Progress®
Kemp® LoadMaster®

Feature Description Network Telemetry

Generated on: 16 September 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 4

Document Purpose 6

Intended Audience 6

Limitations 6

Chapter 2: Network Telemetry Information 8

Chapter 3: Download the Flowmon Collector 10

Chapter 4: Enable and Configure Network Telemetry. 11

Chapter 5: Enable and Configure Network Telemetry in a LoadMaster HA pair. 13

Chapter 6: Troubleshooting. 16

1

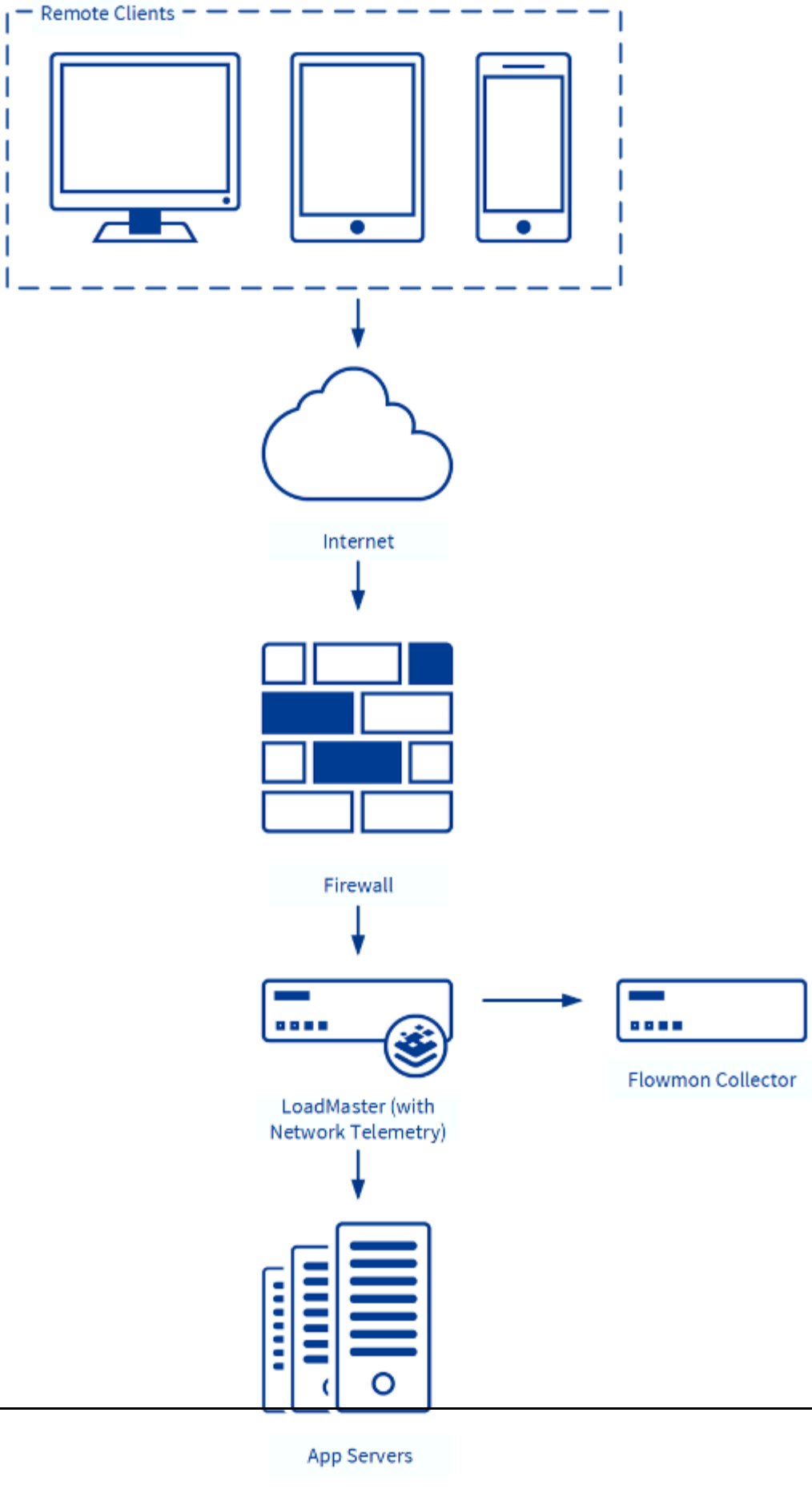
Introduction

Introduction

As of firmware version 7.2.53 (and Long Term Support (LTS) version 7.2.48.4), the LoadMaster can monitor the network traffic traversing its interfaces and generate rich network telemetry in IP Flow Information Export (IPFIX) format.

IPFIX is a flow export standard used to identify and collect application and transaction data in a network infrastructure. Flow data provides visibility into application traffic utilization and structure at any time, enabling you to report on key network performance metrics related to application workload. This is often leveraged as an alternative to full packet capture and analysis for ongoing monitoring of a network infrastructure. Various network devices including switches, firewalls, load balancers, and routers typically provide flow-based feeds to collectors which are then analyzed by a performance monitoring and analytics toolset.

Note: For further details on IPFIX, refer to the following Flowmon page: NetFlow/IPFIX Monitoring.


Remote Clients
Internet
Firewall
LoadMaster (with Network Telemetry)
Flowmon Collector
App Servers

The LoadMaster is able to participate in providing flow data visibility in conjunction with a compatible IPFIX data analysis system. We recommend using the Flowmon Collector for this data analysis.

The network telemetry feature is available on all LoadMaster products with any license or subscription type. The purpose of network telemetry is to understand traffic volume and structure at any time, report on key network performance metrics related to application workload and troubleshoot on operation and performance issues with the ability to drill down to individual session level.

Related Links

For details, see the following topics:

- Document Purpose
- Intended Audience
- Limitations

Document Purpose

Document Purpose

The purpose of this document is to describe how to enable this functionality on the LoadMaster and to gain access to the Flowmon Collector.

Intended Audience

Intended Audience

Anyone who would like to export application flow data from the LoadMaster.

Limitations

Limitations

LoadMaster's Network Telemetry IPFIX data export feature is a limited implementation of the Flowmon Probe on the LoadMaster. It provides visibility into the traffic flow of any LoadMaster and the Virtual Services running on it with limitations when compared against the full functionality provided by the Flowmon Probe appliance. Some limitations are listed below:

- Encrypted traffic (for example, HTTPS) is not decrypted for analysis by the probe on the LoadMaster. This means that high level flow statistics are available for encrypted traffic, but any statistics that would require decryption are not available.
- The probe exports data in IPFIX format only; NetFlowv9 format is currently unsupported on the

LoadMaster.

- Bonded interfaces can be selected on the LoadMaster for probe data, but no data is actually collected.
- Probe data is only collected for interfaces that have either an IP address or VLAN assigned (or both).

These limitations can be overcome by purchasing the full Flowmon Probe appliance for deployment outside of the LoadMaster.

2

Network Telemetry Information

Network Telemetry Information

Exported network telemetry provides information across all network layers including performance metrics and rich application layer telemetry.

Layer	Information
Link layer (L2)	- ARP - MAC addresses - VLAN tag - Interface index
Network and transport layer (L3/L4)	- IP addresses, ports, protocols - Volumetric statistics (bytes, packets, flows) - Timestamp and signaling (TCP flags) - Network performance metrics (Round Trip Time (RTT),

Layer	Information
	Server Response Time (SRT), TCP retransmissions, jitter) - Extended TCP telemetry (Time To Live (TTL), SYN packet size, default TCP window size) - VxLAN ID
Application layer (L7)	- DHCP - DNS - HTTP - Email - Application ID (Network Based Application Recognition (NBAR2)) **Note:** For further details on NBAR2, refer to the following RFC: Cisco Systems Export of Application Information in IP Flow Information Export (IPFIX). - Samba - Extended VoIP - PostgressSQL - MySQL

The network traffic is monitored on the interface level. When SSL offloading with re-encryption is used, network telemetry does not contain any application layer telemetry related to the HTTP protocol. However, TLS/SSL information such as Server Name Indication (SNI), TLS version, or certificate information is available (depending on the TLS version in use).

The reduction ratio of original traffic volume to network telemetry volume is 250:1 which means that monitoring of 1Gbps of traffic generates approximately 4Mbps of traffic statistics. The real value may vary according to traffic structure and mixture of application protocols.

For further details on IPFIX, refer to the following RFC: Information Model for IP Flow Information Export

3

Download the Flowmon Collector

Network telemetry requires an external collector to collect the IPFIX application flow data. The Flowmon Collector is the ideal network monitoring appliance that captures, stores, and processes flow data, including normalization, visualization, and analysis.

To download the Flowmon Collector, follow these steps:

1. In the main menu of the LoadMaster UI, click **Network Telemetry**.
2. Click **Download Flowmon Collector**.

   You will be taken to the Flowmon Collector download page to continue the process.

3. Enter your **Progress ID** and **Password**.

   Note: If you do not have a Progress ID, you can create one here: Create a Progress ID.

4. Click **Sign In**.

   Note: Only one Flowmon trial download is available per Progress ID.

5. Select your hypervisor from the first drop-down list.
6. Select your country from the second drop-down list.
7. Select the check box to agree to the End User License Agreement (EULA).
8. Click **Download now**.

After downloading the file, you must then deploy and run the machine on your chosen hypervisor. For instructions on how to do this, refer to the documentation provided as part of the Flowmon Collector downloadable zip package.

4

Enable and Configure Network Telemetry

Enable and Configure Network Telemetry

Network telemetry is generated per a network interface and is available disabled by default on all new LoadMaster deployments for firmware version 7.2.53 and above. To enable network telemetry navigate to the **Network Telemetry** menu item.

On Long Term Support (LTS) LoadMaster versions, or older versions of the LoadMaster that have been patched to a newer version, you may need to enable the network telemetry feature. To enable the network telemetry feature, click **Network Telemetry**in the main menu of the LoadMaster User Interface (UI) and click **Install**.

After you successfully install network telemetry on the LoadMaster, you should see a number of fields to configure on the **Network Telemetry** screen.

Note: Enabling Network Telemetry may impact performance throughput.

Details on each of these options are below:

- **IP address of Collector:** Define the destination IP address or Fully Qualified Domain Name (FQDN) and port number of your IPFIX collector (for example, **1.1.1.1:2055** or **collector.local:3000**). The IPFIX export runs over the UDP protocol and you must ensure that the collector is reachable over the network from the LoadMaster. Once you configure the collector IP address or FQDN you can validate the network connectivity by clicking **Validate** and clicking **OK**. Validation is based on a plain ICMP ping message and it validates the IP or FQDN (not the port).

Note: IPFIX is a plain text UDP packet stream. We recommend that it should only be exported over a secure network.

- **Active Timeout:** Set the global active timeout value. The default value is **300**.

  This setting ensures that very long flows will be exported in the specified time. The Timeout is checked for each incoming packet. If the corresponding flow is lasting longer than the specified timeout interval, it is deleted from the flow cache and exported to the collector.

- **Inactive Timeout:** Set the global inactive timeout value. The default value is **30**.

  This setting avoids keeping old, inactive flow records in the flow cache forever. When no packets belonging to the flow are observed for the specified timeout interval, the flow record is exported to collector

- **Export Protocol:** The export protocol (**IPFIX** is currently the only selectable protocol).

- **Advanced settings:** Enable/disable the check boxes here depending on what values you would like to collect.

Note: There are some check boxes in the **Advanced settings** section that are not possible to change at present. These will be configurable in a future release.

- **Activate export of Application Flow Data:** Select the relevant interface (or interfaces) to collect IPFIX data for.

The network interface screens (for example, **System Configuration > Network Setup > Interfaces > eth0**) indicate if network telemetry monitoring is enabled or disabled for that interface (depending on what interfaces are selected on the **Network Telemetry** screen)

Note: To enable Network Telemetry on an interface, the interface must have an IP Address. Interfaces configured with Virtual LANs cannot have Network Telemetry enabled unless an IP Address is assigned.

Note: When two LoadMasters are operating as a HA pair, the Network Telemetry traffic will present from the physical address of the LoadMaster and not the shared address. It is necessary to create a profile for both the LoadMasters in the HA pair on the Flowmon Collector.

5

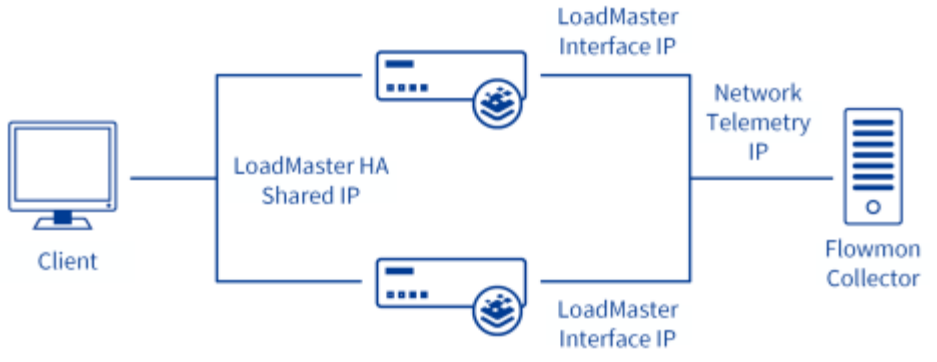
Enable and Configure Network Telemetry in a LoadMaster HA pair

Enable and Configure Network Telemetry in a LoadMaster HA pair

The network telemetry feature can be used in LoadMaster High Availability (HA) mode. Before configuring the network telemetry feature in a HA pair, ensure that both LoadMasters are using the same firmware version (7.2.53 or above).

It is recommended to configure network telemetry over the LoadMaster HA shared IP address after the two LoadMasters have been placed into HA mode.

Note: The communication of flow data only occurs between the active LoadMaster of the HA pair and the configured Collector IP. The LoadMaster determines which interface to use to communicate with the Collector IP using the same process it uses for any outbound connection it originates. This is usually going to be the network interface whose subnet is a match for the collector IP, but could also be another interface if, for example, static routes are used.



To configure the network telemetry feature in HA mode, follow the steps below:

1. Configure the two LoadMasters into HA mode. If already in HA mode, ignore this step.

   Note: For more information on how to configure the LoadMaster in HA mode, refer to the High Availablility (HA) Feature Description.

2. If the add-on package is already installed on both the LoadMasters then:

   - Ensure that the **Collector Endpoint** field is empty.
   - Expand the **Activate Export of Application Flow Data Per Interface** section at the bottom of the page and disable all currently enabled interfaces.

   Note: While upgrading the LoadMaster firmware from version 7.2.52 or below to a newer firmware version, ensure to install the network telemetry feature. To install the network telemetry feature, go to **Network Telemetry** and click **Install**.

3. Open the LoadMaster UI using the HA shared IP address (defined during HA configuration) and navigate to the **System Configuration > Miscellaneous Options > Network Options**.

4. Disable the **Enable Server NAT** option. By default this option is enabled and must be disabled when using network telemetry in HA mode. Making this change on the HA shared IP address makes the change on both HA LoadMasters.

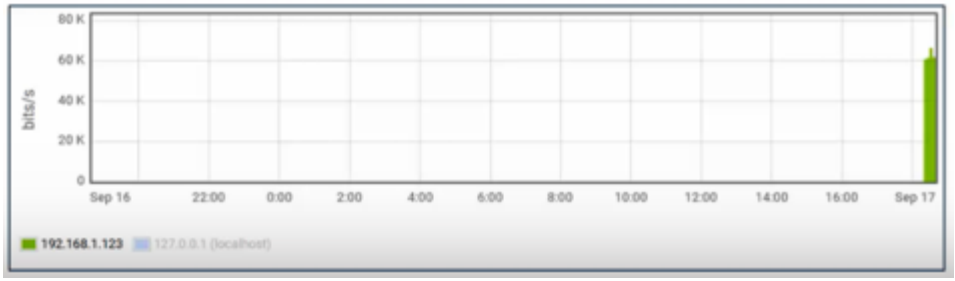
5. Click **Network Telemetry** in the main menu and do the following:

   - Enter the IP address of the **Collector Endpoint** and click the **Set Remote Address**.
   - Expand the **Activate Export of Application Flow Data Per Interface** section and select the network interface check box for which you want to collect the flow data.

   Note: The Network Telemetry settings are propagated to both LoadMasters.

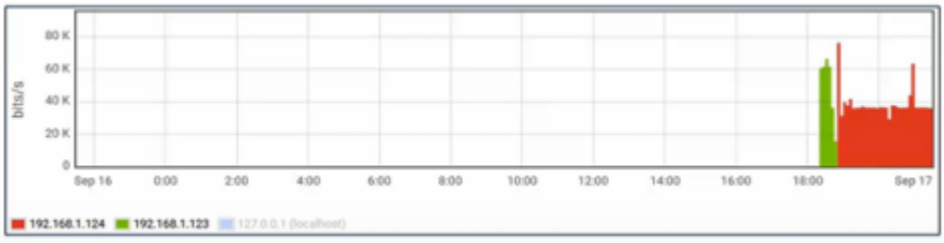
6. Open the Collector UI and navigate to the **Monitoring Center**. The **All Sources** profile is opened by default on that screen. In few minutes, the collector starts receiving the traffic from the active LoadMaster interface IP.

   In the example screenshot below – 192.168.1.123 is the interface address of active unit of the LoadMaster HA pair.



7. Open the active LoadMaster UI of HA pair and click the **System Configuration > System Administration > System Reboot > Reboot** to reboot the active LoadMaster. This moves all traffic to the standby LoadMaster which then becomes the active LoadMaster.

8. Go back to the Collector UI and navigate to the Monitoring Center. The screen now represents the initial standby unit as an active unit. You should see the appropriate interface IP of the former standby (now active) LoadMaster appear in all sources graph in the collector **Monitoring Center** page.



Flowmon Collector Dashboard in LoadMaster HA mode

The Collector starts receiving the data from a LoadMaster in the HA pair. The LoadMaster is represented as a **Source** of Monitoring center and is named using the LoadMaster IP address from which Collector is receiving the flow data. The Collector organizes its Sources into a single Profile named **All Souces**. **Profiles** contain **Channels** that are used to build **Chapters** which are further used to build **Dashboard Widgets**:

Profiles > Channels > Chapters > Dashboard Widgets

As each LoadMaster is communicating with the Collector using its unique interface IP, a separate **Channel** for each LoadMaster is defined with in **Profiles > All Sources**. In comparison, if the shared IP were used, just one channel would be created.

This provides single flexibility when building Report Chapters - the building blocks for Dashboard Widgets:

- The data set used by a **Chapter** is derived from a single **Profile**. The scope of the Chapter can be the entire Profile data set (all Channels) or can be reduced by selecting a subset of the Channels defined.

- Because both LoadMasters are represented by their own **Channels** within **Profiles > All Sources**, a **Chapter** can be built using only one of the LoadMaster HA pair channels, or both depending on the user monitoring and analysis goals.

6

Troubleshooting

Troubleshooting

If you have any issues with the network telemetry export you can use the built-in TCP dump tool as part of the debugging option on the LoadMaster to validate data is exported towards the collector. To perform a TCP dump using the LoadMaster, follow the steps below:

1. In the main menu, go to **System Configuration > Troubleshooting**.
2. In the **TCP dump** section, enter the Collector IP address in the **Address** text box.
3. Click **Start**.
4. Click **Stop** to stop the TCP dump.
5. Click **Download** to download the **.pcap** file.

Ensure that there is no specific network configuration such as a firewall or access control list that is preventing the data from reaching the export target.

You can also troubleshoot from the Collector side. Log into the Flowmon Collector using SSH and run **tcpdump** to check if flow data is reaching the Collector interface.

For detailed information related to TCP dump, refer to the Packet Trace Guide Technical Note.