# Monitoring Citrix SD-WAN

eG Innovations Product Documentation

eG

**Total Performance Visibility**

# Table of Contents

# Table of Figures

# Chapter 1: Introduction

Citrix software-defined wide-area network (SD-WAN) is a service that grants the enterprise with the ability to dynamically connect branch offices and data centers on a global scale. As companies utilize a growing number of cloud-based applications, traditional WAN networks could not maintain consistent high network speed and optimized connectivity. SD-WAN provides IT stakeholders a solution for the above-mentioned issues with better tools to manage several types of internet connections, including broadband and MPLS, as well as 3G/4G/LTE. The SD-WAN solutions leverage policy management tools to improve IT's ability to optimize how data moves between office branches, data centers and cloud. SD-WAN centralizes the rule definition and distribution processes, allowing administrators to group rules and manage policies with a single application, simultaneously.

Today's enterprise infrastructure is supported by WANs but often experience issues due to the high volume of traffic. Organizations that leverage MPLS and other networking solutions may encounter service outages, traffic congestion and packet loss. SD-WAN addresses these problems seamlessly. Ultimately, end users will not even know if their network uses SD-WAN because their applications and services will simply work as intended. The ability for SD-WAN to dynamically route traffic through a hybrid network means that WAN traffic is reduced overall, and network agility increases.

Owing to these capabilities, the Citrix SD-WAN appliance is widely used in various on-premise and cloud infrastructures, where multi-tenancy and seamless access to resources are key for ensuring user satisfaction. In such infrastructures, if the SD-WAN appliance is congested due to unexpected incoming and outgoing traffic or if the appliance is sluggish in routing the traffic due to packet loss, latency and jitter, or the non-critical applications consume more bandwidth, the performance and delivery of the business-critical applications across the infrastructure are sure to be badly hit! For a seamless flow of traffic without congestion, packet loss, latency, etc. and to improve user experience, it is therefore necessary for the administrators to continuously monitor the traffic flow routed via the Citrix SD-WAN appliance. This can be easily achieved using a dedicated monitoring model offered by eG Enterprise.
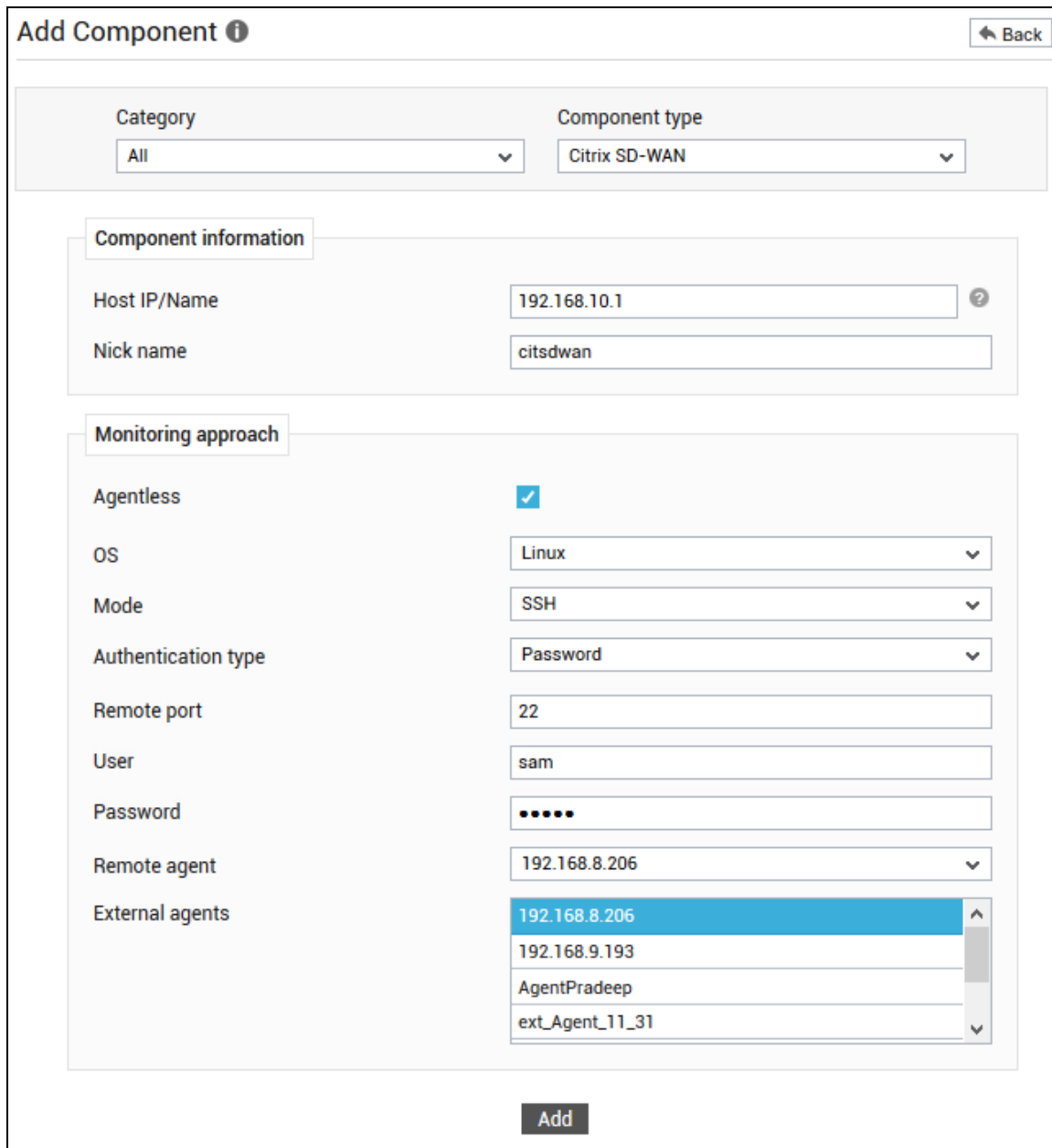
# Chapter 2: How to Monitor Citrix SD-WAN Using eG Enterprise?

eG Enterprise monitors the Citrix SD-WAN appliance using an eG remote agent that is deployed on a remote Windows host in the environment. This agent is capable of monitoring the performance of the SD-WAN by connecting to the appliance via SSH. To enable this connection, you need to specify the valid credentials of a user who can access the target appliance via SSH port while managing the target appliance or monitoring using eG admin interface. The steps for managing the target appliance are provided in the following section.

## 2.1 Managing Citrix SD-WAN

The Citrix SD-WAN appliance cannot be automatically discovered by eG Enterprise. This implies that you will have to manually add the target appliance into the eG Enterprise system to manage it. Remember that the eG Enterprise automatically manages the components that are added manually. Follow the steps below to achieve the same:

1. Login to the eG admin interface.

2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.

3. In the **Components** page that appears, select *Citrix SD-WAN* from the **Component type** drop-down and then click the **Add New Component** button. This will invoke the **Add Component** page as shown in Figure 2.1.

Figure 2.1: Adding a Citrix SD-WAN

4. Specify the **Host IP/Name** and the **Nick name** of the Citrix SD-WAN component in Figure 2.1. Since the target appliance is monitored in an agentless manner, the **Agentless** check box will be checked, by default.

5. Then, select **Linux** as the **OS** and **SSH** as the **Mode**. The **Authentication Type** will be *Password* by default.

6. The **SSH Port** text box will be specified with the default SSH port value 22.

7. Next, provide the credentials of a user who can access the target appliance via the SSH Port, in the **User** and **Password** text boxes.

8. Select the eG agent that will be monitoring the target appliance from the **Remote Agent** drop down list.

9. Choose an external agent for the appliance by picking an option from the **External agents** list box.

10. Then, click the **Add** button to register the changes.

11. Next, click the **Signout** button at the right, top corner of the eG admin interface to sign out. Now, you will be prompted to configure **Network Interfaces** test. To know how to configure this test, refer to *Monitoring Cisco Router* document.

12. Finally, signout of the eG admin interface.

# Chapter 3: Monitoring Citrix SD-WAN

Citrix NetScaler SD-WAN is an all-in-one service and application delivery solution that accelerates application performance, increases application availability and improves application security.



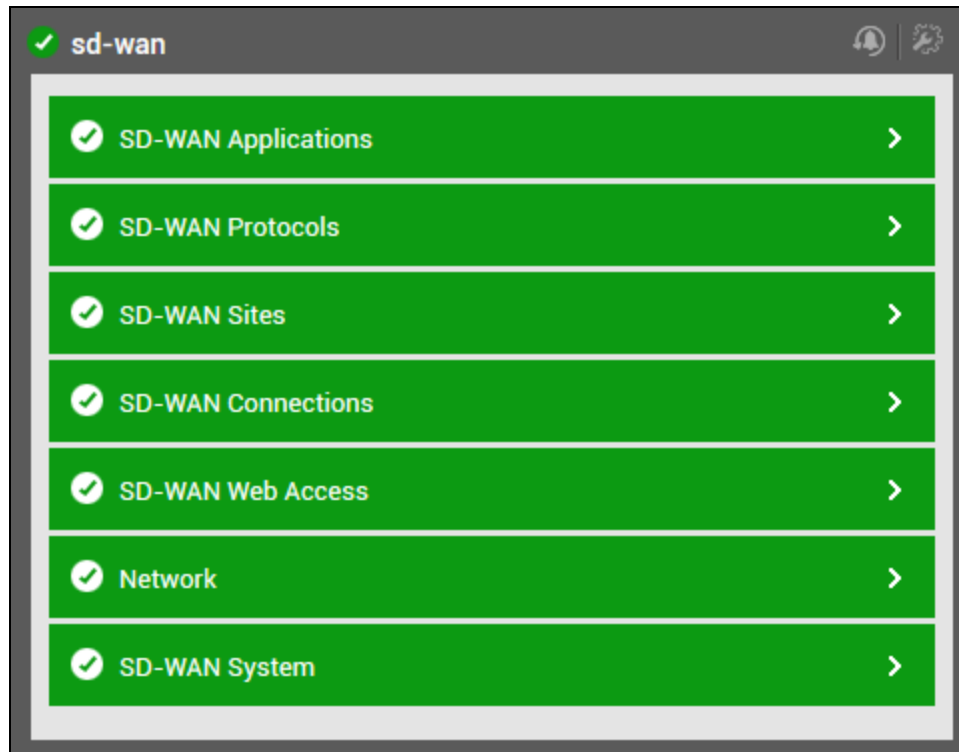Figure 3.1: The Citrix SD-WAN monitoring model

Each layer of Figure 3.1 is mapped to tests pull out a wealth of performance information related to the appliance. These metrics reveal the following:

## 3.1 SD-WAN System Layer

The tests mapped to this layer reveals statistics pertaining to the data/packet traffic over the Passthrough service and different types of service such as Internet, Intranet and Virtual Path.
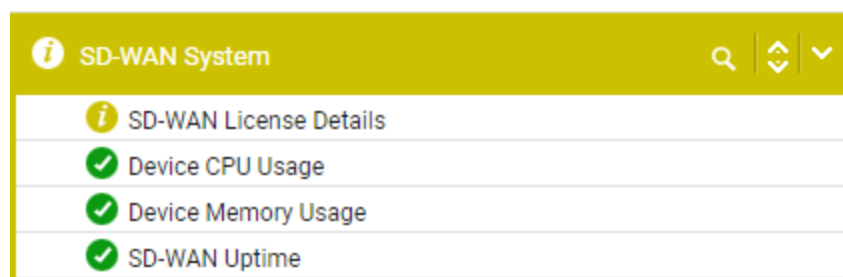
Figure 3.2: The SD-WAN System Layer

## 3.1.1 SD-WAN License Details Test

Using this test, administrators can easily figure out whether the target appliance is currently licensed or not and the maximum bandwidth that the appliance can use for the subscribed license. Moreover, this test also tracks the license usage of the target appliance, and determines when the license is likely to expire.

**Target of the test :** A Citrix SD-WAN

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for the Citrix SD-WAN appliance that is being monitored.

**Configurable parameters for the test**

| Parameter | Description |
| --- | --- |
| Test Period | How often should the test be executed. By default, this is set to 5 minutes. |
| Host | The IP address of the target SD-WAN appliance for which this test is to be configured. |
| Port | Refers to the port at which the target SD-WAN listens to. By default, this will be NULL. |
| Timeout | Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds. |
| Detailed Diagnosis | To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. |
| | The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: |
| | • The eG manager license should allow the detailed diagnosis capability |

| Parameter | Description |
|---|---|
| | • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0. |

**Measurements made by the test**

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| Has license expired? | Indicates whether the target appliance is licensed or not. | | The numeric values that correspond to each of the above-mentioned values are as follows:<br><br>**Measure Value / Numeric Value**<br>Licensed — 0<br>Unlicensed — 1<br><br>**Note:**<br>By default, this measure reports one of the **Measure Value**s listed in the table above to indicate whether the appliance is licensed or not. The graph of this measure however, represents the same using the numeric equivalents alone. |
| Maximum bandwidth supported | Indicates the maximum bandwidth that the appliance can support. | Mbps | |
| Days to expire | Indicates the number of days within which the appliance's license will expire. | Number | If this value is very low, it implies that license will expire very soon. To continue using the appliance, administrators will have to renew the license. |

## 3.1.2 SD-WAN Uptime Test

In most network environments, it is essential to monitor the uptime of critical appliances/services in the infrastructure. By tracking the uptime of each of the appliances/services, administrators can determine what percentage of time an appliance/service has been up. Comparing this value with

service level targets, administrators can determine the most trouble- prone areas of the infrastructure.

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

This test included in the eG agent monitors the uptime of the target Citrix SD-WAN appliance. In addition, this test also reveals the uptime of the Virtual WAN Service configured on the target appliance.

**Target of the test :** A Citrix SD-WAN

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for the target Citrix SD-WAN appliance.

**Configurable parameters for the test**

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. By default, this is set to 5 minutes. |
| Host | The IP address of the target SD-WAN appliance for which this test is to be configured. |
| Port | Refers to the port at which the target SD-WAN listens to. By default, this will be NULL. |
| Timeout | Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds. |

**Measurements made by the test**

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| Has the appliance been rebooted? | Indicates whether the appliance has been rebooted during the last measurement period or not. | | If this measure shows 1, it means that the appliance 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 the appliance was rebooted. |
| Uptime during the last measure period | Indicates the time period | Seconds | If the appliance has not been rebooted |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | that the appliance has been up since the last time this test ran. | | during the last measurement period and the agent has been running continuously, this value will be equal to the measurement period. If the appliance 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 appliance was rebooted 120 secs back, this metric will report a value of 120 seconds. The accuracy of this metric is dependent on the measurement period - the smaller the measurement period, greater the accuracy. |
| Total uptime of the appliance | Indicates the total time that the appliance 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 server has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions. |
| Has the service been rebooted? | Indicates whether the Virtual WAN Service has been rebooted during the last measurement period or not. | | If this measure shows 1, it means that the Virtual WAN Service 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 the service was rebooted. |
| Uptime during the last measure period | Indicates the time duration for which the Virtual WAN Service has been running since the last time this test ran. | Seconds | If the service 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 service was rebooted during the last |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | | | 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 service was rebooted 120 secs back, this metric will report a value of 120 seconds. The accuracy of this metric is dependent on the measurement period - the smaller the measurement period, greater the accuracy. |
| Total uptime of the service | Indicates the time period that the Virtual WAN Service 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 the Virtual WAN Service 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 Network Layer

The tests associated with the Network layer reveal whether a network connection to the Citrix SD-WAN appliance is available or not, and also monitors the current status of the network interfaces supported by the appliance. Additionally, administrators can easily figure out the efficiency of the Ethernet ports in handling the traffic and the errors encountered by the ports. In addition, the tests help tracking the data/packet traffic handled by the access interfaces and WAN links.
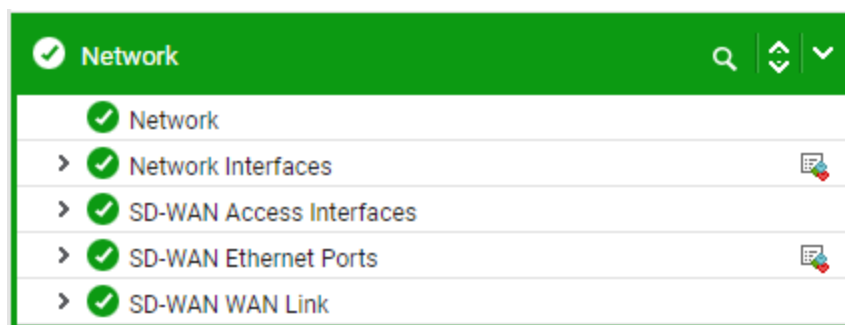


Figure 3.3: The Network Layer

## 3.2.1 SD-WAN Access Interface Test

An Access Interface consisting of a Virtual Interface, WAN endpoint IP Address, Gateway IP Address, and Virtual Path Mode is defined collectively as an interface for a specific WAN link. The Access Interface defines the IP Address and Gateway IP Address for a WAN Link. At least one Access Interface is required for each WAN Link.

- **Virtual Interface** – This is the Virtual Interface that the Access Interface will use. Select an entry from the drop-down menu of Virtual Interfaces configured for a branch site.

- **WAN endpoint IP Address** – This is the IP Address for the Access Interface endpoint from the appliance to the WAN.

- **Gateway IP Address** – This is the IP Address for the gateway router.

- **Virtual Path Mode** – This specifies the priority for Virtual Path traffic on the WAN link. The options are: **Primary**, **Secondary**, or **Exclude**. If the Virtual Path Mode is set to **Exclude**, the Access Interface will be used for Internet and Intranet traffic, only.

- **Proxy ARP** – If this option is enabled, the Virtual WAN Appliance replies to ARP requests for the Gateway IP Address, when the gateway is unreachable.

This test auto-discovers the access interfaces through which the connection is made to the target appliance and reports the traffic and throughput of each access interface.

**Target of the test :** A Citrix SD-WAN

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for every access interface connected to the target SD-WAN appliance.

**Configurable parameters for the test**

| Parameter | Description |
| --- | --- |
| Test Period | How often should the test be executed. By default, this is set to 5 minutes. |
| Host | The IP address of the target SD-WAN appliance for which this test is to be configured. |
| Port | Refers to the port at which the target SD-WAN listens to. By default, this will be NULL. |
| Timeout | Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds. |
| Detailed Diagnosis | To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an |

| Parameter | Description |
|-----------|-------------|
| | optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. |
| | The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: |
| | • The eG manager license should allow the detailed diagnosis capability |
| | • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0. |

## Measurements made by the test

| Measurement | Description | Measurement Unit | Interpretation |
|-------------|-------------|------------------|----------------|
| Proxy ARP state | Indicates the current status of the Proxy ARP. | | If the value of this measure is "Enabled", then the Virtual WAN Appliance replies to ARP requests for the Gateway IP Address, when the gateway is unreachable. The numeric values that correspond to each of the above-mentioned values are as follows: |

| Measure Value | Numeric Value |
|---------------|---------------|
| Disabled | 0 |
| Enabled | 1 |

**Note:**

By default, this measure reports one of the **Measure Value**s listed in the table above to indicate the current status of the proxy ARP. The graph of this measure however, represents the same using the numeric equivalents alone.

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| Reply age | Indicates the time taken to receive the response | Seconds | |
| vPath packets received | Indicates the number of packets received over the this access interface's virtual path. | Packets | This measure is reported only when the Virtual Path Mode is set to Primary or Secondary. |
| vPath packets transmitted | Indicates the number of packets transmitted over the this access interface's virtual path. | Packets | Compare the values of these measures across the access interfaces to figure which access interface handled more packet traffic on the virtual path. |
| vPath data received | Indicates the amount of data received through the virtual path. | MB | These measures are reported only when the Virtual Path Mode is set to Primary or Secondary. |
| vPath data transmitted | Indicates the amount of data transmitted through the virtual path. | MB | Compare the values of these measures across the access interfaces to figure which access interface transmitted and received data traffic on the virtual path. |
| vPath input throughput | Indicates the rate at which the data was received over the virtual path. | Mbps | These measures are reported only when the Virtual Path Mode is set to Primary or Secondary. |
| vPath output throughput | Indicates the rate at which the data was received over the virtual path. | Mbps | The values of these measures help administrators to find out which access interface is most efficient in transmitting and receiving the data over the virtual path. |
| vPath compressed data received | Indicates the amount of compressed data received over the virtual path. | MB | These measures are reported only when the Virtual Path Mode is set to Primary or Secondary. |
| vPath compressed data transmitted | Indicates the amount of compressed data transmitted through the virtual path. | MB | By comparing the values of these measures across the access interfaces, administrators can identify the access interface that received or transmitted the maximum amount of compressed data. |
| Internet packets received | Indicates the number of packets received when | Packets | This measure is reported only when the Virtual Path Mode is set to Exclude. |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | this access interface uses Internet service for handling traffic. | | |
| Internet packets transmitted | Indicates the number of packets transmitted when this access interface uses Internet service for handling traffic. | Packets | This measure is reported only when the Virtual Path Mode is set to Exclude. |
| Internet data received | Indicates the amount of data received when this access interface is used for handling Internet traffic. | MB | This measure is reported only when the Virtual Path Mode is set to Exclude. |
| Internet data transmitted | Indicates the amount of data transmitted when this access interface is used for handling Internet traffic. | MB | This measure is reported only when the Virtual Path Mode is set to Exclude. |
| Internet input throughput | Indicates the rate at which the incoming traffic processed when this access interface is used for handling Internet traffic. | Mbps | These measures are reported only when the Virtual Path Mode is set to Exclude.

The values of these measures help administrators to find out which access interface is most efficient in transmitting and receiving the data over the Internet. |
| Internet output throughput | Indicates the rate at which the outgoing traffic processed when this access interface is used for handling Internet traffic. | Mbps | |
| Intranet packets received | Indicates the number of packets received when this access interface is used for handling Intranet traffic. | Packets | This measure is reported only when the Virtual Path Mode is set to Exclude. |
| Intranet packets transmitted | Indicates the number of packets transmitted when | Packets | This measure is reported only when the Virtual Path Mode is set to Exclude. |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | this access interface is used for handling Intranet traffic. | | |
| Intranet data received | Indicates the amount of data received when this access interface is used for handling Intranet traffic. | MB | This measure is reported only when the Virtual Path Mode is set to Exclude. |
| Intranet data transmitted | Indicates the amount of data transmitted when this access interface is used for handling Intranet traffic. | MB | This measure is reported only when the Virtual Path Mode is set to Exclude. |
| Intranet input throughput | Indicates the rate at which the incoming traffic processed when this access interface is used for handling Intranet traffic. | Mbps | These measures are reported only when the Virtual Path Mode is set to Exclude.

The values of these measures help administrators to find out which access interface is most efficient in transmitting and receiving the data over the Intranet. |
| Intranet output throughput | Indicates the rate at which the outgoing traffic processed when this access interface is used for handling Intranet traffic. | Mbps | |

## 3.2.2 SD-WAN Ethernet Ports Test

Citrix SD-WAN enables communication among the branches and remote sites through its Ethernet ports. Availability and data transfer ability of the ports are important for active and healthy communication in the SD-WAN environment. If the ports are down due to traffic congestion or fatal errors, then the data transferring efficiency and reliability of the ports become questionable. This brings all traffic a near halt and directly affects the communication established through the ports. To avoid such eventualities, administrator should keep track on traffic flowing through the ports so as to ensure reliable communication.

This test monitors all the Ethernet ports on the target Citrix SD-WAN appliance, and reports the current status of link established through each port. In addition, this test also reports the count of frames transmitted/received through each port and the amount of data transferred through each port. Using these statistics, administrators can easily figure out the efficiency of the ports in handling the traffic. In the process, the count of errors encountered by the each port is also revealed. This way, the test proactively alerts administrators about the occurrence of abnormalities (if any) at the ports.

**Target of the test :** A Citrix SD-WAN

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for each Ethernet port on the target Citrix SD-WAN appliance.

**Configurable parameters for the test**

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. By default, this is set to 5 minutes. |
| Host | The IP address of the target SD-WAN appliance for which this test is to be configured. |
| Port | Refers to the port at which the target SD-WAN listens to. By default, this will be NULL. |
| Timeout | Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds. |

**Measurements made by the test**

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| Link state | Indicates the current link status of this Ethernet port. | | The numeric values that correspond to each of the above-mentioned values are as follows: <br><br> <table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Dead</td><td>20</td></tr><tr><td>Bad</td><td>40</td></tr></table> <br> **Note:** <br><br> By default, this measure reports one of |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | | | the **Measure Value**s listed in the table above to indicate the current status of each Ethernet port's link. The graph of this measure however, represents the same using the numeric equivalents alone. |
| Frames transmitted | Indicates the number of frames transmitted through this Ethernet port during the last measurement period. | Frames | |
| Frames received | Indicates the number of frames received through this Ethernet port during the last measurement period. | Frames | |
| Data transmitted | Indicates the amount of data transmitted through this Ethernet port during the last measurement period. | MB | |
| Data received | Indicates the amount of data received through this Ethernet port during the last measurement period. | MB | |
| Errors | Indicates the number of errors encountered on this Ethernet port. | Number | Ideally, the value of this measure should be 0. You can compare this value across the ports to know which port is encountering the maximum number of errors. |

## 3.3 SD-WAN Web Access Layer

The HTTP test mapped to this layer emulates an HTTP access to the web interface of the SD-WAN appliance, and reports the availability and responsiveness of the web console to HTTP requests. In addition to the HTTP test, the layer also monitors the validity of the SSL certificates (if any).

Figure 3.4: The SD-WAN Web Access Layer

To know how to configure these tests, refer to the *Monitoring Apache Web Server* document.

## 3.4 SD-WAN Connections Layer

The tests associated with this layer enable administrators to find out the packet loss, latency and jitter recorded while transmitting/receiving packets over each virtual path and WAN path. In addition, reachability and eligibility for transmitting reof each routing IP address can also be determined.
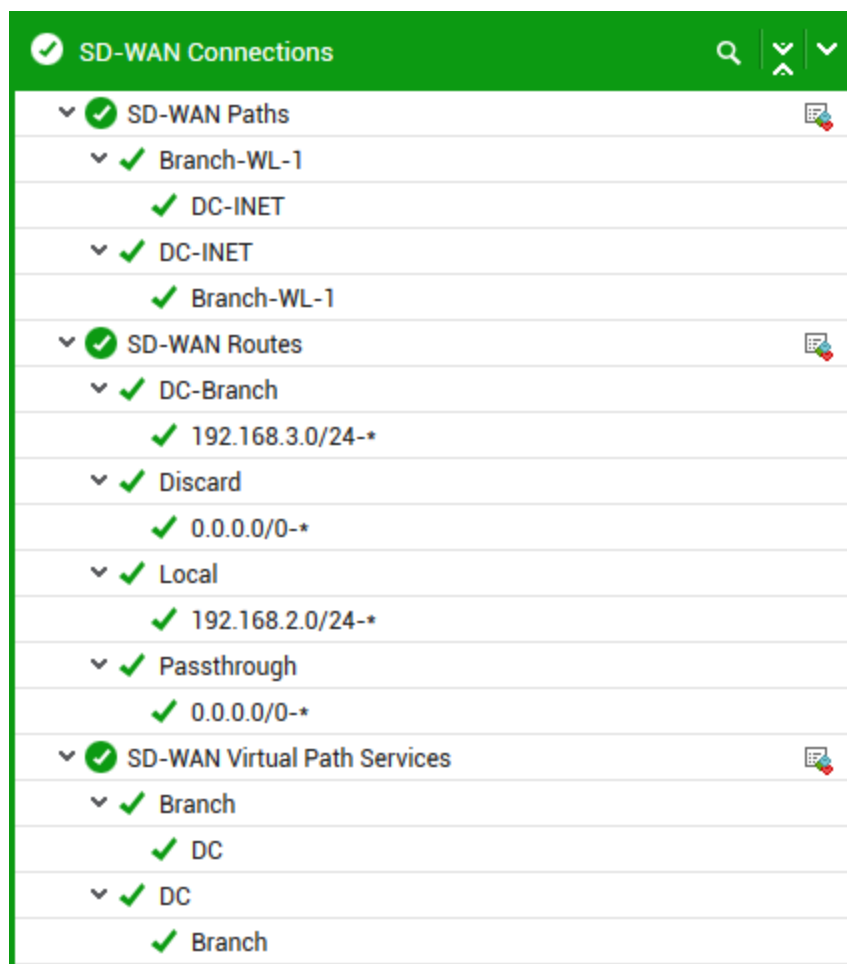
Figure 3.5: The SD-WAN Connections Layer

## 3.4.1 SD-WAN Paths Test

Citrix SD-WAN appliance creates a reliable WAN from diverse network links, also called paths, including MPLS, broadband, and wireless. Typically, the target appliance routes the mission critical applications over the paths with fastest transit time to avoid network latency. In addition, the target appliance enables real-time application traffic duplication to guarantee no loss and balances traffic from high bandwidth applications across multiple links to provide high performance for large file transfers. By continuously monitoring each path link for packet loss, latency, jitter and congestion, administrators can mitigate link outages and errors and move traffic off poor performing links without affecting the applications routed across the links. This in turn helps administrators to maintain consistent performance of the appliance while routing the mission critical applications. This is where the **SD-WAN Paths** test helps administrators!

This test auto-discovers the path links established through the target appliance, and reports the current status of each path link. This test proactively reveals whether/not each path link is impacted by congestion. This revelation helps administrators to identify the path links that are congested and move the traffic off from those links to free them up for the business critical transactions. In addition, this test also reports the jitter, one-way time latency and packet loss over each link. By analyzing these metrics, administrators can easily determine if there is an issue on the path link or not and decide on routing the traffic to other path links if any of the path links is badly affected by congestion, latency and/or loss.

**Target of the test :** A Citrix SD-WAN

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for each path link between the datacenter and branches.

**Configurable parameters for the test**

| Parameter | Description |
| --- | --- |
| Test Period | How often should the test be executed. By default, this is set to 5 minutes. |
| Host | The IP address of the target SD-WAN appliance for which this test is to be configured. |
| Port | Refers to the port at which the target SD-WAN listens to. By default, this will be NULL. |
| Timeout | Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds. |
| Detailed Diagnosis | To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. |
| | The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: |
| | • The eG manager license should allow the detailed diagnosis capability |
| | • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0. |

## Measurements made by the test

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| Path state | Indicates the current status of this path link. | | The numeric values that correspond to the measure values are as follows:<br><br>| Measure Value | Numeric Value | Description |<br>|---|---|---|<br>| Dead | 0 | Indicates that the path hasn't received any packets since 1.5 seconds. |<br>| Bad | 1 | This state is reported when 3 or 4 packets out of 10 are lost. |<br>| Good | 2 | Every 2-3 packets of incoming packets are processed as a sample size used to report conditions back to the local device. |<br><br>**Note:**<br><br>By default, this measure reports one of the **Measure Value**s listed in the table above to indicate the current status of each path link. The graph of this measure however, represents the same using the numeric equivalents alone.<br><br>The detailed diagnosis of this measure |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | | | displays the reason for the state change of each link and the time duration. |
| Congestion | Indicates whether/not this path link is affected by congestion. | | The numeric values that correspond to measure values are as follows:<br><br>| Measure Value | Numeric Value |<br>|---|---|<br>| No | 0 |<br>| Yes | 1 |<br><br>**Note:**<br><br>By default, this measure reports one of the **Measure Value**s listed in the table above to indicate whether each path link is affected by congestion or not. The graph of this measure however, represents the same using the numeric equivalents alone. |
| Virtual path service state | Indicates the current status of the virtual path service on this path link. | | The numeric values that correspond to the measure values are as follows:<br><br>| Measure Value | Numeric Value |<br>|---|---|<br>| Dead | 0 |<br>| Bad | 1 |<br>| Good | 2 |<br><br>**Note:**<br><br>By default, this measure reports one of the **Measure Value**s listed in the table above to indicate the current status of the virtual path service on each path link. The graph of this measure however, represents the same using the numeric equivalents alone.<br><br>The detailed diagnosis of this measure reveals the type of the virtual path service. |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| Maximum transmission unit | Indicates the maximum size of the packets/frames that this path link can transmit. | Bytes | A very high value of this measure may indicate the need for retransmissions if the path link can't transfer large packets. A very low value of this measure may indicate relatively more header overhead and more acknowledgments that have to be sent and handled over the path. Therefore, it is highly recommended that the administrators should not change the default Maximum transmission unit (MTU) value set by the service providers. |
| BOWT | Indicates the total time taken by the packets to travel from its source to its destination over this path link. | Seconds | |
| Jitter | Indicates the time variation in the delay while receiving the packets over this path link. | Seconds | A high value for this measure is indicative of a long time gap between the packets, which needs to be immediately addressed by administrators to avoid . |
| Packets received | Indicates the number of packets received over this path link. | Packets | |
| Packets out of order | Indicates the number of packets delivered in a different order from which they were sent from the source. | Number | The value of this measure is preferred to be low. A high value indicates that too many packets are received out of order, which will drastically increase retransmissions of packets on the network. As a result, the packet transmission will be delayed which will adversely impact the performance of the appliance. |
| Packet loss | Indicates the percentage of packets lost while transmitting through this path link. | Percent | Ideally, a low value is desired for this measure. |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| Data transmission | Indicates the rate at which the data was transmitted over this path link. | Mbps | |

## 3.4.2 SD-WAN Routes Test

In a typical SD-WAN network, the branch offices access applications on the on-premise data center, the cloud data center, or the SaaS applications. The application routing feature of the target SD-WAN appliance, allows you to steer the applications through your network easily and cost-efficiently. For example, when a user on the branch site is trying to access a SaaS application, the traffic can be routed such that the branch offices can access the SaaS applications on the internet directly, without having to go through the data center first. In such a way, users can have quick access to the applications and better experience with the applications. To perform the effective routing in the SD-WAN environment, it is necessary that the routing IP should be able to reach the network easily and eligible to transmit the requests over the network. Whenever any of the routing IP addresses is not able to steer the application traffic over the network, administrators may want to identify the exact technical glitch that caused the issue. This is where the **SD-WAN Routes** test helps administrators!

This auto-discovers all routing IP addresses that are transmitting the requests via the target appliance, and for each IP address, reports the network reachability and eligibility.

**Target of the test :** A Citrix SD-WAN

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for each service:routing IP address.

**Configurable parameters for the test**

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. By default, this is set to 5 minutes. |
| Host | The IP address of the target SD-WAN appliance for which this test is to be configured. |
| Port | Refers to the port at which the target SD-WAN listens to. By default, this will be NULL. |
| Timeout | Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds. |

| Parameter | Description |
|---|---|
| Detailed Diagnosis | To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. |
| | The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: |
| | • The eG manager license should allow the detailed diagnosis capability |
| | • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0. |

## Measurements made by the test

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| Is network reachable? | Indicates whether this route IP address is able to reachable or not. | | The numeric values that correspond to measure values are as follows: <br><br> <table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>No</td><td>0</td></tr><tr><td>Yes</td><td>1</td></tr></table> <br> **Note:** <br><br> By default, this measure reports one of the **Measure Value**s listed in the table above to indicate whether each route IP address is reachable or not. The graph of this measure however, represents the same using the numeric equivalents alone. |
| Route type | Indicates the route type of this IP address. | | The numeric values that correspond to measure values are as follows: |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | | | <table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Static</td><td>0</td></tr><tr><td>Dynamic</td><td>1</td></tr></table> **Note:** By default, this measure reports one of the **Measure Value**s listed in the table above to indicate the type of each IP address. The graph of this measure however, represents the same using the numeric equivalents alone. |
| Is eligible? | Indicates whether/not this IP address is eligible to transmit requests. | | The numeric values that correspond to measure values are as follows: <table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>No</td><td>0</td></tr><tr><td>Yes</td><td>1</td></tr></table> **Note:** By default, this measure reports one of the **Measure Value**s listed in the table above to indicate whether the IP address is reachable or not. The graph of this measure however, represents the same using the numeric equivalents alone. |
| Hits | Indicates the number of times this IP address used to steer the application traffic. | Number | |
| Cost | Indicates the weight for determining the route priority of this IP address. | Number | The value of this measure may vary from 1 to 15. Typically, lower-cost routes take precedence over higher-cost routes. The default value is 5. |

## 3.4.3 SD-WAN Virtual Path Services Test

Virtual path service configured on the Citrix SD-WAN appliance manages traffic across Virtual Paths. A Virtual Path is a logical link between two WAN links established from the target appliance. Each virtual path comprises a collection of WAN Paths combined to provide high service-level communication between two SD-WAN nodes. The virtual path can be static (always exists) or dynamic (exists only when traffic between two SD-WAN appliances reaches a configured threshold). Maintaining the virtual paths at good state and transmitting the packets over the virtual paths with low latency and good/no jitter are important for administrators to ensure reliable communication between the SD-WAN nodes. If, for any reason, any of the virtual paths changes to bad/dead state and/or transmits packets with high latency and bad jitter, the packets transmitted through that virtual path will not reach the destination on time and thus, the communication will become unreliable. In such cases, administrators will have to direct the traffic from the affected virtual path to the other virtual path before anything untoward happens. Using the **SD-WAN Virtual Path Services** test, administrators can track the current status of the virtual path and latency and jitter over the virtual path. Analyzing the metrics reported by the test, administrators can easily detect whether the packet transmission over each virtual path is reliable or not.

This test auto-discovers the virtual paths configured on the target SD-WAN appliance, and for each virtual reports the current status and latency and jitter recorded while transmitting the packets.

**Target of the test :** A Citrix SD-WAN

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for each virtual path configured on the target Citrix SD-WAN appliance.

**Configurable parameters for the test**

| Parameter | Description |
| --- | --- |
| Test Period | How often should the test be executed. By default, this is set to 5 minutes. |
| Host | The IP address of the target SD-WAN appliance for which this test is to be configured. |
| Port | Refers to the port at which the target SD-WAN listens to. By default, this will be NULL. |
| Timeout | Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds. |
| Detailed Diagnosis | To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be |

| Parameter | Description |
|---|---|
| | configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.<br><br>The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:<br><br>• The eG manager license should allow the detailed diagnosis capability<br><br>• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0. |

## Measurements made by the test

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| State | Indicates the current status of this virtual path. | | The numeric values that correspond to the measure values are as follows:<table><tr><td>Measure Value</td><td>Numeric Value</td><td>Description</td></tr><tr><td>Dead</td><td>0</td><td>Indicates that the path hasn't received any packets since 1.5 seconds.</td></tr><tr><td>Bad</td><td>1</td><td>This state is reported when 3 or 4 packets out of 10 are lost.</td></tr><tr><td>Good</td><td>2</td><td>Every 2-3 packets of incoming packets are processed as</td></tr></table> |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | | | <table><tr><th>Measure Value</th><th>Numeric Value</th><th>Description</th></tr><tr><td></td><td></td><td>a sample size used to report conditions back to the local device.</td></tr></table> **Note:** By default, this measure reports one of the **Measure Value**s listed in the table above to indicate the current status of each virtual path link. The graph of this measure however, represents the same using the numeric equivalents alone. The detailed diagnosis of this measure displays the type of each virtual path i.e. whether the link is static or dynamic, and how long the virtual path is in a particular state since it is created. In addition to the above details, whether the virtual path is affected by traffic congestion or not. |
| Maximum transmission unit | Indicates the maximum size of the packets/frames that this virtual path can transmit. | Bytes | A very high value of this measure may indicate the need for retransmissions if the virtual path can't transfer large packets. A very low value of this measure may indicate relatively more header overhead and more acknowledgments that have to be sent and handled over the path. Therefore, it is highly recommended that the administrators should not change the default Maximum transmission unit (MTU) value set by the service providers. |
| Latency | Indicates the time delay | Seconds | |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | recorded while transmitting/receiving the packets through this virtual path. | | |
| Worst jitter | Indicates the worst time variation in the delay recorded over this virtual path. | Seconds | A value of this measure should be very low. |
| Best jitter | Indicates the acceptable time variation in the delay while transmitting/receiving the packets over this virtual path. | Seconds | A gradual/sudden increase in the value of this measure indicates that the jitter on the virtual path is increasing which may lead to poor user experience with the virtual path. |
| Data received | Indicates the rate at which the data was received over this virtual path. | Mbps | |

# 3.5 SD-WAN Sites Layer

The tests mapped to this layer reveals statistics pertaining to the data/packet traffic over the Passthrough service and different types of service such as Internet, Intranet and Virtual Path.



Figure 3.6: The SD-WAN Sites Layer

## 3.5.1 SD-WAN Passthrough Sites Test

Passthrough service on the Citrix SD-WAN appliance manages traffic that is to be passed through the Virtual WAN. Traffic directed to the Passthrough service includes broadcasts, ARPs and other

non-IPv4 traffic. When the target SD-WAN appliance receives the request to transmit the data/packets using the Passthrough service, it simply passes the traffic to the destination without any shaping or modification or delay. However, administrators should ensure that the Passthrough traffic does not consume substantial resources on the WAN links that the appliance is configured to use for other services. Therefore, it becomes necessary that the traffic routed using the Passthrough service should be continuously tracked to keep the Passthrough traffic flow in check. This is where the **SD-WAN Passthrough Sites** test helps administrators!

This test continuously monitors the Passthrough traffic that administrators want to transmit unchanged through the target SD-WAN appliance. With the help of this test, administrators can find out the rate at which the data/packets were transmitted/received and the data/packets dropped while transmitting/receiving through the Passthrough service. These statistics are useful for administrators to detect heavy Passthrough traffic at the earliest and prevent the traffic congestion that may affect the business -critical transactions over the target appliance.

**Target of the test :** A Citrix SD-WAN

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for the target Citrix SD-WAN appliance.

**Configurable parameters for the test**

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. By default, this is set to 5 minutes. |
| Host | The IP address of the target SD-WAN appliance for which this test is to be configured. |
| Port | Refers to the port at which the target SD-WAN listens to. By default, this will be NULL. |
| Timeout | Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds. |

**Measurements made by the test**

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| Data received | Indicates the rate at which the data was received for transmission using the Passthrough service configured on the target | Mbps | It is always recommended that the Passthrough traffic be limited as much as possible. Therefore, a very high value reported for these measures is a cause for concern. It |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | appliance. | | indicates that Passthrough traffic is using high bandwidth rather than the critical applications. As a result, key business transactions will be delayed and the reliability of the target appliance will become questionable. |
| Data transmitted | Indicates the rate at which the data was transmitted for reception using the Passthrough service. | Mbps | |
| Data dropped | Indicates the rate at which the data was dropped while transmitting/receiving using the Passthrough service. | Mbps | |
| Packets received | Indicates the rate at which the packets were received for transmission using the Passthrough service. | Packet/sec | |
| Packets transmitted | Indicates the rate at which the packets were transmitted for reception using the Passthrough service. | Packet/sec | |
| Packets dropped | Indicates the rate at which the packets were dropped while transmitting/receiving using the Passthrough service. | Packet/sec | |

## 3.5.2 SD-WAN Sites Test

The Citrix SD-WAN provides resilient and robust connectivity between remote sites, data centers, and cloud networks. To accomplish this, the tunnels between SD-WAN appliances in the network are established and connectivity between WAN sites is enabled by leveraging route tables that overlay the existing underlay network. SD-WAN route tables can fully replace or coexist with the existing routing infrastructure. The SD-WAN configuration allows static route entries for specific sites, and route entries learned from the underlay network through supported routing protocols; such as OSPF, eBGP, and iBGP. Routes are not only defined by their next hop but by their service type. This determines how the route is forwarded. Below are the main service types in use:

- **Local Service** - This service denotes any route or subnet local to the SD-WAN appliance. This includes the Virtual Interface subnets (automatically creates local routes), and any local route defined in the route table (with a local next hop). The route is advertised to other SD-WAN appliances that have a Virtual Path to this local site where this route is configured when trusted as a partner.

  **Note:**

  Be cautious when adding default routes, and summary routes as local routes as these can result in virtual path routes at other sites. Always check the route tables to make sure the correct routing is in effect.

- **Virtual Path** - This denotes any local route learned from a remote SD-WAN site; that is what is reachable down the virtual paths. These routes are normally automatic, however a virtual path route can be added manually at a site. Any traffic for this route is forwarded to the defined Virtual Path for this destination route (subnet).

- **Intranet** - This service denotes routes that are reachable through a private WAN link (MPLS, P2P, VPN etc.). For example, a remote branch that is on the MPLS network but does not have an SD-WAN appliance. It is assumed that these routes need to be forwarded to a certain WAN router. Intranet Service is not enabled by default. Any traffic matching this route (subnet) is classified as intranet for this appliance for delivery to a site that does not have an SD-WAN solution.

  **Note:**

  Notice that when adding an Intranet route there is no next hop, but rather a forward to an Intranet Service. The Service is associated with a given WAN link.

- **Internet** -This is similar to Intranet but is used to define traffic flowing to public Internet WAN links rather than private WAN links. One unique difference is that the Internet service can be associated with multiple WAN links and set to load balance (per flow) or be active/backup. A default Internet routes gets created when internet service is enabled (it is off by default). Any traffic matching this route (subnet) is classified as Internet for this appliance for delivery to public internet resources.

The above-mentioned service types play an important role in defining the routes among remote sites, data centers, and cloud networks and handling traffic among them. To ensure better performance and user experience in the SD-WAN environment, therefore, it is important for administrators to continuously check the traffic handled using each type of service. By continuously monitoring the data/packet transmission using each service type, administrators can find out which service type is efficient in handling traffic flow between the WAN and LAN connections. For this purpose, administrators can use the **SD-WAN** Sites test.

This test monitors all the type of services used to transfer data/packet in the SD-WAN environment, and reports the rate at which the data/packets were transmitted/received and the data/packets dropped while transmitting/receiving using each type of service. These statistics are useful for administrators to find out the type of service on which heavy traffic or slowness was reported at the earliest and prevent the traffic congestion that may affect the business -critical transactions.

**Target of the test :** A Citrix SD-WAN

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for each type of service on which multicast traffic will be sent to or receive from the WAN sites.

**Configurable parameters for the test**

| Parameter | Description |
| --- | --- |
| Test Period | How often should the test be executed. By default, this is set to 5 minutes. |
| Host | The IP address of the target SD-WAN appliance for which this test is to be configured. |
| Port | Refers to the port at which the target SD-WAN listens to. By default, this will be NULL. |
| Timeout | Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds. |
| Detailed Diagnosis | To make diagnosis more efficient and accurate, the eG Enterprise embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. |
|  | The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: |
|  | • The eG manager license should allow the detailed diagnosis capability |
|  | • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0. |

**Measurements made by the test**

| Measurement | Description | Measurement Unit | Interpretation |
| --- | --- | --- | --- |
| LAN to WAN data | Indicates the rate at which | Mbps |  |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| transmission | the data was transmitted from LAN to WAN on this service type. | | |
| LAN to WAN packet transmission | Indicates the rate at which the packets were transmitted from LAN to WAN on this service type. | Packets/sec | |
| LAN to WAN data dropped | Indicates the rate at which the data was dropped while transmitting/receiving data from LAN on this service type. | Mbps | Ideally, the value of this measure should be zero. |
| LAN to WAN packets dropped | Indicates the rate at which the packets were dropped while transmitting/receiving packets from LAN to WAN on this service type. | Packets/sec | Ideally, the value of this measure should be zero. |
| WAN to LAN data transmission | Indicates the rate at which the data was transmitted from WAN to LAN on this service type. | Mbps | |
| WAN to LAN packet transmission | Indicates the rate at which the packets were transmitted from WAN to LAN on this service type. | Packets/sec | |
| WAN to LAN data dropped | Indicates the rate at which the data was dropped while transmitting/receiving data from WAN to LAN on this service type. | Mbps | Ideally, the value of this measure should be zero. Compare the value of this measure across the service types to find out the service type on which more data loss was reported while transmitting/receiving data. |
| WAN to LAN packets dropped | Indicates the rate at which the packets were dropped while transmitting/receiving data from WAN to LAN on this service type. | Packets/sec | Ideally, the value of this measure should be zero. Compare the value of this measure across the service types to identify the service type on which too many packets were dropped while transmitting/receiving the packets. |

## 3.6 SD-WAN Protocols Layer

The tests associated with this layer enable administrators to find out the following:

- The current status of each IP address in the ARP table of the target SD-WAN appliance;

- The time duration taken by each IP address to receive the response via the ARP protocol;

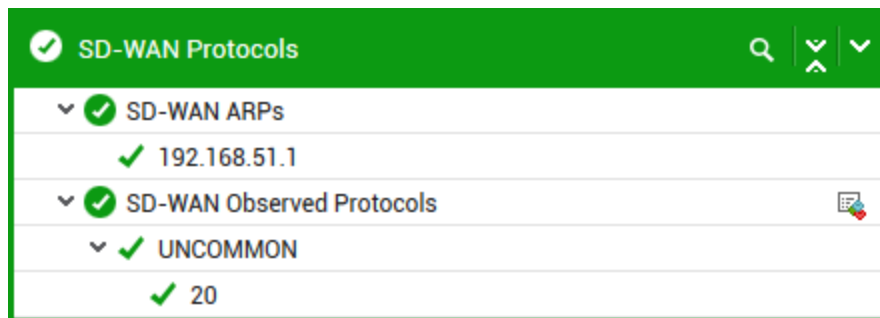- The data/packet traffic between LAN to WAN and WAN to LAN for each rule configured on the target appliance.



Figure 3.7: The SD-WAN Protocols Layer

### 3.6.1 SD-WAN ARPs Test

The Citrix SD-WAN appliance uses Address Resolution Protocol (ARP) to resolve the network layer addresses such as IPv4 addresses, into a link layer physical addresses such as MAC address, while handling traffic among multiple hosts on the network. For this purpose, the target appliance has an ARP look-up table that is populated with the IP addresses of the configured hosts and their equivalent MAC addresses. Lets say, if Host A wants to send a request to Host B in the SD-WAN environment, the request first reaches the target SD-WAN appliance. The appliance then starts looking into the ARP table to see if the MAC address for Host B already exists. If the IP address of Host B is available and active in the table, then the appliance will quickly pass the request to Host B and transfer the response received from Host B to Host A. If the IP address of Host B is not available in the table, then appliance will not be able to route the request to Host B. In such a case, Host A will send a broadcast packet to all hosts in the network using the ARP protocol. Now, the host (Host B) which owns the requested IP will respond to the broadcast with a unicast ARP reply to Host A. Sending the broadcast packet and getting response will take more time than directly receiving response from the destination. Therefore, it is necessary for administrators to know the availability status of the IP addresses in the ARP table to ensure fastest communication among the hosts. This is where the **SD-WAN ARPs** test helps!

This test auto-discovers the IP addresses stored in the ARP lookup table of the target Citrix SD-WAN appliance, and for each IP address, reports the current status. With the help of this measure, administrators can quickly find out whether the monitored IP address is active/dead/inactive in the look-up table and take remedial actions if the IP address is in the bad/inactive/dead state. In the process, this test also reveals the time taken for receiving the response for each IP address. This revelation will help administrators to figure out how quickly the requests are processed and investigate the abnormalities if the response is received with noticeable delay.

**Target of the test :** A Citrix SD-WAN

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for each IP address stored in the ARP look-up table of the Citrix SD-WAN appliance being monitored.

**Configurable parameters for the test**

| Parameter | Description |
| --- | --- |
| Test Period | How often should the test be executed. By default, this is set to 5 minutes. |
| Host | The IP address of the target SD-WAN appliance for which this test is to be configured. |
| Port | Refers to the port at which the target SD-WAN listens to. By default, this will be NULL. |
| Timeout | Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds. |
| Detailed Diagnosis | To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. |
|  | The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: |
|  | • The eG manager license should allow the detailed diagnosis capability |
|  | • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0. |

**Measurements made by the test**

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| State | Indicates current status of this IP address. | | The numeric values that correspond to each of the above-mentioned values are as follows:<br><br>| Measure Value | Numeric Value |<br>|---|---|<br>| Dead | 20 |<br>| Bad | 40 |<br>| Reply_pending | 60 |<br>| Ready_inactive | 80 |<br>| Ready_active | 100 |<br><br>**Note:**<br><br>By default, this measure reports one of the **Measure Value**s listed in the table above to indicate the current status of the IP address. The graph of this measure however, represents the same using the numeric equivalents alone.<br><br>The detailed diagnosis of this measure shows the Mac address of each IP address. In addition, the number of interfaces bound to each IP address and the VLAN details are also revealed. |
| Reply age | Indicates the time duration taken by this IP address to receive a response via the ARP protocol. | Seconds | A sudden/gradual increase in the value of this measure may indicate the slowdown in the network, which may lead to network congestion. |

## 3.6.2 SD-WAN Observed Protocols Test

A particular application in the network can be defined by the group of rules that is applied to it. The SD-WAN configuration editor provides a default list of rule groups, and also lets you to create

custom rule groups and tag individual rules to the application. Using the configuration editor, you can also create rules for traffic flow and associate the rules with applications and classes. You can specify criteria to filter traffic for a flow, and can apply general behavior, LAN to WAN behavior, WAN to LAN behavior, and packet inspection rules. It is important to monitor the LAN to WAN behavior, WAN to LAN behavior, and packet inspection rules periodically so that the any change in the WAN LAN behavior is identified instantly and preemptive measures taken accordingly. The SD-WAN Observed Protocols test helps administrators in taking these pre-emptive measures.

For each configured rule, this test reports the data/packet traffic between LAN to WAN and WAN to LAN. Using this test, administrators can figure out the rule that is most frequently used for LAN TO WAN data/packet transmission and vice versa.

**Target of the test :** A Citrix SD-WAN

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for the each *Rule Group:Rule ID* pair on the target appliance.

**Configurable parameters for the test**

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. By default, this is set to 5 minutes. |
| Host | The IP address of the target SD-WAN appliance for which this test is to be configured. |
| Port | Refers to the port at which the target SD-WAN listens to. By default, this will be NULL. |
| Timeout | Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds. |

**Measurements made by the test**

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| LAN to WAN data transmission | Indicates the amount of data transmitted over the LAN to WAN link for this rule during the last measurement period. | MB | An unusually high value of this measure may indicate a potential congestion or slowdown of traffic over the LAN to WAN link. It also indicates that you may have to reconfigure the appliance with more robust QoS policies to prevent such unpleasant |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | | | eventualities. |
| LAN to WAN packet transmission | Indicates the number of packets transmitted over the LAN to WAN link for this rule during the last measurement period. | Packets | |
| WAN to LAN data transmission | Indicates the amount of data transmitted over the WAN to LAN link for this rule during the last measurement period. | MB | A very high value of this measure may indicate a potential congestion or slowdown of traffic over the WAN to LAN link. It also indicates that you may have to reconfigure the appliance with more robust QoS policies to prevent such unpleasant eventualities. |
| WAN to LAN packet transmission | Indicates the number of packets transmitted over the WAN to LAN link based on this policy during the last measurement period. | Packets | |

## 3.7 SD-WAN Applications Layer

Using the tests mapped to this layer, administrators can measure effectiveness of application QoS policies and classes by tracking the traffic and identify the applications that are consuming high bandwidth.
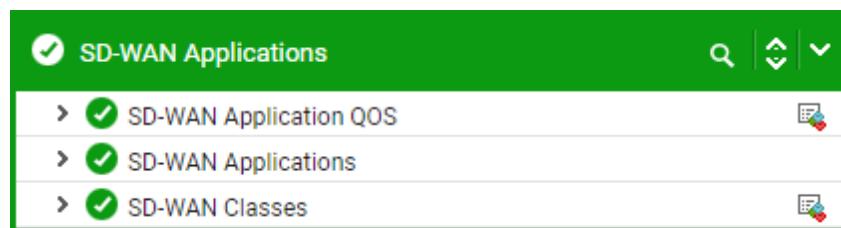


Figure 3.8: The SD-WAN Applications Layer

## 3.7.1 SD-WAN Application QOS Test

The SD-WAN network between the data center and branch offices transports a multitude of applications and data, such as high quality video or real-time voice. The SD-WAN network provides guaranteed, secure, measurable, and predictable services by managing the delay, jitter, bandwidth, and packet loss on the network. To achieve this and accelerate the traffic over the network, administrators define Quality of service (QoS) policies on the target SD-WAN appliance. The SD-WAN appliance has a sophisticated QoS engine that accesses the application traffic and prioritizes the traffic against other applications. With the QoS policies, administrators can set priority to critical traffic and control the traffic flow based on the requirements for WAN network quality. This way, administrators can prevent bandwidth hogging, and manage network bottlenecks to prevent data loss and packet drops. If the appliance is not configured with the right QoS policies, slowdowns during application accesses will become inevitable! To avoid this, administrators should continuously monitor the data/packet transmission performed based on each QoS policy, quickly identify the data/packet loss, and proceed to fine-tune the policies to ensure optimal performance. This is where the **SD-WAN Application QoS** test helps.

For each QoS policy, this test reports the amount of data transmitted to/from the LAN and WAN and the number of packets transmitted to/from the LAN and WAN. Using this revelation, administrators can measure how well the target appliance is managing the traffic over the WAN and LAN links based on the QoS policies, thus pointing to those policies that may require fine-tuning. This test also reports the amount of data and the number of packets dropped during the transmission, thus shedding light on the data/packet loss during the transmission at the earliest.

**Target of the test :** A Citrix SD-WAN

**Agent deploying the test :** An external agent

**Outputs of the test :** One set of results for each *global data center:data center: QoS policy* defined on the target Citrix SD-WAN appliance being monitored.

**Configurable parameters for the test**

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. By default, this is set to 5 minutes. |
| Host | The IP address of the target SD-WAN appliance for which this test is to be configured. |
| Port | Refers to the port at which the target SD-WAN listens to. By default, this will be NULL. |
| Timeout | Specify the time duration (in seconds) beyond which this test should time out in the |

| Parameter | Description |
|---|---|
| | Timeout text box. The default is 10 seconds. |
| Detailed Diagnosis | To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.<br><br>The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:<br><br>• The eG manager license should allow the detailed diagnosis capability<br><br>• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0. |

**Measurements made by the test**

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| LAN to WAN data transmission | Indicates the amount of data transmitted over the LAN to WAN link based on this QoS policy during the last measurement period. | MB | An unusually high value of this measure may indicate a potential congestion or slowdown of traffic over the LAN to WAN link. It also indicates that you may have to reconfigure the appliance with more robust QoS policies to prevent such unpleasant eventualities. |
| LAN to WAN packet transmission | Indicates the number of packets transmitted over the LAN to WAN link based on this policy during the last measurement period. | Packets | |
| WAN to LAN data transmission | Indicates the amount of data transmitted over the WAN to LAN link based on this policy during the last measurement period. | MB | A very high value of this measure may indicate a potential congestion or slowdown of traffic over the WAN to LAN link. It also indicates that you may have to reconfigure the appliance with more robust QoS policies to |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | | | prevent such unpleasant eventualities. |
| WAN to LAN packet transmission | Indicates the number of packets transmitted over the WAN to LAN link based on this policy during the last measurement period. | Packets | |
| Data dropped | Indicates the amount of data dropped during the data transmission between the LAN and WAN based on this policy. | MB | The value of this measure should be zero. |
| Packets dropped | Indicates the number of packets dropped during the packet transmission between the LAN and WAN based on this policy. | Packets | Ideally, there should be no packet drops during transmission. An increase in the value of this measure is an indicator that the appliance may not be able to service the traffic over the network. |

## 3.7.2 SD-WAN Applications Test

The Citrix SD-WAN appliance provides visibility to more than 4,000 applications at each network segment and branch to see what is happening inside application suites such as SharePoint Online within Office 365. With the target SD-WAN appliance, the bandwidth is used efficiently and intelligently reserved for critical applications during peak usage times. The amount of data transmitted/received by an application via the target appliance not only affects the user experience with that application, but also user productivity. If the non-critical applications are transferring more data than the business-critical applications, then the key business transactions will be delayed due to the higher amount of data traffic utilized by the non-critical applications. Therefore, it is a good practice to periodically run the **SD-WAN Applications** test and check the data transmission of each application via the target appliance.

This test auto-discovers the applications that are being accessed via the target Citrix SD-WAN appliance, and reports the amount of data received/transmitted by each application. This way, the test sheds light on the applications that are consuming high bandwidth due to which traffic congestion and slowness are recorded over the network.

**Target of the test :** A Citrix SD-WAN

**Agent deploying the test :** A remote agent

**Outputs of the test :** <mark>One set of results for each application accessed via the Citrix SD-WAN appliance.</mark>

**Configurable parameters for the test**

| Parameter | Description |
| --- | --- |
| Test Period | How often should the test be executed. By default, this is set to 5 minutes. |
| Host | The IP address of the target SD-WAN appliance for which this test is to be configured. |
| Port | Refers to the port at which the target SD-WAN listens to. By default, this will be NULL. |
| Timeout | Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds. |

**Measurements made by the test**

| Measurement | Description | Measurement Unit | Interpretation |
| --- | --- | --- | --- |
| Data received | Indicates the amount of data received by this application during the last measurement period. | MB | Comparing the values of these measures across the applications will help administrators to figure out which application consumed more bandwidth while receiving or transmitting data. |
| Data transmitted | Indicates the amount of data transmitted by this application during the last measurement period. | MB | |
| Total data | Indicates the amount of data received/transmitted by this application during the last measurement period. | MB | Compare the value of this measure across the applications to find out which application transmitted/received a large amount of data. |

## 3.7.3 SD-WAN Classes Test

The Citrix SD-WAN configuration provides a default set of application-classification, rule-filtering, and class-assignment settings that can be applied to any virtual path service in the SD-WAN environment. Using classes, administrators classify a specific type of traffic on the virtual path. To handle the traffic over the virtual path, the classes are associated with the rules based on the current

and expected traffic requirements. Each virtual path can have up to 17 (0-16) classes whereas each class is designated as Real-time, Interactive or Bulk. This, at a high level defines the overall priority of the class in terms of schedule time. By default:

- **Real-time (RT)** classes are used for VoIP or VoIP like applications, such as Skype or ICA audio. In general, we refer to voice only applications that use small UDP packets, that are business critical. Therefore. these classes are given the highest priority and gets up to 50% of the overall scheduler time. Each class can be weighted with respect to the other RT classes, for example, we could have two RT classes one that weighted to 70% and the other to 30%.

- **Interactive (INT)** classes are use for broadest category, and refer to any application that has a high degree of user interaction. Some of these applications, for example video conferencing, is sensitive to latency, and requires high bandwidth. Other applications like HTTPS, may need less bandwidth, but are critical to the business. The INT classes take the next priority to the RT classes and can consume the rest of the scheduler time as the traffic demands.

- **Bulk (BLK)** classes are used for high bandwidth traffic that can tolerate high latency. Applications that handle file transfer and need high bandwidth are categorized as bulk class. These applications involve very little human interference and are mostly handled by the systems themselves. The BLK classes take the lowest priority and can be considered scavenge classes. They can be weighted but they can be completely starved of bandwidth if the INT/RT traffic is consuming all of the scheduler time.

Administrators customize the classes and associate rules to have control over the traffic flow and also reduce manual workload when the network issue is reported. The efficiency of the classes can be measured by tracking the traffic handled by them. If any setbacks are detected in the traffic flow handled by any of the classes and are not addressed in time, data loss, delays and jitter may occur on the network. This in turn, may cause traffic congestion and slowness on the network and may lead to processing bottleneck. To avoid such anomalies, administrator should continuously monitor the data/packet transmission for each class configured on the Citrix SD-WAN appliance. This can be easily achieved using the **SD-WAN Classes** test.

This test auto-discovers the classes configured on the target Citrix SD-WAN appliance, and reports the type of each class. Additionally, this test reports the amount of data transmitted for each class, the amount of data that was pending and the amount of data dropped at regular intervals. In the process, this test also reveals the number of packets dropped during the transmission. Using the statistics reported by this test, administrators can find out how well the data/packet transmission handled using each class.

**Target of the test :** A Citrix SD-WAN

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for *each class* configured on the target SD-WAN appliance.

**Configurable parameters for the test**

| Parameter | Description |
|-----------|-------------|
| Test Period | How often should the test be executed. By default, this is set to 5 minutes. |
| Host | The IP address of the target SD-WAN appliance for which this test is to be configured. |
| Port | Refers to the port at which the target SD-WAN listens to. By default, this will be NULL. |
| Timeout | Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds. |

**Measurements made by the test**

| Measurement | Description | Measurement Unit | Interpretation |
|-------------|-------------|------------------|----------------|
| Class type | Indicates the type of this class. | | The numeric values that correspond to each of the above-mentioned values are as follows: <br><br> | Measure Value | Numeric Value | <br> | Realtime | 0 | <br> | Interact | 1 | <br> | Bulk | 3 | <br> | Other | 4 | <br><br> **Note:** <br><br> By default, this measure reports one of the **Measure Values**s listed in the table above to indicate the type of the class. The graph of this measure however, represents the same using the numeric equivalents alone. |
| Wait time | Indicates the time duration between transmitting packets for this class. | Seconds | A low value is desired for this measure. A sudden/consistent increase in the value of the measure is indicative of delay in packet transmission. |
| Data transmitted | Indicates the amount of | MB | |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | data transmitted for this class during the last measurement period. | | |
| Data pending to transmit | Indicates the amount of data to be transmitted for this class during the last measurement period. | MB | |
| Data dropped | Indicates the amount of data dropped for this class during the last measurement period. | MB | Ideally, this value should be zero. A non-zero value of this measure indicates the data loss and traffic congestion on the network. |
| Packets transmitted | Indicates the number of packets transmitted for this class during the last measurement period. | Packets | |
| Packets pending to transmit | Indicates the number of packets to be transmitted during the last measurement period. | Packets | |
| Packets dropped | Indicates the number of packets dropped during the last measurement period. | Packets | Ideally, this value should be zero. A non-zero value of this measure may indicate the traffic congestion on the network. |

# About eG Innovations

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

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

To learn more visit [www.eginnovations.com](www.eginnovations.com).

**Contact Us**

For support queries, email [support@eginnovations.com](support@eginnovations.com).

To contact eG Innovations sales team, email [sales@eginnovations.com](sales@eginnovations.com).