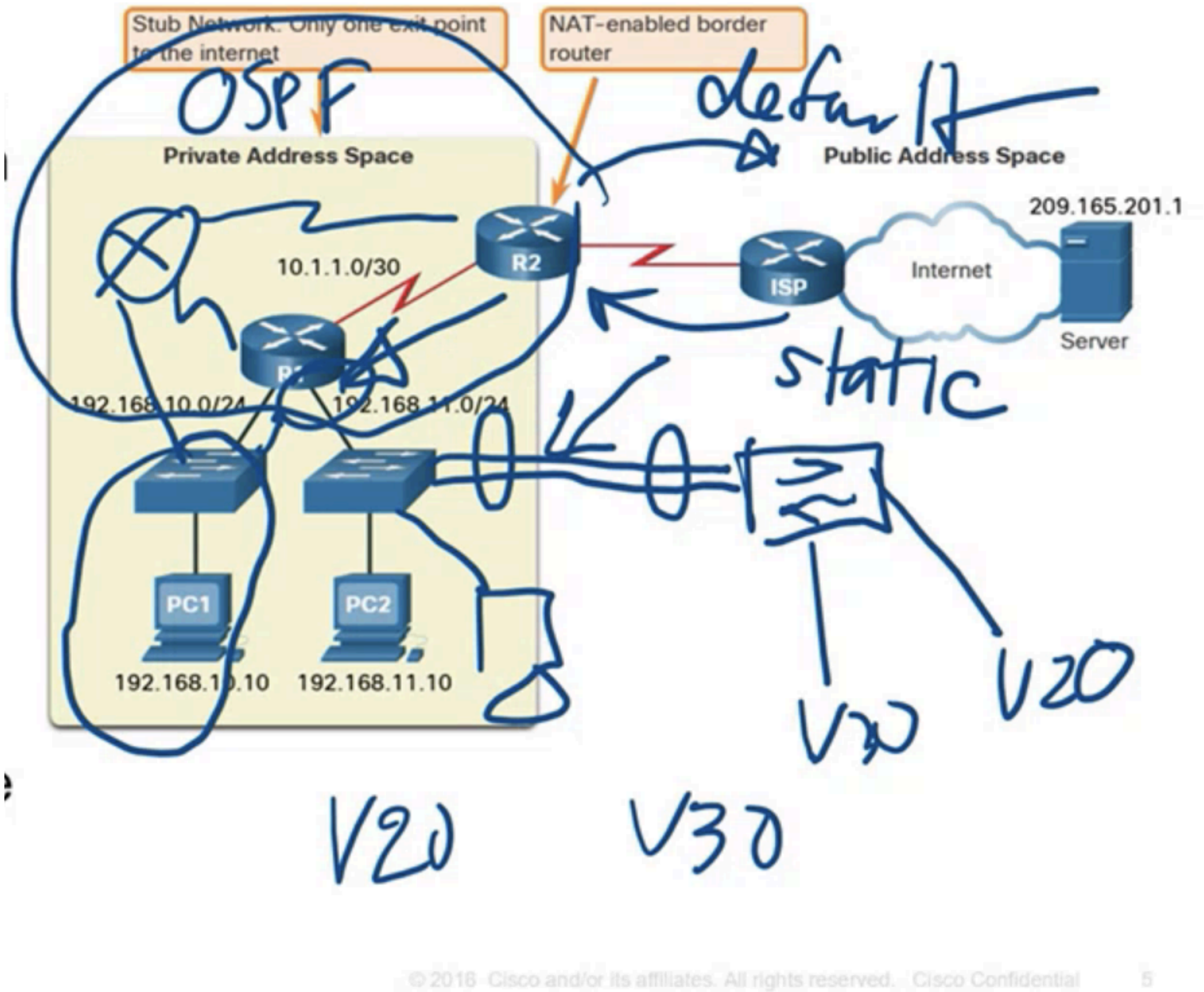
4



The image depicts a network topology diagram with annotations explaining various networking concepts. Here's an overview of the network functions based on the image and the accompanying text:

1. **OSPF (Open Shortest Path First)**: This is a dynamic routing protocol used to find the best path for data packets within an IP network. In the diagram,_ OSPF is likely implemented between the network routers to dynamically discover the optimal paths for data transmission.

2. **VLANs (Virtual Local Area Networks)**: VLANs are used to segment a physical network into multiple logical networks. This allows groups of devices to communicate as if they were on the same physical network, even if they are not. VLANs 20 and 30 are mentioned, indicating different segments within the network.

> "VLAN" stands for Virtual Local Area Network, while "Inter-VLAN" refers to communication between different VLANs.

1. **VLAN (Virtual Local Area Network)**:
   - VLANs are used to logically segment a physical network into multiple virtual networks.
   - Each VLAN operates as if it were a separate physical network, even though multiple VLANs may share the same physical network infrastructure.
   - VLANs are typically used to improve network security, performance, and manageability by isolating traffic and grouping devices logically.
   - Devices within the same VLAN can communicate with each other directly without needing to traverse a router.

2. **Inter-VLAN**:
   - Inter-VLAN communication refers to the ability of devices in different VLANs to communicate with each other.
   - By default, devices in separate VLANs cannot communicate with each other directly because VLANs provide logical isolation.
   - Inter-VLAN communication can be achieved through various methods, including using a router or a Layer 3 switch to route traffic between VLANs.
   - Inter-VLAN communication is necessary for scenarios where devices in different VLANs need to exchange data, such as accessing shared resources like servers, printers, or connecting to the internet.

In summary, VLANs provide logical segmentation within a network, while Inter-VLAN communication allows devices in different VLANs to communicate with each other when necessary.

3. **Inter-VLAN Routing**: It is the process of forwarding network traffic from one VLAN to another using a layer 3 device, typically a router or a layer 3 switch.Inter-VLAN routing allows for the segmentation of a network into multiple VLANs while still enabling communication between them when needed. This segmentation enhances security, reduces broadcast domains, and provides better network performance and management.

4. **Trunking**: This refers to the practice of carrying traffic from multiple VLANs over a single network link between switches through the use of a trunking protocol like IEEE 802.1Q.
A "trunk port" and a "switch port" are both types of ports found on network switches, but they serve different purposes:

1. **Trunk Port**:
   - A trunk port is a special type of port that is configured to carry traffic for multiple VLANs simultaneously.

- Trunk ports use tagging mechanisms like IEEE 802.1Q to differentiate between VLANs and ensure that traffic from different VLANs can traverse the same physical link without becoming mixed.
- Trunk ports are typically used to interconnect switches, routers, or other networking devices, allowing them to exchange traffic for multiple VLANs.

2. **Switch Port**:
   - A switch port is a general term for any port on a network switch.
   - Switch ports can be configured in different modes, including access mode and trunk mode.
   - Access ports are configured to carry traffic for a single VLAN and are typically used to connect end devices such as computers, printers, or IP phones to the switch.
   - Trunk ports, as mentioned earlier, are configured to carry traffic for multiple VLANs and are used for interconnecting networking devices.

In summary, while both trunk ports and switch ports are found on network switches, trunk ports are specifically configured to carry traffic for multiple VLANs, while switch ports can be configured for various purposes, including access or trunking.

5. **EtherChannel**: This technology allows the bundling of several physical Ethernet links to create a logical Ethernet link that provides higher throughput and redundancy. EtherChannels can be used to connect switches, routers, and servers.

Trunk ports and EtherChannels are both used in networking to improve bandwidth and provide redundancy, but they serve different purposes and operate at different layers of the OSI model.

1. **Trunk Port**:
   - A trunk port is a type of port on a network switch that is configured to carry traffic for multiple VLANs simultaneously.
   - Trunk ports use VLAN tagging mechanisms (such as IEEE 802.1Q) to differentiate between VLANs and ensure that traffic from different VLANs can traverse the same physical link without becoming mixed.
   - Trunk ports are typically used to interconnect switches, routers, or other networking devices, allowing them to exchange traffic for multiple VLANs.

2. **EtherChannel**:
   - EtherChannel, also known as port-channel or link aggregation, is a technique used to combine multiple physical Ethernet links into a single logical link.
   - EtherChannel provides increased bandwidth and redundancy by bundling multiple physical links together to form a high-capacity link.
   - EtherChannel can be configured between switches, routers, or servers, allowing for load balancing and fault tolerance across multiple physical links.
   - EtherChannel operates at the data link layer (Layer 2) of the OSI model, while trunking typically operates at the network layer (Layer 3) when used with VLANs.

In summary, while both trunk ports and EtherChannels are used to improve network performance and redundancy, trunk ports are used to carry traffic for multiple VLANs over a single physical link, while EtherChannel is used to aggregate multiple physical links into a single logical link for increased bandwidth and redundancy.

6. **First Hop Redundancy Protocols (FHRP)**: These protocols, such as HSRP (Hot Standby Router Protocol) or VRRP (Virtual Router Redundancy Protocol), provide the ability to configure more than one physical router as a logical gateway to maintain connectivity even if one router fails.

7. **Static Routing**: This involves manually specifying the network routes rather than relying on a routing protocol to dynamically learn and update routing information. Static routes are useful in smaller networks or in stub network scenarios where there is only one path to an external network.

8. **NAT (Network Address Translation)**: NAT is a method used to modify network address information in IP packet headers while in transit across traffic routing devices. This can be used for mapping private local addresses to a public address for internet access.

9. **ACL (Access Control Lists)**: ACLs are used to filter traffic based on rules set for the incoming or outgoing packets. They can be used to increase security by controlling the flow of traffic.

The annotations on the diagram suggest that these concepts are being explained in the context of preparing for a network configuration or educational setting. The discussion seems to revolve around setting up and understanding a network that includes different VLANs, routing protocols, and other network technologies to create a robust and efficient networking environment.
Certainly! Here's a basic rundown of the commands that might be used on Cisco devices for the networking concepts mentioned in the image:

1. **OSPF Configuration**:
https://itexamanswers.net/6-3-6-lab-basic-device-configuration-and-ospf-authentication-answers.html

```plaintext
router ospf 1
network 10.1.1.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.255 area 0
```

2. **VLAN Configuration**:
https://itexamanswers.net/3-3-12-packet-tracer-vlan-configuration-instructions-answer.html

```plaintext
   vlan 20
   name Sales
   vlan 30
   name HR
   ```

3. **Assign VLAN to Switch Port**:
https://itexamanswers.net/3-3-12-packet-tracer-vlan-configuration-instructions-answer.html
   ```plaintext
   interface FastEthernet0/1
   switchport mode access
   switchport access vlan 20
   ```

```
interface GigabitEthernet0/1
 description Connection to Server-1
 switchport mode access
 switchport access vlan 10
```

4. **Inter-VLAN Routing (on a Layer 3 Switch)**:
https://itexamanswers.net/4-3-8-packet-tracer-configure-layer-3-switching-and-inter-vlan-routing-instructions-answer.html
   ```plaintext
   interface Vlan20
   ip address 192.168.20.1 255.255.255.0
   no shutdown

   interface Vlan30
   ip address 192.168.30.1 255.255.255.0
   no shutdown
   ```

5. **Trunk Configuration**:
https://itexamanswers.net/3-4-5-packet-tracer-configure-trunks-instructions-answer.html
   ```plaintext
   interface FastEthernet0/24
   switchport mode trunk
   switchport trunk allowed vlan 20,30

switchport trunk native vlan 99
   ```

```

6. **EtherChannel Configuration**:
https://itexamanswers.net/6-2-4-packet-tracer-configure-etherchannel-instructions-answer.html

int range f0/1-2

switchport mode trunk

  interface range FastEthernet0/1 - 2
  channel-group 1 mode on
  interface Port-channel1
  switchport mode trunk
  ```

7. **First Hop Redundancy Protocols (e.g., HSRP)**:
https://itexamanswers.net/ccnp-switch-chapter-6-lab-6-1-first-hop-redundancy-protocols-hsrp-and-vrrp-version-7.html
  ```plaintext
  interface Vlan20
  standby 1 ip 192.168.20.254
  standby 1 priority 110
  standby 1 preempt
  ```

8. **Static Routing**:
ip route <destination-network> <subnet-mask> <next-hop-ip-address>
https://itexamanswers.net/lab-21-configuring-static-routing-via-ip-addresses.html
https://studylib.net/doc/8812541/lab-2.8.1--basic-static-route-configuration
  ```plaintext
  ip route 0.0.0.0 0.0.0.0 209.165.201.1
  ```

9. **NAT Configuration (overloading)**:
https://itexamanswers.net/6-8-2-lab-configure-nat-for-ipv4-answers.html
  ```plaintext
  access-list 1 permit 192.168.10.0 0.0.0.255
  ip nat inside source list 1 interface FastEthernet0/0 overload
  interface FastEthernet0/0
  ip nat outside
  interface Vlan20
  ip nat inside
  ```

10. **ACL Configuration**:

https://itexamanswers.net/lab-126-configuring-access-control-lists-acls.html

```plaintext
access-list 10 deny host 10.0.0.2

access-list 10 permit any

int fa0/ 1

ip access-group 10 in

exit

Exit

access-list 150 deny tcp host 10.0.0.2 host 20.0.0.2 0.0.0.0 eq www

access-list 150 permit ip any any

int fa0/ 1

ip access-group 150 in

exit

exit


no access-list 150 deny tcp host 10.0.0.2 host 20.0.0.2 eq www

access-list 101 permit tcp <source_subnet> <source_wildcard_mask> any eq 80

access-list 101 permit tcp <source_subnet> <source_wildcard_mask> any eq 443

access-list 101 permit tcp <source_subnet> <source_wildcard_mask> any eq 25

access-list 101 permit udp <source_subnet> <source_wildcard_mask> any eq 53

access-list 101 permit tcp <specific_host> <specific_host_wildcard_mask> any eq 22
```

```
access-list 101 deny ip any any

interface <interface_name>

ip access-group 101 in
```

```
   access-list 100 permit ip 192.168.10.0 0.0.0.255 any
   interface FastEthernet0/1
   ip access-group 100 in
```

Please note that these commands are quite basic and are meant to be used as a starting point. The actual configuration might vary based on the exact requirements of the network, the model of the Cisco device, and the version of the IOS running on it. Always consult the device documentation and use these commands in a controlled environment, such as a lab, before applying them to a production network.
Sure, here are the `show` commands for checking the configuration of each part of the network setup:

1. **To verify OSPF configuration**:
   ```plaintext
   show ip ospf
   show ip ospf neighbor
   show ip route ospf
   ```

2. **To check VLANs**:
   ```plaintext
   show vlan brief
   ```

3. **To verify VLAN assignment to switch ports**:
   ```plaintext
   show interface switchport
   ```

4. **To check Inter-VLAN routing**:
   ```plaintext
   show ip interface brief
   ```

   show running-config interface vlan 20
   show running-config interface vlan 30

5. **To verify trunk configuration**:
   ```plaintext
   show interface trunk
   ```

6. **To verify EtherChannel**:
   ```plaintext
   show etherchannel summary
   ```

7. **To check FHRP (HSRP, VRRP)**:
   ```plaintext
   show standby
   show vrrp (if VRRP is used)
   ```

8. **To verify static routing**:
   ```plaintext
   show ip route static
   ```

9. **To check NAT translations**:
   ```plaintext
   show ip nat translations
   show ip nat statistics
   ```

10. **To verify ACLs**:
    ```plaintext
    show access-lists
    show ip interface | include access-list
    ```

Remember to use these commands in the appropriate context, for example, if you're on a router or a switch. The output will give you detailed information about the current state of each network component. If you're troubleshooting, these commands can help pinpoint where issues may be occurring.

In networking, both trunk ports and EtherChannel are concepts associated with the efficient management of traffic between switches.

1. **Trunk Port:**
   - A trunk port is a network port that is configured to carry traffic for multiple VLANs. It allows the transmission of frames from multiple VLANs across a single physical link between switches.
   - Trunking is essential when you want to extend VLANs across multiple switches. Without trunking, each VLAN would require a dedicated physical link between switches.
   - Trunk ports use a tagging mechanism to identify which VLAN a particular frame belongs to. The most common tagging protocol is IEEE 802.1Q, and this is often the type of encapsulation used when configuring trunk ports on Cisco devices.

   Example of configuring a trunk port in Cisco IOS:
   ```plaintext
   interface GigabitEthernet0/1
   switchport mode trunk
   switchport trunk encapsulation dot1q
   ```

2. **EtherChannel:**
   - EtherChannel, also known as Link Aggregation or Port Channel, involves bundling multiple physical links into a single logical link between two switches. This provides increased bandwidth, redundancy, and load balancing.2
   - EtherChannel is not VLAN-specific. It aggregates the bandwidth of multiple links regardless of VLAN membership.
   - It is commonly used to connect two switches or a switch and a server, and it is independent of VLAN configurations. The links in an EtherChannel can belong to different VLANs.

   Example of configuring an EtherChannel in Cisco IOS:
   ```plaintext
   interface range GigabitEthernet0/1 - 2
   channel-group 1 mode desirable
   ```

   In this example, two physical interfaces (GigabitEthernet0/1 and GigabitEthernet0/2) are being grouped into a logical EtherChannel (channel-group 1).

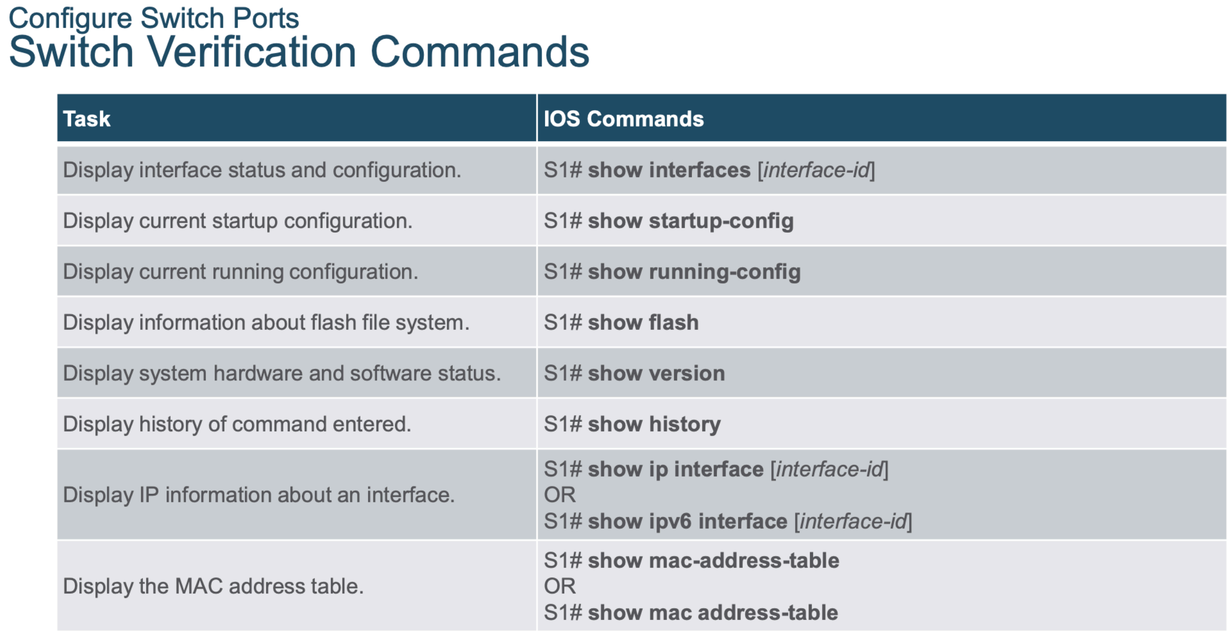
Key Differences:
- **Function:**
  - Trunk ports are used for carrying traffic for multiple VLANs over a single link.
  - EtherChannel aggregates multiple physical links into a single logical link for increased bandwidth and redundancy.

- **Association with VLANs:**

  - Trunk ports are VLAN-specific and are used for inter-VLAN communication.
  - EtherChannel is not VLAN-specific and does not inherently deal with VLANs.

- **Configuration:**
  - Trunk ports are configured to carry traffic for specific VLANs, and you can configure the trunking protocol (e.g., dot1q).
  - EtherChannel is configured to bundle multiple physical links into a logical link, and it is independent of VLAN configurations.

In summary, trunk ports are specifically designed for VLAN traffic, while EtherChannel is a mechanism to aggregate multiple physical links for increased overall bandwidth and redundancy, regardless of VLAN memberships.



Configure Switch Ports

Switch Verification Commands

Task	IOS Commands
Display interface status and configuration.	S1# **show interfaces** [*interface-id*]
Display current startup configuration.	S1# **show startup-config**
Display current running configuration.	S1# **show running-config**
Display information about flash file system.	S1# **show flash**
Display system hardware and software status.	S1# **show version**
Display history of command entered.	S1# **show history**
Display IP information about an interface.	S1# **show ip interface** [*interface-id*] OR S1# **show ipv6 interface** [*interface-id*]
Display the MAC address table.	S1# **show mac-address-table** OR S1# **show mac address-table**

More explanation

—--—---—-------------------------

Sure, here's another example of an OSPF configuration snippet:

```plaintext
router ospf 10
 network 192.168.1.0 0.0.0.255 area 0
 network 10.0.0.0 0.255.255.255 area 1
 network 172.16.0.0 0.0.255.255 area 0
```

Let's break this down:

- `router ospf 10`: This command enters OSPF configuration mode with a process ID of 10.

- `network 192.168.1.0 0.0.0.255 area 0`: This line specifies that the network 192.168.1.0/24 is participating in OSPF Area 0.

- `network 10.0.0.0 0.255.255.255 area 1`: This command indicates that any interface in the range of 10.0.0.0 to 10.255.255.255 (with subnet mask 255.0.0.0) should be included in OSPF Area 1.

- `network 172.16.0.0 0.0.255.255 area 0`: This line specifies that the network 172.16.0.0/16 is participating in OSPF Area 0.

In this example, OSPF is configured with process ID 10, advertising three different networks into OSPF Areas 0 and 1.

In OSPF (Open Shortest Path First), the process ID is a locally significant identifier used to distinguish between multiple instances of OSPF running on the same router. The process ID itself doesn't have any functional significance outside the router where OSPF is configured.

Each OSPF process on a router operates independently of other OSPF processes on the same router. The process ID is used primarily for administrative purposes to help network administrators differentiate between OSPF instances when viewing configuration or troubleshooting.

So, in the context of the configuration snippet provided earlier:

```plaintext
router ospf 10
```

The process ID is set to 10. This means that OSPF on this router is configured to run with process ID 10. If there are other OSPF configurations on the same router, they might have different process IDs.

The choice of "10" for the OSPF process ID in the configuration snippet is arbitrary and depends on the network administrator or the organization's conventions. In practice, network administrators often choose process IDs based on their own internal numbering schemes, organizational policies, or simply personal preference.

Using "10" as the process ID is a common practice because it's easy to remember and manage. Additionally, some network administrators might choose process IDs based on the router's location, function, or importance within the network topology.

Ultimately, the specific number chosen for the OSPF process ID doesn't affect the functionality of OSPF itself; it's simply a label used to identify the OSPF process on a particular router.
—---—--—-------------------------

Certainly! Here's an example of configuring a switch port on a Cisco switch:

```plaintext
interface GigabitEthernet0/1
 description Connection to Server-1
 switchport mode access
 switchport access vlan 10
```

Let's break down this configuration:

- `interface GigabitEthernet0/1`: This command enters interface configuration mode for GigabitEthernet interface 0/1. This is the interface you want to configure.

- `description Connection to Server-1`: This optional command assigns a description to the interface for documentation purposes. It helps you identify the purpose of the interface.

- `switchport mode access`: This command configures the interface as an access port. Access ports are used to connect end devices like computers or servers to the switch. They belong to a single VLAN and do not carry VLAN tagging.

- `switchport access vlan 10`: This command assigns VLAN 10 to the access port. It means that any device connected to this port will be a member of VLAN 10.

This configuration sets up GigabitEthernet0/1 as an access port in VLAN 10, which could be used to connect a server, for example. Remember, the exact syntax and commands might vary depending on the switch model and software version.

Besides the "access" mode, there are two other common modes for switch ports: "trunk" mode and "dynamic" modes. Here's a brief overview of each:

1. **Trunk Mode**:
   - Trunk mode is used to configure a switch port to carry traffic for multiple VLANs.
   - In trunk mode, the switch port can carry traffic for multiple VLANs simultaneously by adding VLAN tags to Ethernet frames.
   - Trunk ports are typically used to interconnect switches or to connect to routers or other networking devices that support VLAN trunking.
   - Example configuration command: `switchport mode trunk`

2. **Dynamic Modes**:
   - There are two dynamic modes: "dynamic auto" and "dynamic desirable".
   - These modes allow the switch port to negotiate its mode with the neighboring device automatically.
   - If one end of the link is set to "dynamic auto" and the other end is set to "dynamic desirable", the link will become a trunk.
   - If both ends are set to "dynamic auto", the link will remain as an access port.
   - If both ends are set to "dynamic desirable", the link will become a trunk.
   - Example configuration commands:
     - `switchport mode dynamic auto`
     - `switchport mode dynamic desirable`

These different modes provide flexibility in configuring switch ports to meet the specific requirements of the network topology and the devices connected to them.

—---—---—---------------------------

The native VLAN in a Cisco switch is the default VLAN for all untagged traffic on a trunk link. Trunk links are used to carry traffic for multiple VLANs between switches, and they use encapsulation methods like IEEE 802.1Q or ISL to differentiate between the VLANs.

The native VLAN is essential for a few reasons:

1. **Interoperability:**
   - Different vendors might have different default settings for native VLANs. Specifying the native VLAN helps ensure interoperability between devices from different manufacturers.

2. **Avoiding VLAN Hopping:**
   - VLAN hopping is a security vulnerability where an attacker sends frames with double-tagged VLAN IDs to gain unauthorized access to traffic in a different VLAN. By setting a specific native VLAN, you can help mitigate the risk of VLAN hopping.

3. **Avoiding Misconfigurations:**
   - Explicitly defining the native VLAN helps prevent misconfigurations or unintentional VLAN assignments. It makes the network more predictable and less prone to errors.

In the provided command example:

```bash
MLS(config-if)# switchport trunk native vlan 99
```

This command is configuring an interface on a switch (MLS) to use VLAN 99 as the native VLAN for trunking. It ensures that any untagged frames received on this trunk interface are treated as part of VLAN 99. This configuration should match the native VLAN setting on the connecting switch to maintain consistency and proper communication between devices.

—---—---—-------------------------

In the provided configuration for HSRP (Hot Standby Router Protocol) on Cisco devices, the command `standby 40 preempt` is configuring the router interface to be in "preempt" mode for the HSRP group 40.

Here's a breakdown of the command:

- `standby 40`: Specifies HSRP group number 40. HSRP allows routers to work together in order to present a virtual router's MAC address and IP address to the network.

- `preempt`: This command enables the router to take back the role of the active router in the HSRP group if its priority is higher than the current active router. If the preempt command is not configured, the router with the highest priority becomes the active router, and it retains that role until its tracked interfaces fail or a router with a higher priority comes online.

In the given context:

- `DLS1(config-if)# standby 40 preempt`: This command is configured on the interface associated with VLAN 40 on the DLS1 router. It indicates that if DLS1 becomes the standby router for HSRP group 40 and its priority becomes higher than the currently active router, DLS1 should take over as the active router for that HSRP group.

Similarly, the `DLS2(config-if)# standby 40 preempt` command is configuring the interface associated with VLAN 40 on the DLS2 router to preemptively take over as the active router for HSRP group 40 if its priority is higher than the currently active router.

—---—---—-------------------------

ACL

Certainly! Let's consider a scenario where a company wants to implement a policy to deny access to certain types of websites during working hours to maintain productivity and reduce security risks.

Scenario: Web Access Policy

Objective: Implement a web access policy to deny access to certain categories of websites during working hours (e.g., social media, gaming, adult content) to improve productivity and minimize security risks associated with inappropriate web usage.

Policy:
1. **Allowed Categories**: During working hours (9:00 AM to 5:00 PM), employees are permitted to access websites related to work-related activities, research, news, and professional development. These categories include:
   - Business and Finance
   - News and Media
   - Education and Reference
   - Technology and Science
   - Search Engines

2. **Denied Categories**: Access to the following categories of websites is denied during working hours:
   - Social Media
   - Online Gaming
   - Adult Content
   - Entertainment (videos, music streaming, etc.)

3. **Implementation**:
   - Utilize a web filtering solution or proxy server capable of categorizing and filtering web traffic based on predefined categories.
   - Configure the filtering rules to permit access to allowed categories and deny access to denied categories during working hours.
   - Implement user authentication mechanisms to track and enforce the policy on a per-user basis, ensuring that exceptions can be made for specific roles or departments if necessary.
   - Configure logging and reporting features to monitor web usage and violations of the policy.

4. **Communication and Training**:
   - Communicate the web access policy to all employees through company-wide announcements, employee handbooks, and training sessions.
   - Clearly explain the rationale behind the policy, its implications for productivity and security, and the consequences of policy violations.
   - Provide guidance on acceptable web usage and encourage employees to use company resources responsibly.

Example Configuration (using a web filtering solution):
```
Time-Based Access Control List (ACL):
permit tcp any any eq 80 time-range work_hours
permit tcp any any eq 443 time-range work_hours
deny tcp any any eq 80
deny tcp any any eq 443

Web Filtering Rules:
Allowed Categories:
permit category business_and_finance
permit category news_and_media
permit category education_and_reference
permit category technology_and_science
permit category search_engines

Denied Categories:
deny category social_media
deny category online_gaming
deny category adult_content
deny category entertainment

User Authentication:
Enable user authentication to enforce the policy on a per-user basis and track web usage.
```

Notes:

- The policy enforcement should be flexible enough to accommodate exceptions for specific users or departments that require access to restricted categories for legitimate business purposes.
- Regular monitoring and review of web usage logs are essential to ensure compliance with the policy and identify any unauthorized access attempts or policy violations.
- Adjust the policy as needed based on evolving business needs, technological advancements, and emerging security threats.

```
! Define time range for working hours (9:00 AM to 5:00 PM)
time-range work_hours
  periodic weekdays 9:00 to 17:00

! Define access control lists (ACLs)
ip access-list extended ALLOWED_TRAFFIC
  permit tcp any any eq 80 time-range work_hours
  permit tcp any any eq 443 time-range work_hours

ip access-list extended DENIED_TRAFFIC
  deny tcp any any eq 80
  deny tcp any any eq 443
```

```
! Define class-maps to match traffic based on ACLs
class-map match-all ALLOWED_TRAFFIC
  match access-group name ALLOWED_TRAFFIC

class-map match-all DENIED_TRAFFIC
  match access-group name DENIED_TRAFFIC

! Define policy-maps to apply actions based on class-maps
policy-map WEB_ACCESS_POLICY
  class ALLOWED_TRAFFIC
    pass
  class DENIED_TRAFFIC
    drop

! Apply the policy-map to the inbound interface
interface GigabitEthernet0/0  ! Replace with the appropriate interface
  service-policy input WEB_ACCESS_POLICY
```

—---—---—------------------------------

Let's say we have a network with the following setup:

- Router A needs to reach the network 192.168.2.0/24, which is connected to Router B at IP address 10.0.0.2.
- Router B has a direct connection to the network 192.168.2.0/24.

Router A's configuration for this static route would look like this:

```
RouterA(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2
```

This configuration tells Router A that in order to reach the network 192.168.2.0/24, it should forward packets to the next hop router with the IP address 10.0.0.2.

Subnet mask

Spanning tree

Route protocol and concept

Acl

Short answer question