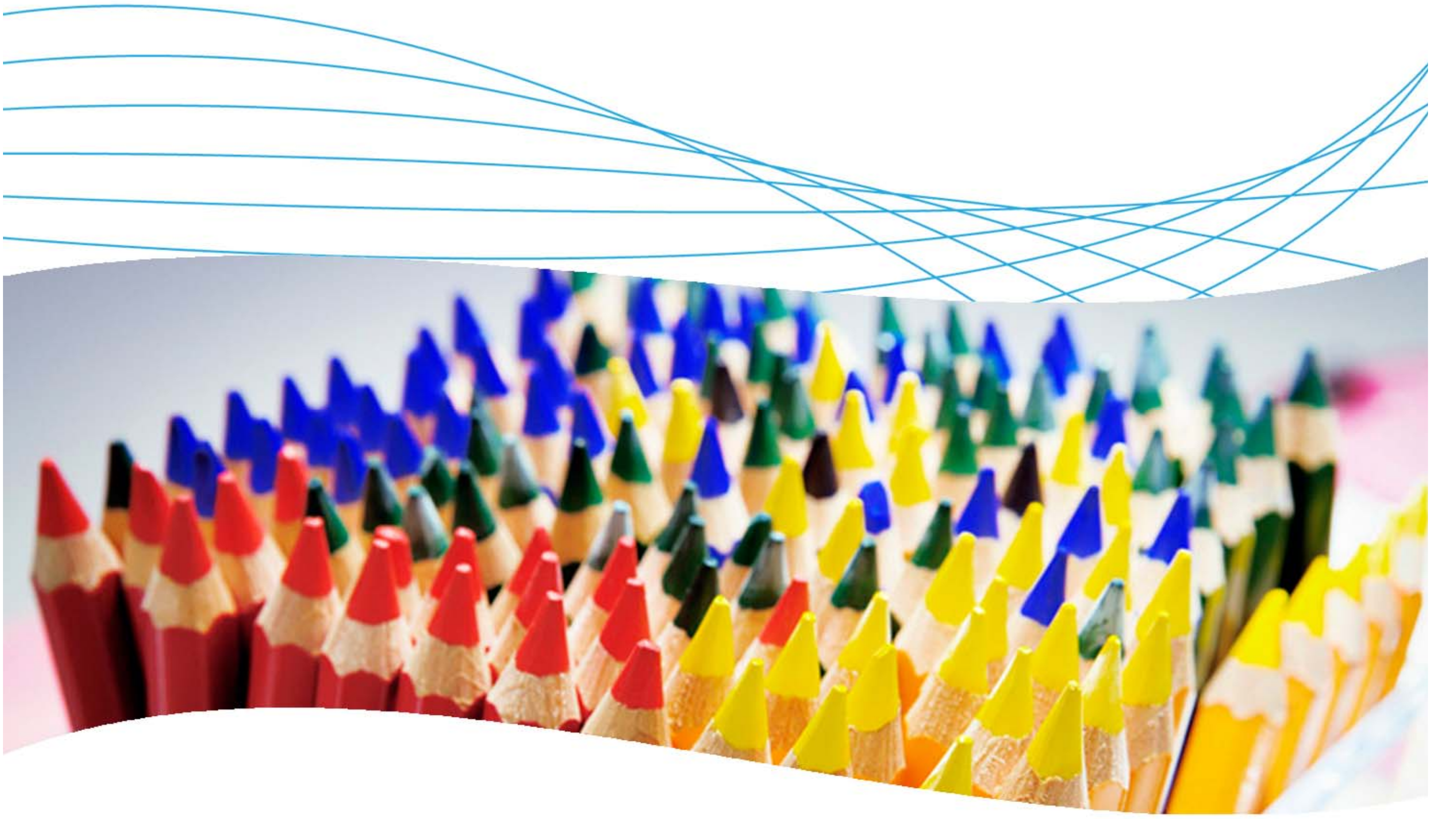
An HP ProCurve Networking Application Note

How to configure Virus Throttle on ProCurve switches



Contents

1. Introduction

This application note explains configuration of HP Virus Throttle (connection rate filtering) on ProCurve switches.

This details the operation of the new version of Virus Throttle. Until the K.12.01 release, Virus Throttle on a ProCurve switch was able to detect virus-like network behavior—identified as a high number of connections to a high number of different IP addresses in a short time—and to prevent the traffic from the originating source from being routed. Thus, in a network with multiple VLANs, an infected machine could only contact other systems in its own VLAN. This was Virus Throttle at layer 3.

Beginning with the K.12.01 release, the switch is now able to block traffic from an infected machine even within a VLAN: if a virus is detected, within a few seconds, the infected system cannot reach any other IP address. This new capability is more efficient and effective, and increases network protection against viruses.

General steps for configuration of Virus Throttle have not changed:

1. You first specify the “sensitivity” of the filter you want to apply; you have a choice of low, medium, high, or aggressive throttling.
2. Then you define the ports to which you apply this filter and the action you want the switch to take if a virus is detected. You can choose from:
   - **Notify-only**: A trap is sent to ProCurve Manager Plus, but the traffic is not blocked
   - **Block** or **throttle**: Traffic is blocked for one minute, time for an administrator to find the machine and take action.

2. Prerequisites

For the command line (CLI) configuration, you will need a switch such as the ProCurve Switch 5406zl that supports the Virus Throttle feature. For configuration with PCM+, you will need to have your switch managed by an already configured PCM+ server.

3. Network diagram

Figure 1 details the hardware configuration referenced in this application note.

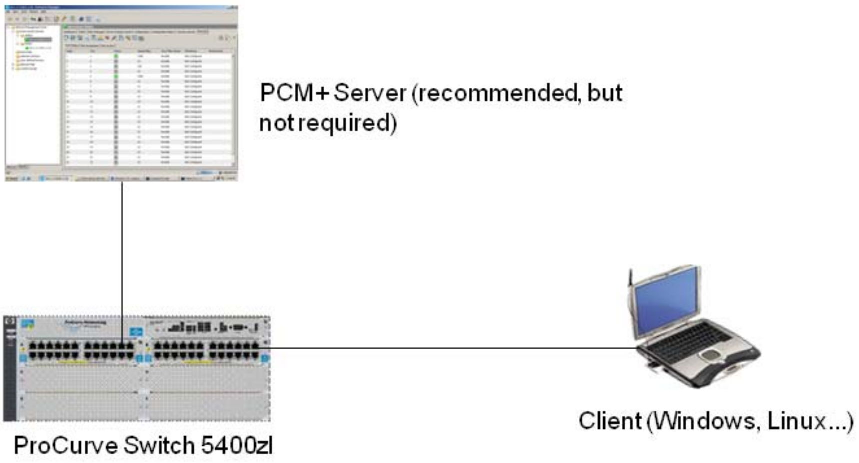

PCM+ Server (recommended, but not required)
ProCurve Switch 5400zl
Client (Windows, Linux...)

Figure 1. Setup for configuring Virus Throttle on a ProCurve switch

You can use either the CLI or PCM+ to configure Virus Throttle on the ProCurve switch.

4. Configuring Virus Throttle with the CLI

Two commands, connection-rate-filter and filter connection-rate, allow configuring Virus Throttle from the command line interface.

For example, here is how to activate virus throttling on ports 1-20, with sensitivity set to high. The following commands will cause traffic to be throttled when triggered by a virus:

```
ProCurve Switch 5400zl# sh run
[...]
connection-rate-filter sensitivity high
[...]
filter connection-rate 1-20 throttle
```

To view virus throttling, use the show connection-rate-filter all command. For example:

```
ProCurve Switch 5400zl# sh connection-rate-filter all

  VLAN ID      | Source IP Address | Filter Mode
  -------------+-------------------+------------
```

The output shows that no host is blocked or throttled yet.

When Virus Throttle is triggered by a client, the show connection-rate-filter all command displays the source IP address of the throttled virus. For example:

```
ProCurve Switch 5400zl# sh connection-rate-filter all

  VLAN ID      | Source IP Address | Filter Mode
  -------------+-------------------+------------
  1            | 10.1.1.100       | THROTTLE
```

5. Using Virus Throttle with PCM+

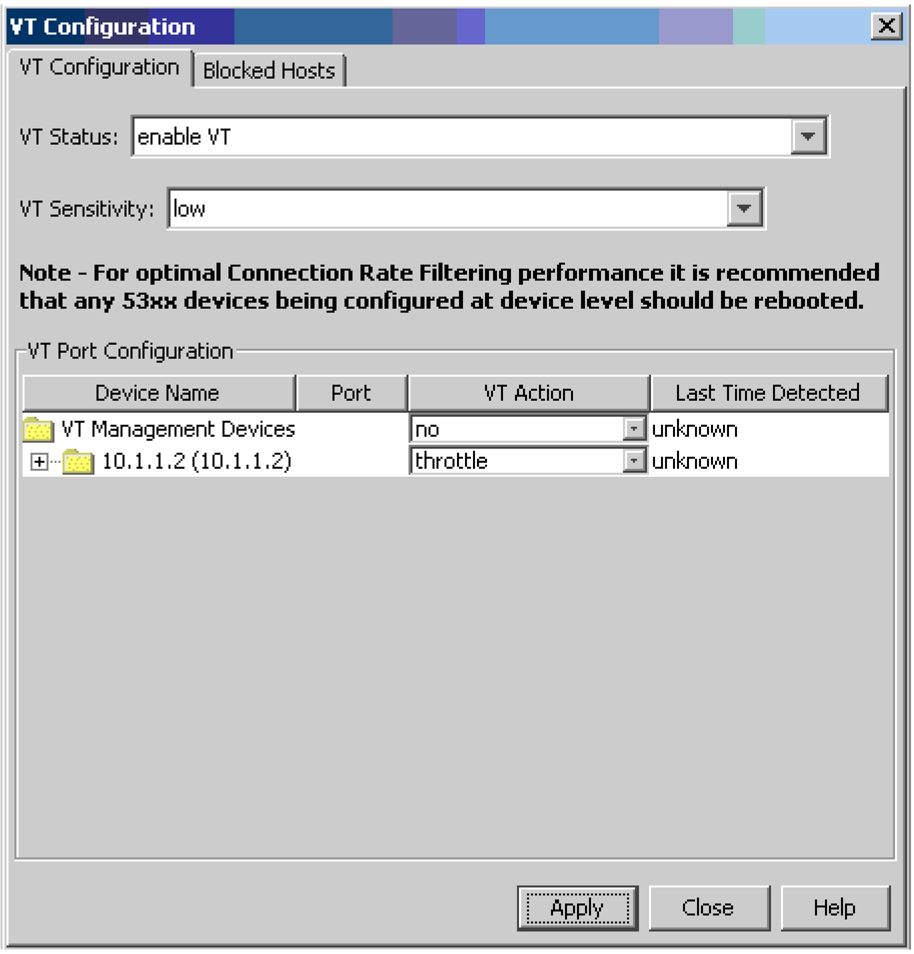
Another way to configure and manage Virus Throttle is with ProCurve Manager Plus.

5.1 Configure Virus Throttle

To configure Virus Throttle in PCM+ 2.2:

1. In PCM+ 2.2, select the switch. In the right pane, in the Dashboard tab (first tab on the left), click on the Virus Throttle icon:

   The VT Configuration window opens:



VT Status: enable VT

VT Sensitivity: low

Note - For optimal Connection Rate Filtering performance it is recommended that any 53xx devices being configured at device level should be rebooted.

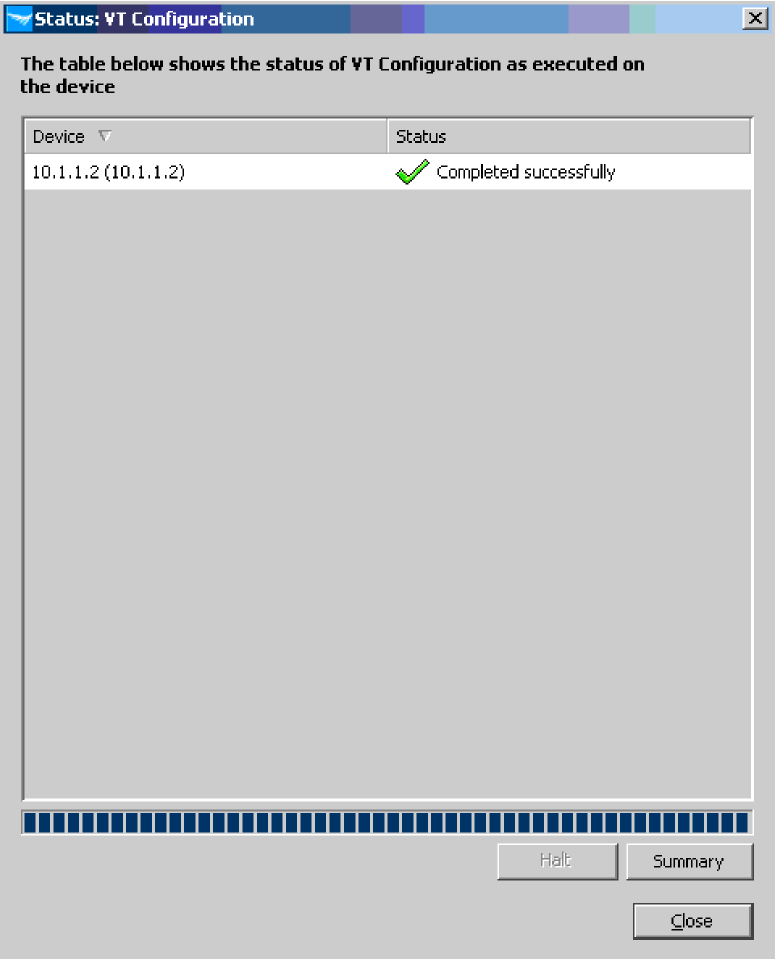
Device Name	Port	VT Action	Last Time Detected
VT Management Devices		no	unknown
⊞ 10.1.1.2 (10.1.1.2)		throttle	unknown

2. In the VT Configuration window set the VT Status to enable VT and the VT Sensitivity to high.

3. Specify the VT Action:
   - To specify virus throttling on all ports of all switches, configure the VT Action for VT Management Devices to throttle.
   - To specify throttling on only one switch, configure the VT Action to throttle for the IP address of the switch.
   - To specify throttling on a port, click the + sign to expand the port list of each switch, and set the VT action to throttle individually on the port.

   The example shows virus throttling specified on all ports of the 5400 switch: VT Action is set to no for VT Management Devices, and to throttle for the switch at 10.1.1.2.

4. Click Apply to enforce this policy on the switch. You see the Status: CT Configuration window, where you can confirm that virus throttling was successfully configured.



Status: VT Configuration

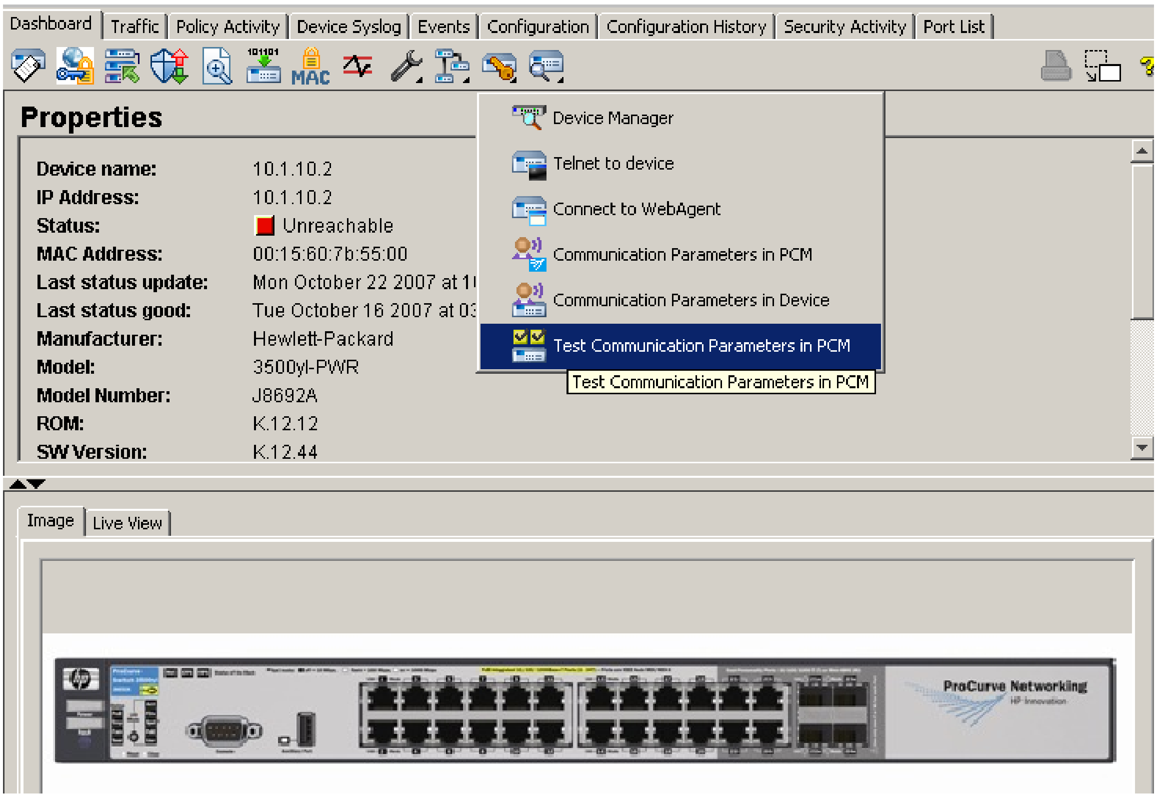
The table below shows the status of VT Configuration as executed on the device

Device	Status
10.1.1.2 (10.1.1.2)	✓ Completed successfully

5.2 Troubleshooting

If the policy enforcement fails, it might be because the Communications Parameters known by PCM+ do not match the actual communication parameters on the device. To check the communication parameters:

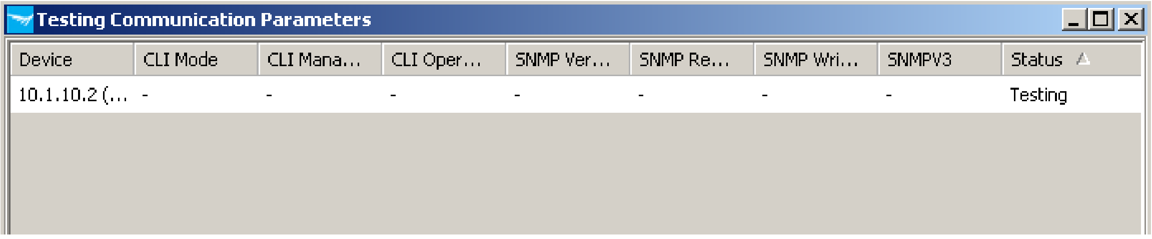
1. In PCM+ highlight the device, and on the Dashboard tab click the second icon from the right. You see a drop-down list of tests:



Properties

Device name:	10.1.10.2
IP Address:	10.1.10.2
Status:	🟥 Unreachable
MAC Address:	00:15:60:7b:55:00
Last status update:	Mon October 22 2007 at 1
Last status good:	Tue October 16 2007 at 0
Manufacturer:	Hewlett-Packard
Model:	3500yl-PWR
Model Number:	J8692A
ROM:	K.12.12
SW Version:	K.12.44

2. Select Test Communication Parameters in PCM+. You see the Testing Communications Parameters window as testing proceeds:

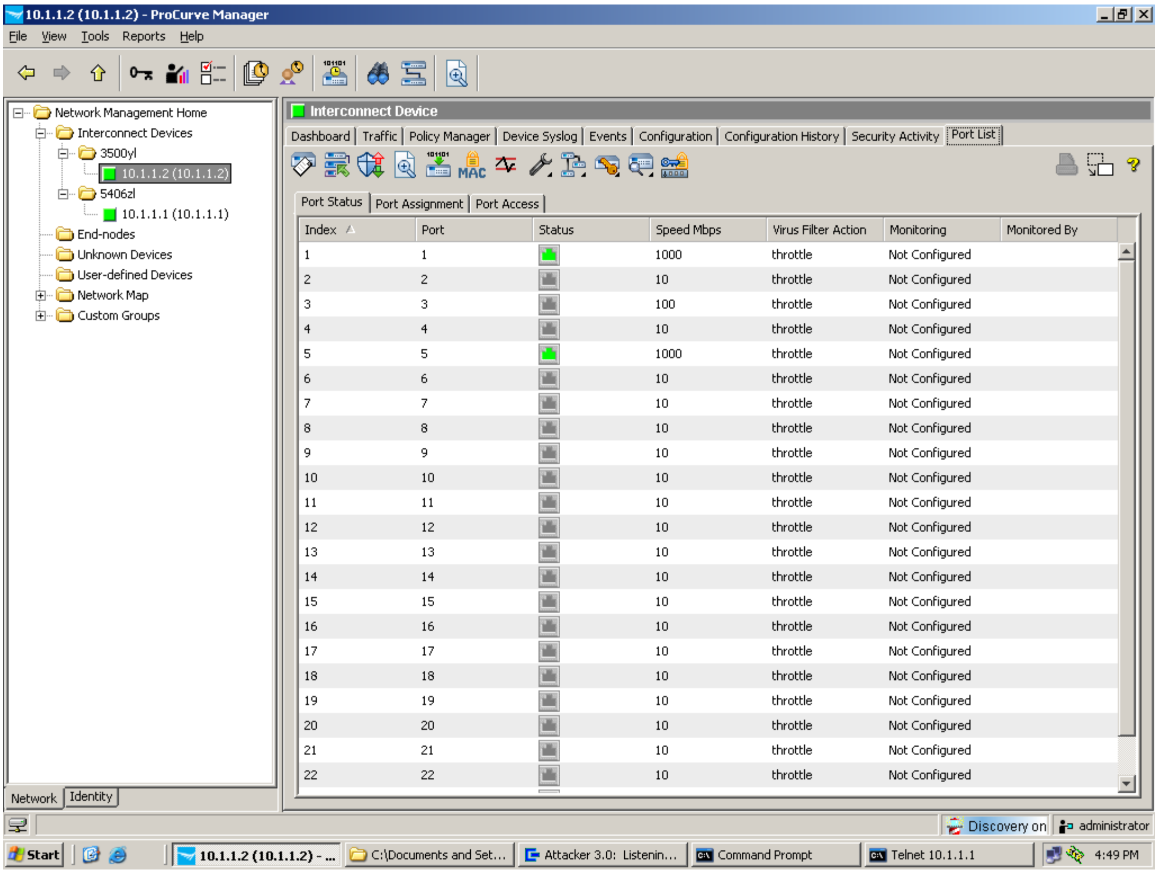


Testing Communication Parameters

Device	CLI Mode	CLI Mana...	CLI Oper...	SNMP Ver...	SNMP Re...	SNMP Wri...	SNMPV3	Status
10.1.10.2 (...	-	-	-	-	-	-	-	Testing

3. Confirm that Success appears against all parameters. If this is not the case, correct any mismatched parameters.

4. Then in PCM+ go to the Port List tab, select Port Status, and verify that the Virus Filter Action has been set to throttle for all ports on the 5400:

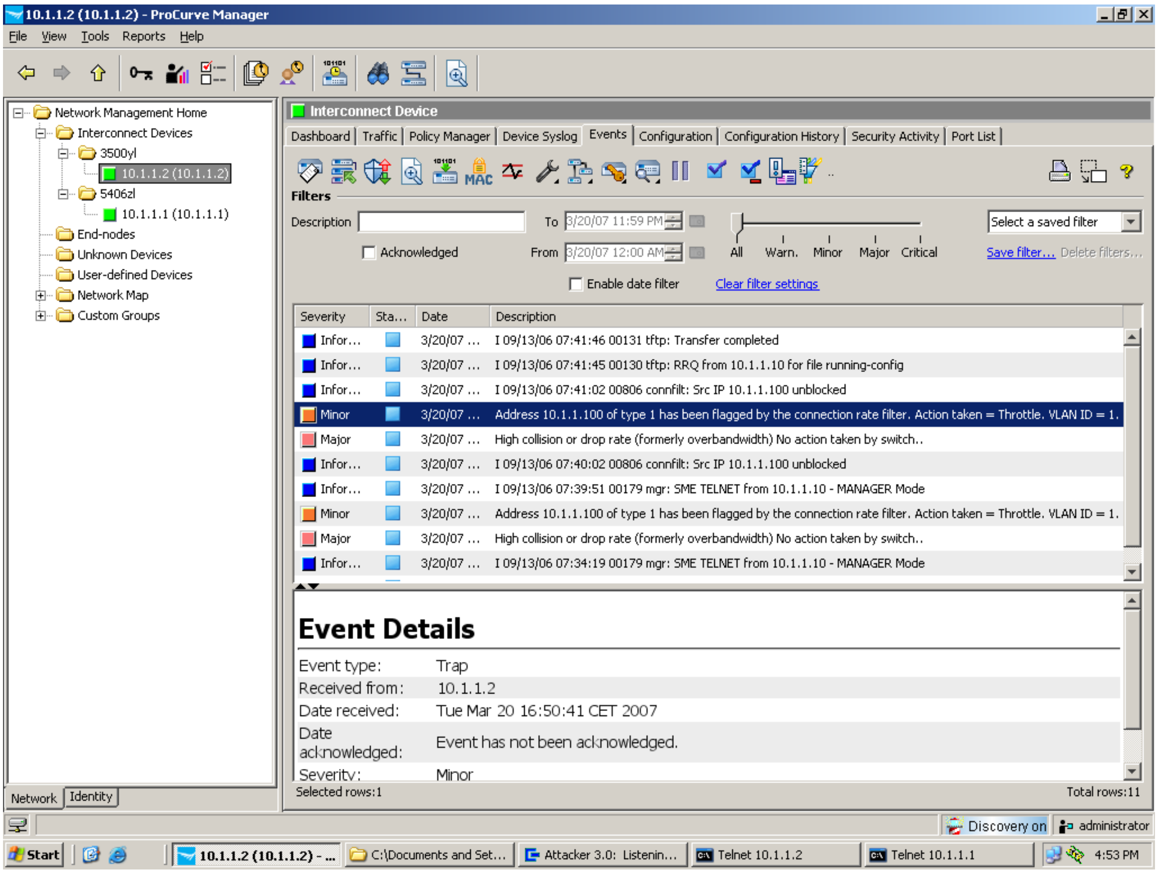


Index	Port	Status	Speed Mbps	Virus Filter Action	Monitoring	Monitored By
1	1	🟩	1000	throttle	Not Configured	
2	2	▨	10	throttle	Not Configured	
3	3	▨	100	throttle	Not Configured	
4	4	▨	10	throttle	Not Configured	
5	5	🟩	1000	throttle	Not Configured	
6	6	▨	10	throttle	Not Configured	
7	7	▨	10	throttle	Not Configured	
8	8	▨	10	throttle	Not Configured	
9	9	▨	10	throttle	Not Configured	
10	10	▨	10	throttle	Not Configured	
11	11	▨	10	throttle	Not Configured	
12	12	▨	10	throttle	Not Configured	
13	13	▨	10	throttle	Not Configured	
14	14	▨	10	throttle	Not Configured	
15	15	▨	10	throttle	Not Configured	
16	16	▨	10	throttle	Not Configured	
17	17	▨	10	throttle	Not Configured	
18	18	▨	10	throttle	Not Configured	
19	19	▨	10	throttle	Not Configured	
20	20	▨	10	throttle	Not Configured	
21	21	▨	10	throttle	Not Configured	
22	22	▨	10	throttle	Not Configured	

5.3 Monitor and block viruses

Once Virus Throttle is configured, you can monitor virus activity and take action when needed:

1. To see if the policy is triggered, select the Events tab. Virus throttling will appear as an event. In the example below you can see that you received a trap from the switch, indicating that Address 10.1.1.100 of type 1 has been flagged by the connection rate filter:



Severity	Sta...	Date	Description
Infor...		3/20/07 ...	I 09/13/06 07:41:46 00131 tftp: Transfer completed
Infor...		3/20/07 ...	I 09/13/06 07:41:45 00130 tftp: RRQ from 10.1.1.10 for file running-config
Infor...		3/20/07 ...	I 09/13/06 07:41:02 00806 connfilt: Src IP 10.1.1.100 unblocked
Minor		3/20/07 ...	Address 10.1.1.100 of type 1 has been flagged by the connection rate filter. Action taken = Throttle. VLAN ID = 1.
Major		3/20/07 ...	High collision or drop rate (formerly overbandwidth) No action taken by switch..
Infor...		3/20/07 ...	I 09/13/06 07:40:02 00806 connfilt: Src IP 10.1.1.100 unblocked
Infor...		3/20/07 ...	I 09/13/06 07:39:51 00179 mgr: SME TELNET from 10.1.1.10 - MANAGER Mode
Minor		3/20/07 ...	Address 10.1.1.100 of type 1 has been flagged by the connection rate filter. Action taken = Throttle. VLAN ID = 1.
Major		3/20/07 ...	High collision or drop rate (formerly overbandwidth) No action taken by switch..
Infor...		3/20/07 ...	I 09/13/06 07:34:19 00179 mgr: SME TELNET from 10.1.1.10 - MANAGER Mode

Event Details

Event type:	Trap
Received from:	10.1.1.2
Date received:	Tue Mar 20 16:50:41 CET 2007
Date acknowledged:	Event has not been acknowledged.
Severity:	Minor

2. To block viruses, return to the VT Configuration window, change the VT Action to block on all ports, and click Apply to apply the new configuration.

3. In the Virus Throttle configuration window, click to the Blocked Hosts tab and confirm that the address of the blocked machine appears.

6. Reference documents

This concludes the procedure for configuring Virus Throttle on ProCurve switches.

For further information about how to configure ProCurve switches to support security, please refer to the following links:

- For PCM+ and IDM manuals:
  http://www.hp.com/rnd/support/manuals/ProCurve-Manager.htm
  http://www.hp.com/rnd/support/manuals/IDM.htm

- For user manuals for ProCurve 3500yl-5400zl-8212zl switches:
  http://www.hp.com/rnd/support/manuals/3500-6200-5400-ChapterFiles.htm

- For ProCurve Switch 2610 series manuals:
  http://www.hp.com/rnd/support/manuals/2610.htm

For further information, please visit www.procurve.eu

4AA2-1722EEE, July 2008