WAN Configuration Commands

Table of Contents

Chapter 1 PPP Configuration Commands 1

1.1 PPP Configuration Commands 1

1.1.1 encapsulation ppp 2

1.1.2 interface multilink 3

1.1.3 interface virtual-tunnel 4

1.1.4 ip local pool 5

1.1.5 multilink bundle-name 6

1.1.6 multilink-group 7

1.1.7 multilink max-fragments 8

1.1.8 multilink max-links 9

1.1.9 multilink min-links 10

1.1.10 peer default ip address 11

1.1.11 peer neighbor-route 12

1.1.12 ppp account 13

1.1.13 ppp authentication 14

1.1.14 ppp authorization 15

1.1.15 ppp chap echo 16

1.1.16 ppp chap hostname 17

1.1.17 ppp chap refuse 18

1.1.18 ppp ddr 19

1.1.19 ppp ipcp rfc-default 20

1.1.20 ppp lcp echo 20

1.1.21 ppp lcp enddisc-type 21

1.1.22 ppp lcp rfc-default 23

1.1.23 ppp lcp 23

1.1.24 ppp max-bad-auth 24

1.1.25 ppp multilink 25

1.1.26 ppp pap refuse 26

1.1.27 ppp pap sent-username 27

1.1.28 ppp timeout authentication 28

1.1.29 ppp timeout ncp 29

1.1.30 ppp timeout lcp 30

1.1.31 show ip local pool 30

1.1.32 show ppp 31

1.1.33 username 32

1.1.34 debug ppp 33

Chapter 2 HDLC Configuration Command 36

2.1 HDLC Configuration Command 36

2.1.1 debug hdlc 36

2.1.2 encapsulation hdlc 38

Chapter 1 **PPP Configuration Commands**

The commands in this chapter are used to configure PPP for the dial WAN connection of the router.

For PPP configuration of the router, refer to section “Configuring PPP”.

For more PPP information, refer to RFC 1661. For more MLP information, refer to RFC 1717.

For more PAP information, refer to RFC 1334. For more CHAP information, refer to RFC 1994.

1.1 PPP Configuration Commands

HTTP configuration commands include:

- encapsulation ppp
- interface multilink
- interface virtual-tunnel
- ip local pool
- multilink bundle-name
- multilink-group
- multilink max-fragments
- multilink max-links
- multilink min-links
- peer default ip address
- peer neighbor-route
- ppp account
- ppp authentication
- ppp authorization
- ppp chap echo
- ppp chap hostname
- ppp chap refuse

- ppp ddr
- ppp ipcp rfc-default
- ppp lcp echo
- ppp lcp enddisc-type
- ppp lcp rfc-default
- ppp lcp [close | listen | open]
- ppp max-bad-auth
- ppp multilink
- ppp pap refuse
- ppp pap sent-username
- ppp timeout authentication
- ppp timeout ncp
- ppp timeout lcp
- show ip local pool
- show ppp
- username
- debug ppp

1.1.1 encapsulation ppp

To set PPP encapsulation on the serial interface or the ISDN interface, run **encapsulation ppp**. You can run **no encapsulation ppp** to cancel PPP encapsulation.

encapsulation ppp no

encapsulation ppp

Parameter

None

Default

PPP is used for encapsulation on the asynchronous serial interface, while HDLC is used for encapsulation on the synchronous serial interface.

Command mode

Interface configuration mode

Explanation

To use the PPP encapsulation, the router must be configured with the IP routing protocol.

Example

The following example shows how to activate PPP encapsulation on interface serial 1/0:

```
!
interface s1/0
  encapsulation ppp
!
```

Related command

ppp authentication

1.1.2 interface multilink

To create a multilink bundle or enter the multilink interface configuration mode, run **interface multilink**. You can run **no interface multilink** to delete the interface.

interface multilink group－number

no interface multilink

Parameter

Parameter	Description
group-number	Number of the multilink bundle

Default

The interface is not configured.

Command mode

Global configuration mode

Explanation

The command first appears in version 1.2.4.

When the multilink interface is first created, it is automatically encapsulated as PPP by default and the multilink is then enabled.

Example

The following example shows how to create multilink bundle 1 and configure the IP address.

```
interface multilink 1
ip address 192.168.20.100 255.255.255.0
```

Related command

multilink-group

1.1.3 interface virtual-tunnel

To create VPDN combining the client and NAS, run **interface virtual-tunnel**. You can run **no interface virtual-tunnel** to delete the interface.

interface virtual-tunnel *interface-number*

no interface virtual-tunnel

Parameter

Parameter	Description
interface-number	Number of the virtual tunnel

Default

The interface is not configured.

Command mode

Global configuration mode

Explanation

When the **virtual-tunnel** interface is created, it is automatically encapsulated as PPP by default and the VPDN connection will be triggered in special conditions.

Example

The following example shows how to create virtual tunnel 1 and configure the IP address.

```
!
interface virtual-tunnel 1
  ip address 192.168.20.100 255.255.255.0
!
```

Related command

ppp ddr

1.1.4 ip local pool

To configure a local address pool to distribute the IP addresses to the peers of the point-to-point interfaces, run **ip local pool**. You can run **no ip local pool** to delete a local address pool.

ip local pool {default | *pool-name begin-ip-address* [*ip-address-number*]}

no ip local pool {**default** | *poolname***}**

Parameter

Parameter	Description
default	Uses the default local address pool to name other address pools.
pool-name	Specified name of the local address pool
begin-ip-address	Beginning IP address in the address pool
ip-address-number	Number of the IP addresses in the address pool, which is optional If this value is not included in the parameters, only the beginning IP address is in the address pool. Each address pool can include up to 1024 IP addresses.

Default

The address pool is not configured.

Command mode

Global configuration mode

Usage description

You can use IP local pool to generate one or multiple local address pools. When a host is plugged, an IP address will be distributed from these address pools to the host. To use an address pool on the interface, run **peer default ip address pool**.

You can run **show ip local pool** to check the address pool.

Example

The following example shows that a local IP address pool named mypool is generated and the included IP address range is from 172.16.23.0 to 172.16.23.255.

```
ip local pool mypool 192.168.23.0 255
```

Related command

show ip local pool

1.1.5 multilink bundle-name

multilink bundle-name name-method

no multilink bundle-name

Parameter

Parameter	Description
authenticated	Username used during remote authentication
both	Username and port name used during remote authentication
endpoint	Uses the name of the remote port.

Default

The username used during remote authentication will be used.

Command mode

Global configuration mode

Explanation

The **multilink bundle-name** command is used to specify the naming method for multilink bundle. You can run **no multilink bundle-name** to specify the naming method of the multilink bundle.

Example

The following example shows how to name bundle using the username and port name used during remote authentication.

```
multilink bundle-name both
```

Related command

interface multilink

ppp multilink

multilink virtual-template

1.1.6 multilink-group

To specify an interface as a part of bundle of special multilink, run **multilink-group** in interface configuration mode.

To delete an interface from the bundle, run **no multilink-group**.

multilink-group *group-number*

no multilink-group

Parameter

Parameter	Description
group-number	Number of multilink bundle

Default

Disabled

Command mode

Interface configuration mode

Usage explanation

All interfaces that you specify in the same bundle must have the same bandwidth. When the **multilink-group** command is used, a multilink interface will be created if the corresponding multilink interface is not created. After the **multilink-group** command is used, all PPP commands can not be used for configuration on the multilink interface, but will be coned by the multilink interface until these commands are cancelled. Hence, the configuration on the interface will be the same as that on the specified multilink interface forever.

Example

The following example shows that interface serial 1/0 will be used as a part of multilink bundle 1.

```
!
interface serial1/0
  encapsulation ppp
  multilink-group 1
!
```

Related command

interface multilink

1.1.7 multilink max-fragments

To specify the maximum number of fragments of each transmission packet on the **multilink bundle** interface, run **multilink max-fragments** in interface configuration mode. To resume its default value, run **no multilink group**.

multilink max-fragments *fragment-number*

no multilink-group

Parameter

Parameter	Description
fragment-number	Number of fragments (1-16)

Default

16

Command mode

Interface configuration mode

Explanation

The command is applied only to the virtual port related with the multilink.

Example

The following example shows how to set the maximum number of fragments on **multilink 1** interface to 10.

```
!
interface multilink 1 multilink
  max-fragments 10
!
```

Related command

interface multilink

interface virtual-template

interface dialer

1.1.8 multilink max-links

To specify the maximum number of the links on the multilink bundle interface, run **multilink max-links** in interface configuration mode. To resume its default value, run **no multilink-group**.

multilink max-links *link-number*

no multilink-group

Parameter

Parameter	Description
links-number	Number of links (1-255)

Default

255

Command mode

Interface configuration mode

Explanation

The command is applied only to the virtual port related with the multilink.

Example

The following example shows how to set the maximum number of links on the **multilink 1** interface to 100.

```
!
interface multilink 1
  multilink max-links 100
!
```

Related command

interface multilink

interface virtual-template

interface dialer

user *username* user-maxlinks

1.1.9 multilink min-links

To specify the minimum number of the links on the multilink bundle interface, run **multilink min-links** in interface configuration mode. To resume its default value, run **no multilink-group**.

multilink min-links *link-number*

no multilink-group

Parameter

Parameter	Description
links-number	Number of links (0-225)

Default

0

Command mode

Interface configuration mode

Explanation

The command is applied only to the virtual port related with the multilink.

Example

The following example shows how to set the minimum number of links on the **multilink 1** interface to 2.

```
!
interface multilink 1
  multilink min-links 2
!
```

Related command

interface multilink

interface virtual-template

interface dialer

1.1.10 peer default ip address

To specify an IP address for the remote peer or obtain the IP address from an IP address pool or the DHCP mechanism. To cancel the IP address pool configuration of the remote peer on the interface, run **no peer default ip address**.

peer default ip address {*ip-address* **| dhcp| pool** [*pool-name*]}

no peer default ip address

Parameter

Parameter	Description
ip-address	Distributes an IP address for the plugged remote peer on the interface. To avoid distributing repeated IP addresses on the interface, the **ip-address** parameter can not be used on the **dialer rotary group** interface and the ISDN interface.
dhcp	Distributes an IP address for the peer through the DHCP protocol.
pool	If the pool name is not specified, the default global mechanism defined by the **ip address-pool** parameter will be used.
pool-name	Name of the local address pool generated by the **IP local-pool** command, which is an optional parameter If an address is obtained from the address pool, the configuration of the default global mechanism will be omitted.

Default

The address pool is not configured.

Command mode

Interface configuration mode

Explanation

The administrator can run the command to configure all possible address pool mechanisms for each interface.

(1) For the interfaces that are not configured through the **peer default ip address** mechanism, the router will use the **ip address-pool** command to define the default global mechanism.

(2) If **peer default ip address pool pool-name** is run, the router will use the locally-configured address pool on the interface. Any address pool will be omitted.

(3) If **peer default ip address ip-address** is run, the specified IP address will be distributed to the port-connected remote terminal and any default global mechanism will be omitted.

Example

The following example shows how to set the local IP address pool of the **mypool** interface.

```
peer default ip address pool mypool
```

The following example shows how to specify the interface to use IP 192.168.3.29.

```
peer default ip address 192.168.3.29
```

The following example shows how to re-enable the default global mechanism of an interface:

```
peer default ip address pool
```

Related command

encapsulation ppp

ip local pool

1.1.11 peer neighbor-route

To re-activate generation of host's route on the interface, run **peer neighbor-route** in interface configuration mode. To cancel the generation of host's route on the interface, run **no peer neighbor-route** in interface configuration mode.

peer neighbor-route

no peer neighbor-route

Parameter

The command has no parameters or keywords.

Default

After the negotiation of PPP IPCP, a route pointing to the remote address of the point-to-point interface is generated.

Command mode

Interface configuration mode

Explanation

The **no peer neighbor-route** command is used only when the default behavior leads to trouble in the network.

Example

The following example shows how to reactivate the default behavior on the interface.

```
peer neighbor-route
```

1.1.12 ppp account

To specify the PPP accounting function on the interface, run **ppp account**. To cancel the PPP accounting function on the interface, run **no ppp account**.

ppp account

no ppp account

Parameter

None

Default

PPP accounting is not performed by default.

Command mode

Interface configuration mode

Explanation

After the accounting function is activated, the statistics information will be sent to the user management module for accounting when the connection is created and disconnected.

Example

The following example shows how to activate the accounting function on interface s1/0.

```
!
interface s1/0
  encapsulation
  ppp ppp account
!
```

Related command

aaa authentication ppp

encapsulation ppp

username password

1.1.13 ppp authentication

To configure the order of CHAP or PAP on an interface, run **ppp authentication**. To cancel the authentication, run **no ppp authentication**.

ppp authentication {**chap|ms-chap|pap**}[[*list-name*|**default**][**callin**]

no ppp authentication

Parameter

Parameter	Description
chap	Activates CHAP on an serial interface.
pap	Activates CHAP on a serial interface.
ms-chap	Activates MS-CHAP on a serial interface.
*list-nam*e	A parameter used together with AAA/TACACS+, specifying the name of the TACACS＋ list during authenticationIf the list name is not designated, the default list will be used. You can run **aaa authentication ppp** to create a list.
default	An optional parameter used together with AAA/TACACS+You can run **aaa authentication ppp** to create a default list.
callin	An optional parameter to specify a received call to be authenticated

When the PPP authentication is conducted, one of the three protocols **chap**, **ms-chap** and **pap**, or any combination of the three protocols will be used.

Default

The PPP authentication is not conducted.

Command mode

Interface configuration mode

Explanation

When one, two or all of CHAP, MS-CHAP and PAP are activated, the local router will authenticate the identification of a remote device before the remote device transmits the data.

(4) PAP authentication requires the remote device to send a name/password peer to check whether the local user database or the remote TACACS/TACACS+ has a corresponding option.

(5) After a challenge is transmitted to a remote device during CHAP authentication, the remote device must encrypt the challenge using public encryption and then return a response message containing encryption results and self-name to a local router. The local router then searches the corresponding encryption in the

local user database or the remote TACACS/TACACS+ database using the name of the remote device. After the encryption is found, it will be used to encrypt the initial challenge. After the encryption, the local router will check whether the encryption result is same to the result returned by the remote device.

PAP, MS-CHAP and CHAP can be activated in any order. If two authentication modes are activated, the first authentication mode will be used to offer requests during the negotiation. If the remote terminal suggests using the second authentication mode or simply refuses the first authentication mode, the second authentication mode will be used. Some remote terminal devices only support CHAP or PAP. As to specify the order of the two authentication methods, you need to base the proper authentication mode on the negotiation capacity of the remote device and the security requirements of the data link. The username and password of PAP will be transmitted as the plain text, which can be captured or reused. However, CHAP can get rid of most of the security bugs so far to be known.

No matter the PPP authentication mode is activated or canceled, the local router will not be affected as to whether the local router will be authenticated for the remote terminal device.

Example

The following example shows how to activate the CHAP authentication and use the **access1** authentication list on interface **s1/0**.

```
interface s1/0
encapsulation ppp
ppp authentication chap access1
```

Related command

aaa authentication ppp

encapsulation ppp

username password

1.1.14 ppp authorization

To activate the AAA authorization on the designated interface, run **ppp authorization** in interface configuration mode.

ppp authorization [**default |** ***list-name***]

no ppp authorization

Parameter

Parameter	Description
default	List name created by the **aaa authorization** command, which is optional
list-name	Name of the designated authorization list, which is optionalIf the name of the authorization list is not designated, use the default value.

Default

The authorization is not enabled.

Command mode

Interface configuration mode

Explanation

After the **aaa authorization** command is enabled and a authorization method list is defined, the authorization corresponding to the authorization list must exist on a proper interface. The **ppp authorization** command is used to apply the specified method list on the specified interface.

Example

The following example shows how to use the **sun** method list on interface **s0/1**.

```
interface s1/0
encapsulation ppp ppp
authorization sun
```

Related command

aaa authorization

1.1.15 ppp chap echo

To set the interval of the CHAP authentication, run the following command:

ppp chap ehco *seconds*

Parameter

Parameter	Description
seconds	Interval of the CHAP authentication, ranging between 0 and 2147483647

Default

The fixed-time CHAP authentication is not enabled and the interval of the CHAP authentication is set to zero.

Command mode

Interface configuration mode

Explanation

When the CHAP authentication is configured, the **second** parameter must be set to more than 0.

Example

The following example shows how to set the name of the local router to **routerA** , and **echo** to 10 seconds when interface serial1/0 conducts the CHAP authentication.

```
interface s1/0
encapsulation ppp
ppp authentication chap
ppp chap hostname
routerA ppp chap echo 10
```

Related command

ppp authentication

ppp authentication

ppp chap hostname

1.1.16 ppp chap hostname

To create the name of the CHAP router, run **ppp chap hostname *hostname***. To cancel the name of the CHAP router, run **no ppp chap hostname *hostname***.

ppp chap hostname *hostname*

no ppp chap hostname *hostname*

Parameter

Parameter	Description
hostname	Name contained in the transmitted CHAP challenge

Default

The function is not enabled. The name of the host router will be transmitted in all CHAP challenges by default.

Command mode

Interface configuration mode

Explanation

The command is always used for the local/remote CHAP authentication.

Example

In the following example, the command is used to encapsulate PPP on interface **dialer 0**. CHAP only authenticate the received calls. The **guest** username will be transmitted with all CJAP challenges and **response** messages.

```
interface dialer 0
encapsulation ppp
ppp authentication chap callin
ppp chap hostname guest
```

Related command

aaa authentication ppp

ppp authentication

ppp chap password

ppp pap

1.1.17 ppp chap refuse

To decline the CHAO authentication mode of the peer, run **ppp chap refuse**.

Parameter

There is no parameters or keywords.

Default

The CHAO authentication mode of the peer to authenticate the local device is allowed by default.

Command mode

Interface configuration mode

Explanation

After **ppp chap refuse** is configured, all users are declined to use the CHAP authentication.

Example

The following example shows how to decline the CHAP authentication on interface serial1/0.

```
interface s1/0
encapsulation ppp
ppp chap refuse
```

Related command

ppp authentication

1.1.18 ppp ddr

To trigger the VPDN connection through packets on the **virtual-tunnel** port, run **ppp ddr**.

Parameter

There is no parameters or keywords.

Default

The packet does not trigger the VPDN connection by default. The VPDN connection will be continuously tried to establish after the port is lined up.

Command mode

Interface configuration mode

Explanation

After PPP DDR is configured, the virtual-tunnel port reports **protocol up** to the upper layer and adds the local route. When the packet from the upper layer is transmitted to the virtual-tunnel port through the local route, the VPDN connection is triggered.

Example

The following example shows how to decline the CHAP authentication on interface serial1/0.

```
!
interface virtual-tunnel
  0 ppp ddr
!
```

Related command

interface virtual-tunnel

1.1.19 ppp ipcp rfc-default

To set the IPCP negotiation to the default value of the PPP protocol, run **ppp ipcp rfc-default**.

Parameter

There is no parameters or keywords.

Default

The IPCP negotiation is not the default value of the protocol, that is, the IPCP negotiation is not performed by default.

Command mode

Interface configuration mode

Explanation

In general, the command need not be configured. The command is used to test the IPCP negotiation or the condition that the IPCP negotiation is not supported by the peer.

Example

The following example shows how to set the IPCP negotiation to the default value of the protocol.

```
ppp ipcp rfc-default
```

Related command

encapsulation ppp

1.1.20 ppp lcp echo

To set the transmission interval of the LCP echo packet, run the following command:

ppp lcp echo *seconds*

Parameter

Parameter	Description
seconds	Transmission interval of the LCP echo packet, ranging between 0 and 2147483647 seconds

Default

10 seconds

Command mode

Interface configuration mode

Explanation

Before the LCP echo packet is transmitted, you should set **second** to a value larger than zero.

Example

The following example shows how to set ICP echo on interface **serial 1/0** to 10 seconds.

```
!
interface s1/0
  encapsulation ppp
  ppp lcp echo 10
!
```

Related command

encapsulation ppp

1.1.21 ppp lcp enddisc-type

To select the identifier type of the **multilink ppp** point, run the following command:

ppp lcp enddisc-type [**null** | **local** | **ip** | **ieee8021** | **ppp** | **psdn**]

Parameter

None

Command mode

Interface configuration mode (multilink port)

Usage Description

The command is used to select the identifier type of the **multilink ppp** point when **multilink ppp** selects the protocol negotiation.

Example

```
37DE_config_m1#ppp lcp enddisc-type
ppp 37DE#debug ppp negotiate
 PPP Serial0/1: LCP   Listen  ; RX <- Config Req, id: 182, len: 32
2003-4-28 11:36:19   making Magic Number: 0xc69038e7
2003-4-28 11:36:19   making Protocol compression
2003-4-28 11:36:19     making Addr/Ctl compression
2003-4-28 11:36:19     making MRRU: 1524
2003-4-28 11:36:19   making ENDDISC: class 4 ,address "000000e3"
2003-4-28 11:36:19
PPP Serial0/1: LCP   Listen  ; TX -> Config Req, id: 8, len: 25
2003-4-28 11:36:19   checking Magic Number: 0xcff04a72
2003-4-28 11:36:19         result Config Ack, option 5, length 6
2003-4-28 11:36:19         making Magic Number: 0xcff04a72
2003-4-28 11:36:19   checking Protocol compression
2003-4-28 11:36:19         result Config Ack, option 7, length 2
2003-4-28 11:36:19         making Protocol compression
2003-4-28 11:36:19     checking Addr/Ctl compression
2003-4-28 11:36:19         result Config Ack, option 8, length 2
2003-4-28 11:36:19         making Addr/Ctl compression
2003-4-28 11:36:19     checking MRRU: 1524
2003-4-28 11:36:19         result Config Ack, option 17, length 4
2003-4-28 11:36:19         making MRRU: 1524
2003-4-28 11:36:19 checking ENDDISC: class 1 ,address "BD-00000059" ,len 11 ,toss(11->0)
2003-4-28 11:36:19 result Config Ack, option 19, length 14
2003-4-28 11:36:19         making ENDDISC: class 1 ,address "BD-00000059"
```

On the previous example, the **icp config request** packet from the local end contains the negotiation contents of enddisc. Here, its type is 4, that is, enddisc type ppp. The negotiation packet of the peer shows the type of enddisc is 1, that is, enddisc type local.

Attached: relation between enddisc number and enddisc name

type	name
0	null
1	local
2	ip
3	ieee8021
4	ppp
5	psdn

1.1.22 ppp lcp rfc-default

To set the LCP negotiation to the default value of the PPP protocol (do not negotiate all LCP options), run **ppp icp rfc-default**.

Parameter

There is no parameters or keywords.

Default

The LCP negotiation option is not the default value of the protocol, that is, the LCP option will be negotiated.

Command mode

Interface configuration mode

Explanation

In general, the command need not be configured. The command is used to test the LCP negotiation or the condition that the LCP negotiation is not supported by the peer.

Example

The following example shows how to set the LCP negotiation to the default value of the protocol.

```
ppp lcp rfc-default
```

Related command

encapsulation ppp

1.1.23 ppp lcp

ppp lcp [**close** | **listen** | **open**]

To open, close and listen the LCP connection, run the previous command.

Parameter

Parameter	Description
close	Closes the LCP connection.
listen	Sets LCP to the listening state.
open	Creates the LCP connection.

Default

The LCP is in the listening state.

Command mode

Interface configuration mode

Explanation

When the current PPP connection is closed by the **ppp lcp close** command, the LCP is in the **closed** state. Afterwards, the connection will not be created even if the remote dial -in is conducted. To start the PPP connection, you must run **ppp lcp listen** or **ppp lcp open**. The **ppp lcp open** command is used to transmit the LCP negotiation request positively.

Example

The following command is used to close the LCP connection.

```
ppp lcp close
```

Related command

encapsulation ppp

1.1.24 ppp max-bad-auth

To configure a point-to-point interface which will not be reset after an unsuccessful authentication, run **ppp max-bad-auth *number***. To immediately reset a point-to-point interface after an unsuccessful authentication, run **no ppp max-bad-auth**.

ppp max-bad-auth *number*

no ppp max-bad-auth

Parameter

Parameter	Description
number	Specifies the times of re-authentication, which ranges between 1 and 255. The default value is 5.

Default

5

Command mode

Interface configuration mode

Explanation

The command can be applied to any ppp-encapsulated serial interface, including the asynchronous serial interface, synchronous interface or ISDN interface.

Example

The following example shows that the BRIO interface can be authenticated twice after the first failed authentication.

```
!
interface bri 0
  encapsulation ppp
  ppp authentication chap
  ppp max-bad-auth 3
!
```

Related command

encapsulation ppp

1.1.25 ppp multilink

To start PPP with multiple links, run **ppp multilink**. To close PPP with multiple links, run **no ppp multilink**.

ppp multilink

no ppp multilink

Parameter

None

Default

The multilink is not started.

Command mode

Interface configuration mode

Explanation

The command can be applied to any ppp-encapsulated serial interface, including the asynchronous serial interface, synchronous interface or ISDN interface.

Example

```
!
interface Dialer0
  ip address 99.0.0.2
  255.0.0.0 encapsulation ppp
  dialer idle-timeout 500
  dialer map 99.0.0.1 name dialname1 broadcast
  81012345678901 dialer load-threshold 30 either
  dialer-group 1
  ppp authentication
  chap ppp multilink
!
```

Related command

encapsulation ppp

1.1.26 ppp pap refuse

To decline the PAP authentication mode of the peer, run **ppp pap refuse**.

Parameter

There are no parameters or keywords.

Default

The PAP authentication can be used on the peer to test the local terminal.

Command mode

Interface configuration mode

Explanation

After ppp pap refuse is configured, all users, legal users included, are declined to use the PAP authentication.

Example

The following example shows how to decline the PAP authentication on interface serial1/0.

```
!
interface s1/0
 encapsulation ppp
 ppp pap refuse
!
```

Related command

ppp authentication

1.1.27 ppp pap sent-username

To activate the PAP support on the remote terminal and use sent-username and password in the PAP request, run **ppp pap sent-username**. To forbid the PAP support on the remote terminal, run **no ppp pap sent-username**.

ppp pap sent-username *username password*

no ppp pap sent-username

Parameter

Parameter	Description
username	User name in the PAP authentication request
password	Password in the PAP authentication request

Default

The remote PAP support is forbidden.

Command mode

Interface configuration mode

Explanation

The command is used to activate the remote PAP support and specify the parameter during the PAP request transmission.

Example

The following example shows how to configure dialer interface 0 to the dialer group head and activate PPP encapsulation on the interface. CHAP or PAP only authenticates the received calls. When the remote terminal requests the router to conduct the PAP authentication, **guset1** and **mykey** will be transmitted to the remote terminal as the username and password respectively.

```
!
interface dialer0
  encapsulation ppp
  ppp authentication chap pap
  callin ppp chap hostname guest1
  ppp pap sent-username guest1 mykey
!
```

Related command

aaa authentication ppp

ppp authentication

ppp chap hostname

1.1.28 ppp timeout authentication

To set the timeout value of PPP authentication, run the following command:

ppp timeout authentication *seconds*

Parameter

Parameter	Description
seconds	Timeout time of negotiation, whose unit is second

Default

The timeout time of the PPP authentication is 3 seconds.

Command mode

Interface configuration mode

Explanation

During PPP authentication, if the echo packet from the peer is not received in the designated interval, PPP resends the authentication packet which is transmitted in the previous time.

Example

The following example shows that the timeout value of PPP authentication is set to 10 seconds.

```
ppp timeout authentication 10
```

Related command

encapsulation ppp

ppp authentication

1.1.29 ppp timeout ncp

To set the timeout value of PPP NCP negotiation, run the following command:

ppp timeout ncp *seconds*

Parameter

Parameter	Description
seconds	Timeout time of NCP negotiation, whose unit is second

Default

The timeout time of the PPP NCP negotiation is 3 seconds.

Command mode

Interface configuration mode

Explanation

During PPP NCP negotiation, if the echo packet from the peer is not received in the designated interval, PPP resends the authentication packet which is transmitted in the previous time.

Example

The following example shows that the timeout value of PPP NCP negotiation is set to 10 seconds.

```
ppp timeout ncp 10
```

Related command

encapsulation ppp

1.1.30 ppp timeout lcp

To set the timeout value of PPP LCP negotiation, run the following command:

ppp timeout lcp *seconds*

Parameter

Parameter	Description
seconds	Timeout time of LCP negotiation, whose unit is second

Default

The timeout time of the PPP LCP negotiation is 3 seconds.

Command mode

Interface configuration mode

Explanation

During PPP LCP negotiation, if the echo packet from the peer is not received in the designated interval, PPP resends the packet which is transmitted in the previous time.

Example

The following example shows that the timeout value of PPP LCP negotiation is set to 10 seconds.

```
ppp timeout lcp 10
```

Related command

encapsulation ppp

1.1.31 show ip local pool

To display the statistics information of the IP address pool, run the following command:

show ip local pool

Parameter

There are no parameters or keywords.

Command mode

Privileged EXEC mode

Explanation

The software will display the general lists and corresponding IP addresses of all defined address pools.

Example

The following is an example of the **show ip local pool** command.

```
Router# show ip local pool
Name      Begin            End             Number
sun       192.168.0.1      192.168.0.10       10
```

Related command

ip local pool

1.1.32 show ppp

To display the statistics information of the IP address pool, run the following command:

show ppp { **multilink |queue| status | version** }

Parameter

Parameter	Description
multilink	Displays relative information about ppp multilink.
queue	Displays the number of messages that the PPP queue has not handled.
Status	Displays the information about interface states which relate with PPP configuration.
version	Version of the PPP module

Command mode

All modes except the user mode

Explanation

The command is used to display information about PPP.

Example

The following is information about the interface state after the command is run:

```
Router# show ppp sta
PPP status information:
    5 links (total)
    1 link (protocol up)
    4 links (protocol down)
Protocol up:
    Name        ID Type     Status              Uptime         Peer
    S2/0        2 ALGC      Network Phase         0:04:32:01   1.0.0.2
Protocol down:
    Name        ID Type     Status              Downtime
    a0/0        1 ADC       Link Dead           0:04:48:15
    vt1         4 LVT       Link Dead           0:04:48:07
    d1          6 D         Link Dead           0:04:48:07
    m1           7 LMU      LCP Phase              0:04:48:07
```

On the previous information, the router is identified that five interfaces are configured PPP; only when interface s2/0 is in the **up** state, the **up** time is 04:32:01. The address of the peer is then 1.0.0.2. Other ports are in the **down** state.

Related command

None

1.1.33 username

To specify a password to use for the caller identifier of PPP CHAP and the PAP, run the following command:

username *name* password *secret*

Parameter

Parameter	Description
name	Host name, server name, user ID or command name
secret	Specifies the password for the local router, access server or remote device during CHAP authentication. The password will be stored on the local server or the access server after encryption, which prevents the password being stolen. The password consists of up to 11 printable ASCII characters, space and underline excluded. There is no limitation for the number of the username/password peer. Any number of remote devices can be authenticated.

Default

Predefined password does not exist.

Command mode

Global configuration mode

Explanation

The command is used to add a **name** entrance for every remote system requiring to be authenticated on the local router or the access server.

As a necessary part of authentication protocol configuration, the **username** command is mandatory. A username entrance must be added if every remote system of the local router and the access server need be authenticated.

Example

The following example shows how to enable CHAP on interface 0. The following information also shows that a password is defined for local server **Adam** and remote server **Eve**.

```
!
hostname Adam
!
interface s1/0
 encapsulation ppp
 ppp authentication chap
 username Eve password theirsystem
!
```

Related command

hostname

1.1.34 debug ppp

It is used to display the PPP parameter negotiation, authentication, message reception and transmission and error information.

debug ppp [***authentication*** **| cbcp |** ***error*** **| multilink |** ***negotiation*** **|** ***packet*** **|** ***raw***] [**interface***]*

Note: the **raw** parameter only used on the asynchronous interface.

Run **no debug snmp** to stop displaying relative information.

Parameter

Parameter	Description
authentication	Enables the debugging switch of the PPP authentication.
cbcp	Enables the debugging switch of the PPP dial-back control protocol.

error	Enables the debugging switch of the incorrect SNMP information.
negotiation	Enables the debugging switch the PPP negotiation.
packet	Enables the debugging switch of the input/output SNMP message.
raw	Enables the debugging switch of the input/output PPP asynchronous packet.
interface	Interface where PPP debugs information

Command mode

EXEC

Usage Description

After the PPP debugging switch is enabled, the PPP parameter negotiation, authentication process, message transmission and reception and error information are exported, helping you to check the PPP fault.

Example

The following example shows the procedure of receiving and transmitting the SNMP message:

```
Router#debug ppp packet s1/2
PPP Serial1/2: TX -> packet, len=88, protocol: LCP
FF 03 00 21 45 00 00 54 00 2F 00 00 FF 01 3E F1   ...!E..T./....   >.
01 00 00 0C 7B 7B 00 02 08 00 CB 37 00 12 00 00     ....{{.....7....
00 02 37 A5 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  ..7.............
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  ................
PPP Serial1/2: RX <- packet, len=85
21 45 00 00 54 9E 73 00 00 FF 01 A0 AC 7B 7B 00  !E..T.s......  {{.
02 01 00 00 0C 00 00 D3 37 00 12 00 00 00 02 37   ........7......  7
A5 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12  ................
13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22  .............          !"
```

Domain	Description
PPP	The currently debugged protocol is the PPP protocol.
Serial1/2	Current debugging interface
TX -> packet	PPP transmitting message
Len=85	Length for transmitting the message
protocol: LCP	Sub-protocol encapsulated in the current PPP protocol
FF 03 00 21 45 00 00 54 00 2F 00 00 FF 01 3E F1 01 00 00 0C 7B 7B 00 02 08 00 CB 37 00 12 00 00 00 02 37 A5 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F	The first four bytes combine the PPP header, while the following content is the data.
...!E..T./....>. ....{{.....7....	ASCII code presentation of message transmitting The content which is not in the

..7............	range of the ASCII code is presented with dots.
RX <- packet	SNMP receives the message.
Len=88	Length for receiving the message
21 45 00 00 54 9E 73 00 00 FF 01 A0 AC 7B 7B 00 02 01 00 00 0C 00 00 D3 37 00 12 00 00 00 02 37 A5 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22	The first byte is 0X21, which is a PPP value after IP and PFC are compressed. The previous value is 0X0021. The following is the data area.
!E..T.s......{{. ....7...... 7 .... !"	ASCII code presentation of message receiving The content which is not in the range of the ASCII code is presented with dots.

The following example shows how to simplify the PPP parameter negotiation.

```
Router#debug ppp negotiation s1/2
PPP Serial1/2: LCP   Listen    ; Start
PPP Serial1/2: LCP   Listen    ; TX -> Config Req, id: 52, len: 14
PPP Serial1/2: LCP   Req Sent; RX <- Config Ack, id: 52, len: 14
PPP Serial1/2: LCP   Ack Rcvd; RX <- Config Req, id: 88, len: 14
PPP Serial1/2: LCP    Ack Rcvd; TX -> Config Ack, id: 88, len: 14
PPP Serial1/2: LCP   Ack Rcvd; Opened
PPP Serial1/2: IPCP Listen   ; Start
PPP Serial1/2: IPCP Listen   ; TX -> Config Req, id: 53, len: 10
PPP Serial1/2: IPCP Req Sent; RX <- Config Req, id: 89, len: 16
PPP Serial1/2: IPCP Req Sent; TX -> Config Ack, id: 89, len: 16
PPP Serial1/2: IPCP Ack Sent; RX <- Config Ack, id: 53, len: 10
PPP Serial1/2: IPCP Ack Sent; Opened
```

Domain	Description
Serial1/2	Current debugging interface
PPP	PPP protocol
LCP	Link control protocol
IPCP	IP control protocol
Listen ˋReq Sent ˋ Ack Rcvd ˋ Ack Sent	State of the PPP protocol
id: 53	Message identifier
len:10	Length of the message

Chapter 2 **HDLC Configuration Command**

2.1 HDLC Configuration Command

HTTP configuration commands include:

- debug hdlc
- encapsulation hdlc

2.1.1 debug hdlc

To display the transmission and reception of the HDLC packet, run **debug hdlc** [***packet*** | ***error*****]** **[*****interface*****]**. Run **no debug hdlc** to stop displaying relative information.

[**no**] **debug hdlc** [***packet*** **|** ***error*****]** [*interface*]

Parameter

Parameter	Description
interface	Interface which displays the HDLC debugging information
packet	Enables the debugging switch of the HDLC reception/transmission message.
error	Enables the debugging switch of the incorrect HDLC information.

Command mode

EXEC

Usage Description

After the HDLC debugging switch is enabled, the HDLC reception/transmission packet or relative error information is exported, helping you to detect the HDLC fault.

Example

The following example shows the procedure of receiving and transmitting the HDLC message:

```
Router#debug hdlc packet s1/2
Router#
Serial1/2 HDLC RX <- packet, len=64
0F 00 08 00 45 00 00 3C BE 4A 00 00 7F 01 B2 BD     ....E..<.J......
C0 A8 00 10 0A 00 00 01 08 00 19 5C 02 00 32 00     ..........\..2.
```

```
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70     abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69       qrstuvwabcdefghi
Serial0/2 HDLC RX <- link check frame, len=22
8F 00 80 35 00 00 00 02 00 00 00 33 00 00 00 C7     ...5.......3....
FF FF 00 00 0B DE                                   ......
```

Domain	Description
HDLC	The currently debugged protocol is the HDLC protocol.
Serial0/2	Current debugging interface
RX <- packet	IP packets which are received by HDLC
len=64	Length for receiving the message
0F 00 08 00 45 00 00 3C BE 4A 00 00 7F 01 B2 BD C0 A8 00 10 0A 00 00 01 08 00 19 5C 02 00 32 00 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69	The first four bytes combine the HDLC frame header, while the following content is the data.
....E..<.J...... ....\..2. abcdefghijklmnop qrstuvwabcdefghi	ASCII code presentation of message receiving The content which is not in the range of the ASCII code is presented with dots.
RX <- link check frame	HDLC receives the link check frame.
len=22	Length of the link check frame
8F 00 80 35 00 00 00 02 00 00 00 33 00 00 00 C7 FF FF 00 00 0B DE	Hex presentation of the link check frame
...5.......3....	ASCII presentation of the link check frame The content which is not in the range of the ASCII code is presented with dots.

```
HDLC Serial0/2: TX -> packet, len=88
0F 00 08 00 45 00 00 54 00 07 00 00 FF 01 A7 9F     ....E..T........
0A 00 00 01 0A 00 00 02 08 00 00 03 00 0A 00 00     ................
00 01 02 E3 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F     ................
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F     ................
HDLC Serial0/2: TX -> link check frame, len=24
8F 00 80 35 00 00 00 02 00 00 01 15 00 00 00 42     ...5...........B
FF FF 30 2E 33 B9 53 01                             ..0.3.S.
```

Domain	Description
HDLC	The currently debugged protocol is the HDLC protocol.
Serial1/2	Current debugging interface
TX -> packet	HDLC is transmitting the IP packet.
len=88	Length for transmitting the message
0F 00 08 00 45 00 00 54 00 07 00 00 FF 01	The first four bytes combine the HDLC frame

A7 9F 0A 00 00 01 0A 00 00 02 08 00 00 03 00 0A 00 00 00 01 02 E3 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F	header, while the following content is the data.
....E..T.......	ASCII code presentation of message transmitting The content which is not in the range of the ASCII code is presented with dots.
TX -> link check frame	HDLC transmits the link check frame.
len=24	Length of the link check frame
8F 00 80 35 00 00 00 02 00 00 01 15 00 00 00 42 FF FF 30 2E 33 B9 53 01	Hex presentation of the link check frame
...5........... B ..0.3.S.	ASCII code presentation of the link check frame The content which is not in the range of the ASCII code is presented with dots.

2.1.2 encapsulation hdlc

To encapsulate HDLC on the interface, run **encapsulation hdlc**. To cancel encapsulation, run **no encapsulation hdlc**.

encapsulation hdlc

no encapsulation hdlc

Parameter

None

Default

None

Command mode

Interface configuration mode

Usage Description

If you run **no encapsulation hdlc**, the HDLC encapsulation is resumed.

Example

The following example shows how to configure the HDLC encapsulation mode of serial interface s1/1:

```
!
interface s1/1
  encapsulation hdlc
```