Ethernet Routing Switch
1600, 8300, 8600, 2500, 4500, 5500
Ethernet Switch
460/470
Engineering

Authentication, Authorization and Accounting (AAA) for ERS and ES Technical Configuration Guide

E.M.E.A. IP Core Sales Engineering
Document Date: November 2010
Document Number : NN48500-558
Document Version: 1.1

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support.

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support.

Abstract

This document provides examples on configuring RADIUS & TACACS+ on the ERS 1600, 8300, 8600, 2500, 4500, 5500 and ES 460/470. This document covers some of the more popular Radius & TACACS+ commands and attributes how to configure server and client side. It gives also various examples with different users and details log files on client and server side. Finally some sniffer traces show how protocols exchange data between server and client.

Table of Contents

Conventions

This section describes the text, image, and command conventions used in this document.

Symbols:

Tip – Highlights a configuration or technical tip.

Note – Highlights important information to the reader.

Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

Text:

Bold text indicates emphasis.

Italic text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

ERS5520-48T# ***show running-config***

Output examples from Avaya devices are displayed in a Lucinda Console font:

ERS5520-48T# ***show running-config***

```
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 5520-24T-PWR
! Software version = v5.0.0.011
enable
configure terminal
```

1. Overview

Access control is the way you control who is allowed access to the network server and what services they are allowed to use once they have access. Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you set up access control on your network device or access server.

Network professionals have always been challenged with having many individuals manage multiple network devices with a single account. When problems occur it is nearly impossible to trace back accountability and identify what changes were made by whom. RADIUS was designed to combat the authentication and accounting (logging tied to user) problem; however, authorization (what an authenticated user was allowed to do) controls were still missing. TACACS+ (latest implementation of TACACS) has the ability to do authentication, authorization and accounting.

2. RADIUS

Remote Access Dial-In User Services (RADIUS) is a distributed client/server system that assists in securing networks against unauthorized access, allowing a number of communication servers and clients to authenticate user identities through a central database. The database within the RADIUS server stores information about clients, users, passwords, and access privileges, protected with a shared secret.

RADIUS is a fully open and standard protocol defined by RFCs (authentication [RFC 2865] and accounting [RFC 2866]). RADIUS protocol is an AAA protocol using IP framing with UDP port 1812 for authentication and port 1813 for accounting.

2.1 Feature Operation

A RADIUS application has two components:

- RADIUS server : A computer equipped with RADIUS server software (for example, a UNIX* workstation) that is located at a central office or campus. It has authentication and access information in a form that is compatible with the client. Typically, the database in the RADIUS server stores client information, user information, password, and access privileges, including the use of shared secret. A network can have at minimum one server for both authentication and accounting, or one server for each service.
- RADIUS client : A switch, router, or a remote access device equipped with RADIUS client software that sends the authentication request to the RADIUS server upon a user attempting to login via the RADIUS client. The client is the network access point between the remote users and the server.

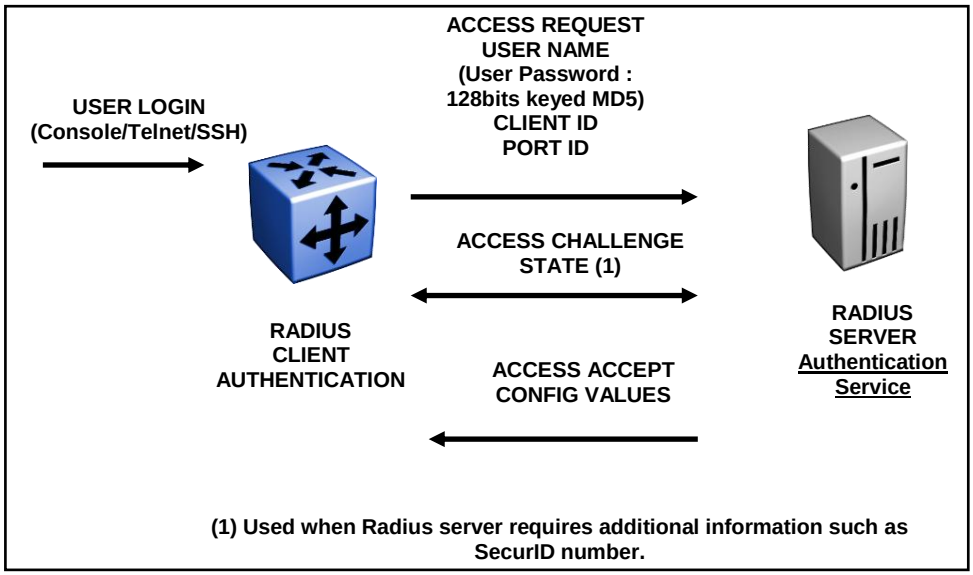
The RADIUS process includes:

- RADIUS authentication, which you can use to identify remote users before you give them access to a central network site.
- RADIUS accounting, which enables data collection on the server during a remote user's dial-in session with the client.

2.1.1 RADIUS Authentication

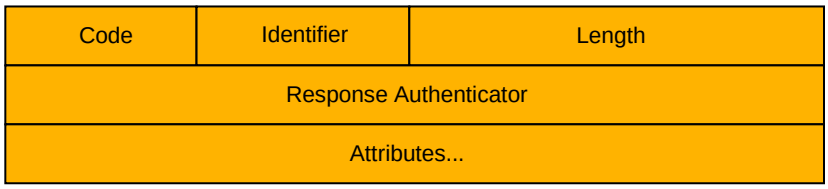
With RADIUS authentication, a remote RADIUS client can authenticate users attempting to log in. The RADIUS server also provides access authority. RADIUS assists network security and authorization by managing a database of users. The switch can use the database to verify user names and passwords, as well as information about the type of access priority available to the user.

When the RADIUS client sends an authentication request, if the RADIUS server requires additional information, such as a SecurID number, it sends a *challenge-response*. Along with the challenge-response, a reply-message attribute is sent. The reply-message is a text string, such as "Please enter the next number on your SecurID card". The maximum length of each reply-message attribute is 253 characters (as defined by the RFC). If you have multiple instances of reply-message attributes that together form a large message which can be displayed to the user, the maximum total length is 2000 characters.



802.1x (EAP), if enabled, has a mandatory requirement to authenticate users by Radius. Hence, Layer two switches supporting 802.1x (EAP) support RADIUS authentication.

RADIUS Packet Format – RFC 2865



RADIUS Codes

1	Access-Request	12	Status-Server (experimental)
2	Access-Accept	13	Status-Client (experimental)
3	Access-Reject	255	Reserved
11	Access-Challenge		

RADIUS Attributes

1	User-Name	7	Framed-Protocol
2	User-Password	8	Framed-IP-Address
3	CHAP-Password	9	Framed-IP-Netmask
4	NAS-IP-Address	10	Framed-Routing
5	NAS-Port	11	Filter-Id
6	Service-Type	12	Framed-MTU

…/…

RADIUS Attributes Cont.

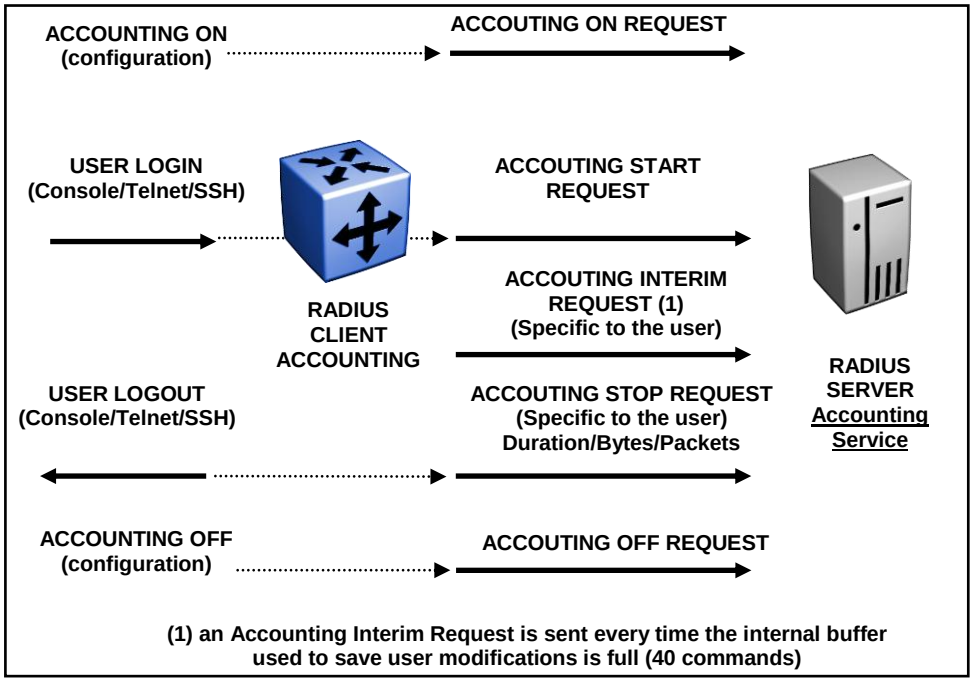
13	Framed-Compression	30	Called-Station-Id
14	Login-IP-Host	31	Calling-Station-Id
15	Login-Service	32	NAS-Identifier
16	Login-TCP-Port	33	Proxy-State
18	Reply-Message	34	Login-LAT-Service
19	Callback-Number	35	Login-LAT-Node
20	Callback-Id	36	Login-LAT-Group
22	Framed-Route	37	Framed-AppleTalk-Link
23	Framed-IPX-Network	38	Framed-AppleTalk-Network
24	State	39	Framed-AppleTalk-Zone
25	Class	60	CHAP-Challenge
26	Vendor-Specific	61	NAS-Port-Type
27	Session-Timeout	62	Port-Limit
28	Idle-Timeout	63	Login-LAT-Port
29	Termination-Action		

UDP frame official port number is 1812, not 1645 (conflicts with the "datametrics" service)

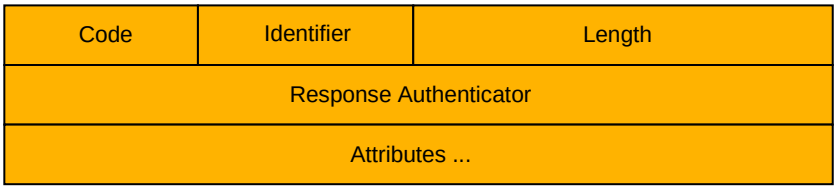
2.1.2 RADIUS Accounting

RADIUS accounting logs all of the activity of each remote user in a session on the centralized RADIUS accounting server. Session IDs for each RADIUS account are generated as 12-character strings. The first four characters in the string form a random number in hexadecimal format. The last eight characters in the string indicate, in hexadecimal format, the number of user sessions started since reboot.

The Network Access Server (NAS) IP address for a session is the address of the switch interface to which the remote session is connected over the network. For a console session, modem session, and sessions running on debug ports, this value is set to 0.0.0.0 (as is done with RADIUS authentication).



RADIUS Packet Format – RFC 2866



RADIUS Codes

4	**Accounting-Request**	**5**	**Accounting-Response**

RADIUS Attributes

40	**Acct-Status-Type**	**46**	**Acct-Session-Time**
41	**Acct-Delay-Time**	**47**	**Acct-Input-Packets**
42	**Acct-Input-Octets**	**48**	**Acct-Output-Packets**
43	**Acct-Output-Octets**	**49**	**Acct-Terminate-Cause**
44	**Acct-Session-Id**	**50**	**Acct-Multi-Session-Id**
45	**Acct-Authentic**	**51**	**Acct-Link-Count**

Radius Attribute 40 : Acct-Status-Type.

Length : 6

Value : The Value field is four octets.

1	**Start**
2	**Stop**
3	**Interim-Update**
7	**Accounting-On**
8	**Accounting-Off**
9-14	**Reserved for Tunnel Accounting**
15	**Reserved for Failed**

UDP frame official port number is 1813, not 1646 (conflicts with the "sa-msg-port" service)

2.1.3 RADIUS Accounting for 802.1x (EAP)

Ethernet Routing Switch 1600, 8600, 8300, 5500 and 4500 supports accounting for 802.1x (EAP) sessions using RADIUS accounting protocol. A user session is defined as the interval between the instance at which a user is successfully authenticated (port moves to authorized state) and the instance at which the port moves out of the authorized state.

2.1.4 RADIUS Accounting for CLI Commands

RADIUS accounting will keep track of user, session duration, number of octects and packets (in and out). This feature allows you to keep track of all CLI commands typed by user during session.

2.1.5 RADIUS User Access Profile

As a network administrator, you can override a user's access to specific CLI commands by configuring the RADIUS server for user authentication. You must still give access based on the existing six access levels in the ERS 8600, but you can customize user access by permitting and preventing access to specific CLI commands.

2.1.6 RADIUS SNMP Accounting

RADIUS accounting will record the duration of the SNMP version 1, 2 or 3 session and the number of packets/octets sent and received during the SNMP session.

2.2 Avaya Switches RADIUS Support

	RADIUS authenti-cation	802.1x (EAP) RADIUS authenti-cation	RADIUS accoun-ting	802.1x (EAP) RADIUS accoun-ting	RADIUS accoun-ting for CLI commands	RADIUS user access profile	RADIUS SNMP accoun-ting
ERS 8600	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ERS 8300	Yes	Yes	Yes	Yes	Yes	Yes	No
ERS 1600	Yes	Yes	Yes	Yes	Yes	Yes	No
ES 460/470	Yes	Yes	No	No	No	No	No
ERS 2500	Yes	Yes	No	Yes	No	No	No
ERS 4500	Yes	Yes	No	Yes	No	No	No
ERS 5500	Yes	Yes	No	Yes	No	No	No

2.3 RADIUS Server Configuration – Using FreeRadius

The following RADIUS Server configuration is based on FreeRadius, www.freeradius.org. Once installed on a Linux host, there are several configuration files to edit as shown below

2.3.1 /etc/raddb/client.conf

This file contains the NAS list with shared secret.

```
client 10.10.50.1 {
        secret          = Dda
        shortname       = 8600
}

client 10.10.44.5 {
        secret          = Dda
        shortname       = 4548GT-PWR
}
```

2.3.2 /etc/raddb/dictionary

This file contains the dictionary file for all clients. You have to create a specific dictionary file (dictionary.nortel) for user access level and add an include statement in the /etc/raddb/dictionary file.

```
$INCLUDE        /usr/share/freeradius/dictionary.nortel
```

2.3.3 /usr/share/freeradius/dictionary.nortel

This file contains specific statements for ERS 8600, 8300 and 1600.

```
VENDOR          Nortel          1584

BEGIN-VENDOR Nortel

ATTRIBUTE       Access-Priority         192     integer

VALUE   Access-Priority         none    0
VALUE   Access-Priority         ro      1
VALUE   Access-Priority         l1      2
VALUE   Access-Priority         l2      3
VALUE   Access-Priority         l3      4
VALUE   Access-Priority         rw      5
VALUE   Access-Priority         rwa     6

#CLI Commands
ATTRIBUTE Cli-Commands 193 string
```

```
#CLI profile
ATTRIBUTE Command-Access 194 integer

VALUE   Command-Access  False   0
VALUE   Command-Access  True    1

#CLI Commands
ATTRIBUTE Commands 195 string

#802 priority (value: 0-7)
ATTRIBUTE EAP-Port-Priority 1 integer

END-VENDOR Nortel
```

2.3.4 /etc/raddb/users

This file contains the users list with user rights and specific parameters. It can also contain the VLAN ID and port priority for 802.1x (EAP) clients – please see “eap” user shown below as an example which defines VLAN ID 51 and port priority 3.

```
bsro    Auth-Type == Local,User-Password == "bsro"
        Service-Type = NAS-Prompt-User

bsrw    Auth-Type == Local,User-Password == "bsrw"
        Service-Type = Administrative-User

ro      Auth-Type == Local,User-Password == "ro"
        Access-Priority = ro

rwa     Auth-Type == Local,User-Password == "rwa"
        Access-Priority = rwa

eap     Auth-Type == EAP,User-Password == "eap"
        Tunnel-Type = 13,
        Tunnel-Medium-Type = 6,
        Tunnel-private-Group-Id = 51,
        EAP-port-Priority = 3
```

The ES 460/470 and ERS 2500, 4500, 5500 switches each has two user access levels: read-only or read-write

The ERS 1600, 8300 and 8600 switches each has six different user access levels: ro, l1, l2, l3, rw and rwa

2.3.5 /etc/raddb/radiusd.conf

This file is the main configuration file for the RADIUS server. You can enable or disable authentication (eap, pap, mschap etc ….) and you can also add extra login information. You will need to uncomment the line **`detail auth_log {.`**

This will create a file with the following format

`detailfile = ${radacctdir}/%{Client-IP-Address}/auth-detail-%Y%m%d`

2.3.6 /etc/init.d/radiusd

This file is the startup file for RADIUS process. Please check that you have a link to **`/etc/rcX.d/S96radiusd`** (X can be 2, 3 or 5 depending on your run level). Also check that radiusd is started with –y flag. You will write details about every authentication request in the radius.log file.

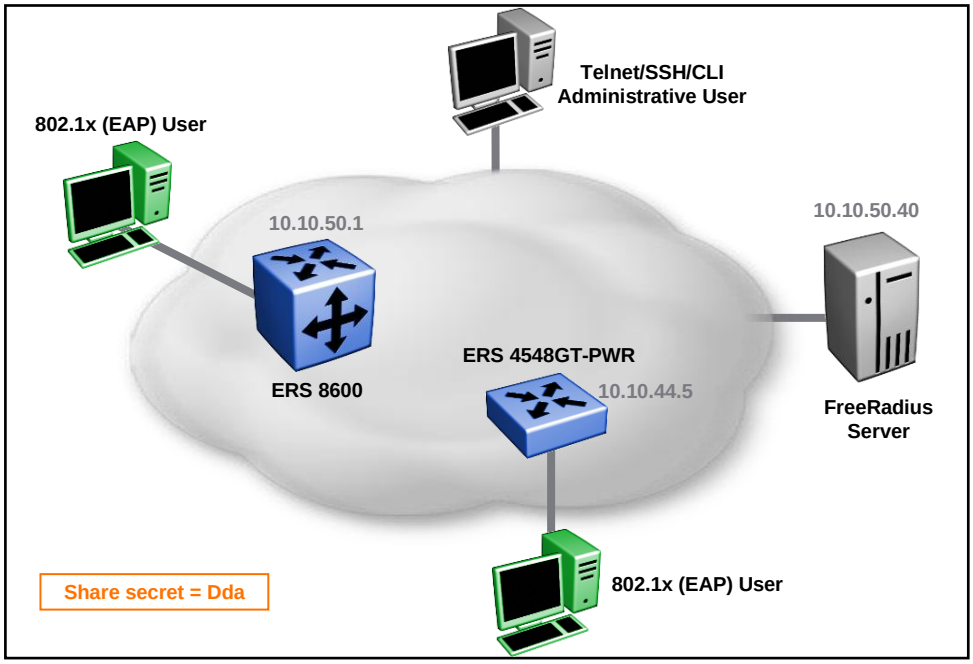
When you modify the configuration file, you have to restart RADIUS process using command

```
[root@linux2 raddb]# /etc/rc2.d/S96radiusd restart
```

2.4 RADIUS Client Configuration

Two different product lines, ES 460/470 Series and ERS 2500, 4500, 5500 each has the same logic for configuration whereas the ERS 1600, 8300 and 8600 each has a different logic for configuration.

Network diagram with RADIUS client and server can be simplified and summarized in the following diagram.



2.4.1 ES 460/470 Series and ERS 2500, 4500, 5500

ACLI or JDM (Java Device Manager) can be used to configure the switch. For simplicity and readability, we will document command line interface commands assuming the RADIUS server IP address is 10.10.50.40, and the client shared secret is “Dda” for telnet access authentication.

To configure RADIUS

```
4548GT-PWR# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
4548GT-PWR(config)# radius-server host 10.10.50.40
4548GT-PWR(config)# radius-server key Dda
4548GT-PWR(config)# radius-server password fallback
4548GT-PWR(config)# cli password switch telnet radius
4548GT-PWR(config)# radius accounting enable
```

To display RADIUS configuration

```
4548GT-PWR(config)# show radius-server
Password Fallback:  Enabled
Primary Host:  10.10.50.40
Secondary Host:  0.0.0.0
Port:  1812
Time-out:  2
Key:  ***************
Radius Accounting is  Enabled
AcctPort:  1813
4548GT-PWR(config)# show cli password type
Console Switch Password Type: None
Console Stack Password Type: None
Telnet/WEB Switch Password Type: RADIUS Authentication
Telnet/WEB Stack Password Type: None
```

The source IP address sent by the switch (Layer 2 operation) is always the Management IP address configured on the switch when sending a RADIUS client authentication request.

There is no way to change source RADIUS IP address. When the switch is configured in routed mode, it uses interface IP address where frame is sent. Hence, if you have multiple IP interfaces facing the core network where a RADIUS request could be sent, you will have to configure the RADIUS server with each IP address.

With the ES 460/470 and ERS 2500, 4500, 5500 switches, you can configure two RADIUS servers, a primary server and a secondary server. If all servers are not reachable (no answers) then local authentication is done if Password Fallback feature is enabled. You get the following message at console:

```
Querying RADIUS server, please wait...
no response from RADIUS servers
```

2.4.2 ERS 1600, 8300 and 8600

ACLI is or JDM (Java Device Manager) can be used to configure the switch, for simplicity and readability, we will document command line interface commands

To configure RADIUS

```
8600A:6# config radius server create 10.10.50.40 secret Dda
8600A:6# config radius server create 10.10.50.40 secret Dda usedby eapol
8600A:6# config radius enable true
8600A:6# config radius acct-enable true
8600A:6# config radius acct-include-cli-commands true
```

To display RADIUS configuration

```
8600A:6# show radius info
Sub-Context: clear config dump monitor show test trace wsm asfm sam
Current Context:
             acct-attribute-value : 193
                      acct-enable : true
        acct-include-cli-commands : true
        access-priority-attribute : 192
             auth-info-attr-value : 91
         command-access-attribute : 194
           cli-commands-attribute : 195
                    cli-cmd-count : 40
               cli-profile-enable : false
                           enable : true
                 igap-passwd-attr : standard
           igap-timeout-log-fsize : 512
                        maxserver : 10
            mcast-addr-attr-value : 90
                    sourceip-flag : false

8600A:6# show radius server config
Sub-Context: clear config dump monitor show test trace wsm asfm sam
Current Context:
                      create :

Name            Usedby Secret           Port    Prio  Retry Timeout Enabled
Acct-port Acct-enabled source-ip
10.10.50.40     cli    Dda              1812    10    1     3       true
1813      true         0.0.0.0
10.10.50.40     eapol  Dda              1812    10    1     3       true
1813      true         0.0.0.0
```

```
                    delete : N/A
                       set : N/A
```

With the ERS 1600, 8300, and 8600, you can change the RADIUS source IP address by using the following command :

```
8000A:6# config radius server create <ipaddr> secret <value> [usedby
<value>] [port <value>] [priority <value>] [retry <value>] [timeout
<value>] [enable <value>] [acct-port <value>] [acct-enable <value>]
[source-ip <value>]
```

With the ERS 1600, 8300, and 8600, you can configure up to ten RADIUS servers (each server is assigned a priority and is contacted in that order). If all servers are not reachable (no answer) then local authentication is done and you will receive the following message:

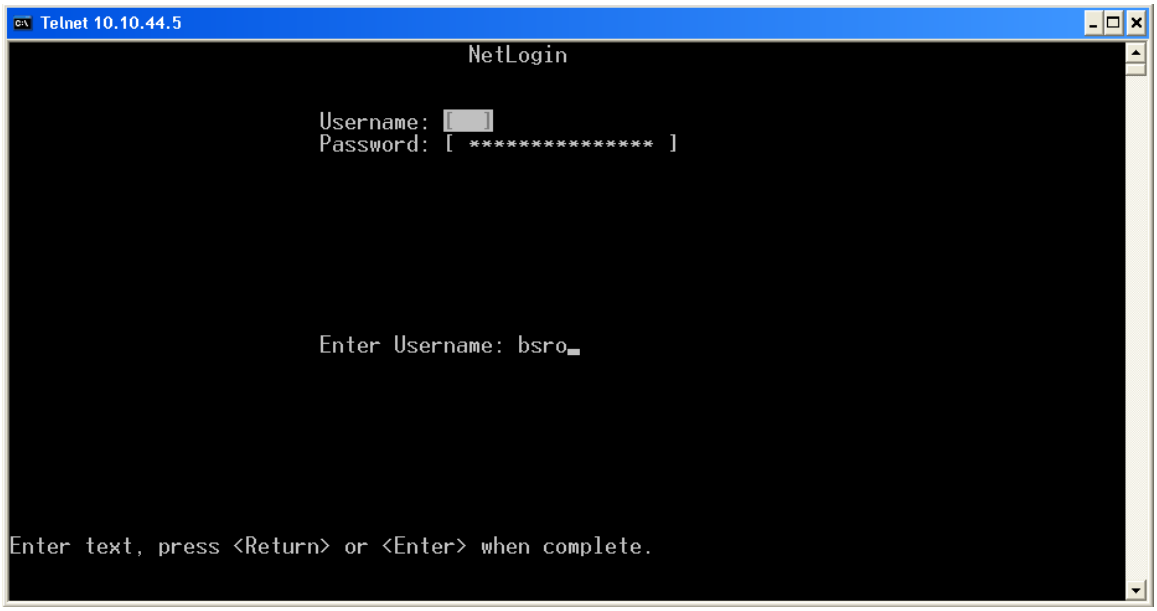
```
No reply from RADIUS server "10.10.50.40(1812)"All RADIUS servers are
unreachable.
```

2.5 RADIUS Server & Client Log Files

In this section, we will demonstrate RADIUS server and client logging on the switch. We will demonstrate a client logging onto a switch, issuing several commands and checking if they are allowed or not based on authentication rights.

2.5.1 ES 460/470 Series and ERS 2500, 4500, 5500 – Read-Only user

Connect to the device via telnet using read-only user (bsro).



Please note that there is no Administrative RADIUS accounting for ES460/470 Series and ERS 2500, 4500, 5500.

RADIUS accounting is only available for 802.1x (EAP) users.

Telnet to Switch with read-only user (bsro) type some commands

```
4548GT-PWR# show clock
    Current SNTP time  :    2008-02-21 15:52:36 GMT+01:00
    Daylight saving time is DISABLED
    Time zone is set to 'METD', offset from UTC is 01:00
4548GT-PWR# conf t
            ^
% Invalid input detected at '^' marker.
4548GT-PWR# exit
```

Read-only user in this example does not have access to switch configuration.

Log file on RADIUS server - /var/log/radius/radius.log

```
Thu Feb 21 15:52:09 2008 : Auth: Login OK: [bsro] (from client 4548GT-PWR
port 0)
```

Log file on RADIUS server - /var/log/radius/radacct/10.10.44.5/auth-detail-20080221

Optional file, need to configure /etc/raddb/radiusd.conf

```
Thu Feb 21 15:52:09 2008
        NAS-IP-Address = 10.10.44.5
        Service-Type = Administrative-User
        User-Name = "bsro"
        Client-IP-Address = 10.10.44.5
        Timestamp = 1203605529
```

Please note that the client-IP-Address is equal to NAS-IP-Address which is not correct. The client-IP-Address is the station where telnet has been issued, which is 10.10.50.10. The reason is the switch does not provide a Client-IP-address field (see sniffer trace). Application artificially copy field.

Log file on RADIUS client

```
4548GT-PWR# show log
I    2008-02-21 15:52:21 GMT+01:00 115      #1 Session opened(radius auth)
from  IP add: 10.10.50.10, access mode: read-only
I    2008-02-21 15:53:50 GMT+01:00 116      #1 Session closed (user logout),
IP   address: 10.10.50.10, access mode: read-only
I    2008-02-21 15:53:50 GMT+01:00 117      #1 Connection closed (user
logout),
 IP address: 10.10.50.10
```

Please note that the log file only displays the user access level (read-only). The log file does not contain any session statistics.

2.5.2 ES 460/470 Series and ERS 2500, 4500, 5500 – Read-Write User

Connect to the device with telnet using read-only user (bsrw).

Telnet to Switch with read-write user (bsrw) type some commands

```
4548GT-PWR# en
4548GT-PWR# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
4548GT-PWR(config)# interface fastEthernet all
4548GT-PWR(config-if)# exit
4548GT-PWR(config)# exit
4548GT-PWR# exit
```

Read-Write user in this example does have access to switch configuration.

Log file on RADIUS server - /var/log/radius/radius.log

```
Thu Feb 21 16:54:24 2008 : Auth: Login OK: [bsrw] (from client 4548GT-PWR
port 0)
```

Log file on RADIUS server - /var/log/radius/radacct/10.10.44.5/auth-detail-20080221

Optional file, need to configure /etc/raddb/radiusd.conf

```
Thu Feb 21 16:54:24 2008
        NAS-IP-Address = 10.10.44.5
        Service-Type = Administrative-User
        User-Name = "bsrw"
        Client-IP-Address = 10.10.44.5
        Timestamp = 1203609264
```

Please note that the client-IP-Address is equal to NAS-IP-Address which is not correct. The client-IP-Address is the station where telnet has been issued, which is 10.10.50.10. The reason is the switch does not provide a Client-IP-address field (see sniffer trace). Application artificially copy field.

Log file on RADIUS client

```
I    2008-02-21 16:54:25 GMT+01:00 124      #1 Session opened(radius auth)
from IP add: 10.10.50.10, access mode: read-write
I    2008-02-21 16:55:17 GMT+01:00 125      #1 Session closed (user logout),
IP address: 10.10.50.10, access mode: read-write
I    2008-02-21 16:55:17 GMT+01:00 126      #1 Connection closed (user
logout), IP address: 10.10.50.10
```

Please note that the log file only displays the user access level (read-only). The log file does not contain any session statistics.

2.5.3 ERS 2500, 4500, 5500 – 802.1x (EAP) User

For this example, we will connect an 802.1x (EAP) supplicant to the switch, authenticate the EAP supplicant, generate some traffic, and then disconnect.

Log file on RADIUS server - /var/log/radius/radius.log

```
Thu Feb 21 17:17:22 2008 : Auth: Login OK: [eap] (from client 4548GT-PWR port
1 cli 00-12-3F-1A-1B-68)
```

Log file on RADIUS server - /var/log/radius/radacct/10.10.44.5/auth-detail-20080221

Optional file, need to configure /etc/raddb/radiusd.conf

```
Thu Feb 21 17:17:22 2008
        NAS-IP-Address = 10.10.44.5
        NAS-Port-Type = Ethernet
        Service-Type = Framed-User
        Message-Authenticator = 0x88721799b12354d60b8336ab285dda67
        NAS-Port = 1
        Framed-MTU = 1490
        User-Name = "eap"
        Calling-Station-Id = "00-12-3F-1A-1B-68"
        EAP-Message = 0x02ff000801656170
        Client-IP-Address = 10.10.44.5
        Timestamp = 1203610642

Thu Feb 21 17:17:22 2008
        NAS-IP-Address = 10.10.44.5
        NAS-Port-Type = Ethernet
        Service-Type = Framed-User
        Message-Authenticator = 0xf59f53234959a19e91f76475e3d9ab6d
        NAS-Port = 1
        Framed-MTU = 1490
        User-Name = "eap"
        Calling-Station-Id = "00-12-3F-1A-1B-68"
        State =
0x554445eb4da34e4372ab674424c945d712a4bd47826574a783596a949d917a931b1f5c81
        EAP-Message = 0x0200001904108317b45b9526d49bd52c243c7b96bd1c656170
        Client-IP-Address = 10.10.44.5
        Timestamp = 1203610642
```

Log file on RADIUS server - /var/log/radius/radacct/10.10.44.5/detail-20080221

```
Thu Feb 21 17:17:23 2008
        NAS-IP-Address = 10.10.44.5
        NAS-Port-Type = Ethernet
        NAS-Port = 1
        User-Name = "eap"
        Acct-Session-Id = "85000001"
        Acct-Status-Type = Start
        Client-IP-Address = 10.10.44.5
        Acct-Unique-Session-Id = "3e7408b4904a799d"
        Timestamp = 1203610643

Thu Feb 21 17:18:08 2008
        NAS-IP-Address = 10.10.44.5
        NAS-Port-Type = Ethernet
        NAS-Port = 1
        User-Name = "eap"
        Acct-Session-Id = "85000001"
        Acct-Status-Type = Stop
        Acct-Input-Octets = 11722
        Acct-Output-Octets = 7387
        Acct-Input-Packets = 100
        Acct-Output-Packets = 78
        Acct-Session-Time = 45
        Acct-Terminate-Cause = Lost-Carrier
        Client-IP-Address = 10.10.44.5
        Acct-Unique-Session-Id = "3e7408b4904a799d"
        Timestamp = 1203610688
```

802.1x (EAP) user has accounting start & stop records in accounting log file

Log file on RADIUS client

```
I    2008-02-21 17:16:41 GMT+01:00 137      EAP Mac AuthFail - unitPort 0x1
macHi 123f1a macLo 1b68
```

Please note that only 802.1x (EAP) login authentication failure are logged, not successful authentication.

2.5.4 ERS 1600, 8300 and 8600 – Read-Only User

For this example, we will connect to the switch using telnet via a read-only (ro) user.

Telnet to Switch with read-only user (ro) type some commands

```
8600A:6> show date
local time:    THU FEB 21 18:08:44 2008 METDST
hardware time: THU FEB 21 17:08:44 2008 UTC
8600A:6> config ?
Sub-Context: cli log
Current Context:

    Info
8600A:6> exit
```

Read-only user in this example does not have access to switch configuration.

Log file on RADIUS server - /var/log/radius/radius.log

```
Thu Feb 21 18:08:07 2008 : Auth: Login OK: [ro] (from client 8600 port 1)
```

Log file on RADIUS server - /var/log/radius/radacct/10.10.50.1/auth-detail-20080221

Optional file, need to configure /etc/raddb/radiusd.conf

```
Thu Feb 21 18:08:07 2008
        User-Name = "ro"
        NAS-IP-Address = 10.10.50.1
        NAS-Port = 1
        Client-IP-Address = 10.10.50.1
        Timestamp = 1203613687
```

Please note that the client-IP-Address is equal to NAS-IP-Address which is not correct. The client-IP-Address is the station where telnet has been issued, which is 10.10.50.10. The reason is the switch does not provide a Client-IP-address field (see sniffer trace). Application artificially copy field.

Log file on RADIUS server - /var/log/radius/radacct/10.10.50.1/detail-20080221

```
Thu Feb 21 18:08:07 2008
        Acct-Status-Type = Start
        NAS-IP-Address = 10.10.50.1
        Acct-Session-Id = "1ef400000012"
        User-Name = "ro"
        Client-IP-Address = 10.10.50.1
        Acct-Unique-Session-Id = "fae1055b429ca034"
        Timestamp = 1203613687
```

```
Thu Feb 21 18:09:29 2008
        Acct-Status-Type = Stop
        Acct-Session-Id = "1ef400000012"
        User-Name = "ro"
        NAS-IP-Address = 10.10.50.1
        Acct-Session-Time = 81
        Acct-Input-Octets = 0
        Acct-Output-Octets = 1871
        Acct-Input-Packets = 0
        Acct-Output-Packets = 94
        Cli-Commands = "show date"
        Cli-Commands = "config ?"
        Cli-Commands = "exit"
        Client-IP-Address = 10.10.50.1
        Acct-Unique-Session-Id = "fae1055b429ca034"
        Timestamp = 1203613769
```

Read-only user has accounting start & stop records in accounting log file. You also have "CLI-Commands" which keep track of all commands typed by user during session.

Please note that the Acct-Input-Octets & Acct-input-Packets are null, which are a known issue fixed in ERS 8600 software release 4.1.6.

Log file on RADIUS client

```
8600A:6# show log file
CPU6 [02/21/08 18:08:08] SW INFO user ro connected from 10.10.50.10 via
telnet
CPU6 [02/21/08 18:09:30] SW INFO Closed telnet connection from 10.10.50.10,
user ro rcmd -2
```

2.5.5 ERS 1600, 8300 and 8600 – Read-Write User

For this example, we will connect to the switch using telnet via a read-write (rwa) user.

Telnet to Switch with read-write user (rwa) type some commands

```
8600A:6# show date
local time:    THU FEB 21 18:24:20 2008 METDST
hardware time: THU FEB 21 17:24:20 2008 UTC
8600A:6# config ?
Sub-Context: atm atmcard bootconfig cli cluster diag r-module ethernet fdb
filter ip ipv6 ipx lacp log mlt naap ntp pos poscard qos radius rmon slot
slpp snmp-server snmp-v3 stg sv lan sys vlacp vlan web-server
Current Context:

    auto-recover-delay <seconds>
    info
    load-encryption-module <3DES|DES|AES>
    mac-flap-time-limit <milliseconds>
    setdate <MMddyyyyhhmmss>

8600A:6# exit
```

Read-write user in this example does have access to switch configuration.

Log file on RADIUS server - /var/log/radius/radius.log

```
Thu Feb 21 18:24:16 2008 : Auth: Login OK: [rwa] (from client 8600 port 1)
```

Log file on RADIUS server - /var/log/radius/radacct/10.10.50.1/auth-detail-20080221

Optional file, need to configure /etc/raddb/radiusd.conf

```
Thu Feb 21 18:24:16 2008
        User-Name = "rwa"
        NAS-IP-Address = 10.10.50.1
        NAS-Port = 1
        Client-IP-Address = 10.10.50.1
        Timestamp = 1203614656
```

Please note that the client-IP-Address is equal to NAS-IP-Address which is not correct. The client-IP-Address is the station where telnet has been issued, which is 10.10.50.10. The reason is the switch does not provide a Client-IP-address field (see sniffer trace). Application artificially copy field.

Log file on RADIUS server - /var/log/radius/radacct/10.10.50.1/detail-20080221

```
Thu Feb 21 18:24:16 2008
        Acct-Status-Type = Start
        NAS-IP-Address = 10.10.50.1
        Acct-Session-Id = "59e000000014"
        User-Name = "rwa"
        Client-IP-Address = 10.10.50.1
        Acct-Unique-Session-Id = "4d1d6de604442704"
        Timestamp = 1203614656

Thu Feb 21 18:24:28 2008
        Acct-Status-Type = Stop
        Acct-Session-Id = "59e000000014"
        User-Name = "rwa"
        NAS-IP-Address = 10.10.50.1
        Acct-Session-Time = 11
        Acct-Input-Octets = 0
        Acct-Output-Octets = 549
        Acct-Input-Packets = 0
        Acct-Output-Packets = 40
        Cli-Commands = "show date"
        Cli-Commands = "config ?"
        Cli-Commands = "exit"
        Client-IP-Address = 10.10.50.1
        Acct-Unique-Session-Id = "4d1d6de604442704"
        Timestamp = 1203614668
```

Read-write user has accounting start & stop records in accounting log file. You also have “CLI-Commands” which keep track of all commands typed by user during session.

Please note that Acct-Input-Octets & Acct-input-Packets are null, which are a known issue fixed in ERS 8600 software release 4.1.6.

Log file on RADIUS client

```
8600A:6# show log file
CPU6 [02/21/08 18:24:16] SW INFO user rwa connected from 10.10.50.10 via
telnet
CPU6 [02/21/08 18:24:28] SW INFO Closed telnet connection from 10.10.50.10,
user
 rwa rcmd -2
```

2.5.6 ERS 1600, 8300, 8600 – 802.1x (EAP) User

For this example, we will connect an 802.1x (EAP) Supplicant to the switch, authenticate, generate some traffic, and then disconnect.

Log file on RADIUS server - /var/log/radius/radius.log

```
Thu Feb 21 18:43:58 2008 : Auth: Login OK: [eap] (from client 8600 port 237
cli 00-12-3F-1A-1B-68)
```

Log file on RADIUS server - /var/log/radius/radacct/10.10.50.1/auth-detail-20080221

Optional file, need to configure /etc/raddb/radiusd.conf

```
Thu Feb 21 18:43:58 2008
        NAS-IP-Address = 10.10.50.1
        Message-Authenticator = 0x6fdcc0dbd43d0d3ed6019dcedc7ae536
        NAS-Port = 237
        Framed-MTU = 1490
        User-Name = "eap"
        Calling-Station-Id = "00-12-3F-1A-1B-68"
        EAP-Message = 0x0201000801656170
        Service-Type = Framed-User
        Client-IP-Address = 10.10.50.1
        Timestamp = 1203615838

Thu Feb 21 18:43:58 2008
        NAS-IP-Address = 10.10.50.1
        Message-Authenticator = 0xc65a435fc430f6e450022dd0725f94a4
        NAS-Port = 237
        Framed-MTU = 1490
        User-Name = "eap"
        Calling-Station-Id = "00-12-3F-1A-1B-68"
        State =
0x97bcb26760f9b35a51e8b7414bd0b77a5eb8bd478adb2817b2faf00b06b49d15345b525b
        EAP-Message = 0x020200190410958a6af03992692be31ae93d09bfe1c0656170
        Service-Type = Framed-User
        Client-IP-Address = 10.10.50.1
        Timestamp = 1203615838
```

Log file on RADIUS server - /var/log/radius/radacct/10.10.50.1/detail-20080221

```
Thu Feb 21 18:43:58 2008
        NAS-IP-Address = 10.10.50.1
        Acct-Session-Id = "e3000000"
        NAS-Port = 237
        User-Name = "eap"
        Acct-Status-Type = Start
        Client-IP-Address = 10.10.50.1
        Acct-Unique-Session-Id = "6f5b9475a3d11c7b"
        Timestamp = 1203615838

Thu Feb 21 18:45:01 2008
        NAS-IP-Address = 10.10.50.1
```

```
        Acct-Session-Id = "e3000000"
        NAS-Port = 237
        User-Name = "eap"
        Acct-Status-Type = Stop
        Acct-Input-Octets = 9288
        Acct-Output-Octets = 5800
        Acct-Session-Time = 62
        Acct-Terminate-Cause = Lost-Carrier
        Client-IP-Address = 10.10.50.1
        Acct-Unique-Session-Id = "6f5b9475a3d11c7b"
        Timestamp = 1203615901
```

802.1x (EAP) user has accounting start & stop records in accounting log file

Log file on RADIUS client

```
8600A:6# show log file
CPU6 [02/21/08 18:43:53] EAP INFO Port 3/46 connecting
CPU6 [02/21/08 18:43:58] EAP INFO Port 3/46 authenticating
CPU6 [02/21/08 18:43:58] EAP INFO Bkend state of Port 3/46 - Recd Respose
from supplicant
CPU6 [02/21/08 18:43:59] EAP INFO Bkend state of Port 3/46 - Recd EAP request
from Server
CPU6 [02/21/08 18:43:59] EAP INFO Bkend state of Port 3/46 - Recd Respose
from supplicant
CPU6 [02/21/08 18:43:59] EAP INFO Bkend state of Port 3/46 - Recd accept from
server
CPU6 [02/21/08 18:43:59] EAP INFO User eap on Port 3/46 is authenticated
```

2.5.7 ERS 8600, 8300 and 1600 – RADIUS User Access Profile

For this example, we will connect to the switch using telnet via a read-write (rw) user. This user has a special profile, it is based on read-write access level but some commands have been disabled (“config ip” and “test”).

You must configure the following three returnable attributes for each user on RADIUS server in **/etc/raddb/users**

- Access priority (single instance) - the access levels currently available on ERS 8600: ro, l1, l2, l3, rw, rwa.
- Command access (single instance) - indicates whether the CLI commands configured on the RADIUS server are allowed or disallowed for the user.
- CLI commands (multiple instances) - the list of commands that the user can/cannot use. The user cannot include allow and deny commands in the list of multiple commands; the commands must be either all allow or all deny.

To configure read-write (rw) user with commands "config ip" & "test" denied.

/erc/raddb/users file to be edited on RADIUS server.

```
rw      Auth-Type == Local,User-Password == "rw"
        Access-Priority = rw,
        Command-Access = "False",
        Commands = "config ip",
        Commands += "test"
```

You must enable user access profile (cli-profile) parameter on RADIUS client.

To configure RADIUS cli-profile on ERS 8600

```
8600A:6# config radius cli-profile-enable true
```

Connect to ERS 8600 with telnet using read-write user.

Telnet to ERS 8600 with read-write user (rwa) type some commands

```
8600A:6# config ip
Permission denied.

8600A:6# config ?

Sub-Context: atm atmcard bootconfig cli cluster diag r-module ethernet fdb
filter ipv6 ipx lacp log mlt naap pos poscard qos rmon slot slpp snmp-server
snmp-v3 stg svlan sys vlacp vlan web-server
Current Context:

    info

8600A:6# test
Permission denied.

8600A:6# exit
```

Read-write user does have access to switch configuration but not to the denied commands.

Please note that if you prevent access to any command, only the lowest option in the command tree cannot be accessed. For example, if you prevent access to the CLI command ***config sys set*** for a user, the user is able to display or execute ***config*** or ***config sys***.

Log file on RADIUS client

```
8600A:6# CPU6 [03/03/08 15:28:13] SW INFO user rw connected from 10.10.50.10
via telnet

CPU6 [03/03/08 15:29:17] SW INFO Closed telnet connection from 10.10.50.10,
user rw rcmd -2
```

Please note that accounting records for rw user will be similar to the ones for ro and rwa users already documented in chapter 2.5.4 and 2.5.5.

The following example shows how to allow read-only (ro) user the command “clear port stat”, as the only possible command under clear port is stats, command can be summarized to “clear port”. File **`/etc/raddb/users`** has to be modified as follow.

```
ro      Auth-Type == Local,User-Password == "ro"
        Access-Priority = ro,
        Command-Access = "True",
        Commands = "clear port"
```

Please note that Command-Access statement is unique, you cannot mix “True” and “False”.

You can have several commands, use syntax = for first line, then use += for following lines, always add comma at the end of the line except last line.

2.5.8 ERS 8600 – RADIUS SNMP Accounting

For this example, we will connect to the switch using Device Manager with SNMPv1 protocol. ERS 8600 needs to be configured in order to have RADIUS SNMP accounting, assuming the RADIUS server IP address is 10.10.50.40 and the client share secret is “Dda” for SNMP accounting.

Please note that RADIUS SNMP accounting requires software release 4.1.3 or above for proper operation.

Configure RADIUS SNMP accounting on RADIUS client.

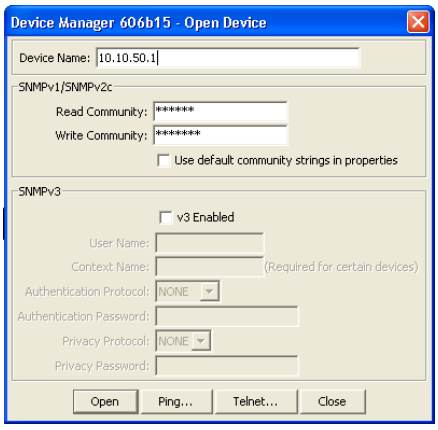
```
8600A:6# config radius server create 10.10.50.40 secret Dda usedby snmp
enable true
8600A:6# config radius snmp enable true
8600A:6# config radius snmp acct-enable true
8600A:6# show radius snmp info

Sub-Context: clear config dump monitor show test trace wsm asfm sam
Current Context:

              abort-session-timer : 180
                      acct-enable : true
                             user : snmp_user
                           enable : true
```

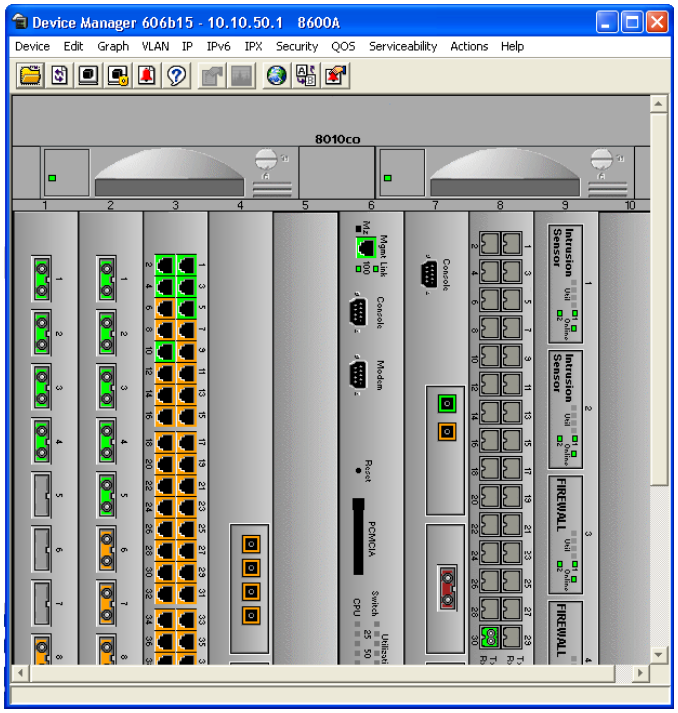
```
re-auth-timer : 180
```

The accounting will be done based on per SNMP Session which will record the duration of that particular session and the number of packets/octets received. Accounting is done for every session. The user for any SNMP session has to be added as “snmp_user”. At the beginning of any session, a start accounting message is sent to the RADIUS server. A stop accounting message is sent a period of time (based on the value configured for abort-session-timer) after the session is terminated. If the abort-session-timer is configured as 30 seconds (default value is 180 seconds) then a stop message is sent 30 seconds after the session is closed. The stop accounting message contains the duration for which the session was maintained and the number of packets/octets received for this session. If the session continues for a long period, then periodically (after every hour; non-configurable) an interim accounting message will be sent, containing the number of packets/octets received for that period for that session and the duration of the session.

Please note that Authentication is still done by the switch and not the RADIUS server. With the implementation of SNMP-v3, more powerful View based Access Control Model (VACM) is used to specifically permit or deny access to various OIDs. Since the security provided by the SNMP-v3 USM and VACM is quite powerful, radius authentication is not implemented for SNMP. Please note that SNMPv1 and SNMPv2 also use VACM for granting access to MIBS (OIDs) on ERS8600.

Launch Device Manager application, select Device -> Open. Enter switch IP address in Device Name field, and then select Open.





In order to simulate a session, open different windows, select VLAN, Vlan or IP, ip, click on a port then select Edit. Finally select Device -> Exit to close Device Manager Application.

Log file on RADIUS server - /var/log/radius/radacct/10.10.50.1/detail-20080304

```
Tue Mar  4 16:07:53 2008
        Acct-Status-Type = Start
        NAS-IP-Address = 10.10.50.1
        Acct-Session-Id = "351500000008"
        Client-IP-Address = 10.10.50.1
        Acct-Unique-Session-Id = "970c6f05416f1f19"
        Timestamp = 1204643273

Tue Mar  4 16:07:53 2008
        Acct-Status-Type = Start
        NAS-IP-Address = 10.10.50.1
        Acct-Session-Id = "752100000009"
        Client-IP-Address = 10.10.50.1
        Acct-Unique-Session-Id = "d265f560f26b031e"
        Timestamp = 1204643273

Tue Mar  4 16:10:53 2008
        Acct-Status-Type = Stop
        Acct-Session-Id = "752100000009"
        NAS-IP-Address = 10.10.50.1
        Acct-Session-Time = 180
        Acct-Input-Octets = 11
        Acct-Output-Octets = 27
        Acct-Input-Packets = 1
        Acct-Output-Packets = 1
        Client-IP-Address = 10.10.50.1
        Acct-Unique-Session-Id = "d265f560f26b031e"
        Timestamp = 1204643453

Tue Mar  4 16:26:23 2008
        Acct-Status-Type = Stop
        Acct-Session-Id = "351500000008"
        NAS-IP-Address = 10.10.50.1
        Acct-Session-Time = 1111
        Acct-Input-Octets = 2167
        Acct-Output-Octets = 5122
        Acct-Input-Packets = 197
        Acct-Output-Packets = 197
        Client-IP-Address = 10.10.50.1
        Acct-Unique-Session-Id = "970c6f05416f1f19"
        Timestamp = 1204644383
```

SNMP session has accounting start & stop records in accounting log file

When a session is opened from JDM with SNMP v1/v2 login, two sessions are opened for the first time, but one of them is closed after N seconds, N being the value configured for abort-session-timer, because Initially Both V1 & V2 packets are sent for authentication, then all the other info is sent are V2 packets. The session which was opened in the beginning for V1 is then closed.

Please note that accounting records for SNMP session will be similar to the ones for ro and rwa users already documented in chapter 2.5.4 and 2.5.5.

2.6 Sniffer Traces on RADIUS Server

2.6.1 RADIUS Authentication Read-Only User

```
Frame 1 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.44.5 (10.10.44.5), Dst: 10.10.50.40 (10.10.50.40)
User Datagram Protocol, Src Port: 1025 (1025), Dst Port: radius (1812)
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x1c (28)
    Length: 56
    Authenticator: 000000070BE3CF61001B25E96800001C
    [The response to this request is in frame 2]
    Attribute Value Pairs
        AVP: l=6  t=NAS-IP-Address(4): 10.10.44.5
        AVP: l=18  t=User-Password(2): Encrypted
        AVP: l=6  t=Service-Type(6): Administrative-User(6)
        AVP: l=6  t=User-Name(1): bsro

Frame 2 (68 bytes on wire, 68 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.44.5 (10.10.44.5)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 1025 (1025)
Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x1c (28)
    Length: 26
    Authenticator: 71B594F70DFDF45D83E88D1062628E07
    [This is a response to a request in frame 1]
    [Time from request: 0.000780000 seconds]
    Attribute Value Pairs
        AVP: l=6  t=Service-Type(6): NAS-Prompt-User(7)
```

2.6.2 RADIUS Authentication Read-Write User

```
Frame 3 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.44.5 (10.10.44.5), Dst: 10.10.50.40 (10.10.50.40)
User Datagram Protocol, Src Port: 1025 (1025), Dst Port: radius (1812)
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x1d (29)
    Length: 56
    Authenticator: 000000070BE3E4AE001B25E96800001D
    [The response to this request is in frame 4]
    Attribute Value Pairs
        AVP: l=6  t=NAS-IP-Address(4): 10.10.44.5
```

```
        AVP: l=18  t=User-Password(2): Encrypted
        AVP: l=6  t=Service-Type(6): Administrative-User(6)
        AVP: l=6  t=User-Name(1): bsrw

Frame 4 (68 bytes on wire, 68 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.44.5 (10.10.44.5)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 1025 (1025)
Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x1d (29)
    Length: 26
    Authenticator: 567FD9538EA68F9182AA0FE9329C4192
    [This is a response to a request in frame 3]
    [Time from request: 0.000656000 seconds]
    Attribute Value Pairs
        AVP: l=6  t=Service-Type(6): Administrative-User(6)
```

2.6.3 RADIUS Authentication & Accounting 802.1x (EAP) User

```
Frame 5 (144 bytes on wire, 144 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.44.5 (10.10.44.5), Dst: 10.10.50.40 (10.10.50.40)
User Datagram Protocol, Src Port: 1025 (1025), Dst Port: radius (1812)
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x1e (30)
    Length: 102
    Authenticator: 000000070BE401AA001B25E96800001E
    Attribute Value Pairs
        AVP: l=6  t=NAS-IP-Address(4): 10.10.44.5
        AVP: l=6  t=NAS-Port-Type(61): Ethernet(15)
        AVP: l=6  t=Service-Type(6): Framed-User(2)
        AVP: l=18  t=Message-Authenticator(80): A4C50C690A97A5B3A2C415D10D91BBF8
        AVP: l=6  t=NAS-Port(5): 1
        AVP: l=6  t=Framed-MTU(12): 1490
        AVP: l=5  t=User-Name(1): eap
        AVP: l=19  t=Calling-Station-Id(31): 00-12-3F-1A-1B-68
        AVP: l=10  t=EAP-Message(79) Last Segment[1]

Frame 6 (170 bytes on wire, 170 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.44.5 (10.10.44.5)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 1025 (1025)
Radius Protocol
    Code: Access-challenge (11)
    Packet identifier: 0x1e (30)
    Length: 128
    Authenticator: A72A36DCE9454579AF9B1511350B175E
    Attribute Value Pairs
        AVP: l=6  t=Tunnel-Type(64) Tag=0x00: VLAN(13)
        AVP: l=6  t=Tunnel-Medium-Type(65) Tag=0x00: IEEE-802(6)
        AVP: l=4  t=Tunnel-Private-Group-Id(81)
        AVP: l=12  t=Vendor-Specific(26) v=Northern Telecom, Ltd.(562)
        AVP: l=24  t=EAP-Message(79) Last Segment[1]
        AVP: l=18  t=Message-Authenticator(80): E111989E198B379760208D08B914677B
```

```
        AVP: l=38  t=State(24): B8D43E1BDB1A306B129DE028F01996DA98FDBE478A1AFC61...

Frame 7 (199 bytes on wire, 199 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.44.5 (10.10.44.5), Dst: 10.10.50.40 (10.10.50.40)
User Datagram Protocol, Src Port: 1025 (1025), Dst Port: radius (1812)
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x1f (31)
    Length: 157
    Authenticator: 000000070BE401AC001B25E96800001F
    [The response to this request is in frame 8]
    Attribute Value Pairs
        AVP: l=6  t=NAS-IP-Address(4): 10.10.44.5
        AVP: l=6  t=NAS-Port-Type(61): Ethernet(15)
        AVP: l=6  t=Service-Type(6): Framed-User(2)
        AVP: l=18  t=Message-Authenticator(80): 3E913F6AAE811CC1633708A608332A40
        AVP: l=6  t=NAS-Port(5): 1
        AVP: l=6  t=Framed-MTU(12): 1490
        AVP: l=5  t=User-Name(1): eap
        AVP: l=19  t=Calling-Station-Id(31): 00-12-3F-1A-1B-68
        AVP: l=38  t=State(24): B8D43E1BDB1A306B129DE028F01996DA98FDBE478A1AFC61...
        AVP: l=27  t=EAP-Message(79) Last Segment[1]

Frame 8 (114 bytes on wire, 114 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.44.5 (10.10.44.5)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 1025 (1025)
Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x1f (31)
    Length: 72
    Authenticator: 29216ADB76413E11A2D70D2A26AA6E29
    [This is a response to a request in frame 7]
    [Time from request: 0.001110000 seconds]
    Attribute Value Pairs
        AVP: l=6  t=Tunnel-Type(64) Tag=0x00: VLAN(13)
        AVP: l=6  t=Tunnel-Medium-Type(65) Tag=0x00: IEEE-802(6)
        AVP: l=4  t=Tunnel-Private-Group-Id(81)
        AVP: l=12  t=Vendor-Specific(26) v=Northern Telecom, Ltd.(562)
        AVP: l=6  t=EAP-Message(79) Last Segment[1]
        AVP: l=18  t=Message-Authenticator(80): DB1F9A8A44C6E736A2797417B50F7EC9

Frame 9 (101 bytes on wire, 101 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.44.5 (10.10.44.5), Dst: 10.10.50.40 (10.10.50.40)
User Datagram Protocol, Src Port: 1024 (1024), Dst Port: radacct (1813)
Radius Protocol
    Code: Accounting-Request (4)
    Packet identifier: 0x9 (9)
    Length: 59
    Authenticator: C58939BF077FC8C434507BADE92C64F5
    [The response to this request is in frame 10]
    Attribute Value Pairs
        AVP: l=6  t=NAS-IP-Address(4): 10.10.44.5
        AVP: l=6  t=NAS-Port-Type(61): Ethernet(15)
```

```
        AVP: l=6  t=NAS-Port(5): 1
        AVP: l=5  t=User-Name(1): eap
        AVP: l=10  t=Acct-Session-Id(44): 85000002
        AVP: l=6  t=Acct-Status-Type(40): Start(1)

Frame 10 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.44.5 (10.10.44.5)
User Datagram Protocol, Src Port: radacct (1813), Dst Port: 1024 (1024)
Radius Protocol
    Code: Accounting-Response (5)
    Packet identifier: 0x9 (9)
    Length: 20
    Authenticator: BE62C3549D966DD1AA397154532F06ED
    [This is a response to a request in frame 9]
    [Time from request: 0.001332000 seconds]

Frame 11 (137 bytes on wire, 137 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.44.5 (10.10.44.5), Dst: 10.10.50.40 (10.10.50.40)
User Datagram Protocol, Src Port: 1024 (1024), Dst Port: radacct (1813)
Radius Protocol
    Code: Accounting-Request (4)
    Packet identifier: 0xa (10)
    Length: 95
    Authenticator: 226B10B0F24DC2AAA1CA673E3EC7517C
    [The response to this request is in frame 12]
    Attribute Value Pairs
        AVP: l=6  t=NAS-IP-Address(4): 10.10.44.5
        AVP: l=6  t=NAS-Port-Type(61): Ethernet(15)
        AVP: l=6  t=NAS-Port(5): 1
        AVP: l=5  t=User-Name(1): eap
        AVP: l=10  t=Acct-Session-Id(44): 85000002
        AVP: l=6  t=Acct-Status-Type(40): Stop(2)
        AVP: l=6  t=Acct-Input-Octets(42): 6907
        AVP: l=6  t=Acct-Output-Octets(43): 3524
        AVP: l=6  t=Acct-Input-Packets(47): 51
        AVP: l=6  t=Acct-Output-Packets(48): 29
        AVP: l=6  t=Acct-Session-Time(46): 23
        AVP: l=6  t=Acct-Terminate-Cause(49): Lost-Carrier(2)

Frame 12 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.44.5 (10.10.44.5)
User Datagram Protocol, Src Port: radacct (1813), Dst Port: 1024 (1024)
Radius Protocol
    Code: Accounting-Response (5)
    Packet identifier: 0xa (10)
    Length: 20
    Authenticator: D72B8E7672D3E0217742C864902CA358
    [This is a response to a request in frame 11]
    [Time from request: 0.001479000 seconds]
```

2.6.4 RADIUS Authentication & Accounting rwa User

```
Frame 13 (97 bytes on wire, 97 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.50.1 (10.10.50.1), Dst: 10.10.50.40 (10.10.50.40)
User Datagram Protocol, Src Port: 1366 (1366), Dst Port: radius (1812)
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0xf3 (243)
    Length: 55
    Authenticator: 000028F3000035F30000157200002F0B
    [The response to this request is in frame 14]
    Attribute Value Pairs
        AVP: l=5  t=User-Name(1): rwa
        AVP: l=18  t=User-Password(2): Encrypted
        AVP: l=6  t=NAS-IP-Address(4): 10.10.50.1
        AVP: l=6  t=NAS-Port(5): 1


Frame 14 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.50.1 (10.10.50.1)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 1366 (1366)
Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0xf3 (243)
    Length: 32
    Authenticator: 656E2696110131703FC73E3B059FE5BE
    [This is a response to a request in frame 13]
    [Time from request: 0.001203000 seconds]
    Attribute Value Pairs
        AVP: l=12  t=Vendor-Specific(26) v=Bay-Networks(1584)
            VSA: l=6 t=Unknown-Attribute(192): 00000006  rwa
                Unknown-Attribute: 00000006


Frame 15 (93 bytes on wire, 93 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.50.1 (10.10.50.1), Dst: 10.10.50.40 (10.10.50.40)
User Datagram Protocol, Src Port: 32000 (32000), Dst Port: radacct (1813)
Radius Protocol
    Code: Accounting-Request (4)
    Packet identifier: 0xf3 (243)
    Length: 51
    Authenticator: 77886F4741D41F177158C4032B17CCAB
    [The response to this request is in frame 16]
    Attribute Value Pairs
        AVP: l=6  t=Acct-Status-Type(40): Start(1)
        AVP: l=6  t=NAS-IP-Address(4): 10.10.50.1
        AVP: l=14  t=Acct-Session-Id(44): 09f500000015
        AVP: l=5  t=User-Name(1): rwa


Frame 16 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
```

```
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.50.1 (10.10.50.1)
User Datagram Protocol, Src Port: radacct (1813), Dst Port: 32000 (32000)
Radius Protocol
    Code: Accounting-Response (5)
    Packet identifier: 0xf3 (243)
    Length: 20
    Authenticator: 862C60235782477D44532C49CB4BD972
    [This is a response to a request in frame 15]
    [Time from request: 0.000637000 seconds]


Frame 17 (175 bytes on wire, 175 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.50.1 (10.10.50.1), Dst: 10.10.50.40 (10.10.50.40)
User Datagram Protocol, Src Port: 32000 (32000), Dst Port: radacct (1813)
Radius Protocol
    Code: Accounting-Request (4)
    Packet identifier: 0xab (171)
    Length: 133
    Authenticator: 2AAC3EA5073595B9482F962350FF269D
    [The response to this request is in frame 18]
    Attribute Value Pairs
        AVP: l=6  t=Acct-Status-Type(40): Stop(2)
        AVP: l=14  t=Acct-Session-Id(44): 09f500000015
        AVP: l=5  t=User-Name(1): rwa
        AVP: l=6  t=NAS-IP-Address(4): 10.10.50.1
        AVP: l=6  t=Acct-Session-Time(46): 18
        AVP: l=6  t=Acct-Input-Octets(42): 0
        AVP: l=6  t=Acct-Output-Octets(43): 619
        AVP: l=6  t=Acct-Input-Packets(47): 0
        AVP: l=6  t=Acct-Output-Packets(48): 74
        AVP: l=17  t=Vendor-Specific(26) v=Bay-Networks(1584)
            VSA: l=11 t=Unknown-Attribute(193): 73686F772064617465
                Unknown-Attribute: 73686F772064617465  cli: show date
        AVP: l=14  t=Vendor-Specific(26) v=Bay-Networks(1584)
            VSA: l=8 t=Unknown-Attribute(193): 636F6E666967
                Unknown-Attribute: 636F6E666967        cli: config
        AVP: l=9  t=Vendor-Specific(26) v=Bay-Networks(1584)
            VSA: l=3 t=Unknown-Attribute(193): 3F      cli: ?
                Unknown-Attribute: 3F
        AVP: l=12  t=Vendor-Specific(26) v=Bay-Networks(1584)
            VSA: l=6 t=Unknown-Attribute(193): 65786974
                Unknown-Attribute: 65786974            cli: exit


Frame 18 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.50.1 (10.10.50.1)
User Datagram Protocol, Src Port: radacct (1813), Dst Port: 32000 (32000)
Radius Protocol
    Code: Accounting-Response (5)
    Packet identifier: 0xab (171)
    Length: 20
    Authenticator: DE41DB6E3E886460786E0FE359190AEF
    [This is a response to a request in frame 17]
    [Time from request: 0.001343000 seconds]
```

2.6.5 RADIUS User Access Profile

```
Frame 1 (96 bytes on wire, 96 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.50.1 (10.10.50.1), Dst: 10.10.50.40 (10.10.50.40)
User Datagram Protocol, Src Port: 1450 (1450), Dst Port: radius (1812)
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x7 (7)
    Length: 54
    Authenticator: 00007807000034B60000321C0000513D
    [The response to this request is in frame 2]
    Attribute Value Pairs
        AVP: l=4  t=User-Name(1): rw
        AVP: l=18  t=User-Password(2): Encrypted
        AVP: l=6  t=NAS-IP-Address(4): 10.10.50.1
        AVP: l=6  t=NAS-Port(5): 1

Frame 2 (115 bytes on wire, 115 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.50.1 (10.10.50.1)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 1450 (1450)
Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x7 (7)
    Length: 73
    Authenticator: AD8EE66C81BB8548F53ABA76A570E89C
    [This is a response to a request in frame 1]
    [Time from request: 0.001087000 seconds]
    Attribute Value Pairs
        AVP: l=12  t=Vendor-Specific(26) v=Bay-Networks(1584)
            VSA: l=6 t=Unknown-Attribute(192): 00000005
                Unknown-Attribute: 00000005
        AVP: l=12  t=Vendor-Specific(26) v=Bay-Networks(1584)
            VSA: l=6 t=Unknown-Attribute(194): 00000000
                Unknown-Attribute: 00000000
        AVP: l=17  t=Vendor-Specific(26) v=Bay-Networks(1584)
            VSA: l=11 t=Unknown-Attribute(195): 636F6E666967206970
                Unknown-Attribute: 636F6E666967206970          config ip
        AVP: l=12  t=Vendor-Specific(26) v=Bay-Networks(1584)
            VSA: l=6 t=Unknown-Attribute(195): 74657374
                Unknown-Attribute: 74657374                    test
```

3. TACACS+

Ethernet Routing Switch 5500, 1600 and 8300 Series all support the Terminal Access Controller Access Control System plus (TACACS+) client. TACACS+ is a security application implemented as a client/server-based protocol that provides centralized validation of users attempting to gain access to a router or network access server.

TACACS+ differs from RADIUS in two important ways:

- TACACS+ is a TCP-based protocol using port 49
- TACACS+ uses full packet encryption, rather than just encrypting the password (RADIUS authentication request)

TACACS+ encrypts the entire body of the packet and uses a standard TACACS+ header

TACACS+ separates authentication, authorization, and accounting services. This means that you can selectively implement one or more TACACS+ services.

TACACS+ provides management of users who access the switch through Telnet, serial, and SSH v2 connections. TACACS+ supports users only on the CLI.

Access to the console interface, SNMP, and Web management are disabled when TACACS+ is enabled.

The TACACS+ protocol is a draft standard available at: ftp://ietf.org/internetdrafts/

draft-grant-tacacs-02

TACACS+ is not compatible with any previous versions of TACACS.

3.1 Terminology

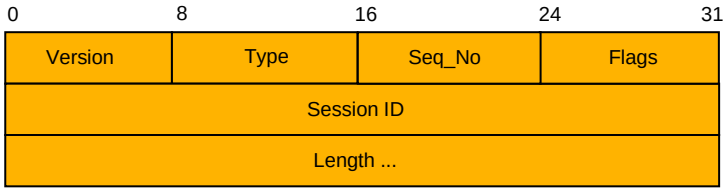
The following terms are used in connection with TACACS+:

- AAA - Authentication, Authorization, Accounting
  - Authentication is the action of determining who a user (or entity) is, before allowing the user to access the network and network services.
  - Authorization is the action of determining what an authenticated user is allowed to do.
  - Accounting is the action of recording what a user is doing or has done.
- Network Access Server (NAS)—any client, such as an Ethernet Routing Switch 1600, 5500 and 8300 Series switches, that makes TACACS+ authentication and authorization requests, or generates TACACS+ accounting packets.
- daemon/server—a program that services network requests for authentication and authorization, verifies identities, grants or denies authorizations, and logs accounting records.
- AV pairs—strings of text in the form "attribute=value" sent between a NAS and a TACACS+ daemon as part of the TACACS+ protocol.

3.2 Feature Operation

During the log on process, the TACACS+ client initiates the TACACS+ authentication session with the server. After successful authentication, if TACACS+ authorization is enabled, the TACACS+ client initiates the TACACS+ authorization session with the server. After successful authentication, if TACACS+ accounting is enabled, the TACACS+ client sends accounting information to the TACACS+ server.

TACACS+ Packet format – RFC Draft*



Version : 0xC0, 0xC1

Type : 0x01 Authentication
0x02 Authorization
0x03 Accounting

Seq_No : Always start with 1 then incremented.

Flags : 0x01unencryption
0x04 Single connection

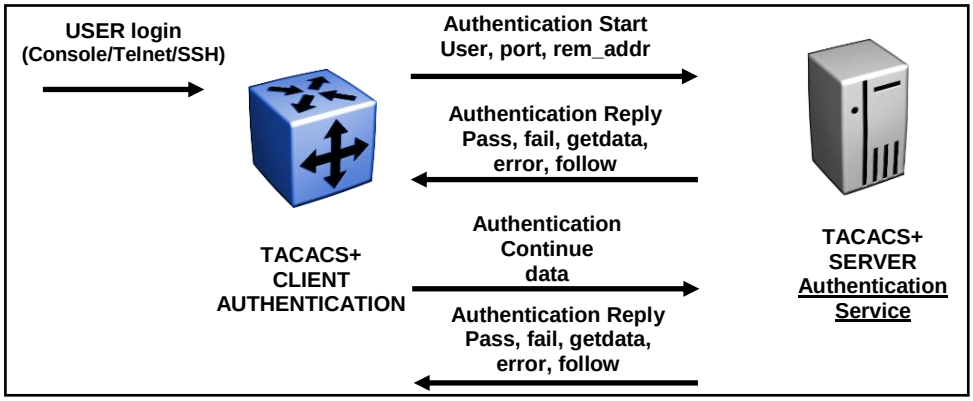
Length : Tacacs+ packet body (without header)

Following information in packet are encrypted with MD5 hashes.

(*) The TACACS+ protocol is a draft standard available at: ftp://ietf.org/internetdrafts/draft-grant-tacacs-02

3.2.1 TACACS+ Authentication

TACACS + authentication offers complete control of authentication through log on/password dialog and response. The authentication session provides username/password functionality.



You cannot enable both RADIUS and TACACS+ authentication on the same interface. However, you can enable RADIUS and TACACS+ on different interfaces; for example, RADIUS on the serial connection and TACACS+ on the Telnet connection.

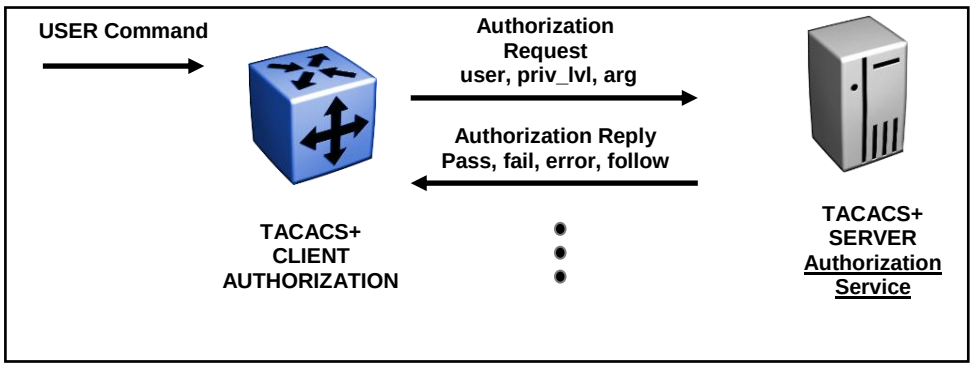
Prompts for log on and password occur prior during the authentication process. If TACACS+ fails because there are no valid servers, then the username and password are used from the local database. If TACACS+ or the local database return an access denied packet, then the authentication process stops. No other authentication methods are attempted.

3.2.2 TACACS+ Authorization

The transition from TACACS+ authentication to the authorization phase is transparent to the user. Upon successful completion of the authentication session, an authorization session starts with the authenticated username. The authorization session provides access level functionality.

TACACS+ authorization enables you to limit the switch commands available to a user. When TACACS+ authorization is enabled, the NAS uses information retrieved from the user profile, which is located either in the local user database or on the security server, to configure the user's session. The user is granted access to a requested command only if the information in the user profile allows it.

TACACS+ authorization is not mandatory for all privilege levels.



When authorization is requested by the NAS, the entire command is sent to the TACACS+ daemon for authorization. You can preconfigure command authorization on the TACACS+ server by specifying a list of regular expressions that match command arguments, and associating each command with an action to deny or permit.

Authorization is recursive over groups. Thus, if you place a user in a group, the daemon looks in the group for authorization parameters if it cannot find them in the user declaration.

If authorization is enabled for a privilege level to which a user is assigned, the TACACS+ server denies any commands for which access is not explicitly granted for the specific user or for the user's group. On the daemon, ensure that each group is authorized to access basic commands such as **`enable`** or **`logout`**.

If the TACACS+ server is not available or an error occurs during the authorization process, the only command available is **`logout`**.

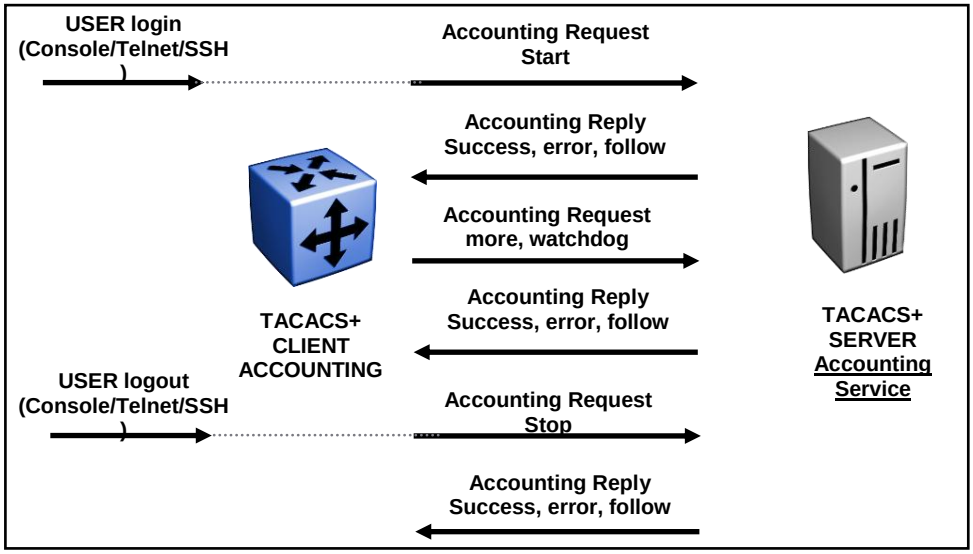
In the TACACS+ server configuration, if no privilege level is defined for a user but the user is allowed to execute at least one command, the user defaults to privilege level 0. If all commands are explicitly denied for a user, the user cannot access the switch at all.

3.2.3 TACACS+ Accounting

TACACS+ accounting enables you to track:

- the services accessed by users
- the amount of network resources consumed by users

When accounting is enabled, the NAS reports user activity to the TACACS+ server in the form of accounting records. Each accounting record contains accounting AV pairs. The accounting records are stored on the security server. The accounting data can then be analyzed for network management and auditing.



TACACS+ accounting provides information about user CLI terminal sessions within serial, Telnet, or SSH shells (in other words, from the CLI management interface).

3.2.4 TACACS+ Session

A TACACS+ session is a single authentication sequence, a single authorization exchange, or a single accounting exchange.

The session concept is important because a session identifier is used as a part of the encryption, and it is used by both ends to distinguish between packets belonging to multiple sessions.

Multiple sessions may be supported simultaneously and/or consecutively on a single TCP connection if both the daemon and client support this.

If multiple sessions are not being multiplexed over a single tcp connection, a new connection should be opened for each TACACS+ session and closed at the end of that session. For accounting and authorization, this implies just a single pair of packets exchanged over the connection (the request and its reply). For authentication, a single session may involve an arbitrary number of packets being exchanged.

The session is an operational concept that is maintained between the TACACS+ client and daemon. It does not necessarily correspond to a given user or user action.

3.2.5 Changing Privilege Levels at Runtime

Users can change their privilege levels at runtime by using the following command on the switch:

```
5510(config)<level-5># tacacs switch level [<level>]
```

where **<level>** is the privilege level the user wants to access. The user is prompted to provide the required password. If the user does not specify a level in the command, the administration level (15) is selected by default.

To return to the original privilege level, the user uses the following command on the switch:

```
5510(config)<level-5># tacacs switch back
```

To support runtime switching of users to a particular privilege level, you must preconfigure a dummy user for that level on the daemon. The format of the user name for the dummy user is `$enab<n>$`, where **<n>** is the privilege level to which you want to allow access.

3.3 Avaya Switches TACACS+ Support

	TACACS+ Authentication	TACACS+ Authorization	TACACS+ Accounting	Multiple session Over single tcp connection	Changing privilege level at runtime
ERS 8600	POI (5.1)	POI (5.1)	POI (5.1)	POI (5.1)	POI (5.1)
ERS 8300	Yes	Yes	No	Yes	No
ERS 1600	Yes	Yes	No	Yes	No
ES 460/470	No	No	No	No	No
ERS 2500	POI (4.2)	POI (4.2)	POI (4.2)	No	POI (4.2)
ERS 4500	POR (5.2)	POR (5.2)	POR (5.2)	No	POI (5.2)
ERS 5500	Yes	Yes	Yes	No	Yes

TACACS is only for administrative users and not for 802.1x (EAP) users. Refer to RADIUS for EAP users.

The following table shows the scheme used to map the access levels to TACACS+ privilege levels.

Access Level	ERS 1600,8300	ERS 5500
none	0	0
ro	1	1
l1	2	
l2	3	
l3	4	
rw	5	5
rwa	6	

3.4 TACACS+ Server Configuration – Using tac_plus

The following TACACS+ Server configuration is based on tac_plus, www.networkforums.net. Once installed on a Linux host, there is a unique configuration file to edit as shown below.

3.4.1 /etc/tacacs/tac_plus.cfg

This file contains all configuration parameters for TACACS+.

```
# Tacacs+ configuration file

key = Dda

# Accounting records log file

accounting file = /var/log/tac_acc.log

#All services are alowed..

user = DEFAULT {
    service = ppp protocol = ip {}
}

user = ro {
    member = level1
    login = cleartext readonly
    expires = "Dec 31 2008"
}

user = bsrw {
    default service = permit
    service = exec {
        priv-lvl = 5
        }
    login = cleartext bsrw
}

user = rwa {
    default service = permit
    service = exec {
        priv-lvl = 6
        }
    login = cleartext rwa
}

user = $enab6$ {
    member = level6
    login = cleartext rwa
}

group = level1 {
    cmd = enable { permit .* }
    cmd = show { permit .* }
```

```
    cmd = exit { permit .* }
    cmd = logout { permit .* }
    service = exec {
    priv-lvl = 1
    }
}

group = level6 {
    cmd = enable { permit .* }
    cmd = configure { permit terminal }
    cmd = show { permit .* }
    cmd = vlan { permit .* }
    cmd = interface { permit .* }
    cmd = router { permit .* }
    cmd = network { permit .* }
    cmd = logout { permit .* }
    service = exec {
    priv-lvl = 6
    }
}
```

You don't need to configure network devices as for RADIUS (client.conf).

3.4.2 /etc/init.d/tac_plus

This file is the startup file for TACACS process. Please check that you have a link to **`/etc/rcX.d/S99tac_plus`** (X can be 2, 3 or 5 depending on your run level). Also check that tac_plus is started with –d flag, you will write details about every request into **`/var/log/tac_plus.log`** file. The values represent bits, so they can be added together. Currently the following values are recognized:

Value	Meaning
8	authorization debugging
16	authentication debugging
32	password file processing debugging
64	accounting debugging
128	config file parsing & lookup
256	packet transmission/reception
512	encryption/decryption
1024	MD5 hash algorithm debugging
2048	very low level encryption/decryption

`Debug = 120` logs authorization, authentication, password and accounting

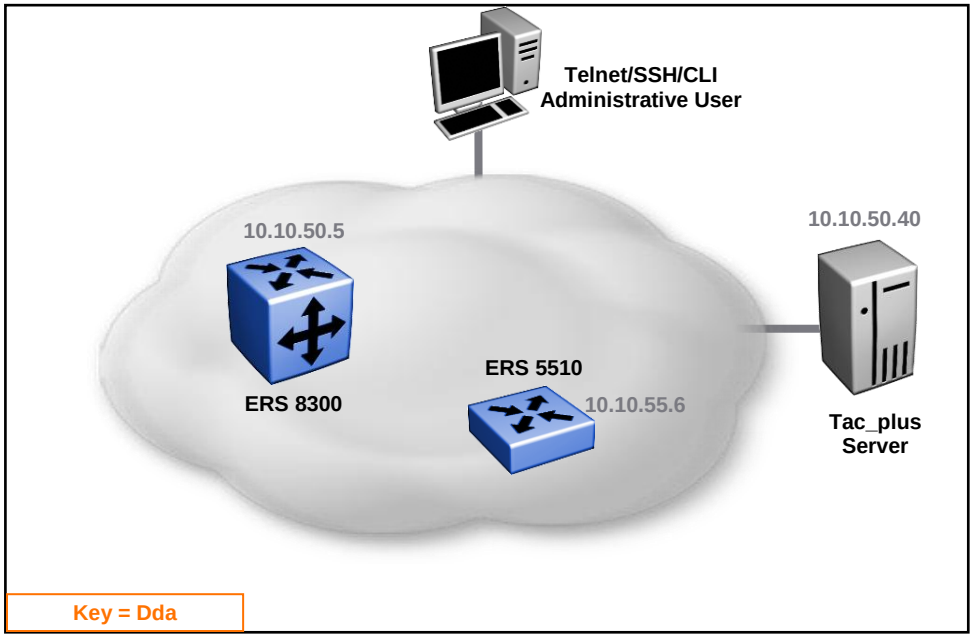
When you modify the configuration file, you have to restart tac_plus process using the following command:

```
[root@linux2 raddb]# /etc/rc5.d/S99tac_plus restart
```

3.5 TACACS+ Client Configuration

Two different product lines, ERS 5500 (and 2500, 4500 in the future) use a specific logic for configuration whereas ERS 1600, 8300 (and 8600 in the future) each uses a different logic for configuration.

Network diagram with TACAC+ client and server can be simplified and summarized as shown below:



3.5.1 ERS 5500

ACLI or JDM (Java Device Manager) can be used to configure the switch. For simplicity and readability, we will document command line interface (CLI) commands assuming the TACACS+ server IP address is 10.10.50.40, and the client key is “Dda” for telnet access authentication.

To configure TACACS+

```
5510# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
5510(config)# tacacs server host 10.10.50.40
5510(config)# tacacs server key  Dda
5510(config)# tacacs authorization enable
5510(config)# tacacs authorization level all
5510(config)# tacacs accounting enable
5510(config)# cli password switch telnet tacacs
```

To display TACACS configuration

```
5510# show tacacs
Primary Host:  10.10.50.40
Secondary Host:  0.0.0.0
```

```
Port:  49
Key:  ***************
TACACS+ authorization is enabled
Authorization is enabled on levels : 0-15
TACACS+ accounting is enabled
```

The source IP address sent by the switch (Layer 2 operation) is always the Management IP address configured on the switch when sending a TACACS+ client message.

There is no way to change the source TACACS+ IP address. When the switch is configured in routed mode, it uses interface IP address where frame is sent.

Hence, if you have multiple IP interfaces facing the core network where a TACACS+ message could be sent, you will have to configure the TACACS+ server with each IP address.

With the ERS 5500 switch, you can configure two TACACS+ servers, a primary server and a secondary server. If all servers are not reachable (no answers) then local authentication is done. You get the following message at console:

```
no response from TACACS+ servers
```

3.5.2 ERS 1600, 8300

ACLI or JDM (Java Device Manager) can be used to configure the switch, for simplicity and readability, we will document command line interface commands:

To configure TACACS+

```
8300:5# config tacacs enable true
8300:5# config tacacs server create 10.10.50.40 key Dda
```

To display TACACS+ configuration

```
8300:5# show tacacs info

Sub-Context: clear config monitor show test trace
Current Context:
                          enable : true

8300:5# show tacacs server config

Sub-Context: clear config monitor show test trace
Current Context:
                      create :

IP address      Status  Key         Port  Prio  Timeout Single Source
SourceEnabled
10.10.50.40     NotConn Dda         49    1     10      false  0.0.0.0
```

```
false

                        delete : N/A
                           set : N/A
```

With the ERS 1600 and 8300, you can change the TACACS+ source IP address by using the following command.

```
Config tacacs server create <ipaddr> key <value> [port <value>]
[priority <value>] [timeout <value>] [single-connection <value>]
[source <value>] [sourceIpInterfaceEnabled <value>]
```

You can change the TACACS+ behavior to support multiplexing sessions over a single TCP connection (default is false) by using the following command.

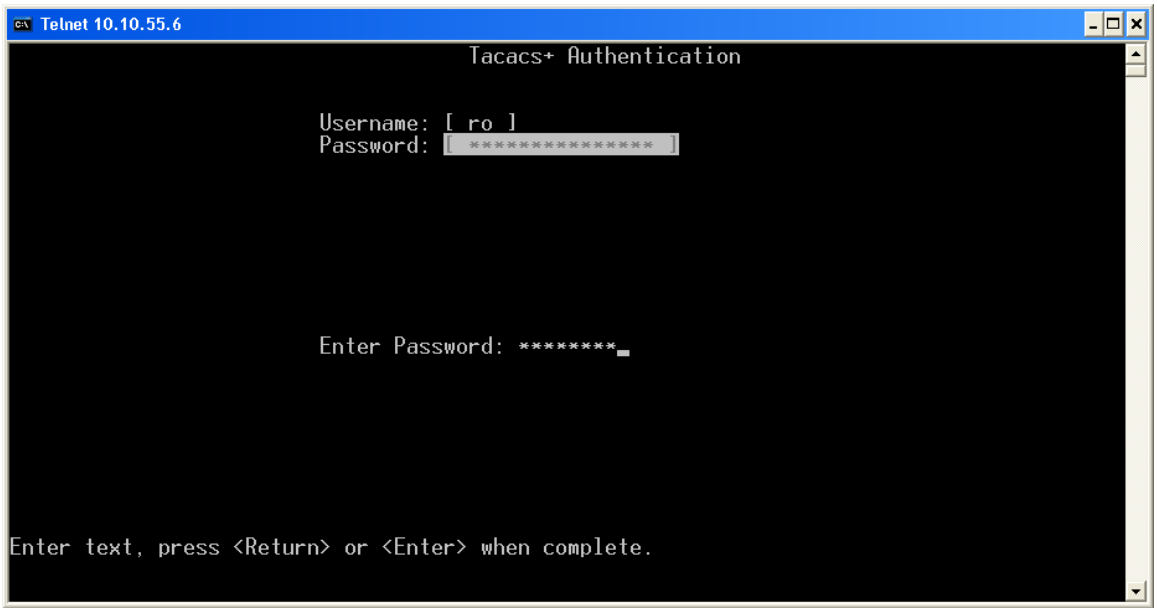
```
Config tacacs server create <ipaddr> key <value> [port <value>]
[priority <value>] [timeout <value>] [single-connection <value>]
[source <value>] [sourceIpInterfaceEnabled <value>]
```

3.6 TACACS+ Server & Client Log Files

In this section, we will demonstrate TACACS+ server and client accessing a switch. We will demonstrate a client logging onto a switch, issuing several commands and checking if they are allowed or not based on authentication rights.

3.6.1 ERS 5500 – Read-Only User

Connect to the device with telnet using read-only user (ro).



Telnet to Switch with read-only user (ro) type some commands

```
5510<level-1>> en
5510<level-1># show clock
    Current SNTP time  :    2008-02-26 14:33:17 GMT+01:00
    Daylight saving time is DISABLED
    Time Zone is set to 'METD', offset from UTC is 01:00
5510<level-1># conf t
%Your command was not authorized
5510<level-1># exit
```

Read-only user in this example does not have access to switch configuration.

Log file on TACACS server - /var/log/tac_acc.log

```
Tue Feb 26 14:30:10 2008        10.10.55.6      ro      Telnet Session 1
10.10.50.10      start   reason=User logged in
Tue Feb 26 14:30:27 2008        10.10.55.6      ro      Telnet Session 1
10.10.50.10      stop    start_time=1631962      stop_time=1631979
elapsed_time=17 reason=User logged out
```

Log file on TACACS server - /var/log/tac_plus.log

Depends on debug value configured /etc/rc5.d/S99tac_plus

```
Tue Feb 26 14:30:10 2008 [16403]: verify: login access for user 'ro' to port
Telnet Session 1 on 10.10.55.6 from 10.10.50.10
Tue Feb 26 14:30:10 2008 [16403]: cfg_check_host_group_access: checking login
access to host '10.10.55.6' for user 'ro'
Tue Feb 26 14:30:10 2008 [16403]: cfg_check_host_group_access: access
permittedbecause host not defined
Tue Feb 26 14:30:10 2008 [16403]: verify: using user/group auth parameters
Tue Feb 26 14:30:10 2008 [16403]: verify: Using auth_method cleartext(11)
with data readonly
Tue Feb 26 14:30:10 2008 [16403]: Password has not expired Dec 31 2008
Tue Feb 26 14:30:10 2008 [16403]: verify: login cleartext authentication
successful
Tue Feb 26 14:30:10 2008 [16403]: default_fn: login query for 'ro' Telnet
Session 1 from 10.10.55.6 accepted
Tue Feb 26 14:30:10 2008 [16404]: Start accounting request
Tue Feb 26 14:30:10 2008 [16404]: 'Tue Feb 26 14:30:10 2008     10.10.55.6
ro       Telnet Session 1        10.10.50.10     start   reason=User logged
in'
Tue Feb 26 14:30:10 2008 [16405]: Start authorization request
```

```
Tue Feb 26 14:30:10 2008 [16405]: do_author: user 'ro' found
Tue Feb 26 14:30:10 2008 [16405]: exec authorization request for ro
Tue Feb 26 14:30:10 2008 [16405]: exec is explicitly permitted by line 97
Tue Feb 26 14:30:10 2008 [16405]: author_svc: nas:service=shell (passed thru)
Tue Feb 26 14:30:10 2008 [16405]: author_svc: nas:cmd= (passed thru)
Tue Feb 26 14:30:10 2008 [16405]: author_svc: nas:absent, server:priv-lvl=1 -
> add priv-lvl=1 (k)
Tue Feb 26 14:30:10 2008 [16405]: author_svc: added 1 args
Tue Feb 26 14:30:10 2008 [16405]: author_svc: out_args[0] = service=shell
input copy discarded
Tue Feb 26 14:30:10 2008 [16405]: author_svc: out_args[1] = cmd= input copy
discarded
Tue Feb 26 14:30:10 2008 [16405]: author_svc: out_args[2] = priv-lvl=1
compacted to out_args[0]
Tue Feb 26 14:30:10 2008 [16405]: author_svc: 1 output args
Tue Feb 26 14:30:10 2008 [16405]: authorization query for 'ro' unknown from
10.10.55.6 accepted
Tue Feb 26 14:30:23 2008 [16406]: Start authorization request
Tue Feb 26 14:30:23 2008 [16406]: do_author: user 'ro' found
Tue Feb 26 14:30:23 2008 [16406]: authorize_cmd: enable
Tue Feb 26 14:30:23 2008 [16406]: line 93 compare enable permit '.*' & ''
match
Tue Feb 26 14:30:23 2008 [16406]: enable  permitted by line 93
Tue Feb 26 14:30:23 2008 [16406]: authorization query for 'ro' unknown from
10.10.55.6 accepted
Tue Feb 26 14:30:25 2008 [16407]: Start authorization request
Tue Feb 26 14:30:25 2008 [16407]: do_author: user 'ro' found
Tue Feb 26 14:30:25 2008 [16407]: authorize_cmd: show clock
Tue Feb 26 14:30:25 2008 [16407]: line 94 compare show permit '.*' & 'clock'
match
Tue Feb 26 14:30:25 2008 [16407]: show clock permitted by line 94
Tue Feb 26 14:30:25 2008 [16407]: authorization query for 'ro' unknown from
10.10.55.6 accepted
Tue Feb 26 14:30:27 2008 [16408]: Start authorization request
Tue Feb 26 14:30:27 2008 [16408]: do_author: user 'ro' found
Tue Feb 26 14:30:27 2008 [16408]: authorize_cmd: exit
Tue Feb 26 14:30:27 2008 [16408]: line 95 compare exit permit '.*' & '' match
Tue Feb 26 14:30:27 2008 [16408]: exit  permitted by line 95
Tue Feb 26 14:30:27 2008 [16408]: authorization query for 'ro' unknown from
10.10.55.6 accepted
Tue Feb 26 14:30:27 2008 [16409]: Start accounting request
Tue Feb 26 14:30:27 2008 [16409]: 'Tue Feb 26 14:30:27 2008     10.10.55.6
ro       Telnet Session 1        10.10.50.10     stop    start_time=1631962
stop_time=1631979        elapsed_time=17 reason=User logged out
```

Log file on TACACS+ client

```
I    2008-02-26 14:30:05 GMT+01:00 139      #1 Successful connection from IP
address: 10.10.50.10
I    2008-02-26 14:30:34 GMT+01:00 140      #1 Session closed (user logout),
IP address: 10.10.50.10, access mode: no security
I    2008-02-26 14:30:35 GMT+01:00 141      #1 Connection closed (user
logout), IP address: 10.10.50.10
```

Please note the log file does not display user login or access level. The log file does not contain any session statistics.

3.6.2 ERS 5500 – Read-Write User

Connect to the device with telnet using read-only user (bsrw).

Telnet to Switch with read-write user (bsrw) type some commands

```
5510<level-5>> en
5510<level-5># show clock
    Current SNTP time  :    2008-02-26 14:35:28 GMT+01:00
    Daylight saving time is DISABLED
    Time Zone is set to 'METD', offset from UTC is 01:00
5510<level-5># config t
Enter configuration commands, one per line.  End with CNTL/Z.
5510(config)<level-5># interface fastEthernet all
5510(config-if)<level-5># exit
5510(config)<level-5># exit
5510<level-5># exit
```

Read-write user in this example does have access to switch configuration.

Log file on TACACS server - /var/log/tac_acc.log

```
Tue Feb 26 14:35:12 2008        10.10.55.6      bsrw    Telnet Session 1
10.10.50.10      start   reason=User logged in
Tue Feb 26 14:35:49 2008        10.10.55.6      bsrw    Telnet Session 1
10.10.50.10      stop    start_time=1632263     stop_time=1632301
elapsed_time=38 reason=User logged out
```

Log file on TACACS server - /var/log/tac_plus.log

Depends on debug value configured /etc/rc5.d/S99tac_plus

```
Tue Feb 26 14:35:12 2008 [16434]: verify: login access for user 'bsrw' to
port Telnet Session 1 on 10.10.55.6 from 10.10.50.10
Tue Feb 26 14:35:12 2008 [16434]: cfg_check_host_group_access: checking login
access to host '10.10.55.6' for user 'bsrw'
Tue Feb 26 14:35:12 2008 [16434]: cfg_check_host_group_access: access
permitted because host not defined
Tue Feb 26 14:35:12 2008 [16434]: verify: using user/group auth parameters
Tue Feb 26 14:35:12 2008 [16434]: verify: Using auth_method cleartext(11)
with data bsrw
Tue Feb 26 14:35:12 2008 [16434]: Password has not expired <no expiry date
set>
Tue Feb 26 14:35:12 2008 [16434]: verify: login cleartext authentication
successful
Tue Feb 26 14:35:12 2008 [16434]: default_fn: login query for 'bsrw' Telnet
Session 1 from 10.10.55.6 accepted
Tue Feb 26 14:35:12 2008 [16435]: Start accounting request
Tue Feb 26 14:35:12 2008 [16435]: 'Tue Feb 26 14:35:12 2008     10.10.55.6
bsrw     Telnet Session 1        10.10.50.10     start   reason=User logged
in'
Tue Feb 26 14:35:12 2008 [16436]: Start authorization request
Tue Feb 26 14:35:12 2008 [16436]: do_author: user 'bsrw' found
Tue Feb 26 14:35:12 2008 [16436]: exec authorization request for bsrw
Tue Feb 26 14:35:12 2008 [16436]: exec is explicitly permitted by line 59
Tue Feb 26 14:35:12 2008 [16436]: author_svc: nas:service=shell (passed thru)
Tue Feb 26 14:35:12 2008 [16436]: author_svc: nas:cmd= (passed thru)
Tue Feb 26 14:35:12 2008 [16436]: author_svc: nas:absent, server:priv-lvl=5 -
> add priv-lvl=5 (k)
Tue Feb 26 14:35:12 2008 [16436]: author_svc: added 1 args
Tue Feb 26 14:35:12 2008 [16436]: author_svc: out_args[0] = service=shell
input copy discarded
Tue Feb 26 14:35:12 2008 [16436]: author_svc: out_args[1] = cmd= input copy
discarded
Tue Feb 26 14:35:12 2008 [16436]: author_svc: out_args[2] = priv-lvl=5
compacted to out_args[0]
Tue Feb 26 14:35:12 2008 [16436]: author_svc: 1 output args
Tue Feb 26 14:35:12 2008 [16436]: authorization query for 'bsrw' unknown from
10.10.55.6 accepted
Tue Feb 26 14:35:14 2008 [16437]: Start authorization request
Tue Feb 26 14:35:14 2008 [16437]: do_author: user 'bsrw' found
Tue Feb 26 14:35:14 2008 [16437]: authorize_cmd: enable
Tue Feb 26 14:35:14 2008 [16437]: cmd enable does not exist, permitted by
default
Tue Feb 26 14:35:14 2008 [16437]: authorization query for 'bsrw' unknown from
10.10.55.6 accepted
Tue Feb 26 14:35:21 2008 [16438]: Start authorization request
Tue Feb 26 14:35:21 2008 [16438]: do_author: user 'bsrw' found
Tue Feb 26 14:35:21 2008 [16438]: authorize_cmd: show clock
Tue Feb 26 14:35:21 2008 [16438]: cmd show does not exist, permitted by
default
```

```
Tue Feb 26 14:35:21 2008 [16438]: authorization query for 'bsrw' unknown from
10.10.55.6 accepted
Tue Feb 26 14:35:24 2008 [16439]: Start authorization request
Tue Feb 26 14:35:24 2008 [16439]: do_author: user 'bsrw' found
Tue Feb 26 14:35:24 2008 [16439]: authorize_cmd: configure terminal
Tue Feb 26 14:35:24 2008 [16439]: cmd configure does not exist, permitted by
default
Tue Feb 26 14:35:24 2008 [16439]: authorization query for 'bsrw' unknown from
10.10.55.6 accepted
Tue Feb 26 14:35:30 2008 [16440]: Start authorization request
Tue Feb 26 14:35:30 2008 [16440]: do_author: user 'bsrw' found
Tue Feb 26 14:35:30 2008 [16440]: authorize_cmd: interface FastEthernet all
Tue Feb 26 14:35:30 2008 [16440]: cmd interface does not exist, permitted by
default
Tue Feb 26 14:35:30 2008 [16440]: authorization query for 'bsrw' unknown from
10.10.55.6 accepted
Tue Feb 26 14:35:32 2008 [16441]: Start authorization request
Tue Feb 26 14:35:32 2008 [16441]: do_author: user 'bsrw' found
Tue Feb 26 14:35:32 2008 [16441]: authorize_cmd: exit
Tue Feb 26 14:35:32 2008 [16441]: cmd exit does not exist, permitted by
default
Tue Feb 26 14:35:32 2008 [16441]: authorization query for 'bsrw' unknown from
10.10.55.6 accepted
Tue Feb 26 14:35:45 2008 [16442]: Start authorization request
Tue Feb 26 14:35:45 2008 [16442]: do_author: user 'bsrw' found
Tue Feb 26 14:35:45 2008 [16442]: authorize_cmd: exit
Tue Feb 26 14:35:45 2008 [16442]: cmd exit does not exist, permitted by
default
Tue Feb 26 14:35:45 2008 [16442]: authorization query for 'bsrw' unknown from
10.10.55.6 accepted
Tue Feb 26 14:35:49 2008 [16443]: Start authorization request
Tue Feb 26 14:35:49 2008 [16443]: do_author: user 'bsrw' found
Tue Feb 26 14:35:49 2008 [16443]: authorize_cmd: exit
Tue Feb 26 14:35:49 2008 [16443]: cmd exit does not exist, permitted by
default
Tue Feb 26 14:35:49 2008 [16443]: authorization query for 'bsrw' unknown from
10.10.55.6 accepted
Tue Feb 26 14:35:49 2008 [16444]: Start accounting request
Tue Feb 26 14:35:49 2008 [16444]: 'Tue Feb 26 14:35:49 2008     10.10.55.6
bsrw     Telnet Session 1        10.10.50.10     stop    start_time=1632263
stop_time=1632301        elapsed_time=38 reason=User logged out'
```

Log file on TACACS+ client

```
I    2008-02-26 14:35:10 GMT+01:00 148      #1 Successful connection from IP
address: 10.10.50.10
I    2008-02-26 14:35:56 GMT+01:00 149      #1 Session closed (user logout),
IP address: 10.10.50.10, access mode: no security
I    2008-02-26 14:35:56 GMT+01:00 150      #1 Connection closed (user
logout), IP address: 10.10.50.10
```

Please note that the log file only displays the connection. The log file does not contain any session statistic.

3.6.3 ERS 1600, 8300 – Read-Only User

Connect to the device with telnet using read-only user (ro).

Telnet to Switch with read-only user (ro) type some commands

```
8300:5> show date
local time:    TUE FEB 26 16:55:03 2008 METDST
hardware time: TUE FEB 26 15:55:03 2008 UTC8300:5> config ?

Sub-Context: cli log
Current Context:

    info

8300:5> exit
```

Read-only user in this example does not have access to switch configuration.

Log file on TACACS server - /var/log/tac_acc.log

```
NO ENTRY.
```

Please note that ERS 1600 and 8300 does not support TACACS+ accounting.

Log file on TACACS server - /var/log/tac_plus.log

Depends on debug value configured /etc/rc5.d/S99tac_plus

```
Tue Feb 26 16:49:21 2008 [16476]: verify: login access for user 'ro' to port
on 10.10.50.5 from 10.10.50.5
Tue Feb 26 16:49:21 2008 [16476]: cfg_check_host_group_access: checking login
access to host '10.10.50.5' for user 'ro'
Tue Feb 26 16:49:21 2008 [16476]: cfg_check_host_group_access: access
permitted because host not defined
Tue Feb 26 16:49:21 2008 [16476]: verify: using user/group auth parameters
Tue Feb 26 16:49:21 2008 [16476]: verify: Using auth_method cleartext(11)
with data readonly
Tue Feb 26 16:49:21 2008 [16476]: Password has not expired Dec 31 2008
```

```
Tue Feb 26 16:49:21 2008 [16476]: verify: login cleartext authentication
successful
Tue Feb 26 16:49:21 2008 [16476]: default_fn: login query for 'ro' unknown-
port from 10.10.50.5 accepted
Tue Feb 26 16:49:21 2008 [16477]: Start authorization request
Tue Feb 26 16:49:21 2008 [16477]: do_author: user 'ro' found
Tue Feb 26 16:49:21 2008 [16477]: exec authorization request for ro
Tue Feb 26 16:49:21 2008 [16477]: exec is explicitly permitted by line 97
Tue Feb 26 16:49:21 2008 [16477]: author_svc: nas:service=shell (passed thru)
Tue Feb 26 16:49:21 2008 [16477]: author_svc: nas:cmd* (passed thru)
Tue Feb 26 16:49:21 2008 [16477]: author_svc: nas:absent, server:priv-lvl=1 -
> add priv-lvl=1 (k)
Tue Feb 26 16:49:21 2008 [16477]: author_svc: added 1 args
Tue Feb 26 16:49:21 2008 [16477]: author_svc: out_args[0] = service=shell
input copy discarded
Tue Feb 26 16:49:21 2008 [16477]: author_svc: out_args[1] = cmd* input copy
discarded
Tue Feb 26 16:49:21 2008 [16477]: author_svc: out_args[2] = priv-lvl=1
compacted to out_args[0]
Tue Feb 26 16:49:21 2008 [16477]: author_svc: 1 output args
Tue Feb 26 16:49:21 2008 [16477]: authorization query for 'ro' unknown from
10.10.50.5 accepted
```

Please note this version of TACACS+ does not support any other TACACS+ arguments in authorization requests, such as cmd, cmd-arg, acl, zonelist, addr, routing, and so on. If you attempt to configure any argument in authorization requests (other than access level and privilege level), the TACACS+ request is dropped by the switch and an error is recorded to system log

Log file on TACACS+ client

```
CPU5 [02/26/08 16:54:56] SW INFO TACACS+ authentication succeeded
CPU5 [02/26/08 16:54:56] SW INFO user ro connected from 10.10.50.10 via telnet
CPU5 [02/26/08 16:55:09] SW INFO Closed telnet connection from IP 10.10.50.10, user
ro
```

3.6.4 ERS 1600, 8300 – Read-Write User

Connect to the device with telnet using read-only user (rwa).

Telnet to Switch with read-write user (rwa) type some commands

```
8300:5# show date
local time:    TUE FEB 26 17:33:03 2008 METDST
hardware time: TUE FEB 26 16:33:03 2008 UTC
8300:5# config ?

Sub-Context: bootconfig cli diag ethernet filter ip lldp log mlt nsna ntp poe
radius rmon
slot slpp stg sys snmp-v3 snmp-server tacacs vlan web-server qos
Current Context:

    auto-recover-delay <seconds>
    info
    load-encryption-module <3DES|DES|AES>
    setdate <MMddyyyyhhmmss>

8300:5# exit
```

Read-write user in this example does have access to switch configuration.

Log file on TACACS server - /var/log/tac_acc.log

```
NO ENTRY.
```

Please note that ERS 1600 and 8300 does not support TACACS+ accounting.

Log file on TACACS server - /var/log/tac_plus.log

Depends on debug value configured /etc/rc5.d/S99tac_plus

```
Tue Feb 26 17:27:24 2008 [16484]: verify: login access for user 'rwa' to port
on 10.10.50.5 from 10.10.50.5
Tue Feb 26 17:27:24 2008 [16484]: cfg_check_host_group_access: checking login
access to host '10.10.50.5' for user 'rwa'
Tue Feb 26 17:27:24 2008 [16484]: cfg_check_host_group_access: access
permitted because host not defined
Tue Feb 26 17:27:24 2008 [16484]: verify: using user/group auth parameters
```

```
Tue Feb 26 17:27:24 2008 [16484]: verify: Using auth_method cleartext(11)
with data rwa
Tue Feb 26 17:27:24 2008 [16484]: Password has not expired <no expiry date
set>
Tue Feb 26 17:27:24 2008 [16484]: verify: login cleartext authentication
successful
Tue Feb 26 17:27:24 2008 [16484]: default_fn: login query for 'rwa' unknown-
port from 10.10.50.5 accepted
Tue Feb 26 17:27:24 2008 [16485]: Start authorization request
Tue Feb 26 17:27:24 2008 [16485]: do_author: user 'rwa' found
Tue Feb 26 17:27:24 2008 [16485]: exec authorization request for rwa
Tue Feb 26 17:27:24 2008 [16485]: exec is explicitly permitted by line 51
Tue Feb 26 17:27:24 2008 [16485]: author_svc: nas:service=shell (passed thru)
Tue Feb 26 17:27:24 2008 [16485]: author_svc: nas:cmd* (passed thru)
Tue Feb 26 17:27:24 2008 [16485]: author_svc: nas:absent, server:priv-lvl=6 -
> add priv-lvl=6 (k)
Tue Feb 26 17:27:24 2008 [16485]: author_svc: added 1 args
Tue Feb 26 17:27:24 2008 [16485]: author_svc: out_args[0] = service=shell
input copy discarded
Tue Feb 26 17:27:24 2008 [16485]: author_svc: out_args[1] = cmd* input copy
discarded
Tue Feb 26 17:27:24 2008 [16485]: author_svc: out_args[2] = priv-lvl=6
compacted to out_args[0]
Tue Feb 26 17:27:24 2008 [16485]: author_svc: 1 output args
Tue Feb 26 17:27:24 2008 [16485]: authorization query for 'rwa' unknown from
10.10.50.5 accepted
```

Please note this version –(Note add version here - of TACACS+ does not support any other TACACS+ arguments in authorization requests, such as cmd, cmd-arg, acl, zonelist, addr, routing, and so on. If you attempt to configure any argument in authorization requests (other than access level and privilege level), the TACACS+ request is dropped by the switch and an error is recorded to system log

Log file on TACACS+ client

```
CPU5 [02/26/08 17:32:59] SW INFO TACACS+ authentication succeeded
CPU5 [02/26/08 17:32:59] SW INFO user rwa connected from 10.10.50.10 via
telnet
CPU5 [02/26/08 17:33:13] SW INFO Closed telnet connection from IP
10.10.50.10, user rwa
```

3.7 Sniffer Traces on TACACS+ Server

3.7.1 TACACS Read-Only User

The following trace displays the TACAC+ tcp flows , including SYN/SYN ACK/ACK (summary line, not detailed). It includes authentication, authorization and accounting. Note that TACACS messages are encrypted and only part of the message can be decoded.

```
No.     Time        Source                Destination           Protocol Info
      1 0.000000    10.10.55.6            10.10.50.40           TCP      1190 > 49
[SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=3264254 TSER=0

No.     Time        Source                Destination           Protocol Info
      2 0.000045    10.10.50.40           10.10.55.6            TCP      49 > 1190
[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=3143898087 TSER=3264254 WS=0


No.     Time        Source                Destination           Protocol Info
      3 0.001412    10.10.55.6            10.10.50.40           TCP      1190 > 49
[ACK] Seq=1 Ack=1 Win=8192 Len=0 TSV=3264254 TSER=3143898087


No.     Time        Source                Destination           Protocol Info
      4 0.001953    10.10.55.6            10.10.50.40           TACACS+  Q:
Authentication

Frame 4 (115 bytes on wire, 115 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.55.6 (10.10.55.6), Dst: 10.10.50.40 (10.10.50.40)
Transmission Control Protocol, Src Port: 1190 (1190), Dst Port: 49 (49), Seq: 1, Ack:
1, Len: 49
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authentication (1)
    Sequence number: 1
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 1919266898
    Packet length: 37
    Encrypted Request

No.     Time        Source                Destination           Protocol Info
      5 0.001985    10.10.50.40           10.10.55.6            TCP      49 > 1190
[ACK] Seq=1 Ack=50 Win=5792 Len=0 TSV=3143898087 TSER=3264254


No.     Time        Source                Destination           Protocol Info
      6 0.002180    10.10.50.40           10.10.55.6            TACACS+  R:
Authentication

Frame 6 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.55.6 (10.10.55.6)
```

```
Transmission Control Protocol, Src Port: 49 (49), Dst Port: 1190 (1190), Seq: 1, Ack:
50, Len: 28
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authentication (1)
    Sequence number: 2
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 1919266898
    Packet length: 16
    Encrypted Reply

No.     Time        Source                Destination           Protocol Info
      7 0.003212    10.10.55.6            10.10.50.40           TCP      1190 > 49
[ACK] Seq=50 Ack=29 Win=8192 Len=0 TSV=3264254 TSER=3143898087


No.     Time        Source                Destination           Protocol Info
      8 0.003618    10.10.55.6            10.10.50.40           TACACS+  Q:
Authentication

Frame 8 (91 bytes on wire, 91 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.55.6 (10.10.55.6), Dst: 10.10.50.40 (10.10.50.40)
Transmission Control Protocol, Src Port: 1190 (1190), Dst Port: 49 (49), Seq: 50, Ack:
29, Len: 25
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authentication (1)
    Sequence number: 3
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 1919266898
    Packet length: 13
    Encrypted Request

No.     Time        Source                Destination           Protocol Info
      9 0.004275    10.10.50.40           10.10.55.6            TACACS+  R:
Authentication

Frame 9 (102 bytes on wire, 102 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.55.6 (10.10.55.6)
Transmission Control Protocol, Src Port: 49 (49), Dst Port: 1190 (1190), Seq: 29, Ack:
75, Len: 36
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authentication (1)
    Sequence number: 4
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
```

```
    Session ID: 1919266898
    Packet length: 24
    Encrypted Reply

No.     Time        Source                Destination           Protocol Info
     10 0.004352    10.10.50.40           10.10.55.6            TCP      49 > 1190
[FIN, ACK] Seq=65 Ack=75 Win=5792 Len=0 TSV=3143898087 TSER=3264254


No.     Time        Source                Destination           Protocol Info
     11 0.005546    10.10.55.6            10.10.50.40           TCP      1190 > 49
[FIN, ACK] Seq=75 Ack=65 Win=8192 Len=0 TSV=3264254 TSER=3143898087


No.     Time        Source                Destination           Protocol Info
     12 0.005586    10.10.50.40           10.10.55.6            TCP      49 > 1190
[ACK] Seq=66 Ack=76 Win=5792 Len=0 TSV=3143898088 TSER=3264254


No.     Time        Source                Destination           Protocol Info
     13 0.006621    10.10.55.6            10.10.50.40           TCP      1191 > 49
[SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=3264254 TSER=0


No.     Time        Source                Destination           Protocol Info
     14 0.006647    10.10.50.40           10.10.55.6            TCP      49 > 1191
[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=3143898088 TSER=3264254 WS=0


No.     Time        Source                Destination           Protocol Info
     15 0.007083    10.10.55.6            10.10.50.40           TCP      1190 > 49
[FIN, ACK] Seq=75 Ack=66 Win=8192 Len=0 TSV=3264254 TSER=3143898087


No.     Time        Source                Destination           Protocol Info
     16 0.007997    10.10.55.6            10.10.50.40           TCP      1191 > 49
[ACK] Seq=1 Ack=1 Win=8192 Len=0 TSV=3264254 TSER=3143898088


No.     Time        Source                Destination           Protocol Info
     17 0.009581    10.10.55.6            10.10.50.40           TACACS+  Q: Accounting

Frame 17 (138 bytes on wire, 138 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.55.6 (10.10.55.6), Dst: 10.10.50.40 (10.10.50.40)
Transmission Control Protocol, Src Port: 1191 (1191), Dst Port: 49 (49), Seq: 1, Ack:
1, Len: 72
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Accounting (3)
    Sequence number: 1
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 2408421135
    Packet length: 60
    Encrypted Request
```

```
No.     Time        Source                Destination           Protocol Info
     18 0.009609    10.10.50.40           10.10.55.6            TCP      49 > 1191
[ACK] Seq=1 Ack=73 Win=5792 Len=0 TSV=3143898088 TSER=3264254


No.     Time        Source                Destination           Protocol Info
     19 0.010068    10.10.50.40           10.10.55.6            TACACS+  R: Accounting

Frame 19 (83 bytes on wire, 83 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.55.6 (10.10.55.6)
Transmission Control Protocol, Src Port: 49 (49), Dst Port: 1191 (1191), Seq: 1, Ack:
73, Len: 17
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Accounting (3)
    Sequence number: 2
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 2408421135
    Packet length: 5
    Encrypted Reply

No.     Time        Source                Destination           Protocol Info
     20 0.010148    10.10.50.40           10.10.55.6            TCP      49 > 1191
[FIN, ACK] Seq=18 Ack=73 Win=5792 Len=0 TSV=3143898088 TSER=3264254


No.     Time        Source                Destination           Protocol Info
     21 0.011295    10.10.55.6            10.10.50.40           TCP      1191 > 49
[ACK] Seq=73 Ack=18 Win=8192 Len=0 TSV=3264254 TSER=3143898088


No.     Time        Source                Destination           Protocol Info
     22 0.011667    10.10.55.6            10.10.50.40           TCP      1191 > 49
[FIN, ACK] Seq=73 Ack=18 Win=8192 Len=0 TSV=3264254 TSER=3143898088


No.     Time        Source                Destination           Protocol Info
     23 0.011681    10.10.50.40           10.10.55.6            TCP      49 > 1191
[ACK] Seq=19 Ack=74 Win=5792 Len=0 TSV=3143898088 TSER=3264254


No.     Time        Source                Destination           Protocol Info
     24 0.012718    10.10.55.6            10.10.50.40           TCP      1192 > 49
[SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=3264254 TSER=0


No.     Time        Source                Destination           Protocol Info
     25 0.012743    10.10.50.40           10.10.55.6            TCP      49 > 1192
[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=3143898088 TSER=3264254 WS=0


No.     Time        Source                Destination           Protocol Info
     26 0.013180    10.10.55.6            10.10.50.40           TCP      1191 > 49
```

```
[FIN, ACK] Seq=73 Ack=19 Win=8192 Len=0 TSV=3264254 TSER=3143898088


No.     Time        Source                Destination           Protocol Info
     27 0.014117    10.10.55.6            10.10.50.40           TCP      1192 > 49
[ACK] Seq=1 Ack=1 Win=8192 Len=0 TSV=3264254 TSER=3143898088


No.     Time        Source                Destination           Protocol Info
     28 0.015704    10.10.55.6            10.10.50.40           TACACS+  Q:
Authorization

Frame 28 (134 bytes on wire, 134 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.55.6 (10.10.55.6), Dst: 10.10.50.40 (10.10.50.40)
Transmission Control Protocol, Src Port: 1192 (1192), Dst Port: 49 (49), Seq: 1, Ack:
1, Len: 68
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 1
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 308467491
    Packet length: 56
    Encrypted Request

No.     Time        Source                Destination           Protocol Info
     29 0.015733    10.10.50.40           10.10.55.6            TCP      49 > 1192
[ACK] Seq=1 Ack=69 Win=5792 Len=0 TSV=3143898089 TSER=3264254


No.     Time        Source                Destination           Protocol Info
     30 0.016581    10.10.50.40           10.10.55.6            TACACS+  R:
Authorization

Frame 30 (95 bytes on wire, 95 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.55.6 (10.10.55.6)
Transmission Control Protocol, Src Port: 49 (49), Dst Port: 1192 (1192), Seq: 1, Ack:
69, Len: 29
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 2
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 308467491
    Packet length: 17
    Encrypted Reply

No.     Time        Source                Destination           Protocol Info
     31 0.016711    10.10.50.40           10.10.55.6            TCP      49 > 1192
```

```
[FIN, ACK] Seq=30 Ack=69 Win=5792 Len=0 TSV=3143898089 TSER=3264254


No.     Time        Source                Destination           Protocol Info
     32 0.017715    10.10.55.6            10.10.50.40           TCP      1192 > 49
[ACK] Seq=69 Ack=30 Win=8192 Len=0 TSV=3264254 TSER=3143898089


No.     Time        Source                Destination           Protocol Info
     33 0.018113    10.10.55.6            10.10.50.40           TCP      1192 > 49
[FIN, ACK] Seq=69 Ack=30 Win=8192 Len=0 TSV=3264254 TSER=3143898089


No.     Time        Source                Destination           Protocol Info
     34 0.018127    10.10.50.40           10.10.55.6            TCP      49 > 1192
[ACK] Seq=31 Ack=70 Win=5792 Len=0 TSV=3143898089 TSER=3264254


No.     Time        Source                Destination           Protocol Info
     35 0.019636    10.10.55.6            10.10.50.40           TCP      1192 > 49
[FIN, ACK] Seq=69 Ack=31 Win=8192 Len=0 TSV=3264254 TSER=3143898089


No.     Time        Source                Destination           Protocol Info
     36 3.109326    10.10.55.6            10.10.50.40           TCP      1193 > 49
[SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=3264260 TSER=0


No.     Time        Source                Destination           Protocol Info
     37 3.109370    10.10.50.40           10.10.55.6            TCP      49 > 1193
[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=3143898398 TSER=3264260 WS=0


No.     Time        Source                Destination           Protocol Info
     38 3.110602    10.10.55.6            10.10.50.40           TCP      1193 > 49
[ACK] Seq=1 Ack=1 Win=8192 Len=0 TSV=3264260 TSER=3143898398



No.     Time        Source                Destination           Protocol Info
     39 3.112310    10.10.55.6            10.10.50.40           TACACS+  Q:
Authorization

Frame 39 (140 bytes on wire, 140 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.55.6 (10.10.55.6), Dst: 10.10.50.40 (10.10.50.40)
Transmission Control Protocol, Src Port: 1193 (1193), Dst Port: 49 (49), Seq: 1, Ack:
1, Len: 74
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 1
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 845883376
    Packet length: 62
```

```
    Encrypted Request

No.     Time        Source                Destination           Protocol Info
     40 3.112343    10.10.50.40           10.10.55.6            TCP      49 > 1193
[ACK] Seq=1 Ack=75 Win=5792 Len=0 TSV=3143898398 TSER=3264260


No.     Time        Source                Destination           Protocol Info
     41 3.112919    10.10.50.40           10.10.55.6            TACACS+  R:
Authorization

Frame 41 (84 bytes on wire, 84 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.55.6 (10.10.55.6)
Transmission Control Protocol, Src Port: 49 (49), Dst Port: 1193 (1193), Seq: 1, Ack:
75, Len: 18
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 2
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 845883376
    Packet length: 6
    Encrypted Reply

No.     Time        Source                Destination           Protocol Info
     42 3.113047    10.10.50.40           10.10.55.6            TCP      49 > 1193
[FIN, ACK] Seq=19 Ack=75 Win=5792 Len=0 TSV=3143898398 TSER=3264260


No.     Time        Source                Destination           Protocol Info
     43 3.114116    10.10.55.6            10.10.50.40           TCP      1193 > 49
[ACK] Seq=75 Ack=19 Win=8192 Len=0 TSV=3264260 TSER=3143898398


No.     Time        Source                Destination           Protocol Info
     44 3.114493    10.10.55.6            10.10.50.40           TCP      1193 > 49
[FIN, ACK] Seq=75 Ack=19 Win=8192 Len=0 TSV=3264260 TSER=3143898398


No.     Time        Source                Destination           Protocol Info
     45 3.114507    10.10.50.40           10.10.55.6            TCP      49 > 1193
[ACK] Seq=20 Ack=76 Win=5792 Len=0 TSV=3143898398 TSER=3264260


No.     Time        Source                Destination           Protocol Info
     46 3.115140    10.10.55.6            10.10.50.40           TCP      1193 > 49
[FIN, ACK] Seq=75 Ack=20 Win=8192 Len=0 TSV=3264260 TSER=3143898398


No.     Time        Source                Destination           Protocol Info
     47 11.515272   10.10.55.6            10.10.50.40           TCP      1194 > 49
[SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=3264277 TSER=0
```

```
No.     Time        Source                Destination           Protocol Info
     48 11.515316   10.10.50.40           10.10.55.6            TCP      49 > 1194
[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=3143899239 TSER=3264277 WS=0


No.     Time        Source                Destination           Protocol Info
     49 11.516803   10.10.55.6            10.10.50.40           TCP      1194 > 49
[ACK] Seq=1 Ack=1 Win=8192 Len=0 TSV=3264277 TSER=3143899239


No.     Time        Source                Destination           Protocol Info
     50 11.518417   10.10.55.6            10.10.50.40           TACACS+  Q:
Authorization

Frame 50 (152 bytes on wire, 152 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.55.6 (10.10.55.6), Dst: 10.10.50.40 (10.10.50.40)
Transmission Control Protocol, Src Port: 1194 (1194), Dst Port: 49 (49), Seq: 1, Ack:
1, Len: 86
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 1
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 126425174
    Packet length: 74
    Encrypted Request

No.     Time        Source                Destination           Protocol Info
     51 11.518448   10.10.50.40           10.10.55.6            TCP      49 > 1194
[ACK] Seq=1 Ack=87 Win=5792 Len=0 TSV=3143899239 TSER=3264277


No.     Time        Source                Destination           Protocol Info
     52 11.519020   10.10.50.40           10.10.55.6            TACACS+  R:
Authorization

Frame 52 (84 bytes on wire, 84 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.55.6 (10.10.55.6)
Transmission Control Protocol, Src Port: 49 (49), Dst Port: 1194 (1194), Seq: 1, Ack:
87, Len: 18
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 2
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 126425174
    Packet length: 6
    Encrypted Reply
```

```
No.     Time        Source                Destination           Protocol Info
     53 11.519153   10.10.50.40           10.10.55.6            TCP      49 > 1194
[FIN, ACK] Seq=19 Ack=87 Win=5792 Len=0 TSV=3143899239 TSER=3264277


No.     Time        Source                Destination           Protocol Info
     54 11.520184   10.10.55.6            10.10.50.40           TCP      1194 > 49
[ACK] Seq=87 Ack=19 Win=8192 Len=0 TSV=3264277 TSER=3143899239


No.     Time        Source                Destination           Protocol Info
     55 11.520632   10.10.55.6            10.10.50.40           TCP      1194 > 49
[ACK] Seq=87 Ack=20 Win=8192 Len=0 TSV=3264277 TSER=3143899239


No.     Time        Source                Destination           Protocol Info
     56 11.521018   10.10.55.6            10.10.50.40           TCP      1194 > 49
[FIN, ACK] Seq=87 Ack=20 Win=8192 Len=0 TSV=3264277 TSER=3143899239


No.     Time        Source                Destination           Protocol Info
     57 11.521037   10.10.50.40           10.10.55.6            TCP      49 > 1194
[ACK] Seq=20 Ack=88 Win=5792 Len=0 TSV=3143899239 TSER=3264277


No.     Time        Source                Destination           Protocol Info
     58 14.996946   10.10.55.6            10.10.50.40           TCP      1195 > 49
[SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=3264284 TSER=0


No.     Time        Source                Destination           Protocol Info
     59 14.996990   10.10.50.40           10.10.55.6            TCP      49 > 1195
[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=3143899587 TSER=3264284 WS=0


No.     Time        Source                Destination           Protocol Info
     60 14.998215   10.10.55.6            10.10.50.40           TCP      1195 > 49
[ACK] Seq=1 Ack=1 Win=8192 Len=0 TSV=3264284 TSER=3143899587


No.     Time        Source                Destination           Protocol Info
     61 14.999844   10.10.55.6            10.10.50.40           TACACS+  Q:
Authorization

Frame 61 (160 bytes on wire, 160 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.55.6 (10.10.55.6), Dst: 10.10.50.40 (10.10.50.40)
Transmission Control Protocol, Src Port: 1195 (1195), Dst Port: 49 (49), Seq: 1, Ack:
1, Len: 94
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 1
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 3031640525
```

```
    Packet length: 82
    Encrypted Request

No.     Time        Source                Destination           Protocol Info
     62 14.999874   10.10.50.40           10.10.55.6            TCP      49 > 1195
[ACK] Seq=1 Ack=95 Win=5792 Len=0 TSV=3143899587 TSER=3264284


No.     Time        Source                Destination           Protocol Info
     63 15.000384   10.10.50.40           10.10.55.6            TACACS+  R:
Authorization

Frame 63 (84 bytes on wire, 84 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.55.6 (10.10.55.6)
Transmission Control Protocol, Src Port: 49 (49), Dst Port: 1195 (1195), Seq: 1, Ack:
95, Len: 18
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 2
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 3031640525
    Packet length: 6
    Encrypted Reply

No.     Time        Source                Destination           Protocol Info
     64 15.000511   10.10.50.40           10.10.55.6            TCP      49 > 1195
[FIN, ACK] Seq=19 Ack=95 Win=5792 Len=0 TSV=3143899587 TSER=3264284


No.     Time        Source                Destination           Protocol Info
     65 15.001551   10.10.55.6            10.10.50.40           TCP      1195 > 49
[ACK] Seq=95 Ack=19 Win=8192 Len=0 TSV=3264284 TSER=3143899587


No.     Time        Source                Destination           Protocol Info
     66 15.001926   10.10.55.6            10.10.50.40           TCP      1195 > 49
[FIN, ACK] Seq=95 Ack=19 Win=8192 Len=0 TSV=3264284 TSER=3143899587


No.     Time        Source                Destination           Protocol Info
     67 15.001941   10.10.50.40           10.10.55.6            TCP      49 > 1195
[ACK] Seq=20 Ack=96 Win=5792 Len=0 TSV=3143899587 TSER=3264284


No.     Time        Source                Destination           Protocol Info
     68 15.003014   10.10.55.6            10.10.50.40           TCP      1196 > 49
[SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV=3264284 TSER=0


No.     Time        Source                Destination           Protocol Info
     69 15.003038   10.10.50.40           10.10.55.6            TCP      49 > 1196
[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=3143899587 TSER=3264284 WS=0
```

```
No.     Time        Source                Destination           Protocol Info
     70 15.003476   10.10.55.6            10.10.50.40           TCP      1195 > 49
[FIN, ACK] Seq=95 Ack=20 Win=8192 Len=0 TSV=3264284 TSER=3143899587


No.     Time        Source                Destination           Protocol Info
     71 15.004420   10.10.55.6            10.10.50.40           TCP      1196 > 49
[ACK] Seq=1 Ack=1 Win=8192 Len=0 TSV=3264284 TSER=3143899587


No.     Time        Source                Destination           Protocol Info
     72 15.006053   10.10.55.6            10.10.50.40           TACACS+  Q: Accounting

Frame 72 (171 bytes on wire, 171 bytes captured)
Ethernet II, Src: NortelNe_0f:8e:04 (00:04:38:0f:8e:04), Dst: DellComp_38:57:5b
(00:06:5b:38:57:5b)
Internet Protocol, Src: 10.10.55.6 (10.10.55.6), Dst: 10.10.50.40 (10.10.50.40)
Transmission Control Protocol, Src Port: 1196 (1196), Dst Port: 49 (49), Seq: 1, Ack:
1, Len: 105
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Accounting (3)
    Sequence number: 1
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 1349224772
    Packet length: 93
    Encrypted Request

No.     Time        Source                Destination           Protocol Info
     73 15.006085   10.10.50.40           10.10.55.6            TCP      49 > 1196
[ACK] Seq=1 Ack=106 Win=5792 Len=0 TSV=3143899588 TSER=3264284


No.     Time        Source                Destination           Protocol Info
     74 15.006538   10.10.50.40           10.10.55.6            TACACS+  R: Accounting

Frame 74 (83 bytes on wire, 83 bytes captured)
Ethernet II, Src: DellComp_38:57:5b (00:06:5b:38:57:5b), Dst: NortelNe_0f:8e:04
(00:04:38:0f:8e:04)
Internet Protocol, Src: 10.10.50.40 (10.10.50.40), Dst: 10.10.55.6 (10.10.55.6)
Transmission Control Protocol, Src Port: 49 (49), Dst Port: 1196 (1196), Seq: 1, Ack:
106, Len: 17
TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Accounting (3)
    Sequence number: 2
    Flags: 0x00 (Encrypted payload, Multiple Connections)
        .... ...0 = Unencrypted: Not set
        .... .0.. = Single Connection: Not set
    Session ID: 1349224772
    Packet length: 5
    Encrypted Reply

No.     Time        Source                Destination           Protocol Info
```

```
     75 15.006618   10.10.50.40           10.10.55.6            TCP      49 > 1196
[FIN, ACK] Seq=18 Ack=106 Win=5792 Len=0 TSV=3143899588 TSER=3264284


No.     Time        Source                Destination           Protocol Info
     76 15.007715   10.10.55.6            10.10.50.40           TCP      1196 > 49
[ACK] Seq=106 Ack=18 Win=8192 Len=0 TSV=3264284 TSER=3143899588


No.     Time        Source                Destination           Protocol Info
     77 15.008090   10.10.55.6            10.10.50.40           TCP      1196 > 49
[FIN, ACK] Seq=106 Ack=18 Win=8192 Len=0 TSV=3264284 TSER=3143899588


No.     Time        Source                Destination           Protocol Info
     78 15.008106   10.10.50.40           10.10.55.6            TCP      49 > 1196
[ACK] Seq=19 Ack=107 Win=5792 Len=0 TSV=3143899588 TSER=3264284


No.     Time        Source                Destination           Protocol Info
     79 15.008897   10.10.55.6            10.10.50.40           TCP      1196 > 49
[FIN, ACK] Seq=106 Ack=19 Win=8192 Len=0 TSV=3264284 TSER=3143899588
```

4. Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

4.1 Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

4.2 Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

4.3 Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

4.4 Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.