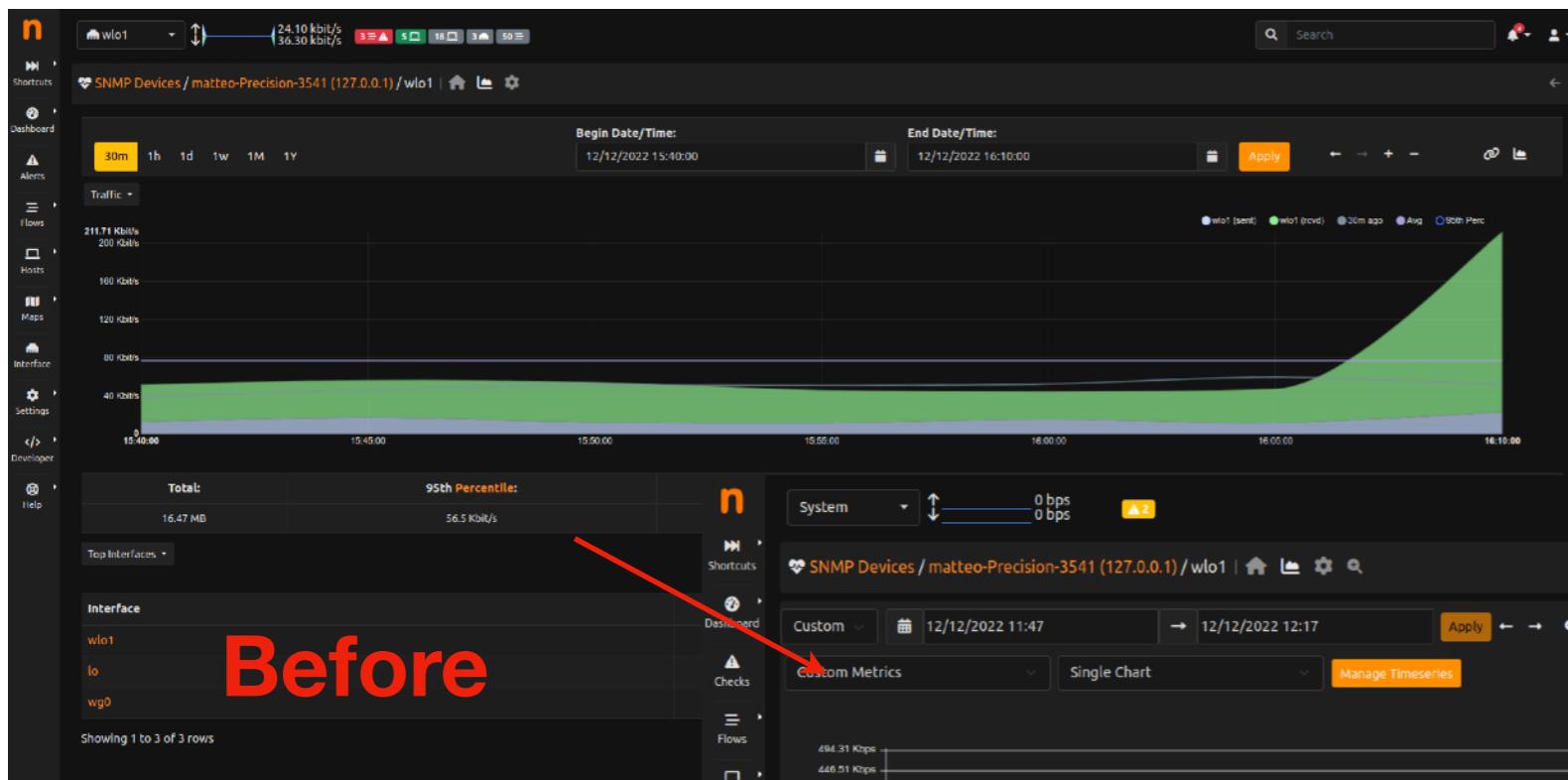
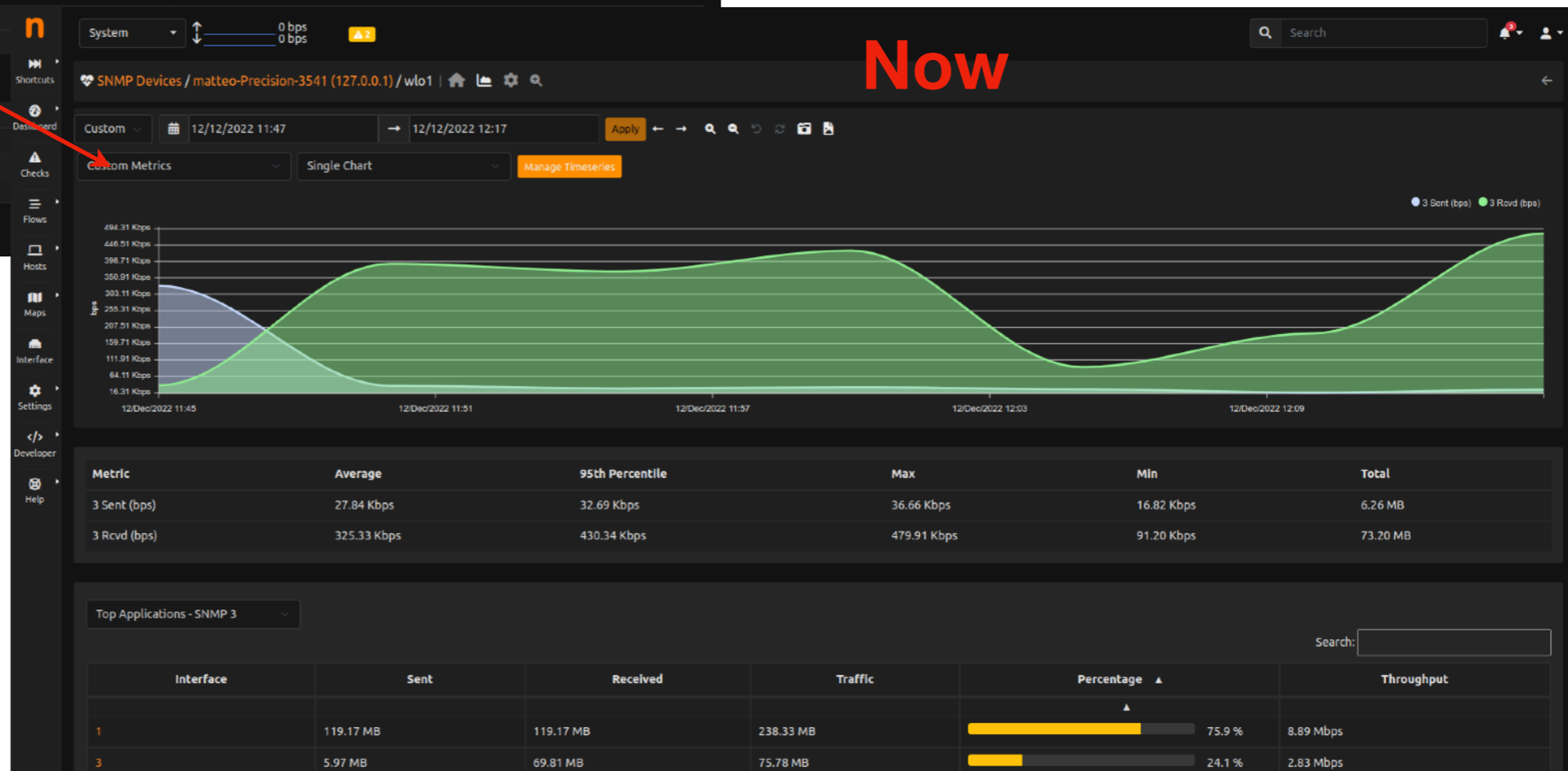


ntopng Webinar: News & Updates

ntopng: UI Refactoring



Before



Now

ntopng: New Maps

The image displays three screenshots of the ntopng interface, illustrating new map features. The top-left screenshot shows a network map with nodes representing hosts and edges representing connections. The top-right screenshot shows the 'Asset Table' view, which lists client and server information for selected hosts. The bottom screenshot shows the 'Service Table' view, which lists hosts and their associated service status.

Asset Table Data:

Client	Server	Asset Family	Last Seen
192.168.1.28	prod-ntp-4.ntp4.pcs5.cano... [185.125.190.57]	NTP	30/11/2022 10:09:16
192.168.1.28	prod-ntp-3.ntp1.pcs5.cano... [185.125.190.56]	NTP	29/11/2022 12:41:10
192.168.1.28	puget.canonical.com [91.189.94.4]	NTP	25/11/2022 10:38:34
192.168.1.28	prod-ntp-5.ntp4.pcs5.cano... [185.125.190.58]	NTP	28/11/2022 13:07:42
matteo-precision-3541.ho... [192.168.1.196]	prod-ntp-4.ntp4.pcs5.cano... [185.125.190.57]	NTP	02/12/2022 10:16:06
matteo-precision-3541.ho... [192.168.1.196]	alphyn.canonical.com [91.189.91.157]	NTP	05/12/2022 10:01:36
matteo-precision-3541.ho... [192.168.1.196]	puget.canonical.com [91.189.94.4]	NTP	07/12/2022 10:06:18
matteo-precision-3541.ho... [192.168.1.196]	prod-ntp-5.ntp4.pcs5.cano... [185.125.190.58]	NTP	12/12/2022 10:47:17
matteo-precision-3541@170 [192.168.1.196]	puget.canonical.com@170 [91.189.94.4]	NTP	07/12/2022 18:34:06

Service Table Data:

Host	Total Edges	Rank	Incoming Edges	Outgoing Edges
all-systems.mcast.net	1	193	1	0
192.168.1.255	2	132	2	0
broadcast	1	132	1	0
www.msfncl.com	1	118	1	0
p135-docws.icloud.com	3	118	2	1
224.0.0.251	1	118	1	0
192.168.1.110	3	92	0	3
matteo-precision-3541	4	92	0	4

NOTES:

- Hosts are represented as circles: Local, Remote, Multicast, Broadcast hosts and MAC addresses.
- Edges represent a communication between two hosts: allowed, denied, and undecided service status.
- Double click on a node to jump to the host map. Use the mouse wheel to zoom in/out.

ntopng: Historical Flow Enchantment

The screenshot displays the ntopng 'Historical Flows' interface. At the top, there's a status bar showing 'wlo1' with traffic statistics: 15.70 Kbps (upload) and 27.40 Kbps (download). Below this is a navigation bar with 'Historical Flows', 'Flows', and 'Analysis' tabs. A filter bar shows 'Last 30 Min' and a time range from '12/12/2022 15:50' to '12/12/2022 16:20'. A large area contains a traffic volume graph. Below the graph, a table lists flow entries. An 'Add Filter' dialog is open, showing a list of filterable fields: Alert Type, Application, Bytes, Category, Cli Network Latency, Client ASN, and Client Country. The 'Alert Type' field is currently selected in the dialog.

Flow	Protocol	Direction	Bytes	Rate	Start	End	Server ASN	L7 Category	Status	Actions
fe80::d6b7:9ff:fe3c:3de... 3 ↔ ip6-allnodes	IPv6-ICMP	ICMPV6						Network	Normal	
matteo-precision-3541 ↔ ff02::16	IPv6-ICMP	ICMPV6						Network	Normal	
fe80::d6b7:9ff:fe3c:3de... 3 ↔ ip6-allnodes	IPv6-ICMP	ICMPV6						Network	Normal	
matteo-precision-3541 ↔ ff02::16	IPv6-ICMP	ICMPV6						Network	Normal	
fe80::d6b7:9ff:fe3c:3de... 3 ↔ ip6-allnodes	IPv6-ICMP	ICMPV6						Network	Normal	
matteo-precision-3541 ↔ ff02::16	IPv6-ICMP	ICMPV6						Network	Normal	
matteo-precision-3541 ↔ ff02::16	IPv6-ICMP	ICMPV6	220 Bytes	1.76 kbps	16:04:29	16:04:29		Network	Normal	
fe80::d6b7:9ff:fe3c:3de... 3 ↔ ip6-allnodes	IPv6-ICMP	ICMPV6	102 Bytes	816 bps	16:04:29	16:04:29		Network	Normal	
fe80::f8b9:93ca:30d6:82e... 6 ↔ ff02::1:ff7a:6bd6	IPv6-ICMP	ICMPV6	86 Bytes	688 bps	16:09:00	16:09:00		Network	Normal	
matteo-precision-3541 ↔ fe80::f8b9:93ca:30d6:82e... 6	IPv6-ICMP	ICMPV6	10	5.31 KB	7.25 kbps	16:09:00	16:09:05	Network	Unidirectional Traffic	
matteo-precision-3541:49726 ↔ p135-docws.icloud.com:53	UDP	DNS	50	166 Bytes	1.33 kbps	16:18:46	16:18:46	Network	Lateral Movement	

ntopng: New XL Version

- Added a new version: XL license
 - Increased the maximum number of exporters (reaching 1024 total exporters)
 - Support to Host Flow Sankey
 - Increased the maximum number of monitored interfaces (up to 64)

ntopng: Performances (1/2)

ntopng analysing a single Wi-Fi Interface, with ClickHouse enabled:

Version	CPU Usage	Memory Usage	Thread Num.
v. 5.5	8~11%	2~2.5%	24~30
v. 5.2	8~11%	2~3%	27~33
v. 4.4	13~17%	6~8%	50~60+

Test done using:

- CPU: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz
- Memory: 8 GB

ntopng: Performances (2/2)

ntopng analysing 4 Interfaces, with ClickHouse enabled:

Version	CPU Usage	Memory Usage	Thread Num.
v. 5.5	15~22%	6~7%	38~42
v. 5.2	23~40%	5~7%	40~46
v. 4.4	30~50%	12~20%	60~70+

Test done using:

- CPU: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz
- Memory: 8 GB

nEdge

- Added support for multi-WAN and multi-LAN
- Added support for VLANs
- Added handling of DHCPd Service