How To | Set Up a RADIUS Server for User Authentication

Introduction

This document provides information on how to set up a RADIUS server to authenticate users who access the device by Telnet or via the console port. It makes use of commands and features modified or added with the release of 2.7.3. and 2.7.4.

This example was tested in the lab with an AT-8948 switch and a FreeRADIUS server on Mandrake 10.0. The AT-8948 configuration may easily be set on any one of Allied Telesyn's Layer 3 switches or routers.

Throughout this document the term **client** refers to the Allied Telesyn device. This is the device that the user tries to login to. The term **server**(s) describes the RADIUS server(s); **user** is the name entered at the console or Telnet login-prompt.

Commands used in this document

```
ADD RADius POrt ACCPort SECret SERVER
SET RADius [TIMEOut=1..15] [DEAdtime=0..1440] [RETransmitcount=1..5]
SHow RADius [DEBug]
ADD USER RSO
ADD USEr=login-name LOgin={True|False|ON|OFf|Yes|No} PAssword=password
[RADiusbackup={ON|OFF|YES|NO|True|False}] [other-options...]
```

What information will you find in this document?

This document provides information on how to configure:

Which product and software version does this information apply to?

The information provided in this document applies to:

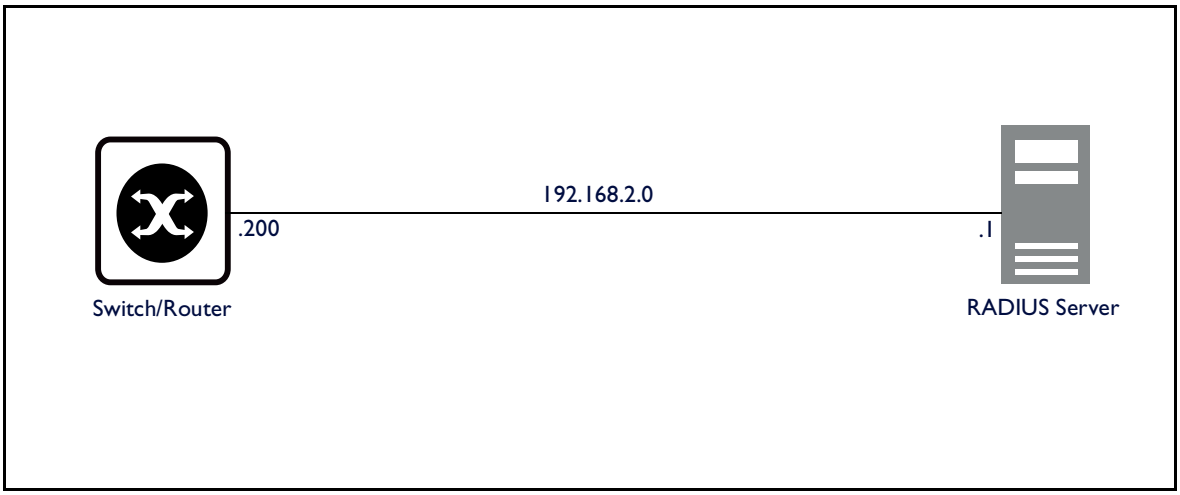
Products: AT-AR440S, AT-AR450S, AT-AR700 Series, Rapier Series, AT-8600 Series, AT-8700 Series, AT-8800 Series, AT-8900 Series, AT-9800 Series, AT-9900 Series, SwitchBlade

Software release: 2.7.3+

Single RADIUS server for user authentication

In this example, we will authenticate all console and Telnet logins through a single RADIUS server.

Figure 1: Network configuration for a single RADIUS server



Configuration

The configuration for this setup is very simple. You need to setup the RADIUS server so that it recognises the client (192.168.2.200). For the RADIUS setup configuration, please refer to *FreeRADIUS sample configuration (on Mandrake 10.0), page 9*.

The client will use the key `"secret"` to identify its authenticity to the server. Access messages will be sent to port 1812 on the server and accounting packets will be sent to port 1813.

Note: *There are no accounting processes for Telnet/SSH/console logins.*

```
Manager > show config dynamic=ip

#
# IP configuration
#
enable ip
add ip interface=vlan1 ip=192.168.2.200

Manager > show config dynamic=radius

#
# RADIUS configuration
#
add radius server=192.168.2.1 secret="secret" port=1812 accport=1813
```

Description

In this setup, console and Telnet logins will first be checked against the local user database. If the name provided at the login prompt is not a local user then the RADIUS server will be queried. The user manager will still have normal Telnet and console access and will not be checked against the RADIUS server unless you have modified this configuration.

If a user fails to authenticate locally and is rejected by the RADIUS server, there will be no indication given to the terminal as to why the user has been denied access. However, an entry will be written to log.

```
24 08:21:59 3 TLNT AUTH  OK    Telnet connection accepted from
  192.168.2.1 (TTY 17)
24 08:22:06 3 USER USER  00011 allied login failed on TTY17,
               reason:No such user
```

Helpful information about the status of the RADIUS server can also be seen with the `show radius` command:

```
Manager > show radius

RADIUS Server Parameters
--------------------------------------------------------------------------------
  Server Retransmit Count....... 3
  Server Timeout................ 6 sec
  Server Dead Time.............. 0 min
--------------------------------------------------------------------------------

  Server           Port  AccPort  Secret  LocalInterface  Status
  ------------------------------------------------------------------------
  192.168.2.1      1812     1813  ******  Not set         Alive
  ------------------------------------------------------------------------
```

This information tells us that the RADIUS server is 192.168.2.1. The port to which Access-Requests are sent by the client to the server is 1812. RADIUS Accounting packets are sent to port 1813. The secret password that is shared between the RADIUS server and the client is not displayed for security reasons. A local interface was not set in this example. The status of the RADIUS server is reported as alive.

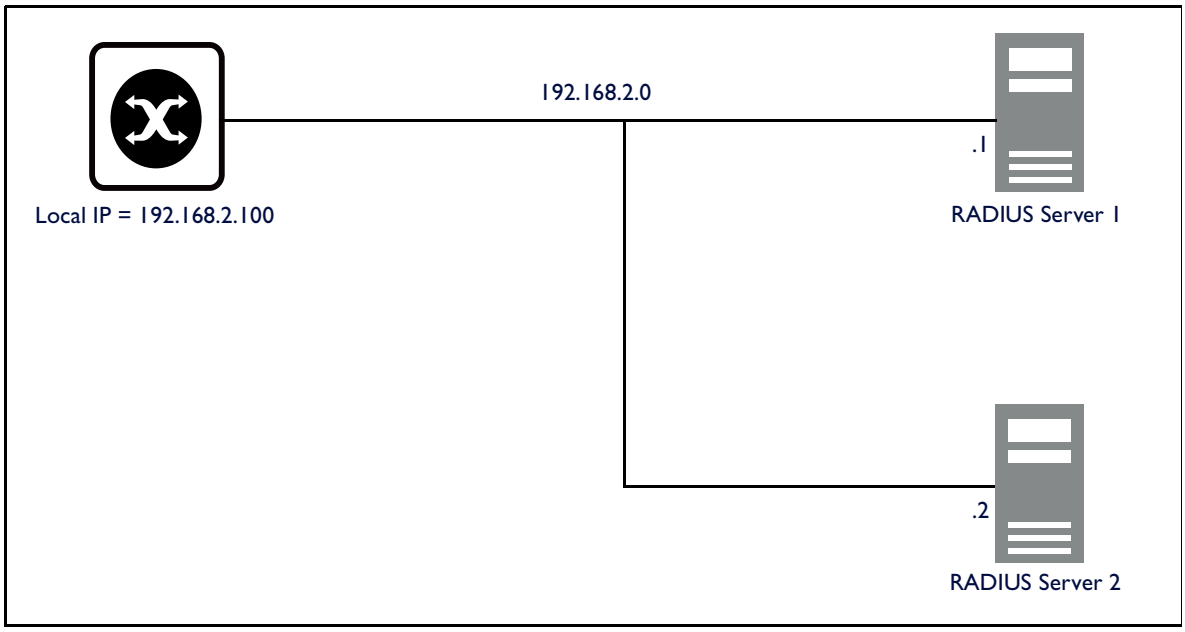
Two RADIUS servers with one for redundancy

To ensure that authentication on your network does not stop when the primary RADIUS server dies, you may choose to configure backup RADIUS servers. In this example, we will use one backup server.

We will change the RADIUS 'retransmit count', 'timeout period' and 'server dead time' on the client to speed up or slow down the wait period before the client decides that the primary server is dead and moves on to query the secondary server.

We will also set the client to use a Local IP as the source address for the packets it sends to the server.

Figure 2: Network configuration for two RADIUS servers



Configuration

The configuration for this setup is also quite straightforward. You need to setup the RADIUS server so that it recognises the client (192.168.2.100). For the RADIUS setup configuration, please refer to *FreeRADIUS sample configuration (on Mandrake 10.0), page 9*.

The client will use the key `"secret"` to identify its authenticity to the server. Access messages will be sent to port 1812 on the server and accounting messages will be sent to port 1813.

Note: *In the case of Telnet/SSH/console logins there are no accounting processes.*

In this example we need to add more than one RADIUS server and in the right order. The first server added will always be consulted first. If that server fails to respond to an Access-Request then the next server will be consulted after a retransmit count and timeout period.

```
Manager > show conf dynamic=ip

#
# IP configuration
#
enable ip
add ip interface=vlan1 ip=192.168.2.200
add ip local=1 ip=192.168.2.100

Manager > show conf dynamic=radius

#
# RADIUS configuration
#
add radius server=192.168.2.1 secret="secret" port=1812 accport=1813 local=1
add radius server=192.168.2.2 secret="secret" port=1812 accport=1813 local=1
```

Description

Your client will now send Access-Request messages to 192.168.2.1 via the local interface (192.168.2.100).

```
Manager > show radius

RADIUS Server Parameters
--------------------------------------------------------------------------
  Server Retransmit Count....... 3
  Server Timeout................ 6 sec
  Server Dead Time.............. 0 min
--------------------------------------------------------------------------

  Server           Port  AccPort  Secret  LocalInterface  Status
  ------------------------------------------------------------------
  192.168.2.1      1812     1813  ******  local1          Alive
  192.168.2.2      1812     1813  ******  local1          Alive
  ------------------------------------------------------------------
```

This information tells us that the first RADIUS server is 192.168.2.1 and the second is 192.168.2.2. The port to which Access-Requests are sent by the client to the server is 1812. RADIUS Accounting packets are sent to port 1813. The secret password that is shared between the server and the client is not displayed for security reasons. Here you see that the LocalInterface value is set to local1 IP 192.168.2.100, this is the source address of RADIUS packets. Both RADIUS servers are reported as being alive.

In this configuration, if the server 192.168.2.1 fails to respond to RADIUS packets sent by the client then the Status will not be marked as dead because of the Server Dead Time value of zero.

Server Dead Time can be configured with the `DEAdtime` command. DEAdtime is the length of time for which the server should be considered dead. The default is 0 minutes. When a RADIUS server cannot be contacted, it is considered 'dead' for a period of time. Configuring this will stop the client from continually trying to contact a server that it has already determined as dead.

```
set radius DEAdtime=1
```

This command tells the client not to send any RADIUS packets for one minute after determining that it is dead. As a result, the status will be changed appropriately.

```
Manager > show radius

RADIUS Server Parameters
--------------------------------------------------------------------------
  Server Retransmit Count....... 3
  Server Timeout................ 6 sec
  Server Dead Time.............. 1 min
--------------------------------------------------------------------------

  Server           Port  AccPort  Secret  LocalInterface  Status
  ------------------------------------------------------------------------
  192.168.2.1      1812     1813  ******  local1          Dead (< 1 min)
  192.168.2.2      1812     1813  ******  local1          Alive
  ------------------------------------------------------------------------
```

If a user attempts to log into this client while the first server is marked as dead, then the client will not send Access-Request packets to the dead server. Instead, the client will try the next server that is marked as alive.

The problem of long wait times for dead servers can be resolved by either changing the Server Retransmit Count, the Server Timeout Count or both.

The Server Retransmit Count value is the number of attempts after the first attempt that the client makes to contact the server. The default value is 3, which means that after 4 unsuccessful attempts to contact a RADIUS server the client will decide that the server is dead, and will move on to the next server that it believes is alive.

The Server Timeout default is 6 seconds. This is the time that the client waits between each unanswered transmit to the server. If the server has not responded in the specified timeout period then the client assumes that communication has failed.

Setting both the Server Retransmit Count and Timeout values can substantially reduce, or increase, the wait time at the login prompt. With the default values of Server Retransmit Count = 3 and Timeout = 6 and two RADIUS servers, if the first server is dead then the minimum time to establish a connection with the second server will be 24 seconds.

transmits (1+t)	multiplied by	timeout	equals	time in seconds
(1+3)	x	6	=	24

24 seconds would be regarded by many network administrators and users to be far too slow. Therefore, the ability to set Deadtime, Server Retransmit and Server Timeout was introduced in software release 2.7.3 to give the network administrator greater control over these times. If you were to reduce the Server Retransmit Count to 1 (minimum) and Timeout to 1 (minimum) then the wait time will be reduced significantly.

transmits (1+t)	multiplied by	timeout	equals	time in seconds
(1+1)	x	1	=	2

Implementing the minimum values would require the reliability of your network to be such that latency and error rates were very low.

Change the order that authentication is done

The use of the `radiusbackup` command changes the approach that the router or switch uses when it authenticates users from RADIUS and the User Authentication Database (the local users configured on the device).

Software releases before 2.7.4 search the User Authentication Database before contacting the RADIUS server. Software releases 2.7.4 and above permit the addition of Radius Unreachable (RU) users. As soon as the radiusbackup is set on a user, the switch or router will query the RADIUS server first.

If the RADIUS server is unreachable and RU users exist, then the router or switch will consult this database after it ascertains the RADIUS server is dead.

You can add any `radiusbackup` command to any user, for example:

```
add user=telnet password=telnet priv=manager login=yes radiusbackup=true
```

It is important to realise that all the other users will not be allowed to log in when the radius server is down unless you add:

```
Set user=<login-name> radiusbackup=true
```

to each user you require to authenticate from the User Authentication Database.

The `show user` command will show you details that includes information about RADIUS backup users:

```
Number of logged in Security Officers currently active ...1
Number of Radius-backup users..... 2
User Authentication Database
------------------------------------------------------------------------------
Username: dave ()
Status: enabled Privilege: Sec Off Telnet: yes Login: yes RBU: yes
Callback number: 0061393546786 Calling number: 5554491
Logins: 2 Fails: 0 Sent: 0 Rcvd: 0
Authentications: 0 Fails: 0
Username: manager (Manager Account)
Status: enabled Privilege: manager Telnet: yes Login: yes RBU: no
Logins: 4 Fails: 0 Sent: 0 Rcvd: 0
Authentications: 0 Fails: 0
------------------------------------------------------------------------------
Active (logged in) Users
------------------------
User Port/Device
Login Time Location
--------------------------------------------------------------------
manager Asyn 0
14:33:22 18-Apr-2002 local
manager Telnet 1
14:33:22 18-Apr-2002 10.1.1.1
--------------------------------------------------------------------
```

Tightening your Telnet security by restricting IP access

The act of reading this document shows that you are interested in securing your system. The system administrator should favour SSH logins over Telnet. Although Telnet traffic is insecure, Telnet can have some tightening of security with the restriction of IP access.

If, for example, your administrator has the IP address10.33.27.16 you may add Remote Security Officer (RSO) access restrictions to permit only that IP address.

```
add user=secoff pass=secoff priv=securityOfficer login=yes
set user=secoff telnet=yes netmask=255.255.255.255
enable user rso
add user rso ip=10.33.27.16
ena system security
```

A security officer has been added and system security has been turned on. While system security is on, the secoff user has greater powers than the manager user. With that power comes great responsibility, so remote connections for security officers have been limited to only connections from the IP address 10.33.27.16.

Normal users, including the manager, may still connect from any IP.

Note: *RSO settings do not control any aspect of SSH. If you want IP-level access-control to your device then the specific SSH user is set with this information. SSH users cannot be checked against a RADIUS database.*

FreeRADIUS sample configuration (on Mandrake 10.0)

In /etc/raddb/clients.conf

```
client 192.168.2.200 {
        secret = secret
        shortname = allied
}
```

In /etc/raddb/users

```
allied Auth-Type := Local, User-Password == "telesyn"
Service-Type = Login-User,
Login-Service = Telnet
```

With this configuration, your user **allied** should have limited Telnet and console access. In fact, **allied** should have these base commands at his/her disposal:

```
Connect Disconnect FINGer Help PING Reconnect SSH TELnet RTElnet TRAce LOGIN
LOGON LOgoff LOgout
```

To give **allied** Security Officer privileges set the Service-Type to 6. To give **allied** Manager privileges then set the Service-Type to 7. These privilege levels should be set with extreme caution. Ensure that you give your users only enough access to fulfil the tasks they are expected to perform.

For the second example, it is necessary to change the client ip to 192.168.2.100 in the file /etc/raddb/clients.conf

General log messages from RADIUS are normally written to /var/log/radius/radius.log, It is useful to watch this file when debugging, you might use this command on your Linux server:

```
tail -vf /var/log/radius/radius.log
```