目 录

1 MAC地址认证典型配置举例 1-1
1.1 简介 1-1
1.2 使用限制 1-1
1.3 MAC地址本地认证典型配置举例 1-1
1.3.1 适用产品和版本 1-1
1.3.2 组网需求 1-1
1.3.3 配置思路 1-1
1.3.4 配置注意事项 1-1
1.3.5 配置步骤 1-2
1.3.6 验证配置 1-2
1.3.7 配置文件 1-3
1.4 MAC地址用户名远程认证典型配置举例 1-4
1.4.1 适用产品和版本 1-4
1.4.2 组网需求 1-4
1.4.3 配置思路 1-4
1.4.4 配置注意事项 1-4
1.4.5 配置步骤 1-5
1.4.6 验证配置 1-6
1.4.7 配置文件 1-7
1.5 固定用户名远程认证典型配置举例 1-7
1.5.1 适用产品和版本 1-7
1.5.2 组网需求 1-8
1.5.3 配置思路 1-8
1.5.4 配置注意事项 1-8
1.5.5 配置步骤 1-8
1.5.6 验证配置 1-9
1.5.7 配置文件 1-10
1.6 MAC地址认证配合ACL下发典型配置举例 1-11
1.6.1 适用产品和版本 1-11
1.6.2 组网需求 1-12
1.6.3 配置思路 1-12
1.6.4 配置注意事项 1-12
1.6.5 配置步骤 1-12

1.6.6 验证配置 ·····1-13
1.6.7 配置文件 ·····1-14

1 MAC地址认证典型配置举例

1.1 简介

本章介绍了使用了 MAC 地址认证实现用户安全接入的典型配置举例。

1.2 使用限制

端口启动 MAC 地址认证与端口加入聚合组及端口加入业务环回组互斥。

1.3 MAC地址本地认证典型配置举例

1.3.1 适用产品和版本

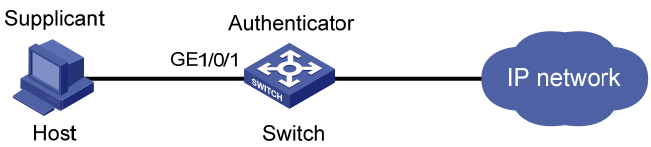
表1 配置适用的产品与软件版本关系

产品	软件版本
S10500系列以太网交换机	Release 1120系列，Release 1130系列，Release 1200系列
S5800&S5820X系列以太网交换机	Release 1808
S5830系列以太网交换机	Release 1115，Release 1118
S5500-EI&S5500-SI系列以太网交换机	Release 2220

1.3.2 组网需求

如 图 1所示，通过配置MAC地址本地认证功能，实现在无需架设服务器的情况下，完成接入用户的安全认证，控制其对Internet的访问。

图1 启动 MAC 地址认证对接入用户进行本地认证



1.3.3 配置思路

- 在 Switch 与用户端相连的端口上配置 MAC 地址认证。
- 为了防止非法 MAC 短时间内的重复认证，可配置 MAC 地址认证定时器。

1.3.4 配置注意事项

- 配置全局 MAC 地址认证一般放在最后，当其他认证参数未配置完成时，会造成合法用户无法访问网络。

- 创建本地用户时，需要注意用户名必须与设备上指定的 MAC 地址认证用户名格式保持一致。

1.3.5 配置步骤

添加本地接入用户。

```
<Switch> system-view
[Switch] local-user 68-05-ca-06-55-7b
New local user added.
[Switch-luser-68-05-ca-06-55-7b] password simple 68-05-ca-06-55-7b
[Switch-luser-68-05-ca-06-55-7b] service-type lan-access
[Switch-luser-68-05-ca-06-55-7b] quit
```

配置 ISP 域，使用本地认证方式。

```
[Switch] domain aabbcc.net
[Switch-isp-aabbcc.net] authentication lan-access local
[Switch-isp-aabbcc.net] quit
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[Switch] mac-authentication domain aabbcc.net
```

配置 MAC 地址认证的下线定时器和静默定时器。即交换机每隔 180 秒就对用户是否下线进行检测；并且当用户认证失败时，需等待 3 分钟后才能对用户再次发起认证。

```
[Switch] mac-authentication timer offline-detect 180
[Switch] mac-authentication timer quiet 180
```

配置 MAC 地址认证用户名格式：使用带连字符的 MAC 地址作为用户名与密码，其中字母小写。

```
[Switch] mac-authentication user-name-format mac-address with-hyphen lowercase
```

开启端口 GigabitEthernet1/0/1 的 MAC 地址认证特性。

```
[Switch] mac-authentication interface GigabitEthernet 1/0/1
 Mac-auth is enabled on port GigabitEthernet1/0/1.
```

开启全局 MAC 地址认证特性。

```
[Switch] mac-authentication
 Mac-auth is enabled globally.
```

1.3.6 验证配置

显示全局 MAC 地址配置信息。

```
<Switch> display mac-authentication
MAC address authentication is enabled.
 User name format is MAC address in lowercase, like xx-xx-xx-xx-xx-xx
 Fixed username:mac
 Fixed password:not configured
          Offline detect period is 180s
          Quiet period is 180s
          Server response timeout value is 100s
          The max allowed user number is 2048 per slot
          Current user number amounts to 1
          Current domain is aabbcc.net
```

```
Silent MAC User info:
          MAC Addr         From Port                     Port Index


GigabitEthernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 1, failed: 364
  Max number of on-line users is 2048
  Current online user number is 1
          MAC Addr         Authenticate State           Auth Index
          6805-ca06-557b   MAC_AUTHENTICATOR_SUCCESS     350
<略>

<Switch> display connection
Slot:  1
Index=350 , Username=68-05-ca-06-55-7b@aabbcc.net
 IP=N/A
 IPv6=N/A
 MAC=6805-ca06-557b

 Total 1 connection(s) matched on slot 1.
 Total 1 connection(s) matched.
```

1.3.7 配置文件

说明

S5500-SI 系列交换机不支持 **port link-mode bridge** 命令。

```
#
 mac-authentication
 mac-authentication timer offline-detect 180
 mac-authentication timer quiet 180
 mac-authentication domain aabbcc.net
 mac-authentication user-name-format mac-address with-hyphen
#
domain aabbcc.net
 authentication lan-access local
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
local-user 68-05-ca-06-55-7b
 password cipher $c$3$KEiYU/nrbJqmp75BldT4m99SzcSQ5Ro3sPRpTvUSd4aGL676
 service-type lan-access
#
```

```
interface GigabitEthernet1/0/1
 port link-mode bridge
 mac-authentication
#
```

1.4 MAC地址用户名远程认证典型配置举例

1.4.1 适用产品和版本

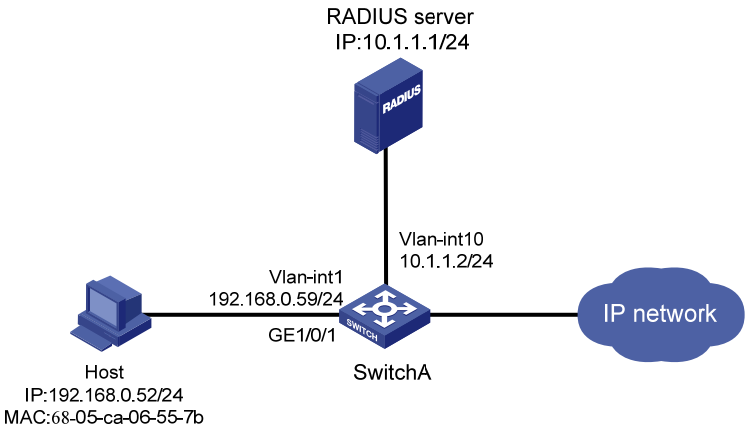
表2 配置适用的产品与软件版本关系

产品	软件版本
S10500系列以太网交换机	Release 1120系列，Release 1130系列，Release 1200系列
S5800&S5820X系列以太网交换机	Release 1808
S5830系列以太网交换机	Release 1115，Release 1118
S5500-EI&S5500-SI系列以太网交换机	Release 2220

1.4.2 组网需求

如 图 2所示，用户Host通过Switch连接到网络。为了提高安全性，可以通过配置MAC地址用户名远程认证，实现在远程服务器上完成用户身份的认证。

图2 启动 MAC 地址认证对接入用户进行 RADIUS 认证



1.4.3 配置思路

请参见 1.3.3 配置思路。

1.4.4 配置注意事项

- 配置全局 MAC 地址认证一般放在最后，当其他认证参数未配置完成时，会造成合法用户无法访问网络。

- 在 RADIUS 服务器上添加用户帐号，用户名必须与设备上指定的 MAC 地址认证用户名格式保持一致。
- 在标准的 RADIUS 协议中，RADIUS 服务器的认证端口为 UDP 端口 1812，我司设备作为 RADIUS 服务器时认证端口为 UDP 端口 1645。因此，本举例中需要在 SwitchA 上配置 RADIUS 方案时，需要指定认证服务器的认证端口号为 1645。

1.4.5 配置步骤

说明

- 按照组网图配置设备各接口的 IP 地址，保证各主机、服务器和设备之间的路由可达。
- 如下服务器配置以 H3C S5500-HI 系列交换机作为 RADIUS server 为例，详细信息可参考相关产品手册。

1. SwitchA 的配置

配置 RADIUS 方案。

```
<SwitchA> system-view
[SwitchA] radius scheme 2000
New Radius scheme
[SwitchA-radius-2000] primary authentication 10.1.1.1 1645 key abc
[SwitchA-radius-2000] user-name-format without-domain
[SwitchA-radius-2000] quit
```

配置 ISP 域的 AAA 方案。

```
[SwitchA] domain domain2
[SwitchA-isp-domain2] authentication lan-access radius-scheme 2000
[SwitchA-isp-domain2] authorization lan-access radius-scheme 2000
[SwitchA-isp-domain2] quit
```

开启端口 GigabitEthernet1/0/1 的 MAC 地址认证特性。

```
[SwitchA] mac-authentication interface gigabitethernet1/0/1
 Mac-auth is enabled on port GigabitEthernet1/0/1.
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[SwitchA] mac-authentication domain domain2
```

配置 MAC 地址认证的下线定时器和静默定时器。即交换机每隔 180 秒就对用户是否下线进行检测；并且当用户认证失败时，需等待 3 分钟后才能对用户再次发起认证。

```
[SwitchA] mac-authentication timer offline-detect 180
[SwitchA] mac-authentication timer quiet 180
```

配置 MAC 地址认证用户名格式：使用带连字符的 MAC 地址作为用户名与密码，其中字母小写。

```
[SwitchA] mac-authentication user-name-format mac-address with-hyphen lowercase
```

开启全局 MAC 地址认证特性。

```
[SwitchA] mac-authentication
 Mac-auth is enabled globally.
```

2. RADIUS server的配置

以 Host 的 MAC 地址作为用户名，创建 RADIUS 用户并进入 RADIUS 服务器用户视图

```
<SwitchB> system-view
[SwitchB] radius-server user 68-05-ca-06-55-7b
```

指定用户的密码为明文 123456。

```
[SwitchB-rdsuser-68-05-ca-06-55-7b] password simple 123456
[SwitchB-rdsuser-68-05-ca-06-55-7b] quit
```

配置 RADIUS 客户端 IP 为 10.1.1.2，共享密钥为明文 abc。

```
[SwitchB] radius-server client-ip 10.1.1.2 key simple abc
```

1.4.6 验证配置

显示全局 MAC 地址配置信息。

```
<SwitchA> display mac-authentication
MAC address authentication is enabled.
 User name format is MAC address in lowercase, like xx-xx-xx-xx-xx-xx
 Fixed username:mac
 Fixed password:not configured
          Offline detect period is 180s
          Quiet period is 180s.
          Server response timeout value is 100s
          The max allowed user number is 2048 per slot
          Current user number amounts to 1
          Current domain is domain2

Silent Mac User info:
         MAC Addr               From Port           Port Index

Gigabitethernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 1, failed: 0
  Max number of on-line users is 2048
  Current online user number is 1
          MAC Addr         Authenticate State           Auth Index
          6805-ca06-557b   MAC_AUTHENTICATOR_SUCCESS    0
<略>

<SwitchA> display connection
Slot:  1
Index=0  ,Username=68-05-ca-06-55-7b@domain2
 IP=N/A
 Ipv6=N/A
 MAC=6805-ca06-557b

 Total 1 connection(s) matched on slot 1.
 Total 1 connection(s) matched.
```

1.4.7 配置文件

说明

S5500-SI 系列交换机不支持 **port link-mode bridge** 命令。

- SwitchA：

```
#
mac-authentication
 mac-authentication timer offline-detect 180
 mac-authentication timer quiet 180
 mac-authentication domain domain2
 mac-authentication user-name-format mac-address with-hyphen
#
radius scheme 2000
 primary authentication 10.1.1.1 1645 key cipher $c$3$eYcHkFXUguZArZkXiCkrPABwQ0+E6g==
 user-name-format without-domain
#
domain domain2
 authentication lan-access radius-scheme 2000
 authorization lan-access radius-scheme 2000
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 mac-authentication
#
```

- Radius server：

```
#
 radius-server client-ip 10.1.1.2 key cipher $c$3$qz/+3koDvrIbRqm1Ghf6a10hS4fLFQ==
#
radius-server user 68-05-ca-06-55-7b
 password cipher $c$3$Xv+yKBbrO2yl0iVyWZfuRJyhm0ZNJkGU/REI5+GZSfJ7vcky
#
```

1.5 固定用户名远程认证典型配置举例

1.5.1 适用产品和版本

表3 配置适用的产品与软件版本关系

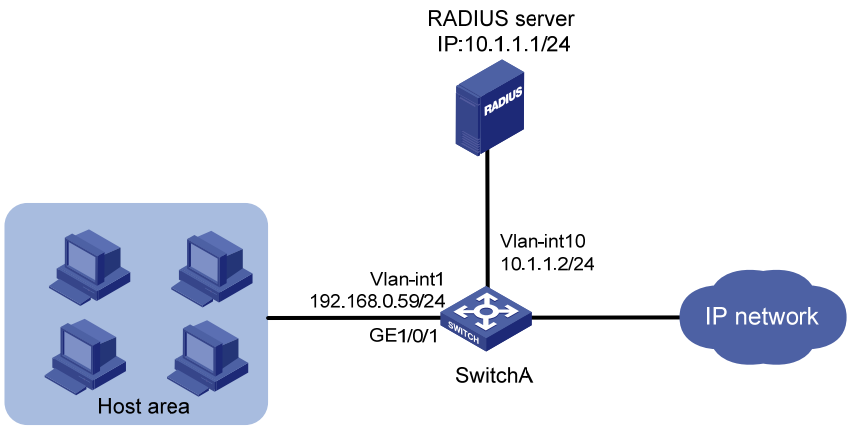
产品	软件版本
S10500系列以太网交换机	Release 1120系列，Release 1130系列，Release 1200系列

产品	软件版本
S5800&S5820X系列以太网交换机	Release 1808
S5830系列以太网交换机	Release 1115，Release 1118
S5500-EI&S5500-SI系列以太网交换机	Release 2220

1.5.2 组网需求

如 图 3所示，对于网络中存在较为安全的多用户区域，可通过配置固定用户名远程认证来完成用户身份的认证。这样可以保留一定的用户扩展需求。

图3 固定用户名远程认证组网示意图



1.5.3 配置思路

请参见 1.3.3 配置思路。

1.5.4 配置注意事项

请参见 1.4.4 配置注意事项。

1.5.5 配置步骤

说明

- 按照组网图配置设备各接口的 IP 地址，保证各主机、服务器和设备之间的路由可达。
- 如下服务器配置以 H3C S5500-HI 系列交换机作为 RADIUS server 为例，详细信息可参考相关产品手册。

1. Switch A的配置

配置 RADIUS 方案。

```
<SwitchA> system-view
[SwitchA] radius scheme 2000
New Radius scheme
[SwitchA-radius-2000] primary authentication 10.1.1.1 1645 key abc
[SwitchA-radius-2000] user-name-format without-domain
[SwitchA-radius-2000] quit
```

配置 ISP 域的 AAA 方案。

```
[SwitchA] domain domain1
[SwitchA-isp-domain1] authentication lan-access radius-scheme 2000
[SwitchA-isp-domain1] authorization lan-access radius-scheme 2000
[SwitchA-isp-domain1] quit
```

开启端口 GigabitEthernet1/0/1 的 MAC 地址认证特性。

```
[SwitchA] mac-authentication interface gigabitethernet1/0/1
 Mac-auth is enabled on port GigabitEthernet1/0/1.
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[SwitchA] mac-authentication domain domain1
```

配置 MAC 地址认证的定时器。

```
[SwitchA] mac-authentication timer offline-detect 180
[SwitchA] mac-authentication timer quiet 180
```

配置 MAC 地址认证使用固定用户名、密码格式。

```
[SwitchA] mac-authentication user-name-format fixed account aaa password simple 123456
```

开启全局 MAC 地址认证特性。

```
[SwitchA] mac-authentication
 Mac-auth is enabled globally.
```

2. RADIUS server的配置

创建 RADIUS 用户“aaa”并进入 RADIUS 服务器用户视图

```
<SwitchB> system-view
[SwitchB] radius-server user aaa
```

指定用户 aaa 的密码为明文 123456。

```
[SwitchB-rdsuser-aaa] password simple 123456
[SwitchB-rdsuser-aaa] quit
```

配置 RADIUS 客户端 IP 为 10.1.1.2，共享密钥为明文 abc。

```
[SwitchB] radius-server client-ip 10.1.1.2 key simple abc
```

1.5.6 验证配置

显示 Switch A 的 MAC 地址配置信息。

```
<SwitchA> display mac-authentication
MAC address authentication is enabled.
User name format is fixed account
 Fixed username:aaa
 Fixed password:******
          Offline detect period is 180s
          Quiet period is 180s.
```

```
          Server response timeout value is 100s
          The max allowed user number is 2048 per slot
          Current user number amounts to 4
          Current domain is domain1

Silent Mac User info:
         MAC Addr              From Port           Port Index

Gigabitethernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 4, failed: 0
  Max number of on-line users is 1024
  Current online user number is 4
          MAC Addr         Authenticate State           Auth Index
          6805-ca06-557b   MAC_AUTHENTICATOR_SUCCESS    0
          6805-ca00-8a11   MAC_AUTHENTICATOR_SUCCESS    1
          6805-ca00-6677   MAC_AUTHENTICATOR_SUCCESS    2
          6805-ca02-1122   MAC_AUTHENTICATOR_SUCCESS    3

<略>

<SwitchA> display connection
Slot:  1
Index=0  ,Username=aaa@domain1
 IP=N/A
 Ipv6=N/A
 MAC=6805-ca06-557b
Index=1  ,Username=aaa@domain1
 IP=N/A
 Ipv6=N/A
 MAC=6805-ca00-8a11
Index=2  ,Username=aaa@domain1
 IP=N/A
 Ipv6=N/A
 MAC=6805-ca00-6677
Index=3  ,Username=aaa@domain1
 IP=N/A
 Ipv6=N/A
 MAC=6805-ca02-1122

 Total 4 connection(s) matched on slot 1.
 Total 4 connection(s) matched.
```

1.5.7 配置文件

说明

S5500-SI 系列交换机不支持 **port link-mode bridge** 命令。

- Switch A：

```
#
mac-authentication
 mac-authentication timer offline-detect 180
 mac-authentication timer quiet 180
 mac-authentication domain domain1
 mac-authentication user-name-format fixed account aaa password cipher
$c$3$6DXUG/ZZMl7AbkMpJEo2uoni19WCI0nJGw
#
radius scheme 2000
 primary authentication 10.1.1.1 1645 key cipher $c$3$eYcHkFXUguZArZkXiCkrPABwQ0+E6g
 user-name-format without-domain
#
domain domain1
 authentication lan-access radius-scheme 2000
 authorization lan-access radius-scheme 2000
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 mac-authentication
#
```

- Radius server：

```
#
 radius-server client-ip 10.1.1.2 key cipher $c$3$qz/+3koDvrIbRqm1Ghf6a10hS4fLFQ==
#
radius-server user aaa
 password cipher $c$3$Xv+yKBbrO2yl0iVyWZfuRJyhm0ZNJkGU/REI5+GZSfJ7vcky
#
```

1.6 MAC地址认证配合ACL下发典型配置举例

1.6.1 适用产品和版本

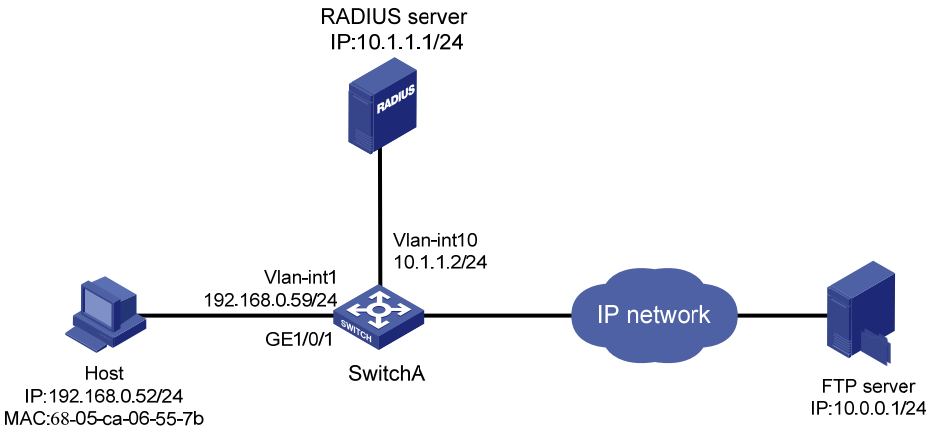
表4 配置适用的产品与软件版本关系

产品	软件版本
S10500系列以太网交换机	Release 1120系列，Release 1130系列，Release 1200系列
S5800&S5820X系列以太网交换机	Release 1808
S5830系列以太网交换机	Release 1115，Release 1118
S5500-EI&S5500-SI系列以太网交换机	Release 2220

1.6.2 组网需求

如 图 4所示，主机Host通过MAC地址认证接入网络，认证服务器为RADIUS服务器。Internet网络中有一台FTP服务器，通过配置MAC地址认证成功后下发ACL功能，实现对接入用户完成身份认证后的访问权限的控制。用户认证成功后可以访问Internet，但不能访问FTP服务器。

图4 下发 ACL 典型配置组网图



1.6.3 配置思路

- 在 Switch 与用户端相连的端口上配置 MAC 地址认证。
- 为了防止非法 MAC 短时间内的重复认证，可配置 MAC 地址认证定时器。
- 在 RADIUS 服务器上添加用户帐号，并授权下发相应编号的 ACL。

1.6.4 配置注意事项

请参见 1.4.4 配置注意事项。

1.6.5 配置步骤

说明

- 按照组网图配置设备各接口的 IP 地址，保证各主机、服务器和设备之间的路由可达。
- 如下服务器配置以 H3C S5500-HI 系列交换机作为 RADIUS server 为例，详细信息可参考相关产品手册。

1. SwitchA的配置

配置 RADIUS 方案。

```
[SwitchA> system-view
[SwitchA] radius scheme 2000
New Radius scheme
```

```
[SwitchA-radius-2000] primary authentication 10.1.1.1 1645 key abc
[SwitchA-radius-2000] user-name-format without-domain
[SwitchA-radius-2000] quit
```

配置 ISP 域的 AAA 方案。

```
[SwitchA] domain domain1
[SwitchA-isp-domain1] authentication lan-access radius-scheme 2000
[SwitchA-isp-domain1] authorization lan-access radius-scheme 2000
[SwitchA-isp-domain1] quit
```

配置 ACL 3000，拒绝目的 IP 地址为 10.0.0.1 的报文通过。

```
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0
[SwitchA-acl-adv-3000] quit
```

开启端口 GigabitEthernet1/0/1 的 MAC 地址认证特性。

```
[SwitchA] mac-authentication interface GigabitEthernet 1/0/1
 Mac-auth is enabled on port GigabitEthernet1/0/1.
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[SwitchA] mac-authentication domain domain1
```

配置 MAC 地址认证的定时器。

```
[SwitchA] mac-authentication timer offline-detect 180
[SwitchA] mac-authentication timer quiet 180
```

配置 MAC 地址认证用户名格式。使用带连字符的 MAC 地址作为用户名与密码。

```
[SwitchA] mac-authentication user-name-format mac-address with-hyphen lowercase
```

开启全局 MAC 地址认证特性。

```
[SwitchA] mac-authentication
 Mac-auth is enabled globally.
```

2. RADIUS server的配置

以 Host 的 MAC 地址作为用户名，创建 RADIUS 用户并进入 RADIUS 服务器用户视图

```
<SwitchB> system-view
[SwitchB] radius-server user 68-05-ca-06-55-7b
```

指定用户的密码为明文 123456。

```
[SwitchB-rdsuser-68-05-ca-06-55-7b] password simple 123456
```

为 RADIUS 用户授权 ACL3000。

```
[SwitchB-rdsuser-68-05-ca-06-55-7b] authorization-attribute acl 3000
[SwitchB-rdsuser-68-05-ca-06-55-7b] quit
```

配置 RADIUS 客户端 IP 为 10.1.1.2，共享密钥为明文 abc。

```
[SwitchB] radius-server client-ip 10.1.1.2 key simple abc
```

1.6.6 验证配置

用户 Host 认证成功后，通过在 SwitchA 上执行 **display connection** 命令可以查看到已上线用户信息。

```
<SwitchA> display connection
Slot:  1
```

```
Index=0  ,Username=68-05-ca-06-55-7b@domain1
 IP=N/A
 Ipv6=N/A
 MAC=6805-ca06-557b

 Total 1 connection(s) matched on slot 1.
 Total 1 connection(s) matched.
```

用户 Host 认证成功后，通过 **ping** FTP 服务器，可以验证认证服务器下发的 ACL 3000 是否生效。

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

C:\>
```

1.6.7 配置文件

说明

S5500-SI 系列交换机不支持 **port link-mode bridge** 命令。

- SwitchA：

```
#
mac-authentication
 mac-authentication timer offline-detect 180
 mac-authentication timer quiet 180
 mac-authentication domain domain2
 mac-authentication user-name-format mac-address with-hyphen
#
acl number 3000
 rule 0 deny ip destination 10.0.0.1 0
#
radius scheme 2000
 primary authentication 10.1.1.1 1645 key cipher $c$3$eYcHkFXUguZArZkXiCkrPABwQ0+E6g==
 user-name-format without-domain
#
domain domain1
 authentication lan-access radius-scheme 2000
 authorization lan-access radius-scheme 2000
```

```
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 mac-authentication
#
```

- Radius server：

```
#
 radius-server client-ip 10.1.1.2 key cipher $c$3$qz/+3koDvrIbRqm1Ghf6a10hS4fLFQ==
#
radius-server user 68-05-ca-06-55-7b
 password cipher $c$3$Xv+yKBbrO2yl0iVyWZfuRJyhm0ZNJkGU/REI5+GZSfJ7vcky
 authorization-attribute acl 3000
#
```