32 Point-to-Point Protocol

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. The base protocol is specified in RFC 1661. Many other RFCs define additional capabilities for network protocol negotiation, management information databases (MIBs), and PPP operation over different kinds of serial channels.

PPP is comprised of three main components. The first component is a method of encapsulating multi-protocol datagrams so that the underlying protocol can be identified; the second component is the Link Control Protocol (LCP) that is used for establishing, configuring, and testing the datalink connection; the third component is a family of Network Control Protocols (NCPs) that are used for establishing and configuring different network-layer protocols such as IP and IPX.

The implementation of PPP for the OmniSwitch WAN Switching Modules supports bridging, IP routing and IPX routing. Data compression of the PPP packets is also supported when the WSM module contains a STAC 9705 Data Compression Coprocessor.

PPP Connection Phases

There are five phases to a PPP connection: Dead, Establish, Authenticate, Network, and Terminate:

Dead. The first phase is called the “Dead” phase because the physical channel has not yet been activated.

Establish. After the physical channel has been activated, the PPP connection enters the second phase, called “Establish,” wherein it attempts to negotiate link-level parameters and options using the Link Control Protocol (LCP). This phase ends when the LCP enters its own “open” state.

Authenticate. After LCP has reached its “open” state, the PPP connection enters the phase called “Authenticate” wherein it tries to identify the peer with which it is attempting to establish a connection. If the authentication option is enabled, either the Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP) is used to perform the authentication. If authentication is not enabled, the PPP connection proceeds to the next phase, “Network.”

Network. After the “Authenticate” phase is successful (or when it is not enabled), the PPP connection proceeds to the next phase, called “Network,” wherein the network protocols are negotiated using the appropriate Network Control Protocol (NCP). For example, to negotiate the use of IP over the PPP connection, the Internet Protocol Control Protocol (IPCP) is used. The details of the negotiation are specific to each network protocol, but may include such tasks as assigning network layer addresses. A network layer protocol must be negotiated successfully before the exchange of protocol packets can proceed; but, once negotiated, the protocol can begin to freely exchange packets. The PPP connection spends most of its time in the “Network” phase, because this is where the active transmission of data occurs.

Terminate. The final phase of a PPP connection is called the “Terminate” phase. This phase begins when authentication is unsuccessful or the channel becomes inoperative. Very often, this phase is simply bypassed, and PPP will return to the idle (Dead) phase when a channel is disconnected.

Data Compression

RFC 1974 specifies the use of STAC-LZS compression with PPP. Data compression allows the payload of a PPP packet, including the protocol ID, to be compressed, saving valuable bandwidth. Compression is negotiated during the Network phase using Compression Control Protocol (CCP), which includes the negotiation of a data compression algorithm and any parameters specific to the algorithm. Once negotiated, all data packets (i.e., non-control protocol packets) from all successfully negotiated protocols are compressed before transmission. The compression algorithm negotiated includes any mechanism for synchronizing the compressor and decompressor.

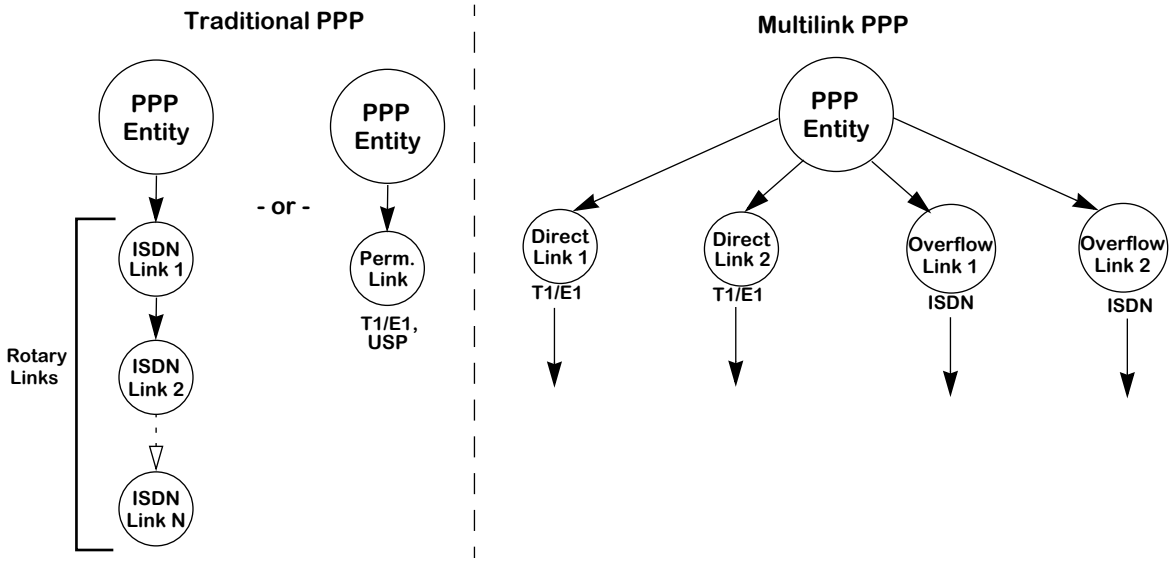
STAC-LZS's maximum data compression ratio is 30:1. The LZS algorithm is optimized to compress all file types as efficiently as possible. Even string matches as short as two octets are effectively compressed. The STAC-LZS compression algorithm supports both single compression history communication and multiple compression history communication.

Often, many streams of information are interleaved over the same link. Each virtual link will transmit data that is independent of other virtual links. Using multiple compression histories can improve the compression ratio of a communication link.

Multi-Link PPP

The main limitation of PPP is implicit in its name: Point-to-Point Protocol, meaning that it is limited to connecting two points over a single physical connection. Multi-Link PPP (MLPPP) extends the functionality of PPP by combining multiple PPP links into a single logical data pipeline, called a "bundle." Unlike standard PPP, MLPPP is not limited to individual links; both physical and virtual connections can be bundled.

Another advantage of MLPPP is that, unlike traditional PPP, the links that comprise the bundle can be different types. For example (as shown in the figure below), dedicated serial links could be combined with dynamic (overflow) ISDN links. The multi-link "bundle" is modeled as a single virtual PPP entity at each node communicating over the direct links as if a single link existed. Overflow links may join or leave the bundle dynamically, as bandwidth requirements dictate.



Traditional vs. Multilink PPP

Multilink Modes of Operation

Multilink PPP supports combinations of both permanent and switched connections. This results in two possible modes of operation:

- permanent connection only
- switched connection only

Note

One important thing to remember when setting up multilinks is that all links to be bundled must exist on the same slot.

Permanent Connection Only

This mode allows multiple links to be joined into a single bundle. Permanent connections can be universal serial ports or fractional T1/E1 ports.

Switched Connection Only

This mode supports only switched connections. The only switched connections currently supported are ISDN calls. This allows multiple switched connections to be joined into a single bundle. In this mode, the first call is initiated as a demand connection, if a frame is available for the peer, or a backup connection, if the primary link becomes inactive, according to the configuration of the ISDN link.

Overview of PPP Configuration Procedures

The configuration of a PPP connection on your switch is divided into three separate tasks. This three-phase strategy was chosen to allow PPP connections to be configured over *any* serial channel interface without requiring the use of multiple PPP configuration displays for each separate type of interface.

Step 1. Configure the Physical Interface to be Used for PPP

The information configured at the physical interface level includes the specification of the type of WSM interface and of any information that is specific to the given type of interface. The interfaces that can support PPP are ISDN, T1/E1, and the Universal Serial Port on all WSM boards.

An ISDN interface (WSM-BRI) requires the specification of the switch type, the local telephone number, and the Service Profile Identifiers (SPIDs) if appropriate for the switch type. The UI commands used to configure ISDN interfaces allow for modifying and viewing ISDN port's configuration and the display of its operational status. See the Chapter 34, "Managing ISDN Ports," for detailed information on configuring an ISDN interface for PPP.

The configuration of a T1/E1 interface is described in Chapter 35, "Managing T1 and E1 Ports."

The configuration of a universal serial port (USP) on a WSM-S board is described in Chapter 30, "Managing WAN Switching Modules." Note that the ISDN board (WSM-BRI) also contains a Universal Serial Port (USP); this port may be configured in a similar manner to the USPs on the WSM-S board.

Step 2. Configure the Operation of PPP Itself

The information configured at the PPP level includes the remote and local user IDs and passwords, network protocol information, the use of data compression, and retry and delay information to be used during PPP connection establishment with LCP. The UI commands used to configure PPP connections (called "PPP Entities") allow for the adding, modifying, and viewing of PPP connections and their operational status. This chapter describes the configuration of PPP Entities (connection configurations) using the **pppadd**, **pppmodify**, **pppdelete**, **pppview**, and **pppstatus** commands.

Step 3. Configure a Link Between the Physical Interface and PPP

As mentioned above, three kinds of physical interfaces can support PPP connections: Universal Serial Ports (on all WSM boards,), T1/E1 channels (on the WSM-FT1/E1 board), and ISDN lines (on the WSM-BRI board).

The "WAN Links" used to support PPP connections vary somewhat, depending upon which type of physical interface is being used for PPP. When the physical interface is a Universal Serial Port (USP) or a fractional T1/E1 channel (which are permanent channels), the port is dedicated to the PPP connection and the "WAN Link" simply identifies the physical interface in terms of the slot and port. When the physical interface being used is an ISDN interface (which provides dynamic, switched connections), the "WAN Link" identifies the numbering information that is to be used to establish the serial connection and the slot/port if necessary. The UI commands used to configure WAN Links allow for the adding, modifying, and viewing of the links, and the display of their operational status. See Chapter 33, "WAN Links" for detailed information on the commands used to configure WAN Links.

Multiple links can be configured when employing Multilink PPP, one for each link in the bundle. For Multilink PPP over ISDN, each link configured for a PPP entity is called every time the connection is attempted and Multilink PPP is successfully negotiated. For normal PPP over ISDN, when a connection with a PPP entity is attempted, each link is called until one is successful.

The PPP Submenu

The WAN menu contains a submenu, named **PPP**, containing commands specific to the Point-to Point-Protocol (PPP).

To display the **PPP** menu, enter the following commands:

```
PPP

?
```

A screen similar to the following displays:

```
Command          PPP Menu
-----------------  -------------------------------------------------------------------------
pppglobal        Add PPP Global configuration record
pppadd           Add PPP configuration record
pppmodify        Modify PPP configuration record
pppdelete        Delete PPP configuration record
pppview          View PPP configuration record(s)
pppstatus        Get Status of PPP configuration records and associated links

 Main      File      Summary   VLAN      Networking
 Interface Security  System    Services  Help
```

PPP Configuration Overview

Your first configuration step is to create a global PPP configuration record using the **pppglobal** command. This global record is used to provide default settings to be used for incoming calls. Then, you can add individual PPP configuration records (called "PPP Entities") for each peer (i.e., for each remote site) with which you wish to be able to establish a point-to-point connection. You will need to know specific information about the remote peers with which you wish to connect in order to successfully configure the PPP Entity.

After you have configured at least one PPP Entity, you can use the other commands on the PPP Menu to modify, delete, view, and display its operational status. You can then add PPP Entities as you need them to support additional PPP connection requirements.

When a port is configured for PPP via the **wpm** command, a PPP entity and a WAN link entry are created automatically. For more information, see Chapter 30, "Managing WAN Switching Modules." .

Setting Global PPP Parameters

The **pppglobal** command is used to set global configuration parameters that are used by the PPP protocol. These parameters are termed "global" because they are the default settings used by the switch to establish connections with incoming calls. These global settings are not tied to a specific peer (i.e., a PPP Entity; see *Adding a PPP Entity* on page 32-8).

To set the global PPP parameters, enter the following command:

```
pppglobal
```

A screen similar to the following displays:

```
PPP Global Configuration:

1)  Default Authentication Type . . . . . PAP
    {(N)one, (P)AP, (C)HAP}
2)  Global User ID sent to remote for Authentication. . . . . =
    {8 characters userid}
3)  Global Password sent to remote for Authentication . . . . . =
    {8 characters password}
4)  Default Compression Type . . . . . = STAC-LZS
    {(N)one, STAC-(L)ZS}
5)  Default Bridge Config Admin Status . . . . . = Disabled
    {(E)nable, (D)isable}
6)  Default IP Config Admin Status. . . . . = Enabled
    {(E)nable, (D)isable}
7)  Default IPX Config Admin Status . . . . . = Disabled
    {(E)nable, (D)isable}

(save/quit/cancel)
  :
```

The fields on this screen have the following meanings:

Default Authentication Type

Specifies the type of authentication that is to be expected on incoming calls. The options are **None**, **PAP**, and **CHAP**. Set this parameter to the type of authentication that you expect your callers to be using. If you enable either PAP or CHAP authentication, the next two parameters must also be set (user ID and password) or the caller's connection requests will be refused. If you set this parameter to **None**, you must also set the Default Bridge, IP and IPX Configuration Administration Status parameters or the caller's connection requests will be refused.

Global User ID sent to remote for Authentication

Specifies the user ID that will be sent to a peer on incoming calls. Enter the text you will transmit on incoming calls. This parameter must contain a value if either PAP or CHAP authentication is being used. The User ID and password received from the peer will be checked against the list of peers (PPP Entities) to attempt to identify the remote peer.

Global Password sent to remote for Authentication

Specifies the password that will be sent to a peer on incoming calls. Enter the text you will transmit on incoming calls. This parameter must contain a value if either PAP or CHAP authentication is being used.

Default Compression Type

Specifies the type of compression that is to be expected on incoming calls. The options are **None** and **STAC-LZS**. If you set this parameter to **None** and your callers are using compression, the caller's connection request may be refused. See *Data Compression* on page 32-2 for a description of STAC-LZS data compression.

Default Bridge Config Admin Status

Specifies whether the bridging function is to be negotiated for incoming calls. More information on the bridging function can be found in *Adding a PPP Entity* on page 32-8. If this parameter is disabled here, but disabled on the caller, the caller's connection request may be refused.

Default IP Config Admin Status

Specifies whether the IP routing function is to be negotiated for incoming calls. More information on the IP routing function can be found in *Adding a PPP Entity* on page 32-8. If this parameter is disabled here, but disabled on the caller, the caller's connection request may be refused.

Default IPX Config Admin Status

Specifies whether the IPX routing function is to be negotiated for incoming calls. More information on the IPX routing function can be found in *Adding a PPP Entity* on page 32-8. If this parameter is disabled here, but disabled on the caller, the caller's connection request may be refused.

Adding a PPP Entity

The **pppadd** command is used to add a PPP Entity configuration record. The PPP Entities you create are identified by numbers called Peer IDs. When you enter the **pppadd** command, you may enter a Peer ID number with the command like this:

```
pppadd <ID number>
```

Alternatively, you can enter the command alone and you will be prompted for a Peer ID. The prompt will identify the next available, unique ID number.

After you enter the **pppadd** command as described above, a screen will be displayed that contains the configuration parameters that make up the PPP Entity. The steps that begin below will take you through the process of adding a PPP Entity.

After you have set the PPP Entity's configuration parameters, you must save them to actually create the PPP Entity. After saving, you will be prompted to add one or more links to be used with the PPP Entity. In other words, the software will automatically issue a **linkadd** command for you. This was designed to help you to quickly create working PPP Entities as they must be associated with at least one link in order to operate. The **linkadd** command, as well as the other commands on the Link menu, are described in Chapter 33, titled "Wan Links."

1. To add a PPP Entity, enter the following command:

```
pppadd
```

A screen similar to the following will display:

```
Add PPP configuration record. Please specify a unique
ID number to identify this record and the remote Peer to communicate with.

Peer ID (1):
```

This prompt is asking you to enter a Peer ID as well as indicating that the next available number is 1. If other Peers have already been configured, the number indicated will be different than is shown above.

2. To answer the prompt, for example, for Peer ID 1, you would enter the following command:

```
1
```

If you have enabled the verbose mode, you will see the following text immediately before the prompts:

```
To change a value, enter the corresponding number, an '=', and the new
value. For example to set a new description, use
 : 2=My new Description
To clear an entry specify the value as '.' as in
  2=.
When complete enter "save" to save all changes, or cancel or Ctrl-C to
cancel all changes. Enter ? to view the new configuration.
```

This text provides brief help on entering commands at the following screens. In the steps that follow below, this help text will *not* be shown.

A screen similar to the following will display:

```
Adding PPP configuration record for Peer ID: 1
Enter PPP parameters:

1)  Description :
    {Enter text up to 30 characters}
2)  Administrative Status ..... Enabled
    {(E)nable, (D)isable}
3)  PPP Mode ..... Normal
    {(N)ormal, (M)ultilink}
4)  Compression Type ..... None
    {(N)one, STAC-(L)ZS}
5)  Bridging Group ..... 1
    {1-65535 or 0 if no Bridging}
      50) Bridge Config Admin Status ..... Enabled
          {(E)nabled, (D)isabled}
      51) PPP Bridging Mode ..... Ethernet Only
          {Bridge (A)ll, (E)thernet Only}
6)  Routing Group ..... 0
    {1-65535 or 0 if no Routing}
7)  Authentication Type ..... None
    {(N)one, (P)AP, (C)HAP}
8)  Max Failure Count ..... 3
    {1..65535}
9)  Max Configure Count ..... 3
    {1..65535}
10) Max Terminate Count ..... 3
    {1..65535}
11) Retry Timeout Value ..... 5
    {Retry Timeout in Second(s) 1..65535}

(save/quit/cancel)
  :
```

The prompts for Bridging, Routing and Authentication (numbered 5, 6, and 7 above), contain suboptions that are displayed only if you have enabled those features.

For example, the screen will display these suboptions for prompts 6 and 7 if you enable them (you will have to enter the **?** command to refresh the display):

```
6)  Routing Group ..... 1
    {1-65535 or 0 if no Routing}
      60) IP Config Admin Status ..... Enabled
          {(E)nabled, (D)isabled}
      61) Remote IP Address (Only valid if IP is enabled) ..... 0.0.0.0
          {Valid IP address notation e.g., x.x.x.x}
      62) IPX Config Admin Status ..... Enabled
          {(E)nable, (D)isable}
7)  Authentication Type ..... PAP
    {(N)one, (P)AP, (C)HAP}
      70) User ID received from remote for Authentication ...
          {8 characters userid}
      71) Password received from remote for Authentication .
          {8 characters password}
      72) User ID sent to remote for Authentication. .....
          {8 characters userid}
      73) Password sent to remote for Authentication .......
          {8 characters password}
```

The fields on the **pppadd** configuration screen have the following meanings:

Description

A textual description for this PPP Entity. You can enter any text you like (up to 30 characters).

Administrative Status

Indicates the Administrative Status of this PPP Entity. **Enabled** will allow the PPP Entity to operate. **Disabled** will disable the PPP Entity without deleting it.

PPP Mode

Can be set to either **Multilink** or **Normal** (single PPP connection).

Compression Type

Controls whether this PPP Entity will perform compression. The one type of compression currently available is STAC-LZS. See *Data Compression* on page 32-2 for details on STAC-LZS compression.

Bridging Group

Indicates the VLAN Group to be used for PPP Bridging. A value of zero (0) indicates that this PPP Entity will not perform a bridging service and will discard all bridged format packets received or transmitted. The suboptions under this heading are:

Bridge Config Admin Status

Used to enable or disable the bridging function for this PPP Entity.

PPP Bridging Mode

Used to select the operational mode for bridging. The options are **Ethernet**, which will enable bridging on Ethernet interfaces only, or **All**, which enables it for all interfaces.

Routing Group

Indicates the VLAN Group to be used for PPP Routing of the IP and IPX protocols. A value of zero (0) indicates that this PPP Entity will not perform a routing service and will discard all routed format packets received or transmitted. The suboptions under this heading are:

IP Config Admin Status

Used to enable or disable the routing of IP packets over PPP. The options are **Enabled** and **Disabled**.

Remote IP Address (Only valid if IP is enabled)

Used to specify the Remote IP address of the PPP connection when IP routing is enabled. Valid IP address notation must be used. If this parameter is set to 0.0.0.0 and IP routing is enabled, the Remote IP address will be learned during Internet Protocol Control Protocol (IPCP) negotiation.

IPX Config Admin Status

Used to enable or disable routing of IPX packets over PPP. The options are **Enabled** and **Disabled**.

Authentication Type

Indicates the type of authentication to be used by this PPP Entity. The options are **None**, **PAP**, and **CHAP**. The suboptions under this heading are:

User ID received from remote for Authentication

Used to specify the User ID to be expected from the remote end during PAP or CHAP authentication.

Password received from remote for Authentication

Used to specify the password to be expected from the remote end during PAP or CHAP authentication.

User ID sent to remote for Authentication

Used to specify the User ID to be sent to the remote end during PAP or CHAP authentication. This parameter is used only for outgoing calls. Incoming calls use the global defaults (see *Setting Global PPP Parameters* on page 32-6 for details).

Password sent to remote for Authentication

Used to specify the password to be sent to the remote end during PAP or CHAP authentication. This parameter is used only for outgoing calls. Incoming calls use the global defaults (see *Setting Global PPP Parameters* on page 32-6 for details).

Max Failure Counter

The maximum number of times a CONFIGURATION_REQUEST packet will be sent when the previous attempts received responses, but did not receive a CONFIGURATION_ACK. This counter applies to all LCP and NCP negotiations.

Max Configure Counter

The maximum number of times a CONFIGURATION_REQUEST packet will be sent when the previous attempts did not receive any responses. This counter applies to all LCP and NCP negotiations.

Max Terminate Counter

The maximum number of TERMINATE_REQUEST packets that will be sent without receiving a TERMINATE_ACK packet. This counter applies to all LCP and NCP negotiations.

Retry Timeout Value

Indicates the number of seconds to wait between CONFIGURATION_REQUEST retries that do not receive a response. This timeout value applies to all LCP and NCP negotiations.

3. When you have made the changes you need to the prompts on this screen, enter the following command to save the PPP Entity:

```
save
```

The following prompt will display:

```
Normal (non-multilink) PPP configuration record created.
Do you wish to define the link at this time y/n (y):
```

If you answer yes to this prompt, a **linkadd** command will be automatically executed for this PPP Entity. For complete details on using the **linkadd** command, see the relevant section in Chapter 33, "WAN Links."

If you answer No to this prompt, a message will appear indicating that the link was not added, but the PPP Entity itself was added.

Note

You can add the link needed for a PPP Entity later if you decide not to do so now. The automatic execution of the **linkadd** command is done here only as a convenience to you.

Modifying a PPP Entity

The **pppmodify** command is used to modify the parameters of an existing PPP Entity. To modify a specific PPP Entity, for example Peer ID 1, enter the following command:

```
pppmodify p1
```

A screen similar to the following displays:

```
Modify PPP for communication to Peer ID: 1
Enter PPP parameters:
1)  Description :
    {Enter text up to 30 characters}
2)  Administrative Status ..... Enabled
    {(E)nable, (D)isable}
3)  PPP Mode ..... Normal
    {(N)ormal, (M)ultilink}
4)  Compression Type ..... None
    {(N)one, STAC-(L)ZS}
5)  Bridging Group ..... 1
    {1-65535 or 0 if no Bridging}
    50)  Bridge Config Admin Status ..... Enabled
         {(E)nabled, (D)isabled}
    51)  PPP Bridging Mode ..... Ethernet Only
         {Bridge (A)ll, (E)thernet Only}
6)  Routing Group ..... 2
    {1-65535 or 0 if no Routing}
    60)  IP Config Admin Status ..... Enabled
         {(E)nabled, (D)isabled}
    61)  Remote IP Address ..... 0.0.0.0
         {IP address or 0.0.0.0 = learn, if IP enabled}
    62)  IPX Config Admin Status ..... Disabled
         {(E)nable, (D)isable}
7)  Authentication Type ..... PAP
    {(N)one, (P)AP, (C)HAP}
    70)  User ID received from remote for Authentication ...
         {0 (No ID) to 8 ASCII characters}
    71)  Password received from remote for Authentication .
         {0 (No Password) to 8 ASCII characters}
    72)  User ID sent to remote for Authentication .........
         {0 (No ID) to 8 ASCII characters}
    73)  Password sent to remote for Authentication .......
         {0 (No Password) to 8 ASCII characters}
8)  Max Failure Count ..... 3
    {1..65535}
9)  Max Configure Count ..... 3
    {1..65535}
10) Max Terminate Count ..... 5
    {1..65535}
11) Retry Timeout Value. ..... 5
    {Retry Timeout in Second(s) 1..65535}

(save/quit/cancel)
  :
```

The fields on this screen are the same as those produced by the **pppadd** command. See *Adding a PPP Entity* on page 32-8 for descriptions of each of these fields.

Make the desired changes to any of the parameters, then enter the **save** command to implement the changes. You will then be returned to the system prompt.

Viewing PPP Entity Configurations

The **pppview** command is used to view the configuration parameters of existing PPP Entities.

Displaying the Configuration of All PPP Entities

To view configuration information on all PPP Entities, enter the following command:

```
pppview
```

A screen similar to the following displays:

```
PPP Configuration for Chassis:

Peer  Admin                Authen-    Compres-  Bridging  Routing
ID    Status  Mode         tication   sion      Group     Group
=====  ======  ==========  =========  ========  ========  =======
1     UP      Normal       None       None      1         0
2     DN      Multilink    PAP        STAC-LZS  1         2
3     UP      Normal       CHAP       None      0         2
```

The fields on this screen have the following meanings:

Peer ID

The number assigned to this PPP Entity when it was added. Used to identify a specific PPP Entity that you want to examine with the **pppview** or **pppstatus** commands.

Admin Status

Indicates the Administrative Status of this PPP Entity. **UP** means that this entity is enabled, or operative. **DN** means that this entity is disabled, or inoperative.

Mode

Indicates whether **Normal** or **Multilink** operation is used by this PPP Entity. Multilink operation is described under the heading *Multi-Link PPP* on page 32-2.

Authentication

Indicates the type of authentication used by this PPP Entity. The options are **None**, **PAP** and **CHAP**. These are two well-established standards currently used for PPP authentication.

Compression

Indicates the type of data compression configured to operate with this PPP Entity. The options are **None**" or **STAC-LZS**." See *Data Compression* on page 32-2 for information on STAC-LZS compression.

Bridging Group

Indicates the VLAN Group to be used for PPP Bridging. A value of zero (**0**) indicates that this PPP Entity will not perform a bridging service and will discard all bridged format packets received or transmitted.

Routing Group

Indicates the VLAN Group to be used for PPP Routing of the IP and IPX protocols. A value of zero (**0**) indicates that this PPP Entity will not perform a routing service and will discard all routed format packets received or transmitted.

Displaying the Configuration of a Specific PPP Entity

To view configuration information on a *specific* PPP Entity, you must enter a Peer ID number with the **pppview** command. For example, to examine Peer ID 1, you would enter the following command:

```
pppview p1
```

A screen similar to the following displays:

```
View PPP configuration record for communication to Peer ID: 1
1)  Description : Entry Peer ID 1
2)  Administrative Status ..... Enabled
3)  PPP Mode ..... Normal
4)  Compression Type ..... Disabled
5)  Bridging Group ..... 1
      50)  Bridge Config Admin Status ..... Enabled
      51)  PPP Bridging Mode ..... Ethernet Only
6)  Routing Group ..... 1
      60)  IP Config Admin Status ..... Enabled
      61)  Remote IP Address ..... 0.0.0.0
      62)  IPX Config Admin Status ..... Disabled
7)  Authentication Type ..... PAP
      70)  User ID received from remote for Authentication ...
      71)  Password received from remote for Authentication .
      72)  User ID sent to remote for Authentication .....
      73)  Password sent to remote for Authentication .....
8)  Max Failure Count ..... 3
9)  Max Configure Count ..... 3
10) Max Terminate Count ..... 3
11) Retry Timeout Value ..... 5
```

The fields on this screen are similar to those produced by the **pppadd** command. A few differences are noted in the descriptions that are given below. Note that you cannot make changes to the parameters on this screen. To do so, you must use the **pppmodify** command instead (see *Modifying a PPP Entity* on page 32-13 for complete information).

Description

The textual description that you entered for this PPP Entity using the **pppadd** command.

Administrative Status

Indicates the Administrative Status of this PPP Entity. The options are **Enabled**, which means that the PPP Entity is operative and **Disabled**, which means that it is inoperative.

PPP Mode

Indicates whether **Normal** or **Multilink** operation is used by this PPP Entity. Multilink operation is described under the heading *Multi-Link PPP* on page 32-2.

Compression Type

Indicates whether this PPP Entity is performing data compression. The options are **Enabled**, which means that the PPP Entity is performing compression, and **Disabled,** which means that the PPP Entity is not currently performing data compression. See *Data Compression* on page 32-2 for more information on data compression.

Bridging Group

Indicates the VLAN Group to be used for PPP Bridging. A value of zero (**0**) indicates that this PPP Entity will not perform a bridging service and will discard all bridged format packets received or transmitted. Also indicated are whether bridging is **Enabled** or **Disabled** and the PPP Bridging mode (**Ethernet** or **All**).

Routing Group

Indicates the VLAN Group number to be used for PPP Routing of the IP and IPX protocols. A value of zero (**0**) indicates that this PPP Entity will not perform a routing service and will instead discard all routed format packets received and not transmit any. The suboptions indicate whether routing of IP packets is **Enabled** or **Disabled**, the Remote IP address of the PPP connection, and whether IPX routing is **Enabled** or **Disabled**. If the Remote IP address is set to 0.0.0.0 and IP routing is enabled, the Remote address will be learned during IPCP negotiation. These suboptions are described under the heading *Adding a PPP Entity* on page 32-8.

Authentication Type

Indicates the type of authentication to be used by this PPP Entity. The options are **None**, **PAP**, and **CHAP**. The suboptions that are indicated (if they are set) are the user ID and password to be expected from the remote end during PAP or CHAP authentication, and the user ID and password to be sent to the remote end during PAP or CHAP authentication. The User ID and password sent to the remote are only used for outgoing calls. Incoming calls use the global defaults (see *Setting Global PPP Parameters* on page 32-6 for details). These suboptions are described under the heading *Adding a PPP Entity* on page 32-8.

Max Failure Counter

The maximum number of times a CONFIGURATION_REQUEST packet will be sent when the previous attempts received responses, but did not receive a CONFIGURATION_ACK. This counter applies to all LCP and NCP negotiations.

Max Configure Counter

The maximum number of times a CONFIGURATION_REQUEST packet will be sent when the previous attempts did not receive any responses. This counter applies to all LCP and NCP negotiations.

Max Terminate Counter

The maximum number of TERMINATE_REQUEST packets that will be sent without receiving a TERMINATE_ACK packet. This counter applies to all LCP and NCP negotiations.

Retry Timeout Value

The delay before trying a CONFIGURATION_REQUEST or a TERMINATE_REQUEST packet. This timeout value applies to all LCP and NCP negotiations.

Displaying PPP Entity Status

The **pppstatus** command is used to view the operational status of one or more PPP Entities.

Displaying the Status of All PPP Entities

To view the operational status of *all* PPP Entities, enter the following command:

```
pppstatus
```

A screen similar to the following displays:

```
                                          IP      IPX     BCP     CCP
Peer    Admin                             Oper    Oper    Oper    Oper
ID      State   Mode                      State   State   State   State
=====   ======= ========== ======== ======== ======= =======
1       UP/UP   Normal     Open     Close    Open    Open
2       UP/UP   Multilink  Open     Open     Open    Open
```

The fields on this screen have the following meanings:

Peer ID

The number assigned to this PPP peer.

Admin State

Indicates the Administrative Status of this PPP Entity. **UP** means that this entity is enabled, or operative. **DN** means that this entity is disabled, or inoperative.

Mode

Indicates whether **Normal**" or **Multilink**" operation is used by this PPP Entity. Multilink operation is described under the heading *Multi-Link PPP* on page 32-2.

IP Oper State

Indicates the operational state of the IP Routing option. **Open** means that IP has successfully negotiated a connection and is able to pass IP packets. **Closed**" means that IP has not yet reached the open" state, and is therefore unable to pass IP packets. The reasons why the state may be closed" are: 1) the call has been disconnected, 2) the protocol is in the process of making a connection, or 3) the IP Routing option was not configured.

IPX Oper State

Indicates the operational state of the IPX Routing option. **Open** means that IPX has successfully negotiated a connection and is able to pass IPX packets. **Closed** means that IPX has not yet reached the open state, and is therefore unable to pass IPX packets. The reasons why the state may be closed are: 1) the call has been disconnected, 2) the protocol is in the process of making a connection, or 3) the IPX Routing option was not configured.

BCP Oper State

Indicates the operational state of the Bridging Control Protocol option. **Open** means that the bridging operation is active. **Closed** means that the bridging operation has not yet reached the open state. The reasons why the state may be closed are: 1) the call has been disconnected, 2) the protocol is in the process of making a connection, or 3) the Bridging option was not configured.

CCP Oper State

The operational state of the compression control protocol option. **Open** means that compression is active. **Closed** means that compression has not reached the open state. The reasons why the state may be closed are: 1) the call has been disconnected, 2) the protocol is in the process of making a connection, or 3) the compression option was not configured.

Displaying the Status of a Specific PPP Entity

To view both the operational status and the relevant statistics of a specific PPP Entity, for example, Peer ID 1, enter the following command:

```
pppstatus p1
```

A screen similar to the following displays:

```
PPP statistics for Peer ID: 2
                          IP        IPX       BCP       CCP
Admin                     Oper      Oper      Oper      Oper
State     Mode            State     State     State     State
======    ======          ======    ======    ======    =======
UP        Normal          Open      Close     Open      Close

LCP Pkts  IPCP Pkts       IPCP Pkts IPCP Pkts BCP Pkts  CCP Pkts
IN/OUT    IN/OUT          IN/OUT    IN/OUT    IN/OUT    IN/OUT
=======   ========        =======   ========  =========
3/4       2/2             0/0       4/4       0/0

                Packets   Packets   Packets   Octets    Octets
                In        Out       In+Out    In        Out       %In   %Out
                ========  ========  ========  ========  ========  ====  =====
Total             2232      1475      3707     91751     66034
Ethernet             0       146       146         0     13413     0     20
8025                 0         0         0         0         0     0      0
FDDI                 0         0         0         0         0     0      0
IP                  79       158       237      7784      6952     8     10
IPX                  0         0         0         0         0     0      0
BPDU              2153      1171      3324     83967     45669    91     69

STAC-LZS        Compressed      Compressed      Uncompressed    Compression
Compression     Frames          Octets          Octets          Ratio
                ============    ============    ============    ============
In                           0               0               0       0.0:1
Out                          0               0               0       0.0:1
IN+Out                       0               0               0       0.0:1
```

The additional fields produced by the **pppstatus** command when a specific Peer ID is entered with the command are as follows:

LCP Pkts IN/OUT

The total number of Link Control Protocol (LCP) packets received (**In**) and transmitted (**Out**) on this PPP connection.

IPCP Pkts IN/OUT

The total number of IP Control Protocol (IPCP) packets received (**In**) and transmitted (**Out**) on this PPP connection.

IPCP Pkts IN/OUT

The total number of IP Control Protocol (IPCP) packets received (**In**) and transmitted (**Out**) on this PPP connection.

BCP Pkts IN/OUT

The total number of BCP packets received (**In**) and transmitted (**Out**) for this PPP connection.

CCP Pkts IN/OUT

The total number of CCP packets received (**In**) and transmitted (**Out**) for this PPP connection.

Also shown on this screen are two tables of statistics. The first table shows various data transmission statistics shown both as a total and sorted by the type of frame encapsulation being used (**Total**, **Ethernet**, **8025**, **FDDI**, **IP**, **IPX**, and **BPDU**). The columns in the first table show the following information for each type of frame encapsulation: the number of packets received (**Packets In**), the number of packets transmitted (**Packets Out)**, the sum of received and transmitted packets (**Packets In+Out**), the number of octets received (**Octets In**), the number of octets transmitted (**Octets Out**), and the percentages received (**%In**) and transmitted (**%Out**) for each type of frame encapsulation.

The second table shows statistics related to the performance of STAC-LZS compression sorted by **In**, **Out**, and **In+Out** categories. The column headings show the number of compressed frames and octets, the number of uncompressed frames and octets, and the overall compression ratio represented by the previous figures.

Deleting a PPP Entity

The **pppdelete** command is used to delete an existing PPP Entity.

1. Before you can delete a PPP Entity, you must first delete all the links associated with it. You do so using the **linkdelete** command (see Chapter 33, "WAN Links"). If you try to delete a PPP Entity that still has links associated with it, the following message will be displayed:

   ```
   Delete PPP Peer ID: 1 aborted because the following link(s) attach to it.
   Link Index: 1, Description: Link Entry: 1, Peer ID: 1
   ```

2. To delete a specific PPP Entity (after deleting all links associated with it), enter the Peer ID number along with the **pppdelete** command. For example, to delete Peer ID 2, enter the following command:

   ```
   pppdelete p2
   ```

   A screen similar to the following displays:

   ```
   This will delete the configuration for PPP Peer ID: 2
   Continue ? {(Y)es, (N)o} : N
   ```

3. To delete this entity, enter **y** and press **Enter.** If you decide to cancel out of the deletion, press **Enter** to accept the default answer of No. The system prompt will reappear.