



PacketFence Network Devices Configuration Guide

for version 3.3.2

PacketFence Network Devices Configuration Guide

Olivier Bilodeau

François Gaudreault

Derek Wuelfrath

Version 3.3.2 - April 2012

Copyright © 2010-2012 Inverse inc.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

The fonts used in this guide are licensed under the SIL Open Font License, Version 1.1. This license is available with a FAQ at: <http://scripts.sil.org/OFL>

Copyright © Barry Schwartz, <http://www.crudfactory.com>, with Reserved Font Name: "Sorts Mill Goudy".

Copyright © Raph Levien, <http://levien.com/>, with Reserved Font Name: "Inconsolata".



9279Vnj

Revision History

Revision 2.2	2012-04-23	OB
HP ProCurve 5300 Series identified as supported.		
Revision 2.1	2012-04-12	FG, OB
Added new configuration documentation for AlliedTelesis. Roles support for AeroHive, Aruba, Meru and Motorola.		
Revision 2.0	2012-02-22	FG, OB
Port to asciidoc. Added Ruckus documentation. Added documentation for Meru PMK caching.		
Revision 1.0	2010-11-22	OBU
First OpenDocument version.		

Table of Contents

About this Guide	1
Other sources of information	1
Note on Inline enforcement support	2
List of supported Network Devices	3
Switch configuration	6
Assumptions	6
3COM	6
AlliedTelesis	10
Amer	12
Avaya	12
Cisco	12
D-Link	22
Dell	23
EdgecorE	23
Enterasys	23
Extreme Networks	26
Foundry	28
HP	29
HP ProCurve	29
Intel	32
Juniper	32
LG-Ericsson	34
Linksys	35
Netgear	36
Nortel	36
SMC	38
Wireless Controllers and Access Point Configuration	39
Assumptions	39
Unsupported Equipment	39
AeroHIVE	40
Avaya	42
Aruba	42
Cisco	45
D-Link	48
Extricom	48
HP	49
Meru	49
Motorola	52
Ruckus	55
Trapeze	56
Xirrus	57
Additional Information	58
Commercial Support and Contact Information	59
GNU Free Documentation License	60

List of Tables

1. Supported network devices 3

About this Guide

This guide covers the configuration of network devices in order to integrate them with PacketFence in VLAN enforcement. Switches, wireless controllers and wireless access points are all considered network devices in PacketFence's terms.

The latest version of this guide is available at <http://www.packetfence.org/documentation/>

Other sources of information

Administration Guide	Covers PacketFence installation, configuration and administration.
Developers Guide	Covers captive portal customization, VLAN management customization and instructions for supporting new hardware.
NEWS	Covers noteworthy features, improvements and bugfixes by release.
UPGRADE	Covers compatibility related changes, manual instructions and general notes about upgrading.
ChangeLog	Covers all changes to the source code.

These files are included in the package and release tarballs.

Note on Inline enforcement support

There is no need to follow the instructions in this guide if you plan on deploying in inline enforcement. In this case all you need to do is to have a flat layer 2 network up to PacketFence's inline interface with no other gateway available for devices to reach out to the Internet.

This technique is usually used when your network hardware doesn't support VLAN enforcement.

List of supported Network Devices

PacketFence supports the following devices:

Table 1. Supported network devices

Vendor	Model	PacketFence Type (used in switches.conf)
3COM	E4800G Switch series	ThreeCom::E4800G
	E5500G Switch series	ThreeCom::E5500G
	NJ220	ThreeCom::NJ220
	SuperStack 3 Switch 4200	ThreeCom::SS4200
	SuperStack 3 Switch 4500	ThreeCom::SS4500
	Switch 4200G	ThreeCom::Switch_4200G
	Aerohive	All AP models
AlliedTelesis	AlliedTelesis AT8000GS	AlliedTelesis::AT8000GS
Amer	L2 Switch SS2R24i	Amer::SS2R24i
Aruba	All Controllers	Aruba
Avaya	Wireless Controllers	Avaya::WC
	See Nortel Below	
Cisco	Aironet 1130 AG	Cisco::Aironet_1130
	Aironet 1240 AG	Cisco::Aironet_1242
	Aironet 1250	Cisco::Aironet_1250
	2100 Wireless Controller	Cisco::WLC_2106
	4400 Wireless Controller	Cisco::WLC_4400
	Catalyst 2900XL Series	Cisco::Catalyst_2900XL
	Catalyst 2950	Cisco::Catalyst_2950
	Catalyst 2960	Cisco::Catalyst_2960
	Catalyst 2970	Cisco::Catalyst_2970
	Catalyst 3500XL Series	Cisco::Catalyst_3500XL
	Catalyst 3550	Cisco::Catalyst_3550
	Catalyst 3560	Cisco::Catalyst_3560
	Catalyst 3750	Cisco::Catalyst_3750
	Catalyst 4500	Cisco::Catalyst_4500
	Catalyst 6500	Cisco::Catalyst_6500

Vendor	Model	PacketFence Type (used in switches.conf)
	Router ISR 1800 Series	Cisco::ISR_1800
	Wireless Services Module	Cisco::WiSM
D-Link	DES 3526	Dlink::DES_3526
	DES 3550	Dlink::DES_3550
	DGS 3100	Dlink::DGS_3100
	DGS 3200	Dlink::DGS_3200
	DWL Access-Points	Dlink::DWL
	DWS 3026	Dlink::DWS_3026
Dell	PowerConnect 3424	Dell::PowerConnect3424
Edge-corE	3526XA	Accton::ES3536XA
	3528M	Accton::ES3528M
Enterasys	Matrix N3	Enterasys::Matrix_N3
	SecureStack C2	Enterasys::SecureStack_C2
	SecureStack C3	Enterasys::SecureStack_C3
	Standalone D2	Enterasys::D2
Extreme Networks	Summit Series	Extreme::Summit
Extricom	EXSW Wireless Switches	Extricom::EXSW
Foundry	FastIron 4802	Foundry::FastIron_4802
HP	E4800G Switch series	HP::E4800G
	E5500G Switch series	HP::E5500G
	MSM 710 Mobility Controller	HP::Controller_MSM710
	ProCurve 2500 Series	HP::Procurve_2500
	ProCurve 2600 Series	HP::Procurve_2600
	ProCurve 3400cl Series	HP::Procurve_3400cl
	ProCurve 4100 Series	HP::Procurve_4100
	ProCurve 5300 Series	HP::Procurve_5300
	ProCurve 5400 Series	HP::Procurve_5400
Intel	Express 460	Intel::Express_460
	Express 530	Intel::Express_530
Juniper	EX Series	Juniper::EX
LG-Ericsson	iPECS Series	LG::ES4500G
Linksys	SRW224G4	Linksys::SRW224G4
Meru	MC Series	Meru::MC
Motorola	RF Switches	Motorola::RFS
Netgear	FSM726v1	Netgear::FSM726v1
Nortel	BPS2000	Nortel::BPS2000
	ERS 2500 Series	Nortel::ERS2500

Vendor	Model	PacketFence Type (used in switches.conf)
	ERS 4000 Series	Nortel::ERS4000
	ERS 5000 Series	Nortel::ERS5000
	ERS 5500 with firmware 6	Nortel::ERS5500_6x
	ES325	Nortel::ES325
	Baystack 470	Nortel::Baystack470
	Baystack 4550	Nortel::Baystack4550
	Baystack 5500 Series	Nortel::Baystack5500
	Baystack 5500 w/ 6.x	Nortel::BayStack5500_6x
Ruckus	Ruckus ZoneDirector	Ruckus
SMC	TigerStack 6128 L2	SMC::TS6128L2
	TigerStack 6224M	SMC::TS6224M
	TigerStack 8824-48M	SMC::TS8800M
Trapeze	Trapeze Controllers	Trapeze
Xirrus	Xirrus WiFi Arrays	Xirrus

Switch configuration

Assumptions

Throughout this configuration example we use the following assumptions for our network infrastructure:

- PacketFence is fully configured with FreeRADIUS running (if you want 802.1X or MAC Auth)
- PacketFence IP address: 192.168.1.5
- Normal VLAN: 1
- Registration VLAN: 2
- Isolation VLAN: 3
- MAC Detection VLAN: 4
- VoIP, Voice VLAN: 100
- use SNMP v2c
- SNMP Trap community: public
- RADIUS Secret: useStrongerSecret

3COM

SuperStack 3 Switch 4200 and 4500

PacketFence supports these 3Com switches *without VoIP* using one trap type:

- linkUp/linkDown
- Port Security (with static MACs)

Don't forget to update the startup config!

linkUp / linkDown only

Global config settings:

```
snmp-agent
snmp-agent target-host trap address udp-domain 192.168.1.5 params securityname
public
snmp-agent trap enable standard linkup linkdown
```

On each interface:

```
port access vlan 4
```

In Port Security

Global config settings:

```
snmp-agent
snmp-agent target-host trap address udp-domain 192.168.1.5 params securityname
public
snmp-agent trap enable
port-security enable
port-security trap addresslearned
port-security trap intrusion
```

On each interface:

```
port access vlan 4
port-security max-mac-count 1
port-security port-mode secure
port-security intrusion-mode blockmac
undo enable snmp trap updown
```

E4800G

PacketFence supports these 3Com switches with the following techniques:

- 802.1X with MAC Authentication fallback
- linkUp/linkDown (not recommended)

Voice over IP support was not explicitly tested during implementation however it does not mean that it won't work.

Don't forget to update the startup config!

linkUp / linkDown only

Global config settings:

```
snmp-agent
snmp-agent target-host trap address udp-domain 192.168.1.5 params securityname
public
snmp-agent trap enable standard linkup linkdown
```

On each interface:

```
port access vlan 4
```

802.1X with MAC Authentication fallback

Global config settings:

```
system-view
  radius scheme PacketFence
    primary authentication 192.168.1.5 1812
    primary accounting 192.168.1.5 1812
    key authentication useStrongerSecret
    user-name-format without-domain
  quit
  domain packetfence.local
    authentication default radius-scheme PacketFence
    authorization default radius-scheme PacketFence
  quit
  domain default enable packetfence.local
  dot1x authentication-method eap
  port-security enable
quit
```

If your management authentication on your switch is default, applying the configuration above will have your authentication switch to a RADIUS based one with PacketFence as the authentication server. It is almost certain that you do not want that!

Below, we will just create a local password for vty accesses (telnet) and nothing on the console. In order to avoid locking yourself out, make sure to verify your configuration!

```
system-view
  user-interface aux 0
    authentication-mode none
  user-interface vty 0 4
    user privilege level 3
    set authentication password simple useStrongerPassword
  quit
quit
```

On each interface:

```
system-view
  interface gigabitEthernet 1/0/xx
    port-security port-mode mac-else-userlogin-secure-ext
    # userlogin-secure-or-mac-ext could be used below instead
    # see the Switch_4200G's documentation for a discussion about it
    undo enable snmp trap updown
  quit
quit
```

where xx stands for the interface index.

E5500G and Switch 4200G

PacketFence supports these 3Com switches with the following techniques:

- 802.1X with MAC Authentication fallback
- linkUp/linkDown (not recommended)

Voice over IP support was not explicitly tested during implementation however it does not mean that it won't work.

Don't forget to update the startup config !

linkUp / linkDown only

Global config settings:

```
snmp-agent
snmp-agent target-host trap address udp-domain 192.168.1.5 params
securityname public
snmp-agent trap enable standard linkup linkdown
```

On each interface:

```
port access vlan 4
```

802.1X with MAC Authentication fallback

Global config settings:

```
system-view
 radius scheme PacketFence
   server-type standard
   primary authentication 192.168.1.5 1812
   primary accounting 192.168.1.5 1812
   accounting optional
   key authentication useStrongerSecret
   user-name-format without-domain
 quit
 domain packetfence.local
   radius-scheme PacketFence
   vlan-assignment-mode string
 quit
 domain default enable packetfence.local
 dot1x authentication-method eap
 port-security enable
quit
```

If your management authentication on your switch is default, applying the configuration above will have your authentication switch to a RADIUS based one with PacketFence as the authentication server. It is almost certain that you do not want that!

Below, we will just create a local password for vty accesses (telnet) and nothing on the console. In order to avoid locking yourself out, make sure to verify your configuration!

```
system-view
  user-interface aux 0
    authentication-mode none
  user-interface vty 0 4
    user privilege level 3
    set authentication password simple useStrongerPassword
  quit
quit
```

On each interface:

```
system-view
  interface gigabitEthernet 1/0/xx
    port-security port-mode mac-else-userlogin-secure-ext
    # userlogin-secure-or-mac-ext could be used below instead
    # see the Switch_4200G's documentation for a discussion about it
    undo enable snmp trap updown
  quit
quit
```

where xx stands for the interface index

NJ220

This switch does not support port-security.

To configure: use web interface to send the linkUp/linkDown traps to the PacketFence server.

AlliedTelesis

AT8000GS

PacketFence supports the AT8000GS switch using :

- Mac Authentication (mac-only)
- 802.1X

VoIP support is limited using 802.1X/MAC authentication. We do have a limitation where the phone needs to be on the same VLAN as the PC (no voice VLAN concept).

Mac Authentication

First, activate 802.1X globally:

```
dot1x system-auth-control
```

Next, configure the RADIUS server and AAA settings:

```
radius-server host 10.0.0.100
radius-server key qwerty
radius-server source-ip 10.0.0.14
aaa authentication dot1x default radius
aaa accounting dot1x radius
```

In order to get mac authentication, you need to enable the guest VLAN globally:

```
interface vlan 5
name "Guest Vlan"
dot1x guest-vlan
exit
```

Finally, enable the necessary 802.1X settings for mac-only authentication:

```
interface ethernet g1
dot1x mac-authentication mac-only
dot1x radius-attributes vlan
dot1x port-control auto
dot1x guest-vlan enable
```

802.1X

The settings are almost the same as the MAC Authentication with some small differences.

First, activate 802.1X globally:

```
dot1x system-auth-control
```

Next, configure the RADIUS server and AAA settings:

```
radius-server host 10.0.0.100
radius-server key qwerty
radius-server source-ip 10.0.0.14
aaa authentication dot1x default radius
aaa accounting dot1x radius
```

Finally, enable the necessary 802.1X settings:

```
interface ethernet g1
dot1x radius-attributes vlan
dot1x port-control auto
```


Amer

PacketFence supports Amer switches *without VoIP* using one trap type:

- linkUp/linkDown

Don't forget to update the startup config!

L2 Switch SS2R24i

Global config settings:

```
create snmp host 192.168.1.5 v2c public
create snmp user public ReadGroup
enable snmp traps
```

On each interface:

```
config vlan default delete xx
config vlan mac-detection add untagged xx
```

where xx stands for the interface index

Avaya

Avaya bought Nortel's wired networks assets. So Avaya switches are, in effect, re-branded Nortels. See [Nortel section](#) of this document for configuration instructions.

Cisco

PacketFence supports Cisco switches with VoIP using three different trap types:

- linkUp/linkDown
- MAC Notification
- Port Security (with static MACs)

On some recent models, we can also use more secure and robust features like:

- MAC Authentication (Cisco's MAC Authentication Bypass or MAB)
- 802.1x (Multi-Host or Multi-Domain)

Depending of the switch model, we recommend the use of the most secure and reliable feature first. In other words, you should consider the following order:

1. 802.1x/MAB
2. Port-Security
3. linkUp/linkDown

2900XL Series and 3500XL Series

linkUP/linkDown SNMP traps

Global config settings:

```
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification
snmp-server host 192.168.1.5 trap version 2c public snmp mac-notification
mac-address-table notification interval 0
mac-address-table notification
mac-address-table aging-time 3600
```

On each interface *without VoIP*:

```
switchport mode access
switchport access vlan 4
snmp trap mac-notification added
```

On each interface *with VoIP*:

```
switchport trunk encapsulation dot1q
switchport trunk native vlan 4
switchport mode trunk
switchport voice vlan 100
snmp trap mac-notification added
snmp trap mac-notification removed
```

2950

Those switches are now supported using 802.1x for networks with or without VoIP. You can also use port-security with static MAC address but we can not secure a MAC on the data VLAN specifically so enable it if there is no VoIP, use linkUp/linkDown and MAC notification otherwise. So on setup that needs to handle VoIP with this switch, go with a 802.1x configuration.

802.1X

Recently, we were able to add the support for 802.1X on those switch even if they are not supporting RADIUS dynamic VLAN assignments.

Global config settings:

```
dot1x system-auth-control
```

AAA Groups and Configuration:

```
aaa new-model
aaa group server radius packetfence
  server 192.168.1.5 auth-port 1812 acct-port 1813
aaa authentication login default local
aaa authentication dot1x default group packetfence
aaa authorization network default group packetfence
```

Radius server configuration:

```
radius-server host 192.168.1.5 auth-port 1812 acct-port 1813 timeout 2
key useStrongerSecret
radius-server vsa send authentication
```

For ports *without* VoIP:

```
switchport access vlan 4
switchport mode access
dot1x port-control auto
dot1x host-mode multi-host
dot1x reauthentication
```

For ports *with* VoIP:

```
switchport access vlan 4
switchport mode access
switchport voice vlan 100
dot1x port-control auto
dot1x host-mode multi-host
dot1x reauthentication
```

Port-Security



Caution

With port-security, if no MAC is connected on ports when activating port-security, we need to secure bogus MAC addresses on ports in order for the switch to send a trap when a new MAC appears on a port. On the other hand, if a MAC is actually connected when you enable port security, you must secure this MAC rather than the bogus one. Otherwise this MAC will lose its connectivity instantly.

Global config settings *without VoIP*:

```
snmp-server enable traps port-security
snmp-server enable traps port-security trap-rate 1
snmp-server host 192.168.1.5 version 2c public port-security
```

On each interface *without VoIP*:

```
switchport mode access
switchport access vlan 4
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address 0200.0000.00xx
```

where xx stands for the interface ifIndex.



ifIndex mapping

Use the following templates for interface IfIndex in bogus MAC addresses (0200.0000.00xx):

- Fa0/1, ..., Fa0/48 1, ..., 48
- Gio/1, Gio/2 49, 50

Global config settings *with VoIP*:

```
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification
snmp-server host 192.168.1.5 trap version 2c public snmp mac-notification
mac-address-table notification interval 0
mac-address-table notification
mac-address-table aging-time 3600
```

On each interface *with VoIP*:

```
switchport voice vlan 100
switchport access vlan 4
switchport mode access
snmp trap mac-notification added
snmp trap mac-notification removed
```

2960



Caution

For 802.1X and MAB configurations, refer to [this section below](#).

PortSecurity for IOS earlier than 12.2(46)SE

Global config settings:

```
snmp-server enable traps port-security
snmp-server enable traps port-security trap-rate 1
snmp-server host 192.168.1.5 version 2c public port-security
```

On each interface *without* VoIP:

```
switchport access vlan 4
switchport port-security
switchport port-security maximum 1 vlan access
switchport port-security violation restrict
switchport port-security mac-address 0200.000x.xxxx
```

where xxxxx stands for the interface ifIndex

On each interface with VoIP:

```
switchport voice vlan 100
switchport access vlan 4
switchport port-security
switchport port-security maximum 2
switchport port-security maximum 1 vlan access
switchport port-security violation restrict
switchport port-security mac-address 0200.000x.xxxx
```

where xxxxx stands for the interface ifIndex



ifIndex mapping

Use the following templates for interface IfIndex in bogus MAC addresses (0200.000x.xxxx):

- Fa0/1...Fa0/48 10001...10048
- Gio/1...Gio/48 10101...10148

PortSecurity for IOS 12.2(46)SE or greater

Since version PacketFence 2.2.1, the way to handle VoIP when using port-security dramatically changed. Ensure that you follow the instructions below. To make the story short, instead on relying on the dynamic MAC learning for VoIP, we use a static entry on the voice VLAN so we can trigger a new security violation, and then authorize the phone MAC address on the network.

Global config settings:

```
snmp-server enable traps port-security
snmp-server enable traps port-security trap-rate 1
snmp-server host 192.168.1.5 version 2c public port-security
```

On each interface *without VoIP*:

```
switchport access vlan 4
switchport port-security
switchport port-security maximum 1 vlan access
switchport port-security violation restrict
switchport port-security mac-address 0200.000x.xxxx
```

where xxxxx stands for the interface ifIndex

On each interface *with VoIP*:

```
switchport voice vlan 100
switchport access vlan 4
switchport port-security
switchport port-security maximum 2
switchport port-security maximum 1 vlan access
switchport port-security maximum 1 vlan voice
switchport port-security violation restrict
switchport port-security mac-address 0200.010x.xxxx vlan voice
switchport port-security mac-address 0200.000x.xxxx vlan access
```

where xxxxx stands for the interface ifIndex



ifIndex mapping

Use the following templates for interface IfIndex in bogus MAC addresses (0200.000x.xxxx):

- Fa0/1...Fa0/48 10001...10048
- Gio/1...Gio/48 10101...10148

2970, 3560, 3550, 3750



Caution

The Catalyst 3550 does not support 802.1x with Multi-Domain, it can only support 802.1x with MAB using Multi-Host, MAB, and Port-Security.

802.1x with MAC Authentication bypass (MultiDomain)

Global config settings:

```
dot1x system-auth-control
```

On each interface:

```

switchport mode access
switchport voice vlan 100
authentication host-mode multi-domain
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer restart 10800
authentication timer reauthenticate 10800
mab
no snmp trap link-status
dot1x pae authenticator
dot1x timeout quiet-period 2
dot1x timeout tx-period 3

```

AAA Groups and Configuration:

```

aaa new-model
aaa group server radius packtfence
  server 192.168.1.5 auth-port 1812 acct-port 1813
aaa authentication login default local
aaa authentication dot1x default group packetfence
aaa authorization network default group packetfence

```

Radius server configuration:

```

radius-server host 192.168.1.5 auth-port 1812 acct-port 1813 timeout 2 key
  useStrongerSecret
radius-server vsa send authentication

```

802.1X with MAC Authentication bypass (MultiHost)

Global config settings:

```

dot1x system-auth-control

```

On each interface:

```

switchport mode access
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer restart 10800
authentication timer reauthenticate 7200
mab
no snmp trap link-status
dot1x pae authenticator
dot1x timeout quiet-period 2
dot1x timeout tx-period 3

```

AAA Groups and Configuration

```

aaa new-model
aaa group server radius packetfence
  server 192.168.1.5 auth-port 1812 acct-port 1813
aaa authentication login default local
aaa authentication dot1x default group packetfence
aaa authorization network default group packetfence

```

Radius server configuration

```

radius-server host 10.10.10.10 auth-port 1812 acct-port 1813 timeout 2 key
  useStrongerSecret
radius-server vsa send authentication

```

MAC Authentication bypass only

Global config settings

```

dot1x system-auth-control

```

On each interface

```

switchport mode access
switchport voice vlan 100
dot1x mac-auth-bypass
dot1x pae authenticator
dot1x port-control auto
dot1x timeout tx-period 5
dot1x reauthentication
authentication periodic
authentication timer restart 10800
authentication timer reauthenticate 7200
mab
no snmp trap link-status

```

AAA Groups and Configuration

```

aaa new-model
aaa group server radius packtfence
  server 192.168.1.5 auth-port 1812 acct-port 1813
aaa authentication login default local
aaa authentication dot1x default group packetfence
aaa authorization network default group packetfence

```

Radius server configuration

```

radius-server host 192.168.1.5 auth-port 1812 acct-port 1813 timeout 2 key
  useStrongerSecret
radius-server vsa send authentication

```


Port-Security

Global config settings

```
snmp-server enable traps port-security
snmp-server enable traps port-security trap-rate 1
snmp-server host 192.168.1.5 version 2c public port-security
```

On each interface *without* VoIP:

```
switchport access vlan 4
switchport port-security
switchport port-security maximum 1 vlan access
switchport port-security violation restrict
switchport port-security mac-address 0200.000x.xxxx
```

where xxxxx stands for the interface ifIndex

On each interface *with* VoIP:

```
switchport voice vlan 100
switchport access vlan 4
switchport port-security
switchport port-security maximum 2
switchport port-security maximum 1 vlan access
switchport port-security violation restrict
switchport port-security mac-address 0200.000x.xxxx
```

where xxxxx stands for the interface ifIndex



ifIndex mapping

Use the following templates for interface IfIndex in bogus MAC addresses (0200.000x.xxxx):

- Fa0/1...Fa0/48 10001...10048
- Gio/1...Gio/48 10101...10148

Stacked 29xx, Stacked 35xx, Stacked 3750, 4500 Series, 6500 Series

The 4500 Series and all the stacked switches work exactly the same way as if they were not stacked so the configuration is the same: they support port-security with static MAC address and allow us to secure a MAC on the data VLAN so we enable it whether there is VoIP or not.

We need to secure bogus MAC addresses on ports in order for the switch to send a trap when a new MAC appears on a port.

Global config settings

```
snmp-server enable traps port-security
snmp-server enable traps port-security trap-rate 1
snmp-server host 192.168.1.5 version 2c public port-security
```

On each interface *without* VoIP:

```
switchport access vlan 4
switchport port-security
switchport port-security maximum 1 vlan access
switchport port-security violation restrict
switchport port-security mac-address 0200.000x.xxxx
```

On each interface *with* VoIP:

```
switchport voice vlan 100
switchport access vlan 4
switchport port-security
switchport port-security maximum 2
switchport port-security maximum 1 vlan access
switchport port-security violation restrict
switchport port-security mac-address 0200.000x.xxxx
```

where xxxxx stands for the interface ifIndex



ifIndex mapping

Use the following templates for interface IfIndex in bogus MAC addresses (0200.000x.xxxx):

- Fa1/0/1...Fa1/0/48 10001...10048
- Gi1/0/1...Gi1/0/48 10101...10148
- Fa2/0/1...Fa2/0/48 10501...10548
- Gi2/0/1...Gi2/0/48 10601...10648
- Fa3/0/1...Fa3/0/48 11001...11048
- Gi3/0/1...Gi3/0/48 11101...11148
- Fa4/0/1...Fa4/0/48 11501...11548
- Gi4/0/1...Gi4/0/48 11601...11648
- ...

Router ISR 1800 Series

PacketFence supports the 1800 series Router with linkUp / linkDown traps. It cannot do anything about the router interfaces (ie: fa0 and fa1 on a 1811). VLAN interfaces ifIndex should also be marked as uplinks in the PacketFence switch configuration as they generate traps but are of no interest to PacketFence (layer 3).

Global config settings:

```
snmp-server enable traps snmp linkdown linkup  
snmp-server host 192.168.1.5 trap version 2c public
```

On each interface:

```
switchport mode access  
switchport access vlan 4
```

D-Link

PacketFence supports D-Link switches without VoIP using two different trap types:

- linkUp/linkDown
- MAC Notification

We recommend to enable linkUp/linkDown and MAC notification together.

Don't forget to update the startup config!

DES3526 / 3550

Global config settings

```
To be contributed...
```

On each interface:

```
To be contributed...
```

DGS3100/3200

Global config settings

```
To be contributed...
```

On each interface:

```
To be contributed...
```

Dell

PowerConnect 3424

PacketFence supports this switch using linkUp/linkDown traps.

Global config settings

```
To be contributed...
```

On each interface:

```
To be contributed...
```

EdgecorE

PacketFence supports Edge-corE switches without VoIP using linkUp/linkDown traps.

Don't forget to update the startup config!

3526XA and 3528M

Global config settings

```
SNMP-server host 192.168.1.5 public version 2c udp-port 162
```

Enterasys

PacketFence supports Enterasys switches *without VoIP* using two different trap types:

- linkUp/linkDown
- MAC Locking (Port Security with static MACs)

We recommend to enable MAC locking only.

Don't forget to update the startup config!

Matrix N₃

linkUp/linkDown traps are enabled by default so we disable them and enable MAC locking only. Also, by default this switch doesn't do an electrical low-level linkDown when setting the port to admin down. So we need to activate a global option called forceLinkdown to enable this behaviour. Without this option, clients don't understand that they lost their connection and they never do a new DHCP on VLAN change.

Global config settings

```
set snmp community public
set snmp targetparams v2cPF user public security-model v2c message-processing v2c
set snmp notify entryPF tag TrapPF
set snmp targetaddr tr 192.168.1.5 param v2cPF taglist TrapPF
set maclock enable
set forceLinkdown enable
```

On each interface:

```
set port trap ge.1.xx disable
set maclock enable ge.1.xx
set maclock static ge.1.xx 1
set maclock firstarrival ge.1.xx 0
set maclock trap ge.1.xx enable
```

where xx stands for the interface index.

SecureStack C₂

linkUp/linkDown traps are enabled by default so we disable them and enable MAC locking only.

Global config settings

```
set snmp community public
set snmp targetparams v2cPF user public security-model v2c message-processing v2c
set snmp notify entryPF tag TrapPF
set snmp targetaddr tr 192.168.1.5 param v2cPF taglist TrapPF
set maclock enable
```

On each interface:

```
set port trap fe.1.xx disable
set maclock enable fe.1.xx
set maclock static fe.1.xx 1
set maclock firstarrival fe.1.xx 0
```

where xx stands for the interface index

SecureStack C₃

This switch has the particular *feature* of allowing more than one untagged egress VLAN per port. This means that you must add all the VLAN created for PacketFence as untagged egress VLAN on the relevant interfaces. This is why there is a VLAN command on each interface below.

linkUp/linkDown traps are enabled by default so we disable them and enable MAC locking only.

Global config settings

```
set snmp community public
set snmp targetparams v2cPF user public security-model v2c message-processing v2c
set snmp notify entryPF tag TrapPF
set snmp targetaddr tr 192.168.1.5 param v2cPF taglist TrapPF
set maclock enable
```

On each interface:

```
set vlan egress 1,2,3 ge.1.xx untagged
set port trap ge.1.xx disable
set maclock enable ge.1.xx
set maclock static ge.1.xx 1
set maclock firstarrival ge.1.xx 0
set maclock trap ge.1.xx enable
```

where xx stands for the interface index

Standalone D₂

linkUp/linkDown traps are enabled by default so we disable them and enable MAC locking only.



Caution

This switch Switch accepts multiple untagged VLAN per port when configured through SNMP. This is problematic because on some occasions the untagged VLAN port list can become inconsistent with the switch's running config. To fix that, clear all untagged VLANs of a port even if the CLI interface doesn't show them. To do so, use: `clear vlan egress <vlans> <ports>`

Global config settings

```
set snmp community public
set snmp targetparams v2cPF user public security-model v2c message-processing v2c
set snmp notify entryPF tag TrapPF
set snmp targetaddr tr 192.168.1.5 param v2cPF taglist TrapPF
set maclock enable
```

On each interface:

```

set port trap ge.1.xx disable
set maclock enable ge.1.xx
set maclock static ge.1.xx 1
set maclock firstarrival ge.1.xx 0
set maclock trap ge.1.xx enable

```

where xx stands for the interface index

Extreme Networks

PacketFence supports Extreme Networks switches using:

- linkUp/linkDown
- MAC Address Lockdown (Port Security)
- Netlogin - MAC Authentication
- Netlogin - 802.1X

Don't forget to save the configuration!

All Extreme XOS based switches

In addition to the SNMP and VLANs settings, this switch needs the Web Services to be enabled and an administrative username and password provided in its PacketFence configuration for Web Services.

MAC Address Lockdown (Port-Security)

linkUp/linkDown traps are enabled by default so we disable them and enable MAC Address Lockdown only.

Global config settings without Voice over IP (VoIP):

```

enable snmp access
configure snmp add trapreceiver 192.168.1.5 community public
enable web http
configure vlan "Default" delete ports <portlist>
configure vlan registration add ports <portlist> untagged
configure ports <portlist> vlan registration lock-learning
disable snmp traps port-up-down ports <portlist>

```

where <portlist> are ports you want to secure. It can be an individual port or a port-range with a dash.

Global config settings with Voice over IP (VoIP):

```

enable snmp access
configure snmp add trapreceiver 192.168.1.5 community public
enable web http
configure vlan "Default" delete ports <portlist>
configure vlan registration add ports <portlist> untagged
configure vlan voice add ports <portlist> tagged
configure ports <portlist> vlan registration lock-learning
configure ports <portlist> vlan voice limit-learning 1
disable snmp traps port-up-down ports <portlist>

```

where <portlist> are ports you want to secure. It can be an individual port or a port-range with a dash.

MAC Authentication

AAA Configuration

```

configure radius netlogin primary server 192.168.1.5 1812 client-ip 10.0.0.8 vr
VR-Default
configure radius netlogin primary shared-secret 12345
enable radius netlogin

```

Netlogin (Mac Authentication)

```

configure netlogin vlan temp
enable netlogin mac
configure netlogin dynamic-vlan enable
configure netlogin dynamic-vlan uplink-ports 50
configure netlogin mac authentication database-order radius
enable netlogin ports 1-48 mac
configure netlogin ports 1-48 mode port-based-vlans
configure netlogin ports 1-48 no-restart

```

802.1X

AAA Configuration

```

configure radius netlogin primary server 192.168.1.5 1812 client-ip 10.0.0.8 vr
VR-Default
configure radius netlogin primary shared-secret 12345
enable radius netlogin

```

Netlogin (802.1X)

```

configure netlogin vlan temp
enable netlogin dot1x
configure netlogin dynamic-vlan enable
configure netlogin dynamic-vlan uplink-ports 50
enable netlogin ports 1-48 dot1x
configure netlogin ports 1-48 mode port-based-vlans
configure netlogin ports 1-48 no-restart

```




Note

You can mix the MAC Authentication and 802.1X on the same switchport. If the device fails 802.1X authentication, it will roll back to the MAC Authentication.

Foundry

FastIron 4802

PacketFence support this switch with optional VoIP using two different trap types:

- linkUp/linkDown
- Port Security (with static MACs)

We recommend to enable Port Security only.

Don't forget to update the startup config!

Those switches support port-security with static MAC address and allow us to secure a MAC on the data VLAN so we enable it whether there is VoIP or not.

We need to secure bogus MAC addresses on ports in order for the switch to send a trap when a new MAC appears on a port.

Global config settings

```
snmp-server host 192.168.1.5 public
no snmp-server enable traps link-down
no snmp-server enable traps link-up
```

On each interface *without* VoIP:

```
int eth xx
  port security
  enable
  maximum 1
  secure 0200.0000.00xx 0
  violation restrict
```

where xx stands for the interface ifIndex.

With VoIP a little more work needs to be performed. Instead of the no-VoIP, put in the following config:

```

conf t
vlan <mac-detection-vlan>
  untagged eth xx
vlan <voice-vlan>
  tagged eth xx

int eth xx
  dual-mode <mac-detection-vlan>
  port security
    maximum 2
    secure 0200.00xx.xxxx <mac-detection-vlan>
    secure 0200.01xx.xxxx <voice-vlan>
  violation restrict
  enable

```

where xxxxxx stands for the interface number (filled with zeros), <voice-vlan> with your voice-VLAN number and <mac-detection-vlan> with your mac-detection VLAN number.

HP

E4800G and E5500G Switch series

These are re-branded 3Com switches, see under the [3Com section](#) for their documentation.

HP ProCurve

PacketFence supports ProCurve switches *without VoIP* using two different trap types:

- linkUp/linkDown
- Port Security (with static MACs)

We recommend to enable Port Security only.

Don't forget to update the startup config!



Note

HP ProCurve only sends one security trap to PacketFence per security violation so make sure PacketFence runs when you configure port-security. Also, because of the above limitation, it is considered good practice to reset the intrusion flag as a first troubleshooting step.

If you want to learn more about intrusion flag and port-security, please refer to the ProCurve documentation.



Caution

If you configure a switch that is already in production be careful that enabling port-security causes active MAC addresses to be automatically added to the intrusion list without a security trap sent to PacketFence. This is undesired because PacketFence will not be notified that it needs to configure the port. As a work-around, unplug clients before activating port-security or remove the intrusion flag after you enabled port-security with: `port-security <port> clear-intrusion-flag`.

2500 Series

linkUp/linkDown traps are enabled by default so we disable them and enable Port Security only.

On 2500's, we need to secure bogus MAC addresses on ports in order for the switch to send a trap when a new MAC appears on a port.

Global config settings:

```
snmp-server community "public" Unrestricted
snmp-server host 192.168.1.5 "public" Not-INFO
no snmp-server enable traps link-change 1-26
```

On each interface:

```
port-security xx learn-mode static action send-alarm mac-address 0200000000xx
```

where xx stands for the interface index

2600 Series and 3400cl Series

linkUp/linkDown traps are enabled by default so we disable them and enable Port Security only.

On 2600's, we don't need to secure bogus MAC addresses on ports in order for the switch to send a trap when a new MAC appears on a port.

Global config settings

```
snmp-server community public manager unrestricted
snmp-server host 192.168.1.5 "public" Not-INFO
no snmp-server enable traps link-change 1-26
```

On each interface:

```
port-security xx learn-mode configured action send-alarm
```

where xx stands for the interface index

4100, 5300, 5400 Series

Port-Security

linkUp/linkDown traps are enabled by default and we have not found a way yet to disable them so do not forget to declare the trunk ports as uplinks in the switch config file.

On 4100's, we need to secure bogus MAC addresses on ports in order for the switch to send a trap when a new MAC appears on a port. The ports are indexed differently on 4100's: it's based on the number of modules you have in your 4100, each module is indexed with a letter.

Global config settings

```
snmp-server community "public" Unrestricted
snmp-server host 192.168.1.5 "public" Not-INFO
no snmp-server enable traps link-change 1-26
```

You should configure interfaces like this:

```
port-security A1 learn-mode static action send-alarm mac-address 020000000001
...
port-security A24 learn-mode static action send-alarm mac-address 020000000024
port-security B1 learn-mode static action send-alarm mac-address 020000000025
...
port-security B24 learn-mode static action send-alarm mac-address 020000000048
port-security C1 learn-mode static action send-alarm mac-address 020000000049
...
```

MAC Authentication (with VoIP)

In order to have MAC Authentication working with VoIP, you need to ensure that the Voice VLAN is tagged on all the port first. You also need to activate lldp notification on all ports that will handle VoIP. Finally, make sure to change the value of the \$VOICEVLANAME variable in the Procurve 5400 module's source code.

RADIUS configuration

```
radius-server host 192.168.1.5 key strongKey
```

MAC Authentication

```
aaa port-access mac-based C5-C7
aaa port-access mac-based C5 addr-limit 2
aaa port-access mac-based C6 addr-limit 2
aaa port-access mac-based C7 addr-limit 2
aaa port-access C5 controlled-direction in
aaa port-access C6 controlled-direction in
aaa port-access C7 controlled-direction in
```

802.1X (with VoIP)

Same as MAC Authentication, you need to ensure that the Voice VLAN is tagged on all the port first if using 802.1X. You also need to activate lldp notification on all ports that will handle VoIP. Finally, make sure to change the value of the \$VOICEVLANAME variable in the Procurve 5400 module's source code.

RADIUS configuration

```
radius-server host 192.168.1.5 key strongKey
```

802.1X

```
aaa authentication port-access eap-radius
aaa port-access authenticator C3-C4
aaa port-access authenticator C3 client-limit 3
aaa port-access authenticator C4 client-limit 3
aaa port-access authenticator active
```

Intel

Express 460 and Express 530

PacketFence support these switches *without VoIP* using one trap type:

- linkUp/linkDown

Exact command-line configuration to be contributed...

Juniper

PacketFence supports Juniper switches without VoIP in MAC Authentication (Juniper's MAC RADIUS) mode.

```

# load replace terminal
[Type ^D at a new line to end input]
interfaces {
  interface-range access-ports {
    member-range ge-0/0/1 to ge-0/0/46;
    unit 0 {
      family ethernet-switching {
        port-mode access;
      }
    }
  }
}

protocols {
  dot1x {
    authenticator {
      authentication-profile-name packetfence;
      interface {
        access-ports {
          supplicant multiple;
          mac-radius {
            restrict;
          }
        }
      }
    }
  }
}

access {
  radius-server {
    192.168.1.5 {
      port 1812;
      secret "useStrongerSecret";
    }
  }

  profile packetfence {
    authentication-order radius;
    radius {
      authentication-server 192.168.1.5;
      accounting-server 192.168.1.5;
    }
    accounting {
      order radius;
      accounting-stop-on-failure;
      accounting-stop-on-access-deny;
    }
  }
}

Ctrl-D
# commit comment "packetfenced"

```

Change the interface-range statement to reflect the ports you want to secure with PacketFence.

LG-Ericsson

PacketFence supports iPECS series switches *without VoIP* using two different trap types:

- linkUp / linkDown
- Port Security (with static MACs)

On some recent models, we can also use more secure and robust features, like:

- MAC Authentication
- 802.1X

ES-4500G Series

LinkUp / LinkDown

Firmware 1.2.3.2 is required for linkUp / linkDown

Prior to config, make sure to create all necessities VLANs and config the appropriate uplink port.

Global config settings

```
snmp-server community public ro
snmp-server community private rw
!
snmp-server enable traps authentication
snmp-server host 192.168.1.5 public version 2c udp-port 162
snmp-server notify-filter traphost.192.168.1.5.public remote 192.168.1.5
```

Firmware is kinda buggy so you'll need to enable linkUp / linkDown using the Web Interface under Administration > SNMP.

Some reports shows that the switch doesn't always send linkDown traps.

On each interface (except uplink)

```
switchport allowed vlan add 4 untagged
switchport native vlan 4
switchport allowed vlan remove 1
switchport mode access
```

Port-Security

Firmware 1.2.3.2 is required for port-security.

Prior to config, make sure to create all necessary VLANs and config the appropriate uplink port.

Global config settings

```
snmp-server community public ro
snmp-server community private rw
!
snmp-server enable traps authentication
snmp-server host 192.168.1.5 public version 2c udp-port 162
snmp-server notify-filter traphost.192.168.1.5.public remote 192.168.1.5
```

On each interface (except uplink)

```
port security max-mac-count 1
port security
port security action trap
switchport allowed vlan add 2 untagged
switchport native vlan 2
switchport allowed vlan remove 1
switchport mode access
```

The above *port security* command may not work using the CLI. In this case, use the Web Interface under the Security → Port Security menu and enable each ports using the checkboxes.

It is also recommended, when using port-security, to disable link-change (UP / DOWN) traps.

Don't forget to update the startup config!

Linksys

PacketFence supports Linksys switches *without VoIP* using one trap type:

- linkUp/linkDown

Don't forget to update the startup config!

SRW224G4

Global config settings

```
no snmp-server trap authentication
snmp-server community CS_2000_le rw view Default
snmp-server community CS_2000_ls ro view Default
snmp-server host 192.168.1.5 public 2
```

On each interface


```
switchport access vlan 4
```

Netgear

FSM726 / FSM726S version 1

PacketFence supports FSM726 / FSM726S version 1 switches *without VoIP* in Port Security mode (with static MACs) – called Trusted MAC table on Netgear’s hardware.

Using the HTTP GUI, follow the steps below to configure such feature. Of course, you must create all your VLANs on the switch as well.

SNMP Settings

In **Advanced** **SNMP** **Community Table**, create a read-write community string and a trap community string. You can use the same community for all the 3 functions (Get, Set, Trap).

Next, under **Advanced** **SNMP** **Host Table**, enable the Host Authorization feature and add the PacketFence server into the allowed host list.

Finally, under **Advanced** **SNMP** **Trap Setting**, enable the authentication trap.

Trusted MAC Security

Under **Advanced** **Advanced Security** **Trusted MAC Address**, create a fake MAC address per port (ie. 02:00:00:00:00:xx where xx is the port number). This will have the effect of sending a security trap to PacketFence when a new device plugs on the port.

Don’t forget to save the configuration!

Nortel

PacketFence supports Nortel switches with VoIP using one trap type:

- Mac Security

Don’t forget to update the startup config!



Note

if you are using a 5500 series with a firmware version of 6 or above, you must use a different module called `Nortel::BayStack5500_6x` in your `/usr/local/pf/conf/switches.conf`. Indeed, Nortel introduced an incompatible change of behavior in this firmware.

BayStack 470, ERS2500 Series, ERS4500 Series, 4550, 5500 Series and ES325

Global config settings

```
snmp-server authentication-trap disable
snmp-server host 192.168.1.5 "public"
snmp trap link-status port 1-24 disable
no mac-security mac-address-table
interface FastEthernet ALL
mac-security port ALL disable
mac-security port 1-24 enable
default mac-security auto-learning port ALL max-addr
exit
mac-security enable
mac-security snmp-lock disable
mac-security intrusion-detect disable
mac-security filtering enable
mac-security snmp-trap enable
mac-security auto-learning aging-time 60
mac-security learning-ports NONE
mac-security learning disable
```

VoIP support

You need to ensure that all your ports are tagged with the voice VLAN. The switch should do the rest for you.

```
vlan create 6 name "Telephone" type port learning ivl
vlan members 6 1-20,23-24
```

BPS2000

You can only configure this switch through menus.

Enable MAC Address Security:

```

MAC Address Security: Enabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Enabled
Generate SNMP Trap on Intrusion: Enabled
Current Learning Mode: Disabled
Learn by Ports: NONE

```

Port	Trunk	Security
1		Enabled
...		
24		Enabled

SMC

TigerStack 6128L2, 8824M and 8848M

PacketFence supports these switches without VoIP using two different trap types:

- linkUp/linkDown
- Port Security (with static MACs)

We recommend to enable Port Security only.

Global config settings

```

SNMP-server host 192.168.1.5 public version 2c udp-port 162
no snmp-server enable traps link-up-down

```

On each interface:

```

port security max-mac-count 1
port security
port security action trap

```

TigerStack 6224M

Supports linkUp/linkDown mode

Global config settings

```

SNMP-server host 192.168.1.5 public version 1

```

Wireless Controllers and Access Point Configuration

Assumptions

Throughout this configuration example we use the following assumptions for our network infrastructure:

- PacketFence is fully configured with FreeRADIUS running
- PacketFence IP address: 192.168.1.5
- Normal VLAN: 1
- Registration VLAN: 2
- Isolation VLAN: 3
- MAC Detection VLAN: 4
- Guest VLAN: 5
- VoIP, Voice VLAN: 100
- use SNMP v2c
- SNMP community name: public
- RADIUS Secret: useStrongerSecret ¹
- Open SSID: PacketFence-Public
- WPA-Enterprise SSID: PacketFence-Secure

Unsupported Equipment

Wireless network access configuration is a lot more consistent between vendors. This is due to the fact that the situation is a lot more standardized than the wired side: VLAN assignment is done centrally with RADIUS and that the client protocol is consistent (MAC-Authentication or 802.1X).

This consistency has the benefit that a lot of the wireless network devices tend to work out-of-the-box with PacketFence. The only missing piece being, in most cases, remote deauthentication of the client which is used for VLAN assignment (deauth user so it'll reconnect and get new VLAN).

So, even if your wireless equipment is not explicitly supported by PacketFence, it's recommended that you give it a try. The next section covers the objectives that you want to accomplish for trying out your equipment even if we don't have configuration for it.

Here are the high-level requirements for proper wireless integration with PacketFence

- The appropriate VLANs must exist
- Allow controller to honor VLAN assignments from AAA (sometimes called AAA override)
- Put your open SSID (if any) in MAC-Authentication mode and authenticate against the FreeRADIUS hosted on PacketFence
- Put your secure SSID (if any) in 802.1X mode and authenticate against FreeRADIUS hosted on PacketFence.
- On registration / isolation VLANs the DHCP traffic must reach the PacketFence server
- On your production VLANs a copy of the DHCP traffic must reach PacketFence where a pfdhcplister listens (configurable in pf.conf under interfaces)

At this point, user registration with the captive-portal is possible and registered users should have access to the appropriate VLANs. However, VLAN changes (like after a registration) won't automatically happen, you will need to disconnect / reconnect. An explanation is provided in introduction section above about this behavior.

You can try modules similar to your equipment if any (read appropriate instructions) or you can try to see if RFC3576 is supported. RFC3576 covers RADIUS Packet of Disconnect (PoD) also known as Disconnect Messages (DM) or Change of Authorization (CoA). You can try the Aruba module if you want to verify if RFC3576 is supported by your hardware.

If none of the above worked then you can fallback to inline enforcement or let us know what equipment you are using on the [packetfence-devel mailing list](#).

AeroHIVE

AeroHIVE products are a bit different compared to the other vendors. They support either a local HiveManager (kind of wireless controller) or a cloud-based HVM. However, the configuration is the same for the local and the cloud-based controller. Note that all the config are made on the HVM and then pushed to the APs.

AAA Client Settings

In the HVM, go to Configuration → AAA Authentication → AAA Client Settings, and insert the proper properties:

- Give a RADIUS Name

- Add a RADIUS server with Authentication as the server type and primary as the role
- Make sure Permit Dynamic Change of Authorization is ticked (RFC 3576)

Public SSID

Again in the HVM, go to Configuration → SSIDs, and create a new SSID with the following:

- Give a Profile Name and an SSID Name
- Choose Open as the Access Security
- Select Enable Mac Authentication
- Select your RADIUS server from the RADIUS Server dropdown list

Secure SSID

In the HVM, go to Configuration → SSIDs, and create a new SSID with the following :

- Give a Profile Name and an SSID Name
- Choose WPA2 Enterprise as the Access Security
- Select WPA2-802.1X as the key management
- Select CCMP as the encryption method
- Select your RADIUS server from the RADIUS Server dropdown list

Roles (User Profiles)

Since PacketFence 3.3.0, we now support user profiles on the AeroHIVE hardware. To build a User Profile, go to Configuration → User Profiles, and create what you need. When you define the switch definition in PacketFence, the role will match the User Profile attribute number. Example

```
roles=CategoryStudent=1;CategoryStaff=2
```

And in the AeroHIVE configuration, you have :

```
StudentProfile attribute number 1  
StaffProfile attribute number 2
```

Last step is to allow the User Profile to be returned for a particular SSID. Go to Configuration → SSIDs → Your_SSID → User Profiles for Traffic Management, and select the User Profiles you will return for the devices.



Note

The VLAN ID is NOT returned by PacketFence if a role is available for a given category. The VLAN ID needs to be configured in the User Profile definition on the AeroHIVE side.

Caching and Roaming

AeroHIVE have a session replication feature to ease the EAP session roaming between two access points. However, this may cause problems when you bounce the wireless card of a client, it will not do a new RADIUS request. Two settings can be tweaked to reduce the caching impact, it is the roaming cache update interval and roaming cache ageout. They are located in Configuration > SSIDs > [SSID Name] > Optional Settings > Advanced.

Avaya

Wireless Controller (WC)

To be contributed....

Aruba

All Aruba OS

In this section, we cover the basic configuration of the Aruba wireless controller for PacketFence via the web GUI. It was done on an Aruba Controller 200 software version ArubaOS 5.0.3.3, tested on a Controller 600 with ArubaOS 6.0 but it should apply to all Aruba models.



Caution

If you are already using your Aruba controllers and don't want to impact your users you should create new AAA profiles and apply them to new SSIDs instead of modifying the default ones.



Note

Starting with PacketFence 3.3, Aruba supports role-based access control. Read the Administration Guide under "Role-based enforcement support" for more information about how to configure it on the PacketFence side.

AAA Settings

In the Web interface, go to Configuration > Authentication > RADIUS Server and add a RADIUS server named "packetfence" then edit it:

- Set Host to PacketFence's IP (192.168.1.5)
- Set the Key to your RADIUS shared secret (useStrongerSecret)

- Click Apply

Under Configuration → Authentication → Server Group add a new Server Group named "packetfence" then edit it to add your RADIUS Server "packetfence" to the group. Click Apply.

Under Configuration → Authentication → RFC3576 add a new server with PacketFence's IP (192.168.1.5) and your RADIUS shared secret (useStrongerSecret). Click Apply. Under Configuration → Authentication → L2 Authentication edit the MAC Authentication Profile called "default" then edit it to change the Delimiter to dash. Click Apply.

Under Configuration → Authentication → L2 Authentication edit the 802.1X Authentication Profile called "default" then edit it to uncheck the Opportunistic Key Caching under Advanced. Click Apply.

Under Configuration → Authentication → AAA Profiles click on the "default-mac-auth" profile then click on MAC Authentication Server Group and choose the "packetfence" server group. Click Apply. Move to the RFC3576 server sub item and choose PacketFence's IP (192.168.1.5) click add then apply.

Under Configuration → Authentication → AAA Profiles click on the "default-dot1x" profile then click on 802.1X Authentication Server Group and choose the "packetfence" server group. Click Apply. Move to the RFC3576 server sub item and choose PacketFence's IP (192.168.1.5) click add then apply.

Public SSID

In the Web interface, go to Configuration → AP Configuration then edit the "default" AP Group. Go in Wireless LAN → Virtual AP create a new profile with the following:

- AAA Profile: default-mac-auth
- SSID Profile: Select NEW then add an SSID (PacketFence-Public) and Network authentication set to None

Secure SSID

In the Web interface, go to Configuration → AP Configuration then edit the "default" AP Group. Go in Wireless LAN → Virtual AP create a new profile with the following:

- AAA Profile: default-dot1x
- SSID Profile: Select NEW then add an SSID (PacketFence-Secure) and Network authentication set to WPA2

Roles

Since PacketFence 3.3.0, we now support roles for the Aruba hardware. To add roles, go in Configuration → Access Control → User Roles → Add. You don't need to force a VLAN usage in the Role since we send also the VLAN ID along with the Aruba User Role in the RADIUS request. Refer to the Aruba User Guide for more information about the Role creation.

Aruba Controller 200

In this section, we cover the basic configuration of the Aruba Controller 200 for PacketFence using the command line interface. We suggest you to use the instructions above for the Web GUI instead.

VLAN definition

Here, we create our PacketFence VLANs, and our AccessPoint VLAN (VID 66). It is recommended to isolate the management of the thin APs in a separate VLAN.


```

vlan 2
vlan 3
vlan 5
vlan 10
vlan 66

```

AAA Authentication Server

```

aaa authentication-server radius "PacketFence"
    host 192.168.1.5
    key useStrongerSecret
aaa server-group "Radius-Group"
    auth-server PacketFence

```

AAA Profiles

```

aaa profile "default-dot1x"
    authentication-dot1x "default"
    dot1x-default-role "authenticated"
    dot1x-server-group "Radius-Group"
    radius-accounting "Radius-Group"
aaa profile "PacketFence"
    authentication-mac "pf_mac_auth"
    mac-server-group "Radius-Group"
    radius-accounting "Radius-Group"

```

WLAN SSIDs: profiles and virtual AP

```

wlan ssid-profile "PacketFence-Public"
    essid "PacketFence-Public"
wlan ssid-profile "PacketFence-Secure"
    essid "PacketFence-Secure"
    opmode wpa2-aes
wlan virtual-ap "Inverse-Guest"
    aaa-profile "PacketFence"
    ssid-profile "PacketFence-Public"
wlan virtual-ap "Inverse-Secure"
    aaa-profile "default-dot1x"
    ssid-profile "PacketFence-Secure"
ap-group "Inverse"
    virtual-ap "Inverse-Guest"
    virtual-ap "Inverse-Secure"
    ids-profile "ids-disabled"

```

Cisco

Aironet 1121, 1130, 1242, 1250



Caution

With this equipment, the same VLAN cannot be shared between two SSIDs. Have this in mind in your design. For example, you need two isolation VLAN if you want to isolate hosts on the public and secure SSIDs.

MAC-Authentication + 802.1X configuration

Radio Interfaces:

```
dot11 vlan-name normal vlan 1
dot11 vlan-name registration vlan 2
dot11 vlan-name isolation vlan 3
dot11 vlan-name guest vlan 5

interface Dot11Radio0
  encryption vlan 1 mode ciphers aes-ccm
  encryption vlan 2 mode ciphers aes-ccm
  ssid PacketFence-Public
  ssid PacketFence-Secure

interface Dot11Radio0.2
  encapsulation dot1Q 2
  no ip route-cache
  bridge-group 253
  bridge-group 253 subscriber-loop-control
  bridge-group 253 block-unknown-source
  no bridge-group 253 source-learning
  no bridge-group 253 unicast-flooding
  bridge-group 253 spanning-disabled

interface Dot11Radio0.3
  encapsulation dot1Q 3
  no ip route-cache
  bridge-group 254
  bridge-group 254 subscriber-loop-control
  bridge-group 254 block-unknown-source
  no bridge-group 254 source-learning
  no bridge-group 254 unicast-flooding
  bridge-group 254 spanning-disabled

interface Dot11Radio0.5
  encapsulation dot1Q 5
  no ip route-cache
  bridge-group 255
  bridge-group 255 subscriber-loop-control
  bridge-group 255 block-unknown-source
  no bridge-group 255 source-learning
  no bridge-group 255 unicast-flooding
  bridge-group 255 spanning-disabled
```

LAN interfaces:

```

interface FastEthernet0.2
  encapsulation dot1Q 2
  no ip route-cache
  bridge-group 253
  no bridge-group 253 source-learning
  bridge-group 253 spanning-disabled

interface FastEthernet0.3
  encapsulation dot1Q 3
  no ip route-cache
  bridge-group 254
  no bridge-group 254 source-learning
  bridge-group 254 spanning-disabled

interface FastEthernet0.5
  encapsulation dot1Q 5
  no ip route-cache
  bridge-group 255
  no bridge-group 255 source-learning
  bridge-group 255 spanning-disabled

```

Then create the two SSIDs:

```

dot11 ssid PacketFence-Secure
  vlan 3 backup normal
  authentication open eap eap_methods
  authentication key-management wpa

dot11 ssid PacketFence-Public
  vlan 2 backup guest
  authentication open mac-address mac_methods
  mbssid guest-mode

```

Configure the RADIUS server (we assume here that the FreeRADIUS server and the PacketFence server are located on the same box):

```

radius-server host 192.168.0.10 auth-port 1812 acct-port 1813 key
  useStrongerSecret
aaa group server radius rad_eap
  server 192.168.0.10 auth-port 1812 acct-port 1813
aaa authentication login eap_methods group rad_eap
aaa group server radius rad_mac
  server 192.168.0.10 auth-port 1812 acct-port 1813
aaa authentication login mac_methods group rad_mac

```

Wireless LAN Controller (WLC) 2106 and 4400

To be contributed...

Wireless Services Module (WiSM)

To be contributed...

D-Link

DWL Access-Points and DWS 3026

To be contributed...

Extricom

EXSW Wireless Switches (Controllers)

In order to have the Extricom controller working with PacketFence, you need to define two ESSID definition, one for the "public" network, and one for the "secure" network. This can be done under a very short time period since Extricom supports RADIUS assigned VLANs out of the box.

You first need to configure you RADIUS server. This is done under the: WLAN Settings → RADIUS tab. Enter the PacketFence RADIUS server information. For the ESSID configuration. in the administration UI, go to WLAN Settings → ESSID definitions. Create the profiles per the following:

Public SSID

- MAC Authentication must be ticked
- Encryption method needs to be set to None
- Select PacketFence as the MAC Authentication RADIUS server (previously added)

Secure SSID

- Encryption method needs to be set to WPA Enterprise/WPA2 Enterprise
- AES only needs to be selected
- Select PacketFence as the RADIUS server (previously added)

The final step is to enable SNMP Agent and SNMP Traps on the controller. This is done under the following tab in the administrative UI: Advanced → SNMP.

HP

ProCurve Controller MSM710

To be contributed...

Meru

Meru Controllers (MC)

In this section, we cover the basic configuration of the Meru wireless controller for PacketFence via the web GUI.

Disable PMK Caching

If you are running a WPA2 SSID, you may need to disable PMK caching in order to avoid deauthentication issues. This is true if you are running AP 300s using any 5.0 versions including 5.0-87, or any versions below 4.0-160.

Here are the commands to run to disable the PMK caching at the AP level. First, login the AP, and run this command to see which radios are broadcasting your SSID. `vap display`

Second, disable the PMK caching on those radios. `radio pmkid radiooo disable`

You can also add those commands to the AP bootscript. Contact your Meru support representative for that part.

VLAN Definition

Here, we create our PacketFence VLANs for client use. Go to Configuration > Wired > VLAN, and select Add.

- VLAN Name is the human readable name (ie. RegistrationVLAN)
- Tag is the VLAN ID
- Fast Ethernet Interface Index refers to the controller's ethernet interface
- IP Address – An IP address for this controller on this VLAN
- Netmask – Network mask for this VLAN
- IP Address of the default gateway – Wired IP router for this VLAN
- Set the Override Default DHCP server flag to off

- Leave the DHCP server IP address and the DHCP relay Pass-Through to default

Click OK to add the VLAN.

AAA Authentication Server

Here, we create our PacketFence RADIUS server for use. Under Configuration Security Radius, select Add.

- Give the RADIUS Profile a name
- Write a description of the profile
- Give the RADIUS IP, RADIUS Secret and the RADIUS authentication port
- Select Colon for the MAC address delimiter
- Select MAC Address as the password type

Click OK to add the RADIUS profile.

AAA Accounting Server

Here, we create our PacketFence RADIUS server for use. Under Configuration Security Radius, select Add.

- Give the RADIUS Profile a name
- Write a description of the profile
- Give the RADIUS IP, RADIUS Secret and the RADIUS accounting port
- Select Colon for the MAC address delimiter
- Select MAC Address as the password type

Click OK to add the RADIUS accounting profile.

AAA Profiles – Open SSID

Here, we create our wireless security profiles for use. Under Configuration Security Profile, select Add.

- Give the security profile a name
- Select Clear as the L2 Modes Allowed
- Leave Data Encrypt empty
- Disable the Captive Portal
- Enable the Mac Filtering

Click OK to save the profile.

MAC Filtering

When using the OpenSSID, you need to activate the mac filtering. Under Configuration Mac Filtering:

- Set ACL Environment State to Permit list enabled

- Select your RADIUS profile

AAA Profiles – Secure SSID

Here, we create our wireless security profiles for use. Under Configuration → Security → Profile, select Add.

- Give the security profile a name
- Select WPA2 as the L2 Modes Allowed
- Select CCMP-AES for Data Encrypt
- Select your PacketFence RADIUS Authentication Profile
- Disable the Captive Portal
- Enable the 802.1X network initiation
- Leave the Mac Filtering to off

Click OK to save the profile.

WLAN SSIDs

Here, we create our SSID and tie it to a security profile. Under Configuration → Wireless → ESS, select Add.

- Give the ESS profile a name, and enable it
- Write an SSID name
- Select your security profile name previously created
- Select your PacketFence RADIUS Accounting Profile (if you want to do accounting)
- Enable the SSID Broadcast
- Make the new AP to join the ESS
- Set the tunnel interface type to RADIUS and Configured VLAN
- Select the registration VLAN for the VLAN Name

Click OK to create the SSID. Repeat those steps for the open and secure SSID by choosing the right security profile.

WLAN SSIDs – Adding to access point

Here, we tie our SSIDs to access points. Under Configuration → Wireless → ESS, select the SSID you want to add to your aps. Then, select the ESS-AP Table, and click Add.

- Select the AP ID from the drop down list
- Click OK to associate the SSID with this AP

Roles (Per-User Firewall)

Since PacketFence 3.3.0, we now support roles (per-user firewall rules) for the Meru hardware. To add firewall rules, go in Configuration → QoS System Settings → QoS and Firewall Rules. When you add a rule, you have to pay attention to two things:

- The rule is applied to the controller physical interface right away, so make sure you are not too wide on your ACL to lock you out!
- The rules are grouped using the Firewall Filter ID (We will use this ID for the roles)

So, since the matching is done using the Firewall Filter ID configuration field, your roles line in switches.conf would look like :

```
roles=Guests=1;Staff=2
```



Note

You need to have the Per-User Firewall license in order to benefit this feature.

Motorola

In order to have the Motorola controller working with PacketFence, you need to define two Wireless LANs definition, one for the "public" network, and one for the "secure" network.

WiNG (Firmware >= 5.0)

AAA Policy (RADIUS server)

First, we need to build the AAA Policy. Under Configuration Wireless AAA Policy, click on the Add button at the bottom right. Configure the RADIUS profile like the following:

- Host: Choose IP Address in the drop down, and put the RADIUS server (PF) IP
- Insert a RADIUS secret passphrase
- Select "Through Wireless Controller" Request Mode



Caution

Since we are using RADIUS Dynamic Authorization, we need to enable the RADIUS accounting. Under the RADIUS accounting tab, click the Add button at the bottom right, and insert the proper values.

Open SSID

Under Configuration Wireless Wireless LANs, click on the Add button at the bottom right. Under Basic Configuration:

- Profile Name : Give a convenient name
- SSID: This is the ESSID name

- Ensure that the WLAN Status is set to enable
- Select Single VLAN as VLAN assignment technique
- Ensure that "Allow RADIUS Override" is selected

Security configuration:

- Select MAC as authentication type
- Select your AAA Policy previously created
- Ensure that you selected Open as the Encryption

Advanced configuration:

- Make sure you select RADIUS Dynamic Authorization

Secure SSID

Under Configuration > Wireless > Wireless LANs, click on the Add button at the bottom right. Under Basic Configuration:

- Profile Name : Give a convenient name
- SSID: This is the ESSID name
- Ensure that the WLAN Status is set to enable
- Select Single VLAN as VLAN assignment technique
- Ensure that "Allow RADIUS Override" is selected

Security configuration:

- Select EAP as authentication type
- Select your AAA Policy previously created
- Ensure that you selected WPA/WPA2-TKIP as the Encryption
- Unselect everything under Fast Roaming (Disable caching)

Advanced configuration:

- Make sure you select RADIUS Dynamic Authorization

Profile (WLAN Mapping)

You have multiple options here. Either, you create a general AP profile, and you assign it to your Aps, or you modify the AP device configuration to map the WLAN to the radio interfaces. For the purpose of this document, we will modify the general profile. Under Profiles > default-apXXX (where XXX is your AP model), in Interface > Radios, edit the existing radios settings. Go to the WLAN Mapping tab, select the two SSIDs and click on the << button.

Profile (Management)

Here, we can configure our SNMP community strings. Located in Configuration Management Management Policy. Again, you can modify the default one, or you can create a brand new Policy.

VLANs

You need to ensure that the uplink interface of the controller is configured as a trunk, and that all the necessary VLANs are created on the device. This is configured under Device `ifsXXXX-MAC` (where XXXX is your controller series, and MAC is the latest 3 octets of its mac address). Edit the device configuration, and go to Interface Ethernet Ports. Ensure that the up1 interface is set as trunk, with all the allowed VLANs. Next, create the VLAN under Interface Virtual Interfaces.

Roles (Per-User Firewall)

Since PacketFence 3.3.0, we now support roles for the Motorola hardware using WiNGS 5.x. To add roles, go in Configuration Security Wireless Client Roles. First create a global policy that will contain your roles. Next, create your Roles by clicking on the Add button on the bottom right. It is important to configure the Group Configuration line properly by setting the string name that we will use in the RADIUS packet. For example, for a Guests Role, you can put Group Configuration Exact Guests, and for a Staff Roles, you can put Group Configuration Exact Staff. In the roles configuration in switches.conf, you would have something like :

```
roles=CategoryGuests=Guests;CategoryStaff=Staff
```

Finally, don't forget to configure the appropriate firewall rules for your Roles! Make sure also to commit the configuration upon your changes.



Note

You need to have an Advanced Security license to enable the Per-User Firewall feature.

Older Firmwares (< 5.0)

Option for Public Wireless LAN

- Check the Dynamic Assignment check-box
- Select "MAC Authentication" under Authentication
- Click "Config..." choose the Colon delimiter format
- Un-check all encryption options
- Under RADIUS put in PacketFence's RADIUS Server information

Option for Secure Wireless LAN

- Check the Dynamic Assignment check-box
- Select "802.1X EAP" under Authentication

- Check WPA/WPA2-TKIP encryption option
- Under RADIUS put in PacketFence's RADIUS Server information

SNMP Global configuration

Add the two Read-Only and Read-Write users under Management Access SNMP Access.

Ruckus

AAA Servers

We need to define the RADIUS and RADIUS accounting (mandatory):

Under Configuration AAA Servers, click on the Create New button. Enter the proper configuration:

- Enter a server name
- Select either RADIUS or RADIUS accounting as the type
- Use PAP as the Auth Method
- Enter the IP address, and shared secret.
- Hit OK

Repeat the steps for the RADIUS and RADIUS accounting types. We need 1 definition for each otherwise RADIUS dynamic authorization won't work.

WLAN Definitions

Under Configuration WLAN, click on the Create New button. Enter the proper configuration:

Open SSID

- Enter a Name/SSID
- Select Standard Usage as the Type
- Select MAC Address as the authentication type
- Select Open as the encryption method
- Select the proper RADIUS server as the authentication server
- Select the proper RADIUS server as the accounting server



Note

The Open SSID does NOT support dynamic VLAN assignments (Firmware 9.3.0.0.83)

Secure SSID

- Enter a Name/SSID
- Select Standard Usage as the Type
- Select WPA2 as the authentication type
- Select AES as the encryption method
- Select the proper RADIUS server as the authentication server
- Select the proper RADIUS server as the accounting server
- Check the Enable Dynamic VLAN checkbox

Trapeze

In order to have the Trapeze controller working with PacketFence, you need to define the RADIUS configuration and the proper service profiles.

RADIUS configuration

```
set radius server PF address 192.168.1.5 timeout 5 retransmit 3 deadtime 0 key
secret
set server group PF-RADIUS members PF
```

Service Profiles

Here we define two service profiles, one for the open SSID (PF-Open) and one for the WPA2-Enterprise SSID (PF-Secure):

```
set service-profile PF-Open ssid-name CSPI-PF-Open
set service-profile PF-Open ssid-type clear
set service-profile PF-Open auth-fallthru last-resort
set service-profile PF-Open cipher-tkip enable
set service-profile PF-Open auth-dot1x disable
set service-profile PF-Open 11n mode-na required
set service-profile PF-Open attr vlan-name WLAN_REG

set service-profile PF-Secure ssid-name CSPI-PF-Secure
set service-profile PF-Secure cipher-tkip enable
set service-profile PF-Secure cipher-ccmp enable
set service-profile PF-Secure wpa-ie enable
set service-profile PF-Secure rsn-ie enable
set service-profile PF-Secure 11n mode-na required
set service-profile PF-Secure attr vlan-name Wlan

set radio-profile default service-profile CSPI-PF-Open
set radio-profile default service-profile CSPI-PF-Secure
```

AAA configuration

Finally, we need to tie the service profiles with the proper AAA configuration.

```
set accounting dot1x ssid PF-Secure ** start-stop PF-RADIUS
set accounting mac ssid PF-Open * start-stop PF-RADIUS
set authentication mac ssid PF-Open * PF-RADIUS
set authentication dot1x ssid PF-Secure ** pass-through PF-RADIUS
```

Xirrus

Xirrus WiFi Arrays

Xirrus Access Points can be configured to work with PacketFence quickly since Xirrus supports RADIUS assigned VLANs out of the box.

First, RADIUS server configuration. Set the RADIUS server to be PacketFence's IP:

```
radius-server ! (global settings)
!
external
  primary server 192.168.1.5
  primary secret useStrongerSecret
!
accounting
  primary server 192.168.1.5
  primary secret useStrongerSecret
exit
exit
exit
```

Enable SNMP Agent on the access point:

```
snmp
!
v2
  community read-write public
  community read-only public
exit
!
exit
```

Finally, don't forget to create the SSID you want and the proper bindings with the LAN. Open SSID should be configured to perform MAC Authentication and Secure SSID should be configured to perform 802.1X (WPA-Enterprise or WPA2-Enterprise).

Additional Information

For more information, please consult the mailing archives or post your questions to it. For details, see:

- packetfence-announce@lists.sourceforge.net: Public announcements (new releases, security warnings etc.) regarding PacketFence
- packetfence-devel@lists.sourceforge.net: Discussion of PacketFence development
- packetfence-users@lists.sourceforge.net: User and usage discussions

Commercial Support and Contact Information

For any questions or comments, do not hesitate to contact us by writing an email to: support@inverse.ca.

Inverse (<http://inverse.ca>) offers professional services around PacketFence to help organizations deploy the solution, customize, migrate versions or from another system, performance tuning or aligning with best practices.

Hourly rates or support packages are offered to best suit your needs.

Please visit <http://inverse.ca/support.html> for details.

GNU Free Documentation License

Please refer to <http://www.gnu.org/licenses/fdl-1.2.txt> for the full license.