



Troubleshooting

- General theory of operation: please read this first!
- What is the problem?
 - No connectivity
 - Bridge mode
 - Bridge Gateway Mode
 - Gateway mode
 - No or little benefit

General Theory of Operation

*Warp*TCP can improve the TCP throughput in networks where the throughput is limited by TCP and not by any physical or quality of service BW constraint.

- *Warp*TCP Proxies are configured between two physical or logical interfaces as pairs
- TCP sessions are terminated in the proxy unless bypassed by bypass rules
 - The downstream TCP connection utilizes Badu Networks' *Warp*TCP congestion control which handles congested networks much better than standard TCP.
- All other traffic passing through the proxy is bypassed and not terminated
 - Multicast is not bypassed in Gateway mode
- VLANs are supported with a logical proxy pair per VLAN
 - Traffic does not mix between VLAN interfaces


Some example network conditions that lead to significant TCP throughput improvements are:

- TCP traffic traveling through VPN tunnels
- Congested Wi-Fi networks
- Long distance connections



Connectivity Issues

First debugging steps

- Verify that all VLANs have a logical pair configured
- Complete all required (and optional) fields in the configuration
- Select “Verify configuration” for each logical pair
 - View results of the verify configuration by selecting 
 - Verify that there are no errors, and check all unverified items “?”
 - See connectivity verification list

Connectivity Verification

Item	Action
Gateway IP addresses on the upstream port of the Warp Engine	There must be a gateway defined in the different modes of operation
The Bridge IP address must not be a network IP address or a broadcast address	The combination of the IP address and the subnet mask determine the network ID and broadcast IP address. The Network Id is the lowest address in the subnet, and the broadcast is the highest. The Proxy IP address must not be on either the Network or Broadcast address.
WarpEngine must be physically connected on both ports	Check to see if the cables are disconnected and if there is link light on the interface
If DHCP is enabled there must be only one DHCP server on each side.	This issue arises if there are two different responses to the DHCP request
If DHCP is enabled It must be in the same VLAN and subnet as the relevant proxy interface	If the DHCP server is not in the same subnet, then the DHCP request from the proxy would not reach it, and the proxy would not receive a valid IP address.
If there is a Firewall, it should allow the TCP traffic to flow through WarpEngine	This can be verified by doing a TCP connection through the proxy to a known server. This known server could be an internet web site. If this is the target, make sure that the browser is not loading cached content which might hide a lack of connectivity.
The VLAN and subnet on each side of WarpEngine must be the same.	The WarpTCP proxy does not route traffic between VLANs, as a result this would result in a loss of connectivity.
The network must not use “split Horizon” routing. For each TCP flow the ACK and Data packets must go through the proxy.	To verify if this is happening take a capture on the diagnostics tab when the client is attempting to do a TCP connection to a known good server. Then view the packets in the capture that the packets coming from the client and going to the server are present in the captures on both sides of the proxy, (Eth2, Eth3) for example.
The network must be routable prior to installing WarpEngine	Prior to installing the proxy, ensure that TCP is routable to a known server. For this test, the traffic should route through all of the gateways that will be used in the deployment. The test can be carried out with a browser, or SSH connection. Make sure that the browser has not cached the content, which might hide connectivity issues.
The IP addresses used by the proxy must not be duplicated in the same network.	In order to verify if this is an issue, you remove the proxy and see if you can ping the same IP address.

Connectivity Verification

Item	Action
Bridge Mode: All downstream devices must be in the same subnet as the bridge IP	The included IP calculator can help identify the IP address range of the subnet
WarpEngine must be able to reach (ARP) default gateways	In order for the WarpEngine to route traffic correctly it needs to be able to get an ARP response from the default gateways. This can be tested by using the ARPprobe function in the Network diagnostics tab.
DHCP must provide a valid IP address	For each interface using DHCP, the DHCP server needs to respond with a Valid IP address. In the event that the DHCP server does not supply an address, the GUI will show a 169.254.254.X address.
The network must successfully route traffic through the proxy	To verify that traffic is being routed to the proxy, take a capture of the proxied interface using the networks diagnostics tab while known traffic is being routed to the box. You can use wireshark to filter the capture results to the specific source and destination IP addresses to ensure that the the desired traffic is reaching the proxy, and that it is being sent out the other port. If you use TCP as the test protocol, then you should be able to see the TCP three way handshake on each side of the proxy.
MTU mismatch or just too small	If there is a mismatch between the MTU on the proxy, and that in the network, it could cause packets to be dropped.
Missing or incorrect VLAN configuration	If a VLAN has not been configured on the proxy, then it will not have connectivity across the proxy. In order to check if this is happening, take a capture on the network diagnostics tab. When the capture is complete you can run the analysis, and it will display a list of all of the VLANs seen in the capture.
Half open TCP sessions	Some applications use a portion of the TCP handshake in order to implement a keep alive monitoring method. When the keep alive monitoring fails, it can break connectivity in the network. To see if this is occurring, a capture can be taken and reviewed. To fix the issue, the TCP sessions with the appropriate destination IP address can be bypassed in the configuration for the logical pair.
Routing failure after hardware bypass	In the event that the proxy is located in a network that has a failover mode, the ARP caches of the gateways may become out of date after a handover occurs. In order to help with this situation, the MAC address on each side of the proxy can be configured to match the gateway on the opposite side of the proxy. As a result, if the proxy NIC goes into hardware bypass, the MAC address does not appear to change. Thus the ARP Caches on the gateways are always correct. In the case of Gateway mode, there need to be routes in each of the gateways on each side of the proxy that will successfully maintain the routing when the proxy has effectively become a wire.

Debugging Benefit Issues

Item	Action
Is the measurement being made correctly?	<p>To make a comparison between proxied and bypassed traffic you need to ensure the following:</p> <ul style="list-style-type: none"> • The comparison between proxied and bypassed traffic needs to be made by alternating bypassed and proxied. • The traffic must pass over the same network including clients and servers for both proxied and bypassed measurements. • Sufficient quantity of measurements must be taken in order to verify that the result is statistically significant
Is the network bandwidth saturated?	<p>If the network is completely saturated, then there is little that can be done from a TCP optimization perspective. To test to see if this is the case you can use a network management tool such as Netflow. If this is not available Iperf can be used to test what the maximum UDP bandwidth available is between the server and the client. If this UDP throughput is similar to the TCP throughput that is being achieved, then there is not much room for improvement.</p>
Packet Fragmentation	<p>When traffic is passed through a VPN, the packet size on the VPN may require that the TCP payload is reduced in order to prevent packet fragmentation. This can be addressed by modifying the MSS on the logical interface of the proxy. In order to determine if this is happening, a capture can be taken on the proxy. If the packets getting to the proxy are not consistently the maximum size after coming through the VPN, then this could be the issue.</p>
Starved proxy	<p>If the connection between the server and the proxy has a lower bandwidth than the connection with the client, the proxy will be starved for data. As a result it will not be able to send data faster because it hasn't received it.</p>
Small TCP flows	<p>For TCP flows that are less than 15KB, TCP does not use congestion control. These packets are sent at line rate. As a result they are already being sent as fast as the network can accept them. As a result unless one of these packets are dropped in the network, the WarpTCP proxy will not add any benefit.</p>
Is the application using TCP ?	<p>Some applications do not use TCP, and as a result will not show any benefit. Some examples of these may include Youtube streaming via QUIC</p>
Web page load times and caching	<p>Web pages typically contain a large number of elements which need to be loaded in order for the web page to complete. There are a number of effects that will make accurate measurements difficult.</p> <ul style="list-style-type: none"> • Small elements (< 15KB) • Content is cached instead of downloaded causing inconsistent results • Long RTT for a large number of elements. • Advertising or other elements that may purposefully delay <p>In order to analyze these issues, a capture needs to be taken during the web page load with and without optimization. Then the individual elements that the page loaded can be checked to see if they are the same, and what the cause of the delay was. In general this is a difficult way to try to evaluate the benefit as a result of these complications.</p>

Debugging Benefit Issues

Item	Action
FTP passive mode	Some hardware in the network may take a long time or not support FTP on the standard port 21. This can be caused by firewalls that do stateful packet filtering and deep packet inspection on FTP to ensure that it is a valid connection. As a result care should be taken to use other ports, for example 31 and 32, when testing with FTP in passive mode.
Significant number of out of order packets	A significant number of out of order packets can degrade the performance of the proxy. As a rough estimate this fraction should be less than 5% of the packets. This normally would only happen in a test network using a WAN emulator that does not maintain packet order. Real networks typically do not generate this amount of out of order packets.
QOS	In some systems, specific types of traffic or TCP flows when exceeding some threshold may have their throughput limited. This throughput limit tends to limit the WarpTCP benefit. Note that some of these methods may be dynamic and kick in after a certain amount of traffic has been sent.