Packets

Published: 2020-03-21

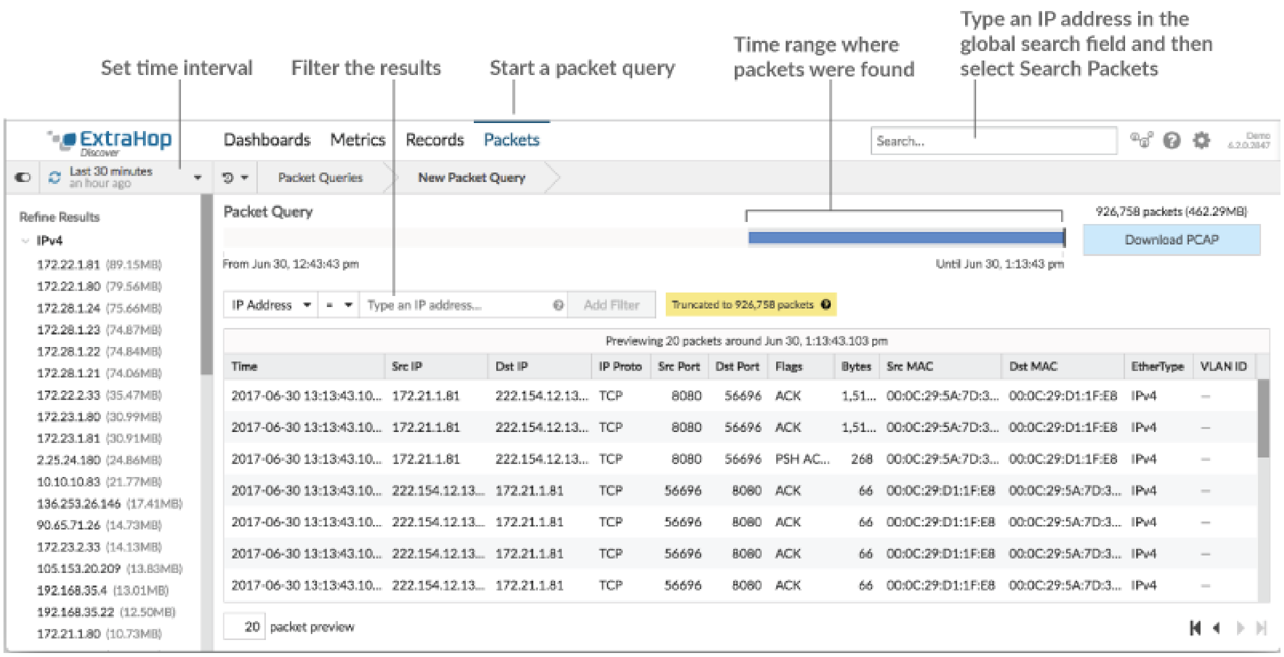
With a Reveal(x) system or an ExtraHop Trace appliance connected to a Discover appliance, you can search for and download packets for selected transactions through the Packets feature in the ExtraHop Web UI and the Packet Search resource in the ExtraHop REST API. The downloaded packets can then be analyzed through a third-party tool, such as Wireshark.

- For ExtraHop Reveal(x) systems that do not include continuous packet capture, you can configure precision packet capture by writing a trigger.
- For Discover appliances, you must deploy a Trace appliance. See the deployment guides for the ExtraHop Trace appliance.

Query for packets

You can launch a quick packet query for the current time interval by clicking **Packets** from the top menu. The ExtraHop system queries packets for the selected time interval, such as the last 30 minutes, and displays the Packet Query page. If you change the time interval, the query starts again. Either end of the gray bar displays a timestamp, which is determined by the current time interval. The time on the right displays the starting point of the query and the time on the left displays the endpoint of the query. The blue bar indicates the time range during which the system found packets. You can drag to zoom on a period of time in the blue bar to run a query again for that selected time interval.

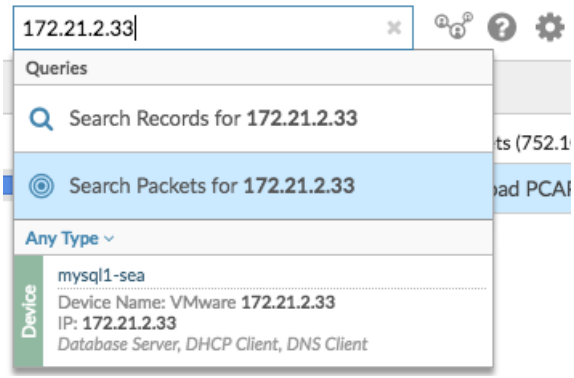
The following figure provides an overview of the Packet Query page and features:



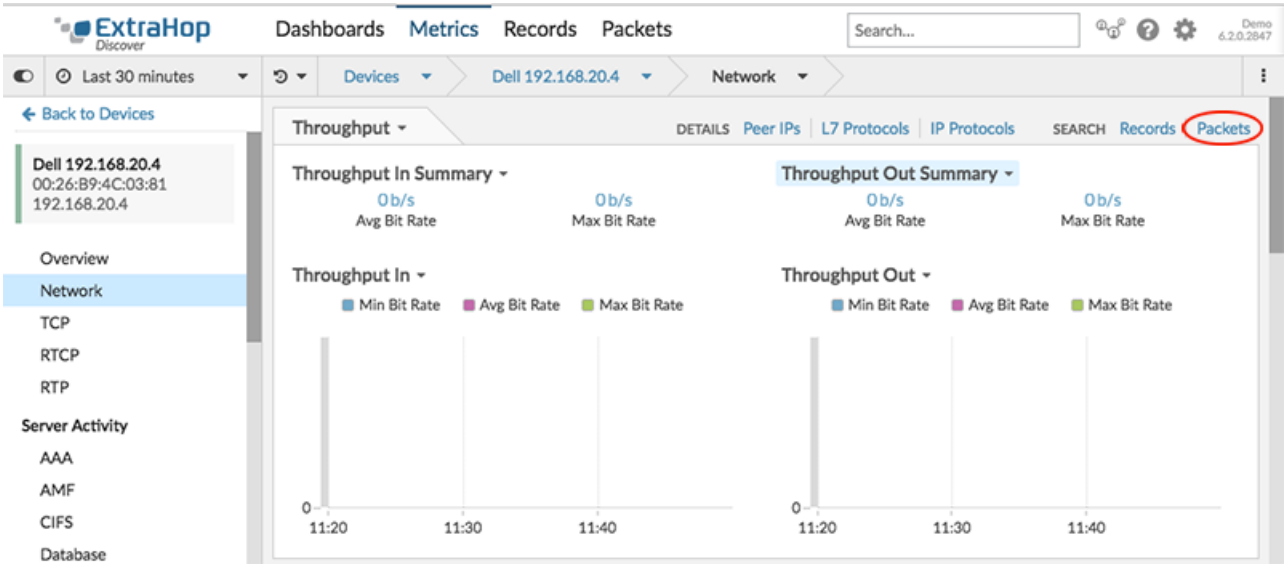
Tip: Filter packets with Berkeley Packet Filter syntax.

There are multiple locations in the ExtraHop Web UI from which you can initiate a packet query:

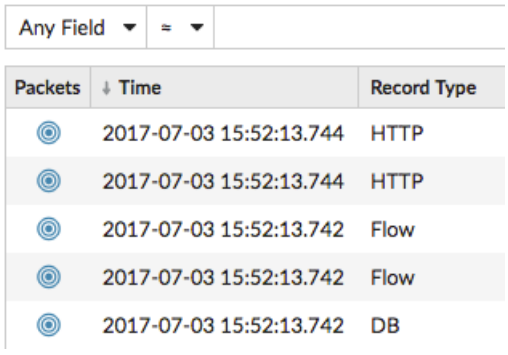
- Type an IP address in the global search field and then select the Search Packets icon .



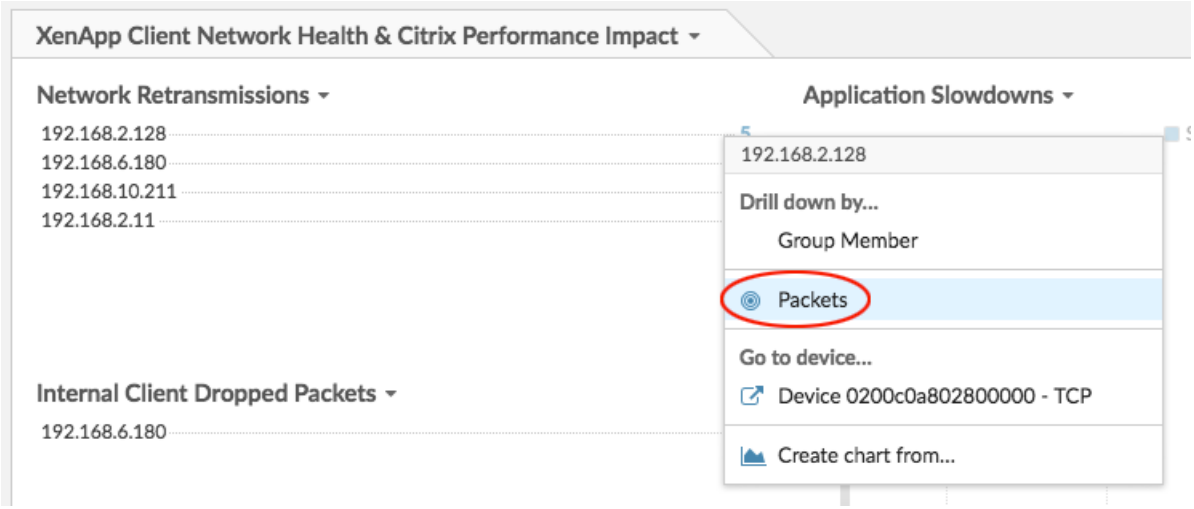
- Click **Packets** from the upper right corner of a device page.



- Click the Packets icon next to any record on a record query results page.



- Click on an IP address or hostname in any chart with metrics for network bytes or packets by IP address to see a context menu. Then, select the Packets icon to query for the device and time interval.


XenApp Client Network Health & Citrix Performance Impact
Network Retransmissions
192.168.2.128
192.168.6.180
192.168.10.211
192.168.2.11
Application Slowdowns
192.168.2.128
Drill down by...
Group Member
Packets
Go to device...
Device 0200c0a802800000 - TCP
Create chart from...
Internal Client Dropped Packets
192.168.6.180