Monitoring HP Procurve Switch

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

HP Procurve Switch is an IP switch that provides reliable 10/100 and 10/100/1000 port connectivity with uplinks to increase secure and fast business traffic. Any issues with the switch could be the possible source of critical problems like abnormal temperature, high resource utilization, or processing overheads! To avoid such issues, the performance of the HP Procurve Switch has to be monitored 24 *7. eG Enterprise helps network administrators to monitor the HP Procurve Switches continuously.

Chapter 2: How to Monitor HP Procurve Switch Using eG Enterprise?

eG Enterprise monitors the HP Procurve Switch using an eG external agent that is deployed on a remote Windows host. This eG agent polls the SNMP MIB of the HP Procurve Switch to gather its performance statistics at configured intervals. Before attempting to monitor the switch, ensure that the switch is SNMP-enabled. To start monitoring the HP Procurve Switch, manage the *HP Procurve Switch* component using the eG admin interface. The procedure for achieving this is discussed in the following section.

2.1 Managing the HP Procurve Switch

Using eG Enterprise, you can auto-discover the HP Procurve Switch as well as manually add the component for monitoring. To manage a *HP Procurve Switch* component, do the following:

1. Log into the eG admin interface.
2. If the HP Procurve Switch is already discovered, then directly proceed towards managing it using the **Components – Manage/Unmanage/Delete** page. To access this page, follow the Components -> Manage/Unmanage/Delete menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. However, if the target switch is yet to be discovered, then run discovery (Infrastructure -> Components -> Discovery) to get it discovered or follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu to manually add the component using the **Components** page. Remember that components manually added are managed automatically.
4. In the **Components** page that appears next, select *HP Procurve Switch* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

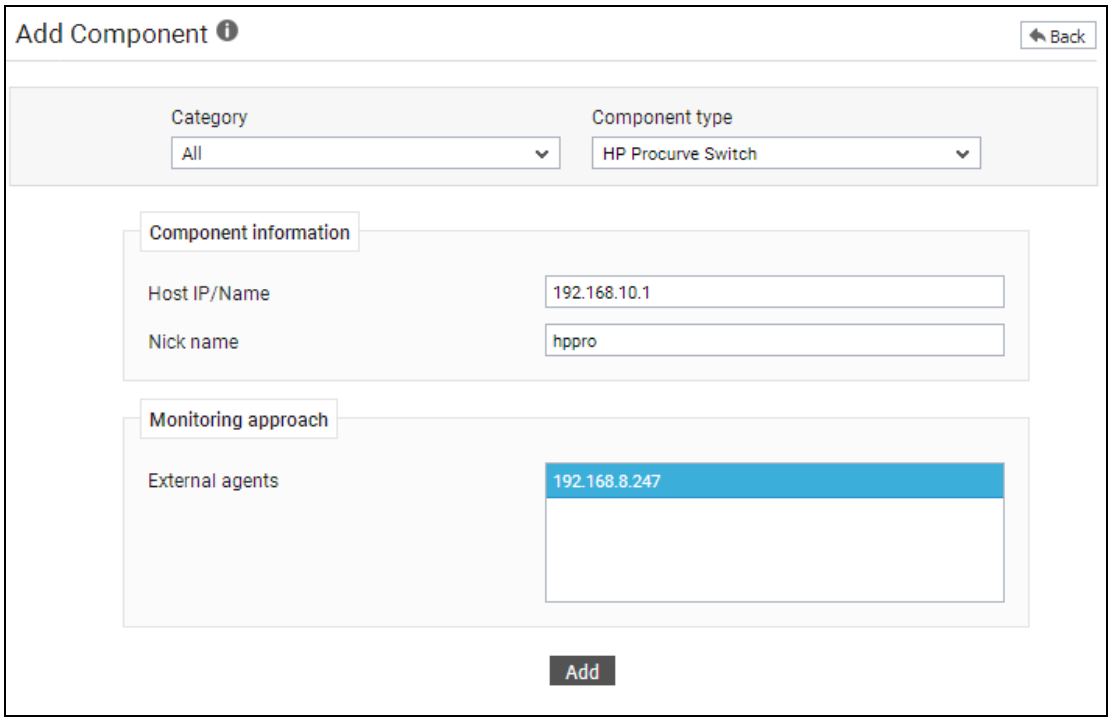
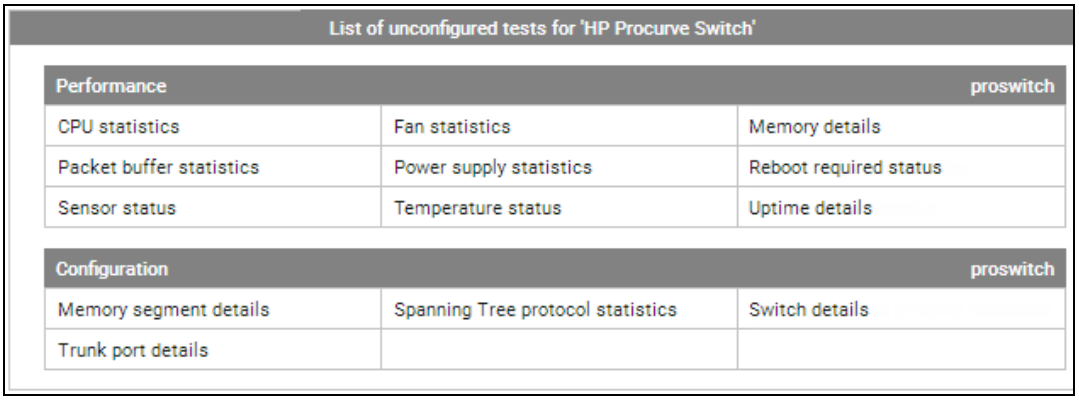


Figure 2.1: Adding the HP Procurve Switch component

5. Specify the **Host IP/Name** and the **Nick name** for the *HP Procurve Switch* component.
6. Choose an external agent for the target switch by picking an option from the **External agents** list box.
7. Then, click the **Add** button to register the changes (see Figure 2.1).
8. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.



List of unconfigured tests for 'HP Procurve Switch'

Performance		proswitch
CPU statistics	Fan statistics	Memory details
Packet buffer statistics	Power supply statistics	Reboot required status
Sensor status	Temperature status	Uptime details

Configuration		proswitch
Memory segment details	Spanning Tree protocol statistics	Switch details
Trunk port details		

Figure 2.2: A list of tests that need to be configured for the HP Procurve Switch

9. Click on any test in the list of unconfigured tests. To know how to configure the tests, refer to **Monitoring the HP Procurve Switch**.
10. Finally, signout of the eG admin interface.

Chapter 3: Monitoring the HP Procurve Switch

eG Enterprise offers a dedicated HP Procurve Switch monitoring model which periodically checks the CPU and memory utilization, the temperature and fans of the switch, the packet buffer etc, so that excessive resource utilization, abnormal temperature increase, power supply failures, etc. can be detected before any irreparable damage occurs.

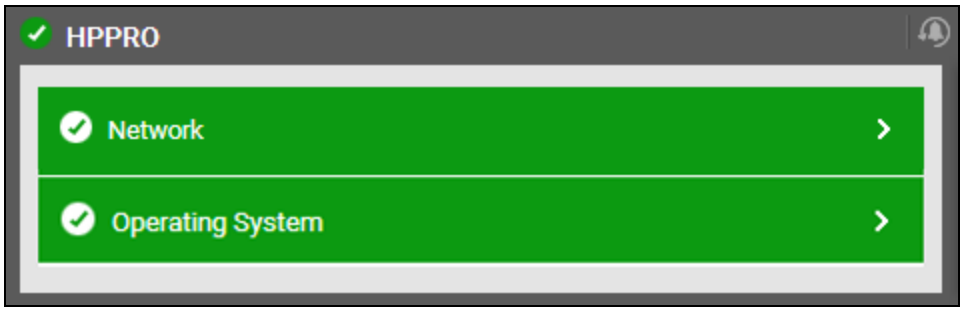


Figure 3.1: The layer model of the HP Procurve Switch

Every layer of Figure 3.1 is mapped to a variety of tests which connect to the SNMP MIB of the target HP Procurve Switch to collect critical statistics pertaining to its performance. The metrics reported by these tests enable administrators to answer the following questions:

- How well the CPU is utilized?
- How well the memory of the target Switch is utilized?
- What is the temperature of the CPU and switch chassis?
- What is the current state of each sensor of the switch?
- What is the current state and utilization of the power supply?
- What is the current status of the fan?
- Does the switch require reboot?
- How long has the switch been up since the restart?
- What is the current size of the packet buffer?

The sections to come will discuss each layer of Figure 3.1 in detail.

3.1 The Operating System Layer

Using this layer, administrators can figure out the CPU, power supply and memory utilization of the HP Procurve Switch. Critical statistics related to temperature sensor and fans of the switch are also closely monitored and reported. Administrator cans also determine the size of the packet buffer allocated to the switch.

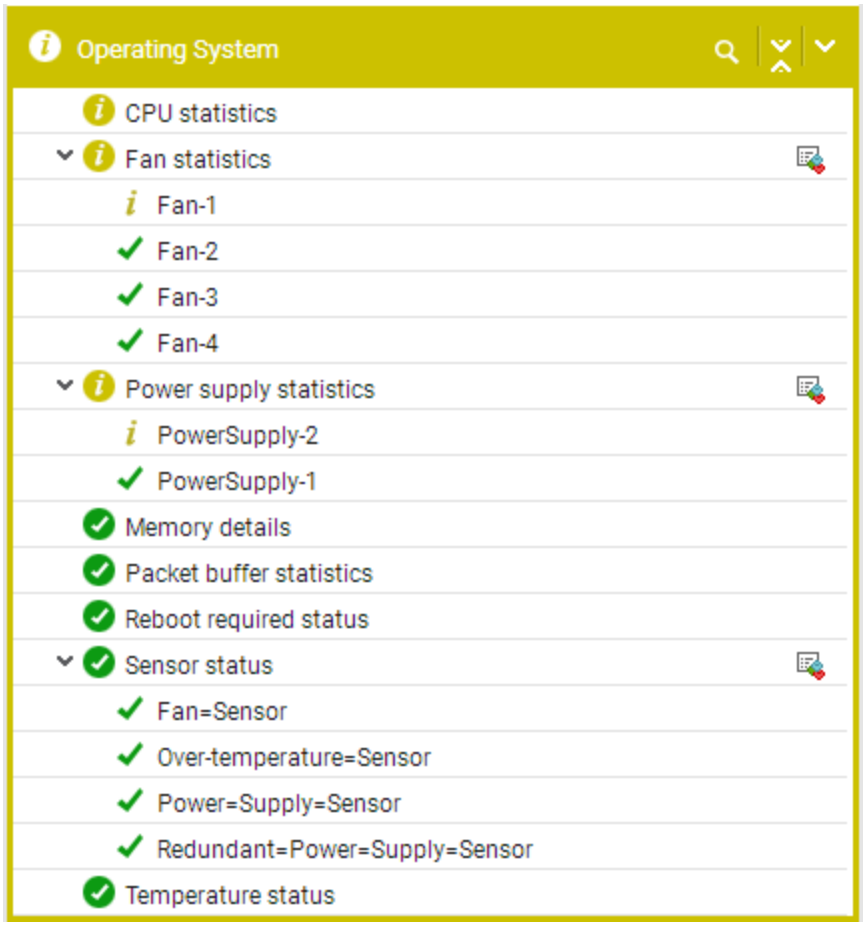


Figure 3.2: The tests associated with the Operating System layer

Let us discuss each test associated with this layer in the following sections.

3.1.1 CPU Statistics Test

One of the probable reasons for the poor performance of the HP Procurve switch is excessive CPU usage. Administrators should hence continuously track how well the switch utilizes CPU resources, so that abnormal usage patterns can be proactively detected and corrected to ensure peak performance of the switch. This CPU usage check can be performed using the **CPU Statistics** test.

At configured intervals, this test monitors the current CPU utilization of the switch and reports excessive usage (if any).

Target of the test : A HP Procurve Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for the HP Procurve Switch that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the

Parameter	Description
	context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU Utilization	Indicates the percentage of CPU that is currently used by the switch.	Percent	Ideally, the value should be low. An unusually high value or a consistent increase in this value is indicative of abnormal CPU usage which requires further investigation.

3.1.2 Fan Statistics Test

The HP Procurve switch is provided with two hot-swappable fan trays. Each fan tray contains multiple number of fans to maintain the temperature of the switch within a permissible range. If the fan suddenly stops running, then the temperature of the core components of the target switch will significantly increase, causing serious damage to the core components. This is why, its good practice to keep track of the fan status using the **Fan Statistics** test. For each fan available on the switch, this test reports the current status and the count of failure events, if any.

Target of the test : A HP Procurve Switch

Agent deploying the test : An external Agent

Outputs of the test : One set of results for each fan in the fan trays of the HP Procurve switch being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the switch listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the switch. This

Parameter	Description
	parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following

Parameter	Description
	encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Fan state	Indicates the current status of this fan.		The values reported by this measure and its numeric equivalents are mentioned in the table below: Measure Value / Numeric Value Failed – 0 Removed – 1 Off – 2 Under speed – 3 Over speed – 4 Ok – 5 Max speed – 6 **Note:**

Measurement	Description	Measurement Unit	Interpretation
			By default, this measure reports the **Measure Value**s listed in the table above to indicate the current status of each fan. The graph of this measure however, represents the status of the fan using the numeric equivalents only - 0 to 6.
Fan failure count	Indicates the number of times this fan failed during the last measurement period.	Number	The value of this measure should be zero.

3.1.3 Power Supply Statistics Test

The HP Procurve switch comes with two redundant power supplies. A sudden failure, erratic voltage fluctuations and abnormal power usage can cause the power supplies to crash, leading to critical damage of the target switch. To avoid such an unpleasant eventuality, administrators need to keep an eye on the power supplies of the switch. The **Power Supply Statistics** test helps administrators in this regard!

This test auto-discovers the power supplies of the target switch and reports the current status of each power supply. In addition, this test also reveals the count of failure events, the current voltage and temperature, and the maximum amount of power utilized from each power supply. Using these statistics, administrators can easily find out the power supply failures, abnormalities in power usage, if any and take remedial measures accordingly.

Target of the test : A HP Procurve Switch

Agent deploying the test : An external Agent

Outputs of the test : One set of results for every power supply in the HP Procurve switch that is being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.

Parameter	Description
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:

Parameter	Description
	• **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Power supply state	Indicates the current status of this power supply.		The values reported by this measure and its numeric equivalents are mentioned in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Maximum power</td><td>0</td></tr>
<tr><td>Not present</td><td>1</td></tr>
<tr><td>Not plugged</td><td>2</td></tr>
<tr><td>Powered</td><td>3</td></tr>
<tr><td>Failed</td><td>4</td></tr>
<tr><td>Permanent failure</td><td>5</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status of each power supply. The graph of this measure however, represents the status of the power supply using the numeric equivalents only - 1 to 6.
</td></tr>
<tr><td>Power supply failure count</td><td>Indicates the number of times this power supply failed during the last measurement period.</td><td>Number</td><td>A zero value is desired for this measure.</td></tr>
<tr><td>Power supply temperature</td><td>Indicates the current temperature of this power supply.</td><td>Celsius</td><td></td></tr>
<tr><td>Power supply voltage</td><td>Indicates the current voltage of this power supply.</td><td>Volts</td><td>The value of this measure should be in the admissible range. If the threshold is violated due to erratic fluctuations, administrators should further initiate investigations.</td></tr>
<tr><td>Power supply current wattage</td><td>Indicates the amount of power that this power supply currently supplies.</td><td>Watts</td><td></td></tr>
<tr><td>Power supply maximum wattage</td><td>Indicates the maximum amount of power that this power supply can supply.</td><td>Watts</td><td>The value of this measure should be in the admissible range.</td></tr>
</table>

3.1.4 Memory Details Test

This test monitors the memory utilization of the HP Procurve switch and proactively alerts administrators to potential resource contentions.

Target of the test : A HP Procurve Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target HP Procurve switch that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the HP switch that is being monitored.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the

Parameter	Description
	eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified Username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total memory	Indicates the total amount of memory configured for the switch.	MB	
Free memory	Indicates the amount of memory that is currently available for use.	MB	A sudden decrease in this value could indicate an unexpected/sporadic spike in the memory utilization of the system. A consistent decrease however could indicate a gradual, yet steady erosion of memory resources, and is hence a cause for concern.
Used memory	Indicates the amount of memory utilized during the last measurement period.	MB	A low value is desired for this measure.
Used memory utilization	Indicates the percentage of memory that is utilized by the switch.	Percent	A value close to 100 indicates that the memory utilization is at its peak. Administrators may therefore be required to add additional memory resources to the switch.

3.1.5 Packet Buffer Statistics Test

To temporarily store packets during bursty network traffic, administrators create a memory space, also called packet buffer using the web-based management console of the HP Procurve switch. The packet buffer can be utilized during the packet transmission delays or retransmitting a request. The target switch uses the packet buffer when the switch encounters high transmission latency and packet loss. Insufficient buffer memory can cause packet loss, delays and processing overheads, which in turn degrades the reliability and performance of the target switch. To avoid such eventualities, buffer memory allocation to the switch should be closely monitored at regular intervals. This can be easily done using the **Packet Buffer Statistics** test!

This test reveals the size of the packet buffer allocated to the switch. In the process, this test also reports how many times the switch failed to access the buffer and how many times the corrupted buffers were deleted. With the help of these statistics, administrators can decide whether they need to add additional resources to the buffer or repair the packet buffer.

Target of the test : A HP Procurve Switch

Agent deploying the test : An external Agent

Outputs of the test : One set of results for the HP Procurve switch that is being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.

Parameter	Description
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Packet buffer size	Indicates the current size of the packet buffer.	KB	A high value is desired for this measure. A sudden decrease in the value of this measure indicates that the packet buffer memory is depleting rapidly, and administrators need to allocate the additional memory to the buffer to avoid packet loss and delay.
Failure count to obtain packet buffer	Indicates the number of times the switch failed to access the packet buffer.	Number	A low value is desired for this measure.
Corrupted buffer deletion count	Indicates the number of times the corrupted buffer was deleted.	Number	

3.1.6 Reboot Required Status Test

Administrators may wish to reboot the switch when the switch is unusually up for longer duration or faulty. To instantly identify whether/not the switch needs to be rebooted, administrators can use the **Reboot required Status** test. At regular intervals, this test reveals whether the target switch needs to be rebooted or not.

Target of the test : A HP Procurve Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target HP Procurve switch that is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the switch that is being monitored.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your

Parameter	Description
	environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified Username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.

Parameter	Description
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Reboot required status	Indicates whether/not the switch needs to be rebooted.		The values that this measure can report and the corresponding numeric values are tabulated below: Measure Value / Numeric Value No / 0 Yes / 1 **Note:** By default, this measure reports the above-mentioned **Measure Value**s while indicating whether/not the switch needs to be rebooted. However, in the

Measurement	Description	Measurement Unit	Interpretation
			graph of this measure will be represented using the numeric equivalents only.

3.1.7 Sensor Status Test

The HP Procurve switch contains power supply, fan, and temperature sensors to monitor its power and temperature. Failure of any of these sensors can bring the switch operations to a halt. Administrators need to be able to promptly detect sensor failures and take corrective actions before any permanent damage is done. The **Sensor Status** test can help administrators in this regard. This test monitors the status of each sensor, and also promptly captures and reports real/potential sensor failures.

Target of the test : A HP Procurve Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each sensor on the target HP Procurve switch that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the HP switch that is being monitored.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote

Parameter	Description
	SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified Username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard

Parameter	Description
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Sensor status</td><td>Indicates the current status of this sensor.</td><td></td><td>The values that this measure can report and the their corresponding numeric values are tabulated below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Good</td><td>4</td></tr>
<tr><td>Not present</td><td>5</td></tr>
<tr><td>Warning</td><td>6</td></tr>
<tr><td>Bad</td><td>7</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current status of each sensor. However, in the graph of this measure sensor status will be represented using the numeric equivalents only.</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
Sensor in warning state	Indicates the number of times that this sensor displayed a "Warning" state during the last measurement period.	Number	A low value is desired for this measure.
Sensor in Failure state	Indicates the number of times this sensor failed during the last measurement period.	Number	The value of this measure should be zero.

3.1.8 Temperature Status Test

This test tracks the current temperature of CPU and chassis of the target switch. Using this test, administrators can check if the temperature of the target switch is within admissible range and can take remedial measures if the temperature threshold is violated.

Target of the test : A HP Procurve Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target HP Procurve switch that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the HP switch that is being monitored.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version

Parameter	Description
	3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified Username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard

Parameter	Description
	• **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU temperature	Indicates the current temperature of the CPU.	Celsius	The values of these measures should be within a permissible range. A significant rise/drop in the values of these measures can cause damage to the core components of the switch.
Chassis temperature	Indicates the current temperature of the switch chassis.	Celsius	

3.2 The Network layer

The **Network** layer handles connectivity of the HP Procurve Switch to the network, and includes packet traffic transmitted to and from the server. Using the tests available in this layer, administrators can determine whether the network link to the target Switch is available or not, the bandwidth availability, the rate of packet transmissions to and from the host and the uptime of the switch. In addition, the administrators can also determine the operational state of the network interfaces and the reason for why the interface is down.

Figure 3.3: The list of tests associated with the Network layer

The **Network Interfaces** test has already been discussed in the *Monitoring Cisco Router* document. The details about the **Network** test is available in the *Monitoring Unix and Windows Servers* document.

3.2.1 Uptime Details Test

In large network environments, it is essential to monitor the uptime of the HP Procurve switch in the infrastructure. By tracking the uptime of the target switch, administrators can determine what percentage of time the switch has been up. Comparing this value with service level targets, administrators can determine the most trouble-prone areas of the infrastructure.

In some environments, administrators may schedule periodic reboots of their switch. By knowing that the switch has been up for an unusually long time, an administrator may come to know that the scheduled reboot task is not working on a switch.

This test included in the eG agent monitors the uptime of the target switch.

Target of the test : A HP Procurve Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target switch that is being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the target switch.

Parameter	Description
	This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the snmpversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP **v3** protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the Username parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the username in the context text box. By default, this parameter is set to none.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if v3 is selected as the snmpversion. From the authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
Encryptflag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to no by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the yes option.
Encrypttype	If this Encryptflag is set to Yes, then you will have to mention the encryption type by selecting an option from the Encrypttype list. SNMP v3 supports the following

Parameter	Description
	encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
Encryptpassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
ReportManagerTime	By default, this flag is set to **Yes**, indicating that, by default, the detailed diagnosis of this test, if enabled, will report the shutdown and reboot times of the device in the manager's time zone. If this flag is set to **No**, then the shutdown and reboot times are shown in the time zone of the system where the agent is running.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Has the system been rebooted?	Indicates whether the switch has been rebooted during the last measurement period or not.		The values that this measure can report and the numeric values they indicate have been listed in the table below: **Measure Value** / **Numeric Value** No / 0 Yes / 1 **Note:**

Measurement	Description	Measurement Unit	Interpretation
			By default, this measure can report the **Measure Value**s mentioned above while indicating whether the switch is rebooted or not. However, the graph of this measure is indicated using the numeric equivalents.
Uptime during the last measure period	Indicates the time period that the switch has been up during the last measurement period.	Seconds	If the switch has not been rebooted during the last measurement period and the agent has been running continuously, this value will be equal to the measurement period. If the switch was rebooted during the last measurement period, this value will be less than the measurement period of the test. For example, if the measurement period is 300 secs, and if the switch was rebooted 120 secs back, this metric will report a value of 120 seconds. The accuracy of this metric is dependent on the measurement period – the smaller the measurement period, greater the accuracy.
Total uptime of the system	Indicates the total time that the switch has been up since its last reboot.	Minutes	Administrators may wish to be alerted if a switch has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.