HUAWEI NetEngine 8100 X, NetEngine 8000 X, NetEngine 8000E X 系列 V800R023C00SPC500

配置指南

文档版本 01

发布日期 2023-09-30

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 配置.....1
1.1 广域网接入.....1
1.1.1 PPP 配置.....1
1.1.1.1 PPP 特性描述.....1
1.1.1.1.1 PPP 介绍.....1
1.1.1.1.2 PPP 原理描述.....2
1.1.1.1.3 PPP 术语与缩略语.....12
1.1.1.2 PPP 配置.....12
1.1.1.2.1 PPP 概述.....12
1.1.1.2.2 PPP 特性限制.....13
1.1.1.2.3 配置接口支持 PPP 协议.....13
1.1.1.2.4 配置 CHAP 单向认证方式.....18
1.1.1.2.5 配置 PAP 单向认证方式.....21
1.1.1.2.6 PPP 配置举例.....23

插图目录

图 1-1 PPP 在协议栈中的位置 2
图 1-2 PPP 报文格式 3
图 1-3 PPP 链路建立过程 6
图 1-4 PAP 认证过程 8
图 1-5 PAP 验证报文帧格式 8
图 1-6 CHAP 的验证过程 10
图 1-7 CHAP 验证报文帧格式 11
图 1-8 配置 PAP 验证组网图 23
图 1-9 配置 CHAP 单向验证组网图 25
图 1-10 配置 CHAP 双向验证组网图 28

表格目录

表 1-1 常见的协议代码 4
表 1-2 常见 code 值 5
表 1-3 常见 Type 中的协商类型值 5
表 1-4 PAP 验证报文帧格式各字段解释表 9
表 1-5 CHAP 验证报文帧格式各字段解释表 11
表 1-6 各协商参数应用场景 14

1 配置

1.1 广域网接入

1.1.1 PPP 配置

1.1.1.1 PPP 特性描述

1.1.1.1.1 PPP 介绍

定义

PPP（Point-to-Point Protocol）协议是一种点到点链路层协议，主要用于在全双工的同异步链路上进行点到点的数据传输。

PPP定义的协议组件包括：

- 数据封装方式，定义封装多协议数据包的方法。
- 链路控制协议LCP（Link Control Protocol），主要用来建立、监控和拆除数据链路。
- 网络层控制协议NCP（Network Control Protocol），主要用来建立和配置不同的网络层协议，协商在该数据链路上所传输的数据包的格式与类型。

同时，PPP还提供了用于网络安全方面的验证协议族PAP（Password Authentication Protocol）和CHAP（Challenge Handshake Authentication Protocol），用于网络安全方面的验证。

当用户对带宽的要求较高时，单个的PPP链路无法提供足够的带宽，这时将多个PPP链路进行捆绑形成MP链路，旨在增加链路的带宽并增强链路可靠性。

目的

PPP协议处于OSI（Open Systems Interconnection）参考模型的第二层，主要用在支持全双工的同异步链路上，进行点到点之间的数据传输。由于它能够提供用户验证，易于扩充，并且支持同异步通信，因而获得广泛应用。

PPP协议是在串行线IP协议SLIP（Serial Line IP）的基础上发展起来的。由于SLIP协议具有只支持异步传输方式、无协商过程（尤其不能协商如双方IP地址等网络层属性）、只能承载IP一种网络层报文等缺陷，在发展过程中，逐步被PPP协议所替代。PPP协议有如下优点：

- 对物理层而言，PPP既支持同步链路又支持异步链路，而X.25等数据链路层协议仅支持同步链路，SLIP仅支持异步链路。
- PPP协议具有良好的扩展性。
- 提供LCP（Link Control Protocol）协议，用于各种链路层参数的协商。
- 提供各种NCP（Network Control Protocol）协议（如IPCP、IPXCP），用于各网络层参数的协商，更好地支持了网络层协议。
- 提供认证协议CHAP（Challenge-Handshake Authentication Protocol）和PAP（Password Authentication Protocol），更好地保证了网络的安全性。
- 无重传机制，网络开销小，速度快。

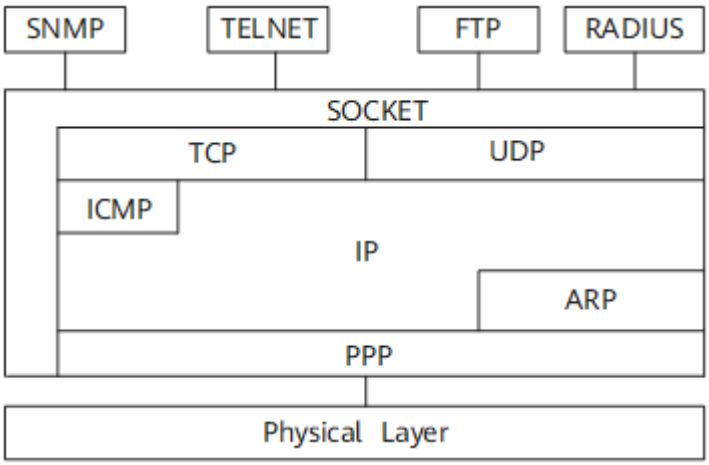
1.1.1.1.2 PPP 原理描述

PPP 的基本概念

PPP 的基本架构

PPP协议处于TCP/IP的数据链路层，主要用在支持全双工的同异步链路上，进行点到点之间的数据传输。

图 1-1 PPP 在协议栈中的位置



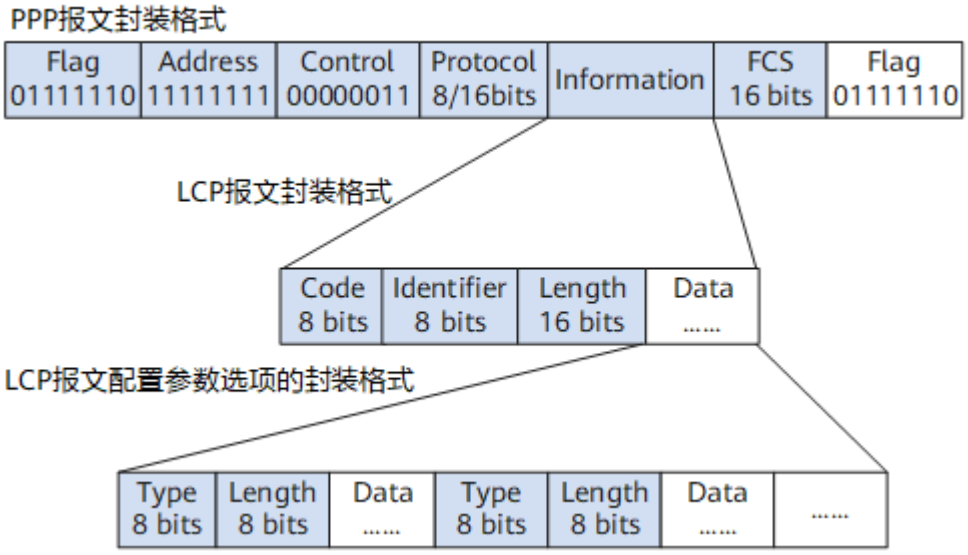
PPP主要由以下几类协议族组成：

- 链路控制协议族，主要用来建立、拆除和监控PPP数据链路。
- 网络层控制协议族，主要用来协商在该数据链路上所传输的数据包的格式与类型。
- PPP扩展协议族，主要用于提供对PPP功能的进一步支持。例如，PPP提供了用于网络安全方面的验证协议族CHAP和PAP。

PPP 报文封装的帧格式

PPP报文封装格式如图1-2所示。

图 1-2 PPP 报文格式



各字段的含义如下：

- Flag域

  Flag域标识一个物理帧的起始和结束，该字节为0x7E。

- Address域

  Address域可以唯一标识对端。PPP协议是被运用在点对点的链路上，因此，使用PPP协议互连的两个通信设备无须知道对方的数据链路层地址。按照协议的规定将该字节填充为全1的广播地址，对于PPP协议来说，该字段无实际意义。

- Control域

  该字段默认值为0x03，表明为无序号帧，PPP默认没有采用序列号和确认机制来实现可靠传输。

  Address和Control域一起标识此报文为PPP报文，即PPP报文头为FF03。

- Protocol域

  Protocol域可用来区分PPP数据帧中信息域所承载的数据包类型。

  Protocol域的内容必须依据ISO 3309的地址扩展机制所给出的规定。该机制规定协议域所填充的内容必须为奇数，也就是要求最低有效字节的最低有效位为“1”，最高有效字节的最低有效位为“0”。

  如果当发送端发送的PPP数据帧的协议域字段不符合上述规定，接收端则会认为此数据帧是不可识别的。接收端向发送端发送一个Protocol-Reject报文，在该报文尾部将填充被拒绝报文的协议号。

表 1-1 常见的协议代码

协议代码	协议类型
0021	Internet Protocol
002b	Novell IPX
002d	Van Jacobson Compressed TCP/IP
002f	Van Jacobson Uncompressed TCP/IP
8021	Internet Protocol Control Protocol
802b	Novell IPX Control Protocol
8031	Bridging NC
C021	Link Control Protocol
C023	Password Authentication Protocol
C223	Challenge Handshake Authentication Protocol

- Information域

  Information域最大长度是1500字节，其中包括填充域的内容。Information域的最大长度称为最大接收单元MRU（Maximum Receive Unit）。MRU的缺省值为1500字节，在实际应用当中可根据实际需要进行MRU的协商。

  如果Information域长度不足，可被填充，但不是必须的。如果填充则需通信双方的两端能辨认出填充信息和真正需要传送的信息，方可正常通信。

- FCS域

  FCS域的功能主要对PPP数据帧传输的正确性进行检测。

  在数据帧中引入了一些传输的保证机制，会引入更多的开销，这样可能会增加应用层交互的延迟。

LCP 报文封装的帧格式

LCP报文封装格式请参见**图1-2**。

在链路建立阶段，PPP协议通过LCP报文进行链路的建立和协商。此时LCP报文作为PPP的净载荷被封装在PPP数据帧的Information域中，PPP数据帧的协议域的值固定填充0xC021。

在链路建立阶段的整个过程中信息域的内容是变化的，它包括很多种类型的报文，所以这些报文也要通过相应的字段来区分。

- Code域

  Code域的长度为一个字节，主要是用来标识LCP数据报文的类型。

  在链路建立阶段，接收方接收到LCP数据报文。当其Code域的值无效时，就会向对端发送一个LCP的代码拒绝报文（Code-Reject报文）。

表 1-2 常见 code 值

code值	报文类型
0x01	Configure-Request
0x02	Configure-Ack
0x03	Configure-Nak
0x04	Configure-Reject
0x05	Terminate-Request
0x06	Terminate-Ack
0x07	Code-Reject
0x08	Protocol-Reject
0x09	Echo-Request
0x0A	Echo-Reply
0x0B	Discard-Request
0x0C	Reserved

- Identifier域

  Identifier域为1个字节，用来匹配请求和响应，当Identifier域值为非法时，该报文将被丢弃。

  通常一个配置请求报文的ID是从0x01开始逐步加1的。当对端接收到该配置请求报文后，无论使用何种报文回应对方，但必须要求回应报文中的ID要与接收报文中的ID一致。

- Length域

  Length域的值就是该LCP报文的总字节数据。它是Code域、Identifier域、Length域和Data域四个域长度的总和。

  Length域所指示字节数之外的字节将被当作填充字节而忽略掉，而且该域的内容不能超过MRU的值。

- Data域

  Data域所包含的是协商报文的内容，这个内容包含以下字段。

  - Type为协商选项类型。
  - Length为协商选项长度，它是指Data域的总长度，也就是包含Type、Length和Data。
  - Data为协商选项的详细信息。

表 1-3 常见 Type 中的协商类型值

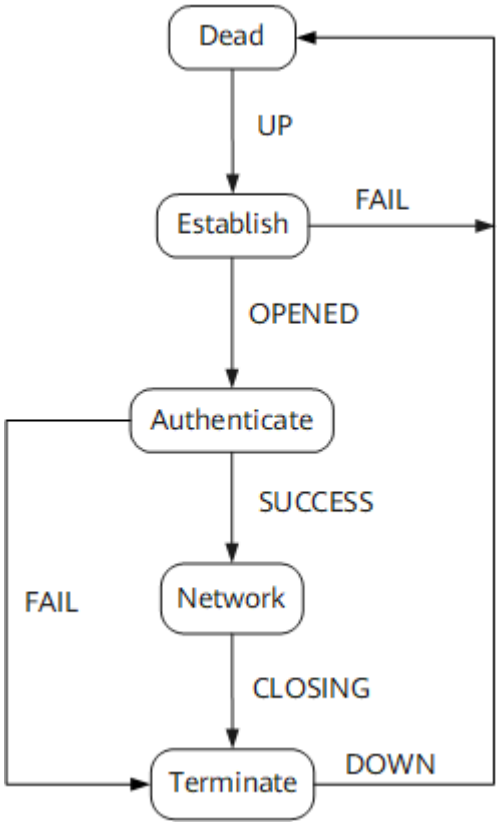
协商类型值	协商报文类型
0x01	Maximum-Receive-Unit
0x02	Async-Control-Character-Map

协商类型值	协商报文类型
0x03	Authentication-Protocol
0x04	Quality-Protocol
0x05	Magic-Number
0x06	RESERVED
0x07	Protocol-Field-Compression
0x08	Address-and-Control-Field-Compression

PPP 的建链过程

PPP链路的建立是通过一系列的协商完成的。

图 1-3 PPP 链路建立过程



PPP运行的过程如图1-3所示。

1. 通信双方开始建立PPP链路时，先进入到Establish阶段。
2. 在Establish阶段，PPP链路进行LCP协商。协商内容包括工作方式是SP（Single-link PPP）还是MP（Multilink PPP）、最大接收单元MRU、验证方式和魔术字（magic number）等选项。LCP协商成功后进入Open状态，表示底层链路已经建立。

3. 如果配置了验证，将进入Authenticate阶段，开始CHAP或PAP验证。如果没有配置验证，则直接进入Network阶段。
4. 在Authenticate阶段，如果验证失败，进入Terminate阶段，拆除链路，LCP状态转为Down。如果验证成功，进入Network阶段，此时LCP状态仍为Open。
5. 在Network阶段，PPP链路进行NCP协商。通过NCP协商来选择和配置一个网络层协议并进行网络层参数协商。只有相应的网络层协议协商成功后（相应协议的NCP协商状态为Open），该网络层协议才可以通过这条PPP链路发送报文。

   NCP协商包括IPCP（IP Control Protocol）、MPLSCP（MPLS Control Protocol）等协商。IPCP协商内容主要包括双方的IP地址。
6. NCP协商成功后，PPP链路将一直保持通信。PPP运行过程中，可以随时中断连接，物理链路断开、认证失败、定时器超时、管理员通过配置关闭连接等动作都可能导致链路进入Terminate阶段。
7. 在Terminate阶段，如果所有的资源都被释放，通信双方将回到Dead阶段，直到通信双方重新建立PPP连接，开始新的PPP链路建立。

Dead 阶段（链路不可用阶段）

Dead阶段也称为物理层不可用阶段。PPP链路都需从这个阶段开始和结束。

当通信双方的两端检测到物理线路激活（通常是检测到链路上有载波信号）时，就会从Dead阶段跃迁至Establish阶段，即链路建立阶段。

链路被断开后也同样会返回到链路不可用阶段。

Establish 阶段（链路建立阶段）

在Establish阶段，PPP链路进行LCP协商。协商内容包括工作方式是SP（Single-link PPP）还是MP（Multilink PPP）、最大接收单元MRU、验证方式和魔术字（magic number）等选项。当完成配置报文的交换后，则会继续向下一个阶段跃迁。

在Establish阶段，LCP的状态机会发生如下改变。

- 当链路处于不可用阶段时，此时LCP的状态机处于初始化Initial状态或准备启动Starting状态。当检测到链路可用时，则物理层会向链路层发送一个Up事件。链路层收到该事件后，会将LCP的状态机从当前状态改变为Request-Sent（请求发送）状态，根据此时的状态机LCP会进行相应的动作，也就是开始发送Configure-Request报文来配置数据链路。
- 如果本端设备先收到Configure-Ack报文，则LCP的状态机从Request-Sent状态改变为Ack-Received状态，本端向对端发送Configure-Ack报文以后，LCP的状态机从Ack-Received状态改变为Open状态。
- 如果本端设备先向对端发送Configure-Ack报文，则LCP的状态机从Request-Sent状态改变为Ack-Sent状态，本端收到对端发送的Configure-Ack报文以后，LCP的状态机从Ack-Sent状态改变为Open状态。
- LCP状态机变为Open状态以后就完成当前阶段的协商，并向下一个阶段跃迁。

下一个阶段既可能是验证阶段，也可能是网络层协议阶段。下一阶段的选择是依据链路两端的设备配置的，通常由用户来配置。

Authenticate 阶段（验证阶段）

缺省情况下，PPP链路不进行验证。如果要求验证，在链路建立阶段必须指定验证协议。

PPP提供密码验证协议PAP和质询握手验证协议CHAP两种验证方式。

说明

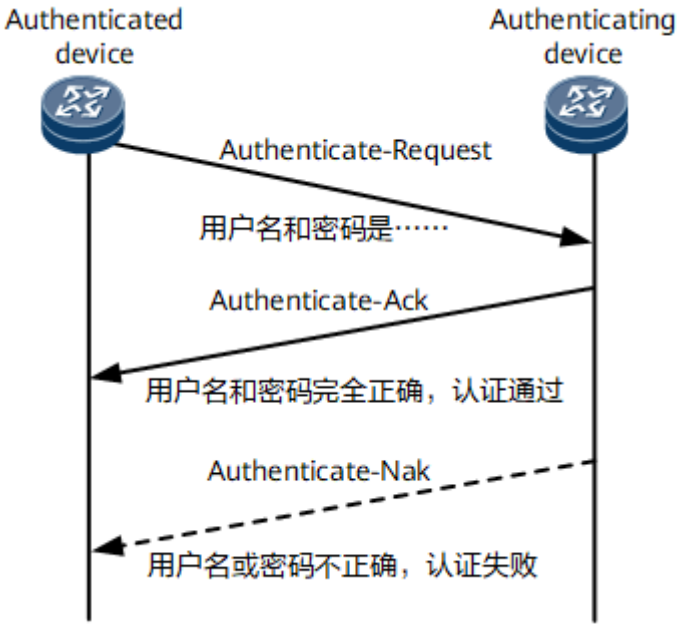
PPP的验证方式又可以分为单向验证和双向验证。单向验证是指一端作为验证方，另一端作为被验证方。双向验证是单向验证的简单叠加，即两端都是既作为验证方又作为被验证方。在实际应用中一般只采用单向验证。

PAP验证过程

PAP验证方式为两次握手验证，采用简单口令。

PAP验证的过程如图1-4所示。

图 1-4 PAP 认证过程

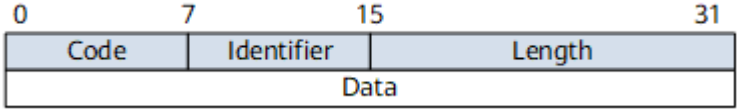


1. 被验证方把本地用户名和口令发送到验证方。
2. 验证方根据本地用户表查看是否有被验证方的用户名
   - 若有，则查看口令是否正确，
     - 若口令正确，则认证通过；
     - 若口令不正确，则认证失败。
   - 若没有，则认证失败。

PAP验证报文帧格式

PAP报文封装在协议域为0xC023的PPP数据链路层帧的信息域中。PAP报文的帧格式如图1-5所示。

图 1-5 PAP 验证报文帧格式



PAP验证报文帧格式中各字段的含义如表1-4所示。

表 1-4 PAP 验证报文帧格式各字段解释表

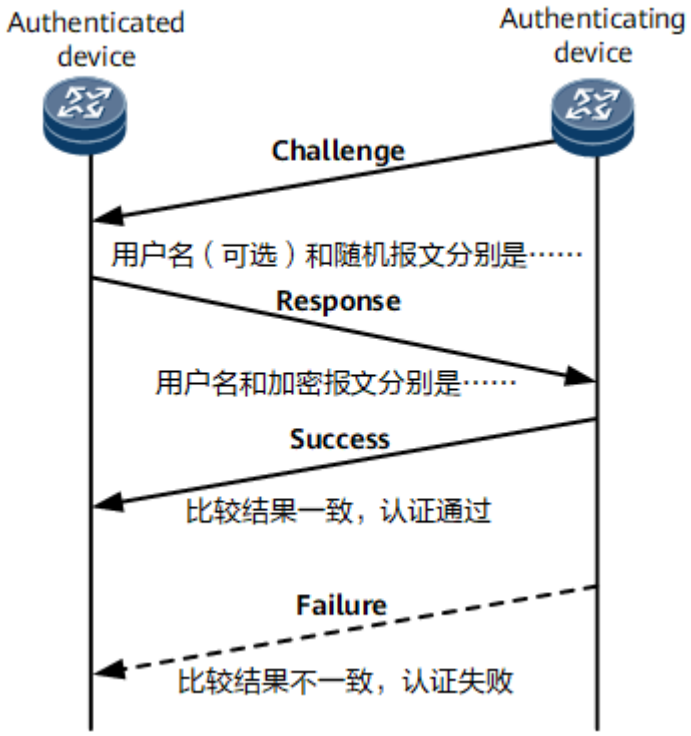
字段	长度（字节）	取值与含义
Code	1	标识PAP数据报的类型。 • Authenticate-Request报文的该字段取值为0x01。 • Authenticate-Ack报文的该字段取值为0x02。 • Authenticate-Nak报文的该字段取值为0x03。
Identifier	1	标识请求报文和应答报文是否匹配。
Length	2	标识包括Code、Identifier、Length和Data域在内的PAP报文长度。 超出此长度的报文将被认为是填充字节并被丢弃。
Data	0或者多个字节	Data域的内容由Code域来决定。

CHAP验证过程

CHAP验证方式为三次握手验证协议。它只在网络上传输用户名，而并不传输用户密码，因此安全性要比PAP高。

CHAP的验证过程如图1-6所示。

图 1-6 CHAP 的验证过程



CHAP单向验证过程分为两种情况：验证方配置了用户名和验证方没有配置用户名。推荐使用验证方配置用户名的方式，这样可以对验证方的用户名进行确认。

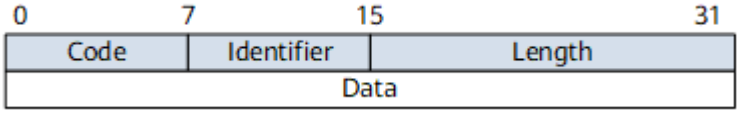
- 验证方配置了用户名的验证过程
  a. 验证方主动发起验证请求，验证方构造一个包含随机数的报文，并同时附带本端的用户名发送给被验证方（Challenge）。
  b. 被验证方接到验证方的验证请求后，先检查本端接口上是否配置了CHAP密码。
     - 如果接口配置CHAP密码，则被验证方根据报文ID、CHAP密码和报文中的随机数，利用hash算法计算hash值，将所得hash值和被验证方自己的用户名发回验证方（Response）。
     - 如果接口未配置CHAP密码，则根据此报文中验证方的用户名在本端的用户表查找该用户对应的密码，根据报文ID、此用户密码和报文中的随机数，利用hash算法计算hash值，将所得hash值和被验证方自己的用户名发回验证方（Response）。
  c. 验证方根据报文ID、自己保存的被验证方密码和Challenge报文中的随机数，利用hash算法计算hash值，并与Response报文中的hash值进行比较，若比较结果一致，认证通过，若比较结果不一致，认证失败。
- 验证方没有配置用户名的验证过程
  a. 验证方主动发起验证请求，验证方向被验证方发送一个包含随机数的报文（Challenge）。
  b. 被验证方接到验证方的验证请求后，根据报文ID、**ppp chap password**命令配置的CHAP密码和报文中的随机数，利用hash算法计算hash值，将所得Hash值和自己的用户名发回验证方（Response）。

c. 验证方根据报文ID、自己保存的被验证方密码和Challenge报文中的随机数，利用hash算法计算hash值，并与Response报文中的hash值进行比较，若比较结果一致，认证通过，若比较结果不一致，认证失败。

CHAP验证报文帧格式

CHAP报文封装在协议域为0xC223的PPP数据链路层帧的信息域中。CHAP报文的帧格式如图1-7所示。

图 1-7 CHAP 验证报文帧格式



CHAP验证报文帧格式中各字段的含义如表1-5所示。

表 1-5 CHAP 验证报文帧格式各字段解释表

字段	长度（字节）	取值与含义
Code	1	标识CHAP报文的类型： • Challenge报文的该字段取值为0x01。 • Response报文的该字段取值为0x02。 • Success报文的该字段取值为0x03。 • Failure报文的该字段取值为0x04。
Identifier	1	标识Challenge报文和Response报文的对应关系。
Length	2	标识包括Code、Identifier、Length和Data域在内的CHAP报文长度。 超出此长度的报文将被认为是填充字节并被丢弃。
Data	0或者多个字节	Data域的内容由Code域来决定。

说明

CHAP与PAP验证存在如下差异：

- PAP认证中，在链路上发送简单口令，完成PPP链路建立后，被验证方会不停地在链路上反复发送用户名和口令，直到身份验证过程结束，所以安全性不高。当实际应用过程中，对安全性要求不高时，可以采用PAP认证建立PPP连接。
- CHAP认证中，验证协议为三次握手验证协议。它只在网络上传输用户名，而并不传输用户密码，因此安全性比PAP认证高。当实际应用过程中，对安全性要求较高时，可以采用CHAP认证建立PPP连接。

Network 阶段（网络层协议阶段）

PPP完成了前面几个阶段，通过NCP协商来选择和配置一个网络层协议并进行网络层参数协商。每个NCP协议可在任何时间打开和关闭，当一个NCP的状态机变成Open状态时，则PPP就可以开始在链路上承载网络层数据传输。

Terminate 阶段（网络终止阶段）

PPP能在任何时候终止链路。当载波丢失、认证失败或管理员人为关闭链路等情况均会导致链路终止。

1.1.1.1.3 PPP 术语与缩略语

术语

无

缩略语

缩略语	英文全称	中文全称
CHAP	Challenge-Handshake Authentication Protocol	挑战握手认证协议
FCS	Frame Check Sequence	帧校验序列
LCP	Link Control Protocol	链路控制协议
MRRU	Max Receive Reconstructed Unit	最大接收重组单元
MRU	Max Receive Unit	最大接收单元
NCP	Network Control Protocol	网络控制协议
PAP	Password Authentication Protocol	密码认证协议
PPP	Point-to-Point Protocol	点到点协议
SLIP	Serial Line Internet Protocol	串行线路因特网协议

1.1.1.2 PPP 配置

PPP协议处于OSI中的数据链路层，同时也处于TCP/IP协议栈的链路层，是一种在点到点链路上传输、封装网络层数据包的数据链路层协议，在SLIP的基础上发展起来的。由于它能够提供用户验证，易于扩充，并且支持同异步通信，因而获得广泛应用。

1.1.1.2.1 PPP 概述

介绍了PPP特性的原理、协议等。

点到点的直接连接是广域网连接的一种比较简单的形式，点到点连接的线路上链路层封装的协议主要有PPP（Point-to-Point Protocol）。

PPP协议处于OSI（Open Systems Interconnection）参考模型的第二层，主要用在支持全双工的同异步链路上，进行点到点之间的数据传输。由于它能够提供用户验证，易于扩充，并且支持同异步通信，因而获得广泛应用。

PPP定义的协议组件包括：

- 数据封装方式，定义封装多协议数据包的方法。
- 链路控制协议LCP（Link Control Protocol），主要用来建立、监控和拆除数据链路。
- 网络层控制协议NCP（Network Control Protocol），主要用来建立和配置不同的网络层协议，协商在该数据链路上所传输的数据包的格式与类型。

同时，PPP还提供了用于网络安全方面的验证协议族PAP（Password Authentication Protocol）和CHAP（Challenge Handshake Authentication Protocol），用于网络安全方面的验证。

当用户对带宽的要求较高时，单个的PPP链路无法提供足够的带宽，这时将多个PPP链路进行捆绑形成MP链路，旨在增加链路的带宽并增强链路可靠性。

1.1.1.2.2 PPP 特性限制

1.1.1.2.3 配置接口支持 PPP 协议

通过配置接口支持PPP协议，完成基本的PPP链路层协议功能，实现点到点之间的数据传输。

应用环境

PPP协议是在点到点链路上承载网络层数据包的一种链路层协议，其定义了一整套的协议，主要包括链路控制协议（LCP）和网络层控制协议（NCP）。

- 在LCP协商阶段，主要进行PPP MRU（Maximum Receive Unit，最大接收单元）、协商超时时间间隔及链路处于Dead状态的时间的协商。
- 在NCP协商阶段，主要对网络层报文的一些属性和类型进行协商。如在IPCP协商中，会进行DNS服务器地址的协商。

为了实时监控链路状态，可以选择配置链路状态监控参数，及时发现链路故障，并做出适当的调整。此外，由于PPP链路不严格限制对端路由和本端路由在同一网段，可以选择配置抑制对端主机路由加入本端直连路由表中的功能，防止出现错误的路由信息。

前置任务

在配置PPP链路层协议之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为Up。

配置接口封装 PPP 协议

配置接口的链路层封装协议类型为PPP。

背景信息

PPP（Point-to-Point Protocol，点对点协议）是一种点到点的链路层协议，易于扩充，并且支持同步和异步通信。在进行PPP链路层协议相关功能配置前，首先需要配置接口的链路层封装类型为PPP。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**link-protocol ppp**，配置接口封装的链路层协议为PPP。

步骤4 执行命令**commit**，提交配置。

----结束

（可选）配置 PPP 协商

配置PPP协商，包括PPP MRU、协商超时时间间隔及DNS服务器地址的协商。

背景信息

PPP链路的建立是通过一系列的协商完成的，当物理链路状态Up后，进入链路建立（Establish）阶段，启动LCP协商。LCP协商成功后，如果配置了网络层协议，则进行NCP协商，对在数据链路上所传输的网络层报文的一些属性和类型进行协商。

表 1-6 各协商参数应用场景

协商参数	应用场景	所处协商阶段
PPP MRU	如果接口下配置了MTU（Maximum Transmit Unit，最大传输单元）值，则需要使能PPP MRU协商功能，使链路两端的MTU协商一致，保证数据的正常传输。当链路两端接口的MTU值不同时，PPP MRU协商结果将采用较小的MTU值作为链路的MTU值，保证通信双方都有接收来自对端的报文能力。	LCP协商阶段
协商超时时间间隔	在PPP LCP协商过程中，本端设备会向对端设备发送LCP协商报文，如果在指定协商时间间隔内没有收到对端的应答报文，则重新发送。	LCP协商阶段

协商参数	应用场景	所处协商阶段
DNS服务器地址协商	设备在进行IPCP协商的过程中可以进行DNS服务器地址协商。设备既可以向对端提供DNS服务器地址，也可以接收对端分配的DNS服务器地址，这样，设备就可以通过分配的DNS服务器来解析域名。 • 当设备通过PPP协议与对端设备相连时，如PC机拨号连接路由器，通过配置DNS服务器地址协商，可以为对端PC机分配DNS服务器地址。 • 当设备通过PPP协议连接运营商的接入服务器时，设备应配置为被动接收对端指定DNS服务器地址。	NCP协商阶段
OSICP和MPLSCP协商	当不同的设备进行对接时，由于不同设备间OSICP和MPLSCP的默认情况不一致，因此，需要配置设备两端是否需要进行交互协商，保证设备两端情况一致。	NCP协商阶段

说明

VS模式下，协商超时时间间隔仅在Admin VS支持。

操作步骤

- 配置PPP MRU协商
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**ppp mru-negotiate** { **ipv4** | **ipv6** }，配置链路控制层进行PPP MRU协商。

  须知

  若接口配置了IPv6 MTU值，需要使能PPP IPv6 MRU协商。需要在接口下依次执行**shutdown**、**commit**、**undo shutdown**、**commit**命令，或执行**restart**、**commit**命令，配置才能生效。

- 配置协商超时时间间隔
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**ppp timer negotiate** *seconds*，配置协商超时时间间隔。
  d. 执行命令**commit**，提交配置。
- 配置DNS服务器地址协商
  – 配置为对端设备分配DNS服务器地址。

i. 执行命令**system-view**，进入系统视图。
ii. 执行命令**interface** *interface-type interface-number*，进入接口视图。
iii. 执行命令**ppp ipcp dns** *primary-dns-address* [*secondary-dns-address*]，配置为对端设备分配DNS服务器地址。

- 配置接受对端分配的任何DNS服务器地址。
  i. 执行命令**system-view**，进入系统视图。
  ii. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  iii. 执行命令**ppp ipcp dns admit-any**，配置接受对端提出的任何DNS服务器地址。

  说明

  当对端设备强制为本端设备指定DNS服务器地址时，可能会由于本端设备不接受该指定，导致双方协商不成功。为了适应这种情况，可以配置**ppp ipcp dns admit-any**命令，接受对端分配的任何DNS服务器地址。

须知

完成DNS服务器地址协商配置后，需要在接口下依次执行**shutdown**、**commit**和**undo shutdown**、**commit**命令，或执行**restart**、**commit**命令，配置才能生效。

----结束

（可选）配置 PPP 链路状态监控

通过配置PPP链路状态监控参数，可以有效监控PPP链路状态。

背景信息

PPP链路状态监控参数包括：

- **保持活跃时间**
  - **轮询时间间隔**

    轮询时间间隔指的是接口发送Keepalive报文的周期。当接口上封装的链路层协议为PPP时，链路层会周期性地向对端发送Keepalive报文。如果接口在5个keepalive周期内无法收到对端应答的Keepalive报文时，链路层则认为对端故障，将链路状态置Down。如果网络的延迟比较大，或拥塞程度较高，可以适当加大轮询时间间隔，以减少网络震荡的发生。
  - **保持活跃数**

    在指定的一次轮询时间间隔内，设备若没有收到对端发送的Keepalive报文，则保持活跃数加1。当达到指定的保持活跃次数后，仍没有收到Keepalive报文，则认为链路故障，将链路状态置为Down。

综上所述，保持活跃时间=轮询时间间隔 × 保持活跃数。如果配置保持活跃时间过短，同时网络的延迟比较大，或拥塞程度较高，可能引起网络震荡。如果配置保持活跃时间过长，可能引起链路检测反应较慢。因此，用户可以根据网络的实际情况，进行合理的设置。

操作步骤

- 配置轮询时间间隔
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**timer hold** *interval*，配置轮询时间间隔。

     说明

     链路两端设备的轮询时间间隔应设为相同的值。如果将两端的轮询时间间隔都设为0，则禁止链路检测功能。
  d. 执行命令**commit**，提交配置。
- 配置保持活跃数
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**commit**，提交配置。

----结束

（可选）抑制对端主机路由加入本端直连路由表

为了防止本端直连路由表中出现错误的路由信息，可以使能抑制对端主机路由加入本端直连路由表的功能。

背景信息

PPP链路不严格限制对端路由和本端路由在同一网段。当PPP链路两端不在同一网段时也可以互通，并且自动将对端不在同一个网段的主机路由加到直连路由表中。因此，当一端配置了错误的IP地址，另一端也会自动把错误的对端主机路由加到本端直连路由表中，造成在网络中发布错误的路由信息。通过使能本功能，可以抑制对端的主机路由添加到本端的直连路由表，防止出现错误的路由信息。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**ppp peer hostroute-suppress**，使能抑制对端主机路由加入本端直连路由表功能。

步骤4 执行命令**commit**，提交配置。

----结束

检查配置结果

完成接口封装PPP协议后，可以查看PPP的配置及状态信息。

前提条件

已完成接口封装PPP协议的所有配置。

操作步骤

- 使用**display interface** [*interface-type* [*interface-number*]]命令，查看封装了PPP协议的接口当前运行状态和统计信息。
- 使用**display ppp information interface** *interface-type interface-number*命令，查看指定接口的PPP链路信息。

----结束

1.1.1.2.4 配置 CHAP 单向认证方式

CHAP验证协议为三次握手验证协议，单向验证过程分为验证方配置了用户名和验证方没有配置用户名两种情况。

应用环境

CHAP验证是在链路建立的开始就完成的，在链路建立完成后的任何时间都可以重复发送再进行验证。

CHAP单向认证是指一端作为验证方，另一端作为被验证方。验证方发送一个“challenge”报文给被验证方。被验证方经过一次哈希算法后，给验证方返回一个值。验证方把自己经过哈希算法生成的值和被验证方返回的值进行比较，若两者匹配，则通过验证；否则，连接被终止。

前置任务

在配置CHAP单向认证之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层为Up。
- 配置接口的链路层协议为PPP。
- 配置AAA模式将被验证方的用户名和密码加入本地用户列表。

验证方配置用户名时以 CHAP 方式认证对端

背景信息

说明

VS模式下，该配置过程仅在Admin VS支持。

CHAP单向认证中当验证方配置了用户名时，可以对验证方的用户名进行确认。

操作步骤

- 验证方的配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**aaa**，进入AAA视图。
  c. 执行命令**local-user** *user-name* **password** [**cipher** *password* | **irreversible-cipher** *irreversible-cipher-password*]，将对端用户名和密码加入本地用户列表。
  d. 执行命令**quit**，退出到系统视图。
  e. 执行命令**interface** *interface-type interface-number*，进入接口视图。

f. 执行命令**ppp authentication-mode chap** [**pap**]，配置本地以CHAP方式验证对端。

ppp authentication-mode chap [**pap**]命令用来在LCP协商时优先进行CHAP协商，若对方不支持CHAP，将会进行PAP协商。如果被验证方对这两种方式都不支持，协商将无法通过。并不表示在一次PPP协商过程同时协商两种验证方式。

g. 执行命令**ppp chap user** *user-name*，配置本地用户名。

h. 执行命令**shutdown**，关闭接口。

i. 执行命令**commit**，提交配置。

j. 执行命令**undo shutdown**，重启接口。

说明

如果在接口视图下更改用户名或密码，必须在相应接口视图下执行命令**shutdown**、**undo shutdown**才能使配置生效。

进行接口重启时，需要在执行命令**shutdown**后执行命令**commit**提交配置。否则配置将不生效。

k. 执行命令**commit**，提交配置。

- 被验证方的配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**aaa**，进入AAA视图。
  c. 执行命令**local-user** *user-name* **password** [**cipher** *password* | **irreversible-cipher** *irreversible-cipher-password*]，将对端用户名和密码加入本地用户列表。
  d. 执行命令**quit**，退出到系统视图。
  e. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  f. 执行命令**ppp chap user** *user-name*，配置本地用户名。
  g. 执行命令**shutdown**，关闭接口。
  h. 执行命令**commit**，提交配置。
  i. 执行命令**undo shutdown**，重启接口。

说明

如果在接口视图下更改用户名或密码，必须在相应接口视图下执行命令**shutdown**、**undo shutdown**才能使配置生效。

进行接口重启时，需要在执行命令**shutdown**后执行命令**commit**提交配置。否则配置将不生效。

  j. 执行命令**commit**，提交配置。

----结束

验证方没有配置用户名时以 CHAP 方式认证对端

验证方没有配置用户名时，使用CHAP方式认证对端。

操作步骤

- 验证方的配置
  a. 执行命令**system-view**，进入系统视图。

b. 执行命令**aaa**，进入AAA视图。

c. 执行命令**local-user** *user-name* **password** [**cipher** *password* | **irreversible-cipher** *irreversible-cipher-password*]，将对端用户名和密码加入本地用户列表。

验证时，在本地配置的AAA用户名中进行查找，如果能够匹配对端接口下配置的用户名和密码，则验证通过。

d. 执行命令**quit**，退出到系统视图。

e. 执行命令**interface** *interface-type interface-number*，进入接口视图。

f. 执行命令**ppp authentication-mode chap** [**pap**]，配置本地以CHAP方式验证对端。

ppp authentication-mode chap [**pap**]命令用来在LCP协商时优先使用CHAP方式验证对端，若对方不支持CHAP方式，将会采用PAP方式验证。如果被验证方对这两种方式都不支持，协商将无法通过。

g. 执行命令**shutdown**，关闭接口。

h. 执行命令**commit**，提交配置。

i. 执行命令**undo shutdown**，重启接口。

说明

如果在接口视图下更改用户名或密码，必须在相应接口视图下执行命令**shutdown**、**undo shutdown**才能使配置生效。

进行接口重启时，需要在执行命令**shutdown**后执行命令**commit**提交配置。否则配置将不生效。

j. 执行命令**commit**，提交配置。

- 被验证方的配置

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

c. 执行命令**ppp chap user** *user-name*，配置本地用户名。

d. 执行命令**ppp chap password** { **simple** *password2* | **cipher** *password1* | *password2* }，配置本地CHAP口令。

验证过程中验证方只把质询报文发送到被验证方。被验证方根据本地设置的口令和质询报文，通过加密算法计算得出一个数值，并将计算得出的数值和自己的主机名发回验证方。

e. 执行命令**shutdown**，关闭接口。

f. 执行命令**commit**，提交配置。

g. 执行命令**undo shutdown**，重启接口。

说明

如果在接口视图下更改用户名或密码，必须在相应接口视图下执行命令**shutdown**、**undo shutdown**才能使配置生效。

进行接口重启时，需要在执行命令**shutdown**后执行命令**commit**提交配置。否则配置将不生效。

h. 执行命令**commit**，提交配置。

----结束

检查配置结果

CHAP单向认证方式功能配置完成后，您可以查看接口的PPP配置和运行状态。

前提条件

已经完成CHAP单向认证方式的所有配置。

操作步骤

- 使用**display interface** [*interface-type* [*interface-number*]]命令看接口的PPP配置和运行状态。

----结束

1.1.1.2.5 配置 PAP 单向认证方式

配置PAP单向认证方式主要包括：配置验证方以PAP方式认证对端及配置被验证方以PAP方式被对端认证等功能。

应用环境

PAP认证方式使用简单口令。被验证方的用户名和密码可以通过AAA模式加入验证方的本地用户列表，也可以通过RADIUS服务器进行。

PAP的单向认证是指通信双方，只有一方作为验证方，而另一方作为被验证方。双向认证也就是双方都既作为验证方，同时也作为被验证方。

本节介绍通过AAA模式将被验证方的用户名和密码加入验证方的本地用户列表完成PAP单向认证的配置。

前置任务

在配置PAP认证方式之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为Up。
- 配置接口的链路层协议为PPP协议。
- 配置AAA模式将被验证方的用户名和密码加入验证方本地用户列表。

配置验证方以 PAP 方式认证对端

配置验证方的PAP认证方式。PAP验证协议为两次握手验证，验证过程仅在链路初始建立阶段进行。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**aaa**，进入AAA视图。

步骤3 执行命令**local-user** *user-name* **password** [**cipher** *password* | **irreversible-cipher** *irreversible-cipher-password*]，将被验证方的用户名和密码加入本地用户列表。

步骤4 执行命令**quit**，退出到系统视图。

步骤5 执行命令**interface** *interface-type interface-number*，进入验证方接口视图。

步骤6 执行命令**ppp authentication-mode pap**，配置本地以PAP方式验证对端。

步骤7 执行命令，重启接口。

1. 执行命令**shutdown**，关闭接口。
2. 执行命令**commit**，提交配置。
3. 执行命令**undo shutdown**，重启接口。

说明

配置完成后，需要执行命令**shutdown**、**undo shutdown**重启接口，配置才能生效。

进行接口重启时，需要在执行命令**shutdown**后执行命令**commit**提交配置。否则配置将不生效。

步骤8 执行命令**commit**，提交配置。

----结束

配置被验证方以 PAP 方式被对端认证

配置被验证方的PAP认证方式。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入被验证方接口视图。

步骤3 执行命令**ppp pap local-user** *user-name* **password** { **simple** *password2* | **cipher** *password1* | *password2* }，配置本地被对端以PAP方式验证时，本地发送PAP用户名和口令。

步骤4 执行命令，重启接口。

1. 执行命令**shutdown**，关闭接口。
2. 执行命令**commit**，提交配置。
3. 执行命令**undo shutdown**，重启接口。

说明

配置完成后，需要执行命令**shutdown**、**undo shutdown**重启接口，配置才能生效。

接口重启时，需要在执行命令**shutdown**后执行命令**commit**提交配置。否则配置将不生效。

步骤5 执行命令**commit**，提交配置。

----结束

检查配置结果

PAP单向认证方式配置完成后，您可以查看当前接口的链路状态和LCP的运行状态。

前提条件

已完成PAP单向认证方式的所有配置。

操作步骤

- 使用**display interface** [*interface-type* [*interface-number*]]命令查看当前接口的链路状态和LCP的运行状态。

----结束

1.1.1.2.6 PPP 配置举例

该部分从PPP的具体的应用场景对PAP认证、CHAP认证进行了详细的描述。

配置 PAP 验证示例

以PAP验证组网为例详细介绍了PAP验证的配置方法、实现原理。

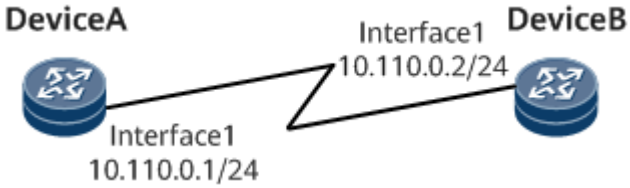
组网需求

如图1-8所示，DeviceA和DeviceB之间通过LMP接口连接，要求DeviceA用PAP方式验证DeviceB。

图 1-8 配置 PAP 验证组网图

说明

本例中Interface1代表Lmpif1/0/0。



配置注意事项

无

配置思路

采用如下的思路配置PAP：

1. 使用AAA认证方案，把DeviceB的用户名和密码加入DeviceA的本地用户列表。
2. 在DeviceA的LMP接口上配置以PAP方式验证DeviceB。
3. 在DeviceB的LMP接口上配置用户名和密码。

数据准备

为完成此配置例，需准备如下的数据：

- DeviceB的用户名和密码
- DeviceA接口的IP地址
- DeviceB接口的IP地址

操作步骤

步骤1 配置DeviceA

将DeviceB的用户名和密码加入DeviceA的本地用户列表。

```
<HUAWEI> system-view
[~HUAWEI] sysname DeviceA
[*HUAWEI] commit
[~DeviceA] aaa
[*DeviceA-aaa] local-user rtb password cipher YsHsjx_202206
[*DeviceA-aaa] local-user rtb service-type ppp
[*DeviceA-aaa] authentication-scheme default1
[*DeviceA-aaa-authen-default1] authentication-mode local
[*DeviceA-aaa-authen-default1] commit
[~DeviceA-aaa-authen-default1] quit
[~DeviceA-aaa] quit
```

配置Lmpif1/0/0的IP地址及封装链路层协议为PPP。

```
[~DeviceA] interface Lmpif 1/0/0
[~DeviceA-Lmpif1/0/0] ip address 10.110.0.1 255.255.255.0
[*DeviceA-Lmpif1/0/0] link-protocol ppp
```

配置DeviceA以PAP方式验证DeviceB。

```
[*DeviceA-Lmpif1/0/0] ppp authentication-mode pap
[*DeviceA-Lmpif1/0/0] undo shutdown
```

提交配置命令。

```
[*DeviceA-Lmpif1/0/0] commit
```

步骤2 配置DeviceB

配置Lmpif1/0/0的IP地址及封装链路层协议为PPP。

```
<HUAWEI> system-view
[~HUAWEI] sysname DeviceB
[*HUAWEI] commit
[~DeviceB] interface Lmpif1/0/0
[~DeviceB-Lmpif1/0/0] ip address 10.110.0.2 255.255.255.0
[*DeviceB-Lmpif1/0/0] link-protocol ppp
```

配置DeviceB向DeviceA发送用户名和密码。

```
[*DeviceB-Lmpif1/0/0] ppp pap local-user rtb password cipher YsHsjx_202206
[*DeviceB-Lmpif1/0/0] undo shutdown
```

提交配置命令。

```
[*DeviceB-Lmpif1/0/0] commit
```

步骤3 验证配置结果

配置完成之后，分别在DeviceA和DeviceB上执行**display interface**命令，可以看到双方的LCP状态均为LCP opened。下面以DeviceA的显示为例。

```
[~DeviceA] display interface Lmpif 1/0/0
Lmpif1/0/0 current state : UP (ifindex: 15)
Line protocol current state : UP
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.110.0.1/24
Link layer protocol is PPP
LCP opened, IPCP opened
Current BW: 100 Mbits
Statistics last cleared:never:
  Last 300 seconds input rate 0 bits/sec, 0 packets/sec
  Last 300 seconds output rate 0 bits/sec, 0 packets/sec
```



```
Input: 0 packets, 0 bytes
Input error: 0 shortpacket, 0 longpacket, 0 CRC, 0 lostpacket
Output: 0 packets, 0 bytes
Output error: 0 lostpackets
Output error: 0 overrunpackets, 0 underrunpackets
```

----结束

配置文件

- DeviceA的配置文件

```
#
sysname DeviceA
#
interface Lmpif1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.110.0.1 255.255.255.0
 ppp authentication-mode pap
#
aaa
 local-user rtb password cipher @%@%j]v~7%f[#S'W>j9zzM)3,*!u@%@%
 local-user rtb service-type ppp
 #
 authentication-scheme default1
  authentication-mode local
#
return
```

- DeviceB的配置文件

```
#
sysname DeviceB
#
interface Lmpif1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.110.0.2 255.255.255.0
 ppp pap local-user rtb password cipher @%@%j]v~7%f[#S'W>j9zzM)3,*!u@%@%
#
return
```

配置 CHAP 单向验证示例

以CHAP单向验证组网为例，详细介绍了CHAP单向验证的配置方法及其实现原理。

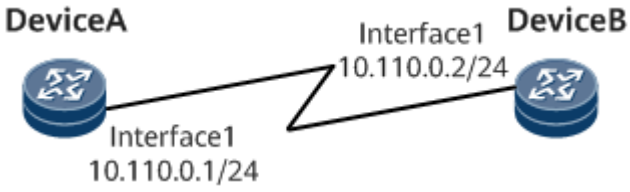
组网需求

在图1-9中，DeviceA和DeviceB之间通过LMP接口连接，要求DeviceA用CHAP方式验证DeviceB，并且验证方DeviceA需要配置用户名。

图 1-9 配置 CHAP 单向验证组网图

说明

本例中Interface1代表Lmpif1/0/0。



配置注意事项

无

配置思路

采用如下的思路配置CHAP单向验证：

1. 使用AAA认证方案，把DeviceB的用户名和密码加入DeviceA的本地用户列表。
2. 在DeviceA的LMP接口上配置以CHAP方式验证DeviceB。
3. 在DeviceA的LMP接口下创建用户名。
4. 在DeviceB的LMP接口下创建用户名和密码。

数据准备

为完成此配置例，需准备如下的数据：

- DeviceA的用户名
- DeviceB的用户名和密码
- DeviceA接口的IP地址
- DeviceB接口的IP地址

操作步骤

步骤1 配置DeviceA

将DeviceB的用户名和密码加入DeviceA的本地用户列表。

```
<HUAWEI> system-view
[~HUAWEI] sysname DeviceA
[*HUAWEI] commit
[~DeviceA] aaa
[~DeviceA-aaa] local-user rtb password cipher YsHsjx_202206
[*DeviceA-aaa] local-user rtb service-type ppp
[*DeviceA-aaa] authentication-scheme default1
[*DeviceA-aaa-authen-default1] authentication-mode local
[*DeviceA-aaa-authen-default1] commit
[~DeviceA-aaa-authen-default1] quit
[~DeviceA-aaa] quit
```

配置Lmpif1/0/0的IP地址并封装链路层协议为PPP。

```
[~DeviceA] interface Lmpif 1/0/0
[~DeviceA-Lmpif1/0/0] ip address 10.110.0.1 255.255.255.0
[*DeviceA-Lmpif1/0/0] link-protocol ppp
```

配置DeviceA以CHAP方式验证DeviceB。

```
[*DeviceA-Lmpif1/0/0] ppp authentication-mode chap
```

配置Device A的用户名。

```
[*DeviceA-Lmpif1/0/0] ppp chap user rta
```

启动接口。

```
[*DeviceA-Lmpif1/0/0] undo shutdown
```

提交配置命令。

```
[*DeviceA-Lmpif1/0/0] commit
```


步骤2 配置DeviceB

配置Lmpif1/0/0的IP地址及封装链路层协议为PPP。

```
<HUAWEI> system-view
[~HUAWEI] sysname DeviceB
[*HUAWEI] commit
[~DeviceB] interface Lmpif 1/0/0
[~DeviceB-Lmpif1/0/0] ip address 10.110.0.2 255.255.255.0
[*DeviceB-Lmpif1/0/0] link-protocol ppp
```

配置DeviceB的用户名和密码。

```
[*DeviceB-Lmpif1/0/0] ppp chap user rtb
[*DeviceB-Lmpif1/0/0] ppp chap password cipher YsHsjx_202206
[*DeviceB-Lmpif1/0/0] undo shutdown
```

提交配置命令。

```
[*DeviceB-Lmpif1/0/0] commit
```

步骤3 验证配置结果

配置完成之后，在DeviceA和DeviceB上执行**display interface**命令，可以看到双方的LCP状态均为LCP opened。下面以DeviceA的显示为例。

```
[~DeviceA] display interface Lmpif 1/0/0
Lmpif1/0/0 current state : UP (ifindex: 15)
Line protocol current state : UP
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.110.0.1/24
Link layer protocol is PPP
LCP opened, IPCP opened
Current BW: 100 Mbits
Statistics last cleared:never
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
      Input:  0 packets, 0 bytes
    Input error: 0 shortpacket, 0 longpacket, 0 CRC, 0 lostpacket
    Output: 0 packets, 0 bytes
    Output error: 0 lostpackets
    Output error: 0 overrunpackets, 0 underrunpackets
```

----结束

配置文件

- DeviceA的配置文件

```
#
sysname DeviceA
#
interface Lmpif1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.110.0.1 255.255.255.0
 ppp authentication-mode chap
 ppp chap user rta
#
aaa
 local-user rtb password cipher @%@%j]v~7%f[#S'W>j9zzM)3,*!u@%@%
 local-user rtb service-type ppp
 #
 authentication-scheme default1
  authentication-mode local
#
return
```


- DeviceB的配置文件

```
#
sysname DeviceB
#
interface Lmpif1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.110.0.2 255.255.255.0
 ppp chap user rtb
 ppp chap password cipher @%@%j]v~7%f[#S'W>j9zzM)3,*!u@%@%
#
return
```

配置 CHAP 双向验证示例

以CHAP双向验证组网为例，详细描述了CHAP双向验证配置方法及其实现原理。

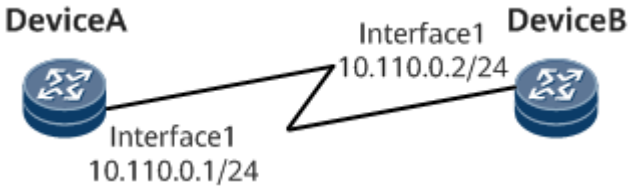
组网需求

在图1-10中，要求DeviceA和DeviceB用CHAP方式进行双向验证。

图 1-10 配置 CHAP 双向验证组网图

说明

本例中Interface1代表Lmpif1/0/0。



配置注意事项

无

配置思路

采用如下的思路配置CHAP双向验证：

1. 使用AAA认证方案，配置DeviceA和DeviceB的本地用户列表。
2. 在DeviceA和DeviceB的LMP接口下创建用户名和密码。
3. 在DeviceA和DeviceB的接口下使能CHAP验证方式。

数据准备

为完成此配置例，需准备如下的数据：

- DeviceA和DeviceB的用户名
- DeviceA和DeviceB的验证密码
- DeviceA接口的IP地址
- DeviceB接口的IP地址

说明

配置时，DeviceA和DeviceB的密码必须相同，否则，验证失败。

操作步骤

步骤1 配置DeviceA

将DeviceB的用户名和密码加入DeviceA的本地用户列表。

```
<HUAWEI> system-view
[~HUAWEI] sysname DeviceA
[*HUAWEI] commit
[~DeviceA] aaa
[~DeviceA-aaa] local-user rtb password cipher YsHsjx_202206
[*DeviceA-aaa] local-user rtb service-type ppp
[*DeviceA-aaa] authentication-scheme default1
[*DeviceA-aaa-authen-default1] authentication-mode local
[*DeviceA-aaa-authen-default1] commit
[~DeviceA-aaa-authen-default1] quit
[~DeviceA-aaa] quit
```

配置Lmpif1/0/0的IP地址及封装链路层协议为PPP。

```
[~DeviceA] interface Lmpif 1/0/0
[*DeviceA-Lmpif1/0/0] ip address 10.110.0.1 255.255.255.0
[*DeviceA-Lmpif1/0/0] link-protocol ppp
```

配置DeviceA的用户名和密码。

```
[*DeviceA-Lmpif1/0/0] ppp chap user rta
[*DeviceA-Lmpif1/0/0] ppp chap password cipher YsHsjx_202206
```

配置DeviceA采用CHAP验证DeviceB。

```
[*DeviceA-Lmpif1/0/0] ppp authentication-mode chap
[*DeviceA-Lmpif1/0/0] undo shutdown
```

提交配置命令。

```
[*DeviceA-Lmpif1/0/0] commit
```

步骤2 配置DeviceB

将DeviceA的用户名和密码加入DeviceB的本地用户列表。

```
<HUAWEI> system-view
[~HUAWEI] sysname DeviceB
[*HUAWEI] commit
[*DeviceB] aaa
[~DeviceB-aaa] local-user rta password cipher YsHsjx_202206
[*DeviceB-aaa] local-user rta service-type ppp
[*DeviceB-aaa] authentication-scheme default1
[*DeviceB-aaa-authen-default1] authentication-mode local
[*DeviceB-aaa-authen-default1] commit
[~DeviceB-aaa-authen-default1] quit
[*DeviceB-aaa] quit
```

配置Lmpif1/0/0的IP地址及封装链路层协议为PPP。

```
[~DeviceB] interface Lmpif 1/0/0
[~DeviceB-Lmpif1/0/0] ip address 10.110.0.2 255.255.255.0
[*DeviceB-Lmpif1/0/0] link-protocol ppp
```

配置DeviceB的用户名和密码。

```
[*DeviceB-Lmpif1/0/0] ppp chap user rtb
[*DeviceB-Lmpif1/0/0] ppp chap password cipher YsHsjx_202206
```


配置DeviceB采用CHAP验证DeviceA。

```
[*DeviceB-Lmpif1/0/0] ppp authentication-mode chap
[*DeviceB-Lmpif1/0/0] undo shutdown
```

提交配置命令。

```
[*DeviceB-Lmpif1/0/0] commit
```

步骤3 验证配置结果

配置完成之后，在DeviceA和DeviceB上执行**display interface**命令，可以看到双方均LCP opened。下面以DeviceA的显示为例。

```
[~DeviceA] display interface Lmpif 1/0/0
Lmpif1/0/0 current state : UP (ifindex: 15)
Line protocol current state : UP
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.110.0.1/24
Link layer protocol is PPP
LCP opened, IPCP opened
Current BW: 100 Mbits
Statistics last cleared:never
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Input:  0 packets, 0 bytes
    Input error: 0 shortpacket, 0 longpacket, 0 CRC, 0 lostpacket
    Output: 0 packets, 0 bytes
    Output error: 0 lostpackets
    Output error: 0 overrunpackets, 0 underrunpackets
```

----结束

配置文件

- DeviceA的配置文件

```
#
sysname DeviceA
#
interface Lmpif1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.110.0.1 255.255.255.0
 ppp authentication-mode chap
 ppp chap user rta
 ppp chap password cipher @%@%EDF~DAdfFD934J3<DAF#*<!@%@%
#
aaa
 local-user rtb password cipher @%@%j]v~7%f[#S'W>j9zzM)3,*!u@%@%
 local-user rtb service-type ppp
 #
 authentication-scheme default1
  authentication-mode local
#
return
```

- DeviceB的配置文件

```
#
sysname DeviceB
#
interface Lmpif1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.110.0.2 255.255.255.0
 ppp authentication-mode chap
 ppp chap user rtb
 ppp chap password cipher @%@%j]v~7%f[#S'W>j9zzM)3,*!u@%@%
```



```
#
aaa
 local-user rta password cipher @%@%EDF~DAdfFD934J3<DAF#*<!@%@%
 local-user rta service-type ppp
 #
 authentication-scheme default1
  authentication-mode local
#
return
```

