在接入服务器上配置基本 AAA

目录

简介

本文档介绍了如何使用 Radius 或 TACACS+ 协议在 Cisco 路由器上配置身份验证、授权和记帐 (AAA)。本文档的目标不是涵盖所有的 AAA 功能，而是对主要的命令加以介绍并提供一些示例和指南。

注意： 在了解 Cisco IOS® 配置前，请阅读关于一般 AAA 配置的部分。如果不这样做，可能导致配置错误并因此锁定。

开始使用前

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

先决条件

有关 AAA 的概述以及 AAA 命令和选项的完整详细信息，请参阅 IOS 12.2 安全配置指南：验证、

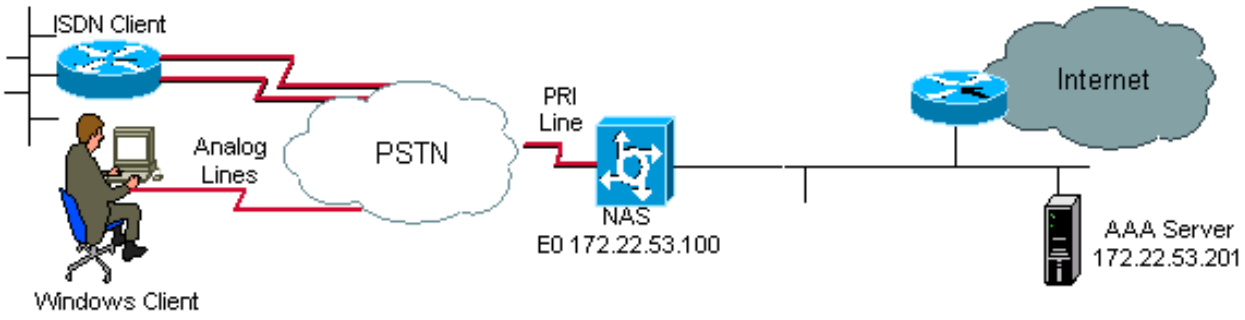
授权和记账。

使用的组件

本文档中的信息基于 Cisco IOS 软件版本 12.1 主线。

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

网络图



一般 AAA 配置

启用 AAA

要启用 AAA，需要在全局配置模式下配置 **aaa new-model** 命令。

注意： 在该命令启用前，其他所有 AAA 命令都是隐藏的。

警告： **aaa new-model** 命令立即对所有线路和接口（控制台线路 **line con 0** 除外）应用本地身份验证。如果启用此命令后向路由器打开了 Telnet 会话（或者在因连接超时而必须重新连接的情况下），用户必须使用路由器的本地数据库进行身份验证。为避免锁定路由器的情况，我们建议您在开始 AAA 配置前先在接入服务器上定义一个用户名和相应的口令。请按如下所示进行操作：

```
Router(config)# username xxx password yyy
```

提示： 在配置 AAA 命令前，先保存您的配置。只有在完成所有 AAA 配置（并对其运行状况感到满意）后，您才能再次保存配置。这样您就可以（在保存配置之前）通过重新加载路由器从意外的锁定状况中恢复过来。

指定外部 AAA 服务器

在全局配置模式下，定义与 AAA 一起使用的安全协议（Radius 和 TACACS+）。如果您不想使用这两种协议，也可以使用路由器上的本地数据库。

如果使用 TACACS+，请发出 **tacacs-server host <IP address of the AAA server> <key>** 命令。

如果使用 Radius，则发出 **radius-server host <IP address of the AAA server> <key>** 命令。

AAA 服务器配置

在 AAA 服务器上，配置以下参数：

- 接入服务器的名称。
- 接入服务器用来与 AAA 服务器通信的 IP 地址。**注意：** 如果两个设备在同一个以太网中，则默认情况下接入服务器在发送 AAA 数据包时会使用以太网接口上定义的 IP 地址。当路由器有多个接口（因此有多个地址）时，这个问题就很重要。
- 在接入服务器中配置的完全一样的密钥 **<key>**。**注意：** 密钥的名称区分大小写。
- 接入服务器使用的协议（TACACS+ 或 Radius）。

有关用于配置上述参数的具体步骤，请参阅 AAA 服务器文档。如果 AAA 服务器配置有误，从 NAS 发出的 AAA 请求将遭到 AAA 服务器的忽略，并且可能无法连接。

AAA 服务器必须拥有一个接入服务器可到达的 IP 地址（执行 **ping** 测试可验证连接）。

配置身份验证

身份验证是在允许用户访问网络和网络服务之前先对其进行验证（通过授权进行检验）。

要配置 AAA 身份验证，请执行以下步骤：

1. 首先，（在全局配置模式下）定义包含身份验证方法的命名列表。
2. （在接口配置模式下）将此列表应用于一个或多个接口。

唯一的例外是默认方法列表（命名为“default”的列表）。默认方法列表自动应用于所有接口，但那些拥有明确定义的命名方法列表的接口除外。定义的方法列表将覆盖默认方法列表。

下面的身份验证示例使用 Radius、登录和点对点协议 (PPP) 身份验证（最常用），解释了方法和命名列表等概念。在所有示例中，均可使用 TACACS+ 替代 Radius 或本地身份验证。

Cisco IOS 软件使用所列出的第一种方法对用户进行身份验证。如果此方法未能响应（通过 ERROR 表明），Cisco IOS 软件将选择方法列表中列出的下一种身份验证方法。此过程将持续下去，直到通过列出的某个验证方法进行了成功的通信或者尝试完列表中定义的所有方法为止。

一定要注意，仅当通过前一种方法未获得任何响应时，Cisco IOS 软件才尝试使用下一种列出的认证方法进行认证。如果在此周期内任意时刻身份验证失败，即 AAA 服务器或本地用户名数据库以拒绝用户访问来作出响应（通过 FAIL 表明），则身份验证进程终止，并且不再尝试其他任何身份验证方法。

要允许用户身份验证，必须在 AAA 服务器上配置用户名和口令。

登录认证

您可以使用 **aaa authentication login** 命令，对希望拥有用于接入服务器（tty、vty、控制台和 aux）的 EXEC 访问权限的用户进行身份验证。

示例 1：依次使用 Radius 和 Local 的 EXEC 访问

```
Router(config)# aaa authentication login default group radius local
```

在上面的命令中：

- 命名列表是默认的列表 (default)。

- 有两种身份验证方法（group radius 和 local）。

所有用户都通过 Radius 服务器（第一种方法）进行身份验证。如果 Radius 服务器不响应，则使用路由器的本地数据库（第二种方法）。对于本地身份验证，需要定义用户名和口令：

```
Router(config)# username xxx password yyy
```

因为我们是在使用 **aaa authentication login** 命令中默认的列表，登录身份验证将自动应用于所有登录连接（例如 tty、vty、控制台和 aux）。

注意： 如果没有 IP 连接、接入服务器未在 AAA 服务器上得到正确的定义或 AAA 服务器未在接入服务器上得到正确的定义，服务器（Radius 或 TACACS+）将不会应答接入服务器发送的 **aaa authentication** 请求。

注意： 仍然使用上面的示例，如果不包括 local 关键字，对应的命令将是：

```
Router(config)# aaa authentication login default group radius
```

注意： 如果 AAA 服务器不应答身份验证请求，身份验证将失败（因为路由器没有可尝试的替代方法）。

注意： **group** 关键字提供了一种对现有服务器主机进行分组的方法。此功能使用户可从配置的服务器主机当中选择一部分主机，将其用于某项特定服务。有关此高级功能的详细信息，请参阅 AAA 服务器组文档。

示例 2：使用线路口令的控制台访问

我们来扩展示例 1 的配置，以便只按照 line con 0 上设置的口令对控制台登录进行身份验证。

这样将定义 CONSOLE 列表，然后应用于 line con 0。

需要进行如下配置：

```
Router(config)# aaa authentication login CONSOLE line
```

在上面的命令中：

- 命名列表是 CONSOLE。
- 只有一种身份验证方法 (line)。

一旦创建了命名列表（在本示例中为 CONSOLE），必须将其应用于线路或接口才能使其生效。通常使用 **login authentication** list_name 来实现这一点：

```
Router(config)# line con 0
Router(config-line)# exec-timeout 0 0
Router(config-line)# password cisco
Router(config-line)# login authentication CONSOLE
```

CONSOLE 列表覆盖 line con 0 中的默认方法列表。您需要输入（在 line con 0 中配置的）口令“cisco”才能获得访问控制台的权限。tty、vty 和 aux 中仍然使用默认列表。

注意： 要采用按照本地用户名和口令进行的控制台访问身份验证，请使用以下命令：

```
Router(config)# aaa authentication login CONSOLE local
```

注意： 这种情况下，用户名和口令必须在路由器的本地数据库中进行配置。列表也必须应用到线路或接口上。

注意： 要取消身份验证，请使用以下命令

```
Router(config)# aaa authentication login CONSOLE none
```

注意： 这种情况下，不对获取控制台访问权限这一活动进行身份验证。列表也必须应用到线路或接口上。

示例 3：使用外部 AAA 服务器的启用模式访问

您可以发起身份验证以便进入启用模式（特权 15）。

需要进行如下配置：

```
Router(config)# aaa authentication enable default group radius enable
```

只需请求口令，用户名为 $enab15$。因此，必须在 AAA 服务器上定义用户名 $enab15$。

如果 Radius 服务器不作应答，则必须输入在路由器上本地配置的启用口令。

PPP 身份验证

aaa authentication ppp 命令用于针对 PPP 连接进行身份验证。它通常用于对希望通过接入服务器访问互联网或中心局的 ISDN 或模拟远程用户进行身份验证。

示例 1：对所有用户都采用一种 PPP 身份验证方法

接入服务器有一个配置为接受 PPP 拨入客户端的 ISDN 接口。我们使用 **dialer rotary-group 0**，但可以在主接口或 Dialer Profile 接口上完成配置。

需要进行如下配置

```
Router(config)# aaa authentication ppp default group radius local
```

此命令使用 Radius 对所有 PPP 用户进行身份验证。如果 Radius 服务器不作应答，则使用本地数据库。

示例 2：使用特定列表进行 PPP 身份验证

要使用命名列表而不用默认列表，请配置以下命令：

```
Router(config)# aaa authentication ppp ISDN_USER group radius Router(config)# int dialer 0
Router(config-if)# pp authentication chap ISDN_USER
```

在本示例中，列表为 ISDN_USER，方法为 Radius。

示例 3：从字符模式会话内部启动 PPP

接入服务器有一个内置调制解调器卡（Mica、Microcom 或 Next Port）。假设配置了 **aaa authentication login** 命令和 **aaa authentication ppp** 命令。

如果某个调制解调器用户首先使用字符模式 EXEC 会话访问路由器（例如，使用 Terminal Window

after Dial），则该用户在 tty 线路上进行身份验证。要启动到数据包模式会话中，用户必须键入 **ppp default** 或 **ppp**。因为已明确配置 PPP 身份验证（使用 **aaa authentication ppp** 命令），所以再次在 PPP 级别对用户进行身份验证。

要避免这种二次身份验证，可使用 **if-needed** 关键字。

```
Router(config)# aaa authentication login default group radius local Router(config)# aaa
authentication ppp default group radius local if-needed
```

注意： 如果客户端直接启动 PPP 会话，PPP 身份验证将直接进行，因为没有对接入服务器进行登录访问。

有关 AAA 身份验证的详细信息，请参阅 IOS 12.2 安全配置指南：配置身份验证和 Cisco AAA 实施案例研究文档。

配置特权

授权是一个控制用户能做什么以及不能做什么的过程。

AAA 授权与身份验证的规则相同：

1. 首先，定义包含授权方法的命名列表。
2. 然后，将此列表应用于一个或多个接口（默认方法列表则例外）。
3. 使用所列出的第一种方法。如果此方法未能响应，则使用第二种方法，依此类推。

方法列表特定于所请求的授权类型。本文档着重介绍“Exec”和“网络”授权类型。

有关其他授权类型的详细信息，请参阅 Cisco IOS 安全配置指南 12.2 版。

Exec 授权

aaa authorization exec 命令确定是否允许用户运行 EXEC shell。通过这种方法可能会返回用户配置文件信息，例如自动命令信息、空闲超时、会话超时、访问列表和特权以及其他一些特定于每位用户的因素。

EXEC 授权只在 vty 和 tty 线路上执行。

以下示例使用 Radius。

示例 1：对所有用户都采用相同的 EXEC 身份验证方法

一旦使用以下命令进行身份验证：

```
Router(config)# aaa authentication login default group radius local
```

对于所有希望登录到接入服务器的用户，都必须使用 Radius（第一种方法）或本地数据库（第二种方法）进行授权。

需要进行如下配置：

```
Router(config)# aaa authorization exec default group radius local
```

注意： 在 AAA 服务器上，必须选择 Service-Type=1 (login)。

注意： 对于此示例，如果不包括 **local** 关键字，并且 AAA 服务器未作响应，将无法进行授权，而且连接也会失败。

注意： 在下面的示例 2 和示例 3 中，无需在路由器上添加任何命令，只需在接入服务器上对配置文件进行配置。

示例 2：从 AAA 服务器指定 EXEC 特权级别

在示例 1 的基础上，如果要允许登录接入服务器的用户直接进入启用模式，请在 AAA 服务器上对以下 Cisco AV 对进行配置：

```
shell:priv-lvl=15
```

这表示用户将直接进入启用模式。

注意： 如果第一种方法未能响应，则使用本地数据库。但是，用户不会直接进入启用模式，必须输入 enable 命令和 **enable** 口令。

示例 3：从 AAA 服务器分配空闲超时

要配置空闲超时（以便在空闲超时的时间过后仍然没有数据流的情况下断开会话的连接），请使用位于用户配置文件下的 IETF Radius 属性 - 28:Idle-Timeout。

网络授权

aaa authorization network 命令对所有网络相关的服务请求（例如 PPP、SLIP 和 ARAP）运行授权。本部分着重介绍最常用的 PPP。

AAA 服务器检查客户端发起的 PPP 会话是否得到了允许。而且，客户端可以请求 PPP 选项：回拨、压缩、IP 地址等。这些选项必须在 AAA 服务器上的用户配置文件中配置。而且，对于具体的客户端，AAA 配置文件可包含将由 Cisco IOS 软件下载并应用于该客户端的属性，例如空闲超时、访问列表及其他特定于每位用户的属性。

以下示例展示了使用 Radius 进行的授权：

示例 1：对所有用户都采用相同的网络授权方法

接入服务器用于接受 PPP 拨入连接。

首先，使用以下命令对用户进行身份验证（按照之前的配置）：

```
Router(config)# aaa authentication ppp default group radius local
```

然后，必须使用以下命令对其进行授权：

```
Router(config)# aaa authorization network default group radius local
```

注意： 在 AAA 服务器上配置：

- Service-Type=7 (framed)

- Framed-Protocol=PPP

示例 2：应用特定于用户的属性

可以使用 AAA 服务器指定特定于每位用户的属性，如 IP 地址、回拨号码、拨号程序空闲超时值或访问列表等。在该实施过程中，NAS 从 AAA 服务器用户配置文件中下载相应的属性。

示例 3：使用特定列表的 PPP 授权

与身份验证类似，我们也可以配置一个命名列表，而不使用默认列表：

```
Router(config)# aaa authorization network ISDN_USER group radius local
```

然后，将此列表应用到接口上：

```
Router(config)# int dialer 0
Router(config-if)# ppp authorization ISDN_USER
```

有关 AAA 身份验证的详细信息，请参阅 IOS 12.2 安全配置指南：配置身份验证和 Cisco AAA 实施案例研究文档。

配置计帐

AAA 记帐功能使您能够跟踪用户访问的服务及其消耗的网络资源量。

AAA 记帐的规则与身份验证及授权的规则相同：

1. 首先，必须定义包含记帐方法的命名列表。
2. 然后，将此列表应用于一个或多个接口（默认方法列表则例外）。
3. 使用所列出的第一种方法；如果此方法未能响应，则使用第二种方法，依此类推。

使用所列出的第一种方法；如果此方法未能响应，则使用第二种方法，依此类推。

- 网络记帐为所有 PPP、Slip 和 AppleTalk 远程访问协议 (ARAP) 会话提供信息：数据包计数、八位字节计数、会话时间、开始和结束时间。
- EXEC 记帐提供关于网络接入服务器的用户 EXEC 终端会话（例如 Telnet 会话）的信息：会话时间、开始和结束时间。

有关其他授权类型的详细信息，请参阅 Cisco IOS 安全配置指南 12.2 版。

以下示例着重介绍如何将信息发送至 AAA 服务器。

配置记帐示例

示例 1：生成开始和结束记帐记录

对于每个拨入 PPP 会话，在客户端通过身份验证后以及断开连接后，会使用 **start-stop** 关键字将记帐信息发送至 AAA 服务器。

```
Router(config)# aaa accounting network default start-stop group radius local
```

示例 2：生成仅结束记帐记录

如果需要仅在客户端断开连接后发送记帐信息，则使用 stop 关键字，并配置以下命令行：

```
Router(config)# aaa accounting network default stop group radius local
```

示例 3：生成关于身份验证和协商失败的资源记录

此时，AAA 记帐为已通过用户身份验证的呼叫提供开始和结束记录支持。

如果身份验证或 PPP 协商失败，则没有身份验证记录。

解决方法是使用 AAA 资源失败结束记帐：

```
Router(config)# aaa accounting send stop-record authentication failure
```

此时将发送结束记录到 AAA 服务器上。

示例 4：启用完全资源记帐

要启用完全资源记帐（在呼叫建立时生成开始记录并在呼叫终止时生成结束记录），请进行如下配置：

```
Router(config)# aaa accounting resource start-stop
```

此命令是在 Cisco IOS 软件版本 12.1(3)T 中引入的。

凭借此命令，呼叫建立和呼叫断开的“开始-停止”记帐记录可对资源与设备的连接进度进行跟踪。独立的用户身份验证“开始-停止”记帐记录将跟踪用户管理进度。这两套记帐记录通过呼叫所拥有的唯一会话 ID 相互关联。

有关 AAA 身份验证的详细信息，请参阅 IOS 12.2 安全配置指南：配置身份验证和 Cisco AAA 实施案例研究文档。

相关信息

- 技术支持 - Cisco Systems