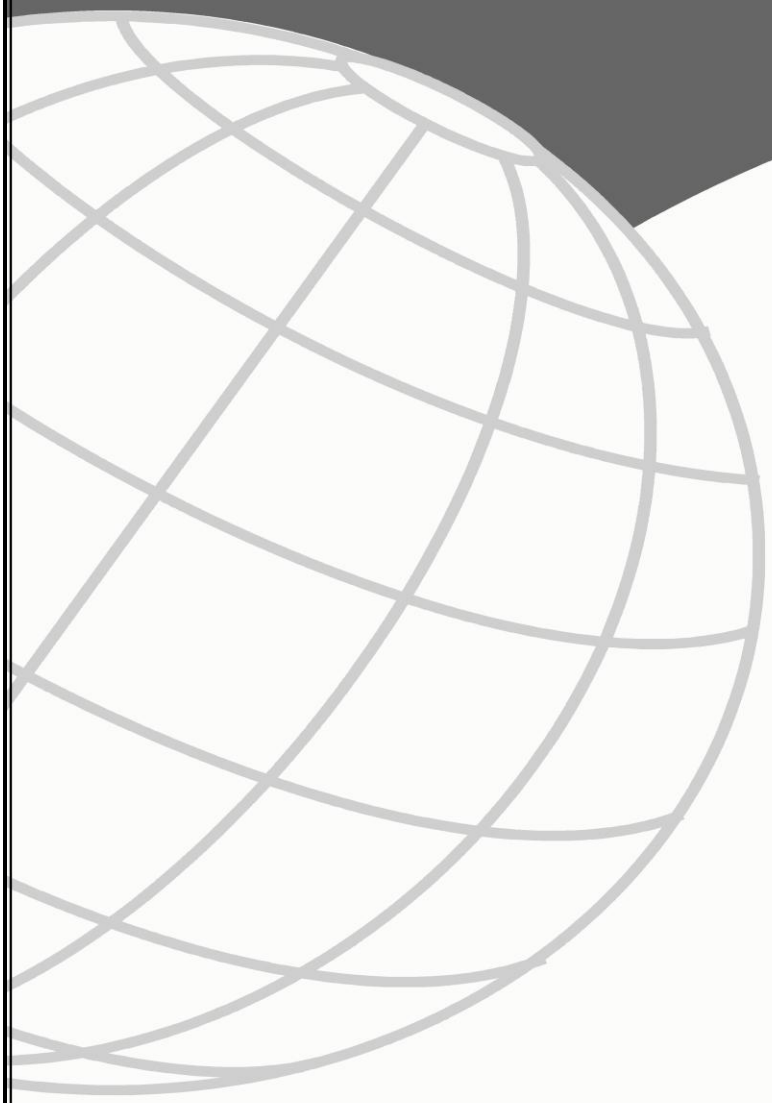


# Monitoring Coyote Point Equalizers

## eG Enterprise v6

**Restricted Rights Legend**

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

**Trademarks**

Microsoft Windows, Windows NT, Windows 2000, Windows 2003 and Windows 2008 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

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

**Copyright**

# Table of Contents

# Table of Figures

# 1

# Monitoring the Coyote Point Equalizer

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

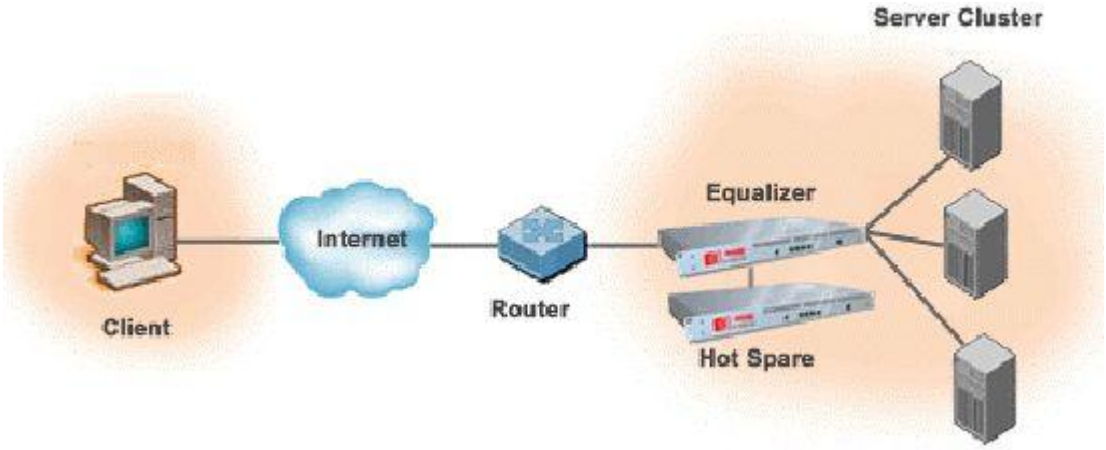


Figure 1.1: Typical deployment architecture of the Equalizer

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

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

eG Enterprise offers a specialized *Coyote Point Equalizer* (see Figure 1.2) monitoring model, which involves a single eG external agent that periodically polls the SNMP MIB of the equalizer, and collects a wide variety of performance information revealing the load on the device and the effectiveness with which the device balances this load across the servers in a farm. In the event of inconsistencies in load balancing, the agent proactively alerts administrators to the potential problem, so that he/she can initiate the relevant remedial action immediately.

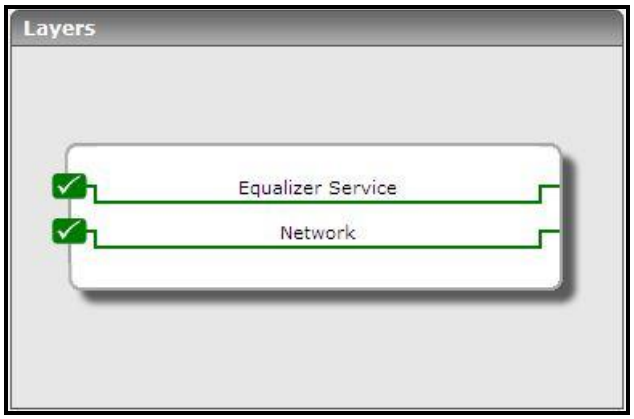


Figure 1.2: The layer model of the Coyote Point Equalizer

Each layer of Figure 1.2 above is mapped to tests that report the following:

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

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

## 1.1 The Network Layer

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

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


Figure 1.3: The tests mapped to the Network layer

Since all the tests displayed in Figure 1.3 have been dealt with extensively in the previous chapters, let us proceed to the next layer.

## 1.2 The Equalizer Service Layer

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

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

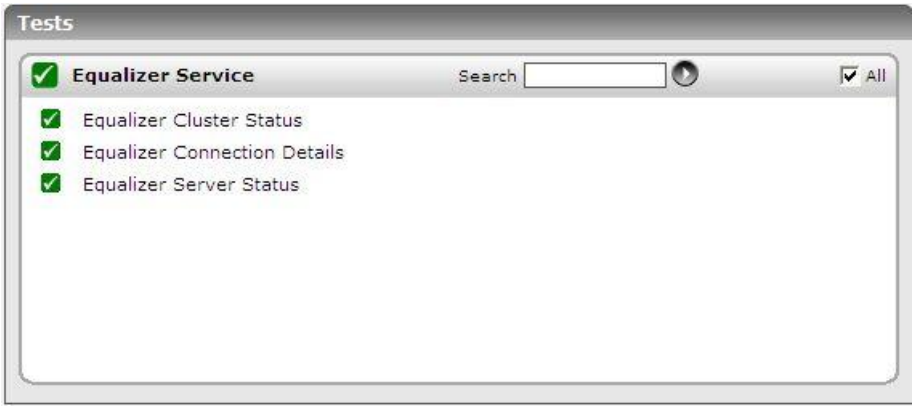


Figure 1.4: The tests mapped to the Equalizer Service layer

## 1.2.1 Equalizer Cluster Status Test

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

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

| | |
|---|---|
| **Purpose** | Reports the current load on the cluster and indicates how busy the servers in the cluster are |
| **Target of the test** | A Coyote Point Equalizer |
| **Agent deploying the test** | An external agent |
| **Configurable parameters for the test** | 1. **TESTPERIOD** – How often should the test be executed<br>2. **HOST** – The IP address of the equalizer<br>3. **PORT** – The port at which the equalizer listens; by default, this is NULL.<br>4. **SNMPPORT** – The port at which the equalizer exposes its SNMP MIB; the default is 161.<br>5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.<br>6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.<br>7. **USERNAME** – This parameter appears only when v3 is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the<br>8. 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.<br>9. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.<br>10. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.<br>11. **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:<br>➢ **MD5** – Message Digest Algorithm<br>➢ **SHA** – Secure Hash Algorithm |

<table>
<tr><td></td><td colspan="3">12. ENCRYPTFLAG – This flag appears only when v3 is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to No by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the Yes option.<br>13. ENCRYPTTYPE – If the encryptflag is set to Yes, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types:<br>➢ DES – Data Encryption Standard<br>➢ AES – Advanced Encryption Standard<br>14. ENCRYPTPASSWORD – Specify the encryption password here.<br>15. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.<br>16. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.<br>17. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the equalizer over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the each cluster managed by the target equalizer</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Cluster load:<br>Indicates the calculated load value for this cluster.</td><td>Number</td><td>This serves as a good indicator of the cluster workload. Comparing the value of this measure across clusters will enable you to identify those clusters that are overloaded.</td></tr>
<tr><td>Current connections:<br>Indicates the number of connections currently active on this cluster.</td><td>Number</td><td>This again serves as a good indicator of the cluster workload.</td></tr>
<tr><td>Total connections:<br>Indicates the total number of connections handled by this cluster.</td><td>Number</td><td></td></tr>
<tr><td></td><td>Throughput:<br>Indicates the rate of data traffic handled by this cluster over the last second.</td><td>MB/Sec</td><td></td></tr>
</table>

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

## 1.2.2 Equalizer Connection Details Test

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

| | |
|---|---|
| **Purpose** | Reports the connection load on the equalizer |
| **Target of the test** | A Coyote Point Equalizer |
| **Agent deploying the test** | An external agent |
| **Configurable parameters for the test** | 1. **TESTPERIOD** – How often should the test be executed<br>2. **HOST** – The IP address of the equalizer<br>3. **PORT** – The port at which the equalizer listens; by default, this is *NULL*.<br>4. **SNMPPORT** – The port at which the equalizer exposes its SNMP MIB; the default is 161.<br>5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.<br>6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.<br>7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.<br>8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned username. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.<br>9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. |

<table>
<tr><td></td><td colspan="3">10. AUTHTYPE – This parameter too appears only if v3 is selected as the SNMPVERSION. From the AUTHTYPE list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:<br>➢ MD5 – Message Digest Algorithm<br>➢ SHA – Secure Hash Algorithm<br>11. ENCRYPTFLAG – This flag appears only when v3 is selected as the SNMPVERSION. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to No by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the Yes option.<br>12. ENCRYPTTYPE – If the ENCRYPTFLAG is set to Yes, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types:<br>➢ DES – Data Encryption Standard<br>➢ AES – Advanced Encryption Standard<br>13. ENCRYPTPASSWORD – Specify the encryption password here.<br>14. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.<br>15. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds<br>16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the equalizer over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No..</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the equalizer being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Level4 total connections:<br>Indicates the number of L4 connections currently processed by the equalizer.</td><td>Number</td><td>This serves as a good indicator of the Level-4 connection load on the equalizer.<br>Level-4 load balancing is to distribute requests to the servers at transport layer, such as TCP, UDP and SCTP transport protocol. The load balancer distributes network connections from clients who know a single IP address for a service, to a set of servers that actually perform the work. Since connection must be established between client and server in connection-oriented transport before sending the request content, the load balancer usually selects a server without looking at the content of the request.</td></tr>
</table>

| | | | |
|---|---|---|---|
| | **Level4 peak connections:**<br>Indicates the high watermark of L4 connections processed by the equalizer. | Number | |
| | **Level4 idle timeout count:**<br>Indicates the number of L4 connections that timed out currently, because they were unused for a long time. | Number | Ideally, the value of this measure should be 0. A sudden/steady increase in this value could be a cause for concern. |
| | **Level7 active connections:**<br>Indicates the number of L7 connections currently active on the equalizer. | Number | Both these measures serve as effective pointers to the L7 connection workload on the equalizer.<br>Layer-7 load balancing, also known as application-level load balancing, is to parse requests in application layer and distribute requests to servers based on different types of request contents, so that it can provide quality of service requirements for different types of contents and improve overall cluster performance. The overhead of parsing requests in application layer is high, thus its scalability is limited, compared to layer-4 load balancing. This is turn implies that a very high value for this measure will be accompanied by a significant increase in the processing overheads, but will ensure improved cluster performance. |
| | **Level7 total connections:**<br>Indicates the total number of L7 connections to the equalizer. | Number | |
| | **Level7 peak connections:**<br>Indicates the high watermark of L7 connections to the equalizer. | Number | |

## 1.2.3 Equalizer Server Status Test

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

| | |
|---|---|
| **Purpose** | Monitors the connection and calculated load on each server in a cluster, promptly detects load imbalances, and alerts administrators to them, so that they can quickly resolve the issue |

| | |
|---|---|
| **Target of the test** | A Coyote Point Equalizer |
| **Agent deploying the test** | An external agent |
| **Configurable parameters for the test** | 1. **TESTPERIOD** – How often should the test be executed<br>2. **HOST** – The IP address of the equalizer<br>3. **PORT** – The port at which the equalizer listens; by default, this is NULL.<br>4. **SNMPPORT** – The port at which the equalizer exposes its SNMP MIB; the default is 161.<br>5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.<br>6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.<br>7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP **v3** protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.<br>8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned username. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.<br>9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.<br>10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the snmpversion. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP **v3** converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:**MD5** – Message Digest Algorithm<br>➢ **SHA** – Secure Hash Algorithm<br>11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.<br>12. **ENCRYPTTYPE** – If the encryptflag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP **v3** supports the following encryption types:<br>➢ **DES** – Data Encryption Standard<br>➢ **AES** – Advanced Encryption Standard |

| | | | |
|---|---|---|---|
| | 13. **ENCRYPTPASSWORD** – Specify the encryption password here.<br>14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.<br>15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.<br>16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**. | | |
| **Outputs of the test** | One set of results for each server in each cluster managed by the equalizer | | |
| **Measurements made by the test** | **Measurement** | **Measurement Unit** | **Interpretation** |
| | **Server load:**<br>Indicates the current calculated load value for this server. | Number | This indicates the workload on the server. By comparing the value of this measure across all the servers in a cluster, you can instantly identify irregularities in load balancing. If found necessary, you can reconfigure the load balancing rules to ensure uniform load distribution across servers. |
| | **Response time:**<br>Indicates how quickly this server is currently responding to client requests. | ms | It is the job of a load balancer to ensure minimal response time for client requests. A high value for this measure could therefore indicate a defective load balancer or one that is improperly configured. Further investigation is hence necessary in this case to identify the root-cause of the anomaly. |
| | **Current connections:**<br>Indicates the number of connections that were active on this server during the last measurement period. | Number | The indicates the connection load on the server. By observing the graph of this measure over time, you can analyze the rate of growth of the load on the server. By comparing the value of this measure across all the servers in a cluster, you can instantly identify overloaded servers; this in turn brings irregularities in load balancing to light. |
| | **Total connections:**<br>Indicates the number of current connections to this server. | Number | If a sudden/consistent increase in the value of this measure is noticed, you might have to investigate further to identify the reason for this occurrence. |
| | **Idle time:**<br>Indicates the time for which this server was idle. | Secs | Ideally, the value of this measure should be low. A high value indicates that the server has remained unused for a long time. This could be owing to inconsistencies in load balancing or because the server is unavailable for use. |

2

# Monitoring Coyote Load Balancer

One of the major enhancements in Coypte Point Equalizer version 10 is the introduction of server pools i.e., groups of servers can be assigned as a unit to an Equalizer virtual cluster (the IP address that presents website client content).

In previous versions of Coyote Point Equalizer, servers were assigned directly to clusters. So, if the same server needs to be included in multiple clusters, separate server definitions have to be created in each cluster thus causing server provisioning and modification time-consuming and error prone. But in version 10 and above, a server is created as a top-level Equalizer object and is then associated with a server pool, creating a server instance of that server in the server pool. The server definition contains the usual IP address, port, and other basic configuration information – while the server instance definition contains an initial server weight value and other options that specifies the server's behavior within the associated server pool.

To monitor the Coyote Point Equalizer of version 10 and above, eG Enterprise system has designed a specialized monitoring model (see Figure 2.1) using the *Coyote Load Balancer* component. An external agent periodically polls the SNMP MIBs of the Equalizer, and collects a wide range of performance metrics across servers, clusters and server pools of the equalizer. If there are any discrepancies found in the load balancing, the eG agent proactively alerts the administrators of any impending problem, thus helping the administrators to take necessary action immediately. .

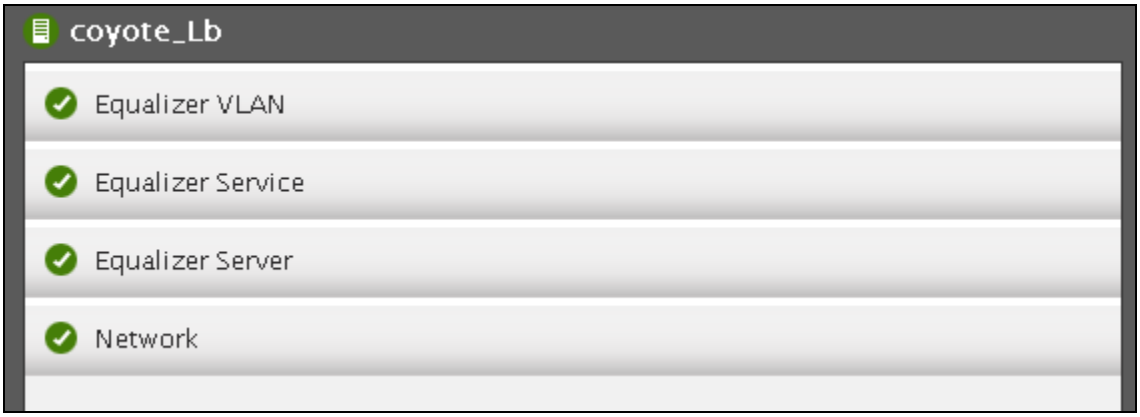


Figure 2.1: The layer model of the Coyote Load Balancer

Each layer of Figure 2.1 above is mapped to tests that report the following:

- How is the connection load on the equalizer? Is the equalizer able to handle the load?
- Which type of connections is the highest on the equalizer - Level-4 or Level-7?
- How many different cluster types s are being managed by the equalizer and how well those cluster types ar able to load balance? Is any cluster of a cluster type overloaded currently? If so, which one is it?
- Which cluster is currently handling the maximum number of connections?

- Which cluster is the busiest in terms of hits to its servers?
- How well the connections are handled by the server pool instances? Which server pool is handling the maximum number of connections?
- Is any server in the server pool currently overloaded? If so which server is overloaded at present?
- 
- Is the equalizer evenly distributing load across all the servers in the cluster, or is any server currently overloaded?
- Is the equalizer able to assure requests of quick responses from the servers, or is any server in the cluster responding slowly to client requests? Is it owing to a badly tuned equalizer?
- Are client connections to a cluster uniformly distributed across all the servers in that cluster? If not, what is the reason for the imbalance?
- Is any server in the cluster idle?

The **Network**, layer of the *Coyote Load Balancer* model is similar to that of a *Windows Generic* server model. Since these tests have been dealt with in the *Monitoring Unix and Windows Servers* document, let us discuss all the other layers in the forthcoming sections.

## 2.1 The Equalizer Server Layer

This layer tracks the connections, data traffic and compressed HTTP responses of each server. Figure 2.2 lists the tests that are currently mapped to the Equalizer Server layer.

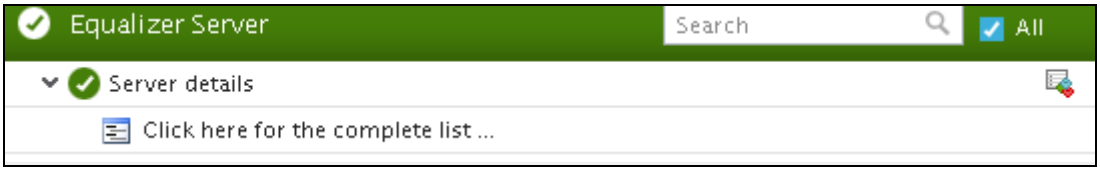


Figure 2.2: The tests mapped to the Equalizer Server layer

### 2.1.1 Server details Test

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

| | |
|---|---|
| **Purpose** | Monitors the connections, data traffic and compressed HTTP responses on each server in a cluster, promptly detects load imbalances, and alerts administrators to them, so that they can quickly resolve the issue. |
| **Target of the test** | A Coyote Load Balancer |
| **Agent deploying the test** | An external agent |

| | |
|---|---|
| **Configurable parameters for the test** | 1. **TEST PERIOD** - How often should the test be executed<br>2. **HOST** – The IP address of the Coyote Load Balancer<br>3. **SNMPPORT** – The SNMP Port number of the Coyote Load Balancer (161 typically)<br>4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.<br>5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.<br>6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.<br>7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.<br>8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.<br>9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:<br>➢ **MD5** – Message Digest Algorithm<br>➢ **SHA** – Secure Hash Algorithm<br>10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.<br>11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:<br>➢ **DES** – Data Encryption Standard<br>➢ **AES** – Advanced Encryption Standard<br>12. **ENCRYPTPASSWORD** – Specify the encryption password here.<br>13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.<br>14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. |

| | | | |
|---|---|---|---|
| | 15. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Coyote Load Balancer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**. | | |
| **Outputs of the test** | One set of results for each server on the Coyote Load Balancer that is to be monitored | | |
| **Measurements made by the test** | **Measurement** | **Measurement Unit** | **Interpretation** |
| | **Total connections:** Indicates the total number of connections to this server. | Number | If a sudden/consistent increase in the value of this measure is noticed, you might have to investigate further to identify the reason for this occurrence. |
| | **Active connections:** Indicates the number of connections that are currently active for this server. | Number | A high value is desired for this measure. This indicates the connection load on the server. By observing the graph of this measure over time, you can analyze the rate of growth of the load on the server. By comparing the value of this measure across all the servers in a cluster, you can instantly identify overloaded servers; this in turn brings irregularities in load balancing to light. |
| | **Connection usage:** Indicates the percentage of connections that are currently used by this server. | Percent | A high value is desired for this measure. This measure is the percentage ratio of *Active connections* mesure to the *Total Connections* measure. |
| | **Total transactions:** Indicates the total number of transactions processed by this server. | Number | |
| | **Data received:** Indicates the amount of data received by this server. | KB | Comparing the value of these measures across the servers will help you identify the server that is most busy in transmitting/receiving the data. This in turn, helps the administrators to determine the load on the server. |
| | **Data transmitted:** Indicates the amount of data transmitted through this server. | KB | |
| | **Current compressed HTTP responses:** Indicates the number of HTTP responses that were compressed by this server. | Number | |

| | | | |
|---|---|---|---|
| | **Total compressed HTTP responses:**<br>Indicates the number of HTTP responses that were compressed by this server since the start of the Coyote Load Balancer. | Number | |

## 2.2 The Equalizer Service Layer

This layer tracks the connections, data traffic and compressed HTTP responses for each cluster type and server pool and promptly alerts the administrators of any potential discrepancies. Apart from this, this layer also tracks the status and failover status of each peer in a failover cluster. Figure 7 lists the tests that are currently mapped to the Equalizer Service layer.

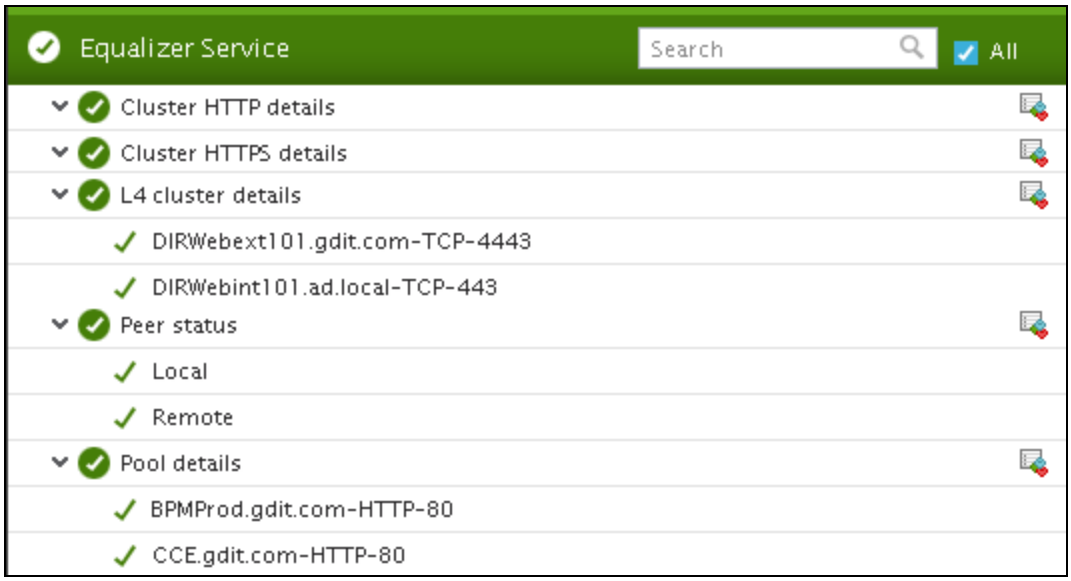


Figure 2.3: The tests mapped to the Equalizer Service layer

### 2.2.1 Peer status Test

When two Equalizers are configured into Active/Passive failover, they form a "failover pair". An Equalizer in a failover pair is called a "peer". At any given time, only one of the Equalizers in a failover pair is actually servicing requests sent to the cluster IP addresses defined in the configuration -- this unit is called the "active peer" or the "current primary" Equalizer in the failover pair. The other Equalizer, called the "passive peer" or "current backup", does not process any client requests.

Both units continually send "heartbeat probes" or "failover probes" to one another. If the current primary does not respond to heartbeat probes, a failover occurs. In this scenario the current backup Equalizer assumes the primary role by assigning the cluster IP addresses to its network interfaces and begins processing cluster traffic.

Administrators may constantly wish to be alerted on the status of the Coyote Load Balacer peer so that they can easily identify the peer that has taken over as the primary. The **Peer status** test helps you identify this. Using this test, administrators can figure out the current state of the peer, the failover state of the peer and the failover mode. This way, administrators may be able to constantly track the peer that has taken over as the primary, if failover occurs.

| | |
|---|---|
| **Purpose** | Helps you figure out the current state of the peer, the failover state of the peer and the failover mode |
| **Target of the test** | A Coyote Load Balancer |
| **Agent deploying the test** | An external agent |

| | |
|---|---|
| **Configurable parameters for the test** | 1. **TEST PERIOD** - How often should the test be executed<br>2. **HOST** – The IP address of the Coyote Load Balancer<br>3. **SNMPPORT** – The SNMP Port number of the Coyote Load Balancer (161 typically)<br>4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.<br>5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.<br>6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.<br>7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.<br>8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.<br>9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:<br>➢ **MD5** – Message Digest Algorithm<br>➢ **SHA** – Secure Hash Algorithm<br>10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.<br>11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:<br>➢ **DES** – Data Encryption Standard<br>➢ **AES** – Advanced Encryption Standard |

<table>
<tr><td></td><td colspan="3">12. ENCRYPTPASSWORD – Specify the encryption password here.<br>13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.<br>14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.<br>15. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Coyote Load Balancer over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each peer of the Coyote Load Balancer that is to be monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Peer state:<br>Indicates the current state of this peer.</td><td></td><td>The value that this measure can report and the corresponding numeric equivalent are mentioned in the table below:<br><table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Heartbeating</td><td>0</td></tr></table><br>  <br>Note<br>By default, this measure reports the Measure Value discussed above to indicate the current state of a peer. In the graph of this measure however, states are represented using the numeric equivalents only.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Peer failover state:<br>Indicates the current failover state of this peer.</td>
<td></td>
<td>The value that this measure can report and the corresponding numeric equivalent are mentioned in the table below:<br><br>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>FOSM Complete</td><td>0</td></tr>
</table>
<br>  <br>Note<br>By default, this measure reports the Measure Value discussed above to indicate the current failover state of a peer. In the graph of this measure however, states are represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Peer failover mode:<br>Indicates the current failover mode of this peer.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric equivalents are mentioned in the table below:<br><br>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Primary</td><td>0</td></tr>
<tr><td>Backup</td><td>1</td></tr>
</table>
<br>  <br>Note<br>By default, this measure reports the Measure Values discussed above to indicate the current failover mode of a peer. In the graph of this measure however, states are represented using the numeric equivalents only.</td>
</tr>
</table>

## 2.2.2 Cluster HTTP details Test

A virtual cluster is a collection of server pools with a single network-visible IP address. All client requests come into Equalizer through a cluster IP address, and are routed by Equalizer to an appropriate server, according to the load balancing options set on the cluster. A cluster is defined after determining the IP addresses for use by the cluster and the Cluster types appropriate for the target configuration. There are five different cluster types that are supported by the Coyote Load Balancer. They are:

- Layer 4 TCP cluster
- Layer 7 TCP cluster

- Layer 4 UDP cluster
- Layer 7 HTTP cluster
- Layer 7 HTTPS cluster

This test monitors the connections, data traffic, compressed data traffic and compressed HTTP responses for each HTTP cluster i.e., the cluster based on the HTTP protocol. Using the metrics of this test, administrators can promptly detect load imbalances and quickly resolve the issue before any serious discrepancies occur.

| | |
|---|---|
| **Purpose** | Monitors the connections, data traffic, compressed data traffic and compressed HTTP responses for each cluster based on the HTTP protocol |
| **Target of the test** | A Coyote Load Balancer |
| **Agent deploying the test** | An external agent |

| | |
|---|---|
| **Configurable parameters for the test** | 1. **TEST PERIOD** - How often should the test be executed<br>2. **HOST** – The IP address of the Coyote Load Balancer<br>3. **SNMPPORT** – The SNMP Port number of the Coyote Load Balancer (161 typically)<br>4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.<br>5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.<br>6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.<br>7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.<br>8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.<br>9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:<br>➢ **MD5** – Message Digest Algorithm<br>➢ **SHA** – Secure Hash Algorithm<br>10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.<br>11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:<br>➢ **DES** – Data Encryption Standard<br>➢ **AES** – Advanced Encryption Standard |

<table>
<tr><td></td><td colspan="3">12. ENCRYPTPASSWORD – Specify the encryption password here.<br>13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.<br>14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.<br>15. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Coyote Load Balancer over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each cluster of the Coyote Load Balancer that is to be monitored</td></tr>
<tr><td rowspan="6">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Total connections:<br>Indicates the total number of connections that are available for this HTTP cluster.</td><td>Number</td><td>If a sudden/consistent increase in the value of this measure is noticed, you might have to investigate further to identify the reason for this occurrence.</td></tr>
<tr><td>Active connections:<br>Indicates the number of connections that are currently active on this HTTP cluster.</td><td>Number</td><td>This measure indicates the connection load on the server. By observing the graph of this measure over time, you can analyze the rate of growth of the load on the server. By comparing the value of this measure across all the clusters, you can instantly identify overloaded clusters; this in turn brings irregularities in load balancing to light.</td></tr>
<tr><td>Connection usage:<br>Indicates the percentage of connections that were used by this HTTP cluster.</td><td>Percent</td><td></td></tr>
<tr><td>Total transactions:<br>Indicates the total number of transactions performed by this HTTP cluster.</td><td>Number</td><td></td></tr>
<tr><td>Data received:<br>Indicates the amount of data received by this HTTP cluster.</td><td>KB</td><td rowspan="2">Comparing the values of these measures across the clusters will help you identify the cluster that is the busiest in the Coyote Load Balancer. This in turn, helps the administrators to identify load balancing irregularities, if any.</td></tr>
<tr><td>Data transmitted:<br>Indicates the amount of data transmitted from this HTTP cluster.</td><td>KB</td></tr>
</table>

| | | | |
|---|---|---|---|
| | **Current compressed HTTP responses:**<br>Indicates the number of HTTP responses that were currently compressed by this HTTP cluster. | Number | |
| | **Total compressed HTTP responses:**<br>Indicates the total number of HTTP responses that wre compressed by this HTTP cluster sice the start of the Coyote Load Balancer. | Number | |
| | **Compressed data received:**<br>Indicates the amount of compressed data received by this HTTP cluster. | KB | Comparing the values of these measures across the clusters will help you identify the cluster that is the most busy cluster in terms of transmitting/receiving compressed data. This in turn, helps the administrators to identify load balancing irregularities, if any. |
| | **Compressed data transmitted:**<br>Indicates the amount of compressed data transmitted through this HTTP cluster. | KB | |

### 2.2.3 Cluster HTTPS details Test

This test monitors the connections, data traffic, compressed data traffic and compressed HTTP responses for each HTTPS cluster. Using the metrics of this test, administrators can promptly detect load imbalances and quickly resolve the issue before any serious discrepancies occur.

| | |
|---|---|
| **Purpose** | Monitors the connections, data traffic, compressed data traffic and compressed HTTP responses for each HTTPS cluster. |
| **Target of the test** | A Coyote Load Balancer |
| **Agent deploying the test** | An external agent |

| | |
|---|---|
| **Configurable parameters for the test** | 1. **TEST PERIOD** - How often should the test be executed<br>2. **HOST** – The IP address of the Coyote Load Balancer<br>3. **SNMPPORT** – The SNMP Port number of the Coyote Load Balancer (161 typically)<br>4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.<br>5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.<br>6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.<br>7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.<br>8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.<br>9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:<br>➢ **MD5** – Message Digest Algorithm<br>➢ **SHA** – Secure Hash Algorithm<br>10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.<br>11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:<br>➢ **DES** – Data Encryption Standard<br>➢ **AES** – Advanced Encryption Standard<br>12. **ENCRYPTPASSWORD** – Specify the encryption password here.<br>13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.<br>14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. |

| | | | |
|---|---|---|---|
| | 15. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Coyote Load Balancer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**. | | |
| **Outputs of the test** | One set of results for each HTTPS cluster of the Coyote Load Balancer that is to be monitored | | |
| **Measurements made by the test** | **Measurement** | **Measurement Unit** | **Interpretation** |
| | **Total connections:** Indicates the total number of connections to this HTTPS cluster. | Number | If a sudden/consistent increase in the value of this measure is noticed, you might have to investigate further to identify the reason for this occurrence. |
| | **Active connections**: Indicates the number of connections that are currently active on this HTTPS cluster. | Number | This measure indicates the connection load on the server. By observing the graph of this measure over time, you can analyze the rate of growth of the load on the server. By comparing the value of this measure across all the clusters, you can instantly identify overloaded clusters; this in turn brings irregularities in load balancing to light. |
| | **Connection usage:** Indicates the percentage of connections that were used by this HTTPS cluster. | Percent | |
| | **Total transactions:** Indicates the total number of transactions performed by this HTTPS cluster. | Number | |
| | **Data received:** Indicates the amount of data received by this HTTPS cluster. | KB | Comparing the values of these measures across the clusters will help you identify the cluster that is the busiest in the Coyote Load Balancer. This in turn, helps the administrators to identify load balancing irregularities, if any. |
| | **Data transmitted:** Indicates the amount of data transmitted from this HTTPS cluster. | KB | |

| | | | |
|---|---|---|---|
| | **Current compressed HTTPS responses:**<br>Indicates the number of HTTPS responses that were currently compressed by this HTTPS cluster. | Number | |
| | **Total compressed HTTPS responses:**<br>Indicates the total number of HTTPS responses that wre compressed by this HTTPS cluster sice the start of the Coyote Load Balancer. | Number | |
| | **Compressed data received:**<br>Indicates the amount of compressed data that is received by this HTTPS cluster. | KB | Comparing the values of these measures across the clusters will help you identify the cluster that is the most busy cluster in terms of transmitting/receiving compressed data. This in turn, helps the administrators to identify load balancing irregularities, if any. |
| | **Compressed data transmitted:**<br>Indicates the amount of compressed data that is transmitted through this HTTPS cluster. | KB | |

## 2.2.4 L4 cluster details Test

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

This test monitors the connections, data traffic, compressed data traffic and compressed HTTP responses for each L4 cluster. Using the metrics of this test, administrators can promptly detect load imbalances and quickly resolve the issue before any serious discrepancies occur.

| | |
|---|---|
| **Purpose** | Monitors the connections, data traffic, compressed data traffic and compressed HTTP responses for each L4 cluster |
| **Target of the test** | A Coyote Load Balancer |
| **Agent deploying the test** | An external agent |

| | |
|---|---|
| **Configurable parameters for the test** | 1. **TEST PERIOD** - How often should the test be executed<br>2. **HOST** – The IP address of the Coyote Load Balancer<br>3. **SNMPPORT** – The SNMP Port number of the Coyote Load Balancer (161 typically)<br>4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.<br>5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.<br>6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.<br>7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.<br>8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.<br>9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:<br>➢ **MD5** – Message Digest Algorithm<br>➢ **SHA** – Secure Hash Algorithm<br>10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.<br>11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:<br>➢ **DES** – Data Encryption Standard<br>➢ **AES** – Advanced Encryption Standard<br>12. **ENCRYPTPASSWORD** – Specify the encryption password here.<br>13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.<br>14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. |

| | | | |
|---|---|---|---|
| | 15. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Coyote Load Balancer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**. | | |
| **Outputs of the test** | One set of results for each L4 cluster of the Coyote Load Balancer that is to be monitored | | |
| **Measurements made by the test** | **Measurement** | **Measurement Unit** | **Interpretation** |
| | **Total connections:** Indicates the total number of connections to this L4 cluster. | Number | If a sudden/consistent increase in the value of this measure is noticed, you might have to investigate further to identify the reason for this occurrence. |
| | **Active connections**: Indicates the number of connections that are currently active on this L4 cluster. | Number | This measure indicates the connection load on the server. By observing the graph of this measure over time, you can analyze the rate of growth of the load on the server. By comparing the value of this measure across all the clusters, you can instantly identify overloaded clusters; this in turn brings irregularities in load balancing to light. |
| | **Connection usage:** Indicates the percentage of connections that were used by this L4 cluster. | Percent | A high value is desired for this measure. |
| | **Total transactions:** Indicates the total number of transactions performed by this L4 cluster. | Number | |
| | **Data received:** Indicates the amount of data received by this L4 cluster. | KB | Comparing the values of these measures across the clusters will help you identify the cluster that is the busiest in the Coyote Load Balancer. This in turn, helps the administrators to identify load balancing irregularities, if any. |
| | **Data transmitted:** Indicates the amount of data transmitted from this L4 cluster. | KB | |

## 2.2.5 Pool details Test

A server is attached to a cluster via a server pool. A server pool is a collection of server definitions, each of which has additional parameters assigned to it in the server pool -- these additional parameters are organized by the server's name and are referred to as server instances within the server pool context. This allows you to associate a distinct set of server instance options (weight, flags, maximum number of connections), to multiple instances of the same

real server in different server pools.

This test monitors the connections, data traffic, compressed data traffic and compressed HTTP responses for each server pool. Using the metrics of this test, administrators can promptly detect load imbalances and quickly resolve the issue before any serious discrepancies occur.

| | |
|---|---|
| **Purpose** | Monitors how well the licenses are managed by the OpenVPN Access server. |
| **Target of the test** | A Coyote Load Balancer |
| **Agent deploying the test** | An external agent |
| **Configurable parameters for the test** | 1. **TEST PERIOD** - How often should the test be executed<br>2. **HOST** – The IP address of the Coyote Load Balancer<br>3. **SNMPPORT** – The SNMP Port number of the Coyote Load Balancer (161 typically)<br>4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.<br>5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.<br>6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.<br>7. **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.<br>9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:<br>➢ **MD5** – Message Digest Algorithm<br>➢ **SHA** – Secure Hash Algorithm<br>10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. |

<table>
<tr><td></td><td colspan="3">11. ENCRYPTTYPE – If the ENCRYPTFLAG is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types:<br>➢ DES – Data Encryption Standard<br>➢ AES – Advanced Encryption Standard<br>12. ENCRYPTPASSWORD – Specify the encryption password here.<br>13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.<br>14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.<br>15. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Coyote Load Balancer over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each server pool of the Coyote Load Balancer that is to be monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Total connections:<br>Indicates the total number of connections that are available for this server pool.</td><td>Number</td><td>If a sudden/consistent increase in the value of this measure is noticed, you might have to investigate further to identify the reason for this occurrence.</td></tr>
<tr><td>Active connections:<br>Indicates the number of connections that are currently active on this server pool.</td><td>Number</td><td>This measure indicates the connection load on the server pool. By observing the graph of this measure over time, you can analyze the rate of growth of the load on the server. By comparing the value of this measure across all the clusters, you can instantly identify overloaded clusters; this in turn brings irregularities in load balancing to light.</td></tr>
<tr><td>Connection usage:<br>Indicates the percentage of connections that were used by this server pool.</td><td>Percent</td><td></td></tr>
<tr><td></td><td>Total transactions:<br>Indicates the total number of transactions performed by this server pool.</td><td>Number</td><td></td></tr>
</table>

| | | | |
|---|---|---|---|
| | **Data received:**<br>Indicates the amount of data received by this server pool. | KB | Comparing the values of these measures across the server pools will help you identify the server pool that is the busiest in the Coyote Load Balancer. This in turn, helps the administrators to identify load balancing irregularities, if any. |
| | **Data transmitted:**<br>Indicates the amount of data transmitted from this server pool. | KB | |
| | **Current compressed HTTP responses:**<br>Indicates the number of HTTP responses that were compressed by this server pool. | Number | |
| | **Total compressed HTTP responses:**<br>Indicates the total number of HTTP responses that were compressed by this server pool since the start of the Coyote Load Balancer. | Number | |
| | **Compressed data received:**<br>Indicates the amount of compressed data received by this server pool. | KB | Comparing the values of these measures across the server pool will help you identify the server pool that is the busiest in the Coyote Load Balancer. This in turn, helps the administrators to identify load balancing irregularities, if any. |
| | **Compressed data transmitted:**<br>Indicates the amount of compressed data transmitted through this server pool. | KB | |

## 2.3 The Equalizer VLAN Layer

This layer tracks the current status of the VLAN and the VLAN subnets. Figure 2.2 lists the tests that are currently mapped to the VLAN Status layer.


Figure 2.4: The tests mapped to the Equalizer VLAN layer

## 2.3.1 VLAN status Test

This test monitors the current state of each VLAN in the Coyote Load Balancer.

| | |
|---|---|
| **Purpose** | Continuously tracks the number of users who are currently connected to the server |
| **Target of the test** | A Coyote Load Balancer |
| **Agent deploying the test** | An external agent |

| | |
|---|---|
| **Configurable parameters for the test** | 1. **TEST PERIOD** - How often should the test be executed<br>2. **HOST** – The IP address of the Coyote Load Balancer<br>3. **SNMPPORT** – The SNMP Port number of the Coyote Load Balancer (161 typically)<br>4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.<br>5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.<br>6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.<br>7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.<br>8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.<br>9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:<br>➢ **MD5** – Message Digest Algorithm<br>➢ **SHA** – Secure Hash Algorithm<br>10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.<br>11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:<br>➢ **DES** – Data Encryption Standard<br>➢ **AES** – Advanced Encryption Standard |

<table>
<tr><td></td><td colspan="3">12. ENCRYPTPASSWORD – Specify the encryption password here.<br>13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.<br>14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.<br>15. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Coyote Load Balancer over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each VLAN of the Coyote Load Balancer that is to be monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>VLAN state:<br>Indicates the current state of this VLAN.</td><td></td><td>The value that this measure can report and the corresponding numeric equivalent are mentioned in the table below:<br><table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Heartbeating</td><td>0</td></tr></table><br>  <br>Note<br>By default, this measure reports the Measure Value discussed above to indicate the current state of a VLAN. In the graph of this measure however, states are represented using the numeric equivalents only.</td></tr>
</table>

## 2.3.2 VLAN subnet status Test

This test monitors the current subnet state of each VLAN in the Coyote Load Balancer.

| | |
|---|---|
| **Purpose** | Continuously tracks the number of users who are currently connected to the server |
| **Target of the test** | A Coyote Load Balancer |
| **Agent deploying the test** | An external agent |

| | |
|---|---|
| **Configurable parameters for the test** | 1. **TEST PERIOD** - How often should the test be executed<br>2. **HOST** – The IP address of the Coyote Load Balancer<br>3. **SNMPPORT** – The SNMP Port number of the Coyote Load Balancer (161 typically)<br>4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.<br>5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.<br>6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.<br>7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.<br>8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.<br>9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:<br>➢ **MD5** – Message Digest Algorithm<br>➢ **SHA** – Secure Hash Algorithm<br>10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.<br>11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:<br>➢ **DES** – Data Encryption Standard<br>➢ **AES** – Advanced Encryption Standard |

<table>
<tr><td></td><td colspan="3">12. ENCRYPTPASSWORD – Specify the encryption password here.<br>13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.<br>14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.<br>15. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Coyote Load Balancer over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each VLAN subnet of the Coyote Load Balancer that is to be monitored</td></tr>
<tr><td>Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td></td><td>Vlan substate:<br>Indicates the current subnet state of this VLAN.</td><td></td><td>The value that this measure can report and the corresponding numeric equivalent is mentioned in the table below:<br><table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Start</td><td>1</td></tr></table><br>  <br>Note<br>By default, this measure reports the Measure Value discussed above to indicate the current subnet state of a VLAN. In the graph of this measure however, states are represented using the numeric equivalents only.</td></tr>
</table>

3

# Conclusion

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

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