Ethernet Routing Switch
2500, 4500, 5000
Engineering

> Management Access Security for ERS 2500, ERS 4500, and ERS 5000 Technical Configuration Guide

Avaya Data Solutions
Document Date: May 31, 2010
Document Number: NN48500-594
Document Version: 1.0

Abstract

This document provides examples on configuring various items related to accessing the ERS 2500, 4500, and 5000 securely for management purposes. This document covers accessing the switch using telnet, HTTP, SSL, SSH, and SNMP.

Revision Control

No	Date	Version	Revised by	Remarks
1	05/19/2010	1.0	PRMGT	Modifications to Software Baseline section

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

On an ERS 2500, ERS 4500, or ERS 5000 series switch, there is no access security enabled by default. This allows a user to access the switch either via the local serial port, HTTP (WEB), or via Telnet without any user name or password protection. Password protection for Telnet, WEB, or SSH (user name & password) can be added using local user names and passwords or authenticating against an external RADIUS or TACACS+ server. In regards to SSH, password authentication can be enable or disabled in addition to using SSH with public key authentication.

By default, SNMPv1/SNMPv2c is enabled using read and write community strings of *public* and *private*. This can be changed if you wish to use community strings for authentication. Or for added security, you may wish to disable SNMPv1 and SNMPv2c and only use SNMPv3.

For added security, a source IP manager control list can be added. This list can contain anywhere from 1 to 50 source IPv4 and/or IPv6 addresses, up to 50 each, that are allowed access to the switch. This control list in turn can be applied to any access method including SNMP, SSH, Telnet, and/or WEB.

If SSH is required, the secure version of the software must be installed on the switch. For each switch model, there is a secure image and standard software image available. All switches ship with the standard agent image installed.

2. Management IP Address

Before adding any type of remote access, we need to add an IP address to the switch and/or stack. An IP address can be added in one of two ways. If the switch is strictly used as a Layer 2 switch, then an IP address can be added via the Layer 2 method using the CLI command *ip address <switch|stack> <IP address> netmask <mask> default-gateway <default GW>*. Otherwise, if the switch is configured for Layer 3, it is recommended to add the switch address via the VLAN interface level.

- Layer 2 method assuming the Management VLAN is 200 using a standalone switch
  - ERS-Stackable(config)# ***vlan create 200 name mgmt type port 1***
  - ERS-Stackable(config)# ***vlan mgmt 200***
  - ERS-Stackable(config)# ***ip address switch 10.1.1.10 netmask 255.255.255.0 default-gateway***

By default all stackable switches will attempt to obtain an IP management address if one has not been configured. The ERS 4500 and ERS 5000 support both bootp and DHCP, while the ERS 2500 supports bootp.

- Layer 3 method assuming the Management VLAN is 200
  - ERS-Stackable(config)# ***vlan create 200 name mgmt type port 1***
  - ERS-Stackable(config)# ***vlan mgmt 200***
  - ERS-Stackable(config)# ***interface vlan 200***
  - ERS-Stackable(config-if)# ***ip address 10.1.1.10 255.255.255.0***
  - ERS-Stackable(config-if)# ***exit***
  - ERS-Stackable(config)# ***ip routing***
  - ERS-Stackable(config)# ***ip route <destination ip> <destination mask> <next hop ip> <1-65535>***

Please note that the management VLAN must be created and assigned as a management VLAN prior to adding an IP address either via the L2 or L3 method. Also, a brouter port cannot be used as the management IP address.

The Ethernet Routing Switch provides 2 additional means to be able to configure a management IP Address.

If you connect to the serial console port of a switch with a factory default configuration, then the switch will automatically start the quickinstall command, which prompts you for IP address configuration information.

Alternatively you can pre-stage the management IP address plus software and configuration information if required using the staging function by including a file IP.cfg in the root directory of a USB drive when you power on the switch.

3. Local password protection

3.1 CLI/WEB Password Protection

By default, on the ERS 2500, ERS 4500, or ERS 5000 series switch, serial port and telnet/web access is allowed without any password protection.

The following command displays the various password options available.

- ERS-Stackable(config)# ***cli password ?***

```
read-only   Modify read-only password
read-write  Modify read-write password
serial      Enable/disable serial port password.
stack       Modify stack passwords.
switch      Modify switch (stand-alone) passwords.
telnet      Enable/disable telnet and web password.
```

The following command displays the various telnet access options. The choices are local user name & password protection, *none, radius, or tacacs*.

- ERS-Stackable(config)# ***cli password <switch|stack> telnet ?***

```
local   Use local password.
none    Disable password.
radius  Use RADIUS password authentication.
tacacs  Use TACACS+ AAA services
```

The following command displays the various local serial port access options. The choices are local user name & password protection, *none, radius, or tacacs*

- ERS-Stackable(config)# ***cli password serial ?***

```
local   Use local password.
none    Disable password.
radius  Use RADIUS password authentication.
tacacs  Use TACACS+ AAA services
```

To add a user name, enter the following command when password security is disabled – please see next section regarding Password Security.

- ERS-Stackable(config)# ***username <user name> <password>***

Enabling telnet password protection, either local user/password or against a RADIUS server, also applies to WEB access.

For the standard image, the default password for the read-only user is *user* and *secure* for the read-write user. For the secure software image, the default password for the read-only user is *userpasswd* and *securepswd* for the read-write user. The default read-only user name is *RO* while the default read-write user name is *RW*. Please note, these user names and passwords are only applicable once you enable local password security.

3.2 Password Security

Password security, if enabled, enhances password security for the switch or stack read-only password and read-write passwords. By default, password security is disabled for the standard software image and enabled for the secure software image. If password security is disabled, there is no minimum restriction on number of characters required or are there any other restrictions. If password security is enabled, then there are restrictions put into place where the password must be between 10 and 15 characters containing at minimum 2 upper, 2 lowercase characters, 2 numbers, and 2 special characters. Password security is enabled from the CLI interface only.

To enable password security, enter the following command:

- ERS-Stackable(config)# ***password security***

To disable password security, enter the following command

- ERS-Stackable(config)# ***no password security***

When Password Security is disabled, upon enabling Password Security, you will be prompted with the following text. Please note, all previous passwords will be cleared.

- ERS-Stackable(config)# ***password security***

```
% RO Switch password should have between 10 and 15 characters.
% Password should contain a minimum of 2 upper, 2 lowercase letters,
% 2 numbers and 2 special characters like !@#$%^&*().
% Please change the password
Enter RO Switch password: **************
% RW Switch password should have between 10 and 15 characters.
% Password should contain a minimum of 2 upper, 2 lowercase letters,
% 2 numbers and 2 special characters like !@#$%^&*().
% Please change the password
Enter RW Switch password: **************
```

Feature/Requirement	Description
Password composition	The password must contain a minimum of 2 of each of the following types of characters: lowercase letters, capital letters, numbers, and special symbols such as !@#$%^&*().
Password length	The password must consist of between 10 and 15 characters.
Log on attempts	The switch allows only a specified maximum number of consecutive failed log on attempts. The number of allowed retries is configurable. The default is three.
Password history	The switch can be configured to store up to 10 previously used passwords. The passwords stored in the password history until they pass out of the history table.
Password update verification	Any password change must be verified by typing the new

	password twice.
Password aging time	Passwords expire after a specified period. The aging time is configurable. The default is 180 days.
Password display masking	Any time a password is displayed or entered in NNCLI, each character of the password is displayed as an asterisk (*).
Password security factory default	By default, password security is enabled on the SSH software image and disabled on the non-SSH software image.

3.3 Telnet Password Protection using Local Authentication

To enable local telnet authentication on a standalone switch, enter the following command:

- ERS-Stackable(config)# ***cli password telnet local***

or

- ERS-Stackable(config)# ***cli password switch telnet local***

These settings can be stored for both switch standalone operation and stack mode operation. It is recommended to make the same setting for both switch standalone and stack operation otherwise if a unit changes operational mode (e.g. unit removed from a stack, or a stack of 2 units and 1 unit fails) then a different setting might become active.

To enable local telnet authentication on a switch stack, enter the following command:

- ERS-Stackable(config)# ***cli password stack telnet local***

To verify the configuration, enter the following command:

- ERS-Stackable(config)# ***show cli password type***

```
Console Switch Password Type: None
Console Stack Password Type: None
Telnet/WEB Switch Password Type: Local Password
Telnet/WEB Stack Password Type: None
```

You have the choice of using the default user names and passwords to access the switch, using the default passwords and changing the user names, and/or changing the default user names and passwords. The default user names are *RO* and *RW* for the read-only and read-write users respectively. For the standard image the default password for *RO* is *user* and *secure* for *RW*. For the secure software image, the default password for *RO* is *userpasswd* and *securepasswd* for *RW*.

To change the default switch or stack CLI passwords, enter the following commands:

- ERS-Stackable(config)# ***cli password <switch|stack> read-only <RO password>***
- ERS-Stackable(config)# ***cli password <switch|stack> read-write <RW password>***

To view the configuration, enter the following command:

- ERS-Stackable# ***show cli password***

```
          Switch
Access Login     Username / Password
------ --------- -----------------------------------
RW     RW        RW / ***************
RO     RO        RO / ***************

           Stack
Access Login     Username / Password
------ --------- -----------------------------------
RW     RW        RW / ***************
RO     RO        RO / ***************
```

The default user names can be changed using the following CLI command:

- ERS-Stackable(config)# ***username <user_name> <user_password> <switch|stack> <ro|rw>***.

3.4 Telnet Access Configuration Examples using Local Users with Password Security disabled

3.4.1 Local Password Configuration - Password Security Disabled

For this configuration example, we will configure the following assuming we are using an ERS5000 stack

- Change the default read-write user name from RW to *user1*
- Change the default read-only user name from RO to *user2*
- Disable Password Security
    - This applies to secure version as Password Security is enabled by default on SSH switch server
- For *user1*, use the password *rwaccess*
- For *user2*, use the password *roaccess*

ERS-STACKABLE: Step 1 – Enable Password Security
ERS-Stackable(config)# ***no password security***
ERS-STACKABLE: Step 2 – Add new user names and passwords
ERS-Stackable(config)# ***username user1 rwaccess stack rw*** ERS-Stackable(config)# ***username user1 rwaccess switch rw*** ERS-Stackable(config)# ***username user2 roaccess stack ro*** ERS-Stackable(config)# ***username user2 roaccess switch ro***
ERS-STACKABLE: Step 3 – Enable telnet local authentication
ERS-Stackable(config)# ***cli password stack telnet local*** ERS-Stackable(config)# ***cli password switch telnet local***

3.4.2 Verify Operations

Step 1 – Verify user names

```
ERS-Stackable(config)# show cli password
```

Result:

```
          Switch
Access Login     Username / Password
------ --------- ----------------------------------
RW     RW        user1 / ***************
RO     RO        user2 / ***************

           Stack
Access Login     Username / Password
------ --------- ----------------------------------
RW     RW        user1 / ***************
RO     RO        user2 / ***************
```

Step 2 – Verify that the cli password type is set for local

```
ERS-Stackable(config)# show cli password type
```

Result:

```
Console Switch Password Type: None
Console Stack Password Type: None
Telnet/WEB Switch Password Type: Local Password
Telnet/WEB Stack Password Type: Local Password
```

If you enable password security at this point, it will prompt you with the following:

```
ERS-Stackable(config)# password security

% RO Switch password should have between 10 and 15 characters.
% Password should contain a minimum of 2 upper, 2 lowercase letters,
% 2 numbers and 2 special characters like !@#$%^&*().
% Please change the password
Enter RO Switch password: **********
Confirm RO Switch password: **********
Enter RO Switch password: **********
Confirm RO Switch password: **********
```

3.4.3 Local Password Configuration - Password Security Enabled

For this configuration example, we will configure the following

- Change the default read-write user name from RW to *admin*
- Change the default read-only user name from RO to *tech*
- Assuming Password Security is enabled by default
    - This applies to secure version as Password Security is enabled by default on SSH switch server
    - With Password Security enabled, the password should contain a minimum of 2 upper, 2 lowercase letters, 2 numbers and 2 special characters like !@#$%^&*().
- For *admin*, use the password *AdminUser@#1234*
- For *tech*, use the password *TechUser@#1234*

ERS-STACKABLE: Step 1 – Add new user names and passwords

```
ERS-Stackable(config)# username admin stack rw

Enter password: ********* (AdminUser@#1234)
Confirm password: *********

ERS-Stackable(config)# username tech stack ro

Enter password: ********* (TechUser@#1234)
Confirm password: *********
```

ERS-STACKABLE: Step 2 – Enable telnet local authentication

```
ERS-Stackable(config)# cli password stack telnet local

ERS-Stackable(config)# cli password switch telnet local
```

4. IP Manager

The IP Manager feature allows you to limit access to the management features on the switch by defining the IP addresses that are allowed access to the switch. You can define up to 50 IPv4 and 50 IPv6 addresses with masks that are allowed to access the switch. If IP Manager is enabled, no other IP addresses are allowed. Access to Telnet, SNMP, SSH, and Web-based management can be configured.

- ERS-Stackable(config)# ***ipmgr ?***

```
snmp       Enable IP Manager control over SNMP traffic.
source-ip  Set source IP address from which connections are allowed
ssh        Enable IP Manager control over SSH sessions.
telnet     Enable IP Manager control over TELNET sessions.
web        Enable IP Manager control over WEB connections.
```

- ERS-Stackable(config)# ***ipmgr source-ip ?***

```
<1-50>    Select which address/mask pair
<51-100>  Select which ipv6 address/prefix
```

4.1 IP Manager Configuration Example

Assuming we wish to restrict Telnet/WEB access to users with IPv4 addresses from unicast IP address 192.168.20.100/32 and subnet 192.168.30.0/24, enter the following commands.

ERS-STACKABLE: Step 1 – Add the IP address to the IP manager list and enable telnet

```
ERS-Stackable(config)# ipmgr telnet
ERS-Stackable(config)# ipmgr source-ip 1 192.168.20.100 mask 255.255.255.255
ERS-Stackable(config)# ipmgr source-ip 2 192.168.30.0 mask 255.255.255.0
```

Ethernet Routing Switch Verify Operations

Step 1 – Verify IP Manager configuration

```
ERS-Stackable# show ipmgr
```

Result:

```
        TELNET Access: Enabled
        SNMP Access:   Disabled
        WEB Access:    Disabled
        SSH Access:    Disabled
        TELNET IP List Access Control: Enabled
        SNMP IP List Access Control:   Enabled
        WEB IP List Access Control:    Enabled
        SSH IP List Access Control:    Enabled
        Allowed Source IP Address  Allowed Source Mask
        -------------------------  -------------------
        1  192.168.20.100             255.255.255.255
        2  192.168.30.0               255.255.255.0
        3  255.255.255.255            255.255.255.255
```

Step 2 – You can also view the user log using the following command

```
ERS-Stackable# show audit log telnet
```

Result:

```
      dx Pri(/Timestamp/Host) Stat Source(Unit)    Uptime        Command
      ------------------------------------------------------------------
      |
      74   <30>42:16:44:41 ERS-Stackable :S telnet(192.168.20.100): 42 days, 16:44:41:
      configure terminal
      75   <30>42:16:44:50 ERS-Stackable :S telnet(192.168.20.100): 42 days, 16:44:50:
      vlan create 89 type port
      77   <30>42:16:45:33 ERS-Stackable :S telnet(192.168.20.100): 42 days, 16:45:33:
      exit
      78   <30>42:16:45:38 ERS-Stackable :S telnet(192.168.20.100): 42 days, 16:45:38:
      exit
```

5. Telnet Password Protection using RADIUS Authentication

Users who access the Avaya switch or stack through Telnet, serial, or SSHv2 (password authentication), can be authenticated against a RADIUS server. The ERS 5000, ERS 4500, and ERS 2500 each support two different user access levels which are read-only and read-write with support for up to two RADIUS servers. RADIUS attribute type 6, Service-Type, is used to determine the access level. The following displays the complete list of RADIUS attribute values for the RADIUS Service-Type attribute where value 6 (Administrative) is used for read-write access and value 7 (NAS Prompt) is used for read-only access

```
Sub-registry: Values for RADIUS Attribute 6, Service-Type
Reference: [RFC2865][RFC3575]
Registration Procedures: IETF Consensus

Registry:
Value  Description                     Reference
-----  ------------------------------  ---------
1      Login
2      Framed
3      Callback Login
4      Callback Framed
5      Outbound
6      Administrative
7      NAS Prompt
8      Authenticate Only
9      Callback NAS Prompt
10     Call Check
11     Callback Administrative
12     Voice                           [Chiba]
13     Fax                             [Chiba]
14     Modem Relay                     [Chiba]
15     IAPP-Register                   [IEEE 802.11f][Kerry]
16     IAPP-AP-Check                   [IEEE 802.11f][Kerry]
17     Authorize Only                  [RFC3576]
18     Framed-Management               [RFC5607]
```

To add a RADIUS server, enter the following command to view the various configurable options:

- `ERS-Stackable(config)# radius-server ?`

```
  host            RADIUS primary host
  key             RADIUS shared secret
  password        RADIUS password fallback
  port            RADIUS UDP port
  secondary-host  RADIUS secondary host
  timeout         RADIUS time-out period
```

To view the various RADIUS settings, enter the following command:

- `ERS-Stackable(config)# radius ?`

```
Configure RADIUS settings
  accounting          Configure RADIUS accounting settings
  dynamic-server      RADIUS Dynamic Authorization Client settings
  reachability        Configure RADIUS server reachability settings
  use-management-ip   Enable Radius use-management-ip flag.
```

Up to two RADIUS servers can be configured. Staring in release 5.4 for the ERS4500 and 4.3 for the ERS2500, the *radius reachability* setting allows either ICMP packets or dummy RADIUS requests to determine if the primary RADIUS server is reachable. By default, ICMP is enabled. If you wish to use dummy RADIUS requests, the switch will generate a regular RADIUS requests periodically with the username *avaya* and a blank password. Hence, it is recommended that you setup an account with the user name *avaya* and a blank password on your RADIUS server to avoid invalid RADIUS user login messages. The following command is used to configure the reachability setting:

- `ERS-Stackable(config)# radius reachability ?`

```
  use-icmp    Enable RADIUS server reachability using ICMP
  use-radius  Enable RADIUS server reachability using RADIUS requests
```

For the ERS 4500, starting in release 5.4, ERS 5000 in release 6.2, or for the ERS 2500, starting in release 4.3, if using the *use-radius* setting when configuring the *radius reachability* parameter, the switch will periodically send RADIUS requests using a user name of *avaya* with a blank password. Hence, your RADIUS server must support blank passwords. This is not the case with Avaya's Ignition Server which does not allow blank passwords. If using Ignition Server, use the default setting of *use-icmp*.

Please note the radius reachability parameter is not available in the latest release (6.1.2) of the ERS5000 series and will be added in release 6.2. By default, the switch will periodically send RADIUS requests using a user name of *nortel* with a blank password to determine RADIUS server reachability. Again, Avaya's Ignition Server does not allow blank passwords, thus, RADIUS requests from an ERS5000 will be rejected.

5.1 Password Fallback

The RADIUS password fallback feature allows the user to log on to the switch or stack by using the local password if the RADIUS server is unavailable or unreachable for authentication. RADIUS password fallback is disabled by default.

To enable RADIUS password fallback, please enter the following command

- `ERS-Stackable(config)# radius-server password fallback`

5.2 Use Management IP

By default, if Layer 3 is enabled, the switch will use the outgoing interface IP address when attempting access to the RADIUS server. If you have multiple outgoing interfaces that can reach the RADIUS server, normally you will have to configure your RADIUS server with each of interface IP addresses used on the switch. However, the *radius use-management-ip* command can be issued to tell the switch to use the switch management IP address for all RADIUS requests independent of the out-going interface.

To enable RADIUS Management IP, please enter the following command

- `ERS-Stackable(config)#` ***`radius use-management-ip`***

5.3 RADIUS Password Configuration Example

5.3.1 Ethernet Routing Switch Configuration

Up to two RADIUS servers are supported on the ERS 5000, ERS 4500, or ERS 2500 series switches. For this configuration example we will simply configure one RADIUS server.

ERS-STACKABLE: Step 1 – Add RADIUS server, enable RADIUS, and enable RADIUS accounting
ERS-Stackable(config)# ***radius-server host 172.168.100.50 key avaya***
ERS-Stackable(config)# ***radius accounting enable***
ERS-Stackable(config)# ***cli password telnet radius***
If the switch is used in a stack, enter the following:
ERS-Stackable(config)# ***cli password stack telnet radius***
ERS-STACKABLE: Step 2 – Optional, enabling password fallback
ERS-Stackable(config)# ***radius-server password fallback***
ERS-STACKABLE: Step 3 – Optional, use management IP
ERS-Stackable(config)# ***radius use-management-ip***

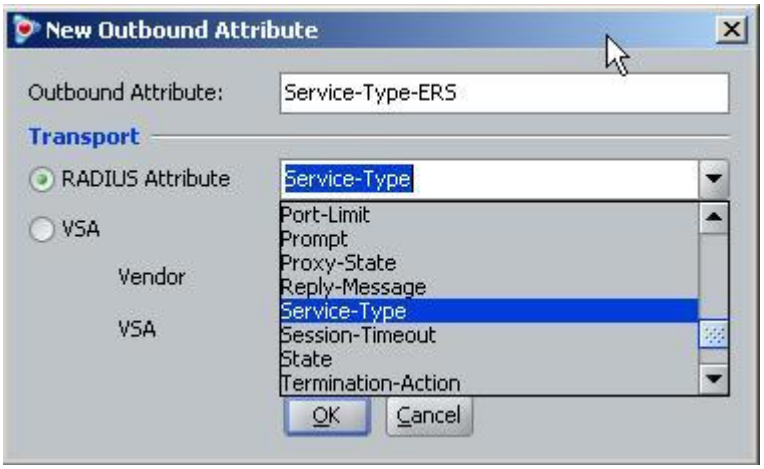
5.3.2 IDE RADIUS Configuration

Assuming we are using Identity Engines Ignition Server as the RADIUS server, please follow the configuration steps below. The following chart displays the outbound attribute values required by the ERS 5000, ERS 4500, or ERS 2500 for each access level using RADIUS attribute type 6 (Service-Type).

Registry Value	Description	ERS Access Level
6	Administrative	Read-Write-All-Access
7	NAS Prompt	Read-Only-Access

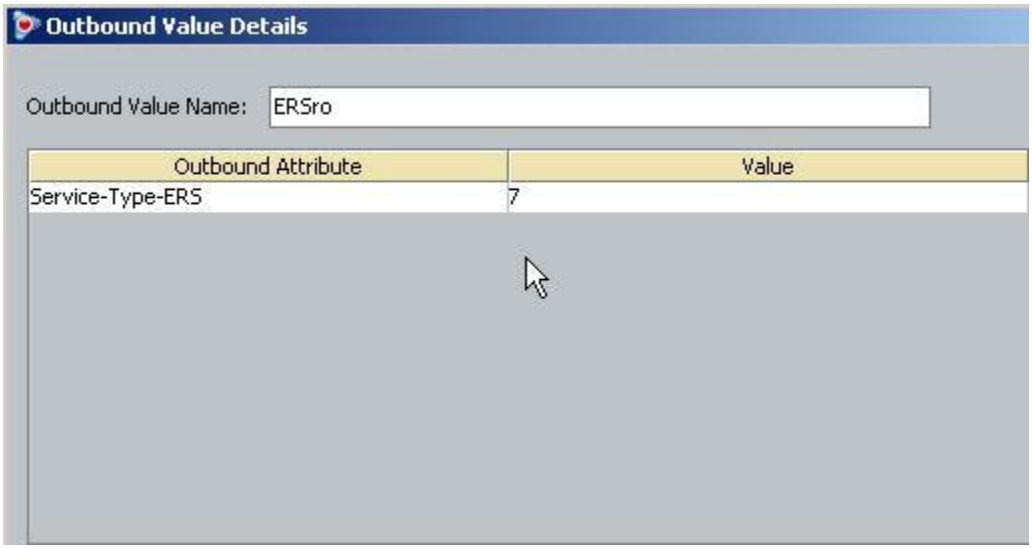
IDE Step 1 – Go to *Site Configuration -> Provisioning -> Outbound Attributes -> New*

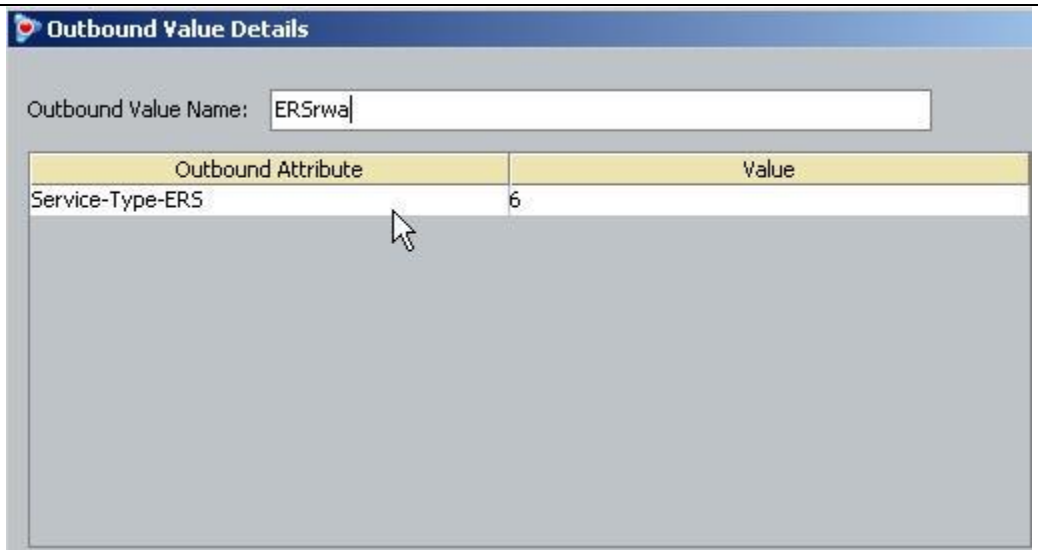
- Via the *Outbound Attribute* window, type in a name for the attribute to be used for access priority (i.e. Service-type-ERS as used in this example), click the *RADIUS Attribute* radio button and select *Service-Type*. Click on *OK* when done.



IDE Step 2 – Go to *Site Configuration -> Provisioning -> Outbound Values -> New*

- Using the Outbound Attribute created in Step 1, we will first add a value of 7 (NAS Prompt) for read-only-access. Start by entering a name via the *Outbound Value Name:* window (i.e. ERSro as used in this example) and click on *New.* Select the Outbound Attributes name created in Step 1 (i.e. Service-type-ERS as used in this example) via the *Choose Global Outbound Attribute:* pull down menu. In the *Value Unsigned – 32 bit* window, enter 7 (i.e. value of 7 signifies NAS Prompt for read-only-access). Click on *OK* twice when done.
- Go to *Site Configuration -> Provisioning -> Outbound Values -> New* again to create the outbound attribute for read-write-access. Using the Outbound Attribute created in Step 1, we will add a value of 6 for read-write-access. Start by entering a name via the *Outbound Value Name:* window (i.e. ERSrwa as used in this example) and click on *New.* Select the Outbound Attributes name created in Step 1 (i.e. Service-type-ERS as used in this example) via the *Choose Global Outbound Attribute:* pull down menu. In the *Value Unsigned – 32 bit* window, enter 6 (i.e. value of 6 signifies Administrative for read-write-access). Click on *OK* twice when done.



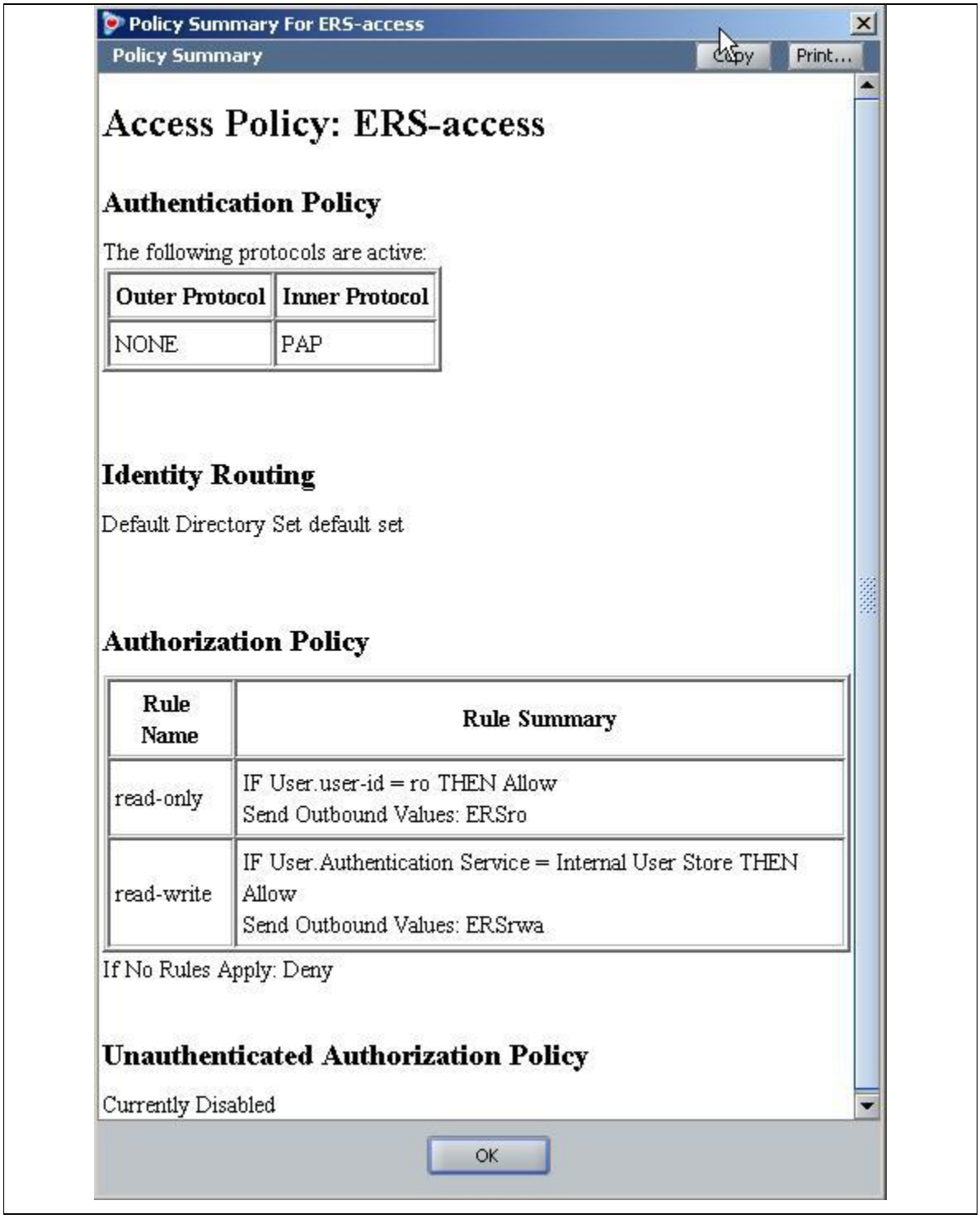


IDE Step 3 – Add Users by going to *Site Configuration -> Directories -> Internal Store -> Internal Users* and click on *New*

- Enter the user name for read-only-access via *User Name:* and enter the password for this user via *Password* and *Confirm Password*. Click on *OK* when done. If you wish, you can also change the expiry date via *Password Expires* if you do not wish to use the default setting of one year
- Repeat again by clicking on New to add the read-write-access user. Enter the user name for read-write-access via *User Name:* and enter the password for this user via *Password* and *Confirm Password*. Click on *OK* when done. If you wish, you can also change the expiry date via *Password Expires* if you do not wish to use the default setting of one year

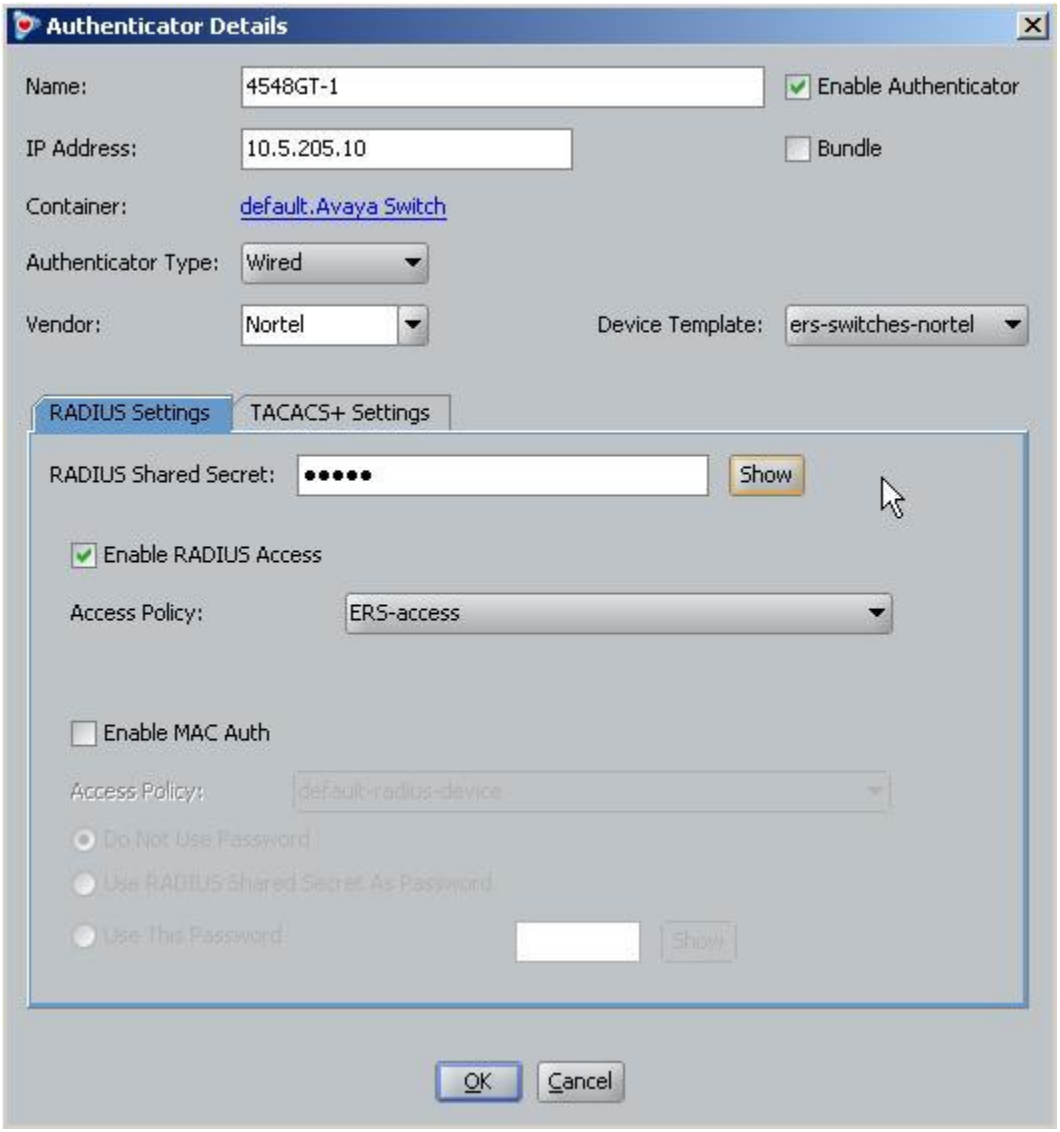
IDE Step 4 – Go to *Site Configuration -> Access Policies -> RADIUS*

- Right-click R*ADIUS* and select *New Access Policy*. Enter a policy name, i.e. ERS-access as used in this example and click on *OK* when done
- Click on the policy we just created, i.e. ERS-access, and click on *Edit* via the *Authentication Policy* tab. Under *Edit Authentication Policy* window, select *NONE -> PAP.* Click on OK when done.
- Go to the *Identity Routing tab* and click on *Edit*. Check off the *Enable Default Directory Set* and click on *OK* when done.
- Go to the *Authorization Policy* tab and click on *Edit.*
    - Once the *Edit Authorization Policy* window pops up, click on *Add* twice simply named *read-only* and *read-write*.
    - For the rule named *read-only*, click on *New* to add a new constraint. From *Attribute Category*, select *User* and scroll down and select *user-id*. Select *Equal To* with *Format* of *None* and enter the read-only-access user id you used in Step 3. Click on *OK* when done. Via *Action*, select *Allow*. From the *All Outbound Values* window, select the output attribute we created above named *ERSro* and click on the less-than arrow key to move the attribute to the *Provision With* window.
    - For the rule named *read-write,* click on *New* to add a new constraint. From *Attribute Category*, select *User* and scroll down and select *user-id*. Select *Equal To* with *Format* of *None* and enter the read-write-access user id you used in Step 3. Click on *OK* when done. Via *Action*, select *Allow*. From the *All Outbound Values* window, select the output attribute we created above named *ERSrwa* and click on the less-than arrow key to move the attribute to the *Provision With* window.
    - When completed, you can view the complete policy by clicking on the *Access Policy Summary* button


Policy Summary For ERS-access
Policy Summary
Copy
Print...
Access Policy: ERS-access
Authentication Policy
The following protocols are active:
Outer Protocol
Inner Protocol
NONE
PAP
Identity Routing
Default Directory Set default set
Authorization Policy
Rule Name
Rule Summary
read-only
IF User.user-id = ro THEN Allow
Send Outbound Values: ERSro
read-write
IF User.Authentication Service = Internal User Store THEN Allow
Send Outbound Values: ERSrwa
If No Rules Apply: Deny
Unauthenticated Authorization Policy
Currently Disabled
OK

IDE Step 5 – Go to *Site Configuration -> Authenticators -> default*

- For example, we will create new container named *Nortel Switch* by right clicking *default* and selecting *Add Container*.
- Go to *Site Configuration -> Authenticators -> default -> Nortel Switch* and click on *New.*
- Enter the settings as shown below making sure you select the policy we created above named *ERS-access* via *Access Policy*. Leave *Enable Authenticator* and *Enable RADIUS Access* checked. Click on *OK* when done.



6. TACACS+

The ERS 5000, ERS 4500, and ERS 2500 all support a TACACS+ client. TACACS+ provides management of users who access the switch through Telnet, serial, and SSHv2 (password authentication) connections using Transmission Control Protocol (TCP). TACACS+ supports users only on the CLI interface. Access to SNMP, and Web management are disabled when TACACS+ is enabled, but, can be re-enabled again once TACACS+ has been enabled.

Unlike RADIUS, which combines authentication and authorization in a user profile, TACACS+ separates both of these functions. The transition is completely transparent to the user. Upon successful user authentication, the TACACS+ server will provide an access level from 1 to 15 to the user depending on how you have setup your TACAS+ sever for each user-id. Within each access level, you can limit the switch commands available to the user. Upon entering a command by an authenticated user, the command is authorized by the TACACS+ server against the command list in the user profile. If the command is not in the user profile, the TACACS+ server will deny the authorization request and in turn, the switch will deny the user command.

Please note, 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. Also, TACACS+ is only for administrative users and cannot be used for 802.1x (EAP) users; RADIUS must be used for 802.1x.

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.

To enable TACACS+, ether the following command to view the various configurable options:

- `ERS-Stackable(config)# tacacs ?`

```
Parameters:
  accounting      TACACS+ accounting tracks what the user does
  authorization   TACACS+ authorization determines what the user is allowed to
                  do
  server          TACACS+ server's primary/secondary host, shared secret key and
                  TCP port
Sub-Commands/Groups:
  switch  Switch between TACACS+ privilege levels
```

Users can also change their privilege levels when in configuration mode by issuing the following command:

- `ERS-Stackable(config)# tacacs switch level <1-15>`

To switch back to the original privilege level, the user need to type in the following command:

- `ERS-Stackable(config)# tacacs switch back`

If you do change access levels, the switch will send out an authentication request using a user-id of *dummy*. However, for command authorization, a user-id of *$enab<x>$* will be used where x is in reference to the privilege level.

6.1 TACACS+ Configuration Example

6.1.1 Ethernet Routing Switch Configuration

ERS-STACKABLE: Step 1 – Add TACACS+ server, enable TACACS+, and enable TACACS+ accounting

```
ERS-Stackable(config)# tacacs server host 172.168.100.50 key
Enter key: *****
Confirm key: *****
ERS-Stackable(config)# tacacs authorization enable
ERS-Stackable(config)# tacacs accounting enable
ERS-Stackable(config)# tacacs authorization level all
```

ERS-STACKABLE: Step 2 – Enable CLI password using TACACS+

```
ERS-Stackable(config)# cli password switch telnet tacacs
% Warning: SNMP/WEB/Console will be disabled
ERS-Stackable level-15># cli password serial tacacs
% Warning: SNMP/WEB will be disabled
```

Please note, SNMP and WEB access which can be re-enabled again after initially enabled TACACS+.

6.1.1.1 Ethernet Routing Switch Verify Operations

Step 1 – Verify user names

```
ERS-Stackable(config)# show tacacs
```

Result:

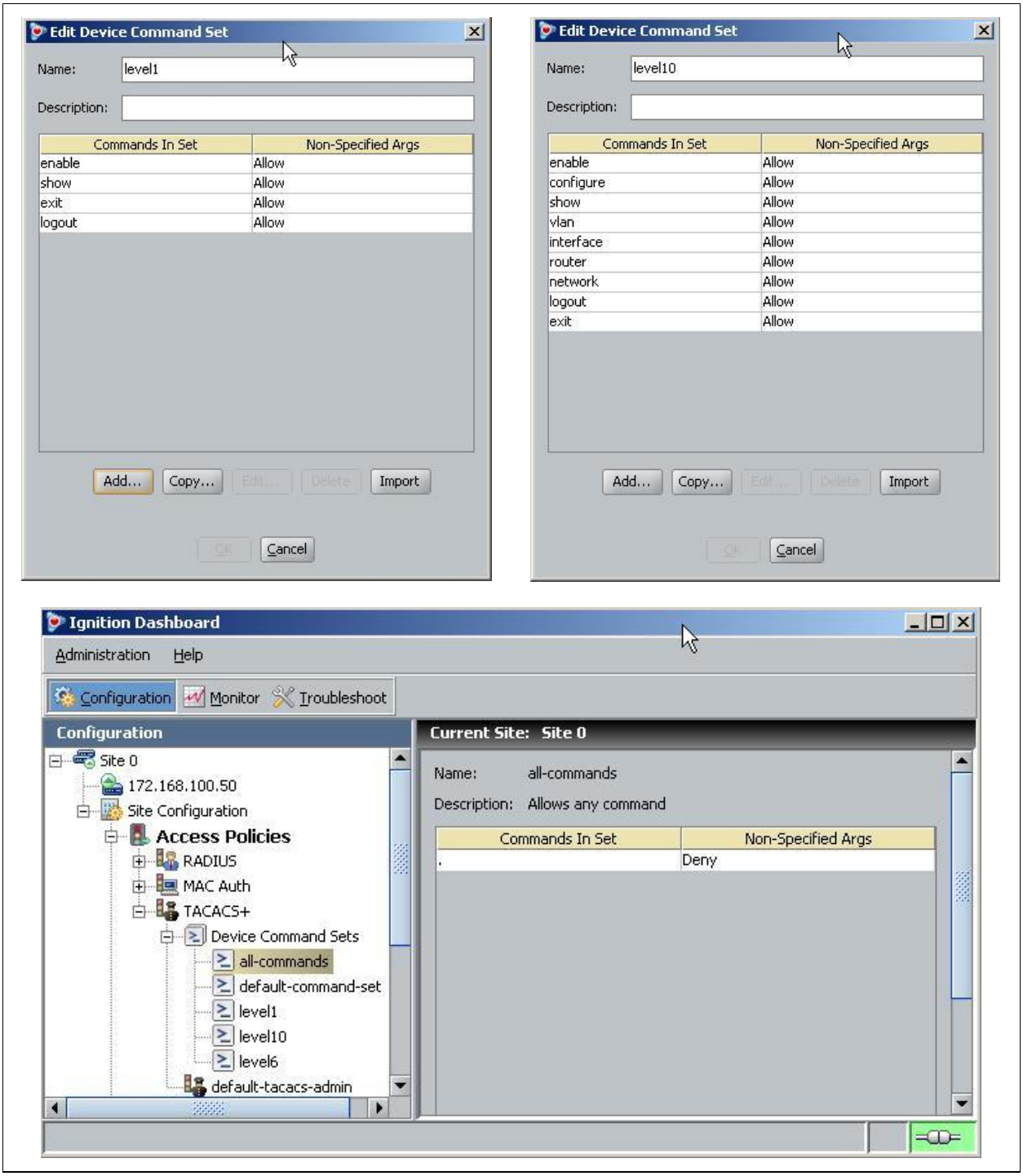
```
        Primary Host:  172.168.100.50
        Secondary Host:  0.0.0.0
        Port:  49
        Key:  ***************
        TACACS+ authorization is enabled
        Authorization is enabled on levels : 0-15
        TACACS+ accounting is enabled
```

6.1.2 IDE TACACS+ Configuration

If we are using Identity Engines Ignition Server as the TACAC+ server, please follow the configuration steps below assuming we wish to add the following:

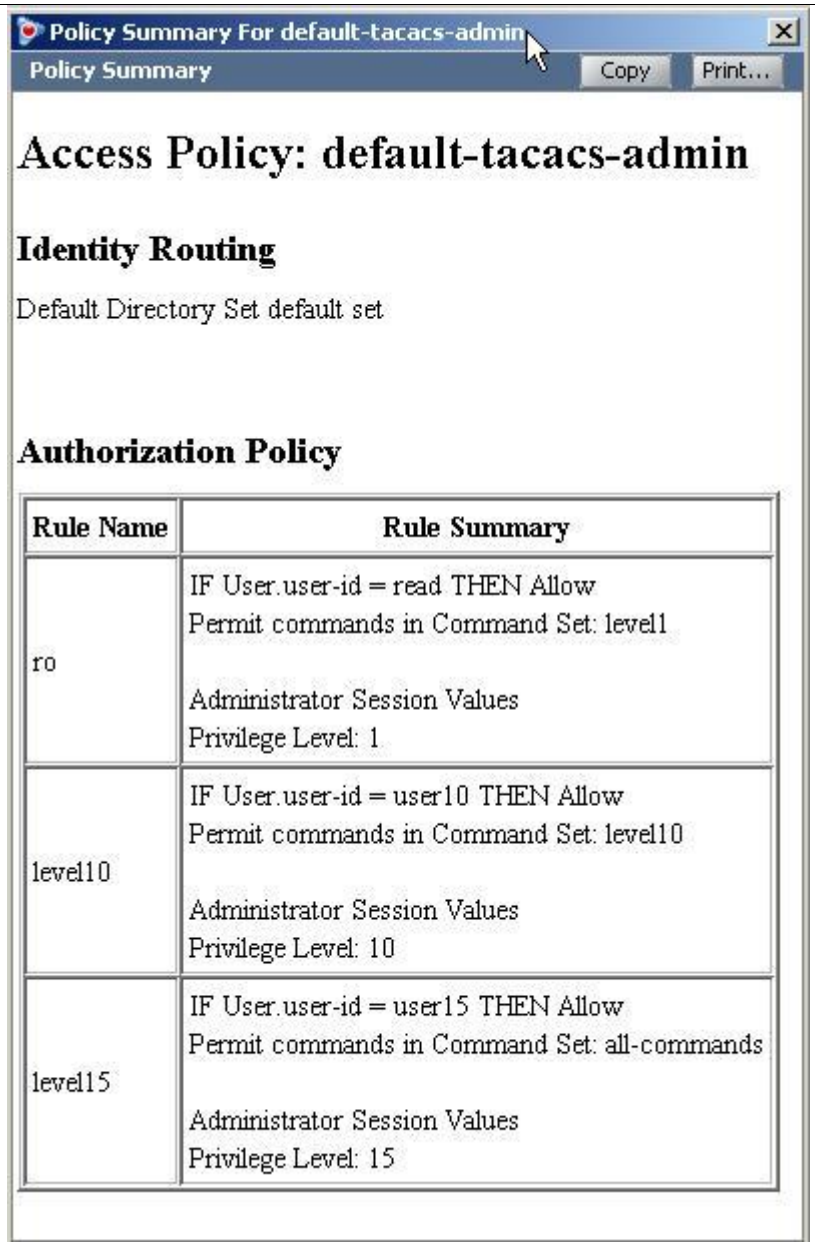
- User Name = read
  - Access Level = 1
  - Read-only access to allow only the following CLI commands: enable, show, exit, and logout
- User Name = user10
  - Access Level = 10
  - Restricted access to allow only the following CLI commands: enable, configure, show, vlan, interface, router, network, logout, and exit
- User Name = user15
  - Access Level = 15
  - Full access

IDE Step 1 – Go to *Site 0 -> Services -> TACACS+*
• Ensure that TACACS+ is enabled, if not, click the *Edit* box and enable TACACS+. The default port, TCP 49, should be left as-is.
IDE Step 2 – Add Users by going to *Site Configuration -> Directories -> Internal Store -> Internal Users* and click on *New*
• Enter the user name of *read* for read-only-access via *User Name:* and enter the password for this user via *Password* and *Confirm Password*. Click on *OK* when done. If you wish, you can also change the expiry date via *Password Expires* if you do not wish to use the default setting of one year. • Repeat again by clicking on *New* to add *user10* and *user15*.
IDE Step 3 – Go to *Site Configuration -> Access Policies -> TACACS+ -> Device Command Sets*
• Click on *New* and enter a name of *level1*. Click on *Add* four separate times to add the commands enable, show, exit, and logout with a Non-Specified Argument of *Allow* as shown below for the access level 1 “ro” user. Click on *OK* when done. • Click on *New* one more time and enter a name of *level10*. Click on *Add* nine separate times to add the commands enable, configure, show, vlan, interface, router, network, logout, and exit, with a Non-Specified Argument of *Allow* as shown below for the access level 10 “user10” user. Click on *OK* when done. • For the access 15 user, we will simply use the default *all-commands* Device Command Sets


Edit Device Command Set
Name: level1
Description:
Commands In Set | Non-Specified Args
enable | Allow
show | Allow
exit | Allow
logout | Allow
Add... Copy... Edit... Delete Import
OK Cancel
Edit Device Command Set
Name: level10
Description:
Commands In Set | Non-Specified Args
enable | Allow
configure | Allow
show | Allow
vlan | Allow
interface | Allow
router | Allow
network | Allow
logout | Allow
exit | Allow
Add... Copy... Edit... Delete Import
OK Cancel
Ignition Dashboard
Administration Help
Configuration Monitor Troubleshoot
Configuration
Site 0
172.168.100.50
Site Configuration
Access Policies
RADIUS
MAC Auth
TACACS+
Device Command Sets
all-commands
default-command-set
level1
level10
level6
default-tacacs-admin
Current Site: Site 0
Name: all-commands
Description: Allows any command
Commands In Set | Non-Specified Args
. | Deny

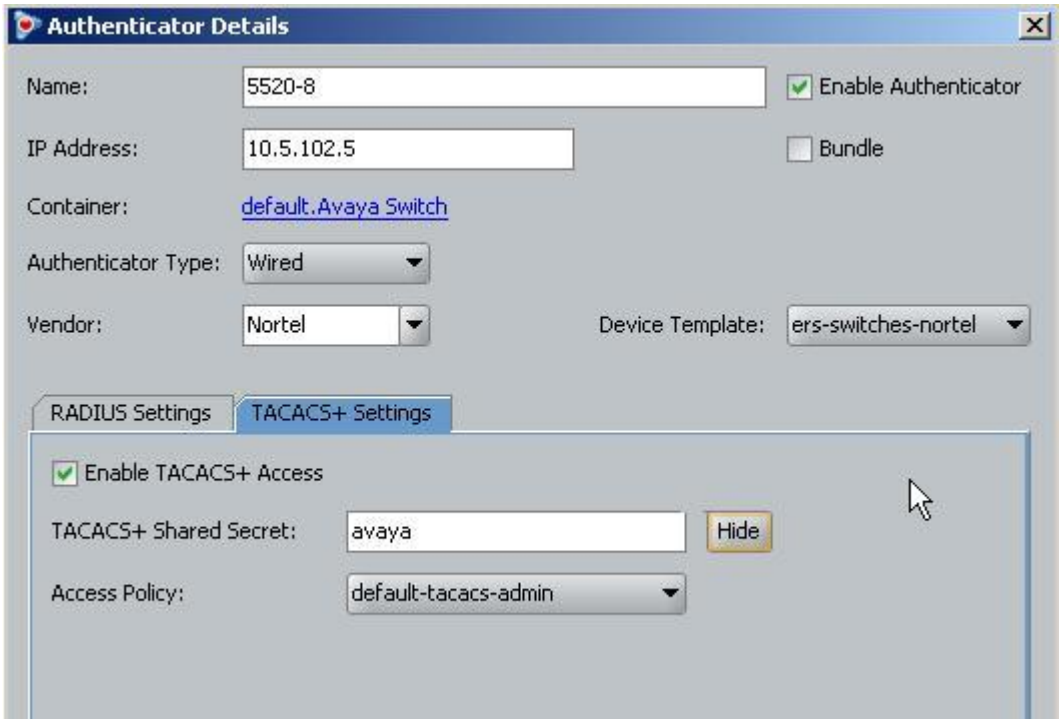
IDE Step 4 – Go to *Site Configuration -> Access Policies -> TACACS+ -> default-tacacs-admin*

- Go to the *Authorization Policy* tab and click on *Edit.*
  - Once the *Edit Authorization Policy* window pops up, click on *Add.* Add three Rules simply named ro, level10, and level15
  - For the rule named *ro*, click on *New* to add a new constraint. From *Attribute Category*, select *User* and scroll down and select *user-id*. Select *Equal To* with *Format* of *None* and enter the read-only-access user id of *read*. Click on *OK* when done. Via *Action*, select *Allow*. Via the *Command Sets* tab, select *level1* via *All Command Sets* and click on the less-than arrow key to move the attribute to the *Allow Commands in Set* window. Next, click on the *Session Values* tab, check off *Privilege Level* and enter 1.
  - For the rule named *level10*, click on *New* to add a new constraint. From *Attribute Category*, select *User* and scroll down and select *user-id*. Select *Equal To* with *Format* of *None* and enter the read-only-access user id of *user10.* Click on *OK* when done. Via *Action*, select *Allow*. Via the *Command Sets* tab, select *level10* via *All Command Sets* and click on the less-than arrow key to move the attribute to the *Allow Commands in Set* window. Next, click on the *Session Values* tab, check off *Privilege Level* and enter 10.
  - For the rule named *level15*, click on *New* to add a new constraint From *Attribute Category*, select *User* and scroll down and select *user-id*. Select *Equal To* with *Format* of *None* and enter the read-only-access user id of *user15.* Click on *OK* when done. Via *Action*, select *Allow*. Via the *Command Sets* tab, select *all-commands* via *All Command Sets* and click on the less-than arrow key to move the attribute to the *Allow Commands in Set* window. Next, click on the *Session Values* tab, check off *Privilege Level* and enter 15.
  - Click on *Ok* when done.
  - When completed, you can view the complete policy by clicking on the *Access Policy Summary* button


Policy Summary For default-tacacs-admin
Policy Summary
Copy
Print...
Access Policy: default-tacacs-admin
Identity Routing
Default Directory Set default set
Authorization Policy
Rule Name
Rule Summary
ro
IF User.user-id = read THEN Allow
Permit commands in Command Set: level1
Administrator Session Values
Privilege Level: 1
level10
IF User.user-id = user10 THEN Allow
Permit commands in Command Set: level10
Administrator Session Values
Privilege Level: 10
level15
IF User.user-id = user15 THEN Allow
Permit commands in Command Set: all-commands
Administrator Session Values
Privilege Level: 15

IDE Step 5 – Go to *Site Configuration -> Authenticators -> default*

- For example, we will create new container named *Avaya Switch* by right clicking *default* and selecting *Add Container*.
- Go to *Site Configuration -> Authenticators -> default -> Avaya Switch* and click on *New*
- Enter a name for the switch via *Name*, add the switch IP address via *IP Address*,. select *Wired* under *Authenticator Type*, select *Nortel* via *Vendor*, select *ers-switches-nortel* via *Device Template* and remove the default check via *Enable RADIUS Access*.
- Under the RADIUS Setting tab, uncheck the *Enable RADIUS Access* setting to disable RADIUS – this is the default setting
- Next, click on the *TACACS+ Settings* tab and check the *Enable TACACS+ Access* box and add the *TACACS+ Shared Secret*.
- Click on O*K* when done. The configuration should look something like the following



7. SSHv2

The ERS 2500, ERS 4500, and ERS 5000 support Secure Shell (SSH). SSH is a client/server protocol for secure remote login and other secure network services over an insecure network. It is essentially a replacement for telnet which is insecure because of its weak authentication method and unencrypted data exchange.

The following SSH clients are supported by the Ethernet Routing Switch:

- Putty SSH (Windows)
- F-secure SSH, v5.3 (Windows)
- SSH Secure Shell 3.2.9 (Windows)
- SecureCRT 4.1
- Cygwin OpenSSH (Windows)
- AxeSSH (Windows)
- SSHPro (Windows)
- Solaris SSH (Solaris)
- MAC OS X OpenSSH (MAC OS X)

SSH can run in either non-secure or secure modes. When SSH is enabled in secure mode, the switch does not accepts Telnet, SNMP, or HTTP connections. You can enable secure mode by issuing either of the following commands.

- ERS-Stackable(config)# ***ssh secure***

```
Enable secure mode will cut off all remote access. Telnet, snmp
and web will be disabled. Are you sure (y/n) ? y
```

- ERS-Stackable(config)# ***ssh secure force***

7.1 SSH Configuration Examples

7.1.1 SSH using Password Authentication

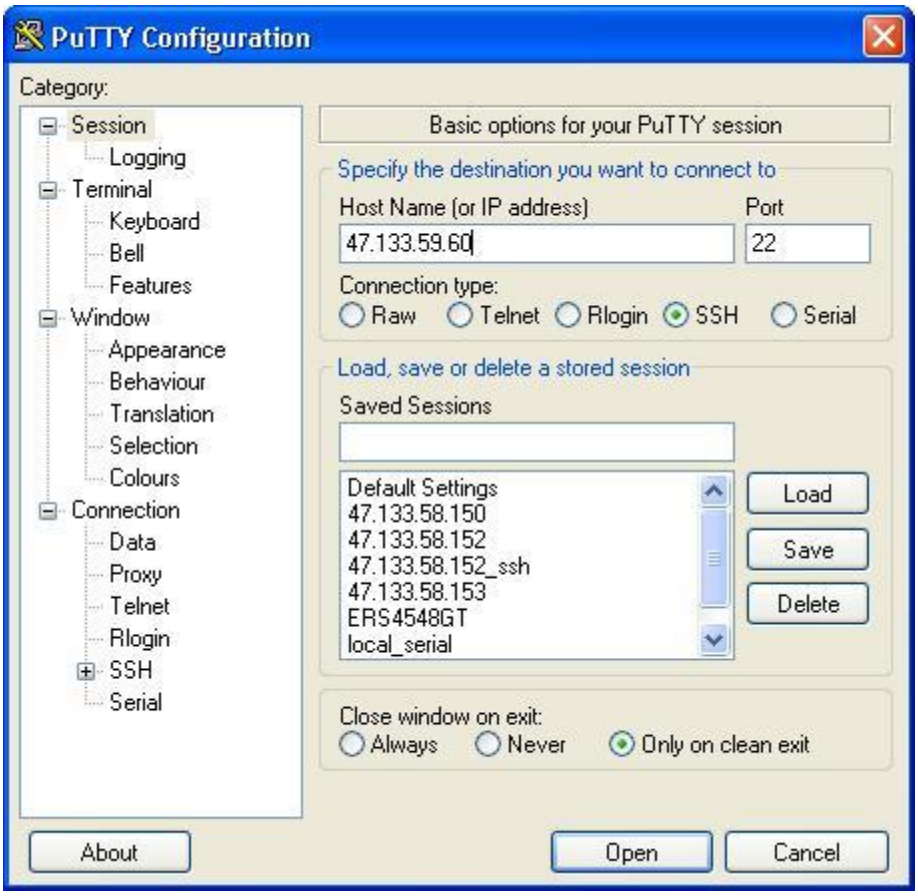
For this configuration example, we will use local password authentication on an ERS4500 switch to authenticate the SSH client. Instead of using local user name and password authentication, the user can be authenticated against a RADIUS or TACACS+ server. In this example, we will simply use local password authentication.

The default read-only and read-write users names of *RO* and *RW* will be used, but, we will change the default password for each user. We will assume password security is not enabled. If it is, follow the guidelines in the Password Security section above. Also, we will enable SSH secure mode which in turn will cut off Telnet, SNMP, and WEB access.

Putty will be used as the SSH Client.

ERS-STACKABLE: Step 1 – Change the default user names assuming a stack configuration and password security is not enabled
ERS-Stackable(config)# ***cli password stack read-only readonlypasswd***
ERS-Stackable(config)# ***cli password stack read-write rwonlypasswd***
ERS-STACKABLE: Step 2 – Enable secure mode
ERS-Stackable(config)# ***ssh secure***
Enable secure mode will cut off all remote access. Telnet, snmp
and web will be disabled. Are you sure (y/n) ? ***y***

Putty: Step 3 – Open up Putty and go to *Session -> Host Name (or IP address)*, enter the IP address of the switch, select *SSH*, and click on *Open* when done



Putty: Step 4 – Click on *Yes* when prompted with the public key fingerprint. You will only be prompted with this message once, unless, you select *No* to accept to accept this fingerprint, but, not save it.

Putty: Step 3 – Enter login credentials, i.e. user name = RW or RO and appropriate password assuming the default user names are used

7.1.2 Verify Operations

Step 1 – Verify SSH session

```
ERS-Stackable# show ssh session
```

Result:

```
        Session  Host
        -------  ----------------------------------------------
        1        47.132.2.13
```

Step 2 – Verify SSH configuration

```
ERS-Stackable# show ssh global
```

Result:

```
        Active SSH Sessions     :  1
        Version                 :  Version 2 only
        Port                    :  22
        Authentication Timeout  :  60
        DSA Authentication      :  True
        Password Authentication :  True
        DSA Auth Key TFTP Server:  47.132.2.13
        DSA Auth Key File Name  :
        DSA Host Keys           :  Exist
        Enabled                 :  Secure
```

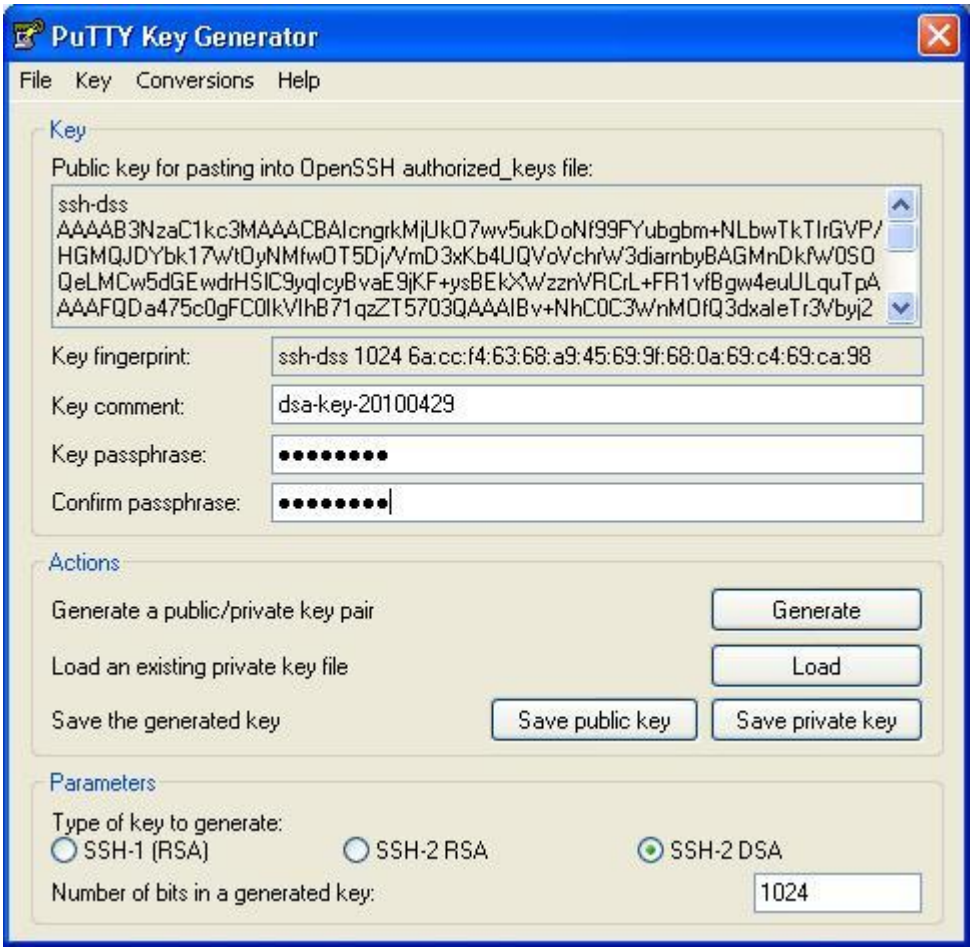
7.1.3 SSH using Public Key Authentication

Using Public Key Authentication is more involved than using SSH password authentication. On the Client, a set of keys (i.e. public/private) must be generated. DSA keys are generated as this is the default public key cipher used by the Ethernet Routing Switch. The client's public key must then be transferred to the switch using TFTP. For this configuration example, we will not enable SSH Secure as we did in the previous SSH configuration example, but, we will disable SSH password authentication, hence, only allowing SSH DSA key authentication.

Putty will be used as the SSH Client while Puttygen will be used to generate a DSA key.

Puttygen: Step 1 – Run Puttygen and select *SSH-2 DSA* key with *1024* bits and click on *Generate* to create both a public and private key. The public key will be uploaded to the switch. You will be prompted to move your mouse to create the key

Puttygen: Step 2 – Enter a *Key passphrase* to be used with this key and click on both Save public key and Save private key. You will be prompted to enter a file name; i.e. for this example, *erskey.pub* was used for the public key and erspriv.ppk was used for the private key

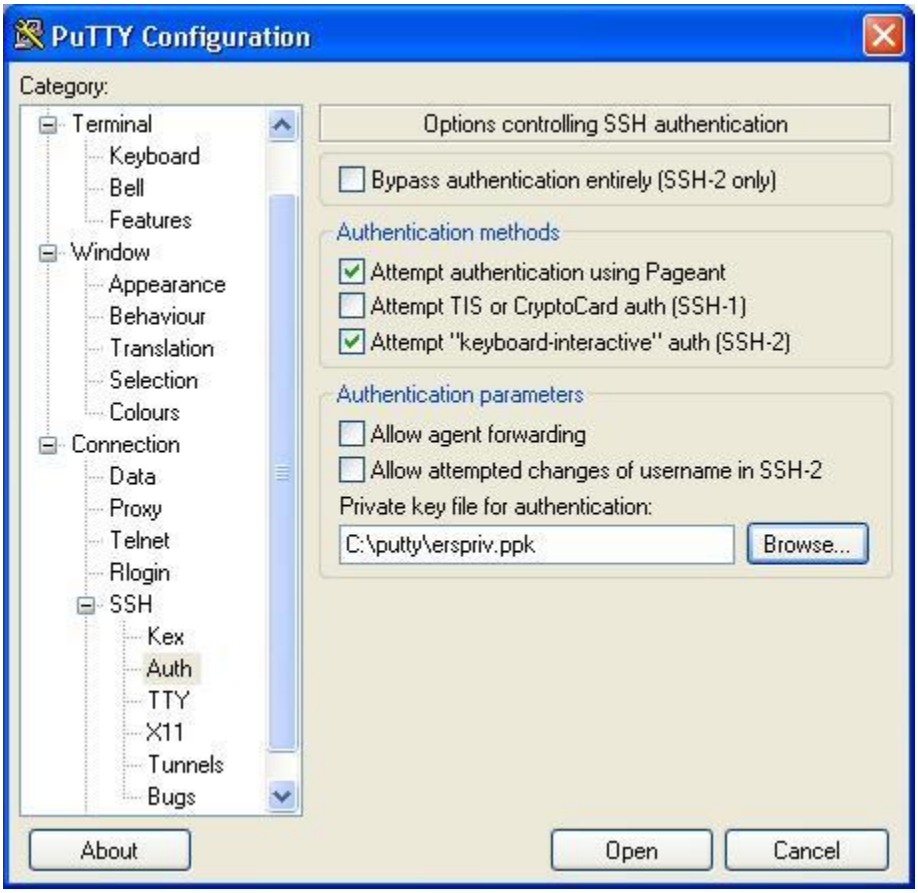


ERS-STACKABLE: Step 3 – Copy the public key to the ERS switch using the public key name you entered in the step above, i.e. erskey.pub. SSH must first be disabled, if enabled, in order to download the key

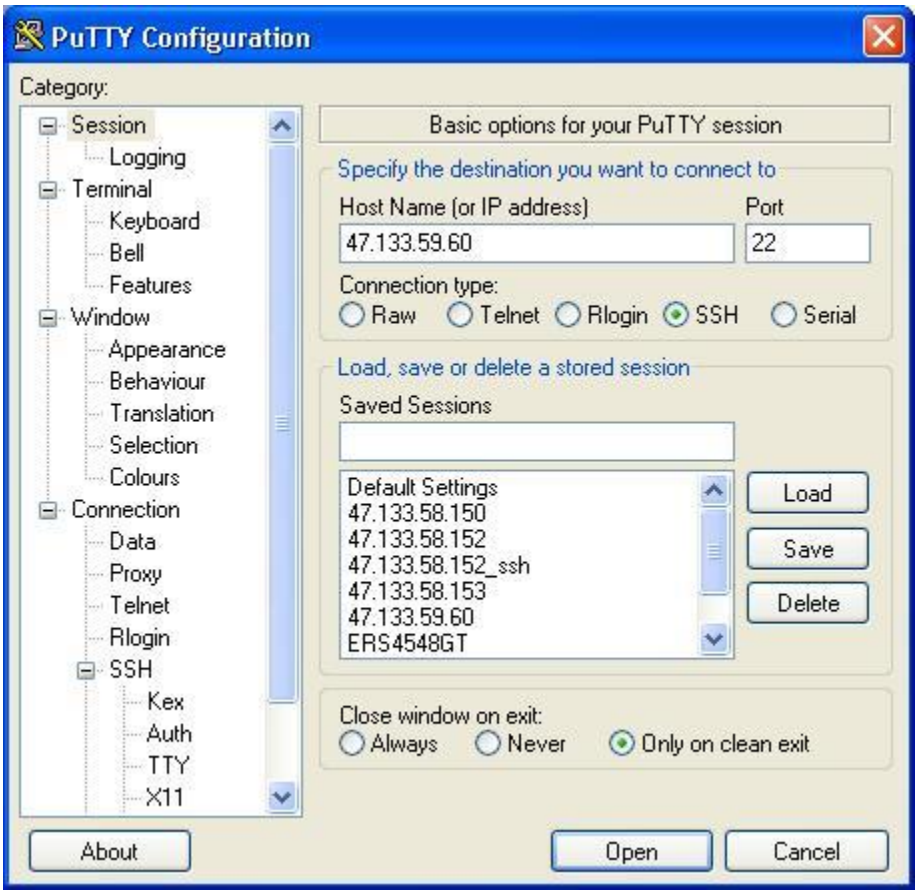
```
ERS-Stackable(config)# no ssh

ERS-Stackable(config)# ssh download-auth-key address 47.132.2.13 key-name
erskey.pub
```

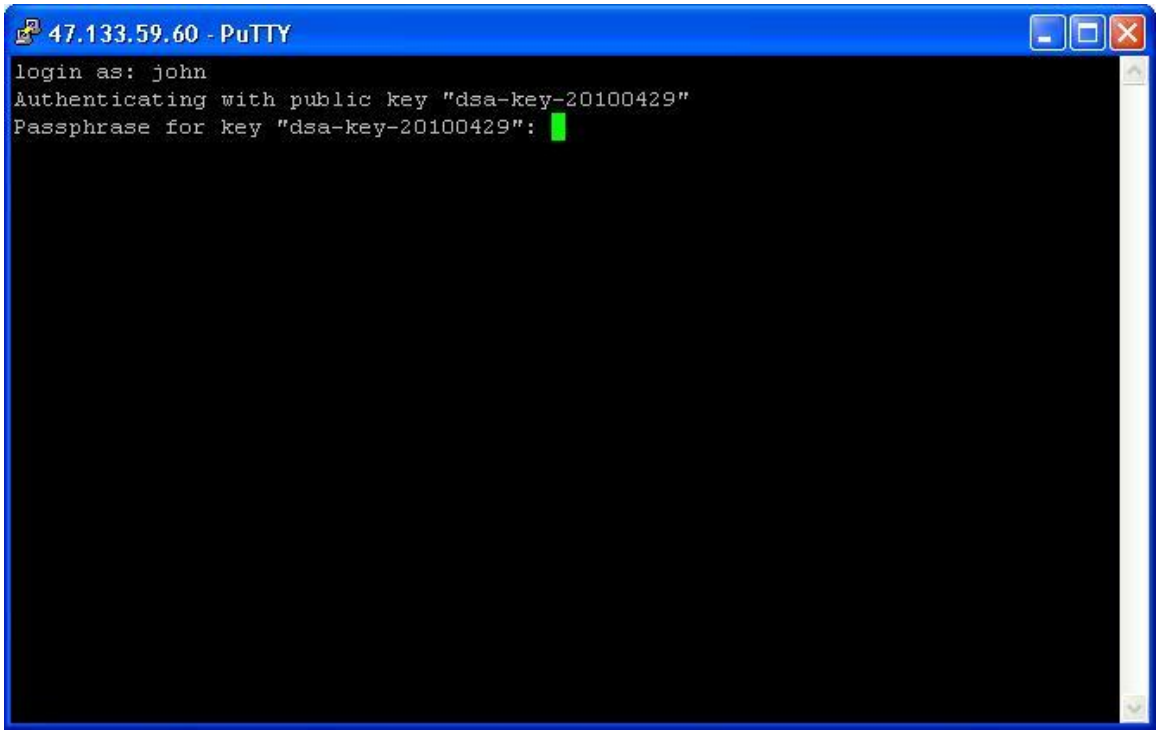
ERS-STACKABLE: Step 4 – Disable SSH password authentication and then re-enable SSH again
`ERS-Stackable(config)#` ***`no ssh pass-auth`***
`ERS-Stackable(config)#` ***`ssh`***
Putty: Step 4 – Open up Putty, scroll down to SSH -> Auth and enter select the private key generated above by clicking on the Browse icon



Putty: Step 5 – Go to *Session -> Host Name (or IP address)* , enter the IP address of the switch, select *SSH*, and click on *Open* when done



Putty: Step 6 – Enter any user name you like when prompted with the login as prompt and enter the DSA Key passphrase from the DSA key you generated above



7.1.4 Verify Operations

Step 1 – Verify SSH session

```
ERS-Stackable# show ssh session
```

Result:

```
        Session  Host
        -------  ----------------------------------------------
        1        47.132.2.13
```

Step 2 – Verify SSH configuration

```
ERS-Stackable# show ssh global
```

Result:

```
        Active SSH Sessions     :  1
        Version                 :  Version 2 only
        Port                    :  22
        Authentication Timeout  :  60
        DSA Authentication      :  True
        Password Authentication :  False
        DSA Auth Key TFTP Server:  47.132.2.13
        DSA Auth Key File Name  :  erskey.pub
        DSA Host Keys           :  Exist
        Enabled                 :  True
```

Step 3 – Verify DSA download public key

```
ERS-Stackable# show ssh download-auth-key
```

Result:

```
        DSA Auth Key TFTP Server:  47.132.2.13
        DSA Auth Key File Name  :  erskey.pub
        Last Transfer Result    :  Success
```

8. WEB Access – Enterprise Device Manager

By default, password authentication is disabled for WEB access to the switch allowing a user to use HTTP to access an Ethernet Routing Switch, i.e. for Enterprise Device Manager Access, without having to enter a user name or password. Password authentication for WEB access is enabled automatically either when local CLI Telnet password security or CLI Telnet RADIUS password security is enabled. IP Manager can also be enabled for WEB access if you wish to restrict access to a few individuals or a particular subnet or subnets. Please note that WEB access is disabled if TACACS+ is enabled.

If secure mode is enabled or simply if SSL is enabled, the Web server listens on TCP port 443 and responds only to HTTPS client browser requests. All existing non-secure connections, TCP port 80, with the browser are closed down.

In the non-secure mode, the Web server listens on TCP port 80, by default, and responds only to HTTP client browser requests. All existing secure connections with the browser are closed down. You can designate the TCP port as a number between 1024 and 65535.

The WEB server demon can either be enabled or disabled by issuing the following command.

- ERS-Stackable(config)# ***web-server ?***

```
disable   Disable HTTP access
enable    Enable HTTP access
```

To enable WEB authentication, enter the following command:

- ERS-Stackable(config)# ***cli password <stack|switch> telnet <local|radius|tacacs>***

To enable IP Manager control for WEB access, enter the following command depending on if IPv4 or IPv6 addressing is used:

- ERS-Stackable(config)# ***ipmgr source-ip <1-50> <IPv4 address/mask>***
- ERS-Stackable(config)# ***ipmgr source-ip <51-100> <IPv6 address/prefix>***
- ERS-Stackable(config)# ***ipmgr web***

In non-secure mode, SSL disabled, if you wish to designate the TCP port number other than TCP port 80, enter the following command:

- ERS-Stackable(config)# ***http-port ?***

```
<1024-65535>  http port number
```

For Enterprise Device Manager to work, the web-server option must be enabled.

Also, TACACS+ cannot be enabled if you wish to enable HTTP access. Please see the section Telnet password protection section above, ether using local authentication or RADIUS authentication if you wish to provide WEB access user name and password protection.

9. Secure Socket Layer Protocol – SSL

Secure Socket Layer (SSL) deployment provides a secure Web management interface.

The SSL server has the following features:

- SSLv3-compliant
- PKI key exchange
- key size of 1024-bit encryption
- RC4 and 3DES cryptography
- MAC algorithms MD5 and SHA-1

Generally, an SSL certificate is generated when

- The system is powered up for the first time and the NVRAM does not contain a certificate that can be used to initialize the SSL server.
- The management interface (NNCLI and SNMP) requests that a new certificate to be generated. A certificate cannot be used until the next system reset or SSL server reset.

SSL certificates are issued and signed by a Certificate Authority (CA) such as VeriSign. Because the management and cost of purchasing a certificate from a CA is a client concern, Avaya issues and signs the SSL certificate with the understanding that it is not a recognized CA.

The SSL certificate contains the following information. The first three items (Issuer, Start Date, End Date) are constant. The remaining items are derived from the RSA host key associated with the certificate. The certificate can be used by issuing the following command.

- ERS-Stackable# ***show ssl certificate***

```
Issuer     : Nortel Networks
Start Date : May 26 2003, 00:01:26
End   Date : May 24 2033, 23:01:26
SHA1 Finger Print:
a4:a7:a9:1e:db:80:c1:8a:f2:20:d7:b7:fe:11:64:48:c8:9b:82:1d
MD5 Finger Print:
df:58:36:c2:d1:e4:2b:31:b7:d8:83:9d:60:e7:9c:a3

RSA Host Key (length= 1024 bits):
408248c22a17def757363e5b71c8c7dc4b8f755c3b8f442c2c0fd8aed1d9c2fd
601ac6ddc6f636df0864f6ce0845d1aedb9cad0bea6c4f2c582da6adeab2f5b5
ffa604112c04c8c10744568a30eca27934a608e8c13ecaf7c831df28f8f62c3b
0e05b4c1b6a2f06bc918882a6a61f8b68fac5a2d66e6341df24218f807c9d9b1
```

To enable SSL or disable SSL, simply enter the following command:

- ERS-Stackable(config)# ***ssl***
- ERS-Stackable(config)# ***no ssl***

To reset the SSL server, enter the following command. If SSL is enabled, existing SSL connections are closed while the SSL server is restarted and initialized with the certificate that is stored in NVRAM.

- ERS-Stackable(config)# ***ssl reset***

To delete and generate a new SSL certificate, enter the following command. Please note the new certificate is used only on the next system reset or SSL server reset. The new certificate is stored in the NVRAM with the file name SSLCERT.DAT. The new certificate file replaces the existing file. On deletion, the certificate in NVRAM is also deleted. The current SSL server operation is not affected by the create or delete operation.

- ERS-Stackable(config)# ***no ssl certificate***

```
Old certificate is deleted on next system or SSL server reset
```

The WEB server demon can either be enabled or disabled by issuing the following command.

- ERS-Stackable(config)# ***web-server ?***

```
disable  Disable HTTP access
enable   Enable HTTP access
```

To enable WEB SSL authentication, enter the following command:

- ERS-Stackable(config)# ***cli password <stack|switch> telnet <local|radius|tacacs>***

To enable IP Manager control for WEB SSL access, enter the following command depending on if IPv4 or IPv6 addressing is used:

- ERS-Stackable(config)# ***ipmgr source-ip <1-50> <IPv4 address/mask>***
- ERS-Stackable(config)# ***ipmgr source-ip <51-100> <IPv6 address/prefix>***
- ERS-Stackable(config)# ***ipmgr web***

10. Simple Network Management Protocol - SNMP

The Ethernet Routing Switch supports all three version of SNMP defined as SNMPv1, SNMPv2, and SNMPv3. SNMPv2 is similar to SNMPv1 in that only Community Strings are used for authentication. SNMPv2 differs from SNMPv1 in that it supports GetBulk and Inform operations. The GetBulk operation is used to retrieve large blocks of data while the Inform operation allows traps to be acknowledged. SNMPv3 specifies a User Security Model (USM) providing for user-name and password authentication, encryption, and control access to management information (MIB). SNMPv3 is not a stand-alone replacement for SNMPv1 and/or SNMPv2. It simply defines security capabilities to be used in conjunction with SNMPv2 or SNMPv1.

10.1 SNMP Basic Operations

You can enable or disable SNMP on the Ethernet Routing Switch using the following command. By default, SNMP is disabled.

- `ERS-Stackable(config)# snmp-server <enable|disable>`

10.2 SNMPv1 Community Strings

SNMPv1 and SNMPv2 simply use a community string match for authentication. To support user name, authentication, and encryption, SNMPv3 must be used. The default SNMP community string can be changed by using the following commands.

To change the SNMP read-write community string, enter the following command depending on the switch model:

- `ERS-Stackable(config)# snmp-server community <enter rw string> rw`
- `ERS-Stackable(config)# snmp-server community rw`

  ```
  Enter community string: <enter rw string>
  Confirm community string: <enter rw string>
  ```

To change the SNMP read-only community string, enter the following command:

- `ERS-Stackable(config)# snmp-server community <enter rw string> ro`
- `ERS-Stackable(config)# snmp-server community ro`

  ```
  Enter community string: <enter ro string>
  Confirm community string: <enter ro string>
  ```

To view the configuration, enter the following command:

- ERS-Stackable(config)# ***show snmp-server***

```
Read-Only Community String: ***************
Read-Write Community String: ***************
Trap #1 IP Address:       0.0.0.0
        Community String: ***************
Trap #2 IP Address:       0.0.0.0
        Community String: ***************
Trap #3 IP Address:       0.0.0.0
        Community String: ***************
Trap #4 IP Address:       0.0.0.0
        Community String: ***************
Authentication Trap: Enabled
AutoTopology: Enabled
```

10.3 SNMP MIB View

To add a new SNMP MIB view, enter the following command:

- ERS-Stackable(config)# ***snmp-server view <view name> <oid .. oid>***

10.4 SNMP Trap Receivers

To add a SNMPv1 trap receiver, enter the following command:

- `ERS-Stackable(config)#` ***`snmp-server host <IPv4/Ipv6 addr>`***

`or (please see note below)`

- `ERS-Stackable(config)#` ***`snmp-server host <IPv4/Ipv6 addr> v1 <SNMPv1 community string>`***

To add a SNMPv2 trap receiver, enter the following command (please see note below)

- `ERS-Stackable(config)#` ***`snmp-server host <IPv4/Ipv6 addr> v2c <SNMPv2 community string> inform timeout <1-2147483647 centi-seconds> retries <0-255>`***

To add a SNMPv3 trap receiver, enter the following command:

- `ERS-Stackable(config)#` ***`snmp-server host <IPv4/Ipv6 addr> v3 <auth|auth-priv|no-auth> <snmpv3 user name> inform timeout <1-2147483647 centi-seconds> retries <0-255>`***

To restore the SNMP host back to it's default value, clear the table, enter the following command:

- `ERS-Stackable(config)#` ***`default snmp-server host`***

The default snmp-server community strings of *public* and *private* cannot be used for SNMPv1 and SNMPv2c Traps generation with community strings. These SNMP community strings do not have a defined notify views, only read and write views. In order to generate traps with community strings, additional SNMP server community string(s) should be defined first supporting a notify view using the NNCLI syntax: *snmp-server community read-view <view name> write-view <view name> notify-view <view name>*

10.5 SNMP System Name, Contact, and Location

To add a switch system name, SNMP sysContact value, enter the following command:

- `2526T-PWR(config)#` ***`snmp-server name 2526T-10`***

  `2526T-10(config)#`

To add a SNMP server contact, SNMP sysContact value, enter the following command:

- 2526T-PWR(config)# ***snmp-server contact <name>***

To add a SNMP location, SNMP sysLocation value, enter the following command:

- 2526T-PWR(config)# ***snmp-server location <string up to 255 chracters using "" between string if spaces are used>***

To change back to the default settings, enter the following commands:

- `2526T-10(config)#` ***`default snmp-server location`***
- `2526T-10(config)#` ***`default snmp-server contact`***
- `2526T-10(config)#` ***`default snmp-server name`***

  `2526T-PWR(config)#`

10.6 Disable SNMPv1 and SNMPv2

SNMPv1 and SNMPv2 access can be disabled by entering the following commands:

- `ERS-Stackable(config)#` ***`no snmp-server community rw`***
- `ERS-Stackable(config)#` ***`no snmp-server community ro`***

10.7 SNMPv3

SNMPv3 provides three levels of access security named noAuthNoPriv, authNoPriv, and authPriv. Security level noAuthNoPriv simply provides a username match for authentication. Security level authNoPriv provide authentication based on ether MD5 or SHA algorithms while authPriv add the addition of DES, 3DES, or AES encryption in addition to authentication.

To add a noAUthNoPriv user, simply enter the following command.

- `ERS-Stackableconfig)#` ***`snmp-server user (user name) <write-view|read-view|notify-view> (view name)`***

To add an authNoPriv security access level, enter the following command. Depending on the switch, the password is either entered after the command or on the same line as the command itself:

- `ERS-Stackable(config)#` ***`snmp-server user (user name) <md5|sha> <write-view|read-view|notify-view>`***
- `ERS-Stackableconfig)#` ***`snmp-server user (user name) <md5|sha> (password) <write-view|read-view|notify-view> (view name)`***

To add an authPriv security access level, enter the following command.

- `ERS-Stackable(config)#` ***`snmp-server user (user name) md5 (password) <des|aes|3des> (privacy password) <write-view|read-view|notify-view>`***

By default, there is a default authNoPriv account with a user name of *initial* and an MD5 password of *initial*. For security reasons, you may want to delete this user account by issuing the command *no snmp-server user initial*.

10.8 Enabling Secure SNMP

The *snmp-server bootstrap* command allows you to specify how you wish to secure SNMP communications, as described in the SNMPv3 standards. It creates an initial set of configuration data for SNMPv3. This configuration data follows the conventions described in the SNMPv3 standard (in RFC 3414 and 3415). This command creates a set of initial users, groups and views.

This command deletes all existing SNMP configurations, hence must be used with care.

The syntax for the snmp-server bootstrap command is:

- ERS-Stackable(config)# ***snmp-server bootstrap ?***

```
minimum-secure  Use minimum security configuration
semi-secure     Use partial security configuration
very-secure     Use maximum security configuration
```

Parameters and variables	Description
<minimum-secure>	Specifies a minimum security configuration that allows read access to everything using noAuthNoPriv, and write access to everything using authNoPriv. **Note:** In this configuration, view restricted matches view internet.
<semi-secure>	Specifies a partial security configuration that allows read access to a small subset of system information using noAuthNoPriv, and read and write access to everything using authNoPriv. **Note:** In this configuration, restricted contains a smaller subset of views than internet view. The subsets are defined according to RFC 3515 Appendix A.
<very-secure>	Specifies a maximum security configuration that allows no access to the users.

10.9 SNMP Configuration Examples

10.9.1 SNMP Community String Configuration Example

For this configuration example, we will configure the following:

- Change the read-write community string to *readwritecommunity*
- Change the read-only community string to *readonlycommunity*
- Add an SNMPv1 trap receiver assuming the IP address is 172.168.100.50
- Add an additional write-view community named *noipreadwrite* with no access to any IP configurable item

ERS-STACKABLE: Step 1 – Enable SNMP

```
ERS-Stackable(config)# snmp-server enable
```

ERS-STACKABLE: Step 1 – Change the default read-write and read-only community strings

```
ERS-Stackable(config)# snmp-server community readwritecommunity rw
ERS-Stackable(config)# snmp-server community readonlycommunity ro
If password security is enabled:
ERS-Stackable(config)# snmp-server community rw
Enter community string: readwritecommunity
Confirm community string: readwritecommunity
ERS-Stackable(config)# snmp-server community ro
Enter community string: readonlycommunity
Confirm community string: readonlycommunity
```

ERS-STACKABLE: Step 2 – Add the trap receiver

```
ERS-Stackable(config)# snmp-server host 172.168.100.50 v1 public
```

ERS-STACKABLE: Step 3 – Add a new SNMP view named *no_ip* with restrictions to the IP

```
ERS-Stackable(config)# snmp-server view no_ip +1.3 -1.3.6.1.4.1.2272.1.8
```

ERS-STACKABLE: Step 4 – Create an new community named *noipreadwrite* with the write-view created above named *no_ip*

```
ERS-Stackable(config)# snmp-server community write-view noipreadwrite
Enter community string: ***** (no_ip)
Confirm community string: ***** (no_ip)
```

Options

ERS-STACKABLE: Enabling IP Manager, assuming IPv4 source IP addresses

```
ERS-Stackable(config)# ipmgr source-ip 1 47.0.0.0 mask 255.0.0.0
ERS-Stackable(config)# ipmgr source-ip 2 172.32.0.0 mask 255.255.0.0
ERS-Stackable(config)# ipmgr source-ip 3 192.50.500.30 mask 255.255.255.255
|
ERS-Stackable(config)# ipmgr source-ip 50 ……
2526T-PWR(config)# ipmgr snmp
```

ERS-STACKABLE: Adding Syslog, i.e. if using COM

```
ERS-Stackable(config)# logging remote address 172.168.100.50
ERS-Stackable(config)# logging remote level informational
ERS-Stackable(config)# logging remote enable
```

10.9.2 Verify Operations

Step 1 – Verify SNMP MIB view

```
2526T-10-PWR# show snmp-server view
```

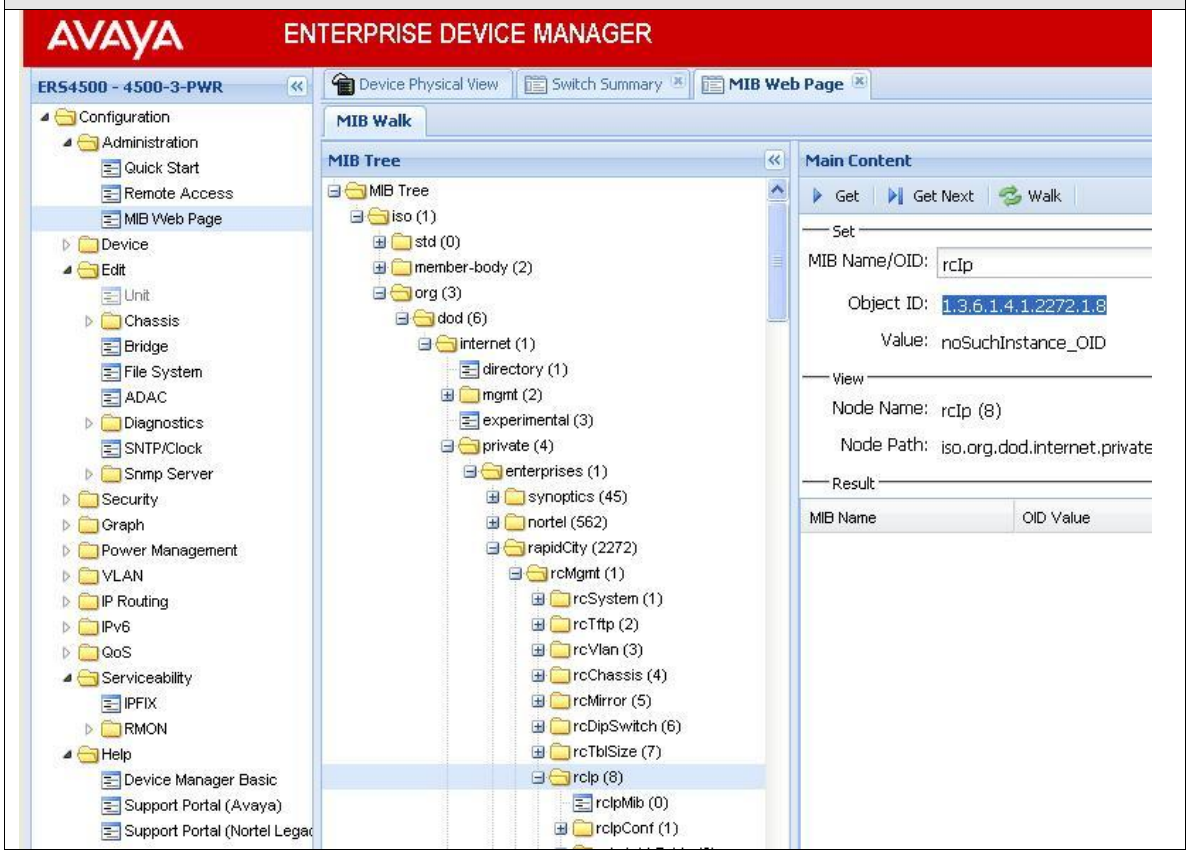
Result:

```
        View Name                       ST RS View Spec(s)
        ------------------------------- -- -- --------------------------------------
        nncli                           RO AC +1.3
                                        RO AC +1.0.8802.1.1.1
                                        RO AC +1.0.8802.1.1.2
                                        RO AC +1.2.840.10006.300.43
        ------------------------------- -- -- --------------------------------------
        no_ip                           NV AC +1.3
                                        NV AC -1.3.6.1.4.1.2272.1.8
        ------------------------------- -- -- --------------------------------------
        snmpv1Objs                      RO AC +1.3
                                        RO AC -1.3.6.1.6
                                        RO AC +1.0.8802.1.1.1
                                        RO AC +1.0.8802.1.1.2
                                        RO AC +1.2.840.10006.300.43
                                        RO AC +1.3.6.1.6.3.10
                                        RO AC +1.3.6.1.6.3.12
                                        RO AC +1.3.6.1.6.3.13
                                        RO AC +1.3.6.1.6.3.1.1.4
                                        RO AC +1.3.6.1.6.3.1.1.5
        ------------------------------- -- -- --------------------------------------
        webSnmpObjs                     RO AC +1.3
                                        RO AC +1.0.8802.1.1.1
                                        RO AC +1.0.8802.1.1.2
                                        RO AC +1.2.840.10006.300.43
        ------------------------------- -- -- --------------------------------------
```

If using EDM, you can use it to perform a MIB walk as shown below.

Open up a browser connection and enter the management IP address of your switch. The result shown below shows the MIB object ID for IP.

Result:



10.9.3 SNMPv3 Configuration Example

Assuming we wish to add the following users:

- SNMPv3 authPriv user using a user name of *userro* with authentication based on MD5 with an authentication password of *readonly*, privacy protocol of 3DES using a password of *despasswdro*.
- SNMPv3 authPriv user using a user name of *userrw* with authentication based on MD5 with an authentication password of readwrite, privacy protocol of 3DES using a password of *despasswd*.

ERS- STACKABLE: Step 1 – Enable SNMP

```
ERS-Stackable(config)# snmp-server enable
```

ERS-STACKABLE: Step 1 – Add SNMPv3 authPriv read-only user

```
ERS-Stackable(config)# snmp-server user userr0 md5 readonly 3des despasswdro
read-view snmpv1Objs
If using password security is enabled:
ERS-Stackable(config)# snmp-server user userro md5 read-view snmpv1Objs 3des
read-view snmpv1Objs
Enter MD5 pass-phrase: ******** (readonly)
Confirm MD5 pass-phrase: ******** (readonly)
Enter 3Des pass-phrase: ********** (despasswdro)
Confirm 3Des pass-phrase: ********** (despasswdro)
```

ERS-STACKABLE: Step 2 – Add SNMPv3 authPriv read-write user

```
ERS-Stackable(config)# snmp-server user userrw md5 readwrite 3des despasswdrw
write-view snmpv1Objs read-view snmpv1Objs
If using password security is enabled:
ERS-Stackable(config)# snmp-server user userrw md5 3des read-view snmpv1Objs
write-view snmpv1Objs
Enter MD5 pass-phrase: ********* (readwrite)
Confirm MD5 pass-phrase: ********* (readwrite)
Enter 3Des pass-phrase: ********** (despasswdrw)
Confirm 3Des pass-phrase: ********** (despasswdrw)
```

The SNMP view name used in this example is one of the default MIB view on the Ethernet Routing Switch which can be viewed by entering the CLI command *show snmp-server view*.

10.9.4 Verify Operations

Step 1 – Verify SNMP users

```
ERS-Stackable(config)# show snmp-server user
```

Result:

```
        ------------------------------------------------------------------------
        User Name:  userro
        SNMP Engine ID:  Local
        Authentication Protocol:  MD5
        Privacy Protocol:  3DES
        Storage Type:  Non Volatile (NVRAM)
        Status:  Active
        Views for Unauthenticated Access:
            Read View:
            Write View:
            Notify View:
        Views for Authenticated Access:
            Read View:
            Write View:
            Notify View:
        Views for Authenticated and Encrypted Access:
            Read View:    snmpv1Objs
            Write View:
            Notify View:
        ------------------------------------------------------------------------
        User Name:  userrw
        SNMP Engine ID:  Local
        Authentication Protocol:  MD5
        Privacy Protocol:  3DES
        Storage Type:  Non Volatile (NVRAM)
        Status:  Active
        Views for Unauthenticated Access:
            Read View:
            Write View:
            Notify View:
        Views for Authenticated Access:
            Read View:
            Write View:
            Notify View:
        Views for Authenticated and Encrypted Access:
            Read View:    snmpv1Objs
            Write View:   snmpv1Objs
            Notify View:
        ------------------------------------------------------------------------
        User Name:  initial
        SNMP Engine ID:  Local
        Authentication Protocol:  MD5
        Privacy Protocol:  None
        Storage Type:  Non Volatile (NVRAM)
        Status:  Active
        Views for Unauthenticated Access:
            Read View:    restricted
            Write View:
            Notify View:  restricted
        Views for Authenticated Access:
            Read View:    internet
            Write View:   internet
            Notify View:  internet
        ------------------------------------------------------------------------
        User Name:  templateMD5
```

```
        SNMP Engine ID:  Local
        Authentication Protocol:  MD5
        Privacy Protocol:  None
        Storage Type:  Non Volatile (NVRAM)
        Status:  Active
        Views for Unauthenticated Access:
            Read View:
            Write View:
            Notify View:
        Views for Authenticated Access:
            Read View:
            Write View:
            Notify View:
        ------------------------------------------------------------------------------
```

10.10 SNMP Trap Notification Control

SNMP Trap functionality on the ERS 4500 5.4, ERS 2500 4.3, and ERS 5000 6.2 is changed to align all SNMP trap control to the new 'notification control' method. Previously on the Ethernet Routing Switch the following functions used this new method: DHCP Snooping, Dynamic ARP Inspection (DAI) and IP Source Guard (IPSG).

The new trap support is based on the bsncNotifyControlTable where each application registers its trap(s) with the table. Each application when registering new traps will set the configuration change flag, so that if autosave is enabled, the new traps will be saved to NVRAM when autosave next executes.

By default, all traps are enabled. Entries in the bsncNotifyControlTable are pre-created, you can not add or delete entries in the table; you can only control if the application will generate SNMP traps.

If a PoE unit is present or is present in a stack, then three PoE specific trap notifications will be present: pethPsePortOnOffNotification, pethMainPowerUsageOnNotification, pethMainPowerUsageOffNotification

The Rapid Spanning Tree (RSTP) specific traps are not available when operating in the Avaya STG or the MSTP modes. If you have configured RSTP notification types and change the switch operational mode, the previous RSTP notification types are saved in the configuration, though will not be displayed in non RSTP mode.

The previous application specific SNMP trap commands are now hidden, so that customers should use the new notification control commands.

> [no] [default] adac traps
> [no] mac-security snmp-trap
> [no] poe-trap
> [no] [default] snmp-server authentication-trap
> [no] [default] spanning-tree rstp traps

The '[no] [default] snmp trap link-status' is still an available CLI command as it provides per port control which is not provided by the SNMP trap Notification control.

The following command displays the various notification type names and the status showing if the notification control is enabled or disabled.

- ERS-Stackable# ***show snmp-server notification-control***

The following commands either enables or disables a notification control type. Please note, the word entered can either be any one of the SNMP descriptions displayed when the *show snmp-server notification-control* command is issued or the OID of a supported notification type. EDM can be used to view both the notification type name and OID where the CLI only shows the name.

- ERS-Stackable(config)# ***snmp-server notification-control <word>***
- ERS-Stackable(config)# ***no snmp-server notification-control <word>***

To add a notification filter and apply it to a SNMP trap host, enter the following commands assuming a SNMPv1 trap receiver is used

- ERS-Stackable(config)# ***snmp-server notify-filter <filter name> <notification name or OID>***
- ERS-Stackable(config)# ***snmp-server host <IPv4 or IPv6 address> v1 <SNMPv1 community string> filter <filter name>***

11. Software Baseline:

Device	Software Release
Ignition Server	6.0.1
Ethernet Routing Switch 5000	Release 6.1.2
Ethernet Routing Switch 4500	Release 5.4
Ethernet Routing Switch 4500	Release 4.3

12. Reference Documentation:

Identity Engines Ignition Server	
Identity Engines Ignition Server, Release 6.0 – Document Collection	http://support.avaya.com/
Ethernet Routing Switch 5000	
Avaya Ethernet Routing Switch 5000 Series Release 6.1 Document Collection	http://support.avaya.com/
Ethernet Routing Switch 4500	
Avaya Ethernet Routing Switch 4500 Series Release 5.4 Document Collection	http://support.avaya.com/
Ethernet Routing Switch 2500	
Avaya Ethernet Routing Switch 2500 Series Release 4.3 Document Collection	http://support.avaya.com/