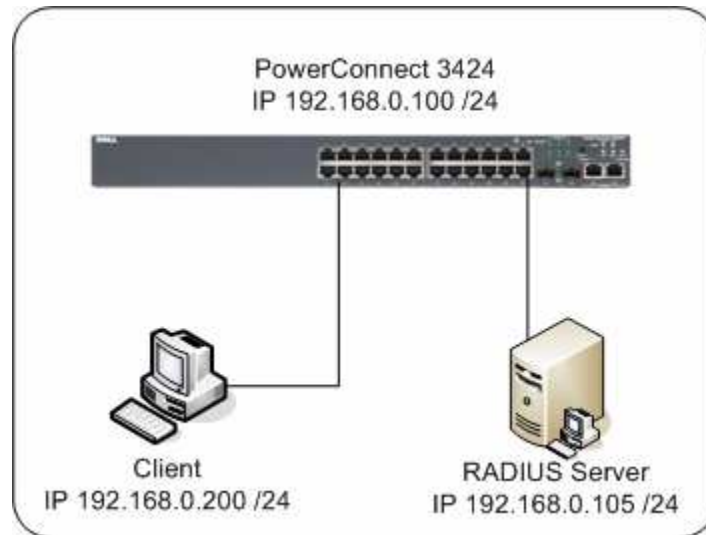


Configuring RADIUS authentication on a PowerConnect 3424 using Cisco Secure ACS

Written by: Greg Gibbs
9/30/2005

The configuration listed in this document is based on the following topology:



Step 1 – Configuring the switch (from defaults)

Configure the IP address for VLAN 1:

```
console# config
console(config)# interface vlan 1
console(config-if)# ip address 192.168.0.100 /24
```

Configure a local user named user1 with password user1 and level 15 privilege:

```
console(config)# username user1 password user1 level 15
```

Define the RADIUS server and specify the shared secret key “mysecretkey”

```
console(config)# radius-server host 192.168.0.105
console(config)# radius-server key mysecretkey
```

Create an authentication method called radius_local that will attempt to authenticate via RADIUS, then use the local database if communication to the radius server cannot be established:

```
console(config)# aaa authentication login radius_local radius local
```

Bind this authentication method list to the telnet line:

```
console(config)# line telnet
console(config-line)# login authentication radius_local
```

Step 2 – Configuring the RADIUS server

Open the Cisco Secure ACS application. This is typically done by typing “http://<IP address>:2002” into a web browser.

Select the Network Configuration tab and add the switch as an AAA Client using the Add Entry button.

CISCO SYSTEMS Network Configuration

Select

AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
5324-30	192.168.0.30	RADIUS (Cisco IOS/PIX)

Add Entry

AAA Servers		
AAA Server Name	AAA Server IP Address	AAA Server Type
blade3	192.168.0.103	CiscoSecure ACS for Windows 2000/NT

Add Entry

Input the AAA Client Hostname, IP Address and shared secret key:

CISCO SYSTEMS Network Configuration

Edit

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Key:

Authenticate Using:

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Submit Submit + Restart Cancel

Click Submit + Restart

Add the server as an AAA Server using the Add Entry button under the AAA Servers section. Input the AAA Server Hostname, IP Address and shared secret key. Use the “Cisco Secure ACS Windows 2000/NT” option for the AAA Server Type:

Add AAA Server

AAA Server Name: RADIUS_Server
AAA Server IP Address: 192.168.0.105
Key: mysecretkey
 Log Update/Watchdog Packets from this remote AAA Server
AAA Server Type: CiscoSecure ACS for Windows 2000/NT
Traffic Type: inbound/outbound

Submit Submit + Restart Cancel

Click Submit + Restart

Select the Group Setup tab and define a group for managing the switch. Edit the group settings to reflect the following options:

Callback – No callback allowed:

Callback

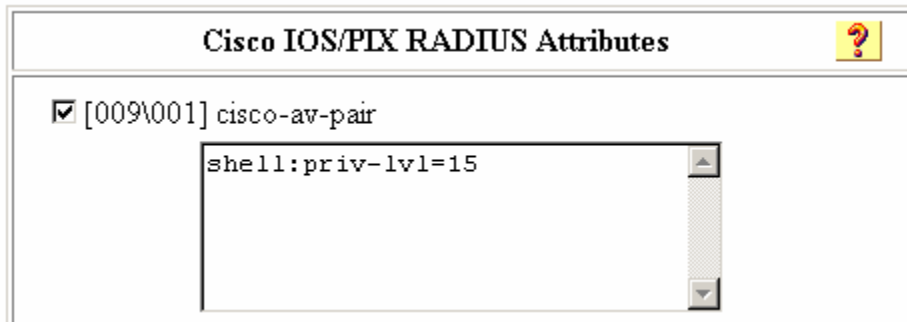
No callback allowed
 Dialup client specifies callback number
 Use Microsoft NT/2000 Callback settings (where possible)

IP Assignment – No IP Address Assignment:

IP Assignment

No IP address assignment
 Assigned by dialup client
 Assigned from AAA Client pool

Cisco IOS/PIX RADIUS Attributes:

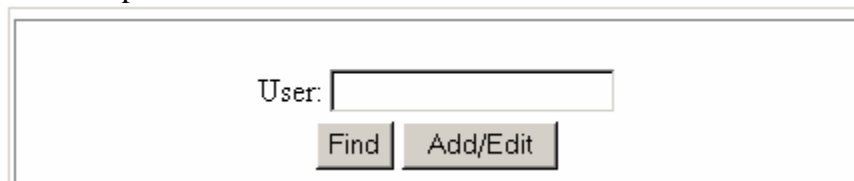


For an Administrator account, use priv-lvl = 15

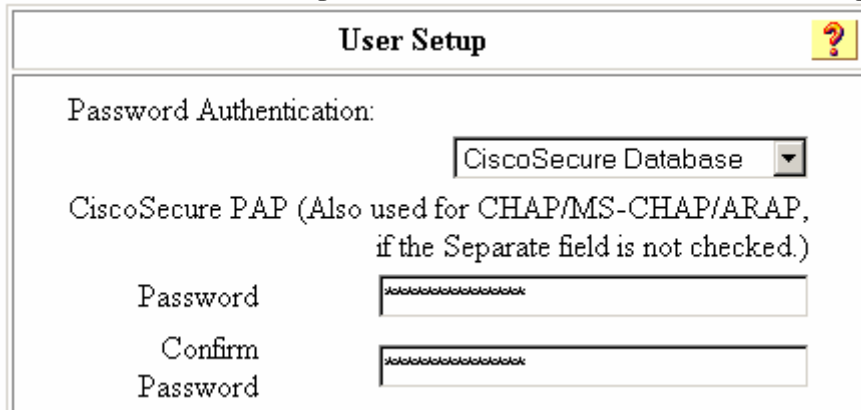
For a Guest account, use priv-lvl=1

Verify that all other Attributes are left unchecked. Click Submit + Restart.

Select the User Setup tab and use the Add/Edit User button to create a user:

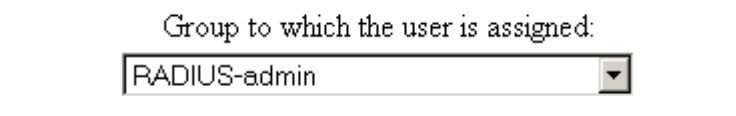


Select the CiscoSecure Database option for the Password Authentication drop-down box:



Configure a password for the user. The same password should be used for PAP and CHAP, so leave the Separate box unchecked.

Use the drop-down box to assign the user to the previously configured group:



Use the group settings for all other options. Submit the changes.

Note: You may need to restart the service after making any changes. To do so, use the Restart button on the System Configuration tab.

Telnet from the client to the switch and use the RADIUS user credentials to authenticate.