Configuration of HP ProCurve Devices in a Campus Environment

Best Practice Document

Produced by CESNET led working group
on Network monitoring
(CBPD111)

Authors: Tomas Podermanski, Vladimir Zahorik
March 2010

Document No: GN3-NA3-T4-CBPD111
Version / date: March 2010
Original language: Czech
Original title: “Configuration of HP ProCurve Devices in a Campus Environment”
Original version / date: Version 1.2 of 3 December 2009
Contact: tpoder@cis.vutbr.cz, zahorik@cis.vutbr.cz

CESNET bears responsibility for the content of this document. The work has been carried out by a CESNET led working group on Network monitoring as part of a joint-venture project within the HE sector in the Czech Republic.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 23 8875, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3)'.


Table of Contents

Executive Summary

This document describes the basic configuration of HP switches in a campus environment. Switches have a fairly large number of configuration options. Only a subset of these options is usually used for an ordinary configuration. This document attempts to summarise the most common settings of the ProCurve switches as they are used in campus networks. The individual configuration examples are arranged to let you cut and paste them while configuring a real switch.

1 Basic Settings and Operations

1.1 Switch Access

The switches in the HP ProCurve series feature several configuration interfaces - web interface, console command line, and interactive menu. The command line and interactive menu are accessible through:

- console port (RS 232 line),
- telnet protocol
- ssh protocol

The command line which can configure all switch parameters is used in all examples below. In many ways management is similar to the Cisco IOS configuration, although there are significant differences.

1.2 Resetting to Factory Default

The first three steps are needed only if you do not know the switch access console password. If you want to cancel the current configuration only and you know the access password, you may omit these steps.

Find the *Clear* and *Reset* buttons on the switch. Press and hold both buttons until the Power and Fault indicators light up.

1. Continue to hold the *Clear* button pressed and release the *Reset* button.
2. Release the *Clear* button when the Self Test indicator starts blinking.
3. The switch is now ready in a factory default configuration.
4. Now you need to run the following command:

```
# erase startup-config
```

   and reboot the switch.

1.3 Firmware Upgrade

Firmware upgrade is a very important step. Always check if a newer firmware version has been released before installing new firmware. The development of firmware for HP switches is quite intensive and new versions with fixes tend to be released relatively often (about every four months). Currently switch firmware is available for free on a website.

Recommendation:
Always look for new firmware releases for your switches. Always use the newest version available for new installations if nothing prevents it.

The switch firmware is stored in the switch flash memory. All switches have a primary and a secondary flash memory. Firmware updates should therefore be done using alternately the primary and secondary flash memory. With this procedure you will always be able to return to the previous version in case of any unexpected problems.

Recommendation:
Use primary and secondary flash memory alternately to update the switch firmware.

The following example assumes that the firmware is stored on your TFTP server and that the TFTP server is accessible through the IP protocol from the switch. In this example the TFTP server address is 10.229.255.15 and the firmware is stored in the file *hp-img/hp54xx/K_14_41.swi* .

We list the flash memory contents

```
hp-test# show flash
Image           Size(Bytes)   Date   Version
-----           ----------  -------- -------
Primary Image   : 9798890   08/27/09 K.14.19
Secondary Image : 7544081   02/26/09 K.13.58
Boot Rom Version: K.12.20
Default Boot    : Primary
```

We verify the TFTP server accessibility

```
hp-test# ping 147.229.255.15
  147.229.255.15 is alive, time = 1 ms
```

The image is now loaded into the secondary flash - confirm the operation by pressing the "y" key. The whole operation takes a few minutes.

```
hp-test# copy tftp flash 147.229.255.15 hp-img/hp54xx/K_14_41.swi secondary
The Secondary OS Image will be deleted, continue [y/n]?  y
....
```

```
Validating and Writing System Software to the Filesystem ...

hp-test#
```

We reboot the switch and choose the secondary flash for the next boot.

```
hp-test# boot system flash secondary

System will be rebooted from secondary image. Do you want to continue [y/n]? y
```

The time that the switch needs to reboot varies by the type of device. It finishes in about one minute for smaller models. However it should not take more than 7 minutes.

We run a repeated check after the boot:

```
hp-test# show flash
Image           Size(Bytes)   Date   Version
-----           ----------  -------- -------
Primary Image   : 9798890   08/27/09 K.14.19
Secondary Image : 7544081   02/26/09 K.14.41
Boot Rom Version: K.12.20
Default Boot    : Secondary

hp-test#
hp-test# show version
Image stamp:    /sw/code/build/btm(t4a)
                Aug 27 2009 05:27:43
                K.14.41
                476
Boot Image:     Secondary
```

1.4 Setting Hostname

```
HP ProCurve 5406zl(config)# hostname hp-test.mgmt.net.vutbr.cz
hp-test.mgmt.net.vutbr.cz(config)#
```

The full domain name of the device can be used as the hostname. If all devices are located in the same administrative domain, then a name without a domain suffix can be used. This will give us a shorter command line prompt, resulting in easier entry of some commands.

```
HP ProCurve 5406zl(config)# hostname hp-test
hp-test (config)#
```

1.5 Setting Passwords

This command will set the basic switch passwords for access by administrators and operators. The switch management has no user administration features and only one password can be set for access by both administrators and operators. Radius servers must be used for authentication if more advanced user administration is required.

In HP devices, a special area that is not readily accessible is used to store passwords. Therefore password settings are not visible in the switch configuration file.

```
hp-test(config)# password all
New password for operator: *******
Please retype new password for operator: *******
New password for manager: *******
Please retype new password for manager: *******
hp-test (config)#
```

Recommendation:
It is advisable to use radius servers for managing users and passwords for authentication. Use passwords set at the switch for emergency access only.

1.6 Time Zone

```
hp-test(config)# time timezone 60
hp-test(config)# time daylight-time-rule Western-Europe
```

1.7 Time Servers

```
hp-test(config)# sntp server 10.229.255.15
hp-test(config)# sntp server priority 1 10.229.255.15
hp-test(config)# timesync sntp
hp-test(config)# sntp unicast
hp-test(config)# sntp 300
```

1.8 Default Gateway

The default gateway can be set only if routing capability is not activated on the switch.

```
hp-test(config)# ip default-gateway 10.229.255.1
```

1.9 Switch Management Access Addresses

If these ranges are not set, the active device can be managed from any address. This applies to access via web, telnet, ssh, and SNMP.

```
hp-test(config)# ip authorized-managers 10.229.3.0 255.255.255.0
hp-test(config)# ip authorized-managers 10.229.240.0 255.255.240.0
```

Recommendation:
When configuring the switch do not forget to limit the management access to the selected network ranges.

Caution:
If you use an IPv6 address to manage the switch, you must not forget to set IPv6 management access restrictions for the switch.

```
hp-test(config)# ipv6 authorized-managers 2001:718:802:3::93e5:30f
ffff:ffff:ffff:ffff::0
```

1.10 Remote Logging

Event logging via the syslog protocol. This command sets the remote server address.

```
hp-test(config)# logging 10.229.255.15
hp-test(config)# logging facility local0
```

Recommendation:
Log events from all switches in the network that you manage on a common syslog server.

1.11 Basic SNMP Configuration

The example configuration assumes setting SNMPv1 and SNMPv2c for reading. This configuration is sufficient for most monitoring applications. We simultaneously set up SNMP traps to addresses 10.229.255.14 and 10.229.255.15.

```
hp-test(config)# snmp-server host 10.229.255.14 "public"
hp-test(config)# snmp-server community "public" manager restricted
```

By default, for HP switches the public community is set to unrestricted. This means that it is possible to write data to the MIB tree via SNMPv2.

Recommendation:
Always verify the switch settings and set the access to restricted. Preferably use SNMPv3 if you want to write to relevant parts of the MIB tree, or at least set a different community string and limit access to the switch management with the *ip authorized-managers* setting.

1.12 Authentication by Radius Servers

Authentication by radius servers can be used for switch management access authentication. Radius server services can also be used to authenticate users for the 802.1x protocol. Only one common set of radius servers can be used to access the management and authenticate users.

Definition of radius servers and encryption key:

```
hp-test(config)# radius-server host 10.229.255.15 key secret_password1
hp-test(config)# radius-server host 10.229.255.14 key secret_password2
```

If radius servers are used only to verify access to management, it is recommended to set the following parameters:

```
hp-test(config)# radius-server timeout 1
hp-test(config)# radius-server retransmit 1
```

If the radius servers are inaccessible for some reason (which is often why you need to access the switch management), the number of repetitions and timeouts are minimised. Thanks to these parameters, the login delay will not be unnecessarily long and the switch will start verifying your login data through the internal switch password sooner.

Next you need to configure services that should be authenticated by the radius server. Here we configure the authentication method for console access, web, telnet, and ssh access. The authentication method is configured separately for the login itself and for entering the privileged mode. Define the primary and secondary authentication method as the command parameters. In the example below the switch tries to authenticate by the radius server at first and if this fails it authenticates the login data by the internal password of the switch.

```
hp-test(config)# aaa authentication console login radius local
hp-test(config)# aaa authentication console enable radius local
hp-test(config)# aaa authentication telnet login radius loca
hp-test(config)# aaa authentication telnet enable radius local
hp-test(config)# aaa authentication web login radius local
hp-test(config)# aaa authentication web enable radius local
hp-test(config)# aaa authentication ssh login radius local
hp-test(config)# aaa authentication ssh enable radius local
```

To make the login process easier it is possible to let the switch enter the privileged mode upon the first login. The administrator accessing the switch does not need to re-enter the login data to enter the privileged mode (the enable command). This must be allowed on the switch by the following command:

```
hp-test(config)# aaa authentication login privilege-mode
```

The radius server side must deliver the following attribute upon login:

```
Service-TYPE = Administrative-User
```

The resulting user definition for FreeRadius may look like this:

```
"admin-user"   Auth-Type := System
   Service-TYPE = Administrative-User
```

1.13 SSH to Access the Switch Management

Before turning on the SSH service, you must generate the private and public keys for SSH. The command to generate the key varies according to the switch type.

HP26xx, HP28xx, HP6108, HP2510-xx, HP54xx, HP3500, HP6600:

```
hp-test(config)# crypto key generate ssh
```

For hp2524:

```
hp-test(config)# crypto key generate
```

To turn the SSH service on:

```
hp-test(config)# ip ssh
```

1.14 Limiting Access via Insecure Protocols

The default switch configuration runs services that allow access to the switch management via insecure protocols, namely the telnet and http protocols. The telnet protocol may be replaced by the SSH service, and the http protocol may be replaced by the https protocol.

```
hp-test(config)# no web-management plaintext
hp-test(config)# no telnet-server
```

Recommendation:
Disable access to the switch via insecure protocols, i.e. telnet and http, if possible.

2 L2 Configuration

2.1 Setting the Communication Parameters of the Switch Port

2.1.1 Speed and Communication Parameters

Switch port parameter configuration is done in the interface context.

```
hp-test(config)# interface b1
hp-test(eth-B1)# name "server_1"
hp-test(eth-B1)# exit

hp-test(config)# interface b1-b24
hp-test(eth-B1-B24)# speed-duplex 100-full
hp-test(eth-B1-B24)# speed-duplex 1000-full
hp-test(eth-B1-B24)# speed-duplex auto-10
hp-test(eth-B1-B24)# speed-duplex auto-100
hp-test(eth-B1-B24)# speed-duplex auto-1000
hp-test(eth-B1-B24)# speed-duplex auto-10-100
hp-test(eth-B1-B24)# exit
```

The speed-duplex parameter can configure the port communication parameters. Contrary to common practice, the port can be configured to modes such as auto-10, auto-100 etc. This configuration sets the port to the desired speed, but speed auto detection remains active for the port. This may be useful for e.g. limiting the port speed for some users or devices.

2.1.2 Port Trunking, LACP

The first step consists of creating a virtual interface (*TrkXX*) and assigning physical ports to it. A port may be created either via the trunk mode (simple packet broadcasting through assigned ports with the round robin algorithm) or *LACP* protocol management.

```
hp-test(config)# trunk b1-b4 trk1 trunk
```

or

```
hp-test(config)# trunk b1-b4 trk1 lacp
```

Displaying port status:

```
hp-test(config)# show trunks

 Load Balancing

  Port | Name                                Type      | Group  Type
  ---- + ---------------------------------- --------- + ------ --------
  B1   | server_1                                      | Trk1   LACP
  B2   | server_2                                      | Trk1   LACP
  B3   | server_3                                      | Trk1   LACP
  B4   | server_4                                      | Trk1   LACP


hp-test(config)# show lacp

                          LACP

   PORT   LACP      TRUNK     PORT      LACP      LACP
   NUMB   ENABLED   GROUP     STATUS    PARTNER   STATUS
   ----   -------   -------   -------   -------   -------
   B1     Active    Trk1      Down      No        Success
   B2     Active    Trk1      Down      No        Success
   B3     Active    Trk1      Down      No        Success
   B4     Active    Trk1      Down      No        Success
```

Recommendation:
Preferably use the LACP protocol for link aggregation.

2.1.3 Broadcast Limit

The broadcast limit can be set individually for each physical interface. The parameter is configured as a percentage rate of the total port bandwidth.

```
hp-test(config)# interface b2-b10
hp-test(eth-B2-B10)# broadcast-limit 20
```

Recommendation:
During normal operations the broadcast limit should be configured for all ports to which end users are connected.

2.1.4 Spanning Tree

Spanning Tree is a protocol used to discover loops in switched networks and to remove such loops.

To turn on STP on the switch:

```
hp-test(config)# spanning-tree
```

Because of the slow convergence of the STP protocol it is advisable to use the Rapid Spanning Tree Protocol. To switch to RSTP:

```
hp-test(config)# spanning-tree force-version rstp-operation
```

Recommendation:
The STP (RSTP) support should be activated on all switches. This setting can prevent network congestion if the network was accidentally looped (e.g. by connecting two network sockets in one office together).

The RSTP configuration is analysed in more detail in a separate document ‘Resilient Campus Networks’.

2.1.4.1 *Bpdu Filtration*

Bpdu can be filtered at the level of individual switch ports. Configuration is done in the following way:

```
hp-test(config)# spanning-tree b1-b24 bpdu-filter
hp-test(config)# spanning-tree b1-b24 bpdu-protection
```

2.1.4.2 *Setting Access Permissions According to 802.1x*

Port based variant. Authorisation at radius servers is identical with access to the eduroam network. The “eduroam” VLAN is used for successful authorisation; otherwise the “vutbrno” VLAN is used.

```
vlan 589
   name "vutbrno"
   no ip address
   tagged 26
   exit
 vlan 578
   name "eduroam"
   no ip address
   tagged 26
   exit
 aaa authentication port-access eap-radius
 radius-server host 10.229.3.92 key iSa8djSda
 radius-server host 10.229.252.12 key iSa8djSda
 aaa port-access authenticator 1-10
```

```
aaa port-access authenticator 1 auth-vid 578
aaa port-access authenticator 1 unauth-vid 589
aaa port-access authenticator 2 auth-vid 578
aaa port-access authenticator 2 unauth-vid 589
aaa port-access authenticator 3 auth-vid 578
aaa port-access authenticator 3 unauth-vid 589
...
aaa port-access authenticator 10 auth-vid 578
aaa port-access authenticator 10 unauth-vid 589
aaa port-access authenticator active
aaa port-access 1-10
```

2.1.5 Discovery of Physical Topology (LLDP, CDP)

LLDP (Local Link Discovery Protocol) and CPD (Cisco Discovery Protocol) are protocols for automated detection of physical connections between switches. The outputs of this detection tend to be used in supervisory management systems to create a map of physical connections.

Both protocols run automatically for most switches and additional configuration is needed only if you want to suppress one of these protocols. To turn the protocols off:

```
hp-test(config)# no cdp run
hp-test(config)# no lldp run
```

In some cases we may want to limit the LLDP and CDP broadcasting to some ports only.

HP26xx, HP28xx, HP6108, HP54xx, ... :

```
hp-test(config)# lldp admin-status a1,a24 txonly
hp-test(config)# no cdp enable a1
```

HP25xx:

```
hp-test(config)# lldp admin-status 1-24 disable
hp-test(config)# no cdp enable a1
```

In some cases we may want to limit the broadcasting of some LLDP items only.

```
hp-test(config)# no lldp config A1 basicTlvEnable port_descr
hp-test(config)# no lldp config A1 basicTlvEnable system_name
hp-test(config)# no lldp config A1 basicTlvEnable system_descr
hp-test(config)# no lldp config A1 basicTlvEnable system_cap
hp-test(config)# no lldp config A1 dot3TlvEnable macphy_config
hp-test(config)# no lldp config A1 medTlvEnable network_policy
hp-test(config)# no lldp config A1 medTlvEnable location_id
```

```
hp-test(config)# no lldp config A1 medTlvEnable poe
hp-test(config)# no lldp config A1 medTlvEnable capabilities
hp-test(config)# no lldp config A1 dot1TlvEnable port-vlan-id
```

How to relaunch the protocol:

```
hp-test(config)# cdp run
hp-test(config)# lldp run
```

HP26xx, HP28xx, HP6108, HP54xx, ... :

```
hp-test(config)# lldp admin-status ethernet 1-26 tx_rx
hp-test(config)# lldp enable-notification ethernet 1-26
hp-test(config)# cdp enable 1-26
```

HP25xx:

```
hp-test(config)# lldp admin-status ethernet 1-26 enable
hp-test(config)# cdp enable 1-26
```

To display information about the other party:

```
hp-test# show lldp info remote-device

 LLDP Remote Devices Information

  LocalPort | ChassisId                 PortId PortDescr SysName
  --------- + ------------------------- ------ --------- ----------------------
  A6        | 00 21 f7 5d 24 00         6      A6        hp-test2
  A7        | 00 1c 2e 91 78 80         24     24        hp-test3
  A8        | 00 1c 2e 44 0c 40         23     23        hp-test4
  A23       | 00 1f fe 1f a5 40         14     14        hp-antL2
  A24       | 00 18 71 e1 20 00         20     A20       hp-ant

hp-test# show cdp neighbors

 CDP neighbors information

 Port Device ID                    | Platform                    Capability
 ---- ---------------------------- + --------------------------- -----------
 A6   00 21 f7 5d 24 00            | ProCurve J8697A Switch 54... R S
 A7   00 1c 2e 91 78 80            | ProCurve J8692A Switch 35... S
 A8   00 1c 2e 44 0c 40            | ProCurve J9019A Switch 25... S
 A23  00 1f fe 1f a5 40            | ProCurve J9049A Switch 29... S
 A24  00 18 71 e1 20 00            | ProCurve J8697A Switch 54... R S
```

Recommendation:
Only suppress the LLDP or CDP information broadcasting when it is really necessary.

2.2 VLAN Configuration

2.2.1 Assigning Ports to VLAN

Create a new VLAN and assign a description

```
hp-test(config)# vlan 666
hp-test(vlan-666)# name "test-vlan"
```

Assign a port to a VLAN – with a 802.1q tag and without a tag

```
hp-test(vlan-666)# tagged b1-b7
hp-test(vlan-666)# untagged b8-b10
```

Displaying the ports assigned to a VLAN:

```
hp-test(vlan-666)# show vlans 666
hp-test(vlan-666)# show vlans test-vlan
```

Setting ports to a mode in which VLANs learn automatically, based on information obtained with the GVRP protocol. This is the default setting of all ports.

```
hp-test(vlan-666)# auto b8-b10
```

Status and Counters - VLAN Information - VLAN 666

```
VLAN ID : 666
Name : test-vlan
Status : Port-based
Voice : No
Jumbo : No
Port Information Mode     Unknown VLAN Status
--------------- -------- ------------ ----------
B1              Tagged   Learn        Down
B2              Tagged   Learn        Down
B3              Tagged   Learn        Down
B4              Tagged   Learn        Down
B5              Tagged   Learn        Down
```

```
B6              Tagged   Learn        Down
B7              Tagged   Learn        Down
B8              Untagged Learn        Down
B9              Untagged Learn        Down
B10             Untagged Learn        Down
```

Displaying VLANs to which the relevant port is assigned:

```
hp-test(vlan-666)# show vlans ports b10

 Status and Counters - VLAN Information - for ports B10

  VLAN ID Name                | Status     Voice Jumbo
  ------- ------------------- + ---------- ----- -----
  666     test-vlan           | Port-based No    No
```

2.2.2 GVRP - Automatic VLAN Broadcasting

The GVRP protocol simplifies network configuration. It lets you automatically create VLAN definitions on switches and automatically assign ports based on information obtained from neighbour switches. This is advisable especially when combined with a protocol to remove ethernet loops - STP, RSTP.

Caution:
The GVRP protocol provides VLAN information broadcasting only. It does not contain tools to remove loops in topology.

Turning GVRP on:

```
hp-test(vlan-666)# gvrp
```

With the default setting the switch will create new VLANs and assign switch ports to relevant VLANs based on information obtained from GVRP.

Caution:
Enabling GVRP in existing installations may bring unexpected consequences. Always activate GVRP after a careful preparation and analysis of possible consequences.

VLANs that were created on the switch through GVRP can be displayed with the following command:

```
hp-test# show vlans

 Status and Counters - VLAN Information

  Maximum VLANs to support : 256
  Primary VLAN : DEFAULT_VLAN
```

```
 Management VLAN :

 VLAN ID Name                 | Status     Voice Jumbo
 ------- -------------------- + ---------- ----- -----
 1       DEFAULT_VLAN         | Port-based No    No
 224     int224               | Port-based No    No
 504     mgmt-vlan            | Port-based No    No
 614     GVRP_614             | Dynamic
 666     test-vlan            | Port-based No    No
```

The VLAN is marked in the status item as Dynamic and it is named GVRP_614.

Ports assigned to the relevant VLAN can be displayed with *show vlans <vlan_id>*

```
hp-test# show vlans 614

 Status and Counters - VLAN Information - VLAN 614

 VLAN ID : 614
 Name : GVRP_614
 Status : Dynamic
 Voice :
 Jumbo :

 Port Information Mode     Unknown VLAN Status
 --------------- -------- ------------ ----------
 A6              Auto     Learn        Up
```

Switch ports cannot be statically assigned to a VLAN learned in this way. This can be done by converting a dynamically created VLAN to static mode. This can be executed with a *static-vlan* command. The following example will convert VLAN 614 to static mode and the B24 gets assigned to this VLAN.

```
hp-test(config)# static-vlan 614
hp-test(config)# vlan 614
hp-test(vlan-614)# name "vlan descr"
hp-test(vlan-614)# untagged b24
hp-test(vlan-614)# exit

hp-test(config)# show vlans 614

 Status and Counters - VLAN Information - VLAN 614

 VLAN ID : 614
 Name : vlan descr
 Status : Port-based
 Voice : No
 Jumbo : No
```

```
Port Information Mode     Unknown VLAN Status
---------------- -------- ------------ ----------
A6               Auto     Learn        Up
B24              Untagged Disable      Down
```

GVRP should be active only on those port switches for which you expect a connection to the network infrastructure. It is advisable to limit GVRP on ports that connect terminal devices.

```
hp-test(config)# interface b1-b24
hp-test(eth-B1-B24)# unknown-vlans disable
```

The command above will suppress GVRP on ports B1 to B24.

Recommendation:
Always disable GVRP for connecting terminal devices.

For switches that are not intermediate ones (typically end switches to connect users) and for which you cannot expect mere VLAN transport, the learning of VLAN from ports should be limited. This process can be configured separately for each port.

```
hp-test(config)# interface b1-b24
hp-test(eth-B1-B24)# unknown-vlans block
```

Caution:
Different types of switches support different numbers of VLANs on switches. If this number is exceeded, then no further VLANs can be created either statically or through GVRP. Network topology and configuration of switches for transit transport must be selected according to the total number of VLANs expected.

2.2.3 IGMP Configuration

IGMP snooping support can be turned on selectively for each VLAN. To turn on the support:

```
hp-test(config)# vlan 614
hp-test(vlan-614)# ip igmp
```

IGMP status and the list of processed groups can be displayed with the *show ip igmp* command

```
hp-test(config)# show ip igmp 614

 Status and Counters - IP Multicast (IGMP) Status
```

```
VLAN ID : 614
VLAN Name : vlan descr
Querier Address : This switch is Querier

 Active Group Addresses Reports Queries Querier Access Port
 ---------------------- ------- ------- ------------------
 224.0.1.60             15222   0
 233.4.200.11           177585  0
 239.255.255.250        7057    0
 239.255.255.253        86354   0
```

Recommendation:
Always activate IGMP snooping on all VLANs of the switch unless you have reason not to.

2.2.4 MLD Snooping

Similarly to IGMP snooping you can activate MLD snooping on each VLAN

```
hp-test(config)# vlan 614
hp-test(vlan-614)# ipv6 mld
```

and display its status

```
hp-test(config)# show ipv6 mld vlan 614
  MLD Service Protocol Info

  VLAN ID : 614
  VLAN Name : vlan descr
  Querier Address : ::
  Querier Up Time : 0h:0m:0s
  Querier Expiry Time : 0h:0m:0s
  Ports with multicast routers :

  Active Group Addresses                    Type ExpiryTime Ports
  ----------------------------------------- ---- ---------- --------------------
```

Recommendation:
Always activate MLD snooping on all VLANs of the switch unless you have reason not to.

2.2.5 DHCP Snooping

First you need to activate DHCP snooping and prepare a list of authorised servers:

```
hp-test(config)# dhcp-snooping
hp-test(config)# dhcp-snooping authorized-server 10.229.206.2
hp-test(config)# dhcp-snooping authorized-server 10.229.208.2
hp-test(config)# dhcp-snooping authorized-server 10.229.212.2

hp-test(config)# interface b2-b10
hp-test(eth-B2-B10)# dhcp-snooping trust
```

Recommendation:
Configure DHCP snooping on all interfaces intended to connect end users.

2.2.6 Access Lists

Access lists can be associated with physical interfaces or VLAN.

```
hp-test(config)# ip access-list extended "test-acl"
hp-test(config-ext-nacl)# 10 permit tcp host 147.229.3.10 any eq 80
hp-test(config-ext-nacl)# 11 permit tcp host 147.229.3.11 any eq 80
```

Connecting an access list with an interface:

```
hp-test(eth-B1)# interface trk1
hp-test(eth-Trk1)# ip access-group test-acl in
```

or with a VLAN:

```
hp-test(config)# vlan 614
hp-test(vlan-614)# ip access-group test-acl in
hp-test(vlan-614)# ip access-group test-acl out
```

Caution:
The empty access list lets all rules through. If at least one rule is assigned to the access list, all packets that do not match any access list rule are discarded.

3 Basic L3 Configuration

This section describes only the basic L3 configuration of the switch.

3.1 Configuring IP Addresses on VLAN

```
hp-test(config)# vlan 614
hp-test(vlan-614)# ip address 147.229.244.1/24
```

3.2 Configuring Routing

The following example shows the basic routing configuration. It assumes only a simple case where the router is assigned to OSPF in one area only.

Turning unicast routing on

```
hp-test(config)# ip routing
```

Caution:
The *ip default-gateway* option is disabled when the *ip routing* option has been activated.

3.3 Static Routing

```
hp-test(config)# ip route 147.229.244.0/24 147.229.254.43
```

3.4 Assigning to OSPF

```
hp-test(config)# vlan 240
hp-test(vlan-240)# ip ospf area 0.0.0.2
hp-test(vlan-240)# ip ospf passive

hp-test(config)# router ospf redistribute connected
hp-test(config)# router ospf redistribute static

hp-test(config)# router ospf restrict 10.0.0.0 255.0.0.0
hp-test(config)# router ospf restrict 172.16.0.0 255.240.0.0
hp-test(config)# router ospf restrict 192.168.0.0 255.255.0.0
```

Recommendation:
For terminating networks never forget to configure passive interface or use redistribution of connected networks.

3.5 DHCP Relay

Forwarding DHCP requests from the relevant network to a remote DHCP server is configured as a VLAN parameter. The DHCP server addresses must be set separately for each network (VLAN).

```
hp-test(config)# vlan 614
hp-test(vlan-614)# ip helper-address 147.229.3.10
hp-test(vlan-614)# ip helper-address 147.229.4.20
```

3.6 Multicast Routing

PIM can be run in SM or DM mode on HP switches. For SM mode a Rendezvous Point can be created on the switch. However, the MSDP protocol does not support the exchange of global multicast information.

Multicast routing support must be turned on first.

```
hp-test(config)# ip multicast-routing
hp-test(vlan-614)# router pim
hp-test(pim)# exit
```

3.6.1 PIM Dense Mode

If you want to use PIM-DM, the protocol must be turned on on individual networks (VLANs).

```
hp-test(config)# vlan 614
hp-test(vlan-614)# ip igmp
hp-test(vlan-614)# ip pim-dense
hp-test(vlan-614-pim-dense)# exit
```

3.6.2 PIM - Rendezvous Point (RP)

The configuration is more complicated for PIM-SM. If a rendezvous point (RP) is not created in the network it must be created first on one of the switches. RP is always connected to a VLAN and IP address. Such VLAN must be set in the RP configuration with the *source-ip-vlan* command.

```
hp-test(config)# router pim
hp-test(pim)# rp-candidate
hp-test(pim)# rp-candidate source-ip-vlan 525
hp-test(pim)# rp-candidate group-prefix 224.0.0.0 240.0.0.0
hp-test(pim)# exit
```

The Boot Strap protocol (BSR) is suitable to spread information about RP. It must be configured on the same switch and same VLAN as RP.

```
hp-test(config)# router pim
hp-test(pim)# bsr-candidate
hp-test(pim)# bsr-candidate source-ip-vlan 525
hp-test(pim)# bsr-candidate priority 10
```

3.6.3 PIM Sparse Mode

The configuration in the terminal VLAN on the terminal switch side is similar (Designated Router – DR) to PIM-DM.

```
hp-test(config)# vlan 614
hp-test(vlan-614)# ip igmp
hp-test(vlan-614)# ip pim-sparse
hp-test(vlan-614-pim-sparse)# exit
```

Caution:
Either the dense or the sparse mode of the PIM protocol can be activated on a switch. Combination of both modes in different networks for a single switch is not possible.

3.6.4 Displaying Information about the PIM protocol

Use the *show ip pim* command to display the protocol status.

Displaying neighbour PIM routers

```
hp-tech# show ip pim neighbor

 PIM Neighbors

  IP Address      VLAN Up Time (sec)      Expire Time (sec)
  --------------- ---- ------------------ ------------------
  147.229.253.246 561  1806726            99
  147.229.254.65  529  930341             104
  147.229.254.122 528  1806726            95
  147.229.254.141 565  1806726            84
  147.229.254.222 567  1806727            89
  147.229.254.226 533  64526              84
```

Information about RP obtained through the BSR protocol:

```
hp-tech# show ip pim rp-set

 Status and Counters - PIM-SM Static RP-Set Information

  Group Address   Group Mask      RP Address      Override
  --------------- --------------- --------------- --------


 Status and Counters - PIM-SM Learned RP-Set Information

  Group Address   Group Mask      RP Address      Hold Time Expire Time
  --------------- --------------- --------------- --------- ---------------
  224.0.0.0       240.0.0.0       147.229.254.6   150       114
```

Displaying the multicast routing table:

```
hp-kol# show ip mroute

 IP Multicast Route Entries

  Total number of entries : 46

  Group Address   Source Address  Neighbor        VLAN
  --------------- --------------- --------------- ----
  224.2.127.254   147.229.10.46   147.229.252.121 621
  224.2.127.254   147.229.10.56   147.229.252.121 621
  226.22.36.120   147.229.10.46   147.229.252.121 621
  226.22.36.123   147.229.10.76   147.229.252.121 621
  226.22.36.124   147.229.10.86   147.229.252.121 621
  233.4.200.11    147.229.192.2   147.229.252.114 619
```

```
  233.4.200.11    147.229.196.2   147.229.252.114 619
  233.4.200.11    147.229.200.2   147.229.252.121 621
  233.4.200.11    147.229.205.2   147.229.252.121 621
  ....
```

3.6.5 Securing the Multicasting Operation

If you run a multicasting operation in your network, this kind of operation should be suitably secured at the terminal networks. Fully open multicasting operation could present security risks.

The following access list associated with a terminal network can be a securing example.

```
ip access-list extended "deny-mcast"
   100 remark "Allow broadcasts"
   100 permit ip 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
   200 remark "enable IGMP – allow users to joun into a group"
   200 permit igmp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
   300 remark "Application – multicast monitoring"
   300 permit udp 0.0.0.0 255.255.255.255 233.4.200.11 0.0.0.0 eq 2220
   400 remark "Application - Messenger"
   400 permit ip 0.0.0.0 255.255.255.255 224.1.0.1 0.0.0.0
   500 remark "Application – Stream server"
   500 permit ip 10.229.3.10 255.255.255 224.1.0.12 0.0.0.0
   1000 remark "The rest of the multicast traffic -> deny"
   1000 deny ip 0.0.0.0 255.255.255.255 224.0.0.0 15.255.255.255 log
   1000 remark "Allow other unicast trafic. "
   6500 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
   exit
```

This access list enables users to receive any group. It prevents the spread of multicasting data by ordinary stations. Only selected groups (used by all users) and stream servers are permitted.

The access list should also be associated with all terminal VLANs

```
  vlan 130
     ip access-group "deny-mcast" vlan
     exit
  vlan 140
     ip access-group "deny-mcast" vlan
     exit
```

Recommendation:
Always secure the multicast operation in a suitable way, so that it cannot be a target of attacks.

4 Auxiliary Tools

4.1 Automated Configuration Download

This script enables an automatic loading of current switch configuration over SSH. This script can be used for tasks such as regular configuration download for archival.

upload-hp (http://hawk.cis.vutbr.cz/~tpoder/GN3/HPCookBook/upload-hp)

4.2 Tech Information Download

This script is used to download tech outputs automatically. It can be useful if you report device hardware or software faults.

getdiag.pl (http://hawk.cis.vutbr.cz/~tpoder/GN3/HPCookBook/getdiag.pl)

4.3 Monitoring Devices

The following file contains a template for the zabbix system (http://www.zabbix.com/). Data about individual switch sensors are checked. Sensors include fan statuses, power supply statuses and chassis temperature. Collected data also include CPU load, allocated memory and device serial number.

HPProcurve_zabbix.xml (http://hawk.cis.vutbr.cz/~tpoder/GN3/HPCookBook/HPProcurve_zabbix.xml)