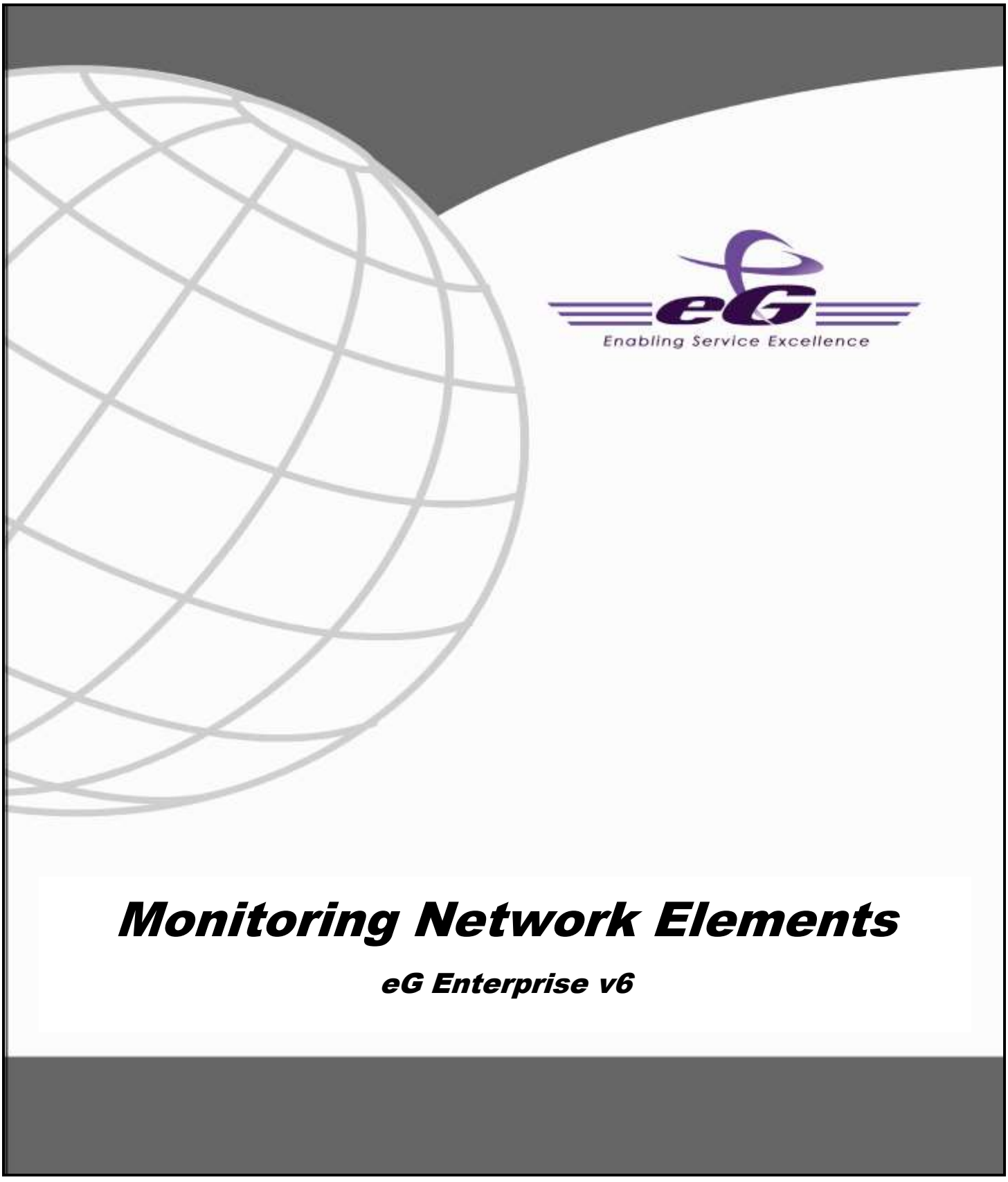

Monitoring Network Elements

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 2008, Windows 2012, Windows 7, Windows 8, and Windows 10 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

Table of Figures

Chapter 1

Introduction

An IT infrastructure includes a number of networking elements – such as routers, nodes, switches, load balancers, etc. These devices not only provide physical connectivity to server components in an IT environment, but also serve as entry points for accessing mission-critical services.

If these network elements fail, the business-critical services might become inaccessible to end-users, thus causing the business to lose revenue and reputation. By periodically monitoring these network elements for faults, and by proactively resolving the issues that surface, administrators can ensure that users receive continued connectivity to the services of interest.

eG Enterprise provides exclusive monitoring models for monitoring the availability and overall health of many network devices. The eG agent deployed on a remote host (i.e., the external agent), contacts the SNMP MIB of the device, and collects key performance statistics pertaining to that device from the MIB.

This document describes each of the eG-developed custom monitors for network elements.

Chapter 2

Monitoring Cisco Routers

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

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

The eG Enterprise suite includes special-purpose monitors for Cisco routers. Using the Cisco Enterprise SNMP MIB, eG agents monitor various metrics of interest relating to Cisco routers. Figure 2.1 depicts the layer model of a Cisco router.

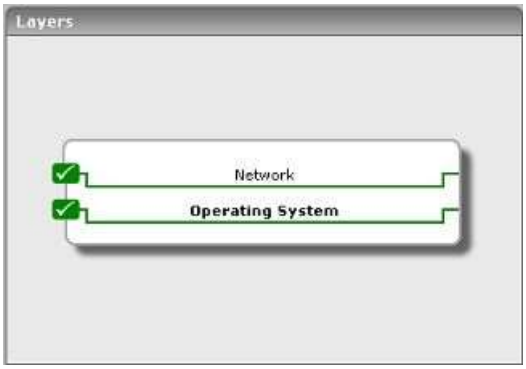

Figure 2.1: Layer model for network elements

The sections to come deal with every layer of Figure 2.1 in detail.

2.1 The Operating System Layer

Like any other server, a Cisco router's **Operating System** layer tracks the CPU and memory utilization of the router. The various tests of interest are as depicted in Figure 2.2:

Figure 2.2: Lists of tests associated with the Operating System layer of a Cisco Router

2.1.1 Cisco CPU Test

Often excess traffic to a router can impose a prohibitive load on the router, making it a bottleneck. This test measures the CPU utilization of a Cisco router by using the Cisco Enterprise SNMP MIB.

Purpose	Monitors the CPU usage of a Cisco router.
Target of the test	A Cisco router
Agent deploying the test	External agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Cisco Router. 3. **SNMPPORT** - The port number through which the Cisco router exposes its SNMP MIB. The default value 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 Cisco router. 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 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**. 16. **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*.
Outputs of the test	One set of results for every router being monitored.

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	CPU utilization: Total percentage CPU utilization of a router.	Percent	A very high value could indicate a CPU bottleneck at the router.

2.1.2 Cisco Memory Test

This test measures the memory utilization of each of the memory pools associated with a Cisco router.

Purpose	This test monitors the memory usage of a Cisco router.
Target of the test	A Cisco Router
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 Cisco Router. 3. **SNMPPORT** - The port number through which the Cisco router exposes its SNMP MIB. The default value 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 Cisco router. 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 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**. 16. **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*.		
Outputs of the test	One set of results for every memory pool of a router being monitored.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Memory utilization: Total percentage memory utilization of a memory pool.	Percent	A utilization value close to 100% is indicative of a memory bottleneck at the router.
	Used Memory: The number of megabytes from the memory pool that are currently in use by applications on the managed device.	MB	A low value is desired for this measure.
	Free Memory: The number of megabytes from the memory pool that are currently unused on the managed device	MB	A high value is desired for this measure.

2.1.3 Cisco Buffers Test

This test monitors the memory allocations within a Cisco router. Various forms of buffer memory allocation failures are tracked and reported. This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Cisco Router* as the **Component type**,

Performance as the **Test type**, choose the test from the **DISABLED TESTS** list, and click on the **>>** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Purpose	Monitors the memory allocations within a Cisco router
Target of the test	A Cisco router
Agent deploying the test	External agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Cisco Router. 3. **SNMPPORT** - The port number through which the Cisco router exposes its SNMP MIB. The default value 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 Cisco router. 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** – The maximum duration (in seconds) for which the test will wait for a response from the router

<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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every router being monitored.</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>No memory errors:
Counts the number of buffer creation failures due to lack of free memory in the router</td><td>Number</td><td>Lack of free memory can result in poor performance by a router - packet drops, packet processing slowdown, etc. can happen. By monitoring when memory errors happen, an administrator can proactively detect performance bottlenecks caused by a router. If memory errors occur often, consider upgrading the memory on the router.</td></tr>
<tr><td>Small buffer misses:
Counts the number of allocations that failed because there were no small buffers available</td><td>Number</td><td>Ideally, the small buffer miss count should be 0. Repeated buffer misses indicates a memory bottleneck in the router. Alternatively, the maximum number of small buffers set when configuring the router may be too low for the traffic being handled.</td></tr>
<tr><td>Medium buffer misses:
Counts the number of allocations that failed because there were no medium buffers available</td><td>Number</td><td>Ideally, the medium buffer miss count should be 0. Repeated buffer misses indicates a memory bottleneck in the router. Alternatively, the maximum number of medium buffers set when configuring the router may be too low for the traffic being handled.</td></tr>
<tr><td></td><td>Large buffer misses:
Counts the number of allocations that failed because there were no large buffers available</td><td>Number</td><td>Ideally, the large buffer miss count should be 0. Repeated buffer misses indicates a memory bottleneck in the router. Alternatively, the maximum number of large buffers set when configuring the router may be too low for the traffic being handled.</td></tr>
</table>

	Huge buffer misses: Counts the number of allocations that failed because there were no huge buffers available	Number	Ideally, the large buffer miss count should be 0. Repeated buffer misses indicates a memory bottleneck in the router. Alternatively, the maximum number of huge buffers set when configuring the router may be too low for the traffic being handled.
	Big buffer misses: Counts the number of allocations that failed because there were no big buffers available.	Number	Ideally, the big buffer miss count should be 0. Repeated buffer misses indicates a memory bottleneck in the router. Alternatively, the maximum number of big buffers set when configuring the router may be too low for the traffic being handled.
	Buffer hits: Indicates the total number of buffer hits.	Number	Ideally, the value of this measure should be high. A very low value could indicate that many allocations have failed owing to the lack of adequate buffers. If the measure repeatedly reports low values, it could be indicative of a memory bottleneck on the router.

2.1.4 Cisco Fans Test

This test monitors the status of all the fans available in a Cisco device.

Purpose	Monitors the status of all the fans available in a Cisco device
Target of the test	A Cisco device
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 host for which the test is to be configured. 3. **SNMPPORT** - The port number through which the Cisco device exposes its SNMP MIB. The default value 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 Cisco device. The default value is 'public'. 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 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**. 16. **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*.		
Outputs of the test	One set of results for every fan on the Cisco device that is monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Current state: Indicates the current state of a fan.	Number	A value of 1 indicates normalcy. A value 2 denotes a warning condition, while a value 3 indicates a critical state. A value of 4 indicates that this fan has been shut down. A value of 6 is reported if the fan is not functioning.

2.1.5 Cisco Power Supply Test

This test monitors the status of all the power supplies available in a Cisco device.

Purpose	Monitors the status of all the power supplies available in a Cisco device
Target of the test	A Cisco device
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 host for which the test is to be configured. 3. **SNMPPORT** - The port number through which the Cisco device exposes its SNMP MIB. The default value 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 Cisco device. The default value is 'public'. 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 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**. 16. **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*.		
Outputs of the test	One set of results for every power supply on the Cisco device that is monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Current state: Indicates the current state of the power supply.	Number	A value of 1 indicates normalcy. A value 2 denotes a warning condition, while a value 3 indicates a critical state. A value of 4 indicates that this power supply has been shut down. A value of 6 is reported if the power supply is not functioning.

2.1.6 Cisco Voltage Test

This test monitors the status of all the voltage test points available on a Cisco device.

Purpose	Monitors the status of all the voltage test points available on a Cisco device
Target of the test	A Cisco device
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 host for which the test is to be configured. 3. **SNMPPORT** - The port number through which the Cisco device exposes its SNMP MIB. The default value 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 Cisco device. The default value is 'public'. 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 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**. 16. **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*.		
Outputs of the test	One set of results for every voltage test point on the Cisco device that is monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Current voltage: Indicates the current voltage as reported by a test point.	mV	
	Current state: Indicates the current state of a voltage test point.	Number	A value of 1 indicates normalcy. A value 2 denotes a warning condition, while a value 3 indicates a critical state. A value of 4 indicates that this test point has been shut down. A value of 6 is reported if the test point is not functioning.

2.1.7 Cisco Temperature Test

This test monitors the ambient temperature of a Cisco device.

Purpose	Monitors the ambient temperature of a Cisco device
Target of the test	A Cisco device
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 host for which the test is to be configured. 3. **SNMPPORT** - The port number through which the Cisco device exposes its SNMP MIB. The default value 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 Cisco device. The default value is 'public'. 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.

<table>
<tr><td></td><td colspan="3">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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every temperature test point on the Cisco device that is 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>Current temperature:
Indicates the current ambient temperature as reported by a test point.</td><td>Celcius</td><td></td></tr>
<tr><td>Current state:
Indicates the current state of a temperature test point.</td><td>Number</td><td>A value of 1 indicates normalcy. A value 2 denotes a warning condition, while a value 3 indicates a critical state. A value of 4 indicates that this test point has been shut down. A value of 6 is reported if the test point is not functioning.</td></tr>
</table>

2.2 The Network Layer

The **Network** layer reflects the status of network connectivity to and from the router. The tests that map to this layer are as follows.

Figure 2.3: List of tests associated with the Network layer

Since the details about the Network test are available in the *Monitoring Unix and Windows Servers* document, the sections that follow will discuss only the other three tests in Figure 2.3.

2.2.1 Network Interfaces Test

The NetworkInterfaces test monitors critical metrics relating to the Network interfaces of a target server/network device using MIB-II support provided by the server/device.

Purpose	Monitors critical metrics relating to the Network interfaces of a target server/network device using MIB-II support provided by the server/device
Target of the test	A Cisco router
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 Cisco Router. 3. Ensure that the specified **HOST** is SNMP-enabled. If not, the test will not function. 4. **SNMPPORT** - The default SNMP port is 25. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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. **ONLYUP** – If the **ONLYUP** flag is set to **Yes**, then only the network interfaces that are operational - i.e. whose MIB-II operStatus variable has a value "up" - are monitored. If this flag is set to **No**, all network interfaces that have an adminStatus of "up" will be monitored. By default, this flag is set to **No**, indicating that by default the test will monitor network interfaces that are up/down.
16. **FULLDUPLEX** - If this value is **Yes**, then it indicates that all interfaces are full duplex. In this case, the eG Enterprise system will compute bandwidth usage % to be, **max(input bandwidth, output bandwidth)*100/total speed**. On the other hand, if this flag is set to **No**, then the computation of bandwidth usage % will be **(input bandwidth + output bandwidth)*100/total speed**.
17. **EXCLUDE** - The **EXCLUDE** text box takes a comma separated list of network interfaces that are to be excluded when performing the test. For example, if this parameter has a value of "Null0", then the Null0 interface of the network device will not be monitored by the eG agent. This specification can also include wild card characters. For instance, to disregard all interfaces which contain the string *ether* and *null* when monitoring, your **EXCLUDE** specification should be: **ether*,*null**.
18. **DISCOVERBYSTATE** – This flag controls how the test discovers network interfaces. If this flag is **No**, the operational state of an interface is not considered when discovering all the network interfaces of a router/switch/network device. If this flag is **Yes**(which is the default setting), only interfaces that have been in the **up** operational state will be considered for monitoring. In this mode, if an interface is down all of the time, it will not be considered for monitoring. However, once the interface starts to function, it will be tracked by the test and alerts generated if the interface state ever changes to **down**.
19. **USEALIAS** and **SHOW ALIAS AND INTERFACE NAME** - Cisco and many network devices allow administrators to set the names for switch/router ports. These names can be set to logical, easily understandable values. Port names can be set in Cisco devices using the command **"set port name"**. For example *set port name 3/24 Federal_credit_union_link.* This command indicates that the port 3/24 is used to support the Federal Credit Union. If the **USEALIAS** parameter is set to **Yes**, then a **SHOW ALIAS AND INTERFACE NAME** parameter will additionally appear, which is set to **No** by default. In this case, the agent will first try to look at the port name (from the *ifAlias* SNMP OID) and use the port name if specified as the descriptor for the test results. If a port name is unavailable or if no port name/alias is specified in the network device setting, the interface description for each port provided in the SNMP MIB-II output is used instead as the descriptor for the test results. On the other hand, if the **USEALIAS** parameter is set to **Yes** and the **SHOW ALIAS AND INTERFACE NAME** parameter is set to **Yes**, then each descriptor of this test will be represented in the format *port name:interface description*.For e.g., *1:local_lan_segment:GigabitEthernet 0/0*. If the **USEALIAS** parameter is set to **No**, then the **SHOW ALIAS AND INTERFACE NAME** parameter option will not appear. In this case therefore, the device name will be displayed as the descriptor of the test.
20. **USEEXTENSION** - By default, this test polls the standard IF MIB (RFC 1213) to collect the required metrics. Set the **USEEXTENSION** flag to **Yes**, if you want the test to poll the Interfaces Group MIB (RFC 2233) for metrics collection. By default this parameter is set to **No**.
21. **TIMEOUT** - The maximum duration (in seconds) for which the test will wait for a response from the network interface

	22. **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**. 23. **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*.		
Outputs of the test	One set of records for each interface of a router		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

<table>
<tr><td rowspan="3">test</td><td>Is the network interface available?:
Indicates the availability of a network interface</td><td></td><td>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:
<table><tr><th>State</th><th>Value</th></tr><tr><td>No</td><td>0</td></tr><tr><td>Yes</td><td>100</td></tr><tr><td>Administratively Down</td><td>200</td></tr><tr><td>Dormant</td><td>300</td></tr><tr><td>Lower layer down</td><td>500</td></tr></table>
Note:

By default, this measure reports one of the States 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 200.</td></tr>
<tr><td>Data transmit rate:
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:
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>
</table>

	Speed: Speed of the network interface	Mbps	This is a static setting – in other words, it is a value that is explicitly set for a network interface through tools such as Cisco admin interface or through commands. This value will hence NOT change with time. eG uses this value to compute the percentage bandwidth usage of a network interface. This value cannot be used to determine how well the network interface is working. If you think that the above value is incorrect for a network interface, you can use the "bandwidth" interface sub-command of Cisco IOS (provided the network device being monitored is a Cisco device) to manually set the correct speed values for each network interface.
	Bandwidth used: Indicates the percentage utilization of the bandwidth available over a network link	Percent	A value close to 100% indicates a network bottleneck.

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 contian 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	

	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.
	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.

2.2.2 Cisco Interfaces Test

This test monitors various statistics of interest for each interface of a Cisco router. It is intended to alert the operator whenever any abnormal activity is detected on any of the Cisco router's interfaces.

Purpose	Monitors various statistics of interest for each interface of a router
Target of the test	A Cisco router
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 Cisco Router. 3. **SNMPPORT** - The port number through which the Cisco router exposes its SNMP MIB. The default value 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 Cisco router. 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.

<table>
<tr><td></td><td colspan="3">14. TIMEOUT – The maximum duration (in seconds) for which the test will wait for a response from the router

15. EXCLUDE - The EXCLUDE text box takes a comma separated list of network interfaces that are to be excluded when performing the test. E.g., if this parameter has a value of "Null0", then the Null0 interface of the Cisco router will not be monitored by the eG agent.

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.

17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of records for each interface of a router</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Reliability value:
Provides the level of reliability of the interface</td><td>Number</td><td>This is representative of how many errors are occurring on the interface. The best reliability value is 255.</td></tr>
<tr><td>Reliability percent:
Indicates the reliability of an interface as a percentage</td><td>Percent</td><td>This is computed as (Reliability value)*100/255. A drop in the value of this measure indicates an error-prone interface.</td></tr>
<tr><td>Delay:
The amount of delay of an interface</td><td>Secs</td><td>This value is measured and reported by the Cisco IOS. This is calculated by adding up the delay along the path to the next router. Any increase in this value is usually attributable to an increase in traffic over an interface.</td></tr>
<tr><td></td><td>Load factor:
The degree of loading of an interface, reported as a percent.</td><td>Percent</td><td>A value of 100% indicates a saturated interface. Consider increasing the speed/capacity of the interface in this case.</td></tr>
</table>

	Data received: The rate of data received by the router over an interface	Mbits/sec	This value is an indicator of the instantaneous traffic received over an interface.
	Data transmitted: The rate of data transmitted by the router over an interface	Mbits/sec	This value is an indicator of the instantaneous traffic transmitted over an interface.
	In queue drops: Number of packets dropped during reception over the interface during the last measurement period	Number	This value counts the number of packets that were not received (i.e., thrown away) because of lack of a system resource (e.g., a buffer). Packets can be dropped even if the number of packets queued on the input side is equal to the input queue limit. Ideally, there should be no queue drops. An increase in queue drops is an indicator that the router may not be able to service the traffic received by it.
	Out queue drops: Number of packets dropped during transmission over the interface during the last measurement period	Number	This value counts the number of packets that were not transmitted (i.e., thrown away) because of various reasons. For example, packets can be dropped because the output queue occupancy has reached the pre-specified queue limit. Packet drops can also occur because of insufficient buffers - e.g., not having a hardware transmission buffer when a packet is fast-switched from one interface to another. Repeated queue drops can indicate congestion at the router.
	Resets: Number of times an interface was reset in the last measurement period	Number	This value counts the number of times an interface internally reset. Repeated resets may be indicative of hardware problems in the router.
	Restarts: Number of times an interface needed to be completely restarted in the last measurement period	Number	This value should be close to zero in most cases.
	CRC errors: Number of input packets in the last measurement period that had cyclic redundancy checksum errors	Number	This value which is mainly relevant for serial lines is one of the factors that affects the reliability of the line.

<table>
<tr><td></td><td>Aborts:
Number of packet receptions in the last measurement period that were aborted due to errors</td><td>Number</td><td></td></tr>
<tr><td></td><td>Collisions:
Number of collisions that occurred over an interface during the last measurement period</td><td>Number</td><td>This value which is mainly relevant for LAN interfaces is one of the factors affecting the reliability of the line.</td></tr>
<tr><td></td><td>Slow packets received:
The rate at which packets routed with slow switching were received.</td><td>Packets/Sec</td><td></td></tr>
<tr><td></td><td>Slow packets transmitted:
The rate at which packets routed with slow switching were transmitted.</td><td>Packets/Sec</td><td></td></tr>
<tr><td></td><td>Link protocol status:
Indicates the current status of the link protocol.</td><td></td><td>The values that this measure can report and their corresponding numeric values have been outlined in the table below:</td></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Up</td><td>1</td></tr>
<tr><td>Down</td><td>0</td></tr>
</table>
Note:

By default, this measure reports one of the Measure Values listed in the table above to indicate the status of the link protocol. The graph of this measure however, represents the same using the numeric equivalents only.
</td></tr>
</table>

2.2.3 Device Uptime Test

In most production environments, it is essential to monitor the uptime of critical network devices in the infrastructure. By tracking the uptime of each of the devices, administrators can determine what percentage of time a device has been up. Comparing this value with service level targets, administrators can determine the most trouble-prone areas of the infrastructure.

In some environments, administrators may schedule periodic reboots of their network devices. By knowing that a specific device has been up for an unusually long time, an administrator may come to know that the scheduled reboot task is not working on a device.

The Device Uptime test included in the eG agent monitors the uptime of critical network devices.

Purpose	To monitor the uptime of a network device
Target of the test	Any network device
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 device. 3. **SNMPPORT** - The port number through which the device exposes its SNMP MIB. The default value 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 device. 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.

<table>
<tr><td></td><td colspan="3">
14. TIMEOUT – The maximum duration (in seconds) for which the test will wait for a response from the router

15. REPORTMANAGERTIME – By default, this flag is set to Yes, indicating that, by default, the detailed diagnosis of this test, if enabled, will report the shutdown and reboot times of the device in the manager's time zone. If this flag is set to No, then the shutdown and reboot times are shown in the time zone of the system where the agent is running.

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.

17. 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.

18. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.

The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
• The eG manager license should allow the detailed diagnosis capability
• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.
</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every device being 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>Has the system been rebooted?:
Indicates whether the server has been rebooted during the last measurement period or not.</td><td>Boolean</td><td>If this measure shows 1, it means that the server was rebooted during the last measurement period. By checking the time periods when this metric changes from 0 to 1, an administrator can determine the times when this server was rebooted.</td></tr>
</table>

	Uptime during the last measure period: Indicates the time period that the system has been up since the last time this test ran.	Secs	If the server has not been rebooted during the last measurement period and the agent has been running continuously, this value will be equal to the measurement period. If the server was rebooted during the last measurement period, this value will be less than the measurement period of the test. For example, if the measurement period is 300 secs, and if the server was rebooted 120 secs back, this metric will report a value of 120 seconds. The accuracy of this metric is dependent on the measurement period – the smaller the measurement period, greater the accuracy.
	Total uptime of the system: Indicates the total time that the server has been up since its last reboot.	Mins	Administrators may wish to be alerted if a server has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions.

Intermittent breaks in network connection, exasperating slowdowns, and inexplicable deterioration in the overall network performance, have become common-place in many IT environments today. Whenever network performance chokes, administrators have to promptly determine which interface is consuming bandwidth excessively and why, so that the road-blocks can be cleared quickly and normalcy can be restored in minutes. However, as this analysis typically takes hours in the real world, the end-user experience suffers as an outcome, causing loss of revenue and reputation.

To avoid such unpleasant eventualities, the eG Enterprise Suite offers specialized network monitoring capabilities vide its eG external agent component. This agent, which is capable of executing on any remote host in your environment, can be easily tuned to monitor the traffic on your critical Cisco routers and periodically report the findings, so that administrators can perform the following in no time:

- Understand how much bandwidth is been utilized by every network interface, and isolate the bandwidth-intensive protocols on each interface;
- Plan bandwidth allocation based on the network usage patterns so observed;
- Closely monitor the traffic on the router to determine who is (i.e., which hosts are) communicating over the network, the top communicators in terms of traffic, and the nature of communication;
- Identify who (i.e., the sources) is generating the maximum traffic, and what is that they are accessing frequently (i.e the destinations);

To collect such useful statistics, the external agent runs a series of tests on the Cisco router. This document discusses each of these tests and explains how the metrics they report enable easy and effective network performance management.

2.2.4 Network Protocols Test

Applications in today's enterprise networks require different levels of service based upon business requirements. The network can provide a variety of services to help ensure that your mission-critical applications receive the bandwidth they need to deliver the desired performance levels. The difficulty is that today's Internet-based and client-server

applications make it difficult for the network to identify and provide the proper level of control you need. NBAR solves this problem by adding intelligent network classification to your infrastructure.

NBAR, an important component of the Cisco Content Networking architecture, is a new classification engine in Cisco IOS® Software that can recognize a wide variety of applications, including Web-based applications and client/server applications that dynamically assign TCP or User Datagram Protocol (UDP) port numbers. After the application is recognized, the network can invoke specific services for that particular application. NBAR currently works with quality-of-service (QoS) features to help ensure that the network bandwidth is best used to fulfill your business objectives.

When run on an NBAR-supported Cisco router, this test periodically polls the NBAR MIB to auto-discover the interfaces for which NBAR is enabled, and reports the following for each discovered interface:

- The network protocols handled by that interface;
- The traffic generated for every protocol;
- The bandwidth utilized per protocol.

This way, the test not only reveals busy, bandwidth-intensive interfaces, but also turns the spotlight on specific protocols on those interfaces that are causing excessive bandwidth consumption. Moreover, with the help of these protocol-level usage metrics, administrators can assess how various interfaces and protocols use the network resources, and accordingly fine-tune network policies.

2.2.4.1 Configuring the eG Agent to use NBAR

The first step to running this test is to enable NBAR on each interface for which you want to collect NBAR statistics.

To enable NBAR, do the following:

The following is a set of commands issued on a router to enable NBAR on the *FastEthernet 0/1* interface.

```
router#enable
Password:*****
router#configure terminal
router-2621(config)#ip cef
router-2621(config)#interface FastEthernet 0/1
router-2621(config-if)#ip nbar protocol-discovery
router-2621(config-if)#exit
router-2621(config)#exit
router-2621(config)#show ip nbar protocol-discovery
```

Please note that the part in red has to be repeated for each interface individually.

Purpose	Auto-discovers the interfaces supported by NBAR-enabled routers, and for each interface, reports the network protocols handled by that interface, the traffic generated for every protocol, and the bandwidth utilized per protocol
Target of the test	A Cisco router
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 device. 3. **SNMPPORT** - The port number through which the device exposes its SNMP MIB. The default value 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 device. 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.

<table>
<tr><td></td><td colspan="3">14. TIMEOUT – The maximum duration (in seconds) for which the test will wait for a response from the router

15. ACTIVE PROTOCOLS ONLY – By default, this flag is set to No, indicating that, by default, this test reports metrics for all protocols handled by an interface. To ensure that the test monitors only those protocols that are currently active, set this flag to Yes.

16. IGNORE INTERFACES- Specify a comma-separated list of interfaces to be excluded from monitoring. By default, the test monitors all interfaces for which NBAR is enabled. Accordingly, this parameter is set to none by default.

17. SHOW PROTOCOLS - By default, the test monitors all protocols handled by an interface. This is why, the SHOW PROTOCOLS parameter is set to all by default. To make sure that the test monitors only specific protocols per interface, provide a comma-separated list of protocols here.

18. MIN BANDWIDTH PERCENT - By default, the value 1 is displayed here. This indicates that, by default, the test will consider only those protocols that are using 1% or more of current traffic. You can increase or decrease this value based on your monitoring needs. If you set this value to 0, then all protocols will be monitored.

19. 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.

20. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every protocol handled by every network interface being 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>Data received:

Indicates the total data received through this interface using this protocol.</td><td>Mbps</td><td></td></tr>
</table>

	Data transmitted: Indicates the total data transmitted by this interface using this protocol.	Mbps	
	Total traffic: Indicates the total traffic - both incoming and outgoing - handled by this interface for this protocol.	Mbps	
	Portion of current traffic for this protocol: Indicates the percentage of total traffic through this interface that pertains to this protocol.	Percent	Compare the value of this measure across protocols to identify the protocol for which there is heavy traffic through this interface.
	Total bandwidth of this interface: Indicates the total bandwidth of this interface.	Mbps	Compare the value of this measure across interfaces to isolate the top consumers of bandwidth usage.
	Percentage of bandwidth for this protocol: Indicates the percentage of total bandwidth that is utilized by this protocol.	Percent	By comparing the value of this measure across protocols, you can easily identify which protocol is bandwidth-intensive.
	Packets received: Indicates the rate at which packets were received through this interface for this protocol.	Pkts/sec	
	Packets sent: Indicates the rate at which packets were transmitted through this interface for this protocol.	Pkts/sec	
	Total packets: Indicates the rate of packet transmission and reception for this protocol.	Pkts/sec	
	Percentage of packet traffic for this protocol: Indicates the percentage of total packet tra that pertains to this protocol.	Percent	Compare the value of this measure across protocols to identify which protocol is experiencing high packet traffic.

	Inbound rate: Indicates the inbound bit rate as determined by Protocol Discovery.	Bits	
	Outbound rate: Indicates the outbound bit rate as determined by Protocol Discovery.	Bits	

2.2.5 Net Flows Test

Cisco IOS NetFlow is a flexible and extensible method to record network performance data. It efficiently provides a key set of services for IP applications, including network traffic accounting, usage-based network billing, network planning, security, Denial of Service monitoring capabilities, and network monitoring. NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing.

By polling the Netflow MIB of a Netflow-enabled Cisco router at configured intervals, this test collects a wide variety of per-flow statistics on traffic on that Cisco router. With the help of these metrics, you can quickly identify the net flow on which a large amount of data was transacted, who the talkers were, the type of communication that they engaged in, and also instantly drill down to the interfaces impacted by this communication.

When users complaint of a network slowdown, knowing which two hosts are engaged in a bandwidth-intensive communication is sure to take you closer to determining what activity the two hosts were performing, and whether it can be terminated to conserve bandwidth.

2.2.5.1 Enabling Netflow using SNMP MIB for Cisco Routers

Cisco IOS NetFlow is a flexible and extensible method to record network performance data. It efficiently provides a key set of services for IP applications, including network traffic accounting, usage-based network billing, network planning, security, Denial of Service monitoring capabilities, and network monitoring. NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing.

By polling the Netflow MIB (SNMP MIB) of a Netflow-enabled Cisco router at configured intervals, this test collects a wide variety of per-flow statistics on traffic on that Cisco router.

eG Enterprise Suite uses the Cisco Netflow MIBs only to collect the required metrics. The collector mechanism i.e., Netflow analyzers is currently not supported by eG Enterprise.

The *Net Flows*, *Top Sources* and *Top Destinations* tests will work only if Netflow is enabled on a router. To achieve this, follow the steps below:

1. Enter global configuration mode on the router or MSFC, and issue the following commands for **each interface** on which you want to enable NetFlow:

interface {interface} {interface_number}

ip route-cache flow

bandwidth <kbps>

exit

This enables NetFlow on the specified interface alone. Remember that on a Cisco IOS device, **NetFlow is enabled on a per-interface basis**. If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15), **ip route-cache flow** command is used to enable NetFlow on an interface. If your router is running Cisco IOS release 12.2(14)S, 12.0(22)S, 12.2(15)T, or later the **ip flow ingress** command is used to enable NetFlow on an interface. The **bandwidth** command is optional, and is used to set the speed of the interface in kilobits per second.

2. Then, issue the following command to break up long-lived flows into 1-minute fragments. You can choose any number of minutes between 1 and 60. If you leave it at the default of 30 minutes your traffic reports will have spikes. It is important to set this value to **1 minute** in order to generate alerts and view troubleshooting data.

   ip flow-cache timeout active 1

3. Next, issue the following command to ensure that flows that have finished are periodically exported. The default value is 15 seconds. You can choose any number of seconds between 10 and 600.

   ip flow-cache timeout inactive 15

4. Finally, enable ifIndex persistence (interface names) globally by issuing the following command in global configuration mode.

   snmp-server ifindex persist

5. This ensures that the ifIndex values are persisted during device reboots.

6. In addition to the steps detailed above, the following commands will have to be executed to enable Top-talkers on that router. **Please note that the Top-talkers needs to be enabled in the global configuration mode and not on a per-interface basis:**

   ip flow-top-talkers

   top 4

   sort-by bytes

   The purpose of each of these commands is detailed in the table below:

ip flow-top-talkers	Enters the configuration mode for the NetFlow MIB and top talkers (heaviest traffic patterns and most-used applications in the network) feature.
sort-by	Specifies the sorting criterion for top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and top talkers feature.
Top	Specifies the maximum number of top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and top talkers feature.

Purpose	Collects a wide variety of per-flow statistics on traffic on that Cisco router
Target of the	A Cisco router

test	
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 device. 3. **SNMPPORT** - The port number through which the device exposes its SNMP MIB. The default value 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 device. 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** – The maximum duration (in seconds) for which the test will wait for a response from the router
15. **REPORT HOST NAMES** – This test captures per-flow statistics on traffic, where each flow is by default represented by the IP addresses of the two hosts communicating over the network. Accordingly, this flag is set to **No** by default. You can set this flag to **Yes** so that a flow is represented using the the names of the hosts instead of their IP addresses.
16. **MINIMUM FLOW PERCENT** - By default, the value *3* is displayed here. This indicates that, by default, the test will consider only those net flows that are using 3% or more of current traffic. You can increase or decrease this value based on your monitoring needs. If you set this value to *0*, then all net flows will be monitored.
17. **REPORT NO OF FLOWS LIMIT** - By default, this parameter is set to *all* indicating that all net flows will be monitored by default. If you want the test to report, say only the top 5 net flows in terms of percentage of data being trafficked, then set this value to *5*.
18. **IGNORE LOCAL TRAFFIC** - By default, this flag is set to **Yes**, indicating that the test will ignore all the intranet traffic on the router. If you want the test to report metrics related to the local traffic as well, set this flag to **No**.
19. **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**.
20. **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*.
21. **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**.
22. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

<table>
<tr><td></td><td colspan="3">The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
The eG manager license should allow the detailed diagnosis capability
Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every net flow discovered from the router being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Data in flow:
Indicates the amount of data transmitted and received in this net flow.</td><td>KB</td><td>Compare the value of this measure across flows to identify which flow is experiencing high levels of network traffic. This way, you can also identify the two hosts that are interacting over the network, generating heavy traffic in the process.
Use the detailed diagnosis of this measure to determine the input and output interfaces that have been impacted by the traffic and their current speeds.</td></tr>
<tr><td>Packets in flow:
Indicates the total number of packets received and transmitted in this net flow.</td><td>Pkts</td><td></td></tr>
<tr><td>Fraction of traffic on input interface for this flow:
Indicates the percentage of total traffic for this flow that is flowing through the input interface.</td><td>Percent</td><td>Compare the value of this measure across flows to know which flow is receiving large volumes of data via the input interface.</td></tr>
<tr><td></td><td>Fraction of traffic on output interface for this flow:
Indicates the percentage of total traffic for this flow that is flowing through the output interface.</td><td>Percent</td><td>Compare the value of this measure across flows to know which flow is transmitting large volumes of data via the output interface.</td></tr>
<tr><td></td><td>Protocol:
Indicates the protocol used in this net flow.</td><td></td><td>The table below lists the protocols that can be reported by this measure, and their numeric equivalents:<table><tr><th>Protocol</th><th>Numeric value</th></tr><tr><td>ICMP</td><td>1</td></tr><tr><td>IGMP</td><td>2</td></tr></table></td></tr>
</table>

			GGP	3
			IPv4	4
			ST	5
			TCP	6
			CBT	7

			EGP	8
			IGP	9
			BBN-RCC-MON	10
			NVP-II	11
			PUP	12
			ARGUS	13
			EMCON	14
			XNET	15
			CHAOS	16
			UDP	17
			MUX	18
			RDP	27
			IPv6	41
			IPv6-Route	43
			IPv6-Frag	44
			IDRP	45
			RSVP	46
			SWIPE	53
			MOBILE	55
			IPv6-ICMP	58
			IPv6-NoNxt	59
			IPv6-Opts	60
			VISA	70
			PVP	75
			DGP	86
			IPIP	94
			PNNI	102
			UDPLite	136

			Note: By default, this measure reports one of the **Protocols** listed in the table above to indicate the protocol for the net flow. The graph of this measure however, represents the same using the numeric equivalents only.

Use the detailed diagnosis of this measure to determine the input and output interfaces that have been impacted by the flow of traffic over the network, and the current speed of these interfaces.

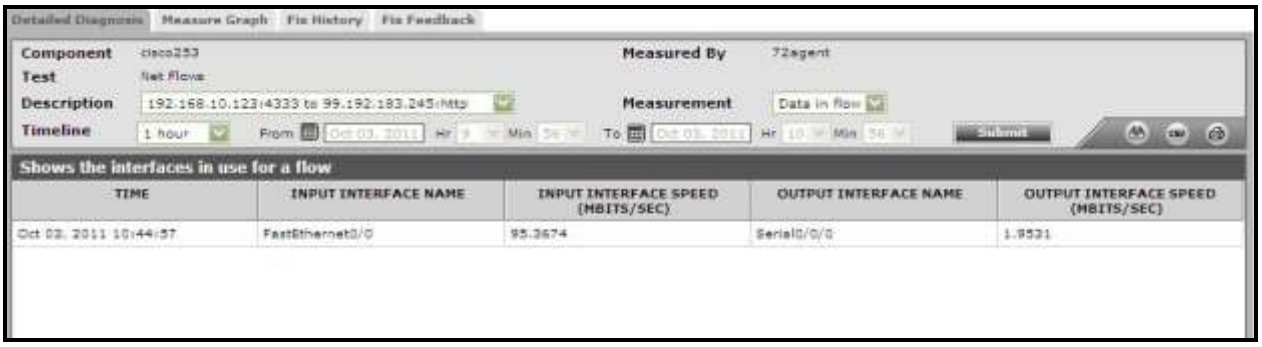

Figure 2. 4: Detailed diagnosis of the Data in flow measure

2.2.6 Top Sources Test

While the **Net flows** test points you to the specific network flows that are trafficking large volumes of data over the network, the **Top Sources** test reveals those hosts whose interactions with other hosts in the environment are resulting in the generation of such data. In the event of a network slowdown, you can use this test to accurately identify hosts whose current network activities are 'suspect' - i.e., you can isolate those hosts that may be engaged in bandwidth-intensive transactions with other hosts, and could hence be contributing to the slowdown.

Purpose	Reveals those hosts whose interactions with other hosts in the environment are resulting in the generation of large volumes of data
Target of the test	A Cisco router
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 device. 3. **SNMPPORT** - The port number through which the device exposes its SNMP MIB. The default value 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 device. 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** – The maximum duration (in seconds) for which the test will wait for a response from the router

15. **REPORT HOST NAMES** – This test captures statistics on traffic that originates from source hosts, where each host is by default represented by its IP address in the eG monitoring console. Accordingly, this flag is set to **No** by default. You can set this flag to **Yes** so that the names of the individual hosts are displayed in the eG monitoring console instead of their IP addresses.

16. **MINIMUM FLOW PERCENT** - By default, the value *3* is displayed here. This indicates that, by default, the test will consider only those sources that are using 3% or more of current traffic. You can increase or decrease this value based on your monitoring needs. If you set this value to *0*, then all net flows will be monitored.

17. **REPORT NO OF FLOWS LIMIT** - By default, this parameter is set to *all* indicating that this test will monitor all sources by default. If you want the test to report, say only the top 5 sources in terms of the amount of traffic they generate in their net flows, then set this value to *5*.

18. **IGNORE LOCAL TRAFFIC** - By default, this flag is set to **Yes**, indicating that the test will ignore the sources of all the intranet traffic on the router. If you want the test to report metrics pertaining to the sources of local traffic as well, set this flag to **No**.

19. **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**.

20. **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*.

21. **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**.

22. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

The option to selectively enable/disable the detailed diagnosis capability will be available

<table>
<tr><td></td><td colspan="3">only if the following conditions are fulfilled:
The eG manager license should allow the detailed diagnosis capability
Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every source host</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Data from this source:
Indicates the amount of data transmitted by this source over the network.</td><td>KB</td><td>Compare the value of this measure across sources to identify which source host is contributing to the high level of network traffic.
Use the detailed diagnosis of this measure to determine the top net flows (in terms of the volume of data transacted) that originated from this source, and the amount of data transacted in bytes and packets in every flow.</td></tr>
<tr><td>This source as fraction of top network flows:
Indicates the percentage of top network flows in which this host is the source.</td><td>Percent</td><td>Compare the value of this measure across sources to know which source is part of many top net flows. A high value is indicative of a 'suspect' source.</td></tr>
<tr><td>Packets from this source:
Indicates the number of data packets transmitted by this source over the network.</td><td>Pkts</td><td>Compare the value of this measure across sources to identify which source host is contributing to the high level of network traffic.</td></tr>
</table>

Use the detailed diagnosis of the *Data from this source* measure to determine the top net flows (in terms of the volume of data transacted) that originated from a particular source, and the amount of data transacted in bytes and packets in every flow. With the help of this detailed diagnosis, you can quickly compare the top net flows, know which net flow generated the maximum traffic, and figure out which destination that traffic was leading to. Once the problem destination is isolated, you can then investigate why traffic to that destination was high - is it because of the type of application executing on that destination? (eg., an online game or a movie that would typically consume a lot of bandwidth), or is it because of a poor network line connecting the source and the destination?

Figure 2. 5: The detailed diagnosis of the Data from this source measure

2.2.7 Top Destinations Test

While the **Top Sources** test indicates the hosts that could be engaging in bandwidth-intensive activities over the network, the **Top Destinations** test sheds light on what those activities might be. This test discovers the destinations of the net flows, and for each destination, reports the data traffic (in bytes and packets) leading to that destination. This way, the test points you to the destinations that are been frequently accessed and the level of traffic they generate.

Purpose	Discovers the destinations of the net flows, and for each destination, reports the data traffic (in bytes and packets) leading to that destination
Target of the test	A Cisco router
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 device. 3. **SNMPPORT** - The port number through which the device exposes its SNMP MIB. The default value 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 device. 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** – The maximum duration (in seconds) for which the test will wait for a response from the router
15. **REPORT HOST NAMES** – This test captures statistics on traffic to destinations, where each destination host is by default represented by its IP address in the eG monitoring console. Accordingly, this flag is set to **No** by default. You can set this flag to **Yes** so that the names of the individual hosts are displayed in the eG monitoring console instead of their IP addresses.
16. **MINIMUM FLOW PERCENT** - By default, the value *3* is displayed here. This indicates that, by default, the test will consider only those destinations that are using 3% or more of current traffic. You can increase or decrease this value based on your monitoring needs. If you set this value to *0*, then all net flows will be monitored.
17. **REPORT NO OF FLOWS LIMIT** - By default, this parameter is set to *all* indicating that this test will monitor all destinations by default. If you want the test to report, say only the top 5 destinations in terms of the amount of traffic they generate in their net flows, then set this value to *5*.
18. **IGNORE LOCAL TRAFFIC** - By default, this flag is set to **Yes**, indicating that the test will ignore the destinations of all the intranet traffic on the router. If you want the test to report metrics pertaining to the destinations of local traffic as well, set this flag to **No**.
19. **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**.
20. **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*.
21. **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**.
22. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

	The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.		
Outputs of the test	One set of results for every destination host		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Data to destination: Indicates the amount of data transmitted to this destination over the network.	KB	Compare the value of this measure across destinations to identify which destination host is contributing to the high level of network traffic. Use the detailed diagnosis of this measure to view the top net flows (in terms of the volume of data transacted) to a particular destination, and the amount of data transacted in bytes and packets in every flow. With the help of this detailed diagnosis, you can quickly compare the top net flows, know which net flow generated the maximum traffic, and figure out which source that traffic originated from. Once the problem source is isolated, you can then investigate why traffic from that source is high. Also, using the detailed diagnosis, you can also identify sources that have interacted with the said destination more than once. This will point you to sources that have frequently connected with the destination.
	This destination as fraction of top network flows: Indicates the percentage of top network flows in which this host is the destination.	Percent	Compare the value of this measure across destinations to know which destination is part of many top net flows. A high value is indicative of a 'suspect' destination.
	Packets to destination: Indicates the number of data packets transmitted by this source over the network.	Pkts	Compare the value of this measure across sources to identify which source host is contributing to the high level of network traffic.

Use the detailed diagnosis of the *Data to destination* measure to view the top net flows (in terms of the volume of data transacted) to a particular destination, and the amount of data transacted in bytes and packets in every flow. With the help of this detailed diagnosis, you can quickly compare the top net flows, know which net flow generated the maximum traffic, and figure out which source that traffic originated from. Once the problem source is isolated,

you can then investigate why traffic from that source is high. Also, using the detailed diagnosis, you can also identify sources that have interacted with the said destination more than once. This will point you to sources that have frequently connected with the destination.

Figure 2. 6: The detailed diagnosis of the Top Destinations measure

2.2.8 Troubleshooting FAQ

- **How can I verify my Netflow and Top talkers features have been enabled successfully?**

  One of the main reasons for the **Net flows** test, **Top Sources** test, and **Top Destinations** test to not report metrics is that the Top talkers may not be configured properly or currently top talkers may not be available. You can verify if your Netflow and Top talkers have been enabled successfully using the following command from the command prompt of the router:

  show ip flow top-talkers

  If the output is available as mentioned in Figure 2.7, then the **Net Flows**, **Top Sources** and **Top Destinations** tests will report the required metrics.

```
TCISL_eG#show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         192.168.8.2     Fa0/1         69.59.235.87    11 2746 3EAC    60
Fa0/0         192.168.11.41   Null          192.168.11.255  11 0089 0089    10
Fa0/0         192.168.11.20   Null          192.168.11.255  11 0089 0089     8
Fa0/0         192.168.9.150   Null          192.168.11.255  11 0089 0089     6
Fa0/0         192.168.11.18   Null          192.168.11.255  11 0089 0089     6
Fa0/0         192.168.8.127   Null          192.168.11.255  11 0089 0089     5
Fa0/0         192.168.8.36    Null          192.168.11.255  11 0089 0089     5
Fa0/0         192.168.9.113   Local         192.168.10.253  11 9035 00A1     5
Fa0/0         192.168.9.113   Local         192.168.10.253  11 D18E 00A1     5
Fa0/0         192.168.9.77    Null          192.168.11.255  11 0089 0089     5
10 of 10 top talkers shown. 20 of 284 flows matched.

TCISL_eG#
```

Figure 2.7: The outputs when top talkers and Netflow is enabled perfectly

If the output as mentioned in Figure 2.8 appears, then you can clearly figure out that the Top talkers have not been configured properly. The tests will report metrics only when both the Netflow and Top talkers are configured and enabled properly.

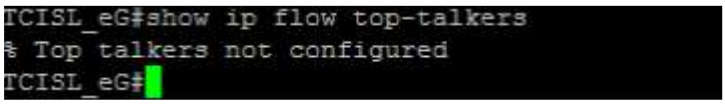

Figure 2.8: The output showing that the top talkers are not configured properly

If the following output (see Figure 2.9) appears, then you can figure out that though the Netflow and Top Talkers are configured and enabled, there are currently no Top talkers available. Therefore metrics will not be reported for the tests.

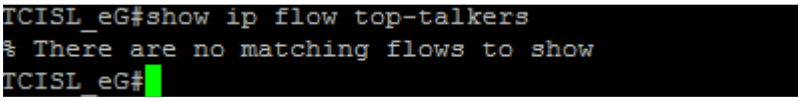

Figure 2.9: The output showing there are no top talkers

- **How do I verify if my NBAR protocol has been discovered successfully?**

  Execute the following command from the command prompt of the Cisco Router:

  show ip nbar protocol-discovery

  If the output as shown in Figure 2.10 appears, then you can confirm that the NBAR protocol has been discovered successfully.

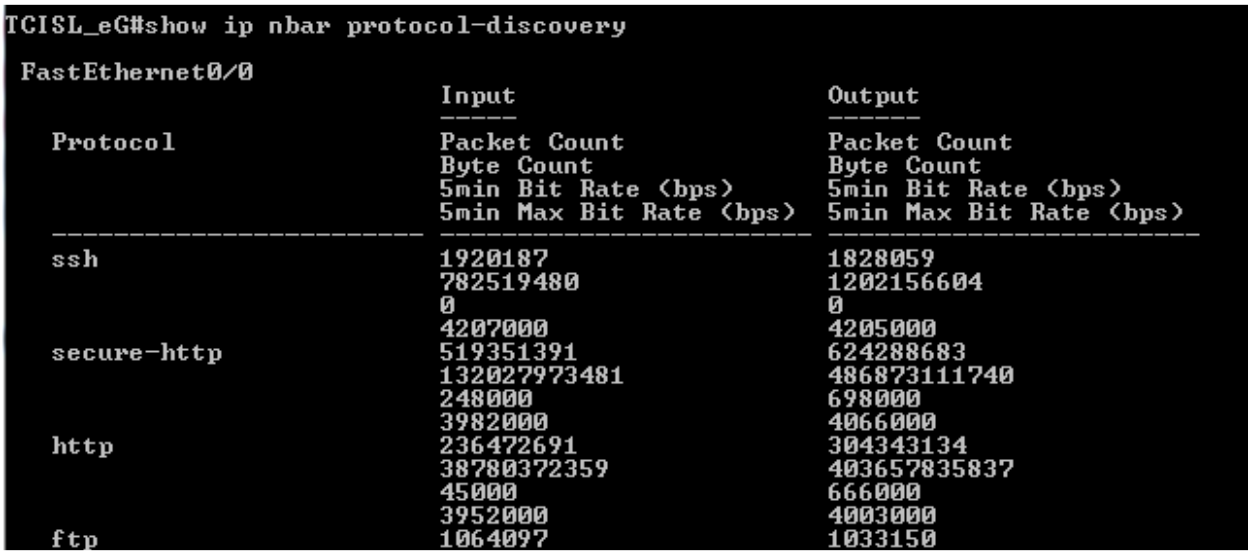

Figure 2.10: The output that appears upon successful NBAR protocol discovery

- **I don't have access to the Cisco Router that I wish to monitor. The Network engineer who manages the Cisco Router is informing me that the Netflow and Top Talkers features are enabled and configured. How can I cross verify if the features have indeed been enabled successfully?**

  Execute the **snmpwalk** command for the following OID from the command prompt of the eG agent install directory:

  .1.3.6.1.4.1.9.9.387.1.7.8.1

  Note that the syntax for the snmpwalk command will vary based on the SNMPVERSION with which the router is configured.

  If the Netflow and Top Talkers features are enabled and configured properly, then the output as shown in Figure 2.11 will appear. **Remember that the output as shown in** Figure 2.11 **will appear only if Top Talkers are available.**

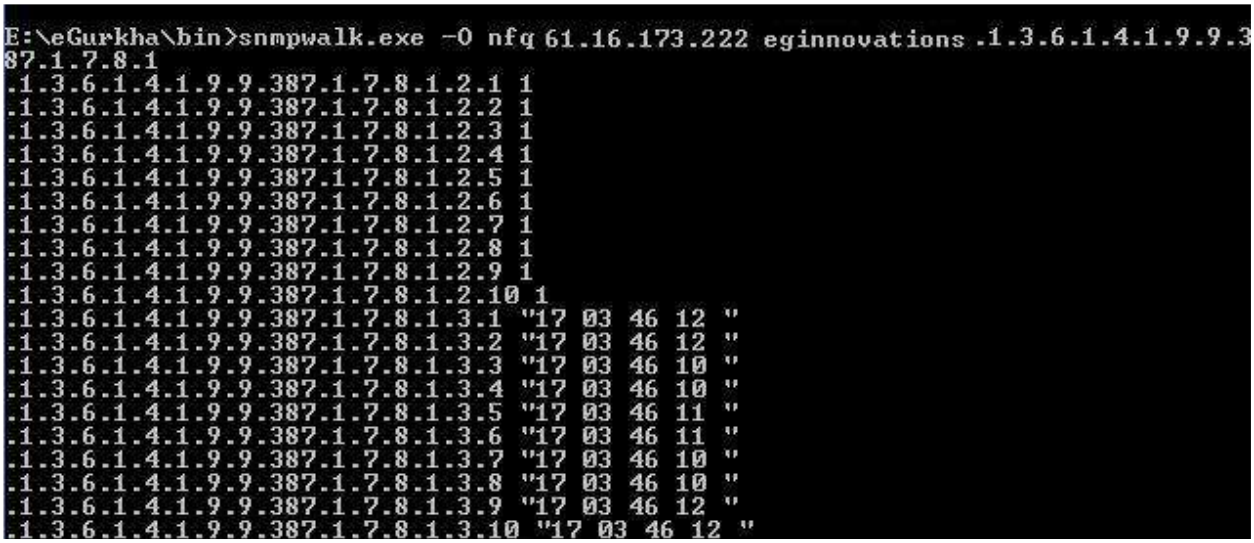

Figure 2.11: The output that appears when Netflow and Top Talkers are enabled

If the Top Talkers are not configured properly or if there are currently no top talkers available, then the output will appear as shown in Figure 2.12.

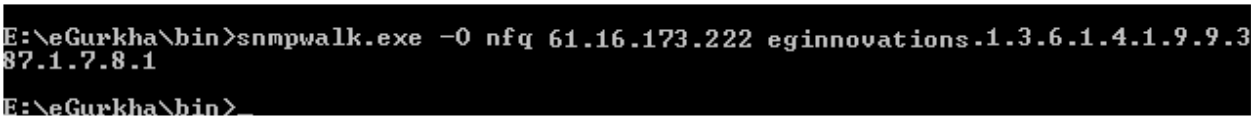

Figure 2.12: The output that appears when top talkers are not available/not configured

:

Chapter 3

Monitoring Network Nodes

Besides routers, eG agents also monitor network nodes. The custom model that eG Enterprise prescribes for monitoring network nodes is depicted by Figure 3.1 below.

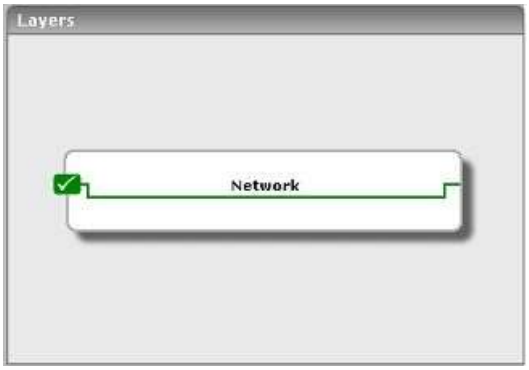

Figure 3.1: The layer model of a network node

The **Network** layer of Figure 3.1 is mapped to a **Network** test which reveals whether the network node is available or not. The metrics reported by this test have been extensively discussed in the *Monitoring Unix and Windows Servers* document.

A **NetworkInterfaces** test and a **Device Uptime** test are also associated with the **Network** layer. For details regarding these tests, refer to Chapter 2 of this document.

Chapter 4

Monitoring Local Directors

A load balancer distributes requests among multiple application servers, with a view to optimally utilizing the available servers. Besides providing scalability and performance enhancements, a load balancer also improves reliability. For example, many load balancers can monitor the status of the different servers they support, and if one of the servers stops responding, a load balancer is able to reroute requests to one of the other servers. By providing a unified virtual image to service requestors, a load balancer enables continuous access to multiple redundant servers for Internet-based e-commerce applications.

In IT infrastructures, load balancers have been used predominantly to balance traffic among multiple web servers. While the traffic they handle has been predominantly TCP-based, recently, some of these load balancers have also been used to handle UDP traffic. Cisco's Local Director product is a very popular load balancer used in IT infrastructures. The eG Enterprise suite includes specialized tests that track the status of a Local Director. The layer model that is used to monitor a Local Director is shown in Figure 4.1.

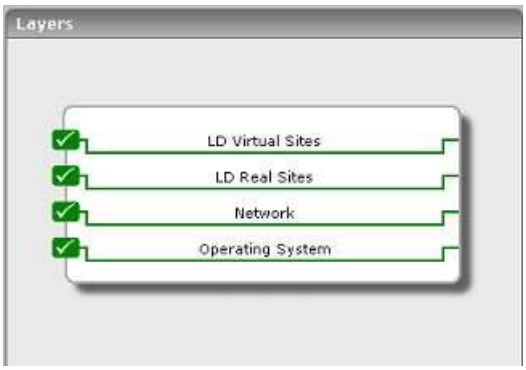

Figure 4.1: Layer model for a Local Director

The following sections discuss each of the layers of Figure 4.1.

4.1 The Operating System Layer

This layer tracks the resource usage of the Local Directory (see Figure 4.2).

Figure 4.2: The tests mapped to the Operating System layer of a Local Director

Both the tests depicted by Figure 4.2 have been discussed elaborately in Chapter 2 of this document.

4.2 The Network Layer

The tests mapped to this layer measure the following:

- The network connectivity of the Local Director and the health of transmissions to and from the Local Director;
- The overall health of all network interfaces configured for the Local Director

Figure 4.3: The tests mapped to the Network layer of a Local Director

The tests depicted by Figure 4.3 have also been handled in Chapter 2 of this document.

4.3 The LD Real Sites Layer

This layer tracks the statistics pertaining to the real servers of the Local Director using the LdRealServer test shown in Figure 4.4.

Figure 4.4: Tests mapping to the LD Real Sites layer

4.3.1 LD Real Servers Test

This test monitors the real servers connected to a Local Director using the snmpwalk command for the OID values provided by the MIB of the Local Director.

Purpose	This test monitors Local Director.
Target of the test	A Local Director
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 Local Director. 3. **SNMPPORT** - The port number through which the Local Director communicates. The default for SNMP 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 Local Director. 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** – The maximum duration (in seconds) for which the test will wait for a response from the Local Director

<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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every Local Director.</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>State:
This measure depicts the state of the server.</td><td>Number</td><td>The state of the server is good if the value reported by this measure is 1. On the other hand the state is unknown, if the value is –1. Any other value reported by this measure signifies that the server is bad.</td></tr>
<tr><td>Connection rate:
Indicates the rate at which connections are made by the Local Director.</td><td>Conns/Sec</td><td>A sudden increase in the number of connections established on a host can indicate either an increase in load to one or more of the applications executing on the host, or that one or more of the applications are experiencing a problem like a slow down.</td></tr>
<tr><td>Data rate:
Indicates the rate of transfer of data.</td><td>MB/Sec</td><td>A significantly high value denotes a heavy traffic in the network.</td></tr>
</table>

4.4 The LD Virtual Sites Layer

The **LD Virtual Sites** layer tracks the statistics pertaining to the virtual servers of the Local Director using the LdVirtualServer test shown in Figure 4.5.

Figure 4.5: Tests mapping to the LD Virtual Sites layer

4.4.1 LD Virtual Server Test

This test monitors the virtual servers of the Local Directors for the OID values provided by the MIB of the Local Director.

Purpose	This test monitors Local Director.
Target of the test	A Local Director
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 Local Director. 3. **SNMPPORT** - The port number through which the Local Director communicates. The default for SNMP 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 Local Directory. 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** – The maximum duration (in seconds) for which the test will wait for a response from the Local Director

<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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every Local Director.</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>State:
This measure depicts the state of the server.</td><td>Number</td><td>The state of the server is good if the value reported by this measure is 1. On the other hand the state is unknown, if the value is –1. Any other value reported by this measure signifies that the server is bad.</td></tr>
<tr><td>Connection rate:
Indicates the rate at which connections are made by the Local Director.</td><td>Conns/Sec</td><td>A sudden increase in the number of connections established on a host can indicate either an increase in load to one or more of the applications executing on the host, or that one or more of the applications are experiencing a problem like a slow down.</td></tr>
<tr><td>Data rate:
Indicates the rate of transfer of data.</td><td>MB/Sec</td><td>A significantly high value denotes a heavy traffic in the network.</td></tr>
</table>

Chapter 5

Monitoring Cisco Catalyst Switches

A network switch is a computer networking device that connects network segments. Low-end network switches appear nearly identical to network hubs, but a switch contains more "intelligence" than a network hub. Network switches are capable of inspecting data packets as they are received, determining the source and destination device of that packet, and forwarding it appropriately. By delivering each message only to the connected device it was intended for, a network switch conserves network bandwidth and offers generally better performance than a hub.

Catalyst is the brand name for a variety of network switches sold by Cisco Systems. Being a popular brand, the Catalyst switch is a regular in many IT infrastructures.

Issues with the switch could be the source of critical infrastructural problems such as excessive bandwidth usage, slow delivery of data packets, or even worse, loss of data during transit!

If such issues are to be averted, then the performance of the Catalyst switch should be monitored 24 x 7.

eG Enterprise has developed an exclusive *Cisco Catalyst Switch* monitoring model (see Figure 5.1), which periodically checks the traffic to and from the switch and the temperature of the switch, so that deviations can be detected before any irrepairable damage is done.

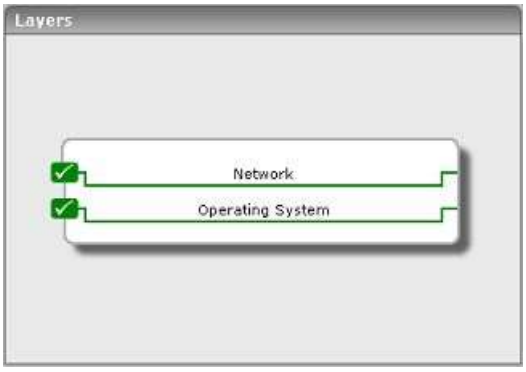

Figure 5.1: Layer model of the Cisco Catalyst Switch

Each of the layers of Figure 5.1 has been briefly discussed in the sections to come.

5.1 The Operating System Layer

This layer tracks the temperature of the Cisco catalyst switch (see Figure 5.2).

Figure 5.2: The tests mapped to the Operating System layer of a Cisco catalyst switch

The CiscoTemperature, CiscoCpu, and CiscoMemory tests have already been discussed in Chapter 2 of this document. This layer is also mapped to the CiscoVoltage and CiscoPowerSupply tests. However, both these tests are disabled by default. To enable the tests, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Cisco Catalyst Siwitch* as the **Component type**, *Performance* as the **Test type**, choose the tests from the **DISABLED TESTS** list, and click on the **>>** button to move the tests to the **ENABLED TESTS** list. Finally, click the **Update** button. For details on these two tests, refer to Chapter 2 of this document.

5.2 The Network Layer

The tests mapped to this layer track the packet transmissions to and from the switch, and the percentage bandwidth used by the switch.

Figure 5.3: The tests that execute on the Network layer of the Cisco Catalyst switch

All the tests depicted by Figure 5.3 have been elaborately discussed in Chapter 2 of this document.

Chapter 6

Monitoring the Cisco VPN Concentrators

The Cisco VPN 3000 Series Concentrators are purpose-built, remote access virtual private network (VPN) platforms that support connectivity mechanisms including IP security (IPSec), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) over IPSec, and Cisco WebVPN (clientless secure sockets layer [SSL] browser-based connectivity). Since they are critical components that provide secure access across disparate networks, VPN concentrators need to be monitored 24*7 to ensure that they are operating well at all times.

eG Enterprise presents a specialized *Cisco VPN* monitoring model (see Figure 6.1), which executes external tests on the VPN concentrator, and reports its current status.

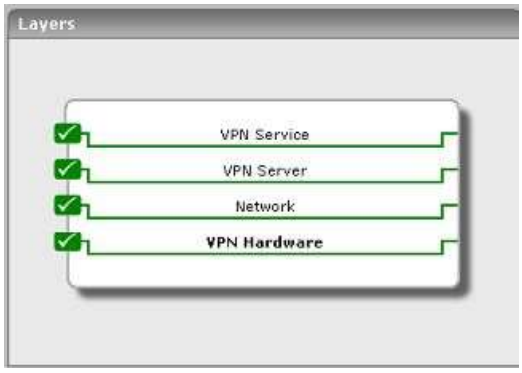

Figure 6.1: The layer model of a Cisco VPN Concentrator

The sections below focus on each layer of Figure 6.1, and tests mapped to the layers.

6.1 The VPN Hardware Layer

This layer, as its name suggests, helps administrators assess the performance of the VPN hardware (see Figure 6.2).

Figure 6.2: The tests mapped to the VPN Hardware layer

6.1.1 VPN Fans Test

The VpnFans test monitors the individual fans on the concentrator and reports whether they are operating normally.

Purpose	Monitors the individual fans on the concentrator and reports whether they are operating normally
Target of the test	A VPN Concentrator
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 host for which the test is being configured 3. **SNMPPORT** - The port number through which the VPN concentrator exposes its SNMP MIB. The default port 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 VPN concentrator. The default is public. 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 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**. 16. **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*.
Outputs of the test	One set of results for every fan on the VPN concentrator being monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Fan1 speed: Indicates the speed of Fan1.	Rpm	
	Fan1 status: Indicates the status of Fan1.	Boolean	If the status is OK, this measure will have a value of 1. Otherwise it will have a value of 0.
	Fan2 speed: Indicates the speed of Fan2.	Rpm	
	Fan2 status: Indicates the status of Fan2.	Boolean	If the status is OK, this measure will have a value of 1. Otherwise it will have a value of 0.
	Fan3 speed: Indicates the speed of Fan3.	Rpm	
	Fan3 status: Indicates the status of Fan3.	Boolean	If the status is OK, this measure will have a value of 1. Otherwise it will have a value of 0.

6.1.2 VPN Temperature Test

The VpnTemperature test monitors the temperature of the different hardware components and alerts if any abnormalities are detected.

Purpose	Monitors the temperature of the different hardware components and alerts if any abnormalities are detected
Target of the test	A VPN Concentrator
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 host for which the test is being configured 3. **SNMPPORT** - The port number through which the VPN concentrator exposes its SNMP MIB. The default port 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 VPN concentrator. The default is public. 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.

<table>
<tr><td></td><td colspan="3">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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every hardware component being monitored</td></tr>
<tr><td rowspan="5">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>CPU temperature:
Indicates the current temperature of the CPU.</td><td>DegreeC</td><td></td></tr>
<tr><td>CPU temperature status:
Indicates the current status of the CPU temperature.</td><td>Boolean</td><td>This metric has a value of 0 if the CPU temperature is abnormal. Otherwise, the value is 1.</td></tr>
<tr><td>Cage temperature status:
Indicates the current cage temperature.</td><td>DegreeC</td><td></td></tr>
<tr><td>Cage temperature:
Indicates the current status of the cage temperature.</td><td>Boolean</td><td>This metric has a value of 0 if the cage temperature is abnormal. Otherwise, the value is 1.</td></tr>
</table>

6.1.3 VPN Voltage Test

The VpnVoltage test monitors whether all voltage levels in the different hardware components are within norms and generates alerts if this is not the case.

Purpose	Monitors whether all voltage levels in the different hardware components are within norms and

	generates alerts if this is not the case
Target of the test	A VPN Concentrator
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 host for which the test is being configured 3. **SNMPPORT** - The port number through which the VPN concentrator exposes its SNMP MIB. The default port 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 VPN concentrator. The default is public. 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 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**. 16. **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*.		
Outputs of the test	One set of results for every hardware component being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Cpu voltage: Indicates the current voltage of the CPU.	Volts	
	Cpu voltage status: Indicates whether the CPU voltage is normal or not.	Boolean	The value is 1 if the voltage is normal. Otherwise, this metric has a value of 0.
	Ps1 3v value: Indicates the current voltage of the 3v power supply 1.	Volts	
	Ps1 3v status: Indicates the status of the 3v power supply's voltage.	Boolean	The value is 1 if the voltage is normal. Otherwise, this metric has a value of 0.
	Ps1 5v value: Indicates the current voltage of the 5v power supply 1.	Volts	
	Ps1 5v status: Indicates the status of the 5v power supply's voltage.	Boolean	The value is 1 if the voltage is normal. Otherwise, this metric has a value of 0.

	Ps2 3v value: Indicates the current voltage of the 3v power supply 2.	Volts	
	Ps2 3v status: Indicates the status of the 3v power supply's voltage.	Boolean	The value is 1 if the voltage is normal. Otherwise, this metric has a value of 0.
	Ps2 5v value: Indicates the current voltage of the 5v power supply 2.	Volts	
	Ps2 5v status: Indicates the status of the 5v power supply's voltage.	Boolean	The value is 1 if the voltage is normal. Otherwise, this metric has a value of 0.
	Board voltage 3v: Indicates the current voltage of the 3v supply to the board.	Volts	
	Board 3v status: Indicates the status of the 3v power supply's voltage.	Boolean	The value is 1 if the voltage is normal. Otherwise, this metric has a value of 0.
	Board voltage 5v: Indicates the current voltage of the 5v supply to the board.	Volts	
	Board 5v status: Indicates the status of the 5v power supply's voltage.	Boolean	The value is 1 if the voltage is normal. Otherwise, this metric has a value of 0.

6.2 The Network Layer

Since the **Network** test, **NetworkInterfaces** test, and **Device Uptime** test associated with this layer have been dealt with in great detail in Chapter 2, let us proceed to the **VPN Server** layer.

6.3 The VPN Server Layer

Using the metrics reported by this layer, administrators can determine whether additional resources need to be allocated to the VPN concentrator for handling the current load.

Figure 6.3: The test mapped to the VPN Server layer

6.3.1 VPN Server Test

The VpnServer test monitors whether the concentrator is adequately sized to handle the current load.

Purpose	Monitors whether the concentrator is adequately sized to handle the current load
Target of the test	A VPN Concentrator
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 host for which the test is being configured 3. **SNMPPORT** - The port number through which the VPN concentrator exposes its SNMP MIB. The default port 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 VPN concentrator. The default is public. 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.

<table>
<tr><td></td><td colspan="3">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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every VPN concentrator being 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>Cpu utilization:
Indicates the current CPU utilization of the VPN Concentrator.</td><td>Percent</td><td>A consistent value greater than 90% indicates a potential bottleneck.</td></tr>
<tr><td>Session utilization:
Indicates the utilization of the VPN concentrator in terms of sessions supported. This value is the ratio of the current sessions to the maximum sessions that the VPN Concentrator can support.</td><td>Percent</td><td></td></tr>
<tr><td></td><td>Throughput utilization:
Indicates the utilization of the VPN concentrator in terms of throughput offered. This value is the ratio of the current throughput to the maximum throughput that the VPN concentrator can support.</td><td>Percent</td><td></td></tr>
</table>

6.4 The VPN Service Layer

The tests mapped to the **VPN Service** layer (see Figure 6.4) measure the throughput of the VPN concentrator and the session load on the server.

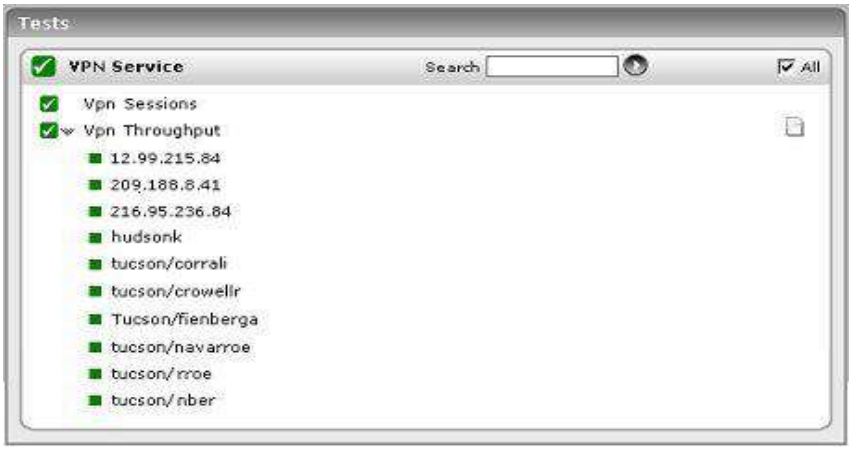

Figure 6.4: The tests associated with the VPN Service layer

6.4.1 VPN Throughput Test

This test tracks the top 10 user sessions with highest data throughput.

Purpose	Tracks the top 10 user sessions with highest data throughput
Target of the test	A VPN Concentrator
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 host for which the test is being configured 3. **SNMPPORT** - The port number through which the VPN concentrator exposes its SNMP MIB. The default port 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 VPN concentrator. The default is public. 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. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

    The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

    - The eG manager license should allow the detailed diagnosis capability
    - Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

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**.

17. **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*.

Outputs of the test: One set of results for every user session being monitored

Measurements made by the test

Measurement	Measurement Unit	Interpretation
Connect time: Indicates the time in mins since when the user connected via the VPN concentrator.	Mins	
Data transmitted: Indicates the data transmitted over the session.	MB	
Data received: Indicates the data received over the session.	MB	eG Enterprise's detailed diagnosis capability will be used to log the IP address of the user, protocol used, encryption type, and the public IP of the user.

6.4.2 VPN Sessions Test

This test monitors the different types of sessions to the Cisco VPN Concentrator.

Purpose	Monitors whether all voltage levels in the different hardware components are within norms and generates alerts if this is not the case
Target of the test	A VPN Concentrator
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 host for which the test is being configured 3. **SNMPPORT** - The port number through which the VPN concentrator exposes its SNMP MIB. The default port 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 VPN concentrator. The default is public. 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.

<table>
<tr><td></td><td colspan="3">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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the VPN concentrator being 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>Active sessions:
Indicates the number of sessions currently actively using the VPN concentrator.</td><td>Number</td><td></td></tr>
<tr><td>New sessions:
Indicates the number of new sessions added in the last measurement period.</td><td>Number</td><td></td></tr>
<tr><td></td><td>Max active sessions:
Indicates the maximum number of active sessions that the VPN concentrator has been configured to handle.</td><td>Number</td><td></td></tr>
</table>

	Session utilization: Indicates the percentage utilization of sessions - this metric is the ratio of the current number of active sessions to the maximum sessions that the concentrator has been configured to handle.	Percent	This measure is a good indicator of the capacity of the concentrator to support more sessions.
	Lan2Lan sessions: Indicates the number of current LAN to LAN sessions supported by the concentrator.	Number	
	Management sessions: Indicates the current number of management sessions to the VPN concentrator.	Number	
	Remote sessions: Indicates the current number of remote sessions handled by the VPN concentrator.	Volts	

Chapter 7

Monitoring the Juniper SA Device

The Juniper Networks Secure Access (SA) VPN is designed for medium to large enterprises, and features performance, scalability, and redundancy for organizations with high volume secure access and authorization requirements. The hardware platform of the SA device is designed to scale to the largest enterprise deployments and optimize application delivery, with available options that include redundant hot swappable hard disks, power supplies and fans, as well as GBIC-based multiple Ethernet ports for the creation of separate physical networks and redundant or meshed configurations. The SA device also features an SSL acceleration chipset to speed CPU-intensive encrypt/decrypt processes, as well as built in compression for all traffic. The SA device is built on the Virtual Extranet (IVE) platform, and uses the Secure Socket Layer (SSL) available in all Web browsers as a means of secure transport.

Any abnormal activity on the Juniper SA device, if not detected on time and resolved, could cause unsavory consequences such as a dramatic increase in the unsafe/unauthorized traffic on your network. Therefore, continuous monitoring of the device becomes mandatory.

By executing a couple of simple tests on the SNMP MIB exposed by the Juniper SA device, the eG external agent performs 24 x 7 monitoring of the SA device, extracts critical performance data from the device, and reports the metrics so gathered to the eG manager. The eG manager in turn, maps these tests to the layers of the unique *Juniper SA* layer model (see Figure 7.1) that it prescribes for the Juniper SA device, and displays the performance data in the eG monitor console.

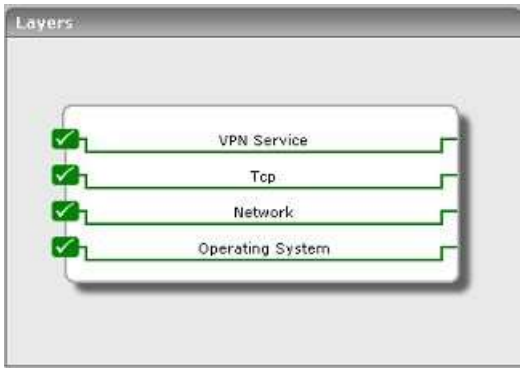

Figure 7.1: The layer model of the Juniper SA VPN

Each of the sub-sections to come will discuss every layer of the layer model, in more detail.

7.1 The Operating System Layer

Using the **IveHostTest** associated with it, the **HOST** layer returns host-level statistics such as the disk space usage, memory usage, etc., of the IVE system.

Figure 7.2: The test associated with the HOST layer

7.1.1 Ive Host Test

The IveHost test reports the host level statistics like disk space, CPU, memory and swap utilization of the Juniper SA device.

Purpose	Reports the host level statistics like disk space, CPU, memory and swap utilization of the Juniper SA device
Target of the test	A Juniper SA device
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 host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper SA device exposes its SNMP MIB. The default port is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Juniper SA device being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Disk space utilization:
Indicates the percentage of disk space utilized on the IVE system.</td><td>Percent</td><td>A value close to 100% can indicate a potential problem situation where applications executing on the system may not be able to write data to the disk partition(s) with very high usage.</td></tr>
<tr><td>Cpu utilization:
Indicates the percentage of CPU utilized on the IVE system.</td><td>Percent</td><td>A high value could signify a CPU bottleneck. The CPU utilization may be high because a few processes are consuming a lot of CPU, or because there are too many processes contending for a limited resource.</td></tr>
<tr><td>Memory utilization:
Indicates the percentage of memory utilized on IVE system.</td><td>Percent</td><td>Ideally, this value should be low.</td></tr>
<tr><td></td><td>Swap utilization:
Indicates the percentage of swap memory utilized on the IVE system.</td><td>Percent</td><td>An unusually high value for the swap usage can indicate a memory bottleneck.</td></tr>
</table>

7.2 The Network Layer

The tests associated with the **Network** layer reflect the status of network connectivity to and from the IVE system, the bandwidth usage of the interfaces supported by the system, and the uptime of the system.

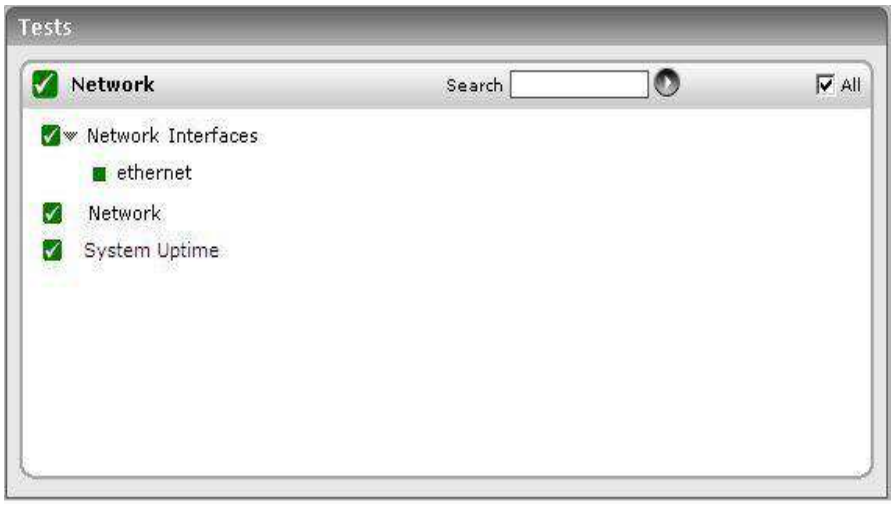

Figure 7.3: The tests associated with the Network layer

All the tests in Figure 7.3 have been dealt with elaborately in many of the previous chapters. Therefore, let us proceed to the next layer.

7.3 The Tcp Layer

The TcpStatistics test associated with the **Tcp** layer measures the incoming and outgoing TCP connections on the IVE system.

Figure 7.4: The test associated with the Tcp layer

7.3.1 TcpStatistics Test

This test reports TCP statistics pertaining to the IVE system.

Purpose	Reports TCP statistics
Target of the test	The Juniper SA device
Agent	An external/remote agent

deploying the test	
Configurable parameters for the test	1. **TEST PERIOD** – How often should the test be executed 2. **HOST** - The host for which the test is to be configured. 3. **SNMPPORT** – The port at which the server 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 target host. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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.

<table>
<tr><td></td><td colspan="3">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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every host being monitored.</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Incoming connections:
Indicates the connections per second received by the server.</td><td>Conns/Sec</td><td>A high value can indicate an increase in input load.</td></tr>
<tr><td>Outgoing connections:
Indicates the connections per second initiated by the server</td><td>Conns/Sec</td><td>A high value can indicate that one or more applications executing on the host have started using a number of TCP connections to some other host(s).</td></tr>
<tr><td>Connection failures:
Indicates the rate of half open TCP connections dropped from the listen queue.</td><td>Conns/Sec</td><td>This value should be 0 for most of the time. A prolonged non-zero value can indicate either that the server is under SYN attack or that there is a problem with the network link to the server that is resulting in connections being dropped without completion.</td></tr>
<tr><td></td><td>Current connections:
Indicates the currently established connections.</td><td>Number</td><td>A sudden increase in the number of connections established on a host can indicate either an increase in load to one or more of the applications executing on the host, or that one or more of the applications are experiencing a problem (e.g., a slow down).</td></tr>
</table>

	Segment rate in: The total number of segments received, including those received with errors. This count includes segments received on currently established connections.	Segments/Sec	
	Segment rate out: Indicates the total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.	Segments/Sec	
	Retransmissions: Indicates the total number of segments retransmitted – that is, the number of TCP segments transmitted containing one or more previously transmitted octets.	Segments/Sec	

7.4 The VPN Service Layer

The wide gamut of services provided by the Juniper SA device are closely monitored using the IveSvc test mapped to the this layer.

Figure 7.5: The test associated with the VPN Service layer

7.4.1 Ive Service Test

The IveSvc test reports the statistics like user sign-ins and various hit ratios of the Juniper SA device.

Purpose	Reports the statistics like user sign-ins and various hit ratios of the Juniper SA device
Target of the test	A Juniper SA device
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 host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper SA device exposes its SNMP MIB. The default port is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Juniper SA device being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Log utilization:
This measure indicates the log file growth in the IVE node.</td><td>Percent</td><td></td></tr>
<tr><td>Signed in web users:
Indicates the number of web users who have signed into the IVE system.</td><td>Number</td><td></td></tr>
<tr><td>Signed in mail users:
Indicates the number of mail users who have signed into the IVE system.</td><td>Number</td><td></td></tr>
<tr><td></td><td>Concurrent users in the IVE node:
Indicates the number of users who have simultaneously logged in for the IVE node.</td><td>Number</td><td></td></tr>
</table>

	Concurrent users in the cluster: Indicates the number of users logged in for the cluster.	Number	
	Total hits: Indicates the total number of hits on the IVE system during the last measurement period.	Number	
	File hits: Indicates the number of files on the IVE system that have been hit during the last measurement period.	Number	
	Web hits: Indicates the number of web hits on the IVE system during the last measurement period.	Number	
	Applet hits: Indicates the number of applet hits on the IVE node during the last measurement period,	Number	
	Terminal hits: Indicates the terminal hits on the IVE system during the last measurement period.	Number	
	Secure app mgr hits: Indicates the number of secure application manager (SAM) hits during the last measurement period.	Number	
	Network connect hits: Indicates the number of network connects hits that have been hits during the last measurement period.	Number	

	Meeting hits: Indicates the number of meeting hits during the last measurement period.	Number	

Chapter 8

Monitoring the Juniper DX Device

The DX Application Acceleration Platform represents a new concept in web server acceleration. It addresses the inefficiencies in server architecture, network architecture, and network protocols that limit the performance of your web site and web servers. The DX appliance solves these inefficiencies by providing its own highly-optimized network architecture and breakthrough data optimization and connection handling capabilities to make your web pages download faster and your web servers more efficient than ever before.

This implies that persistent/even intermittent glitches in the functioning of the DX device could cause a marked deterioration in web server performance. Therefore, continuous monitoring of the device and timely problem detection becomes imperative. This is where the eG Enterprise suite helps big time. By executing a wide variety of tests on the DX device and thoroughly analyzing the critical performance metrics extracted from the SNMP-MIB exposed by the device, the eG Enterprise suite promptly identifies probable issues with the device and proactively cautions administrators of it, so that any damage - big or small - is averted in time.

The tests that the eG agent runs and the measures collected by every test are mapped to each layer of the specialized *Juniper DX* layer model offered by the eG Enterprise suite for the Juniper DX device (see Figure 8.1).

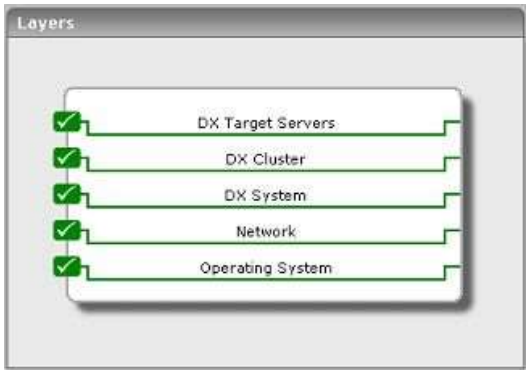

Figure 8.1: Layer model of the Juniper DX device

The sections to come will discuss each of the layers at length.

8.1 The Operating System Layer

Using the SysHost test mapped to it (see Figure 8.2), this layer monitors the CPU and memory utilization of the Juniper DX device.

Figure 8.2: The test associated with the Operating System layer

8.1.1 SysHost Test

This test reports the average CPU and memory utilization of the Juniper DX device.

Purpose	Reports the average CPU and memory utilization of the Juniper DX device
Target of the test	A Juniper DX device
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 host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Juniper DX device being 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>Avg. CPU usage:
Indicates the average CPU utilization of the Juniper DX device.</td><td>Percent</td><td>A high value could signify a CPU bottleneck.</td></tr>
<tr><td>Avg memory usage:
Indicates the average memory utilization of the Juniper DX device.</td><td>Percent</td><td>A very high value of this measure is an indication of high memory utilization on the device.</td></tr>
</table>

8.2 The Network Layer

The **Network** layer measures the network connectivity to and from the Juniper DX device, the availability of its network interfaces, and the uptime of the device (see Figure 8.3).

Figure 8.3: The tests associated with the Network layer

Since these tests have been discussed in great detail in the previous chapters, let us move to the next layer.

8.3 The DX System Layer

With the help of the SysStats test associated with it (see Figure 8.4), the **DX System** layer extracts a wide variety of metrics that enable administrators to assess the following performance parameters:

- Session behaviour on the Juniper DX device
- Request-processing capability of the Juniper DX device
- The data traffic on the device
- The connection-handling capability of the device

Figure 8.4: The tests associated with the DX System layer

8.3.1 System Stats Test

This test reports various statistics related to the session-handling capability, the data traffic, the request processing capability, and the connection-handling capability of the Juniper DX device.

Purpose	Reports various statistics related to the session-handling capability, the data traffic, the request processing capability, and the connection-handling capability of the Juniper DX device

Target of the test	A Juniper DX device
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 host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Juniper DX device being monitored</td></tr>
<tr><td rowspan="5">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Active sessions:
Indicates the number of sessions on the Juniper DX device that are currently active.</td><td>Number</td><td></td></tr>
<tr><td>Sessions handled:
Indicates the number of sessions handled in the last measurement period.</td><td>Number</td><td></td></tr>
<tr><td>Requests handled:
Indicates the number of requests handled in the last measurement period.</td><td>Number</td><td></td></tr>
<tr><td>Requests processed:
Indicates the number of requests processed in the last measurement period.</td><td>Number</td><td></td></tr>
<tr><td></td><td>Connections accepted:
Indicates the number of connections accepted in the last measurement period.</td><td>Number</td><td></td></tr>
</table>

	Connections refused: Indicates the number of connections refused in the last measurement period.	Number	
	Data in: Indicates the data traffic to the Juniper DX device in the last measurement period.	MB	
	Data out: Indicates the data traffic from the Juniper DX device in the last measurement period.	MB	
	Data saved: Indicates the data saved in the last measurement period.	MB	

8.4 The DX Cluster Layer

A Web Cluster is a set of web servers to be accelerated. The DX appliance listens for incoming web traffic to a specific Virtual IP address and port, and distributes it over the target hosts (web servers) in the cluster. Typically, all the web servers in a particular cluster serve identical content; that is, each cluster usually represents a distinct website or property.

The eG agent, by executing the tests associated with the **DX Cluster** layer (see Figure 8.5), reports critical statistics pertaining to each of the web clusters managed by the DX device.

Figure 8.5: The tests associated with the DX Cluster layer

8.4.1 Cluster HTTP Test

This test reports the HTTP statistics per Web cluster that is supported by a Juniper DX device.

Purpose	Reports the HTTP statistics per Web cluster that is supported by a Juniper DX device
Target of the test	A Juniper DX device
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 host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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**. 17. **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*.		
Outputs of the test	One set of results for every Web cluster supported by the Juniper DX device being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Active requests: Indicates the number of active HTTP requests to the cluster.	Number	
	300 responses: Indicates the number of HTTP requests with response code between 300-399 in the last measurement period.	Number	300 responses could indicate page caching on the client browsers. Alternatively 300 responses could also indicate redirection of requests. A sudden change in this value could indicate a problem condition.
	400 errors: Indicates the number of HTTP requests with response code between 400-499.	Number	A high value indicates a number of missing/error pages.
	500 errors: Indicates the number of HTTP requests with response code between 500-599 in the last measurement period.	Number	Since responses with a status code of 500-600 indicate server side processing errors, a high value reflects an error condition.

8.4.2 ClusterHttpStats Test

This test reports the HTTP statistics per Web cluster that is supported by a Juniper DX device.

Purpose	Reports the HTTP statistics per Web cluster that is supported by a Juniper DX device
Target of the test	A Juniper DX device
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 host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every Web cluster supported by the Juniper DX device being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Active requests:
Indicates the number of HTTP requests to the cluster that are currently active.</td><td>Number</td><td></td></tr>
<tr><td>Total requests:
Indicates the total number of HTTP requests to the cluster during the last measurement period.</td><td>Number</td><td></td></tr>
<tr><td>GET requests:
Indicates the number of GET HTTP requests to the cluster.</td><td>Number</td><td></td></tr>
<tr><td></td><td>POST requests:
Indicates the number of POST HTTP requests to the cluster.</td><td>Number</td><td></td></tr>
</table>

8.4.3 Cluster I/O Test

This test reports the IO statistics for every Web cluster that is supported by a Juniper DX device.

Purpose	Reports the IO statistics for every Web cluster that is supported by a Juniper DX device
Target of the test	A Juniper DX device
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 host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every Web cluster served by the Juniper DX device being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Active sessions:
Indicates the number of new sessions in the listen side in the last measurement period.</td><td>Number</td><td></td></tr>
<tr><td>Sessions handled:
Indicates the number of reused sessions in the listen side in the last measurement period.</td><td>Number</td><td></td></tr>
<tr><td>Sessions refused:
Indicates the number of sessions to the cluster that were refused in the last measurement period.</td><td>Number</td><td></td></tr>
<tr><td></td><td>Active requests:
Indicates the number of requests to this cluster that are currently active.</td><td>Number</td><td></td></tr>
</table>

	Total requests: Indicates the total number of requests to the cluster in the last measurement period.	Number	
	Listen data in: Indicates the listen data traffic to this cluster in the last measurement period.	MB	
	Listen data out: Indicates the listen data traffic from this cluster in the last measurement period.	MB	
	Target data in: Indicates the target data traffic to the cluster in the last measurement period.	MB	
	Target data out: Indicates the target data traffic from the cluster in the last measurement period.	MB	

8.4.4 Cluster SSL Test

This test reports the SSL statistics for every Web cluster that is supported by a Juniper DX device.

Purpose	Reports the SSL statistics for every Web cluster that is supported by a Juniper DX device
Target of the test	A Juniper DX device
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 host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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. **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**. 16. **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*.		
Outputs of the test	One set of results for every Web cluster supported by the Juniper DX device being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	New sessions in the listen side: Indicates the number of new sessions in the listen side in the last measurement period.	Number	
	Reused listen sessions: Indicates the number of reused sessions in the listen side in the last measurement period.	Number	
	New target sessions: Indicates the number of new sessions in the target side in the last measurement period.	Number	
	New target reused sessions: Indicates the number of reused sessions in the target side in the last measurement period.	Number	

8.4.5 Cluster Status Test

This test reports the status of the Web cluster that is supported by a Juniper DX device.

Purpose	Reports the status of the Web cluster accelerated by the Juniper DX device
Target of the test	A Juniper DX device
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 host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every Web cluster that is supported by a Juniper DX device</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>Cluster is not available:
Indicates the availability of the Web cluster.</td><td>Percent</td><td>The value 100 indicates that the cluster is available, and 0 indicates that the cluster is not currently available.</td></tr>
</table>

8.5 The DX Target Servers Layer

This layer monitors the performance of the target web servers in a Web cluster, and reports a wide range of performance data pertaining to each of the servers. Figure 8.6 depicts the tests associated with this layer.

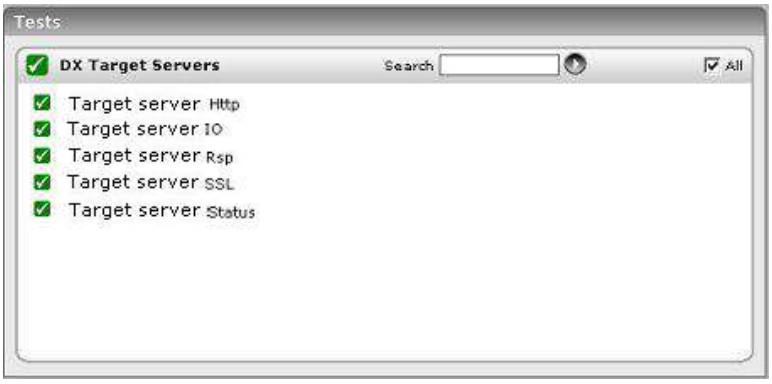

Figure 8.6: The tests associated with the DX Target Servers layer

8.5.1 Target Server Status Test

This test reports the status of the target server in the Web cluster that is supported by a Juniper DX device.

Purpose	Reports the status of the target server in the Web cluster that is supported by a Juniper DX device
Target of the test	A Juniper DX device
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 host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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**. 17. **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*.
Outputs of the test	One set of results for every target server that is supported by the Juniper DX device

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Target server availability: Indicates the availability of the target server.	Percent	A value of 100 indicates that the server is available, and a value of 0 indicates that the server is not currently available.

8.5.2 Target Server I/O Test

This test reports the IO statistics for each of the target servers supported by the Juniper DX device.

Purpose	Reports the IO statistics for each of the target servers supported by the Juniper DX device
Target of the test	A Juniper DX device
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 host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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**. 17. **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*.
Outputs of the test	One set of results for every target server supported by the Juniper DX device being monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Data in: Indicates the data traffic to the target server in the last measurement period.	MB	
	Data out: Indicates the data traffic from the target server in the last measurement period.	MB	

8.5.3 Target Server Response Test

This test reports the HTTP error statistics of the target servers in the Web cluster that is supported by a Juniper DX device.

Purpose	Reports the HTTP statistics of the target servers in the Web cluster that is supported by a Juniper DX device
Target of the test	A Juniper DX device
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 host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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**. 17. **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*.		
Outputs of the test	One set of results for every target server served by the Juniper DX device being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	300 responses: Indicates the number of HTTP requests with response code between 300-399 in the last measurement period.	Number	300 responses could indicate page caching on the client browsers. Alternatively 300 responses could also indicate redirection of requests. A sudden change in this value could indicate a problem condition.
	400 responses: Indicates the number of HTTP requests with response code between 400-499.	Number	A high value indicates a number of missing/errored pages.
	500 responses: Indicates the number of HTTP requests with response code between 500-599 in the last measurement period.	Number	Since responses with a status code of 500-600 indicate server side processing errors, a high value reflects an error condition.

	404 responses: Indicates the number of HTTP requests with the response code 404 in the last measurement period.	Number	The 404 or Not Found error message is an HTTP standard response code indicating that the client was able to communicate with the server but either the server could not find what was requested, or it was configured not to fulfill the request and not reveal the reason why. A 404 error is often returned when pages have been moved or deleted.

8.5.4 Target Server SSL Test

This test reports the SSL statistics of the target servers in the Web cluster that is supported by a Juniper DX device.

Purpose	Reports the SSL statistics of the target servers in the Web cluster that is supported by a Juniper DX device
Target of the test	A Juniper DX device
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 host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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**. 17. **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*.
Outputs of the test	One set of results for every target server supported by the Juniper DX device being monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	New sessions: Indicates the number of new SSL sessions to a target server.	Number	
	Reused sessions: Indicates the number of reused SSL sessions to a target server.	Number	

8.5.5 Target Server Http Test

This test reports the HTTP statistics of the target servers in the Web cluster that is supported by a Juniper DX device.

Purpose	Reports the HTTP statistics of the target servers in the Web cluster that is supported by a Juniper DX device
Target of the test	A Juniper DX device
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 host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

Outputs of the test	One set of results for every target server supported by the Juniper DX device being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	300 responses: Indicates the number of HTTP requests with response code between 300-399 in the last measurement period.	Number	300 responses could indicate page caching on the client browsers. Alternatively 300 responses could also indicate redirection of requests. A sudden change in this value could indicate a problem condition.
	400 errors: Indicates the number of HTTP requests with response code between 400-499.	Number	A high value indicates a number of missing/error pages.
	500 errors: Indicates the number of HTTP requests with response code between 500-599 in the last measurement period.	Number	Since responses with a status code of 500-600 indicate server side processing errors, a high value reflects an error condition.

Chapter 9

Monitoring the 3COM CoreBuilder Switch

The CoreBuilder 3500 Layer 3 high-function switch is a modular, standalone networking device that supports high-performance Fast Ethernet, Gigabit Ethernet, and FDDI interfaces.

Like any other network device, the eG Enterprise system monitors the CoreBuilder switch too using SNMP. The *3Com Core Builder* monitoring model that eG Enterprise has designed, is shown below:

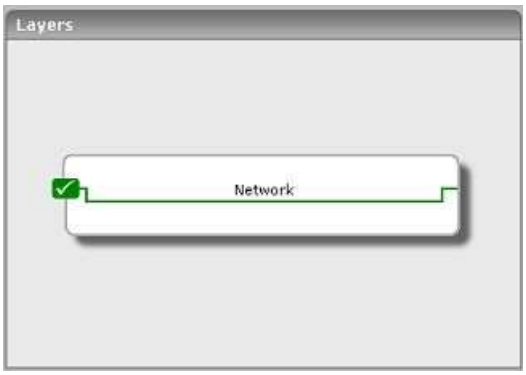

Figure 9.1: The layer model of a 3Com Core Builder

The following section talks about the **Network** layer of Figure 9.1 above.

9.1 The Network Layer

Besides revealing whether the switch is available or not, the tests mapped to the **Network** layer also indicate how well the interfaces supported by the switch are performing (see Figure 9.2).

The external agent monitoring the switch first polls the management module of the SNMP MIB-11, which in turn provides the details of all the other modules, their community strings, etc. Using this information, the agent then contacts the other modules, discovers the network interfaces supported by the switch, and then extracts key statistics pertaining to the availability and speed of each of the network interfaces.

Figure 9.2: The tests mapped to the Network layer of the 3Com Core Builder

As enough has already been said about the **Network** test and the **Device Uptime** test, let us just focus on the CoreBuilder test in Figure 9.2.

9.1.1 Core Builder Test

The CoreBuilder test monitors critical metrics relating to each of the network interfaces of a 3 COM CoreBuilder switch.

Purpose	Monitors critical metrics relating to each of the network interfaces of a 3 COM CoreBuilder switch
Target of the test	A 3COM CoreBuilder 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 server Ensure that the specified **HOST** is SNMP-enabled. If not, the test will not function. 3. **SNMPPORT** - The default SNMP port is 25 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 target device. 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.

<table>
<tr><td></td><td colspan="3">14. ONLYUP – If the ONLYUP flag is set to Yes, then only the network interfaces that are operational - i.e. whose MIB-II operStatus variable has a value "up" - are monitored. If this flag is set to No, all network interfaces that have an adminStatus of "up" will be monitored.
15. FULLDUPLEX - If this value is Yes, then it indicates that all interfaces are full duplex. In this case, the eG Enterprise system will compute bandwidth usage % to be, max(input bandwidth, output bandwidth)*100/total speed. On the other hand, if this flag is set to No, then the computation of bandwidth usage % will be (input bandwidth + output bandwidth)*100/total speed.
16. TIMEOUT - The maximum duration (in seconds) for which the test will wait for a response from the network interface
17. 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.
18. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of records for each interface</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>Availability:
Indicates the availability of a network interface</td><td>Percent</td><td>This value is 100 if an interface is operational - i.e., has an operStatus of "up". The value is 0 otherwise.</td></tr>
<tr><td>Data transmit rate:
Indicates the rate of data being transmitted from the network interface over a network link</td><td>MB/Sec</td><td>This measurement depicts the workload on a network link.</td></tr>
<tr><td></td><td>Data received rate:
The rate of data being received by the network interface over a network link</td><td>MB/Sec</td><td>This measure also characterizes the workload on a network link.</td></tr>
</table>

	Speed: Speed of the network interface	Mbps	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.
	Bandwidth usage: Indicates the percentage utilization of the bandwidth available over a network link	Percent	A value close to 100% indicates a network bottleneck.

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.

Chapter 10

Monitoring F5 BIG-IP Load Balancers

An F5 BIG-IP load balancer distributes the processing and communications activity evenly across groups of servers in a network, so that no single server is overwhelmed. The BIG-IP load balancer keeps a constant check on the incoming and outgoing traffic of the servers in the server pools. By default, it will route the user requests to the most available server that can best handle them (see Figure 10.1). Moreover, the load balancer maintains network connectivity along multiple ISP paths, and thus ensures high availability of the servers in a pool.

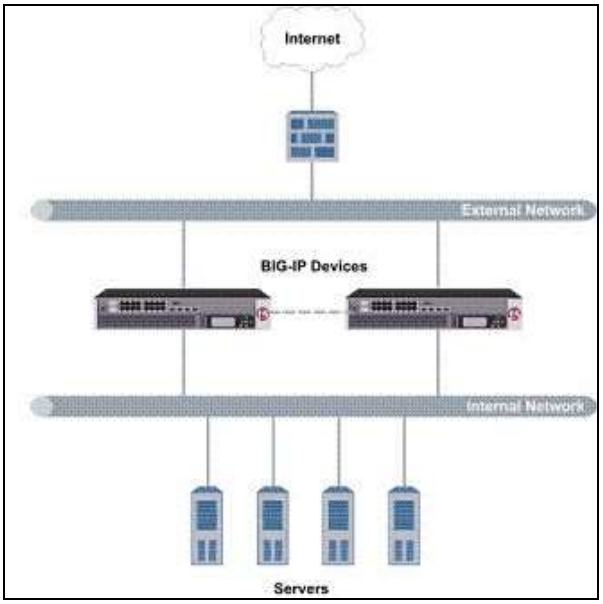

Figure 10.1: How the BIG-IP load balancer works?

Since it plays a critical role in an Internet facing IT infrastructure, even a slight deterioration in the performance of a load balancer can adversely impact the critical IT services of an enterprise, thereby resulting in considerable revenue loss. In order to prevent such adversities, it is imperative that BIG-IP load balancers are continuously monitored.

The eG Enterprise suite provides a specialized *F5 BigIp* model (see Figure 10.2) for managing a BIG-IP load balancer.

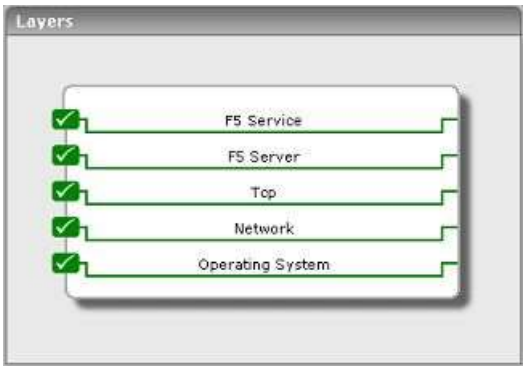

Figure 10.2: The layer model of a BIG-IP load balancer

Every layer of the layer model depicted by Figure 10.2 is mapped to one/more tests, which uses the host's SNMP MIB to extract critical statistics pertaining to the load balancing activity performed by BIG-IP. The performance metrics reported by these measures reveal the following:

System Monitoring	• Is the Big-IP hardware sufficiently sized to handle the incoming load, or is there a CPU or a memory bottleneck? • Is I/O activity on the system abnormal? • Are context switches kept at a minimum, or are there too many threads contending for CPU resources? • How much swap space is currently available in the system? Is it sufficient?
Workload Monitoring	• What is the current total workload on the Big-IP load balancer? Has there been any change in the workload over time? • How much traffic is the load balancer handling? How many connections
Load Distribution monitoring	• Has any of the servers across which the load is being balanced failed? • Is network load balanced across all the servers in the pool? • Is any server in the pool handling more connection requests than others?

Each of the layers is discussed in the sections below.

10.1 The Operating System Layer

The tests associated with this layer (see Figure 10.3) provide valuable insights into the memory and CPU usage of the BIG-IP load balancer. From these tests, an administrator can determine if there is a memory or CPU bottleneck on the load balancer.

Figure 10.3: The tests associated with the Operating System layer

10.1.1 Memory Statistics Test

This test monitors the available and used memory of a BIG-IP load balancer. The Net-SNMP MIB is polled by this test to extract the metrics below:

Purpose	Monitors the available and used memory of a BIG-IP load balancer.
Target of the test	A BIG-IP Load Balancer
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 host for which the test is being configured 3. **SNMPPORT** - The port number through which the BIG-IP load balancer exposes its SNMP MIB. The default port 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.

16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the BIG-IP load balancer being monitored</td></tr>
<tr><td rowspan="5">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Total real memory:
Indicates the total real memory space on the host.</td><td>MB</td><td></td></tr>
<tr><td>Available memory:
Indicates the available real/physical memory space on the host.</td><td>MB</td><td>Ideally, this value should be high.</td></tr>
<tr><td>Free virtual memory:
Indicates available virtual memory on the host.</td><td>MB</td><td></td></tr>
<tr><td>Total swap memory:
Indicates the total swap size configured for the host.</td><td>MB</td><td></td></tr>
<tr><td></td><td>Available swap:
Indicates the available swap space on the host.</td><td>MB</td><td>An unusually low value for the available swap space can indicate a memory bottleneck. Check the memory utilization of individual processes to figure out the process (es) that has (have) maximum memory consumption and look to tune their memory usages and allocations accordingly.</td></tr>
</table>

	Swap memory errors: Indicates whether adequate swap space is available or not.	Boolean	A value of 1 indicates that there is very little swap space left. A value of 0 indicates normalcy with respect to available swap space.
	Shared memory usage: Indicates the total shared memory on the host.	MB	
	Buffered memory: Indicates the total buffered memory on the host.	MB	
	Cached memory: Indicates the total cached memory on the host.	MB	
	Memory swap ins: Indicates the amount of memory swapped in from disk per second.	KB/Sec	
	Memory swap outs: Indicates the amount of memory swapped out to disk per second.	KB/Sec	

10.1.2 System Statistics Test

This test measures the key system performance metrics of a BIG-IP load balancer.

Purpose	Measures the key system performance metrics for a BIG-IP load balancer.
Target of the test	A BIG-IP Load Balancer
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 host for which the test is being configured 3. **SNMPPORT** - The port number through which the BIG-IP load balancer exposes its SNMP MIB. The default port 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the BIG-IP load balancer being 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>I/O sent:
Indicates the rate of I/O blocks sent to a block device during the last measurement period.</td><td>Blocks/Sec</td><td></td></tr>
<tr><td>I/O received:
Indicates the rate of I/O blocks sent from a block device during the last measurement period.</td><td>Blocks/Sec</td><td>When viewed with the IO_sent measure, this reveals the level of I/O activity on the load balancer.</td></tr>
<tr><td></td><td>System interrupts:
Indicates the number of interrupts per second processed by the system/</td><td>Interrupts/Sec</td><td></td></tr>
</table>

	Context switches: Indicates the rate of context switches that happened on the system during the last measurement period.	ContextSwitches/Sec	Context switches occur when a running thread voluntarily relinquishes the processor, is preempted by a higher priority ready thread, or switches between user-mode and privileged (kernel) mode to use an Executive or subsystem service. If the context switch rate is unusually high, it implies that there is excessive contention for CPU resources.
	User CPU utilization: Indicates the current user CPU utilization of the system.	Percent	
	System CPU utilization: Indicates the current system CPU utilization of the system.	Percent	An unusually high value indicates a problem and may be due to too many system-level tasks executing simultaneously.

10.2 The Network Layer

To know the health of the network connection to the load balancer, and the level of traffic emerging from and flowing to the load balancer, use the tests associated with the **Network** layer.

Figure 10.4: The tests associated with the Network layer

These tests have been elaborately discussed in the previous chapters. So, let us proceed to the **Tcp** layer.

10.3 The Tcp Layer

To observe the TCP connections and retransmissions to and from the load balancer, use the TcpStatistics test associated with the **Tcp** layer. This test has already been described in the previous chapters.

Figure 10.5: The test associated with the Tcp layer

10.4 The F5 Server Layer

Every physical server in a server pool is mapped by the BIG-IP load balancer to one or more virtual servers. A Virtual Server is a combination of virtual address and virtual port, associated with a content site that is managed by a BIG-IP system. When the load balancer receives requests from clients to a virtual server, it routes them to the appropriate physical server in the pool.

The F5Status test associated with this layer reports the status of incoming and outgoing traffic through a load balancer (see Figure 10.6).

Figure 10.6: The test associated with the F5 Server layer

10.4.1 F5 Status Test

This test provides key indicators of the workload being handled by the load balancer.

Purpose	Reports various metrics that define the workload being handled by a BIG-IP load balancer.
Target of the test	A BIG-IP Load Balancer
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 host for which the test is being configured 3. **SNMPPORT** - The port number through which the BIG-IP load balancer exposes its SNMP MIB. The default port 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each load balancer.</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Incoming traffic:
Indicates the rate at which data is received by the load balancer during the last measurement period.</td><td>Mbps</td><td>An abnormally high rate of incoming traffic may require additional analysis.</td></tr>
<tr><td>Outgoing traffic:
Indicates the rate at which responses are being sent from the load balancer during the last measurement period.</td><td>Mbps</td><td>An abnormally high rate of outgoing traffic may require additional analysis.</td></tr>
<tr><td>Incoming packet rate:
Indicates the number of packets received per second by the load balancer during the last measurement period.</td><td>Packets/Sec</td><td></td></tr>
<tr><td></td><td>Outgoing packet rate:
Indicates the number of packets sent out per second by the load balancer during the last measurement period.</td><td>Packets/Sec</td><td></td></tr>
</table>

	Current connections: Indicates the number of connections currently established by the load balancer with the servers in the pool.	Number	A very useful metric to trend regarding a load balancer is the total number of concurrent connections. This counts the number of sessions the BIG-IP load balancer is handling. This metric is the number of open TCP sessions that users have currently established. UDP is not included in this of course, as UDP is a connectionless protocol.
	Connection rate: Indicates the rate at which connections have been handled by the load balancer during the last measurement period	Conns/Sec	The connection rate is the most important metric to keep track of for any load balancer as it is typically the most resource-intensive, especially for web sites with small files and a high rate of connections.
	Connection timeouts: Indicates the number of connections that timed out during the last measurement value.	Number	A very high value of this measure indicates frequent connection timeouts. In such a case, you might want to consider resetting the timeout period for connections.
	Memory pool total: Represents the total memory pool available on the system.	MB	
	Memory pool used: Indicates the total memory pool in use by the system.	MB	If this metric is close to the *Memory pool total*, this implies that there is a memory bottleneck on the BIG-IP load balancer.
	Memory pool utilization: Indicates the percentage of memory in the memory pool that has been utilized.	Percent	Ideally, this value should be low. A value close to 100 denotes a memory bottleneck on the load balancer.
	Memory errors: Indicates the total number of memory access errors that occurred during the last measurement period.	Number	Ideally, this value should be 0.

10.5 The F5 Service Layer

Using the tests associated with this layer (see Figure 10.7), eG Enterprise monitors the traffic routed through each of the virtual servers and virtual IP addresses configured on the load balancer.

Figure 10.7: The tests associated with the F5 Service layer

10.5.1 BigIp Pools Test

A BIG-IP pool is a set of devices grouped together to receive traffic according to a load-balancing method. Monitoring of the pools configured for a Big IP load balancer can indicate the relative load on the load balancer from the different pools. The F5 Pools test tracks the status and the traffic on each of the pools configured on the BIG-IP load balancer.

Purpose	Tracks the status and the traffic on each of the pools configured on the BIG-IP load balancer
Target of the test	A BIG-IP Load Balancer
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 host for which the test is being configured 3. **SNMPPORT** - The port number through which the BIG-IP load balancer exposes its SNMP MIB. The default port 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every pool configured for the BIG-IP load balancer being 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>Incoming traffic:
Indicates the rate at which requests are routed through this pool during the last measurement period.</td><td>Mbps</td><td>An abnormally high rate of incoming traffic may require additional analysis. By comparing the values of this metric with the outgoing rate, you can easily identify which pools are experiencing high traffic.</td></tr>
<tr><td>Outgoing traffic:
Indicates the rate at which responses from the servers are transmitted by the pool during the last measurement period.</td><td>Mbps</td><td>An abnormally high rate of outgoing traffic may require additional analysis.</td></tr>
<tr><td></td><td>Incoming packet rate:
Indicates the number of packets per second routed to the physical server(s) in the pool during the last measurement period.</td><td>Packets/Sec</td><td>Both these measure serve as effective indicators of the data load on the load balancer.</td></tr>
</table>

	Outgoing packet rate: Indicates the number of packets per second sent out through the pool during the last measurement period.	Packets/Sec	
	Current connections: Indicates the number of connections currently established for this pool.	Number	Comparison of this metric across pools indicates which of the pools is handling a higher load.
	Connection rate: Indicates the rate at which connections have been established via a pool during the last measurement period.	Conns/Sec	

10.5.2 BigIp Virtual Addresses Test

This test tracks the status and the traffic on each of the virtual IP addresses configured on the BIG-IP load balancer.

Purpose	Reports the status and the traffic on each of the virtual IP addresses configured on the BIG-IP load balancer.
Target of the test	A BIG-IP Load Balancer
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 host for which the test is being configured 3. **SNMPPORT** - The port number through which the BIG-IP load balancer exposes its SNMP MIB. The default port 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.

16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every virtual IP configured on the BIG-IP load balancer being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Status:
Indicates whether this virtual IP address is currently active or inactive.</td><td>Number</td><td>While the value 0 indicates that the virtual IP is inactive, 1 indicates that it is active.</td></tr>
<tr><td>Incoming traffic:
Indicates the rate at which requests are routed through this virtual IP during the last measurement period.</td><td>Mbps</td><td>An abnormally high rate of incoming traffic may require additional analysis. A comparison of the values of this metric with the outgoing rate can be used to identify which of the virtual addresses is seeing high traffic rates.</td></tr>
<tr><td>Outgoing traffic:
Indicates the rate at which responses from the servers are transmitted by the virtual IP during the last measurement period.</td><td>Mbps</td><td>An abnormally high rate of outgoing traffic may require additional analysis.</td></tr>
<tr><td></td><td>Incoming packet rate:
Indicates the number of packets per second routed to the physical server(s) in the pool through this virtual IP during the last measurement period.</td><td>Packets/Sec</td><td></td></tr>
</table>

	Outgoing packet rate: Indicates the number of packets per second sent out through this virtual IP during the last measurement period.	Packets/Sec	
	Current connections: Indicates the number of connections currently established via this virtual IP.	Number	Comparison of this metric across virtual IPs indicates which of the virtual IPs is handling a higher load.
	Connection rate: Indicates the rate at which connections have been established via this virtual IP during the last measurement period.	Conns/Sec	

10.5.3 BigIp Virtual Servers Test

A virtual server is a combination of virtual IP address and port, through which incoming traffic to a server pool is load balanced by the BIG-IP load balancer. This test monitors the status and traffic on every virtual server configured on the BIG-IP.

Purpose	Monitors the status of and the traffic on each of the virtual servers configured on the BIG-IP load balancer.
Target of the test	A BIG-IP Load Balancer
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 host for which the test is being configured 3. **SNMPPORT** - The port number through which the BIG-IP load balancer exposes its SNMP MIB. The default port 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every virtual server configured on the BIG-IP load balancer being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Status:
Indicates whether this virtual server is active or inactive.</td><td>Number</td><td>While the value 0 indicates that the virtual server is inactive, 1 indicates that it is active.</td></tr>
<tr><td>Incoming traffic:
Indicates the rate at which traffic was routed through this virtual server during the last measurement period.</td><td>Mbps</td><td>An abnormally high rate of incoming traffic may require additional analysis.</td></tr>
<tr><td>Outgoing traffic:
Indicates the rate at which traffic was transmitted from a virtual server in the last measurement period.</td><td>Mbps</td><td>An abnormally high rate of outgoing traffic may require additional analysis.</td></tr>
<tr><td></td><td>Incoming packet rate:
Indicates the number of packets per second routed to the physical server(s) in the pool through this virtual server.</td><td>Packets/Sec</td><td></td></tr>
</table>

	Outgoing packet rate: Indicates the number of packets per second sent out through this virtual server.	Packets/Sec	
	Current connections: Indicates the number of connections currently established via this virtual server.	Number	
	Connection rate: Indicates the rate at which connections have been established via this virtual server during the last measurement period.	Conns/Sec	Comparison of this metric across virtual servers indicates which of the virtual servers is handling a higher load.

Chapter 11

Monitoring Brocade SAN Switches

The Brocade SAN Switch is a 16-port embedded switch. It supports link speeds up to 2 Gbit/sec. The Brocade SAN Switch is based on the Brocade Fabric Operating System™ (Fabric OS) version 4.x, and is compatible with the entire Brocade SilkWorm product family.

eG Enterprise embeds a specialized *Brocade SAN switch* monitoring model (see Figure 11.1), which enables users to run periodic status checks on the availability, hardware, and the fabric switches at the heart of the Brocade SAN switch, and reports problems (if any) with those components.

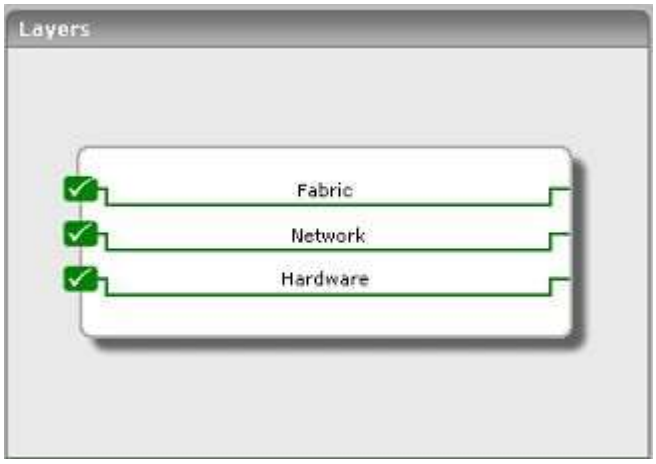

Figure 11.1: The layer model of the Brocade SAN switch

The sections to come discuss each layer of Figure 11.1 in great detail.

11.1 The Hardware Layer

This layer tracks the status of the different types of sensors on the switch (see Figure 11.2).

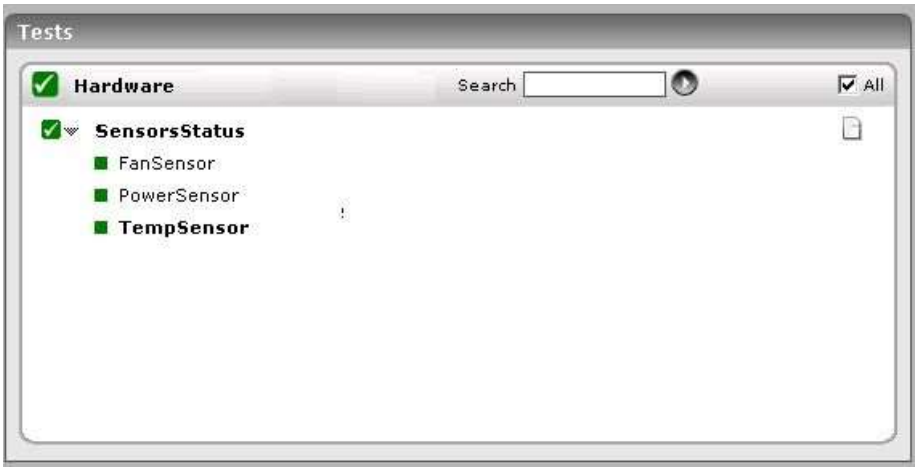

Figure 11.2: The tests mapped to the Hardware layer

11.1.1 SensorsStatus Test

Sensors are of three types namely Fansensor, PowerSensor and TemperatureSensor. The SensorTest monitors each of the above-mentioned sensor types on the Brocade 48000 switch, and reports the number of sensors of every type that are in varying states of activity such as normal, faulty, unknown, or absent.

Purpose	Monitors each sensor type and reports the number of sensors of every type that are in varying states of activity such as normal, faulty, unknown, or absent
Target of the test	A Brocade 48000 switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **PORT** – The port on which the switch is listening 4. **SNMPPORT** – The port at which the switch exposes its SNMP MIB 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.

The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
• The eG manager license should allow the detailed diagnosis capability
• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every type of sensor on the monitored Brocade 48000 switch</td></tr>
<tr><td rowspan="5">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Total sensors:
The total number of sensors of this type currently available on the switch.</td><td>Number</td><td>The detailed diagnosis of this measure, if enabled, provides the complete details of sensors such as the Sensor ID, Sensor name, and the current state of the sensor.</td></tr>
<tr><td>Normal sensors:
The number of sensors of this type that are currently in a normal state.</td><td>Number</td><td></td></tr>
<tr><td>Unknown sensors:
The number of sensors of this type that are currently in an unknown state.</td><td>Number</td><td></td></tr>
<tr><td>Faulty sensors:
The number of sensors of this type that are currently in a faulty state.</td><td>Number</td><td>Ideally, this value should be low.</td></tr>
<tr><td></td><td>Absent sensors:
The number of sensors of this type that are currently absent.</td><td>Number</td><td></td></tr>
</table>

	New nomal sensors: The number of sensors of this type that were in the normal state during the last measurement period.	Number	
	New unknown sensors: The number of sensors of this type that were in the unknown state during the last measurement period.	Number	
	New faulty sensors: The number of sensors of this type that were faulty during the last measurement period.	Number	Ideally, this value should be low.
	New absent sensors: The number of sensors of this type that were absent during the last measurement period.	Number	

11.2 The Network Layer

The tests mapped to this layer indicate whether the switch is available or not, how well the network interfaces supported by the switch are performing, and the uptime of the switch.

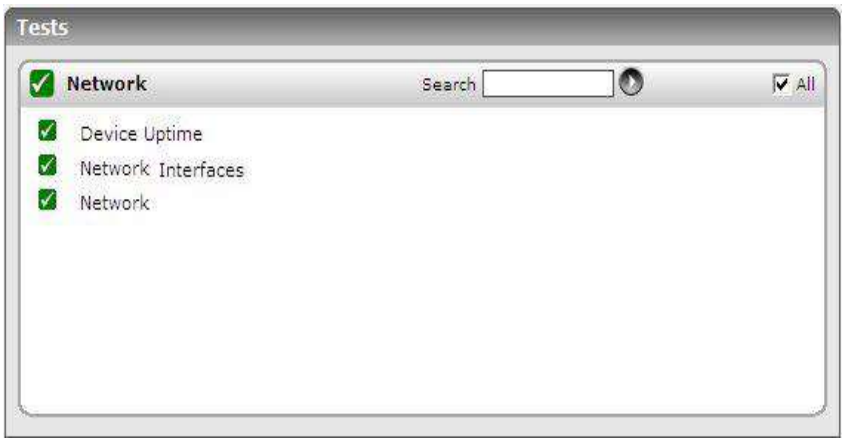

Figure 11.3: The test associated with the Network layer

Since all these tests have been discussed in detail in the Chapter 2 of this document, let us move to the next layer.

11.3 The Fabric Layer

The heart of a SAN are Fibre Channel switches that provide any-to-any connectivity for servers and storage devices. Switch product lines range from entry- to enterprise-level to meet a wide range of changing business requirements. Two or more interconnected switches create a SAN fabric. Fabrics allow you to optimize your SAN for performance, scalability, and availability. Some switches include a high-value fabric operating system that provides intelligence, enabling advanced SAN fabric management, monitoring, and security. The tests associated with the **Fabric** layer report the health of the fabric switch (see Figure 11.4.

Figure 11.4: The tests associated with the Fabric layer

11.3.1 Fabric Ports Test

The FabricPorts test reports the current state of the ports available on the Fabric switch. Typically, a port on a Brocade 48000 switch can be in any of the following states:

- Online
- Offline
- Faulty
- Testing
- Unknown

Using this test, administrators can accurately determine how many ports are in a particular state of activity.

Purpose	Reports the number of ports on a Brocade 48000 switch that are in a particular state of activity
Target of the test	A Brocade 48000 switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **PORT** – The port on which the switch is listening 4. **SNMPPORT** – The port at which the switch exposes its SNMP MIB 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">15. ONLY ONLINE PORTS – By default, this flag is set to No . This implies that the test, by default, reports the count of online and offline ports. If you want the test to report the count of online ports alone (and not offline ports), set this flag to Yes. In this case, the test will report only the count of online ports and not offline ports.
16. 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.
17. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.
The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
• The eG manager license should allow the detailed diagnosis capability
• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Brocade 48000 switch being monitored</td></tr>
<tr><td rowspan="5">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Online ports:
The total number of ports that are currently in the online state.</td><td>Number</td><td></td></tr>
<tr><td>Offline ports:
The number of ports that are currently in the offline state.</td><td>Number</td><td>The detailed diagnosis of this measure, if enabled, lists the ports that are in an offline state.</td></tr>
<tr><td>Faulty ports:
The number of ports that are currently faulty.</td><td>Number</td><td>The detailed diagnosis of this measure, if enabled, lists the ports that are in a faulty state.</td></tr>
<tr><td>Ports under testing:
The number of ports that are currently being tested.</td><td>Number</td><td>The detailed diagnosis of this measure, if enabled, lists the ports that are in testing.</td></tr>
<tr><td></td><td>Unknown ports:
The number of ports that are in the unknown state.</td><td>Number</td><td>The detailed diagnosis of this measure, if enabled, lists the ports that are in an unknown state.</td></tr>
</table>

	New online ports: The total number of ports that were online during the last measurement period.	Number	
	New offline ports: The number of ports that were offline during the last measurement period.	Number	The detailed diagnosis of this measure, if enabled, lists the ports that were in an offline state.
	New faulty ports: The number of ports that were faulty during the last measurement period. .	Number	The detailed diagnosis of this measure, if enabled, lists the ports that were in a faulty state.
	New testing ports: The number of ports that were in testing during the last measurement period.	Number	The detailed diagnosis of this measure, if enabled, lists the ports that were in testing.
	New unknown ports: The number of ports that were in the unknown state during the last measurement period.	Number	The detailed diagnosis of this measure, if enabled, lists the ports that were in an unknown state.

11.3.2 Fabric Port Status Test

Using this test, administrators can determine the current status of the ports on a fabric switch. The ports on a Brocade 48000 switch can be in the enabled, disabled, or loop back state. This test looks for the number of ports on the switch that are in each of the listed states.

Purpose	Reports the number of ports on the switch that are in each of the listed states
Target of the test	A Brocade 48000 switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **PORT** – The port on which the switch is listening 4. **SNMPPORT** – The port at which the switch exposes its SNMP MIB 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.
Outputs of the test	One set of results for every state

Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Ports: The total number of ports that are in this state currently.	Number	The detailed diagnosis of this measure, if enabled, reveals the current state of every port on the fabric switch.

11.3.3 FabricSwitchStatus Test

This test reports the status of the Fabric switch that is being monitored.

Purpose	Reports the number of ports on the switch that are in each of the listed states
Target of the test	A Brocade 48000 switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **PORT** – The port on which the switch is listening 4. **SNMPPORT** – The port at which the switch exposes its SNMP MIB 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.		
Outputs of the test	One set of results for Brocade SAN switch monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Switch status: The current status of the switch.	Boolean	This Boolean value will be either 1 or 0. If it reports a value of 1, it implies that the switch is active or in an online state. If it reports a value of 0, it indicates that the switch is in the offline state or inactive mode.

11.3.4 Fabric PortsTraffic Test

This test is used to provide the port traffic statistics for the ports available in the Fabric switch.

Purpose	Provides the port traffic statistics for the ports available in the Fabric switch
Target of the test	A Brocade 48000 switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **PORT** – The port on which the switch is listening 4. **SNMPPORT** – The port at which the switch exposes its SNMP MIB 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

Outputs of the test	One set of results for every Brocade SAN switch monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Data transmitted: Indicates the total count of the number of Fibre Channel data that the port has transmitted in KB/sec.	KB/Sec	
	Data received: Indicates the total count of the number of Fibre Channel data that the port has received in KB/sec.	KB/Sec	
	Error count: Indicates the total number of count of the number of CRC errors detected for frames received.	Number	
	Short data received: Indicates the total number of count of the number of truncated frames that the port has received.	Number	
	Long data received: Indicates the total number of count of the number of received frames that are too long.	Number	
	EOF data received: Indicates the total number of count of the number of received frames that are too long.	Number	
	C3 discards received: Indicates the total number of count of the number of Class 3 frames that the port has discarded.	Number	

11.3.5 Fabric Event Status Test

This test reports the number and type of events that have occurred on the fabric switch of the Brocade SAN switch. This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Brocade SAN Switch* as the **Component type**, *Performance* as the **Test type**, choose the test from the **DISABLED TESTS** list, and click on the **>>** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Purpose	Reports the number and type of events that have occurred on the fabric switch of the Brocade SAN switch.
Target of the test	A Brocade 48000 switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **PORT** – The port on which the switch is listening 4. **SNMPPORT** – The port at which the switch exposes its SNMP MIB 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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**.
17. **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*.
18. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

    The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

    - The eG manager license should allow the detailed diagnosis capability
    - Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Outputs of the test: One set of results for every Brocade SAN switch monitored

Measurements made by the test

Measurement	Measurement Unit	Interpretation
Critical events: The number of critical events that occurred on the fabric switch.	Number	
Error events: The number of errors that occurred on the fabric switch.	Number	

	Warnings: The number of warning events that occurred on the fabric switch.	Number	
	Information events: The number of information events that occurred on the fabric switch.	Number	

	Debug events: The number of debug events that occurred on the fabric switch.	Number	

Chapter 12

Monitoring the Alcatel Switch

Alcatel OmniSwitch 6600 family switches are advanced 10/100 based stackable layer 3 workgroup switches that provide wire rate L2+ switching, L3 routing and advanced services with high availability for IP communications and mission-critical 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 Alcatel switch are monitored 24 x 7.

eG Enterprise provides a specialized *Alcatel Switch* model to keep track of the internal health and external availability of the Alcatel switch.

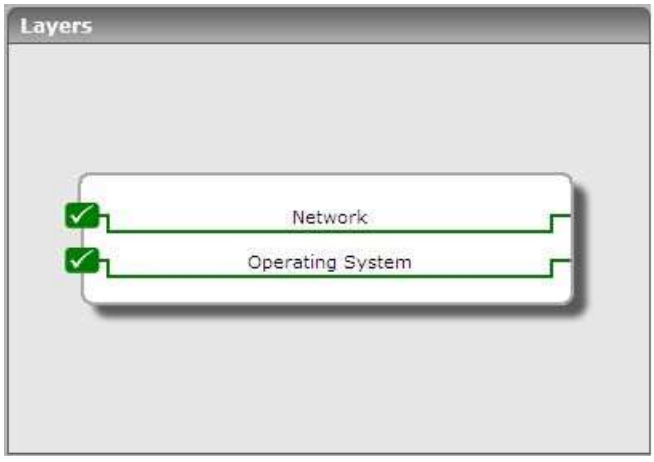

Figure 12.1: Layer model of the Alcatel Switch

This model connects to the SNMP MIB of the switch to collect a wide variety of metrics revealing the following:

- How is the I/O activity on the switch devices? Is it unusually high on any device?
-
- Do the switch devices use CPU and memory optimally, or is any device using these resources

excessively?

- Have the chassis and the chassis management module (CMM) registered unusually high temperatures?
- Are the switch modules using the I/O, CPU, and memory resources available to it effectively? Is any module consuming resources excessively?
- Is any port on the switch unavailable currently?
- Is any port utilizing the CPU, I/O, or memory resources excessively?

The sections to come discuss the layers in the Figure 12.1 in great detail.

12.1 The Operating System Layer

Using the tests associated with this layer, administrators can assess how effectively the switch devices and modules utilize the CPU, memory, and I/O resources available to the switch.

Figure 12.2: The tests associated with the Operating System layer

12.1.1 Alcatel Devices Test

This test reports critical statistics pertaining to the switch device.

Purpose	Critical statistics pertaining to the switch device
Target of the test	An Alcatel switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **PORT** – The port on which the switch is listening 4. **SNMPPORT** – The port at which the switch exposes its SNMP MIB 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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**. 17. **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*.		
Outputs of the test	One set of results for every switch monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Device input utilization: Indicates the device-level input utlization.	Percent	
	Device I/O utilization: Indicates the percentage of I/O used by the device.	Percent	A high value of this measure indicates high I/O activity on the device.
	Device CPU utilization: Indicates the percentage of CPU used up by the device.	Percent	Ideally, this value should be low. A high value is indicative of excessive CPU usage by the device.
	Device memory utilization: Indicates the percentage of memory utilized by the device.	Percent	Ideally, this value should be low. A high value is indicative of excessive memory usage by the device.

	Chassis temperature: Indicates the current chassis temperature.	Deg	A consistent increase in the value of this measure could be a cause for concern.
	CMM CPU temperature: Indicates the current temperature of the chassis management module (CMM) CPU.	Deg	A consistent increase in the value of this measure could be a cause for concern.

12.1.2 Alcatel Modules Test

This test reports the resource usage of each of the modules of the Alcatel switch.

Purpose	Reports the resource usage of each of the modules of the Alcatel switch
Target of the test	An Alcatel switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **PORT** – The port on which the switch is listening 4. **SNMPPORT** – The port at which the switch exposes its SNMP MIB 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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**. 17. **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*.		
Outputs of the test	One set of results for every module on the switch monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Module input utilization: Indicates the input utilization by this module.	Percent	
	Module I/O utilization: Indicates the percentage of I/O used by this module.	Percent	A high value of this measure indicates high I/O activity on the module. Comparing the value of this measure across modules will enable administrators accurately identify that module on which I/O usage is the maximum.
	Module CPU utilization: Indicates the percentage of CPU used up by this module.	Percent	Ideally, this value should be low. A high value is indicative of excessive CPU usage by the module. Comparing the value of this measure across modules will enable administrators accurately identify that module on which CPU usage is unusually high.
	Module memory utilization: Indicates the percentage of memory utilized by this module.	Percent	Ideally, this value should be low. A high value is indicative of excessive memory usage by the module. Comparing the value of this measure across modules will enable administrators accurately identify the module(s) which is consuming memory excessively.

12.2 The Network Layer

The tests mapped to this layer enable administrators to determine the following:

- Whether the switch is available or not
- The current status of the ports on the switch
- The resource usage of the switch ports
- The network traffic to and from the switch
- The bandwidth usage of the network interfaces supported by the switch
- The uptime of the switch

Figure 12.3: The tests associated with the Network layer

Since the **NetworkInterfaces** test, the **Network** test, and **Device Uptime** test have already been discussed in the previous chapters, the section to come will discuss the AlcatelPorts test only.

12.2.1 Alcatel Ports Test

This test reports the status of the ports on the Alcatel switch and their resource usage.

Purpose	Reports the status of the ports on the Alcatel switch and their resource usage
Target of the test	An Alcatel switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **PORT** – The port on which the switch is listening 4. **SNMPPORT** – The port at which the switch exposes its SNMP MIB 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.

17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every port on the switch 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>Is port up?:
Indicates whether this port is up or down currently.</td><td></td><td>The values that this measure can report and their corresponing numeric values have been described in the table below
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Up</td><td>100</td></tr><tr><td>Down</td><td>0</td></tr></table>
Note:

By default, this measure reports one of the Measure Values listed in the table above to indicate the current state of a port. The graph of this measure however, represents the same using the numeric equivalents – 0 and 100.</td></tr>
<tr><td></td><td>Port input utilization:
Indicates the input utilization by the port.</td><td>Percent</td><td></td></tr>
</table>

	Port I/O utilization: Indicates the percentage of I/O used up by this port.	Percent	Ideally, this value should be low. A high value is indicative of excessive I/O activity on the port. Comparing the value of this measure across ports will enable administrators accurately identify that port on which I/O activity peaks.

Chapter 13

Monitoring the Cisco SAN Switch

Cisco MDS 9000 family fabric switches are cost-effective, highly scalable, easy to install, and highly configurable Fibre Channel switches that are ideal for small to medium-sized businesses, along with departmental and remote branch offices needing intelligent storage area networks. With deployment options ranging from stand-alone, top-of-the rack, and blade switches for IBM BladeCenter and HP c-Class BladeSystem, the Cisco MDS 9100 Series Multilayer Fabric Switches provide customers with excellent flexibility, while maintaining consistent feature sets and management capabilities.

All Cisco MDS 9500 Series director switches are based on the same underlying crossbar architecture. Frame forwarding logic is distributed in application-specific integrated circuits (ASICs) on the linecards themselves, resulting in a distributed forwarding architecture. There is never any requirement for frames to be forwarded to the supervisor for centralized forwarding, nor is there ever any requirement for forwarding to drop back into software for processing—all frame forwarding is performed in dedicated forwarding hardware and distributed across all linecards in the system. All advanced features, including virtual SANs (VSANs), VSAN Trunking, Inter-VSAN Routing (IVR) including Fibre Channel Network Address Translation (FC-NAT), Cisco PortChannels (port aggregation), quality of service (QoS), Fibre Channel Congestion Control (FCC), Switch Port Analyzer (SPAN), and Remote Switch Port Analyzer (RSPAN) are implemented within the hardware-based forwarding path and can be enabled without any loss of performance or additional latency. All of these advanced features were built into the Cisco MDS 9000 Family ASICs from the beginning. Second-generation Cisco MDS ASICs augment these capabilities with the addition of class of service (CoS) and port bandwidth reservation capabilities, with more hardware capabilities to be enabled in future Cisco MDS 9000 SAN-OS Software releases.

Forwarding of frames on the Cisco MDS always follows the same processing sequence:

1. Starting with frame error checking on ingress, the frame is tagged with its ingress port and VSAN, enabling the switch to handle duplicate addresses within different fabrics separated by VSANs.
2. Following the frame tagging, input access control lists (ACLs) are used to enforce hard zoning.
3. A lookup is issued to the forwarding and frame routing tables to determine where to switch the frame to and whether to route the frame to a new VSAN and/or rewrite the source/destination of the frame if IVR is being used.
4. If there are multiple equal-cost paths for a given destination device, the switch will choose an egress port based on the load-balancing policy configured for that particular VSAN.
5. If the destination port is congested or busy, the frame will be queued on the ingress linecard for delivery, making use of QoS policy maps to determine the order in which frames are scheduled.
6. When a frame is scheduled for transmission, it is transferred across the crossbar switch fabric to the egress linecard where there is a further output ACL, and the VSAN tag used internal to the switch is stripped from the

front of the frame and the frame is transmitted out the output port.

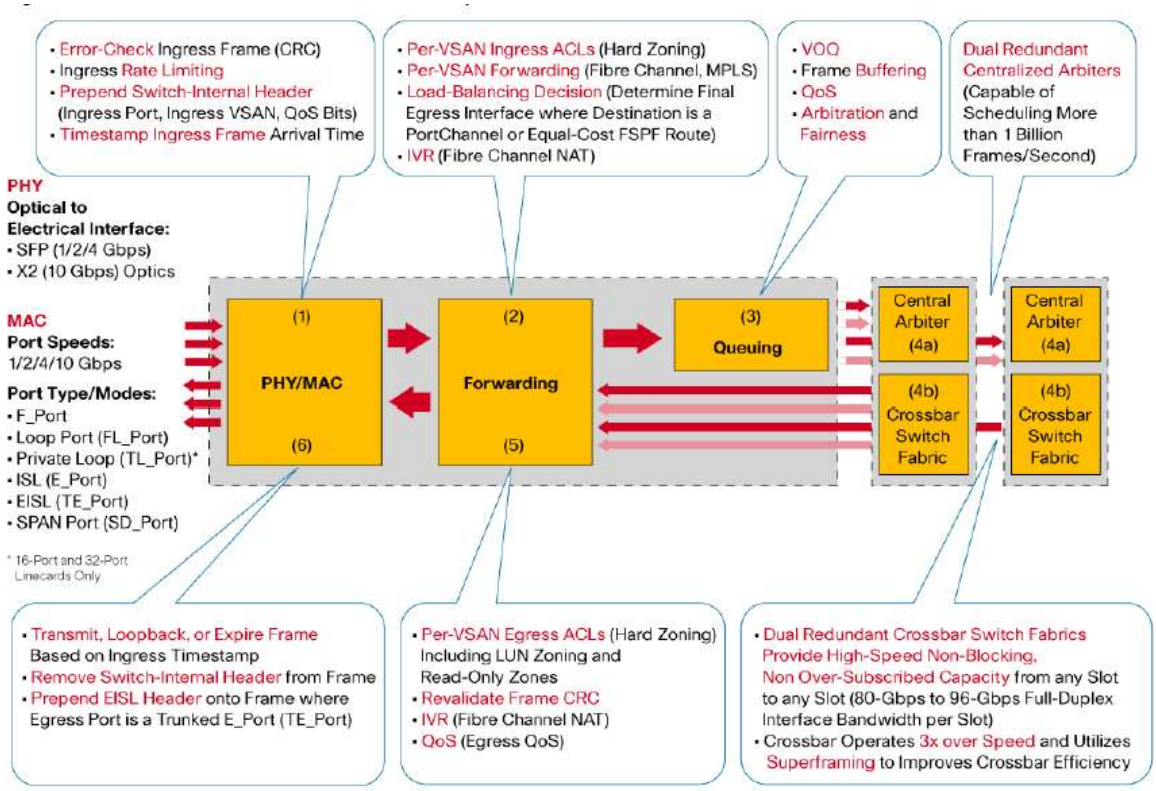

Figure 13.1: Frame flow within Cisco MDS 9000 Family switches

Since the switches serve as the building-blocks for storage networks, glitches in its performance can cause the untimely collapse of your SAN, which in turn might result in significant delays in the delivery of the dependent end-user services and prolonged service outages.

To avoid such adversities, it is imperative that you continuously monitor the Cisco SAN switch. eG Enterprise provides a specialized, 100% web-based *Cisco SAN Switch* model, which periodically verifies the operational status of the switch, captures link failures, and runs health checks on the critical software and hardware components of the switch such as the VSAN, the fan tray, the power supply unit, etc.

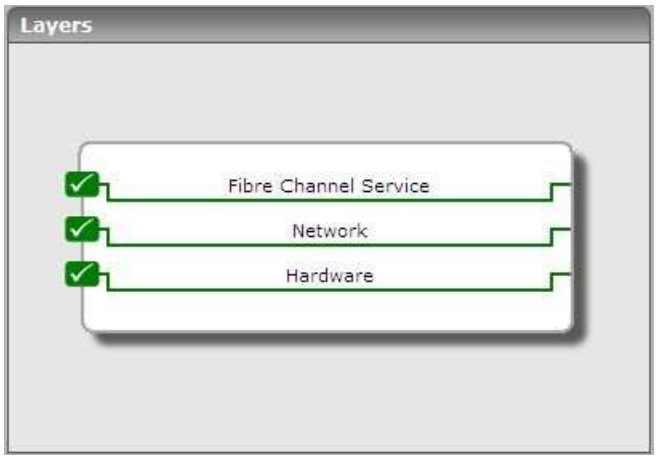

Figure 13.2: The layer model of the Cisco SAN switch

Every layer of Figure 13.2 is mapped to a set of tests that report critical performance statistics pertaining to the switch by connecting to its SNMP MIB. Using these metrics, the following performance queries can be clarified:

- Is the fan tray functioning normally or has experienced a failure? Does the tray have to be replaced?
- Has any power supply unit failed?
- What is the current operational status of the switch port?
- Is any WWN of the port experiencing link failures? If so, which one?

The sections to come discuss the **Hardware**and **Fibre Channel Service** layers only as the **Network** layer is already dealt with in the previous chapters of this document.

13.1 The Hardware Layer

The tests mapped to this layer monitor the health of the core hardware components of the switch – namely, the fan tray, the power supply unit, and the sensors.

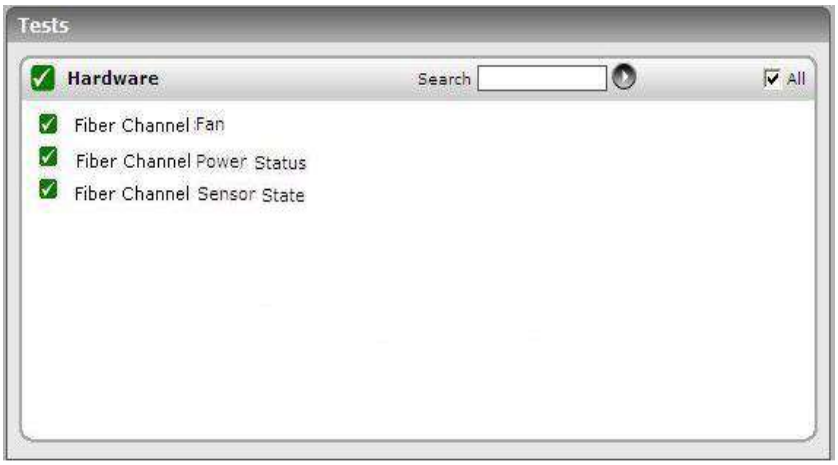

Figure 13.3: The tests mapped to the Hardware layer

13.1.1 Fibre Channel Fans Test

The fan tray, typically mounted by the side of the switch, provides active cooling.

This test reports the current status of the fan tray, based on which administrators would take a call on whether the tray requires a replacement or not.

Purpose	Reports the current status of the fan tray
Target of the test	A Cisco SAN switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **SNMPPORT** – The port at which the 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.

16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every port on the switch 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>Fan tray status:

Indicates the current operational status of the fan tray.</td><td>Number</td><td>This measure can report any of the following values:

• PoweredOn
• PoweredDown
• PartialFailure

The numeric values that correspond to each of the above-mentioned values are as follows:

<table><tr><th>State</th><th>Value</th></tr><tr><td>PoweredOn</td><td>2</td></tr><tr><td>PoweredDown</td><td>3</td></tr><tr><td>PartialFailure</td><td>4</td></tr></table>
Note:

By default, this measure reports one of the States listed in the table above to indicate the status of a fan tray. The graph of this measure however, represents the same using the numeric equivalents – 2 to 4.</td></tr>
</table>

13.1.2 Fibre Channel Power Status Test

This test reports the administrative and operational status of the power supply units of the switch.

Purpose	Reports the administrative and operational status of the power supply units of the switch
Target of the test	A Cisco SAN switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **SNMPPORT** – The port at which the 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.

16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every power supply unit on the switch 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>Admin status:
Indicates the administratively desired FRU power state.</td><td>Number</td><td>This measure can report any value from 1 to 5. The values and the states they represent are discussed hereunder:
1 – On
2 - Off
3 – inlineAuto
4 – inlineOn
5 – PowerCycle</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Operational status:
Indicates the operational FRU power state.</td>
<td></td>
<td>This measure can report any of the following values:

OffEnvOther
On
OffAdmin
OffDenied
OffEnvPower
OffEnvTemp
OffEnvFan
Failed
On but fan failed
Off - Cooling
Off – Connector Rating

The numeric values that correspond to each of the above-mentioned values are as follows:
<table>
<tr><th>State</th><th>Value</th></tr>
<tr><td>OffEnvOther</td><td>1</td></tr>
<tr><td>On</td><td>2</td></tr>
<tr><td>OffAdmin</td><td>3</td></tr>
<tr><td>OffDefined</td><td>4</td></tr>
<tr><td>OffEnvPower</td><td>5</td></tr>
<tr><td>OffEnvTemperature</td><td>6</td></tr>
<tr><td>OffEnvFan</td><td>7</td></tr>
<tr><td>Failed</td><td>8</td></tr>
<tr><td>On but fan failed</td><td>9</td></tr>
<tr><td>Off – Cooling</td><td>10</td></tr>
<tr><td>Off – Connector Rating</td><td>11</td></tr>
</table>
Note:

By default, this measure reports one of the States listed in the table above to indicate the power status. The graph of this measure however, represents the same using the numeric equivalents – 1 to 11.</td>
</tr>
</table>

13.1.3 Fibre Channel Sensor State Test

This test reports the number of sensors in various operational states.

Purpose	Reports the administrative and operational status of the power supply units of the switch
Target of the test	A Cisco SAN switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **SNMPPORT** – The port at which the 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.

16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the switch 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>SensorCount:
Indicates the number of sensors that are available in the available operational status of the sensor.</td><td>Number</td><td>The different operational status of the sensors are as follows:
1 - Ok
2 - Not available
3 - Not operational</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Operational status:
Indicates the operational FRU power state.</td>
<td></td>
<td>This measure can report any of the following values:

OffEnvOther
On
OffAdmin
OffDenied
OffEnvPower
OffEnvTemp
OffEnvFan
Failed
On but fan failed
Off - Cooling
Off – Connector Rating

The numeric values that correspond to each of the above-mentioned values are as follows:
<table>
<tr><th>State</th><th>Value</th></tr>
<tr><td>OffEnvOther</td><td>1</td></tr>
<tr><td>On</td><td>2</td></tr>
<tr><td>OffAdmin</td><td>3</td></tr>
<tr><td>OffDefined</td><td>4</td></tr>
<tr><td>OffEnvPower</td><td>5</td></tr>
<tr><td>OffEnvTemperature</td><td>6</td></tr>
<tr><td>OffEnvFan</td><td>7</td></tr>
<tr><td>Failed</td><td>8</td></tr>
<tr><td>On but fan failed</td><td>9</td></tr>
<tr><td>Off – Cooling</td><td>10</td></tr>
<tr><td>Off – Connector Rating</td><td>11</td></tr>
</table>
Note:

By default, this measure reports one of the States listed in the table above to indicate the power status. The graph of this measure however, represents the same using the numeric equivalents – 1 to 11.</td>
</tr>
</table>

13.2 The Fabric Channel Service Layer

The tests linked to this layer reveal the following:

- The current status and operational mode of the fibre channel switch
- Link failures
- Whether the VSAN is active and can handle traffic or not

Figure 13.4: The tests mapped to the Fibre Channel Service layer

13.2.1 Fibre Channel Details Test

The SAN switch comes bundled with a port security feature that locks down the mapping of an **entity** to a switch port, so that unauthorized devices are denied access to the switch port. The **entity** can be a host, target, or switch and is identified by its World Wide Number (WWN).

This test reports the status and speed statistics related to every WWN of the switch port.

Purpose	Reports the status and speed statistics related to every WWN of the switch port
Target of the test	A Cisco SAN switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **SNMPPORT** – The port at which the 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 target device. 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. **CRITICALERRORCODES** – This test reports a measure named *Operational status*, which indicates the current operational state of every fibre channel port. Typically, the Cisco SAN switch assigns a state code to every port to indicate the operational state of that port – this code is in fact a number between 1 and 131. Of these 131 state codes, a few codes might indicate **Critical** failures, a few could indicate **Major** errors, a few more could denote **Minor** issues, and some may just report general status information.

    To indicate to the eG agent which of the 131 state codes represent **Critical** failures, which ones indicate **Major** errors, and which state codes denote **Minor** issues, the administrator can provide a comma-separated list of codes against the **CRITICALERRORCODES**, **MAJORERRORCODES**, and **MINORERRORCODES** parameters, respectively. For instance, the administrators might consider the codes *3*, *6*, and *7* to be critical, as they represent critical failures such as a *hwfailure*, a *swfailure*, and a *linkfailure*, respectively. Therefore, the **CRITICALERRORCODES** specification in this case will be: *3,6,7*.

    The eG agent on the other hand, internally assigns a number to each of the error code specifications – **3** for **Critical**, **2** for **Major**, **1** for **Minor**, and **0** for **Others**.

    Now, assume that the SNMP MIB of the switch returns the state code *6* for a particular port. In this case, the eG agent first checks whether any of the three test parameters, namely - **CRITICALERRORCODES**, **MAJORERRORCODES**, and **MINORERRORCODES**- are configured with the reported state code – in the case of our example, the **CRITICALERRORCODES** parameter is configured with the state code *6*. Once a match is found, the eG agent automatically reports the value it internally maintains for **Critical** error codes – i.e., the value **3** - as the value of the *Operational status* measure for this port. If a match is not found – i.e., if none of the three parameters mentioned above are configured with the state code representing the current state of the port - then the eG agent automatically reports the value **0** as the value of the *Operational status* measure – this is because, the eG agent automatically assumes that such a state code belongs to the **Others** category.

15. **MAJORERRORCODES** - This test reports a measure named *Operational status*, which indicates the current operational state of every fibre channel port. Typically, the Cisco SAN switch assigns a state code to every port to indicate the operational state of that port – this code is in fact a number between 1 and 131. Of these 131 state codes, a few codes might indicate **Critical** failures, a few could indicate **Major** errors, a few more could denote **Minor** issues, and some may just report general status information.

    To indicate to the eG agent which of the 131 state codes represent **Critical** failures, which ones indicate **Major** errors, and which state codes denote **Minor** issues, the administrator can provide a comma-separated list of codes against the **CRITICALERRORCODES**, **MAJORERRORCODES**, and **MINORERRORCODES** parameters, respectively. For instance, the administrators might consider the codes *11*, 12, and *13* to be major, as they represent major error conditions such as *vsanInactive*, *adminDown*, and *channelAdminDown*, respectively. Therefore, the **MAJORERRORCODES** specification in this case will be: *11,12,13*.

The eG agent on the other hand, internally assigns a number to each of the error code specifications – **3** for **Critical**, **2** for **Major**, **1** for **Minor**, and **0** for **Others**.

Now, assume that the SNMP MIB of the switch returns the state code *13* for a particular port. In this case, the eG agent first checks whether any of the three test parameters, namely - **CRITICALERRORCODES**, **MAJORERRORCODES**, and **MINORERRORCODES**- are configured with the reported state code – in the case of our example, the **MAJORERRORCODES** parameter is configured with the state code *13*. Once a match is found, the eG agent automatically reports the value it internally maintains for **Major** error codes – i.e., the value **2** - as the value of the *Operational status* measure for this port. If a match is not found – i.e., if none of the three parameters mentioned above are configured with the state code representing the current state of a port - then the eG agent automatically reports the value **0** as the value of the *Operational status* measure – this is because, the eG agent automatically assumes that such a state code belongs to the **Others** category.

16. **MINORERRORCODES** – This test reports a measure named *Operational status*, which indicates the current operational state of every fibre channel port. Typically, the Cisco SAN switch assigns a state code to every port to indicate the operational state of that port – this code is in fact a number between 1 and 131. Of these 131 state codes, a few codes might indicate **Critical** failures, a few could indicate **Major** errors, a few more could denote **Minor** issues, and some may just report general status information.

    To indicate to the eG agent which of the 131 state codes represent **Critical** failures, which ones indicate **Major** errors, and which state codes denote **Minor** issues, the administrator can provide a comma-separated list of codes against the **CRITICALERRORCODES**, **MAJORERRORCODES**, and **MINORERRORCODES** parameters, respectively. For instance, the administrators might consider the codes *25*, *29*, and *30* to be minor, as they represent minor error conditions such as a *vsanMismatchIsolation*, *fcotNotPresent*, and *fcotVendorNotSupported*, respectively. Therefore, the **MINORERRORCODES** specification in this case will be: *25,29,30*.

    The eG agent on the other hand, internally assigns a number to each of the error code specifications – **3** for **Critical**, **2** for **Major**, **1** for **Minor**, and **0** for **Others**.

    Now, assume that the SNMP MIB of the switch returns the state code *25* for a particular port. In this case, the eG agent first checks whether any of three test parameters, namely - **CRITICALERRORCODES**, **MAJORERRORCODES**, and **MINORERRORCODES**- are configured with the reported state code – in the case of our example, the **MINORERRORCODES** parameter is configured with the state code *25*. Once a match is found, the eG agent automatically reports the value it internally maintains for **Minor** error codes – i.e., the value *1* - as the value of the *Operational status* measure for this port. If a match is not found – i.e., if none of the three parameters mentioned above are configured with the state code representing the current state of the port - then the eG agent automatically reports the value **0** as the value of the *Operational status* measure – this is because, the eG agent automatically assumes that such a state code belongs to the **Others** category.

	Note: • If you do not want to assign a particular severity to a specific set of error codes, then specify *none* against the corresponding test parameter. For instance, if you do not want to classify any errors as **Minor**, then set the **MINORERRORCODES** parameter to *none*. • If one of the three parameters above – i.e., **CRITICALERRORCODES**, **MAJORERRORCODES**, or **MINORERRORCODES** – is set to *Default*, then it indicates that all those error codes that are not assigned a particular priority will automatically assume this priority. For instance, if the **CRITICALERRORCODES** parameter is set to *3,6,7*, and the **MAJORERRORCODES** parameter is set to *Default*, then, it indicates that all error codes other than 3, 6, and 7 will be automatically assigned the **Major** priority. • At any given point in time, only one of the three parameters can be set to *Default*. • If all three parameters are set to *none*, then the *Operational status* measure will report the value **0**. 17. **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**. 18. **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*. 19. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.
Outputs of the test	One set of results for every WWN of the Fibre Channel Port being monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Admin mode: Indicates the admin mode of this WWN; this is the port mode configured by the user.	Number	If the user configured the port as auto(1), then the port initialization scheme determines the mode of the port. In this case, the user can look at 'fcIfOperMode' to determine the current operating mode of port. If this interface is a Port Channel port, then only auto(1) or ePort(4) is allowed.
	Operational mode: Indicates the current operating mode of this WWN of the fibre channel port.	Number	This object will also be an additional varbind sent in the linkup notification (defined in IF-MIB) in addition to the varbinds defined for this notification.
	Admin speed: Indicates the current port speed configured by the user.	Number	If this interface is a member of a port channel port then this object cannot be modified. Since this is a characteristic of a physical port, this object may not be applicable for some non-physical ports, i.e., the value is instantiated but its value is irrelevant.
	Operational status: Indicates the current operational state of this port.	Number	If the value of this measure is 3, it indicates that the port is currently in a **Critical** state. While the value 2 for this measure indicates a **Major** state, the value 1 indicates a **Minor** state. On the other hand, if the measure reports the value 0, it indicates that the port is not in an erroneous state currently. To know the exact operational state of the port, use the detailed diagnosis of this measure.

13.2.2 Fibre Channel Link Failures Test

This test sheds light on link failures that might have been experienced by one/more WWNs of the Fibre Channel port.

Purpose	Sheds light on link failures that might have been experienced by one/more WWNs of the Fibre Channel port
Target of the test	A Cisco SAN switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **SNMPPORT** – The port at which the 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 target device. 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 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**. 16. **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*.
Outputs of the test	One set of results for every WWN of the Fibre Channel Port being monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Link failures: Indicates the number of link failures currently experienced by this port.	Number	Ideally, this value should be 0.

13.2.3 Fibre Channel VSan Test

A virtual storage area network (VSAN) is a collection of ports from a set of connected Fibre Channel switches, that form a virtual fabric. This test reports the current configurable and operational status of the VSANs.

Purpose	Reports the current configurable and operational status of the VSANs
Target of the test	A Cisco SAN switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **SNMPPORT** – The port at which the 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 target device. 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 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**.

16. **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*.

Outputs of the test: One set of results for every VSAN on the switch being monitored

Measurements made by the test

Measurement	Measurement Unit	Interpretation
Admin mode: Represents the configurable state of this VSAN.		If this measure returns the value *Up*, it indicates that this VSAN is configured and the services are activated. The value *Down* for this measure, on the other hand, indicates that the VSAN is configured, but the services are deactivated. The numeric values that correspond to each of the above-mentioned Up/down values are as follows: **State** / **Value** Up / 1 Down / 0 **Note:** By default, this measure reports one of the **States** listed above. The graph of this measure however, represents the configurable state of a VSAN using the numeric equivalents - *1 or 2*.

<table>
<tr>
<td></td>
<td>Operational mode:
Indicates the operational state of the VSAN - i.e., whether traffic can pass through this VSAN or not.</td>
<td></td>
<td>If this measure returns the value Up, it indicates that this VSAN is up and running and will allow traffic to pass through it. The value Down for this measure, on the other hand, indicates that the VSAN is down.

The numeric values that correspond to each of the above-mentioned Up/down values are as follows:
<table><tr><th>State</th><th>Value</th></tr><tr><td>Up</td><td>1</td></tr><tr><td>Down</td><td>0</td></tr></table>
Note:
By default, this measure reports one of the States listed above. The graph of this measure however, represents the operational state of a VSAN using the numeric equivalents - 1 or 2.</td>
</tr>
</table>

Chapter 14

Monitoring the Cisco CSS

The Cisco CSS 11150 content services switch is a compact, high-performance solution for small-to medium-sized Web sites. Featuring Cisco Web Network Services (Web NS) software, the Cisco CSS 11150 enables Web and application service providers, Web content providers, and enterprises engaged in e-commerce to build global Web Networks optimized for e-commerce transactions and Web content delivery. With its patented content switching technology, the Cisco CSS 11150 gives businesses maximum control in ensuring availability of their Web sites, securing Web site resources without compromising performance, and allocating Web site resources efficiently.

Cisco CSS 11000 series switches learn where specific content resides, either locally or remotely, and dynamically select the best Web server or cache for specific content requests. In a distributed Web site, Cisco CSS 11000 series switches perform comprehensive resource verification before routing user requests, ensuring they are directed to the location that has the best response time and the least load for the requested content. Local server selection is based on server load and application response time, as well as traditional least connections and round-robin algorithms. Global server load balancing is based on Domain Name System (DNS) and proximity by source IP address. Any application that uses standard Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) protocols can also be load-balanced including firewalls, mail, news, chat, and lightweight directory access protocol (LDAP), Simple Network Management Protocol (SNMP), remote monitoring (RMON), and log files.

Glitches in the Cisco CSS' operations can therefore cause serious errors in the load-balancing activity, resulting in requests being routed to slow / heavily loaded locations, and frustrating error messages such as "Server Not Found" becoming common-place! While such aberrations are unwelcome even in less critical environments, the occurrence of these anomalies in mission-critical infrastructures can significantly impact the quality and timely delivery of the important end-user services that overlay these infrastructures. To avoid prolonged service delays or outages, the continuous monitoring of the Cisco CSS is essential.

eG Enterprise provides a specialized *Cisco CSS* monitoring model that monitors the sessions to and services offered by the Cisco CSS, and promptly alerts administrators to deviations (if any) in performance.

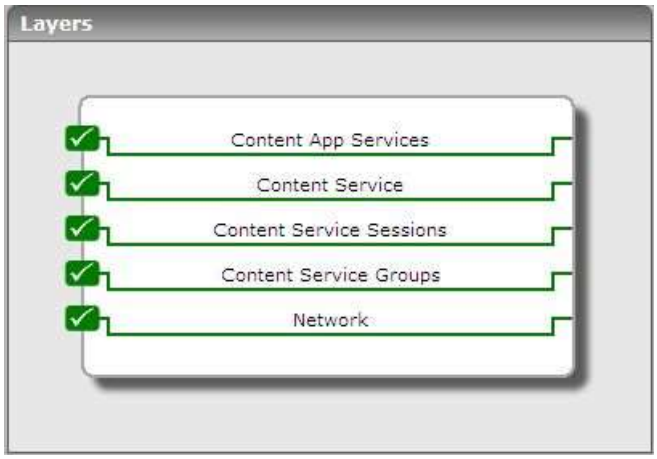

Figure 14.1: The layer model of the Cisco CSS

Every layer of Figure 14.1 is mapped to a wide variety of tests that connect to the SNMP MIB of the Cisco CSS to report useful statistics related to the health of the CSS. Using these metrics, the following questions can be easily answered:

- How many groups have been configured on CSS? Which destination services are associated with each group? What is the current state of each group service? How frequently was the group service accessed?
- Are any groups in a disabled state currently? How many users are currently connected to the enabled groups?
- Is the Cisco CSS overloaded with sessions? Which application IP has generated the maximum session activity on the CSS?
- Which owner frequently accessed the CSS?
- What are the services associated with each owner? How many of these services are currently alive?
- How many services have been configured on the CSS totally? What are they? Are any of these services dying currently? Which service has generated the maximum network traffic?
- Are the services able to process content requests well?
- What are the content rules configured on CSS? What is the current status of each content rule?
- What are the IP interfaces on CSS? Are any of them disabled or waiting for a circuit?
- How many VLAN circuits are configured on CSS?
- Has enough pool memory been allocated to the IP routing table?
- Is the CSS in a redundant state currently? What is the current state of the redundant link? Will the CSS be going into a failover soon?

The sections to come will discuss the top 4 layers of Figure 14.1 only, as the **Network** layer has already been dealt with elaborately in the previous chapters of this document.

14.1 The Content Service Groups Layer

A **Group** represents a collection of local servers that are to be load-balanced. A **service** is a destination location where a piece of content resides physically (a local or remote server and port). Using the tests attached to the **Content Service Groups** layer, you can do the following:

- Determine the current status of the server groups configured on the Cisco CSS;
- Analyze the load on the server groups being load balanced by Cisco CSS;
- Know the current status of each of the services configured for a group;
- Understand how frequently requests were directed to each of the services.

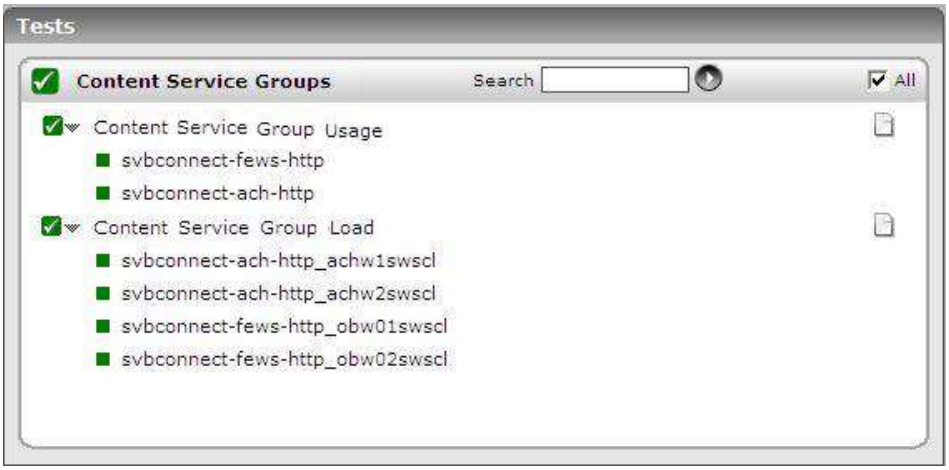

Figure 14.2: The tests mapped to the Content Service Groups layer

14.1.1 Content Service Group Load Test

As stated earlier, a **service** is a destination location where a piece of content resides physically (a local or remote server and port). While load-balancing content requests to a server group, the Cisco CSS identifies the location from which the requested content is to be provided using the service definitions on that group. The ContentServiceGroupLoad test reports the current status of the destination services configured for every group, and helps analyze the extent of usage of the service definitions by reporting the number of times each destination service was accessed for content by the Cisco CSS.

Purpose	Reports the current status of the destination services and helps analyze the extent of usage of the service definitions by reporting the number of times each destination service was accessed for content by the Cisco CSS
Target of the test	A Cisco CSS
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco CSS 3. **SNMPPORT** – The port at which the CSS 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 target device. 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 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**. 16. **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*.		
Outputs of the test	One set of results for every *groupname_destination service* pair discovered by the Cisco CSS		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Group service status: Indicates the current status of this destination service	Boolean	
	Group service hits: Indicates the number of times since the last measurement period, user requests to this group load balanced to this service.	Number	This is a good indicator of the usage of the destination service.
	Group service data sent: Indicates the number of bytes in transmission, which were source NATted using this destination service on this group, during this measurement period.	Bytes	This is a good indicator of the level of traffic handled by the destination service.

14.1.2 Content Service Group Usage Test

A **group**, as already explained, represents a collection of local servers that are to be load-balanced. This test auto-discovers the groups configured on CSS, and reports the status and usage of every group in terms of connections handled by the group and data sent by it.

Purpose	Auto-discovers the groups configured on CSS, and reports the status and usage of every group in terms of connections handled by the group and data sent by it
Target of the test	A Cisco CSS
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco CSS 3. **SNMPPORT** – The port at which the CSS 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 target device. 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 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**. 16. **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*.		
Outputs of the test	One set of results for every group load-balanced by the target Cisco CSS		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Group status: Indicates the current status of this group.	Number	While the value 0 for this measure indicates that the group is currently disabled, the value 1 indicates that the group is enabled.
	No of group data sent: Indicates the number of bytes of group data sent since the last measurement period.	Number	
	No of current group connections: Indicates the number of connections established through this group, currently.	Number	
	No of total group connections: Indicates the total number of connections for this group during this measurement period.	Number	

14.2 Content Service Sessions

The tests mapped to this layer enable you to keep track of the load on the Cisco CSS by periodically monitoring the sessions and user activity on the device.

Figure 14.3: The tests mapped to the Content Service Sessions layer

14.2.1 Content Session Load Test

For every application that connects to the Cisco CSS for processing its load-balancing requests, this test reports the load generated on the Cisco CSS and the current state of the session initiated by the application.

Purpose	For every application that connects to the Cisco CSS for processing its load-balancing requests, this test reports the load generated on the Cisco CSS and the current state of the session initiated by the application
Target of the test	A Cisco CSS
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco CSS 3. **SNMPPORT** – The port at which the CSS 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.

16. 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.

17. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.

The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
• The eG manager license should allow the detailed diagnosis capability
• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every Application IP address served by the target Cisco CSS</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>Application packets received:
Indicates the number of application packets received by the CSS from this application IP, since the last measurement period.</td><td>Number</td><td>These measures are good indicators of the load generated by this application on the Cisco CSS. In the event of a slow-down of the Cisco CSS, you might want to compare the values of these measures across all application Ips to accurately identify the application that coud have overloaded the CSS.</td></tr>
</table>

	Application packets transmitted: Indicates the number of application packets sent by the CSS to this application IP since the last measurement period.	Number	
	Current session state: Indicates the current state of the session initiated by this application.	Number	A session can be in any one of the following states: • 0 – stopped • 1 – Init • 2 – Opened • 3 – Auth • 4 – Up • 5 –Down. • The detailed diagnosis of this measure, if enabled, reveals more details about the session.

The detailed diagnosis of the *Current session state* measure, if enabled, reveals more details about the session such as, the authentication type of the session, the encryption type of the session, and whether Rcmd is enabled/disabled for the session.

Figure 14.4: The detailed diagnosis of the Current session state measure

14.2.2 Content User Load Test

This test monitors the owner activity on the Cisco CSS. An owner is generally the person or company who contracts the Web hosting service to host their Web content and allocate bandwidth as required. Rules are configured on the Cisco CSS for every owner indicating which content accessible by the owner and from where it is to be retrieved.

Purpose	Monitors the owner activity on the Cisco CSS
Target of the test	A Cisco CSS

Agent deploying the test	An external agent
Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco CSS 3. **SNMPPORT** – The port at which the CSS 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.

16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every owner configured on the Cisco CSS</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>Load balancer hits:
Indicates the number of times during this measurement period the owner accessed the load balancer with requests for content.</td><td>Number</td><td>This is a good indicator of the load generated by this owner on the Cisco CSS.</td></tr>
<tr><td>HTTP redirects sent:
Indicates the number of HTTP redirects sent for this owner during this measurement period.</td><td>Number</td><td>HTTP redirects have long been an option to maintain server stickiness in load-balanced environments. Redirects are very reliable and ensure that an Internet/Intranet client stays on a specific server for the duration of a session. The CSS 11000 allows a network administrator to have the CSS 11000 send the HTTP redirect, which eliminates the need for the Web server administrator to redesign a Web site to accommodate HTTP redirects.</td></tr>
</table>

	Load balancer drops: Indicates the total number of requests from this owner that were dropped by the load balancer during this measurement period.	Number	Ideally, this value should be low.
	Data sent: Indicates the total number of bytes sent for this owner during this measurement period.	Bytes	

14.3 The Content Service Layer

The tests associated with the **Content Service** layer and the measures reported by them provide in-depth insights into the status, load, usage, and overall effectiveness of the destination services configured on a Cisco CSS, and the content rules within which the the services are configured.

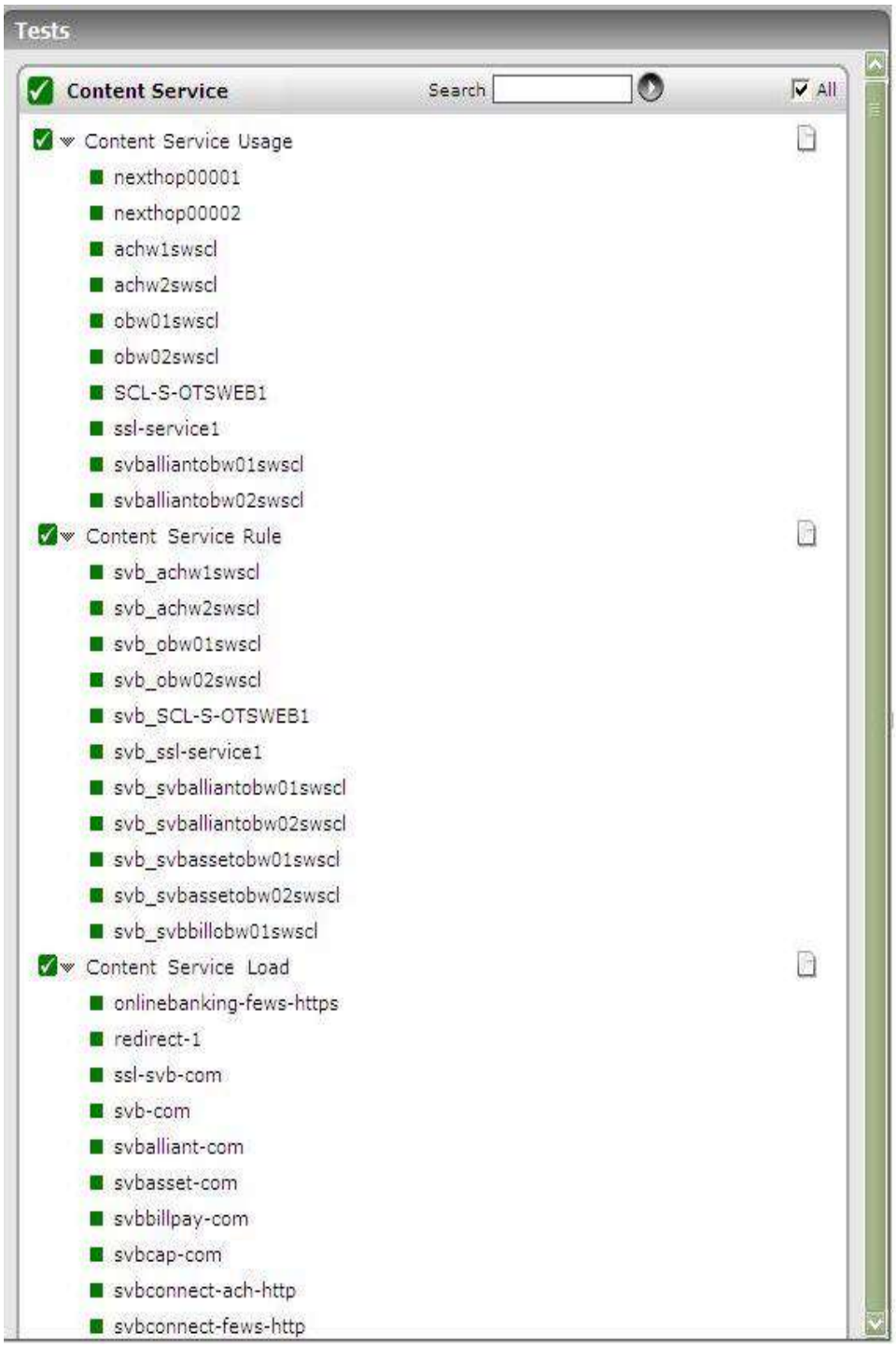

Figure 14.5: The tests mapped to the Content Service layer

14.3.1 Content Service Usage Test

This test reports critical statistics indicating the current status and extent of usage of the content providing services on a Cisco CSS. As already mentioned, a **service** is a destination location where a piece of content resides physically (a local or remote server and port).

Purpose	Reports critical statistics indicating the current status and extent of usage of the content providing services on a Cisco CSS
Target of the test	A Cisco CSS
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco CSS 3. **SNMPPORT** – The port at which the CSS 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every service configured on the Cisco CSS</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Service state:
Indicates the current state of this service.</td><td>Number</td><td>The value of this measure can be any one of the following:
• 1 – Suspended
• 2 – Down
• 4 - Alive
• 5 – Dying</td></tr>
<tr><td>Service enabled:
Indicates whether this service is currently enabled or not.</td><td>Boolean</td><td>The value 0 for this measure indicates that the service is disabled. The value 1 on the other hand implies that the service is enabled.</td></tr>
<tr><td>Service avg min bandwidth:
Indicates the average minimum data sent through this service.</td><td>Bytes</td><td></td></tr>
<tr><td></td><td>Service total bandwidth:
Indicates the total data sent through this service.</td><td>Bytes</td><td>This measure is a good indicator of the network traffic generated through this service.</td></tr>
</table>

	Max service connections: Indicates the maximum number of connections permissible to this service.	Number	
	Total service connections: Indicates the total number of connections to this service during this measurement period.	Number	Ideally, this value should be less than the *Max service connections* measure.
	Average service load: Indicates the number of content requests serviced by this service during this measurement period.	Number	This is a good indicator of the workload and content processing ability of the service.
	Service status: Indicates the current status of this service.	Number	The value of this measure can be any one of the following: • 1 – Suspended • 2 – Down • 4 - Alive • 5 – Dying

14.3.2 Content Service Test

A content rule is a hierarchical rule set containing individual rules that describe which content (for example, .html files) is accessible by visitors to the Web site, how the content is mirrored, on which server the content resides, and how the CSS should process requests for the content. Each rule set must have an owner.

The CSS uses content rules to determine:

- Where the content physically resides, whether local or remote
- Where to direct the request for content (which service or services)
- Which load balancing method to use

Owners can have multiple content rules. For each service discovered from the content rules associated with an owner, this test reports the current status of the service and whether the service has been effectively utilized or not.

Purpose	For each service discovered from the content rules associated with an owner, this test reports the current status of the service and whether the service has been effectively utilized or not
Target of the	A Cisco CSS

test	
Agent deploying the test	An external agent
Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco CSS 3. **SNMPPORT** – The port at which the CSS 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every owner_service pair discovered from the content rules configured on the Cisco CSS</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>No of Content service hits:
Indicates the number of times during this measurement period requests from this owner were served by this service.</td><td>Number</td><td>• This measure is a good indicator of the effectiveness of the service.</td></tr>
<tr><td>Content service data sent:
Indicates the amount of data sent through this service for this owner during this measurement period.</td><td>Bytes</td><td>This measure is a good indicator of the network traffic generated through this service.</td></tr>
<tr><td></td><td>Content service status:
Indicates the current status of this service</td><td>Number</td><td></td></tr>
</table>

	Content service state: Indicates the current state of this service.	Number	The value of this measure can be any one of the following: • 1 – suspended • 2 - up • 4 - alive

14.3.3 Content Rule Test

A content rule is a hierarchical rule set containing individual rules that describe which content (for example, .html files) is accessible by visitors to the Web site, how the content is mirrored, on which server the content resides, and how the CSS should process requests for the content. Each rule set must have an owner.

The CSS uses content rules to determine:

- Where the content physically resides, whether local or remote
- Where to direct the request for content (which service or services)
- Which load balancing method to use

This test auto-discovers the content rules configured on a CSS, and reports the current status and usage patterns pertaining to every content rule.

Purpose	Auto-discovers the content rules configured on a CSS, and reports the current status and usage patterns pertaining to every content rule
Target of the test	A Cisco CSS
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco CSS 3. **SNMPPORT** – The port at which the CSS 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every content rule discovered on the Cisco CSS</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Content status:
Indicates the current status of this content rule.</td><td>Number</td><td>• If the value of this measure is , it indicates that the content rule is enabled. The value 0 on the other hand indicates that the content rule is disabled.</td></tr>
<tr><td>Content hits count:
Indicates the number of user requests during this measurement period that invoked this content rule.</td><td>Bytes</td><td>Ideally, the value of this measure should be high.</td></tr>
<tr><td>Content drops count:
Indicates the number of times the content rule was not able to establish a connection during this measurement period.</td><td>Number</td><td>Ideally, this value should be low.</td></tr>
</table>

	Content byte count: Indicates the number of bytes of data that passed through this content rule during this measurement period.	Number	•

14.4 The Content App Services Layer

A circuit on the CSS is a logical entity that maps IP interfaces to a logical port or group of logical ports, for example, a VLAN. Each VLAN circuit requires an IP address. Assigning an IP address to each VLAN circuit allows the CSS to route Ethernet interfaces (ports) from VLAN to VLAN.

The tests mapped to the **Content App Services** layer reports key statistics related to the performance of the circuits and IP interfaces configured on CSS.

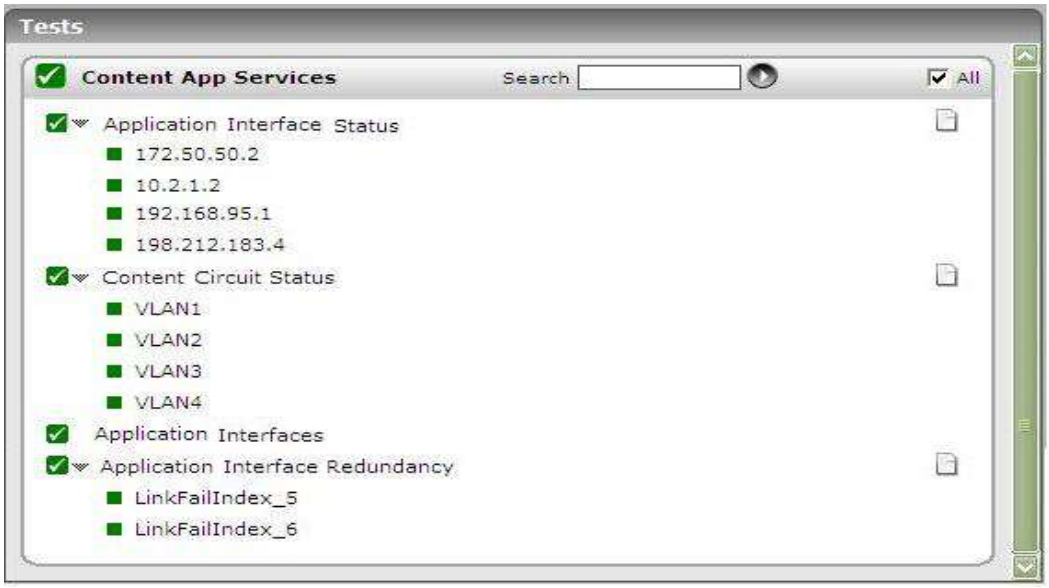

Figure 14.6: The tests mapped to the Content App Services layer

14.4.1 Application Interface Status Test

This test reports the current status of each IP interface on CSS.

Purpose	Reports the current status of each IP interface on CSS
Target of the test	A Cisco CSS
Agent deploying the	An external agent

test	
Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco CSS 3. **SNMPPORT** – The port at which the CSS 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 target device. 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.

<table>
<tr><td></td><td colspan="3">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 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.
16. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every IP interface on CSS</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>Interface state:
Indicates the current state of this interface.</td><td>Number</td><td>• The value that this measure can report and the states they represent are discussed below:
• 1 – Active
• 2 – Disabled
• 3 – Nocircuit; this implies that the interface is waiting for an underlying circuit.
•</td></tr>
<tr><td>Interface redirects enabled:
Indicates whether redirects are enabled or not for this interface.</td><td>Boolean</td><td>The value of this measure indicates whether or not the interface enables the transmission of ICMP packets.
If the transmission is enabled, then the value of this measure will be 1. If not, then this measure will return the value 2.</td></tr>
<tr><td></td><td>Interface status:
Indicates the current status of this interface.</td><td>Number</td><td></td></tr>
</table>

14.4.2 Content Circuit Status Test

This test reports the current status of each VLAN circuit configured on CSS.

Purpose	Reports the current status of each VLAN circuit configured on CSS
Target of the test	A Cisco CSS
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco CSS 3. **SNMPPORT** – The port at which the CSS 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 target device. 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. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0. 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**. 17. **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*.		
Outputs of the test	One set of results for every VLAN circuit configured on CSS		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**Interface type:** Indicates the type of interface associated with this circuit.	Number	• The values that this measure can take and the types they denote are available below: • 6 - Ethernet • 18 - ds1 • 22 – console • 23 - ppp • 30 - ds3 • 32 - frameRelay • 81 - ds0 • 82 - ds0Bundle • 108 - pppMultilink • 117 - ge (Gigabit Ethernet Interface) • 1000 – tunnel and • 1001 - Vlan • The detailed diagnosis of this measure provides additional details about this circuit.
	Logical link count: Indicates the total number of logical links configured for this circuit.	Number	

The detailed diagnosis of the *Interface type* measure indicates what the value of the measure stands for, and also indicates the current state of the circuit.

Figure 14.7: The detailed diagnosis of the *Interface type* measure

14.4.3 Application Interfaces Test

The CSS forwards VLAN circuit traffic to the IP interface. The IP interface passes the traffic to the IP forwarding function where the CSS compares the destination of each packet to information contained in the routing table. The routing table typically contains the output interface and the next-hop address. Once the CSS resolves the packet addresses, it forwards the packet to the appropriate VLAN and destination port.

This test reports useful statistics related to the VLAN-VLAN communication that CSS enables via the IP interfaces configured on it.

Purpose	Reports useful statistics related to the VLAN-VLAN communication that CSS enables via the IP interfaces configured on it
Target of the test	A Cisco CSS
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco CSS 3. **SNMPPORT** – The port at which the CSS 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 target device. 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 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**. 16. **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*.		
Outputs of the test	One set of results for the CSS monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	No of reachable routes: Indicates the current number of reachable routes.	Number	•
	Total no of reachable routes: Indicates the total number of reachable routes during this measurement period.	Number	
	No of reachable hosts: Indicates the number of hosts that are currently reachable.	Number	
	Total no of reachable hosts: Indicates the total number of reachable hosts during this measurement period.	Number	

	Pool memory: Indicates the total amount of memory in bytes allocated for the IP routing table.	Bytes	When there are no additional free entries in the memory pool, more memory is allocated to the pool.
	Redundant state: Indicates the current redundancy state of the monitored CSS.	Number	If this measure reports the value 1, it indicates the 'Init' state. The value 2 on the other hand, indicates the 'Backup' state.
	Total alive uplinks: Indicates the number of alive uplinks during this measurement period.	Number	Within a redundant configuration, CSS allows you to create one/more uplink services with a router's IP address. An uplink service enables the master CSS to monitor the router with a keepalive (ICMP). If the keepalive fails, the master relinquishes control and the backup CSS takes control. The master CSS uses all redundancy uplinks when making the failover decision. If the value of this measure is 0, it indicates that there are no live uplink services. In such a case, the CSS goes into failover.

14.4.4 Application Interface Redundancy Test

CSSs participate in a redundant configuration when a physical redundancy link has been defined between the CSSs. The CSSs use this link to maintain contact and activity status with one another. If the physical link goes down, the master CSS fails over to the backup CSS.

This test monitors the status of the redundancy links configured on a CSS.

Purpose	Monitors the status of the redundancy links configured on a CSS
Target of the test	A Cisco CSS
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco CSS 3. **SNMPPORT** – The port at which the CSS 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 target device. 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 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**. 16. **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*.		
Outputs of the test	One set of results for every redundancy link on the CSS monitored		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**Redundant link status:** Indicates the current status of this redundant link.	Boolean	• While the value 1 indicates that the link is up, the value 0 indicates that it is down. There are two main conditions detected on this redundancy link that drive master and backup states on the CSSs: • The first condition is maintaining the heartbeat, which is an advertisement every second. The master CSS provides this heartbeat on the redundancy link, and the backup CSS keeps track of the heartbeat every three seconds (default). If the heartbeat times out (for example, heartbeats are not detected in this period), then link goes down and the backup takes over as master. • The second condition is that of a VRRP switch priority change. The CSS advertising the highest priority is negotiated to become master. This is the mechanism used by the uplink services, and some of the special commands (described below) for initiating a failover event.

Chapter 15

Monitoring the Coyote Point Equalizer

Coyote Point Equalizer load balancers are a cost-effective appliance-based solution for managing the scalability, availability and performance requirements of any network infrastructure. By effectively managing Internet traffic, the Equalizer product line maximizes network potential by minimizing response times and ensuring site availability.

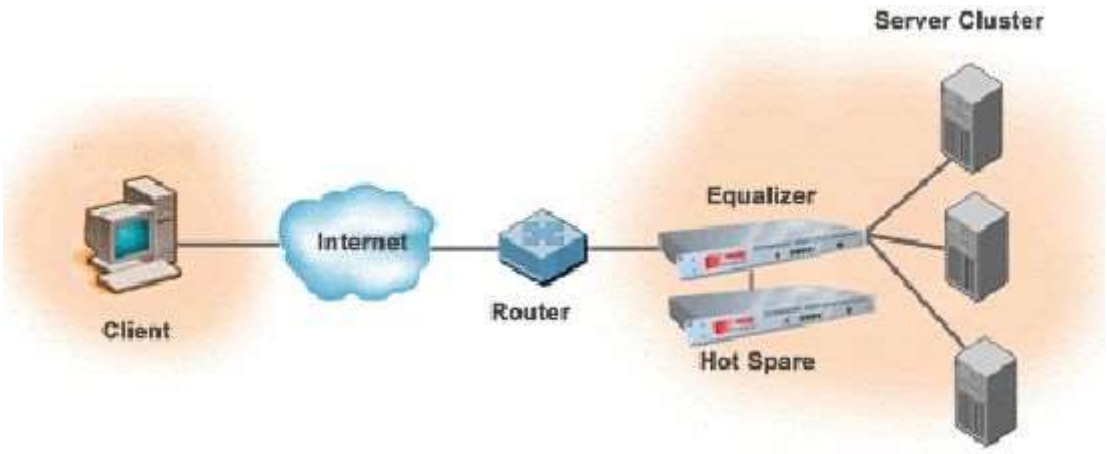

Figure 15.1: Typical deployment architecture of the Equalizer

As a gateway appliance, Coyote Point load balancers are typically deployed in a redundant configuration that includes a hot backup. Client requests are routed through the Equalizer to the appropriate server based on rules set by the administrator.

Since these load balancers are platform and (internet) protocol-independent, they are common-place in mission-critical business environments where maximum performance and high availability are key. Performance issues experienced by the equalizer can therefore adversely impact the availability of the critical services delivered by such environments, disrupting business and causing considerable revenue loss in the process. By continuously monitoring the operations and overall performance of the equalizer, such unpleasant eventualities can be avoided.

eG Enterprise offers a specialized *Coyote Point Equalizer* (see Figure 15.2) monitoring model, which involves a single eG external agent that periodically polls the SNMP MIB of the equalizer, and collects a wide variety of performance information revealing the load on the device and the effectiveness with which the device balances this load across the servers in a farm. In the event of inconsistencies in load balancing, the agent proactively alerts administrators to the potential problem, so that he/she can initiate the relevant remedial action immediately.

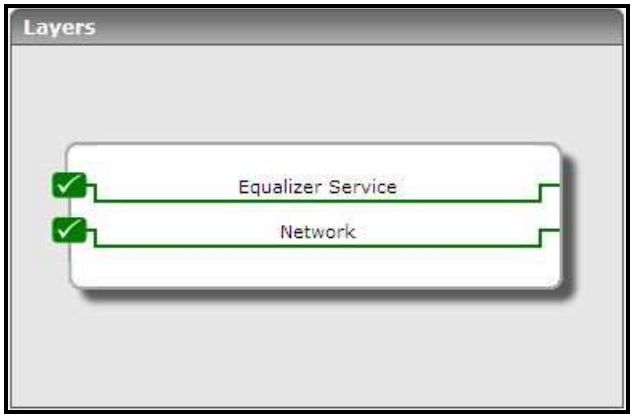

Figure 15.2: The layer model of the Coyote Point Equalizer

Each layer of Figure 15.2 above is mapped to tests that report the following:

- How many clusters are being managed by the equalizer and what are they? Is any cluster overloaded currently? If so, which one is it?
- Which cluster is currently handling the maximum number of connections?
- Which cluster is the busiest in terms of hits to its servers?
- How is the connection load on the equalizer? Is the equalizer able to handle the load?
- Which type of connections is the highest on the equalizer - Level-4 or Level-7?
- Did any connection to the equalizer time out?
- Is the equalizer evenly distributing load across all the servers in the cluster, or is any server currently overloaded?
- Is the equalizer able to assure requests of quick responses from the servers, or is any server in the cluster responding slowly to client requests? Is it owing to a badly tuned equalizer?
- Are client connections to a cluster uniformly distributed across all the servers in that cluster? If not, what is the reason for the imbalance?
- Is any server in the cluster idle?

The sections that will follow will discuss each layer in great detail.

15.1.1 The Network Layer

The tests mapped to the **Network** layer reveal the following:

- The availability of the equalizer and its responsiveness to requests
- The quality of network connections to the equalizer;
- The speed and bandwidth used by each of the network interfaces supported by the equalizer.

Figure 15.3: The tests mapped to the Network layer

Since all the tests displayed in Figure 15.3 have been dealt with extensively in the previous chapters, let us proceed to the next layer.

15.1.2 The Equalizer Service Layer

Using the tests mapped to this layer, you can determine the following:

- The number and type of connections handled by the equalizer;
- The current load on the servers in the cluster and the server responsiveness;
- The load on the clusters managed by the equalizer, and the throughput of each cluster.

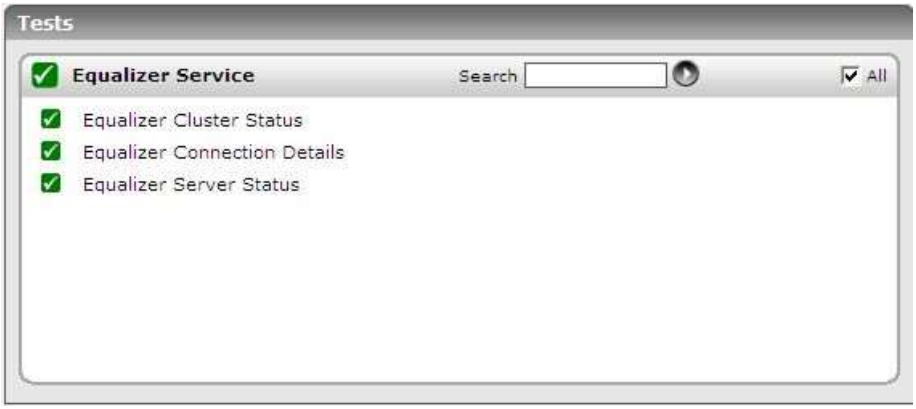

Figure 15.4: The tests mapped to the Equalizer Service layer

15.1.2.1 Equalizer Cluster Status Test

The Equalizer typically manages traffic to a group of servers in a server farm. While the servers in a farm can still be individually accessed, all traffic to the servers will be directed to a separate IP address, called a Virtual Cluster. The Virtual Cluster will accept traffic and distribute it to the available servers.

An Equalizer can be configured to manage multiple server farms/clusters. To be able to accurately assess the workload of the equalizer, you need to have a fair idea of the connection and data load on each of the clusters it manages. The Equalizer Cluster Status test enables you to ascertain the same. For each cluster, this test reports the

current load on the cluster and indicates how busy the servers in the cluster are.

Purpose	Reports the current load on the cluster and indicates how busy the servers in the cluster are
Target of the test	A Coyote Point Equalizer
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the equalizer 3. **PORT** – The port at which the equalizer listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the equalizer exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the each cluster managed by the target equalizer</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Cluster load:
Indicates the calculated load value for this cluster.</td><td>Number</td><td>• This serves as a good indicator of the cluster workload. Comparing the value of this measure across clusters will enable you to identify those clusters that are overloaded.</td></tr>
<tr><td>Current connections:
Indicates the number of connections currently active on this cluster.</td><td>Number</td><td>This again serves as a good indicator of the cluster workload.</td></tr>
<tr><td>Total connections:
Indicates the total number of connections handled by this cluster.</td><td>Number</td><td></td></tr>
<tr><td></td><td>Throughput:
Indicates the rate of data traffic handled by this cluster over the last second.</td><td>MB/Sec</td><td></td></tr>
</table>

	Hit rate: Indicates the rate at which servers in this cluster were accessed for performing transactions.	Mbps	Comparing the value of this measure across clusters will enable you to quickly spot the busiest clusters.

15.1.2.2 Equalizer Connection Details Test

This test not only reports the connection load on the equalizer in numbers, but also points to the nature of the workload by revealing the type of connections handled by the equalizer – this way, administrators can evaluate the workload of the device better. In addition, the test also turns the spotlight on inactive/idle connections, so that administrators can make sure that such connections are kept at a bare minimum.

Purpose	Reports the connection load on the equalizer
Target of the test	A Coyote Point Equalizer
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the equalizer 3. **PORT** – The port at which the equalizer listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the equalizer exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.

17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the equalizer being 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>Level4 total connections:

Indicates the number of L4 connections currently processed by the equalizer.</td><td>Number</td><td>• This serves as a good indicator of the Level-4 connection load on the equalizer.

• Level-4 load balancing is to distribute requests to the servers at transport layer, such as TCP, UDP and SCTP transport protocol. The load balancer distributes network connections from clients who know a single IP address for a service, to a set of servers that actually perform the work. Since connection must be established between client and server in connection-oriented transport before sending the request content, the load balancer usually selects a server without looking at the content of the request.</td></tr>
</table>

	Level4 peak connections: Indicates the high watermark of L4 connections processed by the equalizer.	Number	
	Level4 idle timeout count: Indicates the number of L4 connections that timed out currently, because they were unused for a long time.	Number	Ideally, the value of this measure should be 0. A sudden/steady increase in this value could be a cause for concern.

	Level7 active connections: Indicates the number of L7 connections currently active on the equalizer.	Number	Both these measures serve as effective pointers to the L7 connection workload on the equalizer. Layer-7 load balancing, also known as application-level load balancing, is to parse requests in application layer and distribute requests to servers based on different types of request contents, so that it can provide quality of service requirements for different types of contents and improve overall cluster performance. The overhead of parsing requests in application layer is high, thus its scalability is limited, compared to layer-4 load balancing. This is turn implies that a very high value for this measure will be accompanied by a significant increase in the processing overheads, but will ensure improved cluster performance.
	Level7 total connections: Indicates the total number of L7 connections to the equalizer.	Number	
	Level7 peak connections: Indicates the high watermark of L7 connections to the equalizer.	Number	

15.1.2.3 Equalizer Server Status Test

The real test of the efficiency of a load balancer lies in its ability to uniformly distribute load across the servers in a cluster, thereby ensuring the peak performance and continuous availability of the dependent services. Using the **Equalizer Server Status** test, administrators can accurately judge the efficiency and effectiveness of the equalizer. This test monitors the connection and calculated load on each server in a cluster, promptly detects load imbalances, and alerts administrators to them, so that they can quickly resolve the issue.

Purpose	Monitors the connection and calculated load on each server in a cluster, promptly detects load imbalances, and alerts administrators to them, so that they can quickly resolve the issue
Target of the test	A Coyote Point Equalizer
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the equalizer 3. **PORT** – The port at which the equalizer listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the equalizer exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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**. 17. **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*.		
Outputs of the test	One set of results for each server in each cluster managed by the equalizer		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Server load: Indicates the current calculated load value for this server.	Number	• This indicates the workload on the server. By comparing the value of this measure across all the servers in a cluster, you can instantly identify irregularities in load balancing. If found necessary, you can reconfigure the load balancing rules to ensure uniform load distribution across servers.
	Response time: Indicates how quickly this server is currently responding to client requests.	ms	It is the job of a load balancer to ensure minimal response time for client requests. A high value for this measure could therefore indicate a defective load balancer or one that is improperly configured. Further investigation is hence necessary in this case to identify the root-cause of the anomaly.
	Current connections: Indicates the number of connections that were active on this server during the last measurement period.	Number	The indicates the connection load on the server. By observing the graph of this measure over time, you can analyze the rate of growth of the load on the server. By comparing the value of this measure across all the servers in a cluster, you can instantly identify overloaded servers; this in turn brings irregularities in load balancing to light.

	Total connections: Indicates the number of current connections to this server.	Number	If a sudden/consistent increase in the value of this measure is noticed, you might have to investigate further to identify the reason for this occurrence.
	Idle time: Indicates the time for which this server was idle.	Secs	Ideally, the value of this measure should be low. A high value indicates that the server has remained unused for a long time. This could be owing to inconsistencies in load balancing or because the server is unavailable for use.

Chapter 16

Monitoring the Fibre Channel Switch

In the computer storage field, a **Fibre Channel switch** is a network switch compatible with the Fibre Channel (FC) protocol. It allows the creation of a Fibre Channel fabric, that is currently the core component of most storage area networks. The fabric is a network of Fibre Channel devices which allows many-to-many communication, device name lookup, security, and redundancy. FC switches implement zoning, a mechanism that disables unwanted traffic between certain fabric nodes.

A defective FC switch can wreak havoc in a SAN environment, as it may cause serious security glitches, severe communication lapses, or prolonged breaks in the availability of the SAN environment. By continuously monitoring the state and operations of the switch, you can ensure that you are promptly notified of performance issues with the switch, so as to avoid such outcomes.

eG Enterprise provides a specialized *Fibre Channel Switch* monitoring model that periodically monitors the state of the critical switch components and the load on the switch, so as to proactively alert administrators to unexpected state changes or a sudden/steady increase in the load to the switch. For this purpose, the *Fibre Channel Switch* model employs a single eG external agent that polls the SNMP MIB of the switch to gather the statistics of interest at configured intervals.

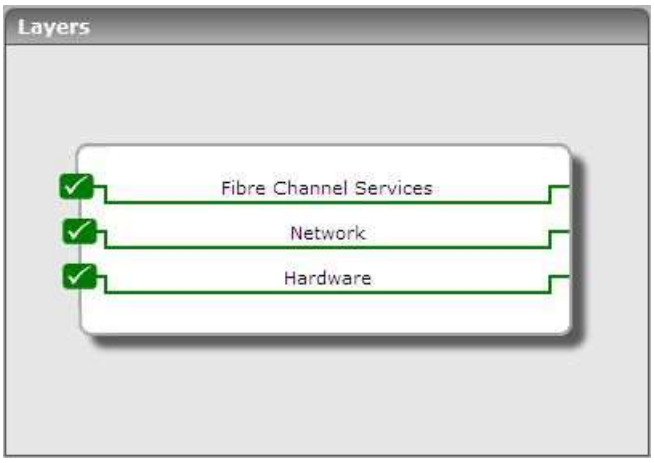

Figure 16.1: Layer model of the Fibre Channel switch

Each layer of Figure 16.1 is mapped to a series of tests that report a wealth of performance data that reveal the health of the fibre channel switch. Using these tests, you can accurately figure out the following:

- Are all critical sensors of the switch in good health? Has any sensor failed? If so, which one is it?
- Is the switch available over the network?

- Are all the network interfaces supported by the switch using bandwidth optimally?
- Is any network interface operating at an abnormal speed?
- Which connection units are currently offline?
- Are there any unused connection units on the switch?
- How is the load on the ports? Is any port overloaded?
- Are all ports in the 'ready' state? Has any port failed?
- Are there 'invalid' ports on the switch?
- Has any port experienced a hardware failure?
- Is any port operating slowly?
- Is any port experiencing too many errors?
- Are link failures/invalid transmissions high on any port?
- Has any port encountered a signal loss/synchronization loss? Is it owing to a poor physical link?

The sections that follow will discuss each of these layers in great detail.

16.1 The Hardware Layer

Using the **Sensor Status** test mapped to this layer, you can be instantly updated with the current status of the power supply, fan, and temperature sensors of the switch.

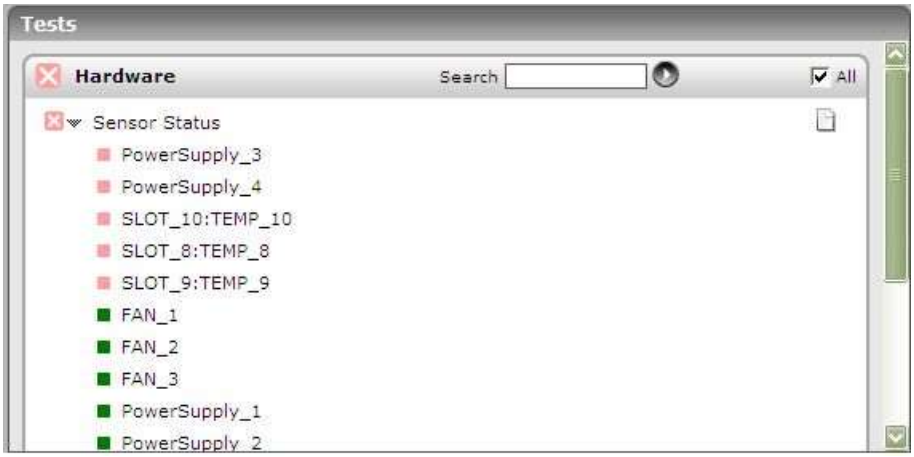

Figure 16.2: The test mapped to the Hardware layer

16.1.1 Fiber Channel Sensors Test

This test reports the current status of each of the sensors on the FC switch.

Purpose	Reports the current status of each of the sensors on the FC switch
Target of the test	An FC SAN switch

Agent deploying the test	An external agent
Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **PORT** – The port at which the switch listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the switch exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.

17. 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.

18. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.

The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
• The eG manager license should allow the detailed diagnosis capability
• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each sensor on the SAN switch being monitored</td></tr>
<tr><td>Measurements made by the</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
</table>

<table>
<tr>
<td>test</td>
<td>Sensor status:
Indicates the current status of this sensor.</td>
<td></td>
<td>
• The table below summarizes the State values reported by this measure and their corresponding numeric equivalents:
<table>
<tr><th>• State</th><th>• Value</th></tr>
<tr><td>• Failed</td><td>• 0</td></tr>
<tr><td>Warning</td><td>• 1</td></tr>
<tr><td>• Unknown</td><td>• 2</td></tr>
<tr><td>• Other</td><td>• 3</td></tr>
<tr><td>• ok</td><td>• 4</td></tr>
</table>
•
Note:
•
• By default, this measure reports the above-mentioned States while indicating the current status of a sensor. However, the in graph of this measure, states will be represented using their corresponding numeric equivalents only.
• Use the detailed diagnosis of this measure to determine the exact state of the sensor.
</td>
</tr>
</table>

16.2 The Network Layer

To know the health of network connections to and from the switch, to measure the responsiveness of the switch, and to assess the bandwidth usage and speed of the network interfaces supported by the switch, use the tests mapped to the **Network** layer.

Figure 16.3: The tests associated with the Network layer

Since both the tests displayed in Figure 16.4 have been dealt with in the previous chapters, let us proceed to the next layer.

16.3 The Fibre Channel Services Layer

The tests mapped to this layer enable network administrators to do the following:

- Promptly detect sudden changes in the operational state or overall health of one/more ports on the switch;
- Be alerted to errors/invalid transmissions at the port-level
- Isolate connection units that have failed;
- Identify overloaded ports or ports that are abnormally slow.

Figure 16.4: The tests mapped to the Fibre Channel Services layer

16.3.1 Fiber Channel Connectivity Units Test

This test reports the current operational state of the connection unit of the switch, and provides periodic updates on the current health of the unit.

Purpose	Reports the current operational state of the connection unit of the switch, and provides periodic updates on the current health of the unit
Target of the test	An FC SAN switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **PORT** – The port at which the switch listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the switch exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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**. 17. **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*. 18. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.
Outputs of the test	One set of results for each connection unit on the SAN switch being monitored

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

<table>
<tr>
<td>test</td>
<td>Operational state of connection unit:
Indicates the current operational state of the connection unit.</td>
<td></td>
<td>

The table below summarizes the State values that this measure can report and their corresponding numeric equivalents:

<table>
<tr><th>State</th><th>Value</th></tr>
<tr><td>Offline</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Online</td><td>100</td></tr>
</table>

Note:

By default, this measure reports the above-mentioned States while indicating the current operational state of the connection unit. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only.
Use the detailed diagnosis of this measure to know the exact state of the connection unit, the number of sensors, and number of ports.

</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>Current health of connection unit:
Indicates the current health of the connection unit.</td>
<td></td>
<td>

The table below summarizes the State values that this measure can report and their corresponding numeric equivalents:

<table>
<tr><th>State</th><th>Value</th></tr>
<tr><td>Failed</td><td>0</td></tr>
<tr><td>Warning</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Other</td><td>3</td></tr>
<tr><td>ok</td><td>100</td></tr>
</table>

Note:

By default, this measure reports the above-mentioned States while indicating the current health of the connection unit. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only.
Use the detailed diagnosis of this measure to know the exact state of the connection unit, the number of sensors, and number of ports.

</td>
</tr>
</table>

16.3.2 Fiber Channel Port Load Test

To proactively capture sporadic or consistent increases in the load on a switch, it is imperative to monitor the traffic handled by each of the ports on the switch. Using the Port Load test, you can study the data, frames, and line resets sent and received by each port on the switch, and thus analyze the load on the switch.

Purpose	Study the data, frames, and line resets sent and received by each port on the switch, and thus analyze the load on the switch

Target of the test	An FC SAN switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **PORT** – The port at which the switch listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the equalizer exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each port on the SAN switch being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Frames transmitted:
Indicates the number of frames / packets / IOs / etc that have been transmitted by this port.</td><td>Number</td><td rowspan="2">• These measures serves as effective indicators of the I/O load on the ports. Comparing the value of these measures across ports will reveal the I/O-intensive ports.</td></tr>
<tr><td>Frames received:
Indicates the number of frames / packets / IOs / etc that have been received by this port.</td><td>Number</td></tr>
<tr><td>Data transmitted:
Indicates the number of octets or bytes that have been transmitted by this port per second.</td><td>KB/Sec</td><td rowspan="2">These measures serve as good indicators of the data traffic handled by a port. Comparing the value of these measures across ports will reveal the busiest ports on the switch.</td></tr>
<tr><td>Data received:
Indicates the number of octets or bytes that have been transmitted by this port per second.</td><td>Number</td></tr>
</table>

	Link resets transmitted: Indicates the number of link resets transmitted by this port.	Number	A link reset is a primitive sequence used during link initialization between ports. Besides indicating the load on a port, these measures also help determine how many ports have tried to establish a link with a particular port, and whether any link initialization attempt has failed.
	Link resets received: Indicates the number of link resets received by this port.	Number	

16.3.3 Fiber Channel Port Status Test

Instantly detect changes in the port state, isolate ports that are operating at abnormal speeds, and be immediately notified of errors/problem conditions experienced by the ports with the help of the Port Status test mapped to this layer.

Purpose	Instantly detect changes in the port state, isolate ports that are operating at abnormal speeds, and be immediately notified of errors/problem conditions experienced by the ports
Target of the test	An FC SAN switch
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the switch 3. **PORT** – The port at which the switch listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the switch exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

	18. **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. 19. **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**. 20. **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*. 21. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.		
Outputs of the test	One set of results for each port on the SAN switch being monitored		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

<table>
<tr>
<td>test</td>
<td>Operational state of port:
Indicates the current operational state of this port.</td>
<td></td>
<td>

The table below summarizes the State values that this measure can report and their corresponding numeric equivalents:

<table>
<tr><th>State</th><th>Value</th></tr>
<tr><td>Offline</td><td>0</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Bypassed</td><td>4</td></tr>
<tr><td>Diagnostics</td><td>5</td></tr>
<tr><td>Online</td><td>100</td></tr>
</table>
Note:

By default, this measure reports the above-mentioned States while indicating the operational state of a port. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only.

Use the detailed diagnosis of this measure to determine the exact state of the port.
</td>
</tr>
</table>

	Current health of port: Indicates the current health of this port.		• The table below summarizes the **State** values that this measure can report and their corresponding numeric equivalents: • • **State** / **Value** • Warning / 1 • Failure / 2 • Unknown / 3 • Unused / 4 • Non participating / 6 • Initializing / 7 • Bypass / 8 • Ols / 9 • Ready / 100 • **Note:** • • By default, this measure reports the above-mentioned **State**s while indicating the operational health of a port. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only. Use the detailed diagnosis of this measure to determine the exact status of the port. Moreover, if the detailed diagnosis of the **Operational state** measure reveals that a port is currently **not in the online state**, then the **Current health** of that port will be **unknown**.

<table>
<tr>
<td></td>
<td>Control status of port:
Indicates the control status of this port.</td>
<td></td>
<td>

The table below summarizes the State values that this measure can report and their corresponding numeric equivalents:

<table>
<tr><th>State</th><th>Value</th></tr>
<tr><td>Offline</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Invalid</td><td>2</td></tr>
<tr><td>Reset</td><td>3</td></tr>
<tr><td>Bypass</td><td>4</td></tr>
<tr><td>Unbypass</td><td>5</td></tr>
<tr><td>ResetCounters</td><td>8</td></tr>
<tr><td>Online</td><td>100</td></tr>
</table>
Note:

By default, this measure reports the above-mentioned States while indicating the control status of a port. However, in the graph of this measure, control states will be represented using their corresponding numeric equivalents only.

Use the detailed diagnosis of this measure to determine the exact control status of the port.
</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>Hardware status of port:
Indicates the current status of the switch hardware.</td>
<td></td>
<td>

The table below summarizes the State values that this measure can report and their corresponding numeric equivalents:

<table>
<tr><th>State</th><th>Value</th></tr>
<tr><td>TxFault</td><td>1</td></tr>
<tr><td>Link Down</td><td>2</td></tr>
<tr><td>Failed</td><td>3</td></tr>
<tr><td>Unknown</td><td>4</td></tr>
<tr><td>Bypass</td><td>5</td></tr>
<tr><td>Loopback</td><td>6</td></tr>
<tr><td>No Media</td><td>7</td></tr>
<tr><td>Active</td><td>100</td></tr>
<tr><td>Ready</td><td>100</td></tr>
</table>
Note:

By default, this measure reports the above-mentioned States while indicating the hardware status of a port. However, in the graph of this measure, hardware states will be represented using their corresponding numeric equivalents only.

Use the detailed diagnosis of this measure to determine the exact hardware status of the port.
</td>
</tr>
</table>

	Port speed: Indicates the speed of the port.	KB/Sec	A sudden/consistent deterioriation in speed could indicate a problem requiring further investigation.
	Number of errors: Indicates the number of errors that have occurred on this port.	Number	Ideally, the value of this measure should be 0. A non-zero value indicates the existence of one/more problems with the port. A very high value is indicative of a problem-prone port.
	Buffer full events: Indicates the number of times when all input buffers of this port were full.	Number	
	Link failures: Indicates the number of link failures experienced by this port.	Number	Ideally, the value of this measure should be 0.
	Invalid frames received: Indicates the number of invalid frames that were transmitted by this port.	Number	Ideally, the value of this measure should be 0. A high value could indicate a bad physical link.
	Invalid words transmitted: Indicates the number of invalid words that were transmitted by this port.	Number	Ideally, the value of this measure should be 0. A high value could indicate a bad physical link.
	Signal loss count: Indicates the number of times a signal loss was detected at this port.	Number	
	Synchronization loss count: Indicates the number of times a synchronization loss was detected at his port.	Number	Ideally, the value of this measure should be 0. If the value of this measure is high, then, you might want to take a look at the value reported by the **Invalid words transmitted** measure to check whether the physical link is really bad and if that caused the loss of synchronization.

Chapter 17

Monitoring the BIG-IP Local Traffic Manager (LTM)

The BIG-IP Local Traffic Manager (LTM) is an application delivery networking system that secures, optimizes, and delivers applications.

This system provides a suite of security services that enhance network and protocol level security, filter application attacks, and thus protect your mission-critical applications. In addition, the BIG-IP Local Traffic Manager removes single points of failure and virtualizes the network and applications using industry-leading L7 intelligence. Furthermore, it includes static and dynamic load balancing methods, which track dynamic performance levels of servers in a group and ensures that all sites are always on, more scalable, and easier to manage.

Since application delivery delays, inefficiencies, and failures can cause prolonged service outages and cost an enterprise money and reputation, the continuous operation and good health of the LTM is of paramount importance. To ensure this, eG Enterprise provides a specialized *F5 Traffic Manager* model.

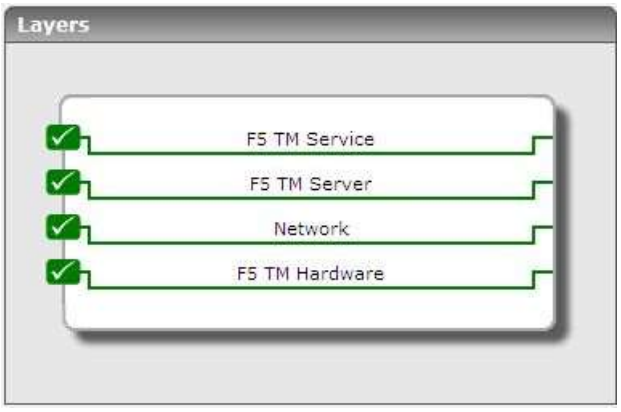

Figure 17.1: Layer model of the F5 Traffic Manager

By periodically polling the SNMP MIB of the traffic manager, the eG external agent extracts useful metrics revealing

the availability of the manager, the resource usage of the manager, the status of the pools managed by the manager, and more! With the help of these metrics, the following questions can be answered easily and accurately:

- Is the LTM available over the network? If so, how quickly is it responding to requests?
- Is any network interface supported by the LTM consuming bandwidth excessively?
- Which is the faster network interface supported by the LTM?
- Is the CPU temperature very high?
- Are any disk partitions on the LTM over-utilized? If so, which ones?
- Has any chassis fan on the LTM failed? If so, which one?
- Is any chassis fan functioning at abnormal speed?
- Is the temperature of any chassis temperature sensor abnormally high?
- What is the current state of each pool configured on the LTM?
- Is any virtual server disabled currently? If so, was it disabled by the parent?

The sections that will follow will discuss each of the layers depicted by Figure 17.1 above.

17.1 The F5 TM Hardware Layer

This layer monitors the critical hardware components of the traffic manager such as CPUs, disk partitions, fans, and temperature sensors, and proactively alerts administrators to hardware failures.

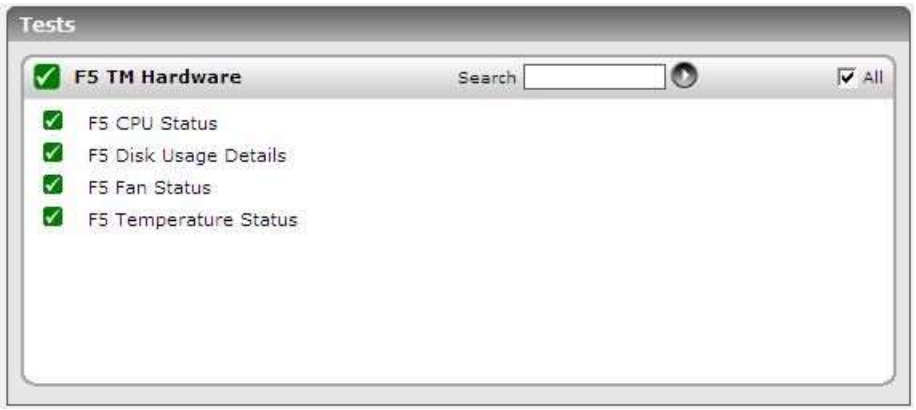

Figure 17.2: The tests mapped to the F5 TM Hardware layer

17.1.1 F5 CPUs Test

This test reports the temperature and fan speed of the CPU supported by the traffic manager.

Purpose	Reports the temperature and fan speed of each processor supported by the traffic manager
Target of the test	A Big-IP/F5 Local Traffic Manager

Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the traffic manager 3. **PORT** – The port at which the traffic manager listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the traffic manager being 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>Cpu temperature:
Indicates the current temperature of the CPU.</td><td>Celsius</td><td>• A high value of this measure is a cause for concern.</td></tr>
<tr><td>Cpu fan speed:
Indicates the current fan speed of the CPU.</td><td>Rpm</td><td></td></tr>
</table>

17.1.2 F5 Disk Usage Test

This test reports the space usage of each disk partition on the traffic manager, and thus indicates which disk is currently running out of space.

Purpose	Reports the space usage of each disk partition on the traffic manager, and thus indicates which disk is currently running out of space
Target of the test	A Big-IP/F5 Local Traffic Manager
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the traffic manager 3. **PORT** – The port at which the traffic manager listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each disk partition on the traffic manager being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Total space:
Indicates the total available space in this disk partition.</td><td>MB</td><td>•</td></tr>
<tr><td>Free space:
Indicates the free space in this disk partition.</td><td>MB</td><td></td></tr>
<tr><td>Used space:
Indicates the amount of space that has been used up onthis partition.</td><td>MB</td><td></td></tr>
<tr><td></td><td>Percent free space:
Indicates the percentage of free space in this disk partition.</td><td>Percent</td><td>Ideally, the value of this measure should be high. A low value is indicative of excessive space usage on the disk partition. Compare the value of this measure across disk partition to accurately identify which partition is facing a potential space crunch.</td></tr>
</table>

17.1.3 F5 Fans Test

This test reports the current state and speed of each fan supported by the traffic manager.

Purpose	Reports the current state and speed of each fan supported by the traffic manager
Target of the test	A Big-IP/F5 Local Traffic Manager
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the traffic manager 3. **PORT** – The port at which the traffic manager listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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**.

17. **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*.

18. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

    The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

    - The eG manager license should allow the detailed diagnosis capability
    - Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Outputs of the test: One set of results for each chassis fan supported by the traffic manager being monitored

Measurements made by the test

Measurement	Measurement Unit	Interpretation
Chassis fan status: Indicates the current status of this fan.	Boolean	Ideally, the value for this measure should be 1, which means the Fan is in good state and it is enabled. If this measure reports the value of 0 or 2, then it implies that the fan is in bad state or the fan is not present. Use the detailed diagnosis of this measure to know exactly what state the numeric value reported by the test represents.
Chassis fan speed: Indicates the actual speed of this chassis fan.	Rpm	

17.1.4 F5 Temperature Test

This test reports the current temperature of the chassis temperature sensor. **Note that this test is only supported on those platforms in which the sensor data is available.**

Purpose	19. Reports the current temperature of the chassis
Target of the test	20. A Big-IP/F5 Local Traffic Manager
Agent deploying the test	21. An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the traffic manager 3. **PORT** – The port at which the traffic manager listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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: 11. **MD5** – Message Digest Algorithm 12. **SHA** – Secure Hash Algorithm 13. **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**. 14. **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: 15. **DES** – Data Encryption Standard 16. **AES** – Advanced Encryption Standard 17. **ENCRYPTPASSWORD** – Specify the encryption password here. 18. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

<table>
<tr><td></td><td colspan="3">19. 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.

20. 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.

21. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the traffic manager being 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>Chassis temperature:

Indicates the current temperature of the chassis temperature sensor.</td><td>Celsius</td><td>Ideally, the value should be low. A high value could be a cause for concern.</td></tr>
</table>

17.2 The Network Layer

Use the **Network** test mapped to this layer to assess the health of network connections to and from the traffic manager. Since this test has been discussed adequately in the previous chapters, let us proceed to the next layer.

Figure 17.3: The test mapped to the Network layer

17.3 The F5 TM Server Layer

With the help of the tests mapped to this layer, you can be promptly alerted to the abnormal state of one/more virtual servers in the pools configured on the traffic manager, and the non-availability of critical ports on the traffic manager.

Figure 17.4: The tests mapped to the F5 TM Server Layer

The section that will follow will discuss the **F5 Virtual Server Status** test alone, as the **TcpPortStatus** test has been dealt with extensively in the previous chapters.

17.3.1 F5 Virtual Servers Test

This test reports the current status of each virtual server in a pool.

Purpose	Reports the current status of each virtual server in a pool
Target of the test	A Big-IP/F5 Local Traffic Manager
Agent deploying the	An external agent

test	
Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the traffic manager 3. **PORT** – The port at which the traffic manager listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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**.

17. **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*.

18. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

    The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

    - The eG manager license should allow the detailed diagnosis capability
    - Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Outputs of the test: One set of results for each virtual server in the pools configured on a traffic manager

Measurements made by the test

Measurement	Measurement Unit	Interpretation
Virtual server status: Indicates the current status of this virtual server.	Boolean	This measure can report a value between or equal to 0 and 3. To know the exact state tha each of these values denote, use the detailed diagnosis of this measure. The values and their states are described below: • 0 - None • 1 - Enabled • 2 - Disabled • 3 - Disabled by parent

17.4 The F5 TM Service Layer

Quickly detect changes in the status of the pools configured on the traffic manager using the test mapped to this layer.

Figure 17.5: The test mapped to the F5 TM Service Layer

17.4.1 F5 Pools Test

This test reports the current status of each of the pools configured on the traffic manager.

Purpose	Reports the current status of each of the pools configured on the traffic manager
Target of the test	A Big-IP/F5 Local Traffic Manager
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the traffic manager 3. **PORT** – The port at which the traffic manager listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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 22. **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 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**.

16. **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*.

17. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

    The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

    - The eG manager license should allow the detailed diagnosis capability
    - Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Outputs of the test: One set of results for each pool configured on a traffic manager

Measurements made by the test

Measurement	Measurement Unit	Interpretation
Pool status: Indicates the current status of this pool.	Boolean	This measure can report a value between or equal to 0 and 3. To know the exact state tha each of these values denote, use the detailed diagnosis of this measure. The values and their states are described below: • 0 - None • 1 - Enabled • 2 - Disabled • 3 - Disabled by parent

Chapter 18

Monitoring the Cisco ASA

In computer networking, **Cisco ASA 5500 Series Adaptive Security Appliances**, or simply **Cisco ASA 5500 Series**, is Cisco's line of network security devices.

In an era that abounds in network security threats, the continuous availability and error-free operation of the Cisco ASA device is of utmost importance in order to protect mission-critical IT infrastructures from malicious virus attacks, and thus ensure the continuous availability of these infrastructures.

To continuously monitor the Cisco ASA device and promptly alert administrators to issues in its performance, eG Enterprise provides the *Cisco ASA* monitoring model.

Figure 18.1: The Cisco ASA layer model

Using the metrics reported by this model, you can answer the following questions quickly and accurately:

- Is any memory pool consuming memory excessively?
- Is the device utilizing its CPU resources optimally? When during the last 5 minutes did the CPU usage peak - during the last 1 second or the last 1 minute?
- What are the types of hardware that support the firewall unit of the device? What is the current state of each hardware type?
- Are too many remote access sessions active on the device? How many users are connected to the device via these sessions?
- Is the device overloaded with sessions? How many of these sessions are currently inactive? Can they be closed?

- Were too many packets dropped by the IPsec Phase-1 IKE global and secondary tunnels? When was packet drop the maximum - when the tunnels were receiving data or transmitting data?

The sections that will follow discuss each layer of the monitoring model depicted by Figure 18.1 above.

18.1 The ASA Hardware Layer

The tests mapped to this layer will enable you to instantly detect the following:

- Hardware failures and the type of hardware that has failed;
- Abnormal CPU usage by the ASA device;
- Excessive memory usage by the device, and the memory pool from which maximum memory resoures have been drained;

Figure 18.2: The tests mapped to the ASA Hardware Layer

18.1.1 ASA Hardware Status Test

This test auto-discovers the various types of hardware that support the firewall unit of the ASA device, and reports the current status of each hardware.

Purpose	Auto-discovers the various types of hardware that support the firewall unit of the ASA device, and reports the current status of each hardware
Target of the test	A Cisco ASA device
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco ASA device 3. **PORT** – The port at which the Cisco ASA device listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the Cisco ASA device exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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**.

17. **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*.

Outputs of the test: One set of results for each type of hardware auto-discovered from the Cisco ASA device being monitored

Measurements made by the test

Measurement	Measurement Unit	Interpretation
Status: Indicates the current status of hardware of this type.	Number	The values that this measure can report and the states they indicate are available in the table below:

Value	State
1	Other
2	up
3	down
4	Error
5	overTemp
6	Busy
7	NoMedia
8	Backup
9	Active
10	Standby

18.1.2 ASA Cpu Details Test

This test enables administrators to figure out how CPU hungry the ASA device is. If the device 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.

Purpose	Enables administrators to figure out how CPU hungry the ASA device is
Target of the test	A Cisco ASA device
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco ASA device 3. **PORT** – The port at which the Cisco ASA device listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the Cisco ASA device exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Cisco ASA device being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>CPU busy (5sec):
Indicates the percentage of time during the last 5 seconds the device was using the CPU.</td><td>Percent</td><td rowspan="3">By comparing the values of all the 3 measures, you can quickly figure out when CPU usage was maximum so that, you can investigate why CPU usage peaked during that time.</td></tr>
<tr><td>CPU busy (1min):
Indicates the percentage of time during the last 1 minute the device was using the CPU.</td><td>Percent</td></tr>
<tr><td>CPU busy (5min):
Indicates the percentage of time during the last 5 minutes the device was using the CPU.</td><td>Percent</td></tr>
</table>

18.1.3 ASA Memory Details Test

To evaluate the memory efficiency of an ASA device, you need to know how each memory pool configured for the device is consuming the available memory resources. This test provides this information. For every memory pool, this test reports the percentage of unused memory in the pool. By comparing the memory usage statistics reported by this test across all memory pools, you can quickly identify which pool is under-sized or is currently running out of memory.

Purpose	For every memory pool, this test reports the percentage of unused memory in the pool
Target of the test	A Cisco ASA device
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco ASA device 3. **PORT** – The port at which the Cisco ASA device listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the Cisco ASA device exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Cisco ASA device being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Total memory:
Indicates the total memory (in MB) available for this memory pool.</td><td>MB</td><td rowspan="3"></td></tr>
<tr><td>Used memory:
Indicates the number of bytes from this pool that are currently used by applications on the managed device.</td><td>MB</td></tr>
<tr><td>Available memory:
Indicates the number of bytes from this pool that are currently available for use by applications.</td><td>MB</td></tr>
<tr><td></td><td>Available free memory:
Indicates the percentage of unused memory in this pool.</td><td>Percent</td><td>Ideally, this value should be high. A low value or a value that consistently decreases could be a cause for concern, as it could indicate the gradual erosion of memory resources from the pool. Under such circumstances, you may either want to resize the pool or investigate what is causing the memory drain and curb it.</td></tr>
</table>

18.2 The Network Layer

The quality of network connections to and from the device, and the overall health, speed, and bandwidth usage of the network interfaces supported by the device can easily assesse using the tests mapped to this layer.

Figure 18.3: The tests mapped to the Network layer

Since all the tests depicted by Figure 18.3 have been elaborately discussed in the previous chapters, let us proceed to the next layer.

18.3 The ASA Sessions Layer

This layer monitors the session load on the device.

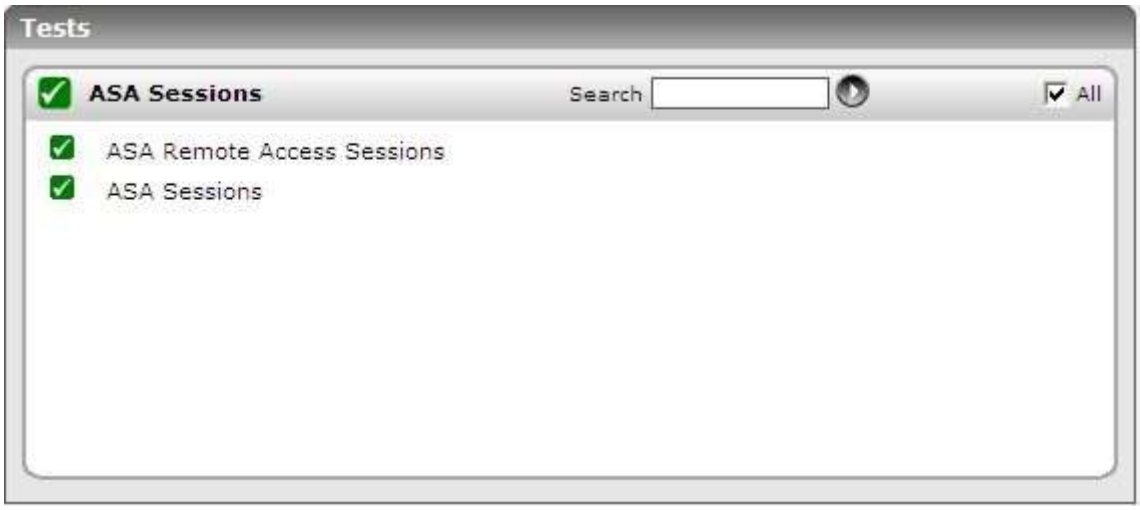

Figure 18.4: The tests associated with the ASA Sessions layer

18.3.1 ASA Remote Access Sessions Test

This test reveals the load generated by remote access sessions by reporting the number of remote access sessions that are currently active on the device, and the number of users connecting to those sessions.

Purpose	Reveals the load generated by remote access sessions by reporting the number of remote access sessions that are currently active on the device, and the number of users connecting to those sessions
Target of the test	A Cisco ASA device
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco ASA device 3. **PORT** – The port at which the Cisco ASA device listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the Cisco ASA device exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Cisco ASA device being 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>Remote sessions:
Indicates the number of sessions that are currently active on the device.</td><td>Number</td><td rowspan="2"></td></tr>
<tr><td>Active users:
Indicates the number of users who have active remote access sessions.</td><td>Number</td></tr>
</table>

18.3.2 ASA Sessions Test

This test serves as a good indicator of the session load on the device.

Purpose	Serves as a good indicator of the session load on the device
Target of the test	A Cisco ASA device
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco ASA device 3. **PORT** – The port at which the Cisco ASA device listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the Cisco ASA device exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Cisco ASA device being 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>Total sessions:
Indicates the total number of sessions to the device.</td><td>Number</td><td rowspan="2"></td></tr>
<tr><td>Active sessions:
Indicates the total number of sessions to the device.</td><td>Number</td></tr>
</table>

18.4 The ASA Tunnels Layer

Tunneling makes it possible to use a public TCP/IP network, such as the Internet, to create secure connections between remote users and a private corporate network. Each secure connection is called a tunnel. The adaptive security appliance uses the ISAKMP and IPsec tunneling standards to build and manage tunnels. ISAKMP and IPsec accomplish the following:

- Negotiate tunnel parameters
- Establish tunnels
- Authenticate users and data
- Manage security keys
- Encrypt and decrypt data

- Manage data transfer across the tunnel
- Manage data transfer inbound and outbound as a tunnel endpoint or router

The adaptive security appliance functions as a bidirectional tunnel endpoint. It can receive plain packets from the private network, encapsulate them, create a tunnel, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination. It can also receive encapsulated packets from the public network, unencapsulate them, and send them to their final destination on the private network.

The tests mapped to this layer monitor the Ike global and secondary tunnels.

Figure 18.5: The tests mapped to the ASA Tunnels layer

18.4.1 Ike Global Tunnels Test

This test measures the level of traffic to and from the IKE global tunnels.

Purpose	Measures the level of traffic to and from the IKE global tunnels
Target of the test	A Cisco ASA device
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco ASA device 3. **PORT** – The port at which the Cisco ASA device listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the Cisco ASA device exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.

17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Cisco device being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Active tunnels:
Indicates the number of IPsec Phase-1 IKE Tunnels that are currently active.</td><td>Number</td><td>IKE (Internet Key Exchange), also called ISAKMP, is the negotiation protocol that lets two hosts agree on how to build an IPsec security association. ISAKMP separates negotiation into two phases: Phase 1 and Phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. This measure reports the number of such tunnels that are currently active.</td></tr>
<tr><td>In packets:
Indicates the number of packets received by all IPsec Phase-1 IKE tunnels.</td><td>Number</td><td></td></tr>
<tr><td>Out packets:
Indicates the number of packets sent by all IPsec Phase-1 IKE tunnels.</td><td>Number</td><td></td></tr>
</table>

	In packets dropped: Indicates the number of packets that were dropped by all IPsec Phase-1 IKE tunnels while receiving data.	Number	Ideally, this value should be low.
	Out packets dropped: Indicates the number of packets that were dropped by all IPsec Phase-1 IKE tunnels while sending data.	Number	Ideally, this value should be low.

18.4.2 Ike Secondary Tunnels Test

This test measures the level of traffic to and from the IKE secondary tunnels.

Purpose	Measures the level of traffic to and from the IKE secondary tunnels
Target of the test	A Cisco ASA device
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TESTPERIOD** – How often should the test be executed 2. **HOST** – The IP address of the Cisco ASA device 3. **PORT** – The port at which the Cisco ASA device listens; by default, this is NULL. 4. **SNMPPORT** – The port at which the Cisco ASA device exposes its SNMP MIB; the default is 161. 5. **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. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **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. 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.

<table>
<tr><td></td><td colspan="3">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.

17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Cisco device being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Active tunnels:
Indicates the number of IPsec Phase-2 IKE Tunnels that are currently active.</td><td>Number</td><td>IKE (Internet Key Exchange), also called ISAKMP, is the negotiation protocol that lets two hosts agree on how to build an IPsec security association. ISAKMP separates negotiation into two phases: Phase 1 and Phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. Phase 2 creates the tunnel that protects data. This measure reports the number of tunnels that protect data.</td></tr>
<tr><td>In packets:
Indicates the number of packets received by all IPsec Phase-2 IKE tunnels.</td><td>Number</td><td></td></tr>
<tr><td>Out packets:
Indicates the number of packets sent by all IPsec Phase-2 IKE tunnels.</td><td>Number</td><td></td></tr>
</table>

	In packets dropped: Indicates the number of packets that were dropped by all IPsec Phase-2 IKE tunnels while receiving data.	Number	Ideally, this value should be low.
	Out packets dropped: Indicates the number of packets that were dropped by all IPsec Phase-2 IKE tunnels while sending data.	Number	Ideally, this value should be low.

Chapter 19

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 **Network elements**. 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.