802.1X AAA ACL **宋斌** 2012-03-14 发表



本配置举例中的AC使用的是WX5002无线控制器, AP使用的是WA2100无线局域网接入 点设备。

本配置举例中,AC通过VLAN2接入Switch,VLAN2的IP地址为1.1.2.1/24,AP通过VLAN 1接入Switch,AP的IP地址为2.1.1.11/24,iMC的IP地址为162.105.34.20/24。网络中有 一个FTP服务器,IP地址为56.1.7.100。各个设备间路由可达。交换机Switch启动DHCP 服务向Client分配IP地址,客户端Client的网关在AC(VLAN2)。Client认证通过后,iM C向Client下发ACL3221,禁止Client访问FTP服务器。

三、 特性介绍:

ACL (Access Control List, 访问控制列表) 提供了控制用户访问网络资源和限制用户访问权限的功能。当用户上线时,如果RADIUS服务器上配置了授权ACL,则设备会根据服务器下发的授权ACL对用户所在端口的数据流进行控制;在服务器上配置授权ACL之前,需要在设备上配置相应的ACL规则。管理员可以通过改变服务器的授权ACL设置或设备上对应的ACL规则来改变用户的访问权限。

授权ACL下发一般可应用在如下场合: 接入同一AC的同一SSID的多个用户, 分别使用不同的资源, 或限制用户使用部分网络资源。

四、主要配置步骤:

在Dot1x接入端配置802.1x和认证。

#配置VLAN虚接口。

[AC] interface Vlan-interface2 [AC-Vlan-interface2] ip address 1.1.2.1 255.255.255.0

启用端口安全Port-security, 配置Dot1x认证方式为EAP。

[AC] port-security enable [AC] dot1x authentication-method eap

配置radius scheme。

[AC] radius scheme testscheme2

[AC-radius-testscheme2] server-type extended

[AC-radius-testscheme2] primary authentication 162.105.34.20

[AC-radius-testscheme2] primary accounting 162.105.34.20

[AC-radius-testscheme2] key authentication testkey2

[AC-radius-testscheme2] key accounting testkey2

[AC-radius-testscheme2] user-name-format without-domain

[AC-radius-testscheme2] quit

配置domain。

[AC] domain testdomain2

[AC-isp-testdomain2] authentication lan-access radius-scheme testscheme2

[AC-isp-testdomain2] authorization lan-access radius-scheme testscheme2 [AC-isp-testdomain2] accounting lan-access radius-scheme testscheme2 [AC-isp-testdomain2] quit

#配置下发的ACL。

[AC] acl number 3221 [AC-acl-adv-3221] rule deny ip destination 56.1.7.100 0 [AC-acl-adv-3221] quit

#配置无线接口WLAN-ESS。

[AC]interface WLAN-ESS 1 [AC-WLAN-ESS1] port access vlan 2 [AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext [AC-WLAN-ESS1] port-security tx-key-type 11key [AC-WLAN-ESS1] undo dot1x handshake [AC-WLAN-ESS1] quit

配置无线服务模板service-template 1。

[AC] wlan service-template 1 crypto
[AC-wlan-st-1] ssid testssid2
[AC-wlan-st-1] authentication-method open-system
[AC-wlan-st-1] bind WLAN-ESS 1
[AC-wlan-st-1] cipher-suite tkip
[AC-wlan-st-1] security-ie wpa
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit

#建立AP,并在AP下绑定服务模板,AP的配置要根据具体的AP和序列号进行配置。

[AC] wlan ap ap2100 model WA2100
[AC-wlan-ap-ap2100] serial-id 210235A22W0079000256
[AC-wlan-ap-ap2100] radio 1
[AC-wlan-ap-ap2100-radio-1] service-template 1
[AC-wlan-ap-ap2100-radio-1] radio enable
[AC-wlan-ap-ap2100-radio-1] quit
[AC-wlan-ap-ap2100] quit

iMC配置

在iMC上配置Dot1x认证项 (iMC版本: 3.20-E2403) 如下:

- (1) 正确安装iMC并导入证书,然后从iMC上添加设备AC(配置略)。
- (2) 增加接入设备,其中共享密钥要与步骤2中配置一致。

送人配查				
★ 共享密钥	testkey2			
* 认证端口	1812	* 计费端口	1813	
* 业务类型	LAN接入业务	* 接入设备类型	НЗС	~
备列表				
选择 选择 有1条记录。	手工增加 全部清除			
选择 选择 有1条记录。 设备名称	手工增加 全部清除 设备PP地址	设备型	पु	删除

(3) 增加服务:配置基本信息中的服务名和服务后缀(与步骤2中的domain name配置一致),授权信息中的证书认证、认证证书类型、认证证书子类型和下发ACL,其他信息可保持缺省值。

前加服务配置					
基本信息			93.060257.3		
* 服务名 * 安全策略	testsrv2		服务后缀	testdomain2	
服务描述	小视用安主策略 🔛				
🗹 可申请 😳					
授权信息 * 導入时段	x N		* 不做定接入区域	T	100
下行建革	7. M	bps	上行速率	π.	Kaps
优先级					
证书以证	○ 不启用 ③ EAP证书以证	○ WAPI证书以证			
认证证书类型 * 分配IP地址	EAP-PEAPULE		认证证书子类型	MS-CHAPV2认证	M
下发VLAN					
□ 下发用户组(SSL VPN考用	B) []				
マ 下发ACL	 ● 手工输入 3221 ● 列表选择 	Ø			
(4) 增加用户,配	置用户testuser27	下加入特定组	1.		
<mark>、用户 >> 増加用户</mark>				②帮助	
ita EBC					
·/////////////////////////////////////					
* 用户姓名 test	user2	* 业件亏妈	222222		
通讯地址		电话		Q	
电子邮件		* 用户分组	未分组		
	确定	取消			
品 用户 >> 增加接入用。	Þ				
<i>美</i> 入信息					
,用户姓名	testuser2	选择	增加用户		
帐号名	testac2		□匿名用户		
密码	•••••		* 密码确认	•••••	
密码 ☑ 允许用户修改密码	•••••	用用户密码控制第	* 密码确认 略	 •••••• 下次登录须修 	改密码
密码 ✓ 允许用户修改密码 失效日期	••••••	月用户密码控制第 🛄 😯	* 密码确认 略	•••••••	改密码
 密码 ✓ 允许用户修改密码 失效日期 最大闲置时长 	••••••	用用户密码控制第 19 3 分钟	* 密码确认 略 在线数量限制	 下次登录须修行 100 	改密码
密码 ✓ 允许用戶修改密码 失效日期 最大闲置时长 登录提示信息	18.	用用户密码控制第 🔝 🕜 分钟	* 密码确认 略 在线数量限制	 下次登录须修订 100 	改密码
 密码 ⑦ 允许用户修改密码 失效日期 最大闲置时长 登录提示信息 (入服务) 		周用户密码控制第 ■ ② 分钟	* 密码确认 略 在线数量限制	 ● 下次登录须修订 100 	设密码
 密码 ① 允许用户修改密码 失效日期 最大用置时长 登录提示信息 入服务 服务名 		用用户密码控制第 副 ② 分钟	* 密码确认 略 在线数量限制 安全策略	 下次量录须修订 100 	改密码
 密码 グ九许用戶修改密码 失效日期 最大和置时长 登录提示信息 入展多 【<u>影务名</u> 008 コもなのなり2001 		用用户密码控制第	* 密码确认 (略) 在线数量限制 (安全策略)	 ■ 下次登录须修订 100 	改密码 9地址
 密码 允许用户修改密码 失效日期 最大闲置时长 登录提示信息 (2) (2) (2) (3) (3) (4) 		用用户密码控制第 副 ③ 分钟 5 后援 1	* 密码确认 (略) 在线数量限制	 ■ 下次窒录须修订 100 	收密码 9地址
 密码 ・ 允许用户修改密码 失效日期 最大闲置时长 登录提示信息 入 服务 (1) (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2		用用户密码控制第 副 3 分钟 5 5 気気 1	* 密码确认 略 在线数星限制	 ■ 下次窒录须能 100 	收密码
 密码 ※ 允许用户修改密码 失效日期 最大闲置时长 登录提示信息 入服务 (1) (1)		用用户密码控制第 III 3 方量 1	* 密码确认 略 在线数量限制	 ■ 下次窒录须能 100 	以密码
 密码 次注用戶修改密码 失效日期 大川置时长 登录提示信息 2 2 2 2 4 <li< td=""><td></td><td>用用户密码控制第 副 ② 分钟 「 「 「 」</td><td>* 密码确认 IPS 在线数量限制</td><td> ■ 下次登录须修订 100 </td><td>以密码</td></li<>		用用户密码控制第 副 ② 分钟 「 「 「 」	* 密码确认 IPS 在线数量限制	 ■ 下次登录须修订 100 	以密码
 密码 次注用户修改密码 失效日期 最大用置时长 登录提示信息 入影 1 2 2 2 2 2 2 2 2 4 4 5 4 4 5 4 4 5 4 4 5 4 <li< td=""><td></td><td>用用户密码控制第 一 で 分钟 「 「 「 」 」 」 」 」 」 」 の の の の の の の の の の の の の</td><td>* 密码确认 (略) 在线数量限制</td><td> ■ 下次登录须修订 100 </td><td>收密码 </td></li<>		用用户密码控制第 一 で 分钟 「 「 「 」 」 」 」 」 」 」 の の の の の の の の の の の の の	* 密码确认 (略) 在线数量限制	 ■ 下次登录须修订 100 	收密码
 密码 ※ 允许用户修改密码 失效日期 最大闲置时长 登录提示信息 (1) (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2		用用户密码控制第 回 3 分钟 方量 1 domain2	* 密码确认 略 在线数量限制	 ■ 下次窒录须能 100 	改密码 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一
 密码 ※ 允许用户修改密码 失效日期 最大闲置时长 登录提示信息 (1) (1) (1) (1) 		用户密码控制第 ② 分钟 「 「 「 」 」 」 」 」 」 」 」 」 」 、 、 、 、 、 、 、 、 、 、 、 、 、	* 密码确认 略 在线数量限制 安全策略	 □ 下次登录须修订 100 用户III 用/□III 	改密码
 密码 ※九洋用戶修改密码 失效日期 最大用置时长 登录提示信息 決断 (1) 2) 在AC上执行d 	eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	開戸密码控制第 一 つ 分 中 1 domain2 輸入用户名 和	* 密码确认 密 在线数量限制 安全策略 和密码, 上线成 词对应的Client的	□ 下次窒录须修行 100 用户II 花功。 MAC地址,目4	改密码 P地址
 密码 ※ 允许用户修改密码 失效日期 最大闲置时长 登录提示信息 決察名 008 zhengshu3001 zhengshu202 zhengshu203 nsw testsrv2 5x 近(1) 2) 在AC上执行d display conneation 		開户密码控制第 一 分 中 「 「 な の の の の の の の の の の の の の	* 密码确认 略 在线数星限制 安全策略 新和密码,上线成 写对应的Client的	 □ 下次窒录须能 100 用户Ⅲ ①功。 MAC地址, 目A 	改密码 P地址 ACL正确
 密码 ※九洋用户修改密码 失效日期 朱次日期 最大闲置时长 登录提示信息 (1) 2) 在AC上执行d (1) (2) 在AC上执行d (2) (1) (2) (1) (2) (1) (2) (1) (3) (1) (4) (1) (4) (1) (5) (1) (5) (1) (6) (1) (7) (1) <li< td=""><td></td><td>開户密码控制第 一 分 サ 「 「 な の の の の の に 、 、 、 、 、 、 、 、 、 、 、 、 、</td><td>* 密码确认 略 在线数量限制 文全策略 (和密码,上线成 可对应的Client的</td><td> □ 下次窒录须修订 100 用户III (功)。 MAC地址, 且A </td><td>改密码 P地址 ACL正确</td></li<>		開户密码控制第 一 分 サ 「 「 な の の の の の に 、 、 、 、 、 、 、 、 、 、 、 、 、	* 密码确认 略 在线数量限制 文全策略 (和密码,上线成 可对应的Client的	 □ 下次窒录须修订 100 用户III (功)。 MAC地址, 且A 	改密码 P地址 ACL正确
 密码 ① 允许用户修改密码 失效日期 最大用置时长 登录提示信息 (1) 2) 大和gshu3001 2) 大和gshu3001 2) 大和gshu202 1) 2) 大名、结果验证: (1) 2) 在AC上执行d (1) 2) 在AC上执行d (1) (2) (3) (4) (4) (5) 		開戸密码控制第 一 ② 分 中 1 domain2 輸入用户名 m可以看到将 ②testdomain1	* 密码确认 密 在线数量限制 安全策略 (和密码,上线成 可对应的Client的	□ 下次窒录须修订 100 用户W (功)。 MAC地址,目A	改密码 一 中地址 ACL正研
 密码 ○ 允许用户修改密码 朱汝日期 最大用置时长 登录提示信息 ② ○ 008 ○ 2hengshu3001 ○ zhengshu202 ○ zhengshu203 ○ nsw ○ testsrv2 び、 左、结果验证: (1) 2) 在AC上执行d 次はsplay conneat Index=139,Us MAC=001b-11 		H用户密码控制第 一 の 分 中 1 domain2 輸入用户名 和 の 可以看到存 の し な い の の の の の の の の の の の の の	* 密码确认 密 在线数量限制 文全策略 (和密码,上线成 同对应的Client的	□ T次輩录须修订 100 用户II 花功。 MAC地址,目A	改密码 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一
 密码 ○ 九许用戶修改密码 失效日期 ● 九行用置时长 登場法示信息 >> >> ● 552 ● 008 ○ 2hengshu3001 ○ zhengshu202 ○ zhengshu203 ○ nsw ○ testsrv2 ● 五、结果验证: (1) 2) 在AC上执行d 次 ☆ display conner Index=139,Ust MAC=001b-11 Total 1 conner 		開戸密码控制第 ■ 分钟	* 密码确认 (略 在线数星限制 (和密码, 上线成 (和密码, 上线成 (和))) (和)) (1)	□ T次聖录須修 100 用户II 花功。 MAC地址,且A	改密码 一 中地址
 密码 ※ 允许用户修改密码 失效日期 最大闲置时长 登录提示信息 次 医多 2 林和gshu3001 2 林和gshu202 2 林和gshu203 nsw 2 thengshu203 nsw 2 testsrv2 五、结果验证: (1) 2) 在AC上执行d 发。 display conner Index=139, US MAC=001b-11 Total 1 conner 		開戸密码控制第 一 の 分 中 う 分 中 う う の う う う う う う う う う う う う う	* 密码确认 (略 在线数星限制 (文全策略) (和) (和) (和) (和) (和) (本) (本) (本) (本) (本) (本) (本) (本) (本) (本	□ T次窒录须修 100 用户II 花功。 MAC地址, 目A	改密码 P地址
 密码 ※九许用户修改密码 失效日期 量大闲置时长 登录提示信息 (1) 2) thengshu202 2) thengshu202 2) thengshu203 1) nsw 2) testsrv2 五、结果验证: (1) 2) 在AC上执行d (1) 2) 在AC上执行d (1) 2) 在AC上执行d (1) 2) 在AC上执行d (1) 2) 在AC上均(1) (1) 2) 在AC上均(1) (1) 2) 在ACL139,US (1) 		開戸密码控制第 一 の 分 中 「 后 気 し 1 1 domain2 本 和 入 用 户 名 、 2 、 4 の 、 の の 、 の 、 の の 、 の の 、 の の の 、 、 の の の 、 の の の 、 の の の 、 の の の の 、 の の の の の 、 の の の の の の の の の の の の の	* 密码确认 率 在线数星限制 交全策略 ;和密码,上线成 可对应的Client的	□ T次登录须修订 100 用户II 花功。 MAC地址,目A	改密码 PHA社 ACL正确
 密码 ※九洋用户修改密码 失效日期 最大闲置时长 登录提示信息 (1) 2) thengshu202 2) thengshu202 2) thengshu203 1) rsw 2) testsrv2 (1) 2) 在AC上执行d (1) 2) 在AC上执行d (1) 2) 在AC上执行d (1) 2) 在AC上切行d (1) 2) 在AC=01b-11 Total 1 conner (1) display conner 		開戸密码控制第 一 の 分 中 に 気 気 し 1 1 domain2 1 domain2 和 入 用 户 名 、 の の の の の の の の の の の の の	* 密码确认 率 在线数星限制 交全策略 5和密码,上线成 可对应的Client的	 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	改密码 P地址
 密码 ※ 允许用户修改密码 失效日期 果大用置时长 登录提示信息 (1) 2) thengshu202 2) thengshu203 2) thengshu203 2) thengshu203 2) thengshu203 2) thengshu203 (1) 2) 在AC上执行d display conneat Index=139,US MAC=001b-11 Total 1 conneat display conneat Index=139,U MAC=001b-11 		開戸密码控制第 一 の 分 中 1 1 domain2 輸入用户名 の 可以看到存 の し testdomain2 9 @testdomair	* 密码确认 率 在线数星限制 文全策略 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	□ T次登录须修订 100 用户Ⅲ (功)。 MAC地址,目A	改密码 P地址
 密码 ※ 允许用户修改密码 失效日期 朱次日期 最大闲置时长 登录提示信息 (入) (2) zhengshu202 zhengshu203 zhengshu203 zhengshu203 zhengshu203 zhengshu204 zhengshu204 zhengshu205 display connect Index=139, US MAC=001b-11 Total 1 connect Index=139, UU MAC=001b-11 IP=N/A 		開戸密码控制第 一 の か 中 の の の の の の の し し の の の し の の の の の の の の の の の の の	* 密码确认 略 在线数星限制 文全文章 和密码, 上线成 可对应的Client的	□ T次登录须修 100 用户II	改密码 一 中地址
 ● 密码 ● 公许用户修改密码 失效日期 量大用量时长 ● 公子 ● 公会		開戸密码控制第 一 の か 中 の の の の の の の し し の の の し の の の の の の の の の の の の の	* 密码确认 略 在线数量限制 文全文章 和密码, 上线成 可对应的Client的	□ T次重录须修订 100 用户II 花功。 MAC地址,且A	改密码 一 中地址

Initial VLAN=2, Authorization VLAN=N/A

ACL Group=3221 User Profile=N/A CAR=Disable Priority=Disable Start=2008-09-02 13:58:58 ,Current=2008-09-02 14:06:15 ,Online=00h07m17s Total 1 connection matched.

(3) Client不能访问FTP服务器56.1.7.100,能正常访问其他网络资源。