WLAN:

WLAN stands for Wireless Local Area Network. It is a type of computer network that allows devices to communicate wirelessly within a limited geographic area, such as a home, office, or public space. WLANs use radio frequency (RF) technology to transmit data between devices, eliminating the need for physical wired connections.

Components of WLAN:

1. **Access Points (APs):**

    - Access points are wireless networking devices that serve as central hubs for connecting wireless devices to the WLAN.
    - APs transmit and receive wireless signals, providing coverage within a specific area known as a cell or coverage area.
    - Multiple APs can be deployed to extend WLAN coverage over a larger area.

2. **Wireless Clients:**

    - Wireless clients are devices such as laptops, smartphones, tablets, and IoT devices that connect to the WLAN to access network resources and services.
    - Clients communicate with APs using wireless network interface cards (NICs) or built-in wireless capabilities.

3. **Wireless Router:**

    - In home or small office environments, a wireless router integrates the functions of a traditional wired router with wireless access point capabilities.
    - Wireless routers provide connectivity to the Internet and enable wireless devices to communicate with each other and access network resources.

Standards:

Frequency band | Technology | Speed | 2.4 GHz IEEE | 802.11 b | 11 Mbps | IEEE | 802.11 g | 54 Mbps | 5.0 GHz | 802.11 n | 150-300 Mbps |

Key Features of WLAN:

1. **Flexibility and Mobility:**

    - WLANs offer flexibility and mobility by enabling devices to connect to the network without being physically tethered to a wired infrastructure.
    - Users can move freely within the coverage area of the WLAN while maintaining network connectivity.

2. **Scalability:**

    - WLANs can be easily scaled to accommodate additional devices and users by adding more access points or upgrading existing infrastructure.

  - Scalability enables WLANs to support growing numbers of wireless devices and expanding network requirements.

3. **Ease of Deployment:**

   - WLANs are relatively easy to deploy compared to wired networks since they eliminate the need for installing physical cables and infrastructure.
   - Wireless access points can be strategically placed to provide optimal coverage and connectivity within the desired area.

4. **Cost Savings:**

   - WLANs can offer cost savings compared to wired networks by reducing the need for expensive cabling and infrastructure.
   - Wireless connectivity also simplifies network management and maintenance tasks.

5. **Convenience:**

   - WLANs provide convenient access to network resources and services without the limitations of physical connections.
   - Users can connect to the WLAN from anywhere within the coverage area, enhancing productivity and collaboration.

WEP

WEP (Wired Equivalent Privacy) is an encryption protocol used to secure wireless networks, particularly older Wi-Fi networks that adhere to the IEEE 802.11b and 802.11g standards. WEP was one of the earliest encryption methods used for wireless networks, but it is now considered to be highly vulnerable to security attacks due to its weak encryption algorithm.

Key Features of WEP:

1. **Encryption Algorithm:**

   - WEP uses the RC4 encryption algorithm to encrypt data transmitted over the wireless network.
   - RC4 is a stream cipher that generates a pseudo-random keystream to encrypt plaintext data.

2. **Shared Key Authentication:**

   - WEP supports shared key authentication, where a pre-shared key (password) is used to authenticate clients attempting to connect to the wireless network.
   - The shared key is used to generate an initialization vector (IV) for encrypting and decrypting data.

3. **Key Lengths:**

   - WEP supports two key lengths: 64-bit and 128-bit.
   - The 64-bit key consists of 40 bits for the key itself and 24 additional bits for the initialization vector (IV).
   - The 128-bit key consists of 104 bits for the key and 24 bits for the IV.

4. **Initialization Vector (IV):**

- WEP uses a 24-bit IV as part of the encryption process.
- The IV is concatenated with the shared key to create the encryption key used to encrypt data packets.
- Due to the limited size of the IV, it can lead to IV reuse and cryptographic vulnerabilities.

Vulnerabilities and Security Issues:

1. **Weak Encryption:**

   - WEP's use of the RC4 encryption algorithm with a limited key length makes it susceptible to brute-force attacks and cryptographic vulnerabilities.
   - Attackers can exploit weaknesses in the RC4 algorithm and recover the WEP key with relatively little effort.

2. **IV Reuse:**

   - WEP's use of a 24-bit IV results in a limited number of possible IVs, leading to IV reuse within the network.
   - IV reuse makes it easier for attackers to perform statistical analysis and launch attacks to recover the WEP key.

3. **Key Management:**

   - WEP lacks robust key management mechanisms, making it challenging to securely distribute and rotate encryption keys.
   - The reliance on pre-shared keys increases the risk of key compromise and unauthorized access to the network.

WPA 1

WPA1 (Wi-Fi Protected Access version 1) is a security protocol designed to address the weaknesses of the earlier WEP (Wired Equivalent Privacy) protocol in securing wireless networks. Introduced as an interim solution before the adoption of WPA2, WPA1 provided significant improvements in security over WEP and helped bridge the transition to stronger encryption standards.

1. **TKIP Encryption:**

   - WPA1 employs Temporal Key Integrity Protocol (TKIP) for encryption, replacing the vulnerable RC4 algorithm used in WEP.
   - TKIP dynamically generates encryption keys for each data packet, addressing the weaknesses of static keys in WEP.

2. **Message Integrity Check (MIC):**

   - WPA1 includes a Message Integrity Check (MIC) mechanism known as Michael (MICHAEL, Michael Integrity Check Algorithm) to detect and prevent tampering with data packets.
   - MIC helps mitigate attacks such as forgery and replay attacks that exploit weaknesses in WEP.

3. **Dynamic Key Management:**

   - WPA1 introduces dynamic key management through the use of the 4-way handshake protocol.

- During the authentication process, WPA1 negotiates session keys between the client device and the access point, providing stronger protection against key reuse attacks.

4. **Authentication Enhancements:**

   - WPA1 supports stronger authentication mechanisms, including Extensible Authentication Protocol (EAP) methods such as EAP-TLS, EAP-TTLS, and PEAP.
   - These methods enhance user authentication and facilitate integration with enterprise authentication systems such as RADIUS servers.

Security Improvements over WEP:

1. **Stronger Encryption:**

   - The use of TKIP encryption in WPA1 provides stronger protection against cryptographic attacks compared to the vulnerable RC4 algorithm used in WEP.

2. **Message Integrity:**

   - The inclusion of MIC in WPA1 helps detect and prevent attacks that tamper with data packets, enhancing the integrity of wireless communications.

3. **Dynamic Key Management:**

   - WPA1's dynamic key management mechanism addresses the key reuse vulnerabilities present in WEP, providing more robust protection against key-based attacks.

> It is 32 bits encryption method 2^32 diffrent method. after every 10 min encryption method changes.

WPA 2

WPA2 (Wi-Fi Protected Access version 2) is a security protocol widely used to secure wireless networks, providing stronger encryption and security features compared to its predecessor, WPA1, and the vulnerable WEP (Wired Equivalent Privacy) protocol. WPA2 is the current standard for securing Wi-Fi networks and is designed to address the weaknesses and vulnerabilities present in earlier protocols.

Key Features of WPA2:

1. **AES Encryption:**

   - WPA2 uses the Advanced Encryption Standard (AES) encryption algorithm with CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for data encryption.
   - AES is a robust encryption algorithm that provides strong security and protection against cryptographic attacks.

2. **Robust Security Enhancements:**

   - WPA2 incorporates security enhancements such as stronger encryption, message integrity checks, and improved key management compared to WPA1.
   - These enhancements enhance the overall security posture of Wi-Fi networks and help mitigate potential security risks.

3. **Authentication Methods:**

    - WPA2 supports various authentication methods, including pre-shared key (PSK) mode and enterprise mode with Extensible Authentication Protocol (EAP) methods such as EAP-TLS, EAP-TTLS, and PEAP.
    - Enterprise mode facilitates integration with centralized authentication servers such as RADIUS (Remote Authentication Dial-In User Service), enhancing user authentication and network security.

4. **Backward Compatibility:**

    - WPA2 maintains backward compatibility with legacy Wi-Fi devices that support earlier security standards such as WPA1 and WEP.
    - This allows for a gradual transition to WPA2 without the immediate need to replace all existing hardware.

Security Improvements over WPA1:

1. **Stronger Encryption:**

    - WPA2 uses the AES encryption algorithm, which is significantly stronger and more secure than the TKIP encryption used in WPA1.
    - AES encryption provides robust protection against cryptographic attacks and ensures the confidentiality and integrity of wireless communications.

2. **Advanced Authentication Mechanisms:**

    - WPA2 supports advanced authentication mechanisms, including 802.1X/EAP authentication, which enables secure authentication and access control for wireless clients.
    - These mechanisms enhance user authentication and prevent unauthorized access to Wi-Fi networks.

3. **Message Integrity Protection:**

    - WPA2 incorporates message integrity checks (MIC) to detect and prevent tampering with data packets, ensuring the integrity of wireless communications.
    - MIC helps mitigate attacks such as forgery and replay attacks that exploit vulnerabilities in earlier security protocols.

> 3 DES encryption used. AES (Advanced Encryption System) It is 128 bits encryption method.

SD-WAN:

SD-WAN (Software-Defined Wide Area Network) is a technology that simplifies the management and operation of a wide area network (WAN) by leveraging software-defined networking (SDN) principles. SD-WAN offers centralized control, automation, and dynamic traffic management capabilities, enabling organizations to optimize network performance, reduce costs, and enhance security.

Key Features of SD-WAN:

1. **Centralized Management:**

- SD-WAN provides centralized management and orchestration of network policies, configurations, and traffic flows.
- Administrators can define network policies, prioritize applications, and enforce security measures from a centralized management interface.

2. **Dynamic Path Selection:**

   - It can utilize multiple transport technologies, including broadband internet, MPLS (Multiprotocol Label Switching), LTE, and others, to ensure efficient data delivery.

3. **Application-Based Routing:**

   - SD-WAN allows organizations to prioritize and route traffic based on application type, performance requirements, and business priorities.
   - Critical applications can be prioritized and routed over the most suitable network path to meet performance objectives and ensure a consistent user experience.

4. **Dynamic Bandwidth Allocation:**

   - SD-WAN dynamically allocates bandwidth resources to different applications and users based on demand, congestion levels, and QoS policies.
   - It can adjust bandwidth allocations in real time to optimize application performance and accommodate fluctuations in network traffic.

5. **Security Integration:**

   - SD-WAN integrates security features such as encryption, firewall, intrusion prevention, and threat detection capabilities into the network infrastructure.
   - It ensures end-to-end security for data transmissions over the WAN, protecting against cyber threats and unauthorized access.

Benefits of SD-WAN:

1. **Improved Performance:**

   - SD-WAN optimizes application performance by dynamically routing traffic over the most efficient path, reducing latency, and minimizing packet loss.

2. **Cost Savings:**

   - By utilizing cost-effective transport options such as broadband internet and prioritizing traffic based on business requirements, SD-WAN helps organizations reduce WAN connectivity costs.

3. **Enhanced Agility:**

   - SD-WAN's centralized management and automation capabilities enable rapid deployment, configuration changes, and network scaling to adapt to evolving business needs.

4. **Enhanced Security:**

   - SD-WAN integrates advanced security features and enforces consistent security policies across the entire network, enhancing protection against cyber threats and ensuring compliance with regulatory requirements.

5. **Business Continuity:**
   - SD-WAN provides resilience and failover capabilities to maintain network connectivity in the event of link failures, outages, or network congestion, ensuring business continuity and uninterrupted operations.

IBSS

IBSS stands for Independent Basic Service Set, also known as ad-hoc mode, in wireless networking. In an IBSS network, wireless devices communicate directly with each other without the need for a central access point (AP).

Key Features of IBSS:

1. **Decentralized Network:**
   - In an IBSS network, devices communicate with each other directly, forming a decentralized network without the need for a central access point.
   - Each device in the IBSS network functions as both a client and an access point, enabling peer-to-peer communication.
2. **Ad-Hoc Mode:**
   - IBSS operates in ad-hoc mode, where wireless devices dynamically form temporary connections with each other as needed.
   - Devices within range can discover and join the IBSS network without requiring any infrastructure or prior configuration.
3. **Flexibility and Mobility:**
   - IBSS networks are highly flexible and suitable for scenarios where infrastructure-based networks are impractical or unavailable.
   - They enable mobile devices to establish wireless connections on the go, allowing for spontaneous collaboration and communication.
4. **Short-Range Communication:**
   - IBSS networks typically have a limited range, as the communication range is determined by the transmission power of individual devices.
   - Devices must be within close proximity to establish and maintain connections within the IBSS network.
5. **Peer-to-Peer Communication:**
   - In an IBSS network, devices communicate with each other directly, enabling peer-to-peer data transmission without relying on a central server or network infrastructure.
   - This allows for efficient data exchange between devices without the need for intermediate routing.

Use Cases of IBSS:

1. **Ad-Hoc Networking:**
   - IBSS networks are commonly used for ad-hoc networking scenarios where devices need to communicate with each other spontaneously, such as in peer-to-peer file sharing, gaming, or collaboration environments.
2. **Wireless Mesh Networks:**
   - IBSS networks can be used as building blocks for wireless mesh networks, where devices form dynamic connections with neighboring nodes to extend network coverage and provide connectivity in areas with limited infrastructure.
3. **Temporary Networks:**
   - IBSS networks are ideal for creating temporary networks in environments where deploying infrastructure-based networks is impractical or cost-prohibitive, such as outdoor events, disaster recovery scenarios, or emergency response situations.
4. **Research and Testing:**
   - IBSS networks are often used in research and testing environments to evaluate wireless networking protocols, algorithms, and performance characteristics in real-world scenarios.

Considerations for IBSS Networks:

1. **Security:**
   - Since IBSS networks lack centralized authentication and encryption mechanisms, security measures such as WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) or WPA3-SAE (Wi-Fi Protected Access 3 - Simultaneous Authentication of Equals) should be implemented to secure communications between devices.
2. **Interference:**
   - Due to the absence of a central access point, IBSS networks may be more susceptible to interference from other wireless devices and environmental factors.
   - Care should be taken to select appropriate channels and optimize device placement to minimize interference and maximize signal quality.
3. **Scalability:**
   - IBSS networks may have limited scalability compared to infrastructure-based networks, as the number of devices that can communicate simultaneously within the network may be constrained by factors such as bandwidth and radio frequency spectrum availability.

BSS:

BSS stands for Basic Service Set in the context of wireless networking, particularly in IEEE 802.11 (Wi-Fi) networks. It represents the most fundamental building block of a wireless network and consists of wireless devices that communicate directly with each other within a limited coverage area.

Basic Service Set (BSS):

1. **Definition:**

   - A Basic Service Set (BSS) is a group of wireless devices that communicate with each other directly in a wireless network.
   - It typically consists of one Access Point (AP) and one or more associated client devices, forming a small-scale network within a limited geographic area.

2. **Components:**

   - **Access Point (AP):** The AP is a central device in the BSS that manages wireless communications, facilitates data transmission, and provides network access to connected devices.
   - **Client Devices (STAs):** Client devices, also known as stations (STAs), are devices such as laptops, smartphones, tablets, and other Wi-Fi-enabled devices that connect to the BSS to access network resources and services.

3. **Coverage Area:**

   - The coverage area of a BSS is limited by factors such as signal strength, transmission power, and environmental conditions.
   - Devices within the BSS can communicate with each other directly, but their range may be restricted to a certain distance from the AP or within the boundaries of the wireless coverage area.

4. **Operating Modes:**

   - BSS can operate in different modes, including infrastructure mode and ad-hoc mode.
   - In infrastructure mode, the BSS includes an AP that facilitates communication between client devices and connects the wireless network to a wired Ethernet network.
   - In ad-hoc mode (also known as Independent BSS or IBSS), devices communicate with each other directly without the need for a central AP, forming a decentralized and self-organizing network.

ESS

The Extended Service Set (ESS) is a concept in wireless networking defined by the IEEE 802.11 standard, commonly known as Wi-Fi. It represents a collection of Basic Service Sets (BSSs) interconnected by a distribution system, typically a wired network infrastructure.

Extended Service Set (ESS):

1. **Definition:**

   - An Extended Service Set (ESS) is a set of interconnected Basic Service Sets (BSSs) that collectively form a single logical wireless network.
   - It allows wireless devices to roam seamlessly between different BSSs while maintaining continuous network connectivity.

2. **Components:**

   - **Basic Service Sets (BSSs):** Each BSS within the ESS consists of an Access Point (AP) and associated client devices (STAs).

- **Distribution System (DS):** The distribution system serves as the backbone network that interconnects multiple BSSs within the ESS. It is typically a wired network infrastructure, such as Ethernet or fiber optic cables.

3. **Roaming:**

   - Clients within the ESS can roam between different BSSs without losing network connectivity.
   - As a client moves out of the coverage area of one BSS and into the coverage area of another BSS within the same ESS, it can seamlessly associate with the new AP and continue communication without interruption.

4. **SSID:**

   - All BSSs within the ESS share the same Service Set Identifier (SSID), which is the name of the wireless network.
   - Clients use the SSID to identify and associate with any BSS within the ESS, regardless of their physical location within the coverage area.

5. **Mobility Management:**

   - Mobility management protocols, such as the IEEE 802.11r Fast BSS Transition (FT) protocol, enhance the roaming experience within an ESS by reducing handover latency and improving security during transitions between BSSs.

Benefits of Extended Service Set (ESS):

1. **Seamless Roaming:**

   - ESS enables seamless roaming for wireless clients, allowing them to move between different BSSs within the same logical network without experiencing interruptions in network connectivity.

2. **Scalability:**

   - ESS provides scalability for wireless networks by allowing the deployment of multiple BSSs to cover larger geographic areas or accommodate a larger number of clients.

3. **Load Balancing:**

   - Distributing clients across multiple BSSs within the ESS can help balance network load and improve overall network performance.

4. **Redundancy and Reliability:**

   - Redundant BSS deployments within the ESS can provide failover and redundancy, ensuring continuous network connectivity even in the event of AP failures or network outages.

WLC

WLC stands for Wireless LAN Controller. It is a network device used in Wi-Fi deployments to centralize the management and control of wireless access points (APs) within a wireless network.

Key Functions of WLC:

1. **Centralized Management:**

   - WLCs provide centralized management and configuration of multiple wireless APs deployed within a network.
   - Administrators can use a single interface to configure, monitor, and troubleshoot APs, simplifying network management and operations.

2. **Radio Resource Management (RRM):**

   - WLCs perform Radio Resource Management functions to optimize wireless network performance and mitigate interference.
   - RRM features include automatic channel selection, transmit power control, and interference detection to ensure optimal radio frequency (RF) conditions.

3. **Wireless Client Management:**

   - WLCs manage wireless client devices' association, authentication, and roaming within the wireless network.
   - They enforce security policies, perform client authentication, and facilitate seamless roaming between APs to maintain connectivity for mobile devices.

4. **Security and Access Control:**

   - WLCs enforce security policies and access control mechanisms to secure the wireless network.
   - They support authentication protocols such as WPA2-Enterprise, 802.1X, and captive portal authentication, along with encryption standards to protect data transmission over the wireless network.

5. **Quality of Service (QoS) Enforcement:**

   - WLCs prioritize and manage traffic based on QoS policies to ensure optimal performance for critical applications.
   - They classify and prioritize traffic based on application type, user profile, or service level agreements (SLAs), and apply QoS policies to prioritize bandwidth allocation accordingly.

6. **Mobility and Roaming Support:**

   - WLCs facilitate seamless mobility and roaming for wireless clients moving between different areas or APs within the wireless network.
   - They coordinate handoffs and maintain session continuity for roaming clients, ensuring uninterrupted connectivity as devices move throughout the coverage area.

7. **Scalability and High Availability:**

   - WLCs support scalability and high availability features to accommodate growing network deployments and ensure continuous operation.
   - They can be deployed in redundant configurations with failover capabilities to minimize downtime and maximize network reliability.

8. **Monitoring and Reporting:**

  - WLCs provide monitoring and reporting features to track wireless network performance, analyze traffic patterns, and generate reports on network usage and health.
  - Administrators can use monitoring tools to troubleshoot issues, optimize network performance, and plan for future capacity requirements.

Deployment Considerations:

1. **Placement and Coverage:**

   - Deploy WLCs strategically to ensure adequate coverage and signal strength throughout the wireless network.
   - Consider factors such as building layout, RF interference, and client density when positioning WLCs and APs.

2. **Redundancy and Resilience:**

   - Implement redundant WLC configurations and high availability features to minimize single points of failure and ensure continuous network operation.
   - Use features such as AP redundancy and seamless roaming to maintain connectivity during WLC failover events.

3. **Integration with Existing Infrastructure:**

   - Integrate WLCs seamlessly with existing network infrastructure, security systems, and management tools to streamline operations and maximize efficiency.
   - Ensure compatibility with network protocols, authentication methods, and security policies to maintain a cohesive network environment.

4. **Security and Compliance:**

   - Implement robust security measures on WLCs to protect against unauthorized access, data breaches, and cyber threats.
   - Enforce encryption standards, access control policies, and security best practices to maintain compliance with regulatory requirements and industry standards.

5. **Capacity Planning:**

   - Perform capacity planning to determine the number of WLCs and APs needed to support current and future network requirements.
   - Consider factors such as client density, application usage, and expected growth to design a scalable and efficient wireless network architecture.

GRE tunnel:

A GRE (Generic Routing Encapsulation) tunnel is a type of tunneling protocol used to encapsulate and transmit data packets between two networks across an intermediate network, such as the Internet. GRE tunnels create a virtual point-to-point connection between two endpoints, allowing for the secure transmission of packets over an untrusted or public network.

Purpose of GRE Tunnels:

1. **Connectivity Between Remote Networks:**

   - GRE tunnels enable the creation of virtual private networks (VPNs) or secure connections between geographically dispersed networks.
   - They facilitate communication between remote networks as if they were directly connected, providing a secure and encrypted data path.

2. **Overlay Networks:**

   - GRE tunnels are often used to create overlay networks by encapsulating packets from one network within GRE headers and transmitting them over another network.
   - This allows for the creation of logical connections between disparate networks, regardless of the underlying physical infrastructure.

3. **Protocol Compatibility:**

   - GRE tunnels support encapsulation of various network layer protocols, including IPv4, IPv6, and non-IP protocols such as IPX and AppleTalk.
   - They provide a flexible and protocol-agnostic mechanism for transmitting data between networks that use different protocols.

How GRE Tunnels Work:

1. **Encapsulation:**

   - In a GRE tunnel, each data packet from the source network is encapsulated within a GRE header before transmission.
   - The GRE header includes information such as the source and destination IP addresses, protocol type, and other control fields.

2. **Transmission:**

   - Once encapsulated, the GRE-encapsulated packets are transmitted across the intermediate network (e.g., the Internet) to the remote endpoint of the GRE tunnel.
   - The intermediate network treats the GRE-encapsulated packets as regular IP packets and forwards them based on their destination IP address.

3. **Decapsulation:**

   - Upon reaching the remote endpoint of the GRE tunnel, the GRE header is removed (decapsulated), and the original data packet is extracted.
   - The decapsulated packet is then forwarded to its destination network based on the information contained in the original packet headers.

4. **Routing and Forwarding:**

   - Routing protocols or static routes are typically used to determine the path of GRE-encapsulated packets between the source and destination networks.
   - Intermediate routers along the path forward GRE-encapsulated packets based on the destination IP address contained within the GRE headers.

Benefits of GRE Tunnels:

1. **Secure Communication:**
   - GRE tunnels provide a secure and encrypted communication channel between networks, protecting data from eavesdropping and tampering.
2. **Network Extension:**
   - GRE tunnels extend the reach of a network across untrusted or public networks, enabling connectivity between geographically dispersed networks.
3. **Protocol Agnostic:**
   - GRE tunnels support encapsulation of various network layer protocols, making them suitable for connecting networks that use different protocols.
4. **Flexibility:**
   - GRE tunnels are highly flexible and can be easily deployed and configured to meet specific networking requirements.

Use Cases:

1. **Site-to-Site VPNs:**
   - GRE tunnels are commonly used to establish secure site-to-site VPN connections between branch offices, data centers, or remote locations.
2. **Overlay Networks:**
   - GRE tunnels facilitate the creation of overlay networks for cloud connectivity, data replication, and disaster recovery.
3. **Mobile and IoT Connectivity:**
   - GRE tunnels can be used to securely connect mobile devices, IoT devices, and remote sensors to centralized networks or cloud services.

configuratin:

```
A(config)# int tunnel 0
A(config-if)# no shutdown
A(config-if)# ip route 172.16.20.1 255.255.255.0
A(config-if)# tunnel source 202.208.220.1
A(config-if)# tunnel destination 110.1.1.1

A(config)# ip route 172.16.30.0 255.255.255.0 172.16.20.2
```

```
B(config)# int tunnel 0
B(config-if)# no shutdown
B(config-if)# ip route 172.16.20.1 255.255.255.0
B(config-if)# tunnel source 202.208.220.1
B(config-if)# tunnel destination 110.1.1.1

B(config)# ip route 172.16.10.0 255.255.255.0 172.16.20.1
B(config)# ip mtu 1400
```