Monitoring Juniper MX Router

eG Innovations Product Documentation

eG

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The Juniper MX-Series Router runs on Junos OS i.e. a reliable, high-performance, modular network operating system that is supported across all of Juniper's physical and virtual routing, switching, and security platforms. The Juniper MX Series routers can be deployed as IP/IP VPN edge routers, Ethernet VPN (EVPN) and virtual private LAN service (VPLS) provider edge (VPLS-PE) routers, MPLS label-switching (LSR) routers, and as Layer2 Ethernet switches or Layer3 IP routers. The Juniper MX router is designed to offer the following features:

- **High availability** - Non-Stop Routing (NSR), Non-Stop Bridging (NSB), Graceful Routing Engine Switchover (GRES), Graceful Restart (GR), and In-Service Software Upgrade (ISSU)

- **Routing** - RIP, OSPF, IS-IS, BGP, and Multicast

- **Switching** - Full suite of Spanning Tree Protocols (STP), Service Provider VLAN tag manipulation, QinQ, and the ability to scale beyond 4,094 bridge domains by leveraging virtual switches

- **Inline services** - Network Address Translation (NAT), IP Flow Information Export (IPFIX), Tunnel Services, and Port Mirroring

- **MPLS** - L3VPN, L2VPNs, and VPLS

- **Broadband services** - PPPoX, DHCP, Hierarchical QoS, and IP address tracking

- **Virtualization** - Multi-Chassis Link Aggregation, Virtual Chassis, Logical Systems, Virtual Switches

With such a large feature set, the use case of the Juniper MX router is very broad. It's common to see it in the core of a Service Provider network, providing BNG, or in the Enterprise providing edge routing or core switching.

Owing to the popularity and use cases of the MX router, it becomes essential for administrators to keep an eye on the health and functions of the core components of the MX router to ensure that users receive continued connectivity to the services of their interest. For this purpose, eG offers a specialized monitoring model for continuously monitoring the MX router and pointing you to the abnormalities in the CPU load, health, memory utilization and network latency on the MX router.

Chapter 2: How to Monitor Juniper MX Router Using eG Enterprise?

eG Enterprise monitors the Juniper MX Router using an eG external agent on a remote host. This eG agent polls the SNMP MIB of the MX Router to gather the statistics related to the MX Router at configured intervals. Before attempting to monitor the MX Router, ensure that the router is SNMP-enabled. To start monitoring the target router, first manage the Juniper MX Router component using the eG admin interface. The procedure for achieving this is discussed in the following section.

2.1 Managing the Juniper MX Router

eG Enterprise can automatically discover the Juniper MX Router, and also lets to manually add the component for monitoring using eG admin interface. To manage a Juniper MX Router component, do the following:

1. Log into the eG admin interface.

2. If the Juniper MX Router is already discovered, then directly proceed towards managing the broker using the **COMPONENTS – MANAGE/UNMANAGE** page.

3. However, if you are yet to discover the Juniper MX Router, then run discovery (Infrastructure -> Components -> Discover) 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.

4. Click on the **Add new Component** button after choosing the *Juniper MX Router* from the **Component Type** drop down list in the **Components** page. This will lead you to the **Add Component** page (Figure 2.1). Remember that components manually added are managed automatically.

Figure 2.1: Adding a Juniper MX Router component

5. Specify the **Host IP/Name** and the **Nick name** of the Juniper MX Router in Figure 2.1.

6. Then, pick an external agent from the **External agents** list box and click the **Add** button to add the component for monitoring.

7. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.

LIST OF UNCONFIGURED TESTS FOR 'JUNIPER ROUTER MX SERIES'		
PERFORMANCE		**MXR**
BGP Environment	CPU Load	CPU Utilization
Device Latency	Device Uptime	Environment Status
Host Resources	Kernel Memory	Memory
Network Interfaces	Temperature	

Figure 2.2: List of Unconfigured tests to be configured for the Juniper MX Router

8. Click on the tests to configure them. To know how to configure these tests, refer to the **Monitoring Juniper MX Router** chapter.

9. To configure the details on configuring the **Network Interfaces** test, refer to *Monitoring Cisco Router* document.

10. Once the **Network Interfaces** test is configured, signout of the eG administrative interface.

Chapter 3: Monitoring Juniper MX Router

The eG Enterprise includes a specialized monitoring model for continuously monitoring the Juniper MX routers. By periodically polling the SNMP MIBs of the target MX Router, the eG external agent pulls out various metrics of interest relating to performance of the MX Routers. Figure 1 depicts the layer model of a Juniper MX router.
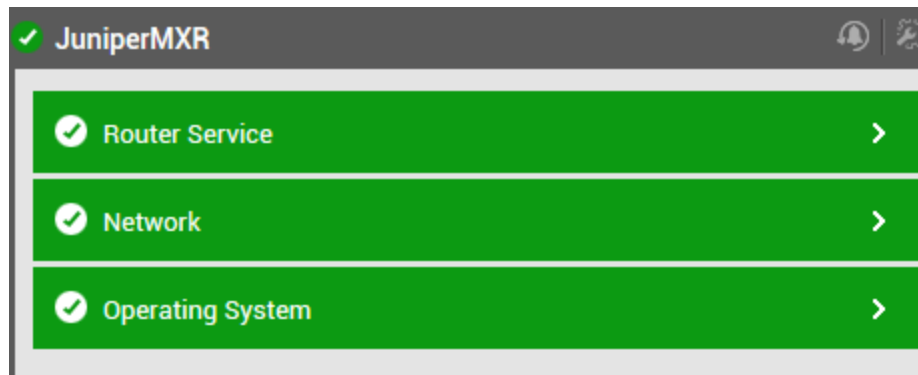

Figure 3.1: The layer model of the Juniper MX Router

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

- Is any of the hardware components of the target router choking due to the excessive CPU load?

- Is there any hardware component of the target router down or running at abnormal speed?

- How well the kernel memory is utilized by the router?

- Which BGP peer is busy processing more number of messages?

- Which type of Real-time performance monitoring (RPM) probe is measuring high latent value?

The tests mapped to the **Network Layer** has already been discussed in the *Monitoring Cisco Routers* document. Therefore, the tests mapped to the **Router Services** and **Operating System** layers will be discussed in the following sections.

3.1 Operating System Layer

This layer tracks the current CPU load, and the current status of each hardware component of the Juniper MX Router. In addition, kernel memory utilization of the MX router is also revealed.
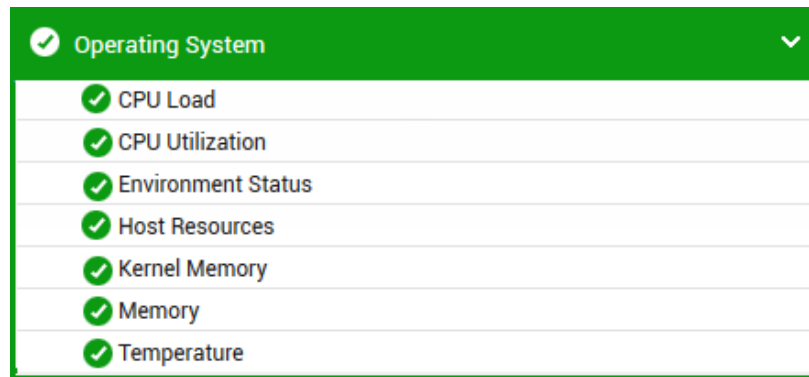
Figure 3.2: The tests mapped to the Operating System layer

3.1.1 Environment Test

The chassis of the Juniper MX router is a rigid sheet-metal structure that houses all other router components. The hardware components in the MX router are:

- Craft interfaces panel

- Cooling system

  - Fan tray

  - Filter tray

  - Filter kit

- Host subsystem

  - Routing Engine

  - Switch and Control Board (SCB). The SCB

- Interface modules

  - DPC

  - DPC or SCB blank panel

  - FPC

  - MIC

  - MIC blank panel

  - MPC

  - PIC

  - Transciever

- Power system

    ○ Power distributionmodule (PDM)

    ○ AC power supply

    ○ DC power supply

    ○ Power supply blank panel

Good health and smooth functioning of the above-said components is vital for proper functioning of the target router. If any of the components is down/inactive or running in abnormal speed or put in stand by mode for longer time than usual , then this may halt the operations of router temporarily or permanently. To avoid such inconveniences, administrators should track the state of each hardware component continuously. Administrators can use the **Environment** test to achieve this.

With the help of this test, administrators can instantly detect the current status of each hardware component of the target router, so that remedial measures can be swiftly initiated to prevent any irrepairable damage to the components and the router.

Target of the test : A Juniper MX router

Agent deploying the test : An external agent

Outputs of the test : One set of results for each hardware component of the Juniper MX router that is to be monitored.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco Router.
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 firewall. 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

Parameters	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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
State	Indicates the current status of this hardware component.		The values reported by this measure and its numeric equivalents are mentioned in the table below: | Measure Value	Numeric Value
---	---
Unknown	1
Running	2
Ready	3
Reset	4
Running at full speed	5
Down	0
Standby	7	 **Note:** By default, this measure reports one of the **Measure Value**s listed in the table

Measurement	Description	Measurement Unit	Interpretation
			above to indicate the current status of each hardware component. In the graph of this measure however, the status will be represented using the numeric equivalents only.

3.1.2 Kernel Memory Test

The Juniper MX router runs on the Junos OS that is a purpose-built networking operating system based on one of the most stable and secure operating systems in the world: FreeBSD. Junos software was designed as a monolithic kernel architecture that places all of the operating system services in the kernel memory space. To ensure all of the operating system services are running without any glitches due to the lack of memory on the kernel space, it is essential to track how well the memory is being utilized from the kernel space allocated on the target router. Using the **Kernel Memory** test, administrators can monitor the kernel memory utilization of the router.

Target of the test : A Juniper MX router

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Juniper MX router that is to be monitored.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the Juniper MX Router.
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 firewall. 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

Parameters	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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Used memory utilization	Indicates the percentage of kernel memory utilized on the target MX router.	Percent	A low value is desired for this measure. A consistent increase in this value could be a cause for some serious concern, as it indicates a gradual, but steady erosion of valuable memory resources. If this unhealthy trend is not addressed soon, it could severely impact the services on the router and degrade the overall performance of the router.

3.2 Router Service Layer

This layer tracks the current status and message processing capability of each BGP peer connected to the target Juniper MX Router. Besides, this layer also captures the network latency collected by various Real-time performance monitoring (RPM) probes.

Figure 3.3: The tests mapped to the Router Service layer

3.2.1 BGP Environment Test

BGP is an exterior gateway protocol (EGP) that is used to exchange routing information among routers in different autonomous systems (ASs). BGP routing information includes the complete route to each destination. BGP uses the routing information to maintain a database of network reachability information, which it exchanges with other BGP systems. BGP uses the network reachability information to construct a graph of AS connectivity, which enables BGP to remove routing loops and enforce policy decisions at the AS level. BGP allows for policy-based routing. You can use routing policies to choose among multiple paths to a destination and to control the redistribution of routing information.

The Junos OS routing protocol software on the Juniper MX router supports BGP version 4. This version of BGP adds support for Classless Interdomain Routing (CIDR), which eliminates the concept of network classes. Instead of assuming which bits of an address represent the network by looking at the first octet, CIDR allows you to explicitly specify the number of bits in the network address, thus providing a means to decrease the size of the routing tables. BGP version 4 also supports aggregation of routes, including the aggregation of AS paths.

This test auto-discovers the BGP peers connected to the target Juniper MX router and for each BGP peer, reports the current status and the count of messages transmitted and received through each BGP peer. This way, administrators may identify the BGP peer that is active/idle/connected and also find out the peer that transmits more number of messages to the target router.

Target of the test : A Juniper MX router

Agent deploying the test : An external agent

Outputs of the test : One set of results for each hardware component of the Juniper MX router that is to be monitored.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the Juniper MX Router.
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 firewall. 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:

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
State	Indicates the current status of this BGP peer.		BGP forms a TCP session with neighbor routers called peers. BGP uses the Finite State Machine (FSM) to maintain a table of all BGP peers and their operational status.
			The values reported by this measure

Measurement	Description	Measurement Unit	Interpretation
			and its numeric equivalents are mentioned in the table below: | Measure value	Numeric Value
---	---
Idle	1
Connect	2
Active	3
Open present	4
Open confirm	5
Established	6	 **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate the current status of each BGP peer. The graph of this measure however, is represented using the numeric equivalents only.
Received message	Indicates the number of messages received by this BGP peer.	Number	Comparing the values of these measures across the BGP peers will help you identify the BGP peer that is busy processing messages.
Transmitted message	Indicates the number of messages transmitted through this BGP neighbor.	Number	

3.2.2 Device Latency Test

Real-time performance monitoring (RPM) is a service available in Junos OS that enables a router to measure metrics such as round-trip delays and unanswered echo requests. Typically, network performance is assessed in real time based on the jitter, delay, and packet loss experienced on the network. To achieve this, RPM exchanges a set of probes with other IP hosts in the network for monitoring and network tracking purposes. These probes are sent from a source node to other destination devices in the network that require tracking. Data such as transit delay and jitter can be collected from these probes, and this data can be used to provide an approximation of the delay and jitter experienced by live traffic in the network. Different live traffic metrics like round-trip time (RTT),

positive egress jitter, negative egress jitter, positive ingress jitter, negative ingress jitter, positive round-trip jitter, and negative round-trip jitter can be gleaned from the results. RPM calculates minimum, maximum, average, peak-to-peak, standard deviation, and sum calculations for each of these measurements. RPM probes can also be used to verify the path between BGP neighbors.

This test auto-discovers the RPM probe types and reveals the network delay collected by each RPM probe type. This way, the test points to the highly latent network paths that could be disrupting traffic in the network.

Target of the test : A Juniper MX router

Agent deploying the test : An external agent

Outputs of the test : One set of results for each RPM probe type.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the Juniper MX Router.
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 firewall. 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

Parameters	Description
	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.
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

Parameters	Description
	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
Latency	Indicates the time delay measured as result of this RPM probe type.	Microseconds	A high value is a cause for concern, as it indicates a potentially latent function.

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.