Determining Why an Interface is Over Capacity

Use Case Abstract

Customer situation

Companies and organizations need to constantly watch for unplanned and unexpected spikes in network traffic and demand. These increases can indicate an attack, so they also need to know which applications, users, or hosts are the cause.

Solution

Use Cisco Stealthwatch® to identify the specific interface that is either overloaded or close to capacity, and identify the applications, users, or hosts that are taxing the network.

Minimum requirements

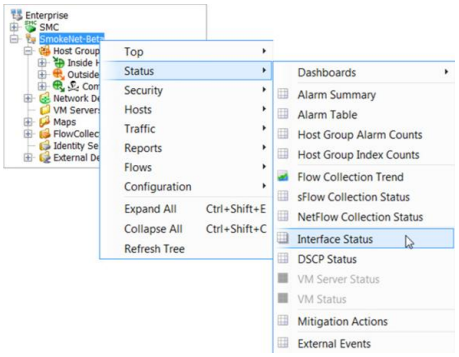
The Cisco Stealthwatch system configuration minimum requirements are:

- Visibility of all host-to-host traffic from the core/distribution
- Flow Sensor or other application-aware device
- Stealthwatch Release 6.5 or greater

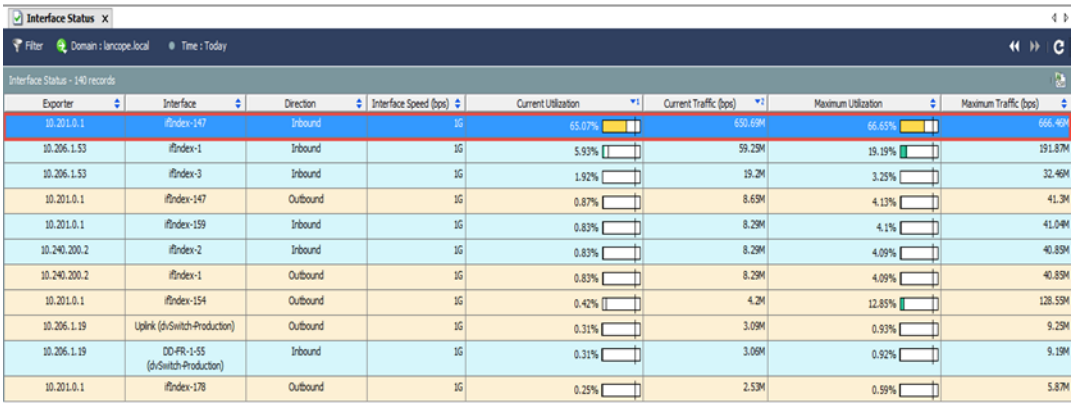
Using NetFlow to Find Traffic Spike

NetFlow allows you to drill into the host flows for each interface to find the cause of the increased network use.

Open the Interface Status document to identify the specific interface that is either overloaded or close to capacity. From the Enterprise tree, right-click the **domain name** and navigate to **Status > Interface Status**.

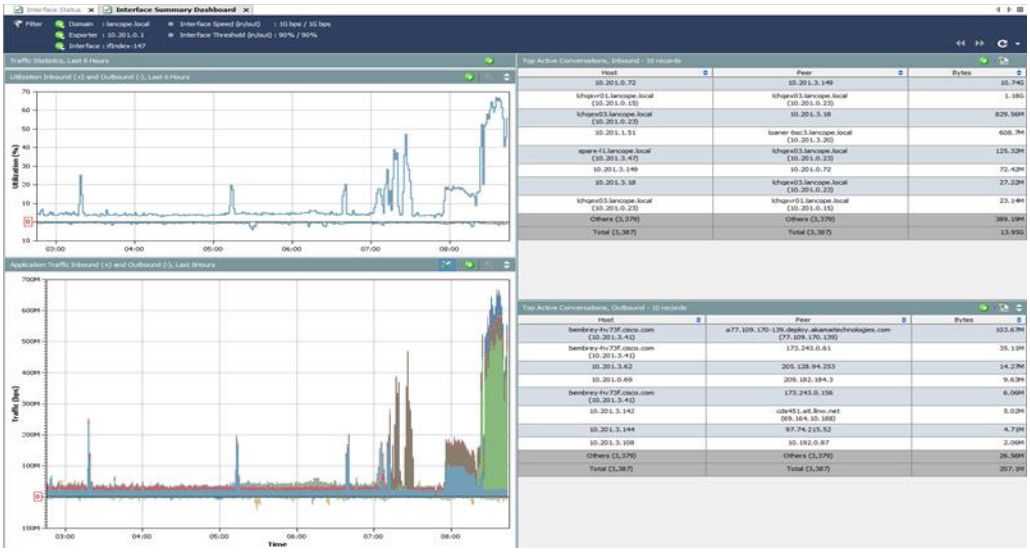


The Interface Status document opens. To identify interfaces that are either overloaded or close to capacity, look for red, orange, or yellow bars in the Current Utilization and Maximum Utilization columns. Double-click an interface with high utilization.



Exporter	Interface	Direction	Interface Speed (bps)	Current Utilization	Current Traffic (bps)	Maximum Utilization	Maximum Traffic (bps)
10.201.0.1	ifIndex-147	Inbound	1G	65.07%	650.69M	66.65%	666.46M
10.206.1.53	ifIndex-1	Inbound	1G	5.93%	59.25M	19.19%	191.87M
10.206.1.53	ifIndex-3	Inbound	1G	1.92%	19.2M	3.25%	32.46M
10.201.0.1	ifIndex-147	Outbound	1G	0.87%	8.69M	4.13%	41.3M
10.201.0.1	ifIndex-159	Inbound	1G	0.83%	8.29M	4.1%	41.04M
10.240.200.2	ifIndex-2	Inbound	1G	0.83%	8.29M	4.09%	40.85M
10.240.200.2	ifIndex-1	Outbound	1G	0.83%	8.29M	4.09%	40.85M
10.201.0.1	ifIndex-154	Outbound	1G	0.42%	4.2M	12.85%	128.55M
10.206.1.19	Uplink (dvSwitch-Production)	Outbound	1G	0.31%	3.09M	0.93%	9.25M
10.206.1.19	DD-FR-1-55 (dvSwitch-Production)	Inbound	1G	0.31%	3.06M	0.92%	9.19M
10.201.0.1	ifIndex-178	Outbound	1G	0.25%	2.53M	0.59%	5.87M

The Interface Summary Dashboard displays, showing interface details.



Determining Why an Interface is Over Capacity

On the right side of the Interface Summary Dashboard, the Top Active Conversations section shows top flows for the interface. In this case, the increased traffic is caused by an inbound conversation with the host 10.201.1.51. For a more detailed look at Top Active Conversations, click **Go To Document** (green circle with the with arrow).

Top Active Conversations, Inbound - 10 records

Host	Peer	Bytes
10.201.1.51	10.201.3.20	579.37M
10.201.0.78	10.192.0.72	16.75M
10.201.1.163	10.202.5.106	11.7M
10.201.1.163	10.201.1.161	11.7M
10.201.1.163	palantir.lancope.local (10.201.1.162)	11.7M
10.201.1.163	10.202.5.4	11.55M
10.201.1.163	10.202.5.86	11.55M
10.201.1.163	10.202.5.2	11.55M
Others (1,849)	Others (1,849)	209.19M
Total (1,857)	Total (1,857)	875.05M

The host responsible for the increased network use (10.201.1.51) is an Undefined TCP service which is filling 573.83M of traffic coming into the network.

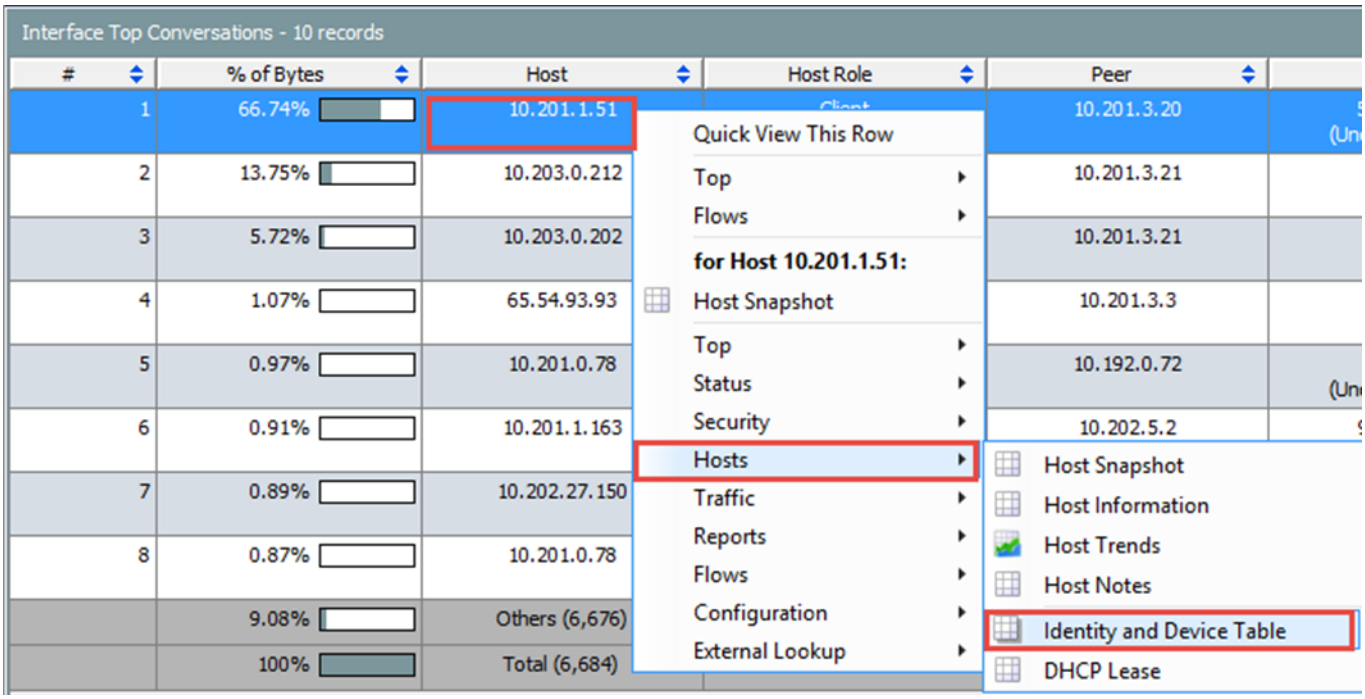
Filter
Domain : lancope.local
Exporter : 10.201.0.1
Interface : ifIndex-147
Interface Speed (in/out) : 1G bps / 1G bps
Interface Threshold (in/out) : 90% / 90%
Direction : Inbound
Time : Last 5 minutes

Interface Top Conversations - 10 records

#	% of Bytes	Host	Host Role	Peer	Port	Bytes	Packets	Flows	Host Bytes Ratio
1	64.21%	10.201.1.51	Server	loaner-bsc3.lancope.local (10.201.3.20)	22609/tcp (Undefined TCP)	573.83M	403,391	1	100%
2	1.89%	10.201.1.163	Client	10.202.5.106	2055/udp (netflow)	16.87M	12,633	1	100%
3	1.89%	10.201.1.163	Client	palantir.lancope.local (10.201.1.162)	2055/udp (netflow)	16.87M	12,633	1	100%
4	1.89%	10.201.1.163	Client	10.201.1.161	2055/udp (netflow)	16.87M	12,633	1	100%
5	1.81%	10.201.1.163	Client	10.202.5.4	2055/udp (netflow)	16.15M	12,095	1	100%
6	1.81%	10.201.1.163	Client	10.202.5.86	2055/udp (netflow)	16.15M	12,095	1	100%
7	1.81%	10.201.1.163	Client	10.201.0.69	2055/udp (netflow)	16.15M	12,095	1	100%
8	1.81%	10.201.1.163	Client	10.202.5.2	9055/udp (Undefined UDP)	16.15M	12,095	1	100%
	22.9%	Others (1,570)	Client and Server	Others (1,570)	Others (1,570)	204.68M	448,116	1,646	92.06%
	100%	Total (1,578)	Client and Server	Total (1,578)	Total (1,578)	893.73M	937,786	1,654	98.06%

If you have Cisco® Identity Service Engine (ISE) installed, you can identify and contact the user. Right-click **the host** and navigate to **Host > Identity and Device Table**.

Determining Why an Interface is Over Capacity



The Identity and Device Table displays, showing that the user responsible for the initial traffic spike is user **aandrews**.

You may also be able to identify the applications contributing to the high traffic volume. Click **Go To Document** (green circle with the with arrow) in the Application Traffic Inbound and Outbound section of the Interface Summary dashboard. A more detailed view of the Interface Application Traffic displays.