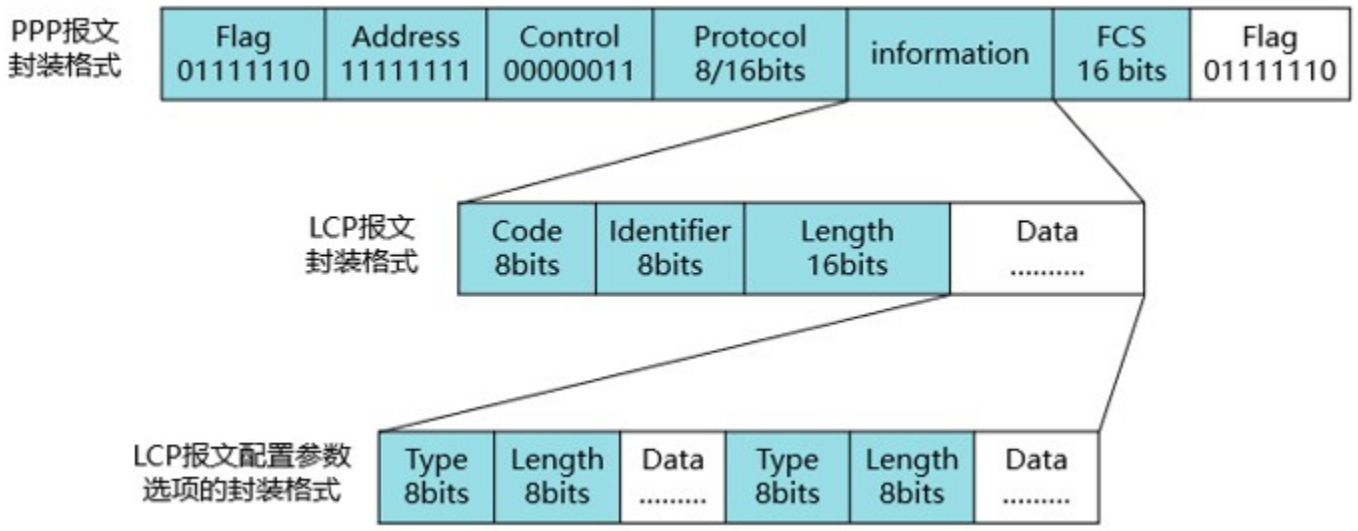
PPP 协议

扩展问题 1：PPP 帧格式，报文结构



Flag： Flag 域标识一个物理帧的起始和结束，该字节为 0x7E

Address：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： 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应答来实现可靠传输（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

扩展问题 2：PPP 连接建立之后，魔术字是否会一致改变？
不会，只要 LCP 协商通过链路建立起来后在链路断开之前，魔术字都不会改变；

扩展问题 3：MRU 不一致的协商过程？
答：以本端的 MRU 发送配置请求消息，对端收到配置请求消息之后，以对端发过来的配置请求携带的 MRU 值进行回复，直接发送 ACK。但是在 MRU 大的一方会把 MRU 改小，使得双方正常收发数据。

扩展问题 4：两端都配置了认证，一端为 CHAP 的认证端，另一端为 PAP 的被认证端，那么 LCP 协商是否会成功？
答：不会，双方会发送 configure-NAK 报文，最终协商不通过。

扩展问题 5：一端为 MP、一端为 SP 的工作方式，那么 LCP 协商能通过吗？
答：能，能够进入 LCP open 状态，双方都是用 SP 的工作方式；

扩展问题 6：如果双方选择的魔术字一样会怎么样？
回复 configure-nak 报文，报文携带不能认同的参数（魔术字），对方收到后，会重新选择一个魔术字。

扩展问题 7：魔术字的作用？
防止物理环路；

扩展问题 8：一端为认证方，一端没有配置认证会怎么样？
LCP 协商不通过。因为认证方发送的 configure-request 报文

中会携带认证方式，对端没有配置认证，所以无法识别认证参数，因此会回复 configure-reject 报文，报文中携带不能识别的参数（认证方式），最终 LCP 协商不通过。

扩展问题 9：只有被认证方，没有认证方可以正常建立 PPP 连接吗？
答：可以。

扩展问题 10：chap 随机数有什么作用?
做 hash 计算和防止重放攻击，每次做认证的随机数都会变化，而随机数的变化会导致 hash 计算结果的变化，从而达到防重放攻击的目的。

扩展问题 11：pap 和 chap 的差别？
（1）chap 采取三次握手，pap 是两次握手
（2）chap 由认证方发起，pap 由被认证发起
（3）chap 携带用户名和 hash，pap 中以明文的方式携带用户名和密码
（4）CHAP 认证用户名可选，PAP 不行（或者说 CHAP 被认证方的接口下可以不配置密码）

扩展问题 12：PPP 认证和 OSPF 认证的区别？
1.一次认证，每个报文都认证
2.二层认证，三层认证
3.C/S 模型，相互认证
4.PPP 认证成功或者失败都会回复消息，而 ospf 不会

扩展问题 13：isis 认证和 ospf 认证的区别？
isis 可以针对不同的报文进行认证，而 ospf 中是针对所有的 ospf 报文进行认证；

扩展问题 14：CHAP 中挑战 id 有什么作用？
（1）挑战 id 和随机数都参与计算 hash
（2）挑战 id 还记录每次会话
被认证在回复 response 中带 ID，认证端根据收到的 ID 找到相应的随机数

扩展问题 15：chap 认证，被认证方一定要有接口密码吗？
答：不一定，如果认证方发送的挑战消息中携带用户名时，密码可以配置在全局数据库中。

扩展问题 16：chap 中，认证方与被认证方的用户名有关系吗？
答：没有必然关系。当接口下没有配置密码时，根据对方发过来的用户名在本地数据库中找到相应的密码来做 hash，用户名本身不参与 hash。

扩展问题 17：PPP 认证如何确定认证方和被认证方？
在 LCP 协商阶段，认证方发送的配置请求消息的认证字段会有相应的认证方式，如果被认证方也配置了同样的认证方式，则会回复 ACK，而后进行认证阶段。

扩展问题 18：两台路由器使用双向认证，一边使用 PAP，一边使用 CHAP，PPP 链路是否可以协商成功？
可以，只要一端为 PAP 认证端，同时又为 CHAP 的被认证端，而另一端为 CHAP 的认证端，同时又为 PAP 的被认证端即可

扩展问题 19：chap 认证的 id 和随机数只要其中的一个进行 chap 认证行不行？
不行，挑战 id 和随机数都参与计算 hash。
挑战 id---用于记录会话

随机数---防止重放攻击

扩展问题 20：既然 pap 认证是不可以加密的，chap 认证是可以加密的，有 chap 认证就行了，为什么还要有 pap 认证？
（1）在对 ppp 链路进行认证的时候可以多一种选择
（2）因为 chap 和 pap 各自有自己适用的场景：
pap---客户要求链路快速建立，同时又要具有一定的安全性时，就可以使用 pap；（还有就是 pap 不需要进行 md5 运算，对设备消耗较小）
chap---客户对网络具有较高的安全性；

扩展问题 21：接口下没有配置 chap password，同时 aaa 中也没有配置 password 的，会怎么样？
答：回复 response 报文，该报文中的 hash 值由（随机数+挑战 ID）MD5 计算得到；最终链路无法建立。

扩展问题 22：认证方发送过来的 challenge 报文中，携带的用户名和验证方接口下配置的用户名不一致会怎么样？
1、被认证方接口下有配置密码，不会去查看发送过来的用户名；
2、被认证方接口下没有配置密码，根据发送过来的用户名去 aaa 数据库下找；
3、被认证方没有配置密码（即在接口下和 aaa 数据库下都没有配置密码），那么被认证方会拿挑战 ID+随机数进行 MD5 计算，并将计算出来的 hash 数值通过 response 报文发送给到对端；

扩展问题 23：PPP 的 CHAP 认证的认证端有带用户名好还是没有带用户名好？
答：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。也可以根据挑战报文的用户名在被认证端中选择不同的密码做 hash。

扩展问题 24：NCP 协商失败会进入到 terminate 吗?
答：不会；Network 协商不通过也不会进入 terminate 阶段，因为这样的话，配置了相应的 IP 地址之后，就可以直接发送业务，不需要重新建立链路后，再进行 NCP 协商。

扩展问题 25：NCP 阶段还没协商完成，是否可以传输 IP 数据？
答：可以的，在 NCP 阶段，只要 IPCP 协商完成后就可以传输 IP 数据了；因为 NCP 不止有 IPCP 协商，还有其他上层协议的协商，例如 mpls cp ， IPV6 CP；

扩展问题 26：掩码应该配置多少位？
答：最好配置 30 位，第一可以节约 ip，第二可以防环。

扩展问题 27：环路怎样产生的？
答：PPP 链路上配置了一个 ip 地址时，会生成一条直连路由（比如：10.1.12.0/2410.1.12.1 s0/0/0）下一跳为本地接口 ip 地址，出接口为本地接口。同时又因为 PPP 链路上互访时不会发出 ARP 请求，请求对端的 MAC 地址，所以当访问一个这段链路上没有的同网段 IP 地址时，根据最长掩码匹配原则，会匹配到该直连路由，发送给到对端，对端收到后，同理又会发回来，就这样形成了环路；

扩展问题 28：以太网链路上会出现这样的环路吗？
不会，因为以太网链路上比 PPP 链路多了一个发送 ARP 请求的过程，要完成数据包的封装才能发送数据包，所以不会产生

环路；

扩展问题 29：两台路由器使用串行链路直连，会生成几条路由？
4 条；
1、10.1.12.0/24 的直连路由，下一跳为自己接口 ip 地址，出接口为自己的接口；
2、为自己的接口生成 32 位的主机路由：10.1.12.1/32；
3、为对端的接口生成 32 位的主机路由：10.1.12.2/32；
4、为自己接口生成一条路由：10.1.12.255/32 的路由；

扩展问题 30：ppp 中默认 mtu 值为多少？
1500。

扩展问题 31：ospf 中默认 mtu 值为多少？
默认为 0，因为默认情况下，不检查接口 MTU，DD 报文中会显示 interface MTU：0。

PPPoE 协议

扩展问题 1：PPPoE 的作用？
让 PPP 数据帧能够在以太网上传递；

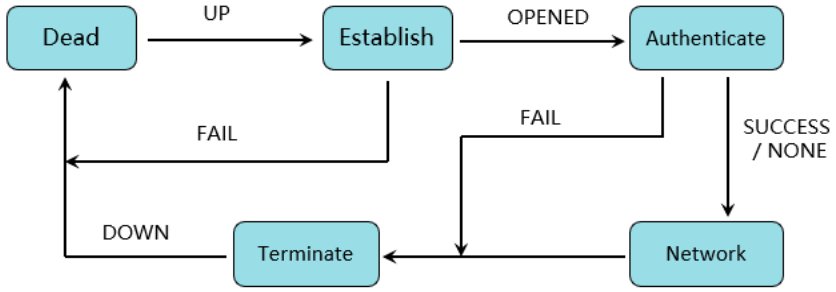
扩展问题 2：PPPoE 为什么可以在以太网上传递？
因为 PPPoE 报文的封装格式是，以太网帧头+PPPoE 报头+PPP 报头,这样的一种封装格式；

扩展问题 3：PPPoE 有什么好处？
PPP 中有认证阶段，需要用到 AAA 数据库，三 A 分别为认证（authentication）、授权（authorization）、审计（audit），可以提供对用户的合法性进行认证，和对用户的使用量进行计费；同时 PPP 中的 NCP 协商阶段中，有动态 IPCP 协商，可以为用户分配 IP 地址等的网络参数；

==========

PPP 建链过程

PPP建链过程

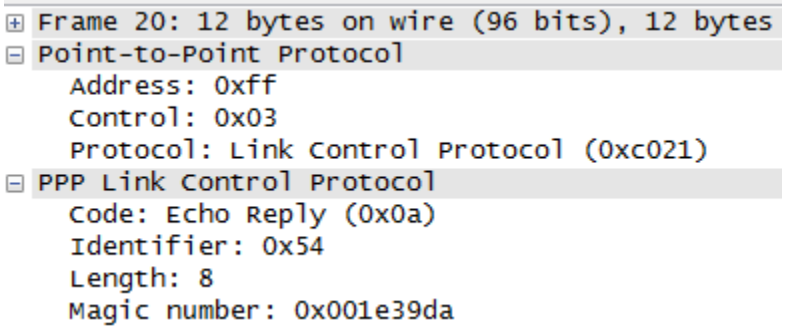


Dead：这是 PPP 工作开始和结束的阶段。当物理层变为可用状态（UP）之后，PPP 进入 Establish 阶段。
Establish：PPP 在此阶段使用 LCP 协商链路层参数。如果链路层参数协商不成功（FAIL），则 PPP 连接建立不成功，PPP 退回到 Dead 阶段。如果链路层参数协商成功（OPENED），则 PPP 进入 Authenticate 阶段。
Authenticate：PPP 在此阶段认证对端，如果认证失败（FAIL），则 PPP 进入 Terminate 阶段；如果认证成功（SUCCESS）或者没配置认证（NONE），则 PPP 进入 Network 阶段。
Network：PPP 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）。

==========

PPP 的认证过程，答题思路是将认证分为两种一种　是 PAP 以及 CHAP　，
分别讲述了一下认证如何建立，携带哪些参数



追问一、魔术字（随机数）有什么用？　答　防环（防重放攻击）
LCP 使用魔术字来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（其它参数也协商成功），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。
追问二、会话 ID 有什么用？　答　表示一次 PPP 会话
追问三、被认证方接口　一定要配置用户名吗？　　必须的

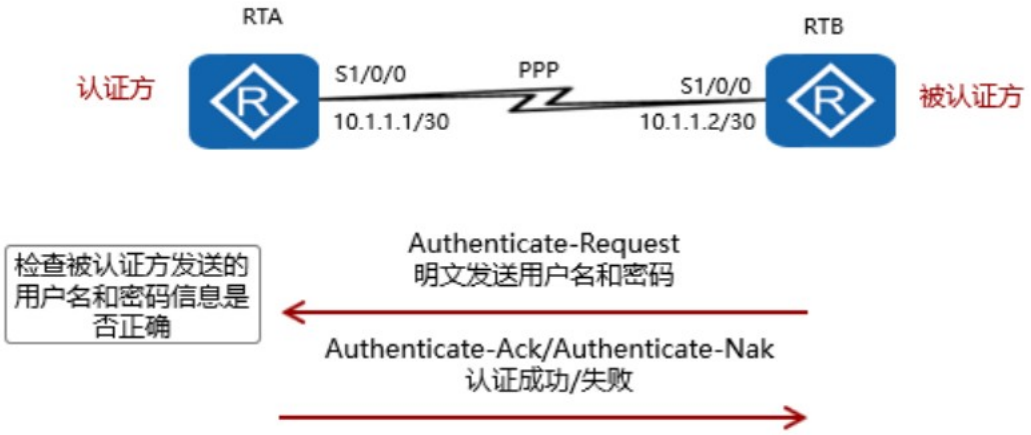
追问四、认证方接口要不要配用户名？
可以不配，讲了下配跟不配有什么区别
1　认证方配置用户名的话，被认证方就可以根据用户名查找本地的用户数据库，找的密码，然后回复给认证方。　2 认证方如果在接口不配用户名，那么发给被认证方的验证请求中不带用户名，被认证方根据接口配置的用户名和密码发送回复报文。

追问五、PPPOE 了解吗？　了解一点，讲了 PPPOE 交互的过程，以及作用
PPPoE 会话建立可分为三个阶段，即 Discovery 阶段、Session 阶段和 Terminate 阶段。

追问六、PAP　跟　CHAP　有什么区别　？　如果 PAP 加密了是不是也是很安全？
这个简单，答了区别，传密码和不传密码，如果 PAP 使用了加密，在认证的时候还是传密码 只是密码使用特定的算法加密了，如果知道了该算法还是能破解的。

PAP 和 CHAP 的认证过程

PAP 认证



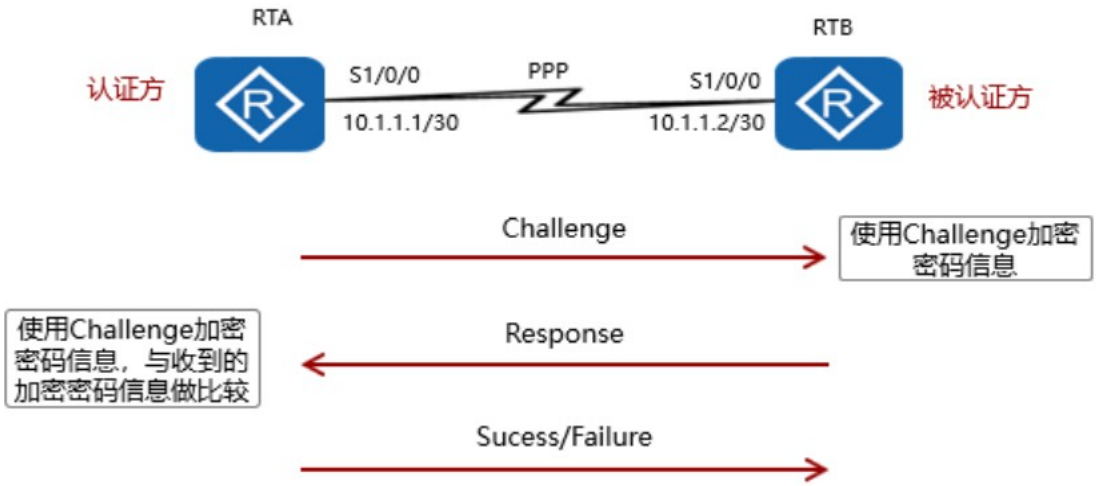
首先被认证方向认证方发送认证请求（包含用户名和密码），以明文形式进行传输，认证方接到认证请求，再根据被认证方发送来的用户名去到自己的数据库认证用户名密码是否正确，如果密码正确，PAP 认证通过，如果用户名密码错误，PAP 认证未通过。

PAP 并不是一种强有效的认证方法，其密码以文本格式在电路上进行发送，对于窃听、重放或重复尝试和错误攻击没有任何保护。

==========

CHAP 认证

CHAP 通过三次握手验证被认证方的身份（密文），在初始链路建立时完成，为了提高安全性，在链路建立之后周期性进行验证



challege　id+随机数+（用户名）
response id+hash 值
sucess/failure

1 认证方主动向被认证方发送“challenge”消息（此认证序列号 id+认证方主机名+随机数）
2 被认证方去到自己的数据库查到认证方主机名对应的密码，用查到的密码结合认证方发来的认证序列号 id 和随机数，经过单向哈希函数 MD5 计算出来的值做应答。

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
（1）认证方配置用户名的话，被认证方就可以根据用户名查找本地的用户数据库，找的密码，然后回复给认证方。
（2）认证方如果在接口不配用户名，那么发给被认证方的验证请求中不带用户名，被认证方根据接口配置的用户名和密码发送回复报文。

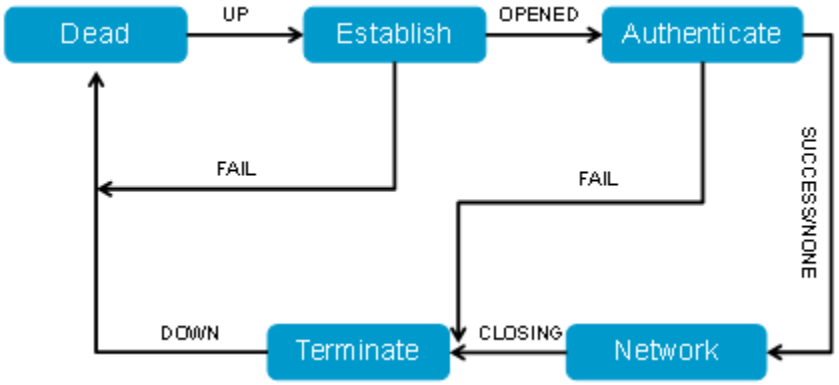
3 根据被认证方发来的认证用户名，认证方在本地数据库中

查找被认证方对应的密码，结合 id 找到先前保存的随机数据和 id 根据 MD5 算法算出一个 Hash 值，与被认证方得到的 Hash 值做比较，如果一致，则认证通过，如果不一致，则认证不通过。

4 经过一定的随机间隔，认证方发送一个新的 challenge 给被认证方，重复步骤 1 到 3 。

==========

“PPP 链路的建立过程是怎么样的？请详细描述”



对于 PPP 链路建立过程的描述如下：

1、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时，就会从 Dead 阶段迁移至 Establish 阶段，即链路 建立阶段。

2、在 Establish 阶段，PPP 链路进行 LCP 参数协商。协商内容包括最大接收单元 MRU、认证方式、魔术字（Magic Number）等选 项。LCP 参数协商成功后会进入 Opened 状态，表示底层链路已经建立。

MRU: 定义最大携带数据包（接收）

Authentication-Protocol:认证方式

Quality-Protocol: 定义是否要使用链路质量监控

Magic-Number: 用来检测环路和不正常的连接错误

Protocol-Field-Compression: 定义是否要启用 protocol 字段压缩 16bit->6bit Address-and-

Control-Field-Compression(ACFC): 定义是否要 压缩地址和控制字字段

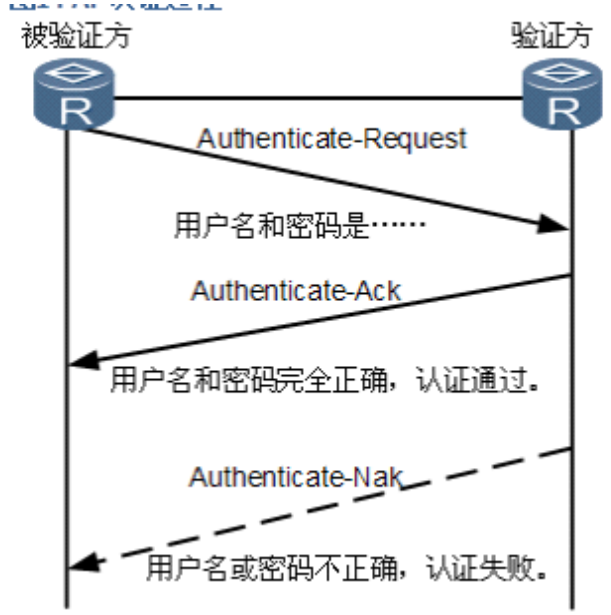
如果参数能识别但是不接受，那就返回 Configure-Nak ("negative acknowledge")，如果参数根本无法识别（也就是对端不支持此功 能）就返回 Configure-Reject

3、多数情况下,链路两端的设备是需要经过认证阶段（Authenticate）后才能够进入到网络层协议阶段。PPP 链路在缺省情况下是 不要求进行认证的。如果要求认证，则在链路建立阶段必须指定认证协议。认证方式是在链路建立阶段双方进行协商的。如果在 这个阶段再次收到了 Configure-Request 报文，则又会返回到链路建立阶段。

PAP ：

PAP 验证协议为两次握手验证，口令为明文。验证过程仅在链路初始建立阶段进行。 当链路建立阶段结束后，用户名和密码将由 被验证方重复地在链路上发送给验证方，直到验证通过或者中止连接。

被验证方把本地用户名和口令发送到验证方。 验证方根据本地用户表查看是否有被验证方的用户名以及口令是否正确，然后返回 不同的响应（接受或拒绝）。



CHAP ：
CHAP（Challenge Handshake Authentication Protocol）验证协议为三次握手验证协议。它只在网络上传输用户名和以密码为原 始参数一部分的 hash 值，而并不传输用户密码，因此安全性要比 PAP 高。
CHAP 认证过程如下；

<1>验证方生成一个挑战数据包，向被验证方发送。里面包含报文 ID、随机数、用户名（华为设备挑战方如果接口没有配置用户名，华为设备默认不携带用户名。友商默认携带路由器的名字）。
<2>被验证方使用接口所配置口令，将报文 ID、随机数和口令放入到 MD5 散列生成器中通过计算得到一个 hash 值。被验证方向验 证方发送一个挑战应答报文。里面包含序列号、hash 值，用户名（用户名是验证发接口配置的用户名称）。

<3>验证方根据对应答信息里的用户名称选择本地 AAA 数据库里用户名所对应的口令。将报文 ID、随机数和口令放入到

MD5 散列生 成器中通过计算得到一个 hash 值。比较生成的 hash 值和应答包中携带的 hash 值。两个 hash 值相同表示认证成功。只有认证成功才 能进入阶段 3 的协商。 CHAP 认证的特点是只在网络上传输用户名，而不是传输口令，因此它的安全性要比 PAP 高。

4、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，该网络层协议才可以通过这条 PPP 链路发送报文。如果在这个阶段收到了 Configure-Request 报文，也会返回到 链路建立阶段。
5、NCP 协商成功后，PPP 链路将保持通信状态。PPP 运行过程中，可以随时中断连接，例如物理链路断开、认证失败、超时定时器 时间、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。
6、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。

以上是基本的内容，考试的时候肯定要必须回答上来，下面就是考官可能会追问到的一些问题了；

口令配置在接口和配置在全局的区别?
被认证方：
第一种情况：如果认证方接口没有配置用户名，也就是挑战报文不携带用户名的情况下，被认证方配置在全局没有意义，必须配置在接口。
第二种情况：如果认证方接口配置了用户名，也就是挑战报文携带用户名的情况下，被认证方先使用接口，后使用全局。

认证方：

只使用全局用户名对应的密码；

认证方发送的消息携带的用户名是什么？
如果认证方在接口配置用户名的话，发送的挑战报文中携带接口配置的用户名。如果接口没有配置用户名的话，不同厂家实现的方式有所不同，有的携带主机名，比如说友商，华为不携带。

CHAP 认证挑战报文里的用户名是怎么来的？
认证方的用户名：认证方的用户名是在认证接口上面配置上去的，如果没有配置用户名，不同的厂家实现方式有所不同，有的是携带设备主机名，我们华为设备上如果接口上没有配置用户名，则发送的挑战报文里是不携带用户名的。
被认证方的用户名：被认证方的用户名也是在接口上配置上去的，而且被认证方接口下必须配置用户名.

认证方发的用户名和被认证方发的用户名本身有没有什么关系？
本身是没有什么强制关联关系的，都是在本地上进行配置的，通过 chap 消息携带到对方去,并据此寻找 password, 如果 secret key mistmatch,则 fail.

被认证方的接口下如果没有配置用户名会导致什么情况？
认证方法送 conf Request ,在被认证方法送 config reject , LCP 协商 authentication 就 fail 了;
Note: 无论认证方是否发送 username ; 被认证方一定也要支持 chap, 一种方式是在接口下也开启 chap authentication mode, 另外一 种方式是接口下一定要添加 ppp chap username ; 只有上面 2 种方法,才能 LCP 协商通过 ; 如果被认证方没有找到 password or 认证方未传输用户名, 都会致验证 failure;

谁会发送认证失败的报文？
认证方发送 chap failure 消息。