



## Solving Ethernet Problems

---

This chapter explains how to solve Ethernet problems and contains the following sections:

- [Ethernet Overview, page 7-2](#)
- [Using show interface Commands, page 7-3](#)
- [Troubleshooting Ethernet Media Problems, page 7-7](#)



---

**Note**

For a description of the features, modifications, and caveats for the Cisco Integrated Communications System 7750 (Cisco ICS 7750) release 2.6.0, refer to the [Release Notes for System Software Release 2.6.0 on the Cisco ICS 7750](#).

---



---

**Note**

Refer to [Ethernet Technologies](#) for additional information on Ethernet network elements, topologies, and structures. For additional information about troubleshooting Ethernet collisions, refer to [Troubleshooting Ethernet Collisions](#).

---

# Ethernet Overview

The term *Ethernet* refers to all carrier sense multiple access collision detect (CSMA/CD) LANs that conform to Ethernet specifications, including Institute of Electrical and Electronics Engineers (IEEE) 802.3.

Both Ethernet and IEEE 802.3 LANs are broadcast networks. In other words, all stations see all frames, regardless of whether they represent an intended destination. Each station must examine received frames to determine whether the station is a destination. If it is a destination, the frame is passed to a higher protocol layer for appropriate processing.

## Types of Connections

The maximum distances for Ethernet and Fast Ethernet network segments and connections depend on the type of transmission cable being used. The terms 10Base-T and 100Base-T are industry terms for the following:

- 10-Mbps transmission rate (10), or 100-Mbps transmission rate (100)
- Using baseband technology (Base)
- By means of twisted pair wires (T)

Ethernet is most similar to IEEE 802.3 10Base-5. Both of these protocols specify a bus topology network with a connecting cable between the end stations and the network medium. In the case of Ethernet, that cable is called a *transceiver cable*. The transceiver cable connects to a transceiver device attached to the physical network medium. The IEEE 802.3 configuration is much the same, except that the connecting cable is referred to as an *attachment unit interface* (AUI), and the transceiver is called a *media attachment unit* (MAU). In both cases, the connecting cable attaches to an interface board (or interface circuitry) within the end station.

## Collisions

Stations on a CSMA/CD LAN can access the network at any time. Before sending data, CSMA/CD stations listen to the network to see if it is already in use. If it is, the station waits to transmit. If the network is not in use, the station transmits. A *collision* occurs when two stations transmit simultaneously. In this case, both

transmissions are damaged, and the stations must retransmit at some later time. Backoff algorithms determine when the colliding stations retransmit. CSMA/CD stations can detect collisions, so they know when they must retransmit.

Collisions are far less frequent in full-duplex mode Ethernet networks.

## Using show interface Commands

When you are troubleshooting Ethernet media, the **show interface ethernet** and **show interface fastethernet** privileged EXEC commands provide several key fields of information that can help you isolate problems related to Ethernet interfaces.

### Syntax

Following are the syntax for the **show interface ethernet** command and the syntax for the **show interface fastethernet** command:

```
show interface ethernet [slot | interface] [accounting]  
show interface fastethernet [slot | interface] [accounting]
```

where:

- *slot* (optional) identifies the slot of a particular card in the Cisco ICS 7750 (legal slot values are 1 through 7).
- *interface* (optional) identifies a particular interface, such as Ethernet 0.
- **accounting** (optional) displays the number of packets of each protocol type that has been sent through the interface.

If you do not provide values for the *slot* and *interface* arguments, the command displays statistics for all Ethernet interfaces on the network. The optional keyword **accounting** displays the number of packets of each protocol type that has been sent through the interface (or all interfaces).

## Understanding Command Output

**Example 7-1** shows sample output from the **show interface ethernet** command for the Ethernet 0 interface. For a description of the most significant fields as indicated by the callouts—the numbers in square brackets—see [Table 7-1](#).

### **Example 7-1** Output of show interface ethernet Command

```
Cisco ICS 7750#show interface ethernet 0
[1] Ethernet 0 is up, line protocol is up
    Hardware is MCI Ethernet, address is aa00.0400.0134 (via 0000.0c00.4369)
    Internet address is 131.108.1.1, subnet mask is 255.255.255.0
[2] MTU 1500 bytes,
    [3] BW 10000 Kbit,
    [4] DLY 1000 usec,
    [5] rely 255/255,
    [6] load 1/255
    Encapsulation ARPA, loopback not set, keepalive set (10 sec)
    ARP type: ARPA, PROBE, ARP Timeout 4:00:00
[7] Last input 0:00:00, output 0:00:00,
    [8] output hang never
[9] Output queue 0/40, 0 drops; input queue 0/75, 2 drops
    Five minute input rate 61000 bits/sec, 4 packets/sec
    Five minute output rate 1000 bits/sec, 2 packets/sec
[10] 2295197 packets input, 305539992 bytes, 0 no buffer
    Received 1925500 broadcasts, 0 runts, 0 giants
    3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    3594664 packets output, 436549843 bytes, 0 underruns
[11] 8 output errors,
    [12] 1790 collisions,
    [13] 10 interface resets,
    [14] 0 restarts
```

**Table 7-1** Descriptions for the show interface ethernet Command Example

Callout	Field	Description
1	Interface and line protocol status	Indicates whether the interface hardware is currently active or whether it has been disabled by an administrator. If the interface is shown as “disabled,” the device has received more than 5,000 errors in a keepalive interval, which is 10 seconds by default. If the line protocol is shown as “down” or “administratively down,” the software processes that handle the line protocol consider the interface unusable (because of unsuccessful keepalives) or the interface has been disabled by an administrator.
2	MTU <sup>1</sup>	Maximum packet size, in bytes, that an interface can handle.
3	BW <sup>2</sup>	Interface bandwidth, in kilobits per second.
4	DLY <sup>3</sup>	Interface delay, in microseconds.
5	Rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
6	Load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
7	Last input and last output	Number of hours, minutes, and seconds since the last packet was successfully received (input) and transmitted (output) by an interface. Last input can help you determine how much time has passed since the failure of a particular interface.
8	Output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long.
9	Output queue, input queue, drops	Number of packets in the output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped due to a full queue.

**Table 7-1** Descriptions for the show interface ethernet Command Example (continued)

Callout	Field	Description
10	Input errors, including CRC errors and framing errors	Total number of errors related to no buffer <sup>4</sup> , runt <sup>5</sup> , giant <sup>6</sup> , CRC <sup>7</sup> , frame <sup>8</sup> , overrun <sup>9</sup> , ignored <sup>10</sup> , and abort. Other input-related errors can also increment the count, so this sum might not balance with the other counts.
11	Output errors	Number of times that the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
12	Collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN. LANs can become overextended when an Ethernet or transceiver cable is too long or when there are more than two repeaters between stations.
13	Interface resets	Number of times that an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds.
14	Restarts	Number of times that an Ethernet controller has been restarted because of errors.

1. MTU = maximum transmission unit.
2. BW = bandwidth.
3. DLY = delay. Delay is the time that it takes for packets to travel between two endpoints. For voice packets, delay manifests itself when long pauses in conversation cause the receiver (the person listening) to start to talk before the sender (the person talking) is finished.
4. No buffer errors occur when a packet is discarded because there was no buffer space. Broadcast storms on Ethernet networks are often responsible for no buffer events. Compare with *ignored*.
5. Runts are packets that are discarded because they are smaller than the medium's minimum packet size. Any Ethernet packet that is less than 64 bytes is considered a runt.
6. Giants are packets that are discarded because they are larger than the medium's maximum packet size. Any Ethernet packet that is more than 1,518 bytes is considered a giant.
7. CRC = cyclic redundancy check. A CRC error occurs when the CRC generated by the originating station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus. A high number of CRCs is usually the result of collisions or a station transmitting bad data.

8. Framing errors occur when packets are received with a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
9. Overruns represent the number of times that the receiver hardware is unable to hand received data to a hardware buffer because the input rate exceeds the receiver's ability to handle the data.
10. Ignored packets are those that are discarded because the interface hardware does not have enough internal buffers. Broadcast storms and bursts of noise can result in an increased number of ignored packets. Compare with *no buffer*.

## Troubleshooting Ethernet Media Problems

The following are possible causes of Ethernet media problems:

- Excessive noise
- Excessive collisions
- Excessive runt frames
- Late collisions
- No link integrity on 10Base-T, 100Base-T4, or 100Base-TX

Table 7-2 describes ways to solve these problems.

**Table 7-2 Ethernet Media Problems and Solutions**

Media Problem	Solution
Excessive noise	<p><b>Step 1</b> Use the <b>show interface ethernet</b> exec command to determine the status of the device's Ethernet interfaces. The presence of many CRC errors but not many collisions is an indication of excessive noise.</p> <p><b>Step 2</b> Inspect the cables for damage.</p> <p><b>Step 3</b> Look for badly spaced taps<sup>1</sup>, which could cause reflections.</p> <p><b>Step 4</b> If you are using 100Base-TX, make sure you are using Category 5 cabling.<sup>2</sup></p>

**Table 7-2 Ethernet Media Problems and Solutions (continued)**

Media Problem	Solution
Excessive collisions	<p><b>Step 1</b> Use the <b>show interface ethernet</b> command to check the rate of collisions. The total number of collisions with respect to the total number of output packets should be 0.1 percent or less.</p> <p><b>Step 2</b> Use a TDR<sup>3</sup> to find any unterminated Ethernet cables.</p> <p><b>Step 3</b> Look for a jabbering<sup>4</sup> transceiver attached to a host. This might require host-by-host inspection or the use of a protocol analyzer.<sup>5</sup></p>
Excessive runt frames	<p><b>Step 1</b> In a shared Ethernet environment, runt frames are almost always caused by collisions. If the collision rate is high, see the “Excessive collisions” problem in this table.</p> <p><b>Step 2</b> If runt frames occur when collision rates are not high or in a switched Ethernet environment, then they are the result of underruns<sup>6</sup> or bad software on a network interface card.</p> <p><b>Step 3</b> Use a protocol analyzer to try to determine the source address of the runt frames.</p>
Late collisions	<p><b>Step 1</b> Use a protocol analyzer to check for late collisions. Late collisions should never occur in a properly designed Ethernet network. They usually occur when Ethernet cables are too long or when there are too many repeaters in the network.</p> <p><b>Step 2</b> Verify that the diameter of the network is within specification.</p>

**Table 7-2 Ethernet Media Problems and Solutions (continued)**

Media Problem	Solution
No link integrity on 10Base-T, 100Base-T4, or 100Base-TX	<p><b>Step 1</b> Make sure that you are not using 100Base-T4 when only two pairs of wire are available. 100Base-T4 requires four pairs.</p> <p><b>Step 2</b> Look for a 10Base-T, 100Base-T4, or 100Base-TX mismatch (such as a card that does not work with a particular interface).</p> <p><b>Step 3</b> Determine whether there is cross-connect (for example, be sure that straight-through cables are not being used between a station and the hub).</p> <p><b>Step 4</b> Check for excessive noise (see the problem “Excessive noise” earlier in this table).</p>

1. The link between a bus and a drop cable that connects a workstation to the bus.
2. Category 5 (CAT5) cables support frequencies up to 100 MHz, while Category 3 (CAT3) cables support frequencies no higher than 16 MHz. For this and other reasons, CAT5 is an increasingly popular choice, especially in networks that carry both data and voice traffic.
3. TDR = time domain reflectometer. A device that sends signals through a network medium to check cable continuity and other attributes. (See the [“Using Third-Party Troubleshooting Tools”](#) section on page 2-22.)
4. Jabber occurs when a device that is experiencing circuitry or logic failure continuously sends random (garbage) data.
5. A specialized computer or program that analyzes the traffic on a LAN. For more information about protocol analyzers (also known as network analyzers), see the [“Using Third-Party Troubleshooting Tools”](#) section on page 2-22.)
6. Each time that a transmitter is running faster than a routing device can handle, the routing device reports an underrun.

