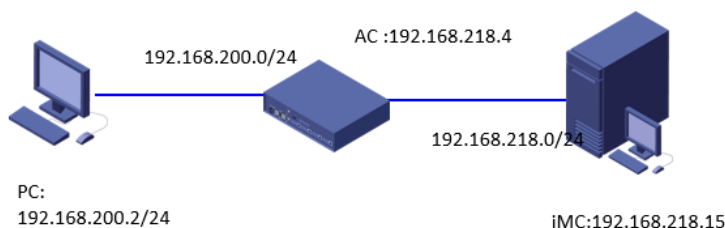


知 iMC EIA 7.2 E0408版本和V7设备配合实现有线802.1x认证的典型配置案例

802.1X

李树兵 2016-08-09 发表

802.1x是目前常见的几种认证之一，很多的公司采用此种认证。本文档简单介绍目前iMC EIA最新版本7.2 E0408配合V7设备实现有线802.1x认证。本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。本文档假设您已了解AAA、802.1x认证。



此案例中认证PC的地址为192.168.200.2（当然，1x认证之前客户端可以不配置地址，通过DHCP自动获取），网关为192.168.200.50，位于AC的interface vlan 100上，另一个接口地址为192.168.218.4，与iMC互联，iMC的地址为192.168.218.15，作为认证的RADIUS服务器。

iMC EIA版本信息：7.2 E0408

VAC版本信息：7.1.064, ESS 1111

一.设备配置:

dot1x //全局视图开启802.1x认证

#

vlan 100 //配置连接的vlan，vlan 100

interface Vlan-interface100 //配置PC的网关

ip address 192.168.200.50 255.255.255.0

#

interface GigabitEthernet1/0

port link-mode route

#

interface GigabitEthernet2/0 //配置连接iMC的接口

port link-mode route

ip address 192.168.218.4 255.255.255.0

#

interface GigabitEthernet3/0 //配置连接认证PC的接口

port link-mode bridge

port access vlan 100

dot1x //接口开启802.1x认证

undo dot1x handshake //关闭握手协议

dot1x mandatory-domain dot1x //指定802.1x认证的domain域为dot1x（此域需要之前配置好，见下面的配置）

#

snmp-agent //配置SNMP参数，用于iMC网管

snmp-agent local-engineid 800063A280000C2994455600000001

snmp-agent community write private

snmp-agent community read public

snmp-agent sys-info version all

snmp-agent target-host trap address udp-domain 192.168.218.15 params securityname public v2c

#

radius scheme 1x //配置 radius scheme 1x

primary authentication 192.168.218.15 //指定认证的服务器地址为192.168.218.15

primary accounting 192.168.218.15 //指定计费的服务器地址为192.168.218.15
accounting-on enable //打开计费功能。在accounting-on功能处于使能的情况下，若集中式设备或分布式设备上的单板重启，则设备或单板会在重启之后发送accounting-on报文通知该方案所使用的RADIUS计费服务器，要求RADIUS服务器停止计费且强制该设备的用户下线。
key authentication cipher \$c\$3\$b/a1wnvGcUzb2wmkDvhgDIKPPkIh1Q== //配置认证的key，这里配置为h3c，此处的密钥要和iMC侧接入设备配置的密钥一致。
key accounting cipher \$c\$3\$5EhXQPYgxzBOJAQLiA0KP4FivGWM8w== //配置计费的key，这里配置为h3c，此处的密钥要和iMC侧接入设备配置的密钥一致。这两个密钥保持一致，因为iMC侧只能配置一个密钥，所以认证和计费密钥要一致。
user-name-format without-domain //配置认证用户不带domain域，对应iMC侧接入服务不能添加服务后缀
nas-ip 192.168.218.4 //指定设备发送RADIUS报文的源地址为192.168.218.4，iMC对应接入设备里面配置的地址也应该为192.168.218.4，否则会导致认证不成功。
#

domain dot1x //配置domain域dot1x
authorization-attribute idle-cut 10 10240000 //类似于V5设备上的idle-cut，用于在设备上检测用户是否在线。指定ISP域imc下的用户闲置切断时间为10分钟，闲置切断时间内产生的流量为10240000字节。
authentication lan-access radius-scheme 1x //设置用户认证的radius方案为dot1x
authorization lan-access radius-scheme 1x //设置用户授权的radius方案为dot1x
accounting lan-access radius-scheme 1x //设置用户计费的radius方案为dot1x
二.iMC配置：

iMC网管加入设备的过程略过，从iMC增加接入设备开始。

第一步：增加接入设备



点击到增加设备的页面，选择“增加”选项



802.1x认证、portal认证以及MAC认证业务类型需要选择“LAN接入业务”，否则认证的时候会提示“no this user”，输入共享密钥，此处密钥需要和设备上配置radius scheme里面认证和计费的密钥一致。点击“选择”增加设备，此处需要先将设备通过iMC网管之后才可以看到。

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 修改接入设备

接入配置

认证端口 *	1812	计费端口 *	1813
业务类型	LAN接入业务	强制下线方式	断开用户连接
接入设备类型	H3C (General)	接入设备分组	无
共享密钥 *	***	确认共享密钥 *	***

设备列表

设备名称	设备IP地址	设备型号
H3C	192.168.218.4	H3C VAC

共有1条记录。

确定 取消

选择好之后如上图，点击确认即可添加成功。

第二步：增加接入策略

接入策略管理

接入策略查询

接入策略名 业务分组

增加

接入策略名	描述	业务分组	修改	删除
1x		未分组		

共有1条记录，当前第1-1，第1/1页。

点击接入策略管理页面，点击“增加”选项进行接入策略的增加

用户 > 接入策略管理 > 接入策略管理 > 修改接入策略

基本信息

接入策略名 * 1x

业务分组 * 未分组

描述

授权信息

接入时段	无	分配IP地址 *	否
下行速率(Kbps)		上行速率(Kbps)	
优先级		下发用户组	
首选EAP类型	EAP-MD5	单次最大在线时长(分钟)	
EAP自协商	启用		

输入策略名，如果没有其他安全要求或者用户限速等要求的话直接点击下面的确定即可。

第三步：增加接入服务

用户 > 接入策略管理 > 接入服务管理

增加 刷新

服务名	服务描述	服务后缀	业务分组	修改	删除
1x			未分组		

点击接入服务管理，点击“增加”选项进行接入服务的增加

资源 用户 业务 告警 报表 系统管理

用户 > 接入策略管理 > 接入服务管理 > 修改接入服务

基本信息

服务名 * 1x 服务后缀

业务分组 * 未分组 缺省接入策略 * 1x

缺省私有属性下发策略 * 不使用 缺省单帐号在线数量限制 * 0

服务描述

☒ 可申请 ☒ 无感知认证

接入场景列表

增加

名称	接入策略	私有属性下发策略	优先级	修改	删除
未找到符合条件的记录。					

输入服务名，缺省接入策略选择为刚刚配置的“1x”，其他的按照默认即可。

第四步：增加接入用户

H3C 智能管理中心

192.168.218.15:8080/imc/acm/acmservice/addAcmServiceTemplate.xhtml

H3C Intelligent Management Center

默认视图 admin 桌面版 帮助 关于 注销

资源 用户 业务 告警 报表 系统管理

用户管理

- 增加用户
- 所有用户
- 用户附加信息
- 用户数量操作
- 导入用户
- 帐号群组管理
- 接入用户管理
- 设备管理
- 终端管理
- 用户接入日志
- 接入策略管理
- 未接入管理

增加用户

基本信息

用户姓名 * test 证件号码 * test 检查是否可用

通讯地址 电话

电子邮件 用户分组 * 未分组

☐ 开通自助帐户

确定 取消

内存已超标，需要深度加速

版权所有 © 2007-2016 杭州华三通信技术有限公司，保留一切权利。

点击“用户”，选择“增加用户”来增加平台用户

资源 用户 业务 告警 报表 系统管理

用户 > 增加用户

增加用户

基本信息

用户姓名 * test 证件号码 * test 检查是否可用

通讯地址 电话

电子邮件 用户分组 * 未分组

☐ 开通自助帐户

确定 取消

内存已超标，需要深度加速

点击确认即可。

Intelligent Management Center

默认视图 admin 桌面版 帮助 关于 注销

资源 用户 业务 告警 报表 系统管理

用户 > 增加用户结果

增加用户完成，您可以继续选择如下操作：

增加接入用户	增加接入用户帐号。
返回用户列表	返回用户列表。
查看用户详细信息	查看刚刚增加的用户的信息。
继续增加用户	继续增加新的用户。

增加平台用户成功，选择增加接入用户

用户管理

用户 > 接入用户 > 增加接入用户

接入信息

用户名 * test 选择 增加用户

帐号名 * 123 ?

☐ 预开用户 ☐ 缺省BYOD用户 ☐ MAC地址认证用户 ☐ 主机名用户 ☐ 快速认证用户

密码 * ... 密码确认 * ...

☒ 允许用户修改密码 ☐ 启用用户密码控制策略 ☐ 下次登录须修改密码

生效时间 失效时间

最大闲置时长(分钟) 在线数量限制

登录提示信息

接入服务

服务名	服务后缀	状态	分配IP地址
1x		可申请	

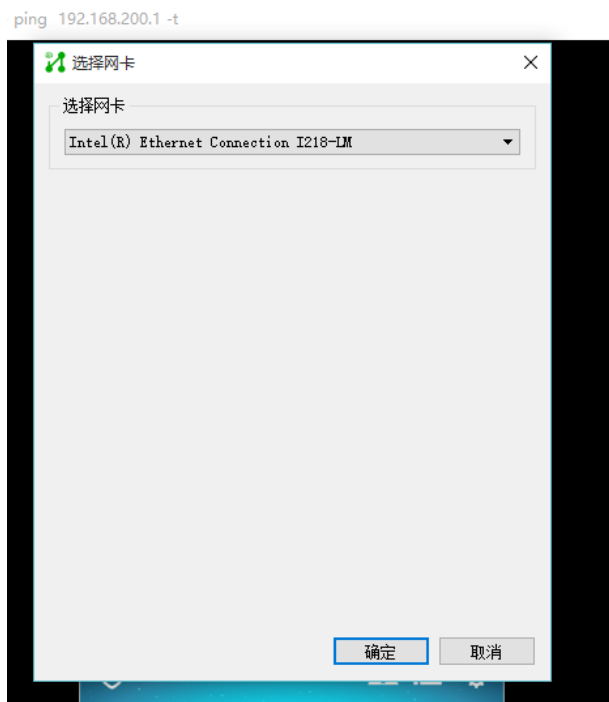
输入接入用户的用户名和密码，接入服务选择刚刚配置的“1x”，点击确定即可完成配置。

三.验证配置：

客户端选择使用iNode客户端登录：



输入用户名和密码



选择电脑进行802.1x认证的网络接口

ping 192.168.200.1 -t



点击确定即可认证成功。

在IMC上查看在线用户：



可以看到此用户在线，可以看到上线时间，从哪个设备上来的等信息。

在设备上查看在线信息：

```
[H3C-GigabitEthernet3/0]dis dot1x
```

Global 802.1X parameters:

802.1X authentication : Enabled

CHAP authentication : Enabled

Max-tx period : 30 s

Handshake period : 15 s

Quiet timer : Disabled

Quiet period : 60 s

Supp timeout : 30 s

Server timeout : 100 s

Reauth period : 3600 s

Max auth requests : 2

SmartOn supp timeout : 30 s

SmartOn retry counts : 3

EAD assistant function : Disabled

EAD timeout : 30 min

Domain delimiter : @

Online 802.1X wired users : 1

Online 802.1X wireless users : 0

GigabitEthernet3/0 is link-up

802.1X authentication : Enabled

Handshake : Disabled

Handshake reply : Disabled

Handshake security : Disabled

Unicast trigger : Disabled

Periodic reauth : Disabled

Port role : Authenticator

Authorization mode : Auto

Port access control : MAC-based

Multicast trigger : Enabled

Mandatory auth domain : dot1x

Guest VLAN : Not configured
Auth-Fail VLAN : Not configured
Critical VLAN : Not configured
Re-auth server-unreachable : Logoff
Max online users : 4294967295
SmartOn : Disabled
EAPOL packets: Tx 66, Rx 40
Sent EAP Request/Identity packets : 50
 EAP Request/Challenge packets: 4
 EAP Success packets: 3
 EAP Failure packets: 3
Received EAPOL Start packets : 7
 EAPOL LogOff packets: 3
 EAP Response/Identity packets : 26

[H3C-GigabitEthernet3/0]dis dot1x sessions

GigabitEthernet3/0 is link-up

Online 802.1X users: 1

MAC address	Auth state
3863-bbb8-a21a	Authenticated

[H3C-GigabitEthernet3/0]dis dot1x conn

[H3C-GigabitEthernet3/0]dis dot1x connection

Total connections: 1

Slot ID: 0

User MAC address: 3863-bbb8-a21a

Access interface: GigabitEthernet3/0

Username: 123

Authentication domain: dot1x

Authentication method: CHAP

Initial VLAN: 100

Authorization untagged VLAN: N/A

Authorization tagged VLAN list: N/A

Authorization ACL ID: N/A

Authorization user profile: N/A

Termination action: Default

Session timeout period: 86400 s

Online from: 2016/08/07 18:28:45

Online duration: 0h 9m 1s

[H3C-GigabitEthernet3/0]dis dot1x statistics

GigabitEthernet3/0 is link-up

EAPOL packets: Tx 68, Rx 42

Sent EAP Request/Identity packets : 52

 EAP Request/Challenge packets: 4

 EAP Success packets: 3

 EAP Failure packets: 3

Received EAPOL Start packets : 7

 EAPOL LogOff packets: 3

 EAP Response/Identity packets : 28

 EAP Response/Challenge packets: 4

 Error packets: 0

[H3C-GigabitEthernet3/0]dis dot1x interface GigabitEthernet 3/0

Global 802.1X parameters:

802.1X authentication : Enabled

CHAP authentication : Enabled

Max-tx period : 30 s

Handshake period : 15 s

Quiet timer : Disabled

 Quiet period : 60 s

Supp timeout : 30 s

Server timeout : 100 s

Reauth period : 3600 s

Max auth requests : 2

```

SmartOn supp timeout      : 30 s
SmartOn retry counts     : 3
EAD assistant function    : Disabled
    EAD timeout          : 30 min
Domain delimiter         : @
Online 802.1X wired users : 1
GigabitEthernet3/0 is link-up
802.1X authentication    : Enabled
Handshake                : Disabled
Handshake reply          : Disabled
Handshake security       : Disabled
Unicast trigger          : Disabled
Periodic reauth          : Disabled
Port role                : Authenticator
Authorization mode        : Auto
Port access control       : MAC-based
Multicast trigger        : Enabled
Mandatory auth domain    : dot1x
Guest VLAN               : Not configured
Auth-Fail VLAN           : Not configured
Critical VLAN            : Not configured
Re-auth server-unreachable : Logoff
Max online users         : 4294967295
SmartOn                  : Disabled
EAPOL packets: Tx 68, Rx 42
Sent EAP Request/Identity packets : 52
    EAP Request/Challenge packets: 4
    EAP Success packets: 3
    EAP Failure packets: 3
Received EAPOL Start packets : 7
    EAPOL LogOff packets: 3
    EAP Response/Identity packets : 28
    EAP Response/Challenge packets: 4
    Error packets: 0
Online 802.1X users: 1
    MAC address    Auth state
    3863-bbb8-a21a  Authenticated
[H3C-GigabitEthernet3/0]dis dot1x
Global 802.1X parameters:
802.1X authentication    : Enabled
CHAP authentication      : Enabled
Max-tx period            : 30 s
Handshake period         : 15 s
Quiet timer              : Disabled
    Quiet period       : 60 s
Supp timeout             : 30 s
Server timeout           : 100 s
Reauth period            : 3600 s
Max auth requests        : 2
SmartOn supp timeout     : 30 s
SmartOn retry counts     : 3
EAD assistant function    : Disabled
    EAD timeout        : 30 min
Domain delimiter         : @
Online 802.1X wired users : 1
Online 802.1X wireless users : 0
GigabitEthernet3/0 is link-up
802.1X authentication    : Enabled
Handshake                : Disabled
Handshake reply          : Disabled
Handshake security       : Disabled
Unicast trigger          : Disabled
Periodic reauth          : Disabled
Port role                : Authenticator

```

Authorization mode : Auto
Port access control : MAC-based
Multicast trigger : Enabled
Mandatory auth domain : dot1x
Guest VLAN : Not configured
Auth-Fail VLAN : Not configured
Critical VLAN : Not configured
Re-auth server-unreachable : Logoff
Max online users : 4294967295
SmartOn : Disabled
EAPOL packets: Tx 69, Rx 43
Sent EAP Request/Identity packets : 53
 EAP Request/Challenge packets: 4
 EAP Success packets: 3
 EAP Failure packets: 3
Received EAPOL Start packets : 7
 EAPOL LogOff packets: 3
 EAP Response/Identity packets : 29
 EAP Response/Challenge packets: 4
 Error packets: 0
Online 802.1X users: 1
 MAC address Auth state
 3863-bbb8-a21a Authenticated

略