

MONITOR



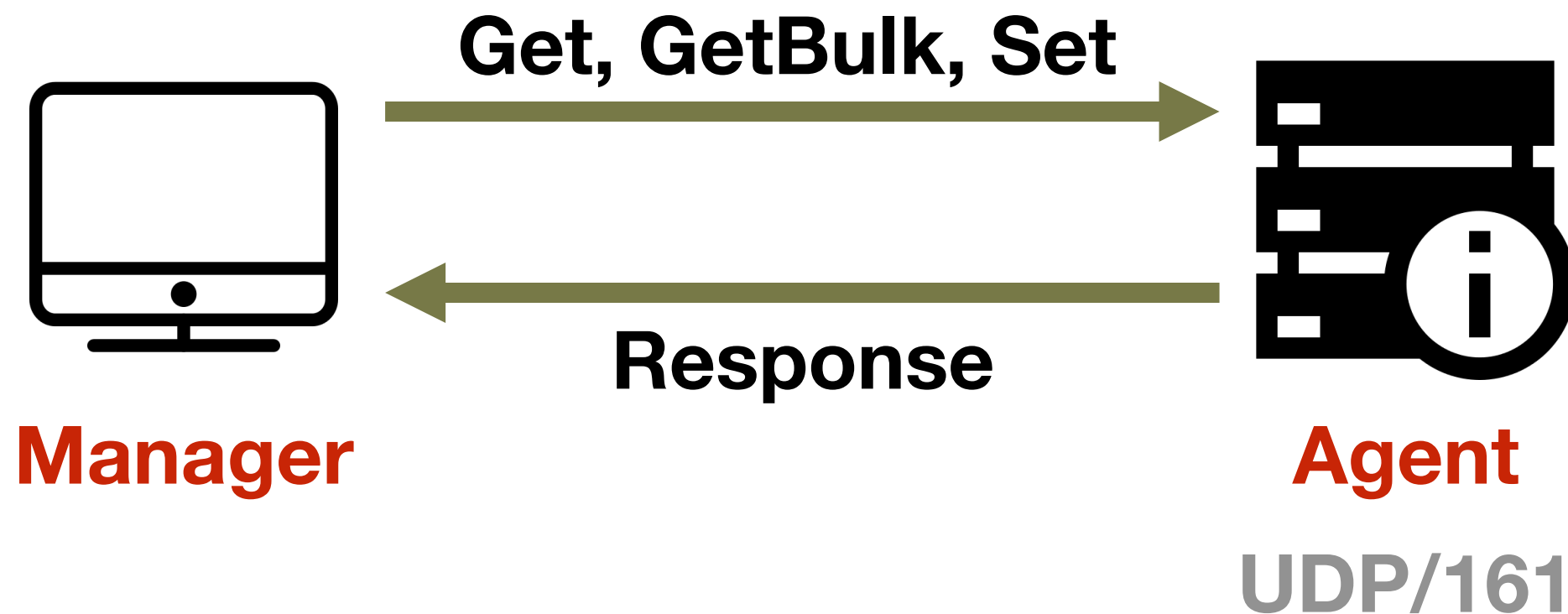
ALL THE THINGS

Agenda

1. Network Inventory
2. Locating Systems
3. Port Control
4. Network Topology
5. Health and Performance
6. Q & A



SNMP is Simple



“Net-SNMP”

- Manager (client) and Agent (server) applications
- CLI tools for testing on Unix/Linux/Windows
- MIB-2 (RFC1213) defines basic support in all Agents
 - Device OS, Model, Location, Description

```
$> snmpget -c public 172.16.20.254 sysLocation.0  
SNMPv2-MIB::sysLocation.0 = STRING: My Data Centre
```

Netdisco Inventory

Netdisco

Inventory

Reports ▾

Admin ▾

arista

Q ▾

logged in as sy0 ▾

Device	Contact	Location	System Name	Model	OS Version	Management IP	Serial	Last Discovered	
a7048lxa.ecmwf.int	DG x2313, DN x2357, OG x2455	CH:LXA	A7048LXA.ecmwf.int	DCS7048TA	4.12.5.1	192.168.254.241	JPE13355097	2014-03-07 07:13	
a7048lxb.ecmwf.int	DG x2313, DN x2357, OG x2455	CX:LXB	A7048LXB.ecmwf.int	DCS7048TA	4.12.5.1	192.168.254.242	JPE13355251	2014-03-07 07:16	
a7048xa.ecmwf.int	DG x2313, DN x2357, OG x2455	TCCB:2	A7048XA.ecmwf.int	DCS7048TA	4.11.4.2	192.168.254.209	JPE13355301	2014-03-07 07:16	
a7048xb.ecmwf.int	DG x2313, DN x2357, OG x2455	TCCA:2	A7048XB.ecmwf.int	DCS7048TA	4.11.4.2	192.168.254.210	JPE13355189	2014-03-07 07:11	
a7050xa.ecmwf.int	DG x2313, DN x2357, OG x2455	CH:C6	A7050XA.ecmwf.int	DCS7050S64	4.11.4.2	192.168.254.219	JPE12320984	2014-03-07 07:11	
a7050xb.ecmwf.int	DG x2313, DN x2357, OG x2455	TL:T2	A7050XB.ecmwf.int	DCS7050S64	4.11.4.2	192.168.254.220	JPE12311719	2014-03-07 07:07	
a75a.ecmwf.int	DG x2313, DN x2357, OG x2455	TCCA:9	A75A.ecmwf.int	DCS7508	4.11.4.2	192.168.254.243	JSH10150010	2014-03-07 07:17	
a75b.ecmwf.int	DG x2313, DN x2357, OG x2455	TCCB:3	A75B.ecmwf.int	DCS7508	4.11.4.2	192.168.254.244	JSH10150004	2014-03-07 07:14	
a75c.ecmwf.int	DG x2313, DN x2357, OG x2455	CH:C6	A75C.ecmwf.int	DCS7504	4.12.5.1	192.168.254.213	JSH12360095	2014-03-07 07:13	
a75d.ecmwf.int	DG x2313, DN x2357, OG x2455	TL:T2	A75D.ecmwf.int	DCS7504	4.12.5.1	192.168.254.214	JSH12380108	2014-03-07 07:17	
azone-a.ecmwf.int	AB X2701, TB X2378, OG x2455	TCCA:C13	azone-a.ecmwf.int	DCS7050S64	4.11.1	10.156.254.11	JPE12250883	2014-04-01 07:05	
azone-b.ecmwf.int	AB X2701, TB X2378, OG x2455	TCCB:C01	azone-b.ecmwf.int	DCS7050S64	4.11.1	10.156.254.12	JPE12181180	2014-04-01 07:05	
torcha.ecmwf.int	DG x2313, DN x2357, OG x2455	CH:S6	TORCHA.ecmwf.int	DCS7050S64	4.11.4.2	192.168.254.231	JSH11220623	2014-03-07 07:17	
torchb.ecmwf.int	DG x2313, DN x2357, OG x2455	CH:S7	TORCHB.ecmwf.int	DCS7050S64	4.11.4.2	192.168.254.232	JSH11280763	2014-03-07 07:17	
torchc.ecmwf.int	DG x2313, DN x2357, OG x2455	CH:E1	TORCHC.ecmwf.int	DCS7050S64	4.11.4.2	192.168.254.222	JPE12332478	2014-03-07 07:17	
torchd.ecmwf.int	DG x2313, DN x2357, OG x2455	CH:E2	TORCHD.ecmwf.int	DCS7050S64	4.11.4.2	192.168.254.223	JPE12331802	2014-03-07 07:12	

Netdisco Device Ports

Netdisco							
Inventory		Reports ▾	Admin ▾	sxopb.ecmwf.int		Q ▾	Logged in as sy0 ▾
Details	Ports	Modules	Neighbors	Addresses	sxopb.ecmwf.int		
	Port	Last Change	Name	Speed	MTU	Native VLAN	Status
^	GigabitEthernet1/1	2013-09-17 13:50:33	castor ActivIdentity Master	1.0 Gbps	1500	20	Up / Up
✖	GigabitEthernet1/2	2013-09-17 13:49:51	emc3-proc	0	1500	20	Down / Down
^	GigabitEthernet1/3	2013-11-15 11:16:48	web15	1.0 Gbps	1500	20	Up / Up
^	GigabitEthernet1/4	2013-12-19 14:33:22	web16	1.0 Gbps	1500	20	Up / Up
^	GigabitEthernet1/5	2013-09-17 13:50:33	dozer	1.0 Gbps	1500	20	Up / Up
^	GigabitEthernet1/6	2014-03-24 21:39:50	web17	1.0 Gbps	1500	20	Up / Up
^	GigabitEthernet1/7	2013-09-17 13:50:33	ethernet1/7	1.0 Gbps	1500	20	Up / Up
^	GigabitEthernet1/8	2014-02-06 15:11:31	web19	1.0 Gbps	1500	20	Up / Up
^	GigabitEthernet1/9	2013-12-03 11:47:18	marhaus BAc-33	1.0 Gbps	1500	20	Up / Up
✖	GigabitEthernet1/10	2013-09-17 13:49:51	ethernet1/10	0	1500	20	Down / Down
↓	GigabitEthernet1/11	2013-09-17 13:49:51	Yoda C1-11	0	1500	20	Up / Down
^	GigabitEthernet1/12	2013-09-17 13:50:33	C2BMSU/S 9Bc-11	1.0 Gbps	1500	20	Up / Up

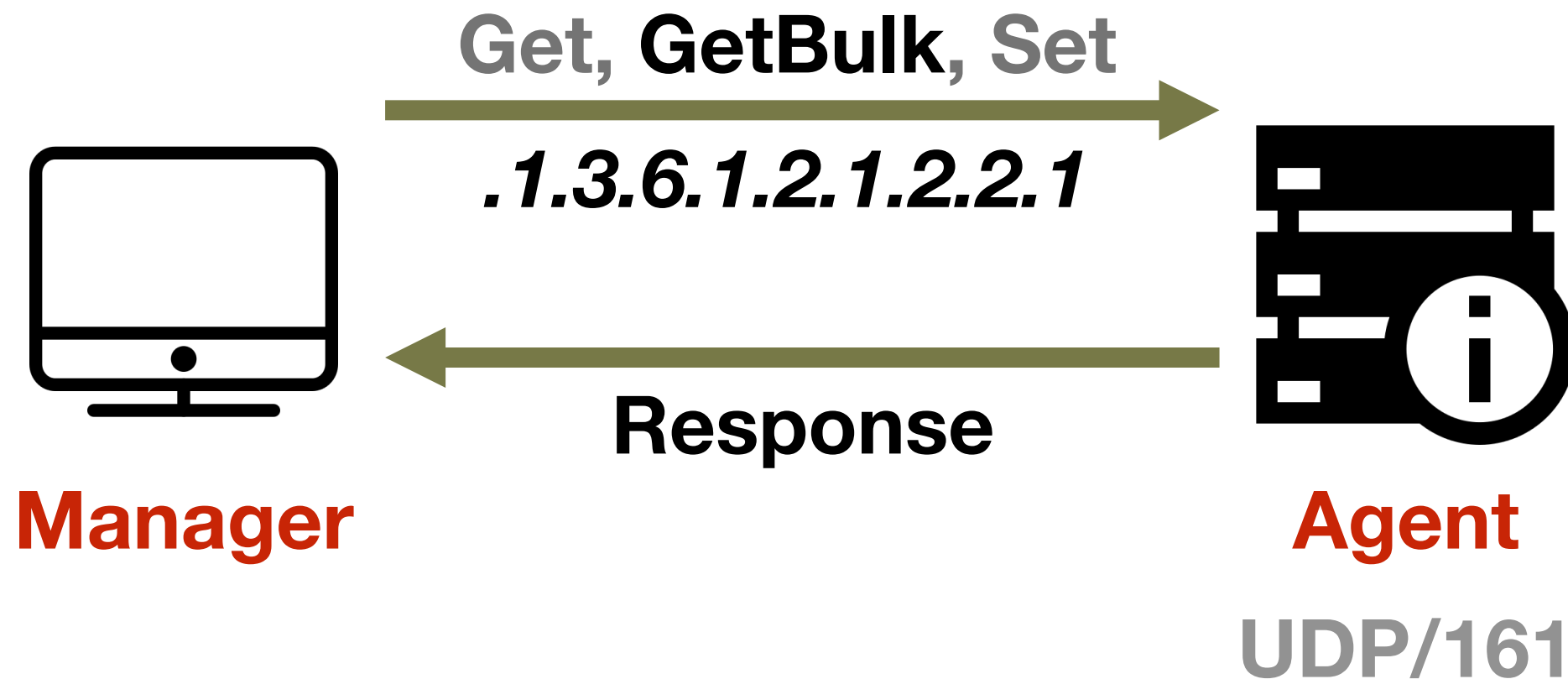
SNMP Tables

ifTable (Interfaces Table)

OID ➡ **.1.3.6.1.2.1.2.2.1.2.3**

ifIndex	ifDescr(2)	ifSpeed(5)	ifOperStatus(8)	ifInOctets(10)	ifInErrors(14)
1	ATM0/0/0	1024000	up	0	0
2	FastEthernet0/0	1000000000	up	1762445913	9
3	FastEthernet0/1	1000000000	down	84230759	0
4	Dialer1	1024000	up	2592322451	0

SNMP GetBulk for Tables



Netdisco Half Duplex Ports Report

Ports in Half Duplex Mode



Device	Port	Description	Duplex
a7048lxb.ecmwf.int	Management1	A7048LXB-Ma1	Half
etsc.ecmwf.int	FastEthernet0/0	to hpn	Half
iccb-mon.ecmwf.int	GigabitEthernet2/1/1	ethernet2/1/1	Half
icf0-voip.ecmwf.int	GigabitEthernet3/1/25	Genserv-Mon	Half

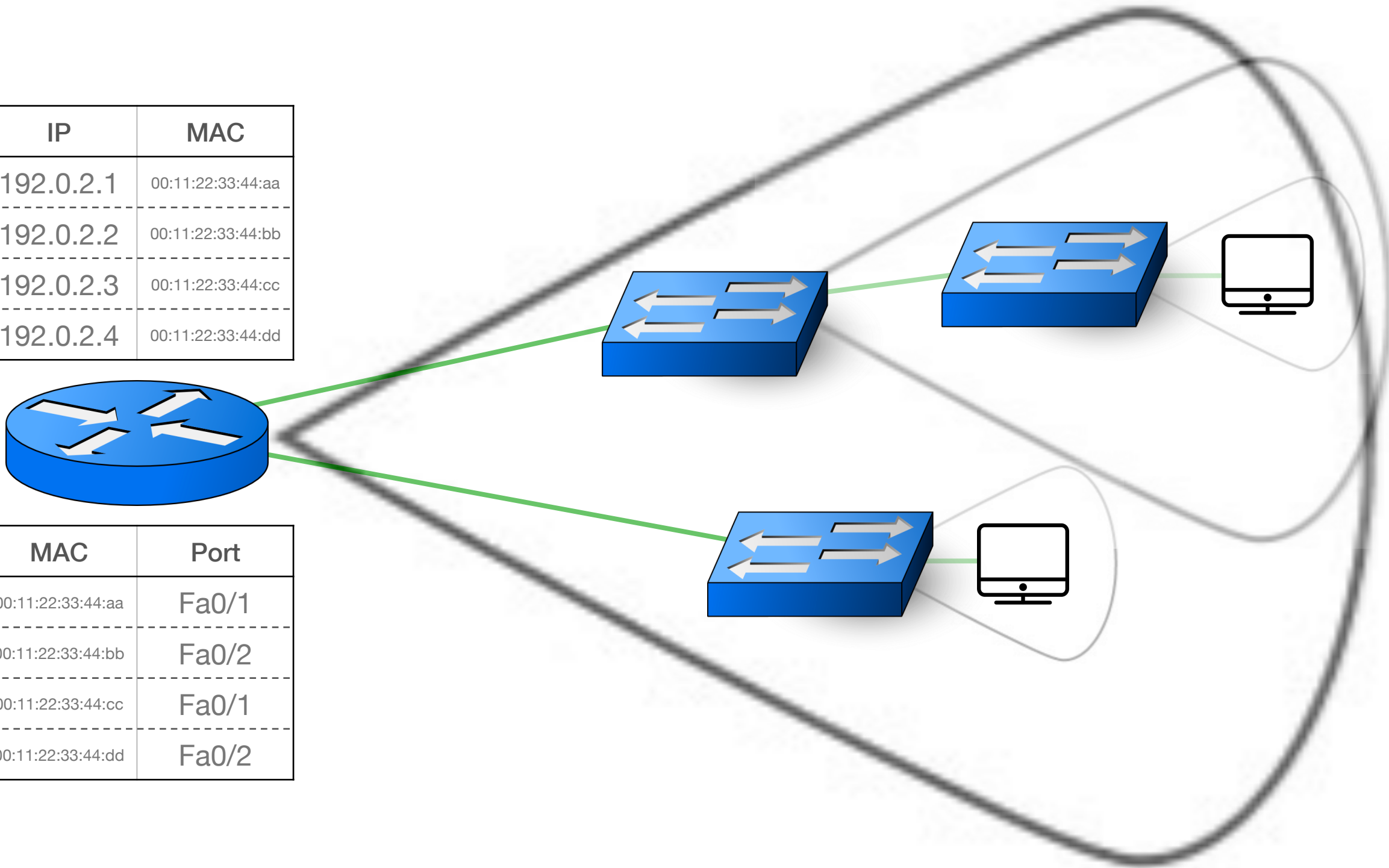


Locating Systems On Your Network

Forwarding Tables

IP	MAC
192.0.2.1	00:11:22:33:44:aa
192.0.2.2	00:11:22:33:44:bb
192.0.2.3	00:11:22:33:44:cc
192.0.2.4	00:11:22:33:44:dd

MAC	Port
00:11:22:33:44:aa	Fa0/1
00:11:22:33:44:bb	Fa0/2
00:11:22:33:44:cc	Fa0/1
00:11:22:33:44:dd	Fa0/2



Netdisco Node Search

Netdisco

Inventory

Reports ▾

Admin ▾

cammag*

Q ▾

Logged in as  sy0 ▾

Device

Node

VLAN

Port

MAC	Vendor	Match	Device or Node	First Seen	Last Seen
00:50:56:00:03:2C	VMware, Inc.	IP → MAC	136.156.168.59 (cammag-vm)	2014-01-27 12:20	2014-03-07 09:23
		Switch Port	136.156.168.252 - GigabitEthernet1/1/15 (icf3-mon.ecmwf.int - ethernet1/1/15)	2014-01-27 11:50	2014-04-01 14:50
6C:F0:49:25:EE:31	GIGA-BYTE TECHNOLOGY CO.,LTD.	IP → MAC	136.156.168.58 (cammag)	2014-01-27 10:04	2014-03-07 09:23
		Switch Port	136.156.168.252 - GigabitEthernet1/1/15 (icf3-mon.ecmwf.int - ethernet1/1/15)	2014-01-23 15:51	2014-04-01 14:50

Netdisco Subnet Utilization Report

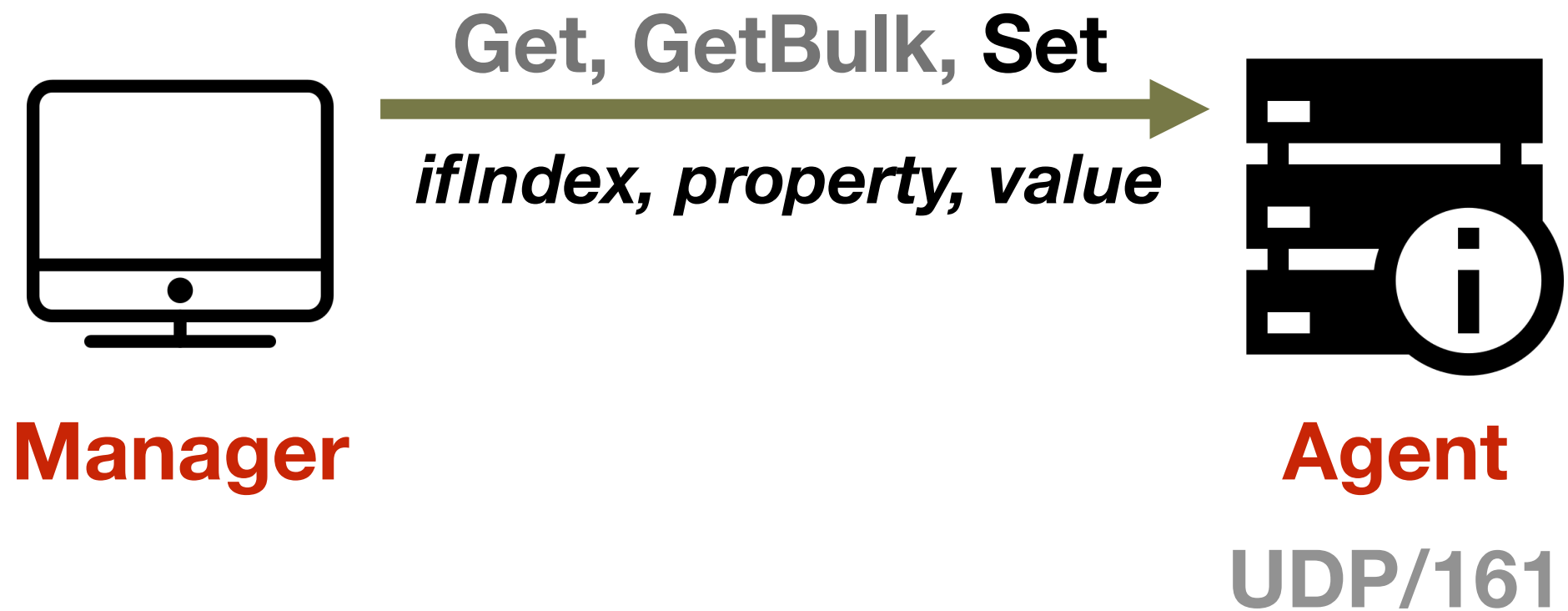
Subnet Utilization

Subnet	Size	Number of Active Nodes	Percent Utilization
193.61.196.0/26	64	6	9
193.61.196.128/27	32	5	16
193.61.196.32/27	32	6	19
193.61.196.96/27	32	6	19



SNMP Set

SNMP Set



Netdisco Port Control

Netdisco Inventory Reports Admin icf3-mon.ecmwf.int Q logged in as sy0						
Details Ports Modules Neighbors Addresses icf3-mon.ecmwf.int 						
	Port	Traffic	Name	Native VLAN	VLAN Membership	Connected Devices
	GigabitEthernet1/1/15 Click to Disable		Oliver's Workstation	168	88, 168	00:50:56:00:03:2C cammag-vm.ecmwf.int (136.156.168.59) 6C:F0:49:25:EE:31 cammag.ecmwf.int (136.156.168.58)

- Please provide a reason for changing the Port Configuration

Remote Exploit Possible

Nessus scan 2014-02-14 22:45 highlighted a problem

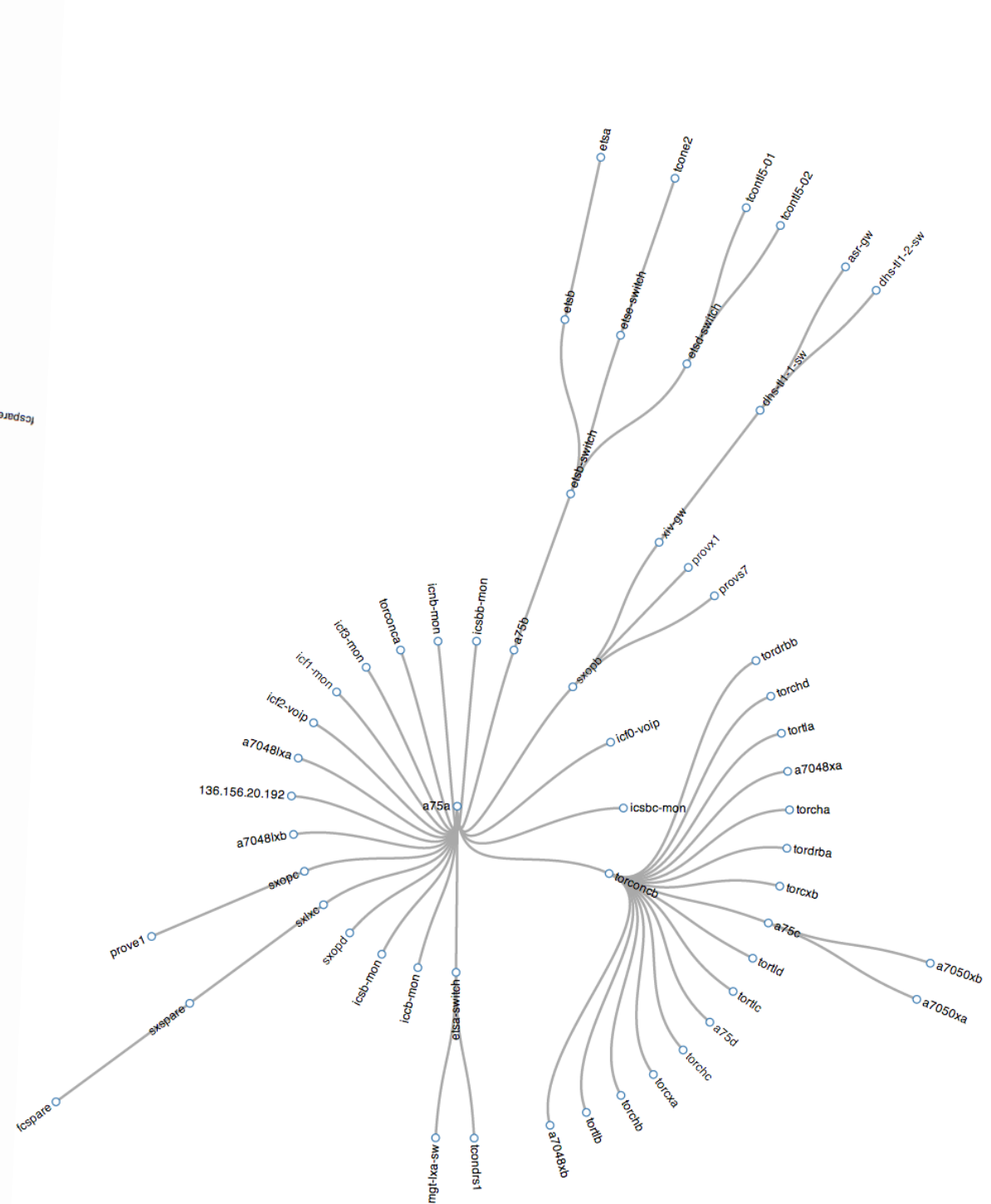
Cancel Continue

Network Topology



Neighbour Protocols

- LLDP - Link Layer Discovery Protocol (CDP, FDP)
- Periodic announcement of device + port + capabilities
- Enable this everywhere except your border/edge ports
- Good for troubleshooting in many situations
- SNMP: just another port-based table (lldpRemTable)

[illegible]

More Reports From SNMP

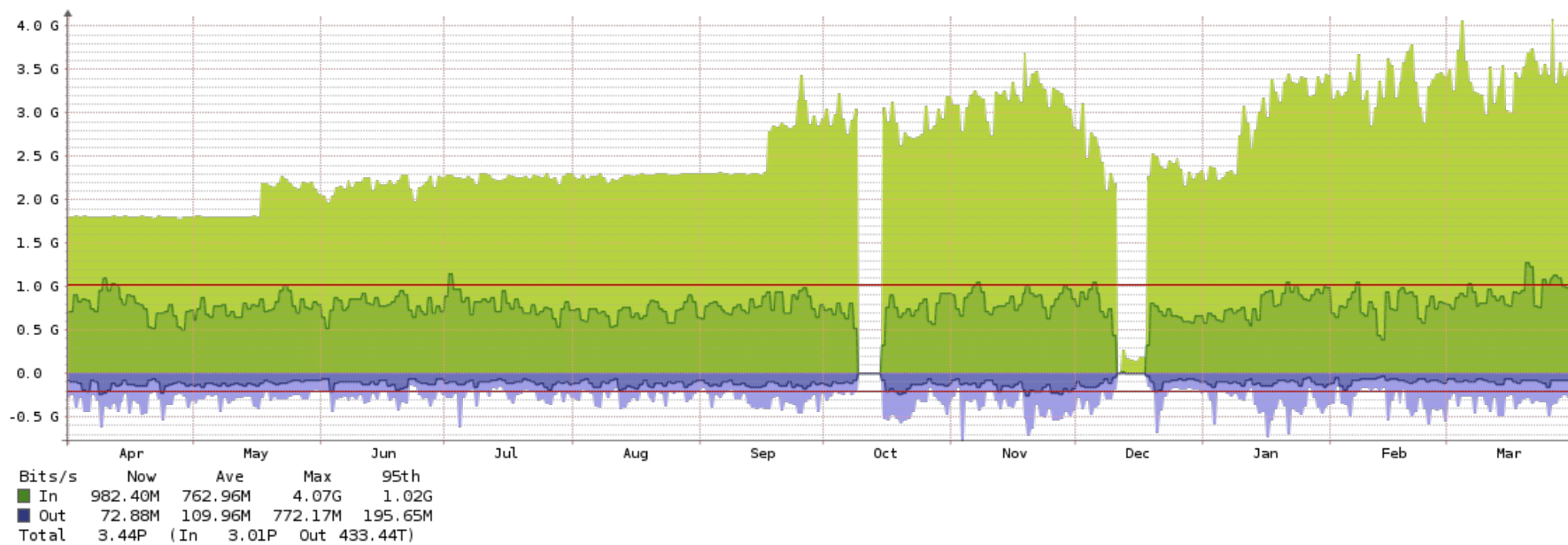
- Inventory by Location, Model, OS...
- PoE Status (ports/mW available/used)
- Ports with multiple Nodes
- Nodes with multiple IPs
- Duplex mismatches between devices
- IP Inventory (next available IP)
- VLAN Inventory
- Access Point Channel/Client/SSID Inventory



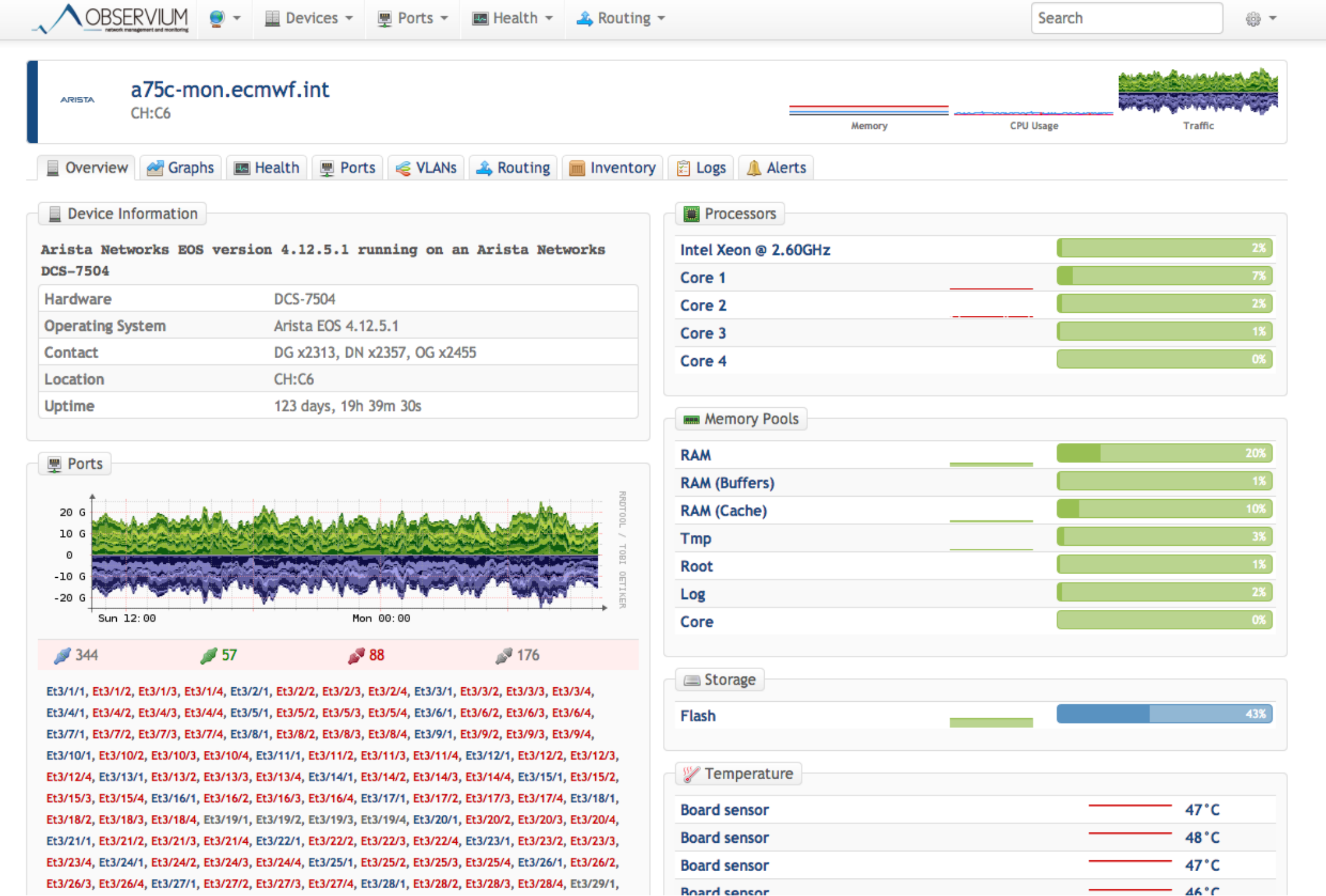
**Health and
Performance**

Observium

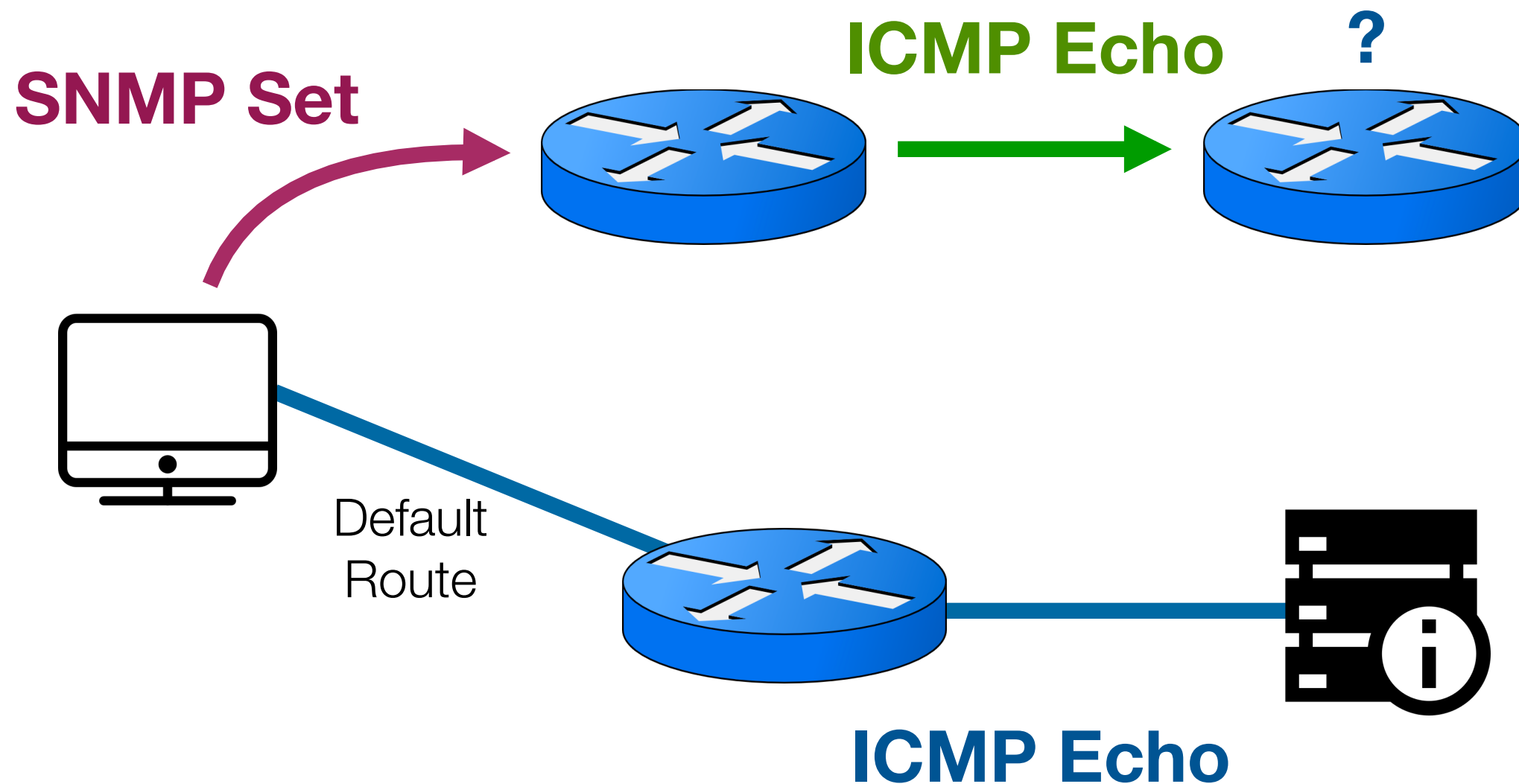
- Auto-discovering
- Traffic, Errors, CPU Load, Temperature, etc
- Simple to use and manage



Observium



DISMAN-PING-MIB (Distributed Management)



Monitor reachability of next-hops otherwise not visible from SmokePing server (e.g. due to routing).

Review

1. Network Inventory
2. Locating Systems
3. Port Control
4. Network Topology
5. Health and Performance
6. Q & A

Q & A

Cavemen - [`http://www.flickr.com/photos/yaketyyak/`](http://www.flickr.com/photos/yaketyyak/)

Computer Stencil - [`https://www.iconfinder.com/iconsets/streamline-icon-set-free-pack`](https://www.iconfinder.com/iconsets/streamline-icon-set-free-pack)

Server Stencil - [`https://www.iconfinder.com/iconsets/picol-vector`](https://www.iconfinder.com/iconsets/picol-vector)

Padlock - [`http://www.flickr.com/photos/carbonnyc/`](http://www.flickr.com/photos/carbonnyc/)

Supreme Being - [`https://www.flickr.com/photos/waitingfortheword/`](https://www.flickr.com/photos/waitingfortheword/)

Treasure Map - [`https://www.flickr.com/photos/angelic0devil6/`](https://www.flickr.com/photos/angelic0devil6/)

Houses - [`https://www.flickr.com/photos/zouny/`](https://www.flickr.com/photos/zouny/)

Orange Car - [`https://www.flickr.com/photos/aloha75/`](https://www.flickr.com/photos/aloha75/)

Useful SNMP Resources

- Cisco Object Navigator
<http://tools.cisco.com/Support/SNMP/do/BrowseOID.do>
- Net-SNMP
<http://www.net-snmp.org/>
- Netdisco
<https://metacpan.org/pod/App::Netdisco>
- SNMP::Info
<https://metacpan.org/pod/SNMP::Info>
- Observium
<http://www.observium.org/>
- SmokePing
<http://oss.oetiker.ch/smokeping/>

Bonus Material



**SNMP
Security**

SNMP Security

- v1 and v2c use **community** shared key (“public”)
- NB this is *not* a shared secret!
- v3 adds users, authentication, encryption
- All devices usually permit read-only v2c with “public”
- Hassle to configure v3, but worth doing once