

# Network Validation for the Internet of Things (IoT)

## Table of Contents

<b>Introducing TeraVM .....</b>	<b>2</b>
Feature Guide Prerequisite.....	3
Introducing TeraVM replay functionality .....	3
Raw Port Playback.....	3
TCP Playback.....	3
UDP Playback .....	4
IP Playback .....	4
Substitution in Playback .....	4
<b>Configuring TeraVM for IoT traffic.....</b>	<b>5</b>
Per flow packet captures of IoT traffic .....	5
Implementing a packet capture on individual application flows .....	6
Implementing a packet capture at the Host (layer2-3) .....	7
Implementing a packet capture on a port or test interface .....	7
Raw port playback GUI configuration .....	7
TCP based IoT traffic capture playback GUI configuration.....	9
IoT TCP Playback Client configuration .....	11
UDP based IoT traffic capture playback GUI configuration .....	13
UDP Playback Sink configuration .....	13
UDP Playback Client .....	14
Emulating a scaled and mixed TCP/UDP IoT sensor driven network.....	16
TeraVM Global Settings configuration for IoT replay amplification .....	17
Using substitution to replace content in the IoT TCP replay files .....	21
Configuring a substitution .....	22
<b>TeraVM performance measurement for IoT replay applications .....</b>	<b>22</b>
Examining the performance of IoT test runs.....	22
Enable per second granularity performance views .....	23
Available Performance Metrics for IoT .....	24
Raw port stateless playback .....	24
TCP IoT playback.....	24
UDP IoT Playback .....	26

## Introducing TeraVM

TeraVM is an IP test solution enabling emulation of a wide range of network traffic types, which are used to test and measure performance of next-generation applications and networks. TeraVM enables emulation, control and performance measurements on a per flow basis which is ideal for representing many IP enabled device types. TeraVM was designed so that each IP flow is treated as a unique individual element.

TeraVM is the only solution today that can accurately represent individual and unique IoT devices at scale, using its proprietary replay functionality. TeraVM is unique as it offers not just the ability to replay a single IoT device on the network but thousands. TeraVM provides up to 1TB of storage capacity, ensuring as new IoT device types – sensors, actuators, etc come available that the traffic profile can easily be stored and used at any time, meeting the growing demand for the new world of digitization.

TeraVM offers the ability to replay IoT traffic profiles with files sizes up to 1.5GB, the largest in the market today.

To implement an IoT traffic flow in TeraVM requires two key components a host (layer 2-3) which is the stateful representation of the networked IoT device configuration e.g. IoT temperature sensor, and an application which is the representation of the traffic protocol (layer 4-7) running on the emulated IoT host.

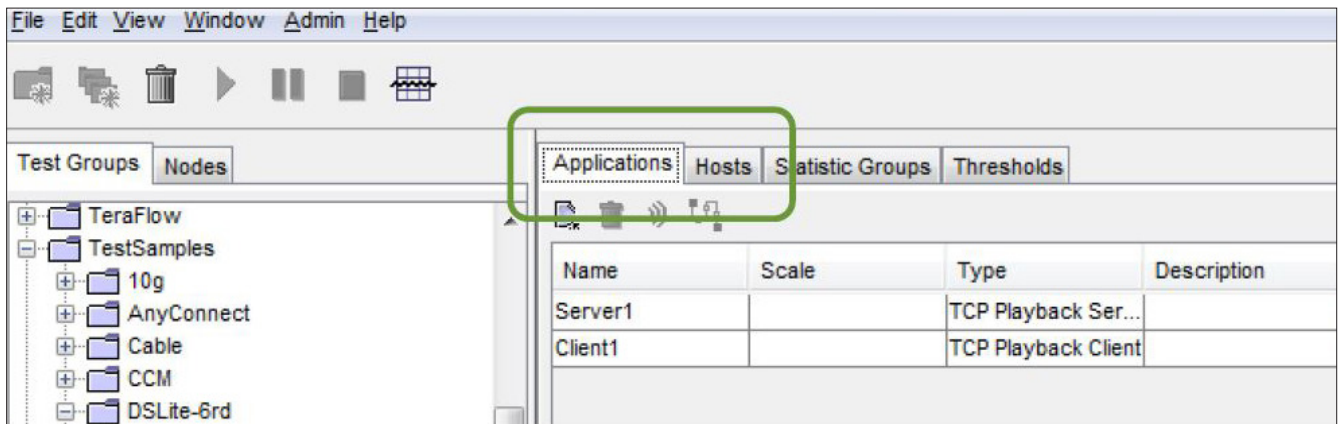


Figure 1: Applications and Host tabs as in the TeraVM GUI

## Feature Guide Prerequisite

The purpose of this document is to outline how to use the TeraVM to represent the stateful flows of IoT devices traversing the network/system under test (NUT/SUT), a prerequisite to this document is that the user is familiar with the basic structure of a test configuration using TeraVM software. For those users unfamiliar with the product, please visit the online customer portal or contact a member of the team for a selection of getting started user guides and video tutorials.

A further prerequisite of this document is that the user is familiar with packet capture tools. For the purpose of this document, the tool used to open and display packet capture files is "Wireshark".

For an introduction to Wireshark packet captures please visit – [http://www.Wireshark.org/docs/wsug\\_html\\_chunked/ChapterCapture.html](http://www.Wireshark.org/docs/wsug_html_chunked/ChapterCapture.html)

It's also assumed that the user has a fully installed and running TeraVM with the analysis tools integrated. Please see the "Getting started guides" for further details on how to integrate the packet analysis tools, using the system environmental variables of your local machine.

## Introducing TeraVM replay functionality

TeraVM provides 4 distinct replay types for representing IoT traffic: Raw port, TCP only, UDP only and IP.

### Raw Port Playback

Raw port as the name suggests is where TeraVM replays the capture file on the test port with no manipulation to any of the content in the file capture. Raw port playback tests are different to other tests in TeraVM, the differences are highlighted as follows:

- Raw port replay does not use a TeraVM host (layer2–3 configuration) to access the NUT.
- The application is completely stateless. No interaction with servers (internal or external to TeraVM).

### TCP Playback

The TCP playback feature is used to replay TCP conversations from the capture file. A TCP conversation consists of the entire set of messages exchanged between two clients involved in a single TCP connection i.e. after the opening SYN and before the closing FIN.

TeraVM allows users to configure a new host (layer 2-3 properties) to which the TCP conversation is parsed, thus replacing the original clients (layer 2-3 properties). A minimum configuration is to have two TeraVM hosts so as to exchange the source/destination parts of the original TCP conversation.

TeraVM's TCP playback enables:

1. Stateful replay of the TCP conversations.
2. Use of the current server time in timestamps or the ability to use the original timestamp of the packet capture.
3. Amplification of a single conversation to many conversations (IoT at scale).
4. Adjustable playback rates e.g. replay a conversation at twice the speed to increase the network load.
5. Substitution of content in the packet capture.

## UDP Playback

TeraVM's UDP playback enables users replay packet captures containing the connectionless protocol. To enable UDP playback, TeraVM requires a minimum of two emulated TeraVM hosts (layer 2-3 configurations). The first host will be the source of the uni-directional conversation and the second is the destination address for the conversation (acts as a sink for the conversation).

TeraVM's UDP playback enables:

1. Stateful replay of the UDP conversations
2. Amplification of a single conversation to many conversations.
3. Adjustable playback rates e.g. replay a conversation at twice the speed to increase the network load.

## IP Playback

TeraVM's IP playback enables users replay complete packet captures containing both TCP and UDP encapsulated payloads. In this instance the user has the ability to map new IP and MAC addresses for existing addresses, whilst maintaining the integrity of the layer 4-7 payload.

A key benefit of TeraVM's IP replay is that the one packet capture can be used to deliver varied load scenarios; that is the user can replay:

- Complete IoT capture files
- Capture files with only the newly mapped IP addresses i.e. (filter out packets which have not been mapped with a new IP address)
- Capture files based on a specified transport protocol
- Amplified traffic load conditions with any of the above settings (IoT at scale)

## Substitution in Playback

A differentiating feature of TeraVM's replay functionality for IoT is the ability to substitute content in the packet capture. For example – a packet capture may be a temperature sensor value, substitution enables the user change the temperature value on each connection e.g. substitute a value "20" for "16" in the temperature data.

TeraVM allows multiple substitutions per packet capture. The user simply defines the substitution offset and the content to be replaced.

# Configuring TeraVM for IoT traffic

## Per flow packet captures of IoT traffic

TeraVM enables replay of 3rd party IoT packet captures. The following section highlights how to use TeraVM's capture tools during a test run. The TeraVM graphical user interface (GUI) is presented in figure 1 below. A key aspect of the GUI is the integrated packet capture management tab. The tab lists all the packet captures a user has implemented during the lifetime of the GUI being opened. Packet captures are dynamic in nature and a user can at any time implement a capture of the traffic in the test run.

*The packet captures are only available in the GUI for the duration of which the GUI is opened by the user. If packet captures caught during the test run are required for later use, they should be stored on a local machine before the GUI is closed.*

Packet captures can be implemented at 3 levels in TeraVM:

- Node: Capture all the traffic at the test interface
- Host: Traffic associated with a specific emulated device
- Application: The actual application conversation between endpoints

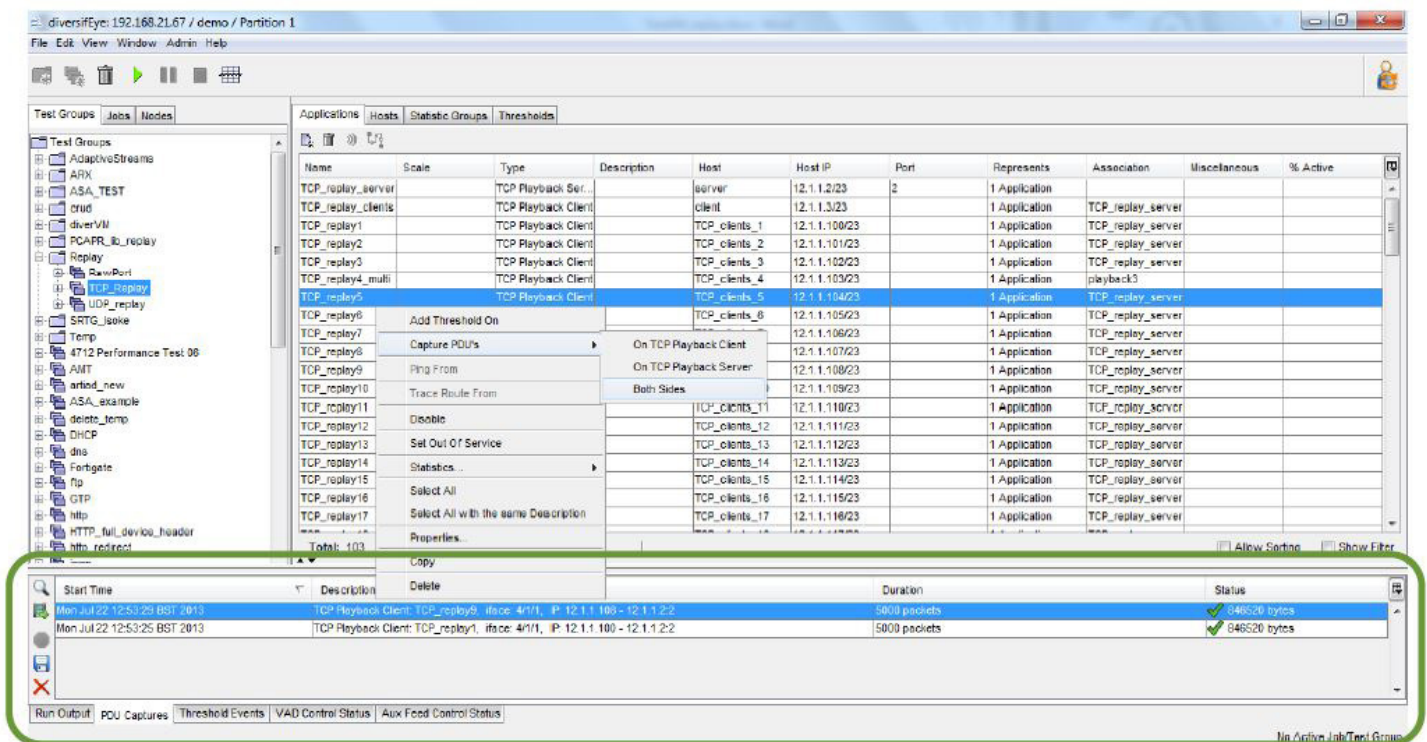


Figure 2: The TeraVM GUI, highlighted is the integrated packet capture management tab

A packet capture may be configured prior to a test being set to play e.g. include in the capture a complete IP address allocation for the emulated IoT host. At some random time into the test run a user can again choose to do a further packet capture on the same host, there is no limits to the number of captures a user may implement on a flow.

### Implementing a packet capture on individual application flows:

1. Select the "Applications" tab in the main GUI window.
2. Left mouse click on a row of interest in the GUI to highlight the flow of interest.
3. Right mouse click on the flow. On the window displayed, hover the mouse pointer over "Capture PDU's".
4. Select from the displayed options the packet capture type required e.g. for TCP replay it's possible to capture on the TCP replay client or the TCP replay server or for both sides.

**1. PDU Capture**

**PDU Capture**

Packets will be captured for the following TCP Playback Client application on the specified interface:

**Application:** TCP\_replay5  
**Interface:** 4/1/1

The capture will be controlled by the following configuration settings:

**Packet Count:** 5000  
**Time Duration:**   
**Packet Length:**   
**Transport Protocol:** TCP

Every Incoming/Outgoing packet with any of the following IP Address pairings as source/destination addresses (or vice-versa) will be captured.

IP Address 1	Port 1	IP Address 2	Port 2
12.1.1.104		12.1.1.2	2

< Prev   Next >   **Finish**   Cancel

Figure 3: Define the packet capture limiting parameters

5. In the window displayed (Figure 3) define the packet capture limiting parameters:
  - a. Packet captures limits are set via a packet count, time parameters or packet length.
  - b. Default capture limit is 5000 packets. However, a user may define a value for all 3 inputs. The capture will stop when any one of the parameters matches the input value.
  - c. Users can edit the IP address and port filters.
    - i. To edit the filter parameter: double left mouse click on the cell to access.
  - d. Select Finish

A user can edit the IP Address and Port filters by left mouse clicking on the cells, to capture all visible packets delete all the entries.

6. The packet capture to be implemented is displayed as the first row in the "PDU Capture" management tab (as shown in Figure 1).
7. Using the "Status" column in the "PDU Captures" tab, a user can determine at which stage the capture is at.
  - a. Capture is running the number displayed will increment i.e. showing activity on the entity under question.
  - b. To stop a capture at any time left mouse the stop symbol in the left hand margin.
  - c. To view the capture, double left mouse click on the row in question. This will automatically open an analysis tool such as Wireshark.

### **Implementing a packet capture at the Host (layer2-3):**

1. Select the "Hosts" tab in the main GUI window.
2. Left mouse click on a row of interest in the GUI to highlight the Host of interest.
3. Right mouse click on the Host. On the window displayed, hover the mouse pointer over "Capture PDU's and select "HOST".
4. Follow on the configuration as per the steps from Step 4 in the section 2.1.1 above.

### **Implementing a packet capture on a port or test interface:**

1. Select the "Nodes" tab in the main GUI window.
2. Left mouse click on a "Test module" to which the test interface is associated.
3. Highlight the card of interest with a left mouse click, expand the interfaces by left mouse clicking on the expand button labelled "+".
4. Left mouse click the interface required for the packet capture. Right mouse click on the interface to display a menu list and select "Capture PDUs".
5. Follow on the configuration steps from Step 4 in the section 2.1.1 above. There is one subtle difference to Figure 2, users have the option to define a filter for the direction of the traffic on which a packet capture is implemented.

## **Raw port playback GUI configuration**

Raw port playback is the easiest of the playback functions to configure for IoT, it's assumed a user is familiar with test configuration in TeraVM and understands the difference between TeraVM Applications and Hosts. In order to pass traffic successfully in a network, the user is required to manipulate the MAC address of the first hop in the capture file. This is a stateless dump of traffic into the network/system under test.

To configure a raw port playback for use for IoT packet capture, use the following steps:

1. Highlight the "Test Groups" folder with a left mouse click. With a right mouse click display the configuration menu, choose to create a test folder or a test group for the dedicated raw port playback.
2. Left mouse click the newly created test group to display the "Applications" and "Hosts" configuration menus.
3. Left mouse click the "Applications" tab, with a left mouse click select the "Add New Applications" icon, from the displayed list mouse over the menu item "Raw Port Playback". Left mouse click the "Raw Port Playback Application" menu item.

*If the menu item is greyed out a license is required to enable the feature, contact your local representative in order to enable the menu item.*



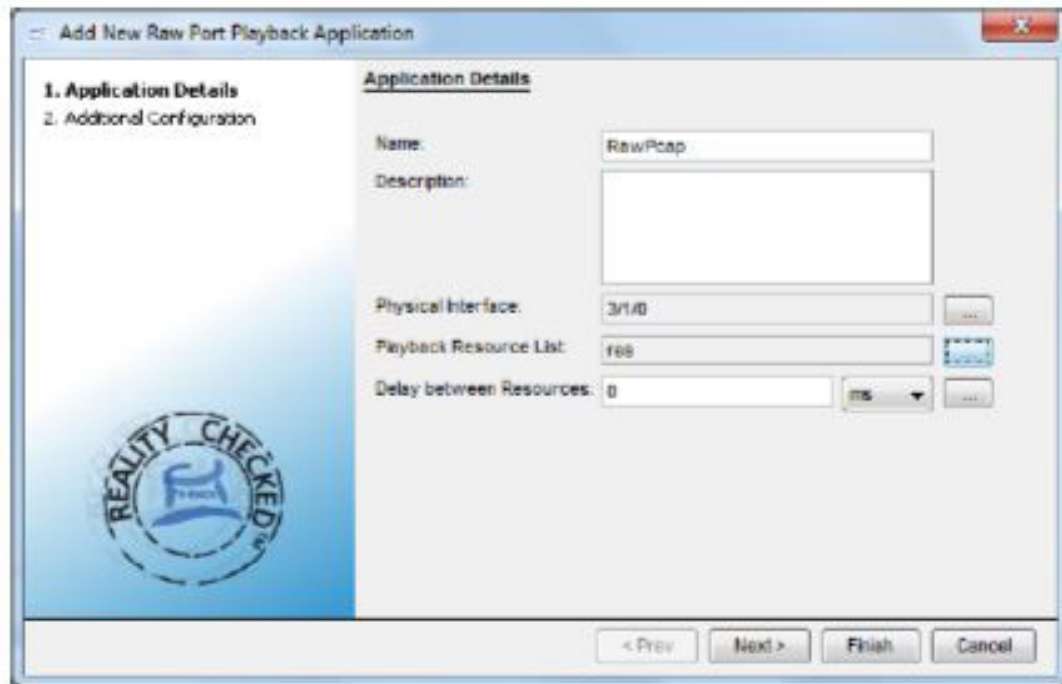


Figure 4: Raw port playback application

4. Complete the configuration by filling the basic parameters as shown in Figure 4 .
  - a. Assign a name to the IoT replay function and description (optional).
  - b. Select the test interface in which the packet capture will be dumped through using the icon on the far right.
  - c. Select the resource or the packet capture that will be place on the test interface.
  - d. Set a delay between repeated replays of the packet capture, default is zero meaning no delay between repeated replays.
5. Using the "Next" button displays the "Additional Configuration" items. These are standard configuration items on all applications and hosts in TeraVM, for more details on exact use see the Help menu, the default settings are enough to begin basic testing.
6. To begin the test, simply press play in the main menu icon bar.

*Raw port playback limits the file replay to one file per interface, if more than one file is required either a) use multiple interfaces or b) use Wireshark's "mergcap" command to merge the separate files into a single file.*



## TCP based IoT traffic capture playback GUI configuration

TeraVM's TCP replay enables stateful replay of the IoT capture file, a minimum of two emulated hosts are required in order to parse the conversation for bi-directional communication. For users new to TeraVM, please see the getting started guide or visit the customer portal on the website for video tutorials on how to configure a host.

To configure a TCP replay of the IoT conversation use the following steps:

### Host configuration

1. Highlight the "Test Groups" folder with a left mouse click. With a right mouse click display the configuration menu, choose to create a test folder or a test group for the TCP playback.
2. Left mouse click the newly created test group to display the "Applications" and "Hosts" configuration menus.
3. Left mouse click the "Hosts" tab, with a left mouse click select the "Add New Host(s)" icon.
4. Complete the host configuration, key things to note when completing the host configuration is the name e.g. client, IP address and MAC address being assigned to the emulated host. The IP and MAC address parameters are parsed into the IoT TCP replay conversation.
5. Repeat step 4 for the second host used in the IoT TCP conversation replay again noting the client name e.g. server, IP and MAC addresses.

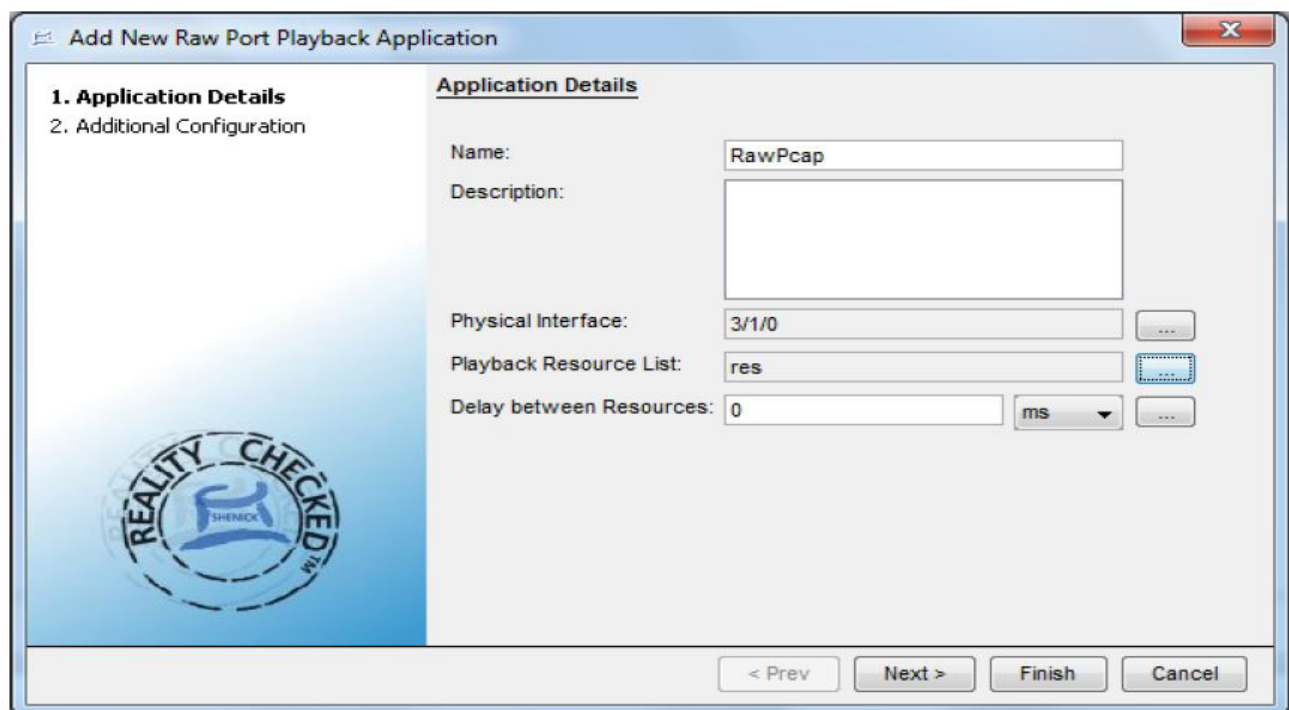


Figure 5: A sample TeraVM host configuration

6. Left mouse click the "Applications" tab, with a left mouse click select the "Add New Applications" icon, from the displayed list mouse over the menu item "TCP Playback". Left mouse click the "TCP Playback Server" menu item.

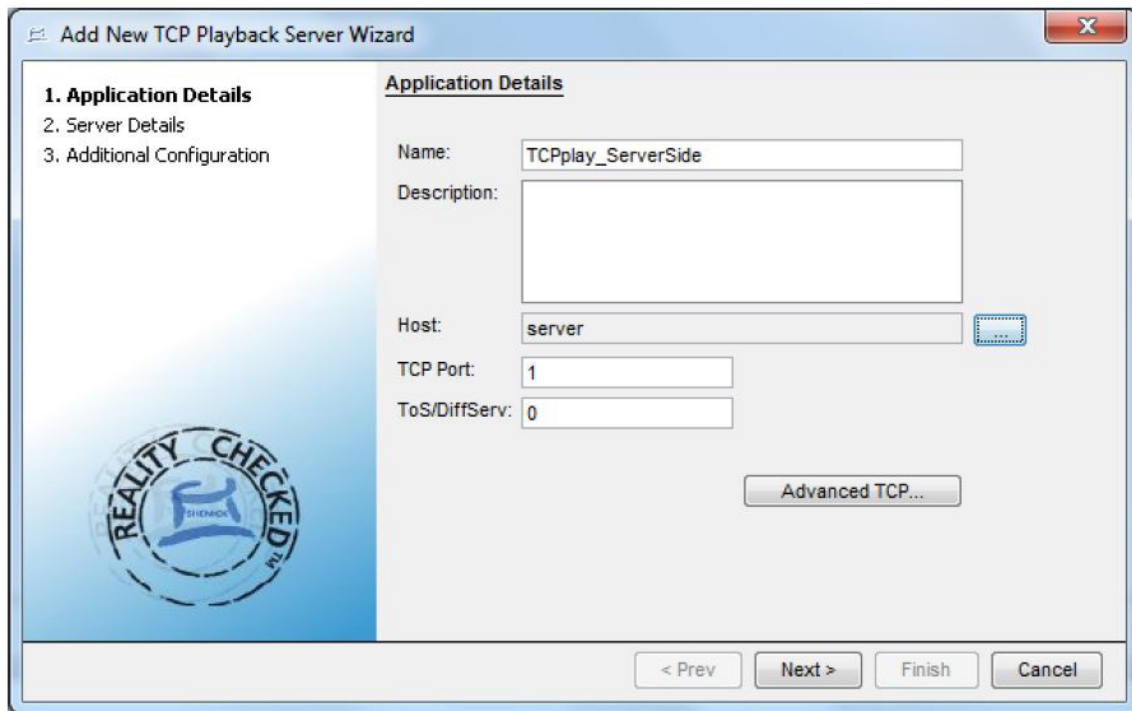


Figure 6: TCP Playback Server side configuration

7. Complete the Application Details configuration
  - a. Assign a Name and a Description (optional) to the server side of the IoT conversation
  - b. Select the preconfigured Host (Figure 5 shows a Host by the name server is used)
  - c. Optional: Assign a TCP port for the server side to listen on, the default value is 1.
  - d. Optional: Assign a TOS/Diffserv value, the default value is 1.
  - e. Select Next to continue the configuration.
8. Complete the IoT server side Details configuration
  - a. Begin by selecting the unique IoT packet capture file which will be used in the replay. Left mouse click the button to the immediate right of the Resource List field entry
    - i. In the newly displayed window, left mouse click the "Add" button half way down the window
    - ii. In the newly displayed window, assign a name to the resource being replayed and then left mouse click the "Add" button on the right of the window.
    - iii. Leave the "Type" in the default state of "Capture File", browse to the file on your local machine by left mouse clicking on the button to immediate right of "File" field.
    - iv. Complete the process of selection by left mouse clicking "OK" twice to close the "Add Playback Resource" and "Add Playback Resource List".
    - v. In the "Select Playback Resource list" window, left mouse click on the file replay resource required in the "Choose Selection" section. Complete the selection by left mouse clicking the "Select" button.

- b. "Use Capture Timings" left mouse click the check box if the original timings are to be used. If unchecked TeraVM will use replace the timing stamps with the current timestamp on the server.
- c. Select the "Next" button to continue.

9. Complete the Additional configurations (optional)

- a. Enable Normal Statistics: Default – select for statistic collection on a 10 second basis
- b. Enable Fine Statistics: Default – select for statistic collection on a per second basis
- c. Aggregate Group: select a grouping of similar like applications to produce an average measurement.

*To replay multiple IoT packet capture files a user will need to configure a playback server for each packet capture type.*

### IoT TCP Playback Client configuration

10. Left mouse click the "Applications" tab, with a left mouse click select the "Add New Applications" icon, from the displayed list mouse over the menu item "TCP Playback". Left mouse click the "TCP Playback Client(s)" menu item.

**Add New TCP Playback Client(s) Wizard**

**1. Application Details**  
2. Client Details  
3. Additional Configuration

**Application Details**

No. of Clients: 1

Configure As: Single Client per Row

Name: TCPplay\_ClientSide

Description:

Host(s): client

TCP Port: ☐ Use Next Available

ToS/DiffServ: 0

Advanced TCP...

< Prev Next > Finish Cancel

Figure 7: TCP Playback Client side configuration

## 11. Complete the Application Details configuration

- a. Assign a Name and a Description (optional) to the client side of the conversation
- b. Select the preconfigured Host (Figure 5 shows a Host by the name client is used)
- c. Optional: Assign a TCP port for the client side to listen on, the default value is to Use Next Available.
- d. Optional: Assign a TOS/Diffserv value, the default value is 1.
- e. Select Next to continue the configuration.

*Advanced TCP settings are used to define a limited number of characteristics such as segment size, transmit buffer size, window size, etc. There is also the ability to rate limit the application requests. See the Help menu item for more details on available configuration options.*

## 12. Complete the Client Details configuration

- a. Server: Use the button to the right of the "Server" field to select the other participant in the conversation, which has already been configured.
- b. Resource List: Select the conversation in which the client will be part of, left mouse click the button to the right. From the window displayed left mouse click on the resource in the resource list selection and click the "Select" button.
- c. Delay Between Connections: If the user wishes to inject a delay between file replays the user can do this by increasing the time from the default 0.
- d. "Use Capture Timings" left mouse click the check box if the original timings are to be used. If unchecked TeraVM will use replace the timing stamps with the current timestamp on the server.
- e. Select the "Next" button to continue.

## 13. Complete the Additional configurations (optional)

- a. Start Time: Enter a value for when the conversation should commence, this is seen as delay from when the test is started.
- b. Stop Time: Enter a value for when the conversation should end. In conjunction with the start time, this is the duration for which the conversation is active in the lifetime of the test run.
- c. Enable Normal Statistics: Default – select for statistic collection on a 10 second basis
- d. Enable Fine Statistics: Default – select for statistic collection on a per second basis
- e. Aggregate Group: select a grouping of similar like applications to produce an average measurement.

## 14. Select "Finish" to complete the configuration. To begin the test, simply press play in the main menu icon bar.

*To amplify an IoT conversation (representing scaled connection of IoT devices) simply repeat the TCP Playback Client configuration as many times as necessary. Amplification is simplified by using the scaled entities (single row entry for multiple hosts and applications) in TeraVM, see the Help menu for more details on using scaled entities.*

## UDP based IoT traffic capture playback GUI configuration

TeraVM UDP replay enables stateful replay of UDP based IoT capture files, a minimum of two emulated hosts are required in order to parse the conversation for the unidirectional communication. A client host will act as a source of the communication and a second host is used to sink the traffic flow. For users new to TeraVM, please see the getting started guide or visit TeraVM's customer portal on the TeraVM website for video tutorials on how to configure a host.

To configure a UDP replay for IoT use the following steps:

### Host configuration

1. Highlight the "Test Groups" folder with a left mouse click. With a right mouse click display the configuration menu, choose to create a test folder or a test group for the UDP playback.
2. Left mouse click the newly created test group to display the "Applications" and "Hosts" configuration menus.
3. Left mouse click the "Hosts" tab, with a left mouse click select the "Add New Host(s)" icon.
4. Complete the host configuration, key things to note when completing the host configuration is the name e.g. source, IP address and MAC address being assigned to the emulated host. The IP and MAC address parameters are parsed into the UDP traffic replay.
5. Repeat step 4 for the second host used in the UDP traffic replay again noting the parameter details e.g. sink, IP and MAC addresses.

### UDP Playback Sink configuration

6. Left mouse click the "Applications" tab, with a left mouse click select the "Add New Applications" icon, from the displayed list mouse over the menu item "UDP Playback". Left mouse click the "UDP Playback Sink" menu item.

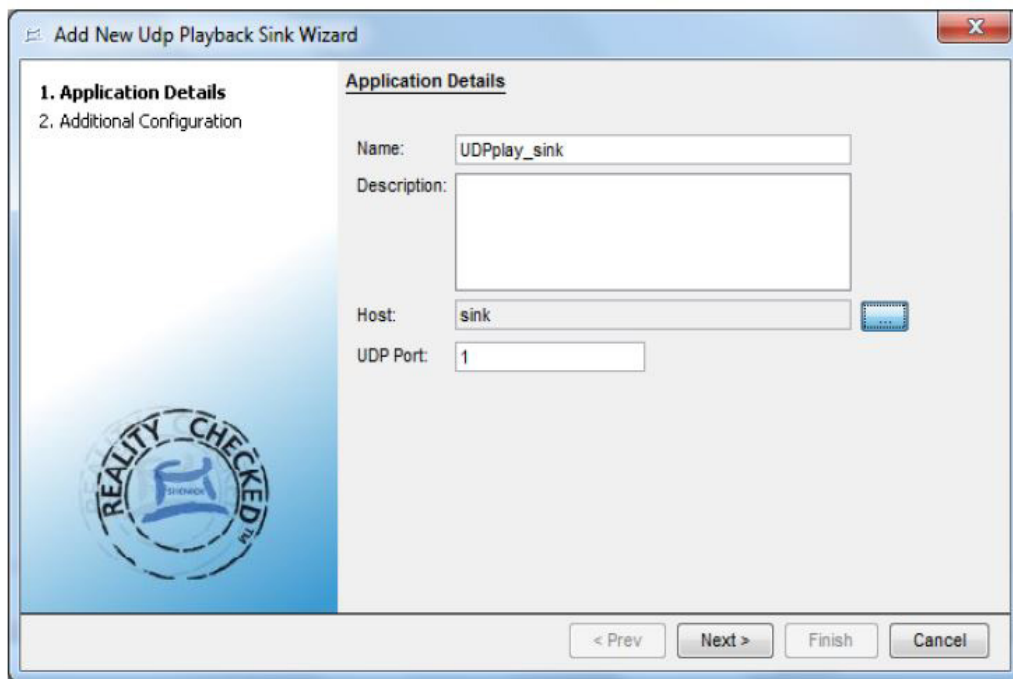


Figure 8: UDP Playback sink configuration

7. Complete the Application Details configuration
  - a. Assign a Name and a Description (optional) to the sink (UDP terminator)
  - b. Select the preconfigured Host (Figure 5 shows a Host by the name sink is used)
  - c. Optional: Assign a UDP port for the sink side to listen on, the default value is 1.
  - d. Optional: Assign a TOS/Diffserv value, the default value is 1.
  - e. Select Next to continue the configuration.
8. Complete the Additional configurations (optional)
  - a. Enable Normal Statistics: Default – select for statistic collection on a 10 second basis
  - b. Enable Fine Statistics: Default – select for statistic collection on a per second basis
  - c. Aggregate Group: select a grouping of similar like applications to produce an average measurement.

*A TeraVM UDP Playback Sink application can sink more than one UDP IoT replay file.*

## UDP Playback Client

9. Left mouse click the "Applications" tab, with a left mouse click select the "Add New Applications" icon, from the displayed list mouse over the menu item "UDP Playback". Left mouse click the "UDP Playback Source(s)" menu item.

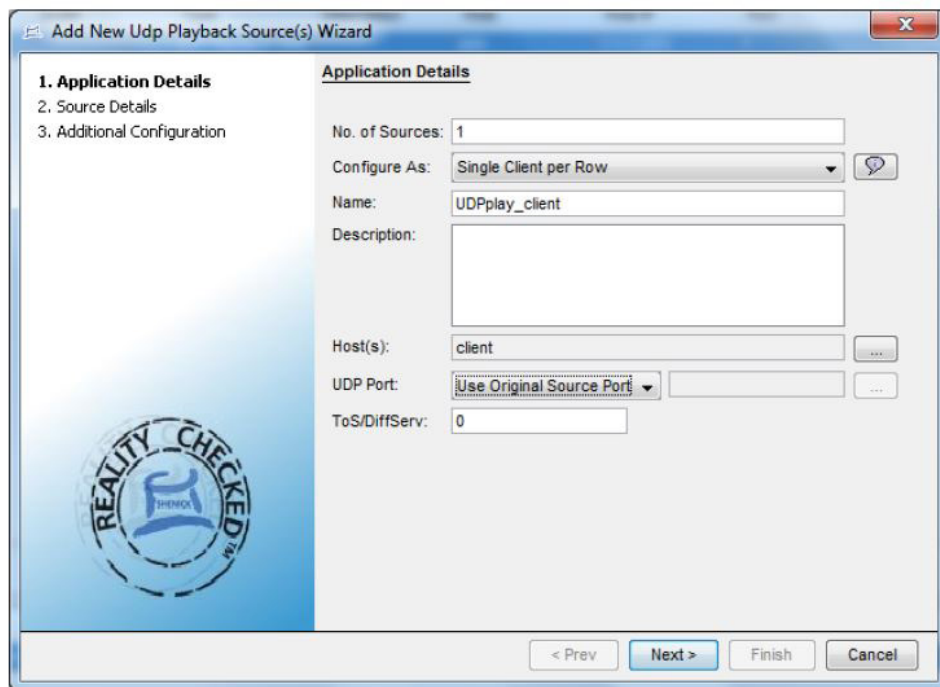


Figure 9: UDP Playback source configuration

## 10. Complete the Application Details configuration

- a. Assign a Name and a Description (optional) to the client side or UDP source
- b. Select the preconfigured Host (Figure 9 shows a Host by the name client is used)
- c. Optional: Assign a UDP port for the UDP source to listen on, the default value is "Use Original Source Port". Other options include use next available or to define a port value or port value ranges.
- d. Optional: Assign a TOS/Diffserv value, the default value is 1.
- e. Select Next to continue the configuration.

## 11. Complete the Source Details configuration

- a. Sink: Use the button to the right of the "Sink" field to select the destination for the UDP traffic, which has already been configured.
- b. Resource List: begin by selecting the packet capture file which will be used in the replay. Left mouse click the button to the immediate right of the Resource List field entry -
  - i. In the newly displayed window, left mouse click the "Add" button half way down the window
  - ii. In the newly displayed window, assign a name to the resource being replayed and then left mouse click the "Add" button on the right of the window.
  - iii. Leave the "Type" in the default state of "Capture File", browse to the file on your local machine by left mouse clicking on the button to immediate right of "File" field.
  - iv. Complete the process of selection by left mouse clicking "OK" twice to close the "Add Playback Resource" and "Add Playback Resource List".
  - v. In the "Select Playback Resource list" window, left mouse click on the file replay resource required in the "Choose Selection" section. Complete the selection by left mouse clicking the "Select" button.
- c. Delay Between Streams: If the user wishes to inject a delay between file replays the user can do this by increasing the time from the default 0.
- d. Rate Multiplier: A user may increase the UDP throughput by increasing the rate beyond 1, to decrease the UDP throughput enter a value greater than 0 and less than 1 e.g. 0.5 = half throughput.
- e. ARP/DNS Delay: TeraVM initiates an Address Resolution Protocol or Neighbor Solicitation (ARP/NS) request in order to locate the sink host, the user has the option to control the wait time between the ARP/NS and the transmission of the first packet from the packet capture file. By default this is 500 milliseconds or minimum wait time.
- f. Select the "Next" button to continue.

## 12. Complete the Additional configurations (optional)

- a. Start Time: Enter a value for when the conversation should commence, this is seen as delay from when the test is started.
- b. Stop Time: Enter a value for when the conversation should end. In conjunction with the start time, this is the duration for which the conversation is active in the lifetime of the test run.



- c. Enable Normal Statistics: Default – select for statistic collection on a 10 second basis
- d. Enable Fine Statistics: Default – select for statistic collection on a per second basis
- e. Aggregate Group: select a grouping of similar like applications to produce an average measurement.

13. Select "Finish" to complete the configuration. To begin the test, simply press play in the main menu icon bar.

*To amplify an IoT conversation simply repeat the UDP Playback Source configuration as many times as necessary, amplification is simplified by using the scaled entities (single row entry for multiple hosts and applications) in TeraVM, see the Help menu for more details on using scaled entities.*

## Emulating a scaled and mixed TCP/UDP IoT sensor driven network

TeraVM IP replay enables stateful replay of an IoT capture file whilst maintaining the integrity of the layer4-7 payload. To use this feature the user must be familiar with TeraVM hosts and subnet hosts. In addition the user is require to use the TeraVM web management interface in order to complete the IP address mappings.

*TeraVM's IP playback is used where it's important to maintain the integrity of the transport protocol handshake, this includes the complete SYN and FIN transaction process.*

Point a browser at the web management interface on the TeraVM controller e.g. [http://TeraVM\\_Controller\\_IPAddress/admin/global/](http://TeraVM_Controller_IPAddress/admin/global/)

From the categories section select the "IP Replay Client Settings", to view the available parameters.

In order to show how to configure IP replay for IoT amplification, the following back to back user scenario is demonstrated using two test interfaces.

Demonstration Scenario		
Amplify a typical IoT traffic profile to represent 100 sensors on a network interface, the original packet capture will contain a mix of TCP and UDP application traffic. Remap the following addresses:		
Original		Mapped To
192.168.1.103	>	192.168.1.100 (the start IP address for 100 IoT sensors)
80.56.12.11	>	100.1.1.2

*In order to quickly build a packet capture of TCP and UDP IoT sensors use Wireshark to capture an interface which has both UDP and TCP activity.*

## TeraVM Global Settings configuration for IoT replay amplification

1. Point a browser at <http://TeraVM\_Controller\_IPaddress/admin/global/>, from the categories section select the "Host Settings".
2. Left mouse click the check box immediate right of the "Disable RESETs/ICMP Port Unreachable messages for TCP/UDP packets to non-listening ports:"
3. Select "Save".

Home Admin Client Install Automation Miscellaneous Online Help

Home > Admin > Global Settings

Version: 010.02.00, diversifEye 10.2, build 132, gcc 2.96, libm 2.2.93, Date: 2013-03-27 14:12:46 +0000 Revision: 74574  
Config Revision: 72635, Modifying config for: All

Categories: Host Settings

Key Logging for IKE/IPsec: OFF

Pseudo-randomise selection of the initial unprivileged TCP port: ☐

Disable RESETs/ICMP Port Unreachable messages for TCP/UDP packets to non-listening ports: ☒

Generate GTP-U Traffic: (tunnel indirect Host traffic between Direct Host and G/W, ignoring Inbound TEID): ☐

Fake an ACK for unmatched TCP SYN-ACKs, (enhanced SYN Flood): ☐

Fake an ACK for unmatched TCP Data Segments, (enhanced GET Flood): ☐

Save Reset

US : 1900 McCarthy Boulevard, Suite 301, Milpitas, CA 95025 Tel: 408-385-7420  
Europe : Brook House, Corrig Avenue, Donaghmore, Co. Dublin, Ireland Tel: +353-1-236-7002

Figure 10: Global settings for Host settings

4. On the global settings page select from the categories section the "IP Replay Settings".
5. In the newly displayed web page, enter a value for "Number of Mappings:" and select "Save".

Demonstration Scenario		
Number of Mappings required is 3 i.e.		
Original		Mapped To
192.168.1.103	>	192.168.1.100 (start IP address for 100 IoT sensors)
80.56.12.11	>	100.1.1.2
89.76.21.12	>	100.1.1.3

Home Admin Client Install Automation Miscellaneous Online Help

Home > Admin > Global Settings

Version: 010.02.00, diversifEye 10.2, build 132, gcc 2.96, i386, glibc 2.2.93, Date: 2013-03-27 14:12:46 +0000 Revision: 74574  
Config Revision: 72635, Modifying config for: All

Categories: IP Replay Settings

IP Protocol Filter, (limits replay to the specified transport protocols): All

Vary TCP/UDP Unprivileged Port numbers and TCP Sequence/ACK numbers: ☒

Comma-separated list of Unprivileged Ports to leave unchanged when varying Port numbers is enabled: 5060,443

Replay Timing Multiplier, (e.g. 1.0 = normal speed, 0.5 = 2 X normal, 2.0 = half speed): 1

Replay packets with unmapped IP Addresses: ☒

Number of Mappings: 3

Map From IP Address: 192.168.1.103	To IP Address: 192.168.1.100	Address Count: 100
Map From IP Address: 86.47.113.237	To IP Address: 100.1.1.2	Address Count: 1
Map From IP Address: 80.111.206.78	To IP Address: 100.1.1.3	Address Count: 1

Save Reset

Figure 11: IP Replay configuration settings

6. Repeat step 4, select from the categories section the "IP Replay Settings".
7. Complete the Address mapping as follows
  - a. Enter a value for "Map From IP Address:" i.e. the original IP address
  - b. Enter a value for "To IP Address:" i.e. the new IP address
  - c. Optional: Address Count. Leave as default 1 or enter a value greater than 1 to replay the packets associated with the original IP address on more than one emulated endpoint.
8. Optional: "IP Protocol Filter": a user can define to replay all protocols in the packet capture or limit the protocols to TCP only, UDP only or TCP and UDP only. Default All.
9. Optional: "Vary TCP/UDP Unprivileged Port numbers and TCP Sequence/ACK numbers:" a user can define if each replay should use new values on each new loop of the replay file. Default disabled. Left mouse click on the checkbox to enable.
10. Optional: "Comma-separated list of Unprivileged Ports to leave unchanged when varying Port numbers is enabled:" a user can define to retain a port number for specific applications e.g. SIP – 5060, HTTPS – 443 if step 9 is enabled. Default blank.
11. Optional: "Replay Timing Multiplier" a user can increase or decrease throughput by entering a value less than 1 or more than 1 respectively, this setting works by adapting the time between packets. Default blank i.e. normal rate
12. Optional: "Replay packets with unmapped IP Addresses:" include the packets which have not been assigned a new IP address. Default is unchecked i.e. packets with no affiliation to the IP address mapping are excluded.
13. Select "Save" to complete the configuration.

## Host configuration

14. In the TeraVM GUI highlight the "Test Groups" folder with a left mouse click. With a right mouse click display the configuration menu, choose to create a test folder or a test group for the UDP playback.
15. Left mouse click the newly created test group to display the "Applications" and "Hosts" configuration menus.

16. Left mouse click the "Hosts" tab, with a left mouse click select the "Add New Host(s)" icon.

- a. Create a virtual subnet host for the IoT network, this is used to map the original IP address to many IP addresses (Demonstration Scenario is for 100 new IoT sensors)
  - i. Name: enter a suitable name value and description (optional)
  - ii. Type: select "Virtual Subnet Host"
  - iii. Network Visible: Enabled
  - iv. IP Address: Enter a network address (using the Demonstration Scenario the request start address is 192.168.1.100 therefore network address is 192.168.1.0)

The screenshot shows the 'Add New Host(s) Wizard' window. On the left, a sidebar lists five steps: 1. General Details (selected), 2. Link Layer Details, 3. Configure Statistics Settings, 4. Activity Settings, and 5. Additional Configuration. The main area is titled 'General Details' and contains several input fields. A green rectangular box highlights the 'Type' dropdown menu, which is currently set to 'Virtual Subnet Host'. Other visible fields include 'No. of Hosts' set to 1, 'Configure As' set to 'Single Host per Row', 'Name' set to 'Subnet\_100users', an empty 'Description' field, a checked 'Network Visible' checkbox, 'IP Address' set to '192.168.21.0/24', and an empty 'Gateway Host' field. At the bottom right, there is an 'Advanced...' button. At the bottom of the window, there are four navigation buttons: '< Prev', 'Next >', 'Finish', and 'Cancel'.

Figure 12: A subnet host selection

- v. Complete the IoT subnet host configuration, key things to note when completing the host configuration is the MAC address and the interface on which the subnet (100 emulated IoT devices) are using.
- b. Create an additional two hosts, this time the "Type" is configured as the standard "Virtual Host".
  - i. IoT Host1: will have an IP address 100.1.1.2 (using the Demonstration Scenario the request address map is 80.56.12.11 > 100.1.1.2)
  - ii. IoT Host2: will have an IP address 100.1.1.3 (using the Demonstration Scenario the request address map 89.76.21.12 > 100.1.1.3)
- c. Create a host using the type "External Host"
  - i. extGW: assign an IP address 192.168.1.1

- d. Assign the "Gateway" for the Hosts as follows (see Figure 13):
  - i. IoT HOST1 > extGW
  - ii. IoT HOST2 > extGW
  - iii. Subnet\_100\_users (IoT sensors) > HOST1

Name	Scale	Interface	IP Assignment	IP Address	G/W Host	G/W IP Address	Description	Type	%
HOST1		4/1/0	Static	100.1.1.2/24	extGW	192.168.1.1		Virtual Host	
HOST2		4/1/0	Static	100.1.1.3/24	extGW	192.168.1.1		Virtual Host	
Subnet_100users		4/1/1	Static	192.168.1.0/24	HOST1	100.1.1.2/24		Virtual Subnet H...	
extGW			Static	192.168.1.1				External Host	

Figure 13: GUI example of host configuration

## Playback application configuration

17. Left mouse click the "Applications" tab, with a left mouse click select the "Add New Applications" icon, from the displayed list mouse over the menu item "Raw Port Playback". Left mouse click the "Raw Port Playback Application" menu item.
18. Complete the playback application configuration by filling in the parameters as follows:
  - a. Name: Assign a name to the replay function and description (optional).
  - b. Physical Interface: Use the button to the right to select the test interface in which the packet capture is associated with, this should be the interface on which the clients are on e.g. (Demonstration Scenario: "Subnet\_100users" host is on 4/1/1)
  - c. Select the resource or the packet capture.
  - d. Set a delay between repeated replays of the packet capture, default is zero meaning no delay between repeated replays.
19. With the application parameters configured, press play in the main menu icon bar to start the test run.

**Add New Raw Port Playback Application**

**1. Application Details**  
2. Additional Configuration

**Application Details**

Name: IPreplay\_Skype\_Web

Description:

Physical Interface: 4/1/1

Playback Resource List: PCAP

Delay between Resources: 0 ms

REALITY CHECKED

< Prev   Next >   Finish   Cancel

Figure 14: IP replay uses the Rawport playback application

*Using the PDU capture tool as per section 2.1, run a packet capture at the interface level, to verify that there is amplification with 100 unique IP addresses using the same layer 4-7 encapsulated payloads.*

## Using substitution to replace content in the IoT TCP replay files

Through the web management interface it's possible to assign substitution to a number of places or offsets in the packet capture. For each replay of the packet the substitution will be made. Users can substitute in a fixed value or dynamic value using a randomization parameter e.g. {NUM2} will input a random 3 digit number.

Point a browser at the web management interface on the TeraVM controller e.g. [http://TeraVM\\_Controller\\_IPAddress/admin/global/](http://TeraVM_Controller_IPAddress/admin/global/)

From the categories section select the "TCP Replay Client Settings", alternatively a user may select the server side responses "TCP Replay Server Settings" in which the substitution is placed.

*Wireshark is used to view and open the original packet capture, using Wireshark it's possible to determine the position of the content to be replaced and the offset required.*

The screenshot shows the TeraVM Global Settings web interface. The 'Categories' dropdown is set to 'TCP Replay Client Settings'. The 'Substitution Parameters' section is highlighted with a green box. It includes the following fields:

- Replay UDP instead of TCP: ☐
- Replay Rate Multiplier: 0.1 (e.g. 1.0 = normal, 0.5 = 2 X normal, 2.0 = half speed)
- Use TCP User Timeout Option to exchange stream IDs: ☐
- Number of Substitutions: 5
- Substitution Offset: 103 String: {NUM2}
- Substitution Offset: 120 String: u{NUM1}
- Substitution Offset: String:
- Substitution Offset: String:
- Substitution Offset: String:

Buttons: Save, Reset

Figure 15: Global settings on the TeraVM controller, selection is TCP Replay Client Settings



## Configuring a substitution

1. Define a value for the "Number of Substitutions" e.g. 5
2. Select Save, re-navigate back to the TCP Replay Client Settings menu (In the refreshed page note that there is now the ability to add up to 5 different substitutions)
3. Define the substitution:
  - a. Offset: Enter the number of bytes from the start of the packet in which the substitution is made.
  - b. String: Define new string or number that will be used in the replacement, a random number can be generated using {NUM}. For more details on substitution in TeraVM please visit the Help menu.

Global settings can be applied on a per TeraVM module basis. With two TeraVM modules a user can faithfully playback the original file with no substitution and use a second module with Global settings applied to playback the same file with substituted content.

## TeraVM performance measurement for IoT replay applications

### Examining the performance of IoT test runs

TeraVM enables per flow performance analysis on each and every one of the emulated IoT flows. While a test is running a user may view performance with per second granularity. Users can use the GUI for live performance views or alternatively users can use the command line to poll the value of a unique metric.

A significant benefit to TeraVM's per flow analysis is the ability to assess performance in terms of "Goodput" versus "Throughput". TeraVM is used to determine performance at a:

- Application level
- Host level
- Test interface level

TeraVM enables users view results live in both a graphical and tabular format.

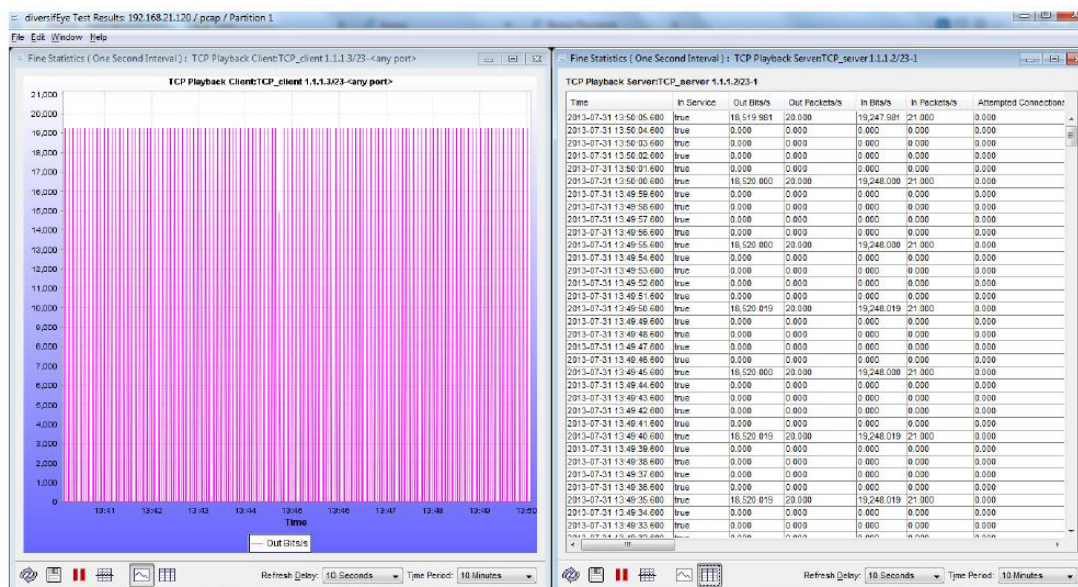


Figure 16: Graphical and tabular view of performance



## Enable per second granularity performance views

To view the fine statistics or per second performance granularity on any row in the test run;

1. Left mouse click on the application or host row in the GUI to highlight, right mouse click to display a menu window.
2. Mouse over "Statistics" in the window displayed, left mouse click on "Enable Fine Statistics" from the submenu which has been displayed.
3. Repeat the above two steps, however this time mouse over the "View Fine Statistics" from the newly appeared choose whether to view the statistics in relation to the source or destination. On successful selection of view a window similar to Figure 16 is shown.
4. In the newly displayed graphical view select the drop down menu in the bottom right hand corner labeled "Refresh Delay". Select the view 1 second.

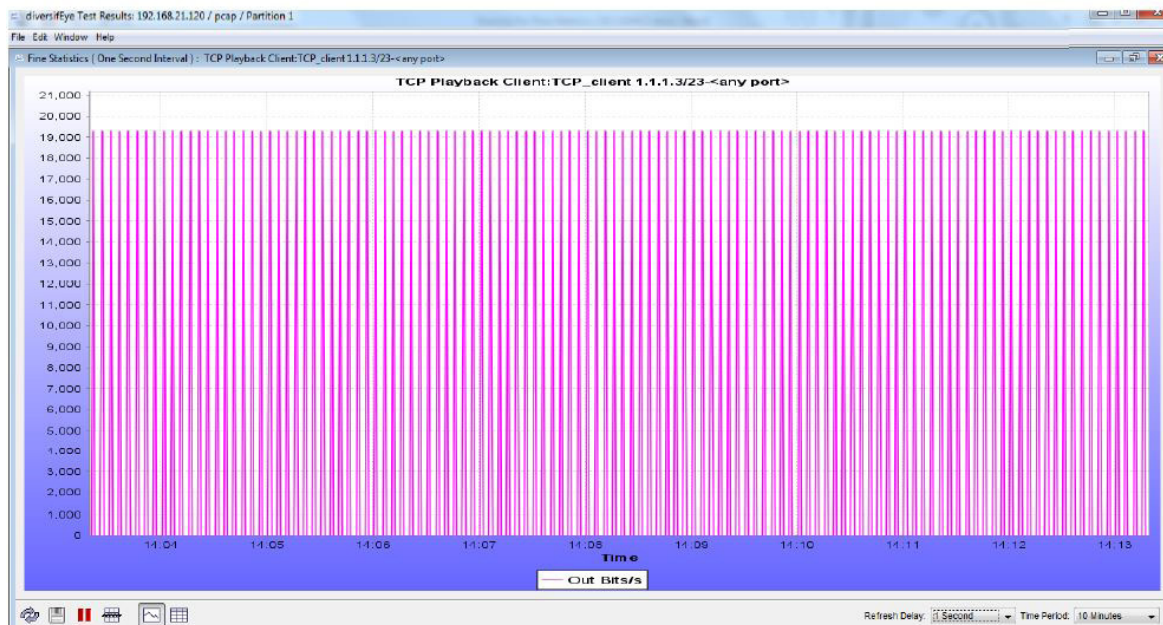


Figure 17: A view with per second granularity enabled

## Available Performance Metrics for IoT

### Raw port stateless playback

Raw Port Playback Server Application Description	Description
In service	Server active in test.
Server active in test.	The number of bits/second sent out by the Server.
Server Out Bits/s	The number of packets/second sent out by the Server.
The number of bits/second sent out by the Server.	The number of bits/second received in by the server.
Server Out Packets/s	The number of packets/second received in by the server.

Raw Port Playback Client Application	Description
In service	Client active in test.
Client Out Bits/s	The number of bits/second sent out by the client.
Client Out Packets/s	The number of packets/second sent out by the client.
Client In Bits/s	The number of bits/second received in by the client.
Client In Packets/s	The number of packets/second received in by the client.

### TCP IoT playback

TCP Playback Server Application	Description
In service	Active as part of test
Server In Bits/s	The number of bits/second received in by this Server.
Server Out Bits/s	The number of bits/second sent out by this Server.
Server In Packets/s	The number of packets/second received in by this Server.
Server Out Packets/s	The number of packets/second sent out by this Server.
Server Retransmitted Packets Client	The number of Retransmitted packets received in by this Server.
Server Out of Sequence In Packets	The number of Out of Sequence packets received in by this Server.
Server Attempted Connections/s	The number of connections/second attempted by this server.
Server Established Connections/s	The number of connections/second established by this server.
Server Failed Connections/s	The number of connections/second that were not established by this server.

## TCP IoT playback continued

TCP Playback Client Application	Description
In service	Client active as part of test
Client Out Bits/s	The number of bits/second sent out by this Client
Client In Bits/s	The number of bits/second received in by this Client.
Client Out Packets/s	The number of packets/second sent out by this Client.
Client In Packets/s	The number of packets/second received in by this Client.
Client Attempted Connections/s	The number of connections/second attempted by this Client.
Client Established Connections/s	The number of connections/second established by this Client.
Client Failed Connections/s	The number of connections/second that were not established by this Client.
Server Established Connections/s	The number of connections/second established by this server.
Server Failed Connections/s	The number of connections/second that were not established by this server.
Client Retransmitted Packets Client	The number of Retransmitted packets received in by this Client.
Client Out of Sequence In Packets Client	The number of Out of Sequence packets received in by this Client.

TCP Playback Client - TCP Connection	Description
SYN/SYNACK Count	Number of SYNACK to ACK of SYNACK.
SYN/SYNACK Mean ms	Mean number of SYNACK to ACK of SYNACK. (ms)
SYN/SYNACK Min ms	Minimum number of SYNACK to ACK of SYNACK. (ms)
SYN/SYNACK Max ms	Maximum number of SYNACK to ACK of SYNACK. (ms)
SYN/Data Count	The number of SYNACK to first byte of data from Client.
SYN/Data Mean ms	The mean number of SYNACK to first byte of data from Client.
SYN/Data Min ms	The minimum number of SYNACK to first byte of data from Client.
SYN/Data Max ms	The maximum number of SYNACK to first byte of data from Client.
FIN/FINACK Count	The number of FIN to FINACK or FINACK to ACK of FIN depending on which side initiates the connection close.
FIN/FINACK Mean ms	The mean number of FIN to FINACK or FINACK to ACK of FIN depending on which side initiates the connection close.
FIN/FINACK Min ms	The minimum number of FIN to FINACK or FINACK to ACK of FIN depending on which side initiates the connection close.
FIN/FINACK Max ms	The maximum number of FIN to FINACK or FINACK to ACK of FIN depending on which side initiates the connection close.

## UDP IoT Playback

UDP Playback Sink	Description
In Bits/s	The number of bits/second received in by this application
In Packets/s	The number of packets/second received in by this application
Time	The timestamp of the packet
In Service	The Sink is active as part of the test

UDP Playback Sink	Description
UDP Playback Source	The number of bits/second sent out by this application
Out Bits/s	The number of packets/second sent out by this application
Out Packets/s	The number of bits/second received in by this application
In Bits/s	The number of packets/second received in by this application
In Packets/s	The timestamp of the packet
Time	The Source is active in the test
In Service	