Chapter 15

L2TP Disconnect Cause Codes

Table 76 describes the Point-to-Point Protocol (PPP) disconnect cause codes that are displayed by the **show l2tp received-disconnect-cause-summary** command, sorted by code number. For additional information, see RFC 3145.

Table 76: PPP Disconnect Cause Codes

Code	Name	Description
0	no info	Code 0 includes disconnect causes that are not specifically identified by other codes. This code is generated in the following circumstances: ■ Internal resource constraints (for example, excessive load or reduced resource availability) have prevented the generation of a more specific disconnect code. ■ RFC 3145 does not define a disconnect code that corresponds to the cause of the disconnection. The following list shows current disconnection causes on an E-series LNS that do not have a specific disconnect cause codes: ■ The peer initiated termination of LCP after the completion of LCP negotiations, but prior to proceeding to authentication of NCP negotiation. No conditions occurred that enabled the LNS to infer a more informative disconnect code. ■ The peer initiated renegotiation of LCP. ■ Invalid local MRU (for example, MRU negotiation has been disabled, but the lower MRU is less than the default MRU of 1500). ■ Unexpected local MLPPP MRRU for existing bundle (RFC 3145 code 10 covers peer MRRU mismatches, but not local mismatches). ■ Authentication failures not covered by any of the authentication-related codes (codes 13-16), such as: ■ Authentication denial of the local LCP by the peer ■ Local authentication failure due to no resources ■ Local authentication failure due to no authenticator
1	admin disconnect	The disconnection was a result of direct administrative action, including: ■ The administrator shut down the network or link interface. ■ The administrator logged out the subscriber.
2	renegotiation disabled	Code 2 is not used; the E-series LNS is always capable of renegotiating LCP if proxy data is not available.

Table 76: PPP Disconnect Cause Codes (continued)

Code	Name	Description
3	normal disconnect	Indicates that one of the following events occurred: ■ user-initiated logout (direction 1) ■ session timeout (direction 2) ■ inactivity timeout (direction 2) ■ address lease expired (direction 2) The E-series LNS determines by inference that a normal disconnect has occurred for direction 1. The LNS does this when the peer initiates LCP termination after proceeding beyond the successful negotiation of LCP (that is, after starting authentication signaling or NCP negotiation).
4	compulsory encryption refused	Code 4 with direction 2 is generated if the following conditions are met: ■ The peer initiates LCP termination without having proceeded beyond the completion of LCP negotiation, and ■ Prior to receiving the terminate request from the peer, the local LCP has sent a Protocol Reject in response to any packet for Encryption Control Protocol (ECP) protocols (protocol codes 0x8053, 0x8055) from the peer. Code 4 with direction 1 is never generated, because the E-series LNS never requests ECP.
5	lcp failed to converge	An LCP configuration error prevented LCP from converging; the two peers attempted to negotiate but did not agree on acceptable LCP parameters.
6	lcp peer silent	LCP negotiation timed out; the LNS did not receive any LCP packets from the LAC.
7	lcp magic number error	A magic number error was detected; this indicates a possible looped back link.
8	lcp keepalive error	The keepalive drop count was exceeded.
9	lcp mlppp endpoint discriminator mismatch	Code 9 is not used. Dynamic MLPPP bundling, which is the only kind of MLPPP bundling supported for MLPPP/L2TP, uses the endpoint discriminator as part of the key for bundle selection. Therefore, there will never be an unexpected endpoint discriminator for an existing MLPPP bundle.
10	lcp mlppp mrru not valid	The link attempted to join an existing MLPPP bundle whose peer maximum received reconstructed unit (MRRU) did not match the peer MRRU negotiated by the link.
11	lcp mlppp peer ssn invalid	Code 11 is not used; the short sequence number (SSN) option is not supported.
12	lcp callback refused	Code 12 with direction 2 is generated when the following conditions are met: ■ The peer initiates LCP termination without having proceeded to NCP negotiation, and ■ Prior to the termination, the local LCP has responded with a negative acknowledgement (NAK) to a callback option (LCP option 13) from the peer. The E-series LNS never generates code 12 with direction 1 because the LNS never requests callback.
13	authenticate timed out	Authentication failed because the authentication protocol timed out; either the CHAP Authenticate Response or the PAP Authenticate Request was not received.
14	authenticate mlppp name mismatch	Code 14 is not used. Dynamic MLPPP bundling, which is the only kind of MLPPP bundling supported for MLPPP/L2TP, uses the authenticated name as part of the key for bundle selection. Therefore, there will never be an unexpected authenticated name for an existing MLPPP bundle.

Table 76: PPP Disconnect Cause Codes (continued)

Code	Name	Description
15	authenticate protocol refused	No acceptable authentication protocol was negotiated by LCP. ■ Code 15 with direction 1 is generated if the peer rejected all of the authentication protocols requested by the local LCP. ■ Code 15 with direction 2 is generated if the following conditions are met: ■ The peer initiates LCP termination without having proceeded beyond completion of NCP negotiation, and ■ During LCP negotiation, the local LCP responded with a NAK to the final authentication protocol requested by the peer.
16	authenticate failure	■ Code 16 with direction 1 is generated if the local authentication of the peer fails (that is, the authenticator sent a PAP NAK or CHAP Failure packet) ■ Code 16 with direction 2 is generated if the peer authentication of the local LCP fails (that is, the authenticator received a PAP NAK or CHAP Failure packet). Note that there are a variety of causes for authentication failures, including bad credentials (bad name, password or secret) and resource problems.
17	ncp no negotiation completed	Code 17 is generated only if an NCP configuration error has prevented NCP negotiation from converging. This occurs when the two peers do not agree on acceptable NCP parameters within the time allowed for upper-layer negotiation. Code 19 takes precedence over code 17 in situations related to address convergence failure.
18	ncp no ncps available	No NCPs were successfully enabled within the time allowed for upper-layer negotiation.
19	ncp addresses failed to converge	An NCP configuration error has prevented NCP negotiation from converging on acceptable addresses. This occurs if the two peers never agree on acceptable NCP addresses within the time allowed for upper-layer negotiation. ■ Code 19 with direction 1 is generated if the peer denies address parameters requested by the local NCP. ■ Code 19 with direction 2 is generated if the local NCP denies address parameters requested by the peer. The IPv6 interface identifier is considered an address for the purposes of code 19. Code 19 takes precedence over code 17 in situations related to address convergence failure.
20	ncp negotiation inhibited	■ Code 20 with direction 2 indicates that an upper layer negotiation was inhibited for any enabled NCP because the required network-layer parameters were not available as a result of the authentication stage. ■ Code 20 with direction 1 is never generated; the NCPs are never enabled if there is no non-null local address.