WAN Configuration

Table of Contents

Chapter 1 **Configuring PPP**

1.1 Overview

PPP provides multiple-protocol transportation on point-point link. The router's main fucntions are:

- It obeys RFC 1661 and supports link controlling protocol(LCP),is used to setup,configure and test data link.
- It obeys RFC 1662 and supports IP encapsulation on PPP, and it can realize IPCP on NCP.
- It obeys RFC 1334 and support several common authentication protocol ,including PAP,CHAP,MC-CHAP and TACACS+.
- It obeys RFC 1144 and support TCP/IP header compression, and it can advance efficiency data throughput.
- It provides broad chooses of items, can adapt many conditions, and it support to link to all kinds of network equipments and hosts through PPP.
- It support synchronism and asynchronism PPP .
- It support PPP multilink ,can realize multiple-link binding.
- It can support "call back", provides more safety.
- It can support RADIUS ,can realize authentication to user ,authorization and accouting when the router is used as a dialing server. The information of users are saved in a host, which switch information with routers through RADIUS.

This Chapter tells how to configure Point-to-Point Protocol (PPP) and introduces the address pool catering to point-to-point link and applicable to asynchronous serial, synchronous serial and ISDN interface.

1.1.1 Implementation Information

PPP protocol is described in RFC 1661. It offers method for encapsulating network layer protocol information on the point-to-point link. PPP protocol can be configured on the following types of physical interfaces:

- Asynchronous serial interface
- ISDN
- Synchronous serial interface

Similarly, by starting using PPP encapsulation at physical interface, PPP is also applied to the corresponding dial interface that uses this physical interface.

Among existing router softwares, PPP implementation supports negotiation option 2: asynchronous controlled character image; Option 3: application of CHAP or PAP authentication. Option 5: magic number configuration option; Option 7: Protocol Field Compression – PFC; Option 8: Address and Control Field Compression -- ACFC.

During the process of LCP negotiation, the software regularly sends negotiation option numbered 5, 7 and 8. The negotiation option 2 will be sent under asynchronous control. If authentication is configured, the negotiation option 3 will be transmitted. .

LCP negotiation option 5 (magic number) is supported on the whole serial interfaces. PPP always negotiates with magic number to detect the loopback link on the line.

Router software of the Company supports CHAP and PAP authentication protocol in the PPP protocol. The detail of authentication can be referred to “The Guide for Security Configuration”.

1.2 PPP Configuration Task List

On serial interface (ISDN included), the following tasks shall be executed for configuring PPP under interface configuration model.

- Invoking PPP Encapsulation

In the following paragraphs, the following tasks can be executed. These tasks are optional and used for offering multiple methods to advance the function of PPP.

- Invoking CHAP or PAP Authentication
- Invoking Callback Control Protocol (CBCP)
- Configuring IP Address Pool
- Disabling or Re-invoking Host Router of Opposite Terminal
- Configuring Multi-link PPP

1. Please refer to the part of “Examples of PPP Configuration”.

1.2.1 Invoking PPP Encapsulation

In order to pack the IP and other network layer protocol data packets on serial line, PPP can be encapsulated. Uder interface configuration model, the following commands can be used to invoke PPP encapsulation:

Command	Function
encapsulation ppp	Invoking PPP encapsulation

1.2.2 Invoking CHAP or PAP Authentication

If PPP protocol invokes CHAP or PAP authentication protocol, it is usually used to indicate which remote routers linking to the center node .

CHAP and PAP were first introduced in RFC 1334, and later, CHAP was updated in RFC1994. These two protocols are supported at both synchronous interface and asynchronous interface. When CHAP or PAP authentication is used, each router and access server need a name to identify itself. Such kind of authentication avoids the possibility that more than one links are built between two routers and prevents the unauthorized access.

CHAP or PAP is applicable to all the serial interface employing PPP encapsulation. The authentication reduces the security risk of router or access server.

Notes：

Before using CHAP or PAP, the PPP encapsulation must be in function.

When an interface invokes CHAP and remote equipment is trying to link to the interface, local reouter or access server will send a CHAP request(or challenges) to remote equipment, and wait for the response from the remote equipment. The challenges packet comprises ID, random digit, and host name or username of the local router.

The expected response includes two parts:

- Encrypted string composed of ID, password and random digit
- Host name or username of the remote equipment

When local router or access server receives the response, it will verify the password through executing the same encryption operation and searching the requested host name or username that are indicated in the response. The security password of the remote equipment and local router must be completely same.

In transmitting the response, the plaintext of password is never transmitted in a purpose of preventing the password from being spiedby other equipment and deterring the illegal access to the system. The remote equipment has no possiblity to link to local router without right response.

CHAP message interchange takes place only after the link is established. Local router or access server requires no password in the later phase of calling. (But local equipment can respond to the request from other equipment during the calling period.)

When PAP is invoked, the remote router that attempts to link local router or access server must transmit an authentication request. If the received authentication request contains the designated username and password, router software will send an authentication acknowledgement.

After CHAP or PAP is invoked, local router or access server requires the authentication by the remote equipment. If the remote equipment does not support the invoked protocol, no communication with the remote equipment will go on.

The following tasks have to be executed for using CHAP or PAP protocol:

1. Invoking PPP encapsulation
2. Invoking CHAP or PAP on the interface
3. CHAP authentication requires configuring host name. PAP authentication requires configuring username and password.

To invoke PPP encapulation, the following commands are used under interface configuration model:

Command	Function
encapsulation ppp	Invoking PPP on the interface

In order to invoke CHAP or PAP authentication, the following commands can be used under interface configuration model:

Command	Function
ppp authentication {**chap** | **ms-chap**|	Defining the supportive authentication method and order of

pap} [**word	default**] [**callin**]	using

The command under global configuration model can be used to designate the password for identifying calling subscriber in CHAP or PAP.

Command	Function
username *name* **password** *secret*	Configuring identification

Remark: Password contains no blank.

1.2.3 Invoking Callback Control Protocol (CBCP)

In CBCP, the terminal making the dial is called Caller; the recipient of the dial is called Answerer.

In LCP negotiation process, if two parties agree to use CBCP, CBCP will run immediately after authentication.

In callback period, call back request sent by answerer lists Callback options acceptable to Caller.

When Caller uses Callback Response to answer, it will list the options it prefers to use.

If Callback Response feedback from Caller is legal and accepted by Answerer, Answerer will use Callback Ack to answer. After receiving Callback Ack, Caller enters Link Termination phase and is ready to receive calling.

If CBCP is used, Caller needs configuring with ppp callback request cbcp (If caller designates a telephone number, it needs configuring dialer caller xx)

In addition to the configuration of ppp callback accept, Answerer does not need configuring a callback telephone number if the callback is not needed. If Caller designates a telephone number, it needs configuring user xx password xx callback-dialstring *dialer called *. If Answerer designates a telephone number, it needs configuring user xx password xx callback-dialstring xx；If Caller is asked to choose one from a group of telephone number provided by Answerer, it needs configuring dialer called xx；xx；xx.

The following tasks have to be executed for using CBCP:

1. Invoking PPP encapsulation.

Command	Function
encapsulation ppp	Invoking PPP at the interface

2. Configuring CBCP at the interface

Command	Function
ppp callback request cbcp	Configuring and invoking CBCP negotiation at the Caller
ppp callback accept	Configuring and invoking CBCP negotiation at the Answerer

3. Configuring the callback telephone number

Command	Function
dialer caller XX	Configuring the callback telephone number designated by Caller at the Caller

user *xx* **password** *xx* **callback-dialstring** {***	*xx***} **dialer called** {*	*xx ; xx ; xx*}	Configuring the telephone number designated by Caller at the Answerer, or designated by Answerer, or Caller chooses one from the group of telephone numbers provided by Answerer.

Answerer first inquires user xx password xx callback-dialstring, then dialer called xx. In addition, the switchboard number and extension number is separated by ",". The different telephone number is separated by "; ". "*" means that Caller designates a telephone number.

1.2.4 Configuring IP Address Pool

Point to point interface shall be able to provide IP address for remote node point through address negotiation of IP control protocol (IPCP). IP address can be obtained through different sources. The address can be configured by entering the command on "EXEC" level, or provided by TACACS+, or comes from local IP address pool.

1. Address Allocation of Opposite Terminal

IP address of opposite terminal can be positioned at an interface through several methods:

- IPCP Negotiation

  If opposite terminal presents an IP address in IPCP address negotiation and does not allocate other addresses for opposite terminal, the submitted terminal will be acknowledged and can only be used in the current session.
- Default IP address

  Default IP address can be set by using the command "peer default ip address".
- IP address or IP address pool allocated by TACACS+

  In IPCP address negotiation, TACACS+ is likely to return an IP address, which can be used by the authenticated user on the dial interface.
- Local Address Pool

  Local address pool includes the collection of consecutive IP address (1024 addresses at most). The idle addresses are used in FIFO (first in first out) mode to minimize the chance of repeated use of address and allow opposite terminal to rebuild a link with the address used in last link. If the address is usable, it will be allocated. Otherwise, another idle address will be allocated.

2. Principle of Priority

The following principle of priority of IP address of opposite terminal helps to determine which IP address to use. Priority ranks from most possible to least possible:

1. The address in local IP address pool (it is not allocated usually unless no other address exists)
2. The address configured by the command "peer default ip address" or "protocol translate".
3. The addresses provided by AAA/TACACS+ or the addresses in the pool nominated by AAA/TACACS+.
4. The address provided by opposite terminal through IPCP negotiation. It will not be accepted, unless no other IP address exists.

3. Affected Interface

Address pool exists in the interfaces that support asynchronous serial, synchronous serial, ISDN BRI and ISDN PRI on which PPP can be run.

4. Configuring IP Address Allocation at the Interfaces

1. Defining IP address pool at the designated interface
2. Allocating an IP address for dial-in users at the designated interface.

The following command is used to define IP address pool for an interface:

Command	Function
ip local pool *poolname* {*begin-ip-address* [*ip-address-number*]}	Creating one or multiple local IP address pools
interface *type number*	Designating interface and entering interface configuration model
peer default *ip address* **pool** *pool-name*	Designating IP address pool used by the interface

The following command is used to allocate an IP address to the designated interface:

Command	Function
ip local pool *poolname* {*begin-ip-address* [*ip-address-number*]}	Creating one or multiple local IP address pool
interface *type number*	Designating interface and entering interface configuration model
peer default ip address *ip-address*	Designating allocated address

1.2.5 Disabling or Re-invoking Host Router of Opposite Terminal

The router of the Company creates host router of opposite terminal automatically under default state, which means it automatically creates a router to the remote IP address at the point to point interface after PPP IPCP negotiation is completed.

Under the interface configuration model, the following command is used to disable the default act or re-invoking the act after it is disabled.

Command	Function
no peer neighbor-route	Disabling host router
peer neighbor-route	Re-invoking host router

1.2.6 Configuring Multi-link PPP

Multi-link PPP Protocol features the functions of providing load balancing on multiple WAN links. Multi-link PPP Protocol realized by the router software of the Company supports message fragment and sequence.

Multi-link allows the message to be fragment and simultaneously transmit the fragments to same remote IP address through multiple point to point links. The start of multi-link is determined on the load limit defined on the dialer. The load is likely to be

made up of incoming communication traffic, or out-coming communication traffic, or both. Multilink PPP allocates bandwidth on the demand and reduces the transmission time on the WAN at the same time.

Multi-link PPP can work at single or multiple interfaces. The usable types of interface includes:

- Serial Interface synchronous or asynchronous
- BRI Interface
- PRI interface

1. Configuring Multi-link PPP on Dial Line

Here is the example of asynchronous serial interface. Dialer and PPP encapsulation shall be supported at the interface first, then a dialer interface is configured to support PPP encapsulation and Multilink PPP.

Under global configuration model, the following command is used to configure asynchronous serial interface.

Command	Function
interface async *number*	Designating an interface
no ip address	Designating no IP address
encapsulation ppp	Invoking PPP encapsulation
line dial	Invoking dial at the interface
dialer rotary-group *number*	Including the interface at the designated dialer rotary group

If needed, the said steps can be repeated at other asynchronous interface.

Remarks: When configuring the interface of dialer rotary-group, its PPP configuration will automatically synchronizes with the interface of corresponding dialer.

the following commands are used to configure Dialer interface:

Command	Function
interface dialer *number*	Defining one dialer rotary group
no ip address	Designating no IP address
dialer load-threshold *load*	Setting the maximum load limit designated by the dial based on demand
ppp multilink	Invoking Multilink PPP.

2. Configuring Multi-link PPP at the Single ISDN BRI Interface

When Multilink PPP is invoked at the ISDN BRI interface, there is no need to define dialer rotary group as ISDN interface itself is a dialer rotary group under default state.

Under global configuration model, the following commands are used to configure ISDN BRI interface:

Command	Function
interface bri *number*	Defining an interface
ip address *ip-address mask*	Designating right IP address

[**secondary**]	
encapsulation ppp	Invoking PPP encapsulation
dialer idle-timeout *seconds*	(Optional) Designating timeouts of dialer idle
dialer load-threshold *load*	Configuring the maximum load limit designated by the dialer based on demand.
dialer map *protocol next-hop-address* [**name** *hostname*] [**broadcast**] [*dial-string*[:*isdn-subaddress*]]	Configuring dialer map
dialer-group *group-number*	Adding the interface to a dialer access group to control start-point access.
ppp authentication [**pap |chap| ms-chap**]	(Optional) Invoking PPP authentication
ppp multilink	Invoking Multilink PPP.

3. Configuring Mutlilink PPP at multiple ISDN BRI Interfaces

When Mutlilink PPP is configured at multiple ISDN BRI interfaces, a dialer rotary interface shall be created and shall be configured into Multilink PPP simultaneously. Then each BRI shall be configured independently and shall be added to the same rotary group.

The configuration for establishing dialer rotary interface is as follows:

Command	Function
interface dialer *number*	Defining an interface
ip address *ip-address mask*	Appointing right IP address
encapsulation ppp	Invoking PPP encapsulation
dialer idle-timeout *seconds*	(Optional) Designating timeout of dial idle
dialer load-threshold *load*	Configuring the maximum load limit designated by the dialer based on demand.
dialer map protocol *next-hop-address* [**name** *hostname*] [**broadcast**] [**dial-string** [:*isdn-subaddress*]]	Configuring dialer map
dialer-group *group-number*	Adding the interface to a dialer access group to control start-point access.
ppp authentication [**pap** |**chap** |**ms-chap**]	(Optional) Invoking PPP authentication
ppp multilink	Invoking Multilink PPP.

Configuring BRI interface subordinated to dialer rotary group is as follows:

Command	Function
interface bri *number*	Defining an interface
no ip address	Configuring no IP address
encapsulation ppp	Invoking PPP encapsulation
dialer idle-timeout *seconds*	(Optional) Designating timeout of dial idle
dialer rotary-group *number*	Adding the interface to a dialer rotary group

dialer load-threshold *load*	Configuring the maximum load limit of dialer

Other BRI interfaces can be configured by repeating.

Remarks: When configuring the interface of dialer rotary-group, its PPP configuration will automatically synchronizes with the interface of corresponding dialer.

4. Configuring Multilink PPP on Private Line

When Mutlilink PPP is configured at multiple private line interfaces, a multilink group interface shall be created and its default is configured into Multilink PPP simultaneously. Then each private line shall be configured independently and shall be added into the same multilink group.

The configuration for establishing multilink group interface is as follows:

Command	Function
interface multilink *group-number*	Defining the interface of multilink group
ip address *ip-address mask*	Designating right IP address
ppp authentication [**pap** **|chap** **|ms-chap**]	(Optional) Invoking PPP authentication
ppp multilink	Invoking Multilink PPP.

Configuring private line interface subordinated to multilink group is as follows:

Command	Function
interface type *number*	Defining an interface
no ip address	Configuring no IP address
encapsulation ppp	Invoking PPP encapsulation
multilink-group *group-number*	Adding the interface to multilink group

Other private line interfaces can be configured by repeating.

Remarks: When configuring the interface of multilink-group, its PPP configuration will automatically synchronizes with the interface of corresponding multilink group.

1.3 Examples of PPP Configuration

The examples of PPP configuration in this section are as follows:

1.3.1 Example of CHAP configuration

The following shows that three equipments invoke CHAP authentication protocol at the interface of serial1/0.

Configuring router1

```
hostname router1
```

```
interface s1/0
encapsulation ppp
ppp authentication chap
username router2 password secret12
username router3 password secret13
```

Configuring router2

```
hostname router2
interface s1/0
encapsulation ppp
ppp authentication chap
username router1 password secret12
username router3 password secret23
```

Configuring router3

```
hostname router3
interface s1/0
encapsulation ppp
ppp authentication chap
username router2 password secret23
username router1 password secret13
```

1.3.2 Example of Multilink PPP Configuration

The following examples show the configuration of Multilink PPP. The first example shows the configuration of a BRI interface, the second example shows the configuration of private line interface subordinated to multilink group interface. The third example shows multilink is configured by using virtual-template.

a. Configuring Multilink PPP at single ISDN BRI interface

```
interface bri 0/3
description connected to router
ip address 192.168.20.100 255.255.255.0
encapsulation ppp
dialer idle-timeout 30
dialer load-threshold 40 either
dialer map 171.1.1.8 name router  81012345678901
dialer-group 1
ppp authentication pap
ppp multilink
```

b. Example of Configuring Multilink PPP at private line interface

```
interface multilink 1
ip address 192.168.20.100 255.0.0.0
```

```
encapsulation ppp
ppp authentication chap
ppp chap hostname router
ppp multilink
interface s1/0
no ip address
encapsulation ppp
ppp authentication chap
ppp chap hostname router
ppp multilink
multilink-gourp 1
interface s1/1
no ip address
encapsulation ppp
ppp authentication chap
ppp chap hostname router
ppp multilink
multilink-gourp 1
interface s1/2
no ip address
encapsulation ppp
ppp authentication chap
ppp chap hostname router
ppp multilink
multilink-gourp 1
```

c. Configuring Multilink PPP by using virtual-template

```
multilink virtual-template 1
interface virtual-template 1
ip address 192.168.20.100
ppp multilink

interface s1/0
physical-layer mode async
no ip address
no ip directed-broadcast
ppp authentication pap
ppp multilink
ppp pap sent-username router mypassword
physical-layer speed 57600

interface s1/1
physical-layer mode async
no ip address
no ip directed-broadcast
ppp authentication pap
```

```
ppp multilink
ppp pap sent-username router mypassword
physical-layer speed 57600
```

Chapter 2 **Configuring HDLC**

2.1 Overview

High-level data link control protocol(HDLC)is derived from synchronization data link control protocol (SDLC) in SNA of IBM.After developing SDLC, IBM provides it to ANSI AND ISO, dividing them to America standard and international standard. And ANSI modified this protocol to advanced data communication CONTROL protocol(ADCCP);ISO modified this protocol to HDLC. Later,CCITT adopted and modified HDLC, and became a part of link access protocol (LAP) and X.25 interface standard. HDLC is a protocol facing to byte ,which guarantees clarities of data.

HDLC is a data packet protocol, it defines an linking encapsulation to IP packet on synchronization, and run TCP/IP on point-to-point serial line.

HDLC is usually used to DDN lines, and it is a simple and high-efficiency protocol.

HDLC Protocol provides the method of encapsulating network layer protocol information at the point to point linkage. This protocol can be configured at the following type of physical interface:

- ISDN
- Synchronous serial port

2.2 HDLC Configuration

When HDLC is configured at serial port (including ISDN), the following tasks shall be executed under interface configuration model.

2.2.1 Invoking HDLC Encapsulation

In order to encapsulate IP data package, HDLC protocol can be encapsulated at serial circuit.

Command	Function
encapsulation hdlc	Invoking HDLC encapsulation