HCRSE102-WAN 技术

WAN 技术知识点：

接口类型，PPP 3 大组件，报文结构，PPP 建立链路的 5 个阶段，LCP 3 类报文（配置报文），LCP 协商参数（魔术字），PAP 认证， CHAP 认证（16 字节摘要），MP 作用，IP-Trunk ，PPPoE 协议

10GE 以太网 标准：IEEE802.3ae
100GE 以太网 标准：IEEE 802.3ba

接口的核心要素：带宽、距离、成本、功耗、密度、兼容、演进

POS:Packet Over SONET/SDH 在 SONET/SDH 上承载 IP 包或其他数据包的传输技术

SONET（Synchronous Optical Network）同步光网络，OC-n/STM-n 序列。
SDH（Synchronous Digital Hierarchy）同步数字系列，是 CCITT 定义的，它使用了 SONET 速率的一个子集，STM-n 序列。

==========

PPP 协议

PPP 协议中提供了一整套方案来解决链路建立、维护、拆除、上层协议协商、认证等问题。

PPP 共定义了三个协议组件，分别是数据封装方式，链路控制协议（Link Control Protocol，LCP）和网络层控制协议（Network Control Protocol，NCP）。

数据封装方式：HDLC PPP

链路控制协议 LCP（Link Control Protocol）定义建立、协商和测试数据链路层连接的方法。

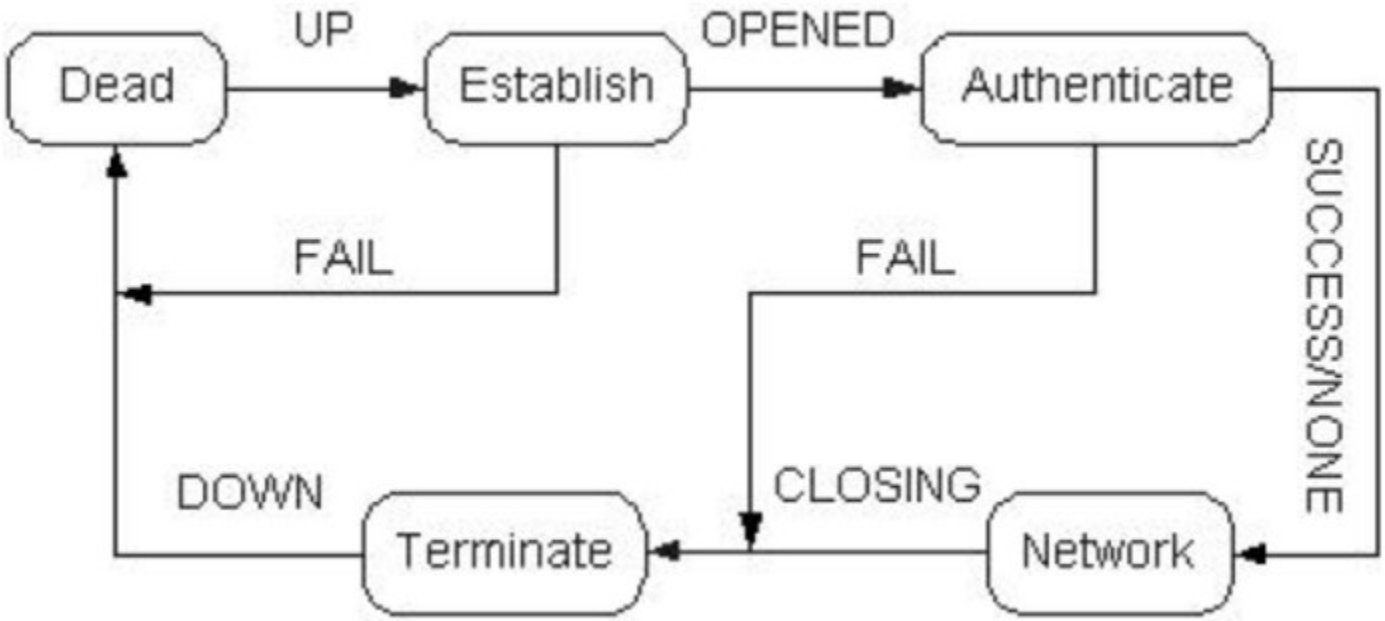
网络控制协议 NCP（Network Control Protocol）；包含一组协议，用于对不同的网络层协议进行连接建立和参数协商。

认证协议，最常用的包括口令验证协议 PAP 和 CHAP，主要用于网络安全方面的验证，验证对端设备的合法性。

PPP 建链 5 个过程

Dead：这是 PPP 工作开始和结束的阶段。
Establish：PPP 在此阶段使用 LCP 协商链路层参数。
Authenticate：PPP 在此阶段认证对端，
Network：PPP 在此阶段使用 NCP 进行网络层参数协商
Terminate：PPP 在此阶段使用 LCP 关闭 PPP 连接。

注意：此处列出的是 PPP 的工作阶段，并非 PPP 的协议状态。由于 PPP 是由一组协议组成的，因此 PPP 本身没有协议状态。只有特定的的协议如 LCP 和 NCP 等才有协议状态和状态转换。



1 Dead 阶段（链路不可用阶段）

Dead 阶段也称为物理层不可用阶段。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。

2 Establish 阶段（链路建立阶段）

接口 UP 之后，就会进入 establish 状态，在 establish 状态，会进行 LCP 协商，主要协商的内容有以下几点：

a.工作方式：SP/MP； 协商使用单链路工作方式还是多链路工作方式

b.接口最大接收单元：MRU；（两端不一致，则向小的协商）

c.魔术字： 魔术字主要用于 PPP 链路上检查环路，主要用于检查物理链路的环路，比如光纤打环测试的时候，就会出现发送的 LCP 报文中的魔术字和接收到的 LCP 报文的魔术字相同的情况；如果相同则会重新选取魔术字；

d.认证方式

备注： MRU 和 MTU 的区别：
MTU：最大传输单元　　MRU：最大接收单元　　，接口的 MRU=MTU

3 Authenticate 阶段（验证阶段）
LCP 协商通过则进入 authentication 阶段，可选阶段，，进行 PAP 或者 CHAP 的认证；

4 Network 阶段（网络层协商阶段）
认证通过则进入 network 阶段；协商成功则 PPP 连接建立成功，开始传输网络层数据包。

5 Terminate 阶段（网络终止阶段）
认证不通过则进入 terminate 阶段，也就是拆链阶段；

LCP 协议有 3 大类报文：
链路配置包，用于建立和配置链路：
Configure-Request（匹配请求），
Configure-Ack（匹配确认），
Configure-Nak（匹配否认），
Configure-Reject（匹配拒绝）。

链路结束包，用于结束一个链路：
Terminate-Request（终止请求）
Terminate-Ack（终止确认）。

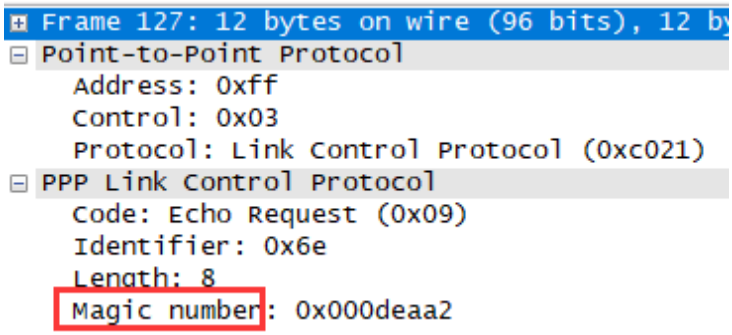
链路维修包，用于管理和调试一个链路：
Code-Reject（代码拒绝），
Protocol-Reject（协议拒绝），

Echo-Request（回波请求），
Echo-Reply（回波应答），
Discard-Request（抛弃请求）。

报文类型	功能描述
Configure-Request	包含发送者试图使用的、没有使用默认值的参数列表。
Configure-Ack	表示完全接受对端发送的Configure-Request的参数取值。
Configure-Nak	表示对端发送的Configure-Request中的参数取值在本地不合法。
Configure-Reject	表示对端发送的Configure-Request中的参数本地不能识别。

LCP 协商的参数
1.最大接收单元 MRU
2.认证协议 PAP/ CHAP
3.魔术字

LCP 使用魔术字（Magic-Number）检测链路环路和其它异常情况。魔术字为随机产生的一个数字，随机机制需要保证两端产生相同魔术字的可能性几乎为 0。



PAP: Password Authentication Protocol, 口令认证协议
CHAP : Challenge Handshake Authentication Protocol, 挑战握手认证协议

PPP 两种验证方式的区别：
PAP 为两次握手验证，口令为明文。
CHAP 为三次握手验证，口令为密文。
PPP 验证对端路由器可以只采用 CHAP 或 PAP 验证方法，也可以采用两种验证方法，按顺序在前一种验证失败之后，采用后一种验证。一般来说，CHAP 验证更为安全可靠。
PAP 由被认证方先发送报文，CHAP 由认证方先发送报文

PAP 认证过程

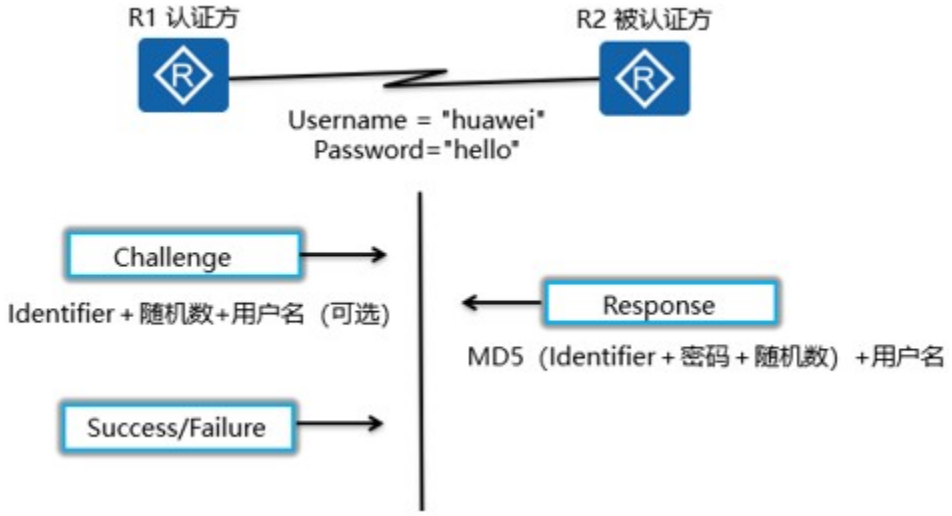
被验证方把本地用户名和口令以明文的形式发送到验证方，验证方根据本地用户表查看是否有被验证方的用户名
若没有，则认证失败，
若有，则查看口令是否正确，若口令正确，则认证通过；若口令不正确，则认证失败。

CHAP 认证过程

认证端接口配置用户名的情况下，被认证端接口用户名一定要配，密码可配可不配；
认证端的接口下没有配置用户名的情况下，被认证端的接口下用户名一定要配，此时密码也必须配置。否则认证过程失败。

认证方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些随机产生的报文（Challenge），并同时将本端的用户名附带上一起发送给被验证方（挑战报文里面包含一个随机数和 ID）



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 ppp chap password 命令，如果配置了该命令，则被验证方用报文 ID、随机数，命令中配置的用户密码和 MD5 算法对该随机报
文进行加密，将生成的密文和接口的用户名发回验证方（Response）。
如果接口上未配置 ppp chap password 命令，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，用报文 ID、随机数，此用户的密钥（密码）和 MD5 算法对该随机报文进行加密，将生成的密文和被验证方自己的用户名发回验证方（Response）

c)验证方用自己保存的被验证方密码和 MD5 算法对原随机报文加密，比较二者的密文，若比较结果一致，认证通过，若比较结果不一致，认证失败

认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些随机产生的报文（Challenge）

b)被验证方接到验证方的验证请求后，利用报文 ID、随机数，ppp chap password 命令配置的 CHAP 密码和 MD5 算法对该随机报文进行加密，将生成的密文和接口的用户名发回验证方（Response）

c)验证方用自己保存的被验证方密码和 MD5 算法对原随机报文加密，比较二者的密文，若比较结果一致，认证通过，若比较结果不一致，认证失败

PAP 与 CHAP 的验证过程分别是由哪方发起的？PAP 和 CHAP 的最大不同点是什么？
PAP 是首先由被验证方将自己的用户名及密码送给验证方；而 CHAP 验证是首先由验证方发起；验证过程的主要区别为：PAP 为明文传送密码，而在 CHAP 验证过程中密码是不在线传送的，属于密文传送。

PAP 的详细验证过程是什么样的？
被认证方将配置的用户名和密码信息使用 Authenticate-Request 报文以明文方式发送给认证方。
认证方收到被认证方发送的用户名和密码信息之后，根据本地配置的用户名和密码数据库检查用户名和密码信息是否匹配，如果匹配，则返回 Authenticate-Ack 报文，表示认证成功。否则，返回 Authenticate-Nak 报文，表示认证失败。

PAP 为两次握手协议，详细验证过程如下：
当两端链路可相互传输数据时，被验证方发送本端的用户名及口令到验证方，验证方根据本端的用户表（或 Radius 服务器）查看是否有此用户，口令是否正确。如正确则会给对端发

送 ACK 报文，通告对端已被允许进入下一阶段协商；否则发送 NAK 报文，通告对端验证失败。一次认证失败并不会直接将链路关闭，只有当验证不过次数达到一定值时，才会关闭链路，来防止因误传、网络干扰等造成不必要的 LCP 重新协商过程。

CHAP 的详细验证过程是什么样的？
LCP 协商完成后，认证方发送一个 Challenge 报文给被认证方，报文中含有 Identifier 信息和一个随机产生的 Challenge 字符串，此 Identifier 即为后续报文所使用的 Identifier。
被认证方收到此 Challenge 报文之后，进行一次加密运算，运算公式为 MD5{ Identifier + 密码 + Challenge }，意思是将 Identifier、密码和 Challenge 三部分连成一个字符串，然后对此字符串做 MD5 运算，得到一个 16 字节长的摘要信息，然后将此摘要信息和端口上配置的 CHAP 用户名一起封装在 Response 报文中发回认证方。

MP（MultiLink PPP）协议

增加带宽，将多个 PPP 链路捆绑使用。
MultiLink PPP 允许将报文分片，分片将从多个点对点链路上送到同一个目的地。

IP-Trunk 协议

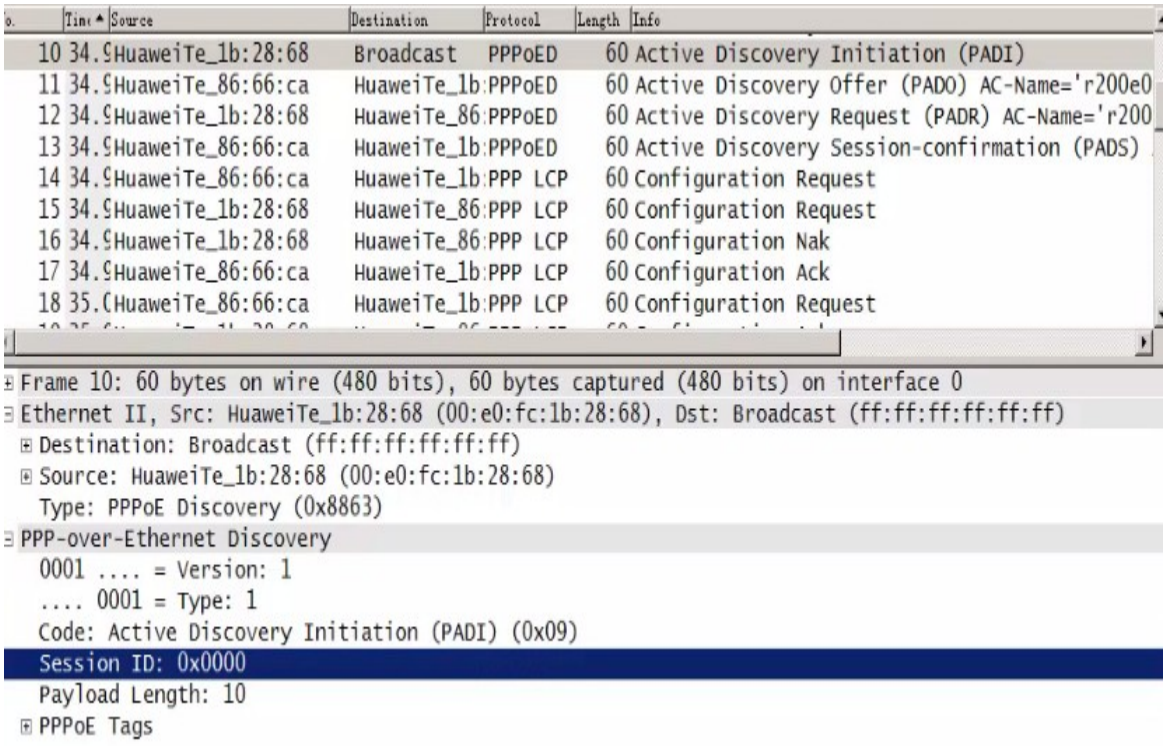
IP-Trunk 一般由 POS 接口构成,成员接口只能使用 HDLC 封装形式。

PPPoE 协议

PPPoE（PPP over Ethernet）协议是一种把 PPP 帧封装到以太网帧中的链路层协议。PPPoE 可以使以太网网络中的多台主机连接到远端的宽带接入服务器，具有适用范围广、安全性

高、计费方便的特点。

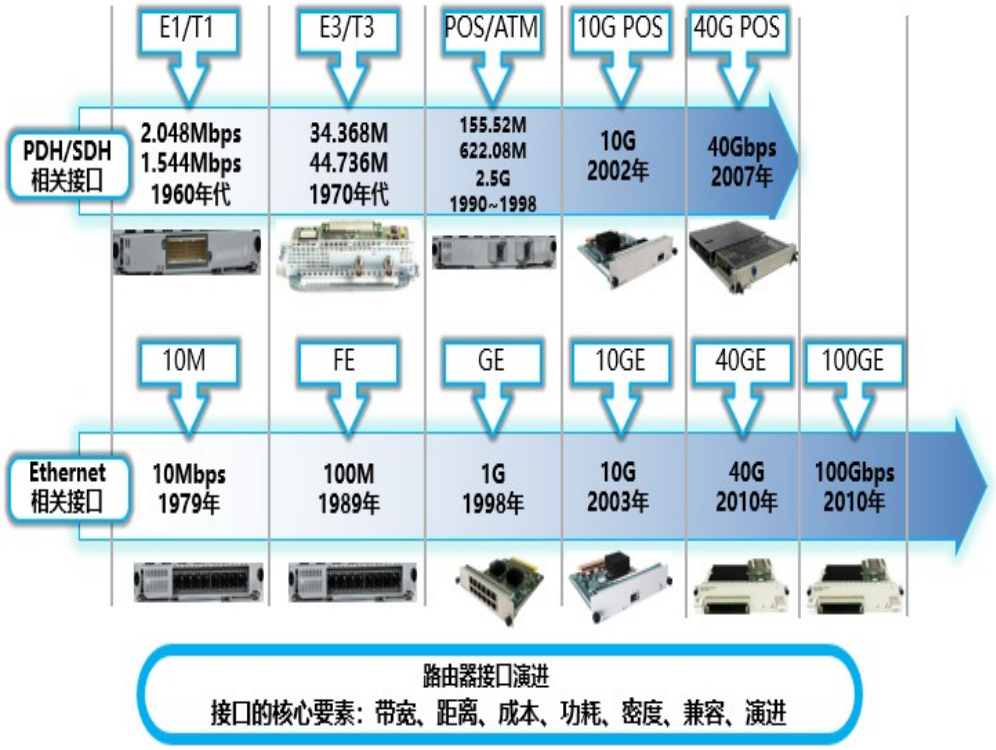
PPPoE 可分为三个阶段 ：Discovery ，Session，Terminate



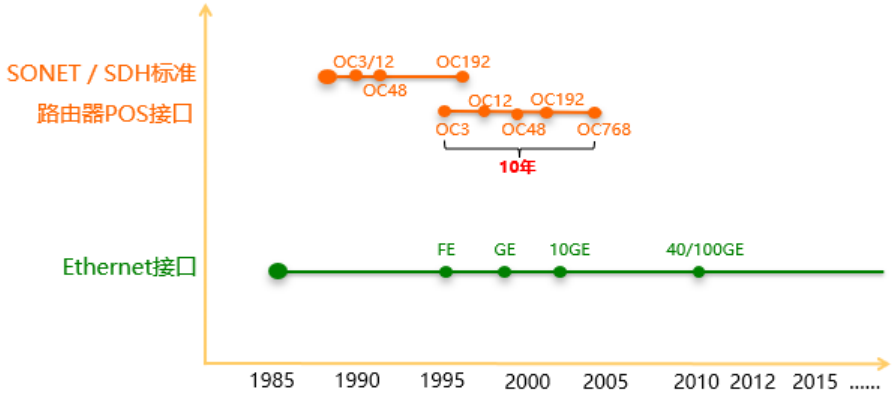
前言

- 本文主要介绍WAN网络中的常见的接口、PPP/MP、POS/IP-Trunk以及PPPoE的原理与配置。

路由器物理接口带宽演进



路由器POS/Ethernet接口演进趋势



- POS接口现网成熟应用
- 以太接口持续发展

以太网接口

- 以太网由Xerox公司PARC研究中心于1973年5月22日首次提出。
- 以太网类型：
  - 10M以太网（标准以太网）
  - 100M以太网（快速以太网）
  - 1000M以太网（千兆以太网）
  - 10G以太网（万兆以太网）
  - 100G以太网（100G以太网）
  - ……

10M/100M以太网

- 10M/100M以太网物理层按照速率等级和传输介质来划分。常见的类型如下：
  - 10BASE-T：采用两对非屏蔽的3类、4类、5类双绞线；
  - 100BASE-TX：采用两对屏蔽双绞线或高质量的5类非屏蔽双绞线；
  - 100BASE-FX：采用两根光纤，一根用于发送，一根用于接收。

- T：表示双绞线；
- TX：表示2对高质量的双绞线；
- FX：表示2根光纤。

1000M以太网

- 1000M以太网标准如下：
  - 1000BASE-T: IEEE802.3ab，5类非屏蔽双绞线
  - 1000BASE-X: IEEE802.3z，多模光纤、单模光纤和150欧平衡屏蔽式双绞线。
  - 1000BASE-CX: 由于最大长度25米，现在应用已经很少。
  - 1000BASE-SX: 短波850nm，激光范围（770～860nm）只用于多模光纤。
  - 1000BASE-LX: 长波1310nm，激光范围（1270～1355nm）主要用于单模光纤，但也可以用于多模光纤。

10GE以太网

- 标准：IEEE802.3ae
- 10Gbs/s 以太网有两类：
  - 串行的10GBase-S/L/E-R/W：
    - 10GBase-S：短距；850nm；多模。
    - 10GBase-L：长距；1310nm；单模。
    - 10GBase-E：超长距；1550nm；单模。
    - W = WAN PHY广域网物理层, 9.95328Gb/s 码率, 采用SONET STS-192c及SDH VC-4-64C封装，可以使用DWDM或SDH/SONET光 / 传输网作传送，使10G以太网无缝接入SDH。
    - R = LAN PHY局域网物理层, 10.3125Gb/s码率。
  - 4路并行WDM (波分复用)的10GBase-LX4：
    - 10GBase-LX4：1310nm；多模。
    - 10GBase-LX4：1310nm；单模。

100GE以太网

- 100G以太网（100GE）标准从开始讨论制订到正式获批发布，经历了长达4年之久：2010年6月，IEEE正式对外宣布IEEE 802.3ba标准。
- 在当前正式发布的802.3ba标准中，对于100Gbps MAC速率，提供了如下物理层规范：
  - 40km单模光纤（SMF）：对应的PHY为100GBASE-ER4，由4个WDM（1310nm, 800GHz波长间隔）通道组成。
  - 10km单模光纤: 对应的PHY为100GBASE-LR4，由4个WDM（1310nm,800GHz波长间隔）通道组成。
  - 100m OM3多模光纤: 对应的PHY为100GBASE-SR10，由10条独立的多模光纤通道（850nm）组成。
  - 7m铜线: 对应的PHY为100GBASE-CR10，由10条独立的铜缆通道组成。

POS接口

- Packet Over SONET/SDH：在SONET/SDH上承载IP包或其他数据包的传输技术。
- POS将长度可变的数据包直接映射进SONET同步载荷中，使用SONET物理层传输标准， 提供了一种高速、可靠、点到点的数据连接。采用光纤进行传输。
- POS常用接口速率：
  - OC-3/STM-1: 155.52Mbps
  - OC-12/STM-4: 622.08Mbps
  - OC48/STM-16: 2488.32Mbps
  - OC192/STM-64: 9953.28Mbps
  - OC768/STM-256:39813.12Mbps
- SONET（Synchronous Optical Network）同步光网络，OC-n/STM-n序列。
- SDH（Synchronous Digital Hierarchy）同步数字系列，是CCITT定义的，它使用了SONET速率的一个子集，STM-n序列。

- OC-n: Optical Carrier level n（光载体等级）是光纤传输的一种单位，最小的单位为 OC-1，其传输数据量约为 51.84 Mbps。
- STM: Synchronous Transport Module，同步传输模块。

Ethernet接口和POS接口的比较

- Ethernet接口和POS接口在速率上，都可以达到10G、40G。在100G Ethernet标准发布后，速率上Ethernet接口更胜一筹。
- POS端口里采用PPP或HDLC的二层封装来承载IP，二层报头开销最长9个字节，也可能是7个字节。而10G LAN和WAN都是以太封装，二层报头开销是18个字节。由此看出，POS接口对IP报文的传输效率更高。
- 成本上，Ethernet接口/Ethernet单板价格更低。例如10GE Ethernet，近似10G POS价格的一半。

接口LAN/WAN模式

- 10G XFP多模光收发模块可以工作在LAN或WAN两种模式，需要根据实际的应用来选择合适的模式。
- 10G LAN/WAN的区别在于封装不同。10G LAN是纯Ethernet封装，10G WAN接口链路层采用Ethernet封装，但是在物理层把封装好的数据直接映射到SDH的序列中。
- 无论是LAN或是WAN模式，都可以用来作为WAN口实现广域网长距离传输。在广域网的两端，两台路由设备接口模式必须相同。
- 在路由器之间存在传输设备的情况下，需要注意与传输设备的配合。一般来说，当传输设备是10G POS时，路由器可以用10G POS、10GE WAN来配合；当传输设备是10G以太时，路由器只能用10GE LAN来配合。需要注意的是，对于当前较新的传输设备而言，无论路由器侧是10GE LAN/WAN还是10G POS都可以支持，只需要更换单板模块和软件配置即可。

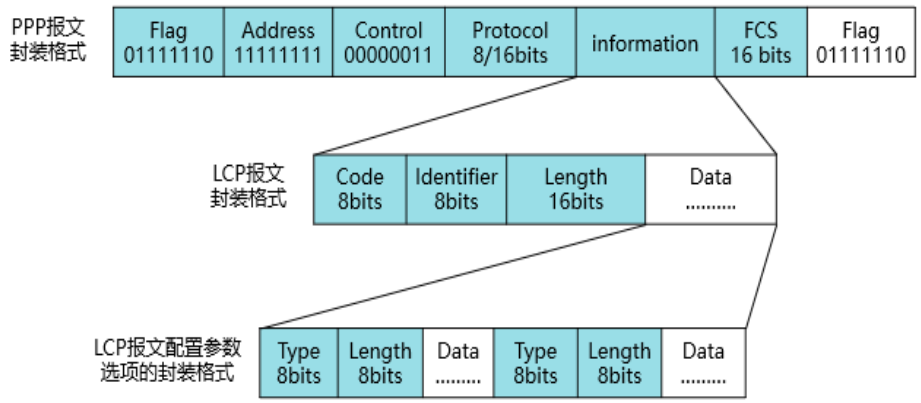
PPP基本概念 - 三大组件

- PPP协议在TCP/IP协议栈中位于数据链路层，是目前应用最广泛的点到点链路层协议。
- PPP的三个组件：
  - 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）：定义建立、协商和测试数据链路层连接的方法。
  - 网络层控制协议（NCP）：包含一组协议，用于对不同的网络层协议进行连接建立和参数协商。

- PPP 共定义了三个协议组件，分别是数据封装方式，链路控制协议（Link Control Protocol，LCP）和网络层控制协议（Network Control Protocol，NCP）。
- 数据封装方式定义了如何封装多种类型的上层协议数据包。
- 为了能适应多种多样的链路类型，PPP 定义了链路控制协议 LCP。LCP 可以自动检测链路环境，如是否存在环路；协商链路参数，如最大数据包长度，使用何种认证协议等等。与其他数据链路层协议相比，PPP 协议的一个重要特点是可以提供认证功能，链路两端可以协商使用何种认证协议并实施认证过程，只有认证成功才会建立连接。这个特点使 PPP 协议适合运营商用来接入分散的用户。
- PPP 定义了一组网络层控制协议 NCP，每一个协议对应一种网络层协议，用于协商网络层地址等参数，例如 IPCP 用于协商控制 IP，IPXCP 用于协商控制 IPX 协议等。

PPP基本概念 - 报文结构

- PPP报文结构

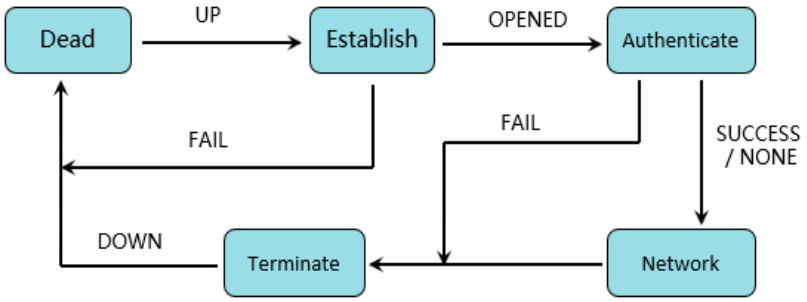


- PPP 报文封转格式
- Flag 域
- Flag 域标识一个物理帧的起始和结束，该字节为 0x7E。
- Address 域
- Address 域可以唯一标识对端。PPP 协议是被运用在点对点的链路上，因此，使用 PPP 协议互连的两个通信设备无须知道对方的数据链路层地址。按照协议的规定将该字节填充为全 1 的广播地址，对于 PPP 协议来说，该字段无实际意义。
- Control 域
- 该字段默认值为 0x03，表明为无序号帧，PPP 默认没有采用序列号和确认来实现可靠传输。
- Address 和 Control 域一起标识此报文为 PPP 报文，即 PPP 报文头为 FF03。
- Protocol 域
- 协议域可用来区分 PPP 数据帧中信息域所承载的数据报类型。
- LCP 报文封装格式
- Code 域

- 代码域的长度为一个字节，主要是用来标识 LCP 数据报文的类型。
- Identifier 域
- 标识域为 1 个字节，用来匹配请求和响应，当标识域值为非法时，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
- 长度域的值就是该 LCP 报文的总字节数据。它是代码域、标志域、长度域和数据域四个域长度的总和。
- 长度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
- 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 为协商的选项具体内容。

PPP基本概念 - 建链过程

- PPP建链过程



- 建链过程
- Dead：这是 PPP 工作开始和结束的阶段。当物理层变为可用状态（UP）之后，PPP 进入 Establish 阶段。
- Establish：PPP 在此阶段使用 LCP 协商链路层参数。如果链路层参数协商不成功（FAIL），则 PPP 连接建立不成功，PPP 退回到 Dead 阶段。如果链路层参数协商成功（OPENED），则 PPP 进入 Authenticate 阶段。
- Authenticate：PPP 在此阶段认证对端，如果认证失败（FAIL），则 PPP 进入 Terminate 阶段；如果认证成功（SUCCESS）或者没配置认证（NONE），则 PPP 进入 Network 阶段。
- Network：PPP 在此阶段使用 NCP 进行网络层参数协商，协商成功则 PPP 连接建立成功，开始传输网络层数据包。当上层协议认为应当关闭此连接（例如按需电路）或者管理员手工关闭 PPP 连接（CLOSING），则 PPP 进入 Terminate 阶段。
- Terminate：PPP 在此阶段使用 LCP 关闭 PPP 连接。PPP 连接关闭（Down）后，PPP 进入 Dead 阶段。

- 注意：此处列出的是 PPP 的工作阶段，并非 PPP 的协议状态。由于 PPP 是由一组协议组成的，因此 PPP 本身没有协议状态。只有特定的的协议如 LCP 和 NCP 等才有协议状态和状态转换（协议状态机）。

LCP协议 - 报文类型

报文类型	功能描述
Configure-Request	包含发送者试图使用的、没有使用默认值的参数列表。
Configure-Ack	表示完全接受对端发送的Configure-Request的参数取值。
Configure-Nak	表示对端发送的Configure-Request中的参数取值在本地不合法。
Configure-Reject	表示对端发送的Configure-Request中的参数本地不能识别。

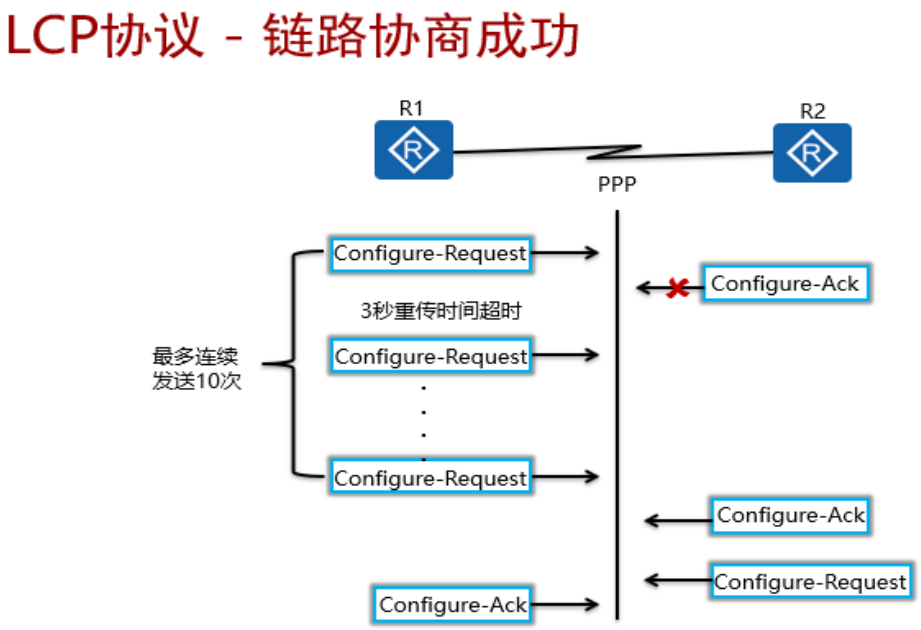
- LCP 协议有 3 大类报文：
- 链路配置包，用于建立和配置链路：Configure-Request（匹配请求），Configure-Ack（匹配确认），Configure-Nak（匹配否认），和 Configure-Reject（匹配拒绝）。
- 链路结束包，用于结束一个链路：Terminate-Request（终止请求）和 Terminate-Ack（终止确认）。
- 链路维修包，用于管理和调试一个链路：Code-Reject（代码拒绝），Protocol-Reject（协议拒绝），Echo-Request（回波请求），Echo-Reply（回波应答），和 Discard-Request（抛弃请求）。

LCP协议 - 用于协商的参数

参数名称	功能描述	协商规则	默认值
最大接收单元 MRU	PPP数据帧中Information字段的总长度。	使用两端设置的较小的值。	1500
认证协议	认证对端使用的认证协议。	被认证方必须支持认证方使用的认证协议并正确配置，否则协商不成功。	不认证
魔术字 Magic-Number	魔术字为一个随机产生的数字，用于检测链路环路，如果收到的LCP报文中的魔术字和本地产生的魔术字相同，则认为链路有环路。	一端支持而另一端不支持，表示链路无环路，认为协商成功；两端都支持则使用检测机制检测环路。	启用

- 用于协商的参数
- 在 VRP 平台上，MRU 参数使用接口上配置的最大传输单元（MTU）值来表示的。
- 常用的 PPP 认证协议有 PAP 和 CHAP（后续章节介绍），一条 PPP 链路的两端可以使用不同的认证协议认证对端，但是被认证方必须支持认证方使用的认证协议并正确配置用户名和密码等认证信息。
- LCP 使用魔术字（Magic-Number）检测链路环路和其它异常情况。魔术字为随机产生的一个数字，随机机制需要保证两端产生相同魔术字的可能性几乎为 0。
- 收到一个 Configure-Request 报文之后，其包含的魔术字需要和本地产生的魔术字做比较，如果不同，表示链路无环路，则使用 Confugure-Ack 报文确认（其他参数也协商成功），表示魔术字协商成功。在后续发送的报文中，如果报文含有魔术字字段，则该字段设置为协商成功的魔术字，LCP 不再产生新的魔术字。
- 如果收到的 Configure-Request 报文和自身产生的魔术字相同，则发送一个 Configure-Nak 报文，携带一个新的魔术

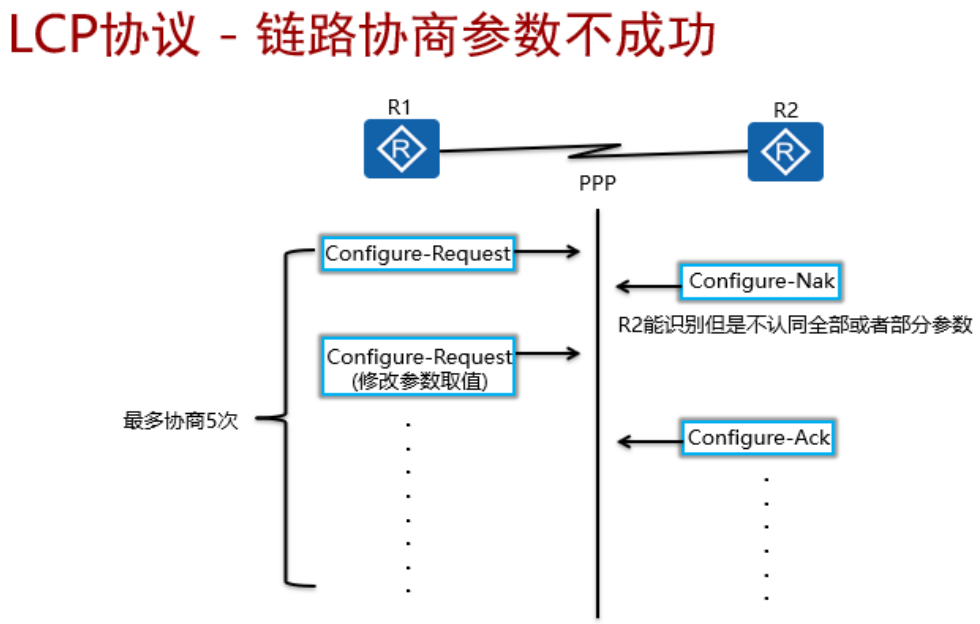
字。然后，不管新收到的 Configure-Nak 报文中是否携带相同的魔术字，LCP 都发送一个新的 Configure-Request 报文，携带一个新的魔术字。如果链路有环路，则这个过程会不停的持续下去，如果链路没有环路，则报文交互会很快恢复正常。



- 链路协商成功
- 如图所示，R1 和 R2 使用串行链路相连，运行 PPP。当物理层链路变为可用状态之后，R1 和 R2 使用 LCP 协商链路参数。本例中，R1 首先发送一个 LCP 报文。
- R1 向 R2 发送 Configure-Request 报文，此报文包含在发送者（R1）上配置的链路层参数，每个链路层参数使用“类型，长度，取值”的结构表示。
- 当 R2 收到此 Configure-Request 报文之后，如果 R2 能识别此报文中的所有链路层参数，并且认为每个参数的取值都是可以接受的，则向 R1 回应一个 Configure-Ack 报文。
- 在没有收到 Configure-Ack 报文的情况下，每隔 3 秒重传一次 Configure-Request 报文，如果连续 10 次发送 Configure-Request 报文仍然没有收到 Configure-Ack 报文，则认为对

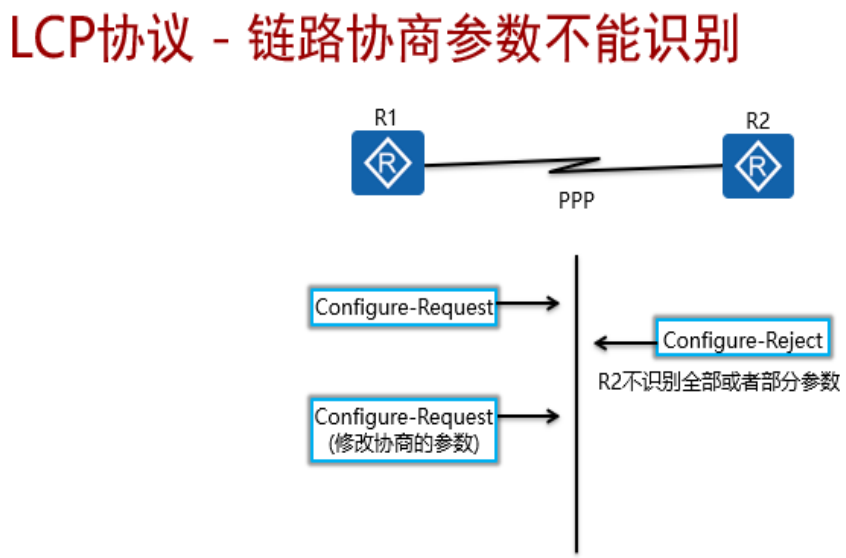
端不可用，停止发送 Configure-Request 报文。

- 注：完成上述过程只是表明 R2 认为 R1 上的链路参数配置是可接受的。R2 也需要向 R1 发送 Configure-Request 报文，使 R1 检测 R2 上的链路参数配置是不是可接受的。



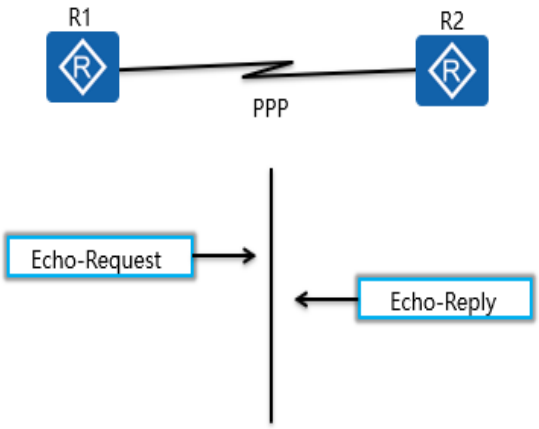
- 链路协商参数不成功
- 当 R2 收到 R1 发送的 Configure-Request 报文之后，如果 R2 能识别此报文中携带的所有链路层参数，但是认为部分或全部参数的取值不能接受，即参数的取值协商不成功，则 R2 需要向 R1 回应一个 Configure-Nak 报文。
- 在这个 Configure-Nak 报文中，只包含不能接受的那部分链路层参数列表，每一个包含在此报文中链路层参数的取值均被修改为此报文的发送者（R2）上可以接受的取值（或取值范围）。
- 在收到 Configure-Nak 报文之后，R1 需要根据此报文中的链路层参数重新选择本地使用的相关参数，并重新发送一个 Configure-Request。
- 连续五次协商仍然不成功的参数将被禁用，不再继续协

商。



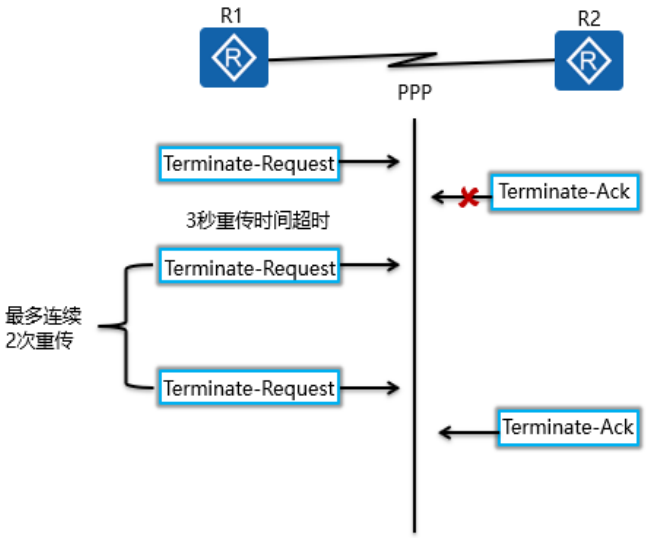
- 链路参数协商参数不能识别
- 当 R2 收到 R1 发送的 Configure-Request 报文之后，如果 R2 不能识别此报文中携带的部分或全部链路层参数，则 R2 需要向 R1 回应一个 Configure-Reject 报文。
- 在此 Configure-Reject 报文中，只包含不被识别的那部分链路层参数列表。
- 在收到 Configure-Reject 报文之后，R1 需要向 R2 重新发送一个 Configure-Request 报文，在新的 Configure-Request 报文中，不再包含不被对端（R2）识别的参数。

LCP协议 - 检测链路状态



- 检测链路状态
- LCP 建立连接之后，可以使用 Echo-Request 报文和 Echo-Reply 报文检测链路状态，收到一个 Echo-Request 报文之后应当回应一个 Echo-Reply 报文，表示链路状态正常。
- VRP 平台默认每隔 10 秒发送一次 Echo-Request 报文。

LCP协议 - 连接关闭



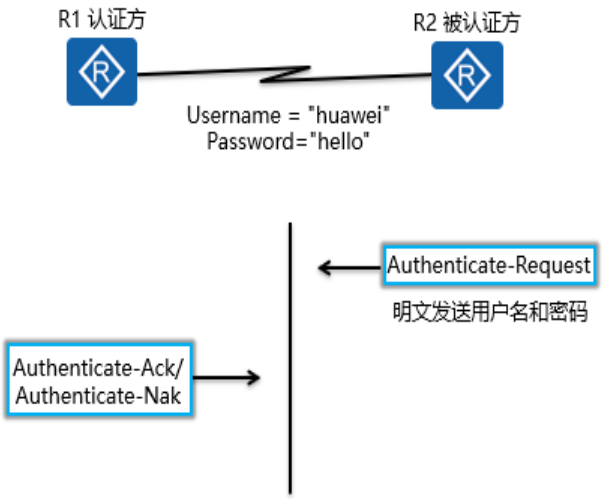
- 连接关闭
- 认证不成功或者管理员手工关闭等原因可以使 LCP 关闭已经建立的连接。
- LCP 关闭连接使用 Terminate-Request 报文和 Terminate-Ack 报文，Terminate-Request 报文用于请求对端关闭连接，一旦收到一个 Terminate-Request 报文，LCP 必须回应一个 Terminate-Ack 报文确认连接关闭。
- 在没有收到 Terminate-Ack 报文的情况下，每隔 3 秒重传一次 Terminate-Request 报文，连续两次重传没有收到 Terminate-Ack 报文，则认为对端不可用，连接关闭。

PAP认证 - 报文类型

报文类型	功能描述
Authenticate-Request	用于被验证方发送用户名和密码，Data字段包含明文用户名和密码信息。
Authenticate-Ack	用于验证方发送验证成功信息，Data字段可以包含文本提示信息。
Authenticate-Nak	用于验证方发送验证失败信息，Data字段可以包含文本提示信息。

- PAP 报文直接封装在 PPP 报文中。

PAP认证 - 工作原理



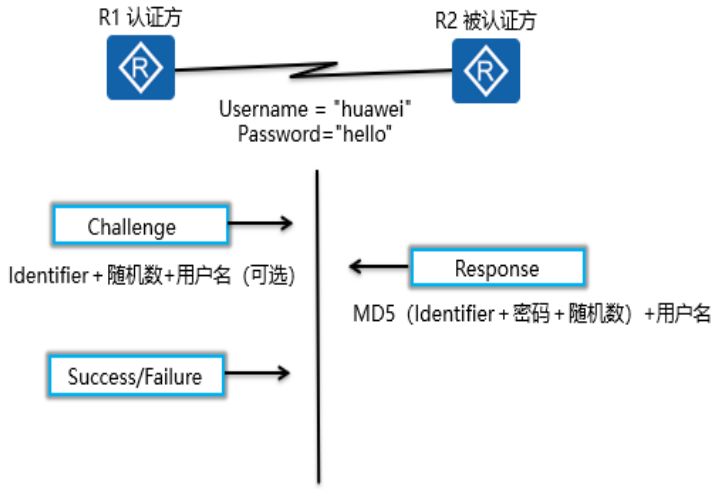
- PAP 工作模式
- 被认证方将配置的用户名和密码信息使用 Authenticate-Request 报文以明文方式发送给认证方，本例中，用户名为“huawei”，密码为“hello”；
- 认证方收到被认证方发送的用户名和密码信息之后，根据本地配置的用户名和密码数据库检查用户名和密码信息是否正确匹配，如果正确，则返回 Authenticate-Ack 报文，表示认证成功，如果不能正确匹配，则返回 Authenticate-Nak 报文，表示认证失败。

CHAP认证 - 报文类型

报文类型	功能描述
Challenge	用于验证方向被验证方发送Challenge，发起验证过程，Data字段包含Challenge.
Response	用于被验证方向验证方返回用户信息，Data字段含有返回的用户名以及加密运算之后的密码信息。
Success	用于验证方向被验证方发送认证成功信息，Data字段可以包含文本提示信息。
Failure	用于验证方向被验证方发送认证失败信息，Data字段可以包含文本提示信息。

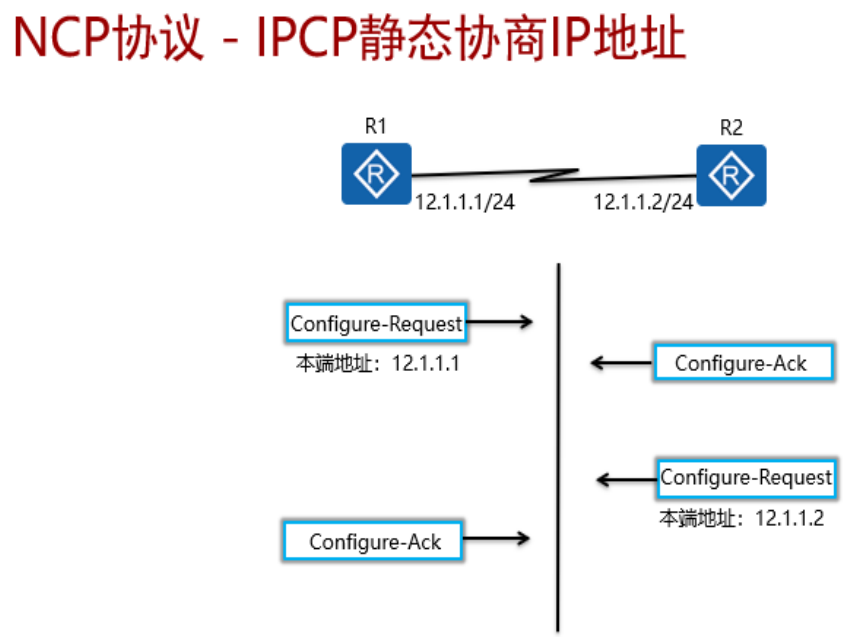
- 使用 Challenge 对密码做加密运算的算法为 MD5{ Identifier + 密码 + Challenge }，意思是将 Identifier、密码和 Challenge 三部分连成一个字符串整体，然后对此字符串做 MD5 运算，得到一个 16 字节长的摘要信息，在 Response 报文中 Data 字段包含的加密运算之后的密码信息就是此摘要信息。

CHAP认证 - 工作原理



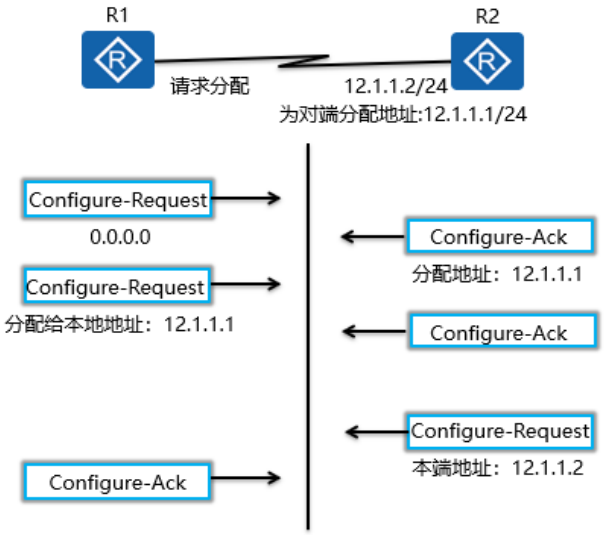
- CHAP 的认证过程需要三次报文的交互。为了匹配请求报文和回应报文，报文中含有 Identifier 字段，一次认证过程所使用的报文均使用相同的 Identifier 信息。CHAP 单向验证过程分为两种情况：验证方配置了用户名和验证方没有配置用户名。推荐使用验证方配置用户名的方式，这样可以对验证方的用户名进行确认。
- 验证方配置了用户名的验证过程（即接口配置命令 ppp chap user username）：
- 验证方主动发起验证请求，验证方向被验证方发送一些随机产生的报文（Challenge），并同时将本端的用户名附带上一起发送给被验证方。
- 被验证方接到验证方的验证请求后，先检查本端接口上是否配置了 ppp chap password 命令，如果配置了该命令，则被验证方将生成的密文（（Identifier + 密码 + 随机数）的 MD5）和自己的用户名发回验证方（Response）。如果接口上未配置 ppp chap password 命令，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，将密文（（Identifier + 密码 + 随机数）的 MD5）和被验证方自己的用户名发回验证方（Response）。
- 验证方将自己本身保存的密码、Identifier 和随机数进行 MD5 算法，和收到 respone 中的密文进行比较，以验证认证是否正确。
- 验证方没有配置用户名（即接口没有配置命令 ppp chap user username）：
- 验证方主动发起验证请求，验证方向被验证方发送一些随机产生的报文（Challenge）。
- 被验证方接到验证方的验证请求后，利用 Identifier、ppp chap password 命令配置的 CHAP 密码和随机数进行 MD5 算法，将生成的密文和自己的用户名发回验证方（Response）。
- 验证方将自己本身保存的密码、Identifier 和随机数进行

MD5 算法，和收到 respone 中的密文进行比较，以验证认证是否正确。



- IPCP，用于协商控制 IP 参数，使 PPP 可用于传输 IP 数据包。
- IPCP 使用和 LCP 相同的协商机制、报文类型，但 IPCP 并非调用 LCP，只是工作过程、报文等和 LCP 相同。
- 两端配置的 IP 地址分别为 12.1.1.1/24 和 12.1.1.2/24（两端 IP 地址即使不在同一网段也会通过 IPCP 协商）。
- 两端静态配置 IP 地址的时候协商过程如下：
- R1 和 R2 都要发送 Configure-Request 报文，在此报文中包含本地配置的 IP 地址。
- R1 和 R2 接收到对端的 Configure-Request 报文之后，检查其中的 IP 地址，如果 IP 地址是一个合法的单播 IP 地址，而且和本地配置的 IP 地址不同（没有 IP 冲突），则认为对端可以使用该地址，回应一个 Configure-Ack 报文。
- 通过 IPCP 发送的信息，PPP 链路的两端都可以知道对端使用的 32 位 IP 地址。

NCP协议 - IPCP动态协商IP地址



- 如图所示，R1 配置为请求对端分配 IP 地址，R2 配置静态 IP 地址 12.1.1.2/24，并且启用 R2 给对端分配 IP 地址的能力，给 R1 分配 IP 地址 12.1.1.1。
- 两端动态协商 IP 地址的过程如下：
- R1 向 R2 发送一个 Configure-Request 报文，此报文中含有 IP 地址 0.0.0.0，一个含有 0.0.0.0 的 IP 地址的 Configure-Request 报文表示向对端请求 IP 地址；
- R2 收到上述 Configure-Request 报文后，认为其中包含的地址（0.0.0.0）不合法，使用 Configure-Nak 回应一个新的 IP 地址 12.1.1.1；
- R1 收到此 Configure-Nak 报文之后，更新本地 IP 地址，并重新发送一个 Configure-Request 报文，包含新的 IP 地址 12.1.1.1；
- R2 收到 Configure-Request 报文后，认为其中包含的 IP 地址为合法地址，回应一个 Configure-Ack 报文；
- 同时，R2 也要向 R1 发送 Configure-Request 报文请求使用地址 12.1.1.2，R1 认为此地址合法，回应 Configure-Ack

报文。

MP基本原理

- MP基本原理
  - 增加带宽，将多个PPP链路捆绑使用。
- MP方式下链路协商过程
  - LCP阶段，也需验证对端接口是否工作在MP方式下。
  - NCP阶段，根据MP-Group接口或指定虚拟接口模板的各项NCP参数（如IP地址等）进行NCP协商。
- 实现方式
  - 虚拟接口模板方式。
  - MP-Group方式。

- MultiLink PPP 允许将报文分片，分片将从多个点对点链路上送到同一个目的地。

配置PPP

- 配置R1和R2的互联接口封装类型为PPP，使用CHAP认证，用户名为Huawei，密码为Hello。


```
aaa
 local-user Huawei password cipher Hello
 local-user Huawei service-type ppp
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode chap
 ppp chap user Huawei
 ip address ppp-negotiate
```

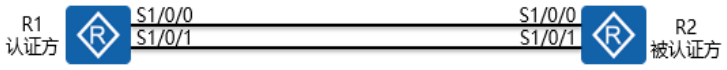
```
interface Serial1/0/0
 link-protocol ppp
 remote address 12.1.1.1
 ppp chap user Huawei
 ppp chap password cipher Hello
 ip address 12.1.1.2 255.255.255.0
```

- 命令含义

- ppp authentication-mode 命令用来设置本端 PPP 协议对对端设备的认证方式。
- ppp chap user 命令用来配置 CHAP 验证的用户名。
- ppp chap password 命令用来配置 CHAP 验证的口令。
- ip address ppp-negotiate 命令用来为本端接口配置 IP 地址可协商属性，使本端接口接受 PPP 协商产生的由对端分配的 IP 地址。
- remote address 命令用来配置为对端分配 IP 地址或指定地址池。
- ppp authentication-mode { chap | pap }
- chap：采用 CHAP 认证方式。
- pap：采用 PAP 认证方式。
- ppp chap user username
- username：设置 CHAP 验证的用户名。
- ppp chap password { cipher | simple } password
- cipher：表示密码为密文显示。
- simple：表示密码为明文显示。
- password：设置 CHAP 认证的口令。

配置MP

- 为了增加接口带宽，将R1与R2的所有互连PPP接口采用MP-Group进行MP绑定；R1与R2之间PAP认证，R1为认证端，R2为被认证端，且用户名为Huawei，密码为Hello。




```
aaa
 local-user Huawei password cipher Hello
 local-user Huawei service-type ppp
#
interface Mp-group0/0/0
 ip address 12.1.1.1 255.255.255.0
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode pap
 ppp mp Mp-group 0/0/0
#
interface Serial1/0/1
 link-protocol ppp
 ppp authentication-mode pap
 ppp mp Mp-group 0/0/0
```

```
interface Mp-group0/0/0
 ip address 12.1.1.2 255.255.255.0
#
interface Serial1/0/0
 link-protocol ppp
 ppp pap local-user Huawei password simple Hello
 ppp mp Mp-group 0/0/0
#
interface Serial1/0/1
 link-protocol ppp
 ppp pap local-user Huawei password simple Hello
 ppp mp Mp-group 0/0/0
```

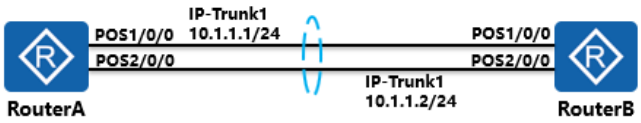
- 命令含义
- interface mp-group 命令用来创建一个 MP-Group 类型的接口并进入 MP-Group 接口视图。
- ppp mp mp-group 命令用来将接口加入指定的 MP-group，使该接口工作在 MP 方式。
- restart 命令用来重新启动当前接口。

IP-Trunk

- Trunk接口分为Eth-Trunk和IP-Trunk两种。
  - Eth-Trunk只能由以太网链路构成。
  - IP-Trunk一般由POS接口构成。
- 在一个IP-Trunk内，可以实现流量负载分担。负载分担分为逐流负载分担和逐包负载分担。
  - 逐流负载分担：当报文的源IP地址和目的IP地址都相同时，这些报文从同一个成员链路上通过。
  - 逐包负载分担：以报文为单位分别从不同的成员链路上发送。
- IP-Trunk的成员接口只能使用HDLC封装形式。IP-Trunk的原理与Eth-Trunk类似。

- Trunk 接口分为 Eth-Trunk 和 IP-Trunk 两种。
- Eth-Trunk 只能由以太网链路构成。
- IP-Trunk 一般由 POS 接口构成。

IP-Trunk配置




```
#
sysname RouterA
#
interface Ip-Trunk1
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
interface Pos1/0/0
 link-protocol hdlc
 undo shutdown
 ip-trunk 1
#
interface Pos2/0/0
 link-protocol hdlc
 undo shutdown
 ip-trunk 1
#
```

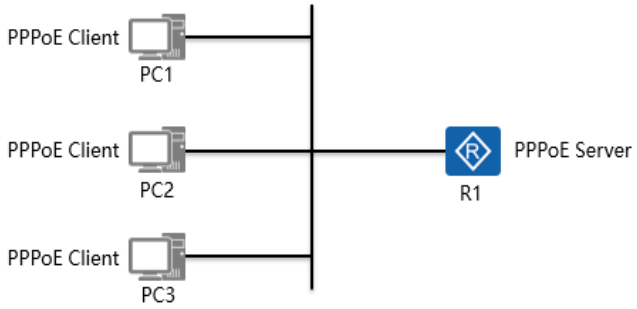
```
#
sysname RouterB
#
interface Ip-Trunk1
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
interface Pos1/0/0
 link-protocol hdlc
 undo shutdown
 ip-trunk 1
#
interface Pos2/0/0
 link-protocol hdlc
 undo shutdown
 ip-trunk 1
#
```

PPPoE概述 (1)

- PPPoE（PPP over Ethernet）协议是一种把PPP帧封装到以太网帧中的链路层协议。PPPoE可以使以太网网络中的多台主机连接到远端的宽带接入服务器。
- 运营商希望把一个站点上的多台主机连接到同一台远程接入设备，同时接入设备能够提供与拨号上网类似的访问控制和计费功能。在众多的接入技术中，把多个主机连接到接入设备的最经济的方法就是以太网，而PPP协议可以提供良好的访问控制和计费功能，于是产生了在以太网上传输PPP报文的技术，即PPPoE。
- PPPoE利用以太网将大量主机组成网络，通过一个远端接入设备连入因特网，并运用PPP协议对接入的每个主机进行控制，具有适用范围广、安全性高、计费方便的特点。

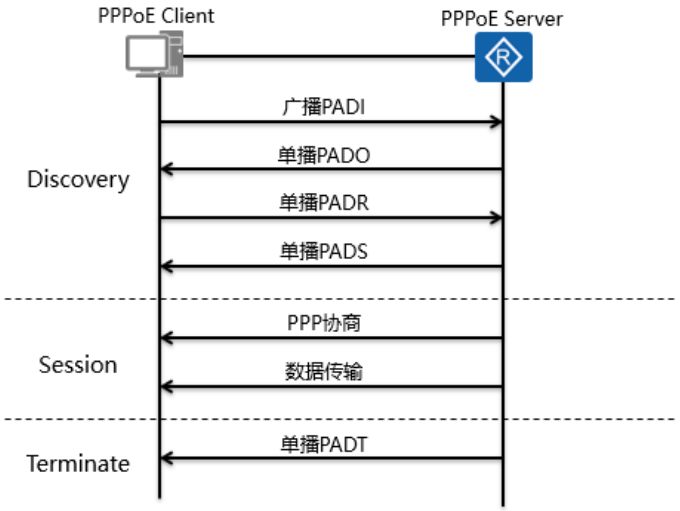
PPPoE概述 (2)

- PPPoE概述
  - PPP应用于以太网以实现广播式的网络中多台主机连接到远端的接入服务器的技术。
  - PPPoE组网结构采用Client/Server 模型。



- PPPoE 概述
- PPPoE 利用以太网将大量主机组成网络，通过一个远端接入设备连入因特网，并运用 PPP 协议对接入的每个主机进行控制，具有适用范围广、安全性高、计费方便的特点。

PPPoE会话建立过程



- PPPoE 可分为三个阶段，即 Discovery 阶段、Session

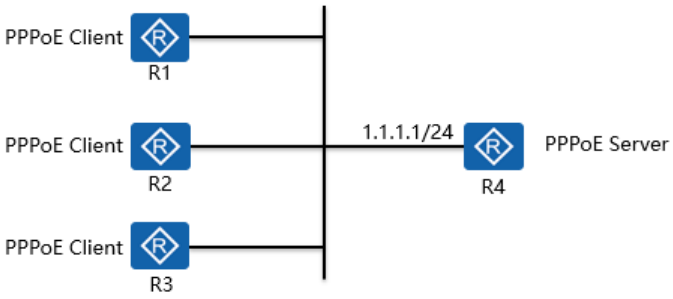
阶段和 Terminate 阶段。

- Discovery 阶段：
- PPPoE Client 广播发送一个 PADI（PPPoE Active Discovery Initial）报文，在此报文中包含 PPPoE Client 想要得到的服务类型信息。
- 所有的 PPPoE Server 收到 PADI 报文之后，将其中请求的服务与自己能够提供的服务进行比较，如果可以提供，则单播回复一个 PADO（PPPoE Active Discovery Offer）报文。
- 根据网络的拓扑结构，PPPoE Client 可能收到多个 PPPoE Server 发送的 PADO 报文，PPPoE Client 选择最先收到的 PADO 报文对应的 PPPoE Server 做为自己的 PPPoE Server，并单播发送一个 PADR（PPPoE Active Discovery Request）报文。
- PPPoE Server 产生一个唯一的会话 ID（Session ID），标识和 PPPoE Client 的这个会话，通过发送一个 PADS（PPPoE Active Discovery Session-confirmation）报文把会话 ID 发送给 PPPoE Client，会话建立成功后便进入 PPPoE Session 阶段。
- 完成后通信双方都会知道 PPPoE 的 Session_ID 及对方 MAC，它们共同确定唯一的 PPPoE Session。
- Seesion 阶段：
- PPPoE Session 上的 PPP 协商和普通的 PPP 协商方式一致。PPPoE Session 的 PPP 协商成功后，就可以承载 PPP 数据报文。在 PPPoE Session 阶段所有的以太网数据包都是单播发送的。
- Terminate 阶段：
- 进入 PPPoE Session 阶段后，PPPoE Client 和 PPPoE Server 都可以通过发送 PADT 报文的方式来结束 PPPoE 连接。PADT 数据包可以在会话建立以后的任意时刻单播发送。在发送或接收到 PADT 后，就不允许再使用该会话发送 PPP 流量

了。

配置PPPoE (1)

- 公司A希望部署PPPoE，现根据需求完成如下配置：
  - R4为PPPoE Server端，为客户端分配IP地址池范围1.1.1.0/24，使用PAP认证模式；
  - R1为PPPoE Client端，认证用户名/密码为HuaweiR1/R1；
  - R2为PPPoE Client端，认证用户名/密码为HuaweiR2/R2；
  - R3为PPPoE Client端，认证用户名/密码为HuaweiR3/R3。



配置PPPoE (2)

- Client R1的配置：

```
interface Dialer1
 link-protocol ppp
 ppp pap local-user HuaweiR1 password cipher
R1
 ip address ppp-negotiate
 dialer user HuaweiR1
 dialer bundle 1
 dialer-group 1
#
interface GigabitEthernet0/0/0
 pppoe-client dial-bundle-number 1
#
dialer-rule
 dialer-rule 1 ip permit
```

- Server R4的配置：

```
ip pool POOL_1
 gateway-list 1.1.1.1
 network 1.1.1.0 mask 255.255.255.0
#
aaa
 local-user HuaweiR1 password cipher R1
 local-user HuaweiR2 password cipher R2
 local-user HuaweiR3 password cipher R3
#
interface Virtual-Template0
 ppp authentication-mode pap
 remote address pool POOL_1
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/0
 pppoe-server bind Virtual-Template 0
```

- 此例中，R1 模拟 PPPoE 客户机 PC 进行 PPPoE 拨号上网，R4 作为 PPPoE Server 对其进行验证和地址分配。