPN):** For spoke-to-spoke and spoke-to-hub VPNs, DMVPN uses NHRP (Next Hop Resolution Protocol) and mGRE (multipoint GRE) tunnels to establish dynamic VPN tunnels on demand, significantly simplifying configurations for many-to-many scenarios.
   * **FlexVPN:** A more modern and flexible VPN solution that can integrate various VPN technologies, including IKEv2, and simplifies complex VPN deployments.
   * **VTI (Virtual Tunnel Interface):** VTI-based VPNs provide a routable interface for the tunnel, allowing routing protocols to run over the VPN. This simplifies routing over VPNs compared to crypto maps.
2. **Describe the types of VPN Tunnels on Cisco Routers:** Cisco routers support various types of VPN tunnels, broadly categorized by their underlying technology and purpose:
   * **IPSec VPNs:** The most common type for secure site-to-site and remote access VPNs. They use IPSec for encryption and authentication.
     + **Site-to-Site IPSec VPN:** Connects two or more fixed locations (e.g., branch office to headquarters) over the internet.
     + **Remote Access IPSec VPN:** Allows individual users (e.g., teleworkers) to securely connect to the corporate network from remote locations.
   * **SSL VPNs (WebVPN/AnyConnect):** Provide secure remote access using SSL/TLS, typically for web-based applications or full network access via a client. They are clientless or use a lightweight client.
   * **GRE (Generic Routing Encapsulation) Tunnels:** Provide a way to encapsulate a wide variety of network layer protocols inside IP tunnels. GRE itself does not provide encryption but is often combined with IPSec (GRE over IPSec) for secure transport.
   * **DMVPN (Dynamic Multipoint VPN):** Combines mGRE, IPSec, and NHRP to create a scalable and dynamic VPN solution for hub-and-spoke and spoke-to-spoke connectivity.
   * **VTI (Virtual Tunnel Interface) Based VPNs:** Use virtual interfaces as tunnel endpoints, allowing routing protocols to operate directly over the VPN tunnel, simplifying routing and management.
   * **FlexVPN:** A unified framework that supports various VPN deployments, including IKEv2 and mGRE, offering flexibility and scalability.
3. **Types of Addresses in NAT (Inside Local, Inside Global, Outside Global, and Outside Local):** NAT uses four types of addresses to facilitate translation:
   * **Inside Local Address:** The IP address of a device on the inside network (your private network) as seen from other devices on the inside network. These are typically private IP addresses (e.g., 192.168.1.10).
   * **Inside Global Address:** The IP address of a device on the inside network as seen from the outside network (the internet). This is a public, globally routable IP address assigned by the NAT device.
   * **Outside Local Address:** The IP address of a device on the outside network (e.g., a web server on the internet) as seen from the inside network. This is often the actual public IP address of the outside device, but it could also be a translated address if the outside network is also using NAT.
   * **Outside Global Address:** The IP address of a device on the outside network as seen from the outside network. This is the globally routable IP address of the outside device. For devices on the internet, the outside local and outside global addresses are usually the same.
4. **Exercise: Configure routing on Router1, Router2, and Router3 for NET 1, NET 2, NET 3, NET 4 so that all computers can communicate:**

This requires configuring routing protocols and/or static routes to ensure all networks (NET 1, NET 2, NET 3, NET 4) can reach each other. Here are configurations for each routing method requested:

**Assumptions:**

* + Interfaces are configured as per the diagram on page 6.
  + Loopback interfaces (if used for router IDs) are configured (not shown in example but good practice).

**1. Static Routing Configuration:**

**Router1:**

interface GigabitEthernet0/0

ip address 192.168.210.254 255.255.255.0

no shutdown

interface Serial0/0/0

ip address 111.111.110.254 255.255.255.252

no shutdown

!

ip route 112.112.113.0 255.255.255.252 111.111.110.253 // Route to NET 3 via Router2

ip route 192.168.213.0 255.255.255.0 111.111.110.253 // Route to NET 4 via Router2

**Router2:**

interface Serial0/0/0

ip address 111.111.110.253 255.255.255.252

no shutdown

interface Serial0/0/1

ip address 112.112.113.254 255.255.255.252

no shutdown

!

ip route 192.168.210.0 255.255.255.0 111.111.110.254 // Route to NET 1 via Router1

ip route 192.168.213.0 255.255.255.0 112.112.113.253 // Route to NET 4 via Router3

**Router3:**

interface GigabitEthernet0/0

ip address 192.168.213.254 255.255.255.0

no shutdown

interface Serial0/0/0

ip address 112.112.113.253 255.255.255.252

no shutdown

!

ip route 111.111.110.0 255.255.255.252 112.112.113.254 // Route to NET 2 via Router2

ip route 192.168.210.0 255.255.255.0 112.112.113.254 // Route to NET 1 via Router2

**2. Default Routing Configuration:** *Note: Default routing is typically used on edge routers (e.g., Router1 and Router3) to point towards a central router (Router2) or the internet.*

**Router1:**

ip route 0.0.0.0 0.0.0.0 111.111.110.253 // Default route to Router2

**Router2:**

// No default route needed here, as it's the central point.

// It should have static routes or dynamic routing to other networks.

// If it's the gateway to the internet, then a default route to ISP.

**Router3:**

ip route 0.0.0.0 0.0.0.0 112.112.113.254 // Default route to Router2

**3. EIGRP Routing Configuration:**

**Router1:**

router eigrp 100

network 192.168.210.0 0.0.0.255 // NET 1

network 111.111.110.0 0.0.0.3 // NET 2

no auto-summary

**Router2:**

router eigrp 100

network 111.111.110.0 0.0.0.3 // NET 2

network 112.112.113.0 0.0.0.3 // NET 3

no auto-summary

**Router3:**

router eigrp 100

network 192.168.213.0 0.0.0.255 // NET 4

network 112.112.113.0 0.0.0.3 // NET 3

no auto-summary

**4. OSPF Routing Configuration:**

**Router1:**

router ospf 1

network 192.168.210.0 0.0.0.255 area 0 // NET 1

network 111.111.110.0 0.0.0.3 area 0 // NET 2

**Router2:**

router ospf 1

network 111.111.110.0 0.0.0.3 area 0 // NET 2

network 112.112.113.0 0.0.0.3 area 0 // NET 3

**Router3:**

router ospf 1

network 192.168.213.0 0.0.0.255 area 0 // NET 4

network 112.112.113.0 0.0.0.3 area 0 // NET 3

*Note: For simplicity, all routers are placed in Area 0 (backbone). In a larger design, you might use different areas.*

**5. BGP Routing Configuration:** *Note: BGP is typically used between Autonomous Systems. For this small setup, it's generally overkill, but here's a conceptual configuration. You'd need to define AS numbers.*

**Router1 (AS 65001):**

router bgp 65001

neighbor 111.111.110.253 remote-as 65002 // Peer with Router2

network 192.168.210.0 mask 255.255.255.0

network 111.111.110.0 mask 255.255.255.252

**Router2 (AS 65002):**

router bgp 65002

neighbor 111.111.110.254 remote-as 65001 // Peer with Router1

neighbor 112.112.113.253 remote-as 65003 // Peer with Router3

network 111.111.110.0 mask 255.255.255.252

network 112.112.113.0 mask 255.255.255.252

**Router3 (AS 65003):**

router bgp 65003

neighbor 112.112.113.254 remote-as 65002 // Peer with Router2

network 192.168.213.0 mask 255.255.255.0

network 112.112.113.0 mask 255.255.255.252

**6. RIP v2 Routing Configuration:**

**Router1:**

router rip

version 2

network 192.168.210.0

network 111.111.110.0

no auto-summary

**Router2:**

router rip

version 2

network 111.111.110.0

network 112.112.113.0

no auto-summary

**Router3:**

router rip

version 2

network 192.168.213.0

network 112.112.113.0

no auto-summary