GÉANT

Cookbook for Configuration of HP Wireless Equipment

Best Practice Document

Authors: Tomas Podermanski, Vladimir Zahorik
March 2010

Table of Contents

Executive Summary

This document describes the configuration of access points of the HP ProCurve series. Both the configuration for eduroam authentication via the 802.1x protocol and configuration using higher-level authentication mechanisms (typically web authentication) are described.

1   Cookbook for Configuration of HP Wireless Equipment

The examples in this document assume that the following VLANs are attached to the switch port which connects the Access Point:

VLAN for management is used only for access point management. This VLAN must also provide access to RADIUS servers where authentication credentials are checked.

802.1Q TAG :	504
IP address:	10.229.255.61
Mask:	255.255.255.0
Default gateway:	10.229.255.1

VLAN with web-based authentication. For this VLAN we assume that authentication is performed via higher-layer protocols. The operation of this network is assumed to be managed by the equipment providing authentication. Typically this is the access gateway providing web authentication. It is advisable to configure this VLAN even if you decided not to use it for normal user operations. In that case we recommend forwarding all traffic to a web server which stores information and manuals required to correctly configure the eduroam network.

802.1Q TAG:	589
Spread with **SSID**:	vutbrno

VLAN eduroam. This is used for users authenticated via eduroam. No other security mechanism is required on this network. Authentication is provided by the 802.1x protocol.

802.1Q TAG:	578
Spread with **SSID**:	eduroam

2   HP ProCurve 530

URL at the manufacturer's website:
http://h10144.www1.hp.com/products/wireless/ProCurve_Access_Point_530/overview.htm

The sample configuration is based on an unconfigured AP or an AP set to factory default. It describes commands entered into the CLI after connecting through a serial port. The resulting configuration can be saved to a file, but it is written in an XML format that is relatively hard to read.

Reset to factory default:

- Press reset and clear.
- Press reset after *LED go off*.
- The initial login data are admin/admin.

```
ProCurve-AP-530 login: admin
Password:
ProCurve Access Point 530#
```

Setting the management password:

```
ProCurve Access Point 530# configure
ProCurve Access Point 530(config)# password manager
```

Country configuration:

```
ProCurve Access Point 530(config)# country cz
```

Configuring basic data. In this sample case

- Management IP address, default GW, DNS, SNTP
- Assigning the management interface to VLAN
- Turning SSH on
-

```
ProCurve Access Point 530(config)# hostname ap-sit
ProCurve Access Point 530(config)# domain net.vutbr.cz
ProCurve Access Point 530(config)# dns primary 10.229.3.10
ProCurve Access Point 530(config)# dns secondary 10.229.3.15
ProCurve Access Point 530(config)# sntp 10.229.255.15
ProCurve Access Point 530(config)# ssh
ProCurve Access Point 530(config)# interface ethernet
ProCurve Access Point 530(ethernet)# management-vlan 504
ProCurve Access Point 530(ethernet)# ip address 10.229.255.61 255.255.255.0
ProCurve Access Point 530(ethernet)# ip default-gateway 10.229.255.1
ProCurve Access Point 530(ethernet)# exit
```

Setting up the radio. The AP has two radio ports. These ports can be configured completely independently. This example uses only radio port no. 1. The other one can be configured in the same way.

```
ProCurve Access Point 530(config)# radio  1
ProCurve Access Point 530(radio1)# channel-policy static 5
ProCurve Access Point 530(radio1)# mode g
ProCurve Access Point 530(radio1)# enable
```

SSID + vlan for web authentication (formerly used the SSID *eduroam-simple*, now uses the SSID *vutbrno*).

```
ProCurve Access Point 530(radio1)# wlan 1
ProCurve Access Point 530(radio1-wlan1)# ssid vutbrno
ProCurve Access Point 530(radio1-wlan1)# vlan 589
ProCurve Access Point 530(radio1-wlan1)# exit
```

SSID + vlan for clients authenticating via 802.1x. Setting SSID, vlan, RADIUS servers for authentication and accounting.

```
ProCurve Access Point 530(radio1)# wlan 2
ProCurve Access Point 530(radio1-wlan2)# ssid eduroam
ProCurve Access Point 530(radio1-wlan2)# vlan 578
ProCurve Access Point 530(radio1-wlan2)# radius primary key
ProCurve Access Point 530(radio1-wlan2)# radius primary ip
ProCurve Access Point 530(radio1-wlan2)# radius secondary key
ProCurve Access Point 530(radio1-wlan2)# radius secondary ip
ProCurve Access Point 530(radio1-wlan2)# radius-accounting primary key
ProCurve Access Point 530(radio1-wlan2)# radius-accounting primary ip
```

```
ProCurve Access Point 530(radio1-wlan2)# radius-accounting secondary key
ProCurve Access Point 530(radio1-wlan2)# radius-accounting secondary ip
ProCurve Access Point 530(radio1-wlan2)# security wpa-8021x
ProCurve Access Point 530(radio1-wlan2)# enable
```

Saving configuration:

```
ProCurve Access Point 530(config)# write memory
```

3 HP ProCurve 420

URL at the manufacturer's website: http://www.hp.com/rnd/products/wireless/420_series/specs.htm

This AP can only broadcast a single SSID. It is up to you if you broadcast the SSID for web authentication or for eduroam. If you decide to use the second option, your clients may not be able to connect at all.

An important note about non-broadcast networks and Windows XP is the following. Connecting to a non-broadcast network is quite tricky in Windows XP. To connect to a non-broadcast network you need to successfully connect at least once at a place where this network is broadcast. This problem is solved with a KB917021 patch. That enables an option "Connect even if the network is not broadcasting". This option will make it easier to connect even to non-broadcast networks.

Links:
* Information: http://support.microsoft.com/kb/917021
* Patch:http://www.microsoft.com/downloads/details.aspx?familyid=2726F32F-D52B-4F84-ACE8-F7FC20195769&displaylang=en

These patches can be applied only if you run Windows Genuine Advantage on your system (http://www.microsoft.com/genuine/).

The sample configuration is based on an unconfigured AP or an AP set to factory default. It describes commands entered into the CLI after connecting through a serial port. The resulting configuration can be saved into a file, but it is written into a file divided into individual segments (ini), making its reconstruction into commands fairly problematic. Furthermore, RADIUS server keys are not stored in this file, and therfore it cannot be used for bulk configuration.

Reset to factory default can be done by keeping the reset key pressed for 5-10 seconds. After the reset, you can log in as admin without any password.

```
Username: admin
Password:
HP ProCurve Access Point 420#
```

Country configuration. For some older software versions sk must be used (some channels were inaccessible for cz).

```
HP ProCurve Access Point 420#country cz
Reboot system now to make the country code change effective? : y
Reboot system...
```

Basic AP setting:

- Setting the password for the admin account.
- Enabling SSH.
- Remote logging and SNTP server

```
HP ProCurve Access Point 420#configure
Enter configuration commands, one per line.
HP ProCurve Access Point 420(config)#management
Enter management commands, one per line.
HP ProCurve Access Point 420(config-mgmt)#password-admin
HP ProCurve Access Point 420(config-mgmt)#ip ssh enable
HP ProCurve Access Point 420(config-mgmt)#end
ProCurve Access Point 530(config)# logging 10.229.255.15
ProCurve Access Point 530(config)# sntp 10.229.255.15
```

Enabling VLAN:

```
HP ProCurve Access Point 420(config)#vlan enable static
Reboot system now? : y
```

Configuring the interface management and assigning to VLAN:

```
HP ProCurve Access Point 420#config
HP ProCurve Access Point 420(config)#interface ethernet
HP ProCurve Access Point 420(if-ethernet)#no ip dhcp
HP ProCurve Access Point 420(if-ethernet)#ip address 10.229.255.61 255.255.255.0
10.229.255.1
HP ProCurve Access Point 420(if-ethernet)#end
HP ProCurve Access Point 420(config)#management-vlanid 504 tagged
```

Turing the radio on, configuring channel:

```
HP ProCurve Access Point 420(config)#interface wireless g
HP ProCurve Access Point 420(if-wireless-g)#channel 3
HP ProCurve Access Point 420(if-wireless-g)#no shutdown
```

SSID + vlan for web authentication (formerly used *eduroam-simple*, now the SSID *vutbrno* is used).

```
HP ProCurve Access Point 420(if-wireless-g)#ssid index 1
HP ProCurve Access Point 420(if-wireless-g-ssid-1)#ssid-name vutbrno
HP ProCurve Access Point 420(if-wireless-g-ssid-1)#vlan-ID 589 tagged
HP ProCurve Access Point 420(if-wireless-g-ssid-1)#primary
HP ProCurve Access Point 420(if-wireless-g-ssid-1)#end
```

SSID + vlan for clients authenticating via 802.1x. Setting SSID, vlan, radius servers for authentication.

```
HP ProCurve Access Point 420(if-wireless-g)#ssid add 2 eduroam
Create new SSID success
HP ProCurve Access Point 420(if-wireless-g)#ssid index 2
HP ProCurve Access Point 420(if-wireless-g-ssid-2)#vlan-ID 578 tagged
HP ProCurve Access Point 420(if-wireless-g-ssid-2)#radius-authentication-server
address
HP ProCurve Access Point 420(if-wireless-g-ssid-2)#radius-authentication-server
key
HP ProCurve Access Point 420(if-wireless-g-ssid-2)#radius-authentication-server
secondary address
HP ProCurve Access Point 420(if-wireless-g-ssid-2)#radius-authentication-server
secondary key
HP ProCurve Access Point 420(if-wireless-g-ssid-2)#security-suite 7 wPA-wpA2
HP ProCurve Access Point 420(if-wireless-g-ssid-2)#end
HP ProCurve Access Point 420(if-wireless-g)#end
```

And finally an adjustment of the prompt:

```
HP ProCurve Access Point 420(config)#prompt ap-sit
ap-sit (config)#
```

4   HP ProCurve Switches

In some cases, running authentication at ports is advantageous. Most state-of-the-art switches fully support 802.1x authentication. The following example describes commands for a simple configuration of HP ProCurve switch ports for access via 802.1x. The sample configuration has the following features:

- The configuration is based on the HP 2510-24 switch and it should be usable for most HP ProCurve switches. So far it was verified on 2524, 2510-24, 2626, 5406zl switches.
- The uplink is on port 26. All key VLANs lead to this port, i.e., management (VID 504), eduroam (VID 578) for users authenticated via 802.1x and vutbrno (VID 589) for clients with no support for 802.1x, i.e., authenticated via web.
- We intend to use ports 1 to 10 for connection of end users directly to Ethernet.
- PEAP is used for authentication - the protocol used for wireless networks.
- Unfortunately this device does not let you define different RADIUS servers for switch management and user authentication. Everything must be solved at the RADIUS server side with a suitable AVP extension. Otherwise the switch management could be accessible to all users, which is definitely undesirable.

Definition of vlan to manage the device and address for access to RADIUS servers:

```
ip default-gateway 10.229.255.1
vlan 504
    name "mgmt-vlan"
    ip address 10.229.255.61 255.255.255.0
    tagged 26
    exit
```

Defining VLAN for authenticated and non-authenticated access. We will not assign user ports to any VLAN.

```
vlan 589
    name "vutbrno"
    tagged 26
    exit
vlan 578
    name "eduroam"
    untagged 1-10
    tagged 26
    exit
```

Definition of the type of authentication method used (EAP) and RADIUS servers:

```
aaa authentication port-access eap-radius radius-server host <radius1_server>
key <radius1_key> radius-server host <radius2_server> key <radius2_key>
```

Turning on authentication at relevant user ports and assigning to VLAN for authenticated and non-authenticated access:

```
aaa port-access authenticator 1-10
aaa port-access authenticator 1-10 auth-vid 578
aaa port-access authenticator 1-10 unauth-vid 589
aaa port-access authenticator active
```

The *show port-access authenticator* command lets you display the client status at individual ports:

```
hp(config)# show port-access authenticator

Port Access Authenticator Status

Port-access authenticator activated [No] : Yes

            Current
  Port Status VLAN ID
  ------------------
  1     Closed 589
  2     Closed 1
  3     Closed 589
  4     Closed 1
  5     Open   578
  6     Closed 1
  7     Closed 1
  8     Closed 1
  9     Closed 1
  10    Closed 1
```

Non-authenticated clients are assigned to the vutbrno VLAN (VID 589) at ports 1 and 3. An authenticated client is correctly connected and assigned to the eduroam VLAN (VID 578) at port 5.

More Best Practice Documents are available at www.terena.org/campus-bp/
....
campus-bp-announcements@terena.org