



CCBOOTCAMP Webinar 3/15/2011

CCIE Security / RS - 802.1x

Tim Rowley – CCIE#25960, CCSI#33858, CISSP

Agenda

- What is it?
- Components
- Basic Operation
- Basic Configuration
- Advanced Features and Configuration
- Verification / Troubleshooting
- ACS Demo – MDA and AD Integration (if time permitted)
- Q&A

What is it?

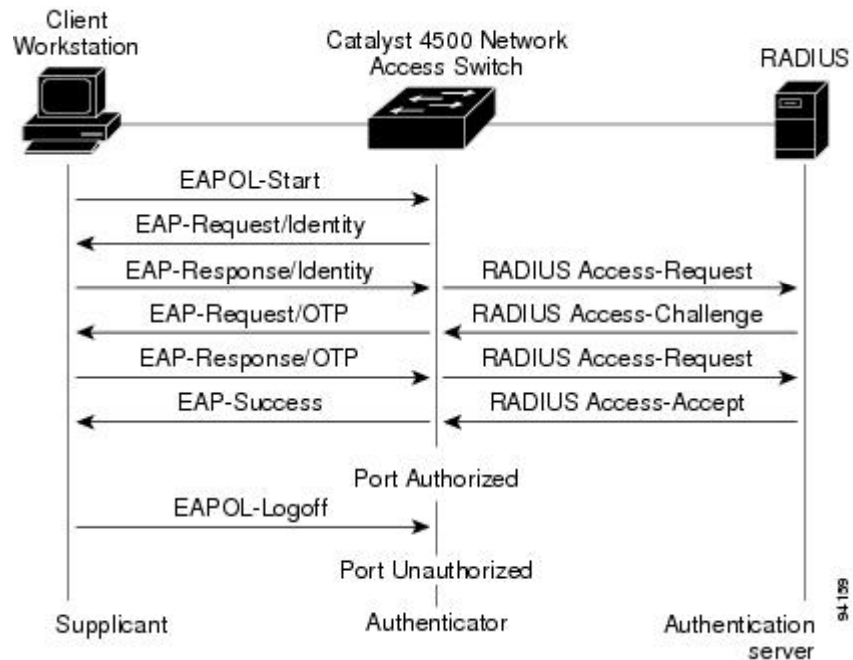
- 802.1x defines port-based authentication as a client-server based access control and authentication protocol which restricts unauthorized clients from connecting to the network. The clients must authenticate with an authentication server before the network switchport allows access to the network
- Also known as NAC Framework NAC-L2-802.1x

Components

- There are three main components to 802.1x:
 - *Client (Supplicant)*: Special software installed on the client device which responds to requests from the network switch.
 - *Authenticator*: Restricts or allows physical network access based on the authentication server's decision. The authenticator acts as a proxy between the client and authentication server.
 - *Authentication Server*: Performs the authentication of the client and notifies the authenticator whether to authorize or restrict network access for the particular client.

Basic Operation

The drawing below shows the authentication process.
(Drawing taken from www.cisco.com)



Basic Configuration

Interface Configuration:

Each interface which will participate (typically applies to user ports only, and not normally configured on ports with static devices behind it such as printer/servers/switches)

```
interface x/x
dot1x port-control auto           ← Allows port to go authorized or unauthorized based on .1x authentication results
dot1x pae authenticator          ← Starts port in unauthorized state, enables .1x
```

Global Configuration:

AAA:

```
aaa new-model
aaa authentication dot1x default group radius           ← Enables dot1x authentication via radius
aaa authorization network default group radius        ← Only needed if ACS is assigning VLAN to switchports
aaa accounting dot1x default start-stop group radius  ← Optional. Will log .1x activity on ACS reports

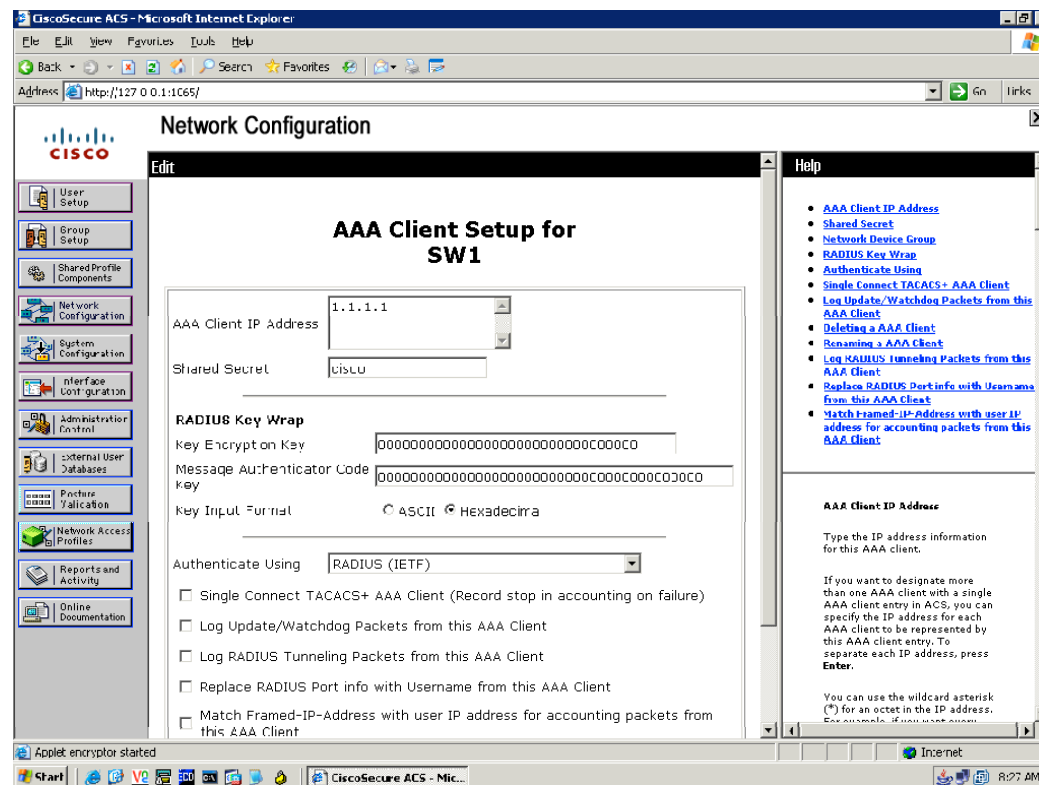
radius-server key <key>
radius-server host <primary ACS IP>
ip radius source-interface vlanx

dot1x system-auth-control                               ← This command globally enables 802.1x, issue this command last.
```

At a minimum the above commands are required on ports which participate in .1x.

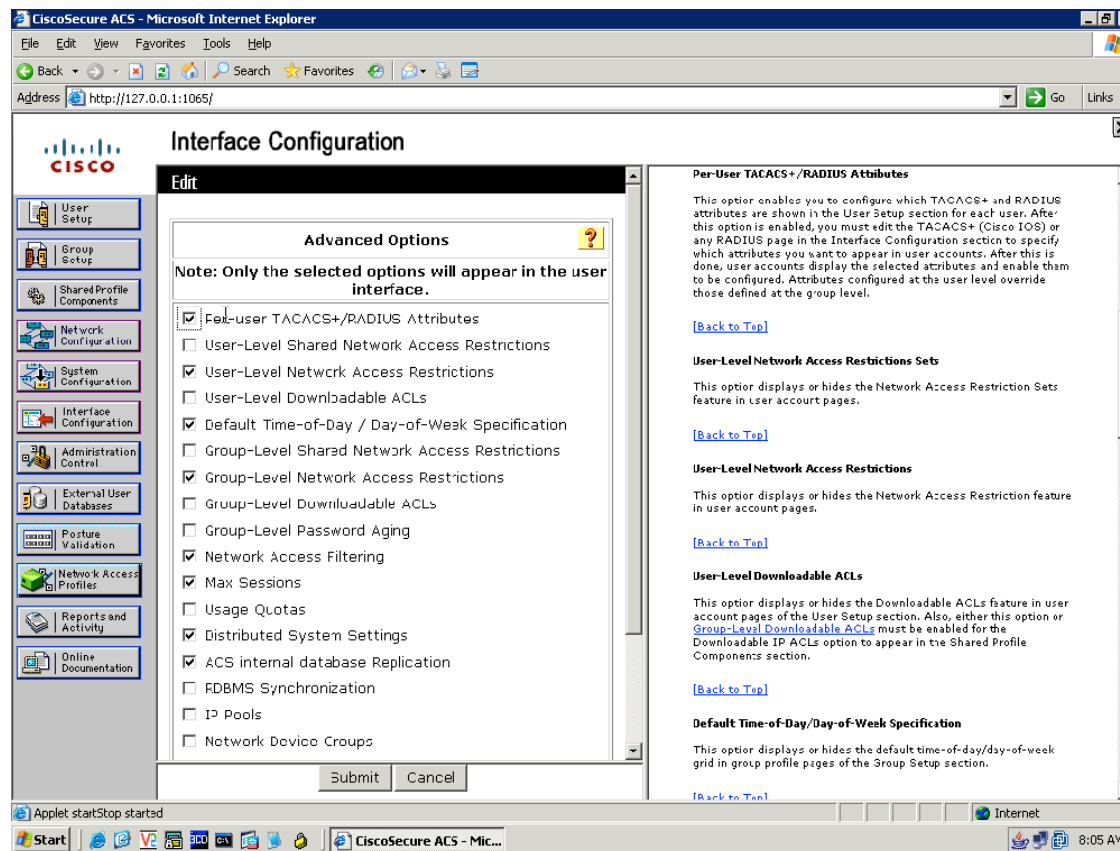
ACS Configuration

Add switch to ACS as RADIUS (IETF). RADIUS (Cisco IOS/PIX 6.0) can also be used, and is required for some advanced features such as MDA.



ACS Configuration

Under Interface Configuration / Advanced Options select Per-User TACACS+/RADIUS Attributes



ACS Configuration

If ACS will be performing VLAN assignment, add the necessary attributes.
Interface Configuration / RADIUS (IETF) and select options 64, 65, and 81
The left column for user and right for group level attributes

- | | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> [064] Tunnel-Type |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> [065] Tunnel-Medium-Type |
| <input type="checkbox"/> | <input type="checkbox"/> [065] Tunnel-Client-Endpoint |
| <input type="checkbox"/> | <input type="checkbox"/> [067] Tunnel-Server-Endpoint |
| <input type="checkbox"/> | <input type="checkbox"/> [069] Tunnel-Password |
| <input type="checkbox"/> | <input type="checkbox"/> [071] ARAP-Features |
| <input type="checkbox"/> | <input type="checkbox"/> [072] ARAP-Zone-Access |
| <input type="checkbox"/> | <input type="checkbox"/> [073] Configuration-Token |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> [081] Tunnel-Private-Group-ID |

ACS Configuration

Add a new user, give a password

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The browser's address bar shows the URL `http://127.0.0.1:1065/`. The main content area is titled "User Setup" and displays the configuration for a new user named "dot1x-user".

The interface includes a left-hand navigation menu with the following items: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation.

The "User Setup" form is divided into several sections:

- Filter:** A section with a checkbox for "Account Disabled".
- Supplementary User Info:** Fields for "Real Name" and "Description".
- User Setup:** A section for "Password Authentication" with a dropdown menu set to "ACS Internal Database". Below this is a note: "CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)". It includes fields for "Password" and "Confirm Password", both masked with dots. There is also a checkbox for "Separate (CHAP/MS-CHAP/ARAP)".

At the bottom of the form are "Submit" and "Cancel" buttons. A "Help" sidebar on the right contains a list of links for various configuration topics, including "Account Disabled", "Deleting a Username", "Supplementary User Info", "Password Authentication", "Group to which the user is assigned", "Callback", "Client IP Address Assignment", "Advanced Settings", "Network Access Restrictions", "Max Sessions", "Usage Quotas", "Account Disable", "Downloadable ACLs", "Advanced TACACS+ Settings", "TACACS+ Enable Control", "TACACS+ Enable Password", "TACACS+ Outbound Password", "TACACS+ Shell Command Authorization", "Command Authorization for Network Device Management Applications", "TACACS+ Unknown Services", "IETF RADIUS Attributes", "RADIUS Vendor-Specific Attributes", and "Time Bound Alternate Group".

Below the links, there is a section titled "Account Disabled Status" with the text: "Select the Account Disabled check box to disable this account; clear the check box to enable the account." and a "[Back to Top]" link. At the very bottom of the help sidebar, there is a section titled "Deleting a Username" with the text: "The Delete button appears only when you are editing an existing user."

The Windows taskbar at the bottom shows the Start button, several application icons, and the system tray with the time "8:18 AM".

ACS Configuration

Scroll down to IETF Attributes, select options 64, 65, and 81 and assign the following values. The VLAN name for option 81 must match the vlan name as shown in show vlan brief.

IETF RADIUS Attributes

[064] Tunnel-Type

Tag Value

Tag Value

[065] Tunnel-Medium-Type

Tag Value

Tag Value

[081] Tunnel-Private-Group-ID

Tag Value

Tag Value

ACS Configuration

If ACS will be performing VLAN assignment, and you've added the switch to ACS as RADIUS (Cisco IOS/PIX 6.0), then select Cisco-AV-Pair 26 from Interface Configuration / RADIUS (Cisco IOS/PIX 6.x). Then add the specific av-pair config to the user or group.


Interface Configuration

Edit

RADIUS (Cisco IOS/PIX 6.x)

User Group

<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	[026/009/001] cisco-av-pair
<input type="checkbox"/>	<input checked="" type="checkbox"/>	[000/000/001] cisco-av-pair

Cisco IOS/PIX 6.x RADIUS Attributes 

[009\001] cisco-av-pair

```
tunnel-type=VLAN
tunnel-medium-type=ALL_802
tunnel-private-group-
id=User_VLAN
```

Advanced Features

- Authentication-Failed VLAN
- Guest VLAN
- Inaccessible Authentication Bypass (IAB)
- Multi-Domain Authentication (MDA)

Auth-Fail VLAN

- Used to provide limited access after failed authentication
- The # of failed attempts is configurable from 1-3, 3 default
- Failed client is placed into a VLAN where an ACL is applied
- Simulated EAP-Success message sent to client
- Client remains in auth-fail VLAN until reauth or reconnect
- Create the VLAN!

Required:

```
switch(config)# vlan <auth-fail vlan #>  
switch(config)# interface x/x  
switch(config-if)# dot1x auth-fail vlan <vlan>
```

Optional:

```
switch(config-if)# dot1x auth-fail max-attempts <attempts>
```

Guest VLAN

- Used to provide limited access for NAHs (NAC agentless hosts) or devices with no supplicant
- Initiated when the client does not respond to EAP packets from switch, not sending any EAPoL packets.
- NAH is placed into a VLAN where an ACL is applied
- Create the VLAN!

Required:

```
switch(config)#vlan <guest vlan #>
```

```
switch(config)#interface x/x
```

```
switch(config-if)#dot1x guest-vlan <vlan>
```

Optional:

```
switch(config-if)#dot1x timeout tx-period <seconds>    default is 5. Range 1 - 65535
```

IAB Mode

- Provides limited access when the Authentication server is down or unreachable
- Pre-configured “critical” ports bypass authentication during IAB mode
- Switch keeps heartbeat with RADIUS to detect the outage
- Create the VLAN!

Required:

```
switch(config)#radius-server host <primary RADIUS IP> auth-port 1645 acct-port 1646
                        test username <name> idle-time <minutes>
switch(config)# vlan <IAB vlan #>
switch(config)# interface x/x
switch(config-if)# dot1x critical
switch(config-if)# dot1x critical vlan <vlan#>
switch(config-if)# dot1x critical recovery action reinitialize
```

Optional:

```
switch(config)# radius dead-criteria time <seconds> tries <#>
switch(config)# radius deadtime <minutes>
```

MDA Mode

- Carves physical port into two domains: DATA and VOICE
- A single data device and voice device independently authenticate onto the port
- Voice-Aware .1x (introduced in 12.2(52) should be used)
- RADIUS sends special attribute

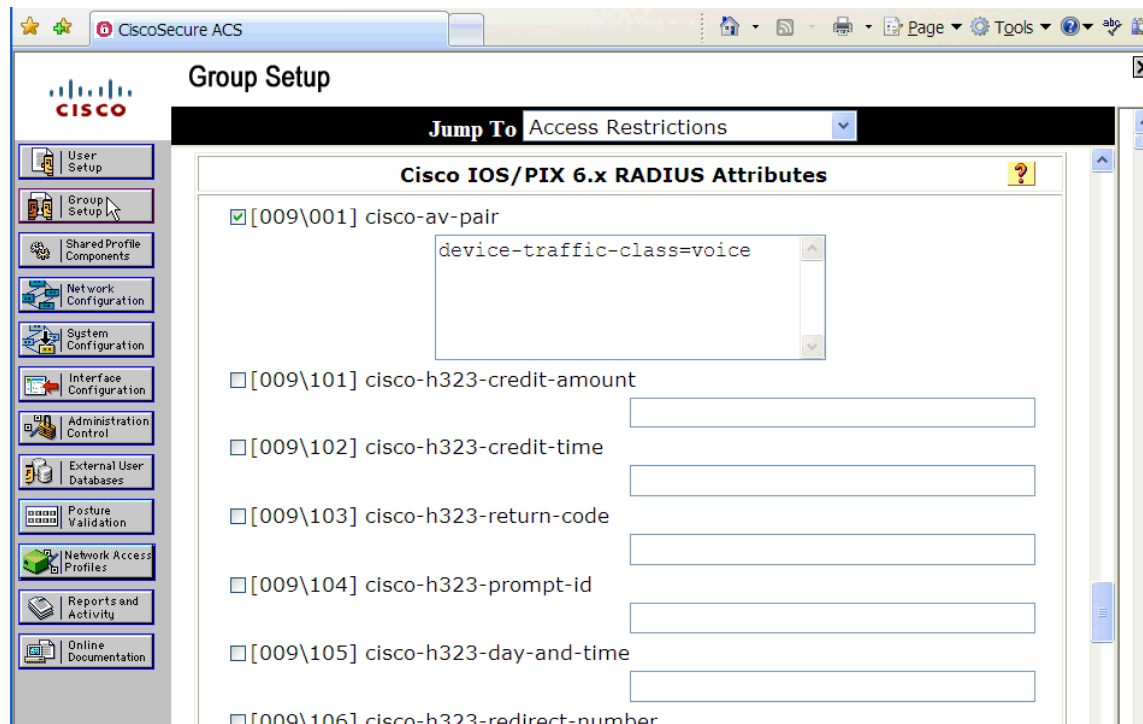
```
switch(config)# radius-server vsa send authentication ←Enable switch ability to recognize  
vendor specific attributes, specifically authentication
```

```
switch(config)# interface x/x  
switch(config-if)# dot1x host-mode multi-domain
```

```
Voice-aware .1x  
errdisable detect cause security-violation shutdown vlan  
errdisable recovery cause security-violation
```

MDA Mode cont.

- Add switch ACS as Cisco (IOS/PIX 6.x RADIUS) flavor
- Within Group or User, jump to this section and add the special attribute to cisco-av-pair



Dot1x vs. Authentication cmds

- Be aware of dot1x command syntax change!
- 12.2(50) config guides start to reference “authentication” form of commands.
- CCIE Security Blueprint says “12.2(44)SE or above”
- Be prepared for both formats for lab AND real world

Command Differences

■ dot1x

- A. dot1x port-control auto
- B. dot1x auth-fail vlan <vlan#>
- C. dot1x critical
- D. dot1x critical vlan <vlan#>
- E. dot1x critical recovery action reinitialize
- F. dot1x guest <vlan#>
- G. dot1x host-mode <mode>
- H. dot1x violation <action>

■ authentication

- A. authentication port-control auto
- B. authentication event fail action authorize vlan <vlan#>
- C. Consolidated into authentication event server dead action authorize vlan <vlan#>
- D. authentication event server dead action authorize vlan <vlan#>
- E. authentication event server alive action reinitialize
- F. authentication event no-response action authorize vlan <vlan#>
- G. authentication host-mode <mode>
- H. authentication violation <action>

Verification/Troubleshooting - 1

```
switch(config)#int f0/1
switch(config-if)#dot1x port-control auto
      ^
% Invalid input detected at '^' marker.
Switch(config-if)#switch mode access
Switch(config-if)#dot1x port-control auto
Switch(config-if)#
```

```
switch(config-if)#authentication ?
% Unrecognized command
switch(config-if)#switch mode access
switch(config-if)#authentication ?
<output removed>
```

- 802.1x is only allowed on certain port types
- Supported on static access, voice, L3 routed ports
- Not supported on trunk, dynamic, etherchannel, SPAN/RSPAN destination ports.

Verification/Troubleshooting - 2

- Be careful when enabling aaa via aaa new-model. Default action for all "login" lines is to prompt for Username/PW

```
switch#sh run | beg line con 0  
line con 0  
line vty 0 4  
password cisco  
login
```

```
switch#10.10.10.10  
Trying 10.10.10.10 ... Open  
  
User Access Verification  
Password:  
switch>
```

```
switch(config)#aaa new-model  
  
switch#10.10.10.10  
Trying 10.10.10.10 ... Open  
  
User Access Verification  
  
Username:
```

```
switch(config)#aaa authentication login VTY line  
switch(config)#line vty 0 4  
switch(config-line)#login authentication VTY
```

```
switch#10.10.10.10  
Trying 10.10.10.10 ... Open  
  
User Access Verification  
  
Password:
```

Verification/Troubleshooting - 3

show aaa server – Use to verify the status of each configured ACS server as determined via the switch.

Example:

RADIUS: id 7, priority 1, host **10.10.10.10**, auth-port 1645, acct-port 1646

State: current UP, duration 245628s, previous duration 240s

Dead: total time 420s, count 2

Authen: request 4358, timeouts 28

Response: unexpected 0, server error 0, incorrect 0, time 58ms

Transaction: success 4330, failure 7

Author: request 0, timeouts 0

Response: unexpected 0, server error 0, incorrect 0, time 0ms

Transaction: success 0, failure 0

Account: request 5, timeouts 4

Response: unexpected 0, server error 0, incorrect 0, time 52ms

Transaction: success 1, failure 1

Elapsed time since counters last cleared: 3d20h18m

RADIUS: id 8, priority 2, host **10.20.20.20**, auth-port 1645, acct-port 1646

State: current UP, duration 246004s, previous duration 0s

Dead: total time 0s, count 0

Authen: request 4324, timeouts 1

Response: unexpected 0, server error 0, incorrect 0, time 99ms

Transaction: success 4323, failure 0

Author: request 0, timeouts 0

Response: unexpected 0, server error 0, incorrect 0, time 0ms

Transaction: success 0, failure 0

Account: request 2, timeouts 0

Response: unexpected 0, server error 0, incorrect 0, time 86ms

Transaction: success 2, failure 0

Elapsed time since counters last cleared: 3d20h18m

Verification/Troubleshooting - 4

show dot1x int <int> details – Use to see current status of the port and which VLAN it is a member of as well as specific dot1x settings on the port

Dot1x Info for FastEthernet0/1

```
-----  
PAE = AUTHENTICATOR  
PortControl = AUTO  
ControlDirection = Both  
HostMode = SINGLE_HOST  
ReAuthentication = Disabled  
QuietPeriod = 60  
ServerTimeout = 30  
SuppTimeout = 30  
ReAuthPeriod = 3600 (Locally configured)  
ReAuthMax = 2  
MaxReq = 2  
TxPeriod = 30  
RateLimitPeriod = 0  
Critical-Auth = Enabled  
Critical Recovery Action = Reinitialize  
Critical-Auth VLAN = 456  
Auth-Fail-Vlan = 123  
Auth-Fail-Max-attempts = 3
```

Dot1x Authenticator Client List

```
-----  
Supplicant = 000d.561a.f2ac  
Auth SM State = AUTHENTICATED  
Auth BEND SM Stat = IDLE  
Port Status = AUTHORIZED  
Authentication Method = Dot1x  
Authorized By = Authentication Server
```

The “Authorized By” field will change dependent on how the port was authorized. The options are:
Authentication Server – Normal operation
Auth-Fail-Vlan - Connecting client failed authentication
Critical-Auth – Connecting client was authenticated while ACS servers were down

Verification/Troubleshooting - 5

show authentication session – This is used to show devices that have been authenticated, and if using multi-domain for VoIP integration, shows how the phone and PC are authenticated into the phone and data domain respectively.

```
Interface MAC Address Method Domain Status Session ID
Gi3/3 0007.3bc2.b093 dot1x VOICE Authz Success 0A0C0A0B00002049473753C4
Gi3/3 001f.e212.19c7 dot1x DATA Authz Success 0A0C0A0B0000204C476AD2C0
```

show vlan brief – Used to show the current vlan a particular port is assigned to, this changes dynamically as the port is shifted around the various 802.1x VLANs

Example:

```
VLAN Name Status Ports
-----
10 User_VLAN active Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8
120 Inaccessible_Authentication_VLAN active
130 Authentication_Failed_VLAN active
140 Guest_VLAN active
```

dot1x initialize interface <int> - Used to manually re-initialize a port and restart the 802.1x process regardless of the ports current state.

dot1x re-authenticate interface <int> - Used to manually re-authenticate a port after a port is already authorized.

ACS Demo



Questions?

www.ccbootcamp.com
1 (877).654.2243

Forums:
www.securityie.com
www.routerie.com
www.voiceie.com

Tim Rowley – trowley@ccbootcamp.com

