

What your SNMP tells me

Dave Phelan

Policy Manager and Senior Network Analyst

Who Am I?

- Dave Phelan
 - Network and Infrastructure engineer for a LONG time
 - Policy Manager/Senior Network Analyst APNIC
 - Likes Cat memes



What is SNMP?

- Simple Network Management Protocol
 - Uses Port 161/UDP for polling and 162/UDP for Traps
 - Used to monitor, and sometimes manage devices
 - 3 Versions (v1, v2c, v3)
 - v1 is considered dead uses communities for “Authentication”
 - v2c added GETBULK and 64-bit counters, still uses communities
 - v3 Added Authentication, Encryption, User-based Access control, and Message Integrity Checks
 - Version 2 is Still deployed heavily.

What is SNMP?

- Simple Network Management Protocol
 - 2 Methods for getting information
 - Polling (GET/GETNEXT/GETBULK) – This is a pull operation
 - Traps - Send a message to a SNMP Manager
 - TRAP – No Ack
 - INFORM – with ACK
- MIB – Management Information Base
 - Database/Dictionary of what information is available on the device
- OID – Object Identifier
 - Unique Numeric Path to a specific Value

Why are you telling me this?

- I have been talking about open SNMP Ports for YEARS!
 - But in a different context (DDoS Reflection and Amplification)
- What information are you leaking to anyone who wants to look?
- Can I rebuild your Network infra based on SNMP Data?

Open SNMP in South Asia

Economy	Open v2c SNMP Devices
Afghanistan	814
Bangladesh	22,782
Bhutan	52
India	52,730
Sri Lanka	165
Maldives	43
Nepal	823
Pakistan	4,900

<https://www.shodan.io/search?query=country%3A{cc}+port%3A161+%22Versions%3A+1%22>

Open SNMP in South Asia

Economy	Open v2c SNMP Devices
Afghanistan	814
Bangladesh	22,782
Bhutan	2
India	52,730
Sri Lanka	8
Maldives	43
Nepal	823
Pakistan	4,900

Not all of this is
ISP Infra
But
Too Much is

<https://www.shodan.io/search?query=country%3A{cc}+port%3A161+%22Versions%3A+1%22>

Now What??
Build a Lab!

Lab Rules!

- ISP Network
 - Edge/Core Devices
 - CG-NAT Devices
 - BNG/BRAS
 - Management Network
 - End Devices(users)
 - Upstream provider(s)
- Can only use snmpwalk and standard/vendor MIBs
- Leave some devices exposed
- Model on things I have seen
 - Real networks with similar topologies
- **Infer from SNMP data only**
 - MAC Tables, Port Descriptions etc

Which MIBs are useful?

- SNMPv2-MIB::sysName - What do you call me?
 - Typically a hostname
- SNMPv2-MIB::sysDescr - What am I?
 - Device Model/Manufacturer
- sysName = CORE-NAT-A
- sysDescr = RouterOS CCR1072-1G-8S+

Which MIBs are useful?

- IP-MIB::ipAdEntAddr
 - Interface Address information
- IF-MIB::ifPhysAddress
 - Interface MAC Address
- IP-MIB::ipNetToMedia
 - Connected device MAC addresses
- This gives me IP address info and allows me to infer neighborhood and connectivity

The first chunk!

- What can I see?



SVC-MGMT-01
CCR1009



CORE-NAT-A
CCR1072



CORE-NAT-B
CCR1036



BNG-A
CCR1036

Initial Discoveries - MGMT



SVC-MGMT-01
CCR1009

- What can I see?
 - Lots of VLANS
 - Many Neighbors
 - Lots of ARP Entries
 - I know it's a Mikrotik
 - Can I use MT specific MIBs?
 - YES!
 - MT Discovery/CDP/LLDP info now available

The first chunk!



SVC-MGMT-01
CCR1009

- Interfaces

ifIndex	Interface Name	Alias	Description	Type	Admin Status	Oper Status	MAC
6	vlan250_mgmt		vlan250_mgmt	I2vlan(135)	up(1)	up(1)	cc:2d:d1:fc:53:88
8	lo		lo	bridge(209)	up(1)	up(1)	cc:2d:d1:fc:53:8c
9	bridge-lan		bridge-lan	bridge(209)	up(1)	up(1)	92:29:a4:63:5a:9f
10	combo1-uplink		combo1-uplink	ethernetCsmacd(6)	up(1)	up(1)	cc:2d:d1:fc:53:88
16	ether7-mx-jnpr		ether7-mx-jnpr	ethernetCsmacd(6)	up(1)	up(1)	cc:2d:d1:fc:53:8e
19	vlan201_office		vlan201_office	I2vlan(135)	up(1)	up(1)	cc:2d:d1:fc:53:88
20	vlan2_core		vlan2_core	I2vlan(135)	up(1)	up(1)	cc:2d:d1:fc:53:88
23	vlan5_server-mgmt		vlan5_server-mgmt	I2vlan(135)	up(1)	up(1)	cc:2d:d1:fc:53:88
25	vlan88_core-ptp		vlan88_core-ptp	I2vlan(135)	up(1)	up(1)	cc:2d:d1:fc:53:88
26	vlan23_mpls-ptp		vlan23_mpls-ptp	I2vlan(135)	up(1)	up(1)	cc:2d:d1:fc:53:88
28	vlan30_tr069		vlan30_tr069	I2vlan(135)	up(1)	up(1)	cc:2d:d1:fc:53:88

The first chunk!



SVC-MGMT-01
CCR1009

- IP Addresses

ifIndex	Interface Name	IP Address	CIDR
6	vlan250_MGMT	172.22.0.1	172.22.0.1/24
12	ether3	192.168.77.1	192.168.77.1/24
19	vlan201_office	10.100.0.1	10.100.0.1/24
20	vlan2_core	240.X.X.62	240.X.X.62/28
23	vlan5_server-mgmt	10.22.30.1	10.22.30.1/24
25	vlan88_core-ntp	240.X.X.68	240.X.X.68/29
26	vlan23_mpls-ntp	10.20.23.1	10.20.23.1/24
28	vlan35_cpe_mgmt	10.35.0.1	10.35.0.1/18

The first chunk!



SVC-MGMT-01
CCR1009

- MT Discovery Neighbors

Local ifIndex	Local Interface	Neighbor Identity	Neighbor IP	Neighbor MAC	Vendor	Platform	Version
10	combo1-uplink	SW-AGG	172.18.10.1	f4:4e:05:95:78:b0	Cisco	N3K-C3064PQ-10GX	Cisco Nexus Operating System (NX-OS) Software, Version X.Y
25	vlan88_core-ptp	CORE-NAT-B	240.X.X.67	08:55:31:16:73:f5	Routerboard	MikroTik	7.22.2 (stable)
20	vlan2_core	CORE-NAT-A	240.X.X.49	dc:2c:6e:7c:20:45	Routerboard	MikroTik	7.19.3 (stable)
25	vlan88_core-ptp	CORE-NAT-A	240.X.X.66	dc:2c:6e:7c:20:45	Routerboard	MikroTik	7.19.3 (stable)

The first chunk!



SVC-MGMT-01
CCR1009

- LLDP Neighbors

SVC-MGMT-01	Remote system	Remote port ID	Chassis MAC
combo1-uplink	SW-AGG	Ethernet1/2	F4:4E:05:95:78:B0
vlan2_core	CORE-NAT-A	vlan2_core	DC:2C:6E:7C:20:45
vlan88_core-ptp	CORE-NAT-B	vlan88_core-ptp	08:55:31:16:73:F5
vlan88_core-ptp	CORE-NAT-A	vlan88_core-ptp	DC:2C:6E:7C:20:45

The first chunk!



SVC-MGMT-01
CCR1009

- Routes

30:7c:5e:3a:5a:a1
Juniper

20:0b:c7:2a:d7:d7
Huawei

Prefix	Next Hop	Index	Interface Name	Type	Proto	Metric1	Status
0.0.0.0/0	240.X.X.65	0		remote(4)	netmgmt(3)	1	active(1)
10.20.10.0/24	10.20.23.5	0		remote(4)	netmgmt(3)	1	active(1)
10.20.23.0/24		26	vlan23_mpls-ptp	local(3)	local(2)	0	active(1)
10.22.30.0/24		23	vlan5_server-mgmt	local(3)	local(2)	0	active(1)
10.35.0.0/20		28	vlan35_cpe_mgmt	local(3)	local(2)	0	active(1)
10.100.0.0/24		19	vlan201_office	local(3)	local(2)	0	active(1)
240.X.X.48/28		20	vlan2_core	local(3)	local(2)	0	active(1)
240.X.X.64/29		25	vlan88_core-ptp	local(3)	local(2)	0	active(1)
172.22.0.0/24		6	vlan250_mgmt	local(3)	local(2)	0	active(1)

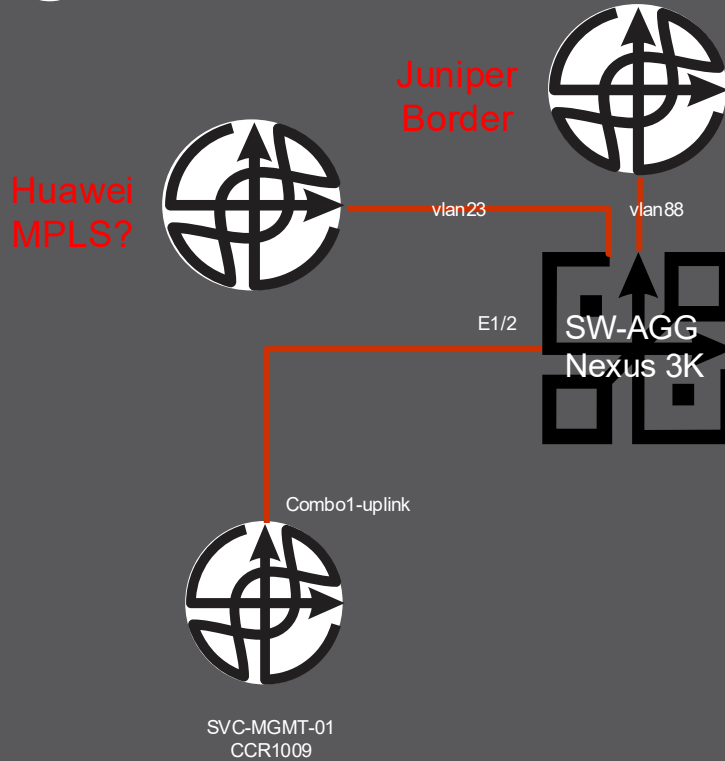
Findings So Far



SVC-MGMT-01
CCR1009

- 4 New “Core” Devices
 - Switch (Cisco Nexus 3K)
 - Huawei SOMETHING (No LLDP)
 - 2 Mikrotik Routers
- Interface IP Addresses
- Route Tables
- Interface and Neighbor MACS
- Lots of Managed CPEs
- Lots of Network switches – Various Vendors
- Lots of Office Devices – PCs, printers, VoIP Phones
- Lots of Servers

Findings So Far



Initial Discoveries – NAT-A



CORE-NAT-A
CCR1072

- Less Devices
 - Small ARP Table
- Possible new Device
 - Port Naming
- LACP Trunks
- Another Upstream?

Next One!



CORE-NAT-A
CCR1072

- Interfaces

ifIndex	Interface Name	Alias	Description	Type	Admin Status	Oper Status	MAC
5	sfp-sfpplus5	LACP:n3k-eth1/9	sfp-sfpplus5	ethernetCsmacd(6)	up(1)	up(1)	dc:2c:6e:7c:20:45
6	sfp-sfpplus6	LACP:n3k-eth1/8	sfp-sfpplus6	ethernetCsmacd(6)	up(1)	up(1)	dc:2c:6e:7c:20:46
7	sfp-sfpplus7	LACP:n3k-eth1/7	sfp-sfpplus7	ethernetCsmacd(6)	up(1)	up(1)	dc:2c:6e:7c:20:47
13	lacp_bundle		lacp_bundle	ieee8023adLag(161)	up(1)	up(1)	dc:2c:6e:7c:20:45
24	UPLINK_2		UPLINK_2	l2vlan(135)	up(1)	up(1)	dc:2c:6e:7c:20:45
26	vlan2_core		vlan2_core	l2vlan(135)	up(1)	up(1)	dc:2c:6e:7c:20:45
29	vlan88_core-ptp		vlan88_core-ptp	l2vlan(135)	up(1)	up(1)	dc:2c:6e:7c:20:45
30	vlan90-mx240-ptp		vlan90-mx240-ptp	l2vlan(135)	up(1)	up(1)	dc:2c:6e:7c:20:45
31	lo		lo	other(1)	up(1)	up(1)	00:00:00:00:00:00

Next One!



CORE-NAT-A
CCR1072

- IP Addresses

ifIndex	Interface Name	IP Address	CIDR
24	UPLINK_2	240.X.X.34	240.X.X.34/30
26	vlan2_core	240.X.X.49	240.X.X.49/28
29	vlan88_core_ptp	240.X.X.66	240.X.X.66/29
30	vlan90_mx240-ptp	240.X.X.73	240.X.X.72/30

Next One!



CORE-NAT-A
CCR1072

- MT Discovery

Local ifIndex	Local Interface	Neighbor Identity	Neighbor IP	Neighbor MAC	Vendor	Platform	Version
6	sfp-sfpplus6	SW-AGG	172.18.10.1	f4:4e:05:95:78:c8	Cisco	Cisco	
7	sfp-sfpplus7	SW-AGG	172.18.10.1	f4:4e:05:95:78:c7	Cisco	Cisco	
5	sfp-sfpplus5	SW-AGG	172.18.10.1	f4:4e:05:95:78:c6	Cisco	N3K-C3064PQ-10GX	Cisco Nexus Operating System (NX-OS) Software, Version X.Y
29	vlan88_core-ptp	CORE-NAT-B	240.X.X.67	08:55:31:26:73:f5	Routerboard	MikroTik	7.22.2 (stable)
26	vlan2_core	SVC-MGMT-01		cc:2d:e0:fc:53:88	Routerboard	MikroTik	7.19.2 (stable)
29	vlan88_nats-ptp	SVC-MGMT-01	240.X.X.68	cc:2d:e0:fc:53:88	Routerboard	MikroTik	7.19.2 (stable)

Next One!



CORE-NAT-A
CCR1072

- LLDP

CORE-NAT-A	Remote system	Remote port ID	Chassis MAC
sfp-sfpplus5	SW-AGG	Ethernet1/4	F4:4E:05:95:78:C6
sfp-sfpplus6	SW-AGG	Ethernet1/6	F4:4E:05:95:78:C8
sfp-sfpplus7	SW-AGG	Ethernet1/5	F4:4E:05:95:78:C7

Next One!



CORE-NAT-A

- Routes

Prefix	Next Hop	Index	Interface Name	Type	Proto	Metric1	Status
0.0.0.0/0	240.X.X.65			remote(4)	netmgmt(3)	1	active(1)
10.10.0.0/20	240.X.X.51	0		remote(4)	netmgmt(3)	1	active(1)
10.10.16.0/20	240.X.X.51	0		remote(4)	netmgmt(3)	1	active(1)
10.10.32.0/20	240.X.X.51			remote(4)	netmgmt(3)	1	active(1)
100.66.0.0/16	240.X.X.74	0		remote(4)	netmgmt(3)	1	active(1)
240.X.X.32/30		24	UPLINK_2	local(3)	local(2)	0	active(1)
240.X.X.48/28		26	vlan2_core	local(3)	local(2)	0	active(1)
240.X.X.64/29		29	vlan88_core-ptp	local(3)	local(2)	0	active(1)
240.X.X.72/30		30	vlan90_mx240-ptp	local(3)	local(2)	0	active(1)
240.X.X.80/28	240.X.X.51	0		remote(4)	netmgmt(3)	1	active(1)
172.22.0.0/24	240.X.X.62	0		remote(4)	netmgmt(3)	1	active(1)

64:d1:54:4c:2a:a1
Mikrotik

84:18:88:3c:a8:d1
Juniper

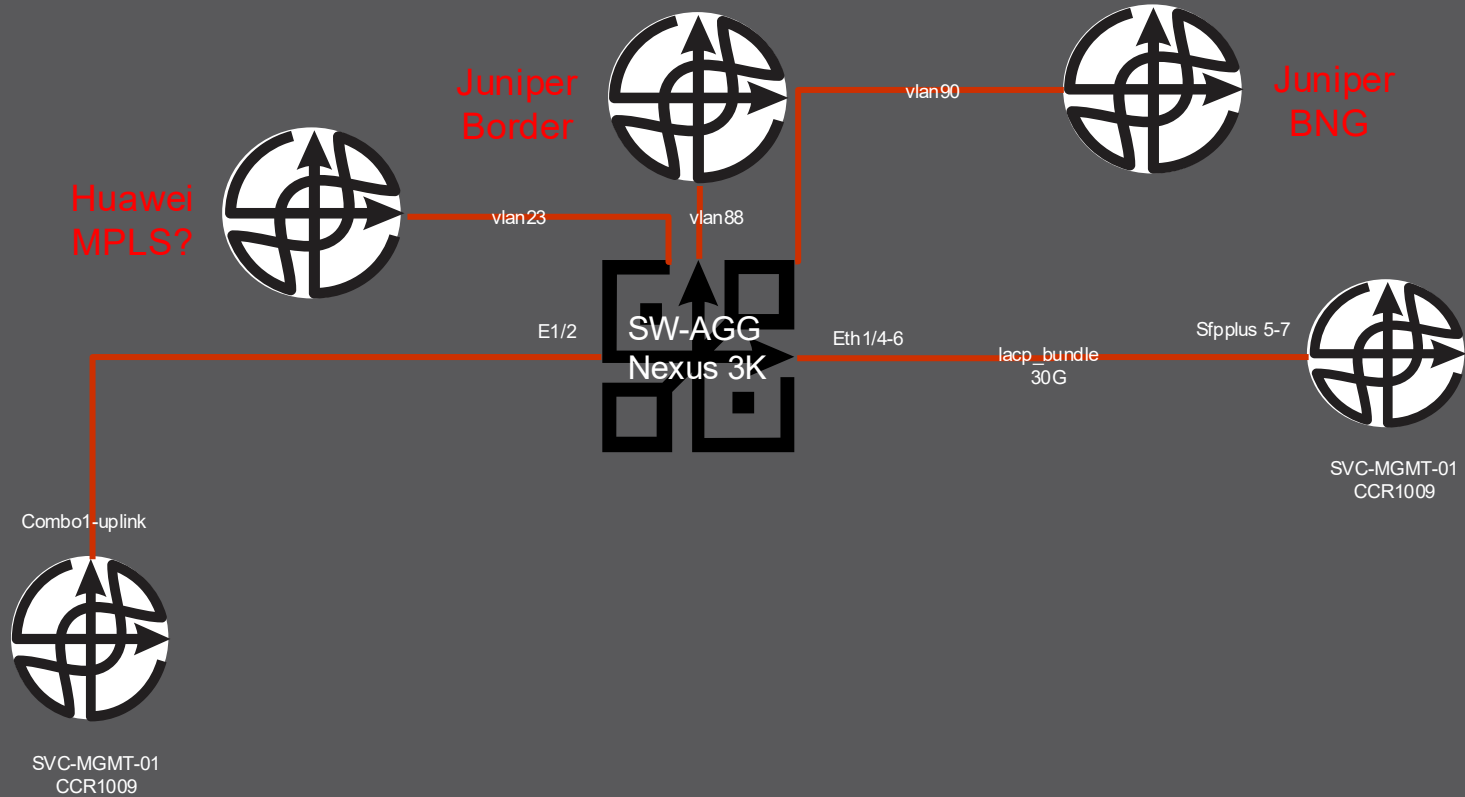
What New things do we know?



CORE-NAT-A
CCR1072

- Routed Private address space
 - Strong Indication this is a NAT Box(Also the name)
- Some evidence of BNGs
 - Possible MX240
 - Another Mikrotik
- Connected to the same SW-AGG
 - 30Gb LACP Trunk
 - VLANs on the Trunk Port

The Network Grows

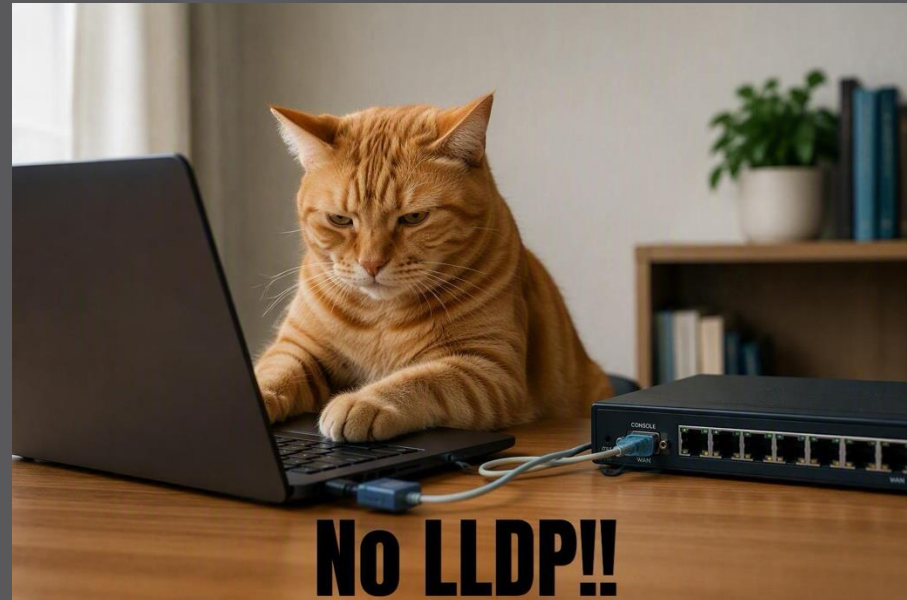


Initial Discoveries – BNG-A



BNG-A
CCR1036

- PPPoE Interfaces
 - Many Users
 - Evidence of PPPoE Server
- No LLDP/MT Discovery ☹️



It's BNG time!



BNG-A
CCR1036

- Interfaces

ifIndex	Interface Name	Alias	Description	Type	Admin Status	Oper Status	MAC	Vendor
1	sfp-sfpplus1	LINK-to-SW-AGG	sfp-sfpplus1	ethernetCsmacd(6)	up(1)	up(1)	64:d1:54:4c:2a:a1	Routerboard.com
13	lo		lo	bridge(209)	up(1)	up(1)	12:51:bb:66:a5:59	
39	vlan311		vlan311	I2vlan(135)	up(1)	up(1)	64:d1:54:4c:2a:a1	Routerboard.com
40	vlan2_core		vlan2_core	I2vlan(135)	up(1)	up(1)	64:d1:54:4c:2a:a1	Routerboard.com

It's BNG time!



BNG-A
CCR1036

- IP Addresses

ifIndex	Interface Name	IP Address	CIDR	Network	Netmask
40	vlan2_core	240.X.X.51	240.X.X.51/28	240.X.X.48/28	255.255.255.240
39	vlan311	240.X.X.81	240.X.X.81/28	240.X.X.80/28	255.255.255.240
39	vlan311	192.168.99.1	192.168.99.1/24	192.168.99.0/24	255.255.255.0

It's BNG time!



BNG-A
CCR1036

- Routes

Matches PPPoE
Devices

PPPoE Server
IP?

Prefix	Next Hop	ifIndex	Interface Name	Type	Proto	Metric	Status
0.0.0.0/0	240.X.X.49	40	vlan2_core	remote(4)	netmgmt(3)	1	active(1)
10.10.0.0/24	10.10.0.1	39	vlan311	local(3)	local(2)	0	active(1)
240.X.X.48/28	240.X.X.51	40	vlan2_core	local(3)	local(2)	0	active(1)
240.X.X.80/28	240.X.X.81	39	vlan311	local(3)	local(2)	0	active(1)
192.168.99.0/24	192.168.99.1	39	vlan311	local(3)	local(2)	0	active(1)

It's BNG time!



BNG-A
CCR1036

- Routes

Prefix	Next Hop	ifIndex	Interface Name	Type	Proto	Metric	Status
0.0.0.0/0	240.X.X.49	40	vlan2_core	remote(4)	netmgmt(3)	1	active(1)
10.10.0.0/24	10.10.0.1	39	vlan311	local(3)	local(2)	0	active(1)
240.X.X.48/28	240.X.X.51	40	vlan2_core	local(3)	local(2)	0	active(1)
240.X.X.80/28	240.X.X.81	39	vlan311	local(3)	local(2)	0	active(1)
192.168.99.0/24	192.168.99.1	39	vlan311	local(3)	local(2)	0	active(1)

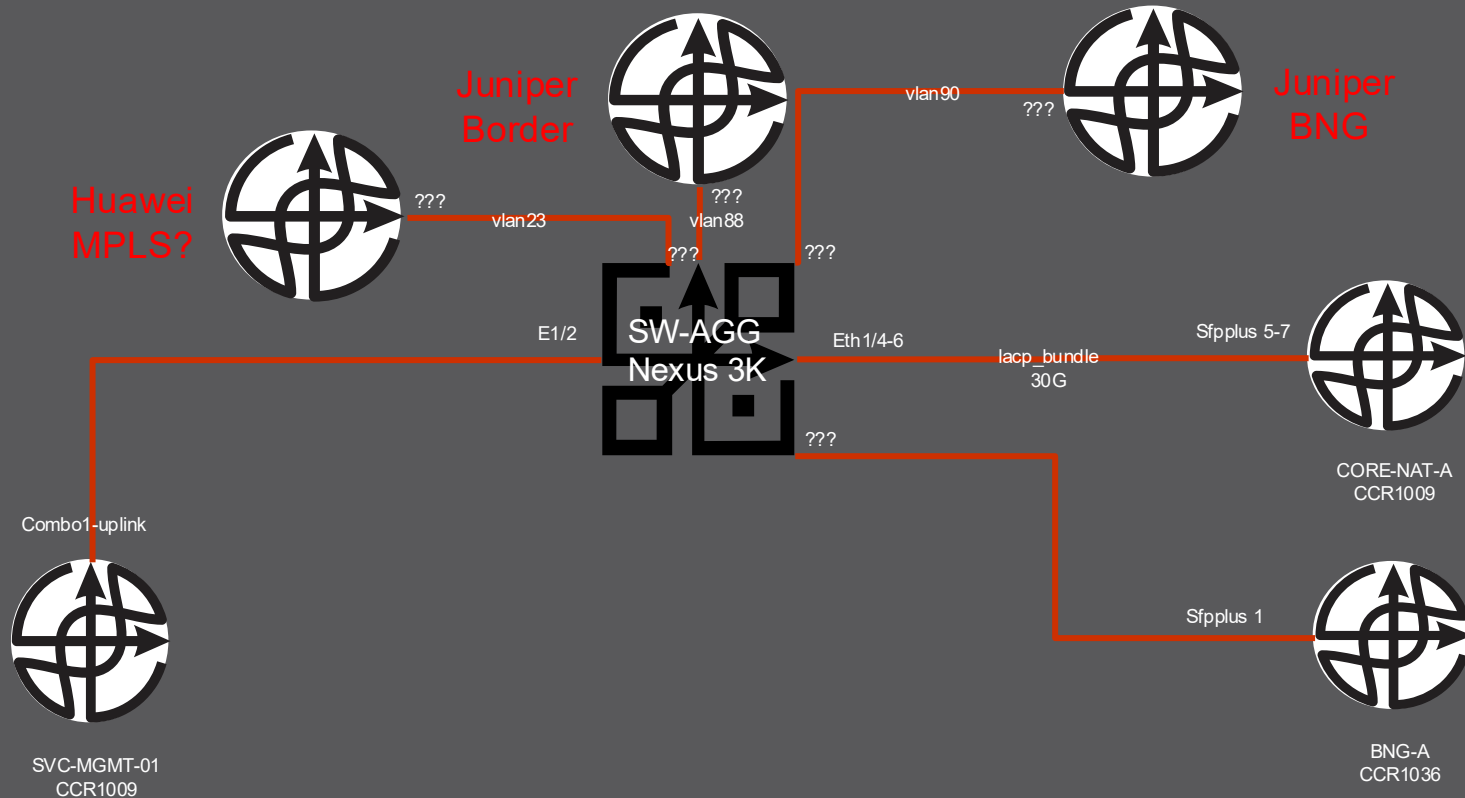
What New things do we know?



BNG-A
CCR1036

- Probably a BNG/BRAS
 - PPPoE users
- Def Route via CORE-NAT-A
- Probably some more targets (Customers) in the Non-NAT Subnet
- Current OS version has issues - CVE-2024-54772
 - SNMPv2-SMI::mib-2.47.1.1.1.1.2.65536 = STRING: "RouterOS 6.49.13 (long-term) on CCR1036-8G-2S+"
 - Username enumeration possible

The Network Grows Again!



Finally – CORE-NAT-B



CORE-NAT-B
CCR1036

- Another NAT Box
- Indications of maybe another BNG
- Indications of Another Upstream/Device

The Last one!



CORE-NAT-B
CCR1036

- Interfaces

ifIndex	Interface Name	Alias	Description	Type	Admin Status	Oper Status	MAC
1	sfp-sfpplus1		sfp-sfpplus1	ethernetCsmacd(6)	up(1)	up(1)	08:55:31:16:73:f5
2	sfp-sfpplus2		sfp-sfpplus2	ethernetCsmacd(6)	up(1)	up(1)	08:55:31:16:73:f6
11	uplink-20g	LACP: Uplink	uplink-20g	ieee8023adLag(161)	up(1)	up(1)	08:55:31:16:73:f5
12	vlan88_core-ptp		vlan88_core-ptp	I2vlan(135)	up(1)	up(1)	08:55:31:16:73:f5
13	vlan91_mx240-ptp		vlan91_mx240-ptp	I2vlan(135)	up(1)	up(1)	08:55:31:16:73:f5
14	lo		lo	other(1)	up(1)	up(1)	00:00:00:00:00:00
15	vlan1889_core-ptp-secondary		vlan1889_core-ptp-secondary	I2vlan(135)	up(1)	up(1)	08:55:31:16:73:f5

The Last one!



CORE-NAT-B
CCR1036

- IP Addresses

New Devices?

ifIndex	Interface Name	IP Address	CIDR	Network	Netmask
12	vlan88_core-ptp	240.X.X.67	240.X.X.67/29	240.X.X.64/29	255.255.255.248
13	vlan91_mx240-ptp	240.X.X.77	240.X.X.77/30	240.X.X.76/30	255.255.255.252
15	vlan1889_core-ptp-secondary	240.X.Y.2	240.X.Y.2/30	240.X.Y.0/30	255.255.255.252

The Last one!



CORE-NAT-B
CCR1036

- LLDP
 - MT Discovery gave us nothing new

CORE-NAT-B	Remote device	Remote port
sfp-sfpplus1	SW-AGG	Ethernet1/15
sfp-sfpplus2	SW-AGG	Ethernet1/16

The Last one!



CORE-NAT-B
CCR1036

- Routes

30:7c:5e:3a:5a:a1
Juniper

84:18:88:3c:a8:d1
Juniper (existing)

Prefix	Next Hop	Index	Interface Name	Type	Proto	Metric	Status
0.0.0.0/0	240.X.X.65	0		remote(4)	netmgmt(3)	2	active(1)
0.0.0.0/0	240.X.Y.1	0		remote(4)	netmgmt(3)	1	active(1)
100.67.0.0/16	240.X.X.78	0		remote(4)	netmgmt(3)	1	active(1)
240.X.X.64/29		12	vlan88_core-ptp	local(3)	local(2)	0	active(1)
240.X.X.76/30		13	vlan91_mx240-ptp	local(3)	local(2)	0	active(1)
240.X.Y.0/30		15	vlan1889_core-ptp-secondary	local(3)	local(2)	0	active(1)

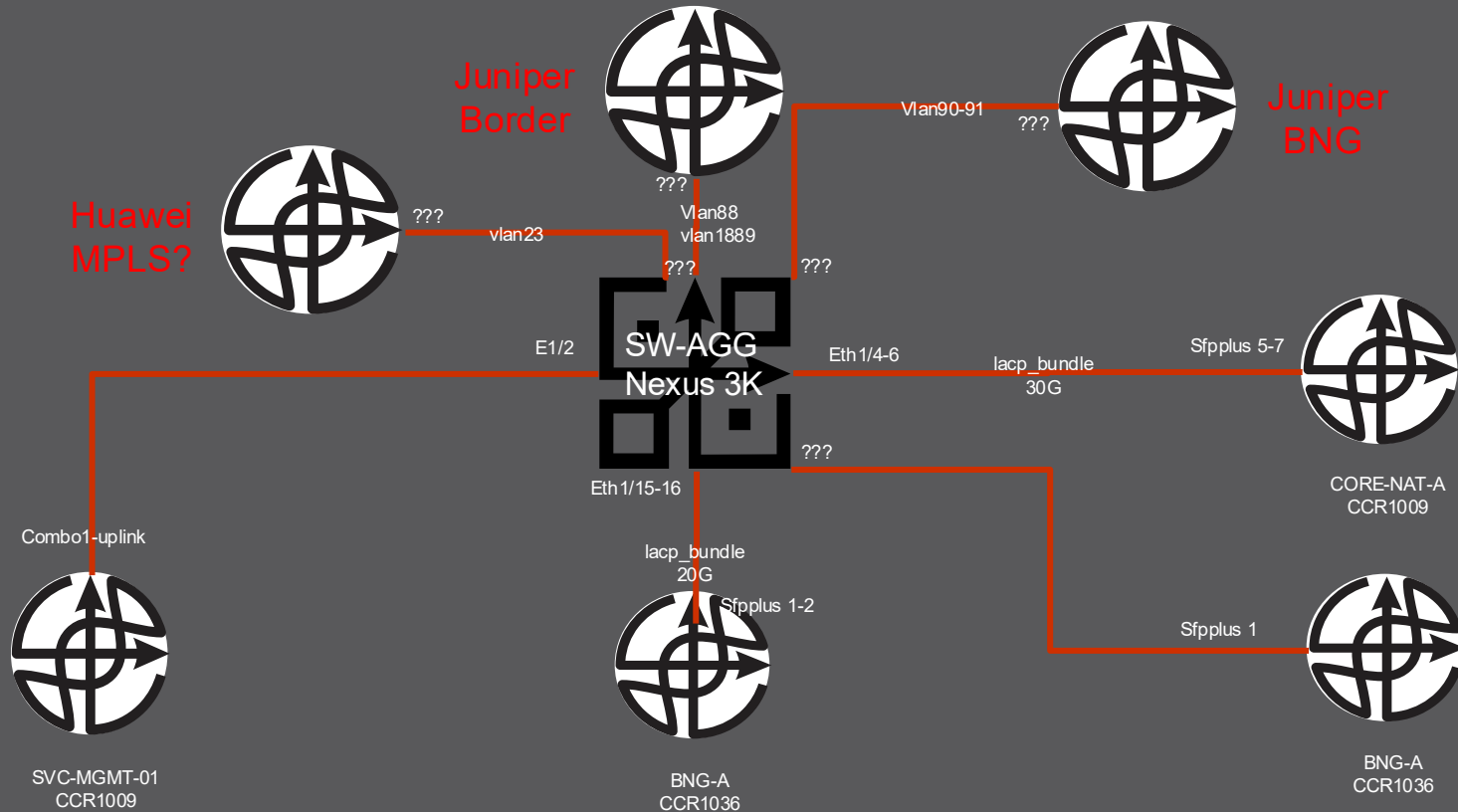
Last Bits!



CORE-NAT-B
CCR1036

- Junipers are working Hard
 - 2 Vlans Per (gateway and BNG)
 - Based on ARP
 - Same physical uplink
- Different NAT Subnet for Second MX240 VLAN

Final Diagram



Conclusions

- This is not exhaustive
 - I could have gone further with the ARP data
 - But I only have 25 Minutes
- I know some of your hardware
 - Vendors
 - Version (Vulnerabilities)
- I know your IP Addressing
 - NAT Subnets
 - CGNAT Box IPs (Targets for DDoS)
 - P2P

Conclusions

- I know what is in your office subnet
 - Servers
 - Workstations
 - Phones
 - Printers
- I know which vendors you use for CPE
- I know you have unsecured SNMP!!!!!!
 - And If I know – Anyone else can find it



Questions?

If any of this resembles your network, check your SNMP Settings