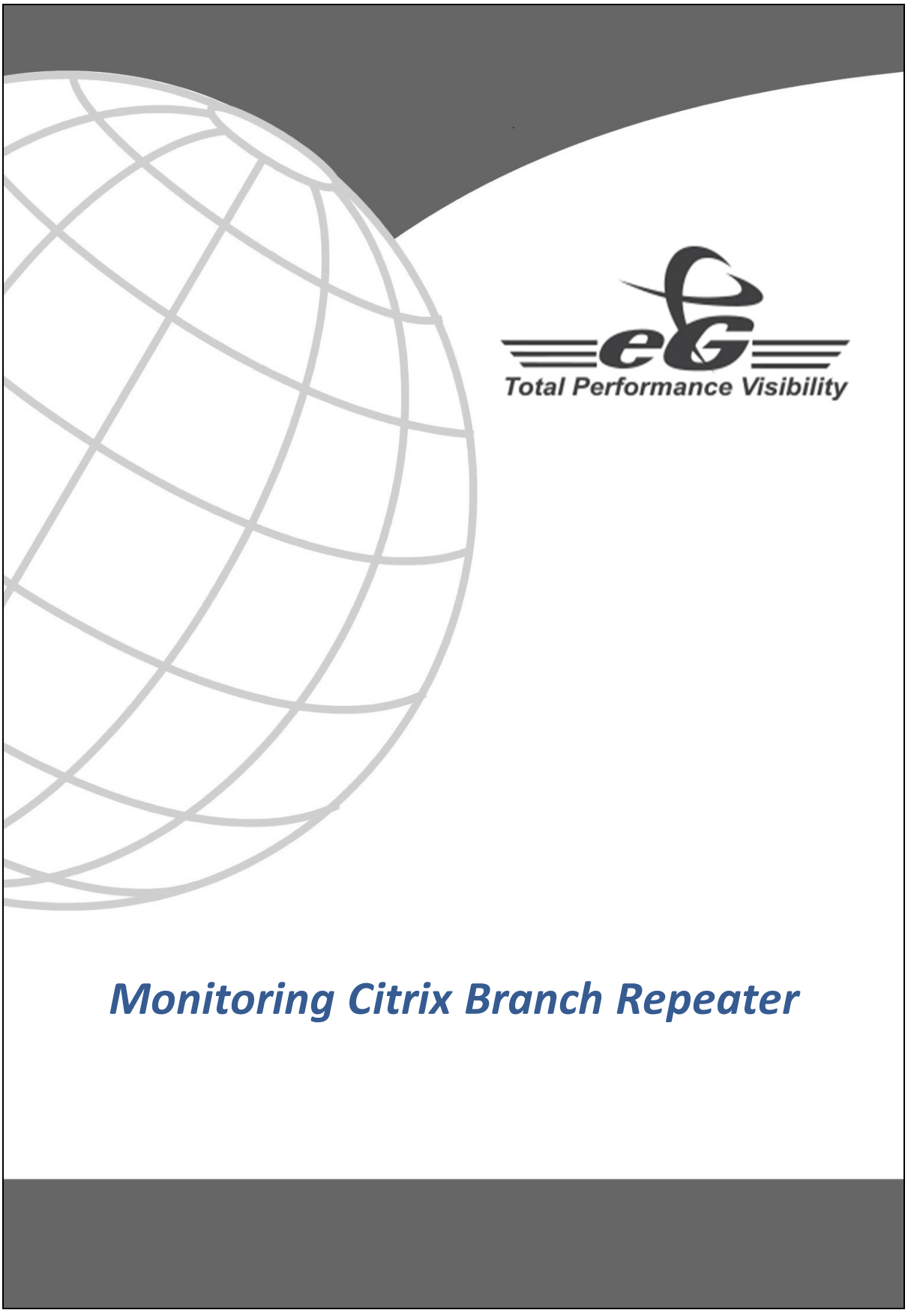


Monitoring Citrix Branch Repeater

Table of contents

INTRODUCTION 1

1.1 How does eG Enterprise Monitor the Citrix Branch Repeater? 4

ADMINISTERING EG MANAGER TO MONITOR CITRIX BRANCH REPEATER 8

THE CITRIX BRANCH REPEATER MONITORING MODEL 10

3.1 The Operating System Layer 10

3.1.1 CBR CPU Utilization Test 10

3.1.2 CBR Uptime Test 12

3.2 The Network Layer 15

3.3 The Branch Repeater App Layer 15

3.3.1 CBR Application Traffic Test 16

3.4 The Branch Repeater Service Layer 20

3.4.1 CBR Scaler Statistics Test 21

3.4.2 CBR Connection Status Test 26

3.4.3 CBR ICA Statistics Test 28

3.4.4 CBR Level Service Class Test 31

3.4.5 CBR Links Test 36

3.4.6 CBR Service Classes Test 41

3.4.7 CBR Quality of Service Test 45

CONCLUSION 50

Table of Figures

Figure 1.1: Inline deployment of the Citrix Branch Repeater 1
Figure 1.2: Virtual inline deployment of the Citrix Branch Repeater 1
Figure 1.3: ICA deployment option 2
Figure 1.4: The SSL deployment mode 2
Figure 1.5: The layer model of Citrix Branch Repeater 3
Figure 1.6: Logging in as admin 4
Figure 1.7: The web console of the Branch Repeater virtual appliance 5
Figure 1.8: Enabling features 5
Figure 1.9: Enabling SNMP 6
Figure 1.10: Configuring SNMP 6
Figure 2.1: Adding a Citrix Branch Repeater 8
Figure 2.2: List of Unconfigured tests to be configured for the Citrix Branch Repeater 9
Figure 3.1: The tests mapped to the Operating System layer 10
Figure 3.2: The tests mapped to the Network layer 15
Figure 3.3: The tests mapped to the Physical Storage layer 16
Figure 3.4: The tests mapped to the Branch Repeater Service layer 21
Figure 3.5: The QoS architecture 45

1

Introduction

Citrix® Branch Repeater™, available as a physical, virtual and a software (Repeater plug-in) appliance, is a service-centric WAN optimization solution that accelerates, controls and optimizes all services-desktops, applications, multi-media and more—for branch and mobile users while reducing IT costs.

How the branch repeater works depends upon how it has been deployed. In an inline deployment (see Figure 1.1), the Branch Repeater appliance uses an accelerated bridge (two Ethernet ports). Packets enter one Ethernet port and exit through the other. As far as the rest of the network is concerned, it is as if the Branch Repeater is not present, its operation is completely transparent.

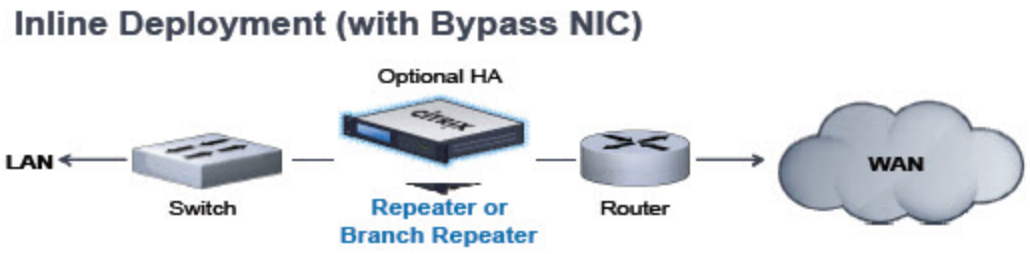


Figure 1.1: Inline deployment of the Citrix Branch Repeater

If inline deployment is not possible, the branch repeaters can be deployed through a virtual inline model. This is achieved via policy-based routing or WCCP redirection, such that traffic of particular types is sent to the branch repeaters of the organization.

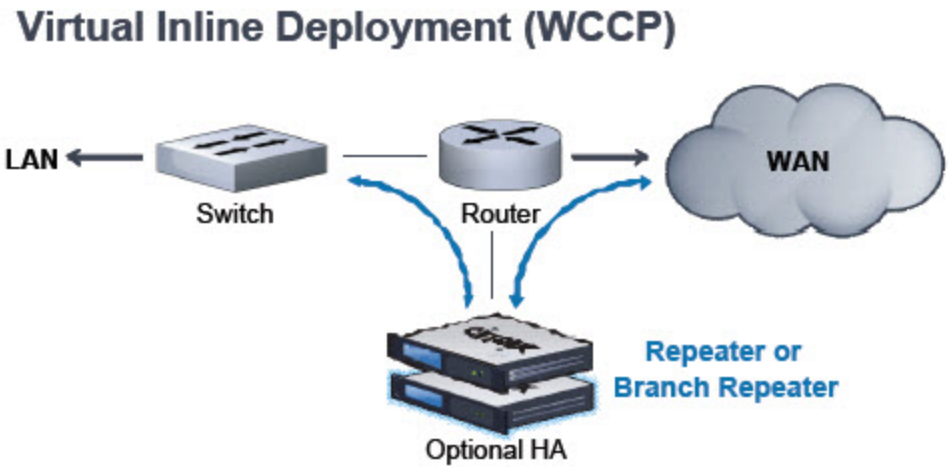


Figure 1.2: Virtual inline deployment of the Citrix Branch Repeater

Figure 1.3 shows the typical ICA deployment option. Typically, connectivity to different branch offices varies and WAN optimization may not be required for every site. This “mixed approach” is possible with the branch

repeater as the appliances detect each other automatically and apply optimization as necessary. However, in all cases there is end-to-end encryption traffic.

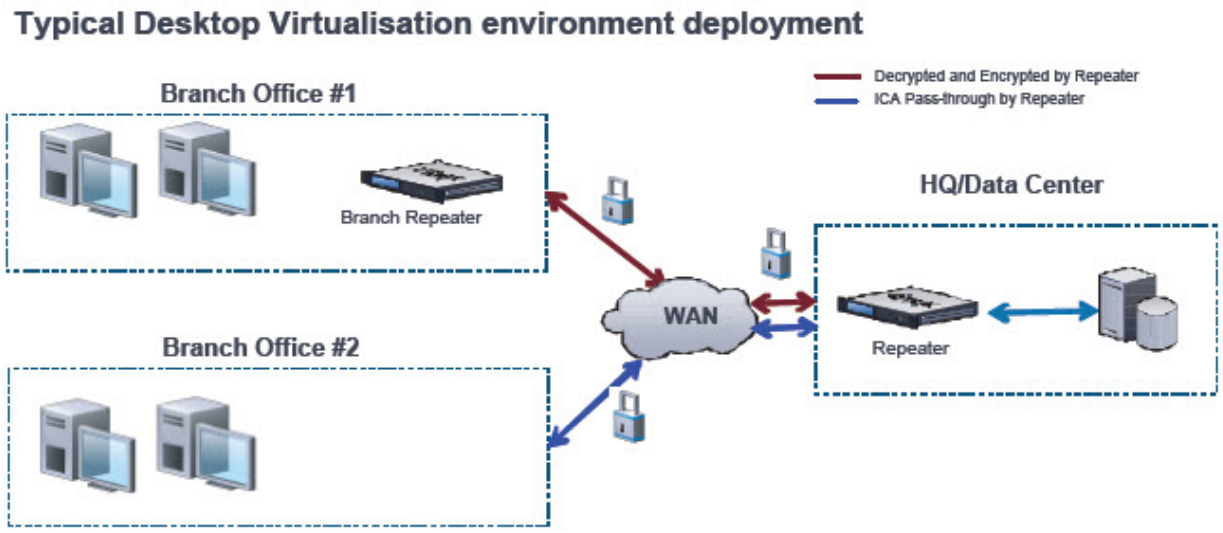


Figure 1.3: ICA deployment option

If deployed in the SSL deployment mode, the branch repeater can accelerate SSL traffic. It does this by splitting the connection into three encrypted segments: client to client appliance, appliance to appliance, and data center appliance to server. In general, the data center appliance masquerades as the server by hosting its security credentials, allowing it to act on the server's behalf.

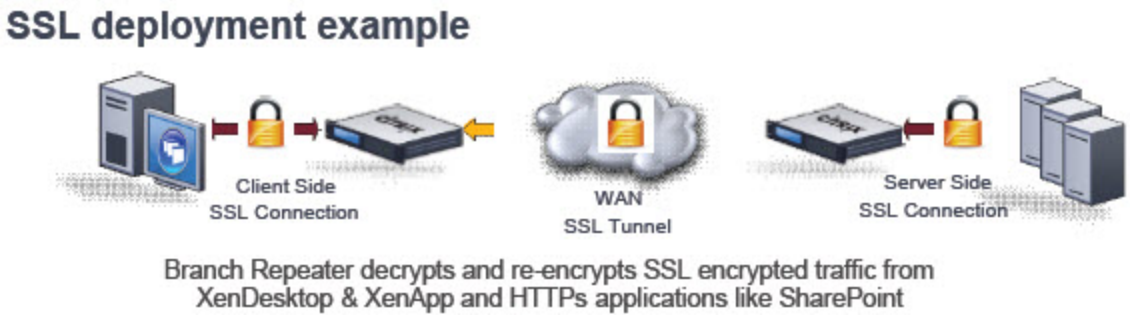


Figure 1.4: The SSL deployment mode

This way, the branch repeater enables server and desktop application virtualization services to be delivered quickly and efficiently to branch offices and mobile users over wide area networks (WAN). If these application users complain of slowness in access, administrators must be able to promptly and precisely pinpoint the root-cause of the slowness – is it the non-availability of the branch repeater? is it because of poorly configured QoS thresholds on the branch repeater? Or is it because of inefficient service class policies defined for the branch repeater? With businesses relying heavily on branch offices to serve customers, to be near partners and suppliers and to expand into new markets, any delay in isolating the source of performance problems with the branch repeater will automatically translate into business losses. If this is to be avoided, the overall performance of the branch repeater has to be continuously monitored and deviations from norms should be brought to the attention of administrators.

eG Enterprise provides a specialized *Citrix Branch Repeater* monitoring model that periodically checks application links, ICA traffic, QoS thresholds, and service class policies managed by the branch repeater, accurately points administrators to the problem areas – be it slow application links or latencies in processing ICA traffic – and helps them initiate and implement corrective action.

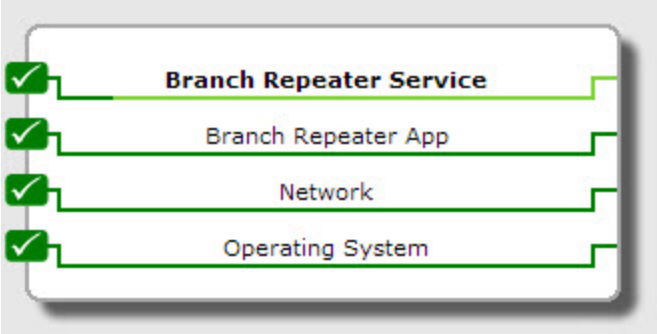


Figure 1.5: The layer model of Citrix Branch Repeater

Each layer of Figure 1.5 above is mapped to a variety of tests, each of which report a wealth of performance information related to the branch repeater. Using these metrics, administrators can find quick and accurate answers to the following performance queries:

- Is the branch repeater available over the network?
- Was the branch repeater rebooted recently?
- How much CPU is the branch repeater consuming?
- Is the accelerated application traffic using the link bandwidth optimally? If not, the traffic for which application is consuming bandwidth excessively?
- Have too many data packets been dropped due to QoS threshold violations? If so, which application has lost the maximum packets? Do the QoS thresholds for that application require fine-tuning?
- How is the load on the branch repeater?
- Is the branch repeater able to deliver a high compression ratio?
- Have too many connections been left unaccelerated by the branch repeater?
- Which ICA application is bandwidth-intensive? How well does the branch repeater accelerate traffic for this ICA application?
- Are the service classes configured in the branch repeater regulating traffic well or are WAN links governed by the service classes still consuming too much bandwidth? If so, which service class is an ineffective accelerator? Should that service class's configuration be reset?
- Are any WAN/LAN links handling more traffic than the bandwidth limit set for them? If so, which are those links?
- Which traffic shaping policies configured in the branch repeater are poor accelerators and require tweaking?

1.1 How does eG Enterprise Monitor the Citrix Branch Repeater?

To monitor the Citrix Branch Repeater, you need to make sure that the branch repeater is *SNMP-enabled*. Then, you need to deploy a single eG external agent on any remote host in the environment and configure that agent to periodically poll the SNMP MIB of the device to pull out metrics of interest.

To enable the SNMP service on the branch repeater, do the following:

1. Connect to the web console of the branch repeater virtual appliance using the URL: http://<IP_address_of_branch_repeater>/.
2. When the login screen depicted by Figure 1.6 appears, provide the credentials of the administrator to login.

Figure 1.6: Logging in as admin

3. Figure 1.7 will then appear.

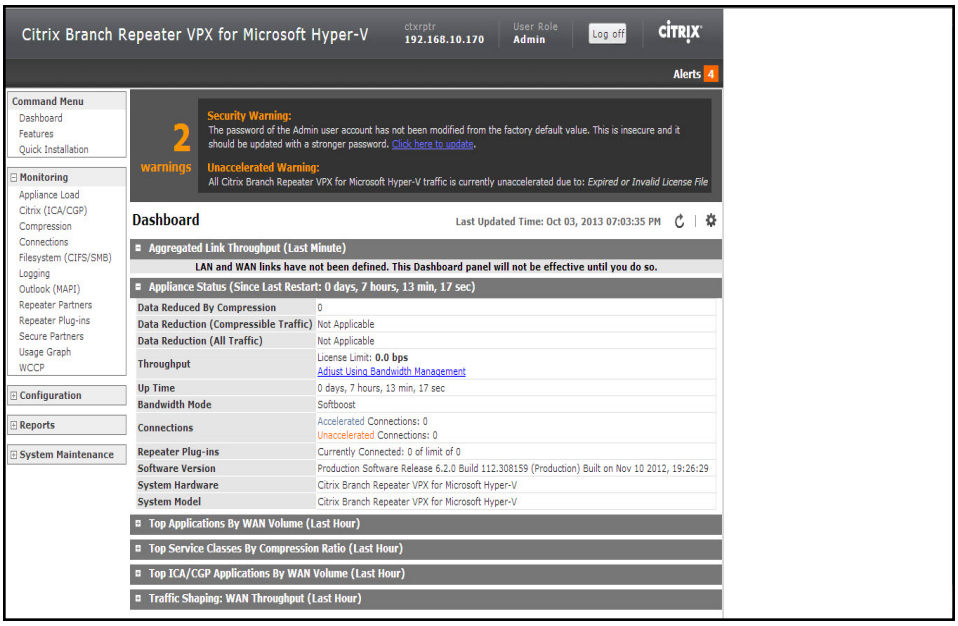


Figure 1.7: The web console of the Branch Repeater virtual appliance

4. Next, click on the **Features** option under the **Command Menu** section in the left panel of Figure 1.7. This will invoke Figure 1.8, using which you can enable/disable any feature you choose.

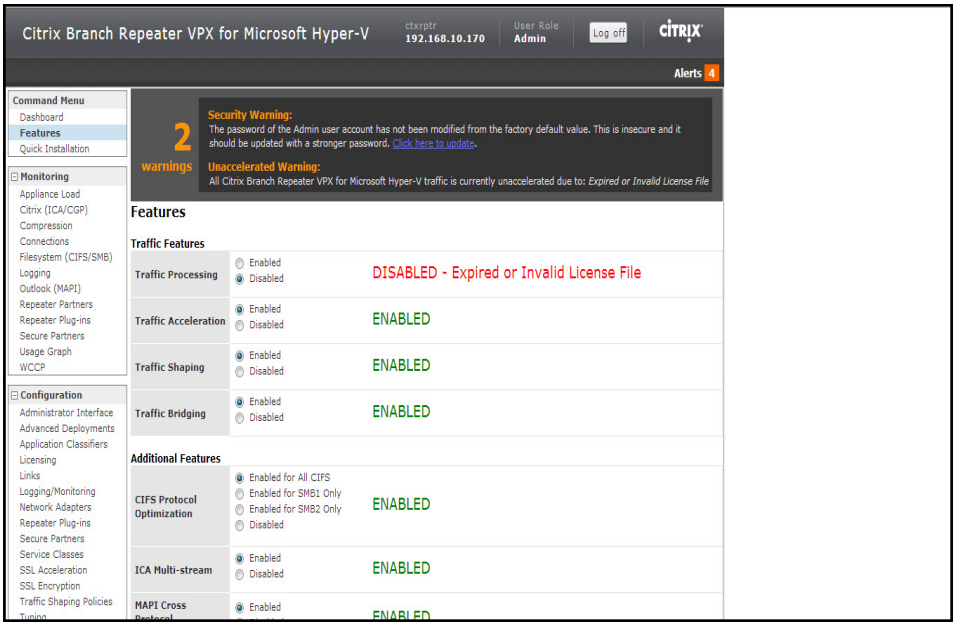


Figure 1.8: Enabling features

5. Keep scrolling down the **Features** page of Figure 1.8 until you find the **SNMP** feature. Pick the **Enable** option against **SNMP** to enable SNMP.

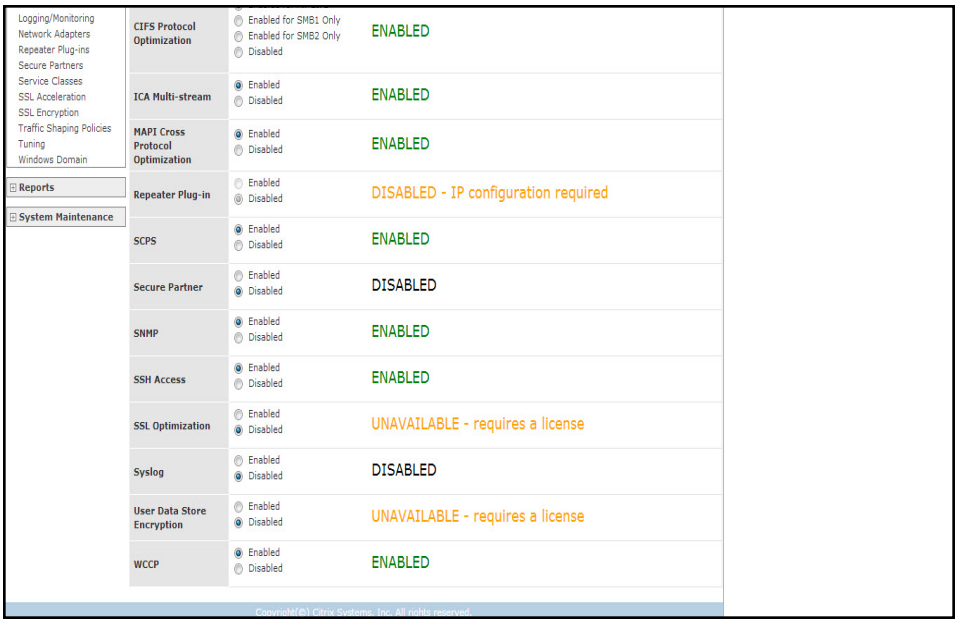


Figure 1.9: Enabling SNMP

6. Then, expand the **Configuration** tree in the left panel of Figure 1.8 and select the **Logging/Monitoring** node within. This will open Figure 1.10.

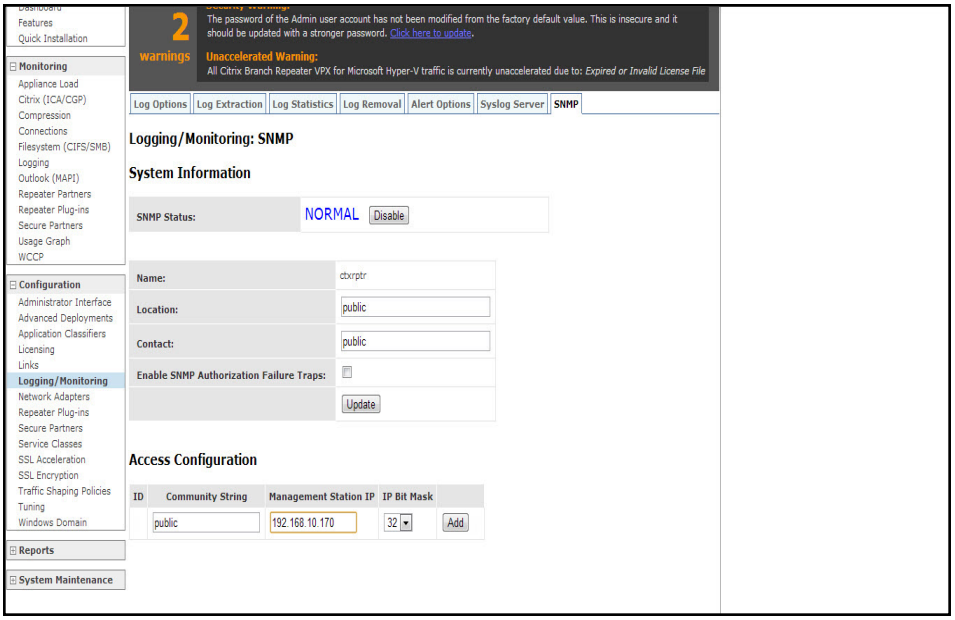


Figure 1.10: Configuring SNMP

7. Ensure that the **SNMP Status** is **NORMAL**. Provide the **Location** and **Contact** details and click the **Update** button. Then, in the **Access Configuration** section, add SNMP monitoring access to the Branch Repeater appliance by setting the following parameters:

- Set the **Community String** to **public**.
- Set the IP address of the host on which the Branch Repeater virtual appliance has been installed against **Management Station IP**.
- Then, click the **Add** button.

Once SNMP is enabled, the eG agent will poll the SNMB MIB of the branch repeater at configured intervals, report a plethora of useful metrics revealing the health of the branch repeater, and present these performance statistics in the eG monitoring model using the hierarchical layer model representation of Figure 1.5.

The chapter that follows will discuss each layer of Figure 1.5 in great detail.

2

Administering eG Manager to Monitor Citrix Branch Repeater

To achieve this, follow the steps given below:

1. Log into the eG administrative interface.
2. eG Enterprise cannot automatically discover the Citrix Branch Repeater. You need to manually add the server using the **COMPONENTS** page (see) that appears when the Infrastructure -> Components -> Add/Modify menu sequence is followed. Remember that components manually added are managed automatically.

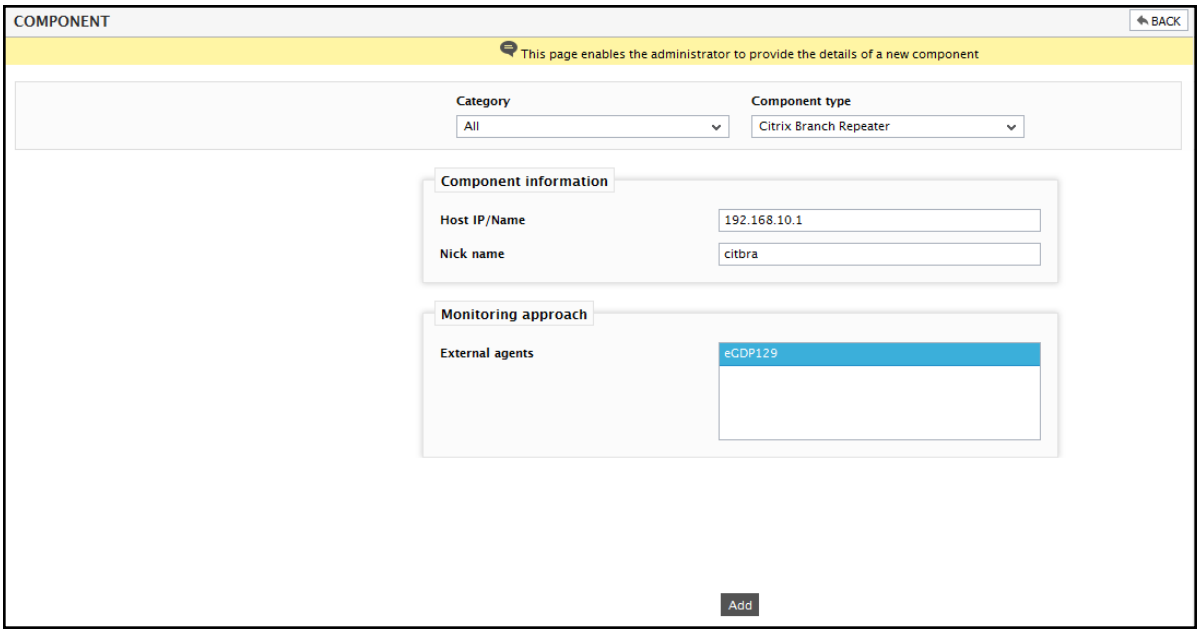
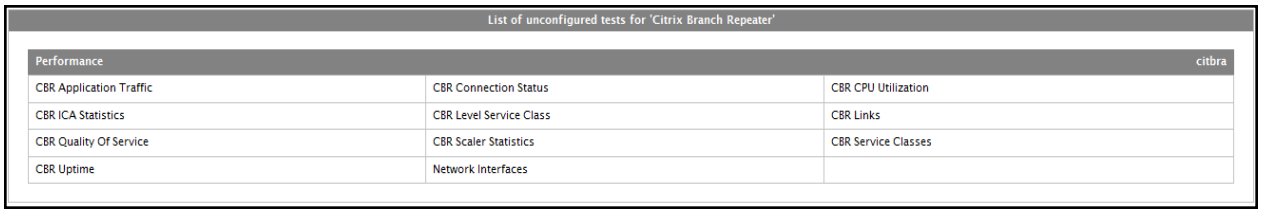


Figure 2.1: Adding a Citrix Branch Repeater

3. Specify the **Host IP** and the **Nick name** of the Citrix Branch Repeater in Figure 2.1. Then click the **Add** button to register the changes.
4. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.


List of unconfigured tests for 'Citrix Branch Repeater'

Performance		citbra
CBR Application Traffic	CBR Connection Status	CBR CPU Utilization
CBR ICA Statistics	CBR Level Service Class	CBR Links
CBR Quality Of Service	CBR Scaler Statistics	CBR Service Classes
CBR Uptime	Network Interfaces	

Figure 2.2: List of Unconfigured tests to be configured for the Citrix Branch Repeater

5. Now, click on the **CBR Application Traffic** test to configure it. To know how to configure the test, click here.
6. Other tests for this component will be configured automatically. Finally, sign out of the eG administrative interface.

3

The Citrix Branch Repeater Monitoring Model

This chapter deep dives into every layer of the Citrix Branch Repeater monitoring model, the tests mapped to each layer, and the measures every test reports.

3.1 The Operating System Layer

The tests mapped to this layer measure the CPU usage and uptime of the Citrix Branch Repeater.

Figure 3.1: The tests mapped to the Operating System layer

3.1.1 CBR CPU Utilization Test

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

Target of the test : A Citrix Branch Repeater

Agent deploying the test : An external agent

Outputs of the test : One set of results for the branch repeater being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed

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

- **AES** – Advanced Encryption Standard

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Cpu usage:	Indicates the percentage of CPU used by the branch repeater.	Percent	A value over 80% is a cause for concern as it indicates excessive CPU usage by the branch repeater.

3.1.2 CBR Uptime Test

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

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

The Uptime test included in the eG agent monitors the uptime of the branch repeater.

Target of the test : A Citrix Branch Repeater

Agent deploying the test : An external agent

Outputs of the test : One set of results for the branch repeater being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the host for which this test is to be configured.

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Has the branch repeater been restarted?:	Indicates whether the device has been rebooted or not.		If this measure shows 1, it means that the branch repeater was rebooted during the last measurement period. By checking the time periods when this metric changes from 0 to 1, an administrator can determine the times when this branch repeater was rebooted.
Uptime during the last measure period:	Indicates the time period that the branch repeater has been up since the last time this test ran.	Secs	If the branch repeater has not been rebooted during the last measurement period and the agent has been running continuously, this value will be equal to the measurement period. If the branch repeater was rebooted during the last measurement period, this value will be less than the measurement period of the test. For example, if the measurement period is 300 secs, and if the branch repeater was rebooted 120 secs back, this metric will report a value of 120 seconds. The accuracy of this metric is dependent on the measurement period – the smaller the measurement period, greater the accuracy.

Measurement	Description	Measurement Unit	Interpretation
Total uptime of the system:	Indicates the total time that the branch repeater has been up since its last reboot.		This measure displays the number of years, months, days, hours, minutes and seconds since the last reboot. Administrators may wish to be alerted if a branch repeater has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions.

3.2 The Network Layer

The tests mapped to this layer periodically check the availability of the VNX system over the network, monitor the network connections for latencies, and measure the traffic on each network interface supported by VNX to identify the busy and bandwidth-intensive interfaces. Since these tests have already been discussed in the Monitoring Network Elements document, let us proceed to the next layer.

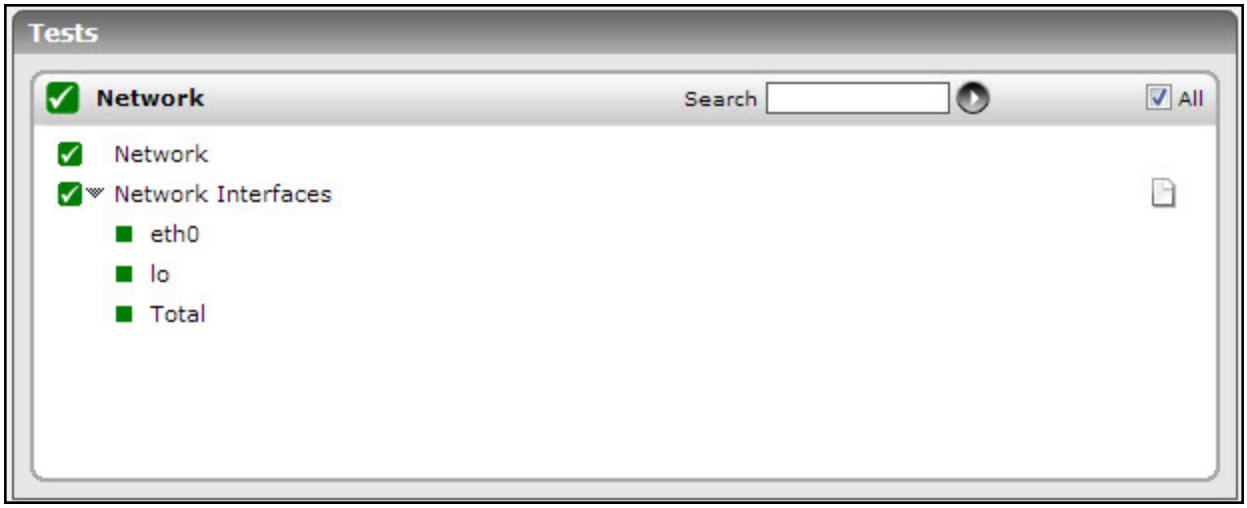


Figure 3.2: The tests mapped to the Network layer

3.3 The Branch Repeater App Layer

Using the **BR Application Traffic** test mapped to it, this layer monitors and reports how well the branch repeater accelerates traffic to and from each of the application links it manages.

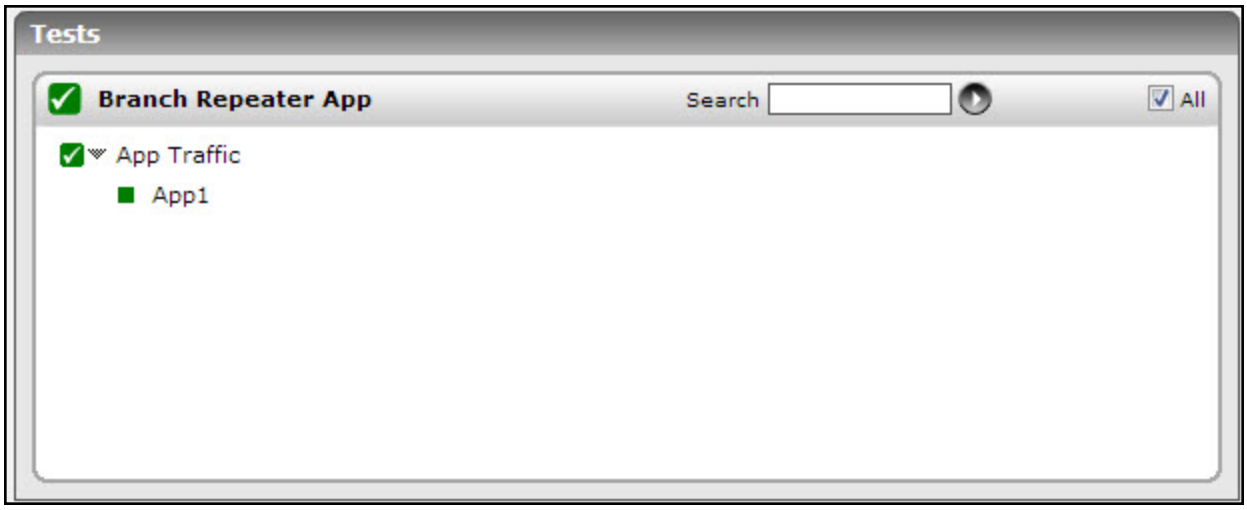


Figure 3.3: The tests mapped to the Physical Storage layer

3.3.1 CBR Application Traffic Test

The real test of the efficiency and overall health of the branch repeater lies in its ability to accelerate application accesses over the wide area network. If the Citrix Branch Repeater is not configured with the right service class policies, QoS thresholds, or compression rules, slowdowns during application accesses will become inevitable! If this is to be avoided, then administrators must keep an eye on every application link managed by the branch repeater, quickly identify links that are handling more or less data than their capacity, and proceed to fine-tune traffic rules over that link via the branch repeater to ensure optimum performance. This is where the **CBR Application Traffic** test helps. For every application link, this test reports the speed at which the link receives and transmits data and packets, thus measuring how well the branch repeater is managing the traffic over the link and pointing to those links that may require traffic optimizations.

Target of the test : A Citrix Branch Repeater

Agent deploying the test : An external agent

Outputs of the test : One set of results for application link handled by the Citrix Branch Repeater being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the host for which this test is to be configured.
3. **SNMPPORT** – The port at which the monitored target exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION**list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then

this parameter will not appear.

6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE**list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG**– This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
13. **ENCRYPTPASSWORD**– Specify the encryption password here.
14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for

instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data transmitted:	Indicates the rate at which data was sent over this application link.	KB/Sec	WAN links have low bandwidth when compared to LAN links. Moreover, any attempt made to send or receive traffic faster than the link throughput can result in congestion. Therefore, the branch repeater should make sure that just about enough data is sent and received over application links to prevent congestion and optimize throughput. If the values of these measures exceed or are dangerously close to the bandwidth limit of the link, it signals a potential congestion or slowdown of traffic over the link. It also indicates that you may have to reconfigure the branch repeater with more robust QoS and compression rules to prevent such unpleasant eventualities.
Data received:	Indicates the rate at which data was received over this application link.	KB/Sec	
Packets transmitted:	Indicates the number of packets transmitted over this application link.	Number	WAN links have low bandwidth when compared to LAN links. Moreover, any attempt made to send or receive traffic faster than the link throughput can result in congestion. Therefore, the branch repeater should make sure that just about enough data packets are sent and received over application links to prevent congestion and maximize throughput. If the values of these measures exceed or are dangerously close to the maximum number of data packets that the link can handle, it signals a potential congestion or slowdown of traffic over the link. It also

Measurement	Description	Measurement Unit	Interpretation
			indicates that you may have to reconfigure the branch repeater with more robust QoS and compression rules to prevent such unpleasant eventualities.
Packets received:	Indicates the number of packets received over this application link.	Number	
Data dropped during transmission:	Indicates the rate of traffic not sent over this application link due to QoS threshold settings.	KB/Sec	QoS (quality-of-service) is a set of policies and priorities assigned to the application traffic prioritized under traffic shaping policies in BR devices. A QoS threshold allows a sender to deliver only as much data as the branch repeater allows it to send, and this data is placed on the link at exactly the right rate to keep the link full but not overflowing. By eliminating excess data, the branch repeater is not forced to discard it. Without the branch repeater, the dropped data would have to be sent again, causing delay. A high value for these measures could therefore indicate one of the following: • The link bandwidth is low and hence the branch repeater has been rightly configured with a QoS threshold that allows only limited data to be sent/received over that link; this excludes a lot of data from transmissions/receptions and maximizes the responsiveness of the link; • The branch repeater has been misconfigured with a QoS threshold that forces the link to send/receive much less data than what it can handle; this causes a lot of data to be unnecessarily dropped from transmissions/receptions, affecting the quality-of-experience in the process. In this case, you may have to fine-tune the QoS policy.
Data dropped during reception:	Indicates the rate of traffic not received over this application link due to QoS threshold settings.	KB/Sec	

Measurement	Description	Measurement Unit	Interpretation
Packets dropped during transmission:	Indicates the number of packets not sent over this application link due to QoS threshold settings.	Number	QoS (quality-of-service) is a set of policies and priorities assigned to the application traffic prioritized under traffic shaping policies in BR devices. A QoS threshold allows a sender to deliver only as much data as the branch repeater allows it to send, and this data is placed on the link at exactly the right rate to keep the link full but not overflowing. By eliminating excess data, the branch repeater is not forced to discard it. Without the branch repeater, the dropped data would have to be sent again, causing delay. A high value of this measure could therefore indicate one of the following: • The link bandwidth is low and hence the branch repeater has been rightly configured with a QoS threshold that allows only limited number of packets to be sent/received over that link; this excludes a lot of packets from transmissions/receptions and maximizes the responsiveness of the link; • The branch repeater has been misconfigured with a QoS threshold that forces the link to send/receive much less data than what it can handle; this causes a lot of packets to be unnecessarily dropped from transmissions/receptions, affecting the quality-of-experience in the process. In this case, you may have to fine-tune the QoS policy.
Packets dropped during reception:	Indicates the number of packets not received over this application link due to QoS threshold settings.	Number	

3.4 The Branch Repeater Service Layer

The tests mapped to this layer reveal how efficient the branch repeater is by monitoring and reporting the following:

- Load on the branch repeater and how well it processes its load;
- How well the branch repeater accelerates ICA traffic;
- Service classes defined in the reporter and whether/not the branch repeater optimizes the throughput of incoming and outgoing traffic for each service class;
- WAN and LAN links managed by the branch repeater and the level of traffic acceleration performed by the branch repeater for each link;
- How each traffic-shaping policy influences the bandwidth consumption of links and whether/not any policy requires fine-tuning

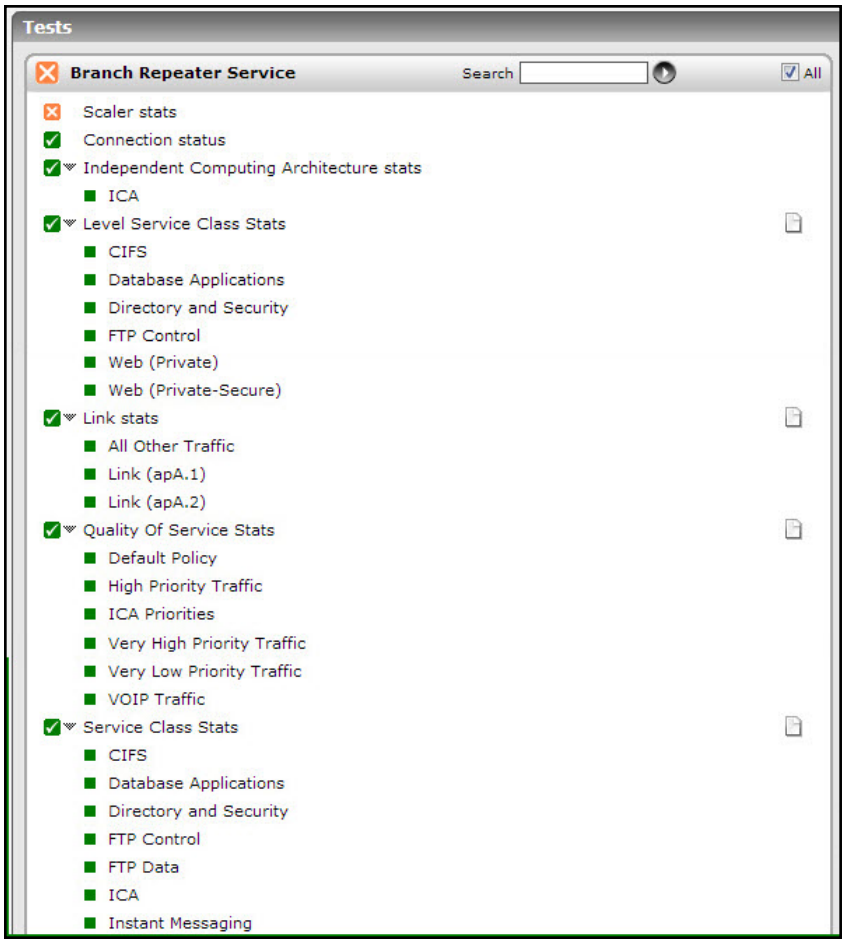


Figure 3.4: The tests mapped to the Branch Repeater Service layer

3.4.1 CBR Scaler Statistics Test

The performance of a Citrix Branch Repeater is often judged based on how well it handles its workload – i.e., how well it accelerates traffic over LAN and WAN links and how many connections it has accelerated over a period of time. A sudden increase in workload coupled with improper configuration can be disastrous – not just in terms of branch repeater performance but also in terms of branch user experience with local and wide area networks. It is therefore best to keep track of the variations in the workload of the branch repeater, so that

potential overload conditions can be detected, and also monitor key configuration settings such as compression algorithms employed by the branch repeater, so that ineffective configurations can be isolated and reset. The **CBR Scaler Statistics** test enables these checks. This test continuously tracks the load on the branch repeater, measures the effectiveness of the repeater by reporting the amount of data and connections it has accelerated, and also brings poor compression algorithms to light by revealing changes in compression ratios over time.

Target of the test : A Citrix Branch Repeater

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Citrix Branch Repeater being monitored

Configurable parameters for the test

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Load in 1 min:	Indicates the average load of the branch repeater during the last minute.	Percent	This measure represents the percentage of processes that are ready to be run. This value is computed by taking the 1-minute load average, multiplying it by 100, and then converting that value to an integer. You may want to observe changes in the value of this measure over time to understand whether/not there is a consistent increase in workload – if so, it

Measurement	Description	Measurement Unit	Interpretation
			could be indicative of a probable overload.
Load in 5 min:	Indicates the average load of the branch repeater during the last 5 minutes.	Percent	This value is computed by taking the 51-minute load average, multiplying it by 100, and then converting that value to an integer. You may want to observe changes in the value of this measure over time to understand whether/not there is a consistent increase in workload – if so, it could be indicative of a probable overload.
Data transmitted in WAN:	Indicates the total amount of accelerated data transmitted over WAN links during the last measurement period.	KB	A high value is desired for these measures, as it denotes high acceleration activity over WAN, which could significantly improve the responsiveness of the WAN links. A consistent drop in these values could indicate a processing bottleneck with the branch repeater or a misconfiguration that is stalling the repeater's traffic acceleration efforts.
Data received in WAN:	Indicates the total amount of accelerated data received over WAN links during the last measurement period.	KB	
Data transmitted in LAN:	Indicates the total amount of accelerated data transmitted over LAN links during the last measurement period.	KB	A high value is desired for these measures, as it denotes high acceleration activity over LAN, which could significantly improve the responsiveness of the LAN links. A consistent drop in these values could indicate a processing bottleneck with the branch repeater or a misconfiguration that is stalling the repeater's traffic acceleration efforts.
Data received in LAN:	Indicates the total amount of accelerated data received over LAN links during the last measurement period.	KB	

Measurement	Description	Measurement Unit	Interpretation
Send compression ratio:	Indicates the compression rate of the accelerated data transmitted during the last measurement period.	Percent	One of the techniques that the Citrix Branch repeater uses to accelerate data transmissions and receptions is compression. A compression algorithm scans the data to be compressed, searching for strings of data that match strings that have been sent before. If no such matches are found, the actual data is sent. If a match is found, the matching data is replaced with a pointer to the previous instance. In a very large matching string, megabytes or gigabytes of data can be represented by a pointer containing only a few bytes, and only those few bytes need be sent over the link. Ideally, the compression algorithm should be able to deliver high compression ratios. So, if the value of these measures drop consistently, it could indicate the usage of a poor compression algorithm. You may then want to consider fine- tuning the compression algorithm to ensure a high compression ratio.
Receive compression ratio:	Indicates the compression rate of the accelerated data received during the last measurement period.	Percent	
Accelerated connections:	Indicates the number of connections that were currently accelerated.	Number	If the number of Accelerated connections is more than the number of Non-accelerated connections, it is a sign of the good health of the branch repeater.
Non- accelerated connections:	Indicates the number of connections that were not accelerated currently.	Number	
Operational state:	Indicates the current operational state of the branch repeater.		The values that this measure can report and their corresponding numeric values have been detailed in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Up</td><td>1</td></tr>
<tr><td>Busy</td><td>100</td></tr>
<tr><td>Down</td><td>101</td></tr>
<tr><td>License Expired</td><td>102</td></tr>
</table>
Note:
By default, this measure reports the above- mentioned Measure Value s while indicating the operational state of the branch repeater. However, in the graph of this measure, the same will be represented using the corresponding numeric equivalents only.
</td></tr>
</table>

3.4.2 CBR Connection Status Test

This test reports the number of connections accelerated by the branch repeater that are currently active.

Target of the test : A Citrix Branch Repeater

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Citrix Branch Repeater being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the host for which this test is to be configured.
3. **SNMPPORT** – The port at which the monitored target exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION**list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version

3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.

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

conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Active connections:	Indicates the number of active accelerated connections.	Number	

3.4.3 CBR ICA Statistics Test

Branch Repeater includes ICA acceleration powered by HDX IntelliCache and HDX Broadcast technologies to optimize virtual application delivery. HDX IntelliCache optimizes delivery across multiple Citrix® XenApp™ and Citrix® XenDesktop™ sessions by locally caching and de-duplicating transmission of common graphics and data within the ICA protocol. HDX Broadcast, on the other hand:

- Optimizes the flow of XenDesktop and XenApp ICA® traffic across multiple connections in a branch by sensing and responding to network and traffic conditions;
- Reduces XenDesktop and XenApp ICA bandwidth consumption by applying optimal compression techniques based on traffic characteristics, infrastructure capabilities and network conditions;
- Orchestrates with XenDesktop and XenApp to participate in the ICA session and provides intelligent acceleration of the ICA protocol by sensing and responding to the network and traffic conditions;
- Allows administrators to define rules that set which types of application traffic or ICA workflows receive the highest priority.

But, how can administrators determine the adequacy of these instrumentations? What if, even after having configured the branch repeater with acceleration rules, administrators continue to receive user complaints related to slowness in ICA connections to virtual desktops? To handle such situations, administrators should keep an eye on the accelerated traffic for each ICA application, measure the throughput of the traffic, and accurately identify those applications for which ICA traffic may have to be regulated further to reduce bandwidth consumption and optimize throughput. To achieve this, administrators can use the **BR ICA Statistics** test. This test monitors the accelerated traffic to and from each ICA application, reports how effectively the branch repeater performs ICA acceleration, and in the process, accurately pinpoints areas for improvement – i.e., points to those applications for which the ICA traffic can be accelerated further by fine-tuning compression and QoS rules in the branch repeater.

Target of the test : A Citrix Branch Repeater

Agent deploying the test : An external agent

Outputs of the test : One set of results for each ICA application managed by the Citrix Branch Repeater being monitored

Configurable parameters for the test

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

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

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data transmitted:	Indicates the rate at which data was transmitted by this ICA application.	KB/Sec	If the value of these measures is well-within the bandwidth limit set for your WAN links, it indicates the efficiency of the branch repeater in maximizing throughput and minimizing bandwidth consumption. If the value of these measures indicates excessive bandwidth usage, then you may have to compare the value of these measures across ICA applications to know which application is consuming the maximum bandwidth. You should then alter the priority of the traffic and ICA workflows related to this application to reduce bandwidth usage.
Data received:	Indicates the rate at which data was received by this ICA application.	KB/Sec	
Data transmitted ratio:	Represents the sent volume of this ICA application as a percent share of the total volume of traffic sent by all ICA applications.	Percent	Compare the value of this measure across applications to identify bandwidth-intensive applications, and to understand how ICA traffic priorities should be set in the branch repeater.

Measurement	Description	Measurement Unit	Interpretation
Data received ratio:	Represents the received volume of this ICA application as a percent share of the total volume of traffic received by all ICA applications.	Percent	Compare the value of this measure across applications to identify bandwidth-intensive applications, and to understand how ICA traffic priorities should be set in the branch repeater.

3.4.4 CBR Level Service Class Test

Service classes are user-defined groups of IP addresses and port numbers that allow the Branch Repeater to accelerate or not accelerate a particular group of connections or a single connection.

Once a service class is created, acceleration (also known as flow control) and compression can be enabled or disabled for that particular service class.

Post service class configuration, it is good practice to observe the accelerated traffic to and from each service class, so that you can check the effectiveness of the acceleration/compression rules that you have set per service class. This is where the **CBR Level Service Class** test helps. This test auto-discovers the service classes configured in the branch repeater, monitors the volume of traffic sent and received by each service class, captures packet drops that occur when QoS thresholds are violated by a service class, and enables administrators to determine the following:

- How well the branch repeater accelerates/compresses traffic to/from service classes;
- Service classes for which acceleration/compression rules may have to be fine-tuned

Target of the test : A Citrix Branch Repeater

Agent deploying the test : An external agent

Outputs of the test : One set of results for each service class configured in the Citrix Branch Repeater being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the host for which this test is to be configured.
3. **SNMPPORT** – The port at which the monitored target exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION**– By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION**list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then

this parameter will not appear.

6. **USERNAME**– This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE**– This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE**list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG**– This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
13. **ENCRYPTPASSWORD**– Specify the encryption password here.
14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for

instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data transmitted:	Indicates the rate at which data was sent by this service class.	KB/Sec	WAN links have low bandwidth when compared to LAN links. Moreover, any attempt made to send or receive traffic faster than the link throughput can result in congestion. Therefore, the branch repeater should make sure that just about enough data is sent and received by the IP addresses and ports grouped under a service class to prevent congestion and optimize throughput.
Data received:	Indicates the rate at which data was received by this service class.	KB/Sec	If the values of these measures exceed or are dangerously close to the bandwidth limit of the WAN links used by a service class, it signals a potential congestion or slowdown of traffic over one/more of those WAN links. It also indicates that you may have to reconfigure the branch repeater with more robust traffic shaping policies to prevent such unpleasant eventualities.
Packets transmitted:	Indicates the number of packets transmitted by this service class.	Number	WAN links have low bandwidth when compared to LAN links. Moreover, any attempt made to send or receive traffic faster than the link throughput can result in congestion. Therefore, the branch repeater should make sure that just about enough data packets are sent and received by the IP addresses and ports grouped under a service class to prevent congestion and optimize throughput. If the values of these measures exceed or

Measurement	Description	Measurement Unit	Interpretation
			are dangerously close to the bandwidth limit of the WAN links used by a service class, it signals a potential congestion or slowdown of traffic over one/more of those WAN links. It also indicates that you may have to reconfigure the branch repeater with more robust traffic shaping policies, acceleration rules, and compression algorithms to prevent such unpleasant eventualities.
Packets received:	Indicates the number of packets received by this service class.	Number	
Data dropped during transmission:	Indicates the rate of traffic not sent by this service class over all its WAN links due to QoS threshold settings.	KB/Sec	QoS (quality-of-service) is a set of policies and priorities assigned to the application traffic prioritized under traffic shaping policies in BR devices. A QoS threshold allows a sender to deliver only as much data as the branch repeater allows it to send, and this data is placed on the link at exactly the right rate to keep the link full but not overflowing. By eliminating excess data, the branch repeater is not forced to discard it. Without the branch repeater, the dropped data would have to be sent again, causing delay. You can compare the value of these measures across service classes to identify that service class, the WAN links of which have dropped the maximum data. This could be owing to any of the following reasons: • The bandwidth of the WAN links used by the service class is low. Hence, very rightly, a high QoS threshold has been set that allows only limited data to be sent/received over those WAN links; as a result, a large amount of data gets automatically excluded from transmissions/receptions over those WAN links, thus maximizing the speed

Measurement	Description	Measurement Unit	Interpretation
			of the links; • The branch repeater has been misconfigured with a high QoS threshold that forces the WAN links used by this service class to send/receive much less data than what it can handle; this causes a lot of data to be unnecessarily dropped from transmissions/receptions, affecting the quality-of-experience in the process. In this case, you may have to fine-tune the QoS policy.
Data dropped during reception:	Indicates the rate of traffic not received by this service class due to QoS threshold settings.	KB/Sec	
Packets dropped during transmission:	Indicates the number of packets not sent over all the WAN links used by this service class due to QoS threshold settings.	Number	QoS (quality-of-service) is a set of policies and priorities assigned to the application traffic prioritized under traffic shaping policies in BR devices. A QoS threshold allows a sender to deliver only as much data as the branch repeater allows it to send, and this data is placed on the link at exactly the right rate to keep the link full but not overflowing. By eliminating excess data, the branch repeater is not forced to discard it. Without the branch repeater, the dropped data would have to be sent again, causing delay. You can compare the value of these measures across service classes to identify that service class, the WAN links of which have dropped the maximum packets. This could be owing to any of the following reasons: • The bandwidth of the WAN links used by the service class is low. Hence, very rightly, a high QoS threshold has been set that allows only limited number of packets to be sent/received over those WAN links; as a result, many data packets gets automatically

Measurement	Description	Measurement Unit	Interpretation
			excluded from transmissions/receptions over those WAN links, thus maximizing the speed of the links; • The branch repeater has been misconfigured with a high QoS threshold that forces the WAN links used by this service class to send/receive fewer data packets than what it can handle; this causes a many data packets to be unnecessarily dropped from transmissions/receptions, affecting the quality-of-experience in the process. In this case, you may have to fine-tune the QoS policy.
Packets dropped during reception:	Indicates the number of packets not received by this service class due to QoS threshold settings.	Number	

3.4.5 CBR Links Test

In order to optimize bandwidth usage, minimize congestions, and maximize the speed of WAN and LAN links, administrators need to define the WAN and LAN links requiring traffic acceleration in the Citrix Branch Repeater, set the bandwidth limit for each of the links for receiving/sending data, and associate each link with traffic shaping policies. But, once the configuration is complete, how can administrators test the correctness of the configuration? For this, administrators can use the **CBR Links** test. For each WAN and LAN link configured in the branch repeater, this test reports real-time metrics of the volume of traffic handled by the link and packet drops over the link. This way, the test reveals those links that are candidates for fine-tuning, owing to their low throughput despite the traffic shaping and acceleration rules that apply to them.

Target of the test : A Citrix Branch Repeater

Agent deploying the test : An external agent

Outputs of the test : One set of results for WAN/LAN link managed by the Citrix Branch Repeater being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the host for which this test is to be configured.
3. **SNMPPORT** – The port at which the monitored target exposes its SNMP MIB; the default is 161.

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data transmitted:	Indicates the rate at which data was sent over this link.	KB/Sec	Any attempt made to send or receive traffic faster than the link throughput can result in congestion. Therefore, the branch repeater should make sure that just about enough data is sent and received over application links to prevent congestion and optimize throughput. If the values of these measures exceed or are dangerously close to the bandwidth limit of the link, it signals a potential congestion or slowdown of traffic over the link. It also indicates that you may have to reconfigure the branch repeater with more robust QoS and compression rules to prevent such unpleasant eventualities.
Data received:	Indicates the rate at which data was received over this application link.	KB/Sec	
Packets transmitted:	Indicates the number of packets transmitted over this link.	Number	Any attempt made to send or receive traffic faster than the link throughput can result in congestion. Therefore, the branch repeater should make sure that just about enough data packets are sent and received over application links to prevent congestion and maximize throughput. If the values of these measures exceed or are dangerously close to the maximum number of data packets that the link can handle, it signals a potential congestion or

Measurement	Description	Measurement Unit	Interpretation
			slowdown of traffic over the link. It also indicates that you may have to reconfigure the branch repeater with more robust QoS and compression rules to prevent such unpleasant eventualities.
Packets received:	Indicates the number of packets received over this link.	Number	
Data dropped during transmission:	Indicates the rate of traffic not sent over this link due to QoS threshold settings.	KB/Sec	QoS (quality-of-service) is a set of policies and priorities assigned to the application traffic prioritized under traffic shaping policies in BR devices. A QoS threshold allows a sender to deliver only as much data as the branch repeater allows it to send, and this data is placed on the link at exactly the right rate to keep the link full but not overflowing. By eliminating excess data, the branch repeater is not forced to discard it. Without the branch repeater, the dropped data would have to be sent again, causing delay. A high value for these measures could therefore indicate one of the following: • The link bandwidth is low and hence the branch repeater has been rightly configured with a QoS threshold that allows only limited data to be sent/received over that link; this excludes a lot of data from transmissions/receptions and maximizes the responsiveness of the link; • The branch repeater has been misconfigured with a QoS threshold that forces the link to send/receive much less data than what it can handle; this causes a lot of data to be unnecessarily dropped from transmissions/receptions, affecting the quality-of-experience in the process. In this case, you may have to fine-tune

Measurement	Description	Measurement Unit	Interpretation
			the QoS policy.
Data dropped during reception:	Indicates the rate of traffic not received over this due to QoS threshold settings.	KB/Sec	
Packets dropped during transmission:	Indicates the number of packets not sent over this link due to QoS threshold settings.	Number	QoS (quality-of-service) is a set of policies and priorities assigned to the application traffic prioritized under traffic shaping policies in BR devices. A QoS threshold allows a sender to deliver only as much data as the branch repeater allows it to send, and this data is placed on the link at exactly the right rate to keep the link full but not overflowing. By eliminating excess data, the branch repeater is not forced to discard it. Without the branch repeater, the dropped data would have to be sent again, causing delay. A high value for these measures could therefore indicate one of the following: • The link bandwidth is low and hence the branch repeater has been rightly configured with a QoS threshold that allows only limited number of packets to be sent/received over that link; this excludes a lot of packets from transmissions/receptions and maximizes the responsiveness of the link; • The branch repeater has been misconfigured with a QoS threshold that forces the link to send/receive much less data than what it can handle; this causes a lot of packets to be unnecessarily dropped from transmissions/receptions, affecting the quality-of-experience in the process. In this case, you may have to fine-tune the QoS policy.
Packets dropped during reception:	Indicates the number of packets not received over this link due to QoS threshold settings.	Number	

3.4.6 CBR Service Classes Test

Service classes are user-defined groups of IP addresses and port numbers that allow the Branch Repeater to accelerate or not accelerate a particular group of connections or a single connection.

Once a service class is created, acceleration (also known as flow control) and compression can be enabled or disabled for that particular service class.

After service class configuration, administrators may want to check how well the branch repeater accelerates the traffic to and from each service class, how effective the compression algorithm mapped to each service class is, and whether any data or connection is left unaccelerated. This analysis will enable administrators to identify those service classes for which many connections are still unaccelerated and those that use poor compression algorithms. To perform this analysis periodically, the **CBR Service Classes** test can be used. For each service class configured in the branch repeater, this test monitors the accelerated traffic on the service class and reports the following:

- For which service class has the branch repeater not accelerated the maximum data and connections?
- For which service class has the branch repeater being unable to compress data traffic significantly?

Such service classes are candidates for configuration tuning.

Target of the test : A Citrix Branch Repeater

Agent deploying the test : An external agent

Outputs of the test : One set of results for each service class configured in the Citrix Branch Repeater being monitored

Configurable parameters for the test

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Current accelerated connection:	Indicates the current number of accelerated connections for this service class.	Number	
Total accelerated connection:	Indicates the total number of accelerated connections for this service class since system startup.	Number	A high value is desired for this measure.
Total accelerated data:	Indicates the total amount of data that was accelerated for this service class during the last measurement period.	KB	A high value is desired for this measure.
Total non-accelerated connections:	Indicates the total number of non- accelerated connections for this service class since system startup.	Number	A low value is desired for this measure. Compare the value of this measure across service classes to know for which service class the maximum number of connections has not been accelerated. The reasons for this will have to be investigated. If ineffective traffic shaping policies or compression rules are responsible for the gradual deterioration in the acceleration rate of the service class, then such policies will have to be revamped to improve performance.
Total non-accelerated data:	Indicates the total amount of data that was not accelerated for this service class during the last measurement period.	KB	Compare the value of this measure across service classes to know for which service class the maximum amount of data has not been accelerated. The reasons for this will have to be investigated. If ineffective traffic shaping policies or compression

Measurement	Description	Measurement Unit	Interpretation
			rules are responsible for the gradual deterioration in the acceleration rate of the service class, then such policies will have to be revamped to improve performance.
Accelerated data before compression:	Indicates the amount of data that was accelerated for this service class before compression during the last measurement period.	KB	
Data transmitted after compression:	Indicates the amount of data that was transmitted for this service class after compression, during the last measurement period.	KB	Compare the value of the Data transmitted after compression and the Data transmitted before compression measures for a service class to figure out how effective compression was. If compression did not reduce the data transmitted for any service class, it is an indication that a poor compression algorithm has been employed by that service class. You will then have to reconfigure the compression ratio that applies to that service class.
Data transmitted before compression:	Indicates the amount of data that was transmitted for this service class before compression, during the last measurement period.	KB	
Data received after compression:	Indicates the amount of data that was received for this service class after compression, during the last measurement period.	KB	Compare the value of the Data received after compression and the Data received before compression measures for a service class to figure out how effective compression was. If compression only mildly reduced the data received for any service class, it is an indication that a poor compression algorithm has been employed by that service class. You will then have to reconfigure the compression ratio that applies to that service class.
Data received before compression:	Indicates the amount of data that was received for this service class before compression, during the last measurement period.	KB	

3.4.7 CBR Quality of Service Test

The Citrix Branch Repeater includes integral quality-of-service (QoS) functionality that classifies traffic by flow and application. This works with various other optimization and compression technologies to control the bandwidth used and improve the user experience.

In Citrix Repeater, a traffic-shaping engine is included to manage all the TCP or User Datagram Protocol (UDP) traffic on WAN links in the incoming as well as outgoing directions. The traffic shaper is based on bandwidth-limited fair queuing, where every connection is assigned a weighted priority based on the assigned policies. Weighted priorities are applied to the actual WAN data transferred, after compression is applied. The weighted priority is based on the Application Classifiers defined in the Service Class, and you can also apply the weighted priorities on a per-link basis.

You can use the following mechanisms to apply Quality of Service:

- **Link Definition**: Informs the traffic shaper which WAN link the packet is using. In a site with multiple links, each link has its own bandwidth limits and is managed independently.
- **Application Classifiers**: Identifies and determines the protocol or application class to which traffic belongs.
- **Service Classes**: Maps applications to acceleration decisions, traffic filters, and traffic-shaping policies.
- **Traffic Shaping Policies**: Informs the traffic shaper about weighted priority and bandwidth limits to assign to which traffic type, the application classifier.

Figure 2.2 depicts the architecture for the QoS capabilities

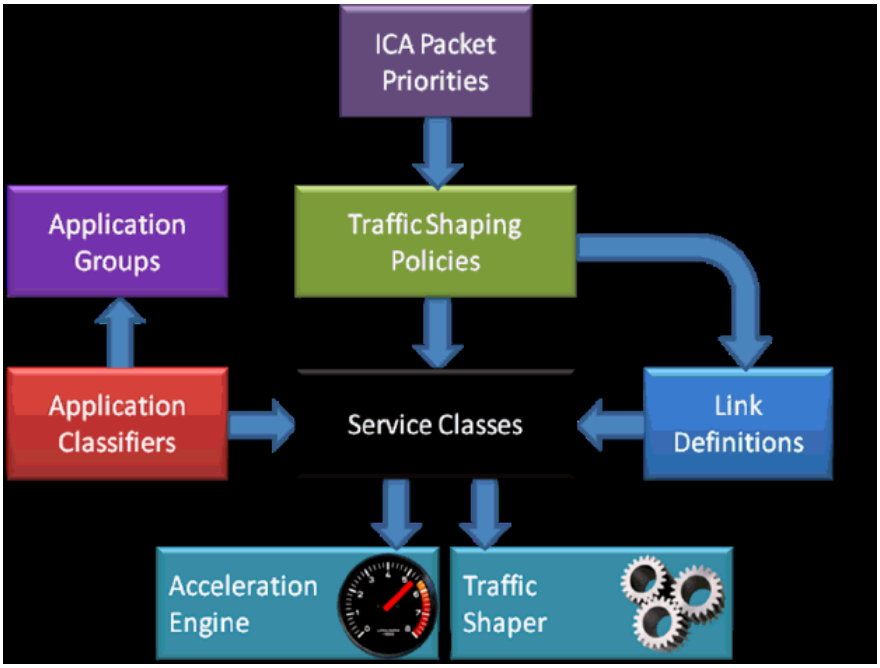


Figure 3.5: The QoS architecture

If branch users complain of link slowdowns, then administrators should be able to identify which traffic-shaping policy governs traffic acceleration on that link and should figure out how to fine-tune that policy to increase link throughput. The **CBR Quality of Service** test helps with this! This test auto-discovers the default and user-configured traffic-shaping policies and closely observes the traffic accelerated by each policy to identify those policies that may have to be tweaked in order to improve the rate of traffic acceleration, optimize bandwidth usage, and reduce packet loss.

Target of the test : A Citrix Branch Repeater

Agent deploying the test : An external agent

Outputs of the test : One set of results for each default and user-configured traffic-shaping policy in the Citrix Branch Repeater being monitored

Configurable parameters for the test

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data transmitted:	Indicates the rate at which data was transmitted for this traffic-shaping policy.	KB/Sec	At any given point in time, the value of these measures should be well-within the incoming and outgoing bandwidth usage limits set for the corresponding traffic-changing policy. If these values consistently grow towards the bandwidth usage limit, it is an indication that the traffic-shaping policy is not very effective. You may then have to fine-tune that policy to optimize bandwidth consumption.
Data received:	Indicates the rate at which data was received for this traffic-shaping policy.	KB/Sec	

Measurement	Description	Measurement Unit	Interpretation
Packets transmitted:	Indicates the number of packets transmitted for this traffic-shaping policy during the last measurement period.	Number	At any given point in time, the value of these measures should be well-within the incoming and outgoing bandwidth usage limits set for the corresponding traffic-changing policy. If these values consistently grow towards the bandwidth usage limit, it is an indication that the traffic-shaping policy is not very effective. You may then have to fine-tune that policy to optimize bandwidth consumption.
Packets received:	Indicates the number of packets received for this traffic- shaping policy during the last measurement period.	Number	
Data received before compression:	Indicates the amount of data that was received for this service class before compression, during the last measurement period.	KB	
Data dropped during transmission:	Indicates the rate of traffic dropped because of this traffic-shaping policy.	KB/Sec	A high value for these measures could indicate one of the following: • The traffic-shaping policy is such that it allows only very limited data to be sent/received over a link; this excludes a lot of data from transmissions/receptions and maximizes the responsiveness of the link; • The traffic-shaping policy has been misconfigured, causing a link to send/receive much less data than what it can handle; this causes a lot of data to be unnecessarily dropped from transmissions/receptions, affecting the quality-of-experience in the process. In this case, you may have to fine-tune the policy.
Data dropped during reception:	Indicates the rate of traffic not received due to this traffic-shaping policy.	KB/Sec	
Packets dropped during	Indicates the number of packets dropped during	Number	A high value for these measures could indicate one of the following:

Measurement	Description	Measurement Unit	Interpretation
transmission:	transmissions due to this traffic-shaping policy.		• The traffic-shaping policy is such that it allows only a few data packets to be sent/received over a link; this excludes a lot of packets from transmissions/receptions and maximizes the responsiveness of the link; • The traffic-shaping policy has been misconfigured, causing a link to send/receive fewer data packets than what it can handle; this causes many packets to be unnecessarily dropped from transmissions/receptions, affecting the quality-of-experience in the process. In this case, you may have to fine-tune the policy.
Packets dropped during reception:	Indicates the number of packets not received due to this traffic-shaping policy.	Number	

4

Conclusion

This document has clearly explained how eG Enterprise monitors the **Citrix Branch Repeater**. We can thus conclude that eG Enterprise, with its ability to provide in-depth insight into the performance of the branch repeater, is the ideal solution for monitoring such environments. For more information on eG Enterprise, please visit our web site at www.eginnovations.com or write to us at sales@eginnovations.com.