Monitoring Peplink WAN Router

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Peplink WAN Router is an ideal single - box solution for medium to large business environments, and allows service providers to enable highly available multi - network services without any complexity. The Peplink WAN Router provides the VPN bonding feature using which administrators can aggregate multiple Internet links into a single bonded data-pipe that is budget-friendly and easily configurable to suit any networking environment. By aggregating the links in the environment, administrators can handle the most demanding traffic without lags or downtime. As a result, the bandwidth for data/packet transmission and transmission speed are increased across office sites.

Excessive packet traffic can choke the Peplink WAN 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. Since unavailability of access points, WAN failures, VPN profiles, and delays can cause prolonged outages and cost an enterprise money and reputation, continuous operation and good health of the router is of great importance. 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 can be initiated immediately. This can be easily achieved using eG Enterprise!

Chapter 2: How to Monitor Peplink WAN Router Using eG Enterprise

eG enterprise monitors the Peplink WAN Router in an agentless manner. For this purpose, you can deploy a single eG agent on a remote Windows host. This agent executes various tests that connect to the SNMP MIB of the router to be monitored, and collects critical statistics of interest. Before attempting to monitor the target router, ensure that the target router is SNMP-enabled. To enable the eG agent to access the SNMP-enabled router, specify the following while configuring the tests:

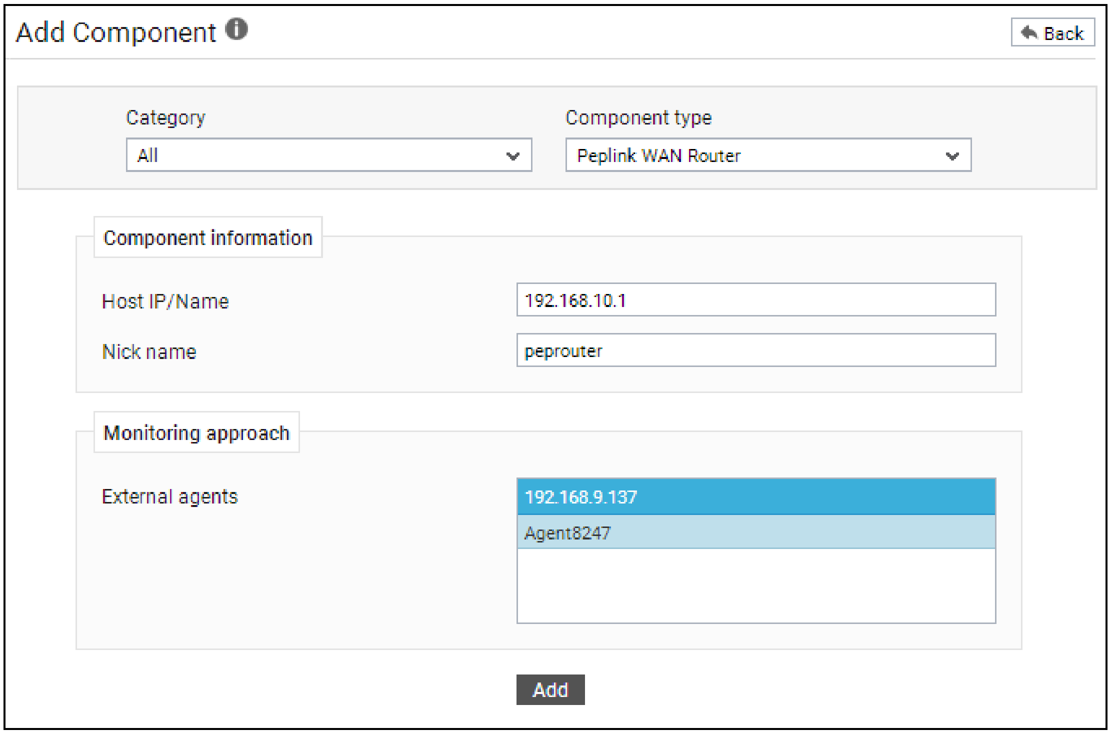
- Port number on which the target router exposes its MIB
- SNMP community to be used for accessing the MIB

To start monitoring the target router, first manage the *Peplink WAN Router* component using the steps explained in the section below.

2.1 Managing Peplink WAN Router

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

1. Log in to the eG admin interface.
2. If the Peplink WAN Router is already discovered, then directly proceed towards managing it using the **Components – Manage/Unmanage/Delete** page.
3. However, if the target router 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 *Peplink WAN Router* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.



Add Component

Category: All

Component type: Peplink WAN Router

Component information

Host IP/Name: 192.168.10.1

Nick name: peprouter

Monitoring approach

External agents: 192.168.9.137, Agent8247

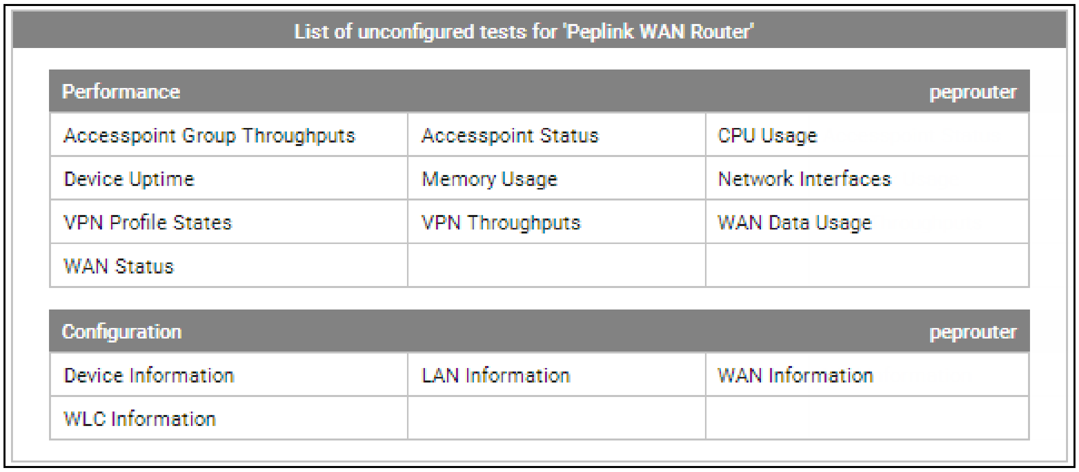
Figure 2.1: Adding the Peplink WAN Router component

5. Specify the **Host IP/Name** and the **Nick name** for the Peplink WAN Router component.

6. Choose an external agent for the target router 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 'Peplink WAN Router'

Performance		peprouter
Accesspoint Group Throughputs	Accesspoint Status	CPU Usage
Device Uptime	Memory Usage	Network Interfaces
VPN Profile States	VPN Throughputs	WAN Data Usage
WAN Status		

Configuration		peprouter
Device Information	LAN Information	WAN Information
WLC Information		

Figure 2.2: A list of tests that need to be configured for the Peplink WAN Router

9. Click on any test in the list of unconfigured tests. To know how to configure the tests, refer to **Monitoring Peplink WAN Router**.

10. Finally, signout of the eG admin interface.

Chapter 3: Monitoring Peplink WAN Router

eG Enterprise offers a special-purpose monitoring model for the Peplink WAN Router to monitor the resource usage and the traffic to and from the target router. Any sudden increase in load or depletion of resources on the router can be instantly detected using the monitored model. This way, the administrators are proactively alerted to the issues and enabled to initiate the remedial actions immediately before the users complain about slowness.

By periodically polling the SNMP MIB of the Peplink WAN Router, eG agents monitor various metrics of interest relating to performance of the target router. Figure 3.1 depicts the layer model of a Peplink WAN Router.

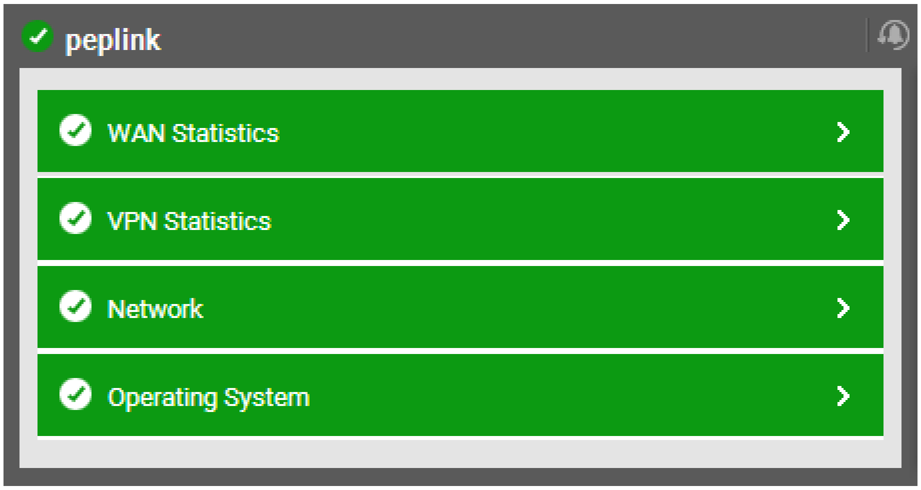


Figure 3.1: Layer model for Peplink WAN Router

Every layer in the Figure 3.1 is mapped to various tests to determine the critical statistics related to the performance of the target router. Using the metrics reported by the tests, administrators can find accurate answers for the following performance queries:

- How well the CPU is utilized by the router?
- How well the memory is utilized by the router?
- What is the current status of each access point connected to the router?
- What is the current state of each VPN profile connected to the router via WAN connection?
- What is the throughtput of VPN profiles?
- What is the current status of each WAN connection to the target router?

- How well the data/packets are transmitted/received through each WAN connection?
- How many packets are actually dropped during transmission/reception?
- How long the router has been up since the last reboot?

Since the tests mapped to the **Network Layer** are elaborately discussed in *Monitoring Cisco Router* document, the sections to come will discuss the other layers in detail.

3.1 Operating System Layer

Using this layer, administrators can figure out the CPU and memory utilization of the Peplink WAN Router.

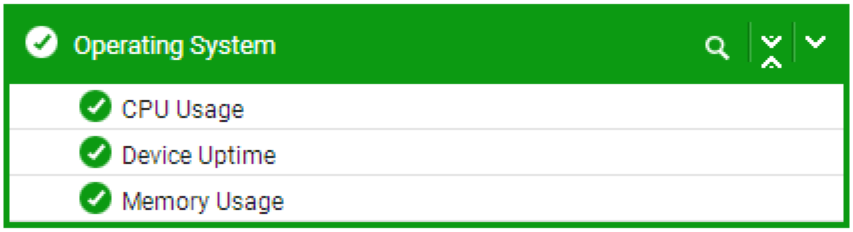


Figure 3.2: The tests associated with the Operating System layer

3.1.1 CPU Usage Test

One of the probable reasons for the poor performance of the Peplink WAN Router is excessive CPU usage. Administrators should hence continuously track how well the router utilizes CPU resources, so that abnormal usage patterns can be proactively detected and corrected to ensure peak performance of the router. This CPU utilization check can be performed using the **CPU Usage** test. At configured intervals, this test monitors the current CPU usage level of the target router.

Target of the test : A Peplink WAN Router

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target router 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.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is

Parameter	Description
	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 host. 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

Parameter	Description
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 usage	Indicates the percentage of CPU utilized by the router.	Percent	Ideally, the value of this measure 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 Device Uptime Test

In most production environments, it is essential to monitor the uptime of the critical network devices such as routers, in the infrastructure. By tracking the uptime of the Peplink WAN Router, administrators can determine what percentage of time the target router 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 router. By knowing that the router has been up for an unusually long time, administrators may come to know that the scheduled reboot task is not working on the router.

This test included in the eG agent monitors the uptime of the target Peplink WAN Router.

Target of the test : A Peplink WAN Router

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target router 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 router. 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

Parameter	Description
	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 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.
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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Is rebooted?</td><td>Indicates whether the router has been rebooted during the last measurement period or not.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>No</td><td>0</td></tr>
<tr><td>Yes</td><td>1</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			Measure Values mentioned above while indicating whether the router is rebooted or not. However, the graph of this measure is indicated using the numeric equivalents.
Uptime	Indicates the time period that the router has been up since the last time this test ran.	Seconds	If the router 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 router 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 router 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	Indicates the total time that the router has been up since its last reboot.	Minutes	Administrators may wish to be alerted if a router has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions.

3.1.3 Memory Usage Test

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

Target of the test : A Peplink WAN Router

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target router 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.
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 target host. 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

Parameter	Description
	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**.

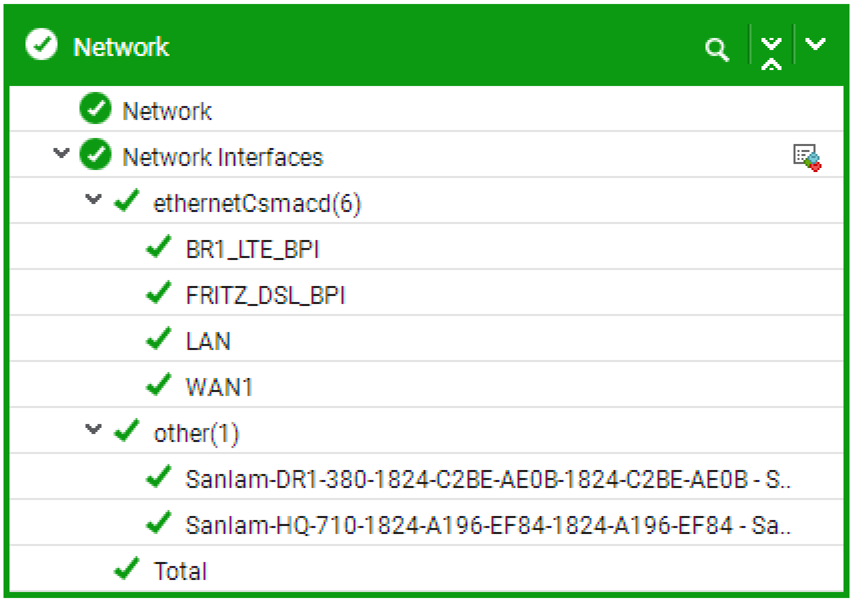
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total memory	Indicates the total amount of memory allocated to the router.	MB	
Used memory	Indicates the amount of memory that is currently	MB	A low value is desired for this measure.

Measurement	Description	Measurement Unit	Interpretation
	used by the router.		
Free memory	Indicates the amount of memory that is available for use on the router.	MB	A high value is desired for this measure.
Memory utilization	Indicates the percentage of memory utilized by the router.	Percent	If the value of this measure is close to 100%, it is indicative of a memory bottleneck at the router.

3.2 The Network Layer

Using the test mapped to this layer, administrators can figure out the uptime of the target router and in the process identify when exactly the router was restarted. In addition, administrators can also easily assess the quality of network connections to and from the router, and the overall health, speed, and bandwidth usage of the network interfaces supported by the router.



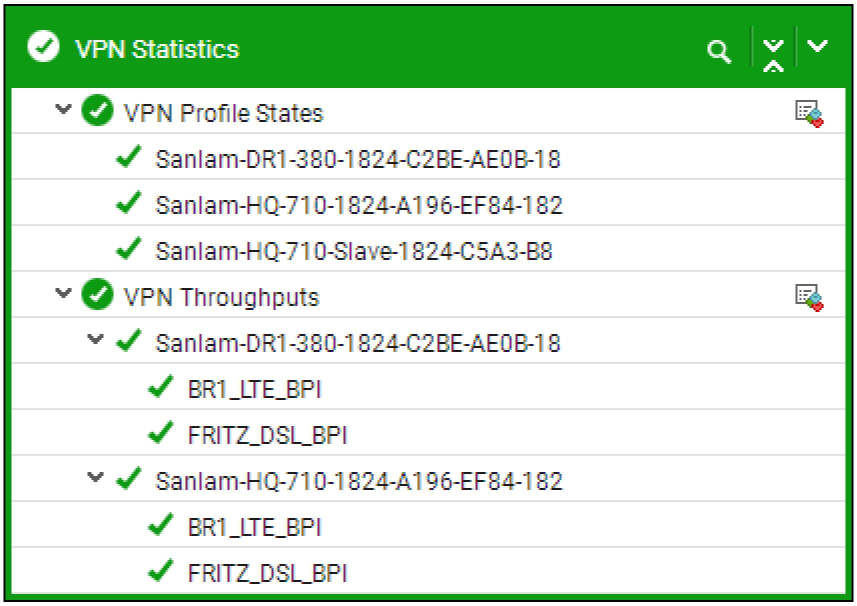
Network
- ✓ Network
- ✓ Network Interfaces
  - ✓ ethernetCsmacd(6)
    - ✓ BR1_LTE_BPI
    - ✓ FRITZ_DSL_BPI
    - ✓ LAN
    - ✓ WAN1
  - ✓ other(1)
    - ✓ Sanlam-DR1-380-1824-C2BE-AE0B-1824-C2BE-AE0B - S..
    - ✓ Sanlam-HQ-710-1824-A196-EF84-1824-A196-EF84 - Sa..
  - ✓ Total

Figure 3.3: The test mapped to the Network layer

To know how to configure the tests mapped to this layer, refer to the *Monitoring Cisco Router* document and *Monitoring Unix and Windows Servers* document.

3.3 VPN Statistics Layer

Using the tests mapped to this layer, administrators can easily find out the status of VPN profiles and also determine the throughput of the WAN connections that are established based on the VPN profiles.



VPN Statistics

- VPN Profile States
  - Sanlam-DR1-380-1824-C2BE-AE0B-18
  - Sanlam-HQ-710-1824-A196-EF84-182
  - Sanlam-HQ-710-Slave-1824-C5A3-B8
- VPN Throughputs
  - Sanlam-DR1-380-1824-C2BE-AE0B-18
    - BR1_LTE_BPI
    - FRITZ_DSL_BPI
  - Sanlam-HQ-710-1824-A196-EF84-182
    - BR1_LTE_BPI
    - FRITZ_DSL_BPI

Figure 3.4: The tests mapped to the VPN Statistics layer

3.3.1 VPN Profile States Test

A VPN, or Virtual Private Network, allows you to create a secure connection to another network over the Internet. To establish the secure connection and to reduce manual effort, administrators use VPN profiles. The VPN profiles include a wide range of necessary connection settings and security settings that are required for the end-users to stay connected to the network via the VPN tunnel. Therefore, it is imperative that the administrators should periodically check if the VPN profile is authenticated or connected or routed properly. Administrators can easily do this check using the **VPN Profile States** test!

This test auto-discovers the VPN profiles on the target Peplink WAN Router and reports the current status of each VPN profile. When the users complain about the issues in establishing connection using the VPN profiles, administrators can use this test to figure out if the VPN profile is stuck in the authentication process or tunnel processing or routing for longer duration. By knowing this detail, administrators can initiate necessary actions to prevent delay in processing the user requests and improve the user experience.

Target of the test : A Peplink WAN Router

Agent deploying the test : An external agent

Outputs of the test : One set of results for each VPN profile on the target router.

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 target host. 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.

Parameter	Description
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
Status	Indicates the current status of this VPN profile.		The values that this measure can report and the numeric values they indicate

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Start</td><td>0</td></tr>
<tr><td>Authenticate</td><td>1</td></tr>
<tr><td>Tunnel</td><td>2</td></tr>
<tr><td>Route</td><td>3</td></tr>
<tr><td>Connected</td><td>4</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b>s mentioned above while indicating the current status of each VPN profile. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

3.3.2 VPN Throughputs Test

When users complain of slowness of the VPN sessions, administrators should first check the throughput of the VPN connections. Throughput reveals how well/badly the VPN tunnel processes network traffic. Low throughput is an indicator of bursty network traffic, which can cause users to experience slowness when interacting through the router. To receive real-time insights into the throughput of the VPN profiles, administrators can use the **VPN Throughputs** test. This test measures the throughput in real-time and alerts administrators if the throughput is low. Additionally, the test also reveals where the bottleneck is - during data reception/transmission?

For each WAN connection established based on the VPN profiles on the target router, this test reports the amount of data sent and received, the number of packets dropped during packet transmission and the time taken for data/packet transmission. The metrics reported by this test help administrators to identify the WAN connections through which the target router experienced more packet loss and transmission delay. Using this revelation, administrators can take remedial actions to alleviate the errors that caused the above-mentioned issues and enhance the user experience.

Target of the test : A Peplink WAN Router

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *VPN profile:WAN connection* that is connected to the target router.

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 target router. 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.

Parameter	Description
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**.

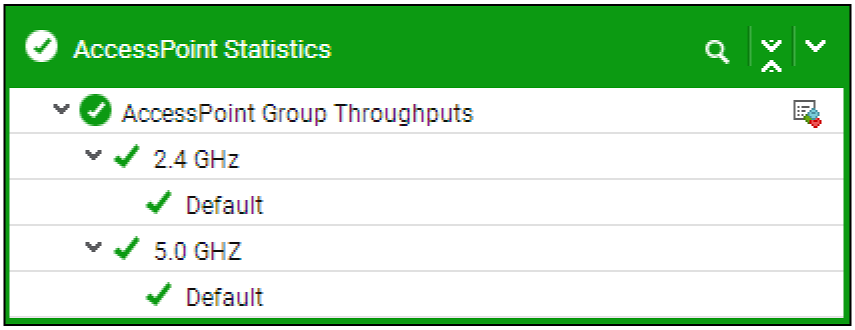
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Transmitted data	Indicates the rate at which data was sent through this	MB/sec	Compare the value of these measures across the WAN connections to figure

Measurement	Description	Measurement Unit	Interpretation
	WAN connection during the last measurement period.		out the WAN connection through which the maximum amount of data was transmitted/received.
Received data	Indicates the rate at which data was received through this WAN connection during the last measurement period.	MB/sec	
Dropped packets	Indicates the number of packets dropped during packet transmission through this WAN connection.	Packets	A low value is desired for this measure.
Latency	Indicates the time taken by this WAN connection for data transmission.	Milliseconds	A low value is desired for this measure. Compare the value of this measure across the WAN connections to identify the slow WAN connection.

3.4 AccessPoint Statistics Layer

The tests mapped to this layer monitor the access points and the access point groups created for the target Peplink WAN Router. These tests report the current status of the access points and the critical measures related to data/packtes transmission through each access point group. By analyzing the metrics reported by this test, administrators can easily find out the throughput of each access point group.



AccessPoint Statistics
- AccessPoint Group Throughputs
  - 2.4 GHz
    - Default
  - 5.0 GHZ
    - Default

Figure 3.5: The test mapped to the AccessPoint Statistics layer

3.4.1 AccessPoint Status Test

In a wireless local area network (WAN), an access point is a station that transmits and receives data (sometimes referred to as a transceiver). The access point connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. Each access point can serve multiple users within a defined network area. If multiple access points are not available for the users to connect, then the users may not be able to connect to the WAN. To avoid such severe hardship, administrators should continuously monitor the access points round the clock. The **AccessPoint Status** test helps administrators in this regards!

This test auto discovers the access points of the target router and reports the current status of each access point. Using this test, administrators can instantly find out the access point that is currently offline.

Target of the test : A Peplink WAN Router

Agent deploying the test : An external agent

Outputs of the test : One set of results for each WAN that is connected to the target router.

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 target host. 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>Status</td><td>Indicates the current status of this access point.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Offline</td><td>0</td></tr>
<tr><td>Online</td><td>3</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b>s mentioned above while indicating the current status of each access point. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

3.4.2 Accesspoint Group Throughputs Test

The Peplink WAN router is associated with multiple access points to serve a large number of WAN users. To manage the access points and simplify the load distribution among the users, administrators create access point groups. By default, the target router is automatically created with a default access point group which can have up to 16 access points. However, administrators can create multiple access point groups using the web admin interface. Using the access point groups so created, administrators can easily share the load among the users and manage the access points without any hassles. Administrators may also wish to calculate the throughput of the access point groups to find out how well/badly the access point groups handle the network traffic in the environment. Poor traffic handling by the access point groups may result in low throughput which indicates bursty network traffic in the environment. This in turn can cause WAN users to experience slowness when interacting through the router. To prevent such eventualities, it is important for the administrators to check the throughput of the access point groups at regular intervals. For this purpose, administrators can use the **Accesspoint Groups Throughputs** test!

This test auto-discovers the access point groups, and reports the amount of data sent and received and the number of packets transmitted and received by each access point group. Using this test, administrators can easily identify the access point group that handled the higher level of traffic to the router.

Target of the test : A Peplink WAN Router

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *access point group* created on the target router.

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 target router. 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

Parameter	Description
	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 • **AES** – Advanced Encryption Standard

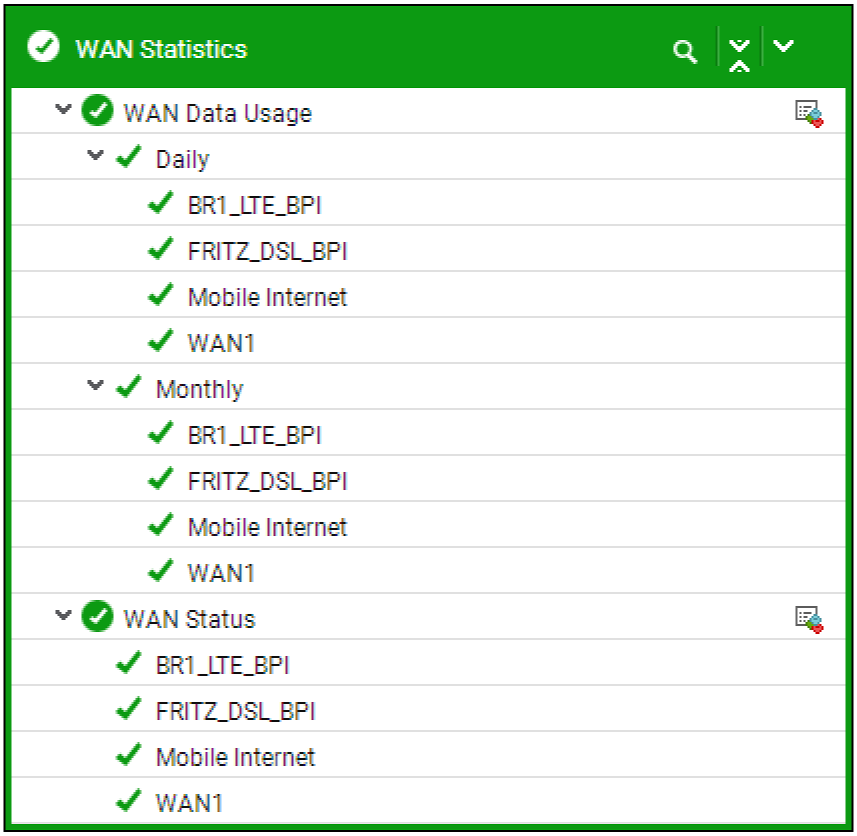
Parameter	Description
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data 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

Measurement	Description	Measurement Unit	Interpretation
Data Transmitted	Indicates the rate at which the data was transmitted from this access point group.	Bytes/sec	Comparing the values of these measures will reveal the access point group that transmitted/received the maximum amount of data.
Data received	Indicates the rate at which the data was received by this access point group.	Bytes/sec	
Packets transmitted	Indicates the number of packets transmitted from this access point group.	Packets	Compare the values of these measures to identify the access point group that transmitted/received the maximum number of packets.
Packets Received	Indicates the number of packets received by this access point group.	Packets	

3.5 WAN Statistics Layer

The tests associated with the WAN Statistics layer and the measures reported by them provide in-depth insights into the data sent and received through each WAN connection at different time frequencies. In addition, the status of the WAN connection is also monitored round the clock and reported.



WAN Statistics

- WAN Data Usage
  - Daily
    - BR1_LTE_BPI
    - FRITZ_DSL_BPI
    - Mobile Internet
    - WAN1
  - Monthly
    - BR1_LTE_BPI
    - FRITZ_DSL_BPI
    - Mobile Internet
    - WAN1
- WAN Status
  - BR1_LTE_BPI
  - FRITZ_DSL_BPI
  - Mobile Internet
  - WAN1

Figure 3.6: The tests mapped to the WAN Statistics layer

3.5.1 WAN Data Usage Test

This test auto-discovers the WAN connections to the target router, and for each WAN connection reports the amount of data received and transmitted during different time periods. Using the metrics reported by this test, administrators can track the traffic through each WAN connection on a daily and monthly basis.

Target of the test : A Peplink WAN Router

Agent deploying the test : An external agent

Outputs of the test : One set of results for each WAN connection that is established to the target router.

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.
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 target router. 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

Parameter	Description
	• **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
Transmitted data	Indicates the amount of data transmitted through this WAN connection.	MB	Compare the values of these measures across the WAN connections to identify the WAN connection that is transmitting and receiving the maximum amount of data.
Received data	Indicates the amount of data received through this WAN connection.	MB	

3.5.2 WAN Status Test

This test auto-discovers the WAN connections that are established to the target router, and reports the current status of each WAN connection. With the help of this test, administrators can easily find out the WAN connections that are currently connected to/disconnected from the router and can also identify the unhealthy /disabled connections. By analyzing the states reported by this test, administrators can initiate further investigation to exactly figure out the reason on why the connections were in Disconnected state or Unhealthy state or Disabled state.

Target of the test : A Peplink WAN Router

Agent deploying the test : An external agent

Outputs of the test : One set of results for each WAN connection established to the target router 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.
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 target router. 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.

Parameter	Description
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
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.

Parameter	Description
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>Status</td><td>Indicates the current status of this WAN connection.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Unknown</td><td>0</td></tr>
<tr><td>Connected</td><td>3</td></tr>
<tr><td>Connecting</td><td>4</td></tr>
<tr><td>Activating</td><td>5</td></tr>
<tr><td>Health Check Fail</td><td>6</td></tr>
<tr><td>Disconnected</td><td>8</td></tr>
<tr><td>Disabled</td><td>9</td></tr>
</table>
<b>Note:</b>
By default, this measure can report the <b>Measure Value</b>s mentioned above while indicating the current status of each WAN connection. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

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.