# interface fastethernet

To select a particular Fast Ethernet interface for configuration, use the **interface fastethernet** command in global configuration mode.

**Cisco 4500 and 4700 Series**

**interface fastethernet** *number*

**Cisco 7200 Series**

**interface fastethernet** *slot*/*port*

**Cisco 7500 Series**

**interface fastethernet** *slot*/*port-adapter*/*port*

## Syntax Description

| | |
|---|---|
| *number* | Port, connector, or interface card number. On a Cisco 4500 or 4700 series routers, specifies the network interface module (NIM) or network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system. |
| *slot* | Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information. |
| *port* | Number of the port being configured. Refer to the appropriate hardware manual for slot and port information. |
| *port-adapter* | Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility. |

## Defaults

No FastEthernet interface will be configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 11.3 | The default encapsulation type was changed to ARPA. |

## Usage Guidelines

This command does not have a **no** form.

## Examples

The following example configures Fast Ethernet interface 0 for standard ARPA encapsulation (the default setting) on a Cisco 4500 or 4700 series router:

```
Router(config)# interface fastethernet 0
```

**Related Commands**

| Command | Description |
|---|---|
| **show interfaces fastethernet** | Displays information about the Fast Ethernet interfaces. |

# interface gigabitethernet

To configure a Gigabit Ethernet interface and enter interface configuration mode, use the **interface gigabitethernet** *slot/port* command in global configuration mode.

**interface gigabitethernet** *slot/port*

To configure a Gigabit Ethernet interface and enter interface configuration mode on a Cisco 7200 VXR router used as a router shelf in an AS5800 Universal Access Server, use the **interface gigabitethernet** *router-shelf/slot/port* command in global configuration mode.

**interface gigabitethernet** *router-shelf/slot/port*

## Syntax Description

| | |
|---|---|
| *router-shelf* | Router shelf in a Cisco AS5800 Universal Access Server. |
| *slot* | Slot number of the interface. |
| *port* | Port number on the interface. |

## Defaults

No Gigabit Ethernet interface is created.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.1 CC | This command was introduced. |
| 12.1(3a)E | Support for the Cisco 7200-I/O-GE+E controller was introduced. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |

## Usage Guidelines

Many features are enabled on a per-interface basis. The **interface gigabitethernet** global configuration command modifies the operation of the Gigabit Ethernet interface on the Cisco 7200-I/O-GE+E.

## Examples

This example illustrates the command syntax for creating a Gigabit Ethernet interface:

```
Router(config)# interface gigabitethernet 0/0
Router(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show interfaces gigabitethernet** | Checks the status and configuration settings of the Gigabit Ethernet interface of the Cisco 7200-I/O-GE+E. |

# interface group-async

To create a group interface that will serve as master to which asynchronous interfaces can be associated as members, use the **interface group-async** command in global configuration mode. To restore the default, use the **no** form of this command.

**interface group-async** *unit-number*

**no interface group-async** *unit-number*

## Syntax Description

| | |
|---|---|
| *unit-number* | Number of the asynchronous group interface being created. |

## Defaults

No interfaces are designated as group masters.

## Command Modes

Global configuration

## Usage Guidelines

Using the **interface group-async** command, you create a single asynchronous interface to which other interfaces are associated as members using the **group-range** command. This one-to-many configuration allows you to configure all associated member interfaces by entering one command on the group master interface, rather than entering this command on each individual interface. You can create multiple group masters on a device; however, each member interface can be associated only with one group.

## Examples

The following example defines asynchronous group master interface 0:

```
Router(config)# interface group-async 0
```

## Related Commands

| Command | Description |
|---|---|
| **group-range** | Creates a list of member asynchronous interfaces (associated with a group interface). |
| **member** | Alters the configuration of an asynchronous interface that is a member of a group. |

# interface multilink

To create a multilink bundle or enter multilink interface configuration mode, use the **interface multilink** command in global configuration mode. To remove a multilink bundle, use the **no** form of this command.

**interface multilink** *group-name*

**no interface multilink**

## Syntax Description

| | |
|---|---|
| *group-number* | Number of the multilink bundle (a nonzero number). |

## Defaults

No interfaces are configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |

## Examples

The following example shows how to create multilink bundle 1:

```
interface multilink 1
 ip address 192.168.11.4 255.255.255.192
 encapsulation ppp
 ppp multilink
 keepalive
```

## Related Commands

| Command | Description |
|---|---|
| multilink-group | Designates an interface as part of a multilink leased line bundle. |
| **ppp multilink fragmentation** | Enables PPP multilink fragmentation. |

# interface port-channel

To specify a Fast EtherChannel and enter interface configuration mode, use the **interface port-channel** command in global configuration mode.

**interface port-channel** *channel-number*

**Syntax Description**

| | |
|---|---|
| *channel-number* | Channel number assigned to this port-channel interface. Range is 1 to 4. |

**Defaults**

No Fast EtherChannel is specified.

**Command Modes**

Global configuration

**Command History**

| Release | Modification |
|---|---|
| 11.1 CA | This command was introduced. |
| 12.1(5)T | This command was integrated into 12.1(5)T. |

**Usage Guidelines**

The Fast EtherChannel feature allows multiple Fast Ethernet point-to-point links to be bundled into one logical link to provide bidirectional bandwidth of up to 800 Mbps. Fast EthernetChannel can be configured between networking devices that support EtherChannel capability.

You can configure the port-channel interface as you would do to any Fast Ethernet interface.

After you create a port-channel interface, you assign Fast Ethernet interfaces (up to four) to it. For information on how to assign a Fast Ethernet interface to a port-channel interface, refer to the **channel-group** interface configuration command.

**Caution** The port-channel interface is the routed interface. Do not enable Layer 3 addresses on the physical Fast Ethernet interfaces. Do not assign bridge groups on the physical Fast Ethernet interfaces because it creates loops. Also, you must disable spanning tree.

**Caution** With Release 11.1(20)CC, the Fast EtherChannel supports Cisco Express Forwarding (CEF) and Distributed Cisco Express Forwarding (dCEF). We recommend that you clear all explicit **ip route-cache distributed** commands from the Fast Ethernet interfaces before enabling dCEF on the port-channel interface. Clearing the route cache gives the port-channel interface proper control of its physical Fast Ethernet links. When you enable CEF/dCEF globally, all interfaces that support CEF/dCEF are enabled. When CEF/dCEF is enabled on the port-channel interface, it is automatically enabled on each of the Fast Ethernet interfaces in the channel group. However, if you have previously disabled CEF/dCEF on the Fast Ethernet interface, CEF/dCEF is not automatically enabled. In this case, you must enable CEF/dCEF on the Fast Ethernet interface.

As you work with the **interface port-channel** command, consider the following points:

- If you configure the Inter-Switch Link (ISL) protocol, you must assign the IP address to the subinterface (for example, **interface port-channel 1.1**—an IP address per VLAN) and you must specify the encapsulation with the VLAN number under that subinterface (for example, **encapsulation isl 100**) for ISL to work.
- Currently, if you want to use the Cisco Discovery Protocol (CDP), you must configure it only on the port-channel interface and not on the physical Fast Ethernet interface.
- If you do not assign a static MAC address on the port-channel interface, the Cisco IOS software automatically assigns a MAC address. If you assign a static MAC address and then later remove it, Cisco IOS software automatically assigns a MAC address.

This command does not have a **no** form.

## Examples

The following example creates a port-channel interface with a channel group number of 1 and adds three Fast Ethernet interfaces to port-channel 1:

```
Router(config)# interface port-channel 1
Router(config-if)# ip address 10.1.1.10 255.255.255.0
Router(config)# interface fastethernet 1/0/0
Router(config-if)# channel-group 1
Router(config)# interface fastethernet 4/0/0
Router(config-if)# channel-group 1
Router(config)# interface fastethernet 5/0/0
Router(config-if)# channel-group 1
```

## Related Commands

| Command | Description |
|---|---|
| **channel-group** | Defines the timeslots that belong to each T1 or E1 circuit. |
| **show interfaces port-channel** | Displays the information about the Fast EtherChannel on Cisco 7500 series routers and Cisco 7000 series routers with the RSP7000 and RSP7000CI. |

# interface pos

To specify the Packet OC-3 interface on the Packet-over-SONET (POS) interface processor and enter interface configuration mode, use the **interface pos** command in global configuration mode.

**Cisco 7000 and Cisco 7500 Series Routers with VIPs**

**interface pos** *slot/port-adapter/port*

**Cisco 7200 Series Routers**

**interface pos** *slot/port*

## Syntax Description

| | |
|---|---|
| *slot* | Specifies the backplane slot number. |
| *port* | On Cisco 7000 series and Cisco 7500 series routers, specifies the ports on a VIP card. The value must be 0. |
| *port-adapter* | Port adapter number on the interface. The value must be 0. |

## Defaults

No POS interface is specified.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |

## Usage Guidelines

This command does not have a **no** form.

## Examples

The following example specifies the single Packet OC-3 interface on the POS OC-3 port adapter in slot 2:

```
Router(config)# interface pos 2/0
```

# interface range

To execute commands on multiple subinterfaces at the same time, use the **interface range** command in global configuration command mode.

**interface range** {**fastethernet** *interfacenumber - interfacenumber* | **gigabitethernet** *interfacenumber - interfacenumber* | **loopback** *number* | **tunnel** *number* | **port-channel** *number* | **vlan** *number* | **macro** *word*}

## Syntax Description

| | |
|---|---|
| **fastethernet** | Fastethernet interface. Range is 1 to 6. |
| **gigabitethernet** | Gigabitethernet interface. Range is 1 to 6. |
| **loopback** | Loopback interface. Range is 0 to 2147483647. |
| **tunnel** | Tunnel interface. Range is 0 to 2147483647. |
| **port-channel** | Port-channel interface. Range is 1 to 256. |
| **vlan** | Catalyst virtual LAN (VLAN). Range is 1 to 4094. |
| **macro** | Specifies a macro keyword. |
| *interfacenumber* **-** *interfacenumber* | Lowest to highest numbers in the range. A hyphen must separate the lowest and highest numbers. For example, 1 - 34. |
| *number* | Interface number. Loopback, port-channel, tunnel, and vlan are each assigned a single interface number such as “5.” |
| *word* | Previously defined keyword, up to 32 characters long. |

## Defaults

No default behavior or values

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(7)XE | This command was introduced. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(2)DD | This command was expanded to support subinterface ranges. |
| 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| 12.2(8)T | This modified command was integrated into Cisco IOS Release 12.2(8)T. |
| 12.2(18.10.02)SX | This command was integrated into Cisco IOS Release 12.2(18.10.02)SX |

## Usage Guidelines

### Configuration Changes

All configuration changes made to a range of subinterfaces are saved to NVRAM, but the range itself does not get savedto NVRAM. Use the **define interface-range** command to create and save a range.

You can enter the range in two ways:

- Specifying up to five interface ranges

- Specifying a previously defined macro

You can specify either the interfaces or the name of a range macro. A range must consist of the same interface type, and the interfaces within a range cannot span slots.

You cannot specify both an interface range and a macro keyword in the same command. After creating a macro, the CLI does not allow you to enter additional ranges. Likewise, if you have already entered an interface range, the CLI does not allow you to enter a macro.

The spaces around the dash in the **interface range** command syntax are required. For example, using a Catalyst 6500 router, the command **interface range fastethernet 1 - 6** is valid; the command **interface range fastethernet 1-6** is not valid.

#### VLAN Ranges

When you define a Catalyst Vlans, valid values are from 1 to 4094. The last VLAN number cannot exceed 4094.

You cannot use the **interface range** command to create switch virtual interfaces (SVIs). You must create SVIs with individual **interface VLAN** commands. You can use the **interface range** command on existing VLAN SVIs. To display VLAN SVIs, enter the **show running-config** command. VLANs not displayed cannot be used in the **interface range** command.

The commands entered under the **interface range** command are applied to all existing VLAN SVIs.

## Examples

The following example shows how to use the **interface range** command to configure a fastethernet range:

```
Router(config)# interface range fastethernet5/1 - 4
Router(config-if-range)#
```

The following example shows how to set a vlan:

```
Cisco-65K(config)#interface range vlan 123
Cisco-65K(config-if-range)#
```

The following example configures the Fast Ethernet subinterfaces within the range from 5/1.1 to 5/1.4 and applies the following VLAN IDs to those subinterfaces:

```
Fast Ethernet5/1.1 = VLAN ID 301 (vlan-id)
Fast Ethernet5/1.2 = VLAN ID 302 (vlan-id = 301 + 2 – 1 = 302)
Fast Ethernet5/1.3 = VLAN ID 303 (vlan-id = 301 + 3 – 1 = 303)
Fast Ethernet5/1.4 = VLAN ID 304 (vlan-id = 301 + 4 – 1 = 304)
```

```
Router(config)# interface range fastethernet5/1 - 4
Router(config-if)# encapsulation dot1q 301
Router(config-if)# no shutdown
Router(config-if)#
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.1, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.2, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.3, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.4, changed state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.1,
changed state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.2,
changed state to up
```

```
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.3,
changed state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.4,
changed state to up
```

The following example shows how to execute a range macro:

```
Router(config)# interface range macro macro1
```

The following exampe shows how to set a gigabitethernet range:

```
Router(config)# interface range gigabitethernet1/1 - 6
Router(config-if-range)#
```

The following example shows how to use the loopback interface:

```
Router(config)# interface range loopback 34567
Router(config-if-range)#
```

The following example shows how to use the tunnel interface:

```
Router(config)# interface range tunnel 55555
Router(config-if-range)#
```

The following example shows how to use the port-channel interface:

```
Router(config)# interface range port-channel 343
Router(config-if-range)#
```

## Related Commands

| Command | Description |
|---|---|
| **define interface range** | Defines an interface range macro. |
| **encapsulation dot1q** | Applies a unique VLAN ID to each subinterface within the range. |
| **interface vlan** | Configures a VLAN interface. |

# interface vg-anylan

To specify the interface on a 100VG-AnyLAN port adapter and enter interface configuration mode on Cisco 7200 series routers and Cisco 7500 series routers, use the **interface vg-anylan** command in global configuration mode.

**Cisco 7200 Series Routers**

**interface vg-anylan** *slot/port*

**Cisco 7500 Series Routers with VIPs**

**interface vg-anylan** *slot/port-adapter/port*

## Syntax Description

| | |
|---|---|
| *slot* | Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information. |
| *port* | Number of the port being configured. Refer to the appropriate hardware manual for slot and port information. |
| *port-adapter* | Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility. |

## Defaults

No interfaces are specified.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |

## Usage Guidelines

The 100VG-AnyLAN port adapter provides a single interface port that is compatible with and specified by IEEE 802.12. The 100VG-AnyLAN port adapter provides 100 Mbps over Category 3 or Category 5 unshielded twisted-pair (UTP) cable with RJ-45 terminators, and supports IEEE 802.3 Ethernet packets.

You configure the 100VG-AnyLAN port adapter as you would any Ethernet or Fast Ethernet interface. The 100VG-AnyLAN port adapter can be monitored with the IEEE 802.12 Interface MIB.

This command does not have a **no** form.

## Examples

The following example specifies the 100VG-AnyLAN port adapter in the first port adapter in slot 1:

```
Router(config)# interface vg-anylan 1/0/0
```

## Related Commands

| Command | Description |
|---|---|
| **framing** | Selects the frame type for the T1 or E1 data line. |
| **show interfaces vg-anylan** | Displays the information about the 100VG-AnyLAN port adapter on Cisco 7200 series routers and Cisco 7500 series routers. |

# international bit

To set the E3 international bit in the G.751 frame used by the PA-E3 port adapter, use the **international bit** command in interface configuration mode. To return to the default international bit, use the **no** form of this command.

**international bit** {**0** | **1**} {**0** | **1**}

**no international bit**

## Syntax Description

| | |
|---|---|
| **0** \| **1** | Specifies the value of the first international bit in the G.751 frame. The default is 0. |
| **0** \| **1** | Specifies the value of the second international bit in the G.751 frame. The default is 0. |

## Defaults

The default value for each bit is 0.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.1 CA | This command was introduced. |

## Usage Guidelines

The **international bit** command sets bits 6 and 8, respectively, of set II in the E3 frame.

To verify the international bit configured on the interface, use the **show controllers serial** EXEC command.

## Examples

The following example sets the international bit to 1 1 on the PA-E3 port adapter in slot 1, port adapter slot 0, interface 0:

```
Router(config)# interface serial 1/0/0
Router(config-if)#  international bit 1 1
```

## Related Commands

| Command | Description |
|---|---|
| **national bit** | Sets the E3 national bit in the G.751 frame used by the PA-E3 port adapter. |
| **show controllers serial** | Displays information that is specific to the interface hardware. |

# invert data

To invert the data stream, use the **invert data** command in interface configuration mode. This command applies only to the Cisco 7000 series routers with the RSP7000 and RSP7000CI, Cisco 7200 series routers, and Cisco 7500 series routers. To disable inverting the data stream, use the **no** form of this command.

**invert data**

**no invert data**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Data is not inverted.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.1 CA and 11.2 P | This command was introduced. |

## Usage Guidelines

### T1 Line Without B8ZS Encoding

If the interface on the PA-8T and PA-4T+ synchronous serial port adapters and the PA-T3 and PA-2T3 synchronous serial port adapters is used to drive a dedicated T1 line that does not have B8ZS encoding (a method to avoid 15 zeros), the data stream must be inverted (both transmitting and receiving data) either in the connecting CSU/DSU or in the interface.

Inverting is a method of avoiding excessive zeroes that is superseded by the use of B8ZS encryption. This option could be needed for use with legacy equipment that supports this option. By inverting the High-Level Data Link Control (HDLC) data stream, the HDLC zero insertion algorithm becomes a ones insertion algorithm that satisfies the T1 requirements. Be careful not to invert data both on the interface and on the CSU/DSU because two data inversions will cancel each other out.

### AMI Line Coding

If the interface on the CT3IP uses alternate mark inversion (AMI) line coding, you must also invert the data on the T1 channel. For more information, see the **t1 linecode** controller configuration command.

## Examples

The following example inverts data on serial interface 3/1/0:

```
Router(config)# interface serial 3/1/0
Router(config-if)# invert data
```

## Related Commands

| Command | Description |
|---|---|
| **t1 linecode** | Specifies the type of linecoding used by the T1 channels on the CT3IP in Cisco 7500 series routers. |

# invert rxclock

To configure UIO serial port 0 or 1 on the Cisco MC3810 when the cable connected is DCE type, use the **invert rxclock** command in interface configuration mode. The command inverts the phase of the RX clock on the UIO serial interface, which does not use the T1/E1 interface. To disable the phase inversion, use the **no** form of this command.

**invert rxclock**

**no invert rxclock**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The receive clock signal is not inverted.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 MA | This command was introduced. |

## Examples

The following example inverts the clock signal on serial interface 1:

```
Router(config)# interface serial 1
Router(config-if)# invert rxclock
```

# invert-transmit-clock

The **invert-transmit-clock** command is replaced by the **invert txclock** command. See the description of the **invert-txclock** command in this chapter for information on the transmit clock signal.

# invert txclock

To invert the transmit (TX) clock signal, use the **invert txclock** command in interface configuration mode. To return the TX clock signal to its initial state, use the **no** form of this command.

**invert txclock**

**no invert txclock**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Transmit clock signal is not inverted.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 11.3 | The **invert-transmit-clock** command was replaced by the **invert txclock** command. |

## Usage Guidelines

Delays between the serial clock transmit external (SCTE) clock and data transmission indicate that the transmit clock signal might not be appropriate for the interface rate and length of cable being used. Different ends of the wire can have variances that differ slightly. The **invert txclock** command compensates for these variances. This command replaces the **invert-transmit-clock** command.

Systems that use long cables or cables that are not transmitting the TxC signal (transmit echoed clock line, also known as TXCE or SCTE clock) can experience high error rates when operating at the higher transmission speeds. For example, if a PA-8T synchronous serial port adapter is reporting a high number of error packets, a phase shift might be the problem. Inverting the clock might correct this shift.

When a PA-8T or PA-4T+ port adapter interface is DTE, the **invert txclock** command inverts the TxC signal it received from the remote DCE. When the PA-8T or PA-4T+ port adapter interface is DCE, this command changes the signal back to its original phase.

## Examples

The following example inverts the clock signal on serial interface 3/0:

```
Router(config)# interface serial 3/0
Router(config-if)# invert txclock
```

# ip director default-weights

To configure default weight metrics for the DistributedDirector, use the **ip director default-weights** command in global configuration mode. To restore the default, use the **no** form of this command.

**ip director default-weights** {[**drp-int** *n*] [**drp-ext** *n*] [**drp-ser** *n*] [**drp-rtt** *n*] [**random** *n*] [**admin** *n*] [**portion** *n*] [**availability** *n*] [**route-map** *n*]}

**no ip director default-weights** {[**drp-int** *n*] [**drp-ext** *n*] [**drp-ser** *n*] [**drp-rtt** *n*] [**random** *n*] [**admin** *n*] [**portion** *n*] [**availability** *n*] [**route-map** *n*]}

## Syntax Description

| | |
|---|---|
| **drp-int** *n* | (Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100.<br><br>This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric (**drp-ext**) to help determine the distance between the router and the client originating the DNS query.<br><br>If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent. |
| **drp-ext** *n* | (Optional) DRP external metric. The range is 1 to 100.<br><br>This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful. |
| **drp-ser** *n* | (Optional) DRP server metric. The range is 1 to 100.<br><br>This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric (**drp-int**) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query.<br><br>If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes. |
| **drp-rtt** *n* | (Optional) DRP round-trip time metric. The range is 1 to 100.<br><br>This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query. |

| | |
|---|---|
| **random** *n* | (Optional) Random metric. The range is 1 to 100.<br>This option selects a random number for each distributed server and defines the "best" server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents. |
| **admin** *n* | (Optional) Administrative metric. The range is 1 to 100.<br>This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service. |
| **portion** *n* | (Optional) Portion metric. The range is 1 to 100.<br>This option assigns a load "portion" to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time. |
| **availability** *n* | (Optional) Availability metric. The range is 1 to 65,535.<br>This option specifies the load information for the DistributedDirector. The default value is 65,535. |
| **route-map** *n* | (Optional) Route-map metric. The range is 1 to 100.<br>This option specifies if a server should be offered to a client. |

## Defaults

The availability default value is 65,535.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.1(18)IA | This command was introduced. |
| 12.1(5)T | The availability and route-map metrics were added. |

## Usage Guidelines

Not all of the metrics need to be configured; however, at least one metric must be configured when this command is used.

Default weights are used for all host names sorted by the DistributedDirector. To override default weights for a certain host, specify host-specific weights in the private DNS server configuration.

When the associated metric is referenced in the sorting decision, it will always be multiplied by the appropriate metric weight. In this way, you can specify that some metrics be weighted more than others. You may determine the weights that you want to use through experimentation. The weights given do not need to add up to 100.

The new availability metric allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

## Examples

The following command configures default weights for the internal and external metrics:

```
ip director default-weights drp-int 10 drp-ext 90
```

## Related Commands

| Command | Description |
|---|---|
| **debug ip director parse** | Shows debugging information for DistributedDirector parsing of TXT information. |
| **debug ip director sort** | Shows debugging information for DistributedDirector IP address sorting. |
| **ip director access-list** | Defines an access list for the DistributedDirector that specifies which subdomain names and host names should be sorted. |
| **ip director cache** | Enables the sorting cache on the DistributedDirector. |
| **ip director host priority** | Configures the order in which the DistributedDirector considers metrics when picking a server. |
| **ip director host weights** | Sets host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name. |
| **ip director server admin-pref** | Configures a per-service administrative preference value. |
| **ip director server portion** | Sets the portion value for a specific server. |
| **ip director server preference** | Specifies DistributedDirector preference of one server over others or takes a server out of service. |
| **show ip director default-weights** | Shows the DistributedDirector default weights. |
| **show ip director servers** | Displays the DistributedDirector server preference information. |

# ip director dfp

To configure the DistributedDirector Dynamic Feedback Protocol (DFP) agent with which the DistributedDirector should communicate, use the **ip director dfp** command in global configuration mode. To turn off the DFP agent, use the **no** form of this command.

**ip director dfp** *ip-address* [*port*] [**retry** *n*] [**attempts** *n*] [**timeout** *n*]

**no ip director dfp** *ip-address* [*port*] [**retry** *n*] [**attempts** *n*] [**timeout** *n*]

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address. |
| *port* | (Optional) Port number to which the distributed servers are configured. The default value is 8080. |
| **retry** *n* | (Optional) Number of times a connection will be attempted. The default value is 5 attempts. |
| **attempts** *n* | (Optional) Delay, in seconds, between each attempt. The default value is 10,000 seconds. |
| **timeout** *n* | (Optional) Maximum amount of time, in seconds, for which DFP information is assumed valid. The default value is 10,000 seconds. |

## Syntax Description

The port default value is 8080.

The retry default value is 5 attempts.

The attempts default value is 10,000 seconds.

The timeout default value is 10,000 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |

## Usage Guidelines

A connection is attempted a specified number of times with a delay of a specified number of seconds between each attempt. Once a connection is established, the DFP protocol will run. If a time interval update has not occurred for this DFP session, the connection breaks and is reestablished as described above.

## Examples

The following example configures the DistributedDirector to communicate with a specified DFP agent:

```
ip director dfp 10.0.0.1 retry 3 attempts 60 timeout 6000
```

# ip director dfp security

To configure a security key for use when connecting to the Dynamic Feedback Protocol (DFP) client named, use the **ip director dfp security** command in global configuration mode. To turn off the security key, use the **no** form of this command.

**ip director dfp security** *ip-address* **md5** *string* [*timeout*]

**no ip director dfp security** *ip-address* **md5** *string* [*timeout*]

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address for the service. |
| **md5** | Security data authentication. Message Digest 5. |
| *string* | Security key. |
| *timeout* | (Optional) Amount of time, in seconds, during which DistributedDirector will continue to accept a previously defined security key. The default value is 0 seconds. |

## Defaults

The timeout default value is 0 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |

## Usage Guidelines

The **ip director dfp security** command should be entered before configuring the **ip director dfp** command, resulting in a connection being made, but it can be entered independently of making a connection.

DFP allows servers to take themselves Out-of-Service and place themselves back In-Service. This function could result in a security risk because a network that is hacked could be shut down even though all the servers are still performing. An optional security vector is included in DFP to allow each message to be verified. The security vector is used to describe the security algorithm being used and to provide the data for that algorithm. The security vector itself is also extensible in that it specifies which security algorithm is being used. This specification allows different levels of security from MD5 to Data Encryption Standard (DES) to be used without overhauling the protocol and disrupting any installed base of equipment. If a receiving unit is configured for the specified security type, all DFP packets must contain that security vector or they are ignored. If a receiving unit is not configured for any security type, the security vector does not have to be present, and if it is present, it is ignored while the rest of the message is processed normally.

## Examples

The following example configures the security key hello:

```
ip director dfp security 10.0.0.1 md5 hello 60
```

**Related Commands**

| Command | Purpose |
|---|---|
| ip director dfp | Configures the DistributedDirector DFP agent with which the DistributedDirector should communicate. |

# ip director host priority

To configure the order in which the DistributedDirector considers metrics when picking a server, use the **ip director host priority** command in global configuration mode. To turn off metric priorities, use the **no** form of this command.

**ip director host** *host-name* **priority** {[**drp-int** *n*] [**drp-ext** *n*] [**drp-ser** *n*] [**drp-rtt** *n*] [**random** *n*] [**admin** *n*] [**portion** *n*] [**availability** *n*] [**route-map** *n*]}

**no ip director host** *host-name* **priority** {[**drp-int** *n*] [**drp-ext** *n*] [**drp-ser** *n*] [**drp-rtt** *n*] [**random** *n*] [**admin** *n*] [**portion** *n*] [**availability** *n*] [**route-map** *n*]}

## Syntax Description

| | |
|---|---|
| *host-name* | Name of the host that maps to one or more IP addresses. Do not use an IP address. |
| **drp-int** *n* | (Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100.<br><br>This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric (**drp-ext**) to help determine the distance between the router and the client originating the DNS query.<br><br>If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent. |
| **drp-ext** *n* | (Optional) DRP external metric. The range is 1 to 100.<br><br>This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful. |
| **drp-ser** *n* | (Optional) DRP server metric. The range is 1 to 100.<br><br>This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric (**drp-int**) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query.<br><br>If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes. |

| | |
|---|---|
| **drp-rtt** *n* | (Optional) DRP round-trip time metric. The range is 1 to 100.<br>This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query. |
| **random** *n* | (Optional) Random metric. The range is 1 to 100.<br>This option selects a random number for each distributed server and defines the "best" server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents. |
| **admin** *n* | (Optional) Administrative metric. The range is 1 to 100.<br>This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service. |
| **portion** *n* | (Optional) Portion metric. The range is 1 to 100.<br>This option assigns a load "portion" to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time. |
| **availability** *n* | (Optional) Availability metric. The range is 1 to 65,535.<br>This option specifies the load information for the DistributedDirector. The default value is 65,535. |
| **route-map** *n* | (Optional) Route-map metric. The range is 1 to 100.<br>This option specifies if a server should be offered to a client. |

## Defaults

The availability default value is 65,535.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.1(18)IA | This command was introduced. |
| 12.1(5)T | The availability and route-map metrics were added. |

## Usage Guidelines

Not all of the metrics need to be specified, but at least one must be specified.

The new availability metric allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

If multiple servers end up with the same metric value, the next metric is considered to determine the "best" server. If multiple metrics have the same priority value, the metrics are added to obtain a *composite metric*. For example, if two metrics have the same priority value, they are first multiplied by their weight values (if specified) and then added together to form the composite metric.

If you do not specify weights for a group of distributed servers, there are no default weights for the Director, and if you have specified priority values, the weight values are set to 1.

Any metrics that have a nonzero weight and that are assigned no priority value are set to a priority value of 101. They are considered after all other metrics that have priority values. As a result, if no priority values are specified for any metric, metrics are treated additively to form one composite metric.

If you do not use priority and multiple servers have the same metric value, the server whose last IP address was looked at will be returned as the "best" server. If you want to return a random IP address in the case of a tie, use metric priority with the **random** metric as the last criterion.

To turn off all priorities on all metrics associated with the defined host name, use the **no ip director host priority** command. You can turn off the priority for a specific metric or metrics using the **no ip director host** *host-name* **priority** [**drp-int** *n*] [**drp-ext** *n*] [**drp-ser** *n*] [**drp-rtt** *n*] [**random** *n*] [**admin** *n*] [**portion** *n*] [**availability** *n*] [**route-map** *n*] command.

## Examples

The following example sets the external metric as the first priority and the administrative metric as the second priority:

```
ip director host www.xyz.com priority drp-ext 1 admin 2
```

## Related Commands

| Command | Description |
|---|---|
| **ip director host connect** | Enables the DistributedDirector to verify that a server is available. |
| **show ip director hosts** | Displays the DistributedDirector host information. |

# ip director host weights

To set host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name, use the **ip director host weights** command in global configuration mode. To turn off weights for a host, use the **no** form of this command.

**ip director host** *host-name* **weights** {[**drp-int** *n*] [**drp-ext** *n*] [**drp-ser** *n*] [**drp-rtt** *n*] [**random** *n*] [**admin** *n*] [**portion** *n*] [**availability** *n*] [**route-map** *n*]}

**no ip director host** *host-name* **weights** {[**drp-int** *n*] [**drp-ext** *n*] [**drp-ser** *n*] [**drp-rtt** *n*] [**random** *n*] [**admin** *n*] [**portion** *n*] [**availability** *n*] [**route-map** *n*]}

## Syntax Description

| | |
|---|---|
| *host-name* | Name of the host that maps to one or more IP addresses. Do not use an IP address. |
| **drp-int** *n* | (Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100.<br><br>This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric (**drp-ext**) to help determine the distance between the router and the client originating the DNS query.<br><br>If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent. |
| **drp-ext** *n* | (Optional) DRP external metric. The range is 1 to 100.<br><br>This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful. |
| **drp-ser** *n* | (Optional) DRP server metric. The range is 1 to 100.<br><br>This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric (**drp-int**) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query.<br><br>If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes. |

| | |
|---|---|
| **drp-rtt** *n* | (Optional) DRP round-trip time metric. The range is 1 to 100.<br>This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query. |
| **random** *n* | (Optional) Random metric. The range is 1 to 100.<br>This option selects a random number for each distributed server and defines the "best" server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents. |
| **admin** *n* | (Optional) Administrative metric. The range is 1 to 100.<br>This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service. |
| **portion** *n* | (Optional) Portion metric. The range is 1 to 100.<br>This option assigns a load "portion" to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time. |
| **availability** *n* | (Optional) Availability metric. The range is 1 to 65,535.<br>This option specifies the load information for the DistributedDirector. The default value is 65,535. |
| **route-map** *n* | (Optional) Route-map metric. The range is 1 to 100.<br>This option specifies if a server should be offered to a client. |

**Note** No host weights are set. If the **ip director default-weights** command is configured, the configured weights are the default.

## Defaults

The availability default value is 65,535.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.1(25)IA | This command was introduced. |
| 12.0(3)T | This command was integrated into Cisco IOS Release 12.0(3)T. |
| 12.1(5)T | The availability and route-map metrics were added. |

## Usage Guidelines

Use host-specific weights when you want to use different metric weights for different virtual host names (for example, www.xyz.com and ftp.xyz.com).

The new availability metric allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

If desired, host-specific weights can instead be configured on the DistributedDirector default DNS server.

For example, you could configure host-specific weights with the following DNS TXT record:

```
hostname in txt "ciscoDD: weights {[drp-int n] [drp-ext n] [drp-ser n] [random n]
[admin n]}"
```

To use the default weights for all metrics associated with this host name, use the **no ip director host weights** command. To use the default weights for a specific metric or metrics, use the **no ip director host** *host-name* **weights** [**drp-int** *n*] [**drp-ext** *n*] [**drp-ser** *n*] [**drp-rtt** *n*] [**random** *n*] [**admin** *n*] [**portion** *n*] [**availability** *n*] [**route-map** *n*] command.

## Examples

The following example sets the DRP internal metric to 4:

```
ip director host www.xyz.com weights drp-int 4
```

## Related Commands

| Command | Description |
|---|---|
| **ip director default-weights** | Configures default weight metrics for the DistributedDirector. |
| **show ip director dfp** | Displays information about the current status of the DistributedDirector connections with a particular DFP agent. |

# ip director server availability

To configure a default availability value for all ports on a server, use the **ip director server availability** command in global configuration mode. To restore the default, use the **no** form of this command.

**ip director server** *ip-address* **availability** {*availability-value* | **dfp** [*availability-value*]}

**no ip director server** *ip-address* **availability** {*availability-value* | **dfp** [*availability-value*]}

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address. |
| *availability-value* | Availability value as it would be represented on the DistributedDirector system. The range is 0 to 65,535. |
| **dfp** [*availability-value*] | Availability value as it would be represented on the LocalDirector system. The range for value is 0 to 65,535. |

## Defaults

The availability default value is 65,535.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |

## Usage Guidelines

There are two methods for specifying a default availability value. These two methods exist because the LocalDirector and the DistributedDirector deal with values in two different ways. All metrics for the DistributedDirector are arranged such that lower is better; however the LocalDirector load information is calculated such that higher is better. Thus, the DistributedDirector translates the metric value upon receipt from the LocalDirector by subtracting the availability from the maximum possible value of 65,535.

## Examples

To configure a default availability to be used if there is no other valid availability information, the following configuration would suffice. The following example shows how to specify the LocalDirector load and DistributedDirector availability, respectively:

```
ip director server 10.0.0.1 availability dfp 1
ip director server 10.0.0.1 availability 65534
```

To make the availability clear and to allow for specifying numbers in both schemes easily, there are two methods of specifying availability information. If the servers are running multiple serves, it may be necessary to configure the default availability value on a per-port basis by using the **ip director server port availability** command.

```
ip director server 10.0.0.1 port availability dfp 65535
ip director server 10.0.0.20 port availability dfp 65535
```

**Related Commands**

| Command | Description |
|---|---|
| **ip director server port availability** | Configures a default availability value for a specific port on a server. |

# ip director server port availability

To configure a default availability value for a specific port on a server, use the **ip director server port availability** command in global configuration mode. To restore the default, use the **no** form of this command.

**ip director server** *ip-address* **port availability** {*availability-value* | **dfp** [*availability-value*]}

**no ip director server** *ip-address* **port availability** {*availability-value* | **dfp** [*availability-value*]}

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address. |
| *availability-value* | Availability value as it would be represented on the DistributedDirector system. The range is 0 to 65,535. |
| **dfp** [*availability-value*] | Availability value as it would be represented on the LocalDirector system. The range for value is 0 to 65,535. |

## Defaults

The availability default value is 65,535.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |

## Usage Guidelines

There are two methods for specifying a default availability value. These two methods exist because the LocalDirector and the DistributedDirector deal with values in two different ways. All metrics for the DistributedDirector are arranged such that lower is better; however the LocalDirector load information is calculated such that higher is better. Thus, the DistributedDirector translates the metric value upon receipt from the LocalDirector by subtracting the availability from the maximum possible value of 65,535.

## Examples

To make the availability clear and to allow for specifying numbers in both schemes easily, there are two methods of specifying availability information. If the servers are running multiple serves, it may be necessary to configure the default availability value on a per-port basis by using the **ip director server port availability** command.

```
ip director server 10.0.0.1 port availability dfp 65535
ip director server 10.0.0.20 port availability dfp 65535
```

To configure a default availability to be used if there is no other valid availability information, the following configuration would suffice. The following example shows how to specify the LocalDirector load and DistributedDirector availability, respectively:

```
ip director server 10.0.0.1 availability dfp 1
ip director server 10.0.0.1 availability 65534
```

**Related Commands**

| Command | Description |
|---|---|
| **ip director server availability** | Configures a default availability value for all ports on a server. |

# keepalive

To enable keepalive packets and to specify the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface, or before bringing the tunnel protocol down for a specific interface, use the **keepalive** command in interface configuration mode. When the keepalive feature is enabled, a keepalive packet is sent at the specified time interval to keep the interface active. To turn off keepalive packets entirely, use the **no** form of this command.

**keepalive** [*period* [*retries*]]

**no keepalive** [*period* [*retries*]]

## Syntax Description

| | |
|---|---|
| *period* | (Optional) Integer value in seconds greater than 0. The default is 10 seconds. |
| *retries* | (Optional) Specifies the number of times that the device will continue to send keepalive packets without response before bringing the interface down. Integer value greater than 1 and less than 255. If omitted, the value that was previously set is used; if no value had been specified previously, the default of 5 is used.<br><br>If using this command with a tunnel interface, specifies the number of times that the device will continue to send keepalive packets without response before bringing the tunnel interface protocol down. |

## Defaults

*seconds*: 10 seconds

*retries*: 5

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(8)T | The *retries* argument was added and made available on tunnel interfaces. |
| 12.2(13)T | The default value for the *retries* argument was increased to 5. |

## Usage Guidelines

### Keepalive Time Interval

You can configure the keepalive time interval, which is the frequency at which the Cisco IOS software sends messages to itself (Ethernet and Token Ring) or to the other end (serial and tunnel), to ensure that a network interface is alive. The interval is adjustable in 1-second increments down to 1 second. An interface is declared down after three update intervals have passed without receiving a keepalive packet unless the retry value is set higher.

**Note** Ethernet interface drivers on some access platforms use keepalive time as the interval to test for network connectivity. By default, Ethernet link failure detection occurs between 1 and 9 seconds. Keepalive packets are still transmitted on the interface during this time.

Setting the keepalive timer to a low value is very useful for rapidly detecting Ethernet interface failures (transceiver cable disconnecting, cable not terminated, and so on).

#### Line Failure

A typical serial line failure involves losing Carrier Detect (CD) signal. Because this sort of failure is typically noticed within a few milliseconds, adjusting the keepalive timer for quicker routing recovery is generally not useful.

#### Keepalive Packets with Tunnel Interfaces

GRE keepalive packets may be sent from both sides of a tunnel, or from just one side. If they are sent from both sides, the period and retry parameters can be different at each side of the link. If you configure keepalives on only one side of the tunnel, the tunnel interface on the sending side might perceive the tunnel interface on the receiving side to be down because the sending interface is not receiving keepalives. From the receiving side of the tunnel, the link appears normal because no keepalives were enabled on the second side of the link.

#### Dropped Packets

Keepalive packets are treated as ordinary packets, so it is possible that they will be dropped. To reduce the chance that dropped keepalive packets will cause the tunnel interface to be taken down, increase the number of retries.

**Note** When adjusting the keepalive timer for a very low bandwidth serial interface, large datagrams can delay the smaller keepalive packets long enough to cause the line protocol to go down. You may need to experiment to determine the best values to use for the timeout and the number of retry attempts.

#### GRE Tunnels with IPsec

When using GRE with IPsec, the keepalives are encrypted like any other traffic. As with user data packets, if the IKE and IPsec security associations are not already active on the GRE tunnel, the first GRE keepalive packet will trigger IKE/IPsec initialization.

#### Default Behaviors

If you enter only the **keepalive** command with no arguments, defaults for both arguments are used.

If you enter only the **keepalive** command and the timeout parameter, the default number of retries (3) is used.

If you enter the **no keepalive** command, keepalive packets are disabled on the interface.

## Examples

The following example sets the keepalive interval to 3 seconds:

```
Router(config)# interface ethernet 0
Router(config-if)#  keepalive 3
```

The following example sets the keepalive interval to 3 seconds and the retry value to 7:

```
Router(config)# interface tunnel 1
Router(config-if)# keepalive 3 7
```

# lbo

To set a cable length longer than 655 feet for a DS-1 link, use the **lbo** command in interface configuration mode on the interface for a T1 link. To delete the **lbo long** value, use the **no** form of this command.

**lbo** {**long** {**gain26** | **gain36**} {**-15db** | **-22.5db** | **-7.5db** | **0db**} | **short** {**133** | **266** | **399** | **533** | **655**}}

**no lbo**

## Syntax Description

| | |
|---|---|
| **gain26** | Specifies the decibel pulse gain at 26 decibels. This is the default pulse gain. |
| **gain36** | Specifies the decibel pulse gain at 36 decibels. |
| **-15db** | Specifies the decibel pulse rate at –15 decibels. |
| **-22.5db** | Specifies the decibel pulse rate at –22.5 decibels. |
| **-7.5db** | Specifies the decibel pulse rate at –7.5 decibels. |
| **0db** | Specifies the decibel pulse rate at 0 decibels. This is the default. |
| **133** | Specifies a cable length from 0 to 133 feet. |
| **266** | Specifies a cable length from 133 to 266 feet. |
| **399** | Specifies a cable length from 266 to 399 feet. |
| **533** | Specifies a cable length from 399 to 533 feet. |
| **655** | Specifies a cable length from 533 to 655 feet. |

## Defaults

**gain26** and **0db**

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 MA | This command was introduced as a Cisco MC3810 controller configuration command. |
| 12.0(5)XE | The command was introduced as an ATM interface command. |
| 12.0(7)XE1 | Support for Cisco 7100 series routers was added. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |

## Usage Guidelines

This command is supported on T1 links only.

Each T1 port can operate in long-haul or short-haul mode. In long haul mode, the user must specify the gain and the line build out. In short-haul mode, the user must specify the cable length in feet.

The transmit attenuation value is best obtained by experimentation. If the signal received by the far-end equipment is too strong, reduce the transmit level by entering additional attenuation.

## Examples

On Cisco 7100 or 7200 series routers, the following example specifies a pulse gain of 36 decibels and a decibel pulse rate of –7.5 decibels:

```
interface atm 1/2
 lbo long gain36 -7.5db
```

# lex burned-in-address

To set the burned-in MAC address for a LAN Extender interface, use the **lex burned-in-address** command in interface configuration mode. To clear the burned-in MAC address, use the **no** form of this command.

**lex burned-in-address** *ieee-address*

**no lex burned-in-address**

## Syntax Description

| | |
|---|---|
| *ieee-address* | 48-bit IEEE MAC address written as a dotted triplet of 4-digit hexadecimal numbers. |

## Defaults

No burned-in MAC address is set.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |

## Usage Guidelines

Use this command only on a LAN Extender interface that is not currently active (not bound to a serial interface).

## Examples

The following example sets the burned-in MAC address on LAN Extender interface 0:

```
Router(config)# interface serial 4
Router(config-if)# encapsulation ppp
Router(config)# interface lex 0
Router(config-if)# lex burned-in-address 0000.0c00.0001
Router(config-if)  ip address 10.108.172.21 255.255.255.0
```

# lex input-address-list

To assign an access list that filters on MAC addresses, use the **lex input-address-list** command in interface configuration mode. To remove an access list from the interface, use the **no** form of this command.

**lex input-address-list** *access-list-number*

**no lex input-address-list**

## Syntax Description

| | |
|---|---|
| *access-list-number* | Number of the access list assigned with the **access-list** global configuration command. It can be a number from 700 to 799. |

## Defaults

No access lists are preassigned to a LAN Extender interface.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |

## Usage Guidelines

Use the **lex input-address-list** command to filter the packets that are allowed to pass from the LAN Extender to the core router. The access list filters packets on the basis of the source MAC address.

The LAN Extender interface does not process MAC-address masks. Therefore, you should omit the mask from the **access-list** commands.

For LAN Extender interfaces, an implicit permit everything entry is automatically defined at the end of an access list. Note that this default differs from other access lists, which have an implicit deny everything entry at the end of each access list.

## Examples

The following example applies access list 710 to LAN Extender interface 0. This access list denies all packets from MAC address 0800.0214.2776 and permits all other packets.

```
Router(config-if)# access-list 710 deny 0800.0214.2776
Router(config)# interface lex 0
Router(config-if)# lex input-address-list 710
```

## Related Commands

| Command | Description |
|---|---|
| **access-list** | Configures the access list mechanism for filtering frames by protocol type or vendor code. |

# lex input-type-list

To assign an access list that filters Ethernet packets by type code, use the **lex input-type-list** command in interface configuration mode. To remove an access list from an interface, use the **no** form of this command.

**lex input-type-list** *access-list-number*

**no lex input-type-list**

## Syntax Description

| | |
|---|---|
| *access-list-number* | Number of the access list that you assigned with the **access-list** command. It can be a number in the range 200 to 299. |

## Defaults

No access lists are preassigned to a LAN Extender interface.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |

## Usage Guidelines

Filtering is done on the LAN Extender chassis.

The LAN Extender interface does not process masks. Therefore, you should omit the mask from the **access-list** commands.

For LAN Extender interfaces, an implicit permit everything entry is automatically defined at the end of an access list. Note that this default differs from other access lists, which have an implicit deny everything entry at the end of each access list.

## Examples

The following example applies access list 220 to LAN Extender interface 0. This access list denies all AppleTalk packets (packets with a type field of 0x809B) and permits all other packets.

```
Router(config-if)# access-list 220 deny 0x809B 0x0000
Router(config)# interface lex 0
Router(config-if)# lex input-type-list 220
```

## Related Commands

| Command | Description |
|---|---|
| **access-list** | Configures the access list mechanism for filtering frames by protocol type or vendor code. |

# lex priority-group

To activate priority output queueing on the LAN Extender, use the **lex priority-group** command in interface configuration mode. To disable priority output queueing, use the **no** form of this command.

**lex priority-group** *group*

**no lex priority-group**

## Syntax Description

| | |
|---|---|
| *group* | Number of the priority group. It can be a number in the range 1 to 10. |

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |

## Usage Guidelines

To define queueing priorities, use the **priority-list protocol** global configuration command. Note that you can use only the following forms of this command:

**priority-list** *list* **protocol** *protocol* {**high** | **medium** | **normal** | **low**}

**priority-list** *list* **protocol bridge** {**high** | **medium** | **normal** | **low**} **list** *list-number*

If you specify a protocol that does not have an assigned Ethernet type code, such as **x25**, **stun**, or **pad**, it is ignored and will not participate in priority output queueing.

## Examples

The following example activates priority output queueing on LAN Extender interface 0:

```
Router(config-if)# priority-list 5 protocol bridge medium list 701
Router(config-if)# lex interface 0
Router(config-if)# lex priority-group 5
```

## Related Commands

| Command | Description |
|---|---|
| **priority-list protocol** | Establishes queueing priorities based on the protocol type. |

# lex retry-count

To define the number of times to resend commands to the LAN Extender chassis, use the **lex retry-count** command in interface configuration mode. To return to the default value, use the **no** form of this command.

**lex retry-count** *number*

**no lex retry-count** *number*

## Syntax Description

| | |
|---|---|
| *number* | Number of times to retry sending commands to the LAN Extender. It can be a number in the range 0 to 100. The default is 10. |

## Defaults

10 retries

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |

## Usage Guidelines

After the router has sent a command the specified number of times without receiving an acknowledgment from the LAN Extender, it stops sending the command altogether.

## Examples

The following example resends commands 20 times to the LAN Extender:

```
Router(config-if)# lex interface 0
Router(config-if)# lex retry-count 20
```

## Related Commands

| Command | Description |
|---|---|
| **lex timeout** | Defines the amount of time to wait for a response from the LAN Extender. |

# lex timeout

To define the amount of time to wait for a response from the LAN Extender, use the **lex timeout** command in interface configuration mode. To return to the default time, use the **no** form of this command.

**lex timeout** *milliseconds*

**no lex timeout** [*milliseconds*]

## Syntax Description

| | |
|---|---|
| *milliseconds* | Time, in milliseconds, to wait for a response from the LAN Extender before resending the command. It can be a number in the range 500 to 60,000. The default is 2000 ms. |

## Defaults

2000 ms (2 seconds)

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |

## Usage Guidelines

The **lex timeout** command defines the amount of time that the router waits to receive an acknowledgment after having sent a command to the LAN Extender.

## Examples

The following example causes unacknowledged packets to be resent at 4-second intervals:

```
Router(config-if)# lex interface 0
Router(config-if)# lex timeout 4000
```

## Related Commands

| Command | Description |
|---|---|
| **lex retry-count** | Defines the number of times to resend commands to the LAN Extender chassis. |

# linecode

To select the line-code type for T1 or E1 lines, use the **linecode** command in controller configuration mode.

**linecode** {**ami** | **b8zs** | **hdb3**}

## Syntax Description

| | |
|---|---|
| **ami** | Specifies alternate mark inversion (AMI) as the line-code type. Valid for T1 or E1 controllers. This is the default for T1 lines. |
| **b8zs** | Specifies B8ZS as the line-code type. Valid for T1 controller only. |
| **hdb3** | Specifies high-density bipolar 3 (hdb3) as the line-code type. Valid for E1 controller only. This is the default for E1 lines. |

## Defaults

AMI is the default for T1 lines.

High-density bipolar 3 is the default for E1 lines.

## Command Modes

Controller configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |

## Usage Guidelines

Use this command in configurations in which the router or access server must communicate with T1 fractional data lines. The T1 service provider determines which line-code type, either **ami** or **b8zs**, is required for your T1 circuit. Likewise, the E1 service provider determines which line-code type, either **ami** or **hdb3**, is required for your E1 circuit.

This command does not have a **no** form.

## Examples

The following example specifies B8ZS as the line-code type:

```
Router(config-controller)# linecode b8zs
```

# line-termination

To specify the line termination for the E1 port on a trunk card, use the **line-termination** command in controller configuration mode. To return to the default line termination, use the **no** form of this command.

**line-termination** {**75-ohm** | **120-ohm**}

**no line-termination**

## Syntax Description

| | |
|---|---|
| **75-ohm** | Specifies 75-ohm unbalanced termination. |
| **120-ohm** | Specifies 120-ohm balanced termination. This is the default. |

## Defaults

120-ohms

## Command Modes

Controller configuration

## Command History

| Release | Modification |
|---|---|
| 11.3(2)AA | This command was introduced. |

## Usage Guidelines

To determine the line termination setting for the port, use the **show controllers e1** command.

## Examples

In the following example, the line termination is set to 75 ohms for the E1 port located in shelf 6, slot 0, port 0:

```
Router# configure terminal
Router(config)# controller e1 6/0/0
Router(config-controller)# line-termination 75-ohm
Router(config-controller)# exit
Router(config)# exit
Router#
```

## Related Commands

| Command | Description |
|---|---|
| **show controllers e1** | Displays information about the E1 links supported by the NPM (Cisco 4000) or MIP (Cisco 7500 series). |

# link-test

To reenable the link-test function on a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router, use the **link-test** command in hub configuration mode. Use the **no** form of this command to disable this feature if a pre-10BaseT twisted-pair device not implementing link test is connected to the hub port.

**link-test**

**no link-test**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Enabled

## Command Modes

Hub configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |

## Usage Guidelines

This command applies to a port on an Ethernet hub only. Disable this feature if a 10BaseT twisted-pair device at the other end of the hub does not implement the link test function.

## Examples

The following example disables the link test function on hub 0, ports 1 through 3:

```
Router(config)# hub ethernet 0 1 3
Router(config-hub)# no link-test
```

## Related Commands

| Command | Description |
|---|---|
| **hub** | Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router. |

# local-lnm

To enable Lanoptics Hub Networking Management of a PCbus Token Ring interface, use the **local-lnm** command in interface configuration mode. To disable Lanoptics Hub Networking Management, use the **no** form of this command.

**local-lnm**

**no local-lnm**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Management is not enabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |

## Usage Guidelines

The Token Ring interface on the AccessPro PC card can be managed by a remote LAN manager over the PCbus interface. At present, the Lanoptics Hub Networking Management software running on an IBM compatible PC is supported.

## Examples

The following example enables Lanoptics Hub Networking Management:

```
Router(config-if)# local-lnm
```

# logging event

To enable notification of interface, subinterface, and Frame Relay data link connection identifier (DLCI) data link status changes, use the **logging event** command in interface configuration mode. To disable notification, use the **no** form of this command.

**logging event** {**dlci-status-change | link-status | subif-link-status [ignore-bulk]**}

**no logging event** {**dlci-status-change | link-status | subif-link-status [ignore-bulk]**}

## Syntax Description

| | |
|---|---|
| **dlci-status-change** | Enables notification of Frame Relay DLCI status changes.<br>**Note** This option is supported only when the encapsulation on the interface is Frame Relay. |
| **link-status** | Enables notification of interface data link status changes. |
| **subif-link-status** | Enables notification of subinterface data link status changes. |
| **ignore-bulk** | Suppresses link status messages for subinterfaces when they are caused by a state change of the main interface. |

## Defaults

For system images, notification of interface, subinterface, and Frame Relay DLCI data link status changes is enabled by default.

For boot images, notification of Frame Relay subinterface and DLCI data link status changes is disabled by default. Notification of interface data link status changes is enabled by default.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0 | This command was introduced. |
| 12.2(32)S | The **ignore-bulk** keyword was integrated into the Cisco IOS Release 12.2(32)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.3(7)T | The **ignore-bulk** keyword was integrated into the Cisco IOS Release 12.3(7)T. |

## Examples

The following example shows how to enable notification of subinterface link status changes:

```
Router(config-if)# logging event subif-link-status
```

The following are examples of Frame Relay DLCI and subinterface status change notification messages filtered by the **logging event** command:

```
00:16:22: %FR-5-DLCICHANGE: Inteface Serial3/0/0:1 - DLCI 105 state changed to INACTIVE
00:16:22: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0/0:1.5, changed state
to down
```

# logging-events

to print typical T3 controller Up and Down messages on a Channelized T3 Port Adapter, use the **logging-events** command in T3 controller configuration mode. Use the **no** form of this command to disable printing of the T3 controller Up and Down messages.

**logging-events** [**detail**]

**[no] logging-events**

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Enables printing the reason code when a T3 controller changes from the Up to Down state. |

## Defaults

The **logging-events** command is the default.

## Command Modes

T3 controller configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(19c) | This command was introduced. |

## Usage Guidelines

When the **no logging-events** command disables printing of the T3 controller Up and Down messages, these messages will neither appear on the console nor in the logs.

## Examples

The following example uses the **logging-events** [**detail**] command to show the Out-of-Frame (OOF) reason code when the T3 controller changes from an Up state to a Down state:

```
Router(config-controller)# logging-events detail

*Jun 19 17:47:50: %CONTROLLER-5-DOWNDETAIL: Controller T3 4/1, changed state to down due
to OOF
```

## Related Commands

| Command | Description |
|---|---|
| t1 logging-events | Prints the typical T1 controller Up and Down messages on a channelized T3 port adapter. |

# loopback (interface)

To diagnose equipment malfunctions between the interface and device, use the **loopback** command in interface configuration mode. To disable the test, use the **no** form of this command.

**loopback**

**no loopback**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |

## Usage Guidelines

### Loopback on HSSI Cards

On High-Speed Serial Interface (HSSI) cards, the loopback function configures a two-way internal and external loop on the HSA applique of the specific interface.

### Loopback on MCI and SCI Serial Interface Cards

On MCI and SCI serial interface cards, the loopback functions when a CSU/DSU or equivalent device is attached to the router or access server. The **loopback** command loops the packets through the CSU/DSU to configure a CSU loop, when the device supports this feature.

### Loopback on MCI and MEC Ethernet Cards

On the MCI and MEC Ethernet cards, the interface receives back every packet it sends when the **loopback** command is enabled. Loopback operation has the additional effect of disconnecting network server functionality from the network.

### Loopback on CSC-FCI FDDI Cards

On the CSC-FCI FDDI card, the interface receives back every packet it sends when the **loopback** command is enabled. Loopback operation has the additional effect of disconnecting network server functionality from the network.

### Loopback on Token Ring Interface Cards

On all Token Ring interface cards (except the 4-megabit CSC-R card), the interface receives back every packet it sends when the **loopback** command is enabled. Loopback operation has the additional effect of disconnecting network server functionality from the network.

### Active Loopback Interfaces

To show interfaces currently in loopback operation, use the **show interfaces loopback** EXEC command.

**Note** Loopback does not work on an X.21 DTE because the X.21 interface definition does not include a loopback definition.

## Examples

The following example configures the loopback test on Ethernet interface 4:

```
Router(config)# interface ethernet 4
Router(config-if)#  loopback
```

## Related Commands

| Command | Description |
|---|---|
| **down-when-looped** | Configures an interface to inform the system it is down when loopback is detected. |
| **show interfaces loopback** | Displays information about the loopback interface. |

# loopback (E3/T3 interface)

To loop the serial interface on a PA-E3 or PA-T3 port adapter, use the **loopback** command in interface configuration mode. To remove the loopback, use the **no** form of this command.

**PA-E3 Port Adapter**

**loopback** {**dte** | **local** | **network** {**line** | **payload**}}

**no loopback**

**PA-T3 Port Adapter**

**loopback** {**dte** | **local** | **network** {**line** | **payload**} | **remote**}

**no loopback**

## Syntax Description

| | |
|---|---|
| **dte** | Sets the loopback after the LIU toward the terminal. |
| **local** | Sets the loopback after going through the framer toward the terminal. |
| **network** {**line** \| **payload**} | Sets the loopback toward the network before going through the framer (**line**) or after going through the framer (**payload**). |
| **remote** | Sends a far-end alarm control (FEAC) to set the remote framer in loopback. |

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.1 CA | This command was introduced. |

## Usage Guidelines

Use this command for troubleshooting purposes.

To verify that a loopback is configured on the interface, use the **show interfaces serial** or **show interfaces loopback** EXEC command.

## Examples

The following example configures the serial interface located in slot 3/0/0 for a local loopback:

```
Router(config)# interface serial 3/0/0
Router(config-if)#  loopback local
```

## Related Commands

| Command | Description |
|---|---|
| **show controllers serial** | Displays information that is specific to the interface hardware. |
| **show interfaces loopback** | Displays information about the loopback interface. |
| **show interfaces serial** | Displays information about a serial interface. |

# loopback (T1 interface)

To loop individual T1 channels on the CT3IP in Cisco 7000 series routers with the RSP7000 and RSP7000CI and in Cisco 7500 series routers, use the **loopback** command in interface configuration mode. To remove the loopback, use the **no** form of this command.

**loopback** [**local** | **network** {**line** | **payload**} | **remote** {**line** {**fdl** {**ansi** | **bellcore**} | **inband**} | **payload** [**fdl**] [**ansi**]}]

**no loopback**

## Syntax Description

| | |
|---|---|
| **local** | (Optional) Loops the router output data back toward the router at the T1 framer and sends an alarm indication signal (AIS) signal out toward the network. |
| **network** {**line** \| **payload**} | (Optional) Loops the data back toward the network before the T1 framer and automatically sets a local loopback at the High-Level Data Link Control (HDLC) controllers (line), or loops the payload data back toward the network at the T1 framer and automatically sets a local loopback at the HDLC controllers (payload). |
| **remote line fdl** {**ansi** \| **bellcore**} | (Optional) Sends a repeating, 16-bit Extended Superframe (ESF) data link code word (00001110 11111111 for FDL ANSI and 00010010 11111111 for FDL Bellcore) to the remote end requesting that it enter into a network line loopback. Specify the **ansi** keyword to enable the remote line Facility Data Link (FDL) ANSI bit loopback on the T1 channel, per the ANSI T1.403 Specification. Specify the **bellcore** keyword to enable the remote SmartJack loopback on the T1 channel, per the TR-TSY-000312 Specification. |
| **remote line inband** | (Optional) Sends a repeating, 5-bit inband pattern (00001) to the remote end requesting that it enter into a network line loopback. |
| **remote payload** [**fdl**] [**ansi**] | (Optional) Sends a repeating, 16-bit ESF data link code word (00010100 11111111) to the remote end requesting that it enter into a network payload loopback. Enables the remote payload FDL ANSI bit loopback on the T1 channel.<br>You can optionally specify **fdl** and **ansi**, but it is not necessary. |

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.1 CA | This command was introduced. |

## Usage Guidelines

Use this command for troubleshooting purposes.

To better diagnose T1 provisioning problems, you can place the remote CSU or remote SmartJack into loopback. The **loopback remote line fdl** interface configuration command allows you to place either the CSU or the SmartJack into loopback:

- **ansi**—Places the CSU into loopback, per the ANSI T1.403 Specification.
- **bellcore**—Places the SmartJack into loopback, per the TR-TSY-000312 Specification.

When both are configured, transmission of LOF indication (yellow alarm) takes priority over transmission of some FDL messages.

If the remote loopback appears not to be working, use the **show controllers t3** command to determine if the given T1 is currently attempting to transmit a LOF indication (yellow alarm):

```
Router# show controllers t3 0/0/0:2
 T3 0/0/0 is up.
   CT3 H/W Version: 5, CT3 ROM Version: 1.2, CT3 F/W Version: 2.5.9
   Mx H/W version: 2, Mx ucode ver: 1.34

   T1 2 is down, speed: 1536 kbs, non-inverted data
   timeslots: 1-24
   FDL per AT&T 54016 spec.
   Transmitter is sending LOF Indication.
   Receiver is getting AIS.
```

If the transmitter is sending a LOF indication, as in the previous example, stop the transmission of the LOF indication (yellow alarm) with the **no t1 yellow generation** configuration command as shown in the following example:

```
Router(config)# controllers t3 0/0/0
Router(config-controll)# no t1 2 yellow generation
Router(config-controll)# Ctrl-D
```

To verify that the transmission of the LOF indication (yellow alarm) has stopped, use the **show controllers t3** command:

```
Router# show controlloers t3 0/0/0:2
 T3 0/0/0 is up.
   CT3 H/W Version: 5, CT3 ROM Version: 1.2, CT3 F/W Version: 2.5.9
   Mx H/W version: 2, Mx ucode ver: 1.34
   T1 2 is down, speed: 1536 kbs, non-inverted data
   timeslots: 1-24
   FDL per AT&T 54016 spec.
   Receiver is getting AIS.
   Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
   Yellow Alarm Generation is disabled
```

Then retry the remote loopback command. When diagnosis is complete, remember to reenable the LOF indication (yellow alarm).

You can also loopback all the T1 channels by using the **loopback** (CT3IP) interface configuration command.

## Examples

The following example configures T1 channel 5 for a local loopback:

```
Router(config)# interface serial 3/0/0:5
Router(config-if)#  loopback local
```

## Related Commands

| Command | Description |
|---|---|
| **loopback (T3 controller)** | Loops the entire T3 (all 28 T1 channels) on the CT3IP in Cisco 7500 series routers. |
| **no t1 yellow generation** | Enables detection and generation of yellow alarms for a T1 channel on the CT3IP in Cisco 7500 series routers. |

# loopback (T3 controller)

To loop the entire T3 (all 28 T1 channels) on the CT3 in a Cisco AS5800 universal access server or on the CT3IP in Cisco 7500 series routers, use the **loopback** command in controller configuration mode. To remove the loopback, use the **no** form of this command.

**loopback** [**local** | **network** | **remote**]

**no loopback**

## Syntax Description

| | |
|---|---|
| **local** | (Optional) Loops the data back toward the router and sends an alarm indication signal (AIS) signal out toward the network. |
| **network** | (Optional) Loops the data toward the network at the T1 framer. |
| **remote** | (Optional) Sends a far-end alarm control (FEAC) request to the remote end requesting that it enter into a network line loopback. FEAC requests (and therefore remote loopbacks) are possible only when the T3 is configured for C-bit framing. The type of framing used is determined by the equipment you are connecting to (for more information, see the **framing** controller command). |

## Defaults

Disabled

## Command Modes

Controller configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |

## Usage Guidelines

Use this command for troubleshooting purposes.

You can also loopback each T1 channel by using the **loopback** interface configuration command for T1.

For more information, refer to the "Troubleshoot the T3 and T1 Channels" section in the "Configuring Serial Interfaces" chapter of the *Cisco IOS Interface Configuration Guide*.

## Examples

The following example configures the CT3 or CT3IP for a local loopback:

```
Router(config)# controller t3 3/0/0
Router(config-controller)# loopback local
```

## Related Commands

| Command | Description |
|---|---|
| **loopback remote (interface)** | Loops packets through a CSU/DSU, over a DS3 link or a channelized T1 link, to the remote CSU/DSU and back. |
| **framing** | Selects the frame type for the T1 or E1 data line. |
| **loopback** | Places the specified module in loopback mode. |

# loopback applique

To configure an internal loop on the High Speed Serial Interface (HSSI) applique, use the **loopback applique** command in interface configuration mode. To remove the loop, use the **no** form of this command.

**loopback applique**

**no loopback applique**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |

## Usage Guidelines

This command loops the packets within the applique to provide a way to test communication within the router or access server. It is useful for sending pings to yourself to check functionality of the applique.

To show interfaces that are currently in loopback operation, use the **show interfaces loopback** EXEC command.

## Examples

The following example configures the loopback test on the HSSI applique:

```
Router(config)# interface serial 1
Router(config-if)# loopback applique
```

## Related Commands

| Command | Description |
|---|---|
| **show interfaces loopback** | Displays information about the loopback interface. |

# loopback dte

To loop packets back to the DTE from the CSU/DSU, when the device supports this feature, use the **loopback dte** command in interface configuration mode. To remove the loop, use the **no** form of this command.

**loopback dte**

**no loopback dte**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |

## Usage Guidelines

This command is useful for testing the DTE-to-DCE cable.

This command is used to test the performance of the integrated CSU/DSU. Packets are looped from within the CSU/DSU back to the serial interface of the router. Send a test ping to see if the packets successfully looped back. To cancel the loopback test, use the **no loopback dte** command.

When using the 4-wire 56/64-kbps CSU/DSU module, an out-of-service signal is transmitted to the remote CSU/DSU.

To show interfaces that are lcurrently in loopback operation, use the **show interfaces loopback** EXEC command.

## Examples

The following example configures the loopback test on the DTE interface:

```
Router(config)# interface serial 0
Router(config-if)# loopback dte
```

## Related Commands

| Command | Description |
|---|---|
| **show interfaces loopback** | Displays information about the loopback interface. |

# loopback line

To loop packets completely through the CSU/DSU to configure the CSU loop, use the **loopback line** command in interface configuration mode. To remove the loop, use the **no** form of this command.

**loopback line** [**payload**]

**no loopback line** [**payload**]

## Syntax Description

| | |
|---|---|
| **payload** | (Optional) Configures a loopback point at the DSU and loops data back to the network on an integrated CSU/DSU. |

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |

## Usage Guidelines

This command is useful for testing the DCE device (CSU/DSU) itself. When the **loopback line** command is configured on the 2-wire 56-kbps CSU/DSU module or the 4-wire 56/64-kbps CSU/DSU modules, the network data loops back at the CSU and the router data loops back at the DSU. If the CSU/DSU is configured for switched mode, you must have an established connection to perform a payload-line loopback. To loop the received data through the minimum amount of CSU/DSU circuitry, issue the **loopback line** command.

When you issue the **loopback line payload** command on an integrated CSU/DSU module, the router cannot transmit data through the serial interface for the duration of the loopback. Choosing the DSU as a loopback point loops the received-network data through the maximum amount of CSU/DSU circuitry. Data is not looped back to the serial interface. An active connection is required when operating in switched mode for payload loopbacks.

If you enable the **loopback line** command on the fractional T1/T1 module, the CSU/DSU performs a full-bandwidth loopback through the CSU portion of the module and data transmission through the serial interface is interrupted for the duration of the loopback. No reframing or corrections of bipolar violation errors or cyclic redundancy check (CRC) errors are performed. When you configure the **loopback line payload** command on the FT1/T1 module, the CSU/DSU performs a loopback through the DSU portion of the module. The **loopback line payload** command reframes the data link, regenerates the signal, and corrects bipolar violations and Extended Super Frame CRC errors.

When performing a T1-line loopback with Extended Super Frame, communication over the facilities data link is interrupted, but performance statistics are still updated. To show interfaces currently in loopback operation, use the **show service-module** EXEC command.

To show interfaces that are currently in loopback operation on other routers, use the **show interfaces loopback** EXEC command.

## Examples

The following example configures the loopback test on the DCE device:

```
Router(config)# interface serial 1
Router(config-if)# loopback line
```

The following example shows how to configure a payload loopback on a Cisco 2524 or 2525 router:

```
Router1(config-if)# loopback line payload
Loopback in progress
Router1(config-if)# no loopback line
```

The following example shows the output on a Cisco 2524 or 2525 router when you loop a packet in switched mode without an active connection:

```
Router1(config-if)# service-module 56k network-type switched
Router1(config-if)# loopback line payload
Need active connection for this type of loopback
% Service module configuration command failed: WRONG FORMAT.
```

## Related Commands

| Command | Description |
|---|---|
| **show interfaces loopback** | Displays information about the loopback interface. |
| **show service-module** | Displays the performance report for an integrated CSU/DSU. |