Configuring ISL Trunking on Catalyst 5500/5000 and 6500/6000 Family Switches

Document ID: 10682

Introduction

This document illustrates how to create a switch−to−switch Inter−Switch Link (ISL) trunk. Trunk ports enable connections between switches to carry traffic from more than one VLAN. If trunking is not enabled, the link that connects the two switches only carries traffic from the VLAN that you have configured on the port. Trunking is not necessary in very simple switched networks with only one VLAN (broadcast domain). In most LANs, a small portion of traffic consists of special protocols that manage the network. (A few examples are Cisco Discovery Protocol [CDP], VLAN Trunk Protocol [VTP], Dynamic Trunking Protocol [DTP], Spanning Tree Protocol [STP], and Port Aggregation Protocol [PAgP].) You also use the management VLAN when you ping or establish a Telnet directly to or from the switch. (If you use Catalyst OS [CatOS], you define the VLAN and the IP address of the switch when you configure the sc0 interface. The Step−by−Step Instructions for CatOS section of this document explains this process.) In a multi−VLAN environment, many network administrators advocate the restriction of this management traffic to a single VLAN. The VLAN is normally VLAN 1. The administrators then configure user traffic to flow in VLANs other than this default VLAN. ISL (Cisco proprietary) is one of two possible trunking protocols for Ethernet. The other protocol is the IEEE 802.1Q standard.

This document covers the procedure to configure ISL trunking between Catalyst 5500/5000 and Catalyst 6500/6000 series switches. The CatOS configuration applies to both Catalyst 5500/5000 and 6500/6000 series switches. However, you can only apply the Cisco IOS® Software configuration to a Catalyst 6500/6000 series switch.

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

The information in this document is based on these software and hardware versions:

- at least one terminal.
- at least one console cable that is suitable for the Supervisor Engine in your switches. (Refer to the document Connecting a Terminal to the Console Port on Catalyst Switches for more information.)
- two Catalyst 5500/5000 or Catalyst 6500/6000 switches (that run CatOS) or two Catalyst 6500/6000 switches (that run Cisco IOS Software) in a lab[1] environment with cleared configurations[2].
- two Ethernet interfaces that are able to support ISL.
- one 10BASE–T crossover cable.

[1]The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

[2] For CatOS, the issue of the **clear config all** command ensured that there was a default configuration. For Cisco IOS Software, the **write erase** command cleared the configuration.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

# Creation of a Switch–to–Switch ISL Trunk

Switches A and B in this topology represent either two Catalyst 5500/5000 switches that run CatOS or two Catalyst 6500/6000 switches that run Cisco IOS Software.
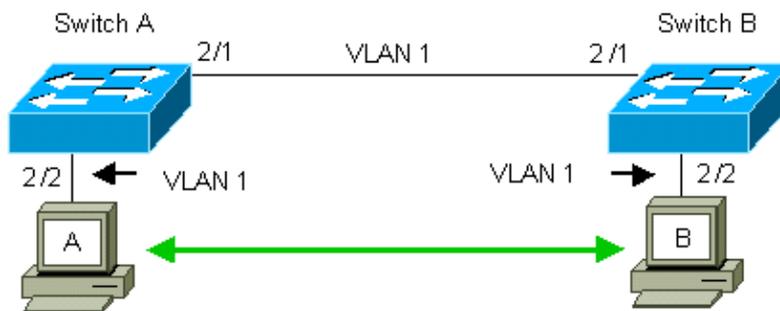
Switches A and B, by default, have the 2/1 ports in VLAN 1. This configuration allows traffic from other ports in VLAN 1 to flow between the switches without the need to configure trunking. References to "the management VLAN" apply to VLAN 1.

Note: VLAN 1 is the default VLAN for all types of Ethernet interfaces, as well as FDDI. VLAN 1 is also the default VLAN for the management interface (sc0).

In the example that follows, you have configured ports 2/2 on both switches in VLAN 2. Traffic from devices that you have attached to the ports in VLAN 2 do not cross over the link between the switches. Therefore, PCs A and B are not able to communicate.
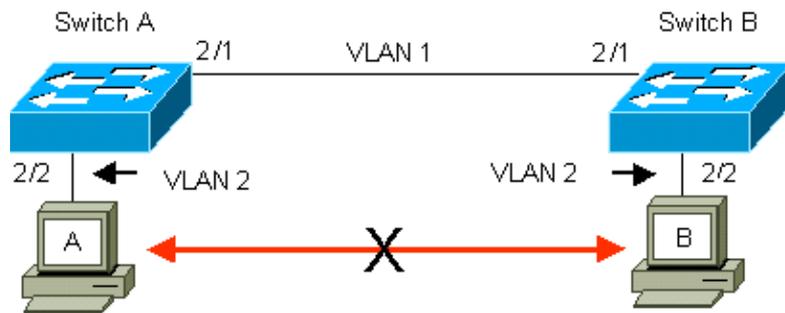
The solution is to enable ISL trunking on the link between switches A and B. Trunking adds a VLAN header to each frame during transmit (multiplex) onto a trunk link. This addition allows the switch at the other end of the link to demultiplex the frames; the switch then forwards the frames to the appropriate VLAN ports.
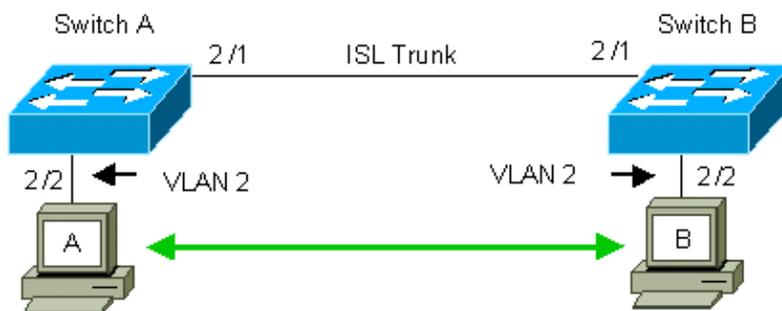
Tasks

These steps guide you through this configuration:

1. Connect a terminal to the switches.
2. Verify ISL support on the ports.
3. Connect the switches.
4. Verify that the ports are operational.
5. Assign IP addresses to the management ports.
6. Verify that the switches are not trunking over the link.
7. Ping from switch to switch.
8. Create a VLAN 2 in each switch.
9. Move the management interface (sc0) to VLAN 2 (for CatOS).
10. Verify that you cannot ping from switch to switch.
11. Configure the same VTP domain name in each switch.
12. Enable trunking between the switches.
13. Verify that the switches are trunking over the link.
14. Ping from switch to switch.

Step−by−Step Instructions for CatOS

Follow these steps:

1. Connect a terminal to the console ports of the switches.

   For more information, refer to this document:

      ♦ Connecting a Terminal to the Console Port on Catalyst Switches
2. Make certain that the ports that you have decided to use support ISL trunking.

There are several types of Ethernet interfaces that support ISL trunking. The 10BASE–T (common Ethernet) ports do not support trunking, while most 100BASE–T (Fast Ethernet) ports do support trunking.

Issue the **show port capabilities** *module_number | module_number/port_number* command on both switches to determine if the ports you use support ISL.

Note: In this example, the command specifies the port designator 2/1. This limits the response to the information that is directly applicable.

```
cat5000> (enable) show port capabilities 2/1
Model                  WS-X5234
Port                   2/1
Type                   10/100BaseTX
Speed                  auto,10,100
Duplex                 half,full
Trunk encap type       802.1Q,ISL
Trunk mode             on,off,desirable,auto,nonegotiate
Channel                2/1-2,2/1-4
Broadcast suppression  percentage(0-100)
Flow control           receive-(off,on),send-(off,on)
Security               yes
Membership             static,dynamic
Fast start             yes
QOS scheduling         rx-(none),TX(1q4t)
COs rewrite            yes
ToS rewrite            IP-Precedence
Rewrite                yes
UDLD                   yes
AuxiliaryVlan          1..1000,1025..4094,untagged,dot1p,none
SPAN                   source,destination
```

3. Connect the two switch ports together with the Ethernet crossover cable.

   In this example, the Switch A 2/1 port connects to the Switch B 2/1 port.
4. To verify that the ports are operational, issue the **show port 2/1** command on Switch A.

```
Switch-A> (enable) show port 2/1
Port  Name               Status     VLAN       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
2/1                      connected  1                 normal a-full a-100 10/100BaseTX

Switch-A> (enable)
```

5. Issue the **set interface sc0 172.16.84.17 255.255.255.0 172.16.84.255** command on Switch A and the **set interface sc0 172.16.84.18 255.255.255.0 172.16.84.255** command on Switch B.

   These commands assign IP addresses from the same subnet to the management ports on both switches. You may also need to specify in the command the VLAN for sc0 (the management VLAN). Include this VLAN if the VLAN is different than the default (VLAN 1).

```
Switch-> (enable) set interface sc0 172.16.84.17 255.255.255.0 172.16.84.255
Interface sc0 IP address, netmask, and broadcast set.
Switch-A> (enable)
```

   If you have the output of a **show interfaces** command from your Cisco device, you can use the Output Interpreter Tool ⬚ (registered customers only) to display potential issues and fixes.
6. To verify that the link between switches A and B is not trunking, issue the **show trunk 2/1** command on Switch A.

```
Switch-A> (enable) show trunk 2/1
```

```
Port      Mode         Encapsulation  Status        Native VLAN
--------  -----------  -------------  ------------  -----------
2/1       auto         isl            not-trunking 1

Port       VLANs allowed on trunk
--------  --------------------------------------------------------------------
2/1       1-1005

Port       VLANs allowed and active in management domain
--------  --------------------------------------------------------------------
2/1       1

Port       VLANs in spanning tree forwarding state and not pruned
--------  --------------------------------------------------------------------
2/1       1
Switch-A> (enable)
```

Note: The term `Native VLAN` in this output indicates the VLAN placement of this port when the port is not in trunking mode. If you have configured the port for 802.1Q trunking, the `Native VLAN` field also indicates the VLAN for which the frames have no tags; all others have tags. (Conversely, with ISL trunking, every data frame has the appropriate VLAN identifier.)

The trunking status should be `not-trunking` because the default mode for the DTP is `auto`. DTP is the strategic replacement for Dynamic ISL (DISL) because DTP incorporates support for 802.1Q trunking negotiation. DTP is available in Catalyst software version 4.x and later, as well as in certain hardware modules. There are five different modes to which you can configure DTP. Cisco Technical Support recommends the configuration of desirable trunking mode on the ports of the trunk link. Step 12 discusses this information in more detail.

7. Ping Switch B from Switch A to verify that the switches can communicate over the link.

```
Switch-A> ping 172.16.84.18
172.16.84.18 is alive
Switch-A>
```

8. To create VLAN 2 in Switch A, issue the **set vlan 2** command on Switch A.

   Switch B learns about VLAN 2 after the establishment of the VTP domain in Step 11.

```
Switch-A> (enable) set vlan 2
Vlan 2 configuration successful
Switch-A> (enable)
```

9. Move the management interface in switches A and B to VLAN 2, which you created in Step 8.

   To change the interface, issue the **set interface sc0 2** command. This output shows the issue of the command on Switch A:

```
Switch-A> (enable) set interface sc0 2
Interface sc0 vlan set.
Switch-A> (enable)
```

   Issue the **show interfaces** command to view the change you just made. This output shows the issue of the command on Switch A. The output shows the new association of interface sc0 and VLAN 2:

```
Switch-A> (enable) show interfaces
sl0: flags=51<UP,POINTOPOINT,RUNNING>
slip 0.0.0.0 dest 0.0.0.0
sc0: flags=63<UP,BROADCAST,RUNNING>
vlan 2 inet 172.16.84.17 netmask 255.255.255.0 broadcast 172.16.84.255
Switch-A> (enable)
```

10. Attempt to ping Switch B from Switch A.

The ping should fail because the management ports are now in VLAN 2 while the link between the switches is in VLAN 1.

```
Switch-A> (enable) ping 172.16.84.18
no answer from 172.16.84.18
Switch-A> (enable)
```

11. Establish the same VTP domain for both switches.

    Issue the **set vtp domain Cookbook** command on both switches.

    Note: The name of the VTP domain is Cookbook.

    ```
    Switch-A> (enable) set vtp domain Cookbook
    VTP domain Cookbook modified
    Switch-A> (enable)
    ```

    If you have the output of a **show vtp domain** command from your Cisco device, you can use the Output Interpreter Tool ⬈ (registered customers only) to display potential issues and fixes.

12. Turn on trunking between the switches.

    To configure port 2/1 on Switch A for desirable mode, issue the **set trunk 2/1 desirable isl** command on Switch A. Switch B is in auto mode. Switch B automatically places the port 2/1 in trunking mode after completion of the DTP negotiation between the two switches.

    Note: Cisco Technical Support recommends the configuration of desirable trunking mode on the ports of the trunk link.

    ```
    Switch-A> (enable) set trunk 2/1 desirable isl
    Port(s) 2/1 trunk mode set to desirable.
    Port(s) 2/1 trunk type set to Isl.
    Switch-A> (enable)
    ```

    If you have the output of a **show trunk** command from your Cisco device, you can use the Output Interpreter Tool ⬈ (registered customers only) to display potential issues and fixes.

    This list describes the five different states for which you can configure DTP:

    ♦ **auto:** The port listens for DTP frames from the neighbor switch. If the neighbor switch indicates that the switch would like to be a trunk, or that the switch is a trunk, auto state creates the trunk with the neighbor switch. The auto state does not propagate any intent to become a trunk; auto state is solely dependent on the neighbor switch to make the trunking decision.
    ♦ **desirable:** DTP is spoken to the neighbor switch to which you want to establish an ISL trunk. The switch with desirable configuration communicates that the switch is able to be an ISL trunk and wants the neighbor switch to also be an ISL trunk. Cisco Technical Support recommends the configuration of desirable trunking mode on the ports of the trunk link.
    ♦ **on:** DTP is spoken to the neighbor switch. The on state automatically enables ISL trunking on the port, regardless of the state of the neighbor switch. The port remains an ISL trunk unless the port receives an ISL packet that explicitly disables the ISL trunk.
    ♦ **nonegotiate:** DTP is not spoken to the neighbor switch. The nonegotiate state automatically enables ISL trunking on the port, regardless of the state of the neighbor switch.
    ♦ **off:** There can be no use of ISL on this port, regardless of the configuration of DTP mode on the other switch port.

    This table shows the 15 possible, unique combinations of DTP modes. The table also shows whether the combinations result in an active bidirectional trunk. While theoretically you can trunk in one direction on a link and not in the other direction, you should not perform this kind of trunking.

Switch A Port/Interface 2/1	Switch B Port/Interface 2/1	ISL Trunk Status
DTP mode auto	DTP mode auto	not–trunking
DTP mode desirable	DTP mode auto	trunking
DTP mode on	DTP mode auto	trunking
DTP mode nonegotiate	DTP mode auto	not–trunking
DTP mode off	DTP mode auto	not–trunking
DTP mode desirable (Cisco Technical Support recommended configuration)	DTP mode desirable (Cisco Technical Support recommended configuration)	trunking
DTP mode on	DTP mode desirable	trunking
DTP mode nonegotiate	DTP mode desirable	not–trunking
DTP mode off	DTP mode desirable	not–trunking
DTP mode on	DTP mode on	trunking
DTP mode nonegotiate	DTP mode on	trunking
DTP mode off	DTP mode on	not–trunking
DTP mode nonegotiate	DTP mode nonegotiate	trunking
DTP mode off	DTP mode nonegotiate	not–trunking
DTP mode off	DTP mode off	not–trunking

You may see other messages that relate to changes to the state of STP on the switch. These messages are not relevant to this document. Refer to the document Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches for more information on this protocol. Because you cleared the configurations in the switches to start, you have the defaults for the STP parameters. The default parameters of STP should provide the connectivity necessary for this document to succeed.

13. To verify the trunk link, issue the **show trunk 2/1** command at the prompt on Switch A.

```
Switch-A> (enable) show trunk 2/1
Port       Mode          Encapsulation  Status        Native VLAN
--------   -----------   -------------  ------------  -----------
2/1        desirable     isl            trunking      1

Port      VLANs allowed on trunk
--------  -----------------------------------------------------------------------
2/1       2,1002-1005

Port      VLANs allowed and active in management domain
--------  -----------------------------------------------------------------------
2/1       2,1002-1005

Port      VLANs in spanning tree forwarding state and not pruned
--------  -----------------------------------------------------------------------
```

```
2/1      2,1002-1005
Switch-A> (enable)
```

You should now see that trunking is operational.

Note: VLANs 1™005 are allowable on all trunk ports by default. You can clear VLAN 1 from the list of allowable VLANs. If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic, for example, CDP, VTP, PAgP, and DTP in VLAN 1. You cannot remove VLANs 1002™005. In CatOS versions earlier than 5.4(x), you cannot remove VLAN 1 from the trunk.

To limit the VLANs on a trunk in CatOS, clear them. Issue the **clear trunk 2/1 1–1001** command. To establish the allowable VLANs on the trunk, issue the **set trunk 2/1 2** command on Switch A.

```
Switch-A>(enable) clear trunk 2/1 1-1001
Removing Vlan(s) 1-1001 from allowed list.
Port 2/1 allowed vlans modified to 4.
Switch-A> (enable)

Switch-A>(enable) set trunk 2/1 2
Adding vlans 2 to allowed list.
Port(s) 2/1 allowed vlans modified to 5.
Switch-A>(enable)
```

In this output, notice the permission of only VLANs 1 and 2 on this trunk link now:

```
Switch-A> (enable) show trunk 2/1
Port      Mode          Encapsulation  Status        Native VLAN
--------  -----------   -------------  ------------  -----------
2/1       desirable     isl            trunking      1

Port      VLANs allowed on trunk
--------  ---------------------------------------------------------------------
2/1       1-1005

Port      VLANs allowed and active in management domain
--------  ---------------------------------------------------------------------
2/1       1-2

Port      VLANs in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
2/1       1-2
Switch-A> (enable)
```

14. Ping Switch B from Switch A to verify that the switches can communicate with each other over the trunk link.

```
Switch-A> ping 172.16.84.18
172.16.84.18 is alive
Switch-A>
```

Troubleshoot the Result

Commands to Use to Troubleshoot CatOS

- **show port capabilities** *mod/port* To see the physical status of a port and the port capabilities.
- **show trunk** *mod/port* To see the trunking information for a particular port.
- **show vtp domain** To display VTP information.
- **show vlan** *vlan_number* To see information on a particular VLAN.
- **show spantree** *vlan_number* To see the status of the spanning tree for a particular VLAN.

- **show interfaces** To display the configuration of sc0 and sl0.
- **ping** To send an Internet Control Message Protocol (ICMP) echo message to another IP host.

Note: In switches with several interfaces and VLANs, include the module/port or VLAN number with the **show** command to restrict the command output. Use of the **?** argument with **show** commands displays which commands allow use of the **mod/port** argument. For example, the **show trunk ?** command indicates that **show trunk mod/port** is allowable.

Step−by−Step Instructions for Cisco IOS Software

Follow these steps:

1. Connect a terminal to the console ports of the switches.

   For more information, refer to this document:

   ♦ Connecting a Terminal to the Console Port on Catalyst Switches
2. Make certain that the ports that you have decided to use support ISL trunking.

   There is currently no command available to view the module or port capabilities in Cisco IOS Software. All 10/100BASE−T, 1000BASE−TX, 100BASE−FX, and 1000BASE−SX/LX/ZX−type Ethernet modules for the Catalyst 6500/6000 series switches support ISL trunking.

   Note: The 10−Gigabit Ethernet switching module (WS−X6501−10GEX4) does not support ISL encapsulation.
3. Connect the two switch ports together with the Ethernet crossover cable.

   In this example, the Switch A 2/1 port connects to the Switch B 2/1 port.
4. To verify that the ports are operational, issue the **show interfaces fastethernet 2/1 status** command.

   The command displays this information:

   ```
   Switch-A# show interfaces fastethernet 2/1 status

   Port    Name                 Status      VLAN       Duplex  Speed Type
   Fa2/1                        connected   1           a-full  a-100 10/100BaseTX
   Switch-A#
   ```
5. Configure a VLAN interface on both switches A and B.

   In the global configuration mode, issue the command **interface vlan 1**. When you configure the IP address, issue the command **ip address 172.16.84.17 255.255.255.0** on Switch A and **ip address 172.16.84.17 255.255.255.0** on Switch B. To configure the switchport 2/1 as a Layer 2 (L2) interface and a member of VLAN 1, issue the commands **interface fastethernet 3/1**, **switchport**, and **switchport access vlan 1**. For more information on the configuration of L2 interfaces in Cisco IOS Software, refer to this document:

   ♦ Configuring Layer 2 Ethernet Interfaces
   ```
   Switch-A(config)# interface vlan 1
   Switch-A(config-if)# ip address 172.16.84.17 255.255.255.0
   Switch-A(config-if)#

   Switch-A(config)# interface fastethernet 2/1
   Switch-A(config-if)# switchport
   Switch-A(config-if)# switchport access vlan 1
   Switch-A(config-if)#
   ```

6. To verify that the link between switches A and B is not trunking, issue the command **show interfaces fastethernet 2/1 trunk**.

```
Switch-A# show interfaces fastethernet 2/1 trunk

Port      Mode            Encapsulation  Status        Native VLAN
Fa2/1     desirable       negotiate      not-trunking  1

Port      VLANs allowed on trunk
Fa2/1     none

Port      VLANs allowed and active in management domain
Fa2/1     none

Port      VLANs in spanning tree forwarding state and not pruned
Fa2/1     none
Switch-A#
```

Note: The term `Native VLAN` in this output indicates the VLAN placement of this port when the port is not in trunking mode. If you have configured the port for 802.1Q trunking, the `Native VLAN` field also indicates the VLAN for which the frames have no tags; all others have tags. (Conversely, with ISL trunking, every data frame has the appropriate VLAN identifier.)

7. Ping Switch B from Switch A to verify that the switches can communicate over the link.

```
Switch-A> ping 66.123.210.122
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.84.18, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/21/92 ms
Switch-A>
```

8. To create VLAN 2 in Switch A, issue the **vlan database** command and the **vlan 2** command on Switch A.

Switch B learns about VLAN 2 after the establishment of the VTP domain in Step 11. For more information on the configuration of VLANs in Cisco IOS Software code, refer to this document:

   ♦ Configuring VLANs

```
Switch-A# vlan database
Switch-A(vlan)# vlan 2
VLAN 2 added:
Name: VLAN0002
Switch-A(vlan)#exit
APPLY completed.
Exiting....
Switch-A#
```

9. Move the management interface on switches A and B to VLAN 2, which you created in Step 8.

In Cisco IOS Software mode, there is no sc0 management interface. Therefore, configure the ports, which connect to host A on Switch A and host B on Switch B, to VLAN 2. Issue the commands **switchport** and **switchport access vlan 2**. Then, use the hosts to perform the ping tests. For this example, configure IP addresses **172.16.85.1/24** on host A and **172.16.85.2/24** on host B.

```
Switch-A(config)# interface fastethernet 2/2
Switch-A(config-if)# switchport
Switch-A(config-if)# switchport access vlan 2
```

Issue the **show interfaces** command to view the change you just made. This output shows the issue of the command on Switch A. The output shows the new association of interface 2/2 and VLAN 2:

```
Switch-A# show interfaces fastethernet 2/2  switchport
Name: Fa2/2
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: up
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 2 (VLAN0002)
Switch-A# show interfaces fastethernet 2/2  switchport
Name: Fa2/2
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: up
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 2 (VLAN0002)

!--- Output suppressed.
```

10. Attempt to ping the host that connects to the alternate switch.

    The ping should fail because the ports are now in VLAN 2 while the link between the switches is in VLAN 1.

    ```
    C:\> ping 172.16.85.1
    Pinging 172.16.85.1 with 32 bytes of data:

    Request timed out.
    Request timed out.
    Request timed out.
    Request timed out.

    Ping statistics for 172.16.85.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

    C:\>
    ```

11. Establish the same VTP domain for both switches.

    Issue the **vtp domain Cookbook** command in global configuration mode.

    Note: The name of the VTP domain is Cookbook.

    For more information on the configuration of VTP parameters with Cisco IOS Software, refer to this document:

    ♦ Configuring VTP

        ```
        Switch-A(config)# vtp domain Cookbook
        Changing VTP domain name from NULL to cookbook
        Switch-A(config)#
        ```

12. Turn on trunking between the switches.

    Configure port 2/1 on Switch A for desirable mode. To configure the encapsulation type and the mode, issue the **switchport trunk encapsulation isl** command and the **switchport mode dynamic desirable** command. Switch B is in auto mode. Switch B automatically places the port 2/1 in trunking mode after completion of the DTP negotiation between the two switches.

Note: Cisco Technical Support recommends the configuration of desirable trunking mode on the ports of the trunk link.

```
Switch-A(config)# interface fastethernet 2/1
Switch-A(config-if)# switchport trunk encapsulation isl
Switch-A(config-if)# switchport mode dynamic desirable
```

This list describes the five different states for which you can configure DTP:

- **auto:** The port listens for DTP frames from the neighbor switch. If the neighbor switch indicates that the switch would like to be a trunk, or that the switch is a trunk, auto state creates the trunk with the neighbor switch. The auto state does not propagate any intent to become a trunk; auto state is solely dependent on the neighbor switch to make the trunking decision.
- **desirable:** DTP is spoken to the neighbor switch to which you want to establish an ISL trunk. The switch with desirable configuration communicates that the switch is able to be an ISL trunk and wants the neighbor switch to also be an ISL trunk.
- **on:** DTP is spoken to the neighbor switch. The on state automatically enables ISL trunking on the port, regardless of the state of the neighbor switch. The port remains an ISL trunk unless the port receives an ISL packet that explicitly disables the ISL trunk. Cisco Technical Support recommends the configuration of desirable trunking mode on the ports.
- **nonegotiate:** DTP is not spoken to the neighbor switch. The nonegotiate state automatically enables ISL trunking on the port, regardless of the state of the neighbor switch.
- **off:** There can be no use of ISL on this port, regardless of the configuration of DTP mode on the other switch port.

This table shows the 15 possible, unique combinations of DTP modes. The table also shows whether the combinations result in an active bidirectional trunk. While theoretically you can trunk in one direction on a link and not in the other direction, you should not perform this kind of trunking.

Switch A Port/Interface 2/1	Switch B Port/Interface 2/1	ISL Trunk Status
DTP mode auto	DTP mode auto	not−trunking
DTP mode desirable	DTP mode auto	trunking
DTP mode on	DTP mode auto	trunking
DTP mode nonegotiate	DTP mode auto	not−trunking
DTP mode off	DTP mode auto	not−trunking
DTP mode desirable (Cisco Technical Support recommended configuration)	DTP mode desirable (Cisco Technical Support recommended configuration)	trunking
DTP mode on	DTP mode desirable	trunking
DTP mode nonegotiate	DTP mode desirable	not−trunking
DTP mode off	DTP mode desirable	not−trunking
DTP mode on	DTP mode on	trunking
DTP mode nonegotiate	DTP mode on	trunking

DTP mode off	DTP mode on	not–trunking
DTP mode nonegotiate	trunking	trunking
DTP mode off	DTP mode nonegotiate	not–trunking
DTP mode off	DTP mode off	not–trunking

You may see other messages that relate to changes to the state of STP on the switch. These messages are not relevant to this document. Refer to the document Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches for more information on this protocol. Because you cleared the configurations in the switches to start, you have the defaults for the STP parameters. The default parameters of STP should provide the connectivity necessary for this document to succeed.

13. To verify the trunk, issue the **show interfaces fastethernet 2/1 trunk** command.

```
Switch-A# show interfaces fastethernet 2/1 trunk

Port        Mode            Encapsulation  Status        Native VLAN
Fa2/1       desirable       isl            trunking      1

Port        VLANs allowed on trunk
Fa2/1       1-1005

Port        VLANs allowed and active in management domain
Fa2/1       1-2,1002-1005

Port        VLANs in spanning tree forwarding state and not pruned
Fa2/1       1-2,1002-1005
```

You should now see that trunking is operational.

Note: VLANs 1™005 are allowable on all trunk ports by default. You can clear VLAN 1 from the list of allowable VLANs. If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic, for example, CDP, VTP, PAgP, and DTP in VLAN 1.

To limit or remove VLANs on a trunk, issue the **switchport trunk allowed vlan remove 1–1001** command in interface configuration mode. The command removes all removable VLANs from the trunk. Issue the **switchport trunk allowed vlan add 2** command to add VLAN 2 to the list of allowable VLANs on the trunk.

```
Switch-A(config-if)# switchport trunk allowed vlan remove 1-1001
Switch-A(config-if)#

Switch-A(config-if)# switchport trunk allowed vlan add 2
Switch-A(config-if)#
```

In this output, notice the permission of only VLANs 2 and 1002™005 on the trunk:

```
Switch-A# show interfaces fastethernet 2/1 trunk

Port        Mode            Encapsulation  Status        Native VLAN
Fa2/1       desirable       isl            2,1002-1005   1

Port        VLANs allowed on trunk
Fa2/1       2,1002-1005

Port        VLANs allowed and active in management domain
```

```
Fa2/1      2,1002-1005

Port       VLANs in spanning tree forwarding state and not pruned
Fa2/1      2,1002-1005
```

14. To verify that the trunk link is operational, attempt to ping across the trunk link.

Ping host A from host B to verify connectivity over VLAN 2.

```
C:\> ping 172.16.85.1

Pinging 172.16.85.1 with 32 bytes of data:

Reply from 172.16.85.1: bytes=32 time<10ms TTL=255
Reply from 172.16.85.1: bytes=32 time<10ms TTL=255
Reply from 172.16.85.1: bytes=32 time<10ms TTL=255
Reply from 172.16.85.1: bytes=32 time<10ms TTL=255

Ping statistics for 172.16.85.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>
```

Troubleshoot the Result

Commands to Use to Troubleshoot Cisco IOS Software

- **show interfaces fastethernet** *port/mod* **trunk** To see the trunking information for a particular interface.
- **show vtp status** To display VTP information.
- **show vlan** *vlan_number* To see information on a particular VLAN.
- **show spanning−tree vlan** *vlan_number* To see the status of the spanning tree for a particular VLAN.
- **show interfaces fastethernet** *port/mod* **switchport** To see L2 interface information.
- **ping** To send an ICMP echo message to another IP host.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for LAN
Network Infrastructure: LAN Routing and Switching
Network Infrastructure: Getting Started with LANs

Related Information

- **LAN Product Support**
- **LAN Switching Technology Support**
- **Technical Support & Documentation – Cisco Systems**