

show ppp

This chapter describes the output of the **show ppp** command.

- show ppp, on page 1
- show ppp full username, on page 2
- show ppp statistics pdsn-service, on page 5

show ppp

Table 1: show ppp Command Output Descriptions

Field	Description
PPP Summary	The total number of PPP sessions that are in progress (either active, dormant, being set up, and being disconnected).
Layer Info	The layer status for the various control protocols used in the establishing of the PPP status. Information is displayed for the following: • **LCP:** Link Control Protocol • **IPCP:** Internet Protocol Control Protocol • **CCP:** PPP Compression Control Protocol The information provided represents the total number of sessions that have successfully negotiated the specified control protocol.

Field	Description
Compression	The total number of PPP sessions that meet of each of the following specified characteristics: Sessions using Van Jacobsen (VJ) header compression in either direction (local to remote or remote to local). Sessions using Robust Header Compression (ROHC) in either direction (local to remote or remote to local). Sessions using either the Normal or Stateless compression modes. Sessions using no compression or one of the following compression protocols in either direction (local to remote or remote to local): • STAC • MPPC • DEFLATE
Errors	The total number of errors recorded for all of the PPP sessions that are in progress (either active, dormant, being set up, and being disconnected). Many of the error statistics are recorded for the receiving (indicated by In) and transmission (indicated by Out) of data packets.
Data Stats	Displays cumulative statistics for all of the data received (indicated by In) and transmitted (indicated by Out).

show ppp full username

Table 2: show ppp full username Command Output Descriptions

Field	Description
Username	The subscriber's username.
Callid	The subscriber's call identification (callid) number.
Msid	The subscriber's mobile station identification (MSID) number.
LCP State	Indicates whether or not the Link Control Protocol (LCP) was successfully negotiated (Opened). If not, Not Opened will be displayed.
mtu	The subscriber's maximum transmission unit (MTU) size in octets.
mru	The subscriber's maximum reception unit (MRU) size in octets.

Field	Description
auth algorithm	The protocol the subscriber used for authentication. Possible protocols are: • **CHAP:** Challenge Handshake Authentication Protocol • **PAP:** Password Authentication Protocol
PFC (loc to rem): (rem to loc):	The PPP PFC transmit and receive settings. (loc to rem): Specifies how Protocol field Compression is applied for PPP packets transmitted to the Peer. Possible values are: • ignore • apply • reject (rem to loc): Specifies whether Protocol Field Compressed PPP packets can be received from the Peer. Possible values are: • allow • deny
ACFC (loc to rem): (rem to loc):	Information is displayed for both directions of the session (remote-to-local and local-to-remote).
async map	The PPP asynchronous control character mapping (a 32-bit map). Information is displayed for both directions of the session (remote-to-local and local-to-remote).
IPCP State	Indicates whether or not the Internet Protocol Control Protocol (IPCP) was successfully negotiated (Opened). If not, Not Opened will be displayed.
IP Header comp	Indicates whether or not Van Jacobsen (VJ) header compression or Robust Header Compression (ROHC) is being implemented for the subscriber's session. If neither, none is displayed. Information is displayed for both directions of the session (remote-to-local and local-to-remote).
Local Address	The PPP local address for the subscriber session.
Remote Address	The IP address assigned to the subscriber's mobile device for the duration of the session.
Primary DNS	Indicates the IP address of the primary Domain Name Server (DNS) assigned to the subscriber.
Secondary DNS	Indicates the IP address of the secondary Domain Name Server (DNS) assigned to the subscriber.

Field	Description
Primary NBNS	Indicates the IP address of the primary NetBIOS Name Server (NBNS) assigned to the subscriber.
Secondary NBNS	Indicates the IP address of the secondary NetBIOS Name Server (NBNS) assigned to the subscriber.
IPV6CP State	Indicates whether or not the Internet Protocol v6 Control Protocol (IPv6CP) was successfully negotiated (Opened). If not, Not Opened will be displayed.
In octs(unframed)	The total number of unframed octets received.
In pkts	The total number of packets received
Out octs(unframed)	The total number of unframed octets sent
Out pkts	The total number of packets sent
In ctrl octs	The total number of control octets received
In ctrl pkts	The total number of control packets received
Out ctrl octs	The total number of control octets sent
Out ctrl pkts	The total number of control packets sent
In framed octs	The total number of framed octets received
Out framed octs	The total number of framed octets sent
In data (unfr/data-cmp) octs	The total number of unframed data compressed data octets received
Out data (unfr/data-cmp) octs	The total number of unframed data compressed data octets sent
In data (iphdr-cmp) octs	The total number of data octets with IP header compression received
Out data (iphdr-cmp) octs	The total number of data octets with IP header compression sent
In data (iphdr-cmp-fail) octs	The total number of data octets with failed IP header compression received
In data (iphdr-cmp-fail) pkts	The total number of data packets with failed IP header compression received
In data (iphdr-rohc) octs	The total number of data octets with ROHC IP header compression received
Out data (iphdr-rohc) octs	The total number of data octets with ROHC IP header compression sent
In data (iphdr-rohc-fail) octs	The total number of data octets with failed ROHC IP header compression received

Field	Description
In data(iphdr-rohc-fail) pkts	The total number of data packets with failed ROHC header compression received
In discards	The total number of input discards
In errors	The total number of input errors
Out discards	The total number of output discards
Out errors	The total number of output errors
Bad address	The total number of bad addresses
Bad control	The total number of bad control messages
Pkt too long	The total number of packets that were too long
Bad FCS	The total number of bad Frame Check Sequences (FCS)
Bad pkt length	The total number of bad packet lengths
Echo req rcvd	The total number of echo requests received
Echo rsp rcvd	The total number of echo responses received
Echo req sent	The total number of echo requests sent
Echo rsp sent	The total number of echo responses sent
Invalid magic-number rcvd	The total number of invalid magic numbers received

show ppp statistics pdsn-service

Table 3: show ppp statistics pdsn-service Command Output Descriptions

Field	Description
PPP statistics for pdsn-service	Indicates the name of the PDSN service for which PPP statistics are being displayed.
total sessions initiated	Indicates the total number of subscriber sessions that have been received by the by the system for processing.
session re-negotiated	Indicates the total number of subscriber sessions that have been re-negotiated by the by the system.
successful sessions	Indicates the total number of subscriber sessions that have been successfully connected by the by the system.
failed sessions	Indicates the total number of subscriber sessions that the system has/have failed to process.

Field	Description
total sessions released	Indicates the total number of subscriber sessions that have been disconnected.
failed re-negotiations	Indicates the number of PPP calls that failed while LCP or IPCP was being re-negotiated.
released by local side	Indicates the total number of subscriber sessions that have been dropped by the system.
released by remote side	Indicates the total number of subscriber sessions that have been dropped by the mobile nodes.
Session Failures	
LCP failure max-retry	Indicates the number of sessions that were released during setup due to the system not receiving a response prior to the expiration of the maximum number of Link Control Protocol (LCP) retries.
LCP failure option-issue	Indicates the number of sessions that were released during setup due to failed negotiations between the system and the mobile nodes over Link Control Protocol (LCP) options.
LCP failure unknown	Indicates the number of calls that failed because of miscellaneous LCP failures.
IPCP failure max-retry	Indicates the number of sessions that were released during setup due to the system not receiving a response prior to the expiration of the maximum number of Internet Protocol Control Protocol (IPCP) retries.
IPCP failure option-issue	Indicates the number of sessions that were released during setup due to failed negotiations between the system and the mobile nodes over Internet Protocol Control Protocol (IPCP) options.
IPCP failure unknown	Indicates the number of calls that failed because of miscellaneous IPCP related failures.
IPv6CP failure max-retry	Indicates the number of IPv6CP calls that failed after the maximum number of retries.
IPv6CP failure option issue	Indicates the number of sessions that were released during setup due to failed negotiations between the system and the mobile nodes over IPv6CP options.
IPv6CP failure unknown	Indicates the number of calls that failed because of miscellaneous IPv6CP related failures.
Authentication failures	Indicates the number of sessions that were released during setup due to subscriber authentication failures
Authentication aborted	Indicates the number of times that authentication was not successful because the peer failed to provide the required request or response packet in time.

Field	Description
remote terminated	Indicates the number of sessions that were released by the mobile node.
lower layer disconnected	Indicates the number of times that the peer terminated the lower protocol layer.
miscellaneous failures	Indicates the number of session failures that occurred due to reasons other than those listed here.
Session Progress	
sessions (re)entered LCP	Indicates the number of sessions entering or re-entering the Link Control Protocol (LCP) phase of call setup.
sessions (re)entered Auth	Indicates the number of sessions entering or re-entering the authentication phase of call setup.
sessions (re)entered IPCP	Indicates the number of sessions entering or re-entering the Internet Protocol Control Protocol (IPCP) phase of call setup.
sessions (re)entered IPv6CP	Indicates the number of sessions entering or re-entering the IPv6CP phase of call setup.
successful LCP	Indicates the number of calls that completed LCP successfully.
successful Authentication	Indicates the number of calls that completed authentication successfully.
Session Re-negotiations	
initiated by local	Indicates the number of session re-negotiations initiated by the system.
initiated by remote	Indicates the number of session re-negotiations initiated by the mobile nodes.
address mismatch	Indicates the number of session re-negotiations that occurred due to mis-matched IP addresses.
lower layer handoff	Indicates the number of times that the PDSN service renegotiated PPP because of a suspicious RP handoff.
parameter update	Indicates the number of times that the PDSN service renegotiated PPP to update some PPP parameters (e.g. DNS address obtained from HA for regular MIP)
other reasons	Indicates the number of session re-negotiations that occurred due to reasons other than those listed here.
connected session re-neg	Indicates the number of PPP renegotiation happened for sessions which are already in connected/established state.
Session Authentication	

Field	Description
CHAP auth attempt	Indicates the number of sessions that attempted to authenticate using the Challenge Handshake Authentication Protocol (CHAP).
CHAP auth success	Indicates the number of sessions that successfully authenticated using the Challenge Handshake Authentication Protocol (CHAP).
CHAP auth failure	Indicates the number of sessions that failed authentication using the Challenge Handshake Authentication Protocol (CHAP).
CHAP auth aborted	Indicates the number of times that CHAP authorization was aborted due to the fact that the peer failed to provide the required CHAP response packet in time.
PAP auth attempt	Indicates the number of sessions that attempted to authenticate using the Password Authentication Protocol (PAP).
PAP auth success	Indicates the number of sessions that successfully authenticated using the Password Authentication Protocol (PAP).
PAP auth failure	Indicates the number of sessions that failed authentication using the Password Authentication Protocol (CHAP).
PAP auth aborted	Indicates the number of times that PAP authorization was aborted due to the fact that the peer failed to provide the required PAP response packet in time.
MSCHAP auth attempt	Indicates the number of sessions that attempted to authenticate using MicroSoft CHAP (MS CHAP).
MSCHAP auth success	Indicates the number of sessions that successfully authenticated using MicroSoft CHAP (MS CHAP).
MSCHAP auth failure	Indicates the number of sessions that failed authentication using MicroSoft CHAP (MS CHAP).
MSCHAP auth aborted	Indicates the number of times that MSCHAP authorization was aborted due to the fact that the peer failed to provide the required CHAP response packet in time.
sessions skipped PPP Auth	Indicates the number of sessions that skipped PPP authorization.
Session Disconnect reason	
remote initiated	Indicates the number of sessions for which the mobile node initiated the disconnection.
remote disc. lower layer	Indicates the number of sessions in which the mobile node disconnected the lower layers of the protocol stack.
admin disconnect	Indicates the number of sessions for which the system initiated the disconnection.

Field	Description
local disc. lower layer	Indicates the number of sessions in which the system disconnected the lower layers of the protocol stack.
idle timeout	Indicates the number of sessions disconnected due to exceeding their idle timeout limit.
absolute timeout	Indicates the number of sessions disconnected due to exceeding their absolute timeout limit.
keep alive failure	Indicates the number of sessions disconnected due to keep alive failures.
no resource	Indicates the number of sessions disconnected due to lack of resources on the local side (CPU and memory).
flow add failure	Indicates the number of sessions for which the Network Processor Unit (NPU) failed to add a flow.
exceeded max LCP retries	Indicates the number of sessions disconnected due to exceeding their maximum number of Link Control Protocol (LCP) retries.
exceeded max IPCP retries	Indicates the number of sessions disconnected due to exceeding their maximum number of Internet Protocol Control Protocol (IPCP) retries.
exceeded max setup timer	Indicates the number of sessions disconnected due to exceeding their maximum amount of time allotted for session setup.
invalid dest-context	Indicates the number of sessions disconnected due to the specification of an invalid destination context. **NOTE:** Refer to the System Administration and Administration Reference for additional information about destination contexts and how they are determined.
LCP option-neg failed	Indicates the number of sessions that were disconnected due to failed negotiations between the system and the mobile nodes over Link Control Protocol (LCP) options.
IPCP option-neg failed	Indicates the number of sessions that were disconnected due to failed negotiations between the system and the mobile nodes over Internet Protocol Control Protocol (IPCP) options.
no remote-ip address	Indicates the number of sessions that were disconnected due to the lack of an IP address for the mobile node.

Field	Description
call type detect failed	Indicates the number of sessions that were disconnected due to the system not being able to determine what type of service to provide for the session. The possible services are: • pdsn-simple-ip • pdsn-mobile-ip • ha-mobile-ip
source address violation	Indicates the number of sessions that were disconnected due to source address violations.
exceeded max IPv6CP retries	Indicates the number of sessions disconnected due to exceeding their maximum amount of time allotted for IPv6CP setup.
IPv6CP option-neg failed	Indicates the number of sessions that were disconnected due to failed negotiations between the system and the mobile nodes over IPv6CP options.
remote disc. upper layer	Indicates the number of times a session was disconnected because the remote peer disconnected the upper protocol layer.
long duration timeout	The number of sessions disconnected due to expiration of the long duration timer.
PPP auth failures	The number of sessions that failed due to PPP authorization failures.
miscellaneous reasons	Indicates the number of sessions that were disconnected for reasons other than those listed here.
Session Data Compression	
sessions negotiated comp	Indicates the total number of sessions that negotiated the use data compression.
STAC Compression	Indicates the total number of sessions that negotiated the use data compression using the STAC protocol.
MPPC compression	Indicates the total number of sessions that negotiated the use data compression using the MPPC protocol.
Deflate Compression	Indicates the total number of sessions that negotiated the use data compression using the DEFLATE protocol.
CCP negotiation failures	Indicates the number of Compression Control Protocol negotiation failures.
Session Header Compression	
VJ compression	Indicates the total number of sessions that negotiated the use of Van Jacobsen (VJ) header compression.

Field	Description
ROHC Compression	Indicates the total number of sessions that negotiated the use of Robust Header Compression (ROHC).
LCP Echo Statistics	
total LCP Echo Req. sent	The total number of LCP Echo requests sent to the peer.
LCP Echo Req. resent	The total number of LCP echo requests retransmitted to the peer.
LCP Echo Reply received	The total number of LCP echo replies received from the peer.
LCP Echo Request timeout	The total number of LCP Echo timeouts that occurred since a Reply was not received.
Receive Errors	
bad FCS errors	Indicates the number of packets received with an invalid Frame Check Sequence (FCS).
unknown protocol errors	Indicates the number of packets received with an invalid protocol type.
bad Address errors	Indicates the number of packets received with a bad address field.
bad control field errors	Indicates the number of packets received with a bad control field.
bad pkt length	Indicates the number of packets received with an invalid packet length.