Troubleshooting Packet Loss Between Devices

Overview
Packet loss is when a piece of data sent from one networked device to another fails to arrive, and can occur for a variety of reasons. The first thing to do when troubleshooting it is to isolate where the loss is occurring.

Determining Packet Loss

On PC
To confirm if packet loss is occurring:

1. Open a command prompt on a client PC, via the Start Menu search for "cmd".
2. Use the ping command:
   
   ```
   ping -n 20 8.8.8.8
   ```

   *This will ping the address 8.8.8.8 20 times. Substitute 8.8.8.8 with whatever address must be tested to.*

3. Once the command has run, a summary will be presented indicating if loss occurred.

4. If no loss occurred, try increasing the "-n" value to something higher (such as 100) to test for a longer period of time.

   ![Ping statistics example]

   *Note: This only tests for packet loss impacting ICMP or all traffic. Protocol specific loss may not be reflected.*

Via Dashboard
Dashboard provides an effective tool to monitor connectivity to a specific IP address. Constant ICMP pings will be sourced from MX WAN to the respective IP.

This tool can be viewed under **Security & SD-WAN > Appliance Status > Uplink**
The packet loss section under Historical data will show us if there is loss in ICMP packets while MX trying to ping 8.8.8.8.

The destination IP address can be configured under Security & SD WAN > SD-WAN & traffic shaping > Uplink statistics

### Determining Where Packet Loss Is Occurring Over Routed Links

If packet loss is seen, the next step is to identify where the packet loss begins to occur. 'tracert' can be used to check each layer 3 device along the path to the destination:

1. Open a command prompt on a client PC, via the Start Menu search for "cmd"
2. use ping command

   tracert -d 8.8.8.8

   This will perform a trace route to 8.8.8.8 and present each hop as an IP address. Substitute 8.8.8.8 with whatever address must be tested to.

3. Wait for the trace to complete, or press CTRL/CMD+C if multiple lines ending with "Request timed out" are encountered.

A lack of response will be represented by an asterisk (*), potentially indicating packet loss, or that the device is configured to not respond. The test may need to be completed multiple times to identify where loss is occurring. If packet loss is frequently encountered after a particular hop, then the issue most likely is with that device or between it and the previous hop. This screenshot illustrates a tracert clear of packet loss. The only device to not respond (hop 11) is likely configured to do so, as there is no packet loss after it.
In this next screenshot, packet loss is regularly encountered beginning with hop 2. This indicates there may be an issue with the ISP gateway, or the link(s) between the Client gateway and ISP gateway. It is recommended to test from multiple clients at different locations in the network to help rule out specific client issues and develop commonality between clients experiencing the problem.

```
C:\Users\testUser>tracert -d 8.8.8.8
Tracing route to 8.8.8.8 over a maximum of 30 hops
1  30 ms  5 ms  12 ms 10.X.X.X  <- Client gateway
2  *       *       13 ms 184.X.X.X  <- ISP gateway
3  *       *       30 ms 208.X.X.X
4  17 ms  *       12 ms 208.X.X.X
5  16 ms  *       *       206.X.X.X
6  28 ms  23 ms  *       216.X.X.X
7  *       *       *       Request timed out.  <- No response received
8  *       75 ms  *       72.X.X.X
9  *       64 ms  41 ms 72.X.X.X
10  70 ms  *       *       216.X.X.X
11  *         *       *       Request timed out.  <- No response received
12  70 ms  62 ms  47 ms 8.8.8.8  <- Target address
```

As a more robust test, the tool MTR can be used to perform a continuous series of traces and present a % of loss at each hop in the path to more clearly identify where the loss is occurring. Output for the above scenario would appear similar to:

```
Hostname      Loss %       <-
10.X.X.X       0            Client gateway
184.X.X.X      75           ISP gateway
208.X.X.X      60
208.X.X.X      70
206.X.X.X      75
216.X.X.X      80
No response from host 100  <- No response received
72.X.X.X       65
72.X.X.X       75
216.X.X.X      70
No response from host 100  <- No response received
8.8.8.8        75            Target address
```

**Determining Packet Loss on WAN Uplink**

If packet loss is observed on the WAN uplink, the next step is to determine if the loss is on the MX or on the ISP side.

You can determine which interface is experiencing less by taking packet captures on the LAN and Internet interfaces of the MX security appliance.

1. Run constant pings from a PC to a public IP address
2. Take simultaneous packet captures on the LAN and WAN of the security appliance
3. Filter the traffic with source and destination IP address and ICMP
4. Check for the ICMP requests are appropriately forwarded from the LAN to the WAN of the MX

5. If traffic is forwarded appropriately from LAN to WAN – MX is likely not the cause of the issue, so you will need to troubleshoot the packet loss further on the ISP side

Determining Where Packet Loss Is Occurring in a Wireless/Switched Network

Tracert only provides information for layer 3 devices in the path, such as routers. However, in the case where packet loss is occurring at the first hop, and must pass through a wireless access point and switch to get there, additional testing is required to isolate the problem. In this case, testing will need to be done multiple times, while getting progressively closer to the layer 3 devices. The following steps are illustrated in the image below:

1. Ping the access point to test wireless quality. If using a Cisco Meraki AP, ping my.meraki.com. If loss begins occurring here, refer to the knowledge base article on troubleshooting wireless performance.

2. Ping a client connected to the same VLAN (if configured) on the switch that the wireless client is connected to. If multiple switches exist along the path, repeat this step as needed. If loss begins occurring here, the issue is most likely:
   - Duplex/speed settings mismatch on the link between the AP and the switch, or switch and wired client
   - Bad cable between the AP and switch, or switch and wired client

3. Connect a client directly to the router/firewall, on the same VLAN as the wireless client, and ping it from the wireless client. If loss begins occurring here, the issue is most likely:
   - Duplex/speed settings mismatch on the link between the switch and the router/firewall, or router/firewall and wired client
   - Bad cable between the AP and switch, or router/firewall and wired client

If testing with Cisco Meraki devices, it is also possible to ping the first MS switch or MX security appliance in the path. The IP address of the switch can be found by navigating to switch.meraki.com and the MX security appliance at wired.meraki.com.
Common Causes of Packet Loss

There are many potential causes of packet loss. This section will outline some of the more common reasons packet loss occurs and what can be done about them.

**Duplex Mismatch**

This occurs when two ends of a link are using different speed/duplex settings, such as 100Mbps/half-duplex and 1000Mbps/full-duplex. When this occurs, some or all traffic will be lost on the link.

To correct this, ensure both sides of the link have identical settings. Ideally, both ends of the connection should be set to "Auto" for both speed and duplex. If a speed or duplex setting must be manually set on one end, ensure that it has been set to the same values on the other end as well.

- Auto ↔ Auto   Good
- 100Mfdx ↔ 100Mfdx   Good
- Auto ↔ 100Mfdx   Bad
- 100Mfdx ↔ 100Mhdx   Bad

**Link Congestion (Too Much Traffic)**

This occurs when more traffic is attempting to go over a network link than it can support. Such as 60Mbps of traffic passing over the same 20Mbps link. This creates a bottleneck, resulting in some traffic being dropped.
There are multiple ways to solve this, including:

- Increase the capacity of the link being overwhelmed to allow for all traffic.
- Apply traffic shaping rules on MX security appliances or MR access points to limit the volume of traffic, particularly focusing on decreasing the volume of undesirable traffic.
- Apply traffic shaping rules on MX security appliances or MR access points to prioritize more important traffic.

**Firewall Blocking Certain Traffic**

Even if packet loss isn’t occurring for all types of traffic, an upstream firewall may be filtering certain types of traffic. This can result in some websites loading and others failing, or some services being accessible, while others are not.

If a firewall exists between two devices/locations experiencing these symptoms, ensure that the firewall is not blocking the traffic that is experiencing the problem.

**Bad Cable or Loose Connection**

A cable that has been poorly/incorrectly terminated or damaged can result in an incomplete or inaccurate electrical signal passing between devices.

Swapping a cable with a new one, or performing a cable test on the one in question, can help to eliminate this as a possibility. Similarly, a cable that has not been fully seated in the port, or has been seated in a port with dust or other non-conductive debris on the pins, can result in an incomplete electrical signal. Be sure to keep all ports free of dust or build-up and ensure cables are securely connected.