
实达网络锐捷

配置基于 802.1X 的 AAA 服务

本章节描述基于 802.1x 的 AAA 服务的配置相关内容。802.1x 用于控制用户对网络访问的认证，并对其提供授权与记帐功能。

本节包含如下内容：

⚠注意 有关本节引用的 CLI 命令的详细使用信息及说明，请参照 CLI 命令集

概述

IEEE 802 LAN 中，用户只要能接到网络设备上，不需要经过认证和授权即可直接使用。这样，一个未经授权的用户，他可以没有任何阻碍地通过连接到局域网的设备进入网络。随着局域网技术的广泛应用，特别是在运营网络的出现，对网络的安全认证的需求已经提到了议事日程上。如何在以太网技术简单、廉价的组网特点的基础上，提供用户对网络或设备访问合法性认证的手段，已经成为业界关注的焦点。IEEE 802.1x 协议正是在这样的背景下提出的。

IEEE802.1x（Port-Based Network Access Control）是一个基于端口的网络存取控制标准，为LAN接入提供点对点式的安全接入。这是IEEE标准委员会针对以太网的安全缺陷而专门制定的标准，能够在利用IEEE 802 LAN的优势基础上，提供一种对连接到局域网设备或用户进行认证的手段。

IEEE 802.1x 标准定义了一种基于“客户端——服务器”（Client-Server）模式实现了限制未认证用户对网络的访问。客户端要访问网络必须先通过认证服务器的认证。

在客户端通过认证之前，只有EAPOL报文（Extensible Authentication Protocol over LAN）可以在网络上通行。在认证成功之后，通常的数据流便可在网络上通行。

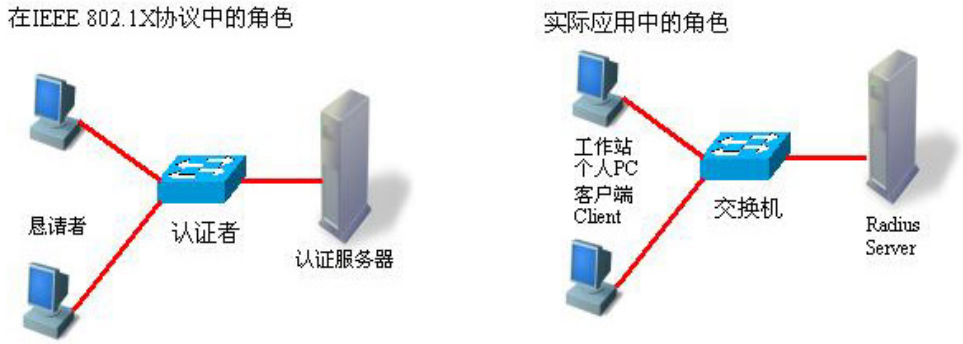
应用802.1x我们的交换机提供了Authentication，Authorization，and Accounting三种安全功能，简称AAA。

Authentication：认证，用于判定用户是否可以获得访问权，限制非法用户
Authorization：授权，授权用户可以使用哪些服务，控制合法用户的权限
Accounting：计账，记录用户使用网络资源的情况；为收费提供依据

我们将从以下几个方面阐述 802.1x

设备的角色

IEEE802.1x 标准认证体系由**恳请者、认证者、认证服务器**三个角色构成，在实际应用中，三者分别对应为：工作站（Client）、交换机(network access server，NAS)、Radius-Server。



恳请者 是最终用户所扮演的角色，一般是个人 PC。它请求对网络服务的访问，并对认证者的请求报文进行应答。恳请者必须运行符合 IEEE 802.1x 客户端标准的软件，目前最典型的就是 Windows XP 操作系统自带的 IEEE802.1x 客户端支持，另外，我们公司也已推出符合该客户端标准的 STAR Supplicant 软件。

认证者 一般为交换机等接入设备。该设备的职责是根据客户端当前的认证状态控制其与网络的连接状态。在客户端与服务器之间，该设备扮演着中介者的角色：从客户端要求用户名，核实从服务器端的认证信息，并且转发给客户端。因此，交换机除了扮演 IEEE802.1x 的认证者的角色，还扮演 RADIUS Client 角色，因此我们把交换机称作 network access server(NAS)，它要负责把从客户端收到的回应封装到 RADIUS 格式的报文并转发给 RADIUS Server，同时它要把从 RADIUS Server 收到的信息解释出来并转发给客户端。

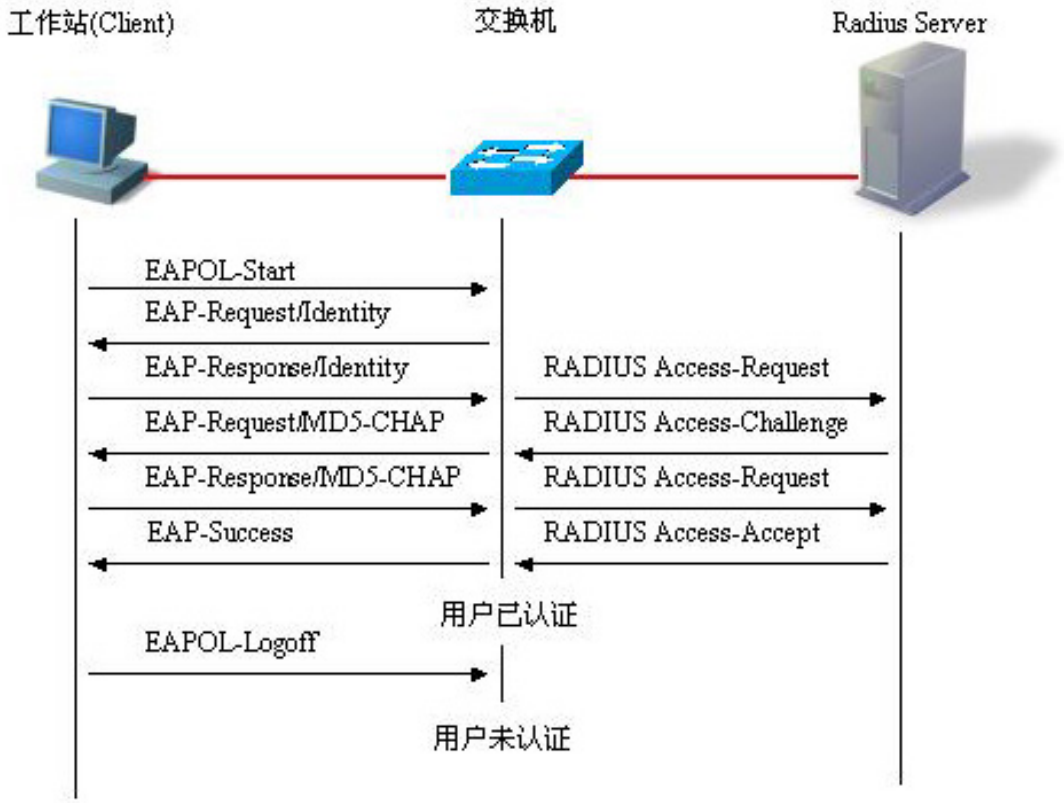
扮演认证者角色的设备有两种类型的端口：受控端口（controlled Port）和非受控端口（uncontrolled Port）。连接在受控端口的用户只有通过认证才能访问网络资源；而连接在非受控端口的用户无须经过认证便可以直接访问网络资源。我们把用户连接在受控端口上，便可以实现对用户的控制；非受控端口主要是用来连接认证服务器，以便保证服务器与交换机的正常通讯。

认证服务器 通常为 RADIUS 服务器，认证过程中与认证者配合，为用户提供认证服务。认证服务器保存了用户名及密码，以及相应的授权信息，一台服务器可以对多台认证者提供认证服务，这样就可以实现对用户的集中管理。认证服务器还负责管理从认证者发来的记帐数据。实达网络科技公司实现的 802.1x 的设备完全兼容标准的 Radius Server，如 MicroSoft win2000 Server 自带的 Radius Server 及 Linux 下的 Free Radius Server。

认证的发起及认证过程中的报文交互

恳请者和认证者之间通过 EAPOL 协议交换信息，而认证者和认证服务器通过 RADIUS 协议交换信息，通过这种转换完成认证过程。EAPOL 协议封装于 MAC 层之上，类型号为 0x888E。同时，标准为该协议申请了一个组播 MAC 地址 01-80-C2-00-00-03，用于初始认证过程中的报文传递。

下图是一次典型的认证过程中，三个角色设备的报文交互过程



该过程是一个典型的由用户发起的认证过程（在一些特殊的情形下，交换机也可能主动发出认证请求，过程与该图一致，只是少了用户主动发出请求这一步）。

已认证用户及未认证用户的状态

802.1x 中根据端口的认证状态来决定该端口上的用户是否允许访问网络，由于我们对 802.1X 进行扩展，是基于用户的，所以，我们是根据一个端口下的用户的认证状态来决定该用户是否允许访问网络资源。一个非受控端口下的所有用户均可使用网络资源，而一个受控端口

下的用户只有处于已认证状态（Authorized）才能访问网络资源。一个用户刚发起认证时，状态处于未认证状态（unauthorized），这时它不能访问网络，在认证通过后，该用户的状态会变为已认证状态（authorized），此时该用户便可以使用网络资源。

如果工作站不支持 802.1x，而该机器连接在受控端口下，当交换机请求该用户的用户名时，由于工作站不支持所以没对该请求做出响应，那么，该用户仍然处于未认证状态（unauthorized），该用户不能访问网络资源。

相反地，如果工作站支持 802.1x，而所连的交换机不支持 802.1x。用户发出的 EAPOL-START 帧无人响应，用户在发送一定数目的 EAPOL-START 帧仍未收到回应的情形下，将认为自己所连的端口是非受控端口，而直接使用网络资源。

在支持 802.1x 的设备下，所有的端口的默认设置是非受控端口，我们可以把一个端口设置成受控端口，从而要求这个端口下的所有用户进行认证。

当用户通过了认证（交换机收到了从 RADIUS Server 服务器发来的成功报文），该用户便转变成已认证状态(authorized)，该用户可以自由使用网络资源。如果，用户认证失败，该用户仍然处于未认证状态，但该用户可以重新发起认证。如果交换机与 RADIUS server 之间的通讯有故障，那么该用户仍然处于未认证状态（unauthorized），网络对该用户来说仍然是不可使用的。

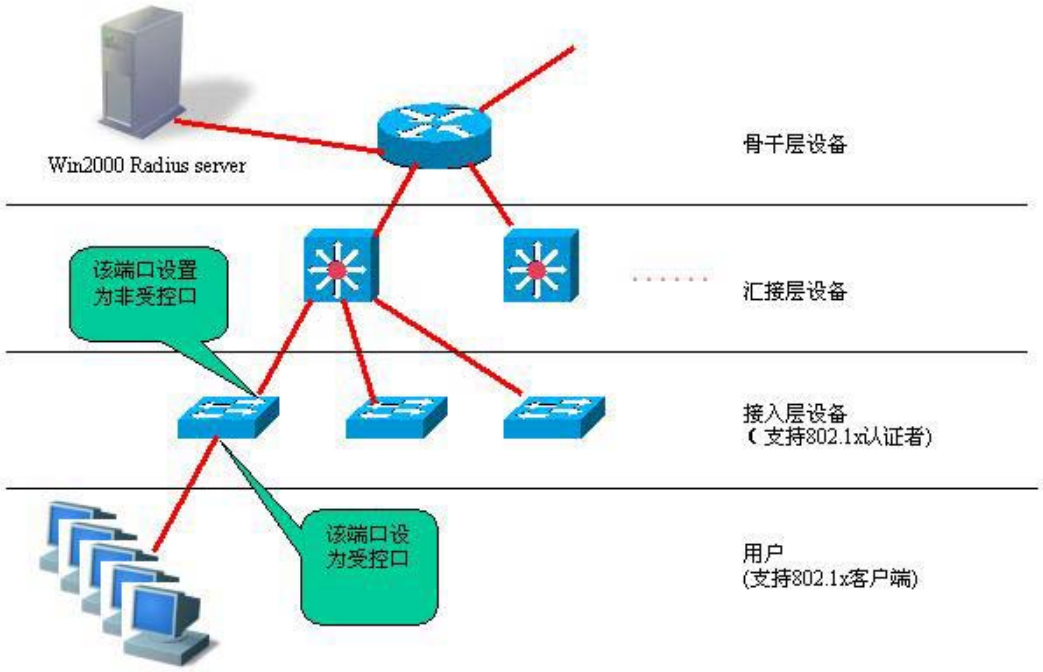
当用户发出 EAPOL-LOGOFF 报文后，该用户的状态由已认证(authorized)转向未认证状态(unauthorized)。

当交换机的某个端口变为 LINK-DOWN 状态，该端口上的所有用户均变为未认证(unauthorized)状态。

当交换机重新启动，该交换机上的所有用户均变为未认证状态(unauthorized)。

典型应用的拓扑结构

A、带 802.1x 的设备作为接入层设备



该方案的说明：

该方案的要求：

1、用户支持 802.1x，即要装有 802.1x 的客户端软件（windowXp 自带，Star-supplicant 或其他符合 IEEE802.1x 标准的客户端软件）。

2、接入层设备支持 IEEE 802.1x

3、有一台（或多台）支持标准 RADIUS 的服务器作为认证服务器

该方案的配置要点：

1、 与 Radius Server 相连的口及上联口，配置成**非受控口**，以便交换机能正常地与服务器进行通讯，以及使已认证用户能通过上联口访问网络资源

2、 与用户连接的端口要设置为**受控口**，以实现对接入用户的控制，用户必须通过认证才能访问网络资源。

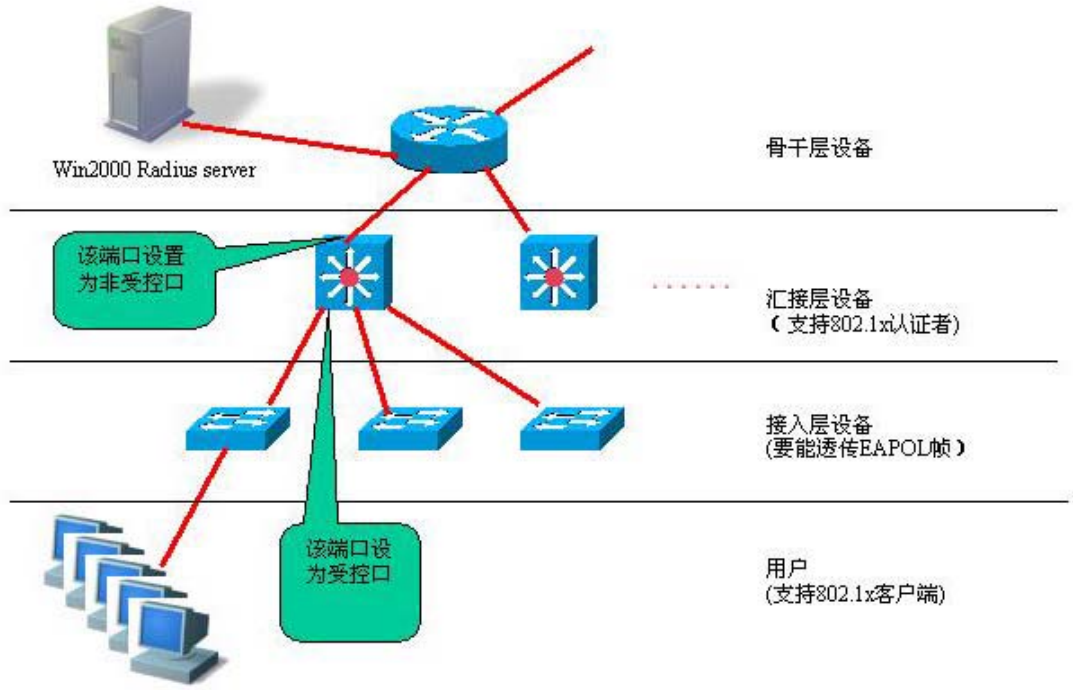
该方案的特点：

1、每台支持 802.1x 的交换机所负责的客户端少，认证速度快。各台交换机之间相互独立，交换机的重起等操作不会影响到其它交换机所连接的用户。

2、用户的管理集中于 Radius Server 上，管理员不必考虑用户连接在哪台交换机上，便于管理员的管理

3、管理员可以通过网络管理到接入层的设备

B、带 802.1x 的设备作为汇接层设备



该方案的说明：

该方案的要求：

1、用户支持 802.1x，即要装有 802.1x 的客户端软件（windowXp 自带，Star-supplicant 或其他符合 IEEE802.1x 标准的客户端软件）。

2、接入层设备支持要能透传 IEEE 802.1x 帧(EAPOL)

3、汇接层设备支持 802.1x（扮演认证者角色）

4、有一台（或多台）支持标准 RADIUS 的服务器作为认证服务器

该方案的配置要点：

1、与 Radius Server 相连的口及上联口，配置成**非受控口**，以便交换机能正常地与服务器进行通讯，以及使已认证用户能通过上联口访问网络资源

2、与接入层交换机连接的端口要设置为**受控口**，以实现对接入用户的控制，用户必须通过认证才能访问网络资源。

该方案的特点：

1、由于是汇接层设备，网络规模大，下接用户数多，对设备的要求高，因为若该层设备发生故障，将导致大量用户不能正常访问网络。

2、用户的管理集中于 Radius Server 上，管理员不比考虑用户连接在哪台交换机上，便于管理员的管理

3、接入层设备可以使用较廉价的非网管型交换机（只要支持 EAPOL 帧透传）

4、管理员不能通过网络直接管理到接入层设备

配置 802.1x

我们将以以下章节说明如何配置 802.1x

802.1x 的默认配置

下表列出 802.1x 的一些缺省值

内容	默认值
认证 Authentication	关闭 DISABLE
记帐 Accounting	关闭 DISABLE
认证服务器(Radius Server) *服务器 IP 地址(ServerIp) *认证 UDP 端口 *密码(Key)	 *无缺省值 *1812 *无缺省值
记帐服务器(Accounting Server) *记帐服务器 IP 地址 *记帐 UDP 端口	 *无缺省值 1813
所有端口的类型	非受控端口（所有端口均无须认证便可直接通讯）
定时重认证 re-authentication	打开
定时重认证周期 reauth_period	3600 秒
认证失败后允许再次认证的间隔	5
重传时间间隔	30 秒

最大重传次数	2 次
客户端超时时间	30 秒，在该段时间内没有收到客户端的响应便认为这次通讯失败
服务器超时时间	30 秒，在该段时间内没有收到服务器的回应，便认为这次通讯失败
某端口下可认证主机列表	无缺省值

802.1x 的配置注意事项

只有支持 802.1x 的产品，才能进行以下设置。
802.1x 既可以在二层下又可以在三层下的设备运行。
要先设置认证服务器的 IP 地址，才能打开 1X 认证。
打开端口安全的端口不允许打开 1X 认证。
Aggregate Port 不允许打开 1X 认证。

配置交换机与 RADIUS SERVER 之间的通讯

Radius Server 维护了所有用户的信息：用户名、密码、该用户的授权信息以及该用户的记帐信息。所有的用户集中于 Radius Server 管理，而不必分散于每台交换机，便于管理员对用户的集中管理。

交换机要能正常地与 RADIUS SERVER 通讯，必须进行如下设置：

Radius Server 端：要注册一个 Radius Client。注册时要告知 Radius Server 交换机的 IP、认证的 UDP 端口（若记帐还要添记帐的 UDP 端口）、交换机与 Radius Server 通讯的约定密码，还要选上对该 Client 支持 EAP 扩展认证方式）。对于，如何在 Radius Server 上注册一个 Radius Client，不同软件的设置方式不同，请查阅相关的文档。

交换机端：为了让交换机能与 Server 进行通讯，交换机端要做如下的设置：设置 Radius Server 的 IP 地址，认证（记帐）的 UDP 端口，与服务器通讯的约定密码。

在特权模式下，按如下步骤设置交换机与 Radius Server 之间的通讯：

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	radius-server host *ip-address*	设置 Radius Server IP 地址。
步骤 3	radius-server auth-port *port-number*	(optional)设置 Radius Server 认证 UDP 端口。
步骤 4	radius-server key *string*	设置 Radius Server 认证密码。
步骤 5	end	退回到特权模式。
步骤 6	write memory	保存配置。
步骤 7	show radius-server	查看 Radius Server 设置。

使用 no radius-server auth-port 命令将 Radius Server 认证 UDP 端口恢复为缺省值。使用

no radius-server key 命令删除 Radius Server 认证密码。以下例子是设置 Server Ip 为 192.1.1.1、认证 Udp 端口为 600、以明文方式设置约定密码：

```
Switch#configure terminal
Switch(config)#radius-server host 192.1.1.1
Switch(config)#radius-server auth-port 600
Switch(config)#radius-server key MsdadShaAdasdj878dajL6g6ga
Switch(config)#end
```

注意 1、官方约定的认证的 UDP 端口为 1812

2、官方约定的记帐的 UDP 端口为 1813

3、交换机与 Radius Server 约定的密码的长度建议不少于 16 个字符

4、交换机与 Radius Server 连接的端口要设置成非受控口

设置 802.1X 认证的开关

当打开 802.1x 认证时，交换机会主动要求受控端口上的主机进行认证，认证不过的主机不允许访问网络。

在特权模式下，按如下步骤打开 1x 认证：

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	aaa authentication dot1x	打开 802.1x 认证功能
步骤 3	end	退回到特权模式。
步骤 4	write memory	保存配置。
步骤 5	show dot1x	查看 802.1x 配置。

使用 no aaa authentication dot1x 命令关闭 802.1x 认证功能。以下例子是打开 802.1x 认证：

```
Switch#configure terminal
Switch(config)#aaa authentication dot1x
Switch(config)#end
```

注意 打开 802.1x 之前要先配置 Radius Server 的 IP 地址，并确保交换机与 Radius Server 之间的通讯正常。若没有 Radius Server 的配合，交换机无法完成认证功能。如何设置 Radius Server 与交换机之间的通讯请见上一章节。

打开/关闭一个端口的认证

在 802.1x 打开的情形下，打开一个端口的认证，则该端口成为受控口,连接在该端口下的用户要通过认证才能访问网络，然而，在非受控端口下的用户可以直接访问网络。

在特权模式下，按如下步骤设置一个端口的认证状态。

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	interface *interface-id*	进入接口设置模式,指定要配置的 Interface
步骤 3	dot1x port-control auto	设置该接口为受控接口（打开接口认证功能）。使用该命令的 no 选项关闭该接口的认证功能。
步骤 4	end	退回到特权模式。
步骤 5	copy running-config startup-config	保存配置。
步骤 6	show dot1x port-control	查看 802.1x 接口认证状态配置。

使用该命令的 no dot1x port-control 命令关闭接口的认证功能。以下例子是设置以太网接口 1/1 为受倥接口：

```
Switch#configure terminal
Switch(config)#interface f 1/1
Switch(config-if)#dot1x port-control auto
Switch(config)#end
```

打开定时重认证

802.1x 能定时主动要求用户重新认证，这样可以防止已通过认证的用户不再使用后被其他用户冒用，还可以检测用户是否断线，使记费更准确。除了可以设定重认证的开关，我们还可以定义重认证的间隔。默认的重认证间隔是 3600 秒。在根据时长进行记费的场合下，要根据具体的网络规模确定重认证间隔，使之既有足够时间完成一次认证又尽可能精确。

在特权模式下，按如下步骤打开/关闭重认证状态，并且设置重认证时间间隔。

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	dot1x re-authentication	打开定时重认证功能。
步骤 3	dot1x timeout re-authperiod *seconds*	设置重认证时间间隔。
步骤 4	end	退回到特权模式。
步骤 5	write memory	保存配置。
步骤 6	show dot1x	查看 802.1x 配置。

使用 no dot1x re-authentication 命令关闭定时重认证功能，使用 no dot1x timeout re-authperiod 命令将重认证时间间隔恢复为缺省值。以下例子是打开定时重认证功能，并设

置重认证时间间隔为 1000 秒：

```
Switch#configure terminal
Switch(config)#dot1x re-authentication
Switch(config)#dot1x timeout re-authperiod 1000
Switch(config)#end
```

注意 若打开重认证，请注意重认证间隔的合理性。要根据具体的网络规模而设置。

改变 QUIET 时间

当用户认证失败时，交换机将等待一段时间后，才允许用户再次认证。Quiet Period 的时间长度便是允许再认证间隔。该值的作用是避免交换机受恶意攻击。Quiet Period 的默认间隔为 5 秒，我们可以通过设定较短的 Quiet Period 使用户可以更快地进行再认证。

在特权模式下，按如下步骤设置Quiet Period的值

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	dot1x timeout quiet-period *seconds*	设置 Quiet Period 值。
步骤 3	end	退回到特权模式。
步骤 4	write memory	保存配置。
步骤 5	show dot1x	查看 802.1x 配置。

使用 no dot1x timeout quiet-period 命令将 Quiet Period 恢复为缺省值。以下例子是设置 Quiet Period 值 500 秒：

```
Switch#configure terminal
Switch(config)#dot1x timeout quiet-period 500
Switch(config)#end
```

设置报文重传间隔

交换机发EAP-request/identity之后，若在一定的时间内没有收到用户的回应，交换机将重传这个报文。该值的默认值为30秒，要根据具体的网络规模进行调整。

在特权模式下，按如下步骤设置报文重传间隔

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	dot1x timeout tx-period *seconds*	设置报文重传间隔，

步骤 3	end	退回到特权模式。
步骤 4	write memory	保存配置。
步骤 5	show dot1x	查看 802.1x 配置。

使用 no dot1x timeout tx-period 命令将报文重传间隔恢复为缺省值。以下例子是设置报文重传间隔为 100 秒：

```
Switch#configure terminal
Switch(config)#dot1x timeout tx-period 100
Switch(config)#end
```

设置最大请求次数

交换机朝 RadiusServer 发出认证请求后,若在 ServerTimeout 时间内没收到 Radius Server 的回应，将重传该报文。最大请求次数指的是交换机重传请求的最大数，超过该次数交换机将认为本次认证失败。默认的重传次数为 2 次，我们要根据具体的网络环境进行调整。

在特权模式下，按如下步骤设置报文重传次数

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	dot1x max-req *count*	设置报文重传次数。
步骤 3	End	退回到特权模式。
步骤 4	write memory	保存配置。
步骤 5	show dot1x	查看 802.1x 配置。

使用 no dot1x max-req 命令将报文重传次数恢复为缺省值。以下例子是设置报文重传次数为 5 次：

```
Switch#configure terminal
Switch(config)#dot1x max-req 5
Switch(config)#end
```

设置最大重认证次数

当用户认证失败后，交换机会尝试几次与用户的认证。在认证次数超过最大重认证次数之后，交换机就认为这个用户已经断线，结束认证过程。系统默认的次数是 2 次，我们可以重新设置这个值。

在特权模式下，按如下步骤设置最大重认证次数：

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	Dot1x reauth-max *count*	设置最大重认证次数。
步骤 3	End	退回到特权模式。
步骤 4	write memory	保存配置。
步骤 5	show dot1x	查看 802.1x 配置。

使用 no dot1x reauth-max 命令将最大重认证次数恢复为缺省值。以下例子是设置最大重认证次数为 3 次：

```
Switch#configure terminal
Switch(config)#dot1x reauth-max 3
Switch(config)#end
```

设置 Server-timeout

该值指的是 Radius Server 的最大响应时间，若在该时间内，交换机没有收到 Radius Server 的响应，将认为本次认证失败。

在特权模式下，按如下步骤设置 Server-timeout、恢复为默认值

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	dot1x timeout server-timeout *seconds*	设置 Radius Server 最大响应时间，使用该命令的no选项将其恢复为缺省值。
步骤 3	End	退回到特权模式。
步骤 4	copy running-config startup-config	保存配置。
步骤 5	show dot1x	查看 802.1x 配置。

把所有的参数设置成默认值

把 802.1x 的所有参数设置成默认值，设置后的结果见 802。1X 的默认值。

在特权模式下，如下操作把所有参数设置成默认值

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	dot1x default	把所有参数设置成默认值。
步骤 3	End	退回到特权模式。
步骤 4	copy running-config startup-config	保存配置。
步骤 5	show dot1x	查看 802.1x 配置。

以下例子是把所有参数设置成默认值：

```
Switch#configure terminal
Switch(config)#dot1x default
Switch(config)#end
```

配置 802.1x 记帐

实达网络公司的 802.1x 实现了记帐功能。该记帐是基于时长的，也就是说 802.1x 记录了

用户第一次认证通过到用户主动退出或交换机检测到用户中断的时间长度。

在用户第一次认证通过之后，交换机会向服务器发一个记帐开始请求，当用户主动离线或交换机检测到用户已离线或用户的物理连接已中断，交换机将向服务器发一个记帐结束请求。Radius Server 将会把这些信息记录在 Radius Server 的数据库上。网管便可以根据这些信息提供记帐的依据。

实达网络公司的 802.1x 十分重视记帐的可靠性，为了避免记帐服务器的意外情况，特别支持记帐备份服务器。当一个服务器由于各种原因而不能提供记帐服务，交换机将自动把记帐信息转发给另一台备份服务器，这大大提高了记帐可靠性。

在用户主动退出的情形下，记帐的时长是精确的；在用户意外中断的情形下，用户记帐的精度以重认证的间隔为准（交换机通过重认证检测一个用户是否意外中断）。

要打开交换机的记帐工作需对交换机做如下的设置：

1、在 Radius Server 注册这台交换机为 Radius Client，如认证时的操作

2、设置记帐服务器的 IP 地址

3、设置记帐的 UDP 端口

4、在 802.1x 打开的前提下，打开记帐服务

在特权模式下，按如下步骤设置记帐服务

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	aaa accounting server *ip-address* [backup]	设置记帐服务器或备份记帐服务器的 IP 地址。
步骤 3	aaa accounting acc-port *acc-port*	设置记帐服务器的 UDP 端口。
步骤 4	aaa accounting	打开 802.1x 记帐功能。
步骤 5	end	退回到特权模式。
步骤 6	write memory	保存配置。
步骤 7	show accounting	查看记帐功能配置。
步骤 7	show accounting	查看记帐功能配置。

使用 no aaa accounting acc-port 命令的将记帐服务器的 UDP 端口恢复为缺省值，使用 no aaa accounting 命令关闭记帐功能。以下例子是设置记帐服务器的 IP 地址为 192.1.1.1、设置备份记帐服务器的 IP 地址为 192.1.1.2、设置记帐服务器的 UDP 端口为 1200、打开 802.1x 记帐功能：

```
Switch#configure terminal
Switch(config)#aaa accounting server 192.1.1.1
Switch(config)#aaa accounting server 192.1.1.2 backup
Switch(config)#aaa accounting acc-port 1200
Switch(config)#aaa accounting
Switch(config)#end
```

注意 1、与 Radius Server 的约定记帐密码与认证相同

2、必须在 802.1x 打开的前提下才能打开记帐

3、802.1x 的记帐功能在默认的情形下是关闭的

4、记帐的数据库格式请见相关的 Radius Server 文档

实达网络产品特有的功能

为了方便宽带运营商及其他特殊场合的用途，实达对 802.1x 的功能在标准的基础上进行了扩展（该扩展是完全基于标准之上，没有任何的与 IEEE 802.1x 不兼容）。

配置 IP 授权模式

实达网络实现的 802.1x，可以强制要求已认证的用户使用固定的 IP。管理员通过配置 IP 授权模式来限定用户获得 IP 地址的方式。IP 授权模式有三种：DISABLE 模式、DHCP SERVER 模式、RADIUS SERVER 模式。下面分别介绍这三种工作模式的特性：

DISABLE 模式（默认）：在该模式下，交换机不对用户的 IP 做限制，用户只需认证通过便可以使用网络。

DHCP SERVER 模式：用户的 IP 通过指定的 DHCP SERVER 获得，只有指定的 DHCP SERVER 分配的 IP 才是合法的 IP。

RADIUS SERVER 模式：用户的 IP 通过 RADIUS SERVER 指定。用户只能用 RADIUS SERVER 指定的 IP 访问网络。

三种模式下的应用模型：

DISABLE 模式：适合不对用户限定 IP 的场合。用户只需通过认证便可以访问网络。

DHCP SERVER 模式：用户 PC 通过 DHCP 获得 IP 地址，管理员通过配置交换机的 DHCP RELAY 来限定用户访问的 DHCP SERVER，这样，只有指定的 DHCP SERVER 分配的 IP 才是合法的。

RADIUS SERVER 模式：用户 PC 使用固定的 IP，RADIUS SERVER 配置了<用户—IP>的对应关系，并通过 RADIUS 的 Framed-IP-Address 属性告知交换机，用户只能用该 IP 才能访问网络。

在特权模式下，如下配置 IP 授权模式：

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	aaa authorization ip-auth-mode {disabled | dhcp-server | radius-server}	配置 IP 授权模式
步骤 3	end	退回到特权模式
步骤 4	Show ip_auth_mode	查看当前的 IP 授权模式
步骤 5	write memory	保存配置

以下例子是把配置 IP 授权模式为 DHCP-SERVER 模式：

```
Switch#configure terminal
Switch(config)# aaa authorization ip-auth-mode dhcp-server
Switch(config)#end
```

发布广告信息

实达网络实现的 802.1x，可以在 Radius Server 端配置 Reply-Message 字段，当认证成功后，该字段的信息可以在实达网络推出的 802.1x 客户端 Star-Supplicant 上显示出来，便于运营商发布一些信息。

该消息只有在用户第一次认证时显示，重认证时，不会显示，这样就避免了对用户的频繁打扰。

广告信息的显示窗口支持 html，会自动把消息中的 http://XXX.XXX.XX 转换成可直接跳转的连接，便于用户查看详细的信息。

广告信息的发布：

1、运行商在 Radius Server 端，配置 Reply Message 属性的内容

⚠注意 1、只有实达的客户端 Star-supplicant 才支持（对本公司交换机的用户免费），其它的客户端看不到信息但不影响使用

2、在交换机端无需设置

某端口下的可认证主机列表

为了增强 802.1x 的安全性，我们在不影响 IEEE 802.1x 的基础上进行了扩展，网管可以限定某个端口的认证的主机列表。如果一个端口下的可认证主机列表为空，则任何用户均可认证；若可认证主机列表不为空，那么只有列表中的主机允许认证。允许认证的主机用 MAC 标识。

添加某一端口下的可认证主机、删除某一端口下的可认证主机

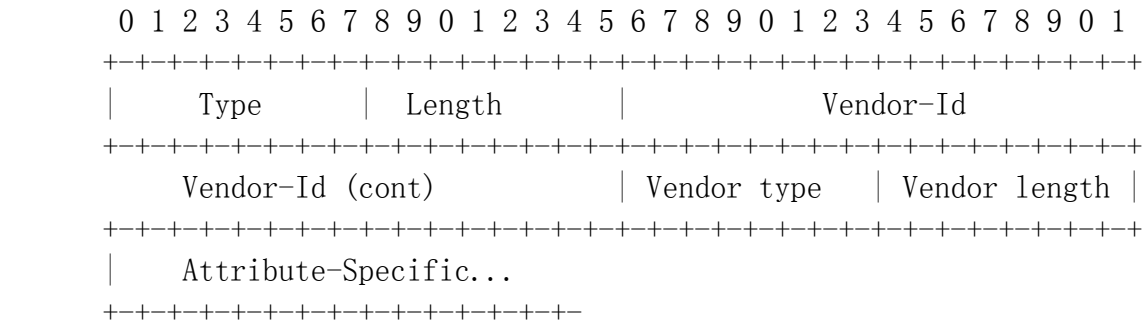
	命令	含义
步骤 1	dot1x auth-address-table address *mac-address* interface *interface-id*	设置可认证主机列表。

⚠注意 若主机列表为空，该端口允许任何主机认证

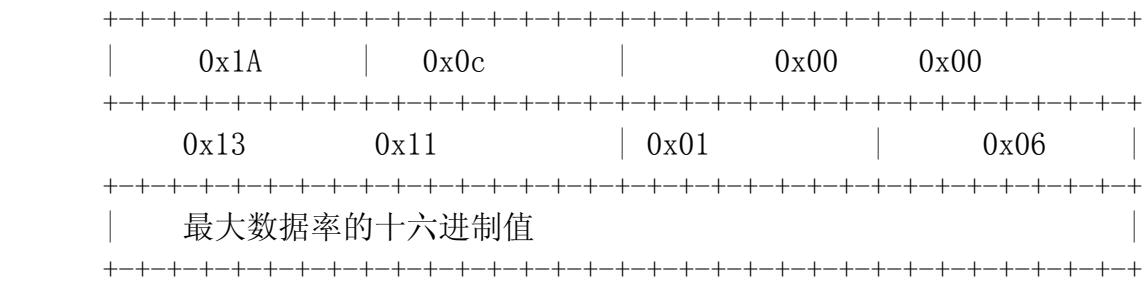
授权

为了方便运营商，我们的产品可以对不同类型的用户提供不同质量的服务，如：提供给用户的最大带宽不同。而这些信息集中于 Radius Server 上，管理员不必对每台交换机进行配置。

由于 Radius 没有标准的属性来表示最大数据率。我们只能通过厂商自定义属性来传递授权信息。我们定义的通用格式如下：

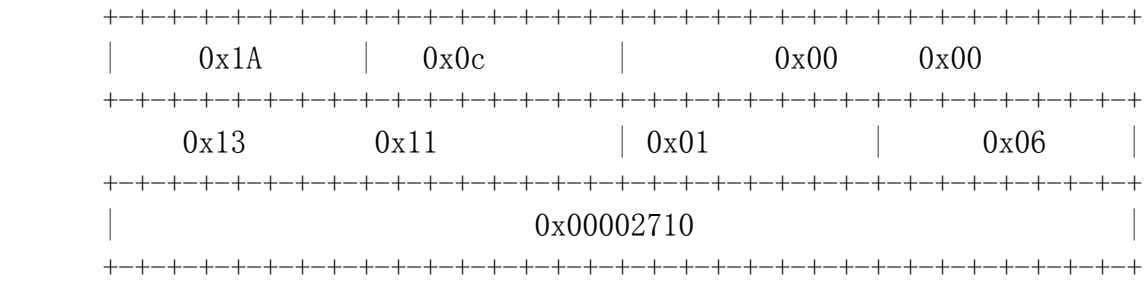


对于最大数据率应填的值如下：



最大数据率的单位：kbps

对于最大数据率为 10M 的用户应填如下：



自定义的头照上填，最大数据率为 10M，即 10000kbsp，转换成 16 进制则 0x00002710，填在相应的字段上即可。

⚠注意 该功能无须设置交换机端。只要交换机端支持授权便可。

配置备份认证服务器

我们的基于 802.1x 认证系统，可以支持备份服务器。当主服务器因各种原因当机之后，交换机将自动向备份服务器提交认证请求。

在特权模式下，我们按如下方式设置备份认证服务器。

	命令	含义
步骤 1	configure terminal	进入特权模式。
步骤 2	radius-server host *ip-address* backup	配置备份认证服务器
步骤 3	End	退回到特权模式
步骤 4	Show radius-server	查看当前的认证模式
步骤 5	write memory	保存配置

以下例子是配置 192.1.1.1 为备份服务器的例子：

Switch#configure terminal

Switch(config)#**radius-server host** 192.1.1.1 **backup**

Switch(config)#end

对在线用户的配置及管理

实达交换机提供了通过 snmp 对已认证用户进行管理的功能。管理员可以通过 snmp 查看已认证用户的信息，还可以强制使一个用户下线。被强制下线的用户必须再次认证才能使用网络资源。

该功能无须配置交换机。

实现用户与 IP 的捆绑

用实达网络公司提供的客户端，以及对 Radius Server 的正确配置，可以实现用户与 IP 的唯一绑定。某个用户必须以管理员分配的 IP 进行认证，否则将不能认证成功。

该功能无须配置交换机，用户需用实达网络公司提供的客户端软件，管理员需配置 Radius Server。

基于端口的流量记费

实达网络交换机除了提供针对时长的记费外，在交换机的每个端口只接入一个用户的情形下，交换机还可以提供针对流量的记费功能。

该功能无须配置交换机，但需 Radius server 支持。

查看 802.1x 的配置及当前的统计值

本公司实现的 802.1X 可以查看丰富的状态机信息，为网管提供了强有力的管理依据，便于管理员对用户状态的时时监控，且方便解决故障。

查看 Radius 认证及记帐相关配置

用 **show radius-server** 命令查看 Radius Server 的相关配置，用 **show accounting** 查看记帐相关配置

```
Switch#sh radius-server
Radius server    : 0.0.0.0
Authentication UDP port    : 1812

Switch#show accounting
Accounting status           : Disabled
Accounting server           : 0.0.0.0
Accounting backup server    : 0.0.0.0
Accounting UDP port         : 1813
```

查看当前的用户数

本公司实现的 802.1X 可以查看两类当前的用户数，一是当前用户数，二是已认证用户数。当前用户数指的是当前认证用户总数（无论是否认证成功）；已认证用户数，指的是已认证通过的用户的总数。

在特权模式下，按如下步骤查看当前用户数及已认证用户数

	命令	含义
步骤 1	show dot1x	查看 802.1x 配置，包括当前用户数和

	已认证用户数。

以下例子是查看 802.1x 配置：

```
Switch#show dot1x
IEEE 802.1X Status    : Enabled
Authentication user number : 0
Current user number       : 0

reauth-enabled    : Disabled
reauth-period     : 3600 s
quiet-period      : 60 s
tx-period         : 30 s
supp-timeout      : 30 s
server-timeout    : 30 s
reauth-max        : 2 s
max-req           : 2 s
```

查看可认证地址列表

本公司实现的 802.1x，对功能进行了扩展，可以设置在某些端口上只有哪些主机可以认证。查看可认证主机列表功能，可以让管理员查看目前已有的设置。

在特权模式下，按如下操作查看可认证主机列表

	命令	含义
步骤 1	dot1x auth-address-table address *mac-address* interface *interface-id*	设置可认证主机列表。
步骤 2	show dot1x auth-address-table	查看可认证主机列表。

使用 no dot1x auth-address-table address *mac-address* interface *interface-id* 命令删除指定的可认证主机列表。以下例子是查看可认证主机列表：

```
Switch#show dot1x auth-address-table
Interface          Address
-----------------  --------------------
 Ethernet1/2       00-D0-F8-11-22-33
```

查看用户认证状态信息

管理员可能查看本交换机的当前用户的认证状态，便于排解故障。

在特权模式下，按如下操作查看用户认证状态信息

	命令	含义
步骤 1	show dot1x summary	查看用户认证状态信息。
步骤 2	show dot1x statistics	查看用户认证工作统计信息。

以下例子是查看用户认证状态信息：

```
Switch#show dot1x summary
Vlan  Address           PaeState        BackendAuth    KeyTx
----  ----------------  --------------  -----------    --------
1     00D0F8000001       Authened        IDLE          DISABLE
```

以下例子是查看用户认证工作统计信息：

```
Switch#show dot1x statistics
```

敏锐把握应用趋势、快捷满足客户需求