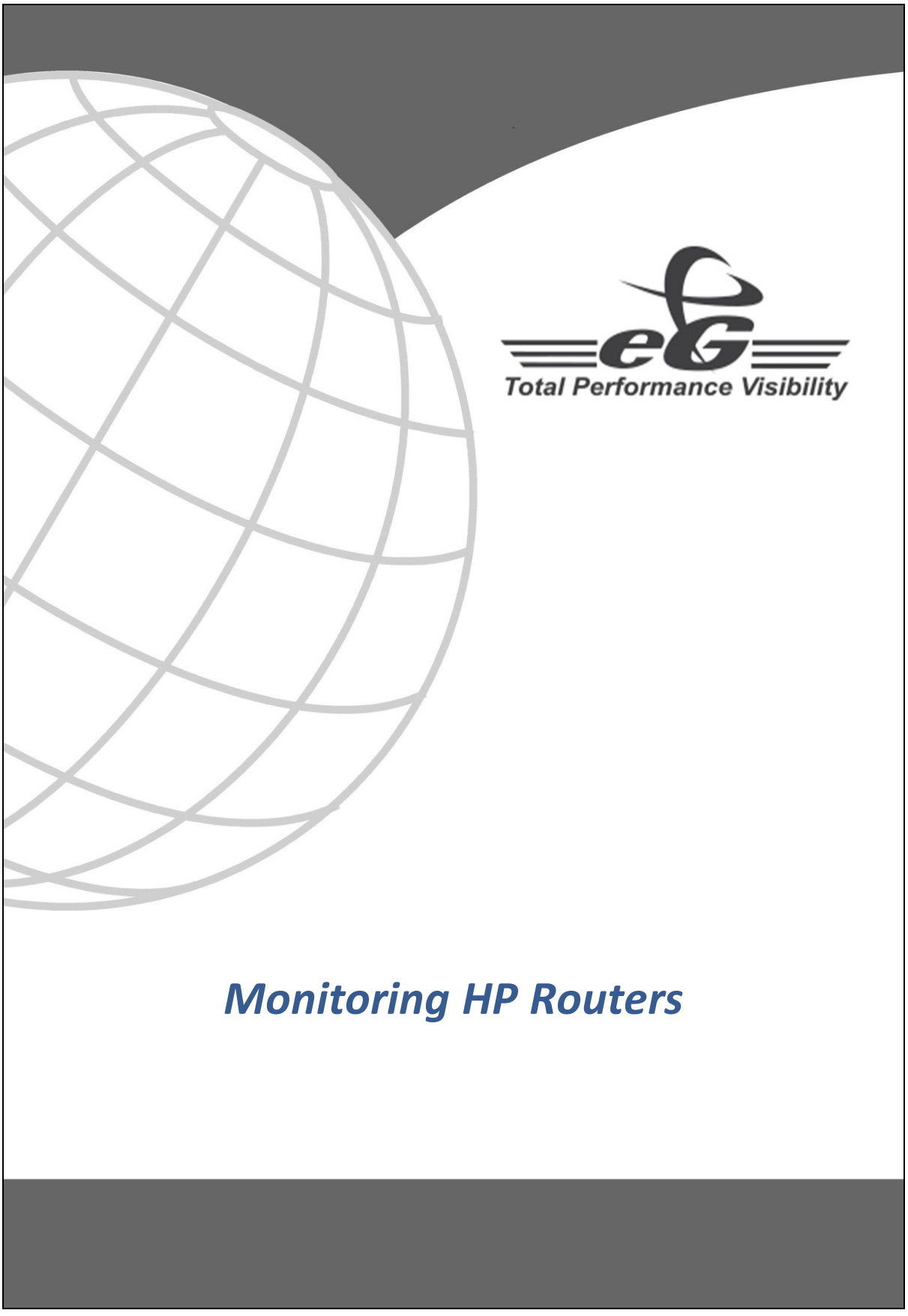

Monitoring HP Routers

Table of contents

Table of Figures

1

Monitoring the HP Router

A router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to.

The HP Routers like MSR 93x, MSR95x series delivers a high-performance small-branch router providing integrated routing, switching, security, SIP, 802.11n WLAN connectivity, and 4G LTE/3G in a single unit. With its converged infrastructure, it enables faster time to service and enhanced performance while simplifying your network through a single management screen and zero-touch deployment. The router increases flexibility and agility, delivering extensive connectivity capabilities in a compact, fixed form factor. These routers are based on open standards for seamless integration within small-branch deployment.

Excessive packet traffic can choke the router, thereby significantly slowing down packet transmission. Similarly, very low unused memory/CPU on the router can also affect the speed with which the router transmits data. It is therefore imperative to monitor the resource usage and the traffic to and from the router, so that any sudden increase in load or erosion of resources can be instantly detected, and remedial action immediately initiated.

The eG Enterprise suite includes a specialized monitoring model to monitor the HP Routers. By periodically polling the SNMP MIBs of the target HP Router, the eG agents pull out various metrics of interest relating to the HP Routers. Figure 1 depicts the layer model of a HP router.

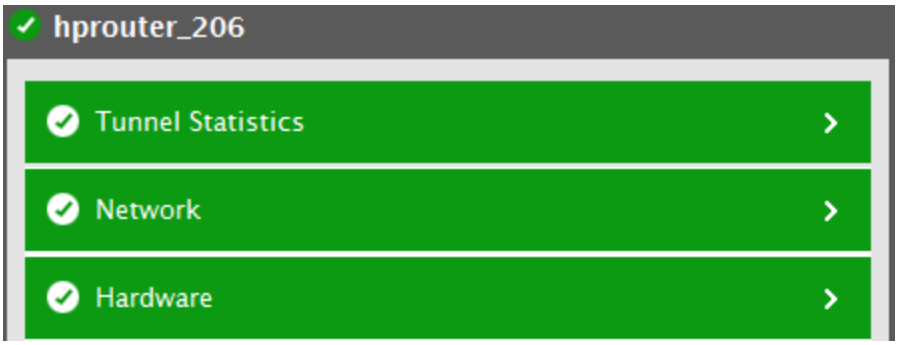

Figure 1.1: The layer model of the HP Router

Every layer of Figure 1.1 is mapped to a variety of tests which connect to the SNMP MIB of the HP Router 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 by the router?
- What is the maximum percentage of CPU utilized and the average CPU utilization?
- How well memory is utilized by the router?
- What is the configured power of the router and the current power of the router?

- What is the current voltage on each voltage test point of the router?
- How many tunnels are currently active on the router?
- How well data/packets are transmitted/received by the router?
- How many packets are actually dropped during transmission/reception?

Since the **Network** layer has been dealt with Monitoring Web Servers document, the sections to come will discuss the remaining layers of Figure 1.1.

1.1 The Hardware Layer

This layer helps administrators to figure out the following:

- The CPU utilized by the router;
- The memory utilization of the router;
- The configured power and current power consumed by the router and
- The voltage at each voltage test point of the router.

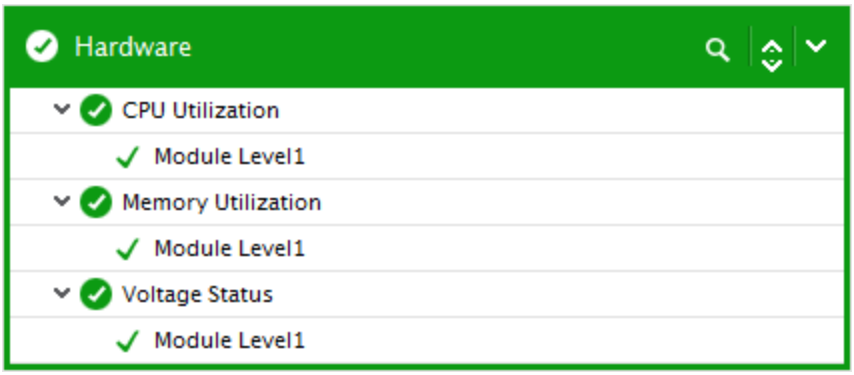

Figure 1.2: The test mapped to the Hardware layer

1.1.1 CPU Utilization Test

Often excess traffic to a router can impose a prohibitive load on the router, choking the CPU and hence making it a bottleneck. This test measures the CPU utilization of the target HP Router. Using this test, administrators can figure out the maximum CPU utilized as well as the average CPU utilization of the router thus helping them analyze CPU utilization patterns of the target router.

Target of the test : A HP Router

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target HP Router being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.

3. **SNMPPORT** – The port number through which the target router exposes its SNMP MIB; the default is 161.
4. **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.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.
6. **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.
7. **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*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **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
11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE** – If the **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

13. **ENCRYPTPASSWORD**– Specify the encryption password here.
14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **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 the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
CPU usage:	Indicates the percentage of CPU utilized by the router.	Percent	A very high value could indicate a CPU bottleneck at the router.
Maximum CPU usage:	Indicates the maximum percentage of CPU utilized by the router.	Percent	
Average CPU usage:	Indicates the average percentage of CPU utilized by the router.	Percent	

1.1.2 Memory Utilization Test

This test monitors the memory utilization of the target HP router and proactively alerts administrators to potential resource contentions, if any.

Target of the test : A HP Router

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target HP Router being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.

3. **SNMPPORT** – The port number through which the target router exposes its SNMP MIB; the default is 161.
4. **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.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **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.
7. **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*.
8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **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
11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE** – If the **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

13. **ENCRYPTPASSWORD**– Specify the encryption password here.
14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **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 the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Total memory:	Indicates the total amount of memory allocated to the managed router device.	MB	
Memory usage:	Indicates the amount of memory that is currently used by the managed router device.	MB	A low value is desired for this measure.
Free memory:	Indicates the amount of memory that is available for use on the managed router device.	MB	A high value is desired for this measure.
Memory utilization:	Indicates the percentage of memory utilized by the managed router device.	Percent	A utilization value close to 100% is indicative of a memory bottleneck at the router.

1.1.3 PowerSupply Details Test

This test reports the power that is configured for the HP router and also measures the current power of the HP router.

Target of the test : A HP Router

Agent deploying the test : An external agent

Outputs of the test : One set of results for each power supply unit of the target HP Router being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **SNMPPORT** – The port number through which the target router exposes its SNMP MIB; the default is 161.
4. **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.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **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.
7. **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*.
8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **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
11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG

agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.

12. **ENCRYPTTYPE** – If the **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
13. **ENCRYPTPASSWORD** – Specify the encryption password here.
14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **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 the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Nominal power:	Indicates the configured power of the managed router device.	milliwatts	
Current power:	Indicates the current power of the managed router device.	milliwatts	The value of this measure should be well within admissible range. If excessive power is recorded, then the router may malfunction leading to severe performance bottlenecks.

1.1.4 Voltage Status Test

This test monitors the current voltage recorded on each voltage test point of the target HP router.

Target of the test : A HP Router

Agent deploying the test : An external agent

Outputs of the test : One set of results for each voltage test point of the target HP Router being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **SNMPPORT** – The port number through which the target router exposes its SNMP MIB; the default is 161.
4. **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.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **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.
7. **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*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **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
11. **ENCRYPTFLAG**– This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.

12. **ENCRYPTTYPE**– If the **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
13. **ENCRYPTPASSWORD**– Specify the encryption password here.
14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **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 the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Voltage:	Indicates the current voltage recorded on this voltage test point.	Volts	The value of this measure should be well within admissible range. If excessive voltage is recorded, then the router may malfunction leading to severe performance bottlenecks.

1.2 The Tunnel Statistics Layer

This layer monitors the number of active tunnels and the traffic flowing through the tunnels created via the HP Router.

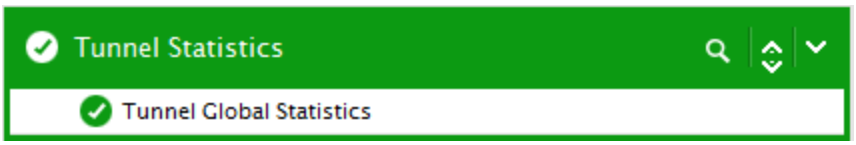

Figure 1.3: The test mapped to the Tunnel Statistics layer

1.2.1 Tunnel Global Statistics Test

A tunnel is a virtual point-to-point link across a multipoint-access network, such as the Internet. Tunnels help you to create secure connections between remote users and a private corporate network via the internet. In a sense, a tunnel emulates a WAN link. A tunneling protocol:

- encapsulates other protocols
- sets up a point-to-point link

When you initiate communication or send data over VPN network via the HP Router, the Tunneling protocol(s) used by the VPN network (like PPTP, L2TP, IPSec etc.) wraps up the data packets into another data packet and encrypts the package that is to be sent through the tunnel. At the receiver's end, the tunneling device/protocol deciphers the package and then strips the wrapped data packet to read and access the original message and reveal the source of packet and other classified information. This way, secure communication is possible with the tunnels. If the traffic through the tunnels are too high or if a tunnel is not available, then, data transmission and reception by the tunnels will take longer than usual which will inturn affect the performance of the HP Router. To avoid such situation, administrators should constantly monitor the level of traffic flowing through the tunnels of the HP Router. The **Tunnel Global Statistics** helps administrators perform the task with ease!

This test reports the number of active tunnels created on the target HP Router and measures the level of traffic to and from the tunnels. Using this test, administrators can be proactively alerted to the discrepancies in the data and packet transmission and reception.

Target of the test : A HP Router

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target HP Router being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **SNMPPORT** – The port number through which the target router exposes its SNMP MIB; the default is 161.
4. **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.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **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.
7. **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*.

8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **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
11. **ENCRYPTFLAG**– This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **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
13. **ENCRYPTPASSWORD**– Specify the encryption password here.
14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **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 the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Active tunnels:	Indicates the number of tunnels that are currently active via the managed router.	Number	There should atleast be one active tunnel at any point of time. If the value of this measure is 0, then this test will not report any other metrics.
Received data:	Indicates the amount of data received through the tunnels by the managed router during the last measurement period.	MB	
Received packets:	Indicates the number of packets received through the tunnels by the managed router during the last measurement period.	Number	
Received drop packets:	Indicates the number of packets that were dropped while packets were being received during the last measurement period.	Number	Ideally, the value of this measure should be zero.
Transmitted data:	Indicates the amount of data transmitted through the tunnels from the managed router during the last measurement period.	MB	
Transmitted packets:	Indicates the number of packets transmitted through the tunnels from the managed router during the last measurement period.	Number	
Transmitted drop packets:	Indicates the number of packets that were dropped	Number	Ideally, the value of this measure should be zero.

Measurement	Description	Measurement Unit	Interpretation
	while packets were being transmitted through the tunnels during the last measurement period.		Comparing the value of this measure with the Received drop packets measure will help administrators identify when exactly the packets dropped were at the maximum - during reception or transmission?

2

Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to the **HP Routers**. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.