Authenticating a Lucent Portmaster 3 with Microsoft IAS and Active Directory

The following tutorial will help you to setup a Portmaster 3 to authenticate your dial in users to Active Directory using IAS (Internet Authentication Service).

IAS is Windows 2000's solution to authenticating RADIUS clients. You will need a Windows 2000 Domain Controller running IAS to proceed.

Setting up the Portmaster

You will need to predetermine some information before setting up the Portmaster. Before proceeding, decide what information will be used for the following:

- Hostname
- System Password
- IAS server IP address and secret
- DNS server IP address
- Line Type (T1/PRI)
- DHCP Address Range for dial in

For this example I used the following setup:

Subnet:	172.16.0.0
Mask:	255.255.0.0
Gateway:	172.16.254.254
Hostname:	myportmaster.mysite.domain.com
Host IP:	172.16.254.253
DHCP Pool:	172.16.1.1 – 172.16.1.16
DNS:	172.16.254.14
	172.16.254.13
SYSLOG Server:	172.16.254.4
RADIUS Server:	172.16.254.10
RADIUS Secret:	radpass

1) Connect to the Portmaster via Null Modem Cable.
    a. I am not sure of the exact needed configuration but, 9600 8-N-1 works.

2) Login to the Portmaster as root by entering
    a. Username: **!root**
    b. Password: *nopassword / blank*

3) First set the System Name. This is the hostname of the Portmaster.
    a. **set sysname myportmaster**

4) Set the Password.

a. **set password mypass**

5) Set the IP Address of the Radius Host. This is the IP address that the Portmaster will use when communicating with the RADIUS Server. This IP Address can be the same as the IP address that you set for the first Ethernet port.
   a. **set host 172.16.254.253**

6) Set your Default Gateway. This can be your Gateway to the Internet or a local router.
   a. **set gateway 172.16.254.254**

7) Turn off RIP advertisements.
   a. **set default off**

8) Set up the name services to be either DNS or NS.
   a. **set namesvc dns**

9) Set the first name server IP address.
   a. **set nameserver 172.16.254.14**

10) set the second name server IP address (if available).
   a. **set nameserver 2 172.16.254.13**

11) Now you will need to set the domain name of the Portmaster. This is the just the name of the domain the Portmaster resides in. For example: If your Portmaster is named myportmaster.mysite.domain.com, then your domain name is mysite.domain.com
   a. **set domain mysite.domain.com**

12) If you have a SYSLOG server running on your network then set the IP address of the SYSLOG server. It is good to use a SYSLOG Server at least in the initial setup to help troubleshoot problems with the Portmaster. If you don't know how to setup SYSLOG in Unix, then you should check out Kiwi Syslog. Kiwi Syslog has a free lite version that will run under Win32. http://www.kiwisyslog.com/
   a. **set loghost 172.16.254.4**
   b. You can also change the terminology it will use to log on the syslog server. If you don't change the terminology the Portmaster will default to kernel.emerg
      i. **set termin port.authent**

13) Now DHCP. To setup the address pool the Portmaster will give to dial in users, enter the following with your own values.
   a. Enter the first address of the DHCP pool. **set assigned 172.16.1.1**
   b. Now enter how many addresses to use. **set pool 15**

This will give me an address pool of 172.16.1.1 – 172.16.1.16

14) Now set the Address of the IAS / RADIUS Server the Portmaster will authenticate to. Remember this is your Active Directory Domain Controller that is running IAS.
    a. **set auth 172.16.254.10**

    Now you will need to establish a secret (or password). This password is used by the RADIUS Client (Portmaster) to authenticate itself before authenticating your users.
    b. **set secret radpass**

15) Now after all of these configurations have been made you will need to save them to the Portmaster.
    a. **save all**

Now that the Portmaster is setup we will need to configure the Ethernet port on the Portmaster. In this example I am only going through setting up the first Ethernet port. You can repeat this process for the second Ethernet port by replacing "0" with "1" in the commands.

16) Give the Ethernet port a IP address. I made this the same as my host address that was used in Step #5.
    a. **set ether0 172.16.254.253**

17) Set the Subnet mask of the Ethernet port.
    a. **set ether0 netmask 255.255.0.0**

18) Set the broadcast address. If you want to use a broadcast address of all ones (172.16.255.255) the use "high" and if you should choose to use a broadcast address of all zeros (172.16.0.0) then use "low". If you are unsure the just choose "high", this is the most commonly used.
    a. **set ether0 broadcast high**

19) For a basic setup you will not need routing. If you should choose to enable this feature after learning more about the Portmaster's functions then you can do that as well. Disable routing.
    a. **set ether0 routing off**

20) Now we need to set the Portmaster to use CHAP instead of PAP. CHAP stands for Challenged Handshake Authentication Protocol. This will provide a secure transmission of your user's passwords and allow the Portmaster to work with Active Directory. I have also found that in testing the two authentication methods, CHAP works the best with MAC OS 10.2.6. There seemed to be a couple problems authenticating MAC OS 10.2.6 to the Portmaster using PAP.
    a. **set chap on**

b. **set pap off**

21) Now save all your configurations
    a. **save all**

The final thing to configure on the Portmaster is the Telco line. You will need to contact your telephone provider if you are unsure of the line type, framing, encoding, or signal. It will be helpful to have the reference guide from www.portmasters.com.

22) Set the Line type. The line can be setup as **isdn**, **t1**, **e1**, **fractional**, **isdn-fractional**, **inband**. If you are unsure what you should use then you should look at the command reference from Portmaster (Page 303-304 in the PDF). In this setup we will use isdn. You should also use isdn if your line is a PRI circuit.
    a. **set line0 isdn**

23) Set the Framing Format. The framing format can be **esf**, **d4**, **crc4**, and **fas**. Probably the most commonly used is going to be **esf** or **d4**. In our example we used esf.
    a. **set line0 framing esf**

24) Set the Encoding method. This can be **b8zs, AMI,** or **hdb3**.
    a. **set line0 enc B8ZS**

25) If you have a channelized T1 then you will need to set the signal to either **wink**, **immediate,** or **fxs**.
    a. **set line0 sig wink**

Your Portmaster should be ready to go now. To view all the configurations you just made you can type: **show global** . If you slip up somewhere along this process or want to just start over you can delete all the configurations. See the last page of this document.

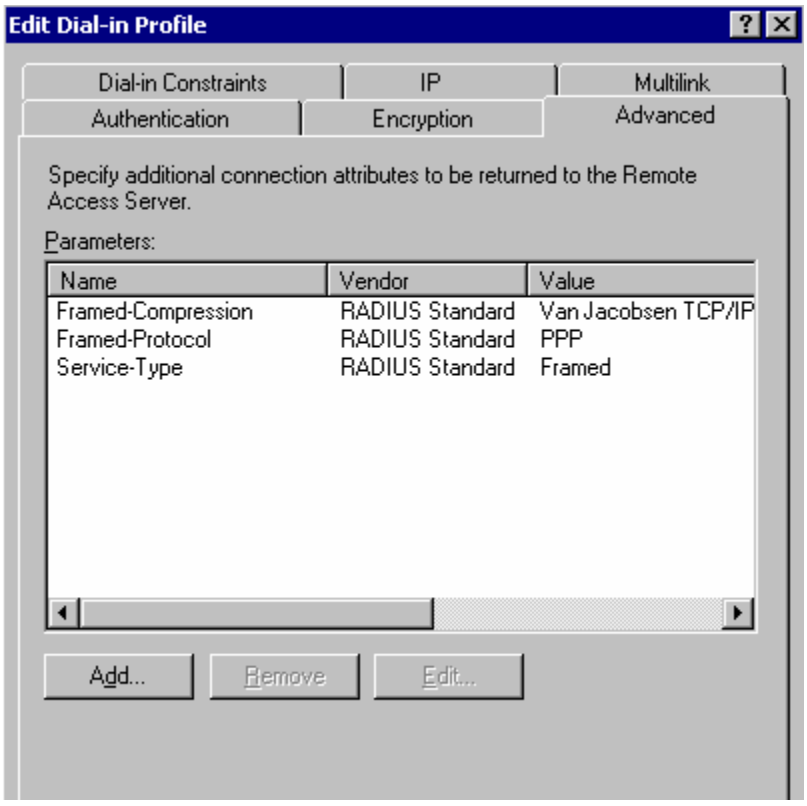
Otherwise proceed to **Setting up IAS**.

Setting up IAS

First we need to add the Portmaster to IAS as a RADIUS client. Here you will need to recall the Portmaster host address and the secret that was setup in the earlier steps.

1) Open IAS and click the Clients folder.
2) Right-Click the "Clients" folder then choose "New Client".
3) For Friendly Name, name your Portmaster in IAS. I will just use my Portmaster's hostname.
    a. Friendly Name: **myportmaster**
4) Choose Protocol: **RADIUS**
5) Click Next.

6) For the Client Address (IP or DNS) enter the IP address of your Portmaster.
    a. **172.16.254.253**
7) For Vendor choose: **Livingston Enterprise's**
8) Click "Client must always send signature attribute". Now enter the secret you used in Step #14.
    a. Secret: **radpass**
    b. Confirm: **radpass**
    c. Click Ok/Finish
9) Now your Portmaster will be listed in the clients folder.
10) Now Click "Remote Access Policies" in the left pane. Then right click the Policy "Allow access if dialin permission is enabled" and choose properties.
11) Check under "If a user matches a condition" that "Grant Permission" is selected.\
12) Click Edit Profile.
13) Select the IP tab. Now choose "Server must supply an IP address".
14) Select the Authentication Tab. The only thing that should be checked under this tab is: **Encrypted Authentication (CHAP)**
15) Click the Advanced Tab.
16) You should add the following Parameters to match what is below.
    a. Frame-Compression: Van Jacobson
    b. Framed-Protocol: PPP



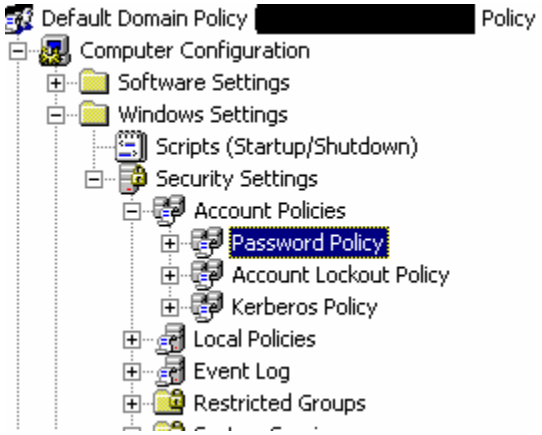
The Portmaster is now setup to communicate with IAS and authenticate your users. There are a couple of things that need to be setup in Active Directory and IAS to allow your users to login.

Active Directory

The first thing to setup in Active Directory is Reverse Encryption. We need to tell Active Directory to store its user's passwords in an encrypted form instead of plain text. Active Directory defaults to store the passwords in plain text. When you change to Reverse Encryption, then all the current users that are in Active Directory will remain to have there passwords stored in plain text. The passwords for current users will not begin to be stored in Reverse Encryption until the password is reset for the user. After changing to Reverse Encryption I found myself having to reset the password on 300 user accounts. Keep in mind you can just reset the password to the same password without changing it. Any new users added after going to Reverse Encryption will have their passwords stored in Reverse Encryption.

* Using Reverse Encryption will not affect the functionality of your Active Directory domain, and you are also not required to change the password on every user in the domain for them to continue logging in to the domain.

1) Open the "Active Directory Users and Computers" snap-in.
2) Right click your domain name in the left pane of the snap-in. Now choose "Properties".
3) Click the Group Policy Tab.
4) If you do not already have a Group Policy Object Link listed. Then click "New" and name it. Now Double-click the Group Policy to edit it.
5) Now navigate to the following group policy key.



6) Now double-click the Key – "Store passwords using reversible encryption for all users in domain" and **enable** it. Click OK to save it.
7) Close Group Policy and Click OK to the Domain Properties.

Now if you will need to reset account passwords, then I suggest going ahead and resetting the password on any account that you will be using for testing you dialup setup. You could also just add a new account to Active Directory for testing the dial up.

Now all you need to do is dial in and authenticate as username and password. The username doesn't need to include the domain (domain\user).

There are a couple GUI Tools you can download to help you with configuring the Portmaster. PMVision is available at www.portmasters.com which will add a GUI feel to those who fear the terminal.

created by: Forrest Beck
forrest.beck@verizon.net

Terminal or telnet into the Portmaster.

1. **Set the console and the debug value.**

   Command> **set console**
   Setting CONSOLE to port S0

   Command> **set debug 0x72**
   Setting debug value to 0x72

2. **Enter the erase configuration command.**

   Command> **erase configuration**
   Erasing FLASH cell 2 - 28F010 ... Succeeded in 82 tries
   Successfully erased FLASH configuration

3. **Reboot the PortMaster.**

   Command> **reboot**