了解和配置 PPP CHAP 认证

目录

简介

质询握手身份验证协议 (CHAP)（已在 RFC 1994 中定义）通过三向握手来验证对等体的身份。 以下是在 CHAP 中执行的一般步骤：

1. 在完成 LCP（链路控制协议）阶段并在两个设备之间协商 CHAP 之后，身份验证程序向对等体发送一条质询消息。
2. 对等体使用通过单向散列函数（消息摘要算法 5 (MD5)）计算的值进行响应。
3. 身份验证程序根据自己计算出的预期散列值检查响应。如果两个值匹配，则身份验证成功；否则，将终止连接。

此认证方法取决于只有证明人和对等体知道的“秘密”。该密钥不会通过链路发送。虽然身份验证只是单向身份验证，您仍可以借助为相互身份验证设置的相同密钥来双向协商 CHAP。

有关 CHAP 的优缺点的详细信息，请参阅 RFC 1994 。

先决条件

要求

本文档的读者应掌握以下这些主题的相关知识：

- 如何通过 **encapsulation ppp** 命令在接口启用 PPP。
- **debug ppp negotiation** 命令输出。有关详细信息，请参阅了解 debug ppp negotiation 输出。
- 能力排除故障，当链路控制协议(LCP)相位不在打开状态。这是因为，在 LCP 阶段已完成并处于打开状态之前，不会开始 PPP 身份验证阶段。如果 **debug ppp negotiation** 命令未表明 LCP 处于打开状态，您需要先对此问题进行故障排除，然后才能继续。

注意： 本文档不讨论 MS-CHAP（版本 1 或版本 2）。有关 MS-CHAP 的详细信息，请参阅 MS-CHAP 技术支持和 MSCHAP 版本 2 文档。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置 CHAP

配置 CHAP 的过程非常简单。例如，假定您有左右两个通过网络连接的路由器，如图 1 所示。

图1 â 在间网络的两路由器连接

要配置 CHAP 身份验证，请完成以下步骤：

1. 在接口上发出 **encapsulation ppp** 命令。
2. 使用 **ppp authentication chap** 命令在两个路由器上启用 CHAP 身份验证。
3. 配置用户名和口令。要执行此操作，请发出 **username username password password** 命令，其中 *username* 是对等体的主机名。请确保：两端上的口令相同。由于路由器名称和口令区分大小写，因此请确保它们完全相同。**注意：** 默认情况下，路由器使用其主机名向对等体标识其身份。然而，可以通过 **ppp chap hostname** 命令更改此 CHAP 用户名。有关详细信息，请参阅使用 ppp chap hostname 和 ppp authentication chap callin 命令执行 PPP 身份验证。

单向和双向验证

CHAP 被定义为单向身份验证方法。然而，您可以在两个方向上使用 CHAP 以创建双向身份验证。因此，通过双向 CHAP，每一端都可以发起单独的三次握手。

在 Cisco CHAP 实施中，默认情况下，被叫方必须认证主叫方（除非认证被完全地关闭了）。所以，被叫方发起的单向身份验证是可能的最低身份验证。然而，主叫方也可以验证被叫方的身份，从而导致双向身份验证。

当您连接到非 Cisco 设备时，通常需要进行单向身份验证。

对于单向身份验证，请在主叫路由器上配置 **ppp authentication chap callin** 命令。

表 1 显示了应在何时配置 callin 选项。

表1 â 什么时候配置呼入选项

认证类型	客户端（主叫）	NAS（被叫）
单向	ppp authentication chap callin	ppp authentication chap
双向	ppp authentication chap	ppp authentication chap

有关如何实现单向身份验证的详细信息，请参阅使用 ppp chap hostname 和 ppp authentication chap callin 命令执行 PPP 身份验证。

CHAP 配置命令和选项

表 2 列出了 CHAP 命令和选项：

表2个â CHAP发出命令和选项

命令	说明
ppp authentication {chap*|ms-chap|ms-chap-v2|eap|pap*} [callin]	此命令使用指定协议对远程 PPP 对等体启用本地身份验证。
ppp chap hostname username name	此命令定义特定于接口的 CHAP 主机名。有关详细信息，请参阅使用 ppp chap hostname 和 ppp authentication chap callin 命令执行 PPP 身份验证。
ppp chap password password	此命令定义特定于接口的 CHAP 口令。
ppp direction callin*|拨出|专用*	此命令强制呼叫方向。请使用此命令，当路由器是混淆的时至于是否呼叫流入或流出的(例如，当已连接背对背或连接由租用的线路和信道服务单元或者数据服务单元(CSU/DSU)或ISDN终端适配器(TA)配置拨号)。

ppp chap refuse [callin]	此命令会禁用对等体的远程身份验证（默认值为启用）。使用此命令，将针对所有呼叫禁用 CHAP 身份验证，这意味着对等体强制用户借助 CHAP 进行身份验证的所有尝试都会遭到拒绝。callin 选项指定路由器拒绝答复所收到的对等体的 CHAP 身份验证质询，但仍然要求对等体答复路由器发送的所有 CHAP 质询。
ppp chap wait	此命令指定呼叫方必须首先进行身份验证（默认值为启用）。此命令指定路由器不会对请求 CHAP 身份验证的对等体进行身份验证，直到对等体已向路由器验证其自己的身份为止。
ppp max-bad-auth value	此命令指定允许的身份验证重试次数（默认值为 0）。此命令可配置一个点对点接口，在认证失败之后不立即重置自己，而是允许指定认证重试的次数。
PPP CHAP splitnames	此隐藏命令允许 CHAP 质询和回应（默认为禁用）中不同的主机名。
ppp chap ignoreus	此隐藏命令忽略使用本地名称的 CHAP 质询（默认值是启用）。

交易示例

以下部分中的关系图表显示了 CHAP 身份验证过程中两个路由器之间发生的系列事件。这些并不表示在 **debug ppp negotiation** 命令输出中看到的实际消息。有关详细信息，请参阅了解 debug ppp negotiation 输出。

呼叫

图2 â 呼叫进来

图 2 显示了以下步骤：

1. 呼入接入到 3640-1。使用 **ppp authentication chap** 命令配置传入接口。
2. LCP 协商 CHAP 和 MD5。有关如何对此进行确定的详细信息，请参阅了解 debug ppp negotiation 输出。
3. 此呼叫要求 3640-1 向主叫路由器发送 CHAP 质询。

挑战

图3 â CHAP质询数据包被建立

图 3 演示了在 CHAP 身份验证过程中两个路由器之间的以下步骤：

1. 构建的 CHAP 质询数据包具有以下特征：01 = 质询数据包类型标识符。ID = 标识质询的序号。random = 路由器生成的合理随机编号。3640-1 = 质询程序的身份验证名称。

2. 在被叫路由器上保存 ID 和随机值。
3. 将质询数据包发送到主叫路由器。维护未处理的质询的列表。

答复

图4 â 收据和MD5处理从对等体的质询信息包

图 4 演示如何接收和处理 (MD5) 对等体发送的质询数据包。路由器按如下方式处理传入的 CHAP 质询数据包：

1. 向 MD5 散列算法生成器提供 ID 值。
2. 向 MD5 散列算法生成器提供随机值。
3. 使用名称 3640-1 查找口令。路由器在质询中查找与此用户名匹配的条目。在本示例中，路由器查找：`username 3640-1 password pc1`
4. 向 MD5 散列算法生成器提供口令。结果将生成单向 MD5 散列 CHAP 质询，并将此质询发送回 CHAP 响应。

回应（续）

图5 â CHAP响应数据包发送对验证器被建立。

图 5 演示如何构建发送给身份验证程序的 CHAP 响应数据包。此关系图显示了以下步骤：

1. 根据以下组件组合响应数据包：02 = CHAP 响应数据包类型标识符。ID = 从质询数据包复制而得。hash = MD5 散列算法生成器的输出（质询数据包的散列消息）。766-1 = 此设备的身份验证名称。对等体在查找验证身份所需的用户名和口令条目时，将需要使用此名称（验证 CHAP 部分将对此进行详细说明）。
2. 然后，将响应数据包发送给质询程序。

验证 CHAP

此部分提供有关如何验证您的配置的提示。

图6 â 挑战者处理响应数据包

图 6 显示了质询程序如何处理响应数据包。下面给出了（在身份验证程序上）处理 CHAP 响应数据包的相关步骤：

1. 使用 ID 查找原始质询数据包。
2. 向 MD5 散列算法生成器提供 ID。
3. 向 MD5 散列算法生成器提供原始质询随机值。
4. 使用名称 766-1 查找来自以下来源之一的口令：本地用户名和口令数据库。RADIUS 或 TACACS+ 服务器。
5. 向 MD5 散列算法生成器提供口令。
6. 然后，将响应数据包中收到的散列值与计算的 MD5 散列值相比较。如果计算和收到的散列值相等，则 CHAP 身份验证成功。

结果

Figure7 â 成功消息传送到呼叫路由器

图 7 演示如何向主叫路由器发送成功消息。它包括以下步骤：

1. 如果身份验证成功，将根据以下组件构建 CHAP 成功数据包：03 = CHAP 成功消息类型。ID = 从响应数据包中复制而得。â 欢迎inâ 是提供一个用户可读的说明的文本消息。
2. 如果身份验证失败，将根据以下组件构建 CHAP 失败数据包：04 = CHAP 失败消息类型。ID = 从响应数据包中复制而得。â 验证failureâ 或其他文本消息，那提供一个用户可读的说明。
3. 然后，将成功或失败数据包发送到主叫路由器。**注意：** 此示例描述单向身份验证。在双向身份验证中，将重复上述整个过程。但是，主叫路由器将发起初始质询。

CHAP 故障排除

有关如何进行故障排除的信息，请参阅排除 PPP 身份验证故障。

相关信息

- 了解 debug ppp negotiation 输出
- 排查 PPP 身份验证故障
- 使用 ppp chap hostname 和 ppp authentication chap callin 命令的 PPP 认证
- 接入技术支持页面
- 技术支持 - Cisco Systems