Ethernet Routing Switch

- ERS 2500
- ERS 3500
- ERS 4500/ 4800
- ERS 5500/ 5600

Virtual Services Platform

- VSP 7000

Engineering

> MAC Address Based Security Technical Configuration Guide

Avaya Data Solutions

Document Date: July 2012

Document Number: NN48500-601

Document Version: 2.1

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

Revision Control

No	Date	Version	Revised By	Remarks
1	1 Aug 2008	1.0	V. Ganjian	Initial draft document release
2	22 Nov 2010	1.1	K. Marshall	Rebranded Avaya
3	September 2012	2.0	L. Stevens	Complete re-write
4	24 Sept 2012	2.1	L. Stevens	Incorporated review changes from JVE

Table of Contents

Figures 5
Tables 5
1. Introduction 7
2. Base configuration setup 12
2.1 Ensuring MAC Security can never accidentally be enabled on uplinks 13
2.2 Disabling SNMP write access just for MAC Security configuration 15
3. Regular MAC Security examples 17
3.1 Controlling exactly which MAC is allowed to use each and every access port 17
3.2 Ensuring that no new unauthorized device (MAC) is added to the network 34
3.3 Using MAC Security to tie down Server MACs using Active/Standby NICs 49
3.4 Achieving MAC based VLANs using MAC Security 63
4. Auto-Learning with MaxMacs example 74
4.1 Ensuring that every access port is used by one and only one device 74
5. Auto-Learning with Sticky-MAC example 86
5.1 MAC Security without having to pre-provision ports when new devices added 86

Figures

Figure 1: Base setup 12
Figure 2: Regular MAC Security; example 1 17
Figure 3: Example 1; unauthorized MAC on non-provisioned port 26
Figure 4: Example 1; unauthorized MAC on provisioned port 28
Figure 5: Example 1; unauthorized MAC sharing connection with authorized MAC 30
Figure 6: Example 1; unauthorized MAC moving to a different port 32
Figure 7: Regular MAC Security; example 2 34
Figure 8: Example 2; a new device is added to the network 43
Figure 9: MAC-Security with Active-Standby NICs; example 3 49
Figure 10: Example 3; servers switch over to Backup NIC 60
Figure 11: Example 3; unauthorized device takes server Standby NIC connection 61
Figure 12: VLAN based MAC-Security; example 4 63
Figure 13: Example 4; unauthorized MAC 70
Figure 14: Example 4; authorized MACs in wrong VLAN 72
Figure 15: Auto-Learning with MaxMacs; example 5 74
Figure 16: Example 5; an unauthorized hub/switch is connected to the network 83
Figure 17: Example 5; an unauthorized WLAN AP is connected to the network 84
Figure 18: MAC Security without any provisioning of new devices; example 6 86
Figure 19: Example 6; a new device is added to the network 97
Figure 20: Example 6; unauthorized MAC on provisioned port 101
Figure 21: Example 6; unauthorized MAC sharing connection with authorized MAC 103
Figure 22: Example 6; unauthorized MAC moving to a different port 106

Tables

Table 1: MAC Security support across Avaya switch family types 7
Table 2: MAC Security capability vs. mode matrix 10
Table 3: MAC Security config commands vs. mode matrix 11

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 Lucida Console font:

```
ERS5520-48T# show sys-info

Operation Mode:         Switch
MAC Address:            00-12-83-93-B0-00
PoE Module FW:          6370.4
Reset Count:            83
Last Reset Type:        Management Factory Reset
Power Status:           Primary Power
Autotopology:           Enabled
Pluggable Port 45:      None
Pluggable Port 46:      None
Pluggable Port 47:      None
Pluggable Port 48:      None
Base Unit Selection:    Non-base unit using rear-panel switch
sysDescr:               Ethernet Routing Switch 5520-48T-PWR
                        HW:02       FW:6.0.0.10  SW:v6.2.0.009
                        Mfg Date:12042004    HW Dev:H/W rev.02
```

1. Introduction

The MAC Security feature offers a number of different ways to restrict access to the network based on the sender's MAC address as well as the number of source MACs seen on the ethernet access port.

The ERS stackables MAC Security feature dates back from the Baystack BaySecure which originally supported the basic static MAC security mode as well as an Auto-Learning mode which was later enhanced with the addition of a Sticky MAC support.

The following list provides a breakdown per switch family in terms of additional MAC Security components and starting from which software version they first became available:

ERS 5000

```
4.2.0   SW      MAC Security Static & Auto-Learning
6.2.0   SW      MAC Security port lock-out enhancement
6.2.0   SW      MAC Security Auto-Learning Sticky MAC Address
```

ERS 4000

```
5.0.0   SW      MAC Security Static & Auto-Learning
5.2.2   SW      MAC Security Auto-Learning Sticky MAC Address
5.4.0   SW      MAC Security Auto-Learning Sticky MAC Address
```

ERS 3500

```
5.0.0   SW      MAC Security Static & Auto-Learning & Sticky MAC Address
```

ERS 2500

```
4.0.0   SW      MAC Security Static
4.2.0   SW      MAC Security Auto-Learning
4.4.0   SW      MAC Security Auto-Learning Sticky MAC Address
```

VSP 7000

```
10.2.0  SW      MAC Security Static & Auto-Learning & Sticky MAC Address
10.2.0  SW      MAC Security port lock-out enhancement
```

Table 1: MAC Security support across Avaya switch family types

This document will focus on the full capabilities of the MAC Security feature regardless of stackable switch family type (i.e. assuming a software release greater or equal to the last one shown in the list above).

First and foremost it is necessary to clarify the various modes and options available. There are essentially three useful ways to use the MAC Security feature:

1. **Regular MAC Security** where a list of allowed MAC addresses is configured against either individual ethernet ports or security lists (which constitute a set of ethernet ports).
   There is no limit to how many MACs can be assigned to a given port, the only limit being that a maximum of 448 MAC can be configured in the MAC Security MAC table.
   If a packet is then received on a MAC Security enabled port with a source MAC address which is not in the list of allowed MAC addresses for that port (or security list) this will trigger a violation and the packet will be discarded.
   The list of authorized MAC addresses can be manually configured and/or updated at any time.
   It is also possible to populate the authorized MAC addresses list for a given port by temporarily suspending MAC Security and activating the Learning mode on selected ports for one-shot learning. However, currently there is no way to leverage Learning against Security-Lists.
   Either way, when a new ethernet access port is to be used, populating the allowed MACs for that

port will require intervention by the network administrator.

2. **Auto-Learning with MaxMacs** where the switch allows learned MAC addresses up to a specified maximum enforced on the ports with MAC Security enabled. This mode works by permanently enabling the Auto-Learning functionality on the ethernet ports and automatically recording every new MAC address seen on the port. If a new MAC address is seen on the port and the number of authorized MAC addresses on the port was already reached this will trigger a violation and the packet arriving with the new MAC address will be discarded.
   The number of allowed MAC addresses which can be defined on the ethernet ports can be set to a value ranging between 1 and 25.
   Note that this mode does not authorize any particular MAC address, it simply ensures connectivity for the 1st X (where X = 1..25) MAC addresses learnt on the port. Also note that the list of recorded MAC addresses is a dynamic list which means entries can age out and do get cleared against ports which are bounced (cable disconnected and re-connected) as well as flushed when the switch is rebooted (MAC addresses learnt by Auto-Learning are not saved to the config file). Hence if the switch is rebooted or ports are bounced, it is likely that a different set of MAC addresses will be allowed on the port depending on the order in which these get learnt. In summary, this mode may or may not be applicable depending on if you wish to allow or not allow new MACs on a port upon a reboot or port bounce.
   In this mode a device can easily move ports as its MAC address will automatically get re-learnt on the new port by the Auto-Learning mode (just as happens for the regular MAC table / FDB).

3. **Auto-Learning with Sticky-Mac** which is just like the previous flavor, in that Auto-Learning and a maximum number of allowed MACs are configured on the ethernet ports, except that now once a MAC address is seen it is made “sticky” to the port where it was seen and automatically saved to the config file.
   Like the previous mode, if a new MAC address is seen on the port and the number of authorized MAC addresses on the port was already reached this will trigger a violation and the packet arriving with the new MAC address will be discarded.
   Unlike the previous mode, there is no aging of the Sticky-MACs and once the number of allowed MACs has been learnt on a port, those MAC addresses will be the only MAC addresses allowed on that port even if the port is bounced or the switch is restarted. Also, unlike the previous mode, devices cannot move from one ethernet port to another. In summary, the MAC is locked to the original port and an intrusion event will be generated if the same MAC appears on another port. If the network administrator wished the MAC address to be moved to another port, the address must be deleted from the original port location. .
   So this mode is essentially similar to the regular MAC Security mode in that it only allows access to certain MAC addresses on the MAC Security enabled ports. It diverges from that mode in two ways:
   a. No initial provisioning is required when a new access port is to be used; the allowed MACs will be Auto-Learned as the 1st device(s) is/are attached
   b. It is not possible to use Security-Lists in this mode

In all 3 modes above, the packets with an offending source MAC will be discarded and will trigger a violation. Upon a violation it is possible to define additional security actions. These can be specified as any combination of the following actions:

- No additional action
- Generate a Trap
- Partition the Port

Under EDM these options are globally specified as follows:

Note – DA-Filtering is an additional MAC Security functionality which, once enabled, is permanent to all MAC Security enabled ports (i.e. it does not only apply when a violation is triggered as could be implied from the EDM Security Action configuration dialog above). With DA-Filtering it is possible to specify a list of up to 10 MAC addresses to which packets originating from a MAC Security port are not allowed to send traffic to. The offending traffic is simply dropped without triggering any violation. This feature is historic and there is no useful application for this capability in its present form, hence this is not covered any further in this document.

It should be noted that while an unauthorized device will never be allowed to send traffic into the network (as its source MAC is blocked) the device can still receive traffic from the network which means the unauthorized device is able to see broadcast and unknown traffic within the VLAN it is connected to. If this is deemed to be unsecure, then the port should be partitioned by setting the corresponding Security Action.

The following table tries to summarize the distinctive characteristics of each of the above 3 modes.

Mode Feature	**Regular MAC Security**	**Auto-Learning with MaxMacs**	**Auto-Learning with Sticky-Mac**
Ability to authorize only manually configured MACs	Yes	No	No
Ability to assign authorized MACs to Security lists instead of ports	Yes	No	No
Ability to authorize only 1 MAC per port	Yes	Yes (with MacMACs = 1; but cannot control what that MAC will be)	Yes (with MacMACs = 1)
Ability to authorize only 1 MAC across 2 or more ports	Yes (using Security-lists)	No, any single MAC will be allowed to move ports	No
Ability to authorize more than 1 MAC per port	Yes (unlimited)	Yes (25 Max; but cannot control what those MACs will be)	Yes (25 max)
Discard packets from unauthorized device/MAC	Yes	Yes	Yes
Prevent unauthorized device from receiving VLAN traffic	Yes (with Security Action set to Partition)	Yes (with Security Action set to Partition)	Yes (with Security Action set to Partition)
Limit the number of devices allowed to use an ethernet	No	Yes	No

port (regardless of their MAC address)			
Ability to alert/shutdown a port when more than X MAC addresses are learnt on the port	No	Yes (using trap/partition Security-Action)	Yes (using trap/partition Security-Action)
Ability to generate an alert (Log message + Trap) upon a security violation	Yes	Yes	Yes
Ability to partition the port upon a security violation	Yes	Yes	Yes
Ability to learn authorized MACs during controlled one-shot learning	Yes (but not with Security-lists)	No	No
Ability to limit the number of authorized MACs on a port	Yes (implied by the number of MACs added to the port's authorized list)	Yes (by setting MaxMac)	Yes (by setting MaxMac)
Intervention required when a new access port is used	Yes (authorized MACs for the port need to be added or Learned; or port needs to be added to an existing security-list)	No	No (authorized MACs will be automatically learned)
A MAC can be authorized to move across any MAC Security enabled port	No	Yes	No
A MAC can be authorized to move across a specified range of MAC Security enabled ports	Yes (using a Security-List)	No	No
List of authorized MACs is saved to config and preserved upon switch restart	Yes	No	Yes

Table 2: MAC Security capability vs. mode matrix

The table below attempts to clarify which CLI commands are relevant to each of the above modes. Commands which are not listed for a given mode are not to be used for that mode.

Mode / Context	Global config commands	Interface config commands
Common to all 3 modes	***mac-security enable|disable*** ***[no] mac-security snmp-trap*** ***mac-security intrusion-detect forever|enable|disable*** ***mac-security intrusion-timer <0-65535>*** ***mac-security snmp-lock enable|disable***	***mac-security enable|disable*** ***[no] mac-security lock-out***
Regular MAC Security	***[no] mac-security security-list <list> <ports>*** ***mac-security mac-address-table address <MAC> port <port>*** ***mac-security mac-address-table address <MAC> security-list <list>*** ***mac-security learning enable|disable*** ***mac-security learning-ports <ports>***	***[no] mac-security learning***
Auto-Learning with MaxMacs		***mac-security auto-learning enable|disable max-addrs <X>***
Auto-Learning with Sticky-Mac	***[no] mac-security auto-learning sticky*** ***mac-security mac-address-table sticky-address <MAC> port <port>***	***mac-security auto-learning enable|disable max-addrs <X>***

Table 3: MAC Security config commands vs. mode matrix

This document will use some real life examples where each of the above modes can be used.

Note that another option for authenticating devices by MAC address is Non-EAP (NEAP) authentication whereby source MAC addresses are authenticated against a centralized RADIUS Server. NEAP was designed for network environments where 802.1X EAP is deployed for network access control in order to allow non-EAP devices, such as a printer or security camera which lacked the 802.1X supplicant. Although not explored as part of this configuration guide, NEAP is another option for authenticating connecting devices based on MAC Address.

2. Base configuration setup

All the examples covered use the same base configuration setup shown in the following figure.

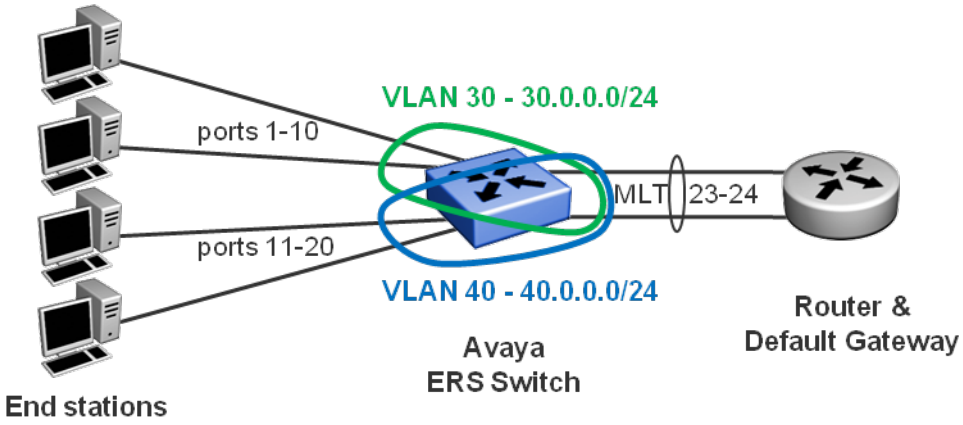


Figure 1: Base setup

For simplicity the Avaya ERS Switch is configured as a simple access layer 2 switch with no IP routing. A separate IP router acts as default gateway for the end stations. However the same configuration examples covered in this document would also work in configurations where the Avaya ERS Switch is acting as an IP router.

End stations communicate over VLAN 30, or VLAN 40, which are port based VLANs configured across access ports as well as the uplinks towards the distribution layer IP router acting as default gateway for the end stations.

Note that the Avaya ERS switch does not have any IP address on VLAN 30 or VLAN 40. The management IP address of the Avaya ERS Switch would be on a separate management VLAN only present on the uplink towards the distribution layer router (VLAN 47 on this setup, not shown in diagram).

Base configuration for Avaya ERS Switch for VLAN 30 and access ports

```
snmp-server enable
snmp-server name "Avaya-ERS-Switch"
ip default-gateway 47.162.221.1
ip address switch 47.162.221.48
ip address netmask 255.255.255.128
vlan create 30,40,47 type port 1
vlan ports 23-24 tagging tagAll
vlan configcontrol flexible
vlan members 1 NONE
vlan members 30 1-10,23-24
vlan members 40 11-20,23-24
vlan members 47 23-24
vlan ports 1-10 pvid 30
vlan ports 11-20 pvid 40
```

```
vlan ports 23-24 pvid 47
vlan configcontrol automatic
mlt 1 name "Trunk #1" enable member 23-24
interface FastEthernet ALL
   spanning-tree port 1-20 learning fast
   spanning-tree port 23-24 learning disable
exit
vlan mgmt 47
mlt spanning-tree 1 stp 1 learning disable
```

2.1 Ensuring MAC Security can never accidentally be enabled on uplinks

The MAC Security feature is only intended as a feature to enable on access ports. Accidentally enabling the feature on the edge switch uplinks can have serious consequences which might end up rendering the edge switch isolated from the rest of the network.

To prevent this from happening, the ERS5000 and VSP7000 have a MAC Security port lock-out feature which can be enabled on the switch uplink ports so that they will never enable or accept any MAC Security related configuration. In our setup we would enable port lock-out on our MLT uplink ports 23&24.

2.1.1 Using ACLI

Enable Port lock-out for MLT uplink ports 23-24

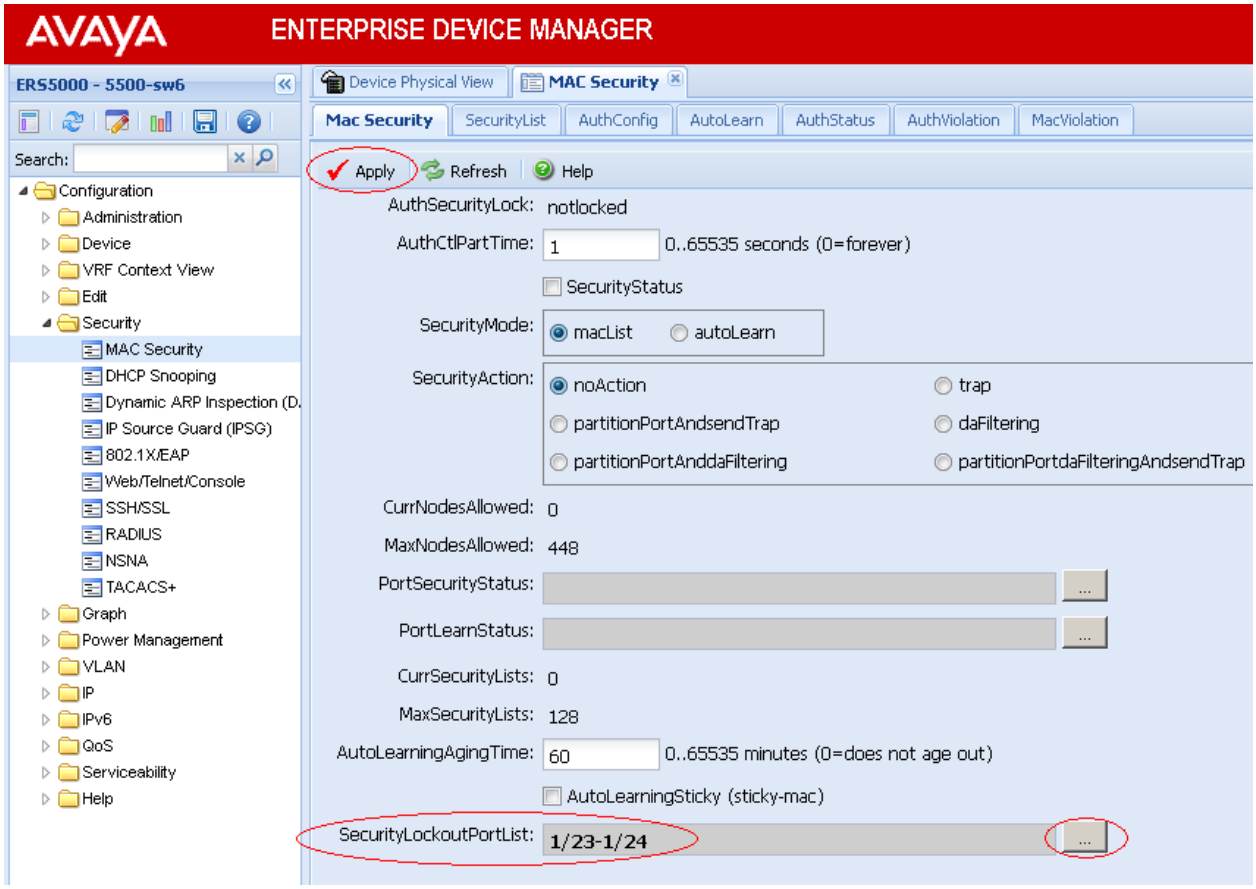
```
Avaya-ERS-Switch(config)# interface FastEthernet 23-24
Avaya-ERS-Switch(config-if)# mac-security lock-out
Avaya-ERS-Switch(config-if)# exit
```

Checking Port lock-out for MLT uplink ports 23-24

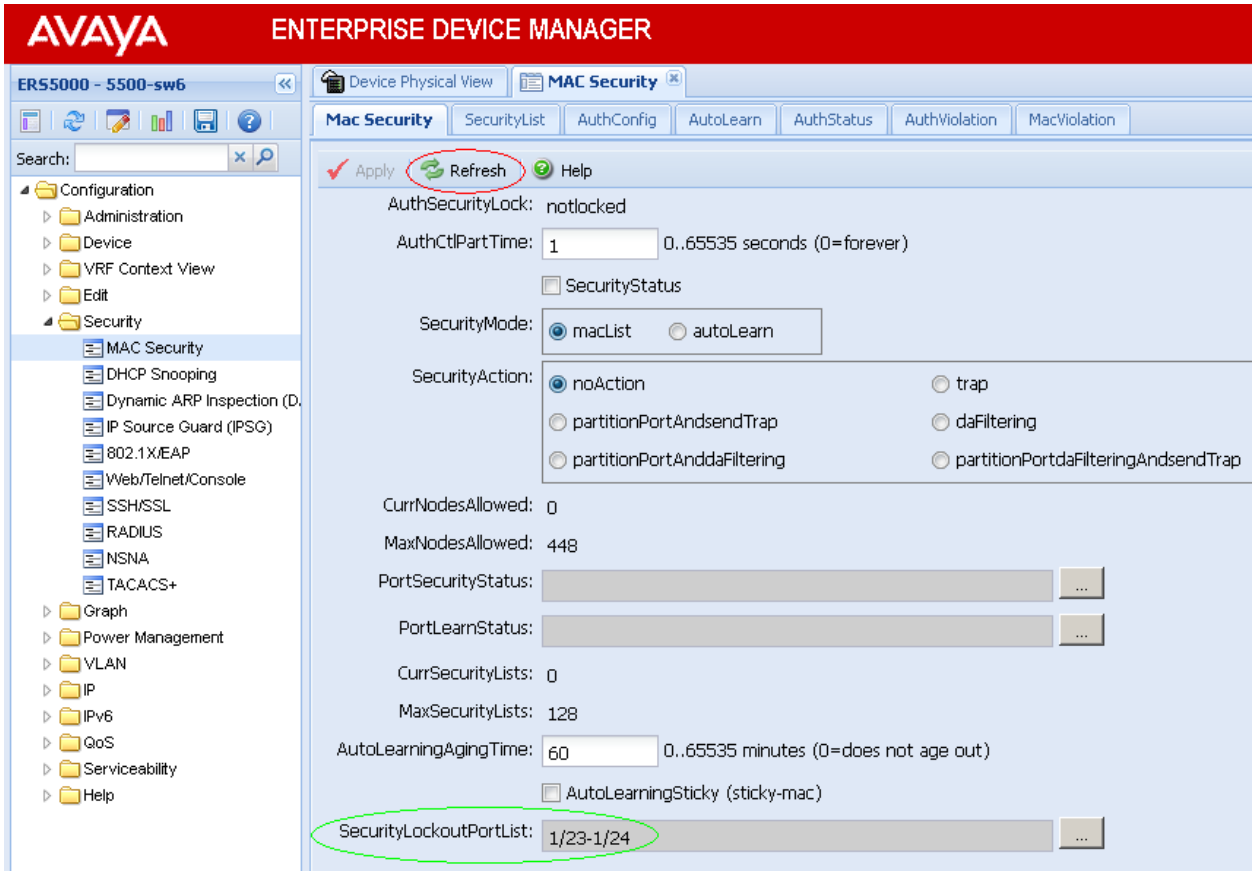
```
Avaya-ERS-Switch# show mac-security port 23-24
Port  Trunk  Security  Auto-Learning  MAC Number Security Locked-out
----  -----  --------  -------------  ---------- ------------------
  23         Disabled     Disabled        2       Enabled
  24         Disabled     Disabled        2       Enabled
```

2.1.2 Using EDM

Enable Port lock-out for MLT uplink ports 23-24



Checking Port lock-out for MLT uplink ports 23-24



2.2 Disabling SNMP write access just for MAC Security configuration

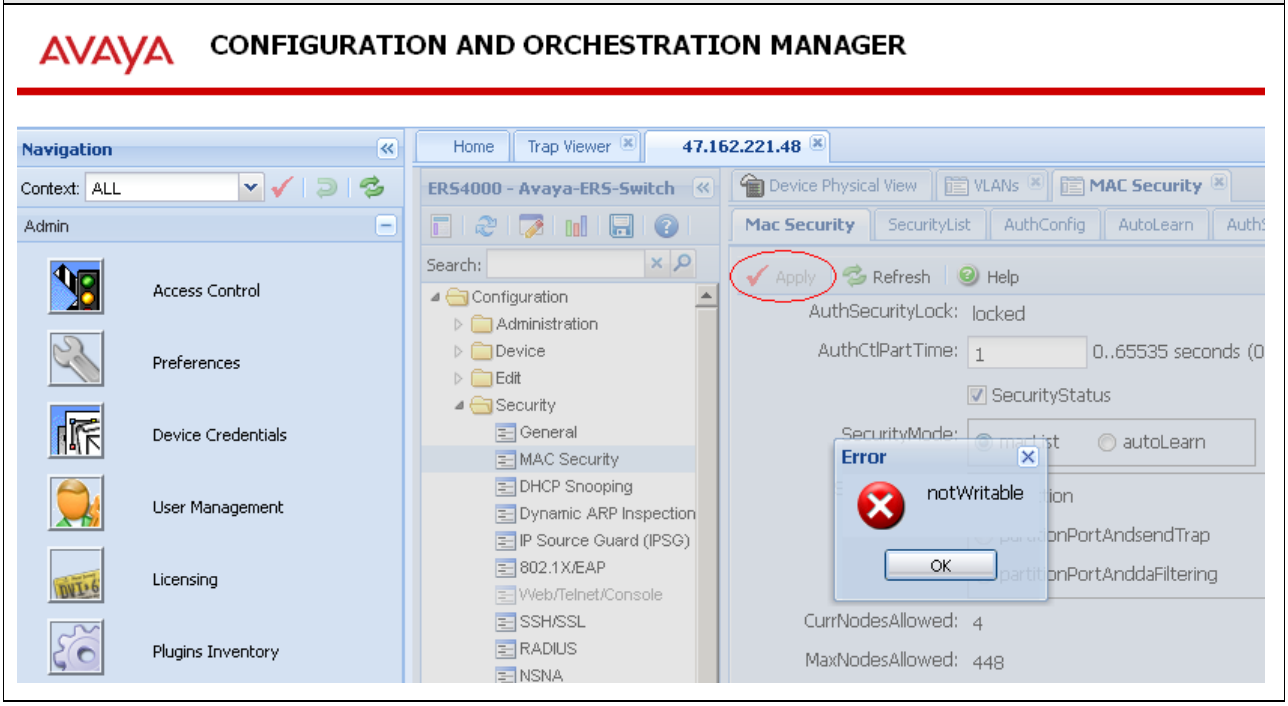
This document covers both ACLI and EDM for configuring each of the examples covered in the sections to come. However, in some environments it may be desirable to only allow control of the MAC Security feature from the ACLI of the switch. To achieve this, MAC Security has the capability to apply an SNMP-lock to the feature.

Disable all SNMP write access to the MAC Security functionality

```
Avaya-ERS-Switch(config)# mac-security snmp-lock enable
```

Now it will no longer be possible to modify MAC-Security from EDM (via COM); any attempt to do so will result in an error; however the MAC Security configuration can still be viewed from COM.

An attempt to now modify the MAC Security config via COM



However, in the case of EDM web-access directly to the switch IP address, it is still possible to modify the MAC Security configuration. Web access on the switch would in any case need to be disabled for security reasons.

Disable web access (HTTP & HTTPS) to the switch (EDM on-box)

```
Avaya-ERS-Switch(config)# web-server disable
```

3. Regular MAC Security examples

3.1 Controlling exactly which MAC is allowed to use each and every access port

In this example, typically favored by the military, every access port is manually configured to allow 1 and only 1 device (and hence MAC address). Before a new device can be added to the network the network administrator must manually add the new MAC address to its allocated access ethernet port's authorized MAC list. In the event of a non-authorized MAC address attempting to send traffic into the network a trap will be sent to the management station and the unauthorized device will not be allowed to send traffic into the network.

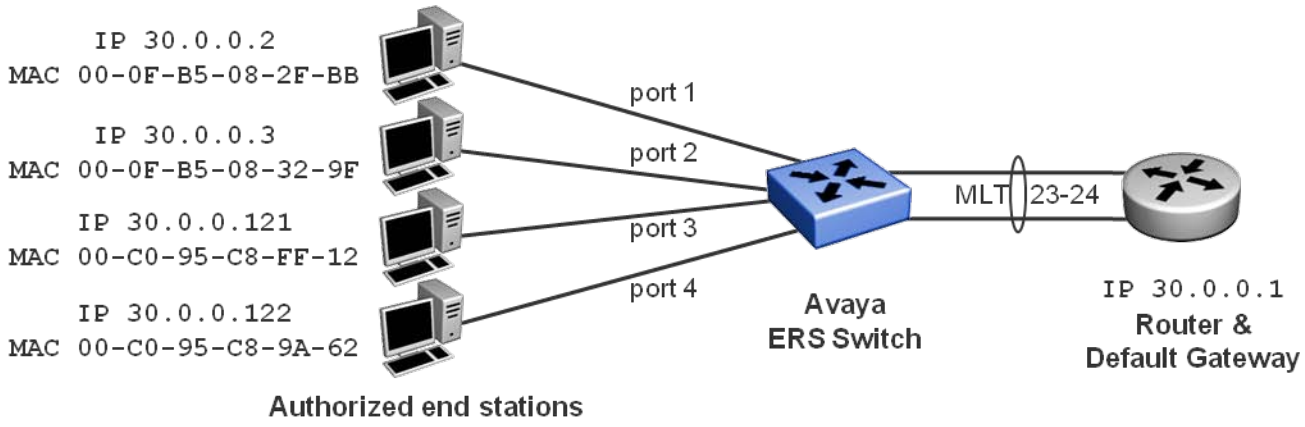


Figure 2: Regular MAC Security; example 1

3.1.1 Using ACLI

3.1.1.1 Initial Switch configuration

Globally enable MAC Security
`Avaya-ERS-Switch(config)#` ***`mac-security enable`***
Enable MAC Security on the access ports
`Avaya-ERS-Switch(config)#` ***`interface FastEthernet 1-20`*** `Avaya-ERS-Switch(config-if)#` ***`mac-security enable`*** `Avaya-ERS-Switch(config-if)#` ***`exit`***
On older software versions you can enable traps upon violation; in more recent software versions the traps are automatically generated and this command no longer exists
`Avaya-ERS-Switch(config)#` ***`mac-security snmp-trap`***

3.1.1.2 Provisioning authorized users

Assign authorized MACs to respective access ports

```
Avaya-ERS-Switch(config)# mac-security mac-address-table address 00-0F-B5-08-2F-BB port 1
Avaya-ERS-Switch(config)# mac-security mac-address-table address 00-0F-B5-08-32-9F port 2
Avaya-ERS-Switch(config)# mac-security mac-address-table address 00-C0-95-C8-FF-12 port 3
Avaya-ERS-Switch(config)# mac-security mac-address-table address 00-C0-95-C8-9A-62 port 4
```

3.1.1.3 Checking MAC Security operational status

Verify that MAC Security is globally enabled

```
Avaya-ERS-Switch# show mac-security config
MAC Address Security: Enabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
MAC Auto-Learning Age-Time:  60 minutes
MAC Auto-Learning Sticky Mode: Disabled
Current Learning Mode: Disabled
Learn by Ports: NONE
```

Verify that MAC Security is enabled on the access ports

```
Avaya-ERS-Switch# show mac-security port
Port  Trunk  Security  Auto-Learning  MAC Number
----  -----  --------  -------------  ----------
   1         Enabled      Disabled        2
   2         Enabled      Disabled        2
   3         Enabled      Disabled        2
   4         Enabled      Disabled        2
   5         Enabled      Disabled        2
   6         Enabled      Disabled        2
   7         Enabled      Disabled        2
   8         Enabled      Disabled        2
   9         Enabled      Disabled        2
  10         Enabled      Disabled        2
  11         Enabled      Disabled        2
  12         Enabled      Disabled        2
  13         Enabled      Disabled        2
```

```
  14          Enabled      Disabled        2
  15          Enabled      Disabled        2
  16          Enabled      Disabled        2
  17          Enabled      Disabled        2
  18          Enabled      Disabled        2
  19          Enabled      Disabled        2
  20          Enabled      Disabled        2
  21          Disabled     Disabled        2
  22          Disabled     Disabled        2
  23    1     Disabled     Disabled        2
  24    1     Disabled     Disabled        2
```

Verify the authorized MAC addresses appear in the MAC Security MAC table

```
Avaya-ERS-Switch# show mac-security mac-address-table
Number of addresses: 4

Unit Port Allowed MAC Address   Type
---- ---- ------------------- ---------
0    1    00-0F-B5-08-2F-BB   Static
0    2    00-0F-B5-08-32-9F   Static
0    3    00-C0-95-C8-FF-12   Static
0    4    00-C0-95-C8-9A-62   Static

Security List Allowed MAC Address   Type
------------- ------------------- ---------
```

Verify the FDB on the switch

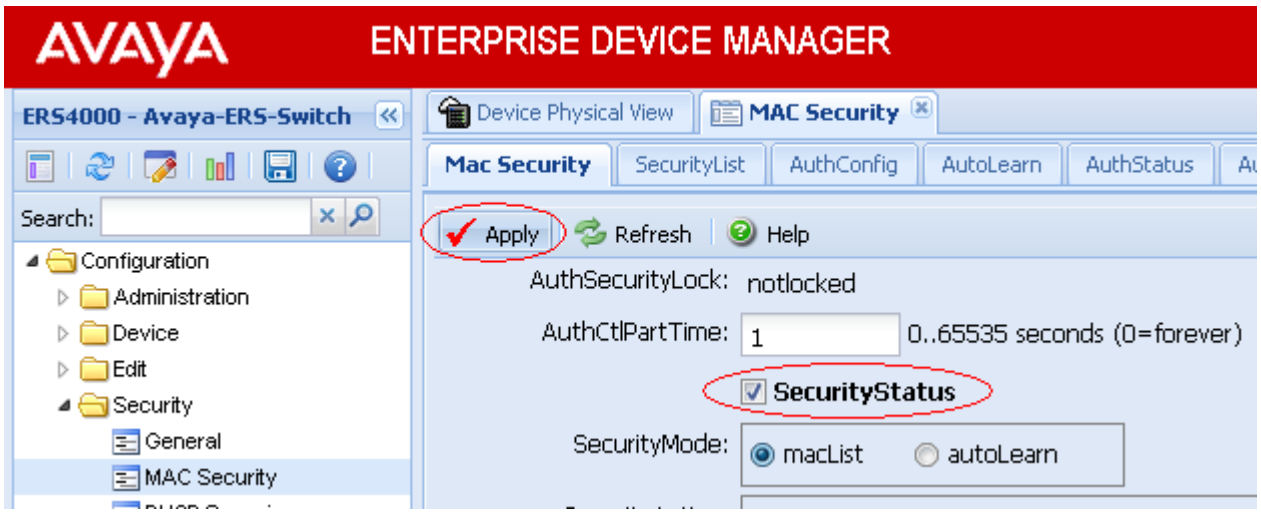
```
Avaya-ERS-Switch# show mac-address-table vid 30
Mac Address Table Aging Time: 300
Learning Enabled Ports 1-26
Number of addresses: 5

   MAC Address    Vid   Type   Source
----------------- ---- ------- -------
00-0F-B5-08-2F-BB   30 Dynamic Port: 1
00-0F-B5-08-32-9F   30 Dynamic Port: 2
```

```
00-C0-95-C8-9A-62   30 Dynamic Port: 4
00-C0-95-C8-FF-12   30 Dynamic Port: 3
00-E0-16-57-6E-81   30 Dynamic Trunk:1
```

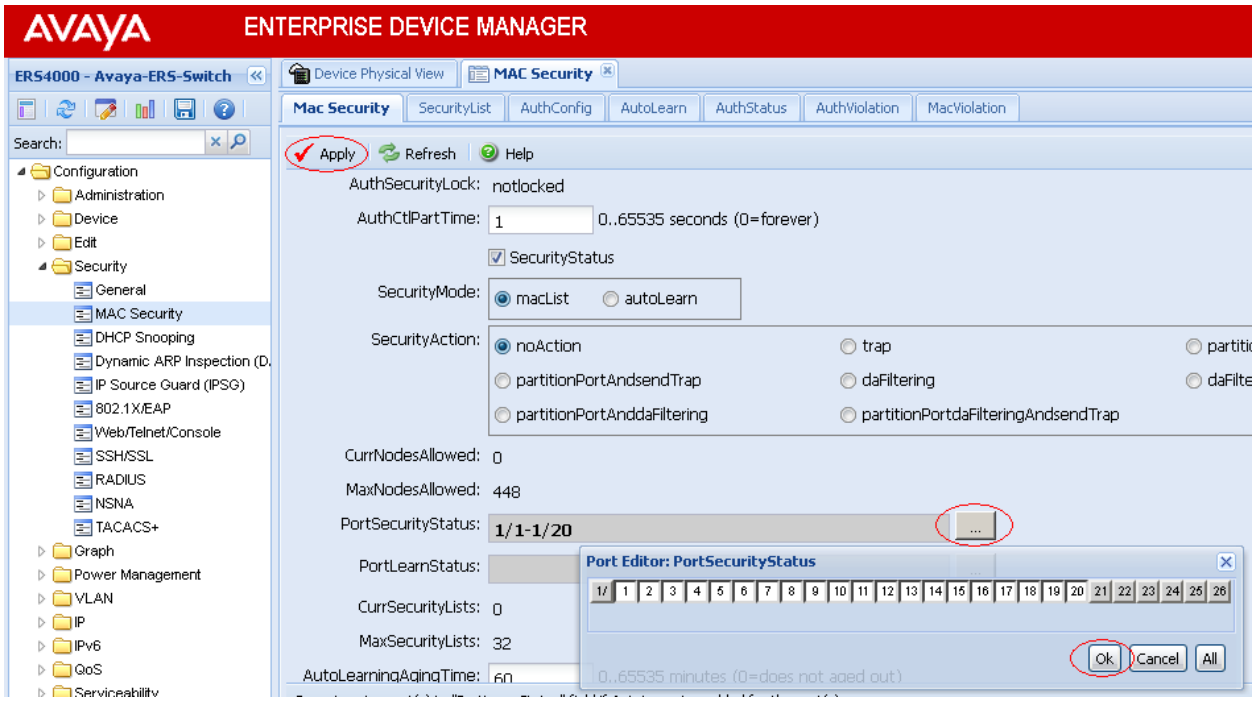
3.1.2 Using EDM

3.1.2.1 Initial Switch configuration

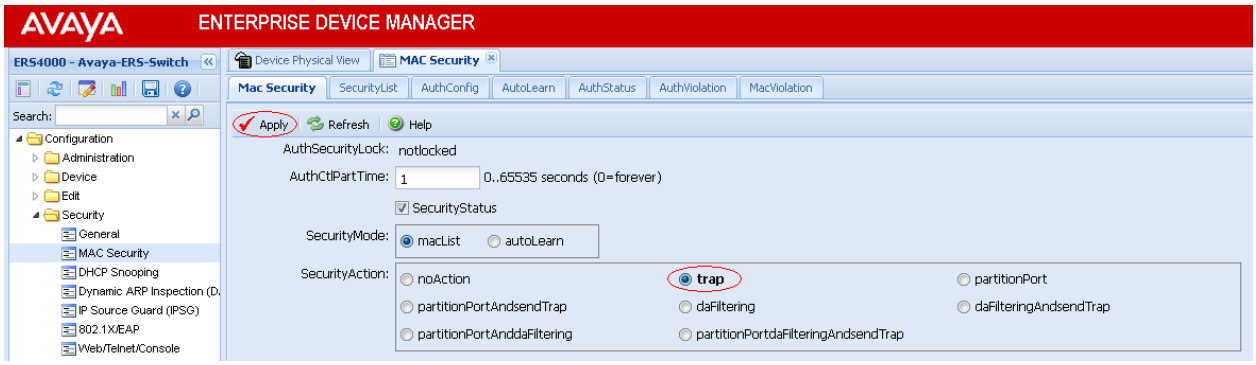
Globally enable MAC Security



Enable MAC Security on the access ports

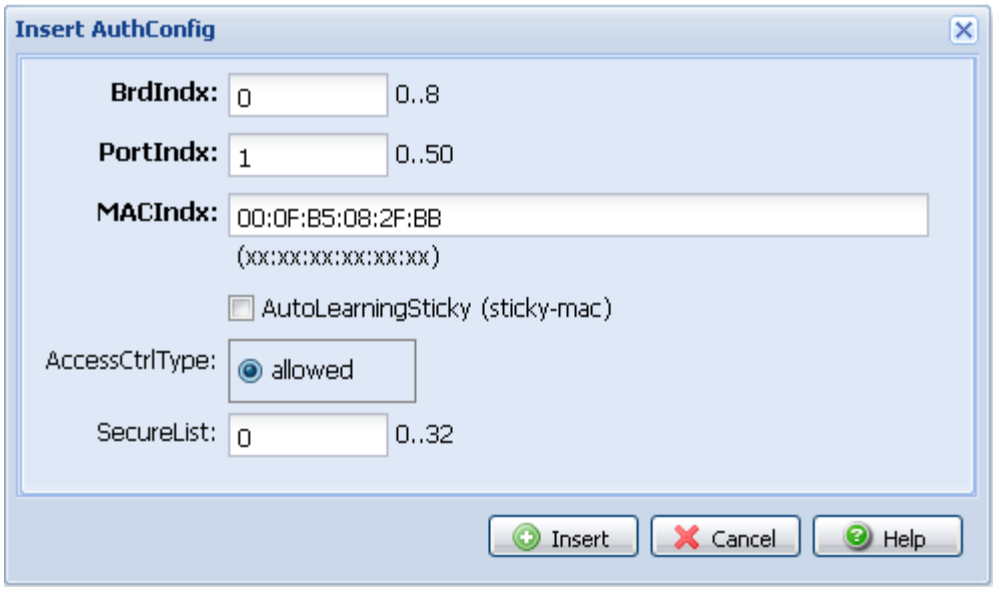


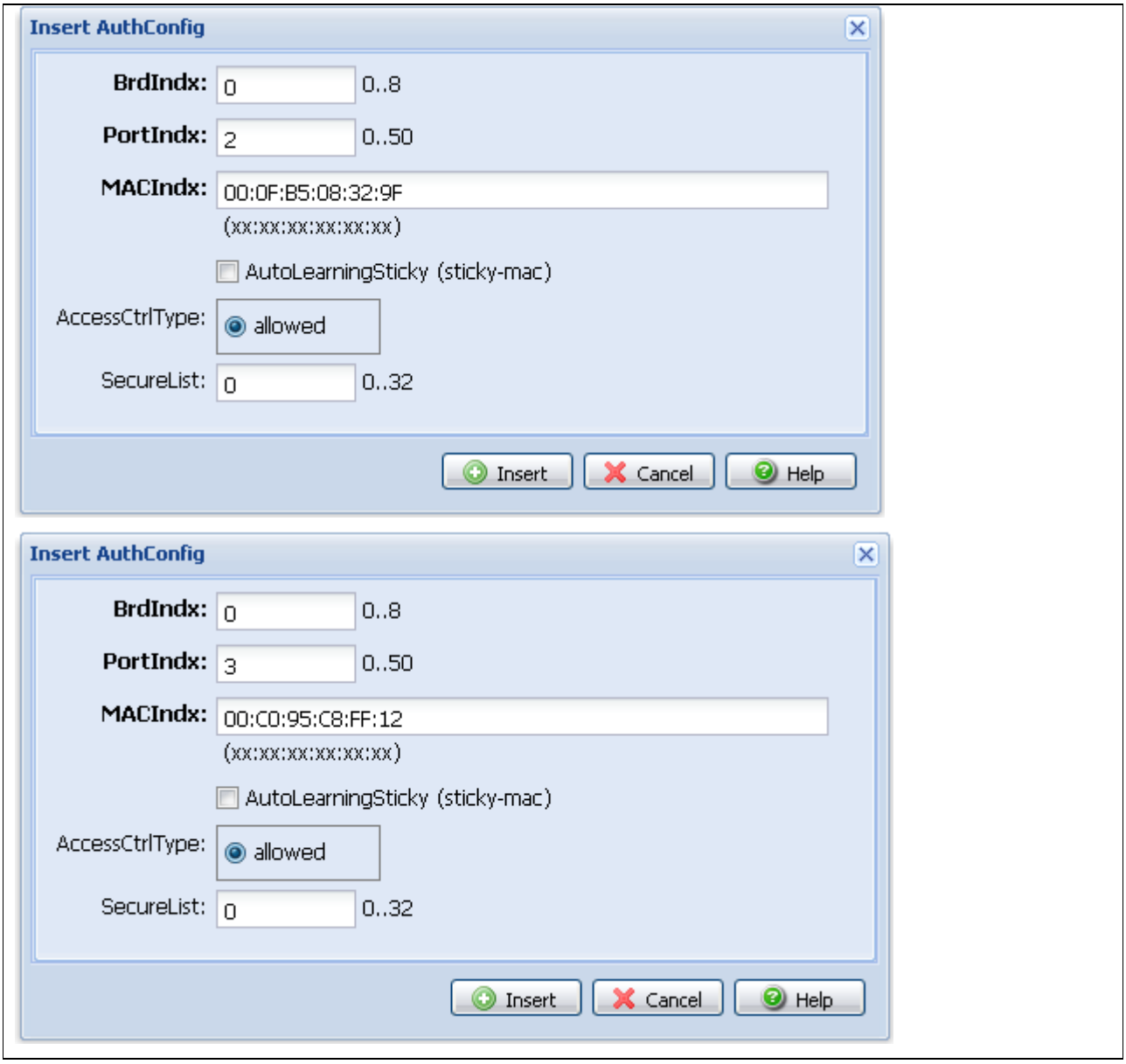
Enable traps upon violation

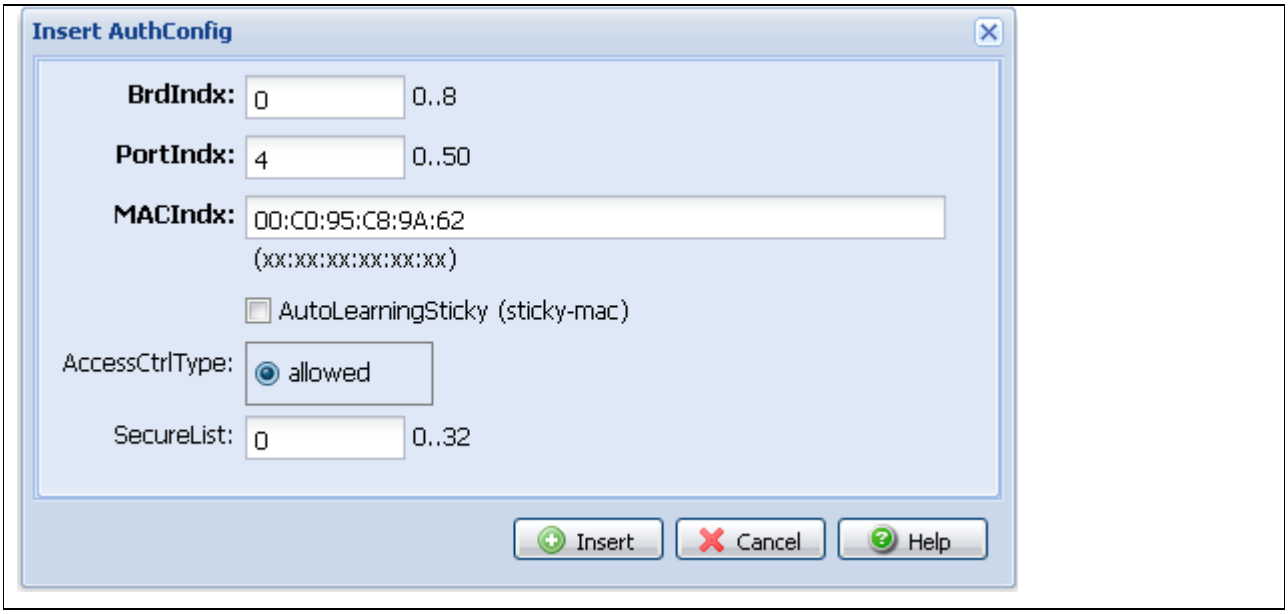


3.1.2.2 Provisioning authorized users

Assign authorized MACs to respective access ports

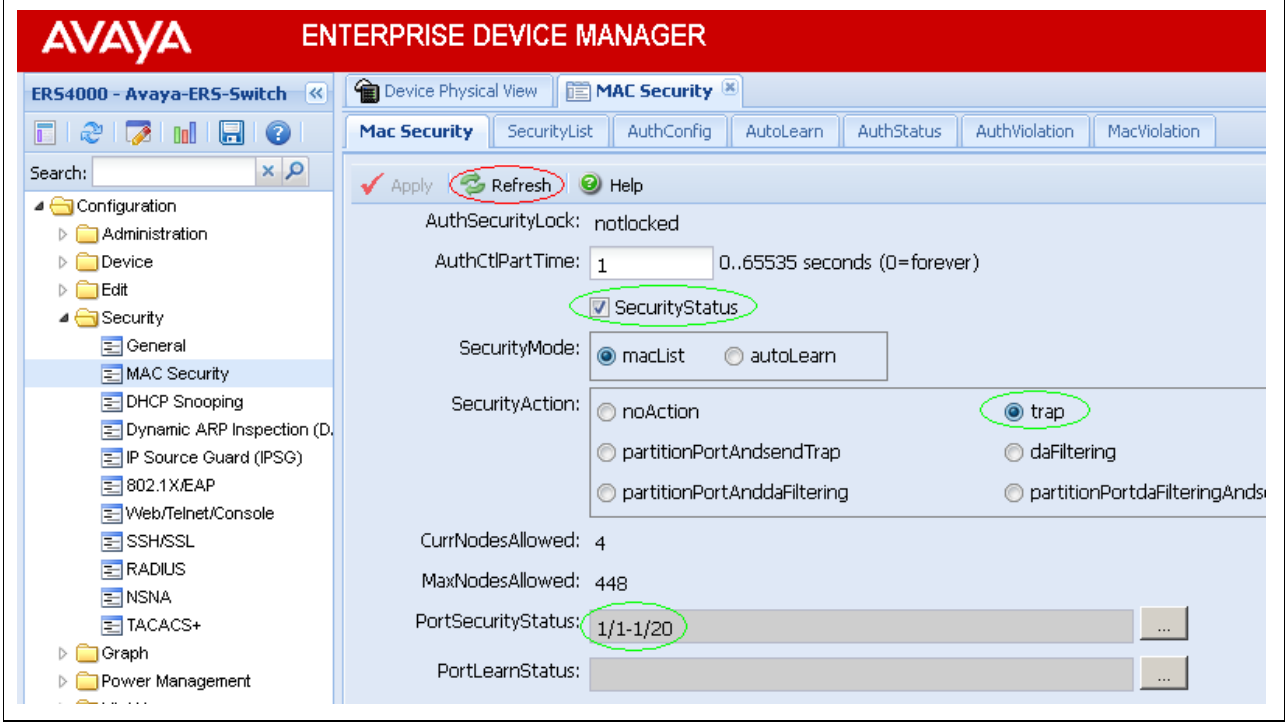



Insert AuthConfig
BrdIndx: 0 0..8
PortIndx: 2 0..50
MACIndx: 00:0F:B5:08:32:9F
(xx:xx:xx:xx:xx:xx)
AutoLearningSticky (sticky-mac)
AccessCtrlType: allowed
SecureList: 0 0..32
Insert
Cancel
Help
Insert AuthConfig
BrdIndx: 0 0..8
PortIndx: 3 0..50
MACIndx: 00:C0:95:C8:FF:12
(xx:xx:xx:xx:xx:xx)
AutoLearningSticky (sticky-mac)
AccessCtrlType: allowed
SecureList: 0 0..32
Insert
Cancel
Help

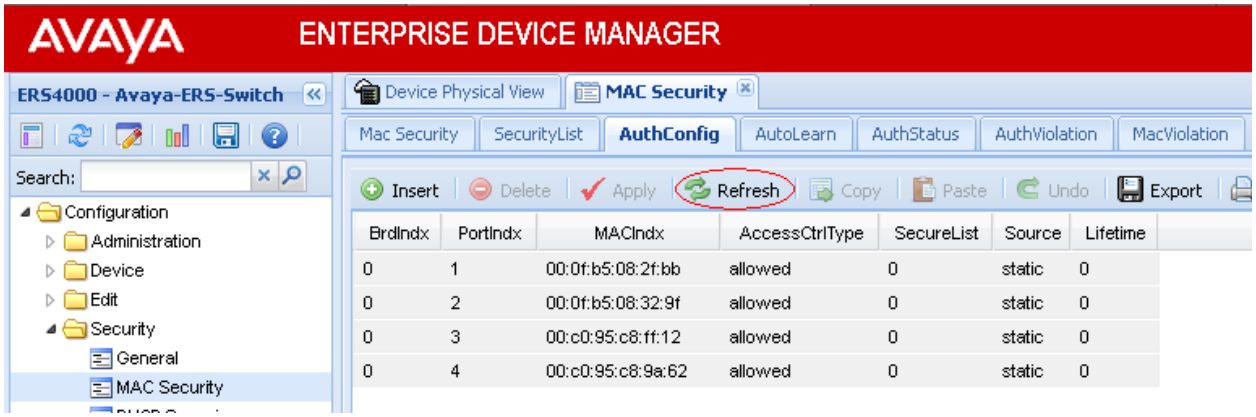


3.1.2.3 Checking MAC Security operational status

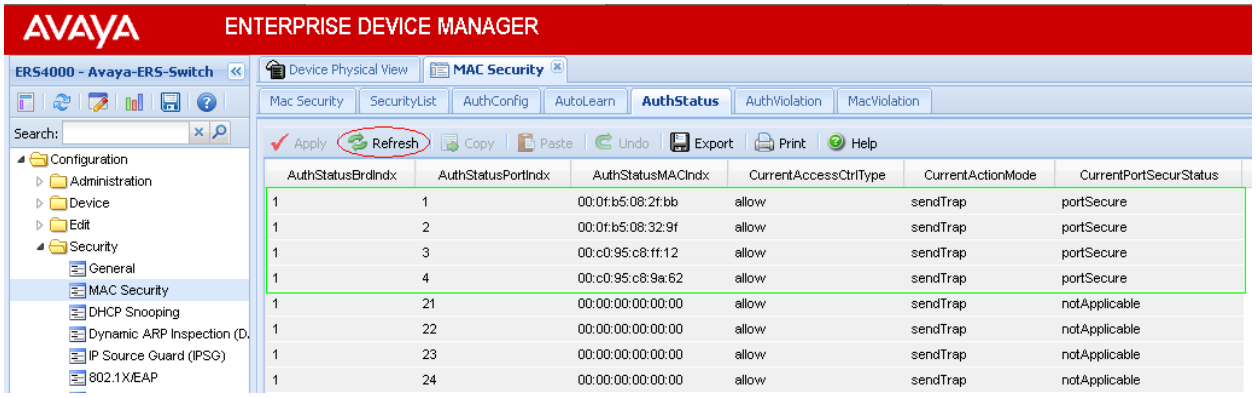
Verify that MAC Security is globally enabled and on access ports



Verify the authorized MAC addresses appear in the MAC Security MAC table



Verify ports 1-4 are authenticated with the correct MAC address



3.1.3 Verifying user connectivity

Verify IP connectivity between the Router and the end stations

```
Router#% ping 30.0.0.2; ping 30.0.0.3; ping 30.0.0.121; ping 30.0.0.122
30.0.0.2 is alive
30.0.0.3 is alive
30.0.0.121 is alive
30.0.0.122 is alive
```

3.1.4 Testing violations

3.1.4.1 Unauthorized MAC on non-provisioned port

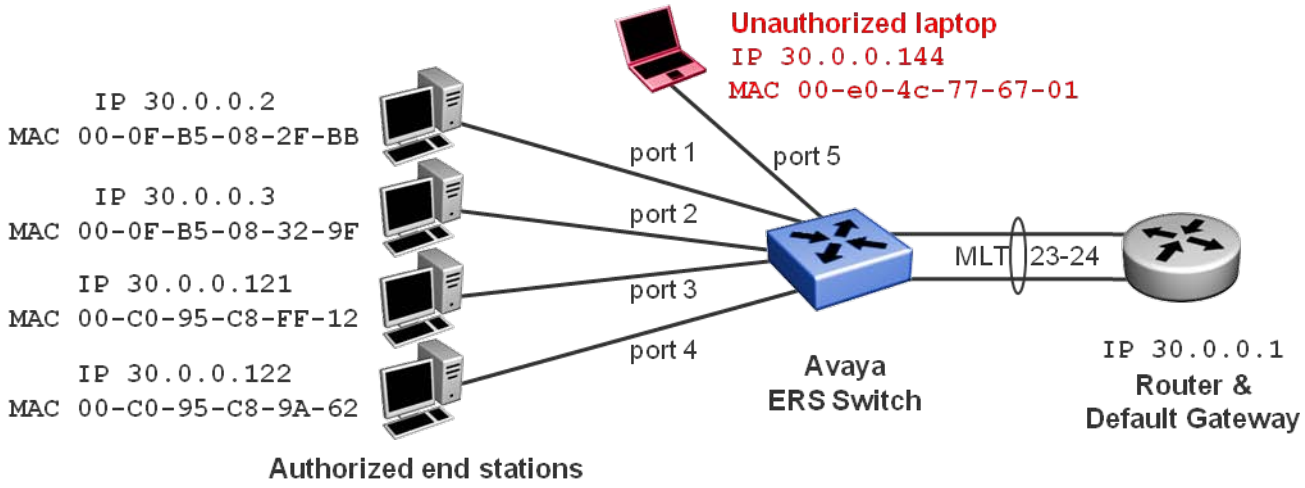


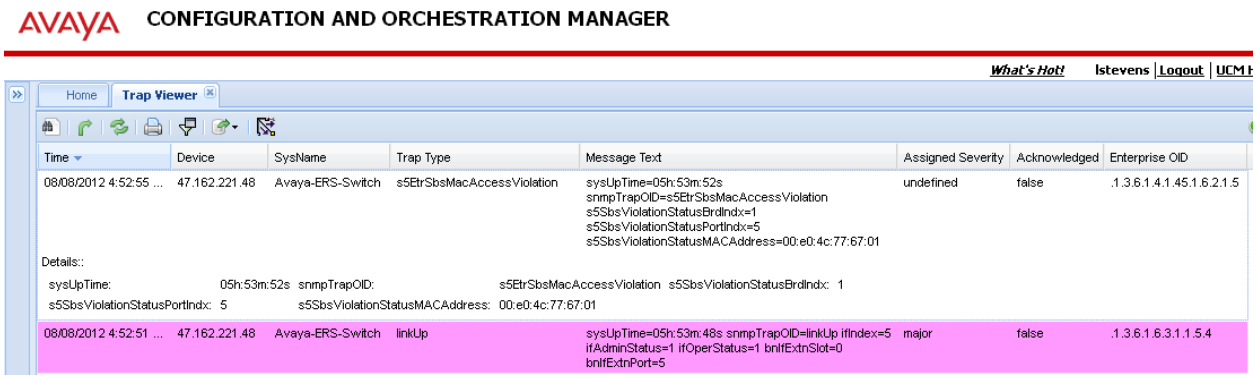
Figure 3: Example 1; unauthorized MAC on non-provisioned port

The unauthorized device is not able to send any traffic into the network; however it is still able to see broadcast and unknown traffic flowing in the VLAN; if this is undesired the MAC Security should be configured to partition the port upon an access violation.

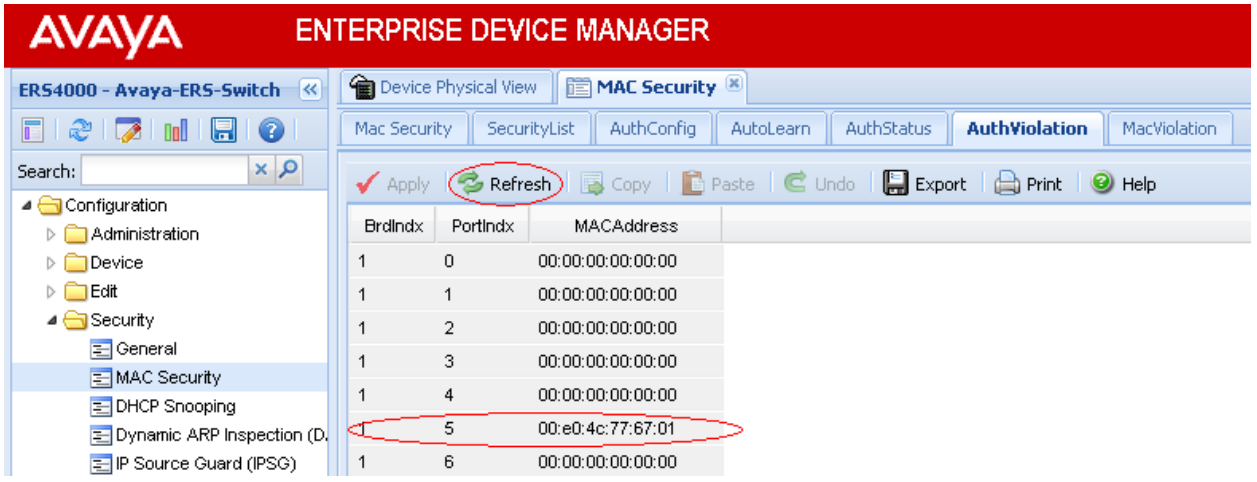
Verify log file on switch

```
Avaya-ERS-Switch# show log
Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
I    00:05:53:48                   1        Link Up Trap for Port: 5
I    00:05:53:52                   2        Bay Secure intruder MAC 00-e0-4c-77-67-01
                                            port 5
I    00:05:53:52                   3        Trap:  s5EtrNewSbsMacAccessViolation
```

Verify traps on Management station (e.g. VPFM or COM)



Verify MAC Security violations from EDM



3.1.4.2 Unauthorized MAC on provisioned port

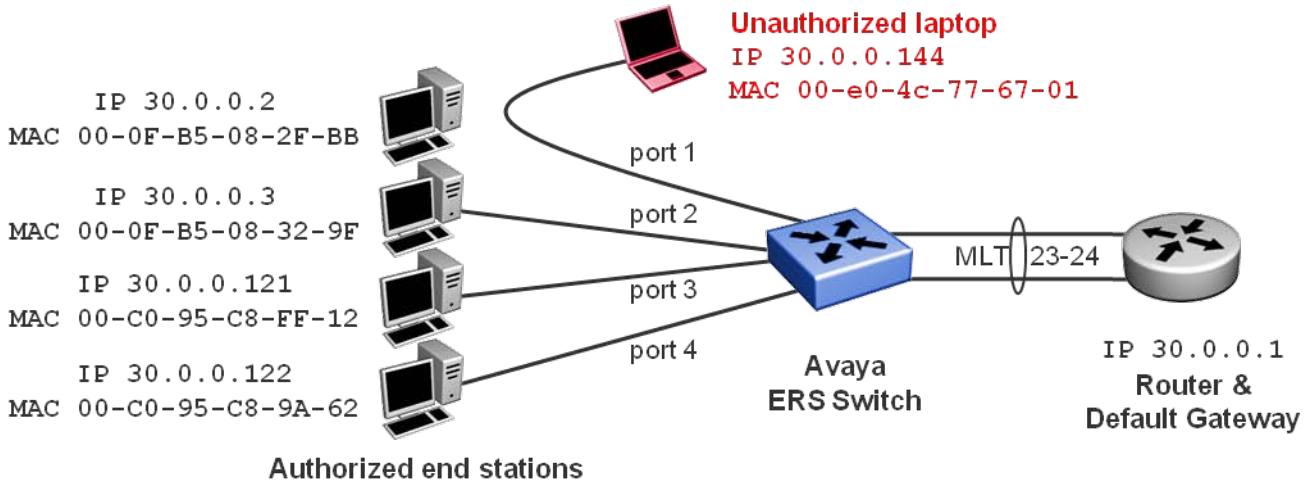


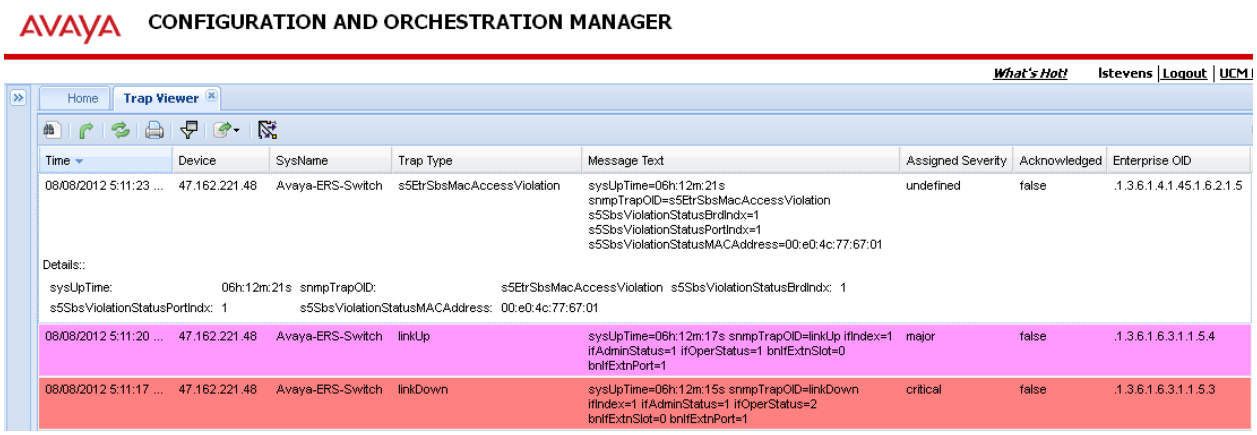
Figure 4: Example 1; unauthorized MAC on provisioned port

The unauthorized device is not able to send any traffic into the network; however it is still able to see broadcast and unknown traffic flowing in the VLAN; if this is undesired the MAC Security should be configured to partition the port upon an access violation.

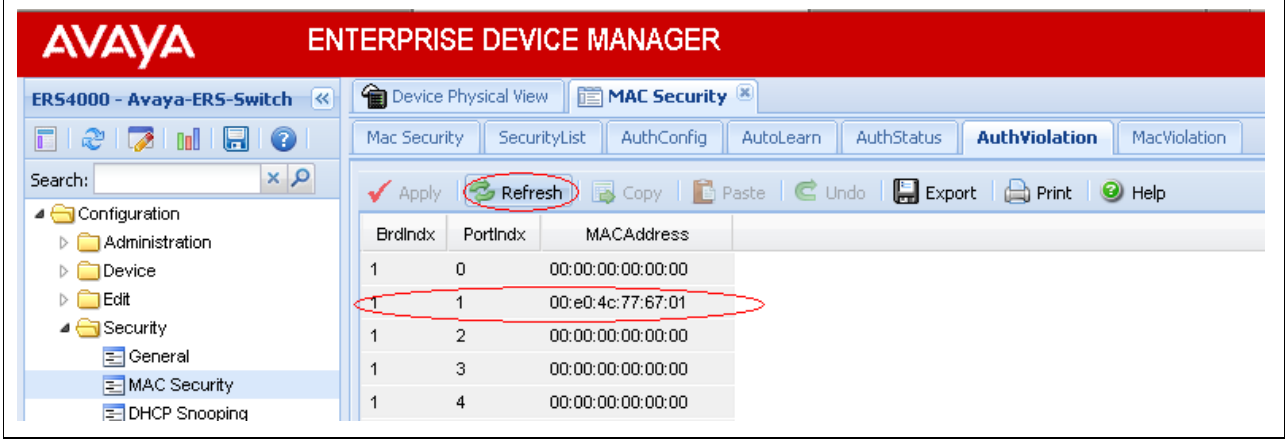
Verify log file on switch

```
Avaya-ERS-Switch# show log
Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
I    00:06:12:15                   1        Link Down Trap for Port: 1
I    00:06:12:17                   2        Link Up Trap for Port: 1
I    00:06:12:21                   3        Bay Secure intruder MAC 00-e0-4c-77-67-01
                                            port 1
I    00:06:12:21                   4        Trap:  s5EtrNewSbsMacAccessViolation
```

Verify traps on Management station (e.g. VPFM or COM)



Verify MAC Security violations from EDM



3.1.4.3 Unauthorized MAC sharing connection with authorized MAC

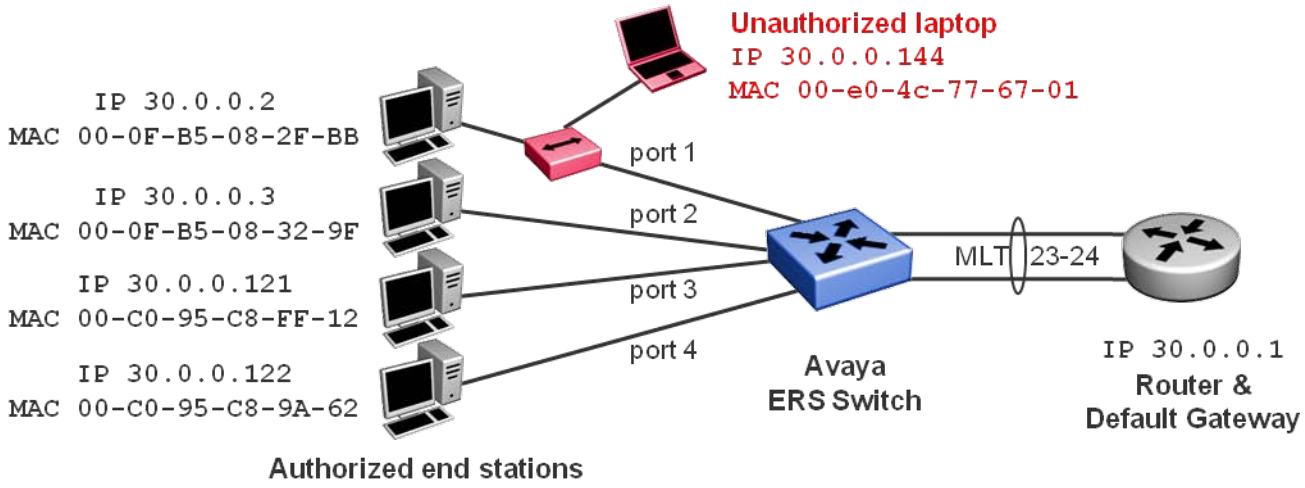


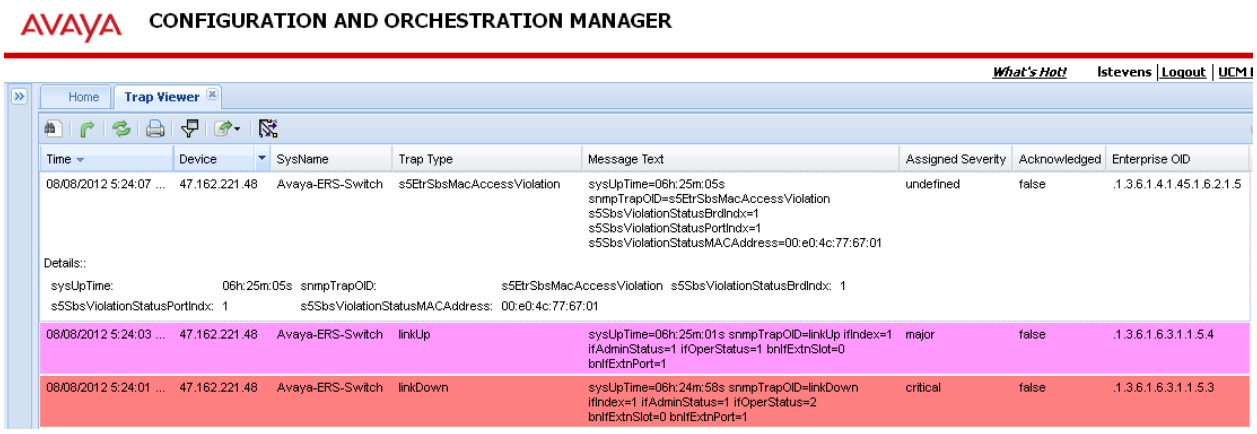
Figure 5: Example 1; unauthorized MAC sharing connection with authorized MAC

The unauthorized device is not able to send any traffic into the network but station with IP 30.0.0.2 can still talk to the network. However the unauthorized device is still able to see broadcast and unknown traffic flowing in the VLAN and, if a shared hub was inserted on the network connection, it can also see all of traffic sent and received by station with IP 30.0.0.2; if this is undesired the MAC Security should be configured to partition the port upon an access violation.

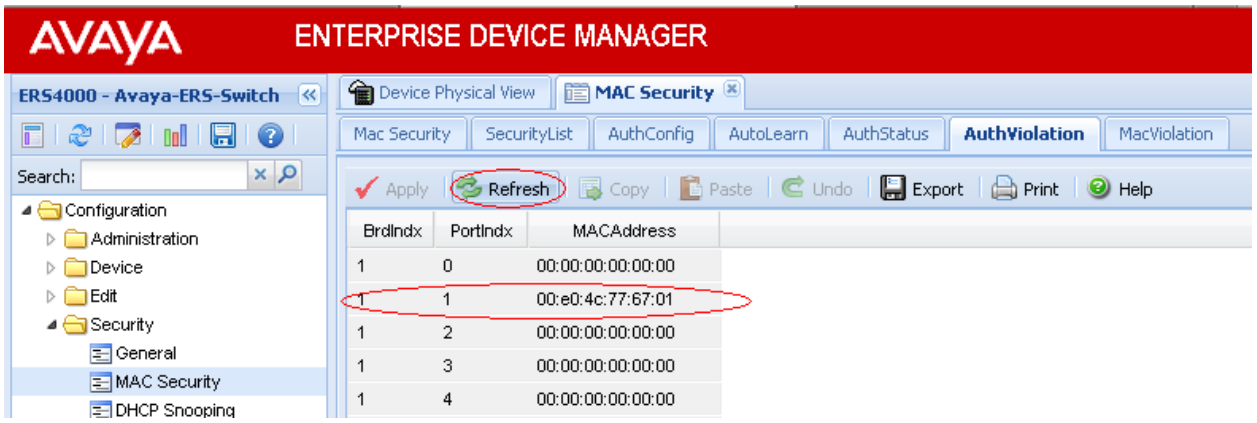
Verify log file on switch

```
Avaya-ERS-Switch# show log
Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
I    00:06:24:58                   1        Link Down Trap for Port: 1
I    00:06:25:01                   2        Link Up Trap for Port: 1
I    00:06:25:05                   4        Bay Secure intruder MAC 00-e0-4c-77-67-01
                                            port 1
I    00:06:25:05                   5        Trap:  s5EtrNewSbsMacAccessViolation
```

Verify traps on Management station (e.g. VPFM or COM)



Verify MAC Security violations from EDM



Note that the authorized device on port 1 retains connectivity, but the unauthorized laptop cannot talk to the network

```
Router#% ping 30.0.0.2; ping 30.0.0.3; ping 30.0.0.121; ping 30.0.0.122; ping 30.0.0.144

30.0.0.2 is alive

30.0.0.3 is alive

30.0.0.121 is alive

30.0.0.122 is alive

no answer from 30.0.0.144
```

Tip – If the network administrator prefers to disable the ethernet port 1 in this scenario, it is sufficient to configure port partitioning security action upon violation.

3.1.4.4 Authorized MAC moving to a different port

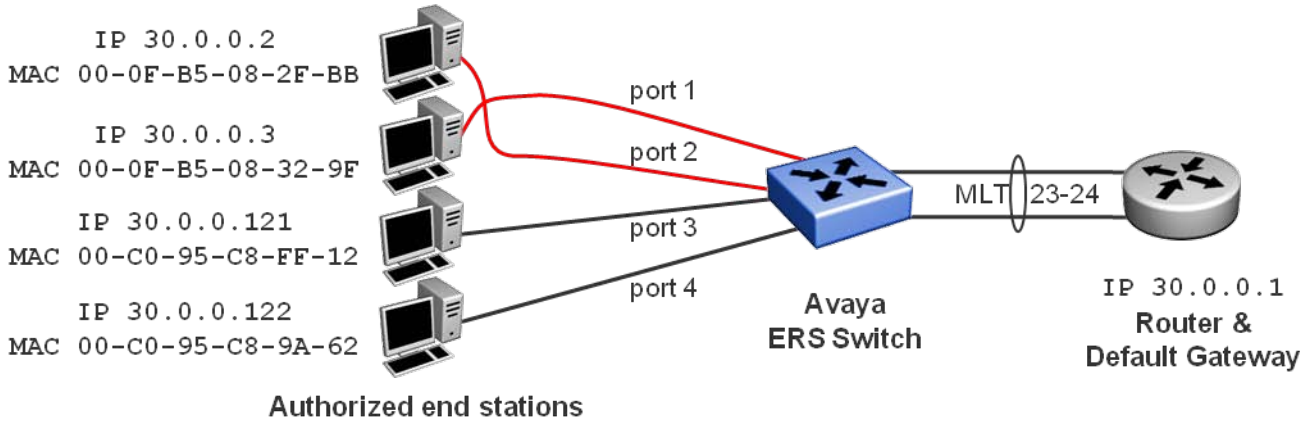


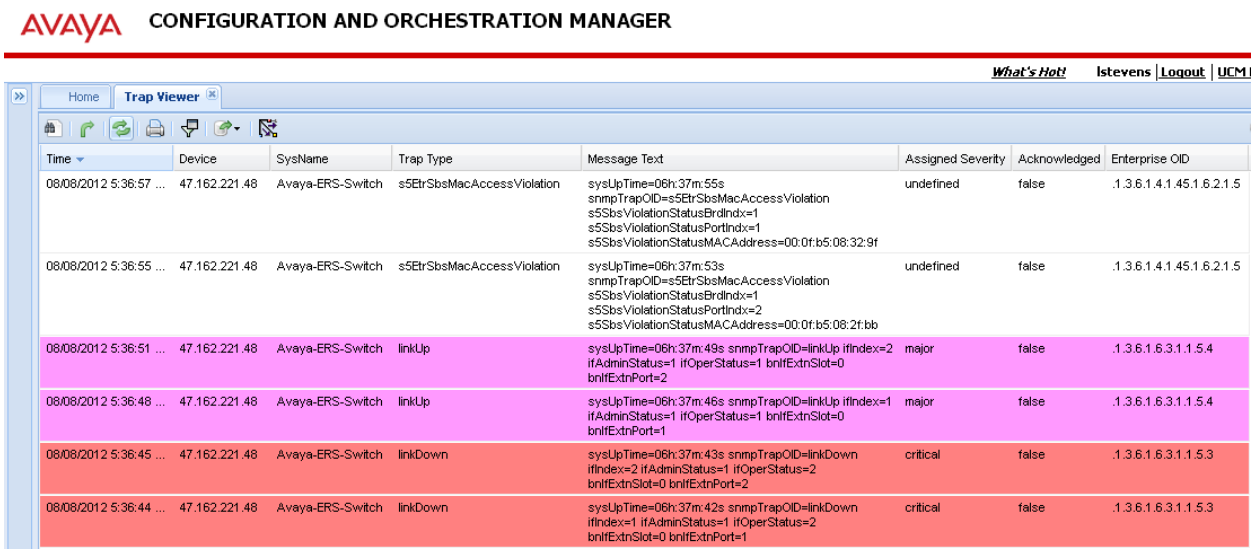
Figure 6: Example 1; unauthorized MAC moving to a different port

Neither of the two end stations with swapped connections can now talk to the network.

Verify log file on switch

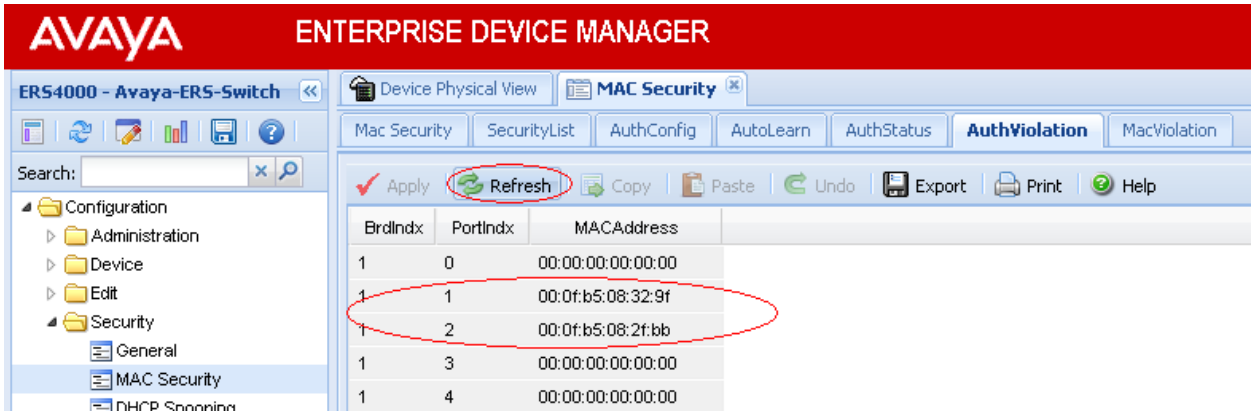
```
Avaya-ERS-Switch# show log
Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
I    00:06:37:42                   1        Link Down Trap for Port: 1
I    00:06:37:43                   2        Link Down Trap for Port: 2
I    00:06:37:46                   3        Link Up Trap for Port: 1
I    00:06:37:49                   4        Link Up Trap for Port: 2
I    00:06:37:53                   5        Bay Secure intruder MAC 00-0f-b5-08-2f-bb
                                            port 2
I    00:06:37:53                   6        Trap:  s5EtrNewSbsMacAccessViolation
I    00:06:37:55                   7        Bay Secure intruder MAC 00-0f-b5-08-32-9f
                                            port 1
I    00:06:37:55                   8        Trap:  s5EtrNewSbsMacAccessViolation
```

Verify traps on Management station (e.g. VPFM or COM)



Time	Device	SysName	Trap Type	Message Text	Assigned Severity	Acknowledged	Enterprise OID
08/08/2012 5:36:57 ...	47.162.221.48	Avaya-ERS-Switch	s5EtrSbsMacAccessViolation	sysUpTime=06h:37m:55s snmpTrapOID=s5EtrSbsMacAccessViolation s5SbsViolationStatusBrdIndx=1 s5SbsViolationStatusPortIndx=1 s5SbsViolationStatusMACAddress=00:0f:b5:08:32:9f	undefined	false	.1.3.6.1.4.1.45.1.6.2.1.5
08/08/2012 5:36:55 ...	47.162.221.48	Avaya-ERS-Switch	s5EtrSbsMacAccessViolation	sysUpTime=06h:37m:53s snmpTrapOID=s5EtrSbsMacAccessViolation s5SbsViolationStatusBrdIndx=1 s5SbsViolationStatusPortIndx=2 s5SbsViolationStatusMACAddress=00:0f:b5:08:2f:bb	undefined	false	.1.3.6.1.4.1.45.1.6.2.1.5
08/08/2012 5:36:51 ...	47.162.221.48	Avaya-ERS-Switch	linkUp	sysUpTime=06h:37m:49s snmpTrapOID=linkUp ifIndex=2 ifAdminStatus=1 ifOperStatus=1 bnlfExtnSlot=0 bnlfExtnPort=2	major	false	.1.3.6.1.6.3.1.1.5.4
08/08/2012 5:36:48 ...	47.162.221.48	Avaya-ERS-Switch	linkUp	sysUpTime=06h:37m:46s snmpTrapOID=linkUp ifIndex=1 ifAdminStatus=1 ifOperStatus=1 bnlfExtnSlot=0 bnlfExtnPort=1	major	false	.1.3.6.1.6.3.1.1.5.4
08/08/2012 5:36:45 ...	47.162.221.48	Avaya-ERS-Switch	linkDown	sysUpTime=06h:37m:43s snmpTrapOID=linkDown ifIndex=2 ifAdminStatus=1 ifOperStatus=2 bnlfExtnSlot=0 bnlfExtnPort=2	critical	false	.1.3.6.1.6.3.1.1.5.3
08/08/2012 5:36:44 ...	47.162.221.48	Avaya-ERS-Switch	linkDown	sysUpTime=06h:37m:42s snmpTrapOID=linkDown ifIndex=1 ifAdminStatus=1 ifOperStatus=2 bnlfExtnSlot=0 bnlfExtnPort=1	critical	false	.1.3.6.1.6.3.1.1.5.3

Verify MAC Security violations from EDM



BrdIndx	PortIndx	MACAddress
1	0	00:00:00:00:00:00
1	1	00:0f:b5:08:32:9f
1	2	00:0f:b5:08:2f:bb
1	3	00:00:00:00:00:00
1	4	00:00:00:00:00:00

Note that the authorized devices cannot communicate on the wrong ethernet port

```
Router#% ping 30.0.0.2; ping 30.0.0.3; ping 30.0.0.121; ping 30.0.0.122
no answer from 30.0.0.2
no answer from 30.0.0.3
30.0.0.121 is alive
30.0.0.122 is alive
```

3.2 Ensuring that no new unauthorized device (MAC) is added to the network

In this example the network administrator wants to start using MAC Security but does not have the time or will to manually configure every single MAC address which is already on his network. The assumption is made that existing MAC addresses on the network are allowed with the intention that once MAC Security has been enabled no further device (MAC) can be added to the network or moved to a different port without the knowledge and permission of the network administrator.

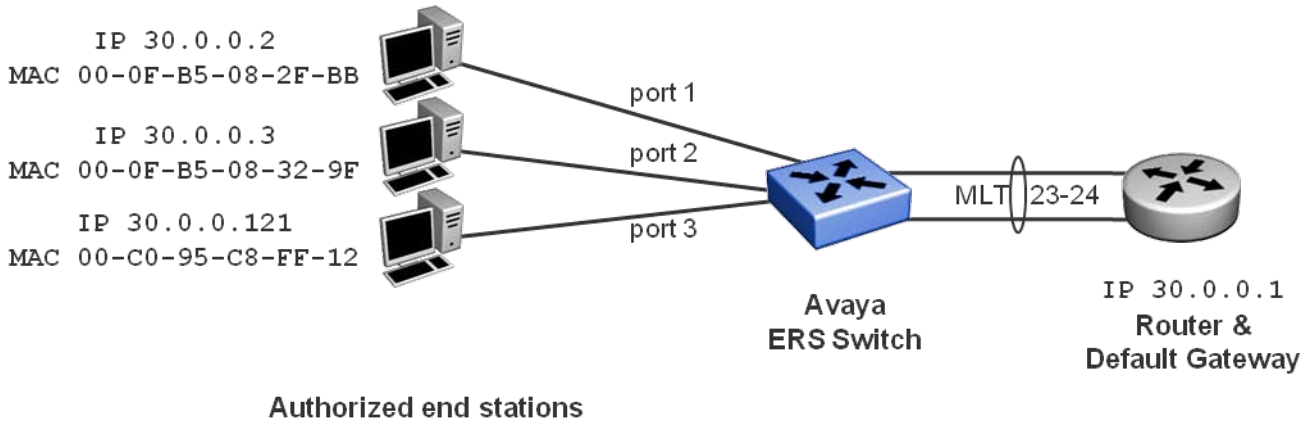


Figure 7: Regular MAC Security; example 2

3.2.1 Using ACLI

3.2.1.1 Initial Switch configuration

Globally enable MAC Security
`Avaya-ERS-Switch(config)# mac-security enable`
Enable learning on the access ports
`Avaya-ERS-Switch(config)# mac-security learning-ports 1-20` `Avaya-ERS-Switch(config)# mac-security learning enable`

Note – There is an alternative syntax for enabling learning on the port interfaces:

```
Avaya-ERS-Switch(config)# interface FastEthernet 1-20
Avaya-ERS-Switch(config-if)# mac-security learning
Avaya-ERS-Switch(config-if)# exit
```

Verify that MAC Security learning mode is enabled

`Avaya-ERS-Switch#% show mac-security config`
`MAC Address Security: Enabled`
`MAC Address Security SNMP-Locked: Disabled`

```
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
MAC Auto-Learning Age-Time:  60 minutes
MAC Auto-Learning Sticky Mode: Disabled
Current Learning Mode: Enabled
Learn by Ports: 1-20
```

Note – Traffic will be unaffected during this time

Now wait a couple of minutes to ensure that all MAC addresses on the switch have been recorded.

View recorded MACs so far

```
Avaya-ERS-Switch# show mac-security mac-address-table
Number of addresses: 3

Unit Port Allowed MAC Address   Type
---- ---- ------------------- ---------
0    1    00-0F-B5-08-2F-BB   Static
0    2    00-0F-B5-08-32-9F   Static
0    3    00-C0-95-C8-FF-12   Static

Security List Allowed MAC Address   Type
------------- ------------------- ---------
```

Once satisfied that all MACs have been recorded, we can proceed to lock these down and activate MAC Security on the access ports.

Disable MAC security learning mode

```
Avaya-ERS-Switch(config)# mac-security learning disable
```

Enable MAC Security on the access ports

```
Avaya-ERS-Switch(config)# interface FastEthernet 1-20
Avaya-ERS-Switch(config-if)# mac-security enable
Avaya-ERS-Switch(config-if)# exit
```

3.2.1.2 Checking MAC Security operational status

Verify that MAC Security is globally enabled

```
Avaya-ERS-Switch# show mac-security config
MAC Address Security: Enabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
MAC Auto-Learning Age-Time:  60 minutes
MAC Auto-Learning Sticky Mode: Disabled
Current Learning Mode: Disabled
Learn by Ports: NONE
```

Verify that MAC Security is enabled on the access ports

```
Avaya-ERS-Switch# show mac-security port
Port  Trunk  Security  Auto-Learning  MAC Number
----  -----  --------  -------------  ----------
   1         Enabled      Disabled        2
   2         Enabled      Disabled        2
   3         Enabled      Disabled        2
   4         Enabled      Disabled        2
   5         Enabled      Disabled        2
   6         Enabled      Disabled        2
   7         Enabled      Disabled        2
   8         Enabled      Disabled        2
   9         Enabled      Disabled        2
  10         Enabled      Disabled        2
  11         Enabled      Disabled        2
  12         Enabled      Disabled        2
  13         Enabled      Disabled        2
  14         Enabled      Disabled        2
  15         Enabled      Disabled        2
  16         Enabled      Disabled        2
  17         Enabled      Disabled        2
  18         Enabled      Disabled        2
  19         Enabled      Disabled        2
```

```
  20          Enabled      Disabled        2
  21          Disabled     Disabled        2
  22          Disabled     Disabled        2
  23    1     Disabled     Disabled        2
  24    1     Disabled     Disabled        2
```

Verify the authorized MAC addresses appear in the MAC Security MAC table

```
Avaya-ERS-Switch# show mac-security mac-address-table
Number of addresses: 3

Unit Port Allowed MAC Address   Type
---- ---- ------------------- ---------
0    1    00-0F-B5-08-2F-BB   Static
0    2    00-0F-B5-08-32-9F   Static
0    3    00-C0-95-C8-FF-12   Static

Security List Allowed MAC Address   Type
------------- ------------------- ---------
```

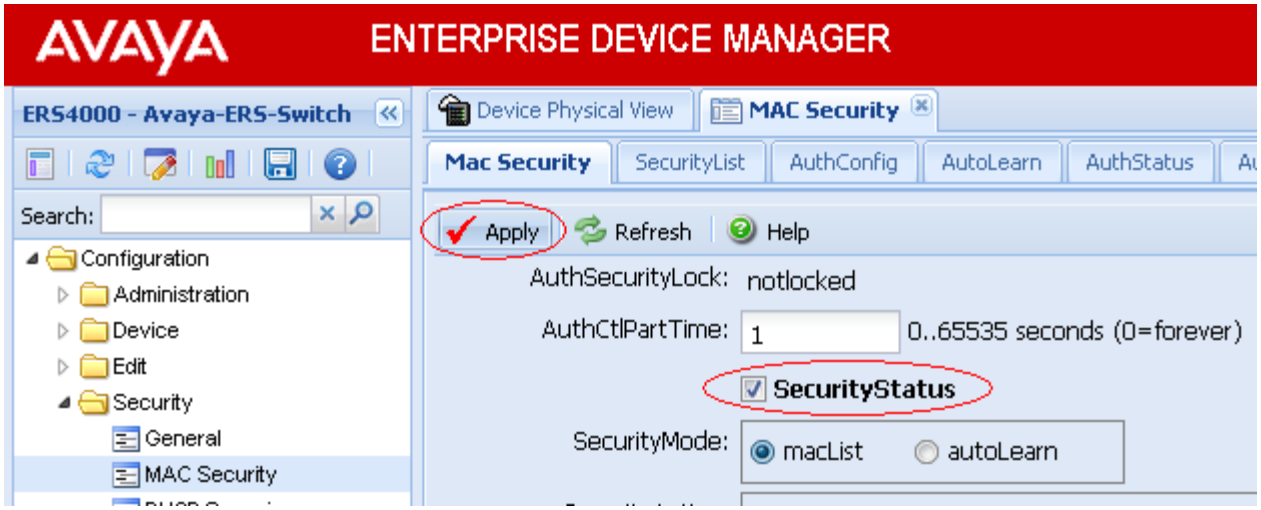
Verify the FDB on the switch

```
Avaya-ERS-Switch# show mac-address-table vid 30
Mac Address Table Aging Time: 300
Learning Enabled Ports 1-26
Number of addresses: 4

   MAC Address    Vid   Type   Source
----------------- ---- ------- -------
00-0F-B5-08-2F-BB   30 Dynamic Port: 1
00-0F-B5-08-32-9F   30 Dynamic Port: 2
00-C0-95-C8-FF-12   30 Dynamic Port: 3
00-E0-16-57-6E-81   30 Dynamic Trunk:1
```

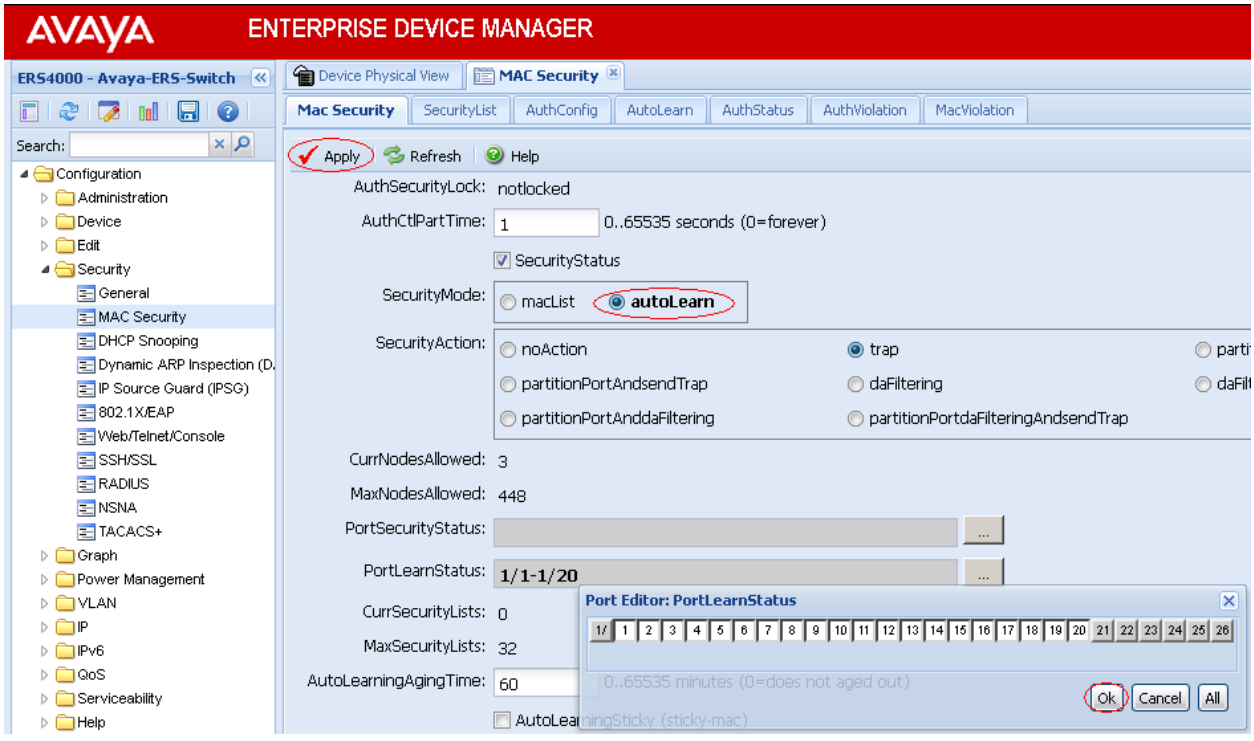
3.2.2 Using EDM

3.2.2.1 Initial Switch configuration

Globally enable MAC Security



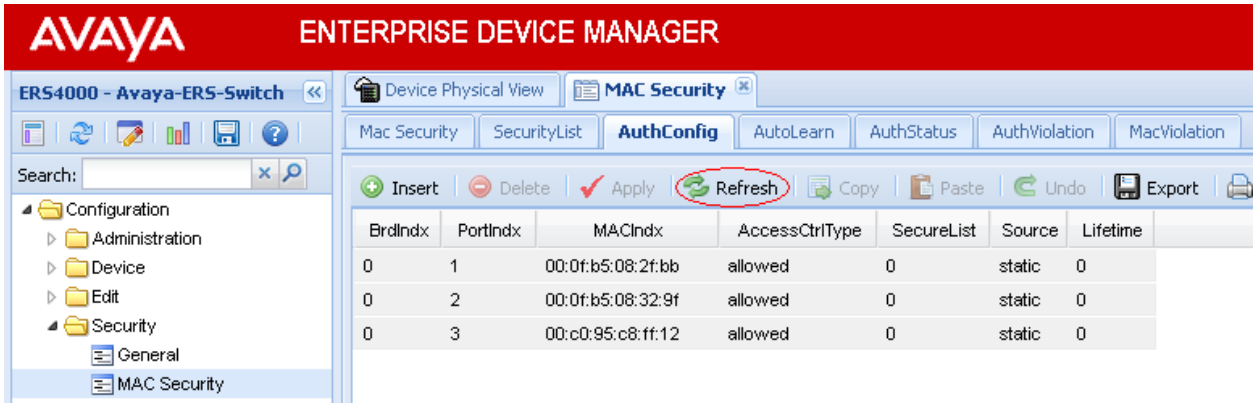
Enable learning on the access ports



Now wait a couple of minutes to ensure that all MAC addresses on the switch have been recorded.

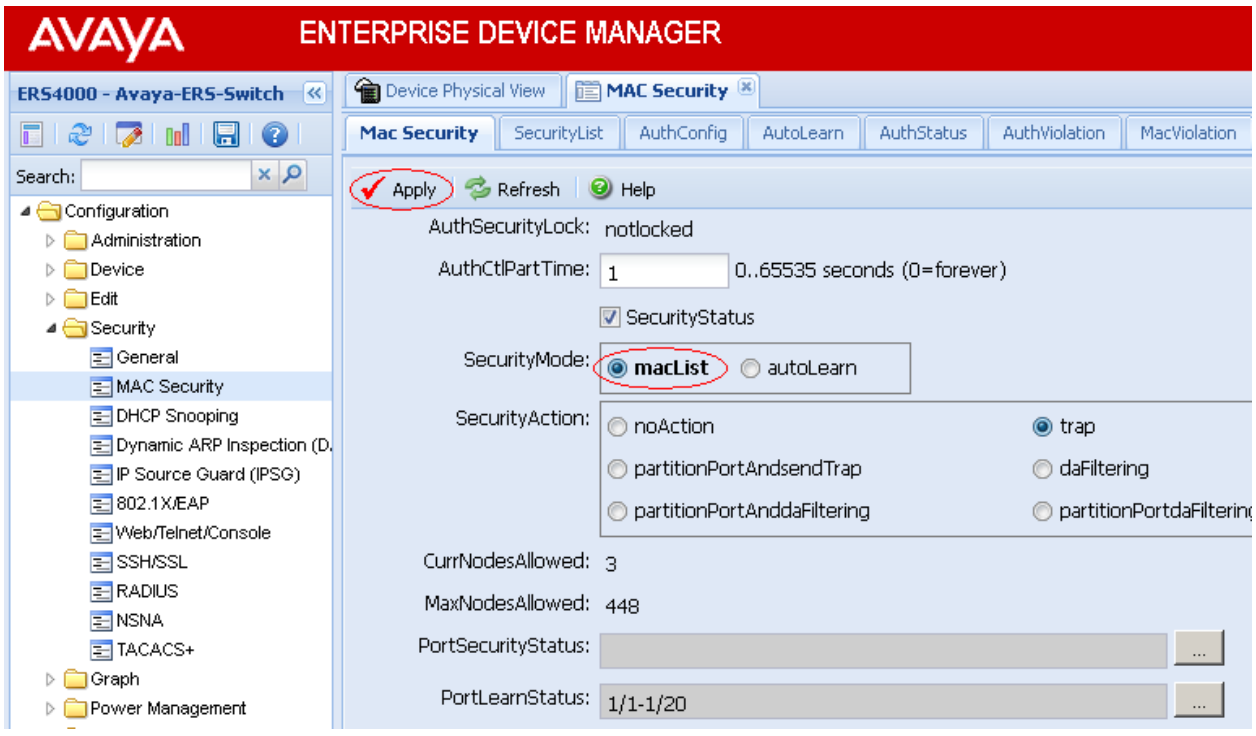
Note – Traffic will be unaffected during this time

View recorded MACs so far



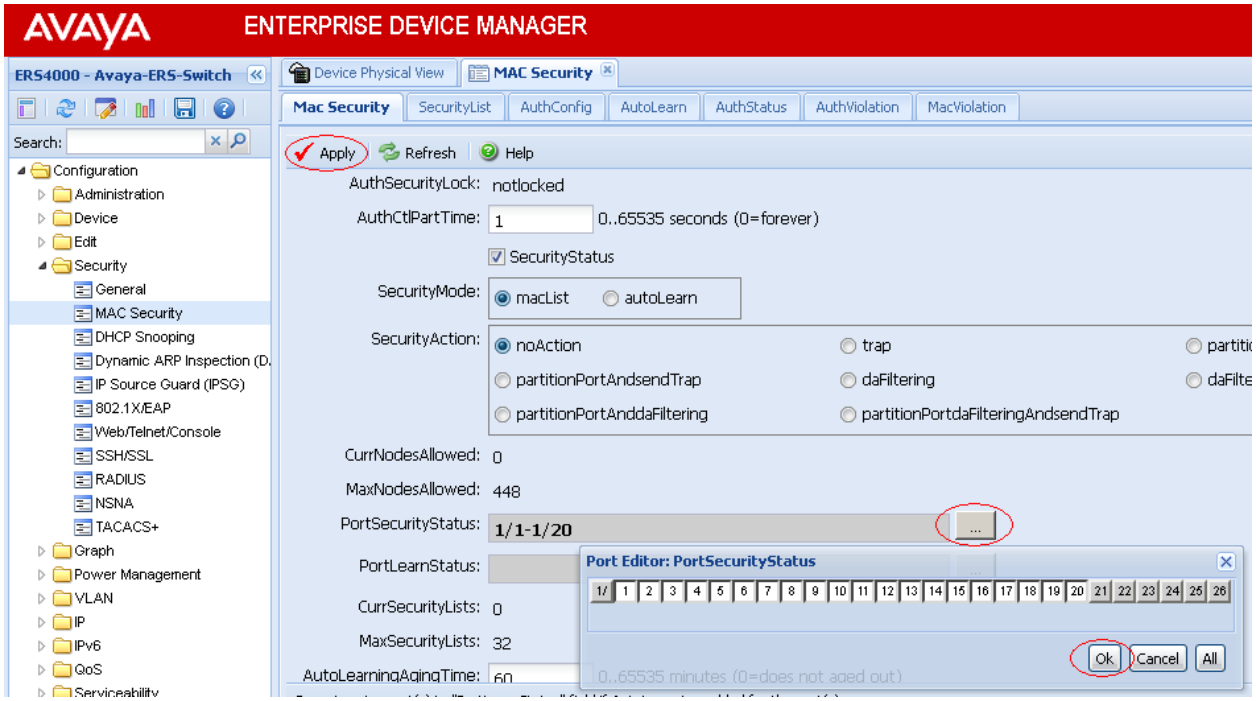
Once satisfied that all MACs have been recorded, we can proceed to lock these down and activate MAC Security on the access ports.

Disable MAC security learning mode

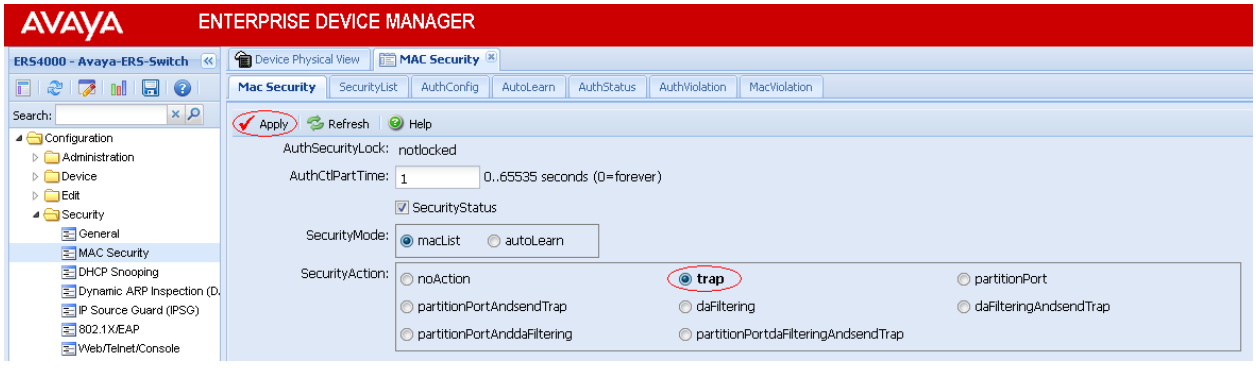


Note – There is no need to clear the ports under PortLearnStatus; after reverting SecurityMode back to macList all ports under PortLearnStatus will be cleared anyway

Enable MAC Security on the access ports

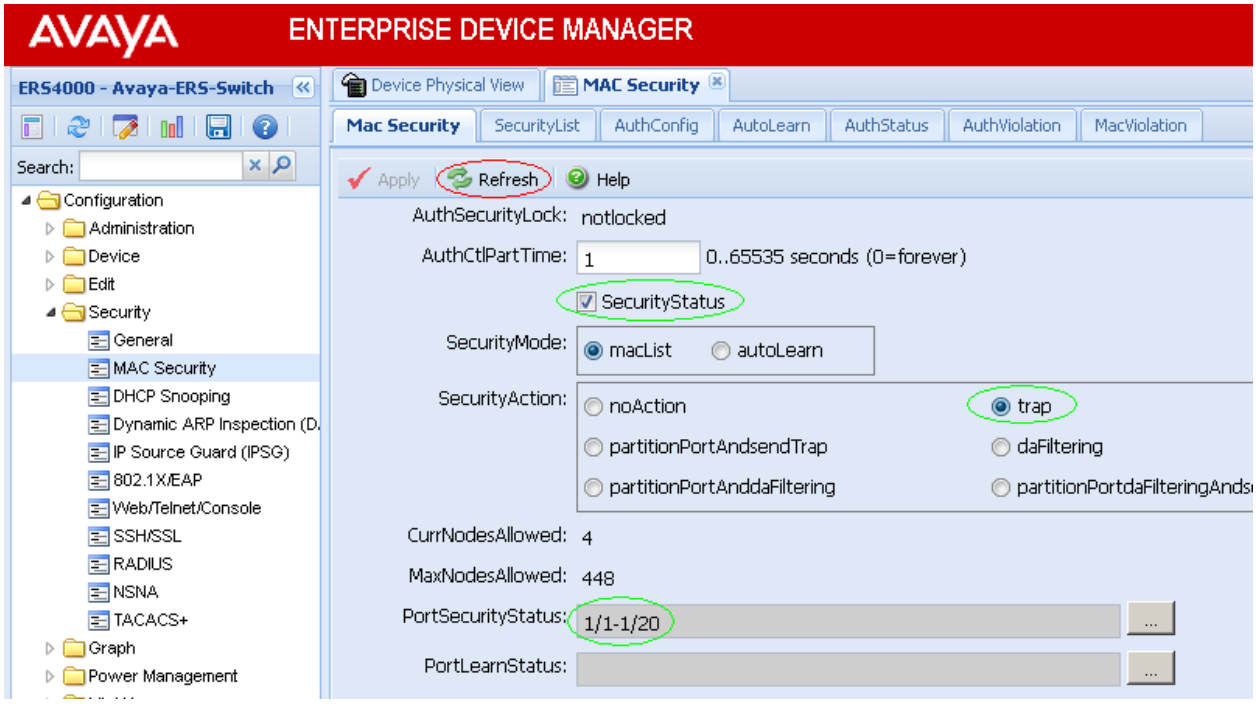


Enable traps upon violation

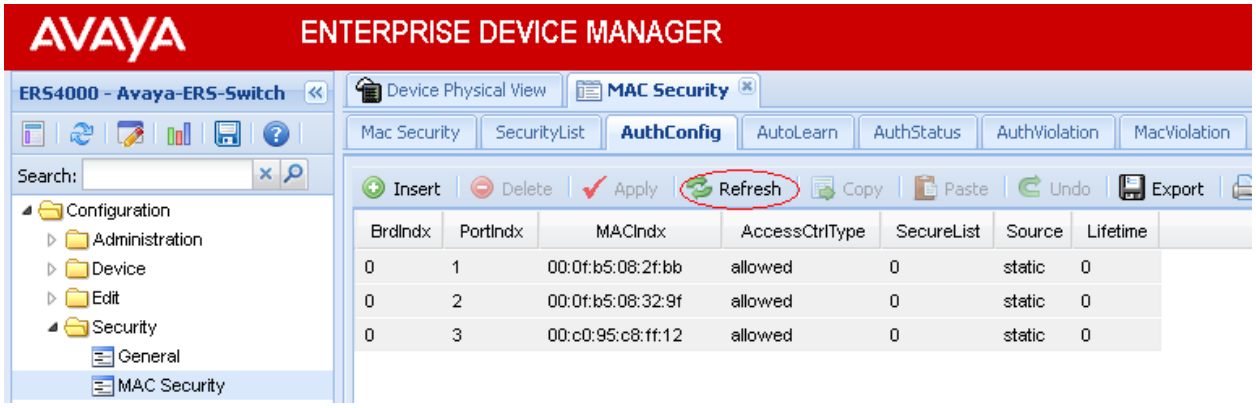


3.2.2.2 Checking MAC Security operational status

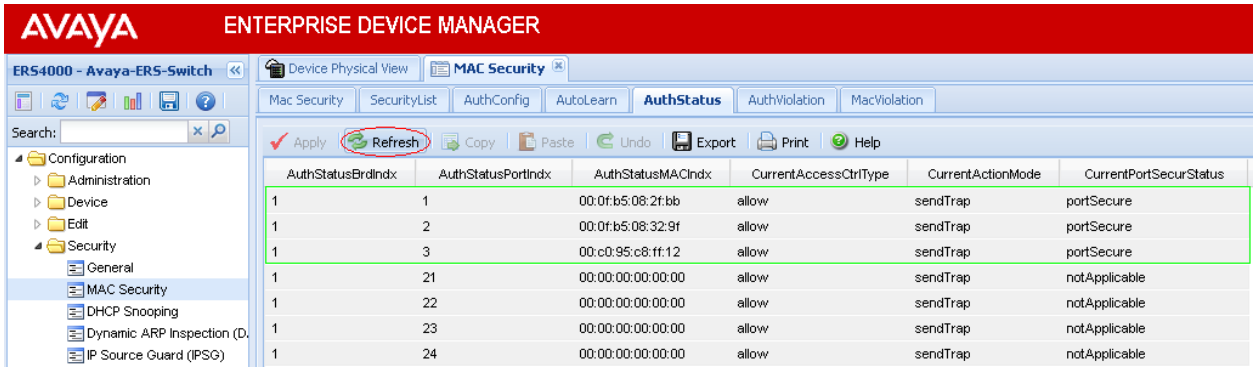
Verify that MAC Security is globally enabled and on access ports



Verify the authorized MAC addresses appear in the MAC Security MAC table



Verify used ports 1-3 are authenticated with the correct MAC address



3.2.3 Verifying user connectivity & switch configuration

Verify IP connectivity between the Router and the end stations

```
Router#% ping 30.0.0.2; ping 30.0.0.3; ping 30.0.0.121
30.0.0.2 is alive
30.0.0.3 is alive
30.0.0.121 is alive
```

Verify the resulting switch config

```
Avaya-ERS-Switch# show running-config
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 4826GTS-PWR+
! Software version = v5.6.1.053
!
! Displaying only parameters different to default
!================================================
enable
configure terminal
[...]
!
! *** MAC-Based Security ***
!
interface FastEthernet ALL
   mac-security port 1-20 enable
```

```
exit
mac-security enable
mac-security mac-address-table address 00.0f.b5.08.2f.bb port 1
mac-security mac-address-table address 00.0f.b5.08.32.9f port 2
mac-security mac-address-table address 00.c0.95.c8.ff.12 port 3
[...]
end
```

Note – The learned MAC addresses are now part of the config file for the switch and thus will be preserved over a switch reboot

3.2.4 When a new device is added to the network

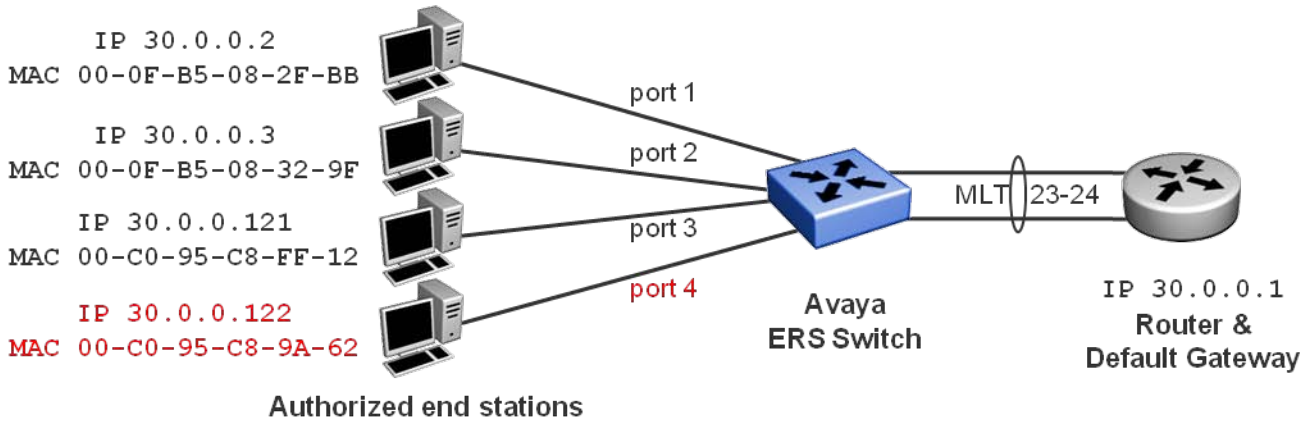


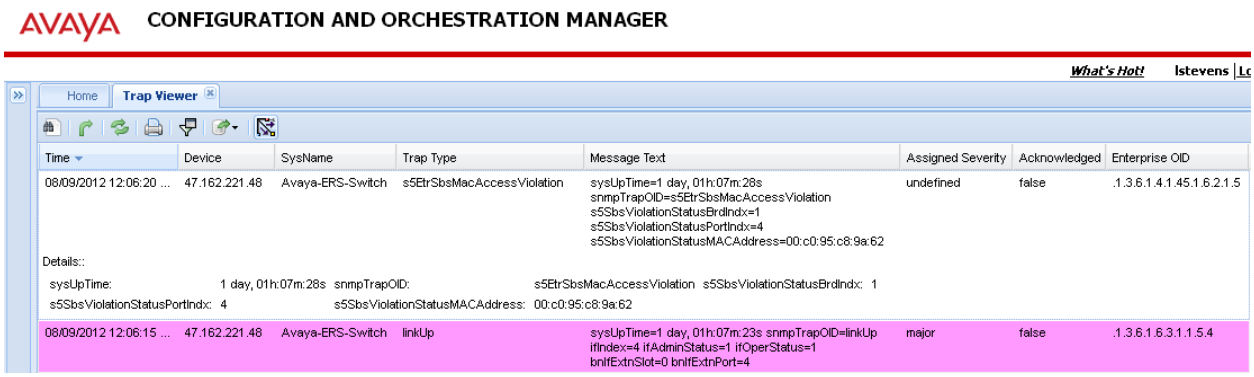
Figure 8: Example 2; a new device is added to the network

In the above diagram a new end station is added to the network on port 4. This will initially trigger a MAC Security violation. The network administrator will then have to take action to (a) verify whether the new end station should be allowed into the network and if so, (b) add the new end station's MAC to the authorized list on the relevant port. In this example, the network administrator does not like typing in MAC addresses so he will use the learning functionality to achieve the same.

Verify log file on switch

```
Avaya-ERS-Switch# show log
Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
I    01:01:07:23                   3        Link Up Trap for Port: 4
I    01:01:07:28                   4        Bay Secure intruder MAC 00-c0-95-c8-9a-62
                                            port 4
I    01:01:07:28                   5        Trap:  s5EtrNewSbsMacAccessViolation
```

Verify traps on Management station (e.g. VPFM or COM)



The network administrator decides to give access to the network to this new device.

3.2.4.1 Using ACLI

Temporarily disable MAC security on port 4

```
Avaya-ERS-Switch(config)# interface FastEthernet 4
Avaya-ERS-Switch(config-if)# mac-security disable
Avaya-ERS-Switch(config-if)# exit
```

Enable learning on access port 4

```
Avaya-ERS-Switch(config)# mac-security learning-ports 4
Avaya-ERS-Switch(config)# mac-security learning enable
```

Note – This has no impact on MAC security or traffic forwarding on the other switch ports.

Wait for the new MAC to be learnt on port 4

```
Avaya-ERS-Switch(config)# show mac-security mac-address-table
Number of addresses: 4

Unit Port Allowed MAC Address   Type
---- ---- ------------------- ---------
0    1    00-0F-B5-08-2F-BB   Static
0    2    00-0F-B5-08-32-9F   Static
0    3    00-C0-95-C8-FF-12   Static
0    4    00-C0-95-C8-9A-62   Static
```

```
Security List Allowed MAC Address   Type
------------ ------------------ ---------
```

Warning – Ensure that only 1 MAC address and the correct MAC address has been learnt against port 4.

We can now proceed to re-enable MAC Security on port 4

Disable MAC Security learning mode

```
Avaya-ERS-Switch(config)# mac-security learning disable
```

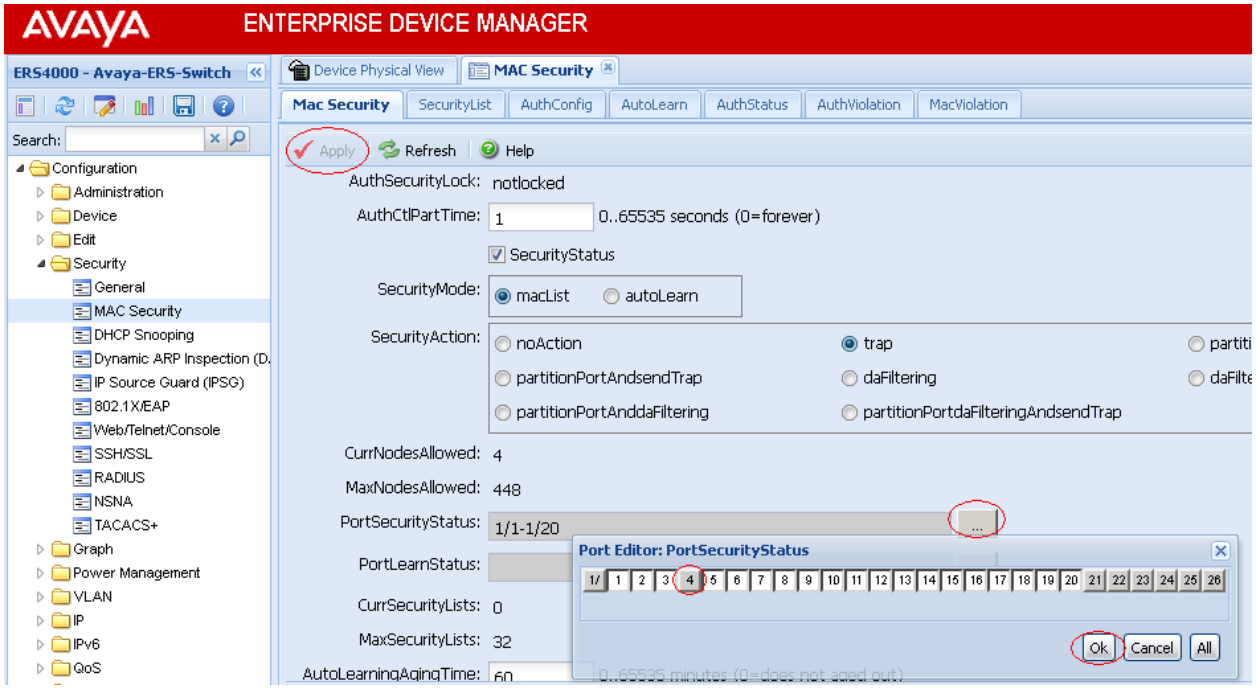
Re-enable MAC security on port 4

```
Avaya-ERS-Switch(config)# interface FastEthernet 4
Avaya-ERS-Switch(config-if)# mac-security enable
Avaya-ERS-Switch(config-if)# exit
```

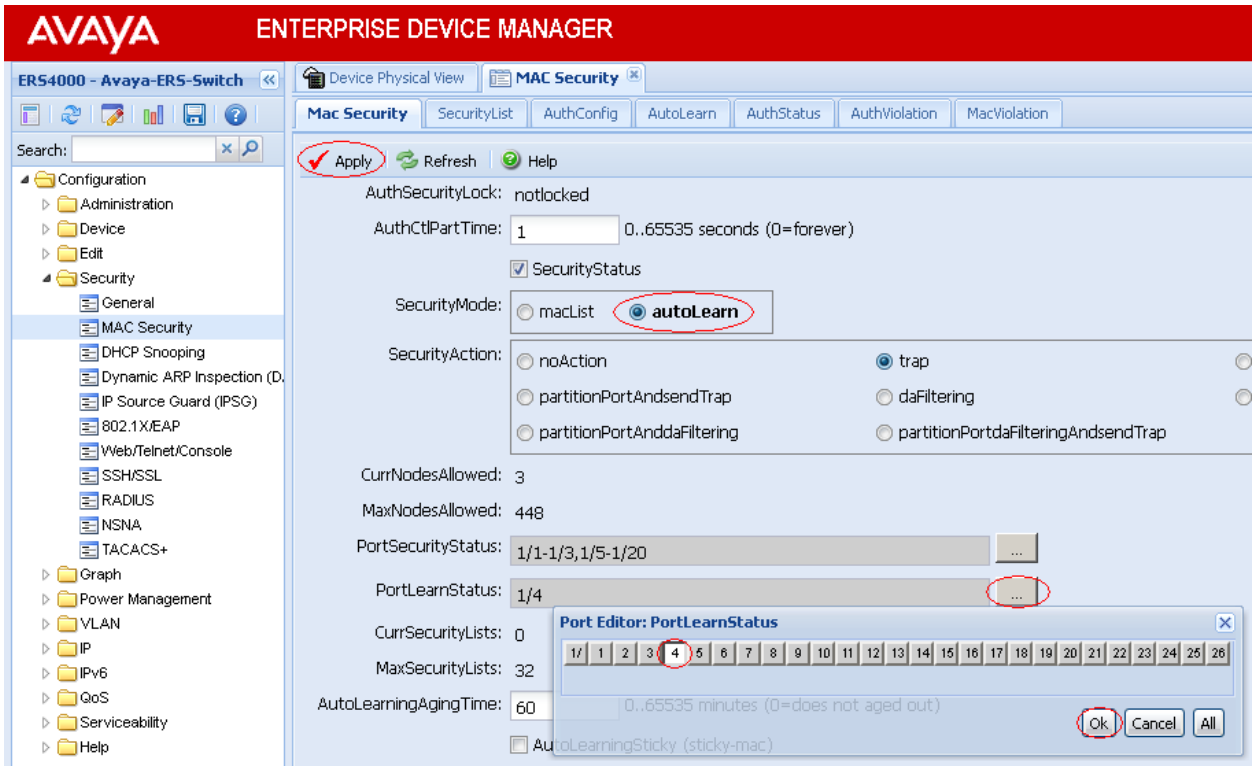
The new user is now securely added to the network.

3.2.4.2 Using EDM

Temporarily disable MAC security on port 4

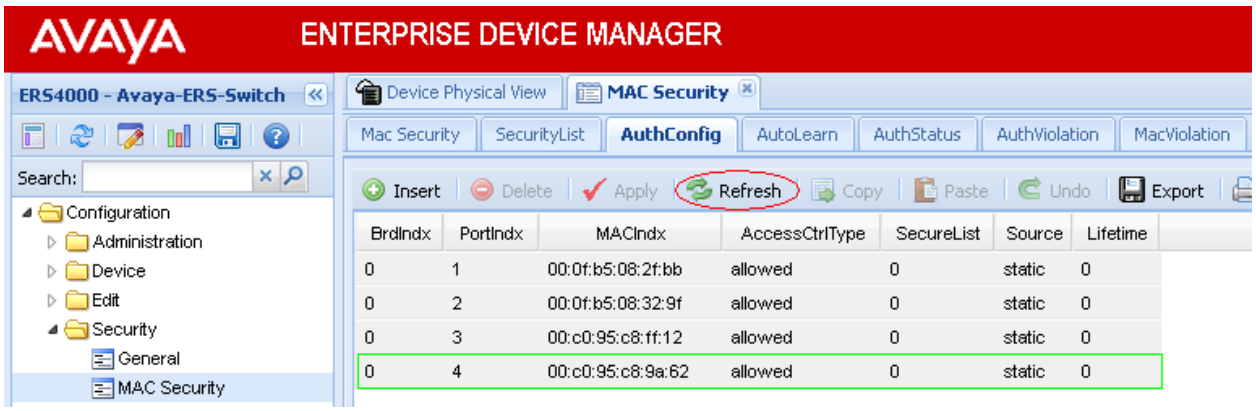


Enable learning on access port 4



Note – This has no impact on MAC security or traffic forwarding on the other switch ports.

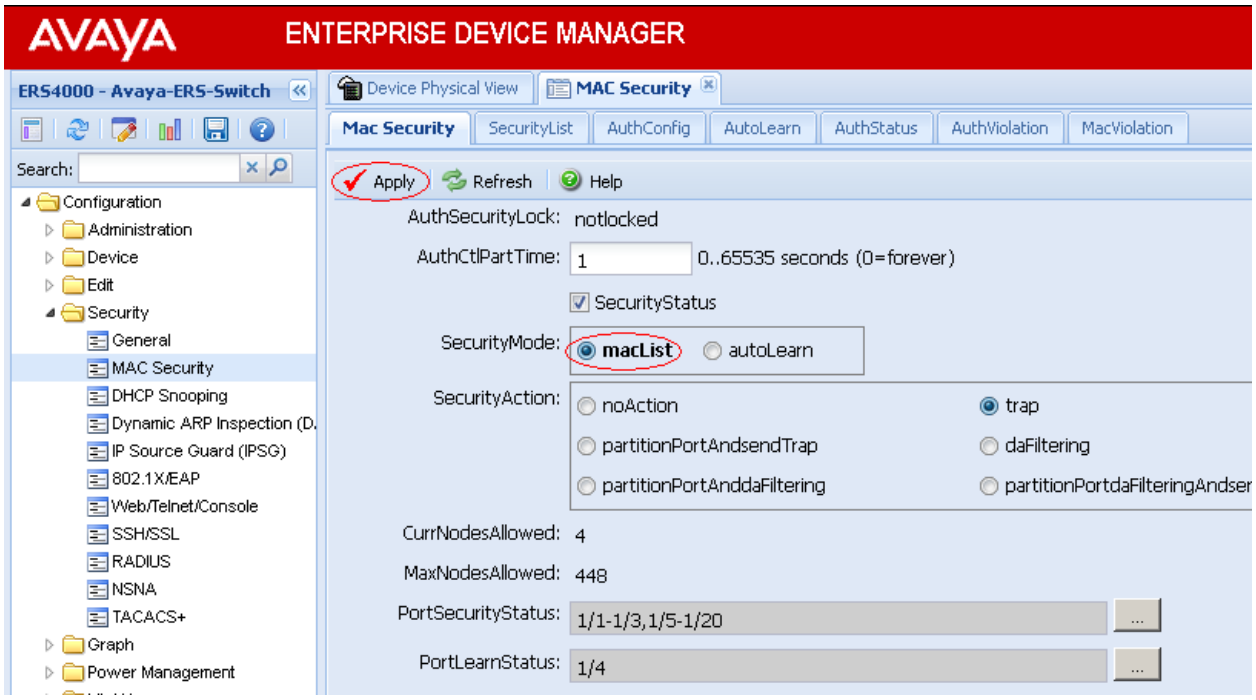
Wait for the new MAC to be learnt on port 4



Warning – Ensure that only 1 MAC address and the correct MAC address has been learnt against port 4.

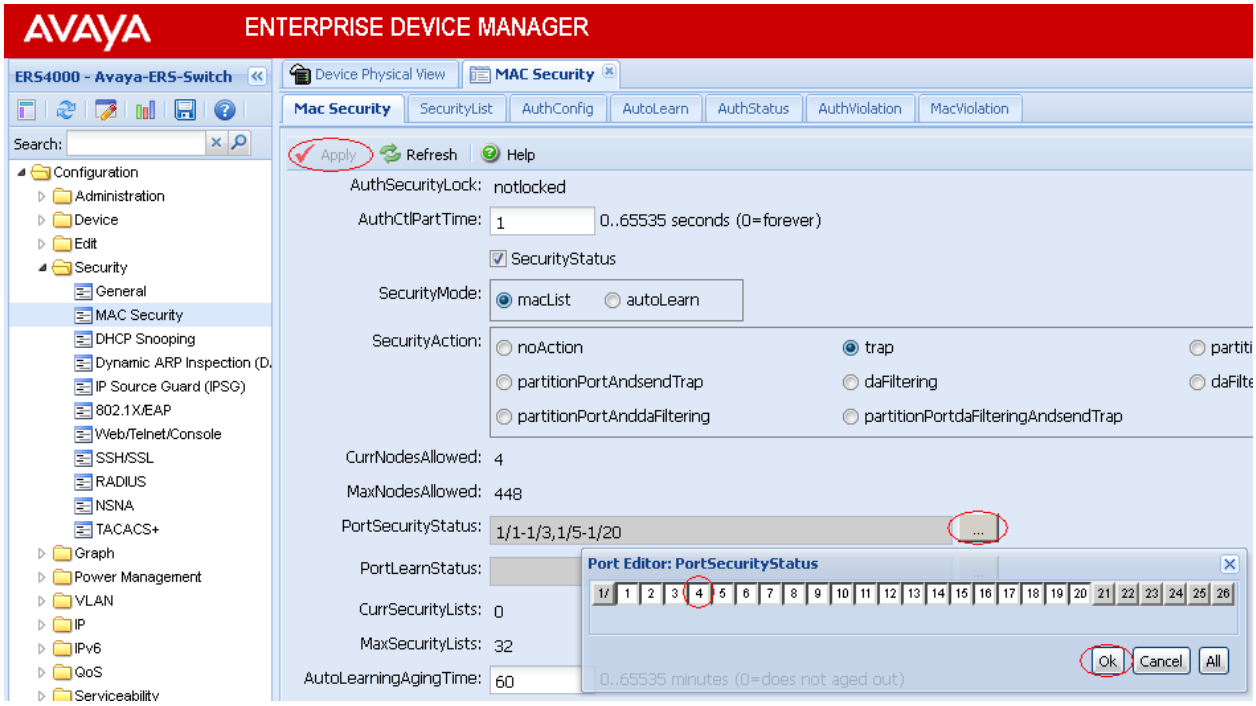
We can now proceed to re-enable MAC Security on port 4

Disable MAC Security learning mode



Note – There is no need to clear the ports under PortLearnStatus; after reverting SecurityMode back to macList all ports under PortLearnStatus will be cleared anyway

Re-enable MAC security on port 4



The new user is now securely added to the network.

3.2.4.3 Checking connectivity

Verify IP connectivity between the Router and the end stations

```
Router#% ping 30.0.0.122
30.0.0.122 is alive
```

3.3 Using MAC Security to tie down Server MACs using Active/Standby NICs

In this example, again another military favorite, we want to use MAC Security in the Data Centre on the server aggregation switches but with the added challenge that the servers can be using dual NICs in Active/Standby fashion.

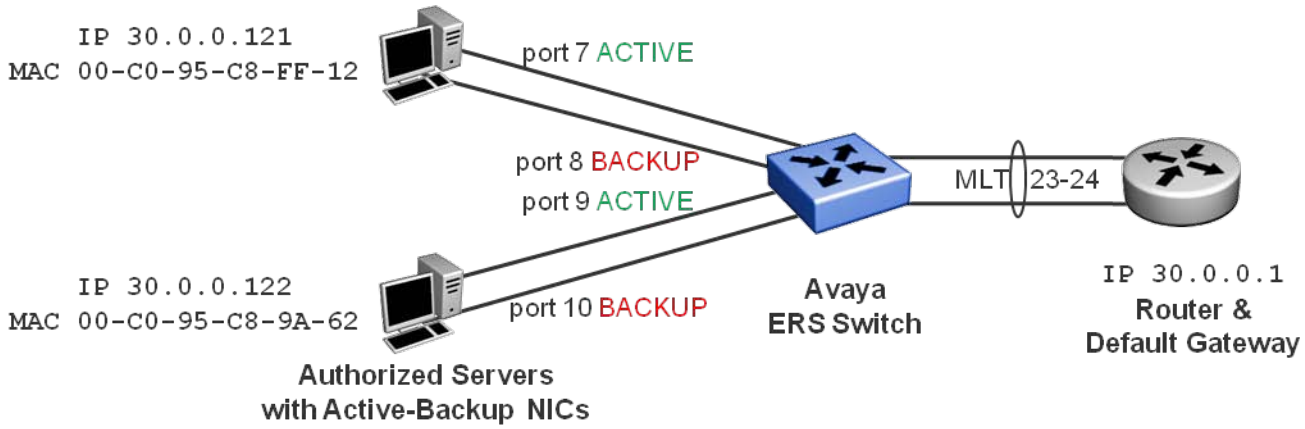


Figure 9: MAC-Security with Active-Standby NICs; example 3

This means that the server MAC address will normally be seen on the ethernet port corresponding to the Active NIC but can move to an alternative ethernet port corresponding to the Standby NIC.

In this example we will use Security Lists which will allow us to tie the authorized MAC addresses to a Security List instead of an ethernet port. The security list will then include the two ethernet ports where the server NICs are connected.

3.3.1 Using ACLI

3.3.1.1 Initial Switch configuration

Create the Security Lists (one for each server)
`Avaya-ERS-Switch(config)#` ***`mac-security security-list 1 7-8`***
`Avaya-ERS-Switch(config)#` ***`mac-security security-list 2 9-10`***

Note – Up to 32 Security Lists can be created.

Globally enable MAC Security
`Avaya-ERS-Switch(config)#` ***`mac-security enable`***
Enable MAC Security on the access ports
`Avaya-ERS-Switch(config)#` ***`interface FastEthernet 1-20`***
`Avaya-ERS-Switch(config-if)#` ***`mac-security enable`***

```
Avaya-ERS-Switch(config-if)# exit
```

3.3.1.2 Provisioning authorized servers

Assign authorized MACs to respective security lists

```
Avaya-ERS-Switch(config)# mac-security mac-address-table address 00-C0-95-C8-FF-12 security-list 1
Avaya-ERS-Switch(config)# mac-security mac-address-table address 00-C0-95-C8-9A-62 security-list 2
```

3.3.1.3 Checking MAC Security operational status

Verify that MAC Security is globally enabled

```
Avaya-ERS-Switch# show mac-security config
MAC Address Security: Enabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
MAC Auto-Learning Age-Time:  60 minutes
MAC Auto-Learning Sticky Mode: Disabled
Current Learning Mode: Disabled
Learn by Ports: NONE
```

Verify the MAC Security Lists

```
Avaya-ERS-Switch# show mac-security security-lists
Security List 1: 7-8
Security List 2: 9-10
Security List 3: NONE
Security List 4: NONE
Security List 5: NONE
Security List 6: NONE
Security List 7: NONE
Security List 8: NONE
Security List 9: NONE
Security List 10: NONE
```

```
Security List 11: NONE
Security List 12: NONE
Security List 13: NONE
Security List 14: NONE
Security List 15: NONE
Security List 16: NONE
Security List 17: NONE
Security List 18: NONE
Security List 19: NONE
Security List 20: NONE
Security List 21: NONE
Security List 22: NONE
Security List 23: NONE
Security List 24: NONE
Security List 25: NONE
Security List 26: NONE
Security List 27: NONE
Security List 28: NONE
Security List 29: NONE
Security List 30: NONE
Security List 31: NONE
Security List 32: NONE
```

Verify that MAC Security is enabled on the access ports

```
Avaya-ERS-Switch# show mac-security port
Port  Trunk  Security  Auto-Learning  MAC Number
----  -----  --------  -------------  ----------
   1         Enabled      Disabled        2
   2         Enabled      Disabled        2
   3         Enabled      Disabled        2
   4         Enabled      Disabled        2
   5         Enabled      Disabled        2
   6         Enabled      Disabled        2
   7         Enabled      Disabled        2
   8         Enabled      Disabled        2
   9         Enabled      Disabled        2
  10         Enabled      Disabled        2
```

```
  11          Enabled      Disabled        2
  12          Enabled      Disabled        2
  13          Enabled      Disabled        2
  14          Enabled      Disabled        2
  15          Enabled      Disabled        2
  16          Enabled      Disabled        2
  17          Enabled      Disabled        2
  18          Enabled      Disabled        2
  19          Enabled      Disabled        2
  20          Enabled      Disabled        2
  21          Disabled     Disabled        2
  22          Disabled     Disabled        2
  23    1     Disabled     Disabled        2
  24    1     Disabled     Disabled        2
```

Verify the authorized MAC addresses appear in the MAC Security MAC table

```
Avaya-ERS-Switch# show mac-security mac-address-table
Number of addresses: 2

Unit Port Allowed MAC Address   Type
---- ---- ------------------- ---------

Security List Allowed MAC Address   Type
------------- ------------------- ---------
2             00-C0-95-C8-9A-62   Static
1             00-C0-95-C8-FF-12   Static
```

Verify the FDB on the switch

```
Avaya-ERS-Switch# show mac-address-table vid 30
Mac Address Table Aging Time: 300
Learning Enabled Ports 1-26
Number of addresses: 3

   MAC Address    Vid   Type   Source
----------------- ---- ------- -------
00-C0-95-C8-9A-62   30 Dynamic Port: 9
```

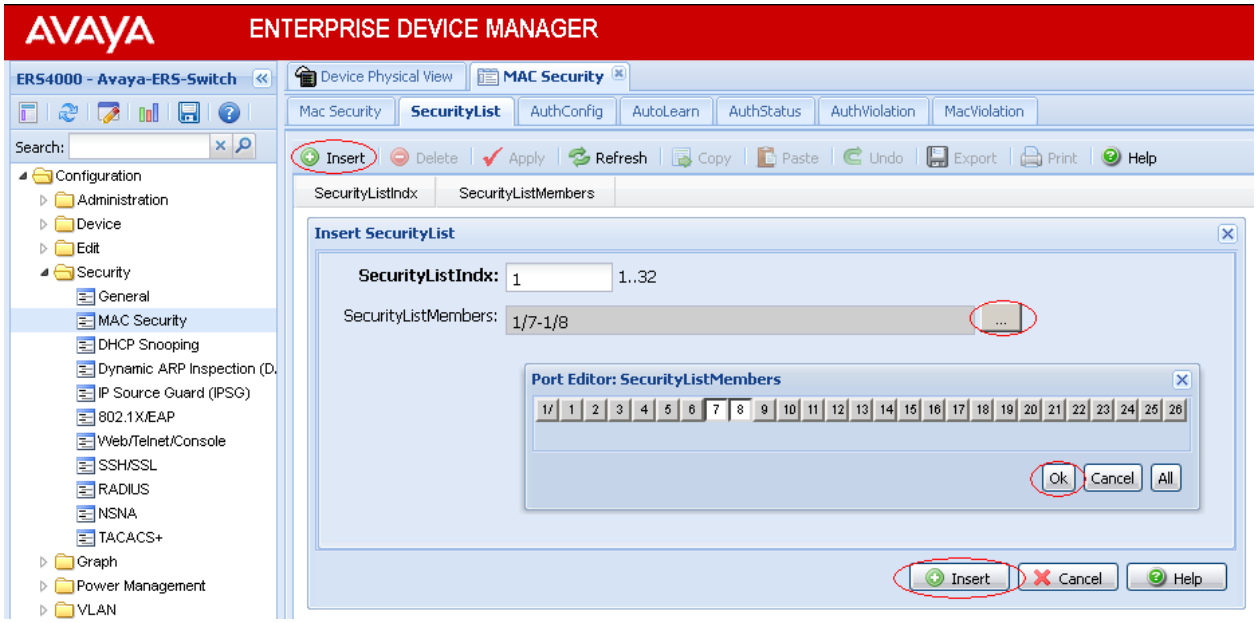
```
00-C0-95-C8-FF-12   30 Dynamic Port: 7
00-E0-16-57-6E-81   30 Dynamic Trunk:1
```

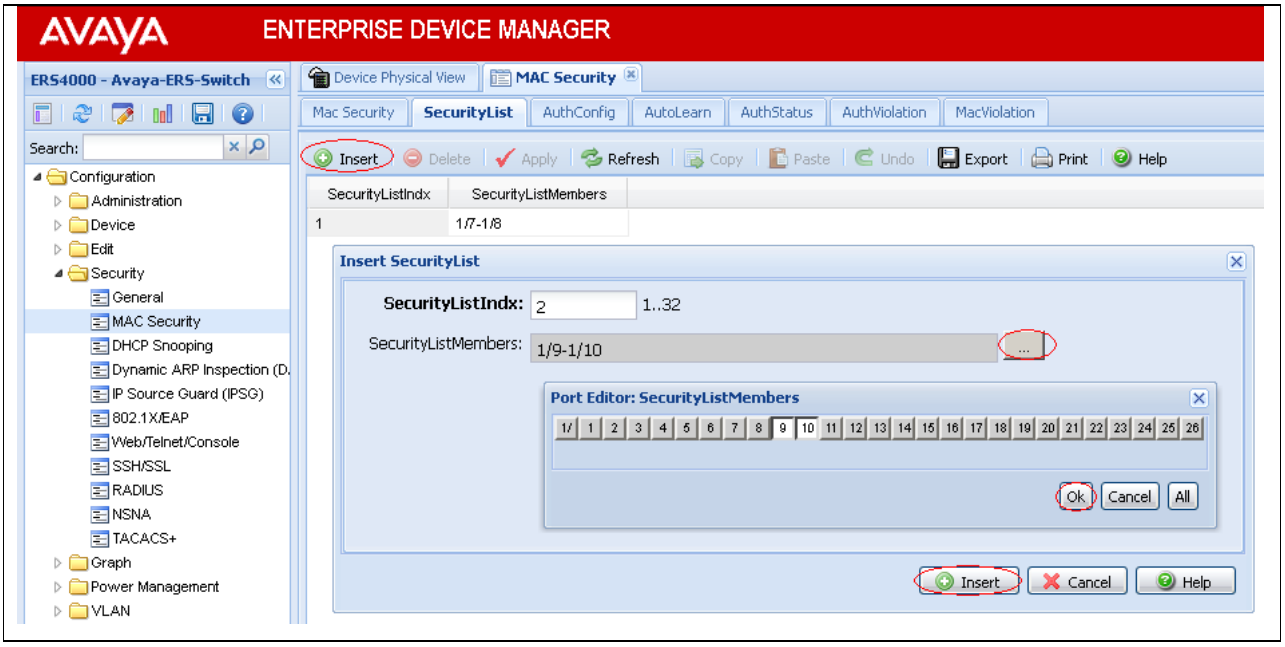
Note – From the FDB we can easily see which port has the Active NIC connected.

3.3.2 Using EDM

3.3.2.1 Initial Switch configuration

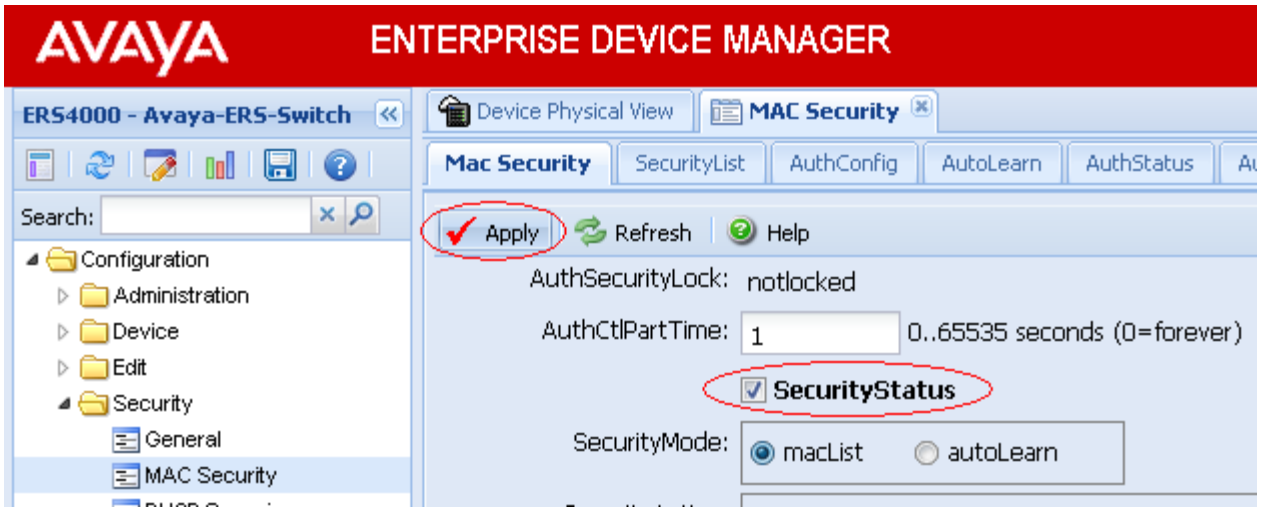
Create the Security Lists (one for each server)



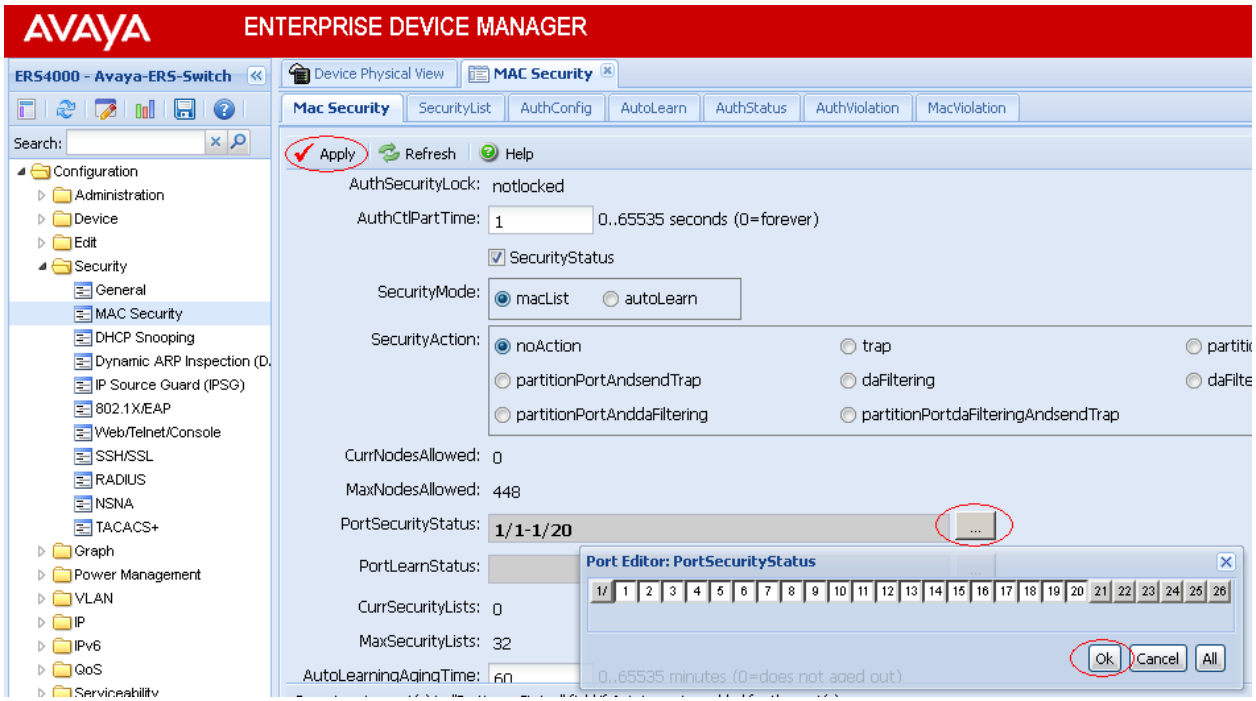


Note – Up to 32 Security Lists can be created.

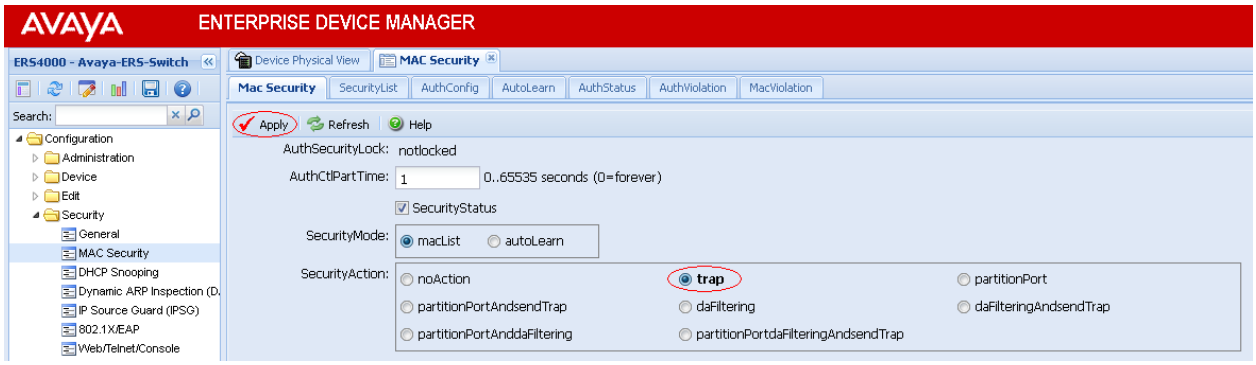
Globally enable MAC Security



Enable MAC Security on the access ports

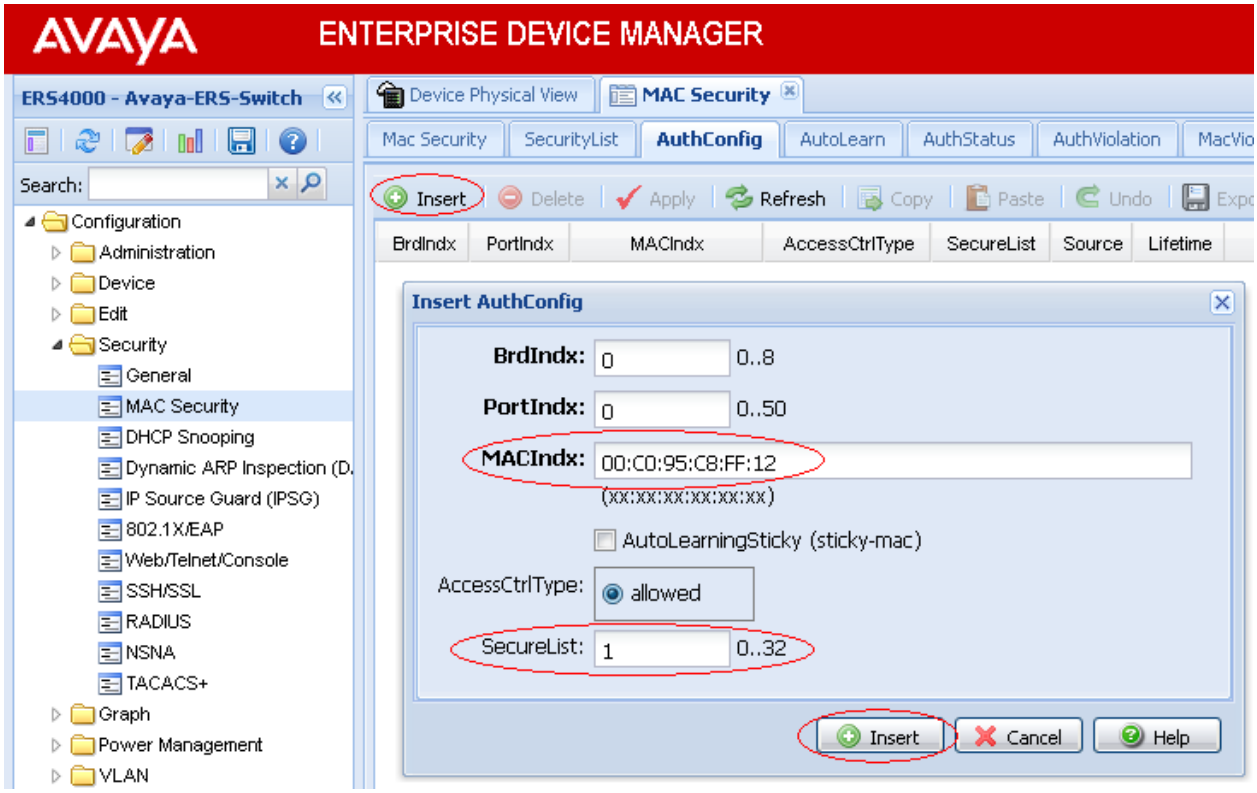


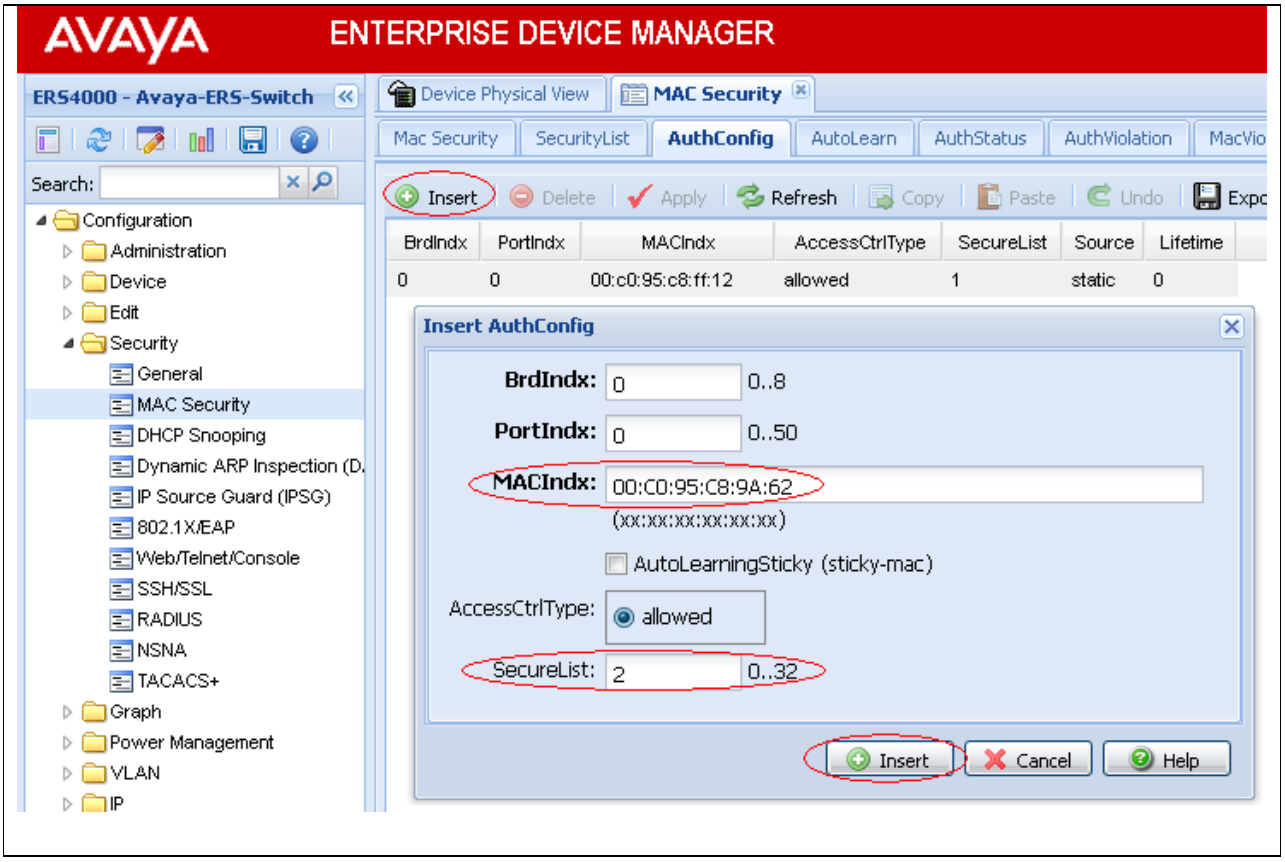
Enable traps upon violation



3.3.2.2 Provisioning authorized servers

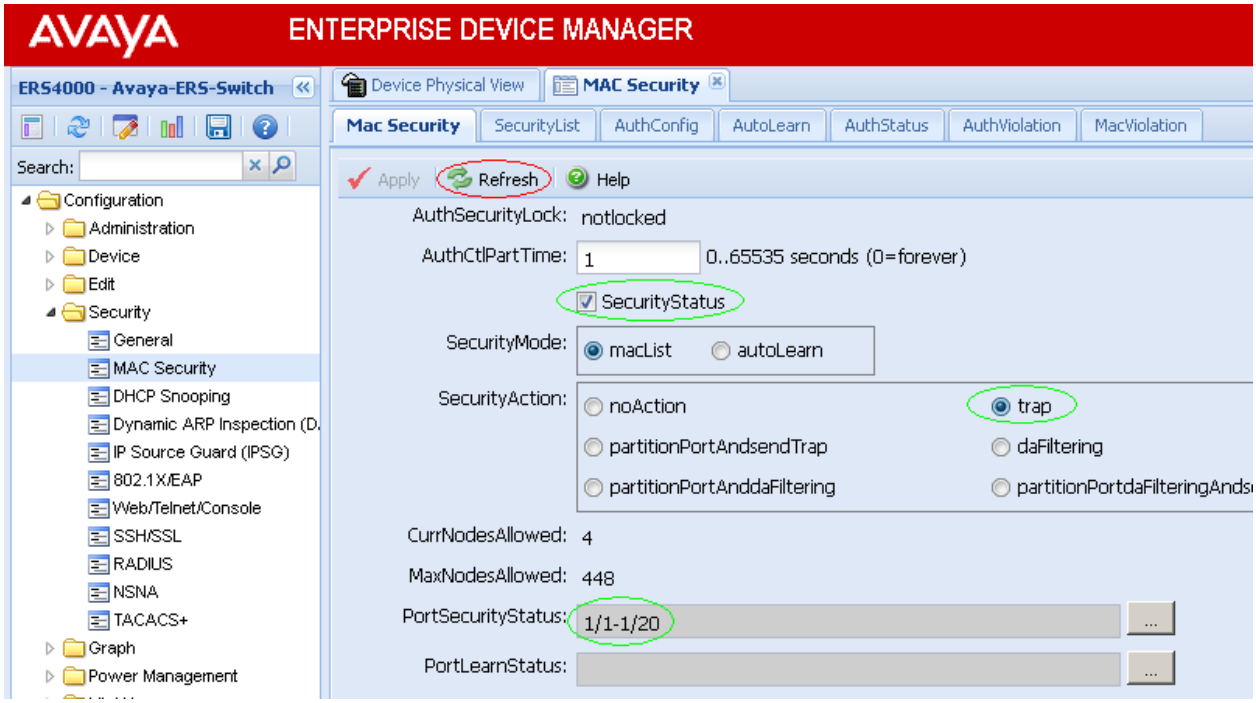
Assign authorized MACs to respective security lists




ENTERPRISE DEVICE MANAGER
ERS4000 - Avaya-ERS-Switch
Search:
Configuration
Administration
Device
Edit
Security
General
MAC Security
DHCP Snooping
Dynamic ARP Inspection (D
IP Source Guard (IPSG)
802.1X/EAP
Web/Telnet/Console
SSH/SSL
RADIUS
NSNA
TACACS+
Graph
Power Management
VLAN
IP
Device Physical View
MAC Security
Mac Security
SecurityList
AuthConfig
AutoLearn
AuthStatus
AuthViolation
MacVio
Insert
Delete
Apply
Refresh
Copy
Paste
Undo
Expo
BrdIndx
PortIndx
MACIndx
AccessCtrlType
SecureList
Source
Lifetime
0
0
00:c0:95:c8:ff:12
allowed
1
static
0
Insert AuthConfig
BrdIndx:
0
0..8
PortIndx:
0
0..50
MACIndx:
00:C0:95:C8:9A:62
(xx:xx:xx:xx:xx:xx)
AutoLearningSticky (sticky-mac)
AccessCtrlType:
allowed
SecureList:
2
0..32
Insert
Cancel
Help

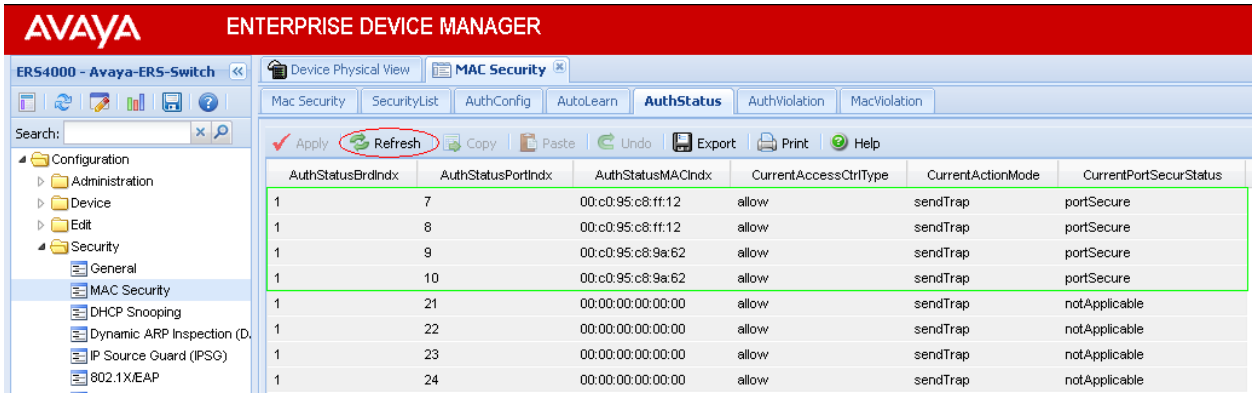
3.3.2.3 Checking MAC Security operational status

Verify that MAC Security is globally enabled and on access ports



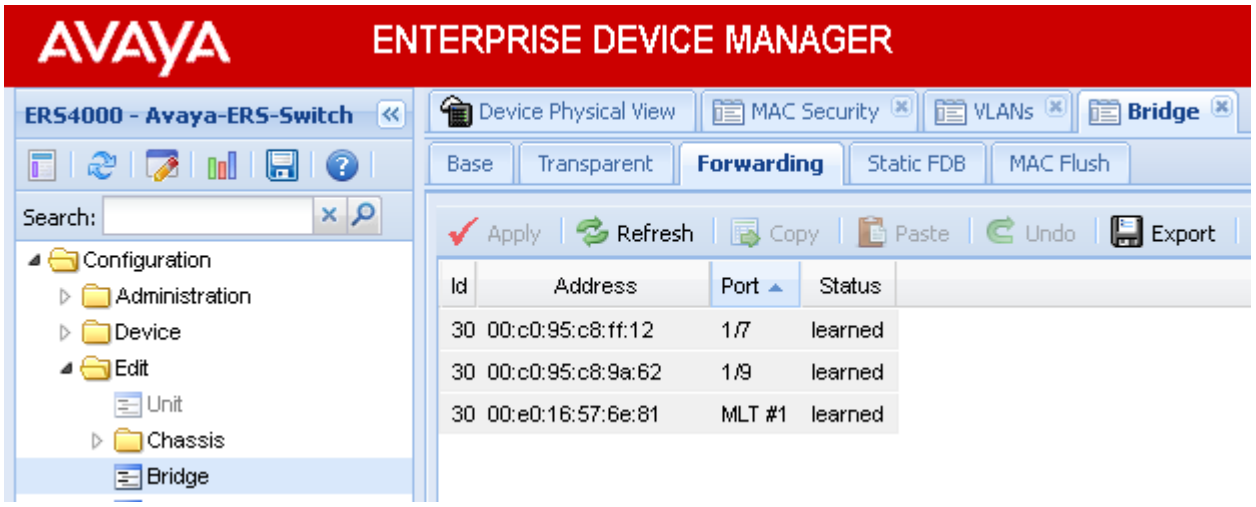
Verify the MAC Security Lists

Verify the authorized MAC addresses appear in the MAC Security MAC table



Note – The authorized MACs are shown against both ports in the Security List.

Verify the FDB on the switch



Note – From the FDB we can easily see which port has the Active NIC connected.

3.3.3 Verifying server connectivity

Verify IP connectivity between the Router and the servers

```
Router#% ping 30.0.0.121; ping 30.0.0.122
30.0.0.121 is alive
30.0.0.122 is alive
```

3.3.4 Verifying server connectivity after Primary NIC failure

Now fail the Active NICs so that the servers start using their backup NICs.

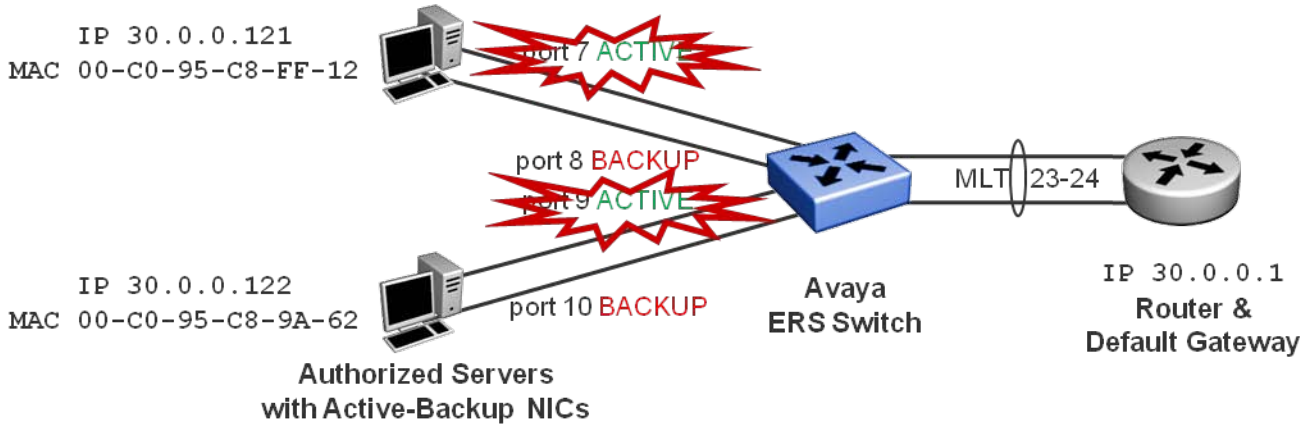


Figure 10: Example 3; servers switch over to Backup NIC

Verify log file on switch

```
Avaya-ERS-Switch# show log
Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
I    01:05:41:03                   1        Link Down Trap for Port: 7
I    01:05:41:08                   2        Link Down Trap for Port: 9
```

Verify IP connectivity between the Router and the servers

```
Router#% ping 30.0.0.121; ping 30.0.0.122
30.0.0.121 is alive
30.0.0.122 is alive
```

Verify the FDB on the switch

```
Avaya-ERS-Switch#% show mac-address-table vid 30
Mac Address Table Aging Time: 300
Learning Enabled Ports 1-26
Number of addresses: 3

   MAC Address    Vid   Type   Source
----------------- ---- ------- -------
```

```
00-C0-95-C8-9A-62   30 Dynamic Port:10
00-C0-95-C8-FF-12   30 Dynamic Port: 8
00-E0-16-57-6E-81   30 Dynamic Trunk:1
```

Note – Servers are now using Standby NIC.

3.3.5 Testing violations

3.3.5.1 Unauthorized device takes server Standby NIC connection

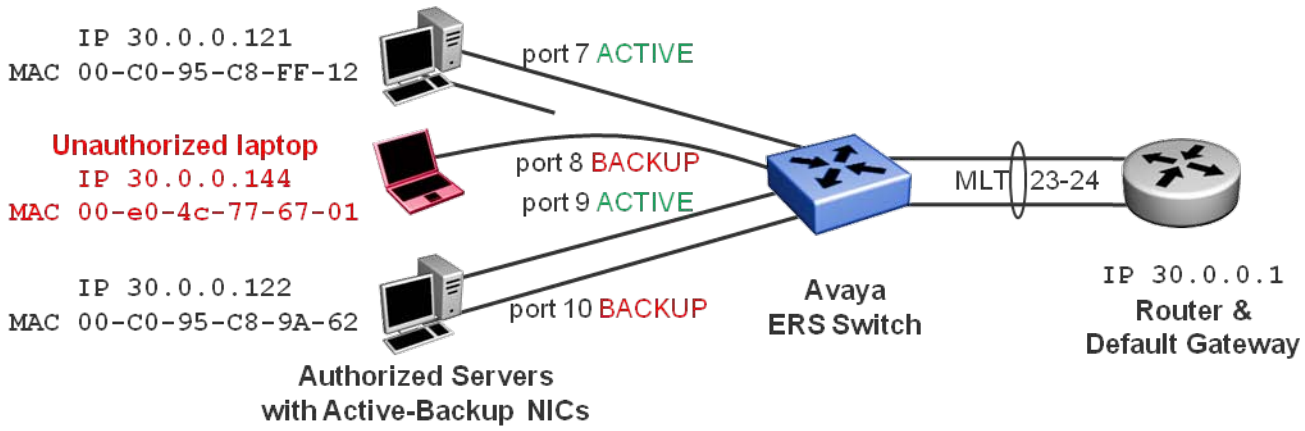


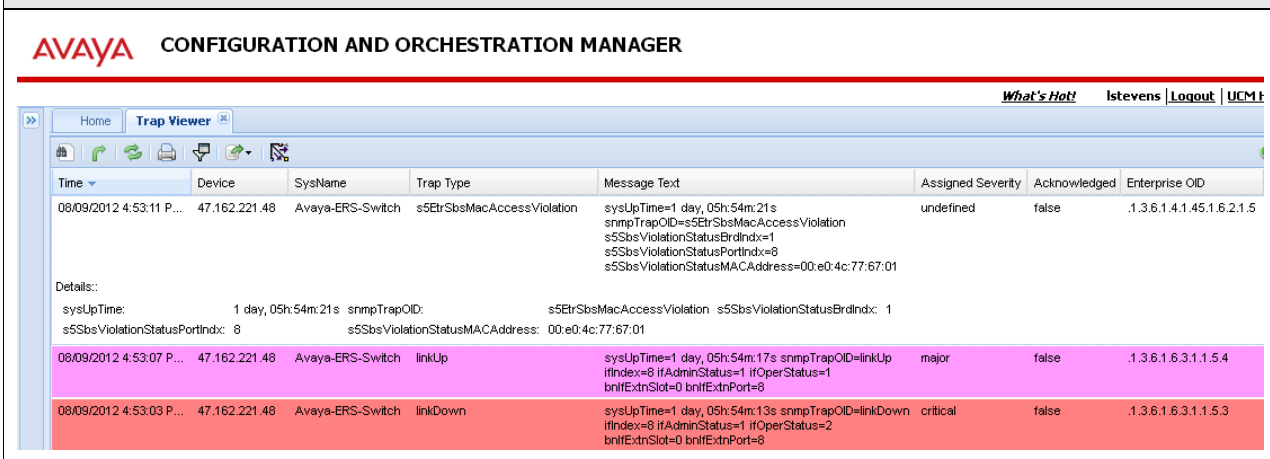
Figure 11: Example 3; unauthorized device takes server Standby NIC connection

The unauthorized device is not able to send any traffic into the network; however it is still able to see broadcast and unknown traffic flowing in the VLAN; if this is undesired the MAC Security should be configured to partition the port upon an access violation.

Verify log file on switch

```
Avaya-ERS-Switch# show log
Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
I    01:05:54:13                   1        Link Down Trap for Port: 8
I    01:05:54:17                   2        Link Up Trap for Port: 8
I    01:05:54:21                   3        Bay Secure intruder MAC 00-e0-4c-77-67-01
                                            port 8
I    01:05:54:21                   4        Trap:  s5EtrNewSbsMacAccessViolation
```

Verify traps on Management station (e.g. VPFM or COM)



3.4 Achieving MAC based VLANs using MAC Security

The Avaya modular ERS8800 and VSP9000 products support MAC based VLANs but the Avaya stackable range does not. This example demonstrates how MAC Security can be used to achieve the same functionality as MAC based VLANs on the stackable product ranges.

In this example, the network administrator wants to tie down a set of MAC addresses to a given VLAN on the ethernet switch. Each VLAN will have a number of authorized MAC addresses which are allowed to communicate on the VLAN across any of the port members of that VLAN. This means that a given MAC address needs to be able to move across any of the port members of the VLAN. Security Lists are used to achieve this.

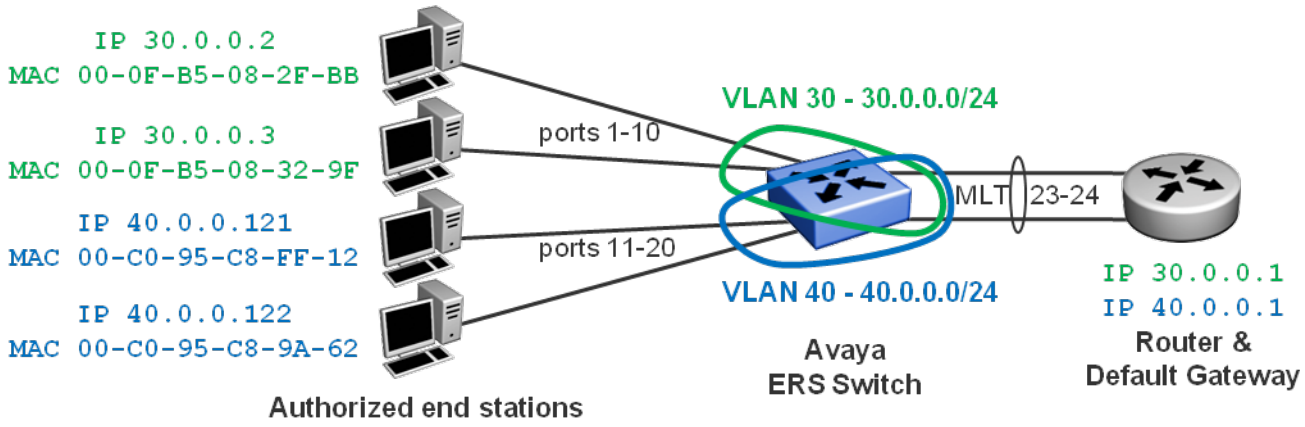


Figure 12: VLAN based MAC-Security; example 4

Since MAC Security MAC learning cannot be used with Security Lists, in this example we are also going to show a possible workaround to achieve MAC learning on Security Lists.

3.4.1 Using ACLI

3.4.1.1 Initial Switch configuration

Create the Security Lists (one for each VLAN)
`Avaya-ERS-Switch(config)#` ***`mac-security security-list 1 1-10`***
`Avaya-ERS-Switch(config)#` ***`mac-security security-list 2 11-20`***

Note – Up to 32 Security Lists can be created.

Globally enable MAC Security
`Avaya-ERS-Switch(config)#` ***`mac-security enable`***
Enable learning on the access ports
`Avaya-ERS-Switch(config)#` ***`mac-security learning-ports 1-20`***
`Avaya-ERS-Switch(config)#` ***`mac-security learning enable`***

Note – There is an alternative syntax for enabling learning on the port interfaces:

```
Avaya-ERS-Switch(config)# interface FastEthernet 1-20
Avaya-ERS-Switch(config-if)# mac-security learning
Avaya-ERS-Switch(config-if)# exit
```

Verify that MAC learning mode is enabled

```
Avaya-ERS-Switch# show mac-security config
MAC Address Security: Enabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
MAC Auto-Learning Age-Time:  60 minutes
MAC Auto-Learning Sticky Mode: Disabled
Current Learning Mode: Enabled
Learn by Ports: 1-20
```

Now wait a couple of minutes to ensure that all MAC addresses on the switch have been recorded.

View recorded MACs so far

```
Avaya-ERS-Switch# show mac-security mac-address-table
Number of addresses: 4

Unit Port Allowed MAC Address   Type
---- ---- ------------------- ---------
0    1    00-0F-B5-08-2F-BB   Static
0    2    00-0F-B5-08-32-9F   Static
0    11   00-C0-95-C8-FF-12   Static
0    12   00-C0-95-C8-9A-62   Static

Security List Allowed MAC Address   Type
------------ ------------------- ---------
```

Note – The MACs have been learnt against the ethernet ports.

We are going to retrieve the running-config of the switch via a Telnet or SSH connection then edit the MAC Security learned MAC addresses in a text editor to point to our Security Lists instead of the ethernet ports and then re-inject the MAC list to the switch config.

Disable MAC security learning mode

```
Avaya-ERS-Switch(config)# mac-security learning disable
```

From a Telnet/SSH connection save the portion in red of the running-config to a text file

```
Avaya-ERS-Switch#% show running-config
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 4826GTS-PWR+
! Software version = v5.6.1.053
!
! Displaying only parameters different to default
!================================================
enable
configure terminal
[...]
!
! *** MAC-Based Security ***
!
mac-security security-list 1 1-10
mac-security security-list 2 11-20
mac-security enable
mac-security mac-address-table address 00.0f.b5.08.2f.bb port 1
mac-security mac-address-table address 00.0f.b5.08.32.9f port 2
mac-security mac-address-table address 00.c0.95.c8.ff.12 port 11
mac-security mac-address-table address 00.c0.95.c8.9a.62 port 12
[...]
```

In a text editor, replace all occurrences of “port 1-10” with “security-list 1” & “port 11-20” with “security-list 2”

File maclist.txt before:

```
configure terminal
mac-security mac-address-table address 00.0f.b5.08.2f.bb port 1
mac-security mac-address-table address 00.0f.b5.08.32.9f port 2
mac-security mac-address-table address 00.c0.95.c8.ff.12 port 11
mac-security mac-address-table address 00.c0.95.c8.9a.62 port 12
end
```

File maclist.txt after:

```
configure terminal
mac-security mac-address-table address 00.0f.b5.08.2f.bb security-list 1
mac-security mac-address-table address 00.0f.b5.08.32.9f security-list 1
mac-security mac-address-table address 00.c0.95.c8.ff.12 security-list 2
mac-security mac-address-table address 00.c0.95.c8.9a.62 security-list 2
end
```

Delete the MAC list on the switch (as we are going to re-inject it)

```
Avaya-ERS-Switch(config)#% no mac-security mac-address-table
MAC addresses auto-learned on ports will not be deleted
```

Copy the maclist.txt file onto a TFTP server and inject it to the switch

```
Avaya-ERS-Switch# configure network address 47.162.221.2 filename maclist.txt
Downloading Config File [|]Downloaded file successfully, executing . . .


Avaya-ERS-Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Avaya-ERS-Switch(config)#mac-security   mac-address-table   address   00.0f.b5.08.2f.bb
security-list 1
Avaya-ERS-Switch(config)#mac-security   mac-address-table   address   00.0f.b5.08.32.9f
security-list 1
Avaya-ERS-Switch(config)#mac-security   mac-address-table   address   00.c0.95.c8.ff.12
security-list 2
Avaya-ERS-Switch(config)#mac-security   mac-address-table   address   00.c0.95.c8.9a.62
security-list 2
Avaya-ERS-Switch(config)#end
Avaya-ERS-Switch#
```

Note – You can also use SFTP instead of TFTP using the command:

`configure sftp address <host-IP> filename maclist.txt username <user>`

Enable MAC Security on the access ports

```
Avaya-ERS-Switch(config)# interface FastEthernet 1-20
Avaya-ERS-Switch(config-if)# mac-security enable
Avaya-ERS-Switch(config-if)# exit
```

3.4.1.2 Checking MAC Security operational status

Verify that MAC Security is globally enabled

```
Avaya-ERS-Switch# show mac-security config
MAC Address Security: Enabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
MAC Auto-Learning Age-Time:  60 minutes
MAC Auto-Learning Sticky Mode: Disabled
Current Learning Mode: Disabled
Learn by Ports: NONE
```

Verify that MAC Security is enabled on the access ports

```
Avaya-ERS-Switch# show mac-security port
Port  Trunk  Security  Auto-Learning  MAC Number
----  -----  --------  -------------  ----------
   1         Enabled      Disabled        2
   2         Enabled      Disabled        2
   3         Enabled      Disabled        2
   4         Enabled      Disabled        2
   5         Enabled      Disabled        2
   6         Enabled      Disabled        2
   7         Enabled      Disabled        2
   8         Enabled      Disabled        2
   9         Enabled      Disabled        2
  10         Enabled      Disabled        2
  11         Enabled      Disabled        2
  12         Enabled      Disabled        2
  13         Enabled      Disabled        2
  14         Enabled      Disabled        2
  15         Enabled      Disabled        2
  16         Enabled      Disabled        2
  17         Enabled      Disabled        2
  18         Enabled      Disabled        2
  19         Enabled      Disabled        2
```

```
  20          Enabled      Disabled        2
  21          Disabled     Disabled        2
  22          Disabled     Disabled        2
  23    1     Disabled     Disabled        2
  24    1     Disabled     Disabled        2
```

Verify the authorized MAC addresses appear in the MAC Security MAC table against Security Lists

```
Avaya-ERS-Switch# show mac-security mac-address-table
Number of addresses: 4

Unit Port Allowed MAC Address   Type
---- ---- ------------------ ---------

Security List Allowed MAC Address   Type
------------- ------------------ ---------
1             00-0F-B5-08-2F-BB   Static
1             00-0F-B5-08-32-9F   Static
2             00-C0-95-C8-9A-62   Static
2             00-C0-95-C8-FF-12   Static
```

Verify the FDB on the switch

```
Avaya-ERS-Switch#% show mac-address-table vid 30
Mac Address Table Aging Time: 300
Learning Enabled Ports 1-26
Number of addresses: 3

   MAC Address    Vid   Type   Source
----------------- ---- ------- -------
00-0F-B5-08-2F-BB   30 Dynamic Port: 1
00-0F-B5-08-32-9F   30 Dynamic Port: 2
00-E0-16-57-6E-81   30 Dynamic Trunk:1

Avaya-ERS-Switch#% show mac-address-table vid 40
Mac Address Table Aging Time: 300
Learning Enabled Ports 1-26
Number of addresses: 3
```

```
   MAC Address    Vid   Type   Source
----------------- ---- ------- -------
00-C0-95-C8-9A-62   40 Dynamic Port:12
00-C0-95-C8-FF-12   40 Dynamic Port:11
00-E0-16-57-6E-8A   40 Dynamic Trunk:1
```

3.4.2 Checking connectivity

Verify IP connectivity between the Router and the end stations

```
Router#% ping 30.0.0.2; ping 30.0.0.3; ping 40.0.0.121; ping 40.0.0.122
30.0.0.2 is alive
30.0.0.3 is alive
40.0.0.121 is alive
40.0.0.122 is alive
```

Move the end-station to alternative ports in the same VLAN

Verify the FDB on the switch

```
Avaya-ERS-Switch#% show mac-address-table vid 30
Mac Address Table Aging Time: 300
Learning Enabled Ports 1-26
Number of addresses: 3

   MAC Address    Vid   Type   Source
----------------- ---- ------- -------
00-0F-B5-08-2F-BB   30 Dynamic Port: 3 (previously was on port 1)
00-0F-B5-08-32-9F   30 Dynamic Port: 4 (previously was on port 2)
00-E0-16-57-6E-81   30 Dynamic Trunk:1

Avaya-ERS-Switch#% show mac-address-table vid 40
Mac Address Table Aging Time: 300
Learning Enabled Ports 1-26
Number of addresses: 3
```

```
   MAC Address     Vid   Type   Source
----------------- ---- ------- -------
00-C0-95-C8-9A-62   40 Dynamic Port:14 (previously was on port 12)
00-C0-95-C8-FF-12   40 Dynamic Port:13 (previously was on port 11)
00-E0-16-57-6E-8A   40 Dynamic Trunk:1
```

Verify IP connectivity between the Router and the end stations again

```
Router#% ping 30.0.0.2; ping 30.0.0.3; ping 40.0.0.121; ping 40.0.0.122
30.0.0.2 is alive
30.0.0.3 is alive
40.0.0.121 is alive
40.0.0.122 is alive
```

3.4.3 Checking Violations

3.4.3.1 Unauthorized MAC

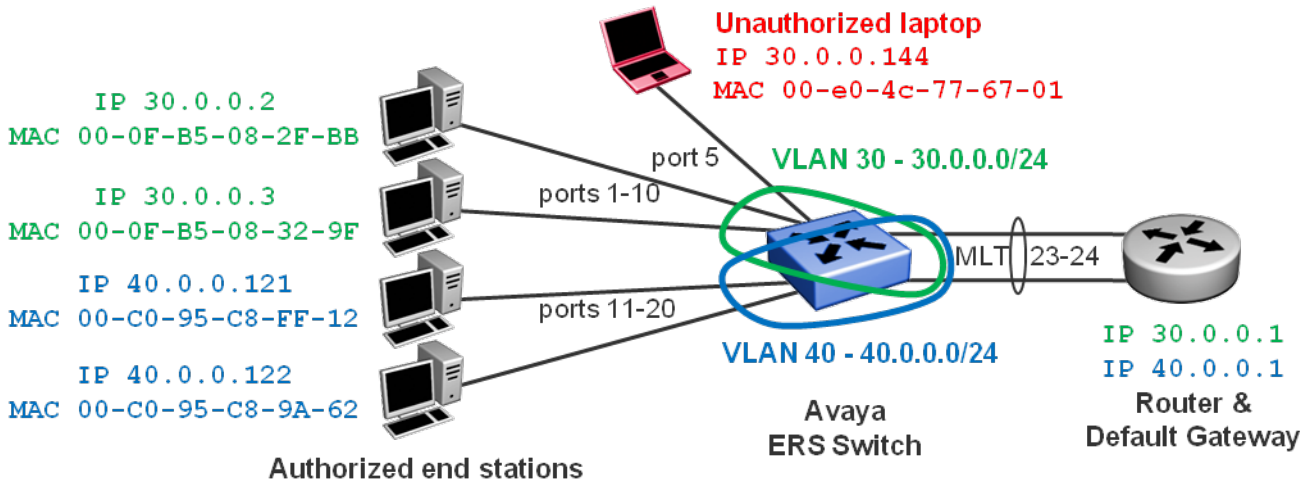


Figure 13: Example 4; unauthorized MAC

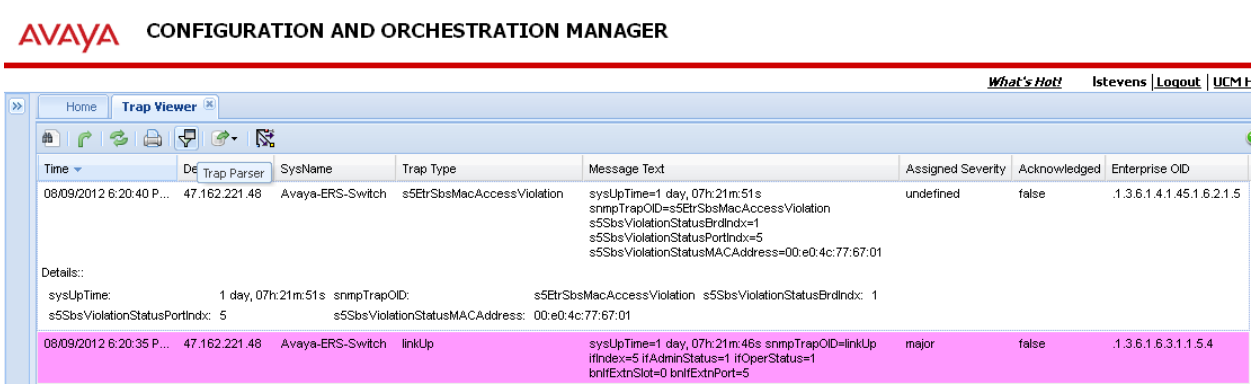
The unauthorized device is not able to send any traffic into the network; however it is still able to see broadcast and unknown traffic flowing in VLAN 30; if this is undesired the MAC Security should be configured to partition the port upon an access violation.

Verify log file on switch

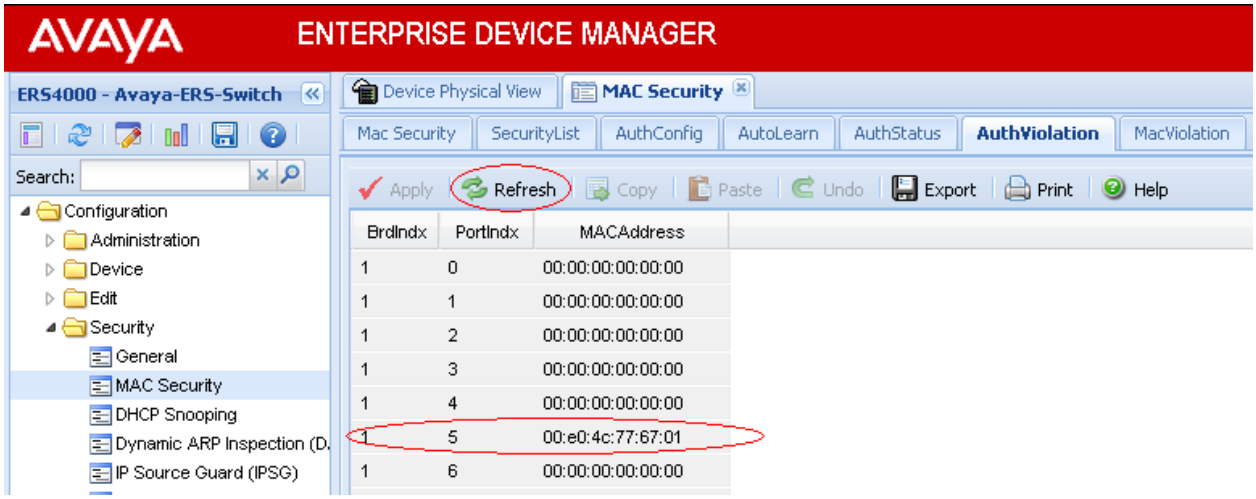
```
Avaya-ERS-Switch# show log
Type Time                          Idx  Src Message
```

```
---- ----------------------------- ---- --- -------
I    01:07:21:46                   1        Link Up Trap for Port: 5
I    01:07:21:51                   2        Bay Secure intruder MAC 00-e0-4c-77-67-01
                                            port 5
I    01:07:21:51                   3        Trap:  s5EtrNewSbsMacAccessViolation
```

Verify traps on Management station (e.g. VPFM or COM)



Verify MAC Security violations from EDM



3.4.3.2 Authorized MACs in wrong VLAN

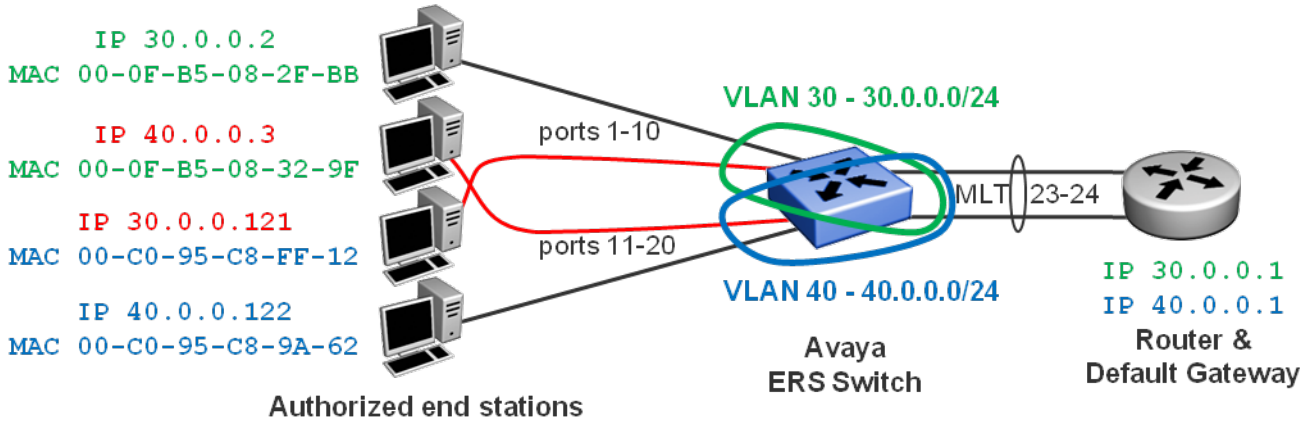


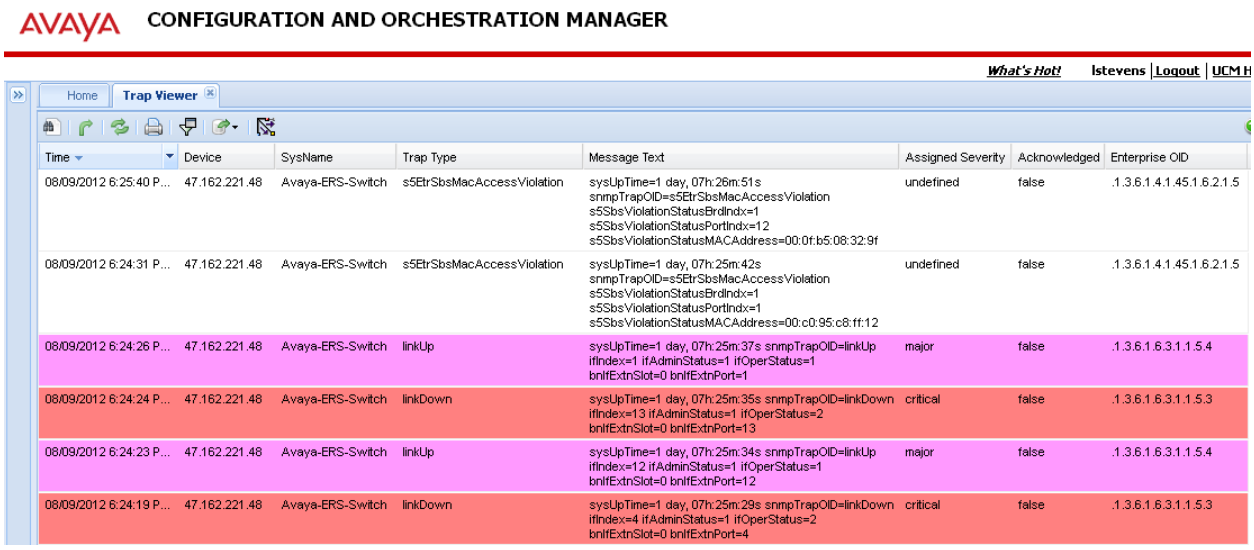
Figure 14: Example 4; authorized MACs in wrong VLAN

Neither of the devices with swapped connections is able to send traffic into the network. Note that, because the swapped devices belonged to different VLANs, their IP addresses were also changed.

Verify log file on switch

```
Avaya-ERS-Switch# show log
Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
I    01:07:25:29                   1        Link Down Trap for Port: 4
I    01:07:25:34                   2        Link Up Trap for Port: 12
I    01:07:25:35                   3        Link Down Trap for Port: 13
I    01:07:25:37                   4        Link Up Trap for Port: 1
I    01:07:25:42                   5        Bay Secure intruder MAC 00-c0-95-c8-ff-12
                                            port 1
I    01:07:25:42                   6        Trap:  s5EtrNewSbsMacAccessViolation
I    01:07:26:51                   7        Bay Secure intruder MAC 00-0f-b5-08-32-9f
                                            port 12
I    01:07:26:51                   8        Trap:  s5EtrNewSbsMacAccessViolation
```

Verify traps on Management station (e.g. VPFM or COM)



Time	Device	SysName	Trap Type	Message Text	Assigned Severity	Acknowledged	Enterprise OID
08/09/2012 6:25:40 P...	47.162.221.48	Avaya-ERS-Switch	s5EtrSbsMacAccessViolation	sysUpTime=1 day, 07h:26m:51s snmpTrapOID=s5EtrSbsMacAccessViolation s5SbsViolationStatusBrdIndx=1 s5SbsViolationStatusPortIndx=12 s5SbsViolationStatusMACAddress=00:0f:b5:08:32:9f	undefined	false	.1.3.6.1.4.1.45.1.6.2.1.5
08/09/2012 6:24:31 P...	47.162.221.48	Avaya-ERS-Switch	s5EtrSbsMacAccessViolation	sysUpTime=1 day, 07h:25m:42s snmpTrapOID=s5EtrSbsMacAccessViolation s5SbsViolationStatusBrdIndx=1 s5SbsViolationStatusPortIndx=1 s5SbsViolationStatusMACAddress=00:c0:95:c8:ff:12	undefined	false	.1.3.6.1.4.1.45.1.6.2.1.5
08/09/2012 6:24:26 P...	47.162.221.48	Avaya-ERS-Switch	linkUp	sysUpTime=1 day, 07h:25m:37s snmpTrapOID=linkUp ifIndex=1 ifAdminStatus=1 ifOperStatus=1 bnIfExtnSlot=0 bnIfExtnPort=1	major	false	.1.3.6.1.6.3.1.1.5.4
08/09/2012 6:24:24 P...	47.162.221.48	Avaya-ERS-Switch	linkDown	sysUpTime=1 day, 07h:25m:35s snmpTrapOID=linkDown ifIndex=13 ifAdminStatus=1 ifOperStatus=2 bnIfExtnSlot=0 bnIfExtnPort=13	critical	false	.1.3.6.1.6.3.1.1.5.3
08/09/2012 6:24:23 P...	47.162.221.48	Avaya-ERS-Switch	linkUp	sysUpTime=1 day, 07h:25m:34s snmpTrapOID=linkUp ifIndex=12 ifAdminStatus=1 ifOperStatus=1 bnIfExtnSlot=0 bnIfExtnPort=12	major	false	.1.3.6.1.6.3.1.1.5.4
08/09/2012 6:24:19 P...	47.162.221.48	Avaya-ERS-Switch	linkDown	sysUpTime=1 day, 07h:25m:29s snmpTrapOID=linkDown ifIndex=4 ifAdminStatus=1 ifOperStatus=2 bnIfExtnSlot=0 bnIfExtnPort=4	critical	false	.1.3.6.1.6.3.1.1.5.3

Verify IP connectivity between the Router and the end stations again

```
Router#% ping 30.0.0.2; ping 40.0.0.3; ping 30.0.0.121; ping 40.0.0.122
30.0.0.2 is alive
no answer from 40.0.0.3
no answer from 30.0.0.121
40.0.0.122 is alive
```

4. Auto-Learning with MaxMacs example

4.1 Ensuring that every access port is used by one and only one device

In this example, the network administrator wants to ensure that user access ports of the network are seeing one and only one device connected. This is a very effective way to detect and prevent users from connecting additional devices to their network connection. For instance, this will immediately detect and prevent a user from introducing a small ethernet hub/switch device on his network connection in an attempt to add extra (unauthorized) devices to the network. Likewise, this will prevent users from connecting a WLAN Access Point (AP) to their network connection, as the end result would be the same.

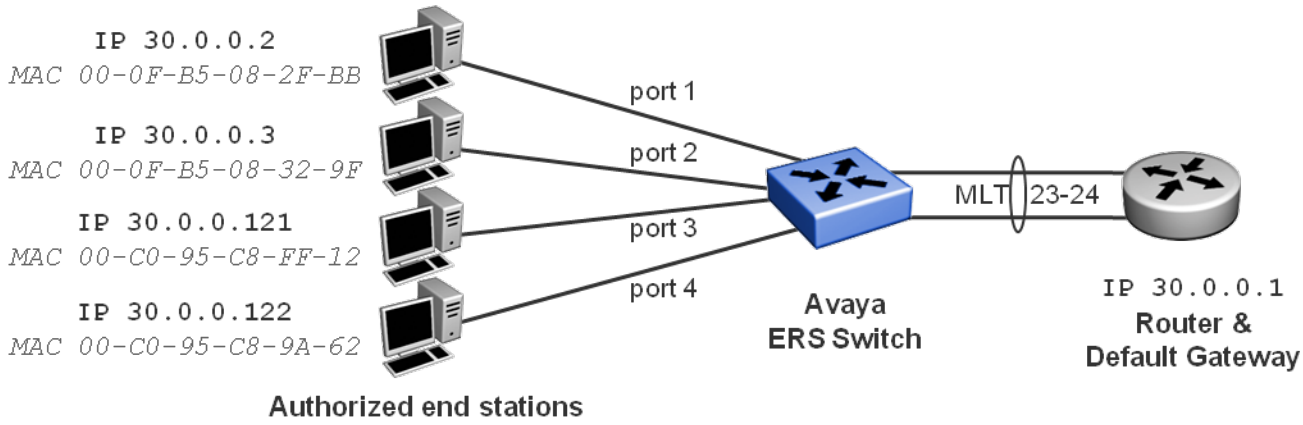


Figure 15: Auto-Learning with MaxMacs; example 5

Note that the device's MAC address is not essential here; it is simply recorded to ensure that no additional MAC (and hence device) can be allowed on the same ethernet port.

Also note that without the Sticky-MAC feature (covered in the next example) MAC bindings in the security table are not persistent across port bounces or switch reboots and can be aged out of the table. This means that in this example it is possible for devices to physically move from one port to the other, even on ports where a MAC had already been recorded. This is because to move those devices the ethernet cable would have to be disconnected and then re-connected on a different port and hence any MAC bindings on the receiving port would have been flushed when the port went down.

The only violation we will be detecting in this mode is multiple MACs on the same port and because we cannot control the order in which those MAC addresses are learnt, it is not useful to rely on the default MAC security violation behavior of denying access to just those MACs learnt later while allowing access to the 1st MAC learnt on the port. Therefore in this example we will configure the ports to partition upon a MAC security violation.

4.1.1 Using ACLI

4.1.1.1 Initial Switch configuration

Globally enable MAC Security
`Avaya-ERS-Switch(config)#` ***`mac-security enable`***

Enable Auto-Learning, MacMac=1 and MAC Security on the access ports

```
Avaya-ERS-Switch(config)# interface FastEthernet 1-20
Avaya-ERS-Switch(config-if)# mac-security auto-learning enable max-addrs 1
Avaya-ERS-Switch(config-if)# mac-security enable
Avaya-ERS-Switch(config-if)# exit
```

Enable permanent partition of the port upon security violation

```
Avaya-ERS-Switch# mac-security intrusion-detect forever
```

Tip – It is also possible to partition the port just temporarily, instead of permanently using these commands:

```
Avaya-ERS-Switch# mac-security intrusion-detect enable
Avaya-ERS-Switch# mac-security intrusion-timer <0-65535>
```

4.1.1.2 Checking MAC Security operational status

Verify that MAC Security is globally enabled

```
Avaya-ERS-Switch# show mac-security config
MAC Address Security: Enabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Forever
DA Filtering on Intrusion Detected: Disabled
MAC Auto-Learning Age-Time:  60 minutes
MAC Auto-Learning Sticky Mode: Disabled
Current Learning Mode: Disabled
Learn by Ports: NONE
```

Verify that Auto-Learning, MaxMac=1 and MAC Security is enabled on the access ports

```
Avaya-ERS-Switch# show mac-security port
Port  Trunk  Security  Auto-Learning  MAC Number
----  -----  --------  -------------  ----------
   1         Enabled      Enabled         1
   2         Enabled      Enabled         1
   3         Enabled      Enabled         1
   4         Enabled      Enabled         1
   5         Enabled      Enabled         1
   6         Enabled      Enabled         1
```

```
   7          Enabled      Enabled         1
   8          Enabled      Enabled         1
   9          Enabled      Enabled         1
  10          Enabled      Enabled         1
  11          Enabled      Enabled         1
  12          Enabled      Enabled         1
  13          Enabled      Enabled         1
  14          Enabled      Enabled         1
  15          Enabled      Enabled         1
  16          Enabled      Enabled         1
  17          Enabled      Enabled         1
  18          Enabled      Enabled         1
  19          Enabled      Enabled         1
  20          Enabled      Enabled         1
  21          Disabled     Disabled        2
  22          Disabled     Disabled        2
  23    1     Disabled     Disabled        2
  24    1     Disabled     Disabled        2
```

Verify the MAC Security MAC table; this will hold the MAC of the 1st device recorded on the ethernet ports; NOTE that the type is Automatic

```
Avaya-ERS-Switch# show mac-security mac-address-table
Number of addresses: 4

Unit Port Allowed MAC Address   Type
---- ---- ------------------- ---------
0    1    00-0F-B5-08-2F-BB   Automatic
0    2    00-0F-B5-08-32-9F   Automatic
0    3    00-C0-95-C8-FF-12   Automatic
0    4    00-C0-95-C8-9A-62   Automatic

Security List Allowed MAC Address   Type
------------- ------------------- ---------
```

Verify the FDB on the switch

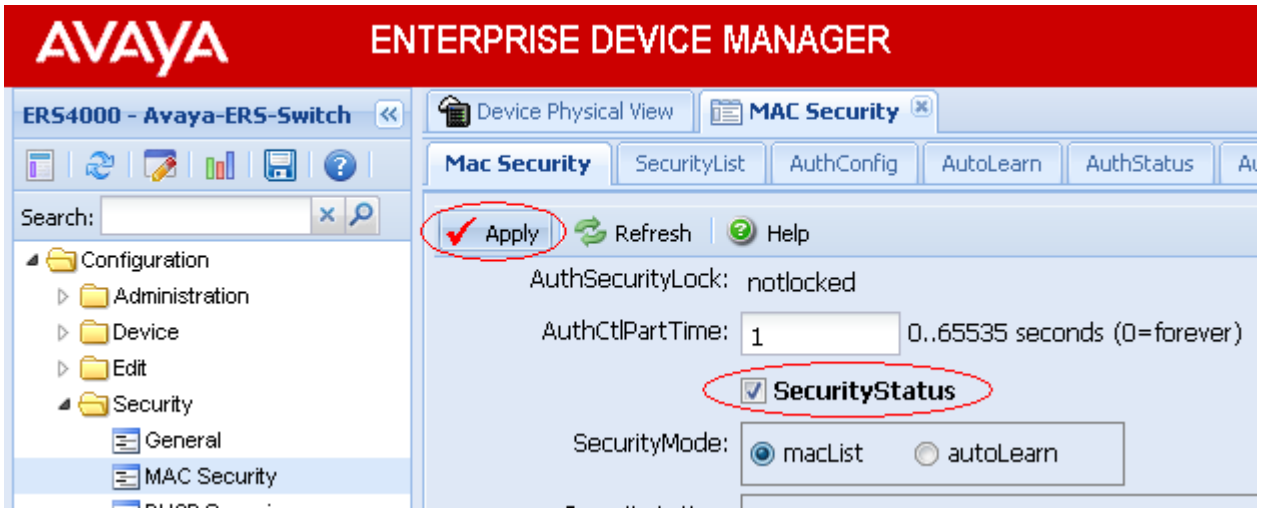
```
Avaya-ERS-Switch# show mac-address-table vid 30
```

```
Mac Address Table Aging Time: 300
Learning Enabled Ports 1-26
Number of addresses: 5

   MAC Address     Vid   Type    Source
----------------- ---- ------- -------
00-0F-B5-08-2F-BB   30 Dynamic Port: 1
00-0F-B5-08-32-9F   30 Dynamic Port: 2
00-C0-95-C8-9A-62   30 Dynamic Port: 4
00-C0-95-C8-FF-12   30 Dynamic Port: 3
00-E0-16-57-6E-81   30 Dynamic Trunk:1
```

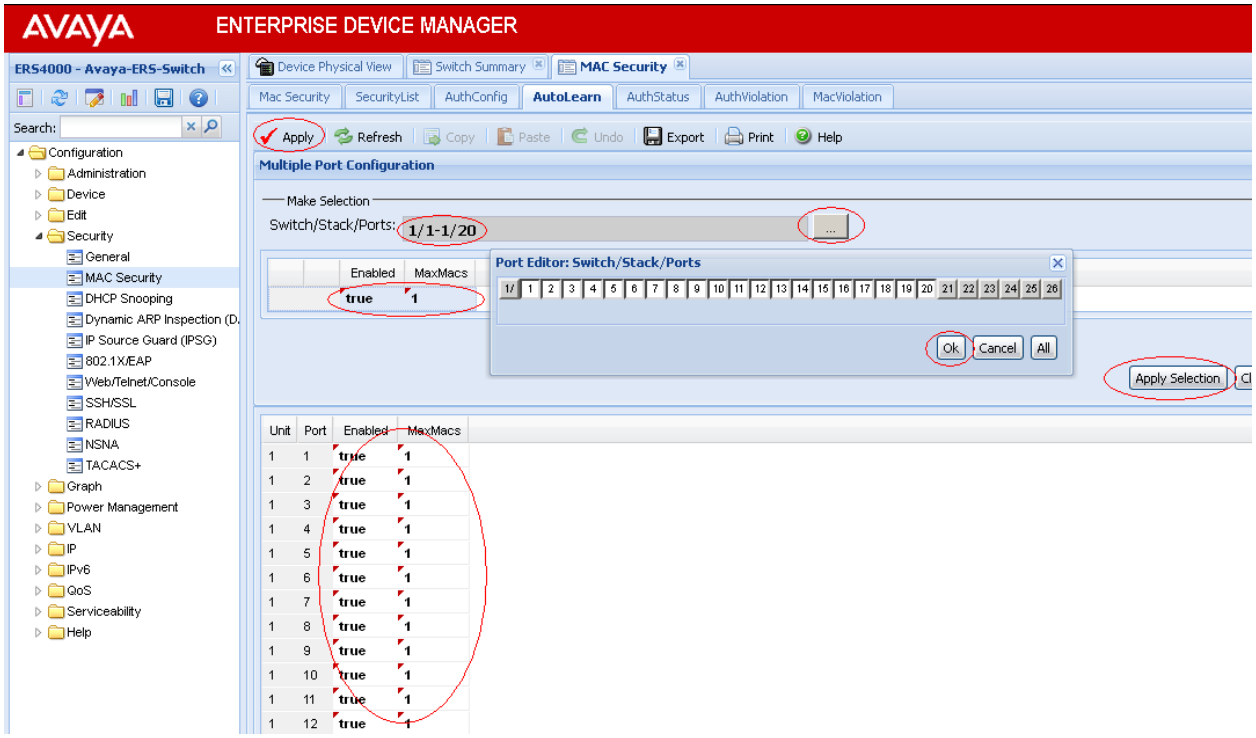
4.1.2 Using EDM

4.1.2.1 Initial Switch configuration

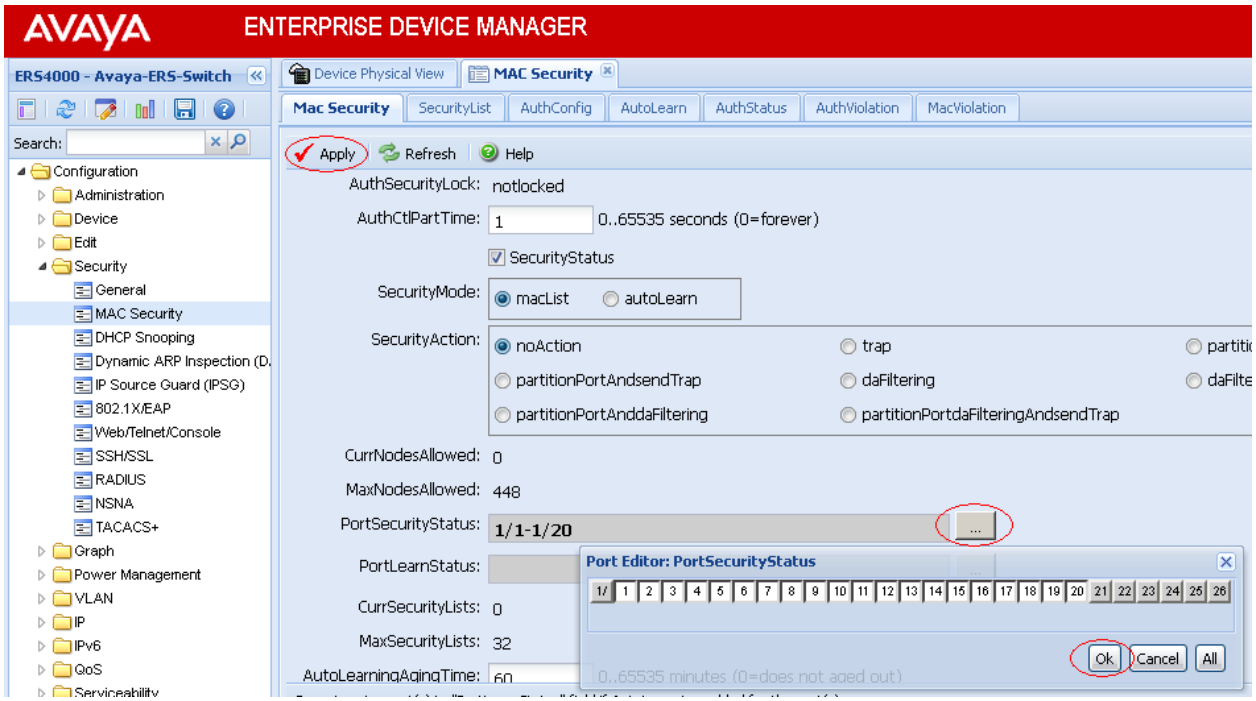
Globally enable MAC Security



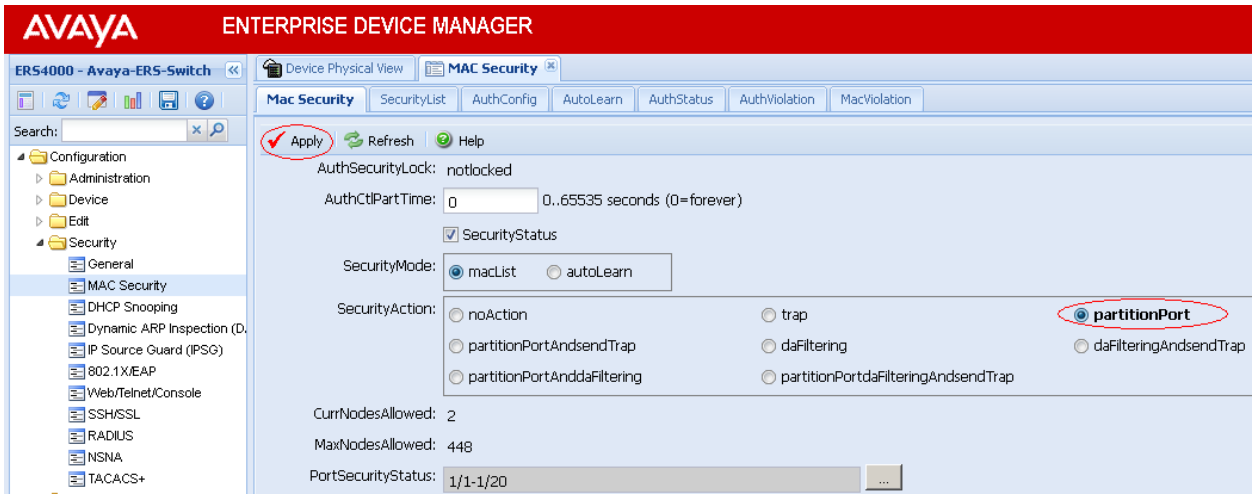
Enable Auto-Learning & MacMac=1 on access ports



Enable MAC Security on the access ports

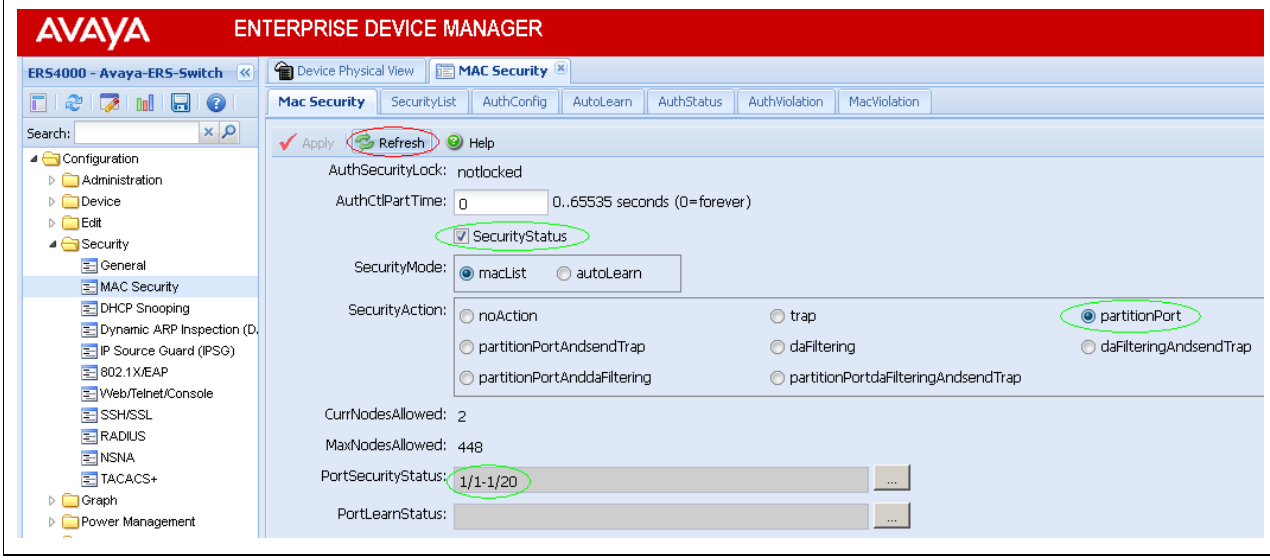


Enable permanent partition of the port upon security violation

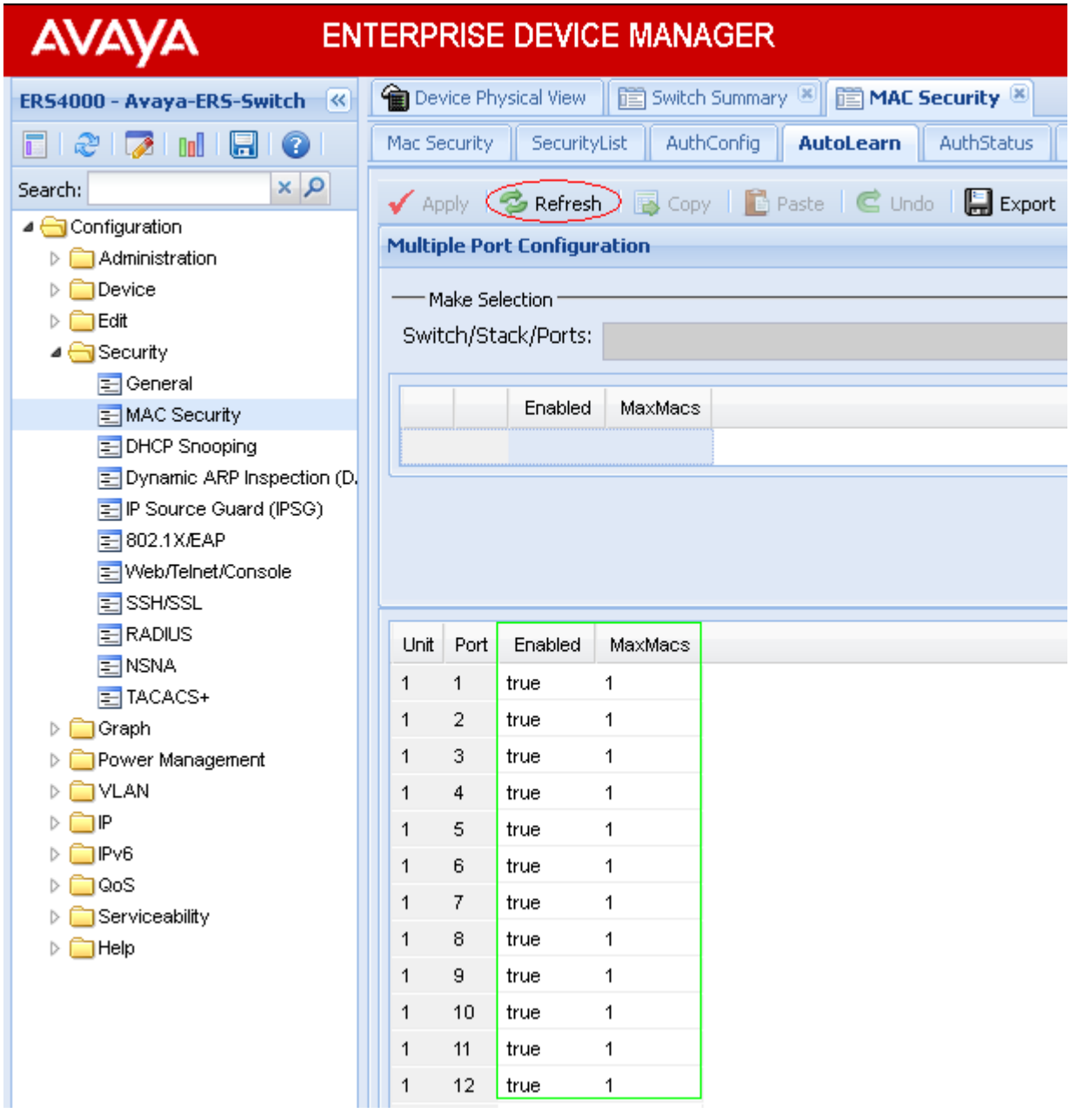


4.1.2.2 Checking MAC Security operational status

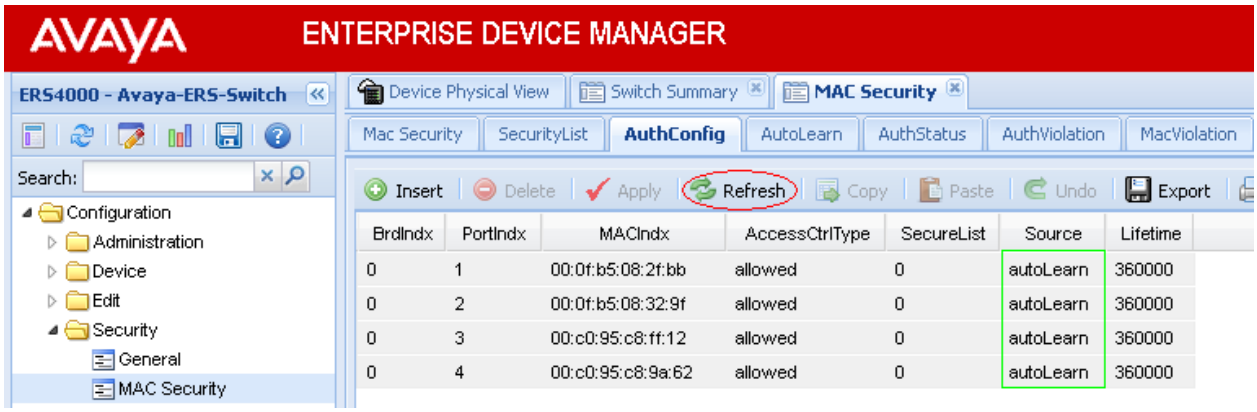
Verify that MAC Security is globally enabled and on access ports and with Security Action set to partitionPort



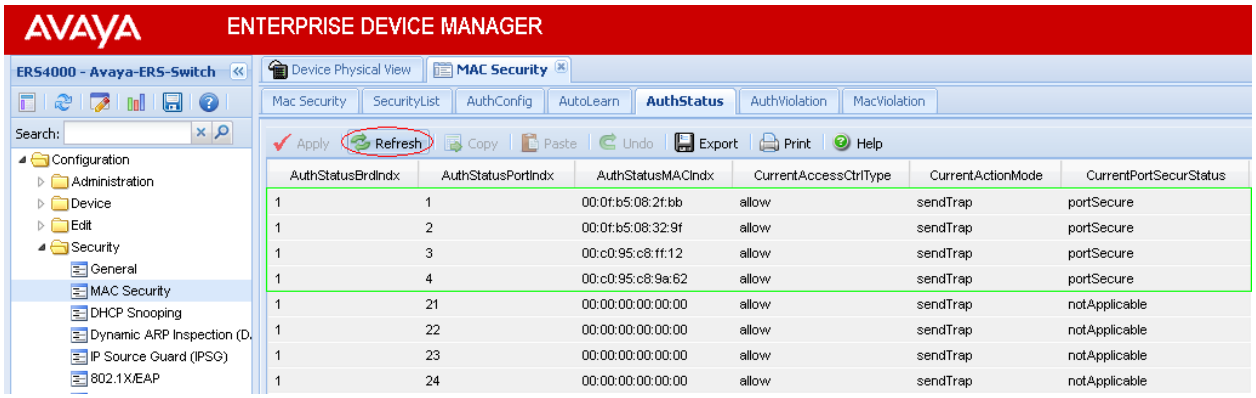
Verify that Auto-Learn is enabled on the access ports and that MacMax is set to 1



Verify the MAC Security MAC table; this will hold the MAC of the 1st device recorded on the ethernet ports; NOTE that the type is autoLearn



Verify ports 1-4 are authenticated with the correct MAC address



4.1.3 Verifying user connectivity

Verify IP connectivity between the Router and the end stations

```
Router#% ping 30.0.0.2; ping 30.0.0.3; ping 30.0.0.121; ping 30.0.0.122
30.0.0.2 is alive
30.0.0.3 is alive
30.0.0.121 is alive
30.0.0.122 is alive
```

4.1.4 Testing violations

4.1.4.1 Unauthorized hub/switch connected to the network

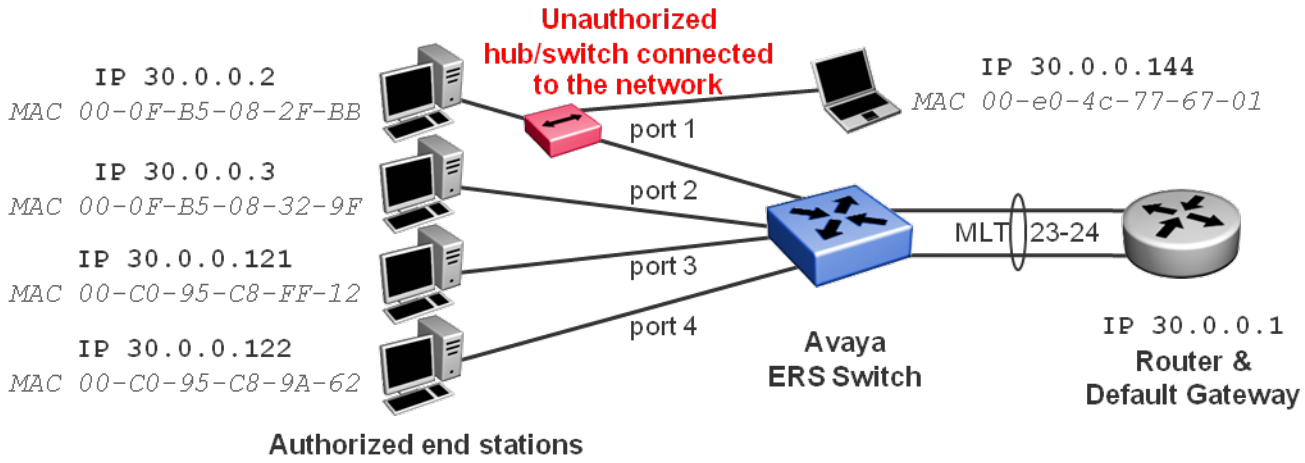


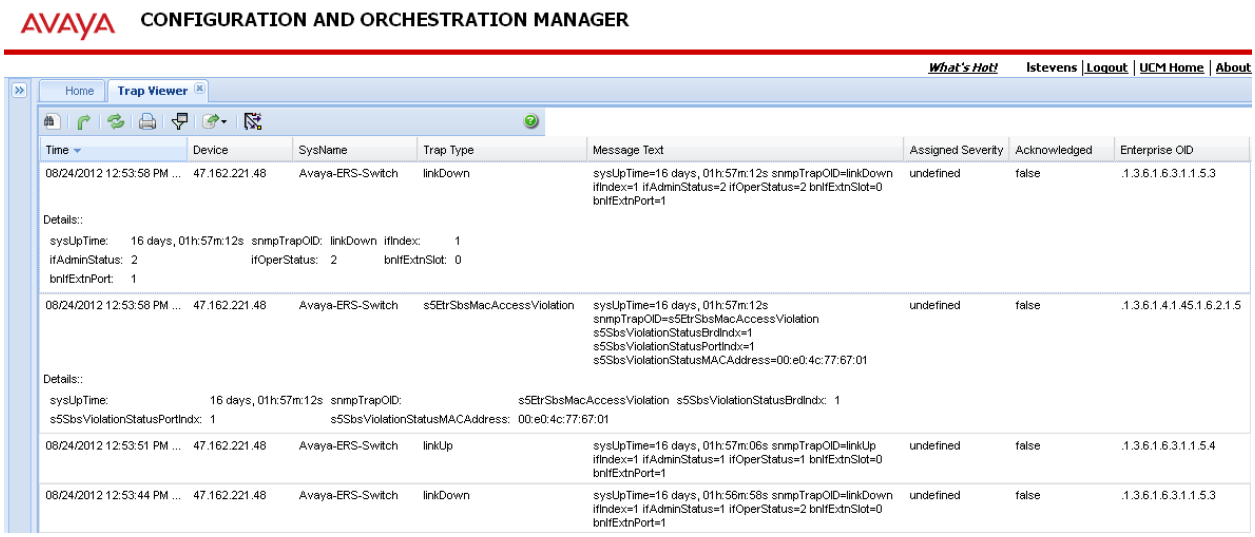
Figure 16: Example 5; an unauthorized hub/switch is connected to the network

Port 1 is partitioned.

Verify log file on switch

```
Avaya-ERS-Switch# show log
Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
I    16:01:56:58                   1        Link Down Trap for Port: 1
I    16:01:57:06                   2        Link Up Trap for Port: 1
I    16:01:57:12                   3        Bay Secure: Exceeded 1 per-port MAC
                                            addresses on port 0/1
I    16:01:57:12                   4        Bay Secure intruder MAC 00-e0-4c-77-67-01
                                            port 1
I    16:01:57:12                   5        Link Down Trap for Port: 1
I    16:01:57:12                   6        Trap:  s5EtrNewSbsMacAccessViolation
```

Verify traps on Management station (e.g. VPFM or COM)



4.1.4.2 Unauthorized WLAN Access Point connected to the network

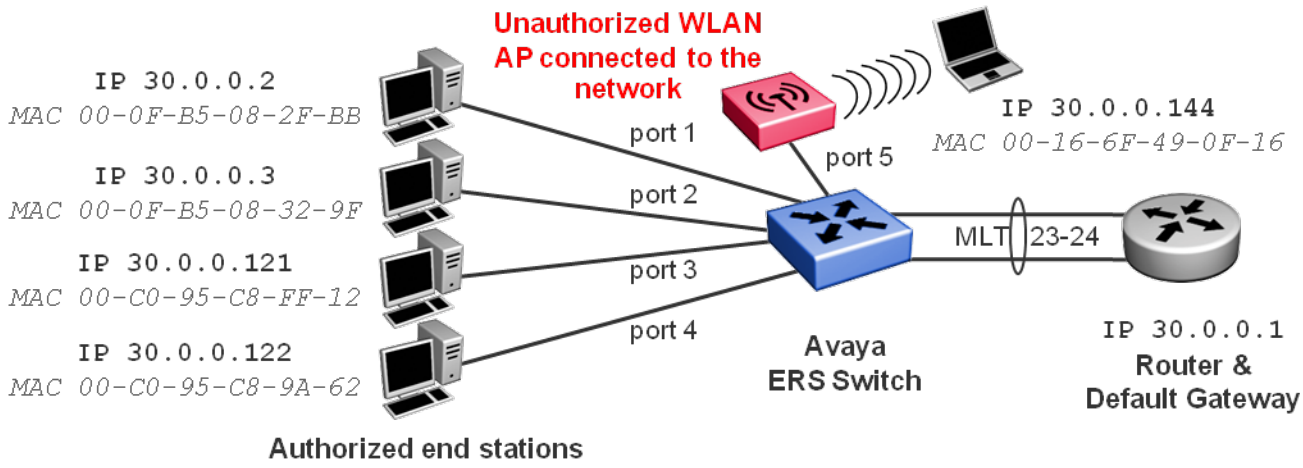


Figure 17: Example 5; an unauthorized WLAN AP is connected to the network

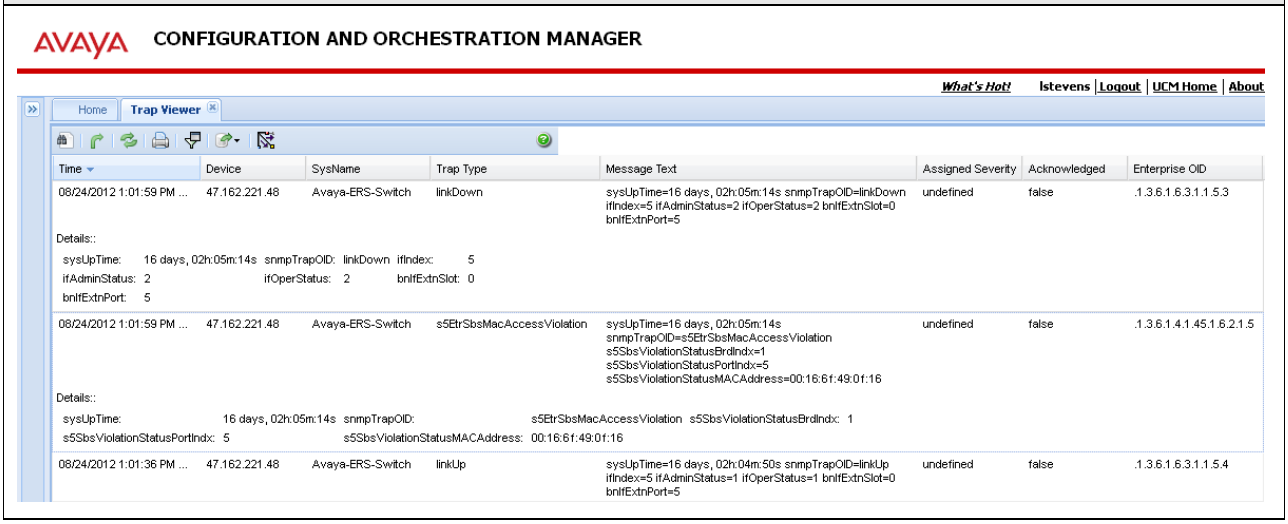
Port 5 is partitioned.

Verify log file on switch

```
Avaya-ERS-Switch# show log
Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
I    16:02:04:50                   1        Link Up Trap for Port: 5
I    16:02:05:14                   2        Bay Secure: Exceeded 1 per-port MAC
```

```
                                        addresses on port 0/5
I    16:02:05:14                3       Bay Secure intruder MAC 00-16-6f-49-0f-16
                                        port 5
I    16:02:05:14                4       Link Down Trap for Port: 5
I    16:02:05:14                5       Trap:  s5EtrNewSbsMacAccessViolation
```

Verify traps on Management station (e.g. VPFM or COM)



5. Auto-Learning with Sticky-MAC example

5.1 MAC Security without having to pre-provision ports when new devices added

In this example, the network administrator, wants the benefits of MAC Security (as provided by regular MAC Security configuration) but does not want the hassle of having to manually provision MAC Security ports whenever a new device is added to the network. The assumption is made that when a new device is added to the network the new MAC address recorded on the ethernet port is automatically tied to that port and considered as authorized. In this scenario, what is considered unauthorized and hence a violation is for a known MAC address to move to a different access port or for additional MAC addresses to be seen on an access port where a MAC address was already recorded.

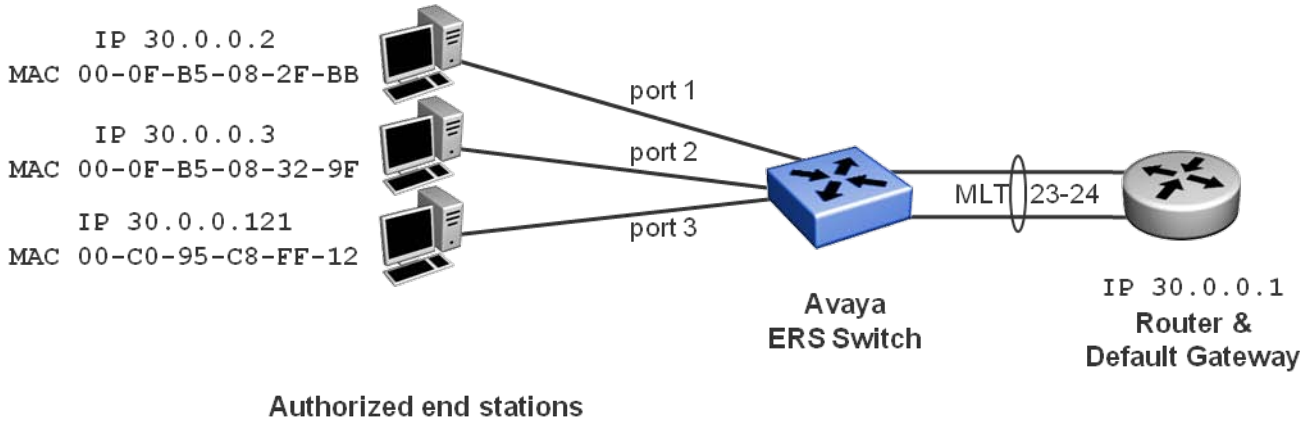


Figure 18: MAC Security without any provisioning of new devices; example 6

5.1.1 Using ACLI

5.1.1.1 Initial Switch configuration

Globally enable MAC Security
Avaya-ERS-Switch(config)# ***mac-security enable***
Enable Auto-Learning Sticky-MAC mode
Avaya-ERS-Switch(config)# ***mac-security auto-learning sticky***
Enable Auto-Learning, MacMac=1 and MAC Security on the access ports
Avaya-ERS-Switch(config)# ***interface FastEthernet 1-20*** Avaya-ERS-Switch(config-if)# ***mac-security auto-learning enable max-addrs 1*** Avaya-ERS-Switch(config-if)# ***mac-security enable*** Avaya-ERS-Switch(config-if)# ***exit***

Warning – Avaya recommends that autosave is disabled when sticky mac is enabled. Otherwise the switch will be constantly saving the configuration when learning new MAC addresses in the MAC Security table. If autosave is disabled it is important to remember to manually save the config prior to any switch restart.

```
Avaya-ERS-Switch(config)# no autosave enable
```

```
Avaya-ERS-Switch(config)# write memory (save config, copy config nvram or copy config nvram block <1-2> also works)
```

5.1.1.2 Checking MAC Security operational status

Verify that MAC Security is globally enabled with Sticky-MAC mode enabled

```
Avaya-ERS-Switch# show mac-security config
MAC Address Security: Enabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
MAC Auto-Learning Age-Time: Forever
MAC Auto-Learning Sticky Mode: Enabled
Current Learning Mode: Disabled
Learn by Ports: NONE
```

Verify that Auto-Learning, MaxMac=1 and MAC Security is enabled on the access ports

```
Avaya-ERS-Switch# show mac-security port
Port  Trunk  Security  Auto-Learning  MAC Number
----  -----  --------  -------------  ----------
   1         Enabled      Enabled         1
   2         Enabled      Enabled         1
   3         Enabled      Enabled         1
   4         Enabled      Enabled         1
   5         Enabled      Enabled         1
   6         Enabled      Enabled         1
   7         Enabled      Enabled         1
   8         Enabled      Enabled         1
   9         Enabled      Enabled         1
  10         Enabled      Enabled         1
  11         Enabled      Enabled         1
  12         Enabled      Enabled         1
  13         Enabled      Enabled         1
```

```
  14          Enabled      Enabled         1
  15          Enabled      Enabled         1
  16          Enabled      Enabled         1
  17          Enabled      Enabled         1
  18          Enabled      Enabled         1
  19          Enabled      Enabled         1
  20          Enabled      Enabled         1
  21          Disabled     Disabled        2
  22          Disabled     Disabled        2
  23    1     Disabled     Disabled        2
  24    1     Disabled     Disabled        2
```

Verify the MAC Security MAC table; this will hold the MAC of the 1st device recorded on the ethernet ports; NOTE that the type is Sticky

```
Avaya-ERS-Switch# show mac-security mac-address-table
Number of addresses: 3

Unit Port Allowed MAC Address   Type
---- ---- ------------------- ---------
0    1    00-0F-B5-08-2F-BB   Sticky
0    2    00-0F-B5-08-32-9F   Sticky
0    3    00-C0-95-C8-FF-12   Sticky

Security List Allowed MAC Address   Type
------------- ------------------- ---------
```

Verify the FDB on the switch

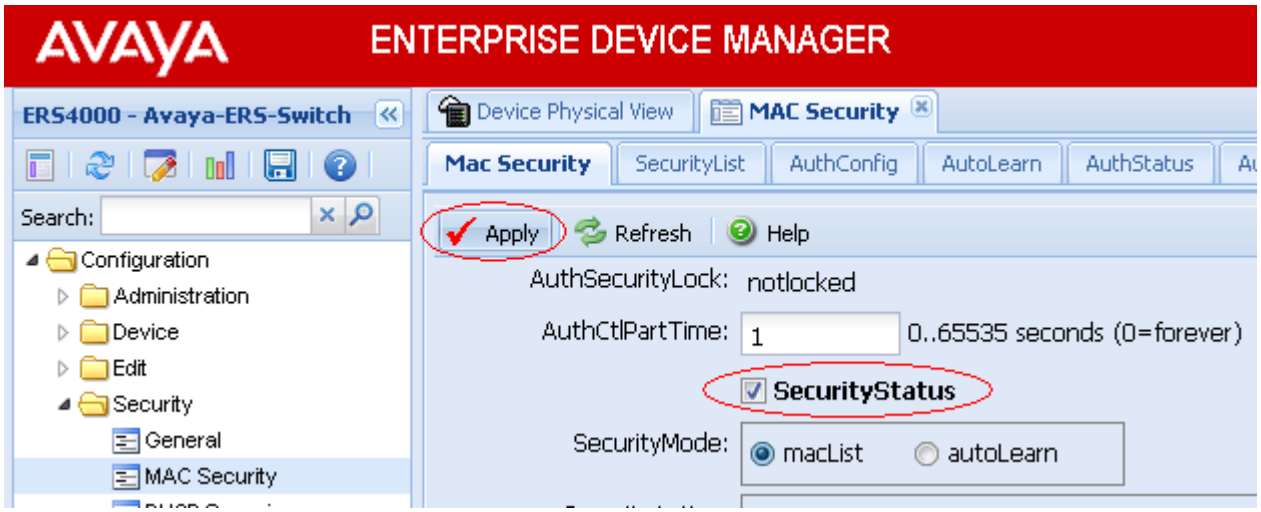
```
Avaya-ERS-Switch# show mac-address-table vid 30
Mac Address Table Aging Time: 300
Learning Enabled Ports 1-26
Number of addresses: 4

   MAC Address    Vid   Type   Source
----------------- ---- ------- -------
00-0F-B5-08-2F-BB   30 Dynamic Port: 1
00-0F-B5-08-32-9F   30 Dynamic Port: 2
```

```
00-C0-95-C8-FF-12   30 Dynamic Port: 3
00-E0-16-57-6E-81   30 Dynamic Trunk:1
```

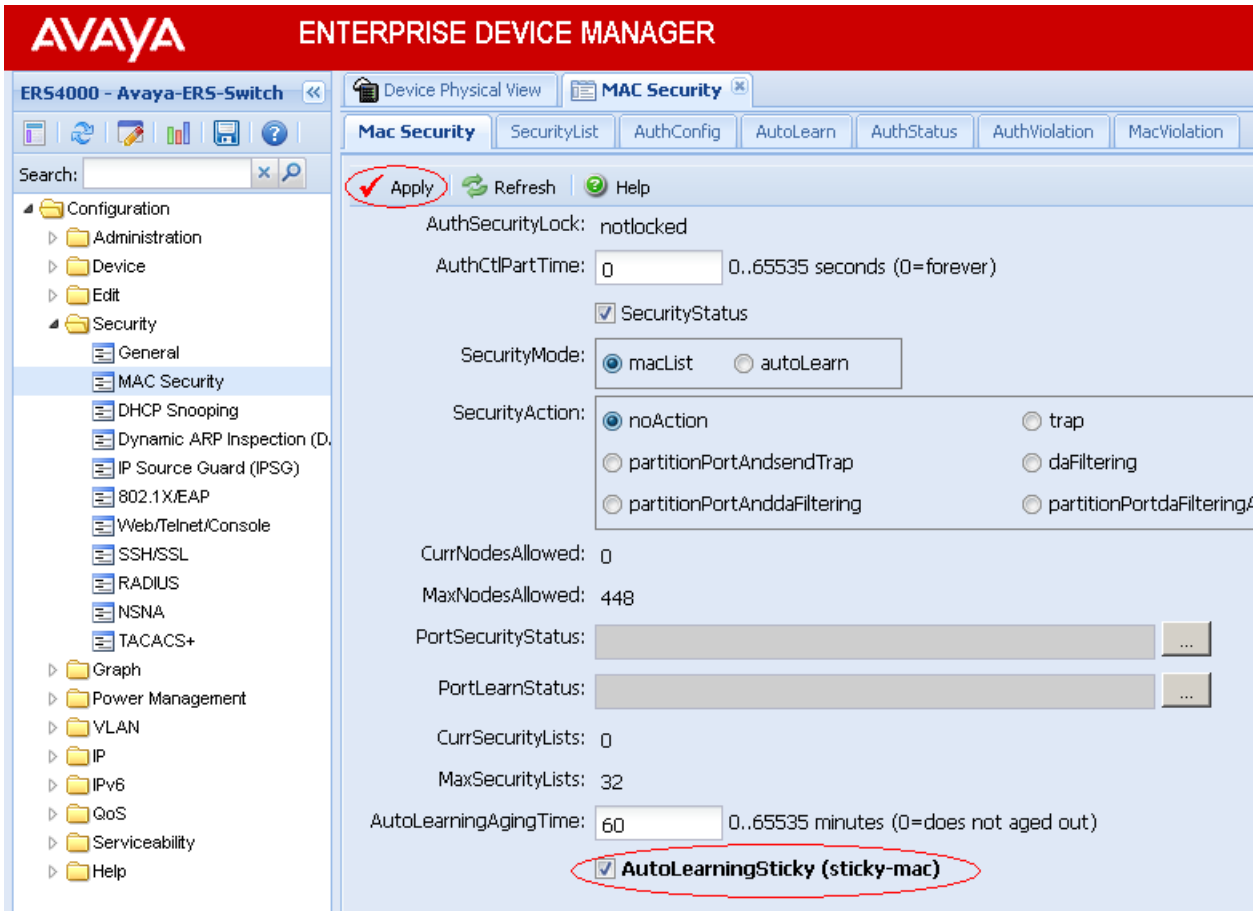
5.1.2 Using EDM

5.1.2.1 Initial Switch configuration

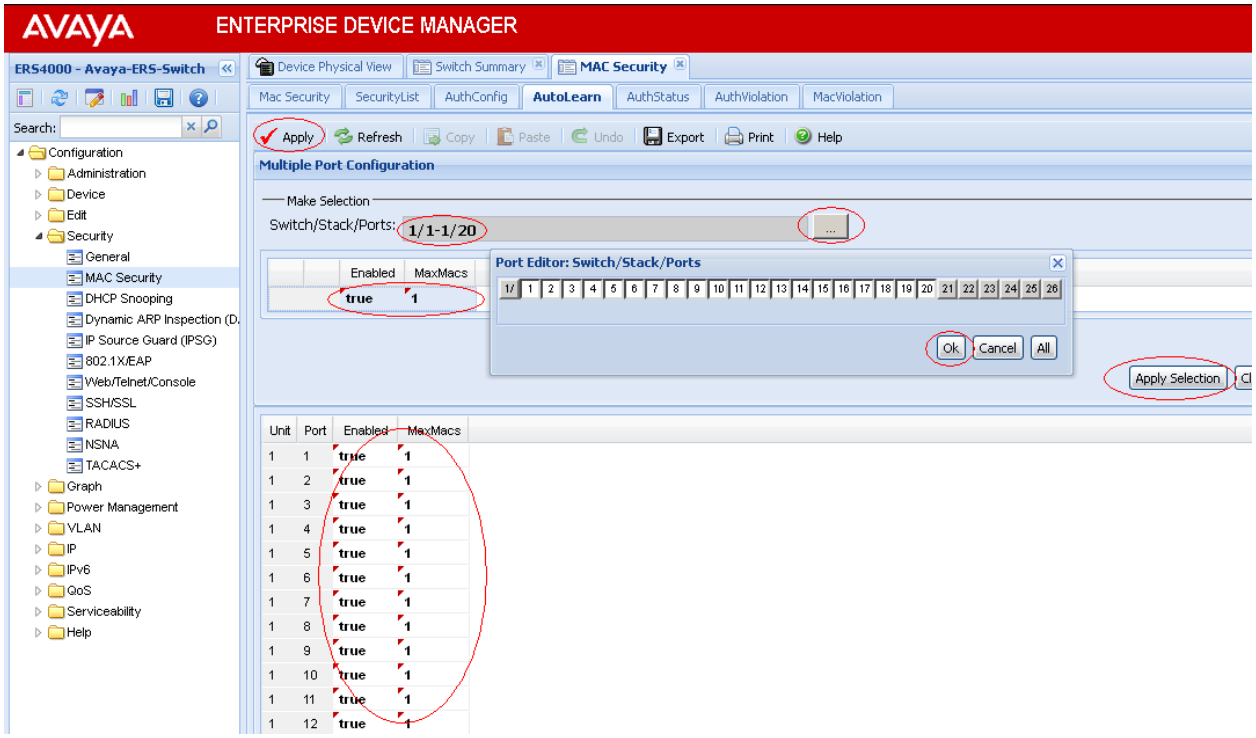
Globally enable MAC Security



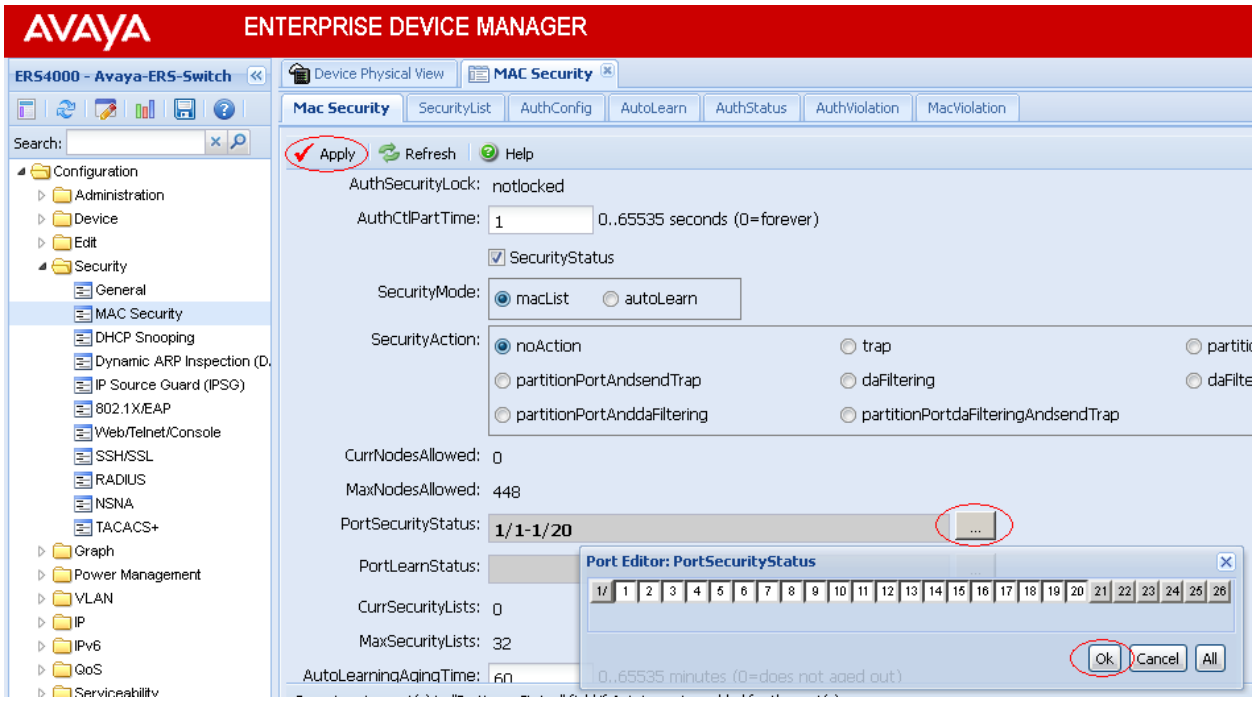
Enable Auto-Learning Sticky-MAC mode



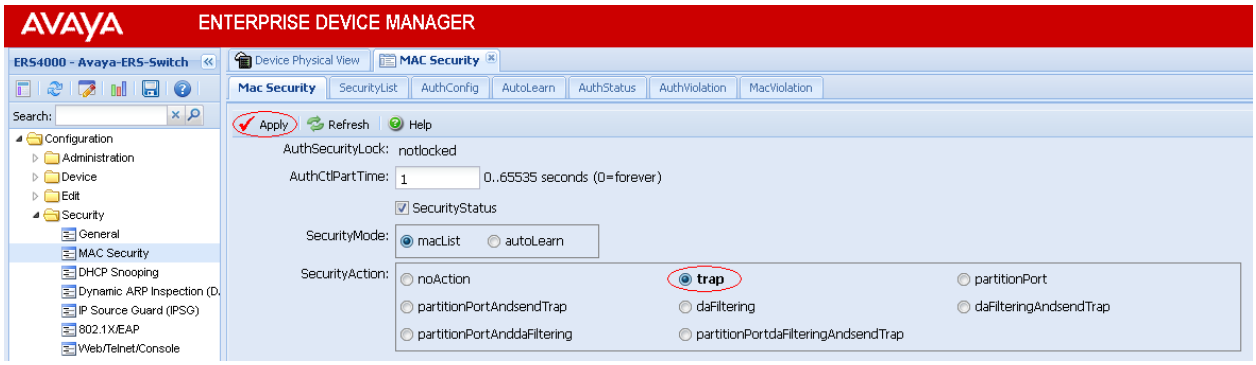
Enable Auto-Learning & MacMac=1 on access ports



Enable MAC Security on the access ports

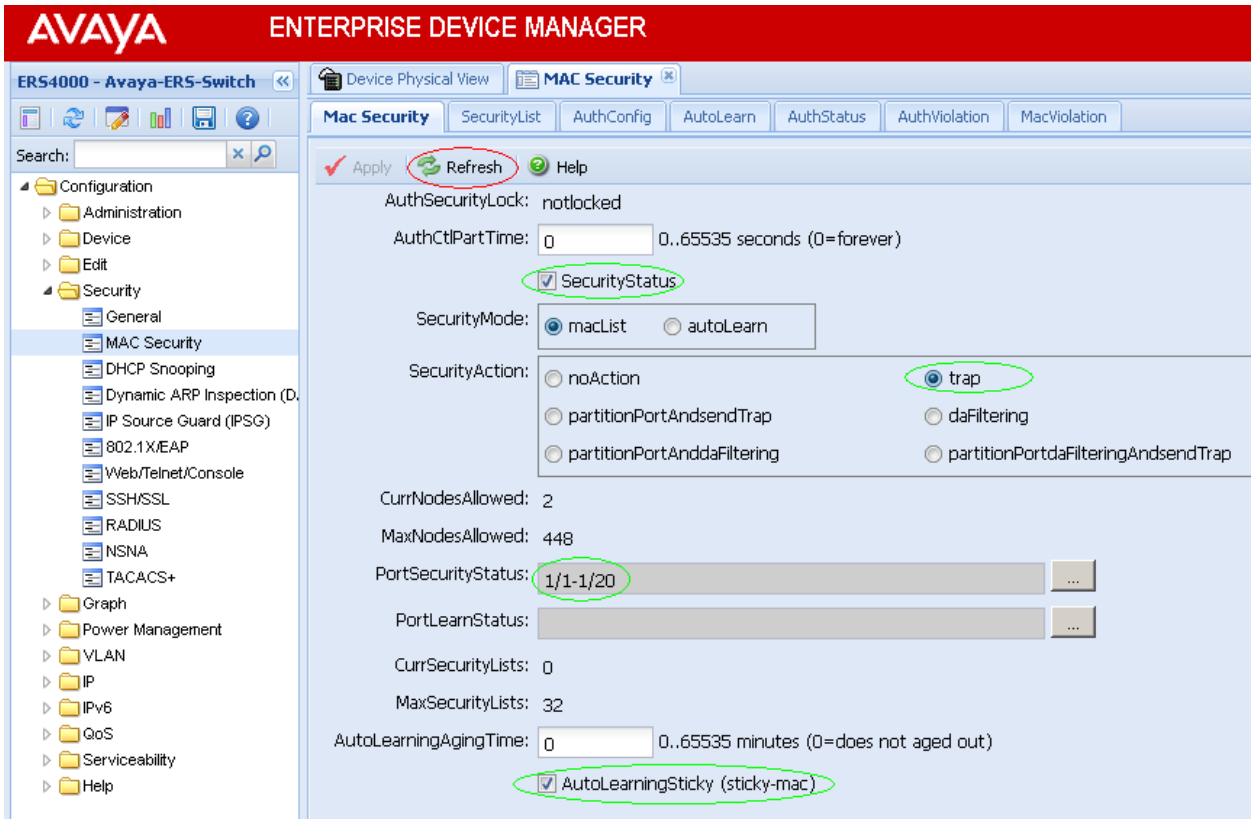


Enable traps upon violation

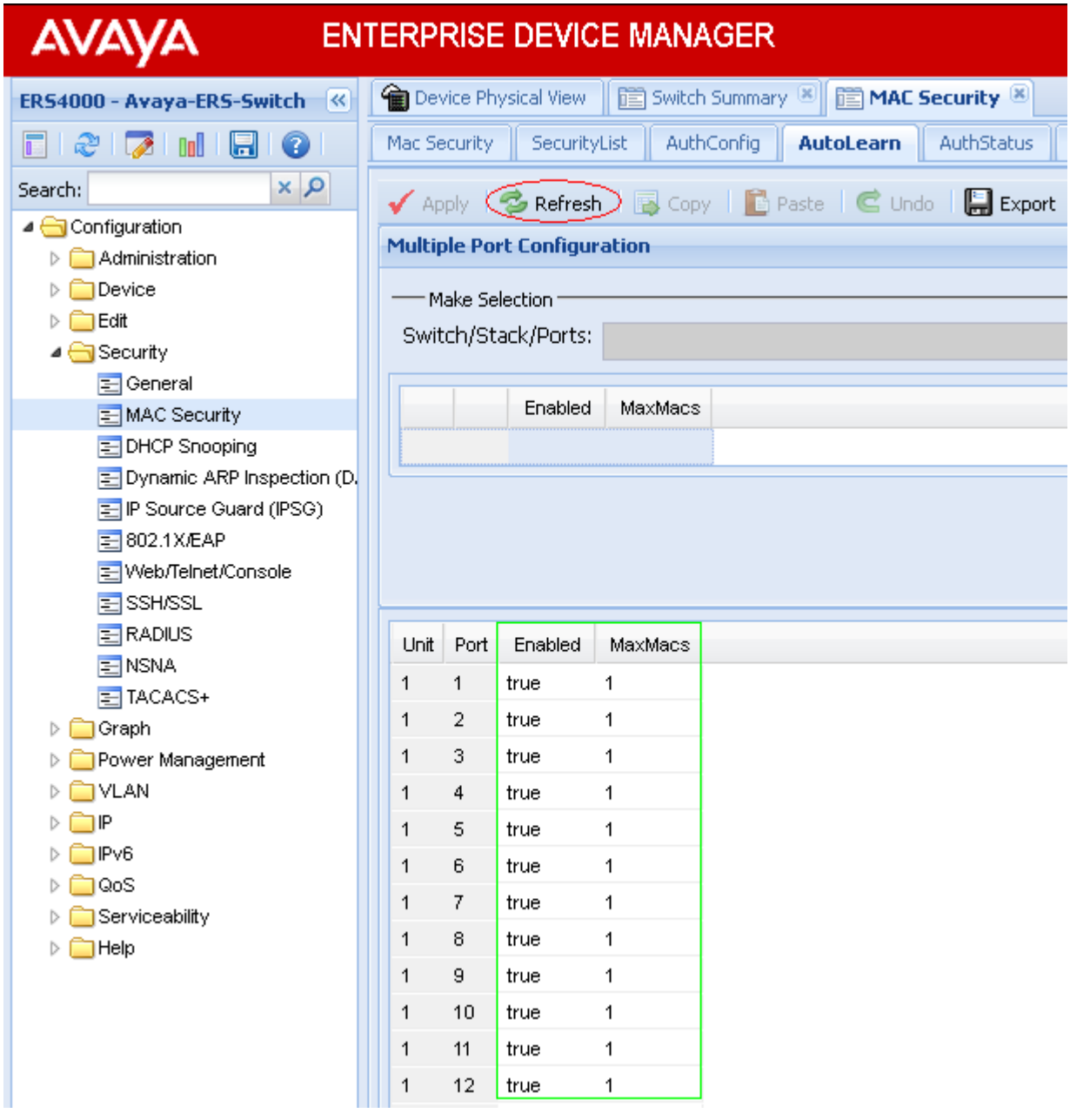


5.1.2.2 Checking MAC Security operational status

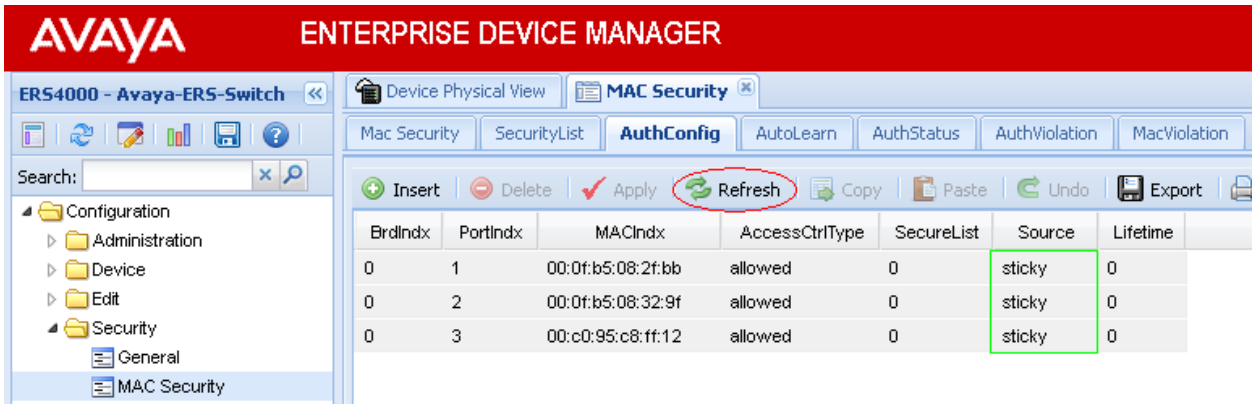
Verify that MAC Security is globally enabled and on access ports, Sticky-MAC mode enabled and Security Action set to trap



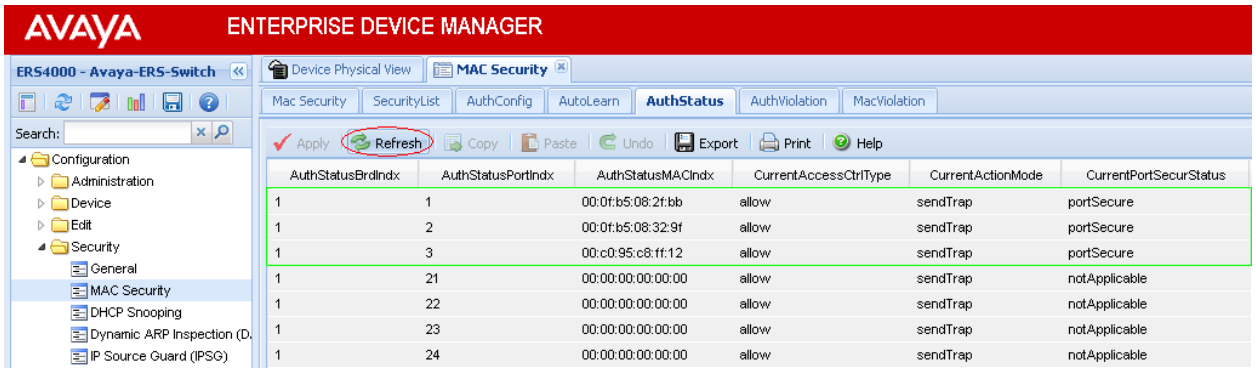
Verify that Auto-Learn is enabled on the access ports and that MacMax is set to 1



Verify the MAC Security MAC table; this will hold the MAC of the 1st device recorded on the ethernet ports; NOTE that the type is Sticky



Verify ports 1-4 are authenticated with the correct MAC address



5.1.3 Verifying user connectivity & switch configuration

Verify IP connectivity between the Router and the end stations

```
Router#% ping 30.0.0.2; ping 30.0.0.3; ping 30.0.0.121
30.0.0.2 is alive
30.0.0.3 is alive
30.0.0.121 is alive
```

Verify the resulting switch config

```
Avaya-ERS-Switch# show running-config
```

```
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 4826GTS-PWR+
! Software version = v5.6.1.053
!
! Displaying only parameters different to default
!================================================
enable
configure terminal
[...]
!
! *** MAC-Based Security ***
!
interface FastEthernet ALL
   mac-security port 1-20 enable
   mac-security auto-learning port 1-20 enable
   mac-security auto-learning port 1 max-addrs 1
   mac-security auto-learning port 2 max-addrs 1
   mac-security auto-learning port 3 max-addrs 1
   mac-security auto-learning port 4 max-addrs 1
   mac-security auto-learning port 5 max-addrs 1
   mac-security auto-learning port 6 max-addrs 1
   mac-security auto-learning port 7 max-addrs 1
   mac-security auto-learning port 8 max-addrs 1
   mac-security auto-learning port 9 max-addrs 1
   mac-security auto-learning port 10 max-addrs 1
   mac-security auto-learning port 11 max-addrs 1
   mac-security auto-learning port 12 max-addrs 1
   mac-security auto-learning port 13 max-addrs 1
   mac-security auto-learning port 14 max-addrs 1
   mac-security auto-learning port 15 max-addrs 1
   mac-security auto-learning port 16 max-addrs 1
   mac-security auto-learning port 17 max-addrs 1
   mac-security auto-learning port 18 max-addrs 1
   mac-security auto-learning port 19 max-addrs 1
   mac-security auto-learning port 20 max-addrs 1
exit
mac-security enable
mac-security auto-learning sticky
```

```
mac-security mac-address-table sticky-address 00.0f.b5.08.2f.bb port 1
mac-security mac-address-table sticky-address 00.0f.b5.08.32.9f port 2
mac-security mac-address-table sticky-address 00.c0.95.c8.ff.12 port 3
 [...]
end
```

Note – The learned MAC addresses are now part of the config file for the switch and thus will be preserved over a switch reboot

5.1.4 Adding a new device

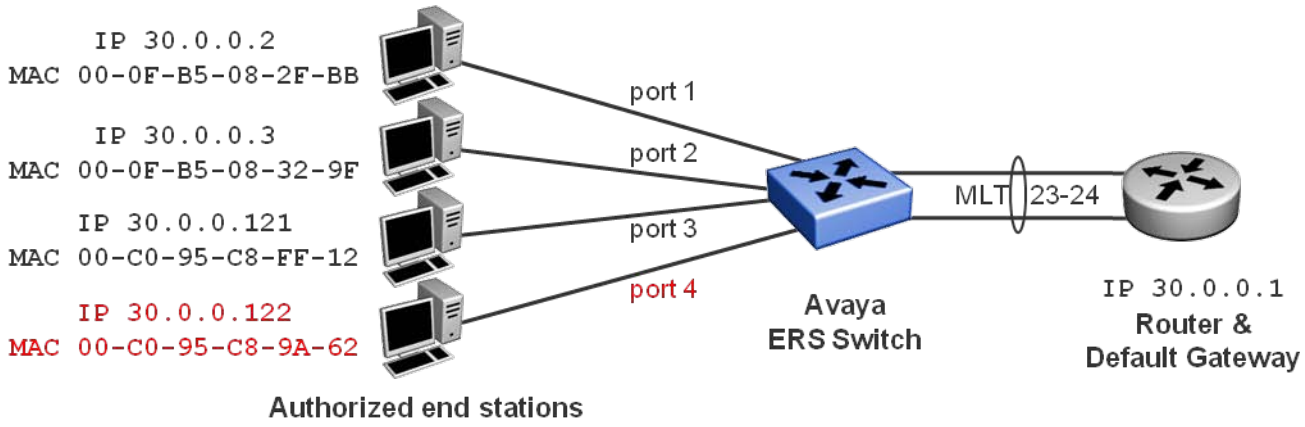


Figure 19: Example 6; a new device is added to the network

No action is required by the network administrator when a new device is added to the network. The device's MAC address is automatically learnt by the Auto-Learning mode and made "Sticky" to the MAC security MAC table.

5.1.4.1 Checking updated MAC Security operational status

Verify the MAC Security MAC table; make sure the MAC of the new device on port 4 is added to the list

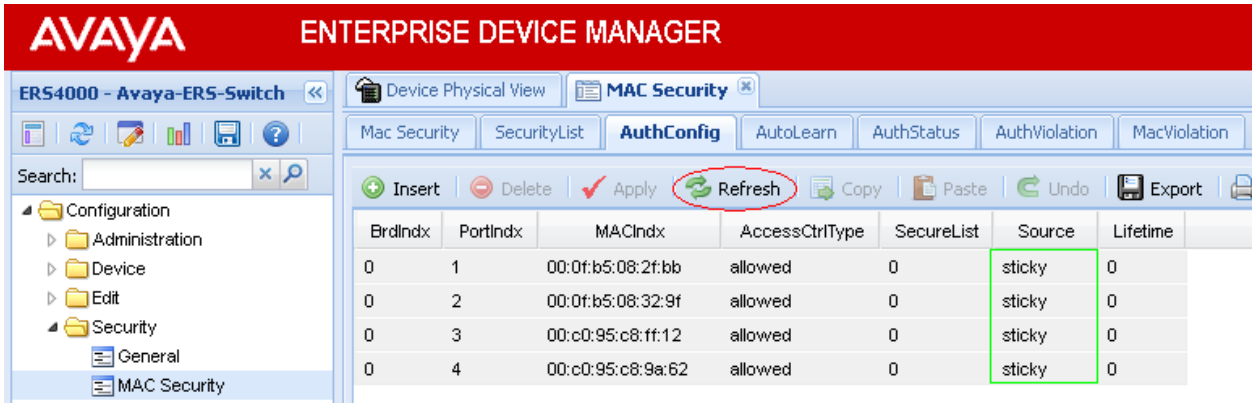
```
Avaya-ERS-Switch# show mac-security mac-address-table
Number of addresses: 4

Unit Port Allowed MAC Address   Type
---- ---- ------------------- ---------
0    1    00-0F-B5-08-2F-BB   Sticky
0    2    00-0F-B5-08-32-9F   Sticky
0    3    00-C0-95-C8-FF-12   Sticky
0    4    00-C0-95-C8-9A-62   Sticky
```

```
Security List Allowed MAC Address   Type
------------ ------------------ ---------
```

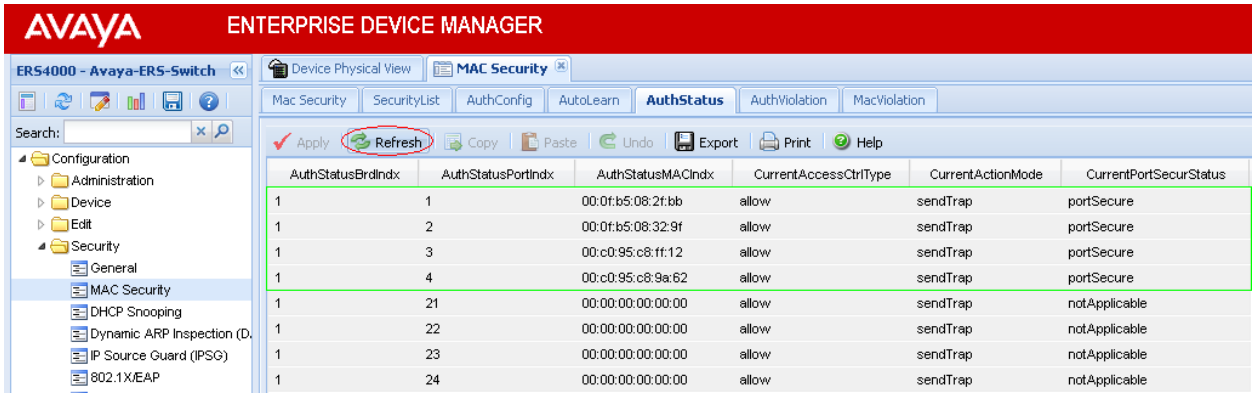
Verify the FDB on the switch

```
Avaya-ERS-Switch# show mac-address-table vid 30
Mac Address Table Aging Time: 300
Learning Enabled Ports 1-26
Number of addresses: 5

   MAC Address    Vid   Type   Source
----------------- ---- ------- -------
00-0F-B5-08-2F-BB   30 Dynamic Port: 1
00-0F-B5-08-32-9F   30 Dynamic Port: 2
00-C0-95-C8-9A-62   30 Dynamic Port: 4
00-C0-95-C8-FF-12   30 Dynamic Port: 3
00-E0-16-57-6E-81   30 Dynamic Trunk:1
```

Under EDM, verify the MAC Security MAC table; make sure the MAC of the new device on port 4 is added to the list



Under EDM, verify ports 1-4 are now authenticated with the correct MAC address



Verify IP connectivity between the Router and the end stations

```
Router#% ping 30.0.0.2; ping 30.0.0.3; ping 30.0.0.121; ping 30.0.0.122
30.0.0.2 is alive
30.0.0.3 is alive
30.0.0.121 is alive
30.0.0.122 is alive
```

Verify the resulting switch config

```
Avaya-ERS-Switch# show running-config
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 4826GTS-PWR+
! Software version = v5.6.1.053
!
! Displaying only parameters different to default
!================================================
enable
configure terminal
[...]
!
! *** MAC-Based Security ***
!
interface FastEthernet ALL
   mac-security port 1-20 enable
```

```
   mac-security auto-learning port 1-20 enable
   mac-security auto-learning port 1 max-addrs 1
   mac-security auto-learning port 2 max-addrs 1
   mac-security auto-learning port 3 max-addrs 1
   mac-security auto-learning port 4 max-addrs 1
   mac-security auto-learning port 5 max-addrs 1
   mac-security auto-learning port 6 max-addrs 1
   mac-security auto-learning port 7 max-addrs 1
   mac-security auto-learning port 8 max-addrs 1
   mac-security auto-learning port 9 max-addrs 1
   mac-security auto-learning port 10 max-addrs 1
   mac-security auto-learning port 11 max-addrs 1
   mac-security auto-learning port 12 max-addrs 1
   mac-security auto-learning port 13 max-addrs 1
   mac-security auto-learning port 14 max-addrs 1
   mac-security auto-learning port 15 max-addrs 1
   mac-security auto-learning port 16 max-addrs 1
   mac-security auto-learning port 17 max-addrs 1
   mac-security auto-learning port 18 max-addrs 1
   mac-security auto-learning port 19 max-addrs 1
   mac-security auto-learning port 20 max-addrs 1
exit
mac-security enable
mac-security auto-learning sticky
mac-security mac-address-table sticky-address 00.0f.b5.08.2f.bb port 1
mac-security mac-address-table sticky-address 00.0f.b5.08.32.9f port 2
mac-security mac-address-table sticky-address 00.c0.95.c8.ff.12 port 3
mac-security mac-address-table sticky-address 00.c0.95.c8.9a.62 port 4
[...]
end
```

Note – If AutoSave is disabled on the switch (which is recommended with MAC Security Auto-Learning and Sticky-MAC) then the network administrator must ensure that the config is saved before rebooting the switch (otherwise newly added Sticky MACs will be lost over a reboot).

5.1.5 Testing violations

5.1.5.1 Unauthorized MAC on provisioned port

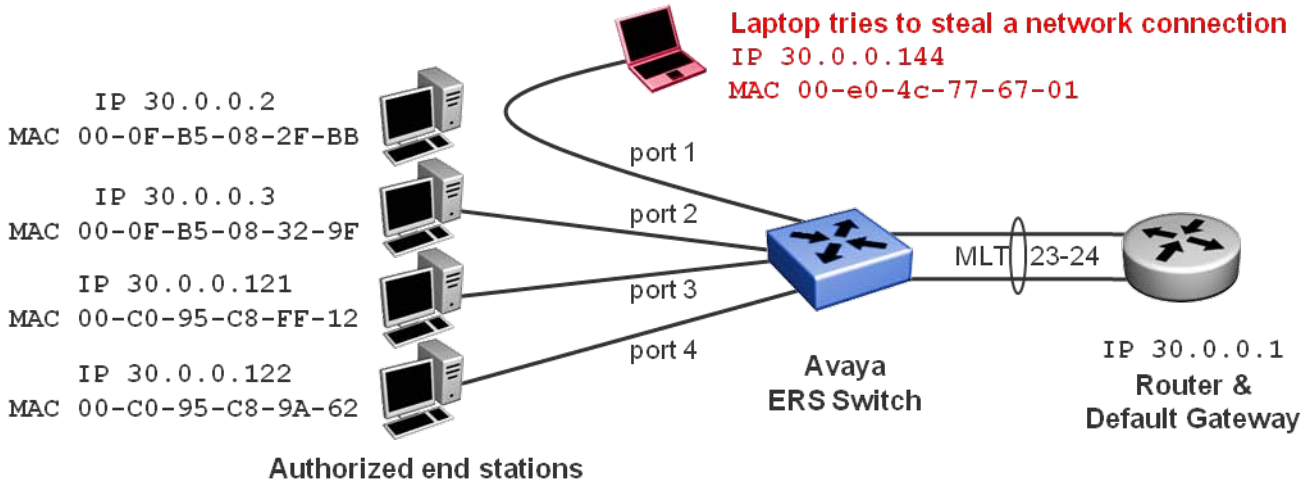


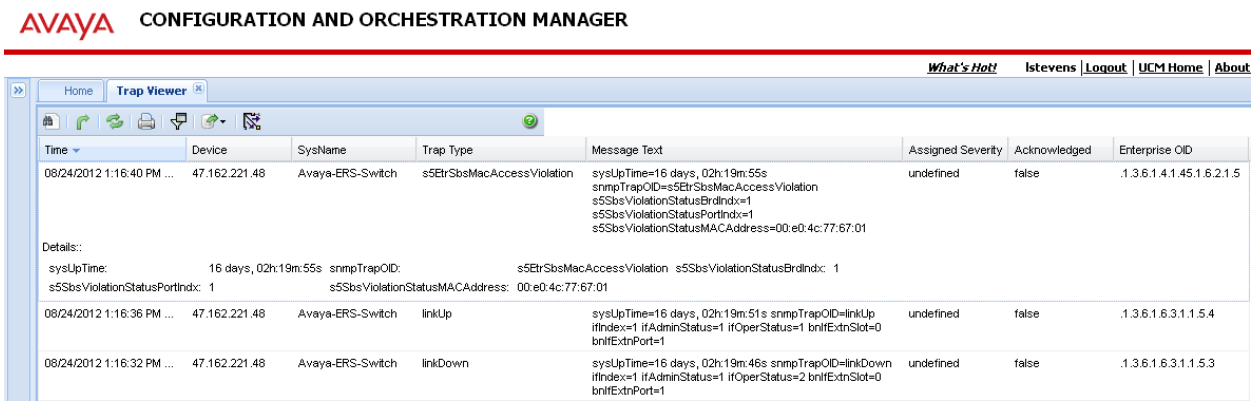
Figure 20: Example 6; unauthorized MAC on provisioned port

The unauthorized device is not able to send any traffic into the network; however it is still able to see broadcast and unknown traffic flowing in the VLAN; if this is undesired the MAC Security should be configured to partition the port upon an access violation.

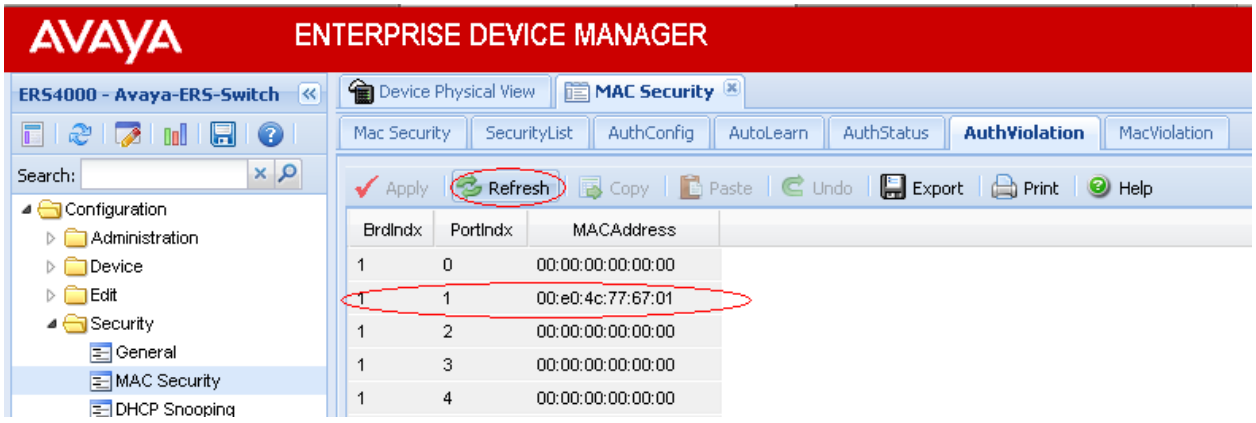
Verify log file on switch

```
Avaya-ERS-Switch# show log

Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
I    16:02:19:46                   1        Link Down Trap for Port: 1
I    16:02:19:51                   2        Link Up Trap for Port: 1
I    16:02:19:55                   3        Bay Secure: Exceeded 1 per-port MAC
                                            addresses on port 0/1
I    16:02:19:55                   4        Bay Secure intruder MAC 00-e0-4c-77-67-01
                                            port 1
I    16:02:19:55                   5        Trap:  s5EtrNewSbsMacAccessViolation
```

Verify traps on Management station (e.g. VPFM or COM)



Verify MAC Security violations from EDM



5.1.5.2 Unauthorized MAC sharing connection with authorized MAC

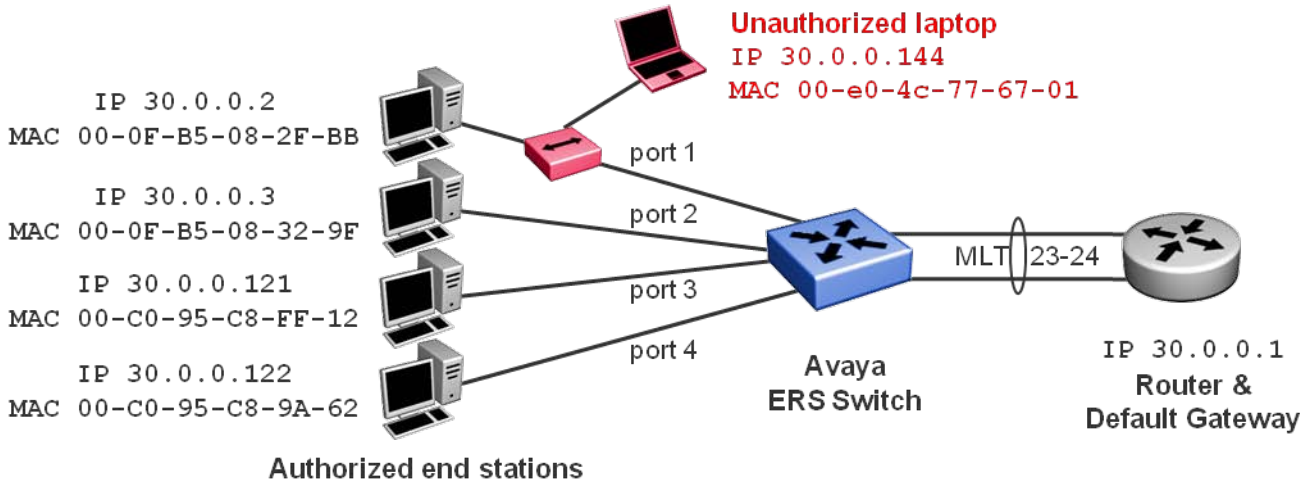


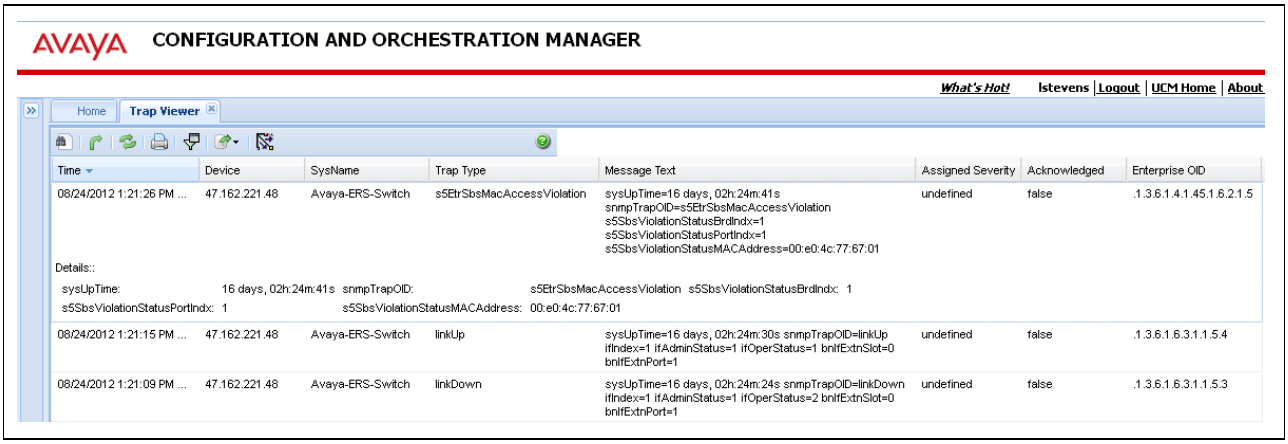
Figure 21: Example 6; unauthorized MAC sharing connection with authorized MAC

The unauthorized device is not able to send any traffic into the network; however it is still able to see broadcast and unknown traffic flowing in the VLAN; if this is undesired the MAC Security should be configured to partition the port upon an access violation.

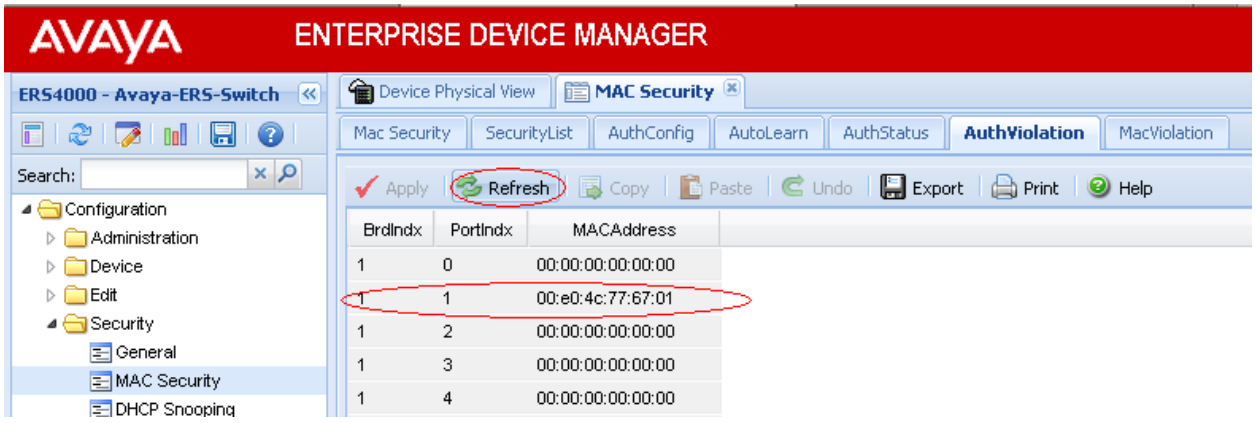
Verify log file on switch

```
Avaya-ERS-Switch# show log
Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
I    16:02:24:24                   1        Link Down Trap for Port: 1
I    16:02:24:30                   2        Link Up Trap for Port: 1
I    16:02:24:41                    3         Bay Secure intruder MAC 00-e0-4c-77-67-01
port 1
I    16:02:24:41                   4        Trap:  s5EtrNewSbsMacAccessViolation
```

Verify traps on Management station (e.g. VPFM or COM)



Verify MAC Security violations from EDM



Note that the authorized device on port 1 retains connectivity, but the unauthorized laptop cannot talk to the network

```
Router#% ping 30.0.0.2; ping 30.0.0.3; ping 30.0.0.121; ping 30.0.0.122; ping 30.0.0.144
30.0.0.2 is alive
30.0.0.3 is alive
30.0.0.121 is alive
30.0.0.122 is alive
no answer from 30.0.0.144
```

Tip – If the network administrator prefers to disable the ethernet port 1 in this scenario, it is sufficient to configure port partitioning security action upon violation.

5.1.5.3 Authorized MAC moving to a different port

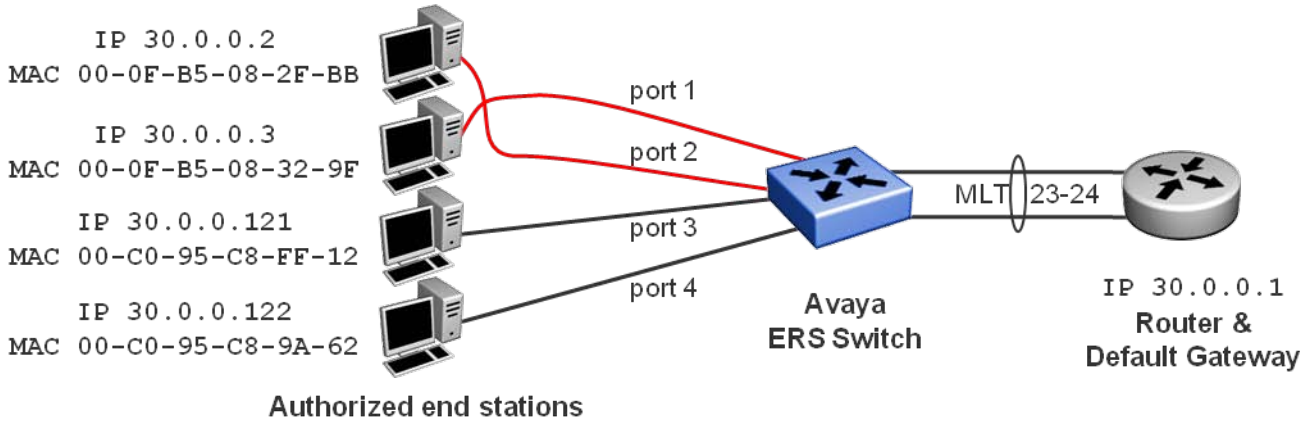


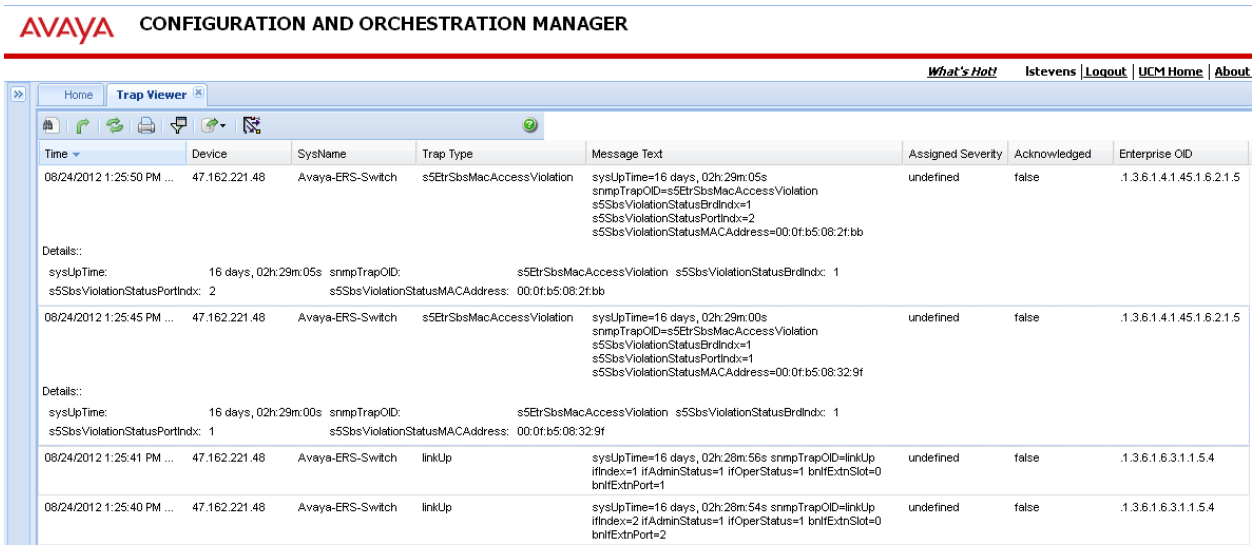
Figure 22: Example 6; unauthorized MAC moving to a different port

Neither of the two end stations with swapped connections can now talk to the network.

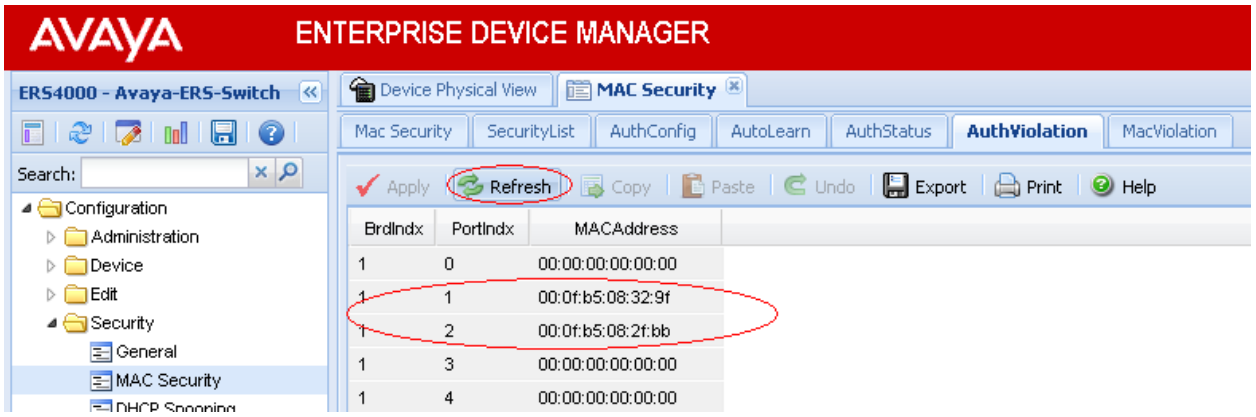
Verify log file on switch

```
Avaya-ERS-Switch# show log
Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
I    16:02:28:50                   1        Link Down Trap for Port: 1
I    16:02:28:51                   2        Link Down Trap for Port: 2
I    16:02:28:54                   3        Link Up Trap for Port: 2
I    16:02:28:56                   4        Link Up Trap for Port: 1
I    16:02:29:00                   5        Bay Secure intruder MAC  00-0f-b5-08-32-9f
                                            port 1 address is Locked on port 2
I    16:02:29:00                   6        Trap:  s5EtrNewSbsMacAccessViolation
I    16:02:29:05                   7        Bay Secure: Exceeded 1 per-port MAC
                                            addresses on port 0/2
I    16:02:29:05                   8        Bay Secure intruder MAC  00-0f-b5-08-2f-bb
                                            port 2 address is Locked on port 1
I    16:02:29:05                   9        Trap:  s5EtrNewSbsMacAccessViolation
```

Verify traps on Management station (e.g. VPFM or COM)



Verify MAC Security violations from EDM



Note that the authorized devices cannot communicate on the wrong ethernet port

```
Router#% ping 30.0.0.2; ping 30.0.0.3; ping 30.0.0.121; ping 30.0.0.122
no answer from 30.0.0.2
no answer from 30.0.0.3
30.0.0.121 is alive
30.0.0.122 is alive
```