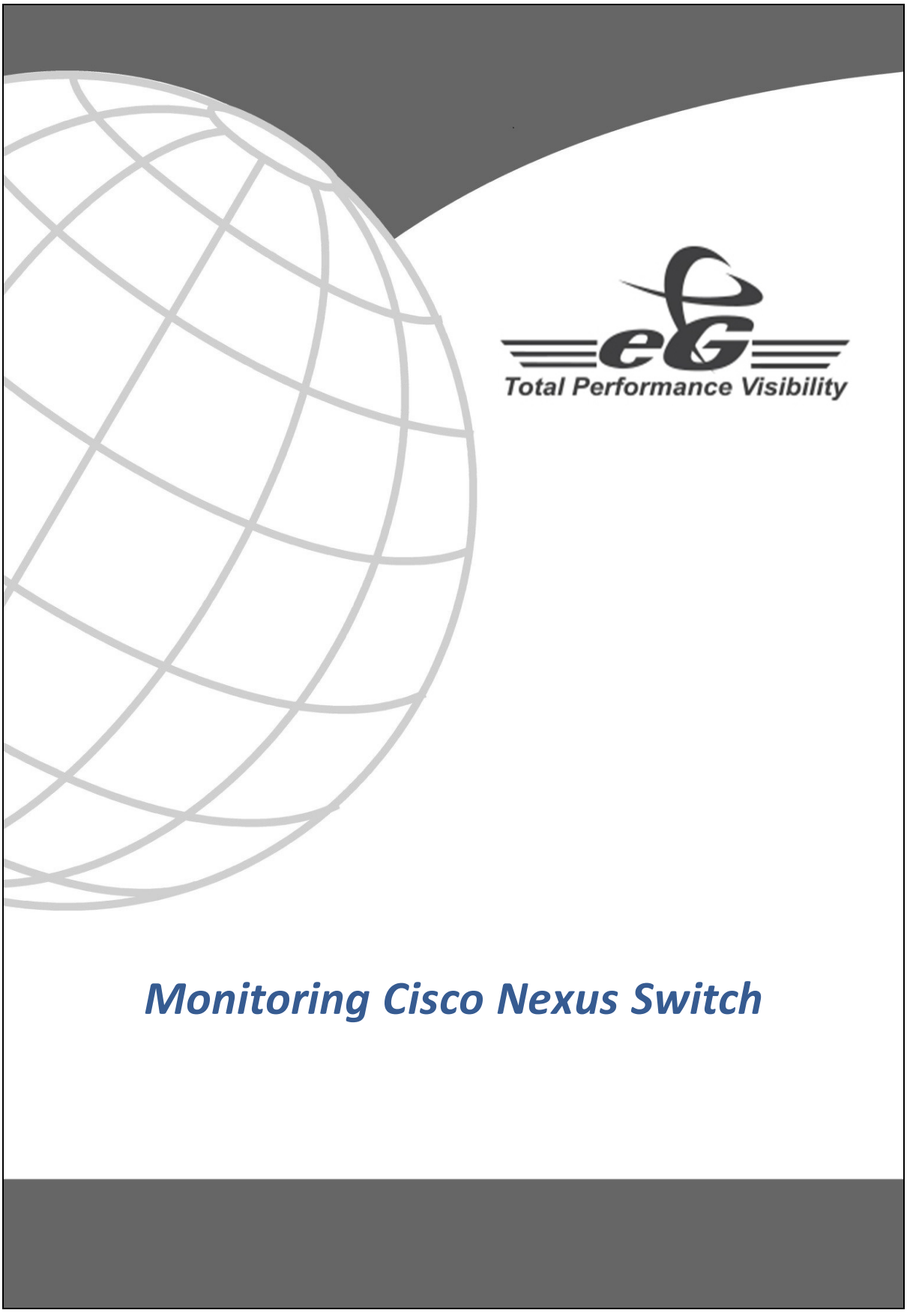

Monitoring Cisco Nexus Switch

Table of contents

Table of Figures

1

Introduction

The Cisco Nexus Series switches are modular and fixed port network switches designed for data centers. Designed as access-layer switches for in-rack deployment, the Cisco Nexus Series Switches helps simplify data center infrastructure, provide high network bandwidth and reduce total cost of ownership. The Cisco Nexus Switch supports I/O consolidation at the rack level, reducing the number of adapters, cables, switches, and transceivers that each server must support, all while protecting investment in existing storage assets.

Any issues with the switch could be the possible source of critical problems like excessive bandwidth usage, abnormal temperature and voltage, high resource utilization, or loss of data during transmission! TO avoid such issues, the performance of the Cisco Nexus Switch has to be monitored 24 *7.

eG Enterprise has developed a dedicated Cisco Nexus Switch monitoring model which periodically checks the data traffic to and from each network interface of the switch, the temperature and voltage of each module of the switch, the resource utilization etc, so that abnormalities can be detected before any irreparable damage occurs.

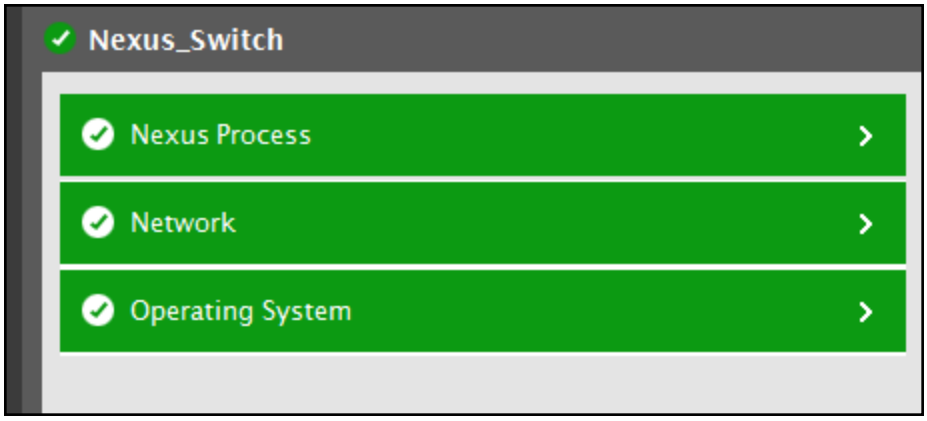

Figure 1.1: The layer model of the Cisco Nexus Switch

Every layer of Figure 1 is mapped to a variety of tests which connect to the SNMP MIB of the target Cisco Nexus Switch to collect critical statistics pertaining to its performance. The metrics reported by these tests enable administrators to answer the following questions:

- How well the CPU is utilized?
- What is the current state of each fan sensor and the speed of each fan?
- How well the memory of each memory module is utilized?
- What is the current state of each sensor of the power supply units?
- What is the current state of each voltage sensor available in the modules of the target Cisco Nexus Switch?
- What is the size of the RAM and NVRAM in the target Cisco Nexus Switch?

- How well the NVRAM is utilized?
- What is the current operational status of each fan?
- Are all the network interfaces of the target Cisco Nexus Switch available?
- How well data is transmitted to and from each network interface?
- Is any network interface connected to the target Cisco Nexus Switch error-prone?

The sections to come will discuss each layer of Figure 1 in detail.

1.1 The Operating System layer

The Operating System layer of the Cisco Nexus Switch tracks the CPU and memory utilization of the switch, current status of the hardware elements etc. The tests of this layer are discussed in the forthcoming sections.

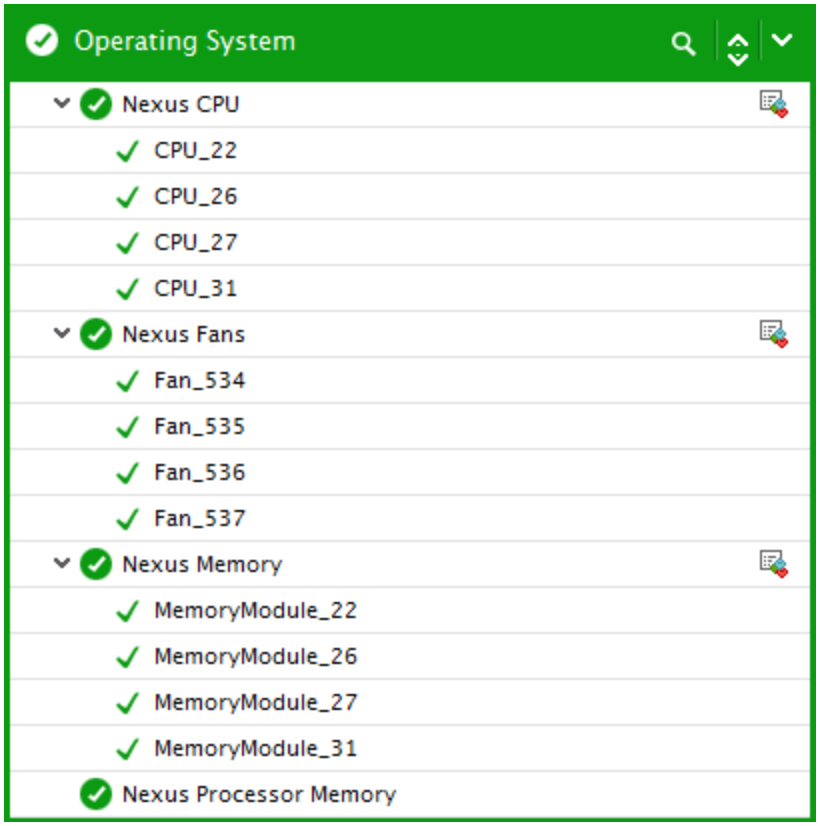

Figure 1.2: The tests associated with the Operating System layer

1.1.1 Nexus CPU Test

This test enables administrators to figure out how CPU hungry the Cisco Nexus Switch is. If the Cisco Nexus Switch is found to consume CPU resources excessively, then, this test will also help administrators determine when exactly during the last 5 minutes did CPU usage peak; this revelation will help them troubleshoot CPU spikes better.

Target of the test : A Cisco Nexus Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each CPU of the target Cisco Nexus Switch that is being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the Cisco Nexus Switch
3. **SNMPPORT** – The port at which the Cisco Nexus Switch exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION**list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE**list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm

11. **ENCRYPTFLAG**– This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG**is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG**is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE**list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
13. **ENCRYPTPASSWORD**– Specify the encryption password here.
14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
CPU usage during the last minute:	Indicates the percentage of time during the last minute the device was using this CPU.	Percent	By comparing the values of these measures, you can quickly figure out when CPU usage was maximum so that, you can investigate why CPU usage peaked during that time.
CPU usage in the last 5 minutes:	Indicates the percentage of time during the last 5 minutes the device was using this CPU.	Percent	

1.1.2 Nexus Fans Test

This test auto-discovers the fans in the target Cisco Nexus Switch and reports the current operational state of each fan. Using this test, administrators can keep a check on the fans that are currently malfunctioning.

Target of the test : A Cisco Nexus Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each fan in the target Cisco Nexus Switch being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the Cisco Nexus Switch
3. **SNMPPORT** – The port at which the Cisco Nexus Switch exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION**list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE**list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG**– This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG**is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG**is set to **YES**, then you will have to mention the encryption type

by selecting an option from the **ENCRYPTTYPE**list. SNMP v3 supports the following encryption types:

- **DES** – Data Encryption Standard
- **AES** – Advanced Encryption Standard

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

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Operation status:	Indicates the current operation state of this fan.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **State / Measure value** – **Numeric Value** Unknown – 1 Up – 2 Down – 3 Warning – 4 **Note:** By default, this measure reports the Measure Values listed in the table above to indicate the current operation state of this fan. The graph of this measure however, represents the status of a server using the numeric equivalents only - 1 to 4.

1.1.3 Nexus Memory Test

This test reports the memory utilization of each memory module available in the target Cisco Nexus Switch. By comparing the memory usage statistics across the memory modules, you can quickly identify the memory module that is under-sized or is currently running out of space.

Target of the test : A Cisco Nexus Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each memory module available in the target Cisco Nexus Switch being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the Cisco Nexus Switch
3. **SNMPPORT** – The port at which the Cisco Nexus Switch exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION**list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.

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

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Total memory:	Indicates the total memory available for this memory module.	GB	
Used memory:	Indicates the amount of memory already utilized in this memory module.	GB	A low value is desired for this measure.
Free memory:	Indicates the amount of memory that is currently available for use in this	GB	A high value is desired for this measure.

Measurement	Description	Measurement Unit	Interpretation
	memory module.		
Memory utilization:	Indicates the percentage of memory that is utilized in this memory module.	Percent	A low value is desired for this measure. A high value or a consistently increasing value is a cause of concern, as it could indicate a gradual erosion of memory in the memory module. In such cases, you may want to resize the memory module or investigate the cause of memory erosion and find a way to arrest the memory erosion.

1.1.4 Nexus Processor Memory Test

This test monitors the processor of the Cisco Nexus Switch and reports the size of the RAM and NVRAM of the processor. In addition, this test reports how well the NVRAM is being utilized and how much of NVRAM is available for use. Using this test, administrators can identify if enough memory resources are available for the processor to function without a glitch! If memory resources are depleting, then administrators can add additional resources to avoid malfunctioning of the Cisco nexus Switch.

Target of the test : A Cisco Nexus Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Cisco Nexus Switch being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the Cisco Nexus Switch
3. **SNMPPORT** – The port at which the Cisco Nexus Switch exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION**list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities.

To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.

7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE**list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG**– This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG**is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG**is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE**list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
13. **ENCRYPTPASSWORD**– Specify the encryption password here.
14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
RAM size:	Indicates the total size of the RAM.	GB	
NVRAM size:	Indicates the total size of non volatile RAM in the switch.	GB	
Used NVRAM:	Indicates the amount of non volatile RAM that is already utilized in the Nexus processor.	GB	
Free NVRAM:	Indicates the amount of non volatile RAM that is still available for use in the Nexus processor.	GB	
Percent usage of NVRAM:	Indicates the percentage of non volatile RAM that is utilized in the Nexus processor.	Percent	A low value is desired for this measure.

1.1.5 Nexus Fan Sensors Test

This test auto-discovers the fans of the target Cisco Nexus Switch and reports the current status of the sensor available in each fan module. In addition, this test also reports the speed at which each fan operates. Using this test, administrators can easily identify the fans that are currently running at abnormal speed.

Target of the test : A Cisco Nexus Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each fan of the target Cisco Nexus Switch being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the Cisco Nexus Switch
3. **SNMPPORT** – The port at which the Cisco Nexus Switch exposes its SNMP MIB; the default is 161.

4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION**list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE**list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG**– This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG**is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG**is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE**list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
13. **ENCRYPTPASSWORD**– Specify the encryption password here.

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

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Sensor status:	Indicates the current state of this fan sensor.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **State / Measure value** — **Numeric Value** OK — 1 Unavailable — 2 Non operational — 3 **Note:** By default, this measure reports the Measure Values listed in the table above to indicate the current state of this fan sensor. The graph of this measure however, represents the status of a server using the numeric equivalents only - 1 to 3.
Speed:	Indicates the current speed of this fan.	RPM	Ideally, the speed of the fan should be within admissible range. An abnormal speed is an indication of the malfunctioning of the fan and administrators should therefore replace the fans immediately for the smooth functioning of the Cisco Nexus Switch.

1.1.6 Nexus Power Sensors Test

This test auto-discovers the power supply units of the Cisco Nexus Switch and reports the current state of the sensor of each power supply unit. In addition, this test reports the current input power to each power supply unit. Using this test, administrators can detect the power supply unit that is damaged due to abnormal input power.

Target of the test : A Cisco Nexus Switch.

Agent deploying the test : An external agent

Outputs of the test : One set of results for each sensor of the power supply unit in the target Cisco Nexus Switch being monitored.

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the Cisco Nexus Switch
3. **SNMPPORT** – The port at which the Cisco Nexus Switch exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION**list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.

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

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Sensor status:	Indicates the current state of the sensor of this power supply unit.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **State** / **Numeric Value** OK – 1 Unavailable – 2 Non operational – 3

Measurement	Description	Measurement Unit	Interpretation
			Note: By default, this measure reports the Measure Values listed in the table above to indicate the current state of the sensor of this power supply unit. The graph of this measure however, represents the status of a server using the numeric equivalents only - 1 to 3.
Power usage:	Indicates the current input power to this power supply unit.	Watts	The value of this measure should be well within admissible range. A sudden increase in the value of this measure indicates the power supply unit is damaged beyond repair.

1.1.7 Nexus Temperature Sensors Test

The Cisco Nexus Switch is by default, provided with built-in automatic temperature sensors for each of the modules (Supervisor, I/O and Fabric). Whenever a temperature sensor detects an abnormal temperature, then the module corresponding to that temperature sensor is shutdown. If an abnormal temperature is detected by the temperature sensor corresponding to the Supervisor module and high-availability is not available, then you have two minutes of time to decrease the temperature beyond which the module will be shutdown. If the modules are shutdown frequently, then the performance of the Cisco Nexus Switch may degrade gradually. To avoid this, it is essential to monitor the operational state and the temperature of each module at regular intervals. The **Nexus Temperature Sensors** test helps administrators in this regard. This test auto-discovers the temperature sensors of the Cisco Nexus Switch and reports the current status of each temperature sensor and the current temperature of each module detected by its corresponding temperature sensors.

Target of the test : A Cisco Nexus Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each temperature sensor available in each module of the target Cisco Nexus Switch that is being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the Cisco Nexus Switch
3. **SNMPPORT** – The port at which the Cisco Nexus Switch exposes its SNMP MIB; the default is 161.

4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION**list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE**list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG**– This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG**is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG**is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE**list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
13. **ENCRYPTPASSWORD**– Specify the encryption password here.

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

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Sensor status:	Indicates the current state of this temperature sensor.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **State / Measure value** — **Numeric Value** OK — 1 Unavailable — 2 Non operational — 3 **Note:** By default, this measure reports the Measure Values listed in the table above to indicate the current state of the sensor of this temperature unit. The graph of this measure however, represents the status of a server using the numeric equivalents only - 1 to 3.
Temperature:	Indicates the current temperature detected by this temperature sensor.	Celsius	Ideally, the value of this measure should be within the admissible temperature range.

1.1.8 Nexus Voltage Sensors Test

For a Cisco Nexus Switch to function without a glitch, it is essential for the three modules (Supervisor, I/O and Fabric) to function properly. If any of the modules do not function as expected, then that particular module

will shutdown automatically. If the modules are frequently shutdown, then the overall performance of the Cisco Nexus Switch may degrade drastically. To avoid this performance degradation, administrators should constantly keep a vigil on the voltage passing through each module. The **Nexus Voltage Sensors** test helps administrators in this regard. This test auto-discovers the voltage sensors in the modules of the Cisco Nexus Switch and reports the current status of each voltage sensor and the current voltage passing through each module.

Target of the test : A Cisco Nexus Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each sensor of each voltage sensor available in each module of the target Cisco Nexus Switch being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the Cisco Nexus Switch
3. **SNMPPORT** – The port at which the Cisco Nexus Switch exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION**list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.

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

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Sensor status:	Indicates the current state of this voltage sensor.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **State / Measure value** – **Numeric Value** OK – 1 Unavailable – 2 Non operational – 3

Measurement	Description	Measurement Unit	Interpretation
			Note: By default, this measure reports the Measure Values listed in the table above to indicate the current state of the sensor of this voltage unit. The graph of this measure however, represents the status of a server using the numeric equivalents only - 1 to 3.
Voltage:	Indicates the current voltage detected by this voltage sensor.	Volts	

1.2 The Network layer

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

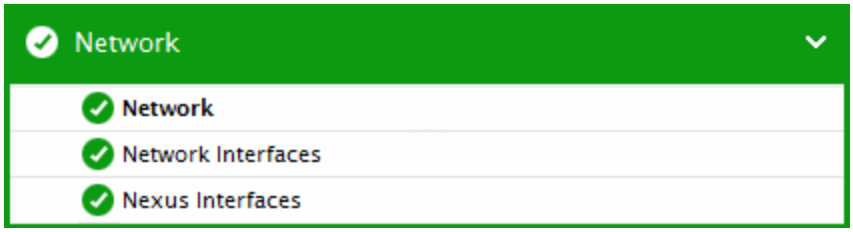

Figure 1.3: The list of tests associated with the Network layer

1.2.1 Nexus Interfaces Test

This test monitors each network interface of the Cisco Nexus Switch and reports the availability and operation state of each network interface. This test also helps administrators in figuring out how well data was transmitted to and from the network interface and the errors encountered in each network interface while data was transmitted/received. Using this test, administrators can identify the network interface that is handling too much of data traffic and the network interface that is error-prone.

Target of the test : A Cisco Nexus Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each network interface of the target Cisco Nexus Switch being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the Cisco Nexus Switch
3. **SNMPPORT** – The port at which the Cisco Nexus Switch exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION**list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE**list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG**– This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG

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

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

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Is the network interface operationally available?:	Indicates the availability of this network interface.		If the operational state (i.e., the running state) of an interface is "up", then, this measure will report the value Yes. If the operational status of an interface is “down”, then this measure will report the value No. On the other hand, if the admin state (i.e., the configured state) of an interface is “down”, then the value of this measure will be: Administratively Down. The numeric values that correspond to each of the above-mentioned states are as follows: **Measure value** / **Numeric Value** No / 0 Yes / 100

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Administratively Down</td><td>200</td></tr>
<tr><td>Dormant</td><td>300</td></tr>
<tr><td>Not Present</td><td>400</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed in the table above to indicate the status of an interface. The graph of this measure however, represents the same using the numeric equivalents – 0 to 300.
</td></tr>
<tr><td>Data transmitted rate:</td><td>Indicates the rate of data being transmitted from the router over a network link.</td><td>MB/Sec</td><td>This measurement depicts the workload on a network link.</td></tr>
<tr><td>Data received rate:</td><td>The rate of data being received by the router over a network link.</td><td>MB/Sec</td><td>This measure also characterizes the workload on a network link.</td></tr>
<tr><td>Speed:</td><td>Indicates the speed of this network interface.</td><td>Mbps</td><td>Some network interface may dynamically change their speed over time - based on external factors/settings. By tracking the speed of an interface over time, an administrator can be aware of such speed changes.</td></tr>
<tr><td>Bandwidth used:</td><td>Indicates the percentage utilization of the bandwidth available over a network link.</td><td>Percent</td><td>A value close to 100% indicates a network bottleneck.</td></tr>
</table>

Note:

The speed of a network interface is based on the value of its SNMP MIB-II variable, which is set using router-specific commands (e.g., the "bandwidth" command of a Cisco router). When a network interface has a fixed maximum speed limit (e.g., Ethernet), the percentage bandwidth will be <= 100%.

In some instances, service providers offer a minimum committed information rate (CIR). In such cases, the speed of the network interface is not fixed and may be set to the minimum CIR. Since user traffic may be in excess of the CIR at times, the percentage bandwidth measure could exceed 100%. In such cases, the percentage bandwidth measure is to be ignored.

Receive errors:	Indicates the rate of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.	Packets/Sec	Ideally, this value should be 0.
Transmit errors:	Indicates the rate at which outbound packets could not be delivered as they contained errors.	Packets/Sec	Ideally, this value should be 0.
In discards:	Indicates the rate at which inbound packets were discarded, though such packets did not contain any errors that could prevent them from being delivered to a higher-layer protocol.	Packets/Sec	One possible reason for discarding such a packet could be to free up buffer space.
Out discards:	Indicates the rate at which outbound packets were discarded, though such packets did not contain any errors that could prevent them from being delivered to a higher-layer protocol.	Packets/Sec	One possible reason for discarding such a packet could be to free up buffer space. If you have a large number of out discards, it means that the network device's output buffers have filled up and the device had to drop these packets. This can be a sign that this segment is run at an inferior speed and/or duplex, or there is too much traffic that goes through this port.
Non- unicast packets received:	Indicates the rate at which packets which were addressed as multicast or broadcast were received by this layer.	Packets/Sec	

Non- unicast packets transmitted:	Indicates the rate at which packets which were addressed as multicast or broadcast were sent by this layer.	Packets/Sec	
Unicast packets received:	Indicates the rate at which packets which were not addressed as multicast or broadcast were received by this layer.	Packets/Sec	
Unicast packets transmitted:	Indicates the rate at which packets which were not addressed as multicast or broadcast were sent by this layer.	Packets/Sec	
Queue length:	Indicates the length of the output packet queue.	Number	A consistent increase in the queue length could be indicative of a network bottleneck.
Unknown protocols:	Indicates the rate at which unknown protocols were received.	Packets/Sec	For packet-oriented interfaces, this measure will report the number of packets received via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, this measure reports the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be 0.
Operation state down reason:	Indicates the current operation state of this network interface.		The values reported by this measure and its numeric equivalents are mentioned in the table below:

State	Numeric Value
Error Disabled	0
Other	1
None	2
Hwfailure	3
LoopbackDiagFailure	4
SwFailure	6
LinkFailure	7
Offline	8
NonParticipating	9
Initializing	10
VsanInactive	11
AdminDown	12
ChannelAdminDown	13
ChannelOperSuspended	14
ChannelConfigurationInProgress	15
RcfInProgress	16
ElpFailureIsolation	17
EscFailureIsolation	18
DomainOverlapIsolation	19
DomainAddrAssignFailureIsolation	20
DomainOtherSideEportIsolation	21
DomainInvalidRcfReceived	22
DomainManagerDisabled	23
ZoneMergeFailureIsolation	24
VsanMismatchIsolation	25
ParentDown	26
SrcPortNotBound	27
InterfaceRemoved	28
FcotNotPresent	29
FcotVendorNotSupported	30
IncompatibleAdminMode	31
IncompatibleAdminSpeed	32
SuspendedByMode	33
SuspendedBySpeed	34
SuspendedByWWN	35
DomainMaxReTxFailure	36

State	Numeric Value
EppFailure	37
portVsanMismatchIsolation	38
LoopbackIsolation	39
UpgradeInProgress	40
IncompatibleAdminRxBbCredit	41
IncompatibleAdminRxBufferSize	42
PortChannelMembersDown	43
ZoneRemoteNoRespIsolation	44
FirstPortUpAsEport	45
FirstPortNotUp	46
PeerFCIPPortClosedConnection	47
PeerFCIPPortResetConnection	48
FcipPortMaxReTx	49
FcipPortKeepAliveTimerExpire	50
FcipPortPersistTimerExpire	51
FcipPortSrcLinkDown	52
FcipPortSrcAdminDown	53
FcipPortAdminCfgChange	54
FcipSrcPortRemoved	55
FcipSrcModuleNotOnline	56
InvalidConfig	57
PortBindFailure	58
PortFabricBindFailure	59
NoCommonVsanIsolation	60
FiconVsanDown	61
InvalidAttachment	62
PortBlocked	63
IncomAdminRxBbCreditPerBuf	64
TooManyInvalidFlogis	65
DeniedDueToPortBinding	66
ElpFailureRevMismatch	67
ElpFailureClassFParamErr	68
ElpFailureClassNParamErr	69
ElpFailureUnknownFlowCtlCode	70
ElpFailureInvalidFlowCtlParam	71
ElpFailureInvalidPortName	72

State	Numeric Value
ElpFailureInvalidSwitchName	73
ElpFailureRatovEdtovMismatch	74
ElpFailureLoopbackDetected	75
ElpFailureInvalidTxBbCredit	76
ElpFailureInvalidPayloadSize	77
BundleMisCfg	78
BitErrRuntimeThreshExceeded	79
LinkFailLinkReset	80
LinkFailPortInitFail	81
LinkFailPortUnusable	82
LinkFailLossOfSignal	83
LinkFailLossOfSync	84
LinkFailNosRcvd	85
LinkFailOlsRcvd	86
LinkFailDebounceTimeout	87
LinkFailLrRcvd	88
LinkFailCreditLoss	89
LinkFailRxQOverflow	90
LinkFailTooManyInterrupts	91
LinkFailLipRcvdBb	92
LinkFailBbCreditLoss	93
LinkFailOpenPrimSignalTimeout	94
LinkFailOpenPrimSignalReturned	95
LinkFailLipF8Rcvd	96
LinkFailLineCardPortShutdown	97
FcspAuthenfailure	98
FcotChecksumError	99
InvalidFabricBindExchange	100
InvalidFabricBindExchange	101
TovMismatch	102
FiconNotEnabled	103
FiconNoPortNumber	104
FiconBeingEnabled	105
EPortProhibited	106
PortGracefulShutdown	107
TrunkNotFullyActive	108

			<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>FabricBindingSwitchWwnNotFound</td><td>109</td></tr><tr><td>FabricBindingDomainInvalid</td><td>110</td></tr><tr><td>FabricBindingDbMismatch</td><td>111</td></tr><tr><td>FabricBindingNoRspFromPeer</td><td>112</td></tr></table> **Note:** By default, this measure reports the Measure Values listed in the table above to indicate the current operation state of the network interface.. The graph of this measure however, represents the status of a server using the numeric equivalents only - 0 to 112.

1.3 The Nexus Process layer

The test pertaining to this layer tracks various statistics pertaining to the processes executing on the target Cisco Nexus Switch. The details of the test is discussed in the section below.

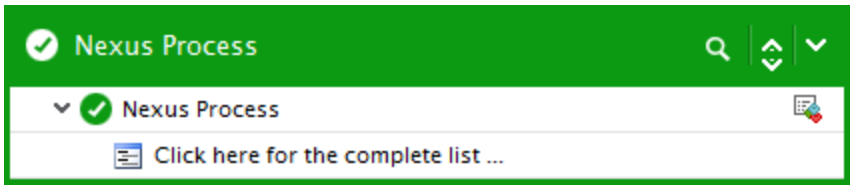

Figure 1.4: The tests associated with the Nexus Process layer

1.3.1 Nexus Process Test

For each process in the software module of the target Cisco Nexus Switch, this test reports the CPU and memory utilization. Using this test, administrators can easily identify the process that is over-utilizing the CPU and memory resources of the Cisco Nexus Switch.

Target of the test : A Cisco Nexus Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each process of the target Cisco Nexus Switch being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the Cisco Nexus Switch

3. **SNMPPORT** – The port at which the Cisco Nexus Switch exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION**list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE**list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG**– This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG**is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG**is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE**list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard

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

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
CPU usage:	Indicates the percentage of CPU utilized by this process.	Percent	A low value is desired for this measure. A high value or a gradual increase in the value would result in a CPU utilization bottleneck where other processes are made to wait longer for the CPU resources.
Allocated memory:	Indicates the amount of memory allocated to this process.	MB	

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 **Cisco Nexus 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.