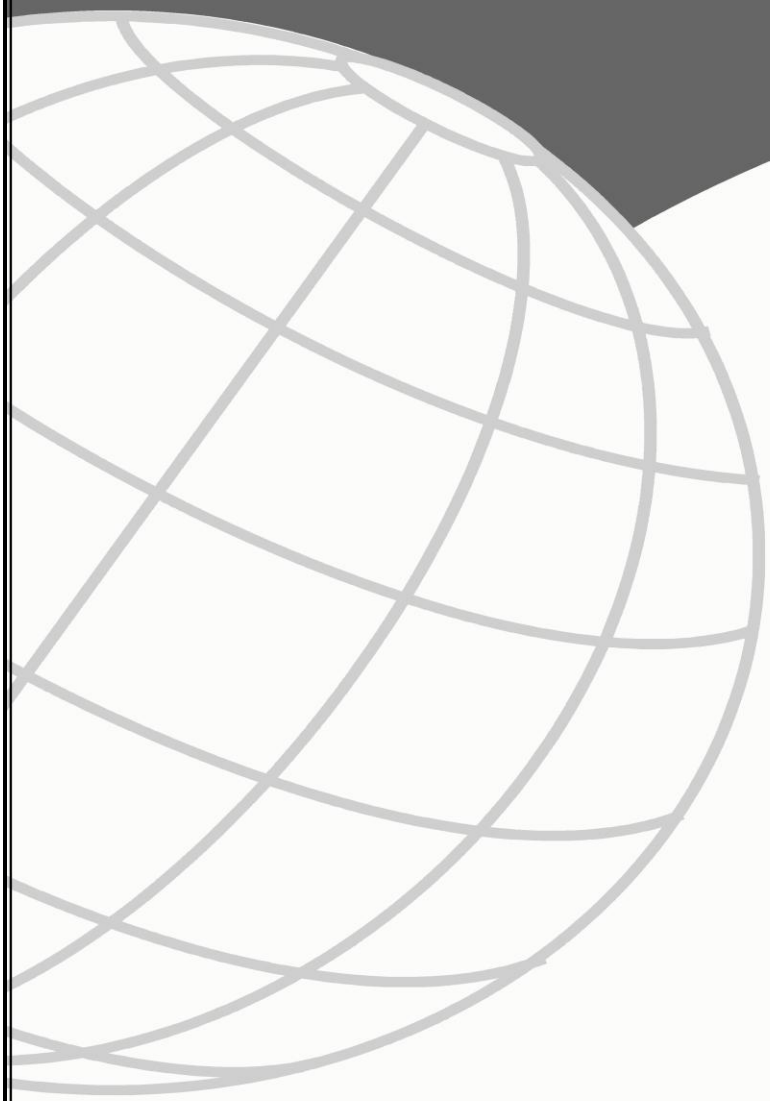

Monitoring Juniper EX Switch

eG Enterprise v6

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows NT, Windows 2003, and Windows 2000 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

Table of Contents

1

Monitoring Juniper EX Switch

Juniper EX Series Ethernet switches deliver access, aggregation, and core layer switching services in branch, campus, and data center networks to ensure fast, secure, reliable delivery of data and applications.

All EX Series Ethernet Switches address escalating demands for high availability, unified communications, mobility and virtualization within enterprise networks. The EX Series switches increase competitiveness and contribute to business success by delivering operational efficiency, business continuity, and network agility for end-to-end enterprise environments.

If this switch, which assures service operators of continuous network connectivity and secure transaction of business, starts malfunctioning suddenly, the connection to mission-critical services will be lost, thereby causing irreparable damage to reputation and revenue. It is therefore imperative that the operations of the Juniper Ex Switch are monitored 24 x 7.

eG Enterprise provides a specialized *Juniper EX Switch* monitoring model (see Figure 1), which periodically polls the SNMP MIB of the switch to measure the CPU usage, temperature and memory of each hardware component of the switch and notifies administrators of potential resource crunches and failures of the power supply, fans etc.

Figure 1: The layer model of the Juniper EX Switch

Using the metrics reported , administrators can find quick and accurate answers for the following performance questions:

- Is the CPU utilization of each hardware component optimal? If not, which hardware component is utilizing the emaximum CPU?
- Which hardware component is consuming the maximum memory resources? Is the buffer memory and heap memory allocated to each hardware component utilized effectively?
- Is the temperature maintained optimally for all the hardware components of the Juniper EX Switch?
- Is any VPN tunnel hogging the bandwidth resources? If so, which one is it?
- Are too many fragmented packets flowing through the firewall? If so, why? Is it because of an incorrect configuration?
- What is the mode of the routing engine available in the Juniper EX Switch?

The **Network** layer of the *Juniper EX Switch* model is similar to that of a *Windows Generic* server model. Since these tests have been dealt with in the *Monitoring Unix and Windows Servers* document, Section 1.1 focuses on the **Operating System** layer.

1.1 The Operating System Layer

This layer tracks the current CPU usage, memory, temperature and the uptime of each hardware component of the Juniper EX Switch. Besides this, this layer helps you in identifying the number of trap messages that were sent by the switch for failures of the power supply units , fans and abnormal deduction in temperature of the hardware components.

Figure 2: The tests mapped to the Firewall Service layer

1.1.1 CPU Utilization Test

This test monitors the current CPU utilization of each hardware component available in the Juniper EX Switch and reports whether/not the hardware component is consuming too much of CPU resources.

Purpose	Monitors the current CPU utilization of the Juniper EX Switch
Target of the test	A Juniper EX Switch
Agent deploying the test	An external agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Juniper EX Switch 3. **SNMPPORT** – The SNMP Port number of the Juniper EX Switch (161 typically) 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.

	6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **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 Juniper EX Switch over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of the test	One set of results for each hardware component of the Junpier EX Switch that is to be monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	CPU utilization: Indicates the percentage of CPU utilized by this hardware component.	Percent	A very high value of this measure indicates a CPU bottleneck. Comparing the value of this measure across the hardware components will help you in identifying the component that is using the CPU resources at its maximum.

1.1.2 Uptime Test

This test measures the uptime of each hardware component of the Juniper EX Switch and reports administrators if any hardware component has been running without reboot for a longer period of time.

Purpose	Measures the uptime of each hardware component of the Juniper EX Switch and reports administrators if any hardware component has been running without reboot for a longer period of time
Target of the test	A Juniper EX Switch
Agent deploying the test	An external agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Juniper EX Switch 3. **SNMPPORT** – The SNMP Port number of the Juniper EX Switch (161 typically) 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.

<table>
<tr><td></td><td colspan="3">
7. AUTHPASS – Specify the password that corresponds to the above-mentioned USERNAME. This parameter once again appears only if the snmpversion selected is v3.
8. CONFIRM PASSWORD – Confirm the AUTHPASS by retyping it here.
9. 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
10. ENCRYPTFLAG – This flag appears only when v3 is selected as the SNMPVERSION. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option.
11. ENCRYPTTYPE – If the ENCRYPTFLAG is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types:
➢ DES – Data Encryption Standard
➢ AES – Advanced Encryption Standard
12. ENCRYPTPASSWORD – Specify the encryption password here.
13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.
14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.
15. 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 Juniper EX Switch over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.
</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each hardware component of the Juniper EX Switch that is to be monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Uptime:
Indicates the total time this hardware component has been up since the last reboot.</td><td>Mins</td><td>Administrators may wish to be alerted if a hardware component has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions.</td></tr>
</table>

1.1.3 Memory Test

This test reports the total memory allocated to each hardware component of the target Juniper EX Switch. Using this test, you can monitor the buffer memory utilization and heap memory utilization of each hardware component. This way, you can identify the hardware component that is running short of memory.

Purpose	reports the total memory allocated to each hardware component of the target Juniper EX Switch. Using this test, you can monitor the buffer memory utilization and heap memory utilization of each hardware component.
Target of the test	A Juniper EX Switch
Agent deploying the test	An external agent.
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Juniper EX Switch 3. **SNMPPORT** – The SNMP Port number of the Juniper EX Switch (161 typically) 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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

<table>
<tr><td></td><td colspan="3">10. ENCRYPTFLAG – This flag appears only when v3 is selected as the SNMPVERSION. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option.
11. ENCRYPTTYPE – If the ENCRYPTFLAG is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types:
➢ DES – Data Encryption Standard
➢ AES – Advanced Encryption Standard
12. ENCRYPTPASSWORD – Specify the encryption password here.
13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.
14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.
15. 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 Juniper EX Switch over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each hardware component of the target Juniper EX Switch that is to be monitored</td></tr>
<tr><td rowspan="3">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Memory:
Indicates the total memory allocated to this hardware component.</td><td>MB</td><td></td></tr>
<tr><td>Buffer utilization:
Indicates the percentage of buffer memory utilized by this hardware component.</td><td>Percent</td><td>A low value is desired for this measure. A gradual/sudden increase in the value of this measure is a cause of concern which indicates that the buffer memory is running short of resources. You can either increase the size of the buffer memory or free up the space that is already utilized to contain the value of this measure within possible limits.
Comparing the value of this measure across the hardware components will help you in identifying the hardware component that is utilizing the memory resources extensively.</td></tr>
</table>

	Heap utilization: Indicates the percentage of heap memory utilized by this hardware component.	Percent	

1.1.4 Temperature Test

This test monitors the temperature of each hardware component of the target Juniper EX switch and alerts if any abnormalities are detected.

Purpose	Monitors the temperature of each hardware component of the target Juniper EX switch and alerts if any abnormalities are detected
Target of the test	A Juniper EX Switch
Agent deploying the test	An external agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Juniper EX Switch 3. **SNMPPORT** – The SNMP Port number of the Juniper EX Switch (161 typically) 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.

<table>
<tr><td></td><td colspan="3">9. 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
10. ENCRYPTFLAG – This flag appears only when v3 is selected as the sNMPVERSION. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option.
11. ENCRYPTTYPE – If the encryptflag is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types:
➢ DES – Data Encryption Standard
➢ AES – Advanced Encryption Standard
12. ENCRYPTPASSWORD – Specify the encryption password here.
13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.
14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.
15. 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 Juniper EX Switch over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each hardwarecomponent of the Juniper EX Switch that is to be monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Temperature:
Indicates the current temperature of this hardware component.</td><td>Celsius</td><td>A gradual/sudden increase in the value of this measure is a cause of concern which could eventually result in the failure of the hardware component.</td></tr>
</table>

1.1.5 Temperature Traps Test

Temperature fluctuation of hardware components, if not promptly detected and resolved, can prove to be fatal to the availability and overall health of a Juniper EX Switch. This test intercepts the temperature traps sent by the hardware components of the switch, extracts information related to temperature errors/failures from the traps, and reports the count of these trap messages to the eG manager. This information enables administrators to detect current

temperature and potential failure of the hardware components due to a sudden shoot up of temperature, understand the nature of these failures, and accordingly decide on the remedial measures.

<table>
<tr><td>Purpose</td><td>Intercepts the temperature traps sent by the hardware components of the switch, extracts information related to temperature errors/failures from the traps, and reports the count of these trap messages to the eG manager</td></tr>
<tr><td>Target of the test</td><td>A Juniper EX Switch</td></tr>
<tr><td>Agent deploying the test</td><td>An external agent</td></tr>
<tr><td>Configurable parameters for the test</td><td>
1. TESTPERIOD - How often should the test be executed
2. HOST - The host for which the test is to be configured.
3. SOURCEADDRESS - Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
4. OIDVALUE - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:
<table>
<tr><th>OID</th><th>Value</th></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.2</td><td>Host_system</td></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.3</td><td>NETWORK</td></tr>
</table>
In this case the OIDVALUE parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.
An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*.
Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID .1.3.6.1.4.1.9156.1.1.2 is found to be HOST and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your OIDVALUE specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be:
Trap5: .1.3.6.1.4.1.9156.1.1.5-any.
</td></tr>
</table>

<table>
<tr><td></td><td colspan="3">5. SHOWOID – Specifying true against SHOWOID will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter false, then the values alone will appear in the detailed diagnosis page, and not the OIDs.
6. TRAPOIDS – By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified SOURCEADDRESSes. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the TRAPOIDS text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing spaces.
7. DD FREQUENCY - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying none against DD FREQUENCY.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each type of event that occurred on the target Juniper EX Switch</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Temperature alerts:
Indicates the number of times this event was triggered during the last measurement period.</td><td>Number</td><td>The failure events may be generated due to the temperature failure of the hardware components of the Juniper EX Switch. If the failure events are not rectified within a certain pre-defined timeperiod, the switch will be shutdown automatically.
Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Juniper EX Switch.</td></tr>
</table>

1.1.6 Power Supplies Test

The chassis of the Juniper EX Switch is a rigid sheet-metal structure that houses the hardware components. The field-replaceable units (FRUs) in the EX series switches are:

- Power supply
- Fan tray
- Uplink module
- SFP transceiver
- SFP+ transceiver

- XFP transceiver

The power supply in the switches is a hot-removable and hot-insertable field-replaceable unit (FRU) that you can install on the rear panel without powering off the switch or disrupting the switching function. Some of the EX series switches have an internal redundant power supply, making the power supply fully redundant.

Abnormal power fluctuation to the hardware components often lead to the malfunctioning of the Juniper EX Switch which when left unnoticed can prove to be fatal to the availability and overall health. This test intercepts the traps sent by the switch, extracts information related to power supply failures from the traps, and reports the count of these trap messages to the eG manager. This information enables administrators to detect the abnormalities in the power supply if any, understand the nature of these failures, and accordingly decide on the remedial measures.

<table>
<tr><td>Purpose</td><td>Intercepts the traps sent by the switch, extracts information related to power supply failures from the traps, and reports the count of these trap messages to the eG manager.</td></tr>
<tr><td>Target of the test</td><td>A Juniper EX Switch</td></tr>
<tr><td>Agent deploying the test</td><td>An external agent</td></tr>
<tr><td>Configurable parameters for the test</td><td>1. TESTPERIOD - How often should the test be executed
2. HOST - The host for which the test is to be configured.
3. SOURCEADDRESS - Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
4. OIDVALUE - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:
<table>
<tr><th>OID</th><th>Value</th></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.2</td><td>Host_system</td></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.3</td><td>NETWORK</td></tr>
</table>
In this case the OIDVALUE parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.
An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*.</td></tr>
</table>

<table>
<tr><td></td><td colspan="3">Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID .1.3.6.1.4.1.9156.1.1.2 is found to be HOST and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your OIDVALUE specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be:

Trap5: .1.3.6.1.4.1.9156.1.1.5-any.

5. SHOWOID – Specifying true against SHOWOID will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter false, then the values alone will appear in the detailed diagnosis page, and not the OIDs.

6. TRAPOIDS – By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified SOURCEADDRESSes. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the TRAPOIDS text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing spaces.

7. DD FREQUENCY - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying none against dd frequency.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each type of event that occurred on the target Juniper EX Switch</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Failed power supplies:
Indicates the number of times this event was triggered due to power supply failure during the last measurement period.</td><td>Number</td><td>The failure events may be generated due to the failure of the Power supply units of the Juniper EX Switch. If the failure events are not rectified within a certain pre-defined timeperiod, the switch will be shutdown automatically.

Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Juniper EX Switch.</td></tr>
</table>

1.1.7 Fans Test

EX4200 switches have a single fan tray on the rear panel. The fan tray is a hot-removable and hot-insertable field-replaceable unit (FRU): You can remove and replace it without powering off the switch or disrupting switch functions.

The fan tray used in the switch comes with load-sharing redundancy that can tolerate a single fan failure at room temperature (below 113° F/45° C) to still provide sufficient cooling.

Under normal operating conditions, the fans in the fan tray run at less than full speed. If a fan fails or the ambient temperature rises above the threshold 113° F (45° C), the speed of the remaining fans is automatically adjusted to keep the temperature within the acceptable range, 32° F (0° C) through 113° F (45° C).

The system raises an alarm if the fan fails or if the ambient temperature inside the chassis rises above the acceptable range. If the temperature inside the chassis rises above the threshold temperature, the system shuts down automatically.

This test intercepts the fan failure traps sent by the switch, extracts relevant information related to the failure from the traps, and reports the count of these trap messages to the eG manager. This information enables administrators to detect the fan failures if any, understand the nature of these failures, and accordingly decide on the remedial measures.

<table>
<tr><td>Purpose</td><td>Intercepts the fan failure traps sent by the switch, extracts relevant information related to the failure from the traps, and reports the count of these trap messages to the eG manager</td></tr>
<tr><td>Target of the test</td><td>A Juniper EX Switch</td></tr>
<tr><td>Agent deploying the test</td><td>An external agent</td></tr>
<tr><td>Configurable parameters for the test</td><td>1. TESTPERIOD - How often should the test be executed
2. HOST - The host for which the test is to be configured.
3. SOURCEADDRESS - Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
4. OIDVALUE - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:
<table>
<tr><th>OID</th><th>Value</th></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.2</td><td>Host_system</td></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.3</td><td>NETWORK</td></tr>
</table></td></tr>
</table>

	In this case the **OIDVALUE** parameter can be configured as *Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network*, where *Trap1* and *Trap2* are the display names that appear as descriptors of this test in the monitor interface. An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to *Failed:*-F**. Typically, if a valid value is specified for an OID in the *OID-value* pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID *.1.3.6.1.4.1.9156.1.1.2* is found to be *HOST* and not *Host_*system, then the test ignores OID *.1.3.6.1.4.1.9156.1.1.2* while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your **OIDVALUE** specification should be: *DisplayName:OID-any*. For instance, to ensure that the test monitors the OID *.1.3.6.1.4.1.9156.1.1.5*, which in itself, say represents a failure condition, then your specification would be: *Trap5: .1.3.6.1.4.1.9156.1.1.5-any*.**SHOWOID** – Specifying **true** against **SHOWOID** will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter **false**, then the values alone will appear in the detailed diagnosis page, and not the OIDs. 6. **TRAPOIDS** – By default, this parameter is set to *all*, indicating that the eG agent considers all the traps received from the specified **SOURCEADDRESS**es. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the **TRAPOIDS** text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, **94.2*,*.1.3.6.1.4.25**, where * indicates leading and/or trailing spaces. 7. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against dd frequency.
Outputs of the test	One set of results for each type of failure event that occurred on the target Juniper EX Switch

Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**Failed fans:** Indicates the number of events of this type that were triggered during the last measurement period.	Number	The failure events may be generated due to the failure of the fans of the Juniper EX Switch. If the failure events are not rectified within a certain pre-defined timeperiod, the storage system will be shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Juniper EX Switch.

1.2 The JEX Service Layer

This layer tracks the CPU mode of each routing engine available in the Juniper EX Switch.

Figure 3: The tests mapped to the JEX Service layer

1.2.1 Switch Details Test

The Routing Engine runs the Junos OS. Software processes that run on the Routing Engine maintain the routing tables, manage the routing protocols used on the router, control the router interfaces, control some chassis components, and provide the interface for system management and user access to the router.

You can install one or two Routing Engines in the router. Each Routing Engine must be installed directly into an SCB. A USB port on the Routing Engine accepts a USB memory device that allows you to load Junos OS. The Routing Engines install into the front of the chassis in vertical slots directly into the SCBs labeled 0 and 1. If two Routing Engines are installed, one functions as the master and the other acts as the backup. If the master Routing Engine fails or is removed and the backup is configured appropriately, the backup takes over as the master.

This test reports the mode of each routing engine available in the Juniper EX Switch.

Purpose	Monitors the mode of each routing engine available in the Juniper Ex Switch
Target of the test	A Juniper EX Switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Juniper EX Switch 3. **SNMPPORT** – The SNMP Port number of the Juniper EX Switch (161 typically) 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the encryptflag is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">15. 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 Juniper EX Switch over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Juniper EX Switch device that is to be monitored</td></tr>
<tr><td>Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td></td><td>Mode:
Indicates the mode of this routing engine.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Unknown</td><td>1</td></tr><tr><td>Master</td><td>2</td></tr><tr><td>Backup</td><td>3</td></tr><tr><td>Disabled</td><td>4</td></tr></table>Note:
This measure reports the Measure Values listed in the table above to indicate the mode of this routing engine. However, in the graph of this measure, the mode of the routing engine is indicated using only the Numeric Values listed in the above table.</td></tr>
</table>

2 Conclusion

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

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