CHAPTER 39

Configuring FDDI/CDDI Switching

This chapter describes how to configure Fiber Distributed Data Interface/Copper Distributed Data Interface (FDDI/CDDI) switching.

Note For complete information on installing Catalyst 5000 family FDDI/CDDI modules, refer to the *Catalyst 5000 Family Module Installation Guide*.

Note For information on configuring FDDI IEEE 802.10 VLAN trunks, see Chapter 40, "Configuring FDDI 802.10 Trunks."

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference* publication for your switch.

This chapter consists of these sections:

- Understanding How FDDI Switching Works, page 39-1
- Default FDDI/CDDI Configuration, page 39-2
- Configuring FDDI/CDDI Switching, page 39-2
- FDDI/CDDI Switching Configuration Examples, page 39-15

Understanding How FDDI Switching Works

FDDI is a LAN standard, defined by ANSI X3T9.5, specifying a 100-Mbps, token-passing network using fiber-optic cable, with transmission distances of up to 2 kilometers (km). FDDI uses a dual-ring architecture to provide redundancy. CDDI is the implementation of FDDI protocols over shielded twisted-pair (STP) and unshielded twisted-pair (UTP) cabling. CDDI transmits at data rates of 100 Mbps over relatively short distances (about 100 meters), also using a dual-ring architecture to provide redundancy.

The Catalyst 5000 family FDDI module functions as an FDDI-Ethernet translation bridge. It translates packets on the external FDDI ring into Ethernet packets within the Catalyst 5000 family switch. Inside a Catalyst 5000 family switch, Ethernet virtual LAN (VLAN) packets are translated into FDDI VLAN packets and encoded in 802.10 format with a Security Association Identifier (SAID) value before they are transmitted across an external FDDI trunk to another switch.

The switch that receives the packets from the trunk decodes the 802.10 format using the SAID value and internally translates the FDDI VLAN packets into Ethernet VLAN packets. Each Ethernet VLAN requires a corresponding, unique FDDI VLAN for translation.

Note When you insert or replace FDDI modules in the switch, clear the module configuration information using the command **clear config** *mod_num* (where *mod_num* is the FDDI slot number) to obtain the correct spanning-tree parameters for the modules.

Default FDDI/CDDI Configuration

Table 39-1 shows the FDDI/CDDI default configuration.

Table 39-1 FDDI/CDDI Default Configuration

Feature	Default Value
Port enable state	All ports are enabled
User-data string	Catalyst 5000
IP fragmentation	Enabled
ICMP unreachable message	Enabled
Native VLAN	VLAN 1
Ethernet-FDDI mapping	None
TL_MIN	40 microseconds
TNotify	30 seconds
TRequest	165,000 microseconds
LER-Alarm	8 (10^{-8})
LER-Cutoff	7 (10^{-7})
Novell IPX[1] protocol translations	• FDDI SNAP[2] to Ethernet 802.3 RAW • FDDI 802.2 to Ethernet 802.3 • Ethernet 802.3 RAW to FDDI SNAP

1. IPX=Internetwork Packet Exchange
2. SNAP=Subnetwork Access Protocol

Configuring FDDI/CDDI Switching

These sections describe how to configure FDDI/CDDI switching:

- Specifying the User-Data String, page 39-3
- Setting the Port Name, page 39-4
- Setting the Port Priority Level, page 39-4
- Setting the Native VLAN on FDDI, page 39-5
- Configuring IP Fragmentation, page 39-6

- Configuring ICMP Unreachable Messages, page 39-6
- Setting the Link Error Rate Alarm, page 39-7
- Setting the Link Error Rate Cutoff, page 39-8
- Setting the Interval between Neighbor Notification Frames, page 39-8
- Setting the Minimum Time to Transfer the FDDI PHY Line State, page 39-9
- Setting the Timer for Negotiating Token Ring Timer, page 39-10
- Setting the Default Internet Packet Exchange Protocol Translations, page 39-10
- Configuring APaRT, page 39-12
- Configuring MAC Address Learning, page 39-14
- Checking Connectivity, page 39-15

Specifying the User-Data String

The user-data string identifies the user-data string in the Station Management (SMT) Management Information Base (MIB) of an FDDI module. The default value is *Catalyst 5000*. You should modify this value to a more meaningful description.

To modify the user-data string, perform this task in privileged mode:

	Task	Command
Step 1	Enter a module number and a unique description or name to identify the FDDI module.	**set fddi userdata** *mod_num userdata_string*
Step 2	Verify the user-data string setting.	**show fddi**

This example shows how to set the user-data string and verify the setting:

```
Console> (enable) set fddi userdata 4 Engineering
Module 4 userdata set to Engineering.
Console> (enable) show fddi
Mod  SMT User-Data               T-Notify  TReq
---  --------------------------  --------  -------
4    Engineering                 15        3500
5    abc                         20        150000

Port   Tlmin     Ler-CutOff  Ler-Alarm
-----  --------  ----------  ---------
4/1    40        10          11
4/2    40        10          11
5/1    40        10          11
5/2    40        9           12
Console> (enable)
```

Setting the Port Name

To set an FDDI/CDDI port name, perform this task in privileged mode:

	Task	Command
Step 1	Configure a name for a port.	**set port name** *mod_num/port_num* [*name_string*]
Step 2	Verify the port name assignment.	**show port** [*mod_num*[*/port_num*]]

This example shows how to set the name of a port and verify the configuration:

```
Console> (enable) set port name 4/1 FDDI Backbone
Port 4/1 name set.
Console> (enable) show port 4
Port Name                 Status   Vlan       Level  Duplex Speed  Type
---- -------------------- -------- ---------- ------ ------ -----  ------------
4/1   FDDI Backbone       connect  1                 half   100    FDDI
4/2                       standby  1                 half   100    FDDI
       Ler
Port CE-State Conn-State Type Neig Con Est Alm Cut Lem-Ct     Lem-Rej-Ct Tl-Min
---- -------- ---------- ---- ---- --------------- ---------- ---------- ------
4/1  isolated active     B    U    yes   9  11  10          0          0 1340000
4/2  isolated standby    A    U    yes   9  11  10          0          0 40
Last-Time-Cleared
--------------------------
Fri May 1 1998, 18:28:51
Console> (enable)
```

Setting the Port Priority Level

When ports request simultaneous access to the switching bus, the switch uses the port priority level to determine the order in which ports have access to the switching bus.

To set the priority level, enter this command in privileged mode:

	Task	Command
Step 1	Configure the priority level for each CDDI or FDDI port.	**set port level** *mod_num/port_num* **normal** | **high**
Step 2	Verify the port priority configuration.	**show port** [*mod_num*[*/port_num*]]

This example shows how to set the port priority of an FDDI/CDDI port to high and verify the configuration:

```
Console> (enable) set port level 4/1 high
Port 4/1 level set to high.
Console> (enable) show port 4
Port Name                 Status   Vlan       Level  Duplex Speed  Type
---- -------------------- -------- ---------- ------ ------ -----  ------------
4/1   FDDI Backbone       connect  1          high   half   100    FDDI
4/2                       standby  1                 half   100    FDDI
       Ler
Port CE-State Conn-State Type Neig Con Est Alm Cut Lem-Ct     Lem-Rej-Ct Tl-Min
---- -------- ---------- ---- ---- --------------- ---------- ---------- ------
4/1  isolated active     B    U    yes   9  11  10          0          0 1340000
4/2  isolated standby    A    U    yes   9  11  10          0          0 40
Last-Time-Cleared
--------------------------
Fri May 1 1998, 18:28:51
Console> (enable)
```

Setting the Native VLAN on FDDI

To assign an Ethernet VLAN to map to the native VLAN on an FDDI port, perform the following task. The native VLAN must be an Ethernet type. The FDDI module translates all native (non-802.10) FDDI traffic to the assigned Ethernet VLAN.

To set up a native VLAN on FDDI, perform this task in privileged mode:

	Task	Command
Step 1	Assign a VLAN to map to native traffic on an FDDI port. The VLAN specified must be an Ethernet type VLAN.	**set vlan** *vlan_num mod_num/port_num*
Step 2	Verify the VLAN configuration.	**show vlan**

This example shows how to set VLAN 50 as the native VLAN for FDDI port 4/1 and how to verify the configuration:

```
Console> (enable) set vlan 50 4/1
VLAN 50 modified.
VLAN 1 modified.
VLAN  Mod/Ports
----  ----------------------
50    4/1

Console> (enable) show vlan 50
VLAN Name                        Type  Status    Mod/Ports
---- --------------------------- ----- --------- ----------------
50   VLAN0050                    enet  active    4/1-2


VLAN SAID       MTU   RingNo BridgeNo StpNo Parent Trans1 Trans2
---- ---------- ----- ------ -------- ----- ------ ------ ------
50   100050     1500  0      0        0     0      0      0
Console> (enable)
```

Configuring IP Fragmentation

IP fragmentation allows the switch to fragment large FDDI IP frames (frames greater than 1514 bytes) into multiple smaller packets so that they can be transmitted on an Ethernet segment. IP fragmentation is enabled by default.

If you disable IP fragmentation, large IP packets are dropped instead of fragmented and forwarded.

To disable IP fragmentation, perform this task in privileged mode:

	Task	Command
Step 1	Disable IP fragmentation.	**set ip fragmentation disable**
Step 2	Verify that IP fragmentation is disabled.	**show ip route**

After entering the **set ip fragmentation disable** command, you see this display:

```
Console> (enable) set ip fragmentation disable
IP fragmentation disabled for module 4
Console> (enable) show ip route
Fragmentation   Redirect   Unreachable
-------------   --------   -----------
disabled        enabled    disabled
The primary gateway: 172.16.52.65
Destination             Gateway                 Flags   Use          Interface
----------------------- ----------------------- ------  ----------   ---------
default                 172.16.52.65            UG            8761   sc0
172.16.52.64            172.16.52.70            U             9734   sc0
default                 default                 UH               0   sl0
Console> (enable)
```

To enable IP fragmentation, perform this task in privileged mode:

	Task	Command
Step 1	Enable IP fragmentation.	**set ip fragmentation enable**
Step 2	Verify that IP fragmentation is enabled.	**show ip route**

Configuring ICMP Unreachable Messages

When you enable Internet Control Message Protocol (ICMP) unreachable messages, the switch returns an ICMP unreachable message to the Internet source host whenever it receives an IP datagram that it cannot deliver. When you disable ICMP unreachable messages, the switch does not notify the Internet source host when it receives an IP datagram that it cannot deliver. ICMP unreachable messages are enabled by default.

To disable ICMP unreachable messages, perform this task in privileged mode:

	Task	Command
Step 1	Disable ICMP unreachable messages.	**set ip unreachable disable**
Step 2	Verify that ICMP unreachable messages are disabled.	**show ip route**

This example shows how to disable ICMP unreachable messages and verify the configuration:

```
Console> (enable) set ip unreachable disable
ICMP Unreachable message disabled.
Console> (enable) show ip route
Fragmentation   Redirect   Unreachable
-------------   --------   -----------
enabled         enabled    disabled
The primary gateway: 172.16.52.65
Destination             Gateway                 Flags   Use         Interface
----------------------- ----------------------- ------  ----------  ---------
default                 172.16.52.65            UG            8761  sc0
172.16.52.64            172.16.52.70            U             9734  sc0
default                 default                 UH               0  sl0
Console> (enable)
```

To enable ICMP unreachable messages, perform this task in privileged mode:

	Task	Command
Step 1	Enable ICMP unreachable messages.	**set ip unreachable enable**
Step 2	Verify that ICMP unreachable messages are enabled.	**show ip route**

Setting the Link Error Rate Alarm

The link error rate (LER)-alarm value defines the LER at which a link connection exceeds a preset alarm threshold. This value is used in the LER threshold test. The default setting of 8 (10^{-8}) link errors per second is sufficient for most networks.

To modify the setting for the LER-alarm, perform this task in privileged mode:

	Task	Command
Step 1	Change the LER-alarm setting.	**set fddi alarm** *mod_num/port_num value*
Step 2	Verify the LER-alarm setting.	**show fddi**

This example shows how to change the LER-alarm setting to 11 (10^{-11}) and verify the configuration:

```
Console> (enable) set fddi alarm 4/1 11
Port 4/1 alarm value set to 11.
Console> (enable) show fddi
Mod  SMT User-Data               T-Notify  TReq
---  --------------------------  --------  -------
4    Engineering                 15        3500
5    abc                         20        150000

Port   Tlmin     Ler-CutOff  Ler-Alarm
-----  --------  ----------  ---------
4/1    40        10          11
4/2    40        10          8
5/1    40        10          8
5/2    40        9           8
Console> (enable)
```

Setting the Link Error Rate Cutoff

The LER-cutoff value determines the LER at which a connection is considered faulty. This value is used in the LER threshold test. The default setting of 7 (10^{-7}) is sufficient for most networks.

To modify the LER-cutoff setting, perform this task in privileged mode:

	Task	Command
Step 1	Change the LER-cutoff setting.	**set fddi cutoff** *mod_num/port_num value*
Step 2	Verify the LER-cutoff setting.	**show fddi**

This example shows how to change the LER-cutoff value to 10 (10^{-10}) and verify the configuration:

```
Console> (enable) set fddi cutoff 4/1 10
Port 4/1 cutoff value set to 10.
Console> (enable) show fddi
Mod  SMT User-Data               T-Notify  TReq
---  --------------------------  --------  -------
4    Engineering                 15        3500
5    abc                         20        150000

Port   Tlmin     Ler-CutOff  Ler-Alarm
-----  --------  ----------  ---------
4/1    40        10          11
4/2    40        7           8
5/1    40        7           8
5/2    40        7           8
Console> (enable)
```

Setting the Interval between Neighbor Notification Frames

The TNotify parameter sets the interval (in seconds) between neighbor notification frames. These frames are sent out to notify neighboring devices of FDDI module Media Access Control (MAC) addresses. Usually, the default of 30 seconds is sufficient. By shortening the interval, you cause more notification frames to be sent.

To adjust the interval between neighbor notification frames, perform this task in privileged mode:

	Task	Command
Step 1	Set TNotify to a value between 2 and 30 seconds.	**set fddi tnotify** *mod_num time*
Step 2	Verify the TNotify setting.	**show fddi**

This example shows how to change the TNotify setting to 15 and verify the configuration:

```
Console> (enable) set fddi tnotify 4 15
Module 4 tnotify set to 15.
Console> (enable) show fddi
Mod  SMT User-Data               T-Notify  TReq
---  --------------------------  --------  -------
4    Engineering                 15        3500
5    abc                         30        150000

Port   Tlmin     Ler-CutOff  Ler-Alarm
-----  --------  ----------  ---------
4/1    40        10          11
4/2    40        7           8
5/1    40        7           8
5/2    40        7           8
Console> (enable)
```

Setting the Minimum Time to Transfer the FDDI PHY Line State

The TL_MIN parameter sets the minimum time to transmit an FDDI physical sublayer (PHY) line state before advancing to the next physical connection management (PCM) state. This setting affects the station and switch interoperability and might hinder the implementation of FDDI repeaters. By default, the TL_MIN parameter is set to 40 microseconds. Normally, you do not need to adjust this parameter.

To set the minimum time to transmit a FDDI PHY line state, perform this task in privileged mode:

	Task	Command
Step 1	Set TL_MIN to a value between 40 and 1,340,006 microseconds.	**set fddi tlmin** *mod_num/port_num microseconds*
Step 2	Verify the TL_MIN setting.	**show fddi**

This example shows how to change the TL_MIN setting to 30 and verify the configuration:

```
Console> (enable) set fddi tlmin 4/1 30
Port 4/1 tlmin set to 30.
Console> (enable) show fddi
Mod  SMT User-Data               T-Notify  TReq
---  --------------------------  --------  -------
4    Engineering                 15        3500
5    abc                         30        150000

Port   Tlmin     Ler-CutOff  Ler-Alarm
-----  --------  ----------  ---------
4/1    30        10          11
4/2    40        7           8
5/1    40        7           8
5/2    40        7           8
Console> (enable)
```

Setting the Timer for Negotiating Token Ring Timer

The TRequest parameter specifies the required value for the Token Ring Timer (TRT) on the FDDI switch. The switch uses this value to negotiate the TRT with other stations. The TRT controls ring scheduling during normal operation and can help detect and recover from serious ring errors. Whenever the TRT value expires, the station uses the TRequest value to negotiate with other stations for the lowest value. The default setting of 165,000 microseconds is sufficient for most networks.

To modify the setting for the TRequest parameter, perform this task in privileged mode:

	Task	Command
Step 1	Set TRequest to a value between 2502 and 165,000 microseconds.	**set fddi trequest** *mod_num time*
Step 2	Verify the TRequest setting.	**show fddi**

After entering the **set fddi trequest** command, you see this display:

```
Console> (enable) set fddi trequest 4 3500
Mac 4/1 treq set to 3500.
Console> (enable) show fddi
Mod  SMT User-Data               T-Notify  TReq
---  --------------------------  --------  -------
4    Engineering                 15        3500
5    abc                         30        165000

Port   Tlmin     Ler-CutOff  Ler-Alarm
-----  --------  ----------  ---------
4/1    30        10          11
4/2    40        7           8
5/1    40        7           8
5/2    40        7           8
Console> (enable)
```

Setting the Default Internet Packet Exchange Protocol Translations

The Catalyst 5000 family switch can forward IPX packets received on FDDI ports to Ethernet ports, or it can forward IPX packets received on Ethernet ports to FDDI ports. To do this, you must configure the switch for specific IPX protocol translations. By default, these IPX protocol translations are configured as follows:

- FDDI SNAP to Ethernet 802.3 RAW
- FDDI 802.2 to Ethernet 802.3
- Ethernet 802.3 RAW to FDDI SNAP

If necessary, you can customize these settings to fit your environment.

Setting the FDDI SNAP-to-Ethernet Translation

FDDI SNAP frames can be translated into these Ethernet frames:

- Ethernet 802.3
- Ethernet SNAP

- Ethernet II
- Ethernet 802.3 RAW (default)

To specify the Ethernet frame type to which FDDI SNAP frames are translated, perform this task in privileged mode:

	Task	Command
Step 1	Configure the desired IPX translation for FDDI SNAP frames.	**set bridge ipx snaptoether** {**8023** | **snap** | **eii** | **8023raw**}
Step 2	Verify the IPX translation.	**show bridge**

This example shows how to specify FDDI SNAP-to-Ethernet 802.3 translation and verify the configuration:

```
Console> (enable) set bridge ipx snaptoether 8023
Bridge snaptoether default IPX translation set.
Console> (enable) show bridge
APaRT Enabled
FDDICHECK Disabled
IP fragmentation Enabled
Default IPX translations:
    FDDI SNAP  to Ethernet     8023
    FDDI 802.2 to Ethernet     8023
    Ethernet 802.3 Raw to FDDI snap
Console> (enable)
```

Setting the FDDI 802.2-to-Ethernet Translation

FDDI 802.2 frames can be translated into these Ethernet frames:

- Ethernet 802.3 (default)
- Ethernet SNAP
- Ethernet II
- Ethernet 802.3 RAW

To specify the Ethernet frame type to which FDDI 802.2 packets are translated, perform this task in privileged mode:

	Task	Command
Step 1	Configure the desired IPX translation for FDDI 802.2 frames.	**set bridge ipx 8022toether** {**8023** | **snap** | **eii** | **8023raw**}
Step 2	Verify the IPX translation.	**show bridge**

This example shows how to specify FDDI 802.2-to-Ethernet SNAP translation and verify the configuration:

```
Console> (enable) set bridge ipx 8022toether snap
8022 to ETHER translation set.
Console> (enable) show bridge
APaRT Enabled
FDDICHECK Disabled
IP fragmentation Enabled
Default IPX translations:
    FDDI SNAP  to Ethernet     8023
    FDDI 802.2 to Ethernet     snap
    Ethernet 802.3 Raw to FDDI snap
Console> (enable)
```

Setting the Ethernet 802.3 RAW-to-FDDI Protocol

Ethernet 802.3 RAW frames can be translated into these FDDI frames:

- FDDI 802.2
- FDDI SNAP (default)
- FDDI RAW

To specify the FDDI frame type to which Ethernet 802.3 RAW frames are translated, perform this task in privileged mode:

	Task	Command
Step 1	Configure the desired IPX translation for Ethernet 802.3 RAW frames.	**set bridge ipx 8023rawtofddi** {**8022** | **snap** | **fddiraw**}
Step 2	Verify the IPX translation.	**show bridge**

This example shows how to specify Ethernet 802.3 RAW-to-FDDI 802.2 translation and verify the configuration:

```
Console> (enable) set bridge ipx 8023rawtofddi 8022
8023RAW to FDDI translation set.
Console> (enable) show bridge
APaRT Enabled
FDDICHECK Disabled
IP fragmentation Enabled
Default IPX translations:
    FDDI SNAP  to Ethernet     8023
    FDDI 802.2 to Ethernet     snap
    Ethernet 802.3 Raw to FDDI 8022
Console> (enable)
```

Configuring APaRT

To increase throughput performance, you can disable the software content-addressable memory (CAM) of the FDDI module. The CAM stores IPX translation information to support Automatic Packet Recognition/Translation (APaRT). Disabling the CAM disables APaRT, which automatically disables **fddicheck**. When APaRT is disabled, you can configure FDDI-to-Ethernet translation values using the **set bridge ipx** command. However, the Enhanced Address Recognition Logic (EARL) CAM continues to provide packet forwarding functionality. To enable **fddicheck**, first enable APaRT.

Note There are serious drawbacks to disabling the CAM in the FDDI software that could impact system performance. When you disable APaRT, only default IPX translations are used. Also, FDDI module hardware filtering is disabled, and all traffic from the FDDI ring is translated and forwarded to the Catalyst 5000 family switch backplane before the EARL CAM can filter it.

To disable APaRT, perform this task in privileged mode:

	Task	Command
Step 1	Disable APaRT on the FDDI module.	**set bridge apart disable**
Step 2	Verify that APaRT is disabled.	**show bridge**

This example shows how to disable APaRT and verify the configuration:

```
Console> (enable) set bridge apart disable
APaRT disabled
Console> (enable) show bridge
APaRT Disabled
FDDICHECK Disabled
IP fragmentation Enabled
Default IPX translations:
    FDDI SNAP  to Ethernet     8023
    FDDI 802.2 to Ethernet     snap
    Ethernet 802.3 Raw to FDDI 8022
Console> (enable)
```

To enable APaRT, perform this task in privileged mode:

	Task	Command
Step 1	Enable APaRT on the FDDI module.	**set bridge apart enable**
Step 2	Verify that APaRT is enabled.	**show bridge**

This example shows how to enable APaRT and verify the configuration:

```
Console> (enable) set bridge apart enable
APaRT enabled
Console> (enable) show bridge
APaRT Enabled
FDDICHECK Disabled
IP fragmentation Enabled
Default IPX translations:
    FDDI SNAP  to Ethernet     8023
    FDDI 802.2 to Ethernet     snap
    Ethernet 802.3 Raw to FDDI 8022
Console> (enable)
```

Configuring MAC Address Learning

You can specify whether an FDDI interface learns MAC addresses that it previously learned from an Ethernet interface. Disabling MAC address learning resolves the problem that occurs when void frames on the FDDI ring and translated Ethernet frames sent by the FDDI interface are received and learned on the same FDDI interface instead of being stripped by the MAC hardware.

To reject MAC address learning, perform this task in privileged mode:

	Task	Command
Step 1	Ensure that APaRT is enabled. You must enable APaRT before you enable fddicheck.	**set bridge apart enable**
Step 2	Set the switch to reject MAC address learning.	**set bridge fddicheck enable**
Step 3	Verify the MAC address learning configuration.	**show bridge**

This example shows how to reject MAC address learning on the switch and verify the configuration:

```
Console> (enable) set bridge apart enable
APaRT enabled
Console> (enable) set bridge fddicheck enable
FDDICHECK enabled
Console> (enable) show bridge
APaRT Enabled
FDDICHECK Enabled
IP fragmentation Enabled
Default IPX translations:
    FDDI SNAP  to Ethernet     8023
    FDDI 802.2 to Ethernet     snap
    Ethernet 802.3 Raw to FDDI 8022
Console> (enable)
```

To allow MAC address learning, perform this task in privileged mode:

	Task	Command
Step 1	Set the switch to reject MAC address learning.	**set bridge fddicheck disable**
Step 2	Verify the MAC address learning configuration.	**show bridge**

This example shows how to enable MAC address learning on the switch and verify the configuration:

```
Console> (enable) set bridge fddicheck disable
FDDICHECK disabled
Console> (enable) show bridge
APaRT Enabled
FDDICHECK Disabled
IP fragmentation Enabled
Default IPX translations:
    FDDI SNAP  to Ethernet     8023
    FDDI 802.2 to Ethernet     snap
    Ethernet 802.3 Raw to FDDI 8022
Console> (enable)
```

Checking Connectivity

Use the **ping** and **traceroute** commands to test connectivity out FDDI/CDDI ports.

To check connectivity out a port, perform this task in privileged mode:

	Task	Command
Step 1	Ping a remote host that is located out the port you want to test.	**ping** [**-s**] *host* [*packet_size*] [*packet_count*]
Step 2	Trace the hop-by-hop route of packets from the switch to a remote host located out the port you want to test.	**traceroute** *host*
Step 3	If the host is unresponsive, check the IP address and default gateway configured on the switch.	**show interface** **show ip route**

This example shows how to ping a remote host and how to trace the hop-by-hop path of packets through the network using the **traceroute** command:

```
Console> (enable) ping somehost
somehost is alive
Console> (enable) traceroute somehost
traceroute to somehost.company.com (10.1.2.3), 30 hops max, 40 byte packets
 1 engineering-1.company.com (173.31.192.206) 2 ms 1 ms 1 ms
 2 engineering-2.company.com (173.31.196.204) 2 ms 3 ms 2 ms
 3 gateway_a.company.com (173.16.1.201) 6 ms 3 ms 3 ms
 4 somehost.company.com (10.1.2.3) 3 ms * 2 ms
```

FDDI/CDDI Switching Configuration Examples

These sections show examples of FDDI/CDDI switching configurations:

- Single Switch Configuration, page 39-15
- Multiple Switch VLAN Configuration Without Trunking, page 39-16

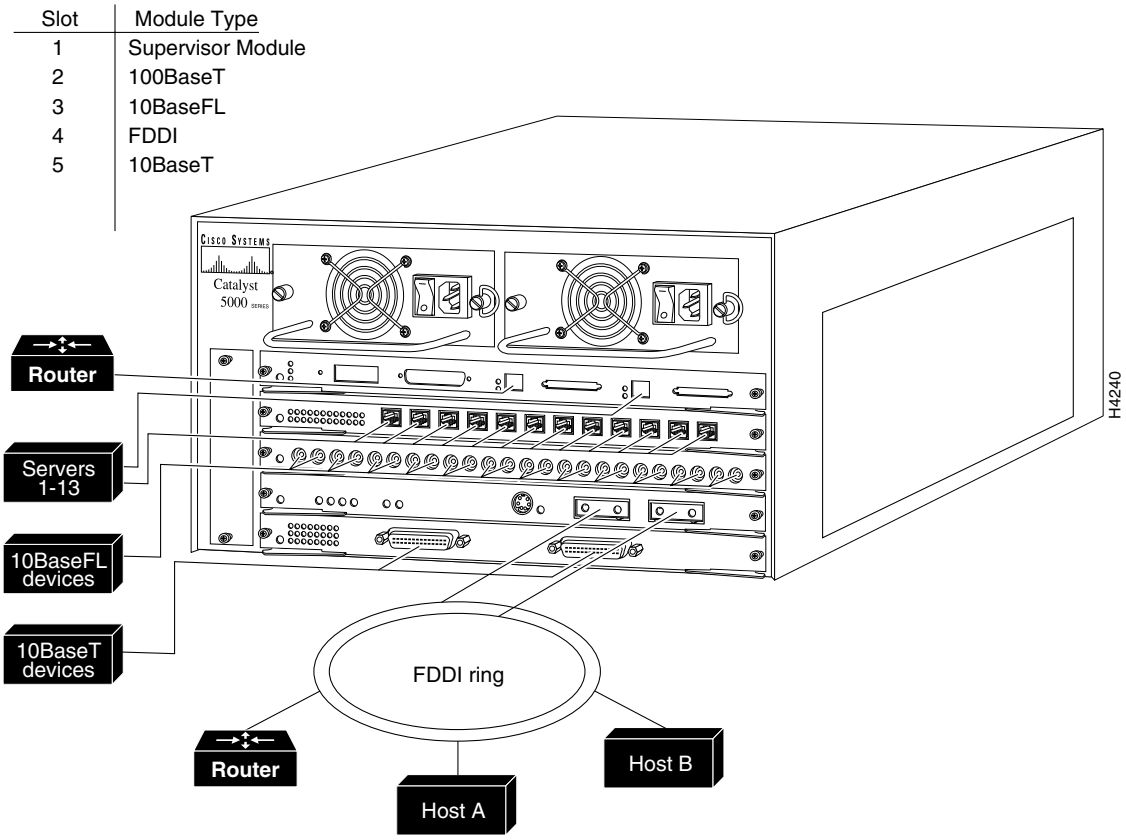
Single Switch Configuration

Figure 39-1 shows a simple Catalyst 5000 family switch configuration and includes these elements:

- FDDI module is in slot 4
- 1 full-duplex, Fast Ethernet connection to a router
- 13 half-duplex, Fast Ethernet connections to servers (1 connection on card 1 and 12 connections on card 2)
- 12 half-duplex, 10BaseFL Ethernet connections to servers
- 2 FDDI connections to an FDDI ring
- 24 half-duplex, 10BaseT Ethernet connections to network devices
- User-data string of “Engineering”
- FDDI SNAP to Ethernet 802.3 protocol translation for IPX data

- Remaining parameters set to default settings:
  - FDDI 802.2 to Ethernet 802.3
  - Ethernet 802.3 RAW to FDDI SNAP
  - TL_MIN parameter set to 62 microseconds
  - TNotify parameter set to 30 seconds
  - TRequest parameter set to 165,000 microseconds
  - IP fragmentation enabled
  - IP unreachable messages enabled

Figure 39-1 Single Catalyst 5000 Family Switch Configuration

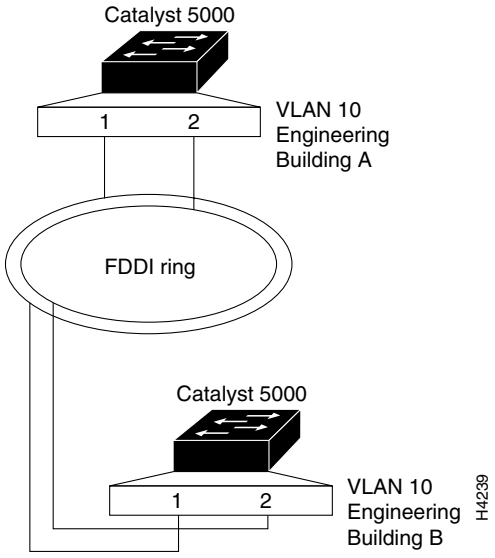


Multiple Switch VLAN Configuration Without Trunking

You can set up VLAN groups across multiple switches without trunking if the switches have any two ports of the same VLAN connected, as shown in Figure 39-2. You need to configure the VLANs individually for both switches using the **set vlan** command.

Note You can set up VLAN groups across multiple switches using trunking, as described in Chapter 40, "Configuring FDDI 802.10 Trunks."

Figure 39-2 Multiple Catalyst 5000 Family Switch VLAN Configuration Without Trunking



This example sets VLAN 10 for the Catalyst 5000 family switch in building A:

```
System1> (enable) set vlan 10 4/1-2
VLAN 10 modified.
VLAN 1 modified.
VLAN  Mod/Ports
---- ------------------------
10    4/1-2
```

This example sets VLAN 10 for the Catalyst 5000 family switch in building B:

```
System2> (enable) set vlan 10 4/1-2
VLAN 10 modified.
VLAN 1 modified.
VLAN  Mod/Ports
---- ------------------------
10    4/1-2
```

This example displays the VLAN 10 setting for the Catalyst 5000 family switch in building A:

```
System1> (enable) show vlan 10
VLAN Name                        Type  Status    Mod/Ports
---- --------------------------- ----- --------- ----------------
10   VLAN0010                    enet  active    4/1-2


VLAN SAID       MTU   RingNo BridgeNo StpNo Parent Trans1 Trans2
---- ---------- ----- ------ -------- ----- ------ ------ ------
10   100010     1500  0      0        0     0      0      0
```

This example displays the VLAN settings for the Catalyst 5000 family switch in building A:

```
System1> (enable) show vlan
VLAN Name                        Type  Status    Mod/Ports
---- --------------------------- ----- --------- ----------------
1    default                     enet  active    1/1-2
10   VLAN0010                    enet  active    4/1-2
20   VLAN0020                    enet  active    2/1-24
1002 fddi-default                fddi  active
1003 token-ring-default          tring active
1004 fddinet-default             fdnet active
1005 trnet-default               trnet active


VLAN SAID       MTU   RingNo BridgeNo StpNo Parent Trans1 Trans2
---- ---------- ----- ------ -------- ----- ------ ------ ------
1    100001     1500  0      0        0     0      0      0
10   100010     1500  0      0        0     0      0      0
20   100020     1500  0      0        0     0      0      0
1002 101002     1500  0      0        0     0      0      0
1003 101003     1500  0      0        0     0      0      0
1004 101004     1500  0      0        0     0      0      0
1005 101005     1500  0      0        0     0      0      0
System1> (enable)
```

This example displays the VLAN 10 setting for the Catalyst 5000 family switch in building B:

```
System2> (enable) show vlan 10
VLAN Name                        Type  Status    Mod/Ports
---- --------------------------- ----- --------- ----------------
10   VLAN0010                    enet  active    4/1-2

VLAN SAID       MTU   RingNo BridgeNo StpNo Parent Trans1 Trans2
---- ---------- ----- ------ -------- ----- ------ ------ ------
10   100010     1500  0      0        0     0      0      0
```

This example displays the VLAN settings for the Catalyst 5000 family switch in building B:

```
System2> (enable) show vlan
VLAN Name                        Type  Status    Mod/Ports
---- --------------------------- ----- --------- ----------------
1    default                     enet  active    1/1-2
10   VLAN0010                    enet  active    4/1-2
20   VLAN0020                    enet  active    2/1-24
1002 fddi-default                fddi  active
1003 token-ring-default          tring active
1004 fddinet-default             fdnet active
1005 trnet-default               trnet active

VLAN SAID       MTU   RingNo BridgeNo StpNo Parent Trans1 Trans2
---- ---------- ----- ------ -------- ----- ------ ------ ------
1    100001     1500  0      0        0     0      0      0
10   100010     1500  0      0        0     0      0      0
20   100020     1500  0      0        0     0      0      0
1002 101002     1500  0      0        0     0      0      0
1003 101003     1500  0      0        0     0      0      0
1004 101004     1500  0      0        0     0      0      0
1005 101005     1500  0      0        0     0      0      0
```