Monitoring Cisco Router

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

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, thereby significantly slowing down packet transmission. Similarly, very low unused memory/CPU on the router can also affect the speed with which the router transmits data. 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-developed custom monitoring model helps network administrators in this regard.

This document describes the eG-developed custom monitor for the Cisco Router.

1.1 How eG Enterprise Monitors Cisco Router?

To monitor a Cisco router, an eG agent requires the router to be SNMP enabled. SNMP can be enabled in a Cisco router using the following command:

```
Router(config)# snmp-server community <community string> RO 5
```

In the above command, **<community string>** is the SNMP community string that is used for read-only (RO) access. The number 5 refers to the access control list (ACL) identifier.

Cisco routers contain access control lists that allow the SNMP access to be restricted to specific hosts only. In such cases, ensure that the eG external agent has SNMP access to the router.

Chapter 1: How does eG Enterprise Monitor Cisco Router?

eG Enterprise monitors the Cisco Router in an agentless manner. For this purpose, an eG external agent is deployed on any remote host in the environment. This agent communicates with the Cisco router and collects the performance metrics from the SNMP-MIB of the router. To achieve this, eG agent requires the router to be SNMP enabled. The procedure to enable the SNMP on the router, refer to the following section.

1.2 Pre-requisites for monitoring the Cisco Router

To enable the SNMP in the Cisco router, use the following command:

```
Router(config)# snmp-server community <community string> RO 5
```

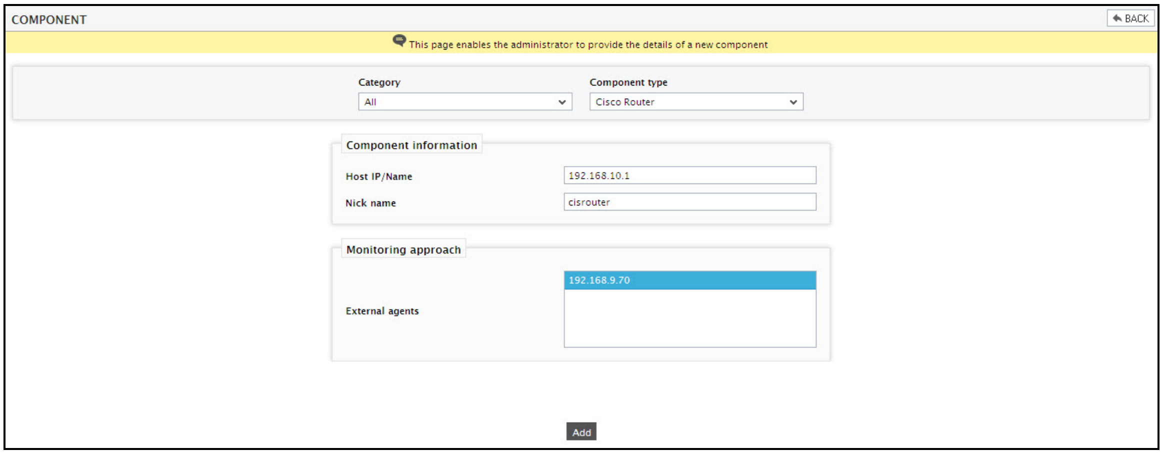
In the above command, **<community string>** is the SNMP community string that is used for read-only (RO) access. The number 5 refers to the access control list (ACL) identifier.

Cisco routers contain access control lists that allow the SNMP access to be restricted to specific hosts only. In such cases, ensure that the eG external agent has SNMP access to the router.

1.3 Managing the Cisco Router

To configure a router for monitoring by eG:

1. Log into the eG administrative interface.
2. If the router is already discovered, then directly proceed towards managing it using the **COMPONENTS - MANAGE/UNMANAGE** page (Infrastructure -> Components -> Manage/Unmanage). However, if it is yet to be discovered, then run discovery (Infrastructure -> Components -> Discovery) to get it discovered or add the router manually using the **COMPONENTS** page (Infrastructure -> Components -> Add/Modify). Remember that components manually added are managed automatically. Discovered components, however, are managed using the **COMPONENTS - MANAGE/UNMANAGE** page.


COMPONENT

This page enables the administrator to provide the details of a new component

Category: All

Component type: Cisco Router

Component information

Host IP/Name: 192.168.10.1

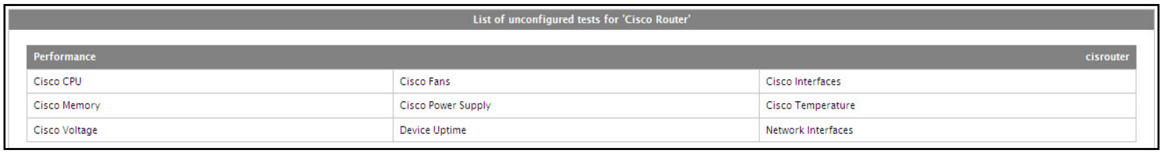
Nick name: cisrouter

Monitoring approach

External agents: 192.168.9.70

Figure 1.1: Adding a new Cisco Router

3. Now, attempt to sign out of the eG administrative interface. Doing so will result in the display of Figure 1.2, which lists all the unconfigured tests of the Cisco Router.



List of unconfigured tests for 'Cisco Router'

Performance		cisrouter
Cisco CPU	Cisco Fans	Cisco Interfaces
Cisco Memory	Cisco Power Supply	Cisco Temperature
Cisco Voltage	Device Uptime	Network Interfaces

Figure 1.2: List of unconfigured tests for the Cisco router

4. Click the **Cisco CPU** test to configure the test. To know how to configure the test, refer to Section **2.1.2**.
5. Finally, signout of the eG administrative interface.

Chapter 2: Monitoring Cisco Routers

The eG Enterprise suite includes special-purpose monitors for Cisco routers to monitor the resource usage and the traffic to and from the Cisco router, so that any sudden increase in load or erosion of resources can be instantly detected, and remedial action immediately initiated.

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.

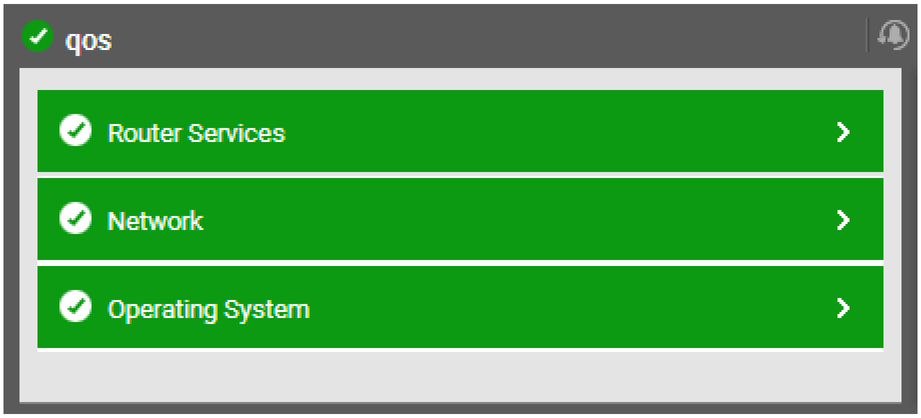
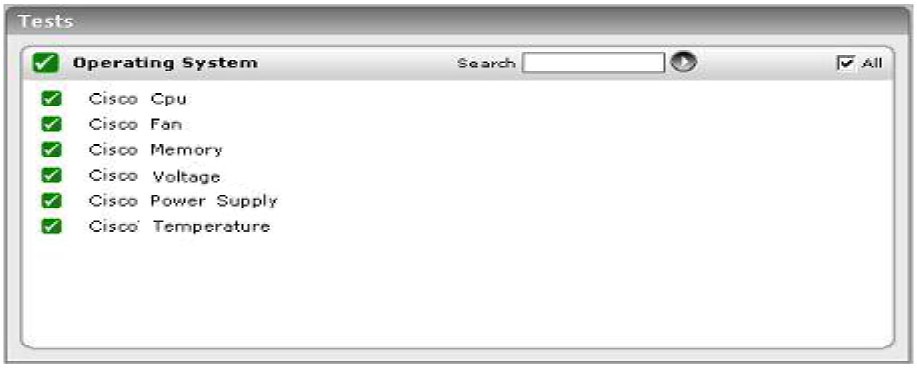


Figure 2.1: Layer model for network elements

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:



☑ Operating System

☑ Cisco Cpu
☑ Cisco Fan
☑ Cisco Memory
☑ Cisco Voltage
☑ Cisco Power Supply
☑ Cisco Temperature

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

2.1.1 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 the Cisco Router as the desired **Component type**, set *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.

Target of the test : A Cisco router

Agent deploying the test : An external agent

Outputs of the test : One set of results for every router being monitored.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco Router.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the snmpversion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this

Parameters	Description
	parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • MD5 – Message Digest Algorithm • SHA – Secure Hash Algorithm
Encryptflag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
Encrypttype	If this Encryptflag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the Encrypttype list. SNMP v3 supports the following encryption types: • DES – Data Encryption Standard • AES – Advanced Encryption Standard

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
No memory errors	Counts the number of buffer creation failures due to lack of free memory in the router	Number	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.
Small buffer misses	Counts the number of allocations that failed because there were no small buffers available	Number	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.

Measurement	Description	Measurement Unit	Interpretation
Medium buffer misses	Counts the number of allocations that failed because there were no medium buffers available	Number	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.
Large buffer misses	Counts the number of allocations that failed because there were no large 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 large buffers set when configuring the router may be too low for the traffic being handled.
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	Ideally, the value of this measure

Measurement	Description	Measurement Unit	Interpretation
	number of buffer hits.		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.

2.1.2 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.

Target of the test : A Cisco router

Agent deploying the test : An external agent

Outputs of the test : One set of results for every router being monitored.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the Cisco Router.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the snmpversion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using

Parameters	Description
	the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • MD5 – Message Digest Algorithm • SHA – Secure Hash Algorithm
Encryptflag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
Encrypttype	If this Encryptflag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the Encrypttype list. SNMP v3 supports the following encryption types: • DES – Data Encryption Standard • AES – Advanced Encryption Standard
Encryptpassword	Specify the encryption password here.

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU utilization	Total percentage CPU utilization of a router.	Percent	A very high value could indicate a CPU bottleneck at the router.

2.1.3 Cisco Fans Test

This test 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

Outputs of the test : One set of results for every fan on the Cisco device that is monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is 161.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default

Parameter	Description
	selection in the snmpversion list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the snmpversion chosen is v3, then this parameter will not appear.
Username	This parameter appears only when v3 is selected as the snmpversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the username parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the USERNAME provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the username in the context text box. By default, this parameter is set to none.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the snmpversion selected is v3.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if v3 is selected as the snmpversion. From the authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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

Measurement	Description	Measurement Unit	Interpretation
			shut down. A value of 6 is reported if the fan is not functioning.

2.1.4 Cisco Power Supply Test

This test 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

Outputs of the test : One set of results for every power supply on the Cisco device that is monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is 161.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the snmpversion chosen is v3, then this parameter will not appear.
Username	This parameter appears only when v3 is selected as the snmpversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access

Parameter	Description
	permissions to be MIB. Therefore, specify the name of such a user against the username parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the USERNAME provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the username in the context text box. By default, this parameter is set to none.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the snmpversion selected is v3.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if v3 is selected as the snmpversion. From the authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
Encryptflag	This flag appears only when v3 is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to no by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the yes option.
Encrypttype	If this Encryptflag is set to Yes, then you will have to mention the encryption type by selecting an option from the Encrypttype list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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.

2.1.5 Cisco Temperature Test

This test monitors the ambient temperature of a Cisco device.

Target of the test : A Cisco device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every temperature test point on the Cisco device that is monitored.

Configurable parameters for the test

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Current temperature	Indicates the current ambient temperature as reported by a test point.	Celsius	
Current state	Indicates the current state of a temperature 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.

2.1.6 Cisco Voltage Test

This test 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

Outputs of the test : One set of results for every voltage test point on the Cisco device that is monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

Parameter	Description
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the snmpversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP **v3** protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the Username parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the context text box. By default, this parameter is set to *none*.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if v3 is selected as the snmpversion. From the authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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

Measurement	Description	Measurement Unit	Interpretation
			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 Memory Test

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

Target of the test : A Cisco device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every memory pool of a router being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is 161.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the snmpversion chosen is v3, then this parameter will not appear.
Username	This parameter appears only when v3 is selected as the snmpversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance

Parameter	Description
	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.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the USERNAME provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the username in the context text box. By default, this parameter is set to none.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the snmpversion selected is v3.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if v3 is selected as the snmpversion. From the authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • MD5 – Message Digest Algorithm • SHA – Secure Hash Algorithm
Encryptflag	This flag appears only when v3 is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to no by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the yes option.
Encrypttype	If this Encryptflag is set to Yes, then you will have to mention the encryption type by selecting an option from the Encrypttype list. SNMP v3 supports the following encryption types:

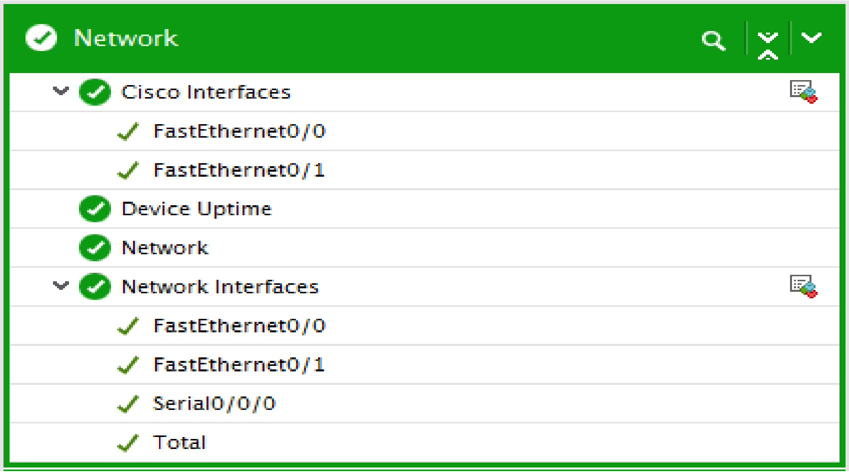
Parameter	Description
	• DES – Data Encryption Standard • AES – Advanced Encryption Standard
Encryptpassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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.

2.2 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.



- ✓ Network
  - ✓ Cisco Interfaces
    - ✓ FastEthernet0/0
    - ✓ FastEthernet0/1
  - ✓ Device Uptime
  - ✓ Network
  - ✓ Network Interfaces
    - ✓ FastEthernet0/0
    - ✓ FastEthernet0/1
    - ✓ Serial0/0/0
    - ✓ Total

Figure 2.3: List of tests associated with the Network layer

Since the details about the **Network** test is 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

This test 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 device

Agent deploying the test : An external agent

Outputs of the test : One set of records for each interface of a router.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.

Parameter	Description
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the snmpversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP **v3** protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the Username parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the username in the context text box. By default, this parameter is set to none.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if v3 is selected as the snmpversion. From the authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:

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

Parameter	Description
	+ output bandwidth)*100/total speed.
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**.
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**.
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 if Alias 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 Usalias 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.
UseExtension	By default, this test polls the standard IF MIB (RFC 1213) to collect the required

Parameter	Description
	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**.
Use IFX Name	By default, this flag is set to **No**, indicating that the eG agent polls the standard IF MIB to collect the performance metrics. If you want the eG agent to poll the *IF-EXTENSION-MIB* to collect the required metrics, set this flag to **Yes**.
Speed Multiply Factor	By default, *none* is displayed against this parameter. This indicates that the actual speed of each network interface of the target network device obtained as bits per second from the SNMP MIB II is automatically converted to Mbps and displayed against the Speed measure in the eG monitor interface. In some environments, network administrators may have explicitly set the speed of the target network device to Kbps or Mbps against the default speed of bits per second. In such cases, specify a suitable value against this parameter. If the speed of the network interface is set to kbps, then specify *1000* against this parameter. Alternately, if the speed of the network interface is set to Mbps, then set *1000000* against this parameter.
Show Concise Metrics	By default, this parameter is set to **No** indicating that the test will report all the metrics related to each network interface in the target environment. If this flag is set to **Yes**, then packet related metrics (for e.g., Non-unicast packets received, Transmit errors, Outbound protocols etc) will not be collected. It is recommended to set this flag to **Yes** in environments where database space is a constraint to collect all the metrics for a large number of network interfaces.
Show Details	By default, this flag is set to **Yes** indicating that the detailed diagnosis of the Bandwidth used measure will provide the maximum amount of data flow through the network interface at a given point of time. It is also mandatory to enable the **Net Flows** Test, to obtain the detailed diagnosis. If you do not wish to obtain the detailed diagnosis for the Bandwidth used measure, then set this flag to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Is the network interface	Indicates the availability of a network interface		If the operational state (i.e., the

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>available?</td><td></td><td></td><td>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>
<b>Note:</b>
By default, this measure reports one of the <b>State</b>s 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</td><td>Indicates the rate of data being transmitted from the router over a network link</td><td>MB/Sec</td><td>This measurement depicts the workload on a network link.</td></tr>
<tr><td>Data received rate</td><td>The rate of data being</td><td>MB/Sec</td><td>This measure also characterizes the</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
	received by the router over a network link		workload on a network link.
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.			

Measurement	Description	Measurement Unit	Interpretation
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	Packets/Sec	

Measurement	Description	Measurement Unit	Interpretation
	were received by this layer.		
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	Number	A consistent increase in the queue

Measurement	Description	Measurement Unit	Interpretation
	the output packet 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.

Target of the test : A Cisco device

Agent deploying the test : An external agent

Outputs of the test : One set of records for each interface of a router

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is 161.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the snmpversion chosen is v3, then this parameter will not appear.
Username	This parameter appears only when v3 is selected as the snmpversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the username parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP

Parameter	Description
	context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the USERNAME provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the username in the context text box. By default, this parameter is set to none.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the snmpversion selected is v3.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if v3 is selected as the snmpversion. From the authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • MD5 – Message Digest Algorithm • SHA – Secure Hash Algorithm
Encryptflag	This flag appears only when v3 is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to no by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the yes option.
Encrypttype	If this Encryptflag is set to Yes, then you will have to mention the encryption type by selecting an option from the Encrypttype list. SNMP v3 supports the following encryption types: • DES – Data Encryption Standard • AES – Advanced Encryption Standard
Encryptpassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Exclude	This text box takes a comma separated list of network interfaces that are to be

Parameter	Description
	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.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to Yes. By default, this flag is set to No.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Reliability value	Provides the level of reliability of the interface	Number	This is representative of how many errors are occurring on the interface. The best reliability value is 255.
Reliability percent	Indicates the reliability of an interface as a percentage	Percent	This is computed as (Reliability value)*100/255. A drop in the value of this measure indicates an error-prone interface.
Delay	The amount of delay of an interface	Secs	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.
Load factor	The degree of loading of an interface, reported as a percent.	Percent	A value of 100% indicates a saturated interface. Consider increasing the speed/capacity of the interface in this case.
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	Mbits/sec	This value is an indicator of the instantaneous traffic transmitted over

Measurement	Description	Measurement Unit	Interpretation
	over an interface		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	Number	This value which is mainly relevant for serial lines is one of the factors that affects the reliability of the line.

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>errors</td><td></td><td></td></tr>
<tr><td>Aborts</td><td>Number of packet receptions in the last measurement period that were aborted due to errors</td><td>Number</td><td></td></tr>
<tr><td>Collisions</td><td>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>Slow packets received</td><td>The rate at which packets routed with slow switching were received.</td><td>Packets/Sec</td><td></td></tr>
<tr><td>Slow packets transmitted</td><td>The rate at which packets routed with slow switching were transmitted.</td><td>Packets/Sec</td><td></td></tr>
<tr><td>Link protocol status</td><td>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:
<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>
<b>Note:</b>
By default, this measure reports one of the <b>Measure Value</b>s 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.

This test included in the eG agent monitors the uptime of critical network devices.

Target of the test : Any network device

Agent deploying the test : An external agent

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

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the snmpversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract

Parameter	Description
	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.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the username in the context text box. By default, this parameter is set to none.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if v3 is selected as the snmpversion. From the authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
Encryptflag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to no by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the yes option.
Encrypttype	If this Encryptflag is set to Yes, then you will have to mention the encryption type by selecting an option from the Encrypttype list. SNMP v3 supports the

Parameter	Description
	following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
Encryptpassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
ReportManagerTime	By default, this flag is set to **Yes**, indicating that, by default, the detailed diagnosis of this test, if enabled, will report the shutdown and reboot times of the device in the manager's time zone. If this flag is set to **No**, then the shutdown and reboot times are shown in the time zone of the system where the agent is running.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to Yes. By default, this flag is set to No.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Has the system been rebooted?	Indicates whether the server has been rebooted during the last measurement period or not.	Boolean	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.

Measurement	Description	Measurement Unit	Interpretation
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.

Target of the test : A Cisco device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every protocol handled by every network interface being monitored .

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.

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

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

Parameter	Description
	Accordingly, this parameter is set to *none* by default.
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.
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.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data received	Indicates the total data received through this interface using this protocol.	Mbps	
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.

Measurement	Description	Measurement Unit	Interpretation
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 traffic 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.

Note:

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 if Index 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.

Target of the test : A Cisco device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every net flow discovered from the router being monitored .

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the snmpversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP **v3** protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the Username parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one

Parameter	Description
	context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the username in the context text box. By default, this parameter is set to none.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if v3 is selected as the snmpversion. From the authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
Encryptflag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to no by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the yes option.
Encrypttype	If this Encryptflag is set to Yes, then you will have to mention the encryption type by selecting an option from the Encrypttype list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
Encryptpassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.

Parameter	Description
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
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.
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.
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*.
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**.
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.
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.

Parameter	Description
	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.

Measurements made by the test

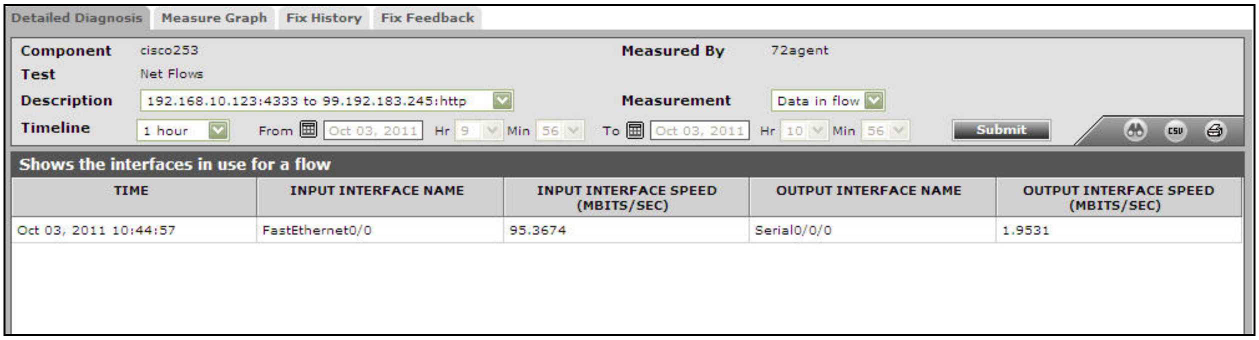
Measurement	Description	Measurement Unit	Interpretation
Data in flow	Indicates the amount of data transmitted and received in this net flow.	KB	Compare the value of this measure across flows to identify which flow is experiencing high levels of network traffic. This way, you can also identify the two 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.
Packets in flow	Indicates the total number of packets received and transmitted in this net flow.	Pkts	
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.	Percent	Compare the value of this measure across flows to know which flow is receiving large volumes of data via the input interface.
Fraction of traffic	Indicates the	Percent	Compare the value of this measure

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>on output interface for this flow</td><td>percentage of total traffic for this flow that is flowing through the output interface.</td><td></td><td>across flows to know which flow is transmitting large volumes of data via the output interface.</td></tr>
<tr><td>Protocol</td><td>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>
<tr><td>GGP</td><td>3</td></tr>
<tr><td>IPv4</td><td>4</td></tr>
<tr><td>ST</td><td>5</td></tr>
<tr><td>TCP</td><td>6</td></tr>
<tr><td>CBT</td><td>7</td></tr>
<tr><td>EGP</td><td>8</td></tr>
<tr><td>IGP</td><td>9</td></tr>
<tr><td>BBN-RCC-MON</td><td>10</td></tr>
<tr><td>NVP-II</td><td>11</td></tr>
<tr><td>PUP</td><td>12</td></tr>
<tr><td>ARGUS</td><td>13</td></tr>
<tr><td>EMCON</td><td>14</td></tr>
<tr><td>XNET</td><td>15</td></tr>
<tr><td>CHAOS</td><td>16</td></tr>
<tr><td>UDP</td><td>17</td></tr>
<tr><td>MUX</td><td>18</td></tr>
<tr><td>RDP</td><td>27</td></tr>
<tr><td>IPv6</td><td>41</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Protocol</th><th>Numeric value</th></tr>
<tr><td>IPv6-Route</td><td>43</td></tr>
<tr><td>IPv6-Frag</td><td>44</td></tr>
<tr><td>IDRP</td><td>45</td></tr>
<tr><td>RSVP</td><td>46</td></tr>
<tr><td>SWIPE</td><td>53</td></tr>
<tr><td>MOBILE</td><td>55</td></tr>
<tr><td>IPv6-ICMP</td><td>58</td></tr>
<tr><td>IPv6-NoNxt</td><td>59</td></tr>
<tr><td>IPv6-Opts</td><td>60</td></tr>
<tr><td>VISA</td><td>70</td></tr>
<tr><td>PVP</td><td>75</td></tr>
<tr><td>DGP</td><td>86</td></tr>
<tr><td>IPIP</td><td>94</td></tr>
<tr><td>PNNI</td><td>102</td></tr>
<tr><td>UDPLite</td><td>136</td></tr>
</table>

Note:
By default, this measure reports one of the **Protocol**s 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.
</td></tr>
</table>

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.



Component cisco253
Test Net Flows
Measured By 72agent
Description 192.168.10.123:4333 to 99.192.183.245:http
Measurement Data in flow
Timeline 1 hour From Oct 03, 2011 Hr 9 Min 56 To Oct 03, 2011 Hr 10 Min 56

Shows the interfaces in use for a flow

TIME	INPUT INTERFACE NAME	INPUT INTERFACE SPEED (MBITS/SEC)	OUTPUT INTERFACE NAME	OUTPUT INTERFACE SPEED (MBITS/SEC)
Oct 03, 2011 10:44:57	FastEthernet0/0	95.3674	Serial0/0/0	1.9531

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.

Target of the test : A Cisco device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every source host.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

Parameter	Description
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the snmpversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP **v3** protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the Username parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the context text box. By default, this parameter is set to *none*.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if v3 is selected as the snmpversion. From the authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm

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

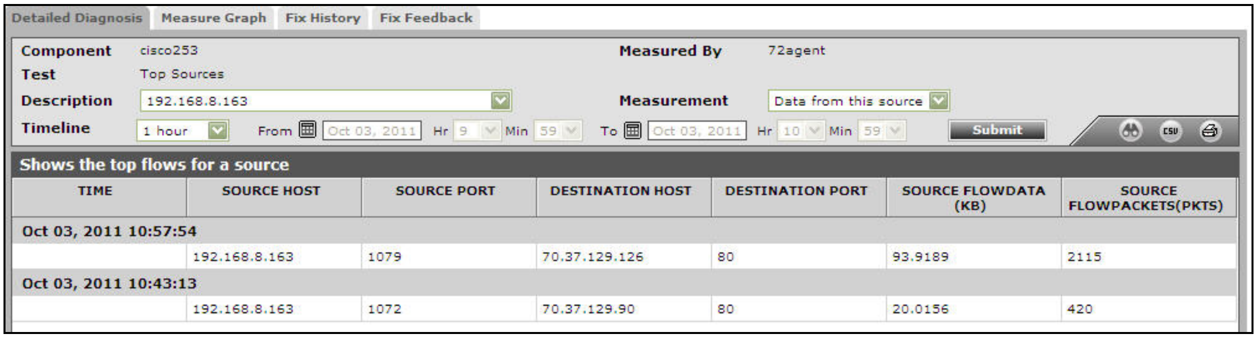
Parameter	Description
	to *5*.
Ignore Local Traffic	By default, this flag is set to **Yes**, indicating that the test will ignore the sources of all the intranet traffic on the router. If you want the test to report metrics pertaining to the sources of local traffic as well, set this flag to **No**.
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.
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.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data from this source	Indicates the amount of data transmitted by this source over the network.	KB	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

Measurement	Description	Measurement Unit	Interpretation
			data transacted) that originated from this source, and the amount of data transacted in bytes and packets in every flow.
This source as fraction of top network flows	Indicates the percentage of top network flows in which this host is the source.	Percent	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.
Packets from this source	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 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?



Component cisco253

Measured By 72agent

Test Top Sources

Description 192.168.8.163

Measurement Data from this source

Timeline 1 hour From Oct 03, 2011 Hr 9 Min 59 To Oct 03, 2011 Hr 10 Min 59

Shows the top flows for a source

TIME	SOURCE HOST	SOURCE PORT	DESTINATION HOST	DESTINATION PORT	SOURCE FLOWDATA (KB)	SOURCE FLOWPACKETS(PKTS)
Oct 03, 2011 10:57:54						
	192.168.8.163	1079	70.37.129.126	80	93.9189	2115
Oct 03, 2011 10:43:13						
	192.168.8.163	1072	70.37.129.90	80	20.0156	420

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.

Target of the test : A Cisco device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every destination host.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the snmpversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP **v3** protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the Username parameter.

Parameter	Description
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the context text box. By default, this parameter is set to *none*.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if v3 is selected as the snmpversion. From the authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
Encryptflag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
Encrypttype	If this Encryptflag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the Encrypttype list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
Encryptpassword	Specify the encryption password here.

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

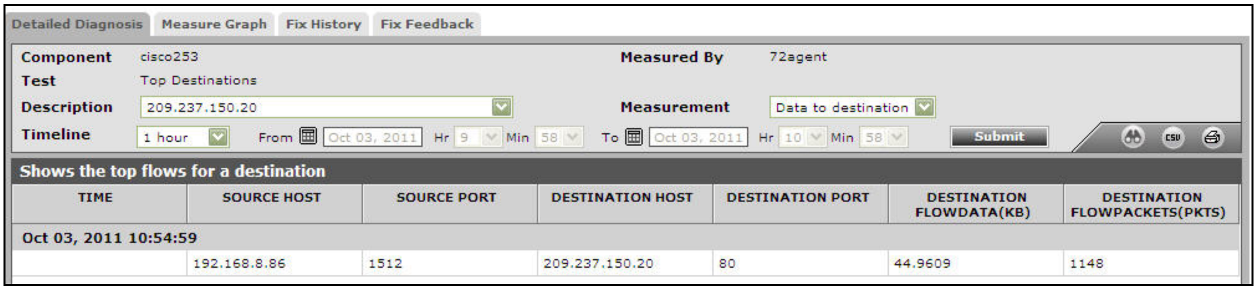
Parameter	Description
	embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **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.

Measurements made by the test

Measurement	Description	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

Measurement	Description	Measurement Unit	Interpretation
			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.



Component cisco253

Test Top Destinations

Description 209.237.150.20

Timeline 1 hour From Oct 03, 2011 Hr 9 Min 58 To Oct 03, 2011 Hr 10 Min 58

Measured By 72agent

Measurement Data to destination

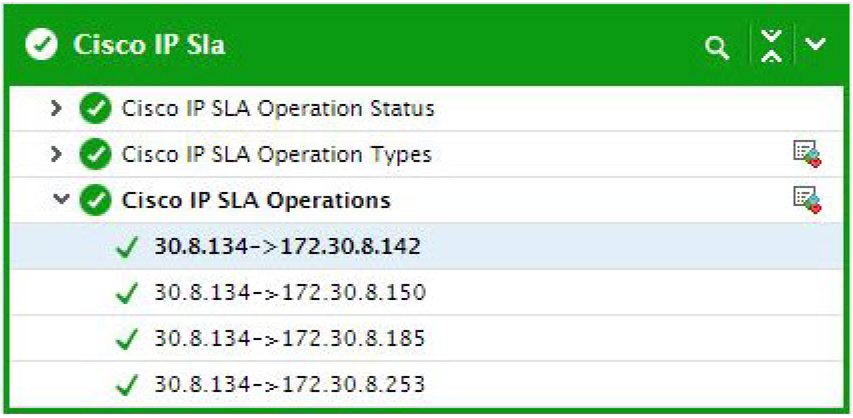
Shows the top flows for a destination

TIME	SOURCE HOST	SOURCE PORT	DESTINATION HOST	DESTINATION PORT	DESTINATION FLOWDATA(KB)	DESTINATION FLOWPACKETS(PKTS)
Oct 03, 2011 10:54:59						
	192.168.8.86	1512	209.237.150.20	80	44.9609	1148

Figure 2.6: The detailed diagnosis of the Top Destinations measure

2.3 The Cisco IP SLA Layer

Cisco IP SLA is a part of Cisco IOS software that allows administrators to analyze IP service levels for IP applications and services by using active traffic monitoring—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance. Cisco IOS IP SLAs can perform network assessments, verify quality of service (QoS), ease the deployment of new services, and assist with network troubleshooting. Using this layer, administrators can determine the status of the monitoring operations performed by an IP SLA, and see detailed metrics reported by the IP SLA for each operation and operation type. This includes metrics such as the round trip time of each operation, packet loss, average latency, count of delayed packets, and packets out of sequence.



Cisco IP Sla

- Cisco IP SLA Operation Status
- Cisco IP SLA Operation Types
- Cisco IP SLA Operations
  - 30.8.134->172.30.8.142
  - 30.8.134->172.30.8.150
  - 30.8.134->172.30.8.185
  - 30.8.134->172.30.8.253

Figure 2.7: List of tests associated with the Cisco IP Sla layer

2.3.1 Cisco IP SLA Operation Status Test

This test reports the count of the Cisco IP SLA operation in each state.

Target of the test : A Cisco device

Agent deploying the test : An external agent

Outputs of the test : One set of results for each status that can be reported for the Cisco IP SLA operations on the Cisco device that is monitored.

Configurable parameters for the test

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Operation status count	Indicates the number of Cisco IP SLA operations in this status.	Number	

2.3.2 Cisco IP SLA Operation Types Test

This test reports the current state of each operation type. In addition, this test reports the round trip time of each operation type, packet loss, average latency, count of delayed packets, and packets out of sequence.

Target of the test : A Cisco device

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type operation of Cisco IP SLA operations on the Cisco device that is monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the Username parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the

Parameter	Description
	SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified Username and Password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such

Parameter	Description
	environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
Use Tag Name	

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Operation status	Indicates the current state of this operation of this operation type.		The values that this measure can report and their corresponding numeric values have been described in the table below <table><tr><th>Measure value</th><th>Numeric value</th></tr><tr><td>OK</td><td>1</td></tr><tr><td>Down</td><td>2, 4, 6 to 16</td></tr><tr><td>Critical</td><td>3</td></tr><tr><td>Unknown</td><td>5</td></tr></table> **Note:** By default, this measure reports one of the **Measure Value**s listed in the table above to indicate the current state of this operation. The graph of this measure however, represents the same using the numeric equivalents mentioned in the table above.
Round trip time	Indicates the time measured between the start of packet transmission from the source device to the start of receiving the acknowledgment from the destination device for this	Miilliseconds	

Measurement	Description	Measurement Unit	Interpretation
	operation type.		
Avg jitter value	Indicates the average variation of response time in receiving the acknowledgment from the destination device for this operation type.	Miilliseconds	
Packets loss	Indicates the total number of packets that were lost during transmission from the source to destination while this operation of this operation type was performed.	Number	Ideally, the value of this measure should be zero.
Average latency	Indicates the average time taken to transmit the response from the destination to the source for this operation type.	Milliseconds	
Mean opinion score	Indicates the percentage of speech quality between the source and destination for this operation type.	Percent	
Packets late arrival	Indicates the total number of packets that were received by the destination with delayed arrival for this operation of the operation type.	Number	
Packets out of sequence	Indicates the number of packets that were not received in the same order as it was transmitted for this operation of this operation type.	Number	

2.3.3 Cisco IP SLA Operations Test

This test reports the current state of each operation of the operation type. In addition, this test reports the round trip time of each operation type, packet loss, average latency, count of delayed packets, and packets out of sequence.

Target of the test : A Cisco device

Agent deploying the test : An external agent

Outputs of the test : One set of results for each Cisco IP SLA operation performed on the Cisco device that is monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the Username parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the

Parameter	Description
	SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified Username and Password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such

Parameter	Description
	environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
Use Tag Name	

Measurements made by the test

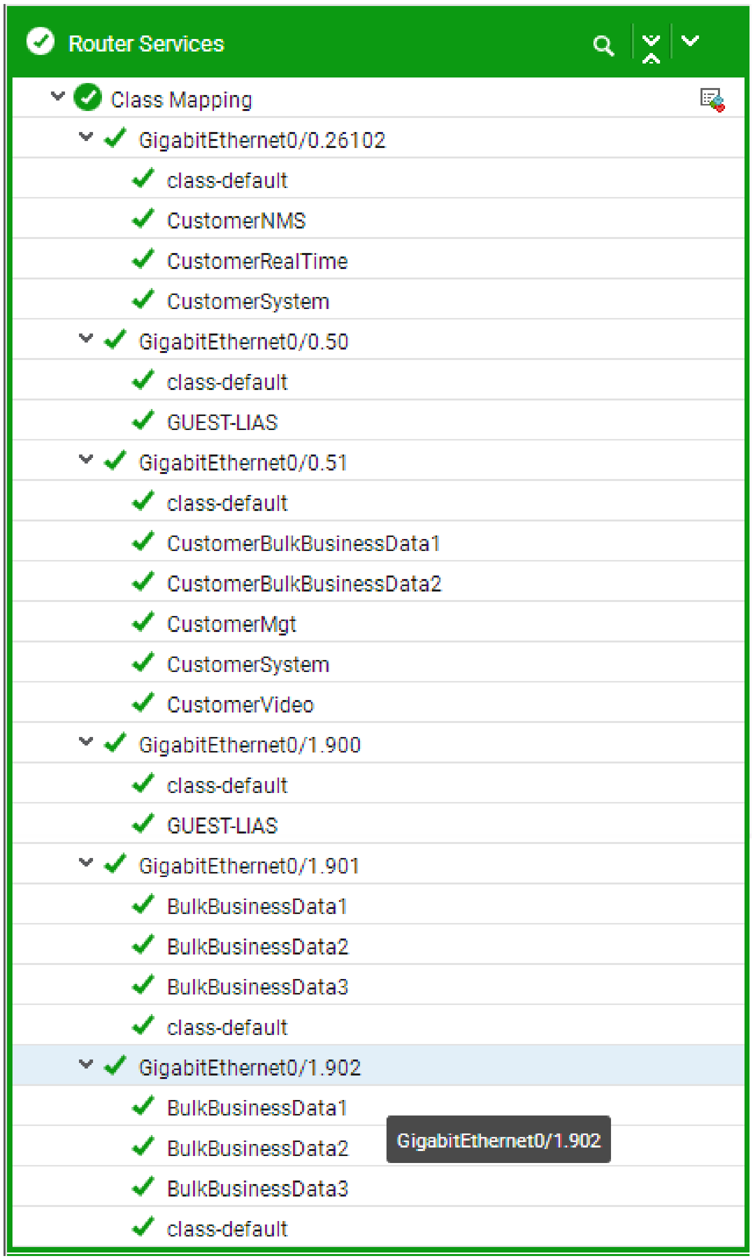
<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Operation status</td><td>Indicates the current state of this operation.</td><td></td><td>The values that this measure can report and their corresponding numeric values have been described in the table below
<table>
<tr><th>Measure value</th><th>Numeric value</th></tr>
<tr><td>OK</td><td>1</td></tr>
<tr><td>Down</td><td>2, 4, 6 to 16</td></tr>
<tr><td>Critical</td><td>3</td></tr>
<tr><td>Unknown</td><td>5</td></tr>
</table>
<b>Note:</b>
By default, this measure reports one of the <b>Measure Value</b>s listed in the table above to indicate the current state of this operation. The graph of this measure however, represents the same using the numeric equivalents mentioned in the table above.</td></tr>
<tr><td>Operation Type</td><td>Indicates the type of this operation.</td><td></td><td>The values that this measure can report and their corresponding numeric values have been described in the table below</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table>
<tr><th>Measure value</th><th>Numeric value</th></tr>
<tr><td>ICMP Echo</td><td>1</td></tr>
<tr><td>Path echo</td><td>2</td></tr>
<tr><td>UDP echo</td><td>5</td></tr>
<tr><td>TCP connect</td><td>6</td></tr>
<tr><td>HTTP</td><td>7</td></tr>
<tr><td>DNS</td><td>8</td></tr>
<tr><td>DHCP</td><td>11</td></tr>
<tr><td>FTP</td><td>12</td></tr>
<tr><td>VOIP</td><td>13</td></tr>
</table>
<b>Note:</b>
By default, this measure reports one of the <b>Measure Value</b>s listed in the table above to indicate the type of this operation. The graph of this measure however, represents the same using the numeric equivalents mentioned in the table above.</td></tr>
<tr><td>Round trip time</td><td>Indicates the time measured between the start of packet transmission from the source device to the start of receiving the acknowledgment from the destination device for this operation.</td><td>Miilliseconds</td><td></td></tr>
<tr><td>Avg jitter value</td><td>Indicates the average variation of response time in receiving the acknowledgment from the destination device for this operation.</td><td>Miilliseconds</td><td></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
Packets loss	Indicates the total number of packets that were lost during transmission from the source to destination while this operation was performed.	Number	Ideally, the value of this measure should be zero.
Average latency	Indicates the average time taken to transmit the responds from the destination to the source for this operation.	Milliseconds	
Mean opinion score	Indicates the percentage of speech quality between the source and destination for this operation.	Percent	
Packets late arrival	Indicates the total number of packets that were received by the destination with delayed arrival for this operation.	Number	
Packets out of sequence	Indicates the number of packets that were not received in the same order as it was transmitted for this operation.	Number	

2.4 The Router Services Layer

Using the tests mapped to this layer, administrators can determine the current status of the BGP neighbors connected to the Cisco Router and the messages transmitted and received through each BGP neighbor. Administrators can also determine the data transmitted and received through the class maps on the target Cisco router and thus identify the class map that drops data too often. **Note that this layer will be visible in the layer model only when one/more test(s) associated with this layer are enabled.**



Router Services

- ✓ Class Mapping
  - ✓ GigabitEthernet0/0.26102
    - ✓ class-default
    - ✓ CustomerNMS
    - ✓ CustomerRealTime
    - ✓ CustomerSystem
  - ✓ GigabitEthernet0/0.50
    - ✓ class-default
    - ✓ GUEST-LIAS
  - ✓ GigabitEthernet0/0.51
    - ✓ class-default
    - ✓ CustomerBulkBusinessData1
    - ✓ CustomerBulkBusinessData2
    - ✓ CustomerMgt
    - ✓ CustomerSystem
    - ✓ CustomerVideo
  - ✓ GigabitEthernet0/1.900
    - ✓ class-default
    - ✓ GUEST-LIAS
  - ✓ GigabitEthernet0/1.901
    - ✓ BulkBusinessData1
    - ✓ BulkBusinessData2
    - ✓ BulkBusinessData3
    - ✓ class-default
  - ✓ GigabitEthernet0/1.902
    - ✓ BulkBusinessData1
    - ✓ BulkBusinessData2
    - ✓ BulkBusinessData3
    - ✓ class-default

Figure 2.8: List of tests associated with the Router Services layer

2.4.1 Class Mapping Test

Classifying network traffic allows you to organize traffic (that is, packets) into traffic classes or categories on the basis of whether the traffic matches specific criteria. Classifying network traffic is the foundation for enabling other QoS features such as traffic shaping and traffic policing on your network. High-priority network traffic or traffic matching specific criteria can be singled out for special handling, and thus, help to achieve peak application performance.

The goal of network traffic classification is to group traffic based on user-defined criteria so that the resulting groups of network traffic can then be subjected to specific QoS treatments. The QoS treatments might include faster forwarding by intermediate routers and switches or reduced probability of the traffic being dropped due to lack of buffering resources.

The network traffic can be classified using the following steps:

- Creating a Class Map for Classifying Network Traffic
- Creating a Policy Map for Applying a QoS Feature to Network Traffic
- Attaching the Policy Map to an Interface

If a class map is not created successfully, then the network traffic classification may not be defined as expected and the traffic cannot be matched to a specific class. Similarly, if the class map handles too much of traffic, then the performance of the application may degrade drastically. To avoid performance degradation, it is necessary to monitor the traffic on each class map so that the class map that is handling excessive traffic can be figured out. The **Class Mapping** Test helps administrators to monitor the network traffic specified for each class map.

This test auto-discovers the class maps on the target Cisco Router and for each class map, monitors the amount of data transmitted/ received. This test also helps administrators figure out the packets transmitted through each class map and identify data drops instantly.

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 the desired **Component type**, set *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.

Target of the test : A Cisco device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every source host.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.

Parameter	Description
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the snmpversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP **v3** protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the Username parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the context text box. By default, this parameter is set to *none*.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if v3 is selected as the snmpversion. From the authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
Encryptflag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by

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

Parameter	Description
	measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Received data	Indicates the amount of data received on this class map.	MB	Compare the value of these measures against the class maps to figure out the class map that is busy processing data.
Transmitted data	Indicates the amount of data transmitted through this class map.	MB	
Bit rate prior to apply policy	Indicates the bit rate captured prior to applying the QoS policy on this class map during the last measurement period.	Kbps	
Bit rate post policy apply	Indicates the bit rate captured after applying the QoS policy on this class map during the last measurement period.	Kbps	
Total packets	Indicates the total number of packets transmitted from this class map.	Packets	
Dropped packets	Indicates the number of packets dropped during transmission from this class map.	Packets	Ideally, the value of this measure should be zero.
Dropped data	Indicates the amount of data dropped during transmission from this class map.	MB	A low value is desired for this measure.
Drop rate	Indicates the rate at which data was dropped during transmission from this class map during the last measurement period.	Kbps	A high value indicates that there is too much of data loss during transmission.

2.4.2 BGP Neighbor Test

BGP (Border Gateway Protocol) is an interdomain routing protocol designed to provide loop-free routing links between separate routing domains that contain independent routing policies (autonomous systems). BGP is designed to run over a reliable transport protocol; it uses TCP (port 179) as the transport protocol because TCP is a connection-oriented protocol. BGP uses a router ID to identify BGP-speaking peers. The BGP router ID is a 32-bit value that is often represented by an IPv4 address. The BGP router ID must be unique to the BGP peers in a network. A BGP-speaking device does not discover another BGP-speaking device automatically. A network administrator usually manually configures the relationships between BGP-speaking devices. A peer device is a BGP-speaking device that has an active TCP connection to another BGP-speaking device. This relationship between BGP devices is often referred to as a neighbor. When a TCP connection is established between peers, each BGP peer initially exchanges all its routes - the complete BGP routing table - with the other peer.

This test auto-discovers the BGP neighbors connected to the target Cisco Router and for each BGP neighbor, reports the current status and the messages transmitted and received through each BGP neighbor. This way, administrators may be alerted to the BGP neighbor that is busy processing messages.

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 the desired **Component type**, set *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.

Target of the test : A Cisco device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every source host.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your

Parameter	Description
	environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the snmpversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP **v3** protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the Username parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the context text box. By default, this parameter is set to *none*.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if v3 is selected as the snmpversion. From the authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
Encryptflag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.

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

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current status of this BGP neighbor.</td><td></td><td>BGP forms a TCP session with neighbor routers called peers. BGP uses the Finite State Machine (FSM) to maintain a table of all BGP peers and their operational status.
The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Idle</td><td>1</td></tr>
<tr><td>Connect</td><td>2</td></tr>
<tr><td>Active</td><td>3</td></tr>
<tr><td>Open present</td><td>4</td></tr>
<tr><td>Open confirm</td><td>5</td></tr>
<tr><td>Established</td><td>6</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s listed in the table above to indicate the current status of each BGP neighbor. The graph of this measure however, is represented using the numeric equivalents only.</td></tr>
<tr><td>Message received</td><td>Indicates the number of messages received by this BGP neighbor.</td><td>Number</td><td rowspan="2">Comparing the value of these measure across the BGP neighbors will help you identify the BGP neighbor that is busy processing messages.</td></tr>
<tr><td>Message transmitted</td><td>Indicates the number of messages transmitted through this BGP neighbor.</td><td>Number</td></tr>
</table>

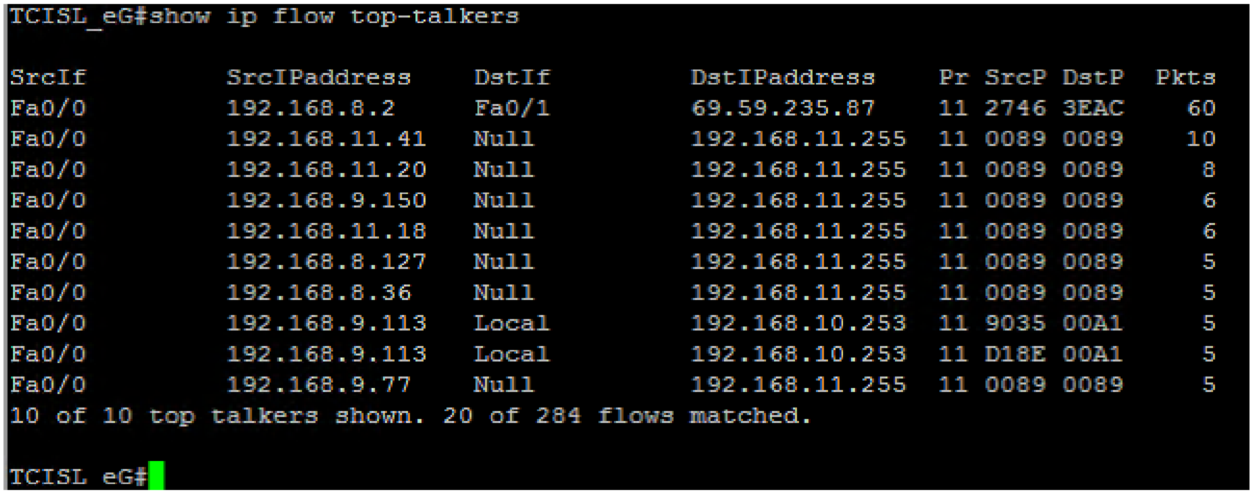
2.5 Troubleshooting FAQ

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

  One of the main reasons for the **Net flow 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 2.9, then the **Net Flows, Top Sources** and **Top Destinations** tests will report the required metrics.



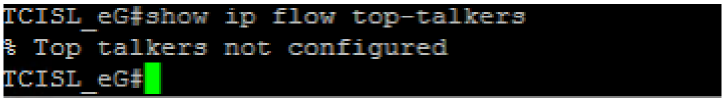
```
TCISL_eG#show ip flow top-talkers

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 2.9: The outputs when top talkers and Netflow is enabled perfectly

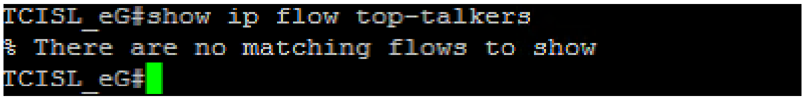
If the output as mentioned in Figure 2.10 appears, then you can clearly figure out that the Top talkers have not been configured properly. The tests will report metrics only when both the Netflow and Top talkers are configured and enabled properly.



```
TCISL_eG#show ip flow top-talkers
% Top talkers not configured
TCISL_eG#
```

Figure 2.10: The output showing that the top talkers are not configured properly

If the following output (see Figure 2.11) 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.



```
TCISL_eG#show ip flow top-talkers
% There are no matching flows to show
TCISL_eG#
```

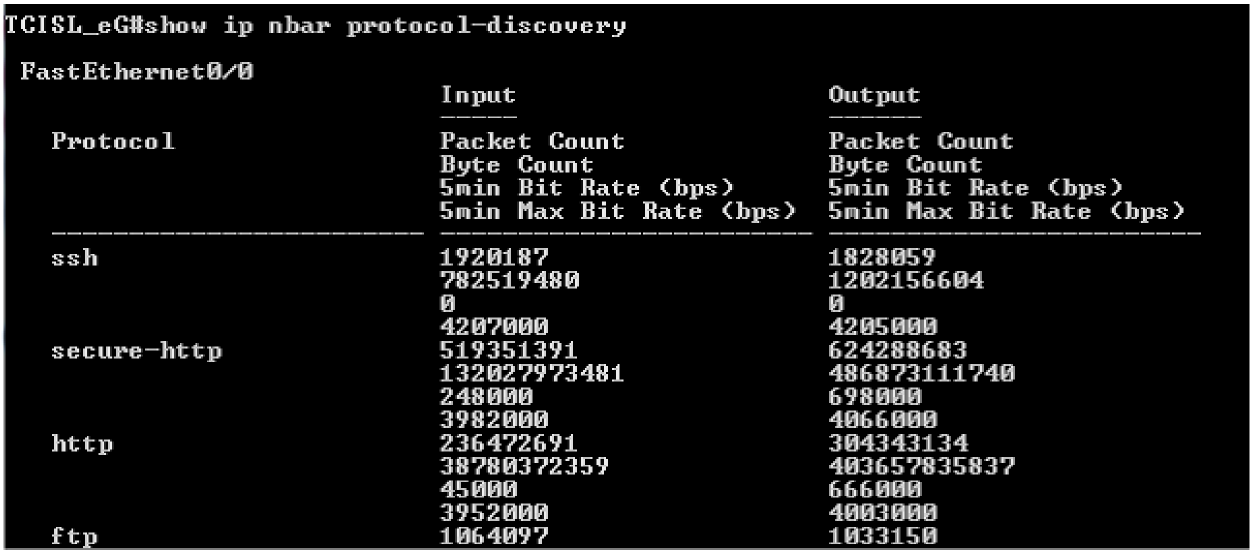
Figure 2.11: The output showing there are no top talkers

- **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 2.12 appears, then you can confirm that the NBAR protocol has been discovered successfully.



```
TCISL_eG#show ip nbar protocol-discovery

 FastEthernet0/0
                            Input                    Output
                            -----                    ------
   Protocol                 Packet Count             Packet Count
                            Byte Count               Byte Count
                            5min Bit Rate (bps)      5min Bit Rate (bps)
                            5min Max Bit Rate (bps)  5min Max Bit Rate (bps)
   ------------------------ ------------------------ ------------------------
   ssh                      1920187                  1828059
                            782519480                1202156604
                            0                        0
                            4207000                  4205000
   secure-http              519351391                624288683
                            132027973481             486873111740
                            248000                   698000
                            3982000                  4066000
   http                     236472691                304343134
                            38780372359              403657835837
                            45000                    666000
                            3952000                  4003000
   ftp                      1064097                  1033150
```

Figure 2.12: The output that appears upon successful NBAR protocol discovery

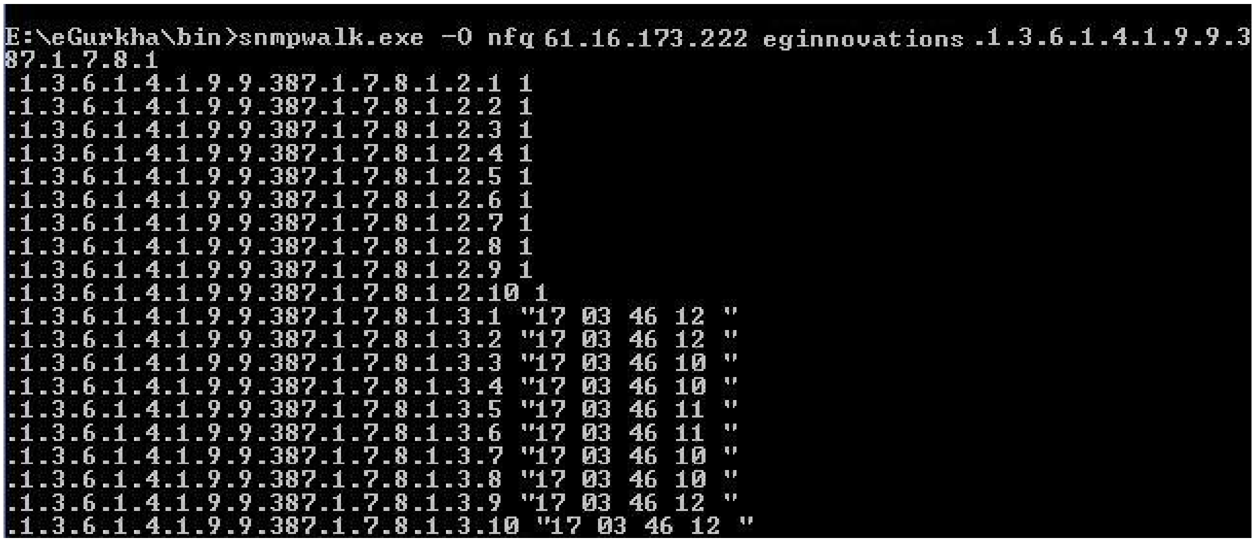
- **I don't have access to the Cisco Router that I wish to monitor. The Network engineer who manages the Cisco Router is informing me that the Netflow and Top Talkers features are enabled and configured. How can I cross verify if the features have indeed been enabled successfully?**

  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.

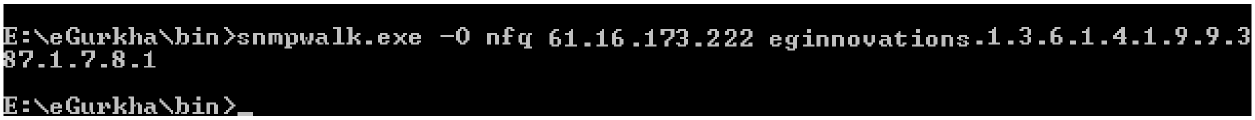
If the Netflow and Top Talkers features are enabled and configured properly, then the output as shown in Figure 2.13 will appear. **Remember that the output as shown in** Figure 2.13 **will appear only if Top Talkers are available**.



```
E:\eGurkha\bin>snmpwalk.exe -O nfq 61.16.173.222 eginnovations .1.3.6.1.4.1.9.9.3
87.1.7.8.1
.1.3.6.1.4.1.9.9.387.1.7.8.1.2.1 1
.1.3.6.1.4.1.9.9.387.1.7.8.1.2.2 1
.1.3.6.1.4.1.9.9.387.1.7.8.1.2.3 1
.1.3.6.1.4.1.9.9.387.1.7.8.1.2.4 1
.1.3.6.1.4.1.9.9.387.1.7.8.1.2.5 1
.1.3.6.1.4.1.9.9.387.1.7.8.1.2.6 1
.1.3.6.1.4.1.9.9.387.1.7.8.1.2.7 1
.1.3.6.1.4.1.9.9.387.1.7.8.1.2.8 1
.1.3.6.1.4.1.9.9.387.1.7.8.1.2.9 1
.1.3.6.1.4.1.9.9.387.1.7.8.1.2.10 1
.1.3.6.1.4.1.9.9.387.1.7.8.1.3.1 "17 03 46 12 "
.1.3.6.1.4.1.9.9.387.1.7.8.1.3.2 "17 03 46 12 "
.1.3.6.1.4.1.9.9.387.1.7.8.1.3.3 "17 03 46 10 "
.1.3.6.1.4.1.9.9.387.1.7.8.1.3.4 "17 03 46 10 "
.1.3.6.1.4.1.9.9.387.1.7.8.1.3.5 "17 03 46 11 "
.1.3.6.1.4.1.9.9.387.1.7.8.1.3.6 "17 03 46 11 "
.1.3.6.1.4.1.9.9.387.1.7.8.1.3.7 "17 03 46 10 "
.1.3.6.1.4.1.9.9.387.1.7.8.1.3.8 "17 03 46 10 "
.1.3.6.1.4.1.9.9.387.1.7.8.1.3.9 "17 03 46 12 "
.1.3.6.1.4.1.9.9.387.1.7.8.1.3.10 "17 03 46 12 "
```

Figure 2.13: 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 2.14.



```
E:\eGurkha\bin>snmpwalk.exe -O nfq 61.16.173.222 eginnovations.1.3.6.1.4.1.9.9.3
87.1.7.8.1

E:\eGurkha\bin>_
```

Figure 2.14: The output that appears when top talkers are not available/not configured

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.