copy the config to nvram: copy running-config startup-config or copy run start

to check the dir write: dir

to erase: erase startup-config

to enable password on user executive mode : line console 0

Password cisco

login

if you want the previous config which you have not saved so the command is copy startup-config running-config

Secure privileged mode access.

S1> enable

S1# configure terminal

S1(config)# enable password c1$c0

S1(config)# exit

Configure an encrypted password to secure access to privileged mode.

The enable password should be replaced with the newer encrypted secret password using the enable secret command. Set the enable secret password to itsasecret.

S1# config t

S1(config)# enable secret itsasecret

S1(config)# exit

S1#

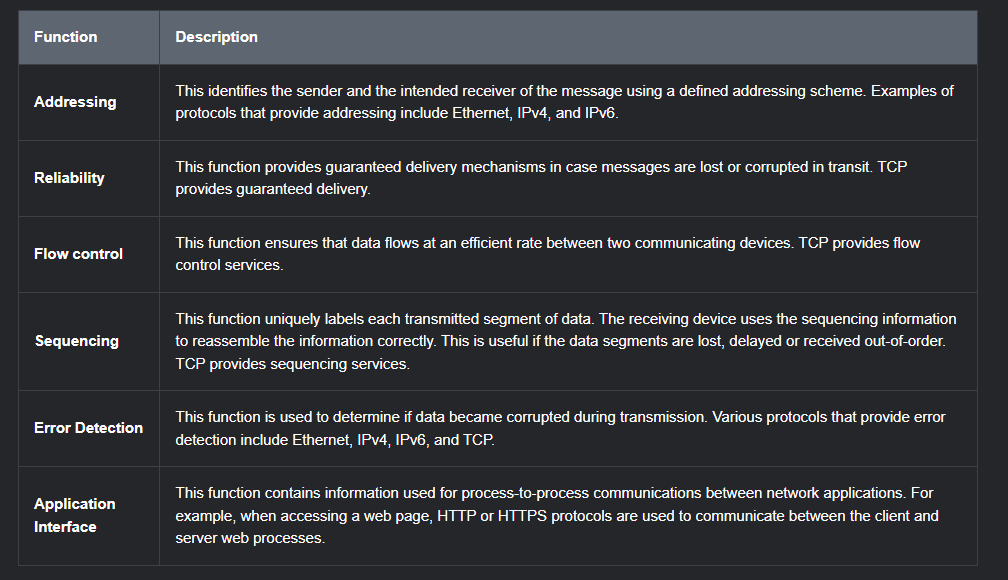
Configure a message of the day (MOTD) banner.

S1# config t

S1(config)# banner motd $ This is a secure system. Authorized Access Only! $

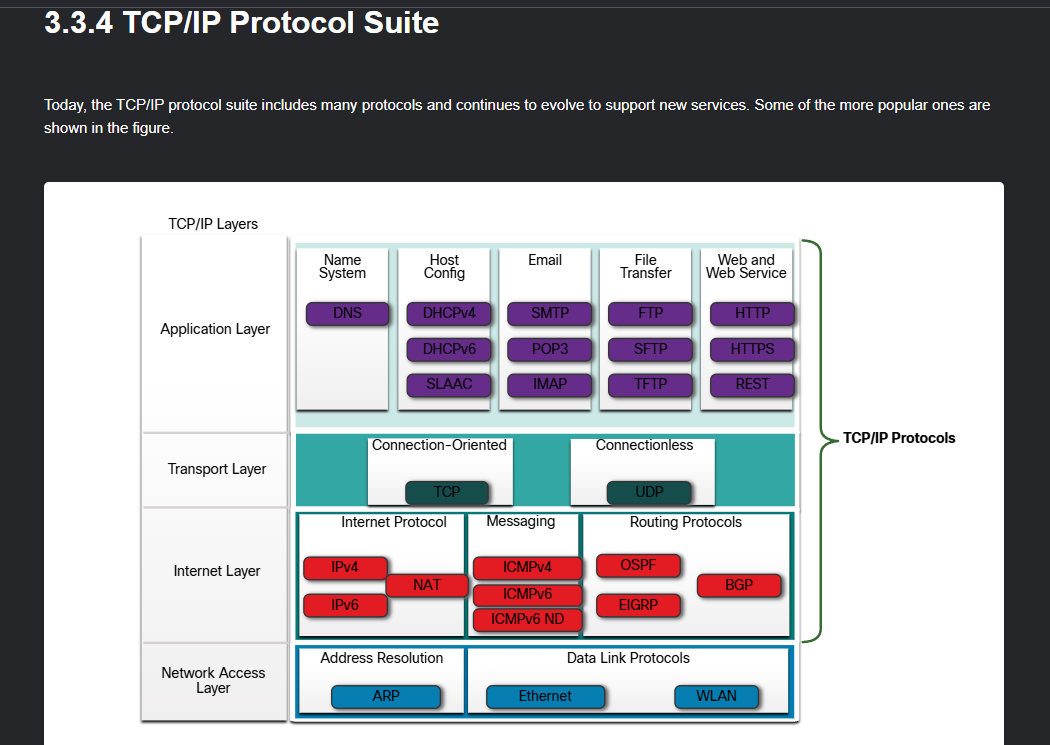
S1(config)# exit

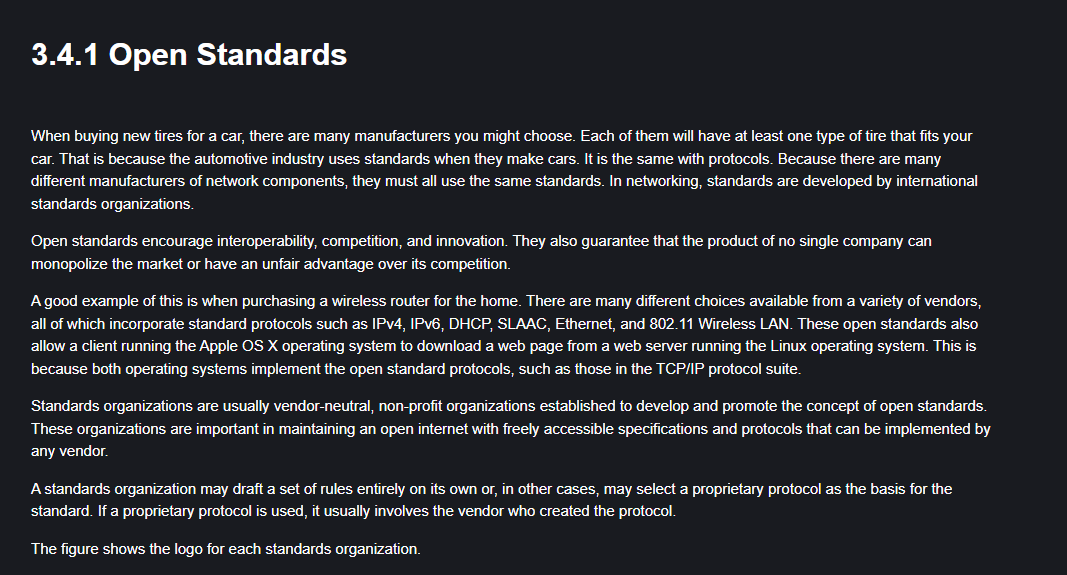
The structure of an IPv4 address is called dotted decimal notation and is represented by four decimal numbers between 0 and 255. IPv4 addresses are assigned to individual devices connected to a network.

network protocol includes 

A black background with white text

AI-generated content may be incorrect.





A close-up of a text

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

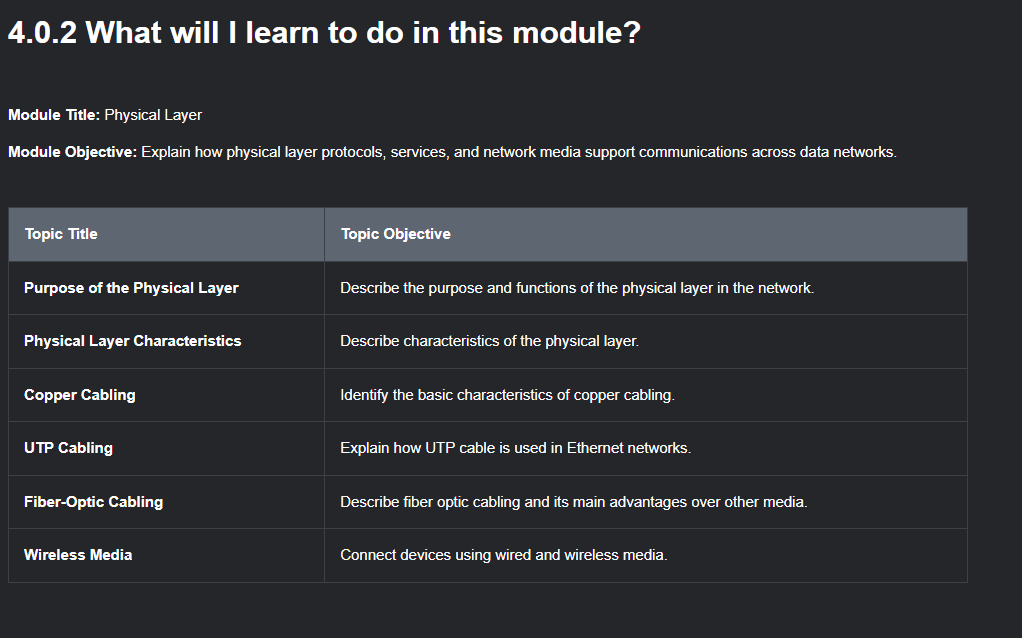
AI-generated content may be incorrect.

A diagram of a computer network

AI-generated content may be incorrect.

A diagram of a network

AI-generated content may be incorrect.



A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A black background with white text

AI-generated content may be incorrect.

A computer screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A diagram of a tube

AI-generated content may be incorrect.

Close up of a yellow and blue cable

AI-generated content may be incorrect.

A close-up of a computer cable

AI-generated content may be incorrect.A close up of a cable

AI-generated content may be incorrect.A close-up of a cable

AI-generated content may be incorrect.

A close up of an orange cable

AI-generated content may be incorrect.

A close-up of a yellow cable

AI-generated content may be incorrect.

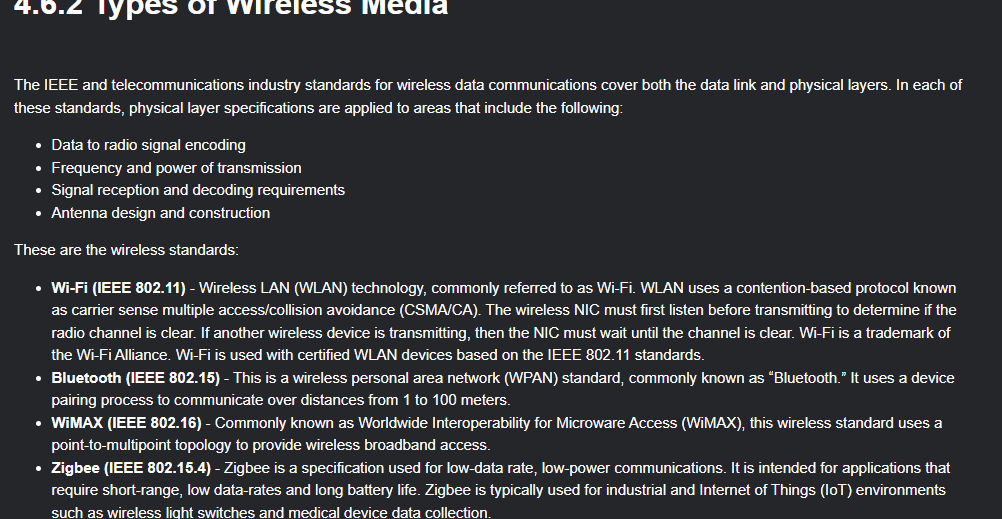
A close up of a cable

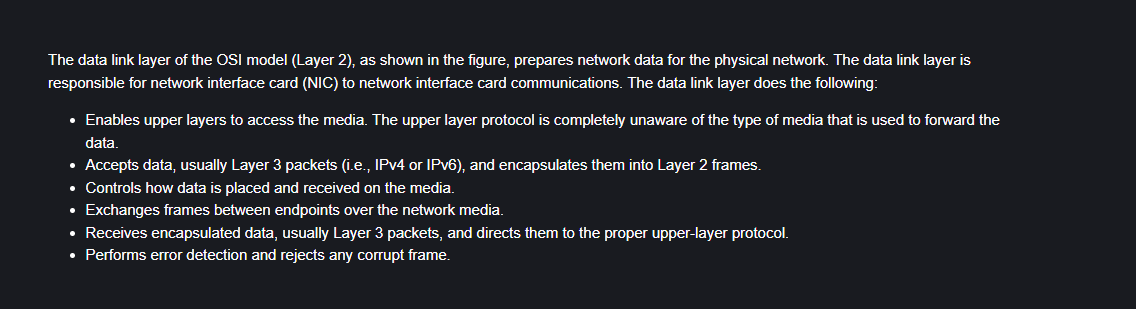
AI-generated content may be incorrect.

A yellow cable with connectors

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect. 



A screenshot of a computer

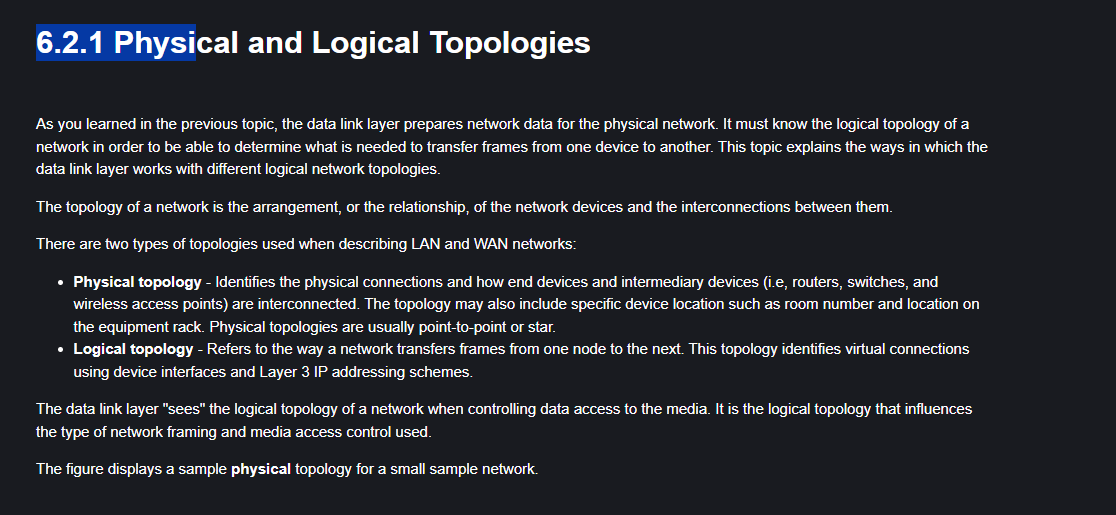
AI-generated content may be incorrect.

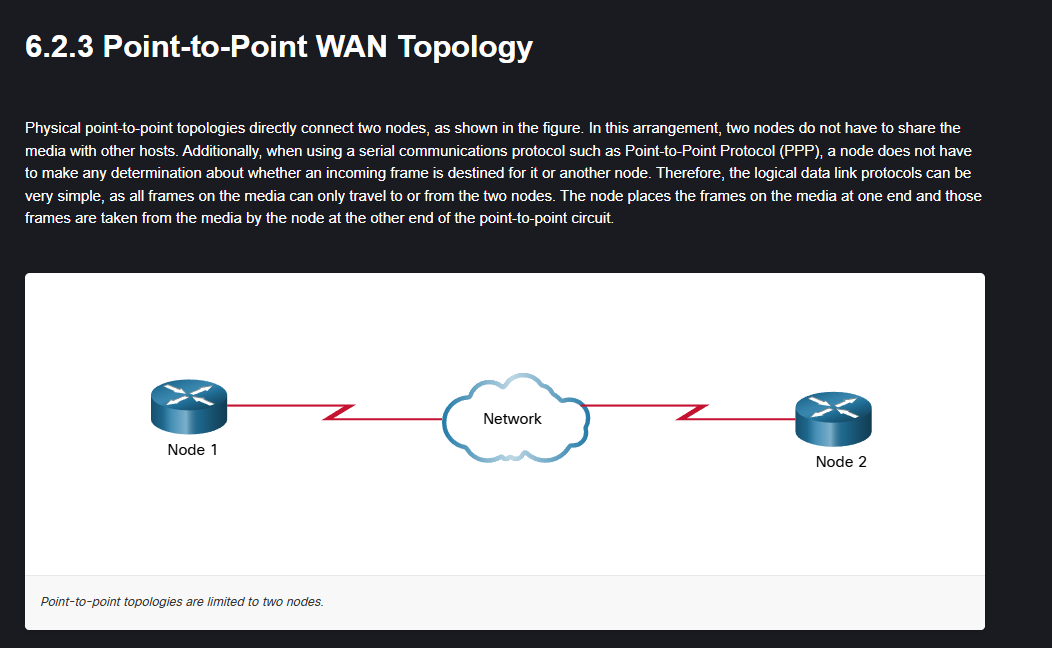
A diagram of a network layer protocol

AI-generated content may be incorrect.

A screenshot of a computer program

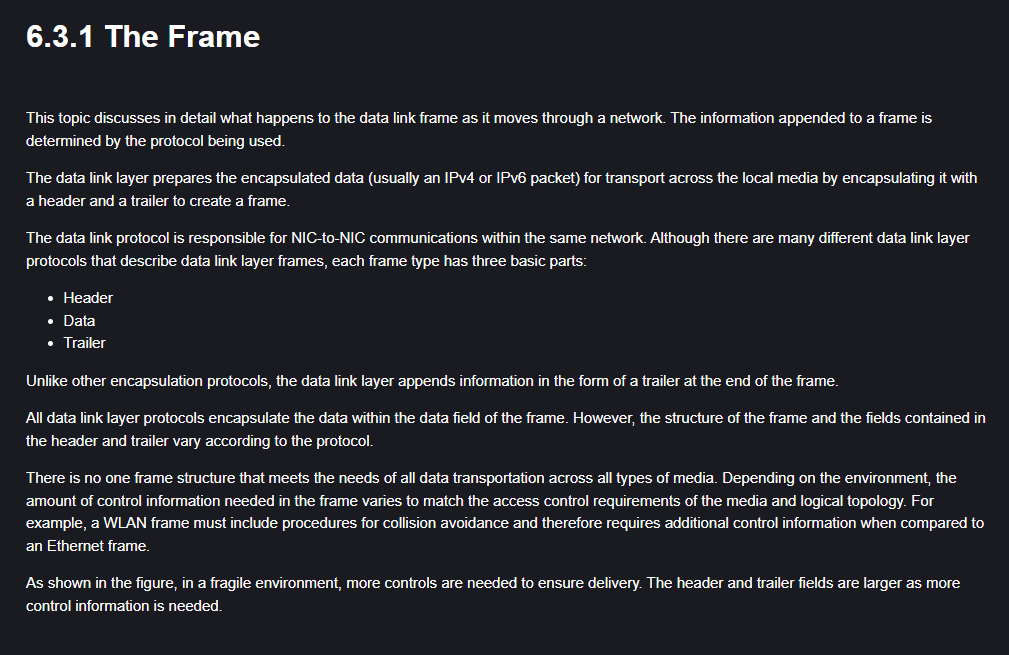
AI-generated content may be incorrect.





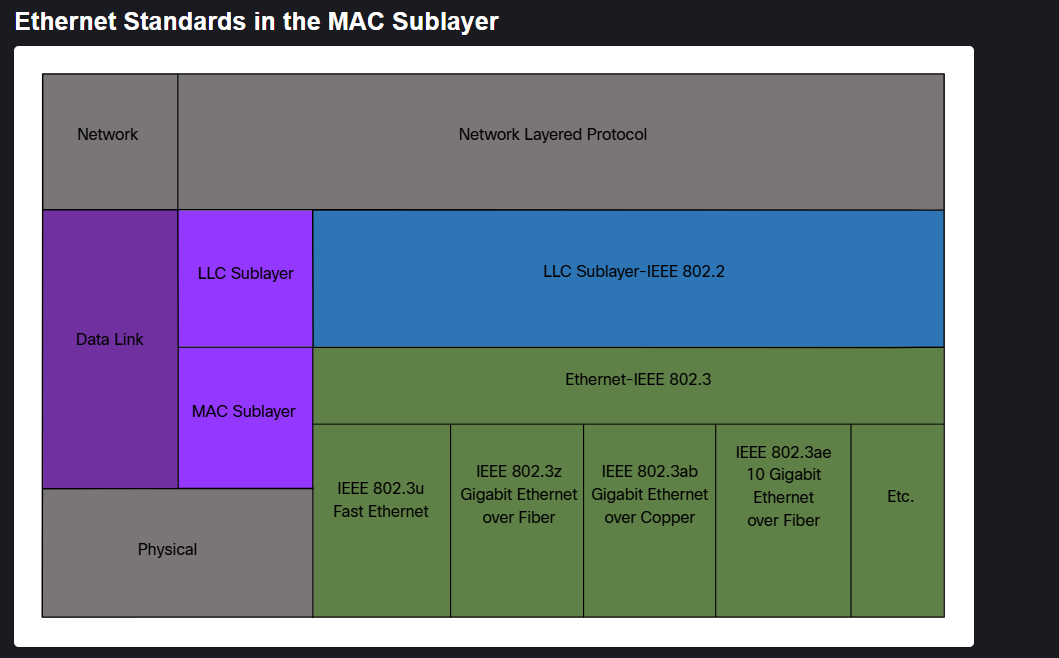
A computer screen shot of a cloud

AI-generated content may be incorrect.



A screenshot of a computer

AI-generated content may be incorrect.

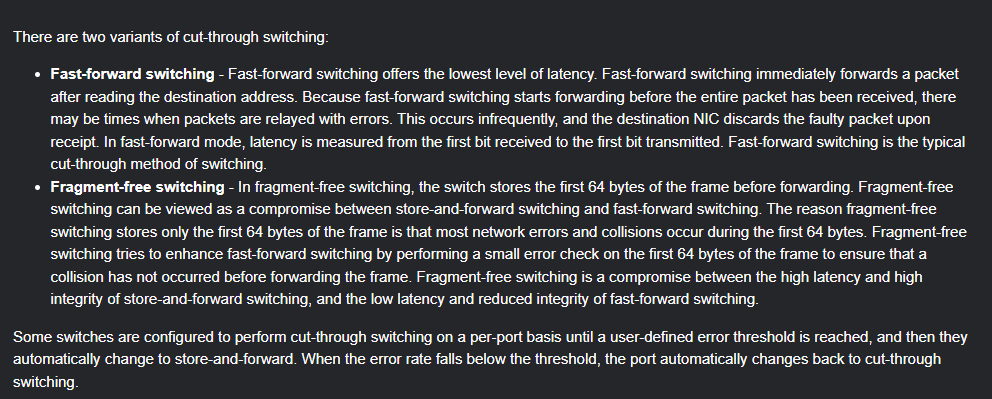


A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A computer network diagram with text

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A black screen with white text

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A diagram of a cloud

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A black background with white text

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A computer screen shot of a black screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A black screen with white text

AI-generated content may be incorrect.

A black screen with white text

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

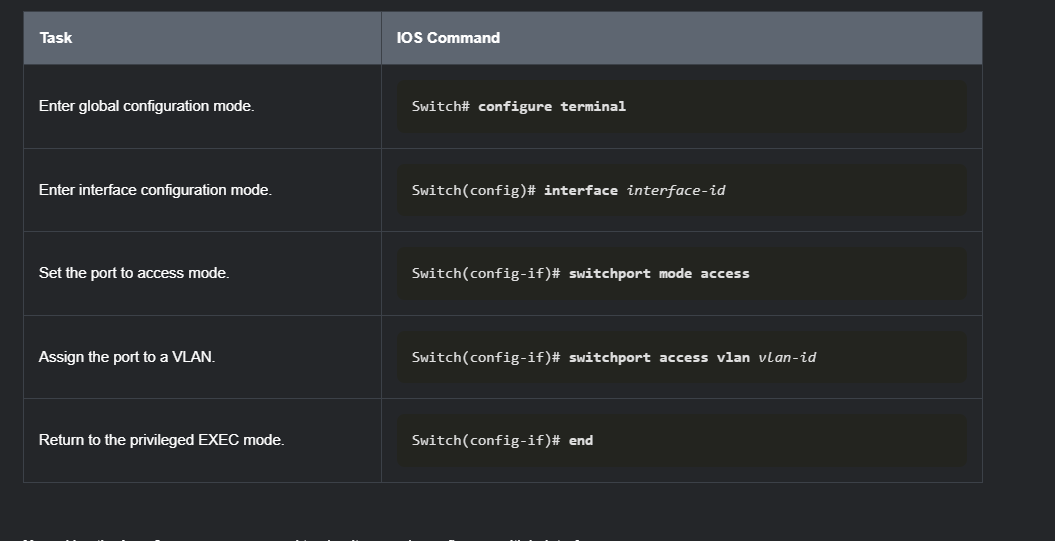
A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.A screen shot of a computer

AI-generated content may be incorrect.



Complete the following steps to create a data VLAN:

* Enter global configuration mode.
* Create VLAN 20.
* Name the VLAN **student**.
* Return to privileged EXEC mode.

S1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#vlan 20

S1(config-vlan)#name student

S1(config-vlan)#end

\*Mar 31, 08:55:14.5555: %SYS-5-CONFIG\_I: Configured from console by console

Display the brief VLAN information.

S1#show vlan

You must enter the exact and full command.

S1#show vlan brief

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24

Gi0/1, Gi0/2

20 student active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Complete the following steps to create a voice VLAN:

* Enter global configuration mode.
* Create VLAN 150.
* Name the VLAN **VOICE**.
* Return to global configuration mode.

S1#configure terminal

S1(config)#vlan 50

You must enter the exact and full command.

S1(config)#vlan 150

S1(config-vlan)#name Vlan voice

You must enter the exact and full command.

S1(config-vlan)#name VlanVoice

You must enter the exact and full command.

S1(config-vlan)#name voice

You must enter the exact and full command.

S1(config-vlan)#name VOICE

S1(config-vlan)#exit

Complete the following steps to assign the data and voice VLANs to a port:

* Enter interface configuration mode. Use **fa0/18** as the interface designation.
* Configure the port as an access port.
* Assign the data VLAN 20 to the port.
* Enable QoS settings with the **mls qos trust cos** command.
* Assign the voice VLAN 150 to the port.
* Return to privileged EXEC mode.

S1(config)#interface fa0/18

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 20

S1(config-if)#mls qos trust cos

S1(config-if)#switchport voice vlan 150

S1(config-if)#end

Display the brief vlan information.

S1#show vlan brief

LAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/19, Fa0/20, Fa0/21

Fa0/22, Fa0/23, Fa0/24, Gi0/1

Gi0/2

20 student active Fa0/18

150 VOICE active Fa0/18

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Complete the following steps to delete and verify a deleted VLAN on a port:

* Enter global configuration mode.
* Enter interface configuration mode. Use **fa0/18** as the interface designation.
* Remove the data VLAN from the port.
* Use the **do** form of the command to display brief VLAN information.

S1#configure terminal

S1(config)#interface fa0/18

S1(config-if)#no switchport access vlan

S1(config-if)#do show vlan brief

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24

Gi0/1, Gi0/2

20 student active

150 VOICE active Fa0/18

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Complete the following steps to assign VLAN 20 to another interface.

* Enter interface configuration mode. Use **fa0/11** as the interface designation.
* Assign VLAN 20 to the port.
* Return to privileged EXEC mode.

S1(config-if)#interface fa0/11

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 20

S1(config-if)#end

Display the brief VLAN information.

S1#show vlan brief

LAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/12, Fa0/13

Fa0/14, Fa0/15, Fa0/16, Fa0/17

Fa0/19, Fa0/20, Fa0/21, Fa0/22

Fa0/23, Fa0/24, Gig0/1, Gig0/2

20 student active Fa0/11

150 VOICE active Fa0/18

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Display the VLAN information specifically for the student VLAN.

S1#show vlan name student

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

20 student active Fa0/11, Fa0/18

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2

---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

20 enet 100020 1500 - - - - - 0 0

Display summary information for VLANs

S1#show vlan summary

Number of existing VLANs : 7

Number of existing VTP VLANs : 7

Number of existing extended VLANS : 0

Display the switchport information. Use **fa0/11** for the interface designation.

S1#show interface fa0/11 switchport

Name: Fa0/11

Switchport: Enabled

Administrative Mode: static access

Operational Mode: down

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: native

Negotiation of Trunking: Off

Access Mode VLAN: 20 (Students)

Trunking Native Mode VLAN: 1 (default)

Voice VLAN: none

(output omitted)

A screenshot of a computer

AI-generated content may be incorrect.

The example shows the configuration of port F0/1 on switch S1 as a trunk port. The native VLAN is changed to VLAN 99 and the allowed VLAN list is restricted to 10, 20, 30, and 99.

S1(config)# **interface fastEthernet 0/1**

S1(config-if)# **switchport mode trunk**

S1(config-if)# **switchport trunk native vlan 99**

S1(config-if)# **switchport trunk allowed vlan 10,20,30,99**

S1(config-if)# **end**

**Note:** This configuration assumes the use of Cisco Catalyst 2960 switches which automatically use 802.1Q encapsulation on trunk links. Other switches may require manual configuration of the encapsulation. Always configure both ends of a trunk link with

S1# **show interfaces fa0/1 switchport**

Name: Fa0/1

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: On

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 99 (VLAN0099)

Voice VLAN: none

Administrative private-vlan host-association: none

Administrative private-vlan mapping: none

Administrative private-vlan trunk native VLAN: none

Administrative private-vlan trunk encapsulation: dot1q

Administrative private-vlan trunk normal VLANs: none

Administrative private-vlan trunk associations: none

Administrative private-vlan trunk private VLANs: none

Operational private-vlan: none

Trunking VLANs Enabled: 10,20,30,99

Pruning VLANs Enabled: 2-1001

**(output omitted)**

**Reset the Trunk to the Default State**

Use the **no switchport trunk allowed vlan** and the **no switchport trunk native vlan** commands to remove the allowed VLANs and reset the native VLAN of the trunk. When it is reset to the default state, the trunk allows all VLANs and uses VLAN 1 as the native VLAN. The example shows the commands used to reset all trunking characteristics of a trunking interface to the default settings.

S1(config)# **interface fa0/1**

S1(config-if)# **no switchport trunk allowed vlan**

S1(config-if)# **no switchport trunk native vlan**

S1(config-if)# **end**

The**show interfaces fa0/1 switchport** command reveals that the trunk has been reconfigured to a default state.

S1# **show interfaces fa0/1 switchport**

Name: Fa0/1

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: On

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 1 (default)

Administrative Native VLAN tagging: enabled

Voice VLAN: none

Administrative private-vlan host-association: none

Administrative private-vlan mapping: none

Administrative private-vlan trunk native VLAN: none

Administrative private-vlan trunk Native VLAN tagging: enabled

Administrative private-vlan trunk encapsulation: dot1q

Administrative private-vlan trunk normal VLANs: none

Administrative private-vlan trunk associations: none

Administrative private-vlan trunk mappings: none

Operational private-vlan: none

Trunking VLANs Enabled: ALL

Pruning VLANs Enabled: 2-1001

**(output omitted)**

This sample output shows the commands used to remove the trunk feature from the F0/1 switch port on switch S1. The **show interfaces f0/1 switchport** command reveals that the F0/1 interface is now in static access mode.

S1(config)# **interface fa0/1**

S1(config-if)# **switchport mode access**

S1(config-if)# **end**

S1# **show interfaces fa0/1 switchport**

Name: Fa0/1

Switchport: Enabled

**Administrative Mode: static access**

**Operational Mode: static access**

**Administrative Trunking Encapsulation: dot1q**

**Operational Trunking Encapsulation: native**

**Negotiation of Trunking: Off**

**Access Mode VLAN: 1 (default)**

**Trunking Native Mode VLAN: 1 (default)**

**Administrative Native VLAN tagging: enabled**

**(output omitted)**

Some Cisco switches have a proprietary protocol that lets them automatically negotiate trunking with a neighboring device. This protocol is called Dynamic Trunking Protocol (DTP). DTP can speed up the configuration process for a network administrator. Ethernet trunk interfaces support different trunking modes. An interface can be set to trunking or nontrunking, or to negotiate trunking with the neighbor interface. Trunk negotiation is managed by DTP, which operates on a point-to-point basis only, between network devices.

DTP is a Cisco proprietary protocol that is automatically enabled on Catalyst 2960 and Catalyst 3650 Series switches. DTP manages trunk negotiation only if the port on the neighbor switch is configured in a trunk mode that supports DTP. Switches from other vendors do not support DTP.

**Caution:** Some internetworking devices might forward DTP frames improperly, which can cause misconfigurations. To avoid this, turn off DTP on Cisco switch interfaces that are connected to devices that do not support DTP.

The default DTP configuration for Cisco Catalyst 2960 and 3650 switches is dynamic auto.

To enable trunking from a Cisco switch to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration mode commands. This causes the interface to become a trunk, but it will not generate DTP frames.

S1(config-if)# **switchport mode trunk**

S1(config-if)# **switchport nonegotiate**

To re-enable dynamic trunking protocol use the **switchport mode dynamic** **auto** command.

S1(config-if)# **switchport mode dynamic auto**

If the ports connecting two switches are configured to ignore all DTP advertisements with the **switchport mode trunk** and the **switchport nonegotiate** commands, the ports will stay in trunk port mode. If the connecting ports are set to dynamic auto, they will not negotiate a trunk and will stay in the access mode state, creating an inactive trunk link.

When configuring a port to be in trunk mode, use the **switchport mode trunk** command. Then there is no ambiguity about which state the trunk is in; it is always on.

**3.5.2 Negotiated Interface Modes**

The **switchport mode** command has additional options for negotiating the interface mode. The full command syntax is the following:

Switch(config-if)# **switchport mode** { **access** | **dynamic** { **auto** | **desirable** } | **trunk** }

The options are described in the table.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Use the **switchport nonegotiate** interface configuration command to stop DTP negotiation. The switch does not engage in DTP negotiation on this interface. You can use this command only when the interface switchport mode is **access** or **trunk**. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

**3.5.3 Results of a DTP Configuration**

The table illustrates the results of the DTP configuration options on opposite ends of a trunk link connected to Catalyst 2960 switch ports. Best practice is to configure trunk links statically whenever possible.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**3.5.4 Verify DTP Mode**

The default DTP mode is dependent on the Cisco IOS Software version and on the platform. To determine the current DTP mode, issue the **show dtp interface** command as shown in the output.

S1# **show dtp interface fa0/1**

DTP information for FastEthernet0/1:

TOS/TAS/TNS: ACCESS/AUTO/ACCESS

TOT/TAT/TNT: NATIVE/NEGOTIATE/NATIVE

Neighbor address 1: C80084AEF101

Neighbor address 2: 000000000000

Hello timer expiration (sec/state): 11/RUNNING

Access timer expiration (sec/state): never/STOPPED

Negotiation timer expiration (sec/state): never/STOPPED

Multidrop timer expiration (sec/state): never/STOPPED

FSM state: S2:ACCESS

# times multi & trunk 0

Enabled: yes

In STP: no

**Note:** A general best practice is to set the interface to **trunk** and **nonegotiate** when a trunk link is required. On links where trunking is not intended, DTP should be turned off.