



# PPTP with MPPE

---

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 5
- Supported Standards, MIBs, and RFCs, page 5
- Prerequisites, page 6
- Configuration Tasks, page 7
- Monitoring and Maintaining PPTP Sessions, page 10
- Configuration Examples, page 11
- Command Reference, page 13
- Debug Commands, page 23

## Feature Overview

The Point to Point Tunneling Protocol (PPTP) with Microsoft Point-to-Point Encryption (MPPE) feature enables Cisco Virtual Private Networks (VPNs) to use PPTP as the tunneling protocol.

## PPTP Overview

PPTP is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across TCP/IP-based data networks. PPTP supports on-demand, multiprotocol, virtual private networking over public networks, such as the Internet. This section describes the following aspects of PPTP:

- Compulsory and Voluntary Tunneling
- PPTP Tunnel Negotiation
- Flow Control Alarm

## Compulsory and Voluntary Tunneling

VPNs are designed based on one of the two following tunneling architecture options:

- Compulsory Tunneling
- Voluntary Tunneling

### Compulsory Tunneling

Compulsory tunneling (also referred to as NAS-initiated tunneling) enables users to dial in to a NAS, which then establishes an encrypted tunnel to the tunnel server. The connection between the client of the user and the NAS is not encrypted.

### Voluntary Tunneling

Voluntary tunneling (also referred to as client-initiated tunneling) enables clients to configure and establish encrypted tunnels to tunnel servers without an intermediate NAS participating in the tunnel negotiation and establishment.

For PPTP, only voluntary tunneling is supported.

## PPTP Tunnel Negotiation

Table 1 describes the protocol negotiation events that establish a PPTP tunnel.

**Table 1 Protocol Negotiation Event Descriptions**

Event	Description
1	The client dials in to the ISP and establishes a PPP session.
2	The client establishes a TCP connection with the tunnel server.
3	The tunnel server accepts the TCP connection.
4	The client sends a PPTP SCCRQ message to the tunnel server.
5	The tunnel server establishes a new PPTP tunnel and replies with a SCCRQ message.
6	The client initiates the session by sending a OCRQ message to the tunnel server.
7	The tunnel server creates a virtual-access interface.
8	The tunnel server replies with a OCRP message.

## Flow Control Alarm

The flow control alarm is a new function that indicates if PPTP detects congestion or lost packets. When a flow control alarm goes off, PPTP reduces volatility and additional control traffic by establishing an accompanying stateful MPPE session.

For more information, see the **pptp flow-control static-rtt** command, and the output from the **show vpdn session** commands in the “Verifying a PPTP Connection” section.

## MPPE Overview

MPPE is an encryption technology developed by Microsoft to encrypt point-to-point links. These PPP connections can be over a dialup line or over a VPN tunnel. MPPE works as a subfeature of Microsoft Point-to-Point Compression (MPPC).

MPPC is a scheme used to compress PPP packets between Cisco and Microsoft client devices. The MPPC algorithm is designed to optimize bandwidth utilization in order to support multiple simultaneous connections.

MPPE is negotiated using bits in the MPPC option within the Compression Control Protocol (CCP) MPPC configuration option (CCP configuration option number 18).

MPPE uses the RC4 algorithm with either 40- or 128-bit keys. All keys are derived from the cleartext authentication password of the user. RC4 is stream cipher; therefore, the sizes of the encrypted and decrypted frames are the same size as the original frame. The Cisco implementation of MPPE is fully interoperable with that of Microsoft and uses all available options, including historyless mode. Historyless mode can increase throughput in lossy environments such as VPNs, because neither side needs to send CCP Resets Requests to synchronize encryption contexts when packets are lost.

## MPPE Encryption Types

Two modes of MPPE encryption are offered:

- Stateful MPPE Encryption
- Stateless MPPE Encryption

### Stateful MPPE Encryption

Stateful encryption will provide the best performance but may be adversely affected by networks experiencing substantial packet loss. If you choose stateful encryption you should also configure flow control to minimize the detrimental effects of this lossiness.

Because of the way that the RC4 tables are reinitialized during stateful synchronization, it is possible that two packets may be encrypted using the same key. For this reason, stateful encryption may not be appropriate for lossy network environments (such as Layer 2 tunnels on the Internet).

### Stateless MPPE Encryption

Stateless encryption provides a lower level of performance, but will be more reliable in a lossy network environment.



---

If you choose stateless encryption you *should not* configure flow control.

---

## Benefits

This feature allows lower-cost, secure services and scalability, as described in the following sections.

## Lower-Cost, Secure Services

Enterprises are increasingly looking to the Internet as a means of enabling new, lower-cost services for their users. The ubiquity of the Internet makes it very easy for remote and mobile users to connect anywhere on the planet; all that is required is an ISP to provide Internet access. At the same time, enterprises are hesitant to trust the Internet as a transport for private company data and are looking for means to use the Internet in a secure way.

PPTP with MPPE provides a solution to this need. PPTP provides a mechanism to tunnel user data across the Internet to the edge of the enterprise network, which allows users to use any ISP account and any Internet-routable IP address to access the edge of the Enterprise network. At the edge, the IP packet is de-tunneled and the IP address space of the enterprise is used for traversing the internal network. MPPE provides an encryption service that protects the datastream as it traverses the Internet. MPPE is available in two strengths: 40-bit encryption, which is widely available throughout the world, and 128-bit encryption, which may be subject to certain export controls when used outside the United States.

ISPs can also leverage PPTP with MPPE when deploying managed services for enterprise customers. In this model, the ISP deploys and manages the PPTP with MPPE tunnel server of the enterprise, or PPTP Network Server (PNS), and manages this service on behalf of the enterprise. The tunnel server may be located at the point of presence (POP) of the ISP, or it may be located at the edge of the enterprise network, but it is managed by the ISP.

## Scalability

A Cisco router running PPTP can support up to 2000 simultaneous PPTP tunnels without MPPE encryption. For PPTP tunnels with MPPE encryption, Cisco routers can currently support up to 500 simultaneous tunnels.

## Restrictions

Only Cisco Express Forwarding (CEF) and process switching are supported. Regular fast switching is not supported.

Only voluntary tunneling—not compulsory tunneling—is supported.

PPTP does not support multilink.

VPDN multihop is not supported.

Because all PPTP signalling is over TCP, TCP configurations will affect PPTP performance in large-scale environments.

MPPE is not supported with TACACS.

MPPE is supported with RADIUS in Cisco IOS Releases 12.0(7)XE1 and later.

MPPE keys are not supported with SNT and CSU.

## Supported Platforms

- Cisco Platforms:
  - Cisco 1600 series
  - Cisco 1720 VPN Access Router
  - Cisco 2500 series
  - Cisco 2600 series
  - Cisco 3600 series
  - Cisco 4000-M series (Cisco 4000-M, 4500-M, 4700-M)
  - Cisco 7000 series
  - Cisco 7100 series
  - Cisco 7200 series
  - Cisco 7500 series
  - Cisco AS5200
  - Cisco AS5300
  - Cisco AS5800
- Windows Clients:
  - Windows 95/98
  - Windows NT 4.0
  - Windows 2000

## Supported Standards, MIBs, and RFCs

### Standards

None

### MIBs

None

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

### RFCs

RFC 2637 *PPTP*

# Prerequisites



**Note**

Windows clients must use MS-CHAP authentication for MPPE to work.

If you are performing mutual authentication with MS-CHAP and MPPE, both sides of the tunnel must use the same password.

To use MPPE with AAA, you must use a RADIUS server that supports the Microsoft Vendor Specific Attribute for MPPE-KEYS.

CiscoSecure ACS NT supports MPPE beginning with release 2.6. CiscoSecure ACS UNIX does not support MPPE.

Before configuring PPTP, enable the following configurations:

- Configuring AAA (Optional)
- Configuring AAA on the RADIUS Server (Optional)
- Creating the Virtual Template for Dial-in Sessions (Required)
- Specifying the IP Address Pool and BOOTP Servers (Optional)

## Configuring AAA

To configure Authentication, Authorization, and Accounting (AAA) on the tunnel server, use the following commands in global configuration mode:

	Command	Purpose
Step 1	<code>PNS(config)# aaa authentication ppp default {group radius   local}</code>	Configures either local or RADIUS AAA authentication.
Step 2	<code>PNS(config)# aaa authorization network default {group radius   local}</code>	Configures either local or RADIUS AAA authorization.
Step 3	<code>PNS(config)# aaa accounting network default start-stop radius</code>	(Optional) Enables AAA accounting that sends a stop accounting notice at the end of the requested user process.
Step 4	<code>PNS(config)# radius-server host ip-address [auth-port number] [acct-port number]</code>	Specifies the IP address of the RADIUS server and optionally the ports to be used for authentication and accounting requests.
Step 5	<code>PNS(config)# radius-server key key</code>	Sets the authentication key and encryption key for all RADIUS communication.

## Configuring AAA on the RADIUS Server

To configure AAA on the RADIUS server, include the following attributes with the Return List Attributes:

```
Framed-Protocol = PPP
MS-CHAP-MPPE-Keys
Service-Type = Framed
```

## Creating the Virtual Template for Dial-In Sessions

To configure the tunnel server to create virtual-access interfaces from a virtual template for incoming PPTP calls, use the following commands beginning in global configuration mode:

	Command	Purpose
<b>Step 1</b>	PNS(config)# <b>interface virtual-template</b> <i>number</i>	Creates the virtual template that is used to clone virtual-access interfaces.
<b>Step 2</b>	PNS(config-if)# <b>ip unnumbered</b> <i>interface-type number</i>	Specifies the IP address of the interface the virtual-access interfaces uses.
<b>Step 3</b>	PNS(config-if)# <b>ppp authentication ms-chap</b>	Enables MS-CHAP authentication using the local username database. All windows clients using MPPE need to use MS-CHAP.
<b>Step 4</b>	PNS(config-if)# <b>peer default ip address pool default</b>	Returns an IP address from the default pool to the client.
<b>Step 5</b>	PNS(config-if)# <b>ip mroute-cache</b>	Disables fast switching of IP multicast.
<b>Step 6</b>	PNS(config-if)# <b>ppp encrypt mppe</b> { <i>auto</i>   <i>40</i>   <i>128</i> } [ <i>passive</i>   <i>required</i> ] [ <i>stateful</i> ]	Enables MPPE encryption on the virtual template.

## Specifying the IP Address Pool and BOOTP Servers

The IP address pool consists of the IP addresses that the tunnel server assigns to clients. You can also provide BOOTP servers, DNS servers, which are specified using the **async-bootp dns-server** command, translate host names to IP addresses. WINS servers, which are specified using the **async-bootp nbns-server** command, provide dynamic NetBIOS names that Windows devices use to communicate without IP addresses.

	Command	Purpose
<b>Step 1</b>	PNS(config)# <b>ip local pool default</b> <i>first-ip-address last-ip-address</i>	Configures the default local pool of IP addresses that will be used by clients.
<b>Step 2</b>	PNS(config)# <b>async-bootp dns-server</b> <i>ip-address1</i> [ <i>additional-ip-address</i> ]	(Optional) Returns the configured addresses of domain name servers in response to BOOTP requests.
<b>Step 3</b>	PNS(config)# <b>async-bootp nbns-server</b> <i>ip-address1</i> [ <i>additional-ip-address</i> ]	(Optional) Returns the configured addresses of Windows NT servers in response to BOOTP requests.

## Configuration Tasks

See the following sections for configuration tasks for the PPTP with MPPE feature.

- Configuring a Tunnel Server to Accept PPTP Tunnels (Required)
- Configuring MPPE on the ISA Card (Optional)
- Tuning PPTP (Optional)

# Configuring a Tunnel Server to Accept PPTP Tunnels

To configure a tunnel to accept tunneled PPP connections from a client, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	PNS(config)# <b>vpdn-group 1</b>	Creates VPDN group 1.
Step 2	PNS(config-vpdn)# <b>accept dialin</b>	Enables the tunnel server to accept dial-in requests.
Step 3	PNS(config-vpdn-acc-in)# <b>protocol pptp</b>	Specifies that the tunneling protocol will be PPTP.
Step 4	PNS(config-vpdn-acc-in)# <b>virtual-template</b> <i>template-number</i>	Specifies the number of the virtual template that will be used to clone the virtual-access interface.
Step 5	PNS(config-vpdn-acc-in)# <b>exit</b>	Exit to higher command mode.
Step 6	PNS(config-vpdn)# <b>local name</b> <i>localname</i>	(Optional) Specifies that the tunnel server will identify itself with this local name.  If no local name is specified, the tunnel server will identify itself with its host name.

# Configuring MPPE on the ISA Card

To offload MPPE encryption from the tunnel server processor to the ISA card, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	PNS(config)# <b>controller isa</b> <i>slot/port</i>	Enters controller configuration mode on the ISA card.
2	PNS(config-controller)# <b>encryption mppe</b>	Enables MPPE encryption.

# Tuning PPTP

To tune PPTP, use one or more of the following commands in VPDN configuration mode:

Command	Purpose
PNS(config-vpdn)# <b>pptp flow-control receive-window</b> <i>packets</i>	Specifies how many packets the client can send before it must wait for the acknowledgment from the tunnel server.
PNS(config-vpdn)# <b>pptp flow-control static-rtt</b> <i>milliseconds</i>	Specifies the timeout interval of the tunnel server between sending a packet to the client and receiving a response.
PNS(config-vpdn)# <b>pptp tunnel echo</b> <i>seconds</i>	Specifies the period of idle time on the tunnel that will trigger an echo message from the tunnel server to the client.

## Verifying a PPTP Connection

To verify that a PPTP network functions properly, perform the following steps:

- Step 1** From the client, dial in to the ISP and establish a PPP session.
- Step 2** From the client, dial in to the tunnel server.
- Step 3** From the client, ping the tunnel server. From the client desktop:
- Click **Start**.
  - Select **Run**.
  - Enter **ping tunnel-server-ip-address**.
  - Click **OK**.
  - Look at the terminal screen and verify that the tunnel server is sending ping reply packets to the client.
- Step 4** From the tunnel server, enter the **show vpdn** command and verify that the client has established a PPTP session.

```
PNS# show vpdn

% No active L2TP tunnels

% No active L2F tunnels

PPTP Tunnel and Session Information (Total tunnels=1 sessions=1)

LocID RemID Remote Name      State   Remote Address  Port  Sessions
13    13    10.1.2.41      estabd  10.1.2.41      1136  1

LocID RemID TunID Intf   Username      State   Last Chg
13    0    13    Vi3   Username      estabd  000030
```

- Step 5** For more detailed information, enter the **show vpdn session all** or **show vpdn session window** commands. The last line of output from the **show vpdn session all** command indicates the current status of the flow control alarm.

```
PNS# show vpdn session all

% No active L2TP tunnels

% No active L2F tunnels

PPTP Session Information (Total tunnels=1 sessions=1)

Call id 13 is up on tunnel id 13
Remote tunnel name is 10.1.2.41
Internet Address is 10.1.2.41
Session username is unknown, state is estabd
Time since change 000106, interface Vi3
Remote call id is 0
10 packets sent, 10 received, 332 bytes sent, 448 received
Ss 11, Sr 10, Remote Nr 10, peer RWS 16
0 out of order packets
Flow alarm is clear.
```

The last line of output from the **show vpdn session window** command indicates the current status of the flow control alarm (under the heading “Congestion”) and the number of flow control alarms that have gone off during the session (under the heading “Alarms”).

```
PNS# show vpdn session window

% No active L2TP tunnels

% No active L2F tunnels

PPTP Session Information (Total tunnels=1 sessions=1)

LocID RemID TunID ZLB-tx  ZLB-rx  Congestion Alarms  Peer-RWS
13    0    13    0      1      clear      0      16
```

**Step 6** For information on the virtual-access interface, enter the **show ppp mppe virtual-accessnumber** command:

```
PNS# show ppp mppe virtual-access3
Interface Virtual-Access3 (current connection)
  Hardware (ISA5/1, flow_id=13) encryption, 40 bit encryption, Stateless mode
  packets encrypted = 0      packets decrypted = 1
  sent CCP resets = 0      receive CCP resets = 0
  next tx coherency = 0      next rx coherency = 0
  tx key changes = 0      rx key changes = 0
  rx pkt dropped = 0      rx out of order pkt= 0
  rx missed packets = 0
```

To update the key change information, reissue the **show ppp mppe virtual-access3** command.

```
PNS# show ppp mppe virtual-access3
Interface Virtual-Access3 (current connection)
  Hardware (ISA5/1, flow_id=13) encryption, 40 bit encryption, Stateless mode
  packets encrypted = 0      packets decrypted = 1
  sent CCP resets = 0      receive CCP resets = 0
  next tx coherency = 0      next rx coherency = 0
  tx key changes = 0      rx key changes = 1
  rx pkt dropped = 0      rx out of order pkt= 0
  rx missed packets = 0
```

## Monitoring and Maintaining PPTP Sessions

To monitor and maintain PPTP with MPPE sessions, use the following EXEC commands:

Command	Purpose
<b>clear vpdn tunnel</b> [ <b>ppptp</b>   <b>l2f</b>   <b>l2tp</b> ] <i>network-access-server gateway-name</i>	Shuts down a specific tunnel and all the sessions within the tunnel.
<b>debug aaa authentication</b>	Displays information on AAA authentication.
<b>debug aaa authorization</b>	Displays information on AAA authorization.
<b>debug ppp chap</b>	Displays CHAP packet exchanges.
<b>debug ppp negotiation</b>	Displays information about packets sent during PPP start-up and detailed PPP negotiation options.
<b>debug ppp mppe</b>	Displays debug messages for MPPE events.

Command	Purpose
<code>debug vpdn event [protocol   flow-control]</code>	Displays VPDN errors and basic events within the protocol (such as L2TP, L2F, PPTP) and errors associated with flow control. Flow control is only possible if you are using L2TP and the remote peer "receive window" is configured for a value greater than zero.
<code>debug vpdn l2x-events</code>	Displays L2F and L2TP events that are part of tunnel establishment or shutdown.
<code>debug vpdn l2x-errors</code>	Displays L2F and L2TP protocol errors that prevent tunnel establishment or normal operation.
<code>debug vpdn packet [control   data] [detail]</code>	Displays protocol-specific packet header information, such as sequence numbers if present, such as flags and length.

## Configuration Examples

The following example shows the running configuration of a tunnel server configured for PPTP using an ISA card to perform 40-bit MPPE encryption. It does not have a AAA configuration.

```

Current configuration
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname PNS
!
no logging console guaranteed
enable password lab
!
username tester41 password 0 lab41
!
!
!
!
ip subnet-zero
no ip domain-lookup
!
vpdn enable
!
vpdn-group 1
! Default PPTP VPDN group
  accept-dialin
  protocol pptp
  virtual-template 1
  local name cisco_pns
!
!
!
memory check-interval 1
!
!
controller ISA 5/0
  encryption mppe
!
process-max-time 200
!

```

```
interface FastEthernet0/0
 ip address 10.1.1.12 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.2.12 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 no ip directed-broadcast
 shutdown
 framing c-bit
 cablelength 10
 dsu bandwidth 44210
!
interface Serial1/1
 no ip address
 no ip directed-broadcast
 shutdown
 framing c-bit
 cablelength 10
 dsu bandwidth 44210
!
interface FastEthernet4/0
 no ip address
 no ip directed-broadcast
 shutdown
 duplex half
!
interface Virtual-Template1
 ip unnumbered FastEthernet0/0
 no ip directed-broadcast
 ip mroute-cache
 no keepalive
 ppp encrypt mppe 40
 ppp authentication ms-chap
!
ip classless
 ip route 172.29.1.129 255.255.255.255 1.1.1.1
 ip route 172.29.63.9 255.255.255.255 1.1.1.1
 no ip http server
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

# Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

- **clear vpdn tunnel**
- **encryption mppe**
- **ppp encrypt mppe**
- **pptp flow-control receive-window**
- **pptp flow-control static-rtt**
- **pptp tunnel echo**
- **show ppp mppe**

## clear vpdn tunnel

To shut down a specified tunnel and all the message identifiers (MIDs) within it, use the **clear vpdn tunnel** EXEC command.

```
clear vpdn tunnel [pptp | l2f | l2tp] network-access-server gateway-name
```

Syntax Description		
<b>pptp</b>	(Optional)	Clears the specified Point-to-Point Tunneling Protocol (PPTP) tunnel.
<b>l2f</b>	(Optional)	Clears the specified Layer 2 Forwarding (L2F) tunnel.
<b>l2tp</b>	(Optional)	Clears the specified Layer 2 Tunneling Protocol (L2TP) tunnel.
<i>network-access-server</i>		Name of the network access server at the far end of the tunnel, probably the point of presence of the public data network or the ISP.
<i>gateway-name</i>		Host name of home gateway at the local end of the tunnel.

Command Modes	
	EXEC

Command History	Release	Modification
	11.2 P	This command was introduced.
	12.0(5)XE5	The <b>pptp</b> keyword was added.

Usage Guidelines	
	This command is used primarily for troubleshooting. You can use the command to force the tunnel to come down without unconfiguring it (the tunnel could be restarted immediately by a user logging in).

Examples	
	The following example clears a tunnel between a network access server called orion and a home gateway called samson:

```
clear vpdn tunnel orion samson
```

# encryption mppe

To enable Microsoft Point-to-Point Encryption (MPPE) encryption on an Industry-Standard Architecture (ISA) card, use the **encryption mppe** ISA controller configuration command. To disable MPPE encryption, use the **no** form of this command.

**encryption mppe**

**no encryption mppe**

**Syntax Description** This command has no keywords or arguments.

**Defaults** IPSec is the default encryption type.

**Command Modes** ISA controller configuration

Command History	Release	Modification
	12.0(5)XE5	This command was introduced.

**Usage Guidelines** Using the ISA card offloads MPPE from the router processor and will improve performance in large-scale environments.

The router must be rebooted for the change from **encryption ipsec** to **encryption mppe** to take effect.

**Examples** The following example enables MPPE encryption on the ISA card in slot 5, port 0:

```
PNS(config)# controller isa 5/0
PNS(config-controller)# encryption mppe
```

Related Commands	Command	Description
	<b>ppp encrypt mppe</b>	Enables MPPE encryption on the virtual template.
	<b>show ppp mppe</b>	Displays MPPE information for an interface.
	<b>debug ppp mppe</b>	Displays debug messages for MPPE events.

# ppp encrypt mppe

To enable Microsoft Point-to-Point Encryption (MPPE) encryption on the virtual template, use the **ppp encrypt mppe** interface configuration command. Use the **no** form of this command to disable MPPE encryption.

```
ppp encrypt mppe {auto | 40 | 128} [passive | required] [stateful]
```

```
no ppp encrypt mppe
```

### Syntax Description

<b>auto</b>	All available encryption strengths are allowed.
<b>40</b>	Only 40-bit encryption is allowed.
<b>128</b>	Only 128-bit encryption is allowed.
<b>passive</b>	(Optional) MPPE will not offer encryption, but will negotiate if the other tunnel endpoint requests encryption.
<b>required</b>	(Optional) MPPE must be negotiated, or the connection will be terminated.
<b>stateful</b>	(Optional) MPPE will only negotiate stateful encryption. If the <b>stateful</b> keyword is not used, MPPE will first attempt to negotiate stateless encryption, but will fall back to stateful if the other tunnel endpoint requests stateful.

### Defaults

Disabled.  
The default encryption type is stateless.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.0(5)XE5	This command was introduced.

### Usage Guidelines

To use the **encryption mppe** command, PPP encapsulation must be enabled.



#### Note

The **ppp authentication ms-chap** command must be added to the interface that will carry PPTP-MPPE traffic. All Windows clients using MPPE need MS-CHAP. This is a Microsoft design requirement.

The **auto** keyword is only offered on 128-bit images.  
All of the configurable MPPE options must be identical on both tunnel endpoints.



#### Caution

Because of the way that the RC4 tables are reinitialized during stateful synchronization, it is possible that two packets may be encrypted using the same key. For this reason, stateful encryption may not be appropriate for lossy network environments (such as Layer 2 tunnels on the Internet).

**Examples**

The following example shows a virtual template configured to perform 40-bit MPPE encryption:

```
interface Virtual-Template1
 ip unnumbered FastEthernet0/0
 no ip directed-broadcast
 ip mroute-cache
 no keepalive
 ppp encrypt mppe 40
 ppp authentication ms-chap
```

**Related Commands**

Command	Description
<b>encryption mppe</b>	Enables MPPE encryption on the ISA card.
<b>interface virtual-template</b>	Creates a virtual template interface.
<b>ppp authentication</b>	Enables CHAP, PAP, MS-CHAP or a combination of methods and specifies the order in which the authentication methods are selected on the interface.

## pptp flow-control receive-window

To specify how many packets the client can send before it has to wait for the tunnel server's acknowledgment, use the **pptp flow-control receive-window** VPDN configuration command. Use the **no** form of this command to return to the default value.

**pptp flow-control receive-window** *packets*

**no pptp flow-control receive-window**

<b>Syntax Description</b>	<i>packets</i>	Number of packets the client can send before it has to wait for the tunnel server's acknowledgment. Range: 1 - 64 packets.
---------------------------	----------------	---

<b>Defaults</b>	16 packets
-----------------	------------

<b>Command Modes</b>	VPDN configuration
----------------------	--------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(5)XE5	This command was introduced

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>pptp flow-control static-rtt</b>	Specifies the tunnel server's timeout interval between sending a packet to the client and receiving a response.

## pptp flow-control static-rtt

To specify the timeout interval of the tunnel server between sending a packet to the client and receiving a response, use the **pptp flow-control static-rtt** VPDN configuration command. Use the **no** form of this command to return to the default value of 1500 milliseconds (ms).

**pptp flow-control static-rtt** *milliseconds*

**no pptp flow-control static-rtt**

<b>Syntax Description</b>	<i>milliseconds</i>	Timeout interval of the tunnel server between sending a packet to the client and receiving a response.  Range: 100 -to 5000 milliseconds.						
<b>Defaults</b>	1500 ms							
<b>Command Modes</b>	VPDN configuration							
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.0(5)XE5</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.0(5)XE5	This command was introduced.			
Release	Modification							
12.0(5)XE5	This command was introduced.							
<b>Usage Guidelines</b>	If the session times out, the tunnel server does not retry or resend the packet. Instead the flow control alarm is set off, and stateful mode is automatically switched to stateless.							
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>pptp flow-control receive-window</b></td> <td>Specifies how many packets the client can send before it must wait for the acknowledgment from the tunnel server.</td> </tr> <tr> <td><b>pptp tunnel echo</b></td> <td>Specifies the period of idle time on the tunnel that will trigger an echo message from the tunnel server to the client.</td> </tr> </tbody> </table>	Command	Description	<b>pptp flow-control receive-window</b>	Specifies how many packets the client can send before it must wait for the acknowledgment from the tunnel server.	<b>pptp tunnel echo</b>	Specifies the period of idle time on the tunnel that will trigger an echo message from the tunnel server to the client.	
Command	Description							
<b>pptp flow-control receive-window</b>	Specifies how many packets the client can send before it must wait for the acknowledgment from the tunnel server.							
<b>pptp tunnel echo</b>	Specifies the period of idle time on the tunnel that will trigger an echo message from the tunnel server to the client.							

# pptp tunnel echo

To specify the period of idle time on the tunnel that will trigger an echo message from the tunnel server to the client, use the **pptp tunnel echo** VPDN configuration command. Use the **no** form of this command to return to the default value of 60 seconds.

**pptp tunnel echo** *seconds*

**no pptp tunnel echo**

<b>Syntax Description</b>	<i>seconds</i>	Echo packet interval in seconds.
		Range: 0 to 1000 seconds.

<b>Defaults</b>	60 seconds
-----------------	------------

<b>Command Modes</b>	VPDN configuration
----------------------	--------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
		12.0(5)XE5

<b>Usage Guidelines</b>	If the tunnel server does not receive an echo reply within 20 seconds, it will tear down the tunnel. This 20-second interval is hard coded.
-------------------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>pptp flow-control receive-window</b>	Specifies how many packets the client can send before it must wait for the acknowledgment from the tunnel server.
	<b>pptp flow-control static-rtt</b>	Specifies the timeout interval of the tunnel server between sending a packet to the client and receiving a response.

# show ppp mppe

To display Microsoft Point-to-Point Encryption (MPPE) information for an interface, use the **show ppp mppe** privileged EXEC command.

```
show ppp mppe {serial | virtual-access}[number]
```

Syntax Description	serial	Displays MPPE information for all serial interfaces.
	virtual-access	Displays MPPE information for all virtual-access interfaces.
	number	(Optional) Displays MPPE information for only the specified interface.

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	12.0(5)XE5	This command was introduced.

**Usage Guidelines** None of the fields in the output from the **show ppp mppe** command are fatal errors. Excessive packet drops, misses, out of orders, or CCP-Resets indicate that packets are getting lost. If you see such activity and have stateful MPPE configured, you may want to consider switching to stateless mode.

**Examples** The following example displays MPPE information for virtual-access interface 3:

```
PNS# show ppp mppe virtual-access3
Interface Virtual-Access3 (current connection)
  Hardware (ISA5/1, flow_id=13) encryption, 40 bit encryption, Stateless mode
  packets encrypted = 0      packets decrypted = 1
  sent CCP resets = 0      receive CCP resets = 0
  next tx coherency = 0    next rx coherency = 0
  tx key changes = 0      rx key changes = 0
  rx pkt dropped = 0      rx out of order pkt= 0
  rx missed packets = 0
```

To update the key change information, reissue the **show ppp mppe virtual-access3** command:

```
PNS# show ppp mppe virtual-access3
Interface Virtual-Access3 (current connection)
  Hardware (ISA5/1, flow_id=13) encryption, 40 bit encryption, Stateless mode
  packets encrypted = 0      packets decrypted = 1
  sent CCP resets = 0      receive CCP resets = 0
  next tx coherency = 0    next rx coherency = 0
  tx key changes = 0      rx key changes = 1
  rx pkt dropped = 0      rx out of order pkt= 0
  rx missed packets = 0
```

Table 2 describes significant fields in the output:

**Table 2** *show ppp mppe Output Field Descriptions*

<b>Field</b>	<b>Description</b>
packets encrypted	Number of packets that have been encrypted
packets decrypted	Number of packets that have been decrypted
sent CCP resets	Number of CCP-Resets sent. One CCP-Reset is sent for each packet loss that is detected in stateful mode. When configured for stateless MPPE, this field is always zero.
next tx coherency	The coherency count (the sequence number) of the next packet to be encrypted.
next rx coherency	The coherency count (the sequence number) of the next packet to be decrypted.
key changes	Number of times the session key has been reinitialized. In stateless mode, the key is reinitialized once per packet. In stateful mode, the key is reinitialized every 256 packets or when a CCP-Reset is received.
rx packet dropped	Number of packets received and dropped. A packet is dropped because it is suspected of being a duplicate or already received packet.
rx out of order pkt	Number of packets received that are out of order.
rx missed packets	Number of packets received that indicated that a packet has been missed elsewhere.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>pptp flow-control static-rtt</b>	Specifies the timeout interval of the tunnel server between sending a packet to the client and receiving a response.

# Debug Commands

This section documents the new **debug ppp mppe** command. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

# debug ppp mppe

To display debug messages for Microsoft Point-to-Point Compression (MPPC) events, use the **debug ppp mppe** EXEC command. Use the **no** form of this command to disable MPPC debugging.

**debug ppp mppe**

**no debug ppp mppe**

**Syntax Description** This command has no keywords or arguments.

**Defaults** Disabled

Command History	Release	Modification
	12.0(5)XE5	This command was introduced.

Related Commands	Command	Description
	<b>encryption mppe</b>	Enables MPPE encryption on the ISA card.
	<b>ppp encrypt mppe</b>	Enables MPPE encryption on the virtual template.
	<b>show ppp mppe</b>	Displays MPPE information for an interface.



■ debug ppp mppe