Cartographer
Mapping the Duke Network

Sean Dilda

Duke University

Why do we need this?

- Network changes faster than diagrams

- Troubleshooting network problems is hard!
  - What port is this computer on?
  - What VLAN?
  - What firewalls does this go through?
  - Who is using this IP?

What does it do?

- Logs into every switch/router every three hours
- Builds internal map of network

Lookup IP / Hostname

IP Info

IP	152.3.182.3
Internal DNS Name	web.phy.duke.edu
External DNS Name	web.phy.duke.edu
Subnet	152.3.182.0/25 (Show in IPAM)
Subnet Name	(none)
VRF	physics
VLAN	600

IP Type	DHCP Reserved
All Names in IPAM	news.phy.duke.edu, web.phy.duke.edu, webdev.phy.duke.edu, www.phy.duke.edu
IPAM MAC Address	00:1A:4A:20:DA:D4

View in IPAM

MAC Addresses (ARP Table)

MAC Address	Seen By	Interface	Last ARP	
00:1A:4A:20:DA:D4 (Qumranet)	physics-024mr-dist-1	Vlan600	Today (Apr 17, 2017 @ 12:53 AM)	Clear ARP Entry

Show Historic (1)

Switch Ports

Switch Name	Interface	VLAN	Speed	Last Seen	
physics-004sr-dist-1	TenGigabitEthernet1/6	600	10 G	Today (Apr 17, 2017 @ 02:15 AM)	Block 00:1A:4A:20:DA:D4

Show Historic (1)

Lookup MAC

MAC Address: 00:1A:4A:20:DA:D4

MAC Vendor	Qumranet Inc. (Qumranet)
Splunk	DHCP Logs
	Wireless Logs

Dukereg Info

IPs
10.136.84.52	DHCP_FREE	2017-03-17 09:10 EDT - 2017-03-17 09:40 EDT
152.3.182.3	DHCP_RESERVED	

View in IPAM

IPs

IP	Seen By	Interface	VRF	Last ARP
152.3.182.3	physics-024mr-dist-1	Vlan600	physics	Today (Apr 20, 2017 @ 01:06 AM)

Show Historic (1)

Switch Ports

Switch Name	Interface	VLAN	Speed	Last Seen	
physics-004sr-dist-1	TenGigabitEthernet1/6	600	10 G	Today (Apr 20, 2017 @ 02:15 AM)	Block 00:1A:4A:20:DA:D4

Show Historic (2)

Switch/Router Interfaces

Interface Info

Device	physics-004sr-dist-1
Interface	TenGigabitEthernet1/6
Description	
Status	Up (connected)
Speed	10 G
Full Duplex	Yes
MTU	1500
MAC Address	6C:41:6A:BA:CD:85
Type	Switchport
Mode	Trunk

VLAN				
	700	152.3.183.0/24	physics	Physics 2 (152.3.183.0/24)
	100	10.248.83.0/24	voip	Physics VoIP (10.248.83.0/24)
	200	10.140.3.128/25	management	Physics NetMgmt (10.140.3.128/25)
		10.140.3.128/25	default	Physics NetMgmt (10.140.3.128/25)
	300	10.148.182.0/24	private	Physics Private (10.148.182.0/24)

Connected MAC Addresses

8 MAC Addresses
Hide

MAC	VLAN	Last Seen
00:1A:4A:16:01:59 (Qumranet)	600	2017-04-17 02:15 EDT
00:1A:4A:20:DA:97 (Qumranet)	701	2017-04-17 02:15 EDT
00:1A:4A:20:DA:CD (Qumranet)	600	2017-04-17 02:15 EDT
00:1A:4A:20:DA:D3 (Qumranet)	600	2017-04-17 02:15 EDT

Lookup Switch/Router

Device Info

Name	physics-024mr-dist-1
Type	IOS
Function	Switch-Router
Software Version	03.09.01.E
Hardware	WS-C4500X-16
Serial Number	JAE17220AN7
Management IP	10.140.3.129
LAN	LAN 12 (Graph)
Last Queried	2017-04-17 14:23 EDT

Building	Physics Building
Room/Location	024
Building Type	Academic Administrative
Address	120 Science Dr
	Durham, NC 27708
Lat/Long	36.0032861493877 / -78.942528228977
Floor Plan	🖼

[Edit Device] [Run Update] [Delete Device]

IPs

47 IPs
Show

Local Subnets

47 Subnets
Hide

CIDR	Name	VRF	VLAN
10.136.80.0/21	Physics Compute Nodes (10.136.80.0/21)	physics	701
10.136.97.0/24	Physics TUNL (10.136.97.0/24)	physics	301

Switch/Router continued

Interfaces

87 Interfacess
Hide

FastEthernet1	10 M	Down			
Port-channel1	20 G	Up	1, 100, 101,...		
Port-channel10	20 G	Up	100, 200, 30...	physics-004-sr-2	physics-004sr-dist-1 (Port-channel1)
Port-channel12	20 G	Up	101, 200, 30...		fel-106-a-1-1 (Port-channel12)
Port-channel13	20 G	Up	100, 200, 30...		physics-024mr-a-5 (Port-channel13)
Port-channel14	10 G	Up	102, 200, 30...	Physic-Tunl-rm311-a-1	physics-tunl-311-a-1 (Port-channel14)
Port-channel2	20 G	Up	1, 100, 101,...		
Port-channel5	20 G	Up	100, 200, 30...	physics-024mr-a-1	physics-024mr-a-1-1 (Port-channel5)
Port-channel6	20 G	Up	100, 200, 30...	physics-024mr-a-2	physics-024mr-a-2-1 (Port-channel1)
Port-channel7	20 G	Up	100, 200, 30...	physics-067mr-a-1	physics-067mr-a-1-1 (Port-channel7)
Port-channel8	20 G	Up	100, 200, 30...	physics-067mr-a-2	physics-067mr-a-2-1 (Port-channel8)
Port-channel9	20 G	Up	100, 200, 30...	physics-004-sr-1	physics-004-sr-1 (Port-channel1)
TenGigabitEthernet1/1/1	10 G	Up	1, 100, 101,...		
TenGigabitEthernet1/1/10	10 G	Up	100, 200, 30...	physics-004-sr-2	physics-004sr-dist-1 (TenGigabitEthernet1/16)
TenGigabitEthernet1/1/11	1 G	Up	603	physics-274j-a-1.netcom.duke.edu (g1/1/2	
TenGigabitEthernet1/1/12	10 G	Up	101, 200, 30...	fel-106-a-1-1	fel-106-a-1-1 (TenGigabitEthernet1/1/4)
TenGigabitEthernet1/1/13	10 G	Up	100, 200, 30...	physics-004-sr-2	physics-024mr-a-5 (TenGigabitEthernet0/1)
TenGigabitEthernet1/1/14	10 G	Up	102, 200, 30...	Physic-Tunl-rm311-a-1	physics-tunl-311-a-1 (TenGigabitEthernet1/1/4)
TenGigabitEthernet1/1/15	10 G	Down	1		
TenGigabitEthernet1/1/16	10 G	Down	1		

VRF Info

physics

Subnets		
CIDR	**Name**	**Router(s)**
10.136.18.128/26	Ciemas Physics	ciemas-b407b-dist-1
10.136.18.224/28	Physics Hudson	annex-059-dist-1
10.136.80.0/21	Physics Compute Nodes (10.136.80.0/21)	physics-024mr-dist-1
10.136.96.0/24	Physics FFSC (10.136.96.0/24)	frenchscience-0016-dist-1
10.136.97.0/24	Physics TUNL (10.136.97.0/24)	physics-024mr-dist-1
10.136.98.0/24	Physics FEL (10.136.98.0/24)	physics-024mr-dist-1
10.136.99.0/24	PhyVRF-BioSciDC	biosci-001-dist-1
10.144.176.0/25	French Science TUNL QuickReg (10.144.176.0/25)	frenchscience-0016-dist-1
10.148.177.0/24	Physics Openflow	physics-024mr-dist-1
10.185.16.0/26	PHYSICS-PHYSICS-BIO-SDN-01	biosci-001-dist-1
10.236.114.64/27	OIT-PHYSICS-ATCSDN-01	atc-s-2000-d-1-1
10.236.243.80/28	physics-vrf-ipe-sp	tel1-ipe, wel1-ipe

Show VLAN

VLAN 701

LAN 2 (Graph)

Subnets

CIDR	Name	Router	VRF
10.185.0.128/28	OIT-OPENFLOW-ATC-01	atc-s-2000-d-1-1	openflow

Switches

|	
atc-4500x-2116-sdn-1	TenGigabitEthernet1/2, TenGigabitEthernet1/3, TenGigabitEthernet1/4
atc-s-2000-d-1-1	Port-channel1, Port-channel2, TenGigabitEthernet1/1/5

LAN 12 (Graph)

Subnets

CIDR	Name	Router	VRF
10.136.80.0/21	Physics Compute Nodes (10.136.80.0/21)	physics-024mr-dist-1	physics

Switches

physics-004-sr-1	GigabitEthernet1/0/13, GigabitEthernet1/0/14, GigabitEthernet1/0/15, GigabitEthernet1/0/16, GigabitEthernet1/0/17, GigabitEthernet1/0/18, Gi
physics-004sr-dist-1	Port-channel5, TenGigabitEthernet1/10, TenGigabitEthernet1/11, TenGigabitEthernet1/12, TenGigabitEthernet1/13, TenGigabitEthernet1/14, Ter

Mapping Layer 2
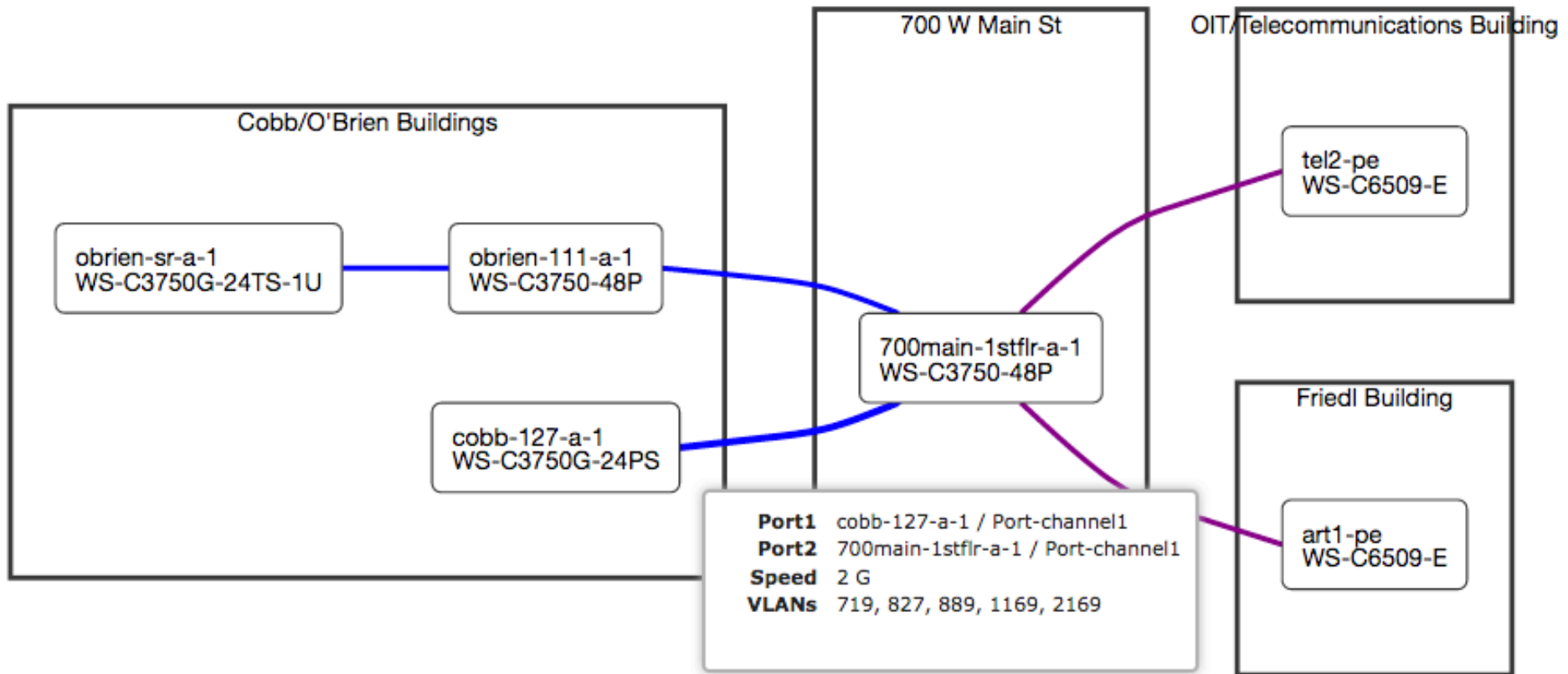
Buildings

Building ID	Name	Address	Type	Locale
8349	700 W Main St	700 W Main St		
8348	Cobb/O'Brien Buildings	610-614 W Main St		

Devices

To see a graph of how the devices interconnect, click here

Name	Function	Model	Software Version
700main-1stflr-a-1	Switch	WS-C3750-48P	12.2(55)SE10
cobb-127-a-1	Switch	WS-C3750G-24PS	12.2(55)SE10
obrien-111-a-1	Switch	WS-C3750-48P	12.2(50)SE5
obrien-sr-a-1	Switch	WS-C3750G-24TS-1U	12.2(55)SE10

Subnets

CIDR	Name	VLAN	VRFs	Buildings
10.136.50.0/23	University Development Cobb-O'Brien (10.136.50.0/23)	889	development	Cobb/O'Brien Buildings, 700 W Main St
10.140.80.0/27	700 Fuller St NetMgmt (10.140.80.0/27)	1169	management	Cobb/O'Brien Buildings, 700 W Main St
10.140.80.64/26	700 Fuller St NetMgmt (10.140.80.64/26)	1169	management	Cobb/O'Brien Buildings, 700 W Main St
10.148.30.0/27	700 Main St Private (10.148.30.0/27)	2169	private	Cobb/O'Brien Buildings, 700 W Main St
10.150.13.64/27	OIT-DCO-WESTVILLIAGE700MAIN-01	825	dco	700 W Main St
10.150.13.96/27	OIT-DCO-WESTVILLIAGEOBRIEN-01	826	dco	Cobb/O'Brien Buildings, 700 W Main St
10.150.13.128/27	OIT-DCO-WESTVILLIAGECOBB-01	827	dco	Cobb/O'Brien Buildings, 700 W Main St
10.248.6.0/24	700 Fuller VoIP (10.248.6.0/24)	719	voip	Cobb/O'Brien Buildings, 700 W Main St
10.248.73.128/25	700 Main Street VoIP	1913	voip	700 W Main St
152.3.107.0/27	West Village Athletics (152.3.107.0/27)	675	athletics	700 W Main St
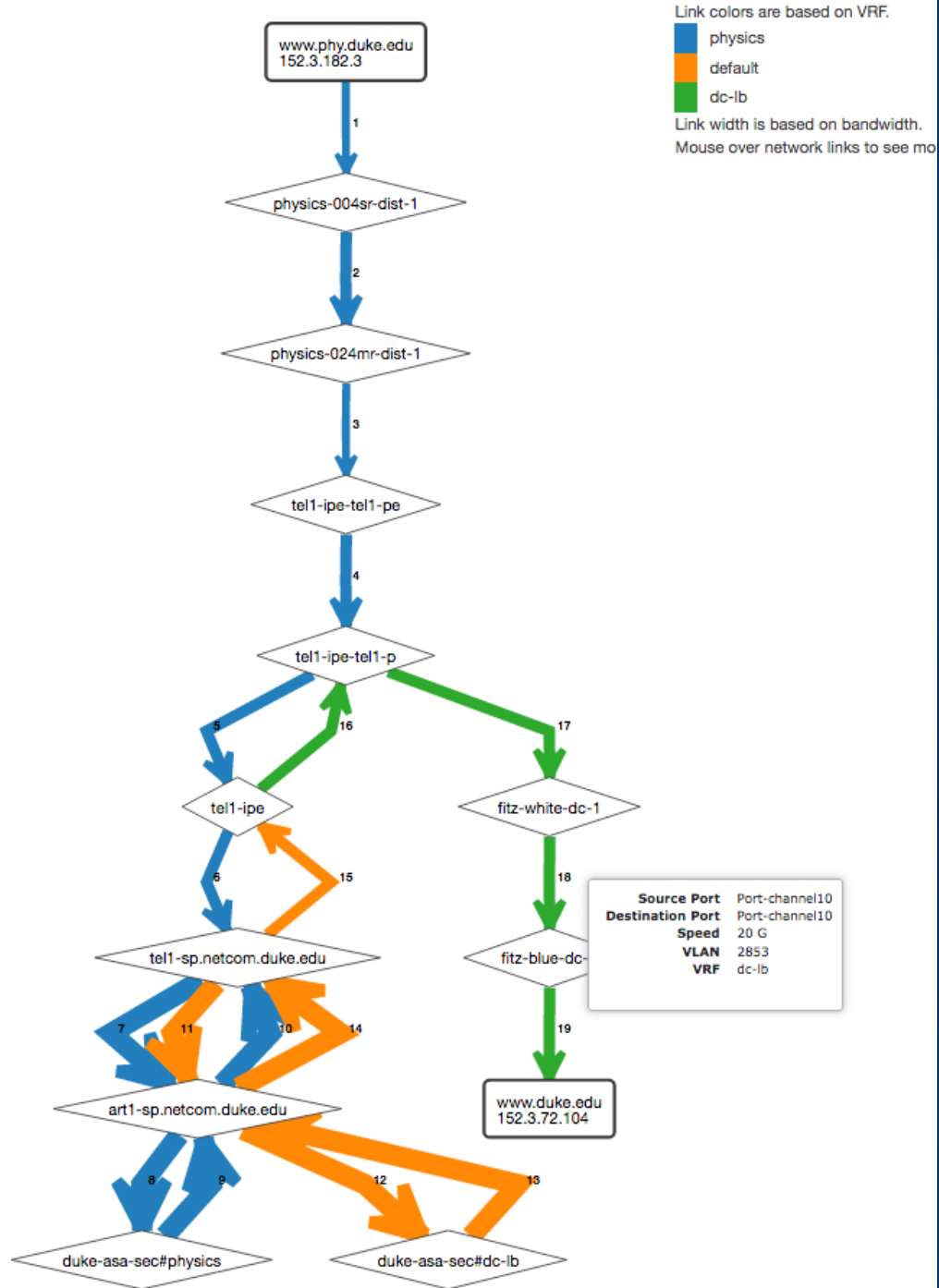
Who can use it?

- All IT staff across the university

- Anyone with access to IPAM

Modifying the Network

Port permissions based on IPAM permissions

- Change port VLAN
- Bounce wired port (great for PoE)
- Clear ARP entry
- Block from network (ITSO only)

Next Steps

- F5 Load Balancers

- Firewall Rules / Network ACLs

- IPS blacklists

Old Method

1. Troubleshoot as much as possible
2. Ask networking to provide some extra info
3. Troubleshoot some more
4. Ask networking for extra info
5. <repeat>

New Method

1. Troubleshoot
2. Get necessary info from Cartographer

Problems are solved faster with fewer man hours involved. System Administrators and Networking staff have more time to solve other problems