Monitoring 3Com Switch

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The “smart” voice-ready 3Com® Baseline Switch Plus Family delivers Layer 2 enterprise-class Gigabit switching solutions, customized and priced for small and mid-sized organizations. These managed switches offer tremendous value to small and medium businesses looking for a low cost solution who need a level of control over their network not offered by unmanaged switching products, without sacrificing the advanced functionality normally found on higher-end managed switching products.

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

Any issues with the switch could be the possible source of critical problems like abnormal temperature, high resource utilization, or unauthorized user access! To avoid such issues, the performance of the 3Com Switch has to be monitored 24 *7. The eG Enterprise Suite helps network administrators to continuously monitor the 3Com Switches in the target environment.

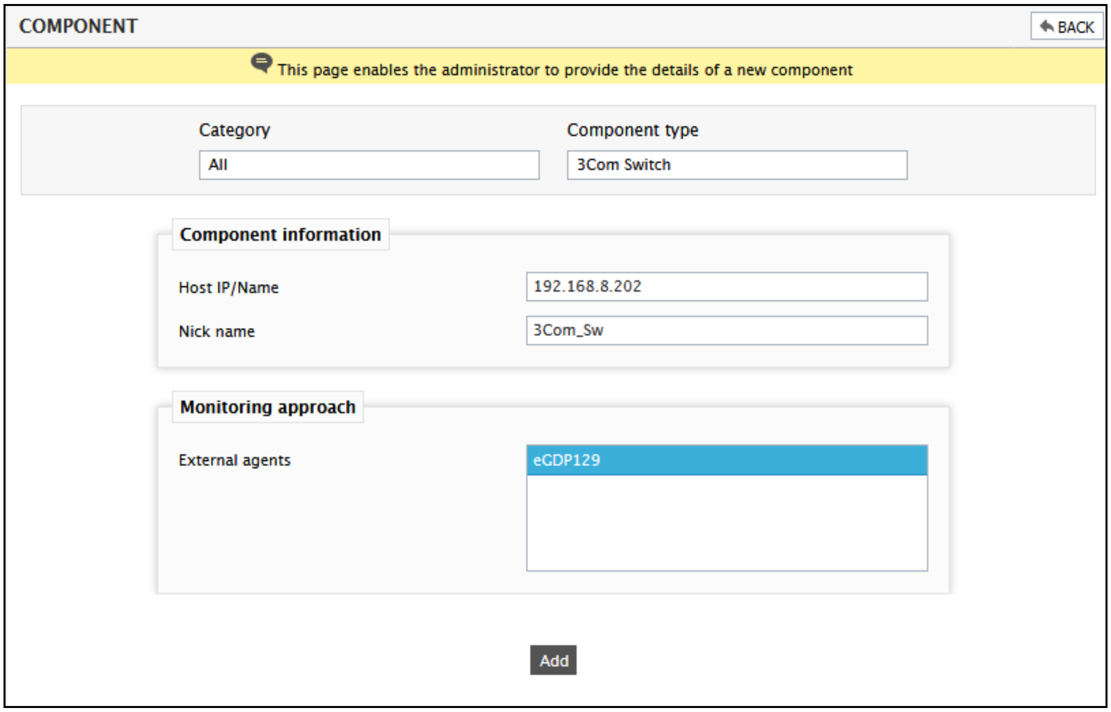
Chapter 2: How to Monitor 3Com Switch Using eG Enterprise?

eG Enterprise monitors the 3Com Switch using an eG external agent on a remote host. This eG agent polls the SNMP MIB of the switch to gather the statistics related to the 3Com Switch at configured intervals. Before attempting to monitor the 3Com switch, ensure that the switch is SNMP-enabled.

2.1 Managing the 3Com Switch

The eG Enterprise cannot automatically discover the 3Com Switch. This implies that you need to manually add the component for monitoring using eG administrative interface. Remember that the components added manually will be automatically managed by eG Enterprise. To manage a 3Com Switch component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENTS** page that appears next, select *3Com Switch* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.



COMPONENT

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

Category: All

Component type: 3Com Switch

Component information

Host IP/Name: 192.168.8.202

Nick name: 3Com_Sw

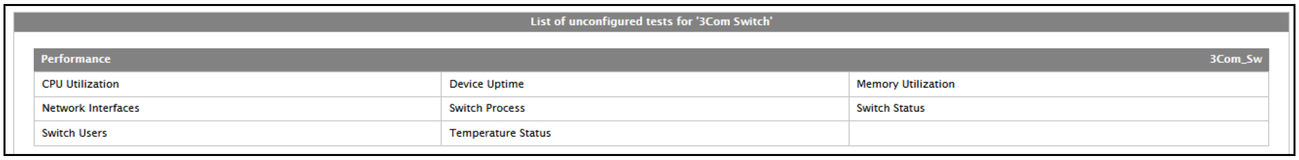
Monitoring approach

External agents: eGDP129

Figure 2.1: Adding a 3Com Switch

4. Specify **Host IP/Name** and **Nick name** for the 3Com Switch component (see Figure 2.1). Then, click on the **Add** button to register the changes.

5. When you attempt to sign out, a list of unconfigured tests appears (see Figure 2.2).

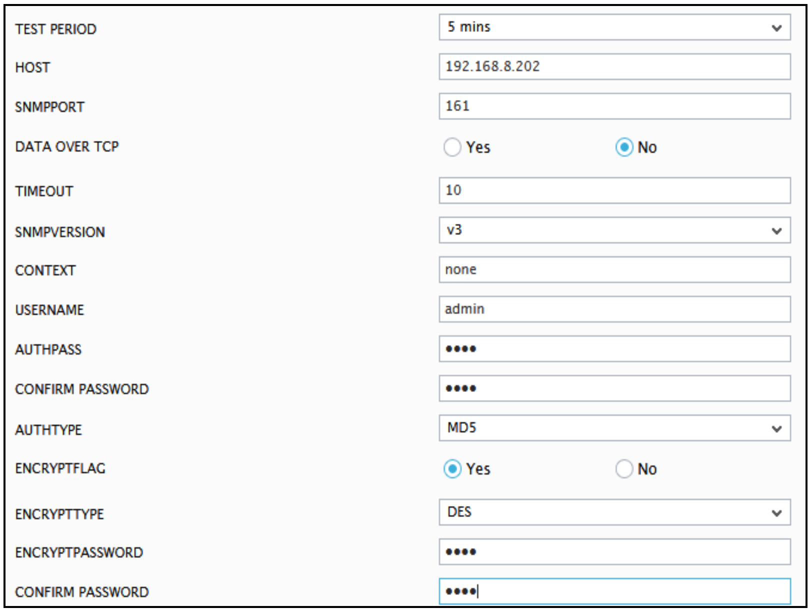


List of unconfigured tests for '3Com Switch'

Performance		3Com_Sw
CPU Utilization	Device Uptime	Memory Utilization
Network Interfaces	Switch Process	Switch Status
Switch Users	Temperature Status	

Figure 2.2: A list of unconfigured tests

6. Click on any test in the list of unconfigured tests. For instance, click on the **CPU Utilization** test to configure it. In the page that appears, specify the parameters as shown in Figure 2.3.



TEST PERIOD	5 mins
HOST	192.168.8.202
SNMPPORT	161
DATA OVER TCP	○ Yes ● No
TIMEOUT	10
SNMPVERSION	v3
CONTEXT	none
USERNAME	admin
AUTHPASS	••••
CONFIRM PASSWORD	••••
AUTHTYPE	MD5
ENCRYPTFLAG	● Yes ○ No
ENCRYPTTYPE	DES
ENCRYPTPASSWORD	••••
CONFIRM PASSWORD	••••

Figure 2.3: Configuring the CPU Utilization test

7. To know how to configure these parameters, refer to **Monitoring the 3Com Switch** chapter.
8. Once all the tests are configured, signout of the administrative interface.

Chapter 3: Monitoring the 3Com Switch

eG Enterprise offers a dedicated 3Com Switch monitoring model which periodically checks the data traffic to and from each network interface of the switch, the temperature and voltage of each module of the switch, the resource utilization etc, so that abnormalities can be detected before any irreparable damage occurs.

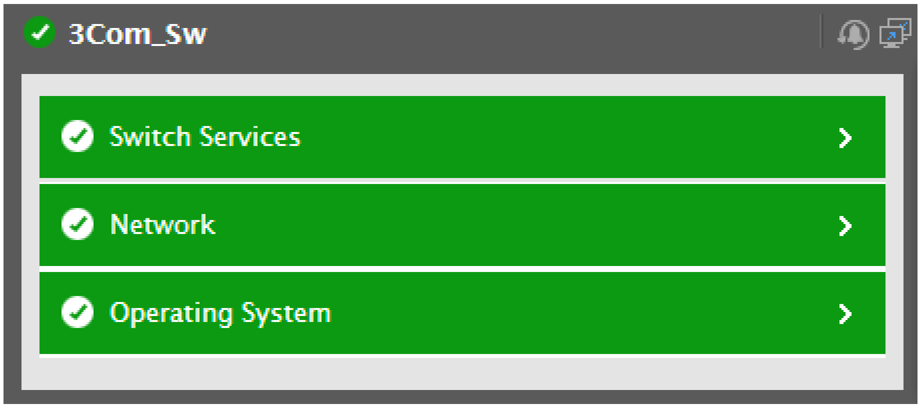


Figure 3.1: The layer model of the 3Com Switch

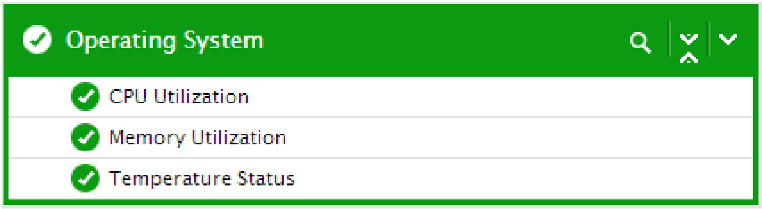
Every layer of Figure 3.1 is mapped to a variety of tests which connect to the SNMP MIB of the target 3Com Switch to collect critical statistics pertaining to its performance. The metrics reported by these tests enable administrators to answer the following questions:

- How well the CPU is utilized?
- How well the memory of the target 3Com Switch is utilized?
- What is the current temperature of the 3Com switch?
- How well each process executing on the 3Com Switch is utilizing the CPU resources? Which process is utilizing the maximum amount of CPU resources?
- How many users are currently in the active state?
- How many blocked users are trying to use the target 3Com Switch?

The sections to come will discuss each layer of Figure 3.1 in detail.

3.1 The Operating System Layer

Using this layer, administrators can figure out the CPU and memory utilization of the 3Com Switch. The temperature of the switch is also closely monitored and reported.



Operating System

CPU Utilization

Memory Utilization

Temperature Status

Figure 3.2: The tests associated with the Operating System layer

Let us discuss each test associated with this layer in the following sections.

3.1.1 CPU Utilization Test

One of the probable reasons for the poor performance of the 3COM switch is excessive CPU usage. Administrators should hence continuously track how well the switch utilizes CPU resources, so that abnormal usage patterns can be proactively detected and corrected to ensure peak performance of the switch. This CPU usage check can be performed using the **CPU Utilization** test. At configured intervals, this test monitors the current and maximum CPU usage levels of the switch and reports excessive usage (if any).

Target of the test : A 3Com Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for the 3Com Switch that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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 switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.

Parameter	Description
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the Authpass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **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
Current usage	Indicates the percentage of CPU that is currently used by the switch.	Percent	Ideally, the value should be low. An unusually high value or a consistent increase in this value is indicative of abnormal CPU usage which requires further investigation.
Maximum usage	Indicates the maximum percentage of the CPU used by the switch.	Percent	

3.1.2 Memory Utilization Test

This test monitors the memory utilization of the 3Com switch and proactively alerts administrators to potential resource contentions.

Target of the test : A 3Com Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target 3Com switch that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the host that is being monitored.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified Username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:

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
Total memory	Indicates the total amount of memory configured for the switch.	MB	
Free memory	Indicates the amount of memory that is currently available for use.	MB	A sudden decrease in this value could indicate an unexpected/sporadic spike in the memory utilization of the system.

Measurement	Description	Measurement Unit	Interpretation
			A consistent decrease however could indicate a gradual, yet steady erosion of memory resources, and is hence a cause for concern.
Memory usage	Indicates the percentage of memory that is utilized by the switch.	Percent	A value close to 100 indicates that the memory utilization is at its peak. Administrators may therefore be required to add additional memory resources to the switch.

3.1.3 Temperature Status Test

This test monitors the temperature of the target 3Com switch and alerts administrators to potential abnormalities, if any.

Target of the test : A 3Com switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target 3Com switch that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the host that is being monitored.
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 switch. 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

Parameter	Description
	3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified Username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Current temperature	Indicates the current temperature of the switch.	Celsius	Ideally, the value of this measure should be within the prescribed limits. A gradual/sudden increase in the value of this measure is a cause of concern which could eventually result in the failure of the switch.

3.2 The Switch Services layer

Using the tests mapped to this layer, administrators can figure out the process that is over utilizing the CPU resources of the target 3Com Switch and the count of active users and blocked users on the 3Com Switch.

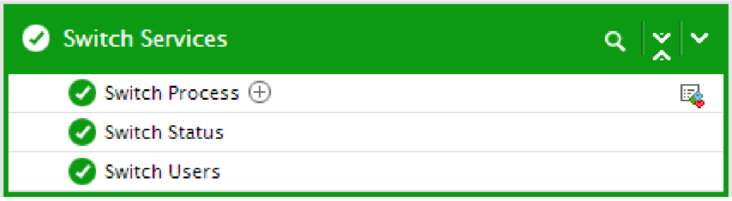


Figure 3.3: The tests associated with the Switch Services layer

Each test of this layer is discussed in detail in the forthcoming sections.

3.2.1 Switch Process Test

This test auto-discovers the processes running on the target 3Com switch and reports the percentage of CPU resources utilized by each process. Using this test, administrators can easily identify the process that is over-utilizing the CPU resources of the switch.

Target of the test : A 3Com Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each process executing on the target 3Com switch being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host that is being monitored.
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 switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An

Parameter	Description
	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.
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

Parameter	Description
	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**.
Show Process	By default, this flag is set to *All* indicating that all the processes executing on the target switch will be monitored. Sometimes administrators may want to monitor the processes which are in the busy state alone. This can be done by setting this flag to *Busy* option. This implies that the test will report the CPU busy measure only for the processes that are in the busy state.

Measurements made by the test

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

3.2.2 Switch Users Test

This test tracks the users who are currently active on the target 3Com switch and the users who were blocked on the switch. The detailed diagnosis of this test reveals the name of the users along with the privilege vested to each user. Using this detailed revelation, administrators can figure out any unauthorized access to the switch before the target environment is invaded by unauthorized users!

Target of the test : A 3Com Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target 3Com Switch being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host that is being monitored.
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 switch. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified Username and password into a 32-bit format to ensure security of SNMP

Parameter	Description
	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**.
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

Parameter	Description
	- 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
Active users	Indicates the number of users who are currently active on the switch.	Number	The detailed diagnosis of this measure reveals the name of the users who are active on the switch and the privilege level of each user.
Blocked users	Indicates the number of users who were blocked to access the switch.	Number	A sudden/gradual increase in the value of this measure may be a potential threat due to unauthorized users trying to access the switch. The detailed diagnosis of this measure reveals the name of the users who were blocked and the privilege level of each user.

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.