Network Devices Configuration Guide
for PacketFence version 9.3.0
# Table of Contents

1. About this Guide ........................................................................................................... 1
2. Other sources of information ...................................................................................... 1
3. Note on Inline enforcement support .......................................................................... 2
4. Note on RADIUS accounting .................................................................................... 3
5. List of supported Network Devices ........................................................................... 4
6. Assumptions ............................................................................................................... 5
7. 3COM ......................................................................................................................... 5
8. Alcatel .......................................................................................................................... 11
9. AlliedTelesis ............................................................................................................... 14
10. Amer ......................................................................................................................... 19
11. Avaya ......................................................................................................................... 19
12. Brocade ..................................................................................................................... 21
13. Cisco ........................................................................................................................ 24
14. Cisco Small Business (SMB) ................................................................................... 52
15. D-Link ......................................................................................................................... 54
16. Dell .............................................................................................................................. 56
17. Edge core ................................................................................................................... 60
18. Enterasys ................................................................................................................... 60
19. Extreme Networks ..................................................................................................... 63
20. Foundry ..................................................................................................................... 65
21. H3C ............................................................................................................................. 66
22. HP ............................................................................................................................... 69
23. HP ProCurve .............................................................................................................. 71
24. Huawei ....................................................................................................................... 78
25. IBM ............................................................................................................................ 80
26. Intel ............................................................................................................................. 81
27. Juniper ....................................................................................................................... 81
28. LG-Ericsson ............................................................................................................... 85
29. Linksys ...................................................................................................................... 87
30. Netgear ...................................................................................................................... 87
31. Nortel ......................................................................................................................... 90
32. Pica8 .......................................................................................................................... 92
33. SMC ......................................................................................................................... 93
34. Ubiquiti ...................................................................................................................... 94
35. Wireless Controllers and Access Point Configuration ............................................... 97
   Assumptions ............................................................................................................... 97
   Unsupported Equipment ............................................................................................ 97
   Aerohive Networks .................................................................................................... 98
   Anyfi Networks ......................................................................................................... 114
   Avaya ........................................................................................................................ 117
   Aruba .......................................................................................................................... 117
   Belair Networks (now Ericsson) .................................................................................. 135
   Brocade ..................................................................................................................... 136
   Cambium ................................................................................................................... 136
   Cisco ........................................................................................................................... 140
   CoovaChilli ............................................................................................................... 156
   D-Link ......................................................................................................................... 158
   Extricom ..................................................................................................................... 158
   Fortinet FortiGate ...................................................................................................... 159
   hostapd (OpenWrt Chaos Calmer 15.05) ................................................................... 160
Chapter 1

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 https://packetfence.org/documentation/

Other sources of information

- **Clustering Guide**
  Covers installation in a clustered environment.

- **Developer's Guide**
  Covers API, captive portal customization, application code customizations and instructions for supporting new equipment.

- **Installation Guide**
  Covers installation and configuration of PacketFence.

- **Upgrade Guide**
  Covers compatibility related changes, manual instructions and general notes about upgrading.

- **NEWS.asciidoc**
  Covers noteworthy features, improvements and bug fixes by release.

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, except RADIUS inline. 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.
Enabling RADIUS accounting on your network devices will increase significantly your database size and can cause performance issues. You should be aware of this and use accounting only if you really need it.
List of supported Network Devices

PacketFence supports a whole lot of different wireless and wired network equipment from various vendors running different versions. Since we want to provide the most accurate information and avoid duplication of that same information, please refer to our website https://packetfence.org/about.html#material

You'll find on this page the enforcement modes supported by each and every single piece of equipment we tested and worked with.
Chapter 5

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
- Guest VLAN: 5
- VoIP, Voice VLAN: 100
- use SNMP v2c
- SNMP Read community: public
- SNMP Write community: private
- 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`
- `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`

### In MAC Auth

- Voice vlan : 6
- Normal vlan : 1
- Registration vlan : 2
- Isolation vlan : 3

### Global config settings:

- `lldp enable`
- `lldp timer tx-interval 5`
- `lldp compliance cdp`
- `lldp compliance cdp`

- `port-security enable`
- `MAC-authentication domain packetfence`
radius scheme system
radius scheme packetfence
server-type extended
primary authentication 192.168.1.5
primary accounting 192.168.1.5
key authentication Packetfence
key accounting cipher Packetfence
user-name-format without-domain

domain packetfence
authentication radius-scheme packetfence
accounting radius-scheme packetfence
vlan-assignment-mode string
accounting optional
domain system

voice vlan mac-address f4ea-6700-0000 mask ffff-ff00-0000 description Cisco IP Phone
undo voice vlan security enable
voice vlan 6 enable

On each interface with VoIP:

interface Ethernet1/0/1
  stp edged-port enable
  lldp compliance admin-status cdp txrx
  port link-type hybrid
  port hybrid vlan 6 tagged
  port hybrid vlan 1 2 3 untagged
undo voice vlan mode auto
voice vlan enable
port-security max-mac-count 3
port-security port-mode mac-authentication
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:
Chapter 5

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
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.
Alcatel

OS6250, OS6450

PacketFence supports this switch using 802.1X, Mac authentication and also supports VoIP.

Global configuration

First define any VLAN that you want to use on the switch.

```plaintext
vlan 2
vlan 5
vlan 20
vlan 100
```

Next, configure the RADIUS server to be PacketFence

```plaintext
aaa radius-server "packetfence" host 192.168.1.5 key useStrongerSecret
aaa authentication mac packetfence
aaa authentication 802.1X packetfence
```

You now need to configure a user profile (equivalent of a role) that will determine which VLAN is assigned to the device. In this case the profile names are unreg, employee and guest.

```plaintext
aaa user-network-profile name unreg vlan 2
aaa user-network-profile name guest vlan 5
aaa user-network-profile name employee vlan 20
```

Next, configure the switch in PacketFence. In the case of this example, the uplink is port 1/1.

```plaintext
[192.168.1.10]
mode=production
description=alcatel
type=Alcatel
radiusSecret=useStrongerSecret
uplink_dynamic=0
uplink=1001
RoleMap=Y
VlanMap=N
registrationRole=unreg
isolationRole=unreg
defaultRole=employee
guestRole=guest
```

802.1X

First, make sure you followed the steps above in Global configuration
Chapter 5

You will need to configure the ports you want to do authentication on.

```plaintext
vlan port mobile 1/2
vlan port 1/2 802.1X enable
802.1X 1/2 supplicant policy authentication pass group-mobility block fail block
802.1X 1/2 non-suppliant policy authentication pass group-mobility block fail block
```

### MAC Authentication

First, make sure you followed the steps above in *Global configuration* and *802.1X*

Next configure the interface to bypass 802.1X authentication

```plaintext
802.1X 1/2 supplicant bypass enable
```

### VoIP

PacketFence supports VoIP on Alcatel by having multiple devices using multiple untagged VLANs on the same port.

First configure the user profile for voice. In this example it is only isolating it on another VLAN but any user profile attributes can be added to the profile.

```plaintext
aaa user-network-profile name voice vlan 3
```

Next, make sure you enable VoIP in the switch configuration in PacketFence and configure the voiceRole.

```plaintext
[192.168.1.10]
VoIPEnabled=Y
voiceRole=voice
```

### OS6860

PacketFence supports this switch using 802.1X, Mac authentication and also supports VoIP.

**Note**

This documentation is made for Alcatel OS 8.1+. Lower versions do not support this configuration.

### Global configuration

First define any VLAN that you want to use on the switch.

```plaintext
vlan 2 admin-state enable
vlan 5 admin-state enable
vlan 20 admin-state enable
vlan 100 admin-state enable
```
Next, configure the RADIUS server to be PacketFence

```
aaa radius-server "packetfence" host 192.168.1.5 key useStrongerSecret
aaa device-authentication mac packetfence
aaa device-authentication 802.1X packetfence
```

You now need to configure an edge profile (equivalent of a role) that will determine which VLAN is assigned to the device. In this case the profile names are `unreg`, `employee` and `guest`.

```
unp edge-profile unreg
  unp edge-profile unreg redirect enable
  unp edge-profile unreg authentication-flag enable
  unp vlan-mapping edge-profile unreg vlan 2

unp edge-profile guest
  unp edge-profile guest redirect enable
  unp edge-profile guest authentication-flag enable
  unp vlan-mapping edge-profile guest vlan 5

unp edge-profile employee
  unp edge-profile employee redirect enable
  unp edge-profile employee authentication-flag enable
  unp vlan-mapping edge-profile employee vlan 20
```

⚠️ **Caution**

Make sure you enable the redirect on **all** your roles as the access reevaluation will not work without it.

Next, configure the switch in PacketFence. In the case of this example, the uplink is port 1/1/1.

```
[192.168.1.10]
mode=production
description=alcatel
type=Alcatel
radiusSecret=useStrongerSecret
uplink_dynamic=0
uplink=1001
RoleMap=Y
VlanMap=N
registrationRole=unreg
isolationRole=unreg
defaultRole=employee
guestRole=guest
```

**MAC Authentication**

First, make sure you followed the steps above in **Global configuration**

You will need to create an edge template and apply it on the ports you want to do authentication on.
Chapter 5

```yaml
unp edge-template pf_mab
unp edge-template pf_mab mac-authentication enable
unp edge-template pf_mab classification enable
unp port 1/1/2 port-type edge
unp port 1/1/2 edge-template pf_mab
```

**802.1X**

First, make sure you followed the steps above in *Global configuration*

You will need to create an edge template and apply it on the ports you want to do authentication on.

```yaml
unp edge-template pf_dot1x
unp edge-template pf_dot1x 802.1X-authentication enable
unp edge-template pf_dot1x mac-authentication enable
unp edge-template pf_dot1x 802.1X-authentication failure-policy mac-authentication
unp port 1/1/2 port-type edge
unp port 1/1/2 edge-template pf_dot1x
```

**VoIP**

PacketFence supports VoIP on Alcatel by having multiple devices using multiple untagged VLANs on the same port.

First configure the edge profile for voice. In this example it is only isolating it on another VLAN but any edge profile attributes can be added to the profile.

```yaml
unp edge-profile voice
unp edge-profile voice redirect enable
unp edge-profile voice authentication-flag enable
unp vlan-mapping edge-profile voice vlan 100
```

Next, make sure you enable VoIP in the switch configuration in PacketFence and configure the `voiceRole`.

```
[192.168.1.10]
VoIPEnabled=Y
voiceRole=voice
```

---

**AlliedTelesis**

**AT8000GS**

PacketFence supports the AT8000GS switch using:

- MAC Authentication
- 802.1X
• 802.1X + VOIP

Assumptions

PacketFence management IP: 192.168.1.5
Switch management IP: 10.0.0.14
Guest VLAN (Internet): VLAN 1

MAC Authentication

First, enable 802.1X globally:

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

Next, configure the RADIUS server and AAA settings:

```bash
radius-server host 192.168.1.5
radius-server key useStrongerSecret
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:

```bash
interface vlan 1
name "Guest Vlan"
dot1x guest-vlan
exit
```

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

```bash
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, enable 802.1X globally:

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

Next, configure the RADIUS server and AAA settings:

```bash
radius-server host 192.168.1.5
radius-server key useStrongerSecret
radius-server source-ip 10.0.0.14
aaa authentication dot1x default radius
aaa accounting dot1x radius
```
Finally, enable the necessary 802.1X settings:

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

**802.1X + VOIP**

First, enable 802.1X globally:

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

Next, configure the RADIUS server configuration and AAA settings:

```bash
radius-server host 192.168.1.5
radius-server key useStrongerSecret
radius-server source-ip 10.0.0.14
aaa authentication dot1x default radius
aaa accounting dot1x radius
```

Then, LLDP configuration:

```bash
hostname switch-name
ip domain-name domain.local
lldp med network-policy 1 voice vlan 100 vlan-type tagged dscp 34
lldp med network-policy 2 voice-signaling vlan 100 vlan-type tagged dscp 34
```

Finally, enable the necessary 802.1X and VOIP settings on each interface:

```bash
interface ethernet g1
dot1x port-control force-authorized
no dot1x guest-vlan enable
no dot1x mac-authentication
no dot1x radius-attributes vlan
no dot1x re-authentication
switchport mode trunk
switchport trunk native vlan 5
switchport trunk allowed vlan add 100
lldp med enable network-policy
lldp med network-policy add 1
lldp med network-policy add 2
```

**GS950**

PacketFence supports the GS950 switch using:

- MAC Authentication
- 802.1X (without fallback to MAC authentication)
Global configuration

First, ensure that the VLANs you want to assign are part of the VLAN database via the following page:

Note that they only need to be tagged on the trunk and don’t need any specific configuration for the dynamic VLAN assignment here.

Next, configure the RADIUS server (Security→RADIUS):

Next, configure an SNMP community (SNMP→Community Table)

MAC authentication

Go in Security→Port Access Control, select the port you want to enable MAB on, and ensure you set:
• Authentication Mode: MAC Based
• Port Control: Auto
• Supplicant Mode: Single
• VLAN Assignment: Enabled

802.1x

Go in Security→Port Access Control, select the port you want to enable MAB on, and ensure you set:

• Authentication Mode: 802.1X
• Port Control: Auto
• Supplicant Mode: Multiple
• VLAN Assignment: Enabled

PacketFence configuration

Ensure you configure at least:

• Type: Allied Telesis GS950
• RADIUS secret: useStrongerSecret
• SNMP Version: v2c
• SNMP Community Read: private
• SNMP Community Write: private
If you are using MAC authentication on this switch, you must adjust the FreeRADIUS configuration so it transforms the EAP requests this switch sends into requests that PacketFence will interpret as MAC authentication. This configuration will also set missing attributes in the RADIUS requests since this switch doesn’t follow the standard attributes that are usually sent during RADIUS authentication.

To adjust it, go in `/usr/local/pf/conf/radiusd/packetfence` and add the following below the line that contains `packetfence-eap-mac-policy`:

```
packetfence-allied-gs950-mab
```

And then restart FreeRADIUS:

```
# /usr/local/pf/bin/pfcmd service radiusd restart
```

---

**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.
802.1X with MAC Authentication Bypass and VoIP

**Note**

The configuration below requires an ntp server. We use the PacketFence server as the NTP server but any other one will do. If you want to use the PacketFence server for NTP, make sure you install the appropriate service and open port 123 in `/usr/local/pf/conf/iptables.conf`

Global config settings:

```plaintext
sntp server primary address 192.168.1.5
sntp enable
radius server host 192.168.1.5 acct-enable
radius server host key useStrongerSecret
radius server host key useStrongerSecret used-by eapol
radius server host key useStrongerSecret used-by non-eapol
radius dynamic-server client 192.168.1.5
radius dynamic-server client 192.168.1.5 secret useStrongerSecret
radius dynamic-server client 192.168.1.5 enable
radius dynamic-server client 192.168.1.5 process-change-of-auth-requests
radius dynamic-server client 192.168.1.5 process-disconnect-requests
```

```plaintext
vlan create 2,3,4,5 type port
vlan create 100 type port voice-vlan
vlan name 2 "Reg"
vlan name 3 "Isol"
vlan name 4 "Detect"
vlan name 5 "Guest"
vlan name 100 "Voice"
```

```plaintext
#Uplink configuration
vlan ports 24 tagging tagAll
vlan configcontrol autopvid
```

```plaintext
eapol multihost allow-non-eap-enable
eapol multihost radius-non-eap-enable
eapol multihost non-eap-phone-enable
eapol multihost use-radius-assigned-vlan
eapol multihost non-eap-use-radius-assigned-vlan
eapol multihost eap-packet-mode unicast
eapol multihost non-eap-reauthentication-enable
eapol multihost adac-non-eap-enable
no eapol multihost non-eap-pwd-fmt ip-addr
no eapol multihost non-eap-pwd-fmt port-number
eapol multihost voip-vlan 1 enable vid 100
```
Brocade

Note
By default, all deconnections will be done using SNMP.

ICX 6400 Series
Those switches are supported using 802.1X for networks with or without VoIP.

- Global config settings:

```plaintext
aaa authentication dot1x default radius
radius-server host 192.168.1.5 auth-port 1812 acct-port 1813 default
radius-server key useStrongerSecret

vlan 1 name DEFAULT-VLAN by port
! vlan 100 by port
tagged ethe 1/1/xx ethe 1/1/yy
```
Where \( xx \) and \( yy \) represent the range of ports where you want PacketFence enforcement.

**MAC-Authentication without VoIP**

- Enable MAC-Authentication globally

```plaintext
mac-authentication enable
mac-authentication mac-vlan-dyn-activation
```

- Enable MAC-Authentication on each interface you want PacketFence active

```plaintext
mac-authentication enable
mac-authentication enable-dynamic-vlan
```

**MAC-Authentication with VoIP**

- Enable cdp globally

```plaintext
cdp run
```

- Apply the following configuration on each interface you want PacketFence active

```plaintext
dual-mode
mac-authentication enable
mac-authentication enable-dynamic-vlan
voice-vlan 100
cdp enable
```

**802.1X/MAC-Auth**

- Enable 802.1X globally

```plaintext
dot1x enable
re-authentication
enable ethe 1/1/xx
```

Where \( xx \) is the switch port number

- Apply the following configuration on each interface you want PacketFence active

```plaintext
dot1x port-control auto
dual-mode
mac-authentication enable
mac-authentication enable-dynamic-vlan
voice-vlan 100
```

**Firmware 08.0.80 and above**

**802.1x/MAC-Auth**

Those switches are supported using 802.1X for networks with or without VoIP.
• RADIUS server configuration

    radius-server host 192.168.1.5 auth-port 1812 acct-port 1813 default key useStrongerSecret dot1x mac-auth no-login

• Authentication configuration

    aaa authentication dot1x default radius
    authentication
        auth-default-vlan 2
        re-authentication
        auth-fail-action restricted-vlan
        dot1x enable
        dot1x enable ethe 1/1/1
        dot1x port-control auto ethe 1/1/1
        dot1x macauth-override
        dot1x timeout tx-period 3
        dot1x timeout quiet-period 2
        mac-authentication enable
        mac-authentication enable ethe 1/1/1

The configuration above enables authentication on port 1/1/1 - make sure you change this to the ports where you want to perform enforcement.

• SNMP configuration

    snmpserver community public ro
    snmpserver community private rw

• PacketFence configuration

While configuring the switch in PacketFence, ensure you set at least the following values: * Definition, Type: Brocade Switches * RADIUS, Secret Passphrase: useStrongerSecret * SNMP, Version: v2c * SNMP, Community Read: public * SNMP, Community Write: private

VoIP

In order to enable VoIP, you first need to enable LLDP then define the network policy for tagging VoIP traffic on the ports where PacketFence is enabled.

    lldp run
    lldp med network-policy application voice tagged vlan 5 priority 5 dscp 46 ports ethe 1/1/1

Note

Make sure you change VLAN 5 to the VLAN you use for VoIP

• PacketFence configuration

While configuring the switch in PacketFence, ensure you set at least the following values: * Roles, voice VLAN: 5 * Definition, VoIP: enabled
Radius CLI Login

If you want to use the server PacketFence to authenticate users on the Brocade switch.

- Configure the radius server to send user authentication request to PacketFence

```text
aaa authentication login default radius local
```

**Note**

Make sure to have a local account in case the switch can not reach the PacketFence server

Cisco

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

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

You also need to make sure that lldp or cdp notification is configured on all ports that will handle VoIP.

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 / 3500XL Series

**SNMP | linkUP/linkDown**

Global config settings:
Chapter 5

```
snmp-server community public RO
snmp-server community private RW
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

#### Warning

Make sure that you have a local account, because enabling 802.1X or MAB will ask for a username and password on the next login.

#### Global config settings:

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

#### AAA 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
```
AAA configuration (accounting):

```
aaa accounting dot1x default start-stop 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
```

On each interface \textit{without VoIP}:

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

On each interface \textit{with VoIP}:

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

\textbf{Port-Security}

\begin{itemize}
\item \textbf{Caution}
\end{itemize}

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 \textit{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 \textit{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 \textit{ifIndex}.

\textbf{ifIndex mapping}

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

- Fa0/1, ..., Fa0/48 \( \Rightarrow 1, ..., 48 \)
- Gi0/1, Gi0/2 \( \Rightarrow 49, 50 \)

Global config settings with VoIP:

```
snmp-server community public RO
snmp-server community private RW
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
```

\textbf{3550 (802.1X with MAB)}

\textbf{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.

\textbf{Caution}

The Catalyst 3550 does not support CoA. \texttt{Minimal IOS required for CoA is 12.2(52)SE.} Latest available IOS for 3550 is 12.2(46)SE. Set "Deauthentication Method" to “SNMP” in PacketFence Administration GUI under Network→ Switches for the switch IP configured below.
Chapter 5

Global settings:

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

Enable SNMP on the switch:

```
snmp-server community public RO
snmp-server community private RW
```

On each interface:

```
switchport mode access
dot1x mac-auth-bypass
dot1x pae authenticator
dot1x port-control auto
dot1x violation-mode protect
dot1x timeout quiet-period 2
dot1x timeout reauth-period 7200
dot1x timeout tx-period 3
dot1x reauthentication
```

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 community public RO
snmp-server community private RW
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
- Gi0/1...Gi0/48 → 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 community public RO
snmp-server community private RW
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 \text{xxxx} stands for the interface \text{ifIndex}.

On each interface with VoIP:

\begin{verbatim}
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
\end{verbatim}

where \text{xxxx} stands for the interface \text{ifIndex}

\textbullet \quad \text{ifIndex mapping}

Use the following templates for interface \text{IfIndex} in bogus MAC addresses (0200.000x.xxxxx):

\begin{itemize}
  \item Fa0/1...Fa0/48 \rightarrow 10001...10048
  \item Gi0/1...Gi0/48 \rightarrow 10101...10148
\end{itemize}

\section*{2960, 2970, 3560, 3750}

\textbf{Note}  
You shouldn’t use any port-security features when doing 802.1X and/or Mac Authentication. This can cause unexpected behavior.

\textbf{Warning}  
Make sure that you have a local account, because enabling 802.1X or MAB will ask for a username and password on the next login.

\section*{Global settings:}

\begin{verbatim}
dot1x system-auth-control
aaa new-model
aaa group server radius packetfence
  server name pfnac
aaa authentication login default local
aaa authentication dot1x default group packetfence
aaa authorization network default group packetfence
\end{verbatim}

RADIUS server configuration:
radius server pfnac
  address ipv4 192.168.1.5 auth-port 1812 acct-port 1813
  automate-tester username dummy ignore-acct-port idle-time 3
  key 0 useStrongerSecret
radius-server vsa send authentication

CoA configuration

aaa server radius dynamic-author
  client 192.168.1.5 server-key useStrongerSecret
  port 3799

Activate SNMP v1 on the switch:

snmp-server community public RO

802.1X with MAC Authentication bypass (MultiDomain)

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
  authentication violation replace
  mab
  no snmp trap link-status
  dot1x pae authenticator
  dot1x timeout quiet-period 2
  dot1x timeout tx-period 3

802.1X with MAC Authentication bypass (MultiHost)

On each interface:
MAC Authentication bypass only

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
authentication violation replace mab
no snmp trap link-status
```

802.1X on various models of 2960

There's a lot of different versions of the Catalyst 2960. Some of them may not accept the command stated in this guide for 802.1X.

We have found a couple of commands that are working great or MAB:

On each interface

```
switchport mode access
authentication order mab
authentication port-control auto
mab
dot1x pae authenticator
```

But, as it is difficult for us to maintain the whole list of commands to configure each and every different model of 2960 with different IOS, please refer to Cisco documentation for very specific cases.
Port-Security

Global config settings

```
softmax-server community public RO
softmax-server community private RW
softmax-server enable traps port-security
softmax-server enable traps port-security trap-rate 1
softmax-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 `xxxx` 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 `xxxx` 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
- Gi0/1…Gi0/48 → 10101…10148

**Web auth**

The Catalyst 2960 supports web authentication from IOS 12.2.55SE3. This procedure has been tested on IOS 15.0.2SE5.

In this example, the ACL that triggers the redirection to the portal for registration is `registration`.

Configure the global configuration of the switch using the section `MAC Authentication bypass only` of the 2960 in this document.

Then add this additional configuration on the global level
ip device tracking
ip http server
ip http secure-server
snmp-server community public RO
snmp-server community private RW

Add the required access lists

ip access-list extended registration
deny ip any host <your captive portal ip>
permit tcp any any eq www
permit tcp any any eq 443

Then on each controlled interface

switchport access vlan <vlan>
switchport mode access
authentication priority mab
authentication port-control auto
authentication periodic
authentication violation replace
mab
spanning-tree portfast

PacketFence switch configuration

- Select the type to Cisco Catalyst 2960
- Set the Registration role to registration (If left empty then it will use the role name)
- Set Role by Web Auth URL for registration to http://<your_captive_portal_ip>/Cisco::Catalyst_2960
- The URL can contain dynamic parameters, like the MAC address ($mac), the switch IP ($switch_ip), the username ($user_name).
- Screenshots of this configuration are available in the Cisco WLC section of this guide.

Downloadable ACLs

The Catalyst 2960 supports RADIUS pushed ACLs which means that you can define the ACLs centrally in PacketFence without configuring them in your switches and their rules will be applied to the switch during the authentication.

These ACLs are defined by role like the VLANs which means you can define different ACLs for your registration VLAN, production VLAN, guest VLAN, etc.

Add the following configuration setting on the global level

ip device tracking

For IOS 12.2, you need to create this acl and assign it to the switch port interface:
Chapter 5

ip access-list extended Auth-Default-ACL
  permit udp any range bootps 65347 any range bootpc 65348
  permit udp any any range bootps 65347
  permit udp any any eq domain
  deny ip any any

interface GigabitEthernetx/y/z
  ...
  ip access-group Auth-Default-ACL in
  ...

Before continuing, configure your switch to be in MAC authentication bypass or 802.1X.

Now in the PacketFence interface go in the switch configuration and in the Roles tab.

Check **Role by access list** and you should now be able to configure the access lists as below.

For example if you want the users that are in the registration VLAN to only use HTTP, HTTPS, DNS and DHCP you can configure this ACL in the registration category.

![Switch 172.21.2.3](image-url)

---

Copyright © 2019 Inverse inc.
Now if for example, your normal users are placed in the *default* category and your guests in the *guest* category.

If for example the *default* category uses the network 192.168.5.0/24 and your guest network uses the network 192.168.10.0/24.

You can prevent communications between both networks using these access lists.

You could also only prevent your guest users from using shared directories.
Or also you could restrict your users to use only your DNS server where 192.168.5.2 is your DNS server.
Web auth and Downloadable ACLs

It's possible to mix web authentication and downloadable ACLs starting from version 12.2 of the IOS, each roles can be configured to forward the device to the captive portal for an http or an https and only allow specific traffic with the ACL. To do that, you need to configure PacketFence with Role by Web Auth URL and with Role by access list (For each role you need). On the switch you need to change the Auth-Default-ACL to add the portal IP address:

For IOS 12.2:

```
ip access-list extended Auth-Default-ACL
    permit udp any any eq www
    permit udp any any eq domain
    permit udp any eq bootpc any eq bootps
deny ip any any
```

And assign this ACL on the switch port yo want to do ACL per port.
interface GigabitEthernetx/y/z
  ...
ip access-group Auth-Default-ACL in
  ...

For IOS 15.0:

Extended IP access list Auth-Default-ACL
  10 permit udp any range bootps 65347 any range bootpc 65348
  20 permit udp any any range bootps 65347
  30 deny ip any any

conf t
  ip access-list extend Auth-Default-ACL
  21 permit ip any host ip_of_the_captive_portal

For IOS 15.2:

Extended IP access list Auth-Default-ACL
  10 permit udp any any eq domain
  20 permit tcp any any eq domain
  30 permit udp any eq bootps any
  40 permit udp any eq bootpc
  50 permit udp any eq bootpc any
  60 deny ip any any

conf t
  ip access-list extend Auth-Default-ACL
  51 permit ip any host ip_of_the_captive_portal

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 community public RO
snmp-server community private RW
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.xxxxx

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.xxxxx

where xxxxx stands for the interface ifIndex

ifIndex mapping

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

- 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
- ...

IOS XE Switches

PacketFence supports the IOS XE switches in MAC Authentication Bypass, 802.1X and web authentication.

MAC Authentication Bypass

Global config settings:

dot1x system-auth-control
Chapter 5

On each interface:

```
authentication host-mode multi-domain
authentication order mab
authentication priority mab
authentication port-control auto
authentication periodic
authentication timer restart 10800
authentication timer reauthenticate 10800
authentication violation replace
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 192.168.1.5 auth-port 1812 acct-port 1813 timeout 2 key
useStrongerSecret
radius-server vsa send authentication
```

CoA configuration:

```
aaa server radius dynamic-author
  client 192.168.1.5 server-key useStrongerSecret
  port 3799
```

Activate SNMP on the switch:

```
snmp-server community public RO
```

**802.1X only**

Follow the same configuration as for MAC Authentication Bypass but change the `authentication priority` line with the following:

```
authentication priority dot1x
```

**802.1X with MAC Authentication fallback**

Follow the same configuration as for MAC Authentication Bypass but change the `authentication priority` line with the following:
Chapter 5

authentication priority dot1x mab

Web auth

Web auth requires at least MAC Authentication Bypass to be activated on the switchport but can also work with 802.1X. Configure your switchports as you would usually do, then add the following access lists.

```
ip access-list extended redirect
deny ip any host 192.168.1.5
deny udp any any eq domain
deny tcp any any eq domain
deny udp any any eq bootpc
deny udp any any eq bootps
permit tcp any any eq www
permit tcp any any eq 443
ip access-list extended registered
permit ip any any
```

Global config settings:

```
ip device tracking
```

PacketFence switch configuration:

- Select the type to *Cisco Catalyst 2960*
- Set the *Registration* role to *registration* (If left empty then it will use the role name)
- Set Role by Web Auth URL for registration to http://<your_captive_portal_ip>/Cisco::Catalyst_2960
- The URL can contain dynamic parameters, like the MAC address ($mac), the switch IP ($switch_ip), the username ($user_name).
- Screenshots of this configuration are available in the Cisco WLC section of this guide.

**Note**

AAA authentication is slow to come up after a reload of the IOS XE switches. This makes the recovery from a reboot longer to complete. This is due to a bug in IOS XE. A workaround is to execute the following command: `no aaa accounting system default start-stop group tacacs+`.

Identity Networking Policy

Starting from version 15.2(1)E (IOS) and 3.4.0E (IOSXE), Cisco introduced the Identity Based Networking Services. It means that you can create an authentication workflow on the switch and create interfaces templates.

To enable it:

```
authentication display new-style
```
Chapter 5

Global config settings:

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

AAA groups and configuration:

```
aaa new-model
aaa group server radius packetfence
    server name packetfence
!
aaa authentication login default local
aaa authentication dot1x default group packetfence
aaa authorization network default group packetfence
radius-server vsa send authentication
```

RADIUS server configuration:

```
radius-server dead-criteria time 5 tries 4
radius-server deadtime 1
radius server packetfence
    address ipv4 192.168.1.5 auth-port 1812 acct-port 1813
    key useStrongerSecret
    automate-tester username cisco ignore-acct-port idle-time 1
```

CoA configuration:

```
aaa server radius dynamic-author
    client 192.168.1.5 server-key useStrongerSecret
    port 3799
```

Enable SNMP on the switch:

```
snmp-server community public RO
```

Enable HTTP and HTTPS server:

```
ip http server
ip http secure-server
```

Enable IP device tracking:

```
ip device tracking
```

Fallback ACL:

```
ip access-list extended ACL-CRITICAL-V4
    permit ip any any
```

Service Template:
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
  voice vlan
service-template CRITICAL_AUTH_VLAN
service-template CRITICAL-ACCESS
description *Fallback Policy on AAA Fail*
  access-group ACL-CRITICAL-V4
!

Class map:

class-map type control subscriber match-any IN_CRITICAL_AUTH
  match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
  match activated-service-template CRITICAL_AUTH_VLAN
  match activated-service-template CRITICAL-ACCESS
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH
  match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
  match activated-service-template CRITICAL_AUTH_VLAN
  match activated-service-template CRITICAL-ACCESS
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
  match result-type aaa-timeout
  match authorization-status unauthorized
!
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
  match result-type aaa-timeout
  match authorization-status authorized
!
class-map type control subscriber match-all DOT1X_NO_RESP
  match method dot1x
  match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all MAB_FAILED
  match method mab
  match result-type method mab authoritative
!
class-map type control subscriber match-all DOT1X_FAILED
  match method dot1x
  match result-type method dot1x authoritative

Policy map:

On the 3 following configurations if the RADIUS server is down then we will apply CRITI-
CAL_AUTH_VLAN, DEFAULT_CRITICAL_VOICE_TEMPLATE and CRITICAL-ACCESS service tem-
plate. If the RADIUS server goes up then it reinitializes the authentication if the port is in IN_CRITI-
CAL_VLAN.

for 802.1X with MAC Authentication fallback:
policy-map type control subscriber DOT1X_MAB
  event session-started match-all
    10 class always do-until-failure
    10 authenticate using dot1x priority 10
  event authentication-failure match-first
    5 class DOT1X_FAILED do-until-failure
      10 terminate dot1x
      20 authenticate using mab priority 20
    10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
      10 activate service-template CRITICAL_AUTH_VLAN
      20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
      30 activate service-template CRITICAL-ACCESS
      40 authorize
      50 pause reauthentication
    20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
      10 activate service-template CRITICAL_AUTH_VLAN
      20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
      30 activate service-template CRITICAL-ACCESS
      40 pause reauthentication
      50 authorize
    30 class DOT1X_NO_RESP do-until-failure
      10 terminate dot1x
      20 authenticate using mab priority 20
    40 class MAB_FAILED do-until-failure
      10 terminate mab
      20 authentication-restart 10800
    60 class always do-until-failure
      10 terminate dot1x
      20 terminate mab
      30 authentication-restart 10800
  event agent-found match-all
    10 class always do-until-failure
    10 terminate mab
    20 authenticate using dot1x priority 10
  event aaa-available match-all
    10 class IN_CRITICAL_AUTH do-until-failure
      10 clear-session
    20 class NOT_IN_CRITICAL_AUTH do-until-failure
      10 resume reauthentication
  event inactivity-timeout match-all
    10 class always do-until-failure
    10 clear-session
  event authentication-success match-all
    10 class always do-until-failure
    10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
  event violation match-all
    10 class always do-all
    10 replace

for MAC Authentication only:
policy-map type control subscriber MACAUTH
event session-started match-all
  10 class always do-until-failure
  10 authenticate using mab priority 10
  event authentication-failure match-first
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
  10 activate service-template CRITICAL_AUTH_VLAN
  20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
  30 activate service-template CRITICAL-ACCESS
  40 authorize
  50 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
  10 activate service-template CRITICAL_AUTH_VLAN
  20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
  30 activate service-template CRITICAL-ACCESS
  40 pause reauthentication
  50 authorize
  30 class always do-until-failure
  10 terminate mab
  20 authentication-restart 30
  event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
  10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
  10 resume reauthentication
  event inactivity-timeout match-all
  10 class always do-until-failure
  10 clear-session
  event authentication-success match-all
  10 class always do-until-failure
  10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE

for 802.1X only:
policy-map type control subscriber DOT1X
event session-started match-all
  10 class always do-until-failure
  10 authenticate using dot1x priority 10
event authentication-failure match-first
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
  10 activate service-template CRITICAL_AUTH_VLAN
  20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
  30 activate service-template CRITICAL-ACCESS
  40 authorize
  50 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
  10 activate service-template CRITICAL_AUTH_VLAN
  20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
  30 activate service-template CRITICAL-ACCESS
  40 pause reauthentication
  50 authorize
  30 class DOT1X_FAILED do-until-failure
  10 terminate dot1x
  40 class DOT1X_NO_RESP do-until-failure
  10 terminate dot1x
  60 class always do-until-failure
  10 terminate dot1x
  20 authentication-restart 10800
event agent-found match-all
  10 class always do-until-failure
  10 authenticate using dot1x priority 10
event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
  10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
  10 resume reauthentication
event inactivity-timeout match-all
  10 class always do-until-failure
  10 clear-session
event authentication-success match-all
  10 class always do-until-failure
  10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE

Interface Template (802.1X MAC Authentication):
template identity-template-mab
dot1x pae authenticator
spanning-tree portfast edge
switchport access vlan 1
switchport mode access
switchport voice vlan 100
mab
access-session host-mode multi-domain
access-session control-direction in
access-session closed
access-session port-control auto
authentication periodic
authentication timer reauthenticate server
service-policy type control subscriber DOT1X_MAB

Interface Template (MAC Authentication):

template identity-template-macauth
dot1x pae authenticator
spanning-tree portfast edge
switchport access vlan 1
switchport mode access
switchport voice vlan 100
mab
access-session host-mode single-host
access-session control-direction in
access-session closed
access-session port-control auto
authentication periodic
authentication timer reauthenticate server
service-policy type control subscriber MACAUTH

Interface Template (802.1X):

template identity-template-dot1x
dot1x pae authenticator
spanning-tree portfast edge
switchport access vlan 1
switchport mode access
switchport voice vlan 100
mab
access-session host-mode single-host
access-session control-direction in
access-session closed
access-session port-control auto
authentication periodic
authentication timer reauthenticate server
service-policy type control subscriber DOT1X

On each interface for 802.1X with MAC Authentication:
source template identity-template-mab
dot1x timeout tx-period 5

On each interface for MAC Authentication:

source template identity-template-macauth

On each interface for 802.1X:

source template identity-template-dot1x
dot1x timeout tx-period 5

To see what is the status of a port let's run:

sh access-session interface fastEthernet 0/2 details

Interface: FastEthernet0/2
MAC Address: 101f.74b2.f6a5
IPv6 Address: Unknown
IPv4 Address: 172.20.20.49
User-Name: ACME\bob
Status: Authorized
Domain: DATA
Oper host mode: multi-domain
Oper control dir: in
Session timeout: 12380s (server), Remaining: 12206s
Timeout action: Terminate
Common Session ID: AC148729000000C000F8B7A
Acct Session ID: Unknown
Handle: 0x9C000001
Current Policy: DOT1X_MAB

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
Vlan Group: Vlan: 20
Idle timeout: 30 sec

Method status list:
 Method   State
   dot1x   Authc Success

Debug command:

In order to be able to debug the Identity Networking Policy you can launch the following command in the switch cli:

term mon
debuge pre all
**DHCP Option 82**

In order to enable the DHCP Option 82, you need to add the following parameters. Let's say you want to enable it for the vlan 1 to 1024:

```
ip dhcp snooping
ip dhcp snooping vlan 1-1024
```

On uplink interfaces:

```
ip dhcp snooping trust
```

**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
```

**EAP-FAST authentication Support**

PacketFence supports Cisco NEAT through EAP-MD5, EAP-FAST, EAP-GTC and EAP-MSCHAPv2 authentication methods. Upon successful authentication against PacketFence, the authenticator switch will give trunk access to the supplicant switch.


The following configuration example contains required changes to be applied on both authenticator and supplicant switches to provide EAP-FAST authentication against PacketFence.

**Authenticator**

Global settings:

```
aaa group server radius packetfence
server 192.168.1.5 auth-port 1812 acct-port 1813
aaa authentication dot1x default group packetfence
aaa authorization network default group packetfence
```
cisp enable

Uplink configuration:

interface FastEthernet0/20
switchport mode access
authentication port-control auto
dot1x pae authenticator

Supplicant

Global settings (replace username and password):

cisp enable

eap profile EAP_PRO
  method fast

dot1x credentials EAP_PRO
  username switches
  password 7 03174C02120C29495D
  ! Password is switches
  !
dot1x supplicant force-multicast

Uplink settings:

interface GigabitEthernet1/0/24
switchport mode trunk
dot1x pae supplicant
dot1x credentials EAP_PRO
dot1x supplicant eap profile EAP_PRO

Device Sensor for Cisco Equipment

Device sensor is a way to be able to receive some information about endpoints from the RADIUS accounting packet. (like DHCP, CDP, LLDP and HTTP information) In order to enable Device Sensor feature, you need to add the following parameters to your switch configuration:

radius server packetfence
address ipv4 192.168.1.5 auth-port 1812 acct-port 1813
key useStrongerSecret
aaa group server radius packetfence
  server name packetfence
!
aaa accounting update newinfo
aaa accounting identity default start-stop group packetfence
!
device-sensor filter-list dhcp list dhcp-list
  option name host-name
  option name parameter-request-list
  option name class-identifier
!
device-sensor filter-list lldp list lldp-list
  tlv name system-description
!
device-sensor filter-list cdp list cdp-list
  tlv name version-type
  tlv name platform-type
!
device-sensor filter-list dhcp list lldp-list
device-sensor filter-spec dhcp include list dhcp-list
device-sensor filter-spec lldp include list lldp-list
device-sensor filter-spec cdp include list cdp-list
device-sensor notify all-changes

This configuration will make the switch send information about DHCP, LLDP and CDP of the endpoint in the RADIUS accounting packets.

Cisco Small Business (SMB)

The Cisco Small Business switches support MAC based authentication (MAB) as well as 802.1X and VoIP. Both technologies can be combined and will work correctly together on the same switchport.

Nothing is required to activate VoIP on the switch, you must simply configure the voice VLAN you want PacketFence to assign in the PacketFence switch configuration as well as enabling VoIP there. Note that your phones must not tag their packets on the network and should send their traffic untagged when connected into a PacketFence enabled port. This means you should not have the voice VLAN capabilities enabled on the switch itself as they might conflict with the authorization attributes returned by PacketFence.

Global configuration

⚠️ Caution

Before executing these steps, make sure you have a local account configured to login on the switch or are pointing to a RADIUS server for management. Otherwise, you will not be able to login into the switch anymore.
Chapter 5

You must first define your RADIUS server and point it to PacketFence:

```
dot1x system-auth-control
radius-server key useStrongerSecret
radius-server host 192.168.1.5
```

```
aaa accounting dot1x start-stop group radius
```

```
snmp-server community public ro view Default
snmp-server community private rw view Default
```

SNMP configuration for the Cisco SG300:

```
snmp-server community public ro view DefaultSuper
snmp-server community private rw view DefaultSuper
```

**MAC Authentication**

In order to configure MAC authentication, you must enable it on each interface

```
interface x/y/z
  dot1x host-mode multi-sessions
  dot1x reauthentication
  dot1x timeout quiet-period 10
  dot1x timeout server-timeout 5
  dot1x timeout supp-timeout 3
  dot1x authentication mac
  dot1x radius-attributes vlan
  dot1x port-control auto
  spanning-tree portfast
  switchport mode general
  switchport general pvid 2
```

**802.1X with MAB**

In order to configure 802.1X with a fall-back to MAC authentication, you must enable it on each interface
interface x/y/z
dot1x host-mode multi-sessions
dot1x reauthentication
dot1x timeout quiet-period 10
dot1x timeout server-timeout 5
dot1x timeout supp-timeout 3
dot1x authentication dot1x mac
dot1x radius-attributes vlan
dot1x port-control auto
spanning-tree portfast
switchport mode general
switchport general pvid 2

Once you have configured your switchports, you must configure the switch in PacketFence with the following information:

- **Definition→Type:** Cisco SG500
- **Definition→Mode:** production
- **Definition→Deauthentication Method:** SNMP
- **Definition→VoIP enabled if you need VoIP on this switch.**
- **Roles→voice VLAN** set to the VLAN you want to assign to the VoIP devices connecting to this switch.
- **RADIUS→Secret Passphrase:** useStrongerSecret
- **SNMP→Version:** v2c
- **SNMP→Community Read:** public
- **SNMP→Community Write:** private

### 802.1X commands

- `show dot1x`
- `show dot1x users`

### 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

<table>
<thead>
<tr>
<th>To be contributed...</th>
</tr>
</thead>
</table>

On each interface:

<table>
<thead>
<tr>
<th>To be contributed...</th>
</tr>
</thead>
</table>

**DGS3100/3200**

Enable MAC notification:

```text
enable mac_notification
config mac_notification interval 1 historysize 1
config mac_notification ports 1:1-1:24 enable
```

Enable linkup/linkdown notification:

```text
enable snmp traps
enable snmp linkchange_traps
```

Add SNMP host:

```text
create snmp host 192.168.1.5 v2c public
```

Enable MAC base access control:

```text
enable mac_based_access_control
config mac_based_access_control authorization attributes radius enable local disable
config mac_based_access_control method radius
config mac_based_access_control password useStrongerSecret
config mac_based_access_control password_type manual_string
config mac_based_access_control max_users no_limit
config mac_based_access_control trap state enable
config mac_based_access_control log state enable
```

On each interface:

```text
config mac_based_access_control ports 1:1 state enable
config mac_based_access_control ports 1:1 max_users 128
config mac_based_access_control ports 1:1 aging_time 1440
config mac_based_access_control ports 1:1 block_time 300
config mac_based_access_control ports 1:1 mode host_based
```
Dell

Note

When doing MAC Authentication, there is a known issue with some Dell switches. If you get errors where the device is using EAP type MD5, but PacketFence is expecting PEAP, you will need to edit the line `default_eap_type = peap` under the section `eap` in the file `/usr/local/pf/conf/radiusd/eap.conf` to `default_eap_type = md5`.

Force 10

PacketFence supports this switch using RADIUS, MAC-Authentication and 802.1X.

Global config settings

```bash
radius-server host 192.168.1.5 key s3cr3t auth-port 1812
```

MAB interface configuration:

```bash
interface GigabitEthernet 0/1
no ip address
switchport
dot1x authentication
dot1x mac-auth-bypass
dot1x auth-type mab-only
no shutdown
```

802.1X interface configuration:

```bash
interface GigabitEthernet 0/1
no ip address
switchport
dot1x authentication
no shutdown
```

PowerConnect 3424

PacketFence supports this switch using linkUp/linkDown traps.

Global config settings to define the RADIUS server
configure
radius-server host auth 10.34.200.30
name PacketFence
usage 802.1x
key s3cr3t
exit

Configure CoA

aaa server radius dynamic-author
client 10.34.200.30 server-key s3cr3t
auth-type all
exit

Enable authentication and globally enable 802.1x client authentication via RADIUS

authentication enable
aaa authentication dot1x default radius
aaa authorization network default radius
dot1x system-auth-control

(Optional)

dot1x dynamic-vlan enable

On the interface, enable MAC based authentication mode, enable MAB, and set the order of authentication to 802.1X followed by MAC authentication. Also enable periodic re-authentication.

interface te1/0/4
dot1x port-control mac-based
dot1x mac-auth-bypass
authentication order dot1x mab
dot1x reauthentication
default mab pap
exit

authentication order mab
authentication priority mab

N1500 Series Switch

PacketFence supports this switch using RADIUS, MAC-Authentication, 802.1x and VoIP

802.1X with MAC Authentication fallback and VoIP

We assume that the switch ip is 192.168.1.254

First on the uplink add this configuration:
dot1x port-control force-authorized
switchport mode trunk
switchport trunk allowed vlan 1-5,100

Global config settings

configure
vlan 2,3,4,5,100
vlan 2
name "Registration"
vlan 3
name "Isolation"
vlan 4
name "Mac detection"
vlan 5
name "Guest"
vlan 100
name "VoIP"

authentication enable
dot1x system-auth-control
aaa authentication dot1x default radius
aaa authorization network default radius
dot1x dynamic-vlan enable
voice vlan
aaa server radius dynamic-author
client 192.168.1.5 server-key "useStrongerSecret"
exit
radius-server host auth 192.168.1.5
name "PacketFence"
usage 802.1x
key "useStrongerSecret"
exit
aaa server radius dynamic-author
client 192.168.1.5 server-key "useStrongerSecret"
exit

snmp-server community "private" rw
snmp-server community "public" ro

On each interface (not uplink)
switchport voice detect auto
switchport mode general
switchport access vlan 10
dot1x port-control mac-based
dot1x reauthentication
dot1x mac-auth-bypass
authentication order mab
authentication priority mab
lldp transmit-tlv sys-desc sys-cap
lldp transmit-mgmt
lldp notification
lldp med confignotifcation
voice vlan 100
exit

N2000 Series (N2024P)

This configuration was tested with firmware version 6.2.1.6

Global config settings:

Radius configuration:

aaa authentication login "defaultList" local
authentication enable
dot1x system-auth-control
aaa authentication dot1x default radius
aaa authorization network default radius
dot1x dynamic-vlan enable
radius-server key "useStrongerSecret"
radius-server host auth 192.168.1.5
name "PacketFence"

802.1X interface configuration:

interface Gi0/0/1
switchport mode general
switchport general allowed vlan add 1-3,100
dot1x port-control mac-based
dot1x unauth-vlan 2
dot1x mac-auth-bypass
authentication order mab dot1x
voice vlan 100
exit
Chapter 5

**Edge core**

PacketFence supports Edge-corE switches without VoIP using linkUp/linkDown traps.
PacketFence also supports MAC authentication on the Edge-corE 4510

### 3526XA and 3528M

**Global config settings**

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

### 4510

**Basic configuration**

```
network-access aging
snmp-server community private rw
snmp-server community public rw

radius-server 1 host 192.168.1.5 auth-port 1812 acct-port 1813 timeout 5
retransmit 2 key useStrongerSecret
radius-server key useStrongerSecret
```

**On each controlled interface**

```
interface ethernet 1/8
switchport allowed vlan add <your list of allowed vlans> untagged
network-access max-mac-count 1
network-access mode mac-authentication
```

### 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 behavior. 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 \textit{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
- RADIUS authentication for CLI access

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>
cfgure vlan registration add ports <portlist> untagged
cfgure ports <portlist> vlan registration lock-learning
disable snmp traps port-up-down ports <portlist>
```

where \textit{<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 add mac-list default
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.

RADIUS authentication for CLI access

Configure RADIUS server IP address as primary server and the switch IP address as the client-ip. Be sure to specify the correct virtual router.

```
configure radius mgmt-access primary server <SERVER_IP> 1815 client-ip <CLIENT_IP>
vr <VR>
```

Configure the RADIUS shared-secret

```
configure radius mgmt-access primary shared-secret <SHARED_SECRET>
```

Enable RADIUS for management access

```
enable radius mgmt-access
```

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.

---

**H3C**

**S5120 Switch series**

PacketFence supports these switches with the following technologies:

- 802.1X (with or without VoIP)
- 802.1X with MAC Authentication fallback (with or without VoIP)
- MAC Authentication (with or without VoIP)

**802.1X**

RADIUS scheme creation:
radius scheme packetfence
primary authentication 192.168.1.5 1812 key useStrongerSecret
primary accounting 192.168.1.5 1813 key useStrongerSecret
user-name-format without-domain

ISP-Domain creation:

domain packetfence
authentication default radius-scheme packetfence
authentication lan-access radius-scheme packetfence
authorization lan-access radius-scheme packetfence

SNMP settings:

snmp-agent
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info version v2c

Global configuration:

port-security enable
dot1x authentication-method eap

Global configuration (with VoIP):

Add the following to the previous global configuration.

undo voice vlan security enable
lldp compliance cdp

Interfaces configuration:

port link-type hybrid
port hybrid vlan 5 untagged
port hybrid pvid vlan 5
mac-vlan enable
stp edged-port enable
port-security max-mac-count 1
port-security port-mode userlogin-secure
port-security intrusion-mode blockmac
dot1x re-authenticate
dot1x max-user 1
dot1x guest-vlan 5
undo dot1x handshake
dot1x mandatory-domain packetfence
undo dot1x multicast-trigger

Interfaces configuration (with VoIP):
Add the following to the previous interfaces configuration.

```plaintext
port hybrid vlan 100 tagged
undo voice vlan mode auto
voice vlan 100 enable
lldp compliance admin-status cdp txrx
port-security max-mac-count 3
dot1x max-user 2
```

### 802.1X with MAC Authentication fallback

Since using MAC Authentication as a fallback of 802.1X, use the previous 802.1X configuration and add the followings.

This configuration is the same with or without VoIP.

**Global configuration:**

```plaintext
mac-authentication domain packetfence
```

**Interfaces configuration:**

```plaintext
mac-authentication guest-vlan 5
port-security port-mode userlogin-secure-or-mac
```

### MAC Authentication

**RADIUS scheme creation:**

```plaintext
radius scheme packetfence
primary authentication 192.168.1.5 1812 key useStrongerSecret
primary accounting 192.168.1.5 1813 key useStrongerSecret
user-name-format without-domain
```

**ISP-Domain creation:**

```plaintext
domain packetfence
authentication default radius-scheme packetfence
authentication lan-access radius-scheme packetfence
authorization lan-access radius-scheme packetfence
```

**SNMP settings:**

```plaintext
snmp-agent
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info version v2c
```

**Global configuration:**
port-security enable
mac-authentication domain packetfence

Global configuration (with VoIP):
Add the following to the previous global configuration.
undo voice vlan security enable
lldp compliance cdp

Interfaces configuration:
port link-type hybrid
port hybrid vlan 5 untagged
port hybrid pvid vlan 5
mac-vlan enable
stp edged-port enable
mac-authentication guest-vlan 5
port-security max-mac-count 1
port-security port-mode mac-authentication
port-security intrusion-mode blockmac

Interfaces configuration (with VoIP):
Add the following to the previous interfaces configuration.
port hybrid vlan 100 tagged
undo voice vlan mode auto
voice vlan 100 enable
lldp compliance admin-status cdp txrx
port-security max-mac-count 3

HP

HPE 1910 Serie

The HP 1910 Serie is based on the 3Com OS and most of the configuration will be done from the GUI.

VLAN creation: * go to Network, VLAN, * click on the Create tab * create the VLANs

Configure PacketFence as a RADIUS server: * go to Authentication, RADIUS * click on the RADIUS Server tab * from Server Type, select Authentication Server * from Primary Server, give the PacketFence IP address * click Apply

Then: * click on the RADIUS Setup tab * check the box Authentication Server Shared Key * give the shared key * from Username Format, select without-domain * click Apply

Create a new authentication domain: * go to Authentication, AAA, * click on the Domain Setup tab,
Warning
We will need to create a specific authentication domain and not making it as the default domain.

Configure the 802.1X and authentication method: * go to Authentication * click on the 802.1X tab * check the Enable 802.1X box * from Authentication Method, select EAP

Configure the authentication domain:
INFO: Even limited, there is a command line access.

- connect to the switch using ss,
- type the command:
  ```
  _cmdline-mode on
  ```
- password is: 512900
- Type the commands:
  ```
  System-view
  Mac-authentication domain YOUR_DOMAIN_NAME
  Mac-authentication user-name-format mac-address with-hyphen
  ```
- change the YOUR_DOMAIN_NAME with the one from your environment
- do not close your terminal, we will come back to this later
- from the GUI, go to Authentication, 802.1X
- from Port, select the port your are connected to. GigabitEthernet X/X/X
- from Port Control, select MAC Based
- from Max Number of Users, give 2
- check the box Enable Re-Authentication
- click on Apply

Enable the MAC Authentication in SSH, as well: * back on the SSH terminal * type the following command:
  ```
  Mac-authentication interface gX/X/X
  ```
- modify the interface name for your environment

The configuration is done.

E4800G and E5500G Switch series
These are re-branded 3Com switches, see under the 3Com section for their documentation.
Chapter 5

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:

```plaintext
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

**CLI authentication**

You can use PacketFence for RADIUS CLI authentication on the 2500 Series.

Global config settings

```plaintext
radius-server host 192.168.1.5 key useStrongerSecret
aaa authentication ssh login radius local
aaa authentication telnet login radius local
```

Next, make sure you configure the switch in PacketFence accordingly as well as the proper administrative access. Refer to the Administration Guide for more details.

**2600 Series and 3400cl Series**

**Port-Security**

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

```plaintext
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

**MAC Authentication (Firmware > 11.72)**

In order to enable RADIUS mac authentication on the ports, you first need to join the ports to either the registration or the mac detection vlan (as a security measure).

Next, define the RADIUS server host:

```
radius-server host 192.168.1.5 key useStrongerSecret
```

Next, we create a server-group that points to the PacketFence server,

```
aaa server-group radius "packetfence" host 192.168.1.5
```
Configure the AAA authentication for MAC authentication to use the right server-group:

```bash
aaa authentication mac-based chap-radius server-group "packetfence"
```

Optionally, you can configure the SSH and telnet authentication to point to PacketFence (make sure you also follow instructions in the Administration Guide to activate the CLI access):

```bash
aaa authentication login privilege-mode

aaa authentication ssh login radius server-group packetfence local
aaa authentication telnet login radius server-group packetfence local
```

Finally, enable MAC authentication on all necessary ports:

```bash
aaa port-access mac-based 1-24
```

Don't forget to permit address moves and the reauth period. x represents the port index:

```bash
aaa port-access mac-based x addr-moves
aaa port-access mac-based x reauth-period 14400
```

(Thanks to Jean-Francois Laporte for this contribution)

### 2610

#### 802.1X

Define the RADIUS server host:

```bash
radius-server host 192.168.1.5 key "useStrongerSecret"
radius-server host 192.168.1.5 acct-port 1813 key "useStrongerSecret"
```

Define the SNMP configuration:

```bash
snmp-server host 192.168.1.5 community "public" informs trap-level not-info
no snmp-server enable traps link-change C1
```

Configure the server-group:

```bash
aaa server-group radius "packetfence" host 192.168.1.5
```

Configure authentication:

```bash
aaa authentication port-access eap-radius server-group "packetfence"
aaa authentication mac-based chap-radius server-group "packetfence"
```

Configure the port-security:
Chapter 5

```
port-security C1 learn-mode port-access action send-alarm
```

Configuration of the port:

```
aaa port-access authenticator C1
aaa port-access authenticator C1 client-limit 1
aaa port-access authenticator active
aaa port-access mac-based C1
aaa port-access mac-based C1 addr-moves
aaa port-access mac-based C1 reauth-period 14400
aaa port-access C1 controlled-direction in
```

(Thanks to Denis Bonnenfant for this contribution)

## 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

Downloadable ACLs

HP and Aruba switches running the ArubaOS-Switch operating system (previously called ProVision) support dynamic RADIUS-assigned ACLs. It requires RADIUS authentication using the 802.1X, Web authentication or MAC authentication available on the switch. You can define ACLs in PacketFence so that they can be automatically applied on the ports of the switches based on the role assigned. We have tested it successfully on the Aruba 2930M and 3810 series on version 16.05.0004.

To use this feature, first configure RADIUS and the authentication method on your switch. Next, in the PacketFence web admin interface, go to Configuration → Policies and Access Control → Switches. Click on the switch you want, then on the Roles tab, and check Role by access list. Now you are able to add ACLs for each role.

Configure RADIUS operation on the switch:

radius-server host <ipv4-address> key <key-string>

Configure RADIUS network accounting on the switch (optional).

aaa accounting network <start-stop|stop-only> radius

You can also view ACL counter hits using either of the following commands:

show access-list radius <port-list>
show port-access <authenticator|mac-based|web-based> <port-list> clients detailed
Configure an authentication method. Options include 802.1X, web-based authentication, and MAC authentication. You can configure 802.1X, web-based authentication, and/or MAC authentication to operate simultaneously on the same ports.

- **802.1X Option:**
  ```
  aaa port-access authenticator <port-list>
  aaa authentication port-access chap-radius
  aaa port-access authenticator active
  ```

- **MAC Authentication Option:**
  ```
  aaa port-access mac-based <port-list>
  ```

- **Web Authentication Option:**
  ```
  aaa port-access web-based <port-list>
  ```

This command configures web-based authentication on the switch and activates this feature on the specified ports.

For example, if you want the users that are in the registration VLAN to only use HTTP, HTTPS, DNS and DHCP you can configure this ACL in the registration role.

![Switch 172.21.2.3](image)

Now, your normal users are placed in the default role and your guests in the guest role.

The default role uses the network 192.168.5.0/24 and guest uses the network 192.168.10.0/24.
You can prevent communications between both networks using these access lists.

Switch configuration

Switch 172.21.2.3

- **default**
  - deny in tcp from any to 192.168.10.0/24
  - permit in tcp from any to any

- **guest**
  - deny in tcp from any to 192.168.5.0/24
  - permit in tcp from any to any

- **gaming**
- **voice**

You could also only prevent your guest users from using shared directories.

Switch configuration

Switch 172.21.2.3

- **default**
- **guest**
  - deny in tcp from any to any 445
  - deny in tcp from any to any 139
  - permit in tcp from any to any

- **gaming**
- **voice**
You could also restrict your users to use only your DNS server where 192.168.5.2 is your DNS server.

Huawei

PacketFence supports the S5710 switch from Huawei.
Basic configuration

```text
l2protocol-tunnel user-defined-protocol 802.1X protocol-mac 0180-c200-0003 group-mac 0100-0000-0002
domain pf

dot1x enable
dot1x dhcp-trigger

radius-server template packetfence
  radius-server shared-key cipher <yourSecret>
  radius-server authentication 192.168.1.5 1812
  radius-server accounting 192.168.1.5 1813
  radius-server retransmit 2
  radius-server authorization 192.168.1.5 shared-key cipher <yourSecret>

aaa
  authentication-scheme abc
  authentication-mode radius
  accounting-scheme abc
  accounting-mode radius
domain pf
  authentication-scheme abc
  accounting-scheme abc
  radius-server packetfence

snmp-agent
  snmp-agent local-engineid 800007DB0304F9389D2360
  snmp-agent community write cipher <privateKey>
  snmp-agent sys-info version v2c v3
```

MAC authentication

```text
interface GigabitEthernet0/0/8
dot1x mac-bypass mac-auth-first
dot1x mac-bypass
dot1x max-user 1
dot1x reauthenticate
dot1x authentication-method eap
```

802.1X

```text
interface GigabitEthernet0/0/8
dot1x mac-bypass
dot1x max-user 1
dot1x reauthenticate
dot1x authentication-method eap
```
IBM

RackSwitch G8052

PacketFence supports only 802.1X authentication. It has been tested on version 7.9.11.0.

RADIUS configuration

```
RS G8052(config)# radius-server primary-host 192.168.1.5
RS G8052(config)# radius-server enable
RS G8052(config)# radius-server primary-host 192.168.1.5 key useStrongerSecret
```

802.1X (dot1x) configuration

```
RS G8052(config)# dot1x enable
```

SNMP configuration

```
RS G8052(config)# snmp-server read-community packetfence
RS G8052(config)# snmp-server write-community packetfence
```

Port configuration

```
RS G8052(config)# configure terminal
RS G8052(config)# interface port 1
RS G8052(config-if)# dot1x mode auto
RS G8052(config-if)# dot1x quiet-time 2
RS G8052(config-if)# dot1x server-timeout 3
RS G8052(config-if)# dot1x re-authenticate
RS G8052(config-if)# dot1x re-authentication-interval 10800
RS G8052(config-if)# dot1x vlan-assign
RS G8052(config-if)# end
```

PacketFence configuration

In order to configure the IBM RackSwitch G8052 switch module, go in the PacketFence administration interface under **Configuration→Switches→Add switch**

Definition:
Chapter 5

IP: This will be the IP of the IBM StackSwitch G8052 switch on the management network
Description: IBM StackSwitch G8052
Type: IBM RackSwitch G8052
Mode: Production
Deauthentication: SNMP
Dynamic Uplinks: Checked

Roles:

Role by VLAN ID: checked
registration VLAN: 2
isolation VLAN: 3
default: 10

Radius:

Secret Passphrase: useStrongerSecret

Snmp:

SNMP Version: 2c
SNMP Read Community: packetfence
SNMP Write Community: packetfence

Click Save to add the switch

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 in MAC Authentication (Juniper’s MAC RADIUS) mode and 802.1X. PacketFence supports VoIP on the EX2200 (JUNOS 12.6) and EX4200 (JUNOS 13.2)
# 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;
        }
      }
    }
  }
}

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;
  }
}

ethernet-switching-options {
  secure-access-port {
    interface access-ports {
      mac-limit 1 action drop;
    }
  }
}

snmp {
  name "EX 4200";
  description juniper;
}
Change the `interface-range` statement to reflect the ports you want to secure with PacketFence.

**VoIP configuration**

```plaintext
# load replace terminal
[Type ^D at a new line to end input]
protocols{
    lldp {
        advertisement-interval 5;
        transmit-delay 1;
        ptopo-configuration-trap-interval 1;
        lldp-configuration-notification-interval 1;
        interface all;
    }
    lldp-med {
        interface all;
    }
}

ethernet-switching-options {
    secure-access-port {
        interface access-ports {
            mac-limit 2 action drop;
        }
    }
    voip {
        interface access-ports {
            vlan voice;
            forwarding-class voice;
        }
    }
}

vlans {
    voice {
        vlan-id 3;
    }
}

Ctrl-D
# commit comment "packetfenced VoIP"
```
802.1X configuration

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

Ctrl-D

`# commit comment "packetfenced dot1x"`

MAC Authentication configuration

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

Ctrl-D

`# commit comment "packetfenced mac auth"`

Configuration for MAC authentication floating devices

To support floating devices on a Juniper switch you need to configure the `flap-on-disconnect` option on each interface individually and remove it from the access-ports group.
# load replace terminal
[Type ^D at a new line to end input]
protocols {
    dot1x {
        authenticator {
            authentication-profile-name packetfence;
            interface {
                ge-0/0/1.0 {
                    mac-radius{
                        flap-on-disconnect;
                    }
                }
                ge-0/0/2.0 {
                    mac-radius{
                        flap-on-disconnect;
                    }
                }
                .......
            }
            access-ports {
                supplicant multiple;
                mac-radius {
                    restrict;
                }
            }
        }
    }
}
Ctrl-D
# commit comment "configured for floating devices"

Note

**flap-on-disconnect** option takes effect only when the **restrict** option is also set.

---

**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 necessaries 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 necessaries 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

The "web-managed smart switch" models GS108Tv2/GS110/GS110TP are supported with Link up/down traps only.

Higher-end "fully managed" switches including FSM726v1 are supported in Port Security mode.
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 (i.e. 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!

GS108Tv2 / GS110T / GS110TP

PacketFence supports certain lower-end Netgear switches in Link Up/Link Down traps. These “web-managed” switches have no command-line interface and only a subset of the port security and 802.1X functionality needed to interoperate with PacketFence in these more advanced modes. There is no way to send a trap upon port security violation, and there is only pure 802.1X, no MAC Address Bypass.

Switch Configuration

It can be difficult to find the advanced features in the web GUI. We recommend using the GUI “Maintenance” tab to Upload the configuration to a file, and then edit it there.

Hints on file upload/download:

From the File Type menu, choose Text Configuration.

If you’re uploading to the TFTP root directory, leave Path blank.

At the top of the config file, you need:
Chapter 5

vlan database
vlan 1,2,3,4,5
vlan name 1 "Normal"
vlan name 2 "Registration"
vlan name 3 "Isolation"
vlan name 4 "MAC Detection"
vlan name 5 "Guest"
exit

In the same section as "users passwd", you need to specify your PacketFence server’s management address:

snmptrap useStrongerSecret ipaddr 192.168.1.5

In the same section as the "voip oui" lines, you need to allow your SNMP server:

snmp-server community "public"
snmp-server community rw useStrongerSecret
snmp-server community ipaddr 192.168.1.5 public
snmp-server community ipmask 255.255.255.0 public
snmp-server community ipaddr 192.168.1.5 useStrongerSecret
snmp-server community ipmask 255.255.255.0 useStrongerSecret
no voip vlan

You should use port 1 as the uplink. If you connect port 1 of a GS108Tv2 switch into a Power over Ethernet switch, then the GS108Tv2 does not need AC power. If you bought GS110T(P) switches, presumably it’s for the SFP uplink option. You’ll want to configure both port 1 and the SFP ports 9-10 as trunks:

interface 0/1
no snmp trap link-status
ip dhcp filtering trust
vlan pvid 1
vlan ingressfilter
vlan participation include 1,2,3,4,5
vlan tagging 2,3,4,5
no auto-voip
exit

Each user-facing, PacketFence-managed port should be configured like:

interface 0/2
vlan pvid 4
vlan ingressfilter
vlan participation include 4
no auto-voip
exit

M Series

PacketFence supports the Netgear M series in wired MAC authentication without VoIP.
Switch configuration

---

radius server host auth 192.168.1.5 radius server key auth 192.168.1.5 (then press enter and input your secret) radius server primary 192.168.1.5 radius server host acct 192.168.1.5 radius server key acct 192.168.1.5 (then press enter and input your secret)

aaa session-id unique dot1x system-auth-control aaa authentication dot1x default radius authorization network radius radius accounting mode

---

On your uplinks

---

dot1x port-control force-authorized

---

On your interfaces

---

interface 0/x dot1x port-control mac-based dot1x timeout guest-vlan-period 1 dot1x mac-auth-bypass exit

---

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-addrs
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:
Chapter 5

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Trunk</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>Enabled</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Pica8

PacketFence supports Pica8 switches without VoIP using CoA to:

- bounce-host-port
- reauthenticate-host

Notes

- SNMP is not supported yet
- Port Security is not supported

For interfaces with MAC Authentication, perform the following:

```
set interface gigabit-ethernet ge-1/1/25 family ethernet-switching port-mode trunk
set protocols dot1x interface ge-1/1/25 auth-mode mac-radius
set protocols dot1x interface ge-1/1/25 dynamic-vlan-enable true
set protocols dot1x traceoptions interface ge-1/1/25 flag all disable false
```

For interfaces with 802.1X, perform:

```
set interface gigabit-ethernet ge-1/1/4 family ethernet-switching port-mode trunk
set protocols dot1x interface ge-1/1/4 auth-mode dot1x
set protocols dot1x interface ge-1/1/4 dynamic-vlan-enable true
set protocols dot1x traceoptions interface ge-1/1/4 flag all disable false
```

Global configuration:
set protocols dot1x aaa radius nas-ip 10.10.51.169
set protocols dot1x aaa radius authentication server-ip 192.168.1.5 shared-key
useStrongerSecret
set protocols dot1x aaa radius dynamic-author client 192.168.1.5 shared-key
useStrongerSecret
set protocols dot1x traceoptions interface ge-1/1/4 flag all disable false
set protocols dot1x traceoptions flag radius disable false
set vlans vlan-id 10
set vlans vlan-id 20
set vlans vlan-id 30
commit

- 10.10.51.169 is the switch IP
- For interfaces where auth-mode is unknown, use the following command set protocols dot1x interface ge-1/1/12 auth-mode dot1x-mac-radius This allows the switch to first try 802.1X and if there is no response from the client then fallback to MAC Authentication.
- Create VLAN(s) on the switch as per your requirements
- Please note that traceoptions are only for debugging

**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

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

On each interface:

```bash
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

Ubiquiti

EdgeSwitch

PacketFence supports the EdgeSwitch with the following techniques:

- 802.1X with MAC Authentication fallback
- 802.1X with MAC Authentication fallback with VoIP

802.1X with MAC Authentication fallback

We assume that the switch ip is 192.168.1.254

First on the uplink add this configuration:

```
dot1x port-control force-authorized
vlan participation include 1,2,3,4,5,100
vlan tagging 2,3,4,5,100
```

Global config settings:

```
vlan database
vlan 1
vlan 2
vlan 3
vlan 4
vlan 5
vlan 100
exit
```

```
configure
dot1x system-auth-control
aaa authentication dot1x default radius
authorization network radius
dot1x dynamic-vlan enable
radius accounting mode
radius server host auth "192.168.1.5" name "PacketFence"
radius server key auth "192.168.1.5"
```

Enter secret (64 characters max): useStrongerSecret
Chapter 5

radius server primary "192.168.1.5"
no radius server msgauth "192.168.1.5"
radius server attribute 4 192.168.1.254

radius server attribute 32 "EdgeSwitch"
radius server host acct "192.168.1.5" name PacketFence-ACCT
radius server key acct "192.168.1.5"

Enter secret (64 characters max): useStrongerSecret

snmp-server community public ro
snmp-server community private rw
exit

On each interface (not uplink)

dot1x port-control mac-based
dot1x re-authentication
dot1x timeout reauth-period 1800
dot1x timeout supp-timeout 10
dot1x timeout guest-vlan-period 3
dot1x timeout server-timeout 1800
dot1x mac-auth-bypass
dot1x unauthenticated-vlan 4
vlan participation include 1,2,3,4,5,100
exit

802.1X with MAC Authentication fallback with VoIP

We assume that the switch ip is 192.168.1.254

First on the uplink add this configuration:

dot1x port-control force-authorized
vlan participation include 1,2,3,4,5,100
vlan tagging 2,3,4,5,100

Global config settings:

vlan database
vlan 1
vlan 2
vlan 3
vlan 4
vlan 5
vlan 100
exit
configure
dot1x system-auth-control
aaa authentication dot1x default radius
authorization network radius
dot1x dynamic-vlan enable
voice vlan 100
radius accounting mode
radius server host auth "192.168.1.5" name "PacketFence"
radius server key auth "192.168.1.5"
Enter secret (64 characters max): useStrongerSecret

radius server primary "192.168.1.5"
no radius server msgauth "192.168.1.5"
radius server attribute 4 192.168.1.254

radius server attribute 32 "EdgeSwitch"
radius server host acct "192.168.1.5" name PacketFence-ACCT
radius server key acct "192.168.1.5"
Enter secret (64 characters max): useStrongerSecret

snmp-server community public ro
snmp-server community private rw
exit

On each interface (not uplink)

dot1x port-control mac-based
dot1x re-authentication
dot1x timeout reauth-period 1800
dot1x timeout supp-timeout 10
dot1x timeout guest-vlan-period 3
dot1x timeout server-timeout 1800
dot1x mac-auth-bypass
dot1x unauthenticated-vlan 4
vlan participation include 1,2,3,4,5,100
voice vlan 100
auto-voip protocol-based
lldp transmit
lldp receive
lldp transmit-tlv port-desc
lldp transmit-tlv sys-name
lldp transmit-tlv sys-desc
lldp transmit-tlv sys-cap
lldp transmit-mgmt
lldp notification
lldp med
lldp med confignotification
exit
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
- 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.

\textsuperscript{1}Be careful to change the secret key to a much stronger one. A 16 character random secret with digits, upper case and lower case characters is recommended.
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 pfdhclistener 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 Networks**

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

**MAC Authentication and 802.1X Configuration**

**Assumptions**

- the network architecture is in order to give access to the Aerohive Access Point, and has access to Internet
- the VLANs are defined for registration, isolation and management networks
- from this documentation, we will assume that the VLANs tags are define like following:
  - PacketFence Management VLAN: 1 IP address: 192.168.1.5
  - registration VLAN ID 2, subnet 192.168.2.0/24
  - isolation VLAN ID 3, subnet 192.168.3.0/24
  - production VLAN ID 10, subnet 172.16.1.0/24
- the VLANs are spanned in the switches and switching L2 equipments, from the *Production Network* to the PacketFence server(s)
• the VLANs are allowed in the trunks
• Aerohive Access Point is loaded with HiveOS with version 6 or later
• HiveManager with version 6 or later
• Wireless AP: 172.16.1.1
• RADIUS Secret: useStrongerSecret

Configure the Aerohive APs and SSID

Logon to your HiveManager interface:

• for this example, we assume that we are on the Cloud MyHive.aerohive.com solution
• from HiveManager, click on your HiveManagerOnline Instances VHM-XXXXXX
• from Network Configuration / 1-Choose Network Policy, click on New
• give a name to your Policy, and click Create
• from 2-Configure Interfaces and User Access, SSID, click on Choose and click on New
• give a SSID Profile Name, SSID Name

For an open (no encryption) SSID using MAC-based authentication:

• click on New
  • SSID Access Security: Open
  • check the box Enable MAC authentication
  • click on Save
For a secure SSID using 802.1X:

- click on New
  - SSID Access Security: **WPA/WPA2 802.1X (Enterprise)**
  - Key Management: **WPA2-(WPA2 enterprise)-802.1X**
  - Encryption method: **CCMP (AES)**

- click on Save
- from SSID, be sure to have selected both SSIDs previously created, and click OK

Add the RADIUS parameters created before:

- under Authentication click on **<RADIUS Setting>**, and click on New
- from RADIUS Name, give the name of the PaketFence server, for example
from Add a New RADIUS Server, in IP Adresse/Domain Name, put the PacketFence Server IP
hive the Shared Secret (useStrongerSecret) and Confirm it
and Click on Apply

deploy the Optionnal Setting(not supported by RADIUS Proxy) section and check the Permit Dynamic Change of Authorization Message (RFC 3576)
click on Save
• next to your SSID Name Click on the <RADIUS Setting>, Click OK

We will create the default VLAN to be assign by the AP, when a new endpoint get in the SSID:

• Under User Profile, Click on Add/Remove, and Click on New, in the Default section
  • You will need to create one User Profile for each VLANs used, for us, we will create 3 Users Profiles, Registration, Isolation and Production
  • from name, give the name of a rule to manage the VLANs with PacketFence (Registration ; Isolation ; Production)
  • from Attribute Name, give the VLAN ID of the VLAN
  • from Default VLAN, Click on the (+) (New)
  • as a VLAN ID, give the VLAN ID earlier Registration(2) , Isolation(3) or Production(10)
  • click on Save and click on Save again on the Configure interfaces and User Access

Create and add the other VLANs:

• Follow the same procedure to create the others VLANs

Once done with the VLANs configuration:

• From the Choose User Profiles, select the Default tab and click on you Registration VLAN tag
• From the Authentication tab, select the Isolation and the Production VLANs tag
• Click on Save

For our example, here is what it looks like, with two SSIDs
Then, click on Continue, on top right of the page.

Push your configuration to your AP:

- from Configure and Update Devices, check your AP in Device to Update
- click on Update
- select Update Devices
- from HiveOS Number of devices running earlier versions of HiveOS, select Upgrade these devices to the latest version of HiveOS
- click on Update
- wait until the date and time appears under Update Status

**Note**

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. The other way to support Roaming is to enable SNMP trap in the Aerohive configuration to PacketFence server. PacketFence will recognize the ahConnectionChangeEvent and will change the location of the node in his base.

**Configure PacketFence**

We will now need to create a new switch in PacketFence to be able to manage the endpoints behind the Aerohive APs.

Logon to your PacketFence interface:

- from Configuration / Policies and Access Control / Switches /
- on the line where there is the default, on the right, Click on CLONE
In Definition:

- **IP Address/MAC Address/Range (CIDR)**, give the network address of your Production network; For us, it will be **172.16.1.1**
- **Description**, give a description so you can quickly see what it is about
- from the **Type** list, select **Aerohive AP**
- from **Mode** select **Production**
- **Switch Group** by default set to **None**
- **Deauthentication Method** set to **RADIUS**
- click **SAVE**
Chapter 6

From Role:

- set all VLAN ID for each roles

New Switch

<table>
<thead>
<tr>
<th>Role by VLAN ID</th>
<th>registration 2</th>
<th>isolation 3</th>
<th>macDetection 4</th>
<th>inline 6</th>
<th>default 10</th>
<th>guest</th>
<th>gaming</th>
<th>voice 5</th>
<th>REJECT -1</th>
</tr>
</thead>
</table>

INVALIDATE CACHE  CLOSE  SAVE

CLOSE  SAVE
From RADIUS:

- modify the secret passphrase previously sets in the Aerohive HiveManager
- click on SAVE

This ends the PacketFence configuration.

Web Auth (External Captive Portal) Configuration

In this section we will describe the WebAuth configuration using PacketFence as an external captive portal.

Assumptions

In this part, it is recommended that the default VLAN must be the native VLAN. This way, the AP and the others network equipments will be able to manage VLANs.

You already have a Network Policy and at least one Access Point configured.

Configure the external captive portal

Create a new Captive Portal Profile:

- from the HiveManager, go to CONFIGURATION → ADVANCED CONFIGURATION → AUTHENTICATION → Captive Web Portals
- click on New
- give it a name
- Registration Type must be External Authentication
- click on Captive Web Portal Login Page Settings to deploy the configuration window
- Login URL must be http://192.168.1.5/AeroHIVE::AP
- Password Encryption : No Encryption (Plaintext Password)
- click on Save
Create a SSID to enable Captive Portal functionality:

- from the HiveManager, go to **CONFIGURATION → SSIDS**
- click on the New button
- give your Profile and SSID a name
- from **SSID Access Security**, check **Enable Captive Web Portal**
- before clicking on the button **Save** you should have something like this:
Configure and broadcast your SSID:

- from the HiveManager, go to **CONFIGURATION → NETWORK POLICIES**
- choose Network Policy and click OK, you should see this:
under Authentication click on <Captive Web Portal> and select the captive portal previously configured

once the <RADIUS Settings> appears under the captive portal, click on it

on that new window Choose RADIUS click New

give it a description and a name

under RADIUS Servers click New

Click on Apply

click on Optional Settings (not supported by RADIUS Proxy) and check Permit Dynamic Change of Authorization Messages (RFC 3576)

Click on the Save button
Configure the User profile:

- under User Profile, click on Add/Remove and click on New

- enter the profile name, the VLAN ID and create the default VLAN as the same as the attribute number
• create a new default VLAN, click on the + button

![VLANs > New](image)

• click the Save button

• make sure the new user profile name is selected and then Save

Push the configuration to the Access Point: * click on Continue * select the AP and click Update
- Update Devices * under Configuration: select Perform a complete configuration update for all selected devices * under HiveOS: select Don't upgrade * click on Update * wait until the AP is back online

**Configure PacketFence**

Configure the Production interface to send the Portal:

• go to Configuration → Network Configuration → Interfaces
• under Logical Name, click on your interface name,
• Additional listening daemon(s), Add portal
• click on SAVE
MAC Authentication/802.1X and Web Auth Configuration

In this case we want to be able to enable a MAC Authentication/802.1X and Web Auth SSID on the same wireless equipment. By default it’s not possible to provide a MAC Authentication/802.1X SSID and a Web Auth SSID with the same switch configuration, but by using the Switch Filters it will be possible to do it.

We will assume that we have an up and running SSID (YourSecuredSSID) already configured with Mac Authentication/802.1X:

- from this documentation, we will assume that the VLANs tags are defined like following:
  - PacketFence Management VLAN: 1 IP address: 192.168.1.5
  - registration VLAN ID 2, subnet 192.168.2.0/24
  - isolation VLAN ID 3, subnet 192.168.3.0/24
• production VLAN ID 10, subnet 172.16.1.0/24

Our SSID will be named YourOpenSSID, assuming that we want to provide a public Internet hotspot for example.

**Add a New SSID**

You should create a new SSID, as explained before, secured or open, as you need.

**Configure Filters in PacketFence**

Logon to your PacketFence server:

• Go to *Configuration → Advanced Access Configuration → Filter Engines*
• From the tab *Switch filters*,
• Go to the bottom of the configuration file and set the following section.

```plaintext
[SSID]
filter = ssid
operator = is
value = YourOpenSSID

[1:SSID]
scope = radius_authorize
param1 = ExternalPortalEnforcement => Y
param2 = VlanMap => N
```

Click on **SAVE**.

**Note**

The default configuration in the *Switch filters* for *ExternalPortalEnforcement* is set to **N**

**Advanced Topics**

**Roles (User Profiles)**

PacketFence supports user profiles on the Aerohive equipment. 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. For example:

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

And in the Aerohive configuration, you have:

```plaintext
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.

In version 6 or later of the HiveOS, we do return VLAN ID matching the number that the User Profile has. Create your User Profile in the HiveManager as usual, assign the matching VLAN, and in PacketFence configuration add the wanted VLAN ID in the section Roles by VLAN.

**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
```

Anyfi Networks

This section will discuss about the configuration of your Anyfi Gateway and Controller in order to use it with our configured PacketFence environment.

**Deploy Anyfi Controller and Gateway**

First thing, you will need to deploy the Anyfi Gateway and Controller on your network and configure basic connectivity between both of them.

When installing the Anyfi Gateway, have one interface in trunk mode for the packet bridge. In this example it will be `eth2` which is the last card on the machine.

**Anyfi Gateway Basic Configuration**

Connect to the gateway using SSH and enter configuration mode. Now you need to add the configuration for `br0` which will link the access point traffic to your network.
In this example **eth1** will be the management interface of the Anyfi Gateway and **eth2** will be the interface that will contain the outbound WiFi traffic.

```plaintext
interfaces {
    ethernet eth1 {
        address <your management ip address>/<mask>
        duplex auto
        smp_affinity auto
        speed auto
    }
    ethernet eth2 {
        bridge-group {
            bridge br0
        }
        duplex auto
        smp_affinity auto
        speed auto
    }
}
```

**Open SSID Configuration**

Still in configuration mode, configure the RADIUS server and SSID security.
Secure SSID Configuration

Still in configuration mode, configure the Anyfi Gateway to broadcast a WPA2 enterprise SSID.

```yaml
service {
  anyfi {
    gateway secure-gw {
      authentication {
        eap {
          radius-server <Management IP of PacketFence> {
            port 1812
            secret useStrongerSecret
          }
        }
      }
      bridge br0
      controller <IP or FQDN of the Anyfi Controller>
      isolation
      nas {
        identifier anyfi
        port 3799
      }
      ssid DemoSecure
      wpa2 {
      }
    }
  }
}
```
Deploy Access Point

You will now need to install CarrierWRT on a compatible access point and configure the Anyfi Controller in it. Depending on the access point you’re using, the method to install CarrierWRT will vary. For specifics about the CarrierWRT installation, refer to Anyfi’s documentation. Once this step is done, the SSID should be broadcasted.

Avaya

Wireless Controller

Note

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.

**WIPS**

In order to use the WIPS feature in PacketFence, please follow those simple steps to send the traps to PacketFence.
Chapter 6

First, configure PacketFence to be a trap receiver. Under Configuration > SNMP > Trap Receivers, add an entry for the PF management IP. By default, all traps will be enabled. If you want to disable some, you will need to connect via CLI, and run the `snmp-server trap disable <trapname>` command.

**WebAuth**

First of all you will need to configure a guest VLAN.

![Guest VLAN Configuration](image1)

Next, you will need to configure a RADIUS server.

![RADIUS Server Configuration](image2)

```
aaa authentication-server radius "packetfence"
host 192.168.1.5
key useStrongerSecret
```

Add your RADIUS server to a AAA group, under Security -> Authentication -> Servers -> Server Group:

```
aaa server-group "packetfence"
auth-server "packetfence" position 1
```

Then define the RFC 3576 server, which will allow you to do CoA.
aaa rfc-3576-server "192.168.1.5"
key useStrongerSecret

Next, you will need to create the policy that will redirect users to the PacketFence captive portal when they are not authenticated. Go to **Security -> Authentication -> L3 Authentication -> Captive Portal Authentication Profile.**

<table>
<thead>
<tr>
<th>Default Role</th>
<th>PF-Open-guest-logon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect Guest Role</td>
<td>PF-Open-guest-logon</td>
</tr>
<tr>
<td>Login</td>
<td>True</td>
</tr>
<tr>
<td>Logout popup window</td>
<td>True</td>
</tr>
<tr>
<td>Use HTTP for authentication</td>
<td>False</td>
</tr>
<tr>
<td>Logon wait minimum wait</td>
<td>5 sec</td>
</tr>
<tr>
<td>Logon wait maximum wait</td>
<td>10 sec</td>
</tr>
<tr>
<td>Logon wait CPU utilization threshold</td>
<td>60 %</td>
</tr>
<tr>
<td>Max Authentication failures</td>
<td>0</td>
</tr>
<tr>
<td>Authentication Protocol</td>
<td>PAP</td>
</tr>
<tr>
<td>Login page</td>
<td><a href="https://portal.fqdn/Aruba">https://portal.fqdn/Aruba</a></td>
</tr>
<tr>
<td>Welcome page</td>
<td><a href="https://portal.fqdn/Aruba">https://portal.fqdn/Aruba</a></td>
</tr>
</tbody>
</table>

Adding user vlan in redirection URL
Add a controller interface in the redirection URL
Allow only one active user session

**White List**
- svr-grp-rdssh

**Black List**
- svr-grp-rdssh

Show the acceptable use policy page
User idle timeout
Redirect URL
Bypass Apple Captive Network Assistant
aaa authentication captive-portal "packetfence-externalportal"
default-role auth-guest
redirect-pause 3
no logout-popup-window
login-page https://192.168.1.5/Aruba
switch-ip-in-redirection-url

Now create the policy for the guest access, for example Internet only.

Add the authentication for the Captive Portal Profile via Security -> Authentication -> L3 Authentication -> Captive Portal Authentication Profile -> Server Group:

aaa authentication captive-portal "packetfence-externalportal"
server-group "packetfence"

Adjust the configuration of the AAA profile through Security -> Authentication -> Profiles -> AAA Profiles:

[Image of AAA Profile configuration]

Copyright © 2019 Inverse inc.
aaa profile "packetfence-externalportal"
initial-role packetfence-portal
radius-interim-accounting
radius-accounting "packetfence"
rfc-3576-server "192.168.1.5"

Define a policy to permit the traffic.
First add a destination, Advanced Services -> Stateful Firewall -> Destinations:

netdestination packetfence-portal
host 192.168.1.5

Create an ACL for the redirection, Security -> Firewall Policies:
Source NAT on VLAN

```bash
ip access-list session "packetfence-externalportal"  
alias "user" alias "packetfence-portal" "svc-http" permit queue low  
alias "user" alias "packetfence-portal" "svc-https" permit queue low
```
Enable the "firewall allow-tri-session":

```
firewall allow-tri-session
```

Source NAT per Application

```
ip access-list session "packetfence-externalportal"
alias "user" alias "packetfence-portal" "svc-http" src-nat queue low
alias "user" alias "packetfence-portal" "svc-https" src-nat queue low
```

Now add the newly created policy to the Captive Portal Profile, Security -> User Roles:
user-role "packetfence-portal"
access-list session "packetfence-externalportal" position 1
access-list session "captiveportal" position 2
access-list session "guest-logon-access" position 3
access-list session "block-internal-access" position 4
access-list session "v6-logon-control" position 5
access-list session "captiveportal6" position 6
captive-portal "packetfence-externalportal"

Finally create the SSID and associate the profile to it, Virtual AP profile:

wlan virtual-ap "packetfence-externalportal"
ssid-profile "packetfence-externalportal"
aaa-profile "packetfence"

General AP settings and master-slave controller case.
### Virtual AP > GNet-Guest-vap_prof

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual AP enable</td>
<td>On</td>
</tr>
<tr>
<td>VLAN (Guest VLAN ID)</td>
<td>124</td>
</tr>
<tr>
<td>Forward mode</td>
<td>Tunnel</td>
</tr>
<tr>
<td>Allowed band</td>
<td>All</td>
</tr>
<tr>
<td>Band Steering</td>
<td>Off</td>
</tr>
<tr>
<td>Steering Mode</td>
<td>Prefer-5GHz</td>
</tr>
<tr>
<td>Dynamic Multicast Optimization (DMO)</td>
<td>Off</td>
</tr>
<tr>
<td>Dynamic Multicast Optimization (DMO) Threshold</td>
<td>6</td>
</tr>
<tr>
<td>Drop Broadcast and Multicast</td>
<td>Off</td>
</tr>
<tr>
<td>Convert Broadcast ARP requests to unicast</td>
<td>On</td>
</tr>
<tr>
<td>Authentication Failure Blacklist Time</td>
<td>3600 sec</td>
</tr>
<tr>
<td>Blacklist Time</td>
<td>3600 sec</td>
</tr>
<tr>
<td>Deny inter user traffic</td>
<td>Off</td>
</tr>
<tr>
<td>Deny bmc range</td>
<td>--NONE--</td>
</tr>
<tr>
<td>DoS Prevention</td>
<td>Off</td>
</tr>
<tr>
<td>HA Discovery on-association</td>
<td>On</td>
</tr>
<tr>
<td>Mobile IP</td>
<td>Off</td>
</tr>
<tr>
<td>Preserve Client VLAN</td>
<td>Off</td>
</tr>
<tr>
<td>Remote-AP Operation</td>
<td>Standard</td>
</tr>
<tr>
<td>Station Blacklisting</td>
<td>Off</td>
</tr>
<tr>
<td>Strict Compliance</td>
<td>Off</td>
</tr>
<tr>
<td>VLAN Mobility</td>
<td>Off</td>
</tr>
<tr>
<td>FDB Update on Assoc</td>
<td>Off</td>
</tr>
</tbody>
</table>
### AAA Profile

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial role</td>
<td>PF-Open-guest-logon</td>
</tr>
<tr>
<td>MAC Authentication Default Role</td>
<td>guest</td>
</tr>
<tr>
<td>802.1X Authentication Default Role</td>
<td>guest</td>
</tr>
<tr>
<td>L2 Authentication Fail Through</td>
<td></td>
</tr>
<tr>
<td>User idle timeout</td>
<td>enable seconds</td>
</tr>
<tr>
<td>RADIUS Interim Accounting</td>
<td></td>
</tr>
<tr>
<td>User derivation rules</td>
<td>--NONE--</td>
</tr>
<tr>
<td>Wired to Wireless Roaming</td>
<td></td>
</tr>
<tr>
<td>SIP authentication role</td>
<td>--NONE--</td>
</tr>
<tr>
<td>Device Type Classification</td>
<td></td>
</tr>
<tr>
<td>Enforce DHCP</td>
<td></td>
</tr>
<tr>
<td>MAC Authentication Profile</td>
<td>mac_auth_packetfence</td>
</tr>
<tr>
<td>MAC Authentication Server Group</td>
<td>PacketFence</td>
</tr>
<tr>
<td>802.1X Authentication Profile</td>
<td>PacketFence</td>
</tr>
<tr>
<td>802.1X Authentication Server Group</td>
<td>PacketFence</td>
</tr>
<tr>
<td>RADIUS Accounting Server Group</td>
<td></td>
</tr>
<tr>
<td>XML API server</td>
<td></td>
</tr>
<tr>
<td>RFC 3576 server</td>
<td>PF Cluster IP</td>
</tr>
</tbody>
</table>

### SSID Profile

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name (SSID)</td>
<td>PF-Open</td>
</tr>
</tbody>
</table>

#### 802.11 Security

- **Network Authentication**: 
  - None
  - 802.1x/WEP
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
- **Encryption**: 
  - Open
  - WEP
### SSID Profile

#### Basic
- **SSID enable**: On

#### Advanced
- **ESSID**: `FF-Open`
- **Encryption**:
  - `opensystem`
  - `dynamic-wep`
  - `wpa-tkip`
  - `wpa-psk-tkip`
  - `wpa-psk-aes`
  - `wpa2-aes`
  - `wpa2-psk-tkip`
  - `wpa2-psk-aes`
  - `wpa2-tkip`

#### DTIM Interval
- **Value**: 1 beacon periods

#### 802.11a Basic Rates
- On: 6, 9, 12, 18, 24
- Off: 36, 48, 54

#### 802.11a Transmit Rates
- On: 6, 9, 12, 18, 24
- Off: 36, 48, 54

#### 802.11g Basic Rates
- On: 1, 2, 5, 6, 9, 11
- Off: 12, 18, 24, 36
- Off: 40, 54

#### 802.11g Transmit Rates
- On: 1, 2, 5, 6, 9, 11
- Off: 12, 18, 24, 36
<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Station Ageout Time</td>
<td>1000 sec</td>
</tr>
<tr>
<td>Max Transmit Attempts</td>
<td>8</td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>2333 bytes</td>
</tr>
<tr>
<td>Short Preamble</td>
<td></td>
</tr>
<tr>
<td>Max Associations</td>
<td>64</td>
</tr>
<tr>
<td>Wireless Multimedia (WMM)</td>
<td></td>
</tr>
<tr>
<td>Wireless Multimedia U-APSD (WMM-UAPSD)</td>
<td></td>
</tr>
<tr>
<td>PowerSave</td>
<td></td>
</tr>
<tr>
<td>WMM TSPEC Min Inactivity Interval</td>
<td>0 msec</td>
</tr>
<tr>
<td>Overrides DSCP mappings for WMM clients</td>
<td></td>
</tr>
<tr>
<td>DSCP mapping for WMM voice AC</td>
<td></td>
</tr>
<tr>
<td>DSCP mapping for WMM video AC</td>
<td></td>
</tr>
<tr>
<td>DSCP mapping for WMM best-effort AC</td>
<td></td>
</tr>
<tr>
<td>DSCP mapping for WMM background AC</td>
<td></td>
</tr>
<tr>
<td>Multiple Tx Replay Counters</td>
<td></td>
</tr>
<tr>
<td>Hide SSID</td>
<td></td>
</tr>
<tr>
<td>Deny_Broadcast Probes</td>
<td></td>
</tr>
<tr>
<td>Local Probe Request Threshold (dB)</td>
<td>0</td>
</tr>
<tr>
<td>Disable Probe Retry</td>
<td></td>
</tr>
<tr>
<td>Battery Boost</td>
<td></td>
</tr>
<tr>
<td>WEP Key 1</td>
<td></td>
</tr>
<tr>
<td>WEP Key 2</td>
<td></td>
</tr>
</tbody>
</table>
### High-throughput SSID Profile

**Basic**

- **General**
  - High throughput enable (SSID)
  - 40 MHz channel usage
  - Very High throughput enable (SSID)
  - 80 MHz channel usage (VHT)

- **Transmit Beamforming**
  - VHT - Explicit Transmit Beamforming

---

**Advanced**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP Key 4</td>
<td></td>
</tr>
<tr>
<td>Retype:</td>
<td></td>
</tr>
<tr>
<td>WEP Transmit Key Index</td>
<td>1</td>
</tr>
<tr>
<td>WPA Hexkey</td>
<td></td>
</tr>
<tr>
<td>Retype:</td>
<td></td>
</tr>
<tr>
<td>WPA Passphrase</td>
<td></td>
</tr>
<tr>
<td>Retype:</td>
<td></td>
</tr>
<tr>
<td>Maximum Transmit Failures</td>
<td>0</td>
</tr>
<tr>
<td>BC/MC Rate Optimization</td>
<td></td>
</tr>
<tr>
<td>Rate Optimization for delivering EAPOL frames</td>
<td>✓</td>
</tr>
<tr>
<td>Strict Spectralink Voice Protocol (SVP)</td>
<td></td>
</tr>
<tr>
<td>802.11g Beacon Rate</td>
<td>default</td>
</tr>
<tr>
<td>802.11a Beacon Rate</td>
<td>default</td>
</tr>
<tr>
<td>Multicast Rate</td>
<td>default</td>
</tr>
<tr>
<td>Advertise QBSS Load IE</td>
<td></td>
</tr>
<tr>
<td>Advertise Location Info</td>
<td></td>
</tr>
<tr>
<td>Advertise AP Name</td>
<td></td>
</tr>
<tr>
<td>Enforce user vlan for open stations</td>
<td></td>
</tr>
</tbody>
</table>

---

[Show Reference] [Save As] [Reset]
### High-throughput SSID Profile

**Basic**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>High throughput enable (SSID)</td>
<td>✓</td>
</tr>
<tr>
<td>40 MHz channel usage</td>
<td>✓</td>
</tr>
<tr>
<td>Very High throughput enable (SSID)</td>
<td>✓</td>
</tr>
<tr>
<td>80 MHz channel usage (VHT)</td>
<td>✓</td>
</tr>
<tr>
<td>BA AMSDU Enable</td>
<td>✓</td>
</tr>
<tr>
<td>Temporal Diversity Enable</td>
<td>✓</td>
</tr>
<tr>
<td>Legacy stations</td>
<td>✓</td>
</tr>
<tr>
<td>Low-density Parity Check</td>
<td>✓</td>
</tr>
<tr>
<td>Maximum number of spatial streams usable for STBC reception</td>
<td>1</td>
</tr>
<tr>
<td>Maximum number of spatial streams usable for STBC transmission</td>
<td>1</td>
</tr>
<tr>
<td>MPDU Aggregation</td>
<td>✓</td>
</tr>
<tr>
<td>Max received A-MPDU size</td>
<td>65535</td>
</tr>
<tr>
<td>Max transmitted A-MPDU size</td>
<td>65535</td>
</tr>
<tr>
<td>Min MPDU start spacing</td>
<td>0</td>
</tr>
<tr>
<td>Short guard interval in 20 MHz mode</td>
<td>✓</td>
</tr>
<tr>
<td>Short guard interval in 40 MHz mode</td>
<td>✓</td>
</tr>
<tr>
<td>Short guard interval in 80 MHz mode</td>
<td>✓</td>
</tr>
<tr>
<td>Supported MCS set</td>
<td>0-23</td>
</tr>
<tr>
<td>VHT - Supported MCS map</td>
<td>9, 9, 9, 9</td>
</tr>
<tr>
<td>VHT - Explicit Transmit Beamforming</td>
<td>✓</td>
</tr>
<tr>
<td>VHT - Transmit Beamforming Sounding Interval</td>
<td>25</td>
</tr>
<tr>
<td>Maximum VHT MPDU size</td>
<td>11454</td>
</tr>
</tbody>
</table>

**Advanced**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of MSDUs in an A-MSDU on best-effort AC</td>
<td>2</td>
</tr>
<tr>
<td>Maximum number of MSDUs in an A-MSDU on background AC</td>
<td>2</td>
</tr>
<tr>
<td>Maximum number of MSDUs in an A-MSDU on video AC</td>
<td>2</td>
</tr>
<tr>
<td>Maximum number of MSDUs in an A-MSDU on voice AC</td>
<td>0</td>
</tr>
</tbody>
</table>
Chapter 6

The next step will be to configure the Aruba WiFi controller for WebAuth in PacketFence, add the switch with the model choice Aruba Network.
Check the box External Portal Enforcement, in the Roles section, choose Role by Switch Role, as the registration role, enter your default role: packetfence-portal and choose the policy matching roles, for instance guest: internet-only.

**CLI authentication**

In order to enable CLI login on the Aruba controller via the PacketFence server, you need to point management authentication to the RADIUS server you created while configuring the SSIDs in the previous sections above.

aaa authentication mgmt default-role read-only enable server-group PacketFence

**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"

All Aruba Instant OS

Add your packetfence instance to your configuration:

wlan auth-server packetfence

ip 192.168.1.5
port 1812
acctport 1813
timeout 10
retry-count 5
key useStrongerSecret
nas-ip [Aruba Virtual Controller IP]
rfc3576

Add dynamic vlan rules and mac auth to your ssid profile:

wlan ssid-profile SSID
index 0
  type employee
  essid ESSID
  wpa-passphrase WPA-Passphrase
  opmode wpa2-psk-aes
  max-authentication-failures 0
  vlan 1
  auth-server packetfence
  set-vlan Tunnel-Private-Group-Id contains 1 1
  set-vlan Tunnel-Private-Group-Id contains 4 4
  rf-band all
  captive-portal disable
  mac-authentication
  dtim-period 1
  inactivity-timeout 1000
  broadcast-filter none
  radius-reauth-interval 5
  dmo-channel-utilization-threshold 90

Belair Networks (now Ericsson)

BE20

The Belair Networks BE20s are fairly easy to configure.

Add VLANs

On the BE20 Web Interface, click on Eth-1-1. By default, there will be nothing in there. You need to first create an untagged VLAN (VLAN 0). In order to do that, you need to set the PVID, Reverse PVID, and the VLAN field to 0. Then click add.

Repeat that step for each of your VLANs by entering the proper VLAN ID in the VLAN field.

AAA Servers

Once you have the VLANs setup, you need to add PacketFence into the AAA Server list. Go to System → Radius Servers. Click on Add server, and fill out the proper information.

- Ensure the Enabled checkbox is selected
- IP Address: Insert the IP Address of the PacketFence Management Interface
- Shared Secret: Insert the shared secret for RADIUS communication

When done, click on the Apply button.

Secure SSID

Since the BE20 doesn't support Open SSID with MAC Authentication, we will only describe how to configure a WPA2-Enterprise SSID. First, we will configure the 5GHz antenna.
Click on **Wifi-1-1 → Access SSID Config**. From the **Configuration for SSID** dropdown, select the 1 entry. Modify the fields like the following:

- **SSID**: Put your SSID Name you would like
- **Type**: Broadcast
- **Use Privacy Mode**: WPA2(AES) with EAP/DOT1x
- **RADIUS NAS Identifier**: You can put a string to identify your AP
- **Radius Accounting Enabled**: Checkbox Selected
- **Radius Station ID Delimiter**: dash
- **Radius StationId Append Ssid**: Checkbox Selected
- **RADIUS Server 1**: Select the AAA Server you created earlier

When done click **Apply**. Repeat the same configuration for the 2.4GHz Antenna (Wifi-1-2).

That should conclude the configuration. You can now save the configs to the flash by hitting the **Config Save** button on top of the Interface.

---

**Brocade**

**RF Switches**

See the [Motorola RF Switches](#) documentation.

---

**Cambium**

**cnPilot E410**

**802.1X**

To setup the Cambium cnPilot E410 AP to use 802.1x, first, you need to already have configured the VLANs that will be used in the AP under **Configure → Network**. Make sure that in **Configure → Network → Ethernet Ports**, the port is configured to **Trunk Multiple VLANs**, and the list of VLANs are allowed.

Next, go to **Configure → WLAN**, and click on **Add WLAN**. Give it the desired ID, and enter your SSID, default VLAN, and select **WPA2 Enterprise** for Security.
In the **RADIUS Server** tab, enter the management IP address of PacketFence (VIP in case of a cluster) and the Radius secret for Authentication and Accounting servers.

Check the **Dynamic Authorization** and **Dynamic VLAN** boxes and save.

**MAC Authentication**

To enable MAC authentication in the Cambium E410, go to **Configure → WLAN**, select your WLAN, set the Security to open and click on the tab **Access**.

In the **MAC Authentication** section, select Radius as the policy, and check the box for **Password** to use the MAC address as the password in the Radius request. Click on Save.
Web Authentication

To enable Web Authentication, go to your WLAN in Configure → WLAN, create a new WLAN with open Security, and click on the tab Guest Access to set the following:

- Enable: check the box
- Portal Mode: External Hotspot
- Access Policy: Radius
- Redirect Mode: HTTP
- External Page URL: http://IP ADDRESS OF PACKETFENCE/Cambium
- External Portal Type: Standard
- Success Action: Your preferred action.
- Prefix Query Strings in Redirect URL: check the box
- Redirection URL Query String: check Client IP
- Redirect: check HTTP-only

Click Save.

In the Add Whitelist section, add the IP address or domain name of your PacketFence server, then save.
On PacketFence web admin, in the Switch configuration for your AP, Roles tab, check Role by Web Auth URL box, and enter `http://IP_ADDRESS_OF_PACKETFENCE/Cambium` in the registration field.
Cisco

Aironet 1121, 1130, 1242, 1250, 1600

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 192.168.1.5 auth-port 1812 acct-port 1813 key useStrongerSecret
  aaa group server radius rad_eap
    server 192.168.1.5 auth-port 1812 acct-port 1813
  aaa authentication login eap_methods group rad_eap
  aaa group server radius rad_mac
    server 192.168.1.5 auth-port 1812 acct-port 1813
  aaa authentication login mac_methods group rad_mac

Aironet 1600

CoA and radius:
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
aaa server radius dynamic-author
client 192.168.1.5
server-key 7 useStrongerSecret
port 3799
auth-type all

Aironet (WDS)

To be contributed...

Wireless LAN Controller (WLC) or Wireless Services Module (WiSM)

In this section, we cover the basic configuration of the WiSM for PacketFence using the web interface.

- First, globally define the FreeRADIUS server running on PacketFence (PacketFence's IP) and make sure **Support for RFC 3576** (also called **Support for CoA**) is enabled. When the option is missing from your WLC, it is enabled by default.

- Then we create two SSIDs:
  - PacketFence-Public: non-secure with MAC authentication only
  - PacketFence-Secure: secure with WPA2 Enterprise PEAP/MSCHAPv2
In the secure SSID, make sure 802.1X is enabled and select the appropriate encryption for your needs (recommended: WPA + WPA2)

- No layer 3 security
- We set the IP of the FreeRADIUS server

- VERY IMPORTANT: Allow AAA override (this allows VLAN assignment from RADIUS)

- Edit the non-secure SSID: Enable MAC authentication at level 2

- Nothing at level 3
- We set the IP of the FreeRADIUS server

- VERY IMPORTANT: Allow AAA override (this allows VLAN assignment from RADIUS)

- Finally, in Controller > Interfaces tab, create an interface per VLAN that could be assigned
Warning
When creating interfaces, it’s important to configure DHCP servers. Otherwise, WLC will block DHCP requests.

You are good to go!

Wireless LAN Controller (WLC) Web Auth

In this section, we cover the basic configuration of the WLC Web Auth for PacketFence using the web interface. The idea is to forward the device to the captive portal with an ACL if the device is in an unreg state and allow the device to reach Internet (or the normal network) by changing the ACL once registered. In the unreg state, the WLC will intercept the HTTP traffic and forward the device to the captive portal.

In this sample configuration, the captive portal uses the IP address 172.16.0.250, the administration interface uses the IP address 172.16.0.249 and the WLC uses the IP address 172.16.0.248. The DHCP and DNS servers are not managed by PacketFence (WLC DHCP Server, Production DHCP Server)

- First, globally define the FreeRADIUS server running on PacketFence (PacketFence’s Administration Interface) and make sure Support for RFC 3576 is enabled (if not present it is enabled by default)

- Then we create a SSID:
  - OPEN SSID: non-secure with MAC authentication only
Chapter 6

Wireless Controllers and Access Point Configuration

Copyright © 2019 Inverse inc.
Note

On more recent controllers, the value *Radius NAC* in the NAC State setting will be called *ISE NAC*.

- Then you have to create two ACLs - one to deny all traffic except the required one to hit the portal (*Pre-Auth-For-WebRedirect*) and the other one to allow anything (*Authorize_any*).

- Then the last step is to configure the WLC in PacketFence. Role by Web Auth URL.
Role definition

Switch 172.26.0.248

Role by Web Auth URL

<table>
<thead>
<tr>
<th>Role</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>registration</td>
<td><a href="http://172.16.0.250/Cisco.WLC">http://172.16.0.250/Cisco.WLC</a></td>
</tr>
</tbody>
</table>

Role Mapping by Switch Role

<table>
<thead>
<tr>
<th>Role</th>
<th>Registration</th>
<th>isolation</th>
<th>macDetection</th>
<th>inline</th>
<th>voice</th>
<th>default</th>
<th>guest</th>
<th>gaming</th>
</tr>
</thead>
<tbody>
<tr>
<td>inline</td>
<td>Pre-Auth-For-WebRedirect</td>
<td></td>
<td></td>
<td>inline</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>voice</td>
<td>isolation</td>
<td></td>
<td></td>
<td>voice</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>default</td>
<td>isolation</td>
<td></td>
<td>macDetection</td>
<td>default</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>guest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gaming</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Wireless LAN Controller (WLC) IPSK

In this section, we cover the basic configuration of the WLC IPSK feature. Starting from WLC 8.5 release, Cisco introduces the IPSK feature. Identity PSKs are unique pre-shared keys created for individuals or groups of users on the same SSID.

In this section we will cover the WLC configuration and the PacketFence configuration.

WLC Configuration:

- First, globally define the RADIUS server running on PacketFence (PacketFence's IP) and make sure Support for RFC 3576 (also called Support for CoA) is enabled. When the option is missing from your WLC, it is enabled by default.

- Next, configure a new SSID like in the following screenshots
### Wireless Controllers and Access Point Configuration

#### General
- **WPA2 Policy**: Enabled
- **WPA2 Encryption**: AES, TKIP, CCMP256, GC
- **OSEN Policy**: Disabled

#### Security
- **Authentication Key Management**
  - **802.1X**: Enable
  - **CCKM**: Enable
  - **PSK**: Enable
  - **FT 802.1X**: Disable
  - **FT PSK**: Disable
  - **PSK Format**: ASCII
  - **SUITEB-1X**: Disable
  - **SUITEB192-1X**: Disable
  - **WPA gtk-randomize State**: Disable

#### Lobby Admin Configuration
- **Lobby Admin Access**: Disable
PacketFence Configuration:

- First because there is no way to detect in the RADIUS request that the request is for an SSID configured for IPSK, you need to configure PacketFence to trigger IPSK on a connection profile. To do that, create a new connection profile, set a Filter based on the SSID (Example SSID PSK_SSID), enable IPSK and set a default PSK key. So each time a device will connect on this specific SSID PacketFence will know that it has to answer with specific VSA attributes.

- Second step is to associate the device to a user, you have two ways to do it, the first one is to manually edit an user and in Miscellaneous tab fill the PSK entry (8 characters minimum) then
edit a node and change the owner with the one you just edit before. The second way to associate
the device is to use a provisioner. There are also 2 ways to do it, use the “IPSK” provisioner (it
will show you a page on the portal with the PSK key to use and the SSID to connect to, or use
the “Windows/Apple Devices/Android” provisioner and configure it to do IPSK.

![Provisioning Entry Windows](image)

Troubleshooting ignored RADIUS replies

In the event the WLC ignores the RADIUS replies from PacketFence (you receive multiple requests
but access is never granted), validate the following elements:

- RADIUS secret is properly configured in PacketFence and the WLC controller.
- The SSL certificate used by PacketFence is not expired.

Device Sensor

When using a Cisco WLC, you can enable device sensor by making sure the configuration looks
like the following screenshot:
Note
Please refer to the wired configuration of Cisco equipment to learn more about device sensor.

CoovaChilli

This section has been created in order to help setting up a consumer grade access point running CoovaChilli integration with PacketFence to use UAM capabilities along with PacketFence feature set.

Assumptions

- You have a CoovaChilli capable access point running LEDE/OpenWRT, on which CoovaChilli is installed (CoovaChilli installation is not covered in this guide);
- A working PacketFence server, a CoovaChilli capable access point, and Internet is functional;
- A PacketFence WebAuth enforcement setup will be deployed;

Access Point and CoovaChilli Configuration

We go ahead and start by configuring the access point and CoovaChilli running on it.

These instructions assume that CoovaChilli is installed on the access point. If it’s not, we suggest you search relevant information on the Internet to install CoovaChilli as there are too many network equipment vendors that support CoovaChilli to accurately document this step here.
These instructions also assume that you have an SSID configured on the access point. Assumption is also made that the network interface / bridge is configured and assigned for the given SSID.

You should also make sure to have a default route properly configured on the access point (so that it can access the Internet) and that DNS resolution is working.

Also note that changes on the OpenWRT access point are done using SSH shell access.

Please note that any interface name reference might be different from one equipment vendor to another.

**Configure chilli**

chilli configuration might differ from one equipment vendor to an other one. Just make sure to follow these configuration guidelines and you should be all-set.

- chilli configuration file can be found under

  ```
  /etc/config/chilli
  ```

- Edit the following parameters to integrate with PacketFence

  ```
<table>
<thead>
<tr>
<th>option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>option disabled 1</td>
<td>enabled</td>
</tr>
<tr>
<td>option dns1</td>
<td>Set this to a working DNS server (this will be used by hotspot clients)</td>
</tr>
<tr>
<td>option dns2</td>
<td>Set this to a working DNS server (this will be used by hotspot clients)</td>
</tr>
<tr>
<td>option ipup</td>
<td>/etc/chilli/up.sh (Depending on the package, the script path might need to be adjusted)</td>
</tr>
<tr>
<td>option ipdown</td>
<td>/etc/chilli/down.sh (Depending on the package, the script path might need to be adjusted)</td>
</tr>
<tr>
<td>option radiusservserver1</td>
<td>PacketFence management IP</td>
</tr>
<tr>
<td>option radiusservserver2</td>
<td>PacketFence management IP</td>
</tr>
<tr>
<td>option radiusssecret</td>
<td>The RADIUS secret that will be used between chilli and PacketFence</td>
</tr>
<tr>
<td>option radiusnasid</td>
<td>Access-point IP address</td>
</tr>
<tr>
<td>option dhcpif</td>
<td>The network interface / bridge assigned to the SSID (Hotspot clients network)</td>
</tr>
<tr>
<td>option uamserver</td>
<td>http://PACKETFENCE_MANAGEMENT_IP/CoovaChilli</td>
</tr>
<tr>
<td>option ssid</td>
<td>SSID name</td>
</tr>
<tr>
<td>option nasip</td>
<td>Access-point IP address</td>
</tr>
<tr>
<td>option coaport 3799</td>
<td></td>
</tr>
</tbody>
</table>
  ```

A startup script might be required depending on the equipment vendor. Again, a quick documentation search on the Internet might be the best solution to find the best one.

Once set up, you might want to activate chilli at boot (by using the startup script) and finally, reboot the AP.

**PacketFence Configuration for CoovaChilli Integration**

Having a working PacketFence installation and a configured LEDE / OpenWRT access point running CoovaChilli, the last step is PacketFence configuration for CoovaChilli integration.
To do so, login to the PacketFence web administration interface if it is not already done.

**Switch configuration**

Click on the *Configuration* tab and select the *Switches* menu option under the *NETWORK* section on the left hand side.

On the bottom of the page, click the *Add switch to group* button then select the *default* to bring up the *New Switch* configuration modal window.

**Definition tab**

- **IP**: Access-point IP address
- **Type**: CoovaChilli
- **Mode**: Production
- **External Portal Enforcement**: Checked

**RADIUS tab**

- **Secret Passphrase**: The RADIUS secret configured in the previous step

Click *Save*

**Portal configuration**

It is required to disable HTTPS redirection by clicking the *Configuration* tab and then the *Captive portal* menu option on the left hand side. Make sure *Secure redirect* is unchecked.

---

**D-Link**

**DWL Access-Points and DWS 3026**

- **Note**: 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 your 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.

---

**Fortinet FortiGate**

This section shows how to configure a 802.1X SSID on a Fortigate 50E running on FortiOS 5.4.

You will need to have the CLI access on the Fortigate to do the configuration.

**RADIUS**

```
FGT50E # config user radius
FGT50E (radius) # edit packetfence
  new entry 'packetfence' added
FGT50E (packetfence) # set server 192.168.1.5
FGT50E (packetfence) # set secret useStrongerSecret
FGT50E (packetfence) # set nas-ip 192.168.1.1
FGT50E (packetfence) # set radius-coa enable
FGT50E (packetfence) # config accounting-server
FGT50E (accounting-server) # edit 1
  new entry '1' added
FGT50E (1) # set status enable
FGT50E (1) # set server 192.168.1.5
FGT50E (1) # set secret useStrongerSecret
FGT50E (1) # end
FGT50E (packetfence) # end
```
802.1X SSID

FGT50E #config wireless-controller vap
FGT50E (vap) # edit PF-Secure
new entry 'PF-Secure’ added
FGT50E (PF-Secure) # edit "PF-Secure"
FGT50E (PF-Secure) # set vdom "root"
FGT50E (PF-Secure) # set ssid "PF-Secure"
FGT50E (PF-Secure) # set security wpa2-only-enterprise
FGT50E (PF-Secure) # set auth radius
FGT50E (PF-Secure) # set radius-server "packetfence"
FGT50E (PF-Secure) # set schedule "always"
FGT50E (PF-Secure) # set local-bridging enable
FGT50E (PF-Secure) # set dynamic-vlan enable
FGT50E (PF-Secure) # end

hostapd (OpenWrt Chaos Calmer 15.05)

Introduction

This section will provide an example for the configuration of an open SSID (not encrypted) and a secure SSID (802.1X). You will need to install wpad and hostapd. These two SSIDs will do RADIUS authentication against PacketFence. You can not have both SSID configured on the same access point at the same time, there is a limitation with the DAE server.

Assumptions

- You have a configured PacketFence environment with working test equipment
- The management IP of PacketFence will be 192.168.1.10 and has s3cr3t as its RADIUS shared secret
- You have an access point with OpenWrt Chaos Calmer 15.05 installed

Quick installation

Packages Installation

You can install the packages from the web interface of OpenWrt.

Go to System → Software

First update the repos by clicking the button Update lists if it's not up to date.

Then you will have to install the packages of Hostapd and wpad.
Go to the tab *Available packages* and then search for the package hostapd into the *Filter: field*.

Click Install the hostapd-common package, the actual version is 2015-03-25-1.

Do the same process for the wpad package version 2015-03-25-1.

**Note**

You will need the packages hostapd-common and wpad if they are not installed by default.

**Dynamic VLAN Configuration**

Connect using SSH to the AP and create the file ./etc/config/hostapd.vlan

```
* wlan0.#
```

**Hostapd Configuration**

You will need to modify the hostapd script that comes with the package that we previously installed.

Connect using SSH to the AP and run these commands:

```
   cd /lib/netifd/
   mv hostapd.sh hostapd.sh.old
   opkg install curl
   curl --insecure https://github.com/inverse-inc/packetfence/tree/devel/addons/hostapd/hostapd-15.05.sh > hostapd.sh
   wifi
```

**Configure the SSIDs**

To configure the PF-Open SSID, we will edit the file ./etc/config/wireless:

```
# Definition of the radio
config wifi-device 'radio0'
    option type 'mac80211'
    option channel '11'
    option hwmode '11g'
    option path 'pci0000:00/0000:00:00.0'
    option htmode 'HT20'

# Configuration of the Open SSID
    option device 'radio0'
    option mode 'ap'
    option vlan_file '/etc/config/hostapd.vlan'
    option vlan_tagged_interface 'eth0'
    option vlan_naming '0'
    option dynamic_vlan '2'
    option auth_port '1812'
    option auth_server '192.168.1.10'
    option auth_secret 's3cr3t'
    option acct_port '1813'
    option acct_server '192.168.1.10'
    option acct_secret 's3cr3t'
    option dae_port '3799'
    option dae_client '192.168.1.10'
    option dae_secret 's3cr3t'
    option nasid 'Lobby'
    option encryption 'none'
    option ssid 'OpenWRT-Open'

Configure the PF-Secure SSID:
Chapter 6

### Definition of the radio

```c
# Definition of the radio
config wifi-device 'radio0'
    option type 'mac80211'
    option channel '11'
    option hwmode '11g'
    option path '/pci0000:00/0000:00:00.0'
    option htmode 'HT20'

config wifi-iface
    option device 'radio0'
    option mode 'ap'
    option vlan_file '/etc/config/hostapd.vlan'
    option vlan_tagged_interface 'eth0'
    option vlanNaming '0'
    option dynamic_vlan '2'
    option auth_port '1812'
    option auth_server '192.168.1.10'
    option auth_secret 's3cr3t'
    option acct_port '1813'
    option acct_server '192.168.1.10'
    option acct_secret 's3cr3t'
    option dae_port '3799'
    option dae_client '192.168.1.10'
    option dae_secret 's3cr3t'
    option nasid 'Lobby'
    option encryption 'wpa2'
    option ssid 'OpenWRT-Secure'
```

In order to apply this configuration, when you are connected using SSH on the AP, run the command `wifi`. It will reload the configuration and broadcast the SSID. If you want to debug, you can use the command `logread`.

**Note**

It's known that you can't put 2 SSIDs with the same dae server at the same time. The deauthentication will not work on the second SSID.

### PacketFence Configuration

Log in to the PacketFence administration web page and go under Configuration → Policies and Access Control → Switches → Add switch.

**Definition:**

- **IP Address/MAC Address/Range (CIDR):** IP of your access point
- **Type:** Hostapd
- **Mode:** production
- **Deauthentication Method:** RADIUS
- **Dynamic Uplinks:** Checked

**Roles:**
• **Role by VLAN ID**: Checked
• **Registration**: Your registration VLAN ID
• **Isolation**: Your isolation VLAN ID

**RADIUS:**

• **Secret Passphrase**: s3cr3t

Save this configuration by clicking the **Save** button.

**Troubleshoot**

There are few things you can do/check to see if your configuration is working.

To check the wireless configuration: `uci show wireless` or `cat /etc/config/wireless`

To check if your configuration (depend on the equipment) is correctly set into the Hostapd configuration file: `cat /var/run/hostapd-phy0.conf`

---

**Huawei**

**AC6605 Controller**

PacketFence supports this controller with the following technologies:

• Wireless 802.1X
• Wireless MAC Authentication

**Controller configuration**

Setup NTP server:

```
<AC>system-view
[AC] ntp-service unicast-server 208.69.56.110
```

Setup the radius server (@IP of PacketFence) authentication + accounting:

```
```

**Note**

In this configuration I will use the ip address of the VIP of PacketFence: 192.168.1.2; Registration VLAN : 145, Isolation VLAN : 146
Create an Secure dot1x SSID

Activate the dotx globally:

```
<AC>system-view
[AC] dot1x enable
```

Create your secure dot1x ssid:

Configure WLAN-ESS 0 interfaces:

```
[AC] interface Wlan-Ess 0
[AC-Wlan-Ess0] port hybrid untagged vlan 145 to 146
[AC-Wlan-Ess0] dot1x enable
[AC-Wlan-Ess0] dot1x authentication-method eap
[AC-Wlan-Ess0] permit-domain name your.domain.com
[AC-Wlan-Ess0] force-domain name your.domain.com
[AC-Wlan-Ess0] default-domain your.domain.com
[AC-Wlan-Ess0] quit
```

Configure AP parameters:

Configure radios for APs:
Configure a security profile named huawei-ap. Set the security policy to WPA authentication, authentication method to 802.1X+PEAP, and encryption mode to CCMP:

```plaintext
[AC-wlan-view] security-profile name huawei-ap-wpa2
[AC-wlan-sec-prof-huawei-ap-wpa2] quit
```

Configure a traffic profile:

```plaintext
[AC-wlan-view] traffic-profile name huawei-ap
[AC-wlan-wmm-traffic-huawei-ap] quit
```

Configure service sets for APs, and set the data forwarding mode to direct forwarding:

The direct forwarding mode is used by default.

```plaintext
[AC-wlan-view] service-set name PacketFence-dot1x
[AC-wlan-service-set-PacketFence-dot1x] ssid PacketFence-Secure
[AC-wlan-service-set-PacketFence-dot1x] wlan-ess 0
[AC-wlan-service-set-PacketFence-dot1x] service-vlan 1
[AC-wlan-service-set-PacketFence-dot1x] security-profile name huawei-ap-wpa2
[AC-wlan-service-set-PacketFence-dot1x] traffic-profile name huawei-ap
[AC-wlan-service-set-PacketFence-dot1x] forward-mode tunnel
[AC-wlan-service-set-PacketFence-dot1x] quit
```

Configure VAPs and deliver configurations to the APs:

```plaintext
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] service-set name PacketFence-dot1x
[AC-wlan-radio-1/0] quit
[AC-wlan-view] commit ap 1
```

**Create your Open ssid**

Activate the mac-auth globally:
Create your Open ssid:

Configure WLAN-ESS 1 interfaces:

```
<AC>system-view
[AC] mac-authen
[AC] mac-authen username macaddress format with-hyphen
[AC] mac-authen domain your.domain.com
```

```
[AC interface Wlan-Ess 1
[AC-Wlan-Ess1] port hybrid untagged vlan 145 to 146
[AC-Wlan-Ess1] mac-authen
[AC-Wlan-Ess1] mac-authen username macaddress format without-hyphen
[AC-Wlan-Ess1] permit-domain name your.domain.com
[AC-Wlan-Ess1] force-domain name your.domain.com
[AC-Wlan-Ess1] default-domain your.domain.com
[AC-Wlan-Ess1] quit
```

Configure AP parameters:

```
[AC]wlan
[AC-wlan-view] security-profile name huawei-ap-wep
[AC-wlan-sec-prof-huawei-ap-wep] quit
```

Configure service sets for APs, and set the data forwarding mode to direct forwarding:

```
[AC-wlan-view] service-set name PacketFence-WEP
[AC-wlan-service-set-PacketFence-WEP] ssid PacketFence-Open
[AC-wlan-service-set-PacketFence-WEP] wlan-ess 1
[AC-wlan-service-set-PacketFence-WEP] service-vlan 1
[AC-wlan-service-set-PacketFence-WEP] security-profile name huawei-ap-wep
[AC-wlan-service-set-PacketFence-WEP] traffic-profile name huawei-ap (already created before)
[AC-wlan-service-set-PacketFence-WEP] forward-mode tunnel
[AC-wlan-service-set-PacketFence-WEP] quit
```

Configure VAPs and deliver configurations to the APs:

```
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] service-set name PacketFence-WEP
[AC-wlan-radio-1/0] quit
[AC-wlan-view] commit ap 1
```
Meraki

To add the AP on PacketFence use the internal IP of the AP.

The Disconnect port field must be set to 1700.

WebAuth

In this section, we will cover the configuration of the Meraki controller to use Web authentication.

Note

While using the WebAuth mode on the Meraki controller, you need to use "Role mapping by Switch Role" and "Role by Web Auth URL" in the tab Roles from the switch configuration.

Configure your SSID as shown below:
Network access

Association requirements
- Open (no encryption)
  Any user can associate
- Pre-shared key
  Users must enter a passphrase to associate
- MAC-based access control (no encryption)
  RADIUS server queried at association time
- WPA2-Enterprise
  User credentials are validated with 802.1X at association time

Splash page
- None (direct access)
  Users can access the network as soon as they associate
- Click-through
  Users must view and acknowledge your splash page before being allowed on the network
- Sign-on with Meraki authentication
  Users must enter a username and password before being allowed on the network
- Sign-on with SMS Authentication
  Users enter a mobile phone number and receive an authentication code via SMS.
  After a trial period of 24 hours, you will need to connect with your Twilio account on the Network-wide settings page.
- Billing (paid access)
  Users choose from various pay-for-access options, or an optional free tier
- Systems Manager Sentry enrollment
  Only devices with Systems Manager can access this network
- Cisco Identity Services Engine (ISE) Authentication
  Users are redirected to the Cisco ISE web portal for device postureing and guest access

RADIUS servers

<table>
<thead>
<tr>
<th>#</th>
<th>Host</th>
<th>Port</th>
<th>Secret</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.1.5</td>
<td>1812</td>
<td><strong>---------</strong></td>
<td><img src="X" alt="Modify" /> <img src="X" alt="Test" /></td>
</tr>
</tbody>
</table>

RADIUS testing
- RADIUS testing disabled

RADIUS CoA support
- RADIUS CoA enabled

RADIUS accounting
- RADIUS accounting is enabled

RADIUS accounting servers

<table>
<thead>
<tr>
<th>#</th>
<th>Host</th>
<th>Port</th>
<th>Secret</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.1.5</td>
<td>1813</td>
<td><strong>---------</strong></td>
<td><img src="X" alt="Modify" /> <img src="X" alt="Test" /></td>
</tr>
</tbody>
</table>

Add a server

RADIUS attribute specifying group policy name
- Amspace-ACL-Name
It is mandatory that you use the Airespace-ACL-Name as "RADIUS attribute specifying group policy name".

The switch module to use for this configuration is "Meraki cloud controller V2".

Next, configure the roles for the devices on your network. Go in Network-wide→Group policies, then you will be able to create policies that can be configured as roles in the switch configuration of PacketFence. Creation of the policy Guest:
Your configuration for the tab "Roles" in PacketFence will look like the following:
<table>
<thead>
<tr>
<th>Role by Switch Role</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>registration</td>
<td>registration</td>
</tr>
<tr>
<td>isolation</td>
<td>isolation</td>
</tr>
<tr>
<td>macDetection</td>
<td>macDetection</td>
</tr>
<tr>
<td>inline</td>
<td>inline</td>
</tr>
<tr>
<td>default</td>
<td>Authorized devices</td>
</tr>
<tr>
<td>guest</td>
<td>Guest</td>
</tr>
<tr>
<td>gaming</td>
<td></td>
</tr>
<tr>
<td>voice</td>
<td>voice</td>
</tr>
</tbody>
</table>
URL in registration field should be in the form: http://<your_captive_portal_ip>/Meraki::MR_v2

**VLAN enforcement**

This section will cover how to configure the Meraki WiFi controller to use with VLAN enforcement, use the configuration in the section WebAuth for the SSID.

In the configuration of PacketFence, use "Role by VLAN ID" and fill your VLANs matching roles.
You should already have one port setup as Uplink, using a mode trunk, with at least your Registration and Production VLAN allowed on it.

The Meraki switch offer configuration for VLAN enforcement only.

You will need to access the Meraki dashboard to configure your switch. When you reach it you will need first to create a policy. You can create a "MAC authentication bypass" or a "802.1X" policy. Depending if you want to authenticate user via dot1x or MAB. You cannot combine both neither use a fallback mode on the same port, each port with a policy applied will be exclusive to MAB or dot1x.

To access the policy creation go to Switch→Access policies in the Meraki dashboard menu. From there create a new policy, use the example below to create your policy.
You now need to apply one of your policies to ports. To do so, go to Switch→Switch ports and chose your options. To add a policy you created earlier, select it in the drop down list in Access policy. You need to configure the port in "mode access", the default access VLAN is not important if your VLANs are properly configured on PacketFence.
It is possible to use RADSEC between Meraki and PacketFence in order to perform RADIUS over TCP and encrypted using TLS. Before performing the steps outlined in this section, make sure you have a working SSID using normal unencrypted RADIUS by following the steps in the sections above.
Then, in order to enable RADSEC, go in your SSID configuration and under RADIUS proxy, select Use Meraki proxy and save the settings.

After saving, check the RADSEC checkbox and save your settings.

Now, on your PacketFence server, you must add the Meraki CA root to the trusted Certificate Authorities of FreeRADIUS when performing RADSEC. You should download the Meraki CA certificate from here http://changeme.com/meraki-root.crt and append it to the content of /usr/local/pf/raddb/certs/ca.pem on your PacketFence server.

Next, restart radiusd to reload the CA certificates using:

```
# /usr/local/pf/bin/pfcmd service radiusd restart
```

**Note**

RADSEC is done over port 2083 so make sure your server is available via a public IP address for this port and allows connections from your Meraki cloud controller. Refer to the Meraki documentation for details.

**Mikrotik**

This configuration has been tested on Access Point OmniTIK U-5hnD with RouterOS v6.18 and only MAC-Authentication is available now. The only deauthentication method available is SSH, so create an account in the Mikrotik AP and fill the information in PacketFence switch configuration. Also don’t forget to use the pf account to ssh on the Access Point to receive the ssh key.

**Open SSID**

In this setup we use the interface ether5 for the bridge (Trunk interface) and ether1 as the management interface.

Configure your access point with the following configuration:
Webauth

You can use webauth (external captive portal) on Mikrotik APs. In order to do so, you will have to activate the hotspot feature in the AP configuration as well as modify the redirection template so that it points to PacketFence.
First, you must establish an FTP connection to your access point and replace the content of hotspot/login.html with the following:

```html
<html>
<head><title>.../title</head>
<body>
$(if chap-id)
<noscript>
<center><b>JavaScript required. Enable JavaScript to continue.</b></center>
</noscript>
$(endif)
<center>If you are not redirected in a few seconds, click 'continue' below<br>
<form name="redirect" action="http://192.168.1.5/Mikrotik" method="get">
<input type="hidden" name="mac" value="$(mac)"
<input type="hidden" name="ip" value="$(ip)"
<input type="hidden" name="username" value="$(username)"
<input type="hidden" name="link-login" value="$(link-login)"
<input type="hidden" name="link-orig" value="$(link-orig)"
<input type="hidden" name="error" value="$(error)"
<input type="hidden" name="chap-id" value="$(chap-id)"
<input type="hidden" name="chap-challenge" value="$(chap-challenge)"
<input type="hidden" name="link-login-only" value="$(link-login-only)"
<input type="hidden" name="link-orig-esc" value="$(link-orig-esc)"
<input type="hidden" name="mac-esc" value="$(mac-esc)"
<input type="hidden" name="ap-id" value="AP_IP_ADDRESS_HERE"
<input type="hidden" name="chap-id" value="$(chap-id)"
<input type="hidden" name="chap-challenge" value="$(chap-challenge)"
<input type="hidden" name="link-login-only" value="$(link-login-only)"
<input type="hidden" name="link-orig-esc" value="$(link-orig-esc)"
<input type="hidden" name="mac-esc" value="$(mac-esc)"
<input type="hidden" name="ap-id" value="AP_IP_ADDRESS_HERE"
<input type="submit" value="continue">
</form>
<script language="JavaScript">
<!--
 document.redirect.submit();
//-->
</script></center>
</body>
</html>
```

Next, in the login.html you have just uploaded, make sure you change AP.IP_ADDRESS_HERE by the management IP address of your access point and 192.168.1.5 by the IP address of your PacketFence captive portal.

Now, you must configure the hotspot feature on your AP. This configuration is done on top of an existing SSID you have previously configured which is on interface wlan1. Adjust the interface name if needed.

```
ip hotspot
setup

hotspot interface: wlan1

local address of network: 10.5.50.1/24
masquerade network: yes
```

Set pool for HotSpot addresses
address pool of network: 10.5.50.2-10.5.50.254

Select hotspot SSL certificate

select certificate: none

Select SMTP server

ip address of smtp server: 0.0.0.0

Setup DNS configuration

dns servers: 8.8.8.8

DNS name of local hotspot server

dns name: myhotspot

Create local hotspot user

name of local hotspot user: admin
password for the user:

Next, you need to allow access to the PacketFence portal in the hotspot access list. Change 192.168.1.5 with the IP address you pointed to in login.html

/ip hotspot walled-garden
add dst-host=192.168.1.5
add src-address=192.168.1.5

/ip hotspot walled-garden ip
add action=accept disabled=no dst-host=192.168.1.5
add action=accept disabled=no src-address=192.168.1.5

Now, you will also need to configure the hotspot to point to your PacketFence RADIUS server:

/radius
add address=192.168.1.5 secret=useStrongerSecret service=hotspot

/ip hotspot profile
add hotspot-address=10.5.50.1 name=hsprof1 use-radius=yes

Next, you need to configure PacketFence to use webauth for this Access Point using the following switches.conf configuration. Change AP_IP_ADDRESS_HERE by the IP address you’ve put in login.html.
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 radio00 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)
Chapter 6

- 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.

Mojo Networks

PacketFence supports SSIDs configured with 802.1X and Web Authentication

Create the RADIUS Profile

First, create a RADIUS Profile for PacketFence.
• Login to the https://dashboard.mojonetworks.com

• Go to Wireless Manager

• Then click on Configuration → Device Configuration → RADIUS Profiles → Add a RADIUS Profile

| Profile Name: NAME_OF_PROFILE_FOR_PACKETFENCE |
| IP Address: IP_OF_PACKETFENCE |
| Authentication Port: 1812 |
| Accounting Port: 1813 |
| Shared Secret: useStrongerSecret |

Click on Save.

Configure the SSID:

802.1X Secure

• Login to the https://dashboard.mojonetworks.com

• Go to Wireless Manager

• Then click on Configuration → Device Configuration → SSID Profiles → Add a new Profile → WLAN

| Profile Name: PF-Secure-802.1X |
| SSID: PF-Secure |
| Security: WPA2; 802.1X |
| NAS ID: %m-%s |
| Dynamic VLANs: Enable VLAN Pool 1,2,4,5 (All VLANs that you will use) |
| Called-Station-ID: %m-%s |
| COA: Checked |

RADIUS Authentication
Primary Authentication Server: PacketFence RADIUS profile created above.

RADIUS Accounting Server Details
Primary Accounting Server: PacketFence RADIUS profile created above.

Click the Save button to save the PF-Secure SSID configuration.

Web Authentication

To enable the external captive portal, go to the SSID Profiles page in Device Configuration. Add a new Wi-Fi profile with the following attributes:
Profile Name: Name of the new profile
SSID: Name of your SSID
Security: Open

**Security**

Security Mode: Open

Client Isolation: Enabling Client Isolation will void L2TIF functionality in Hotspot Settings of SSID Profile.
Secondary Authentication

Network: VLAN ID for clients

Network:

VLAN ID: 2

Range: 0 to 4094. To map to untagged VLAN in switch port, enter VLAN ID = 0, irrespective of what VLAN ID is assigned to untagged VLAN in switch.


**External Splash Page with RADIUS Authentication**

Splash Page URL: http://IP.OR.HOSTNAME_OF_PACKETFENCE/Mojo
Shared Secret: ••••

RADIUS Settings

Define RADIUS server used to authenticate the user with the credentials entered on the splash page.

On the right, add the IP address or hostname of PacketFence to the Walled Garden Sites.
Save the newly created profile.

Broadcast the SSID on the Access Point:

- Go to Configuration → Device Template → System Template
- Then Radio Settings → Define settings for model → Chose your AP model
- Finally Radio 1 - 2x2 b/g/n Configuration → Add SSID Profile → Select your SSID profile previously created (802.1X or Web authentication profile) → Ok

Click the Save button to broadcast the PF-Secure SSID.

Configure the Mojo Networks AP in PacketFence:

**802.1X**

Add a Switch with the IP address of the Access Point (AP) with the following configuration:

- Go to Configuration → Network → Switches → Add switch to group → Default
Chapter 6

**Web Authentication**

Add a switch with the IP address for the Access Point (AP) with the following configuration:

- Go to **Configuration → Network → Switches → Add switch to group → Default**

**Important**

Clone the newly created switch and enter **192.0.2.254** or the MAC address of the AP.
Motorola

In order to have the Motorola RFS 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**

**Accounting configuration:**

- **Make sure you select "Enable RADIUS Accounting"**
• Select the previously configured AAA Policy

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)

Accounting configuration:

• Make sure you select “Enable RADIUS Accounting”
• Select the previously configured AAA Policy

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.
Chapter 6

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 → rfsXXXX-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.

WIPS

In order to enable the WIPS functionality on the Motorola, you need to follow this procedure. The steps have been done using the CLI.

First, Create a wips-policy:

```
wips-policy Rogue-AP
history-throttle-duration 86400
event ap-anomaly airjack
event ap-anomaly null-probe-response
event ap-anomaly asleep
event ap-anomaly ad-hoc-violation
event ap-anomaly ap-ssid-broadcast-in-beacon
event ap-anomaly impersonation-attack
ap-detection
```

Next, create an event policy:

```
event-system-policy PF-WIDS
event wips wips-event syslog off snmp on forward-to-switch off email off
```

Next, create or adjust your management policy to configure the SNMP traps. Here is an example policy, please note the two last lines:
management-policy default
no http server
https server
ssh
user admin password 1
e4c93663e3356787d451312eeb8d4704ef09f2331a20133764c3dc3121f13a5b role superuser
access all
user operator password 1
7c9b1fbb2ed75bb50dbaa0b563eac722b0676b45fed726d3e4e563b0c87d236d role monitor
access all
no snmp-server manager v3
snmp-server community public ro
snmp-server community private rw
snmp-server user snmpoperator v3 encrypted des auth md5 0 operator
snmp-server user snmptrap v3 encrypted des auth md5 0 motorola
snmp-server user snmpmanager v3 encrypted des auth md5 0 motorola
snmp-server enable traps
snmp-server host 10.0.0.100 v2c 162

You then need to tell your controller to use the event policy:

rfs6000 5C-0E-8B-17-F2-E3
...
use event-system-policy PF-WIDS

Finally, you need to configure a radio interface on your AP to act as a sensor. Here is an example configuration for a dual-radio AP650:

ap650 00-23-68-86-EB-BC
use profile default-ap650
use rf-domain default
hostname ap650-86EBBC
country-code ca
use wips-policy Rogue-AP
interface radio1
rf-mode sensor
channel smart
power smart
data-rates default
no preamble-short
radio-share-mode off
interface radio2
...

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
Chapter 6

- 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

**WIPS**

To enable the WIPS feature of the Ruckus in order to send SNMP traps to PacketFence, the setup is fairly simple.

First, configure the controller to send the traps to PacketFence. Under **Configure > System > Network Management > SNMP Trap**:

* Select "Enable SNMP Trap" * Put the PacketFence Management IP in the Trap Server IP field

**Note**

The traps will arrive with the "public" community string

Next, you need to configure the Alarm Settings. Under **Configure > Alarm Settings**, make sure the following are selected:

*Rogue AP Detected *SSID-Spoofing AP Detected *MAC-Spoofing AP Detected *LAN Rogue AP Detected

Finally, enable the WIPS feature on the controller. Under **Configure > WIPS > Intrusion Detection and Prevention**, make sure both box are selected, click Apply.

**Web Authentication**

In order to use PacketFence as an external captive portal for web authentication, you will need to configure first your RADIUS authentication and accounting server (see steps above).
Hotspot configuration

Configure the Hotspot service profile to redirect devices to your PacketFence portal. Go on the ZoneDirector administration web page to the section Configure→Hotspot Services→Create New

1. Name of your Hotspot service
3. Start Page: redirect to the following URL: http://192.168.1.5
4. Authentication Server: Select the PacketFence authentication RADIUS server (default port 1812)
5. Accounting Server: Select the PacketFence accounting RADIUS server (default port 1813)
6. Click on the Walled Garden and authorize the IP of PacketFence management interface

Save your configuration.
WLAN configuration

Go to Configure→WLANs→WLANs→Create New

1 - Name of your SSID
2 - Type: Hotspot Service (WISPr)
3 - Authentication Method: Open
4 - Encryption Method: None
5 - Hotspot Services: Your hotspot service name that you configured
6 - Access VLAN: The VLAN ID that should be assigned to devices after authentication

Save your configuration.

PacketFence configuration

On the ZoneDirector configuration in PacketFence, you will need to specify -1 as the registration VLAN in order to display the captive portal to the end device.
You will need to deactivate the force secure redirect on the captive portal under **Configuration → Captive Portal → Secure redirect → Unchecked**

The captive portal needs to listen on the management interface, so you will need to add the portal daemon to the management interface under **Configuration → Interfaces → Management Interface**

Example:

```
[interface eth0]
ip=192.168.1.5
type=management,portal
mask=255.255.255.0
```

To apply the configuration, restart PacketFence using the following command: `service packetfence restart`

**Ruckus Roles**

**Roles Configuration**

Ruckus allows you to define roles. These roles link all users to the internal WLAN and permit access to all WLAN by default. You can still limit access to certain WLAN.

To create a new user Role:

1. Go to Admin & Services > System > Roles. The Roles page appears, displaying a Default role in the Roles table.
2. Click Create New.
3. Enter a Name and a short Description for this role.
4. Choose the options for this role from the following:
   - **Group Attributes**: Fill in this field only if you are creating a user role based on Group attributes extracted from an Active Directory server. Enter the User Group name here. Active Directory/LDAP users with the same group attributes are automatically mapped to this user role.
   - **Allow All WLANs**: You have two options: (1) Allow Access to all WLANs, or (2) Specify WLAN Access. If you select the second option, you must specify the WLANs by clicking the check box next to each one.
PacketFence Configuration

On the PacketFence side you need to use role by switch role and add the Group Attribute you created on the Ruckus side.

So when a device will connect on the SSID, PacketFence will return a VLAN identifier and a RuckusUserGroup attribute and if the role is allowed on the WLAN then the device will be authorized on the WLAN. In the case that the role is not allowed on the WLAN then the device will not be allowed to connect.
Ruckus SmartZone

Webauth

SmartZone configuration

First, you will need to define your RADIUS server in Configuration→Service and Profiles→Authentication.

Create your server using the following information (where 192.168.1.5 is the IP address of your PacketFence management interface):

- **IP Address**: 192.168.1.5
- **Port**: 1812
- **Secret**: useStrongerSecret

Then, in Configuration→Service and Profiles→Accounting, create a server with the following information:

- **IP Address**: 192.168.1.5
- **Port**: 1813
- **Secret**: useStrongerSecret

After, create a Hotspot in Configuration→AP Zones→Your Zone→Hotspot WISPr→Create New. Adjust 192.168.1.5 to the IP address of your portal.

![SmartZone configuration screenshot](image-url)
Then, still on this page, in the *Walled Gardens*, make sure you add the portal IP address in this list.

Next, you will need to configure your WLAN to use the Hotspot authentication and point it to PacketFence. Also ensure you set *Use the controller as a proxy*.

![Image of Ruckus SmartZone configuration interface]

Now, you should configure the Northbound API of the SmartZone so PacketFence can communicate with it. In order to do so, go in *Configuration→System→Northbound Portal Interface* and set the *Password* and save it. Keep the password closeby as it will be required for the PacketFence configuration. In this example, it will be `passwordForNorthboundAPI`.

In order to receive the information not encrypted in the URL, you will need to connect on the Ruckus SmartZone controller using SSH and do the following command:

```
no encrypt=mac-ip
```

**PacketFence configuration**

In PacketFence, add a switch in *Configuration→Switches* with the following configuration:

- *Definition→External Portal Enforcement* should be enabled
- *Definition→Type*: *Ruckus SmartZone Wireless Controller*
- *Definition→Mode*: *production*
- *Roles→Role by VLAN ID* should be enabled
- *Roles→registration VLAN*: `-1`
- *Roles→Role by Switch Role* should be disabled
- *RADIUS→Secret passphrase*: `useStrongerSecret`
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**

```plaintext
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 (PacketFence-Public) and one for the WPA2-Enterprise SSID (PacketFence-Secure):

```plaintext
set service-profile PF-Open ssid-name PacketFence-Public
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 PacketFence-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 PacketFence-Public
set radio-profile default service-profile PacketFence-Secure
```

**AAA configuration**

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

```plaintext
set accounting dot1x ssid PacketFence-Secure ** start-stop PF-RADIUS
set accounting mac ssid PacketFence-Public * start-stop PF-RADIUS
set authentication mac ssid PacketFence-Public * PF-RADIUS
set authentication dot1x ssid PacketFence-Secure ** pass-through PF-RADIUS
```
Chapter 6

Ubiquiti

Web Authentication

In order to configure web authentication (external captive-portal) on Ubiquiti access points, you must have access to a Unifi controller and your APs must be connected to it.

First, you must configure the guest policy. Go in Settings→Guest Control and configure it as shown below:

Make sure you enabled Enable Guest Portal, and that you’ve set External portal server.

You also need to enter the IP address of a portal enabled interface on the PacketFence server in Custom Portal. Then in the ACCESS CONTROL section, add that same IP address to the Pre-Authorization Access

Then, still in the settings, create or edit a new SSID with the following settings:
Once this is done, you will need to define all your APs MAC addresses in the PacketFence switches with a configuration similar to this:

```
[00:11:22:33:44:55]
description=Ubiquiti AP
ExternalPortalEnforcement=Y
type=Ubiquiti::Unifi
controllerIp=1.2.3.4
wsTransport=HTTPS
wsUser=admin
wsPwd=admin
```

Where:

- **wsTransport** is the protocol used to connect to port 8443 of the Unifi controller and should be HTTPS. This is configured in the Web Services tab of the switch.
- **wsUser** is a valid administrator username on your Unifi controller. This is configured in the Web Services tab of the switch.
- **wsPwd** is the password that is associated to the wsUser. This is configured in the Web Services tab of the switch.
- **controllerIp** is the IP address of your Unifi controller. This is configured in the Definition tab of the switch.

### VLAN Enforcement

In order to configure VLAN enforcement on the Unifi controller, you need first to configure a RADIUS profile, then a secure wireless network.

Important: You cannot reuse a VLAN ID for dynamic VLAN if it is set as a static value for another SSID on the same AP. So, if you have a SSID set to use VLAN 10, you cannot use VLAN ID 10 for RADIUS controlled VLAN users as those users will not get an IP address.

Note that VLAN enforcement for an open SSID is not supported yet by the controller and access point.
AAA Configuration

Secure SSID

There is a special case when you want to be able to deauthenticate a device when it is connected on the secure SSID.

By default pmksa caching is enabled and applies even when a deauthentication request is sent to the controller, meaning you will not get a new RADIUS request afterwards. To disable this cache you will need to create a file on the controller.

First verify the site where your access point is managed. To do this, under the administration interface of the controller, select the appropriate "Current Site" then in the URI check the value just after site.

In this case the URL is https://192.168.1.6:8443/manage/site/4j4ee7x4/ so the site id is 4j4ee7x4.

Next connect on the controller via SSH and go in /usr/lib/unifi/data/sites/4j4ee7x4 (replace 4j4ee7x4 with your site id) and create a file named config.properties with the following content:

```
config.system_cfg.1=aaa.1.auth_cache=disabled
config.system_cfg.2=aaa.4.auth_cache=disabled
```

The numbers 1 and 4 are the profile id configured on the access point. To be sure you have the correct id, you can connect on the access point via SSH or via the debug terminal and do:
BZ.v3.9.3# cat /tmp/system.cfg | grep ssid
  aaa.1.ssid=PacketFence-Secure
  wireless.1.ssid=PacketFence-Secure
  wireless.1.hide_ssid=false
  aaa.2.ssid=PacketFence-Public
  wireless.2.ssid=PacketFence-Public
  wireless.2.hide_ssid=false
  aaa.3.ssid=vport-802AA8863D5B
  wireless.3.ssid=vport-802AA8863D5B
  wireless.3.hide_ssid=true
  aaa.4.ssid=PacketFence-Secure
  wireless.4.ssid=PacketFence-Secure
  wireless.4.hide_ssid=false
  aaa.5.ssid=PacketFence-Public
  wireless.5.ssid=PacketFence-Public
  wireless.5.hide_ssid=false

You can see that PacketFence-Secure appears in 1 and 4 (2 radios).

For additional details, feel free to ask for support directly in the Ubiquiti forum:  https://community.ubnt.com/t5/UniFi-Wireless/Feature-request-disable-pmksa-caching/m-p/2112479#M257628

Next you will need to create a secured profile:
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).

External portal SSID

- Set Encryption / Authentication to None / Open
- Then check the WPR checkbox
- Then in in the section Web Page Redirect Configuration set Server to External Login
- Set the Redirect URL to http://192.168.1.5/Xirus
- Set the Redirect Secret to any passphrase of your choice
- In the RADIUS Configuration section set the RADIUS server to point to your PacketFence server
VPN Configuration

Cisco ASA

AnyConnect

PacketFence supports Cisco ASA VPN with AnyConnect.

You can force VPN users to authenticate first on the captive portal and based on the role of the device allow it and/or set dynamic ACL.

In this example we assume that the Cisco ASA have 2 interfaces, one Management (192.168.2.1) where the VPN is activated and another one Registration (192.168.1.6) that is facing the PacketFence server (192.168.1.5).

Before trying to configure PacketFence with the Cisco ASA first be sure that when you connect with AnyConnect and when the VPN is up that your device is able to reach Internet.
ip local pool VPN_POOL 192.168.255.10-192.168.255.254 mask 255.255.255.0

interface GigabitEthernet0/0
  nameif MANAGEMENT
  security-level 0
  ip address 192.168.2.1 255.255.255.0

interface GigabitEthernet0/1
  nameif Registration
  security-level 0
  ip address 192.168.1.5 255.255.0.0

same-security-traffic permit inter-interface
same-security-traffic permit intra-interface

object network NETWORK_OBJ_192.168.255.0_24
  subnet 192.168.255.0 255.255.255.0

access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any any host 192.168.1.5
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www
access-list redirect extended permit tcp any any eq https

route MANAGEMENT 0.0.0.0 0.0.0.0 192.168.2.254 1

aaa-server PacketFence protocol radius
  authorize-only
  interim-accounting-update periodic 1
  merge-dacl before-avpair
dynamic-authorization

aaa-server PacketFence (Registration) host 192.168.1.5
timeout 5
key useStrongerSecret
authentication-port 1812
accounting-port 1813

http server enable
http 192.168.0.0 255.255.0.0 MANAGEMENT

webvpn
enable MANAGEMENT
anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 8
anyconnect image disk0:/anyconnect-linux-64-4.0.00051-k9.pkg 9
anyconnect image disk0:/anyconnect-macosx-i386-4.0.00051-k9.pkg 10
anyconnect profiles VPN_client_profile disk0:/VPN_client_profile.xml
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable
group-policy GroupPolicy_VPN internal
group-policy GroupPolicy_VPN attributes
dns-server value 1.1.1.1
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain value acme.com
webvpn
anyconnect profiles value VPN_client_profile type user
tunnel-group VPN type remote-access
Chapter 8

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
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/ for details.
GNU Free Documentation License

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