XENA™
Test. Improve. Repeat.

APPLICATION NOTE

PCAP Replay

Reproduce your own reality with Vulcan PCAP Replay

How to capture traffic into PCAP files and replay on Xena's Vulcan traffic generation & analysis platform to reproduce your own reality for stateful performance verification.

Contents

APPLICATION NOTE

Stateful PCAP replay is an effective way to reproduce reality to your system under test and test the behaviors of your devices that are not visible with modeled traffic. Vulcan's advanced Layer 4 replay provides a platform to replay your own PCAP with flexibility and scalability. In case of packet loss by the network, which is a normal behavior of any IP networks, Vulcan's stateful TCP stack makes sure that the information delivery is reliable by means of TCP retransmission. Adaptive congestion control can be enabled with the measurement of round-trip latency between the client and the server.

This application note describes how to make your or PCAP file that conform to Vulcan's replay engine, and how to use Vulcan's replay scenario to scale up the traffic for high-performance testing.

CAPTURE REAL-WORLD TRAFFIC INTO PCAP

The simplest way to quickly generate a PCAP file is to use a network traffic analysis software, e.g. Wireshark, or other similar tools. We will use Wireshark in this section to demonstrate how to capture the traffic we want to replay.

This section will describe how to capture traffic into a PCAP file using Wireshark. In-depth use of Wireshark is out of the scope of this section. For more on how to use Wireshark, please refer to https://www.wireshark.org

LAUNCH WIRESHARK

Launch Wireshark and you should see the window as shown Figure 1. On this window, you are presented with options to select from which network interface you would like to capture traffic. Figure 1 shows that there are two network interfaces on the demo PC, Ethernet and Wi-Fi. The activity indicators show whether there is any traffic on that interface. You can see that the Wi-Fi interface is active while the Ethernet interface shows no traffic. Thus, we will use the Wi-Fi interface to capture traffic.

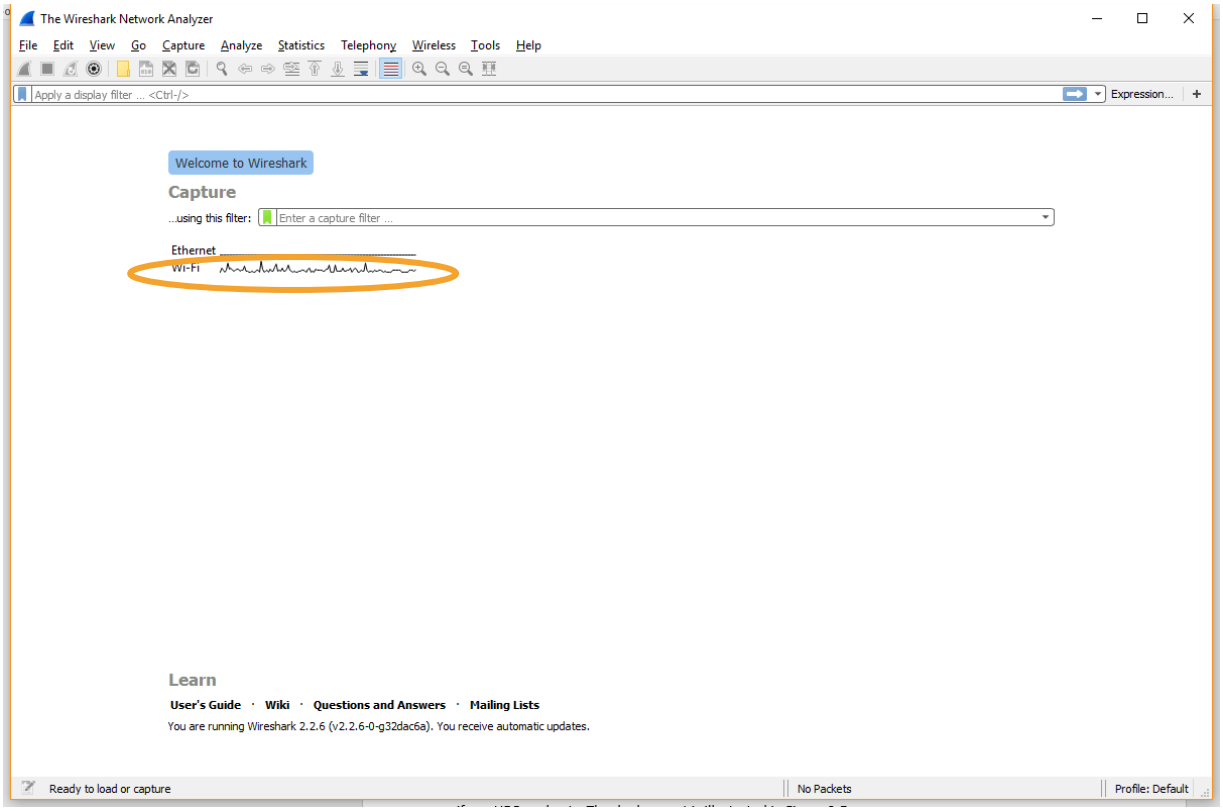

Figure 1. Launch Wireshark

Get Ready With the Application

Before capturing traffic, you should have an idea what to capture. If you want to capture traffic from YouTube, you should launch your web browser and prepare to enter the URL. If you want to capture traffic from Netflix, you should have the program ready.

Preparing the application, you want to capture traffic from, before starting Wireshark is a good practice because once you start capturing, packets will pour into the buffer and it might affect the performance of your PC. Thus, get things ready in advance will save you some effort from struggling with a slow computer.

Select Interface and Capture

Once you think the application you want to capture traffic from is ready, you can begin to initiate the capture. As shown in Figure 2, select the interface and then click the “Start capturing packets” button.

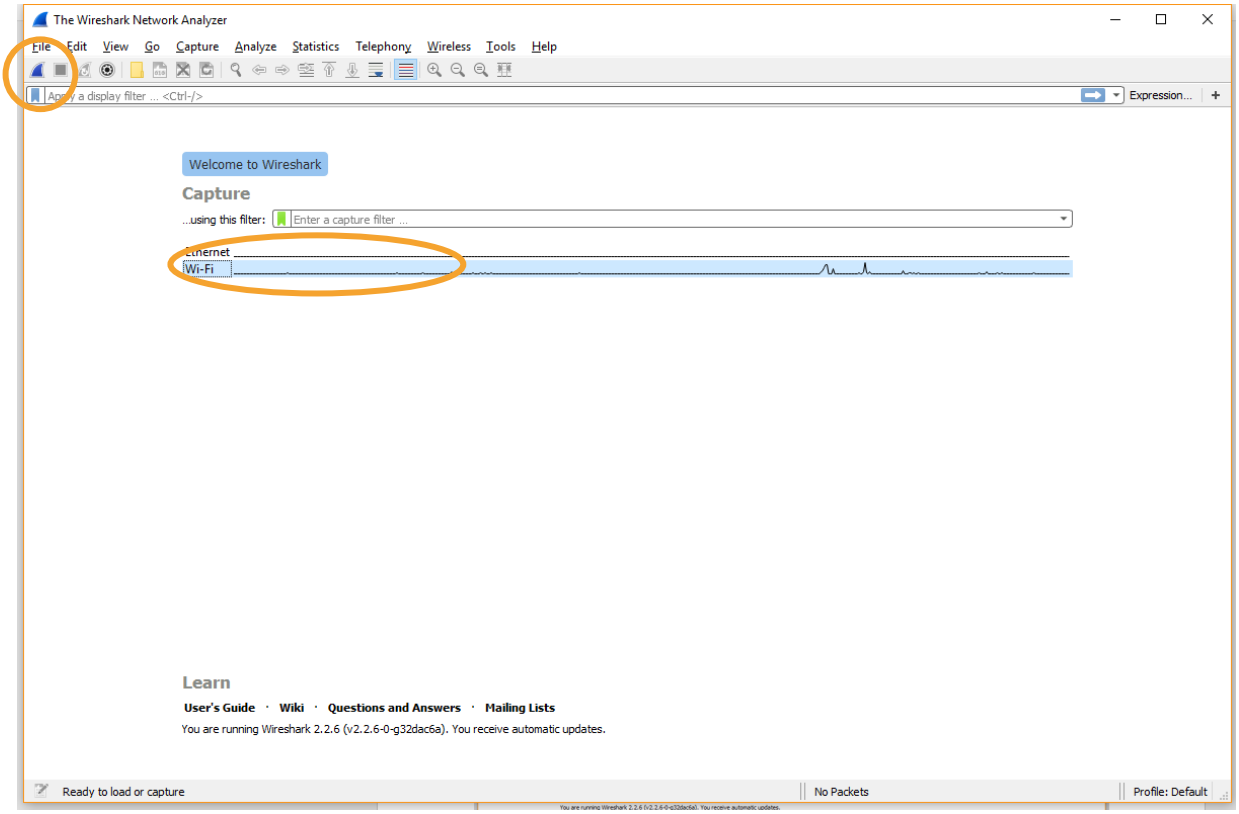

Figure 2. Select the interface and start capturing packets

As soon as you start the capture, you will see packets being shown in the program window. At this time, you can start your application and all the traffic between your PC and the server will be recorded, as shown in Figure 3.

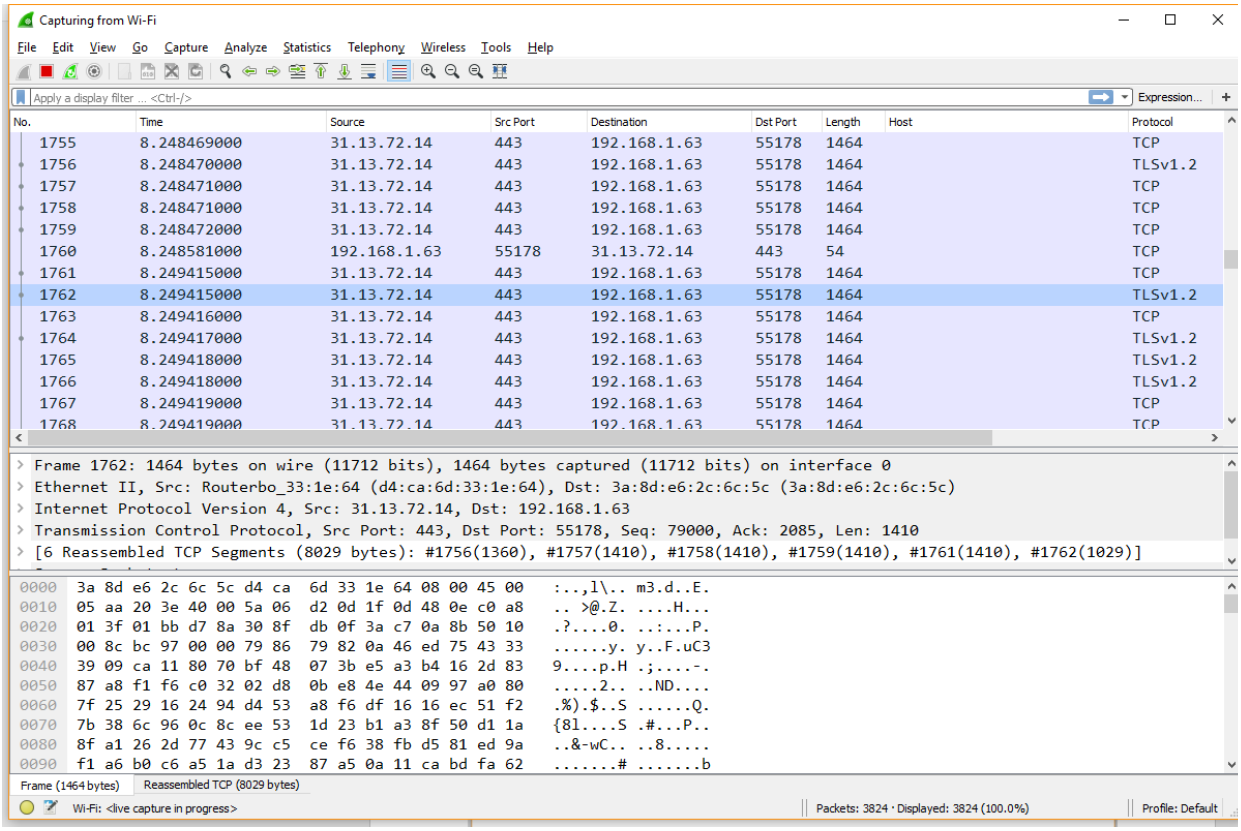

Figure 3. Capturing packets

SELECT THE TRAFFIC YOU WANT TO REPLAY

When you have captured the traffic you want, you can stop capturing by clicking the red “stop” button.

There will be many packets from different applications in Wireshark. This is simply because your PC runs not only the application you want, but also many other applications (visible or hidden) that you may not notice. If your Wireshark is in promiscuous mode, it may also capture broadcast packet such as ARP.

You need to filter out the traffic/sessions you want to replay from the mess. Click Statistics tab and go to Conversation, as shown in Figure 4.

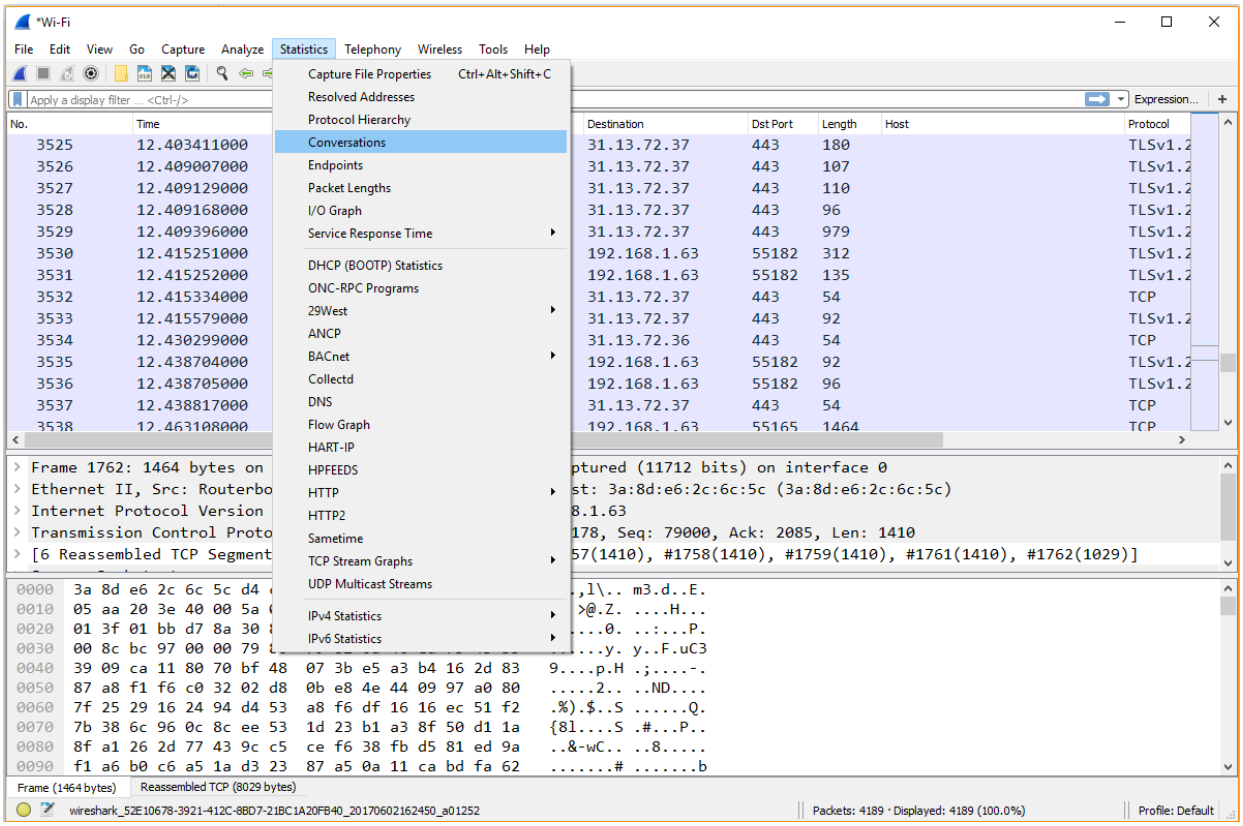

Figure 4. Use Statistics->Conversation to select the traffic you want

After click the Conversation, Wireshark will analyze the captured traffic and present conversations (sessions) for you, as shown in Figure 5. In this window, you will see the conversation on different network layers, Ethernet, IPv4, IPv6, TCP and UDP. The number beside each tab shows how many conversation there are, seen from this layer.

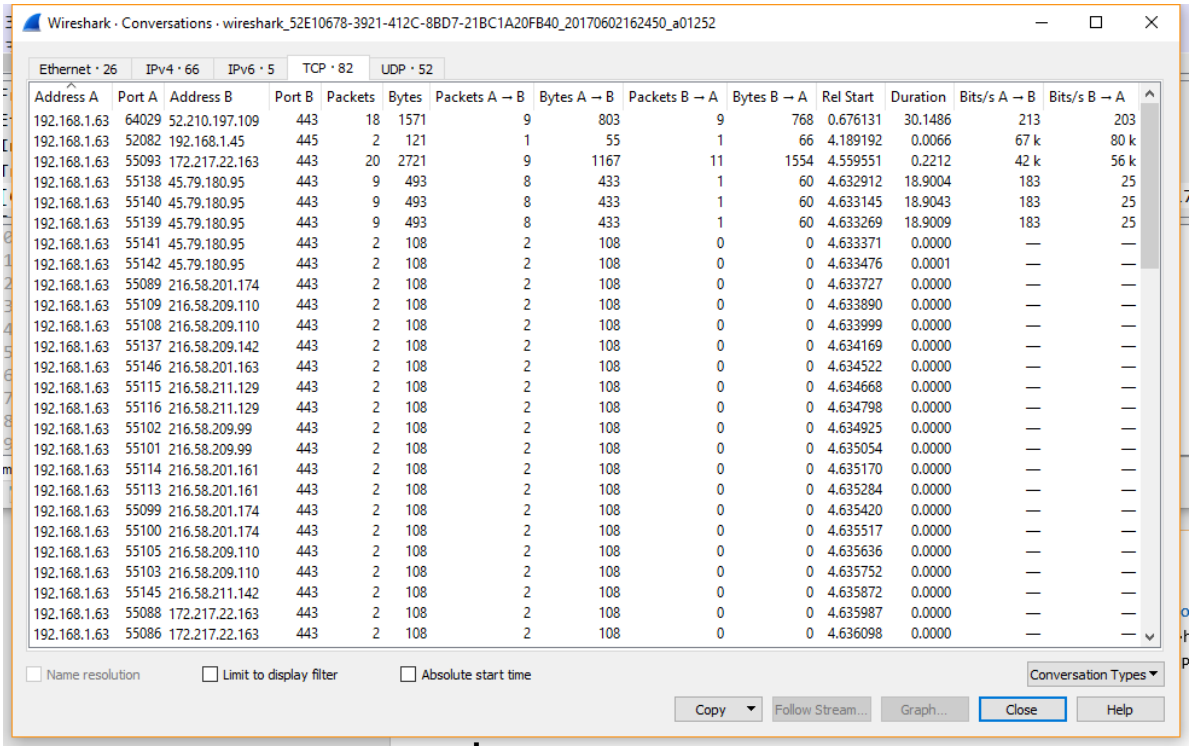

Figure 5. Conversation/session analysis

Look through the list of conversations and find the correct one(s) you want to save into a PCAP file. You can right-click on the conversation as shown in Figure 6 and select Apply as Filter -> Selected. Wireshark will automatically create a display filter for you and show you only the traffic you are interested in, as shown in Figure 7.

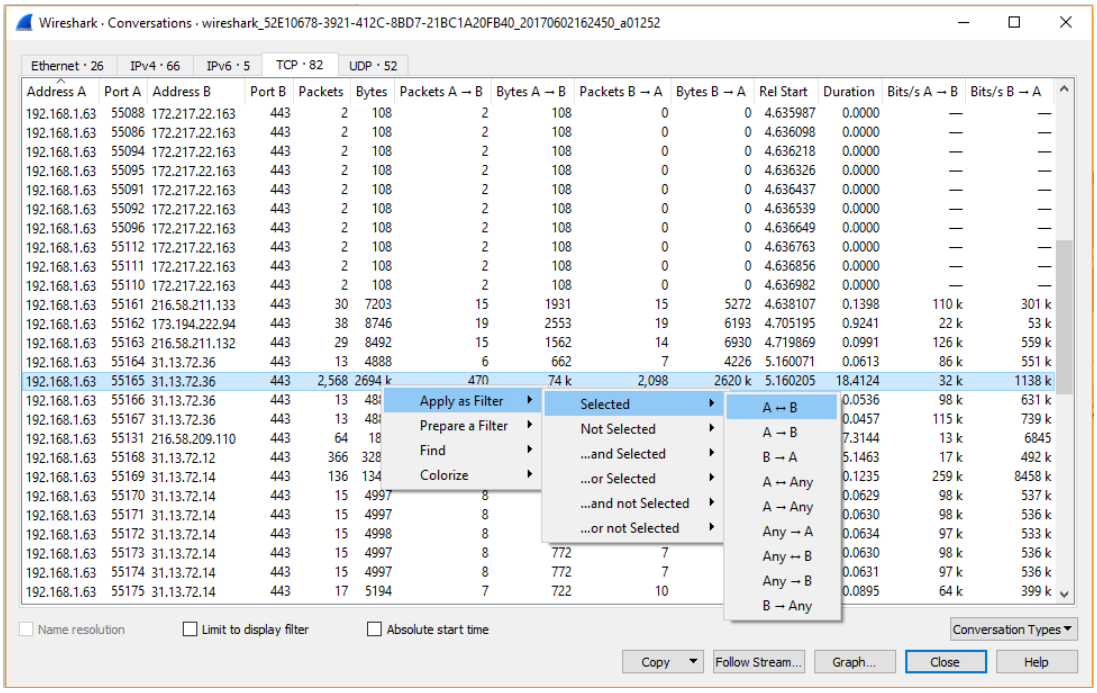

Figure 6. Select the conversation and apply as filter.

After filtering out the traffic you want to save, click File -> Export Specified Packets, and save the displayed packets into a PCAP file.

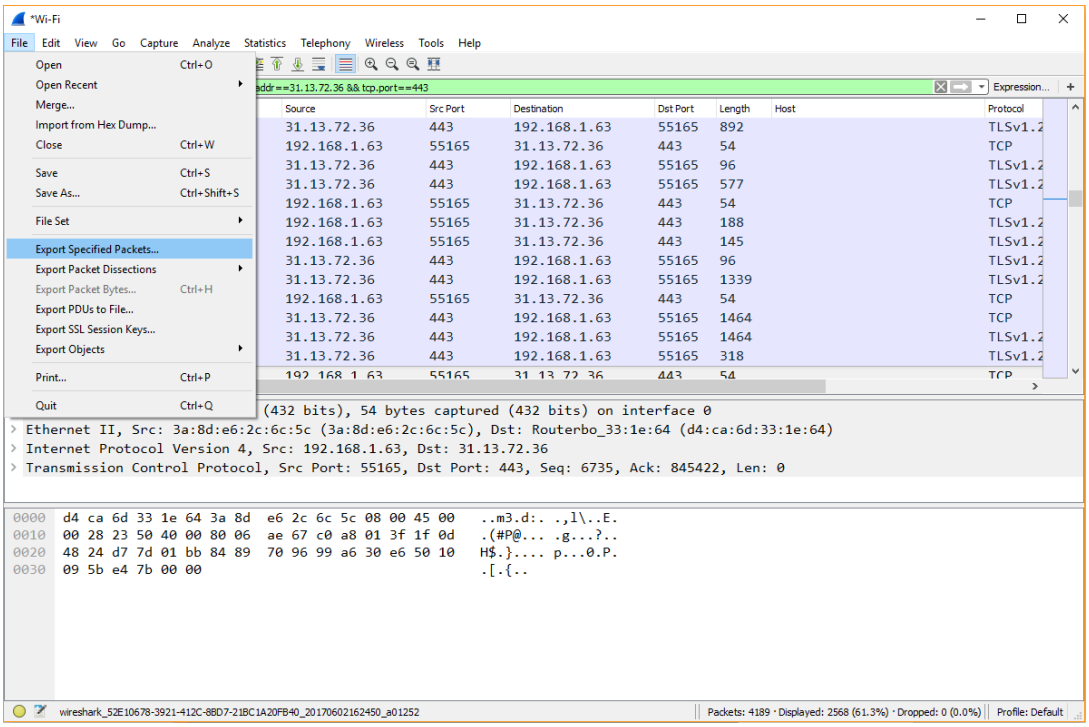

Figure 7. Save the displayed packets into a PCAP file

MAKE PCAP COMFORMING TO XENA REPLAY RULES

There are some rules for the PCAP file to be properly parsed and replay. Make sure your PCAP conforms to the following rules:

1. Max number of segments per PCAP:
   - 1 million segments for VulcanCompact,
   - 2 million segments for VulcanBay.
2. Max number of connections per PCAP:
   - 256 for VulcanCompact
   - 256 for VulcanBay
3. Max size per PCAP file
   The maximum size of the PCAP file depends on the average TCP/UDP segment size. PCAP files larger than 1GB are in generate supported, as long as the number of segments and connections are within the range defined by (1) and (2).
4. One source IP address (one-client-to-many-servers communication)
   You can either capture your traffic on a PC like Figure 8 (A), or capture traffic after a NAT router as in Figure 8 (B). Both cases will have one-to-many traffic.
5. No IP fragmentation
6. Recorded TCP maximum segment size/UDP packet size should below:
   - 1460 bytes (TCP+IPv4)
   - 1440 bytes (TCP+IPv6)
   - 1472 bytes (UDP+IPv4)
   - 1452 bytes (UDP+IPv6)
7. PCAP should contain either IPv4 or IPv6, but not both in one file.
8. Only TCP and UDP packets will be replayed.

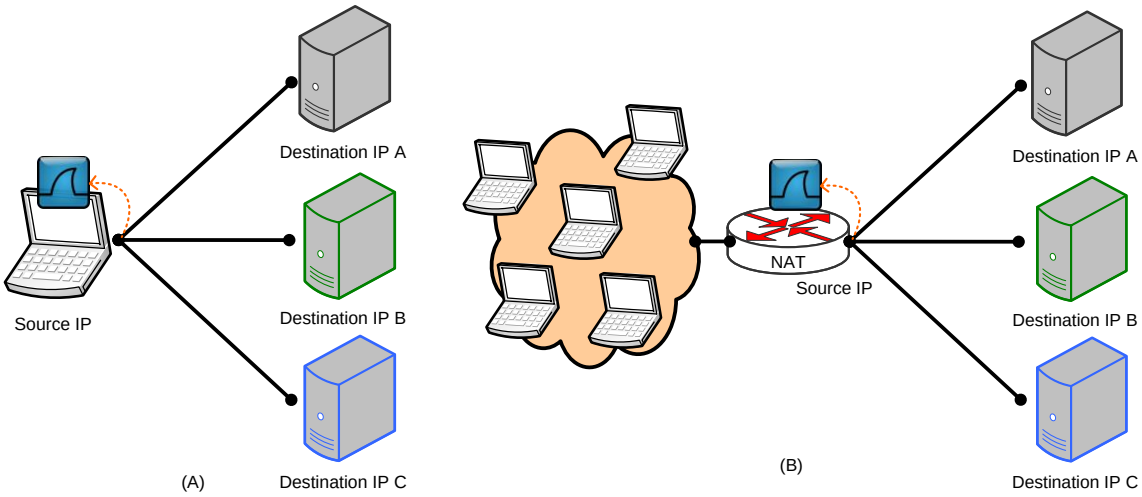

Figure 8. Traffic should be one-to-many

IF YOUR PCAP FILE VIOLATES ANY OF THE RULES ABOVE, THE PARSER WILL REPORT IT WHEN THE PCAP HAS BEEN UPLOADED TO THE CHASSIS.

USE PCAP FILE FOR REPLAY

This section describes how to import a PCAP file for Layer 4 PCAP relay using VulcanManager. More details about how to use VulcanManager can be found here:
https://xenanetworks.com/vulcanmanager-users-manual/

CREATE RELAY SCENARIO

Add a Replay scenario into a test case as shown in Figure 9. Notice that you need to select the IP version beforehand. After clicking OK, you can find your PCAP file in the dialog window.

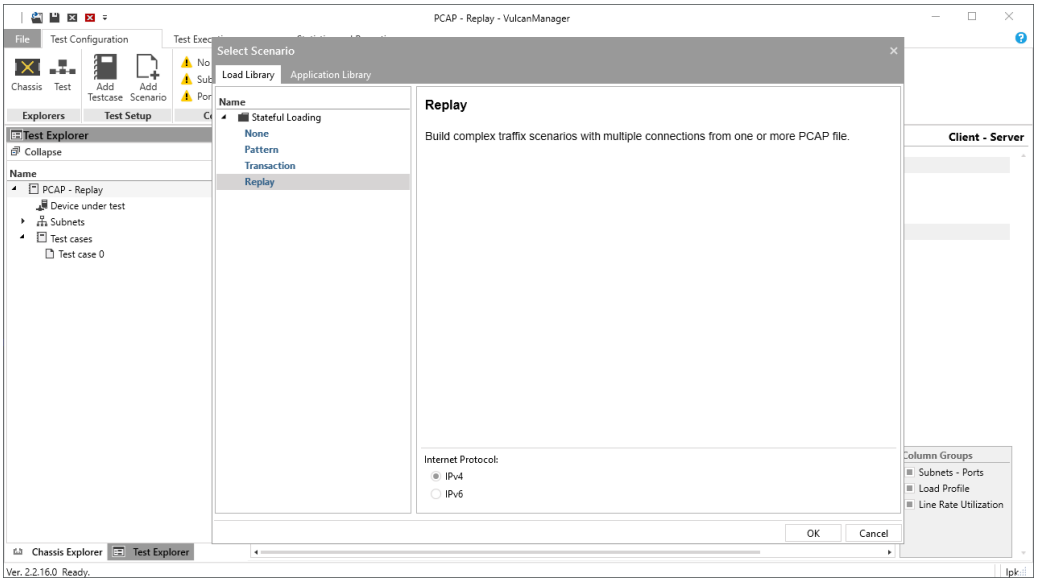

Figure 10. PCAP import dialog window

We will see the PCAP import dialog window as in Figure 10 showing the progress. The PCAP will first be uploaded to the chassis. Then the PCAP parser will parse and analyze the file. When the import is finished, you will be able to see the analysis result including number of connections, Layer 4 protocols, number of segments, and total payload size. Click OK to proceed.

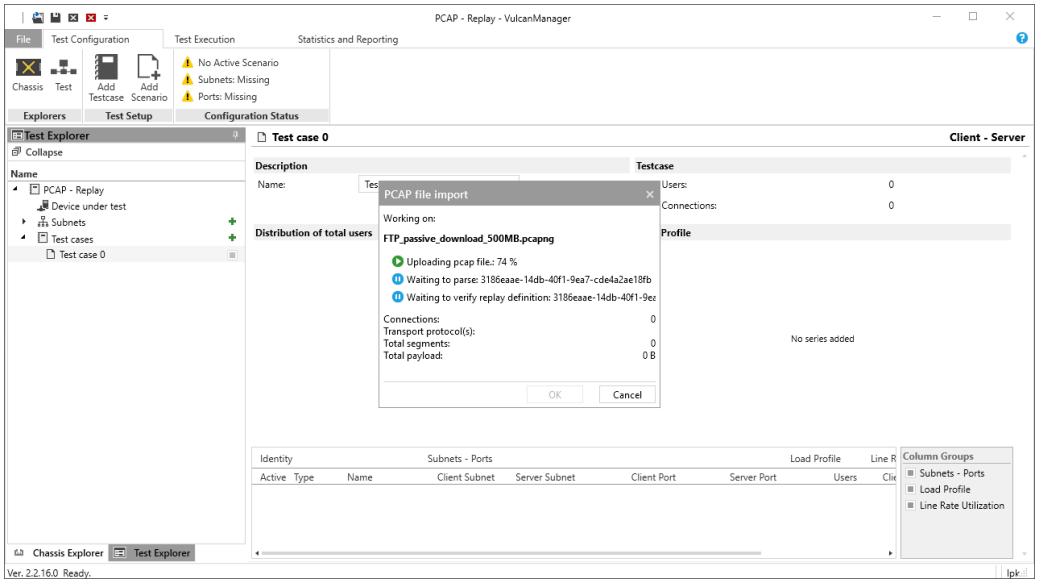

Figure 10. PCAP import dialog window

SCALE YOUR TRAFFIC

As shown in Figure 11, you have successfully created a replay scenario using the PCAP file you have made. By default, the number of users is set to 100,000, which means the tester will duplicate the PCAP traffic 100,000 times, each of which is assigned a new IP address. This is the reason for Rule 3 (one-to-many communication) because the replay engine can scale the traffic.

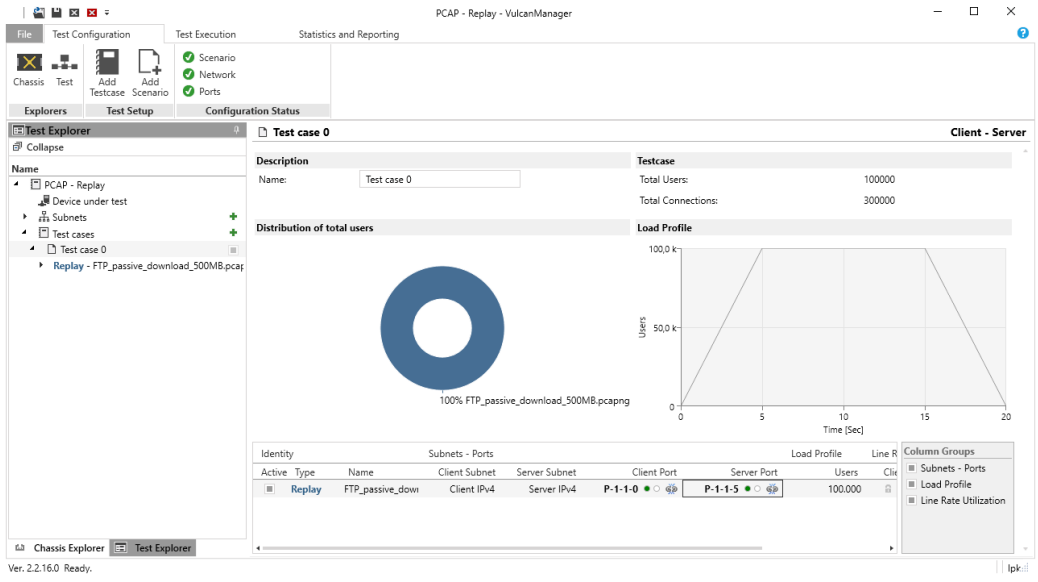

Figure 11. PCAP import dialog window

COMPOSE YOUR OWN PLAYLIST WITH MULTIPLE PCAP FILES

You can also build your own "playlist" by importing multiple PCAP files into one test case. Repeatedly creating Replay scenarios into one test case will allow you to simultaneously play or sequentially play PCAP files.

Figure 12 shows an example of two Replay scenarios in one test case. By configuring the load profile for each replay scenario, you can simultaneously or sequentially play your PCAP files. Make sure to assign different subnet ranges to the server side to avoid socket conflict.

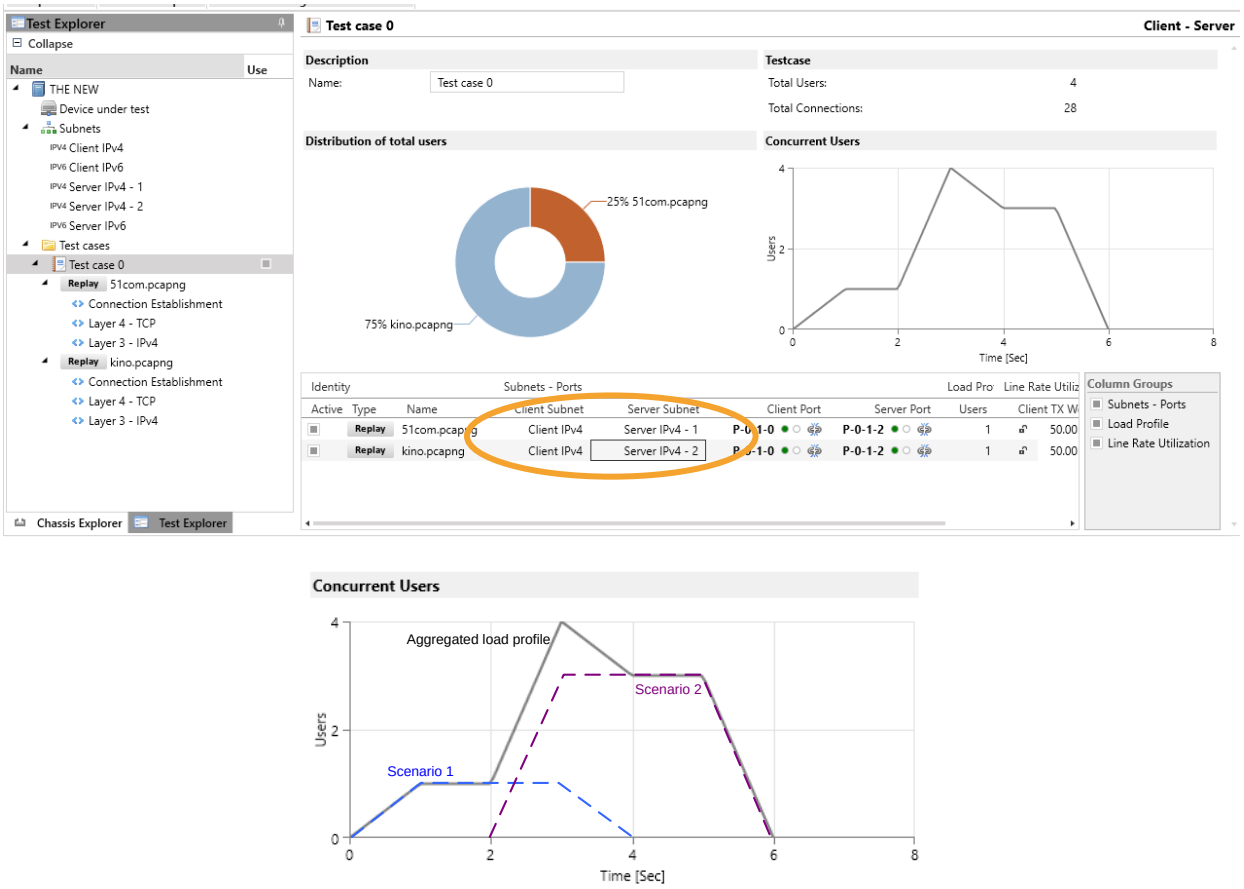

Figure 12. Make your own "playlist" by creating multiple replay scenarios in one test case

LOOP YOUR PCAP

You can loop the replay of a PCAP file with either the same source IP address or different source IP addresses by configuring “User Updates” in the “Connection Establishment” entry of the test scenario, as shown in Figure 13.

Click the “Connection Establishment” entry under the scenario and find “User Updates” section. Choose among “No rebirth”, “With same Src IP”, and “With new Src IP”, and input repetitions. If the repetition is set to 0 or left empty, the loop will continue till the end of the test.

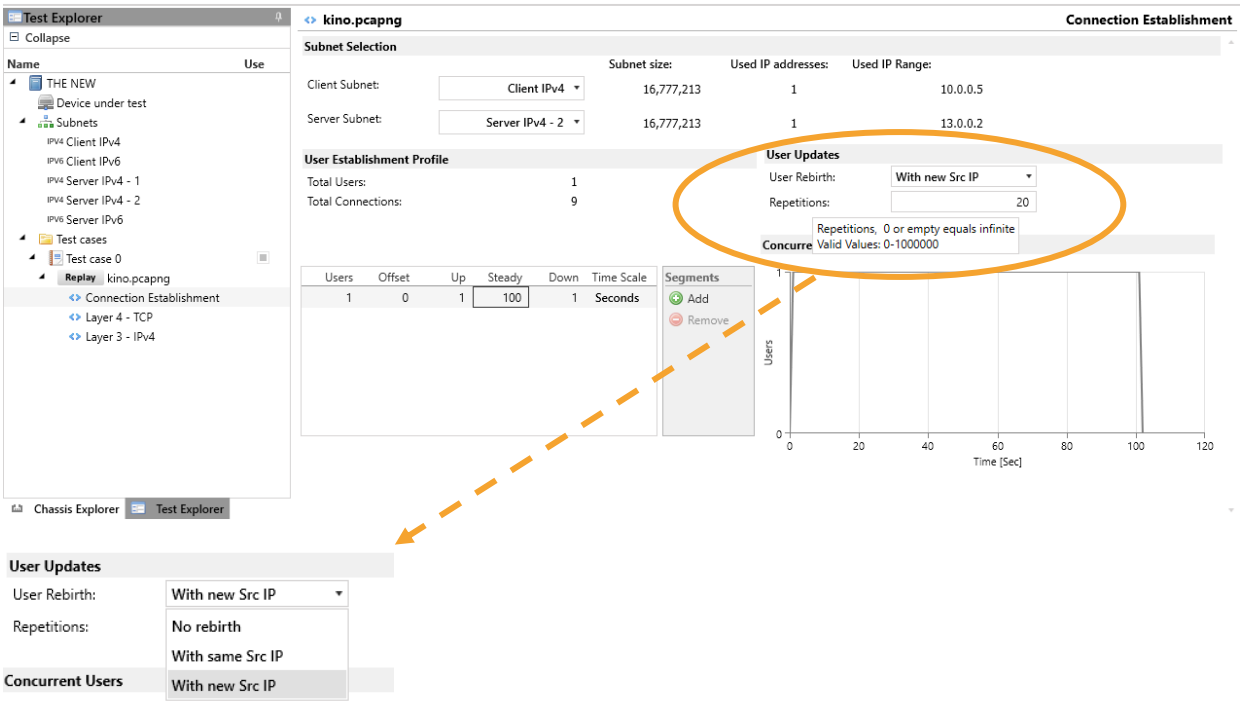

Figure 13. Loop your PCAP replay scenario

THINGS YOU SHOULD KNOW ABOUT XENA PCAP REPLAY

Xena PCAP replay is Layer-4 payload replay (more can be read on http://xenanetworks.com/advanced-stateful-layer-4-replay-white-paper/), thus it is different from stateless packet replay.

PAYLOAD REPLAY

Xena PCAP replay parser extracts the layer-4 payloads, and replay them with new headers. Thus, the replayed traffic may have different Ethernet headers, IP headers, and TPC/UDP headers, depending on how you configure the new MAC addresses and IP addresses. Destination ports are preserved, but source port numbers are replaced by ports in the ephemeral source port range suggested by the Internet Assigned Numbers Authority (IANA).

PRESERVED PAYLOAD

The payload is replayed as is. Users cannot modify the payload for replay.

NEW CONNECTION

TCP handshake (SYN, SYN-ACK, ACK) and teardown (FIN, ACK) will be added to the TCP session if no handshake/ teardown is present in the file.

RELIABLE DELIVERY

In case of packet loss, Xena TCP stack will retransmit.

CONGESTION CONTROL

TCP congestion control can be turned on or off according to users' need.

TCP AND UDP REPLAY

Only TCP and UDP packets are replayed. If there are packets such as ARP in the PCAP, they will not be replayed.

REPLAY WITH SPEED-UP OR SLOW-DOWN

Usually the PCAP file is recorded with a certain bandwidth, e.g. capturing a streaming content at 1 Mbps rate (Layer 1 rate) for 600 seconds. When replaying this PCAP at a high bandwidth, e.g. 1Gbps, the duration of the replay will be shortened to 0.6 second (speed-up). If you want to maintain the same duration as it is in the PCAP file, you should remember to modify the rate to a lower value (slow-down). Read more on https://xenanetworks.com/vulcanmanager-users-manual/