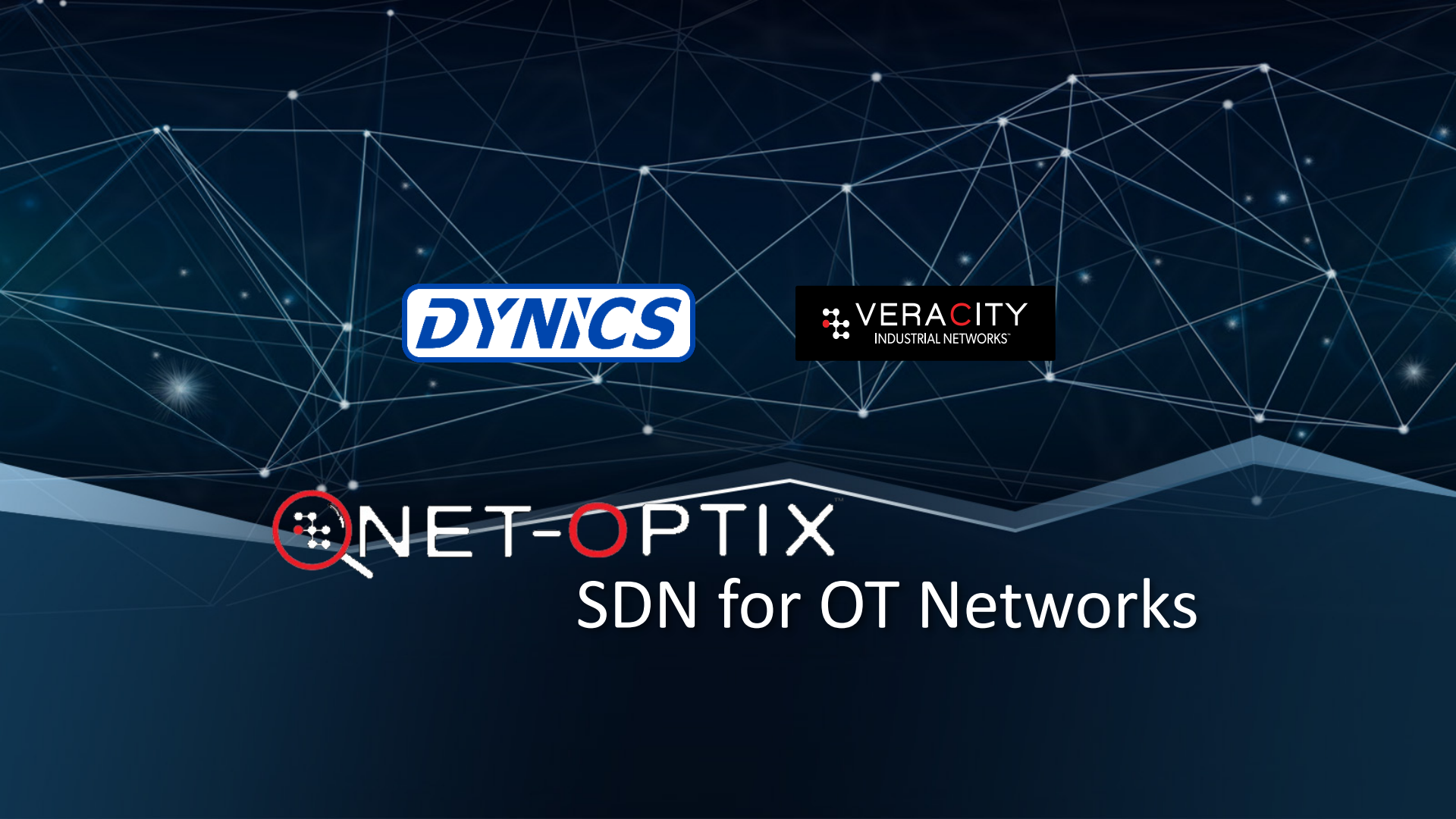

DYNICS
VERACITY
INDUSTRIAL NETWORKS
NET-OPTIX
SDN for OT Networks

Serious technology presented in a casual way

I've been doing this for a long time. I can talk all the tech that technical folks love. However, in this session I'm going to try to reach that happy medium between being overly technical and not being technical enough.

Having said that…

I am available to do a deeper technical dive or a more 30,000 foot view of the technology that I, and increasingly others, believe will disrupt and change OT networking in the near future.

What is a Software Defined Network (SDN) ?

-DEEP BREATH-

A network which decouples network control and packet forwarding functions, enabling the network control to become directly programmable and abstracted from applications and network services.

-WHEEZE-

What does that mean to normal people?

It means a centrally managed, flexible, programmable, open standards based and vendor neutral network for the OT space. It means OT or IT staff can easily manage the network, make changes as needed, and remain secure, all without having a degree in “network”

What common OT network problems are solved?

- OEM engineers waiting for customer OT or IT to configure switches and then charging for time lost due to no connectivity
- No or out-of-date switch backups for any switches in the network
- Cables plugged into the wrong ethernet ports on the switch
- Firmware issues or mismatches between f/w on switches
- Loops created in the network by poor choices in cabling
- Not having visibility into what devices are on the network and what and where they are connected
- No visibility regarding protocols are in use on the network

What common OT network problems are solved?

- No visibility into events on the network in close to real-time
- Inability to prevent unwanted device communications
- Inability to prevent unwanted protocols on the network
- Poorly updated or lost network topology drawings
- No redundancy or reliability without adding a lot of complexity
- Painful learning curve for non-network savvy OT folks
- Painful replacement of switches or edge devices (such as PLCs)
- The spread/introduction of malware or ransomware

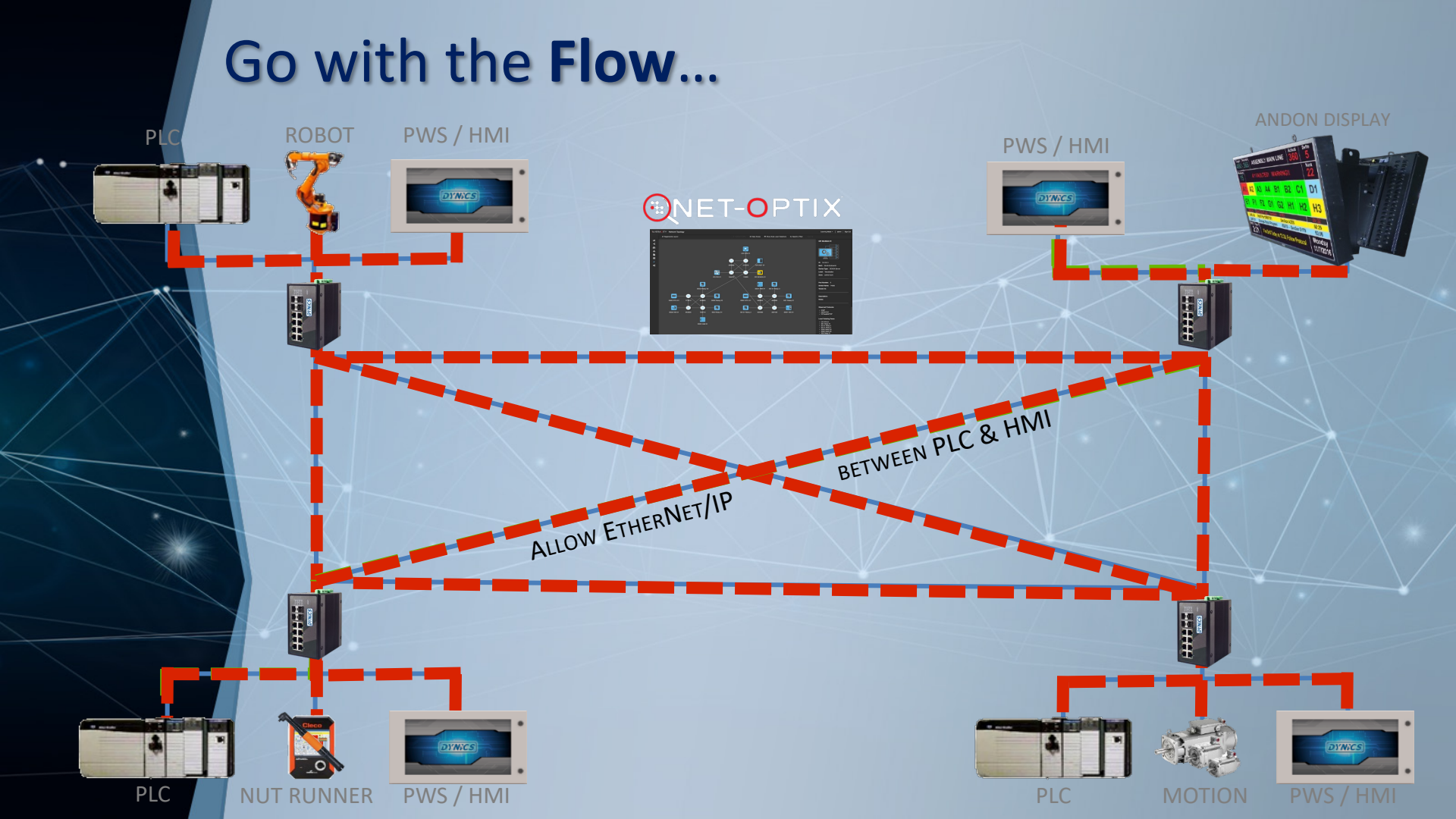
!!! FUN FACT !!!

SDN Network is IEEE 802.3 Ethernet compliant.

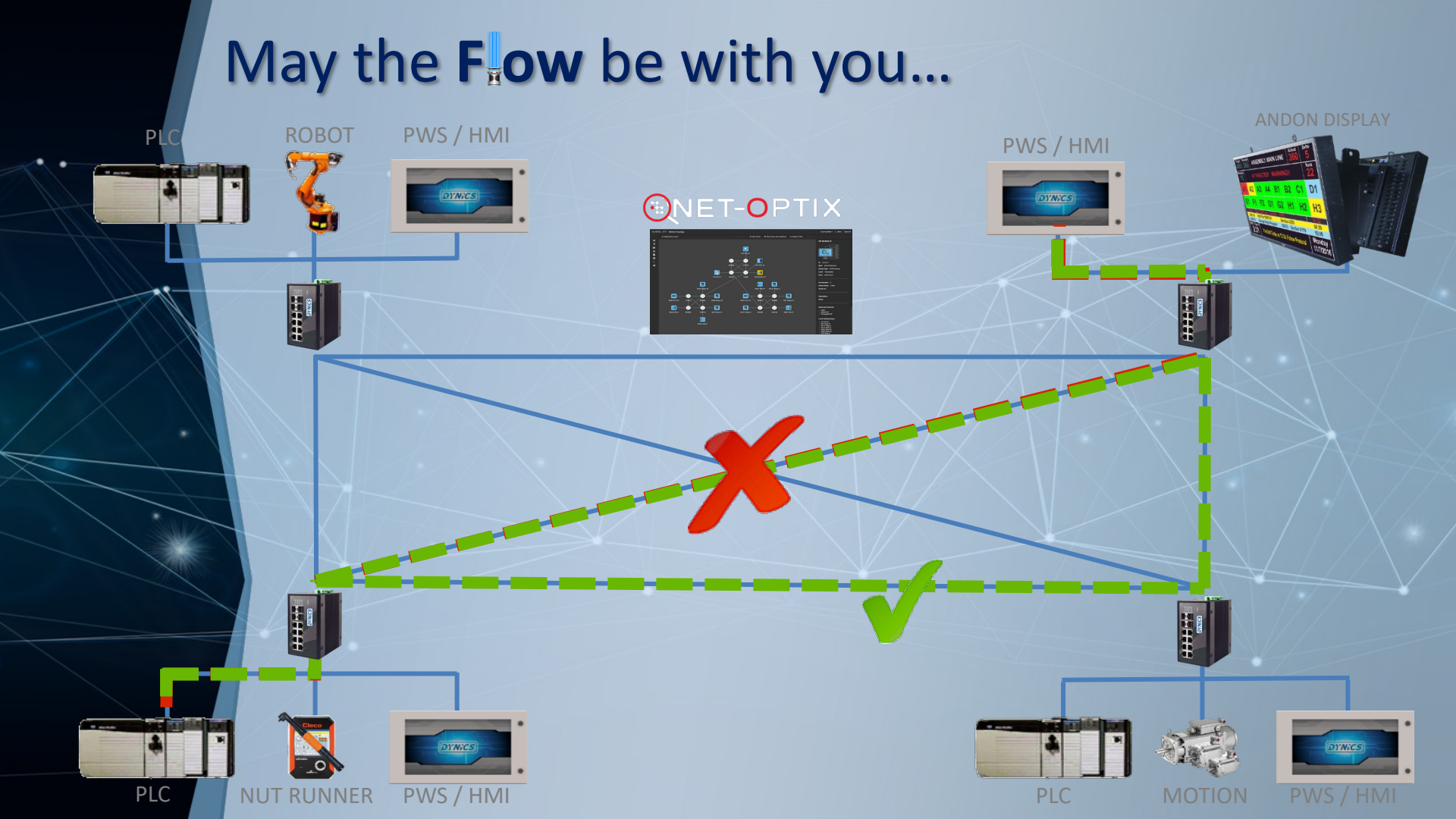
What does that mean to normal people?

It’s the same Ethernet you’re using on your networks today, runs the same applications, same data, same everything. The only difference between an SDN network and a network of managed switches is how the network is managed. Have an app you like and use, keep using it.

Go with the **Flow**…

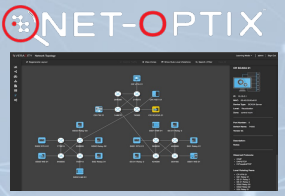


May the Flow be with you…



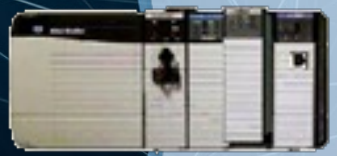
Allowed Traffic

Known



2

EtherNet/IP is an allowed flow between the PLC and the Nut Runner



PLC

1

EtherNet/IP

3

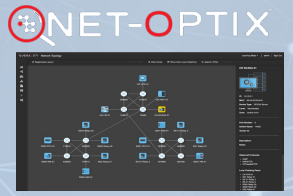
EtherNet/IP

NUT RUNNER

Known traffic is handled between the switches.
No need to ask the SDN Controller how to handle the traffic.

Allowed Traffic

Unknown or New



What do I do with Modbus TCP from the PLC to the Nut Runner?

3

Write an allow flow and pass it. The switches will remember next time.

2

1

Modbus TCP

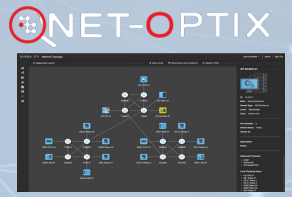
4

Modbus TCP

NUT RUNNER

Explicitly Disallowed Traffic

Explicitly Denied



Notify the SDN Controller to update the audit log and alert users.

Profinet is known to be explicitly blocked on the network.

PLC

1

Profinet

2

2

Profinet

NUT RUNNER

!!! FUN FACT !!!

VLANS, RSTP, LOOPS, Complexity are a thing of the past…

What does that mean to normal people?

There is no need to create multiple VLANs to segment the network for security. SDN micro-segments the network with point to point (device to device) flows which are exponentially more granular and secure than VLANs. You can't create a loop in an SDN network, and there is no need for topology protocols such as RSTP, PVST, Ring protocols. Cable the network however makes sense for the application/system.

!!! FUN FACT !!!

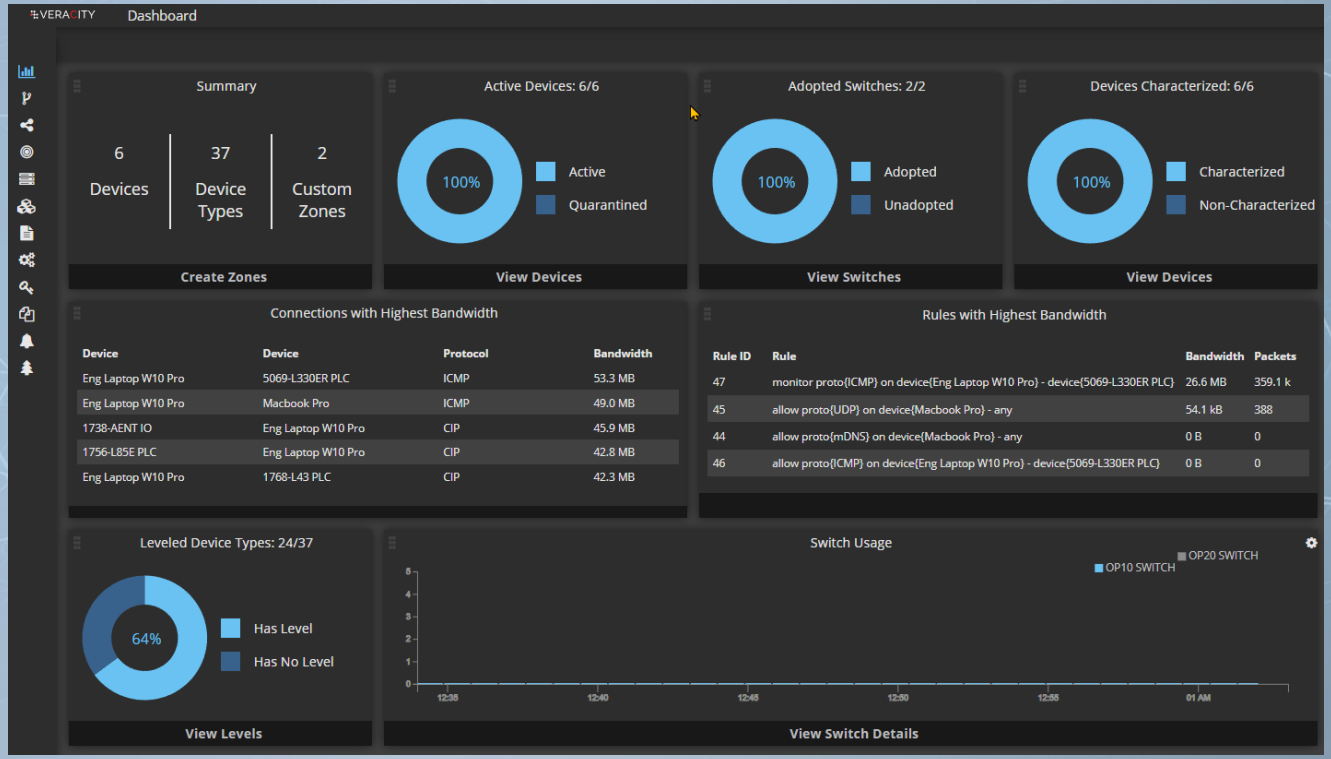
Net-Optix allows you to connect your spanky new SDN network to your existing older technology (legacy) networks.

What does that mean to normal people?

If there is a need to connect an existing network that uses RSTP and has configured VLANs, Net-Optix will automatically detect that at the point of connection to the legacy network and talk the talk, IE – understand the vlans and the spanning tree protocol. Net-Optix knows the lingo the traditional network is talking.

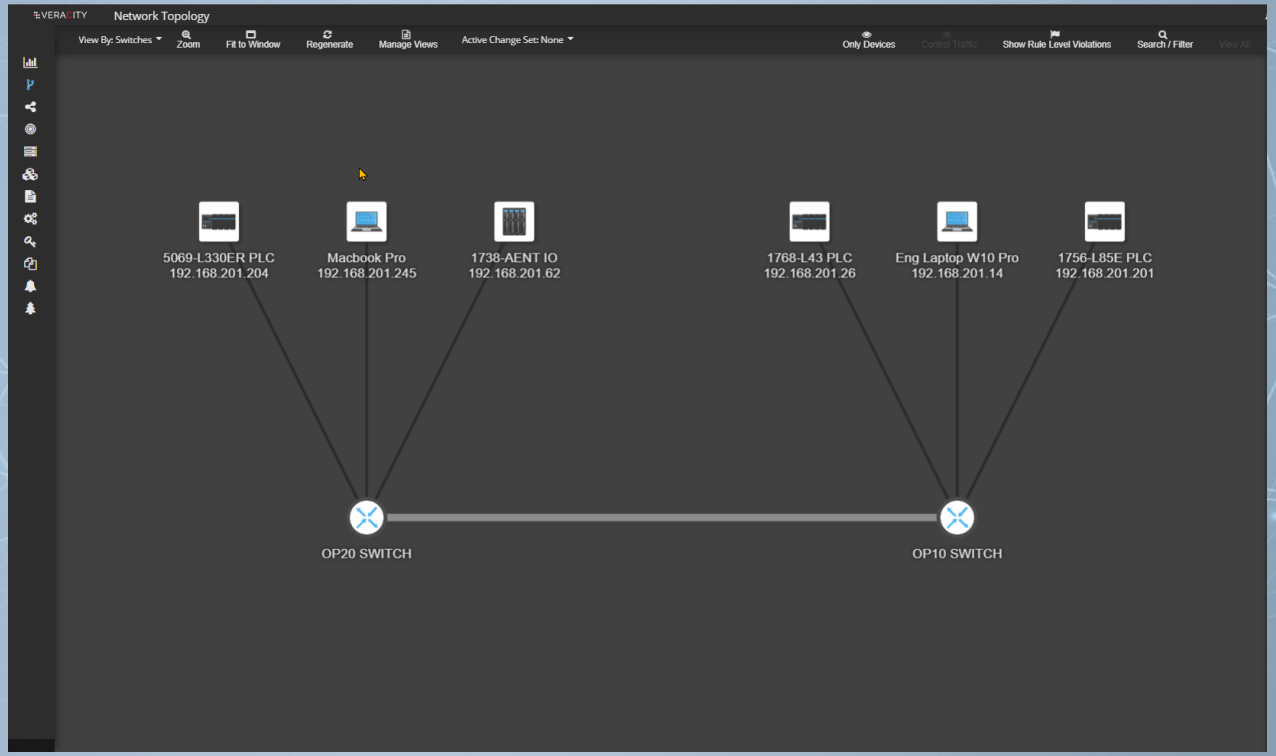
NET-OPTIX DASHBOARD

A quick look at network statistics



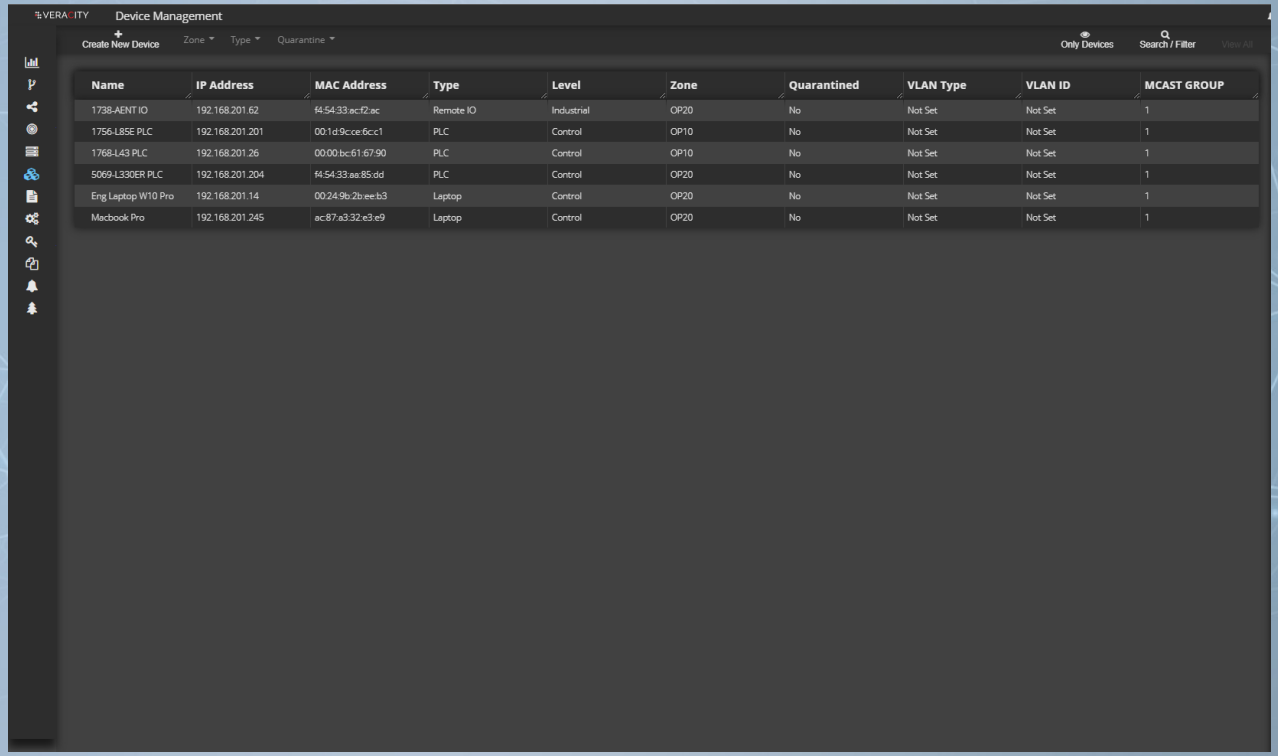
NET-OPTIX NETWORK TOPOLOGY

A view of the network connections



NET-OPTIX DEVICE MANAGEMENT (ASSETS)

A view of the devices (assets) on the network



Name	IP Address	MAC Address	Type	Level	Zone	Quarantined	VLAN Type	VLAN ID	MCAST GROUP
1738-AENT IO	192.168.201.62	f4:54:33:ac:f2:ac	Remote IO	Industrial	OP20	No	Not Set	Not Set	1
1756-L85E PLC	192.168.201.201	00:1d:9c:ce:6c:c1	PLC	Control	OP10	No	Not Set	Not Set	1
1768-L43 PLC	192.168.201.26	00:00:bc:61:67:90	PLC	Control	OP10	No	Not Set	Not Set	1
5069-L330ER PLC	192.168.201.204	f4:54:33:aa:85:dd	PLC	Control	OP20	No	Not Set	Not Set	1
Eng Laptop W10 Pro	192.168.201.14	00:24:9b:2b:ee:b3	Laptop	Control	OP20	No	Not Set	Not Set	1
Macbook Pro	192.168.201.245	ac:87:a3:32:e3:e9	Laptop	Control	OP20	No	Not Set	Not Set	1

!!! FUN FACT !!!

Net-Optix allows you enter “learning mode” where the traffic on the network is learned and rules are automatically generated.

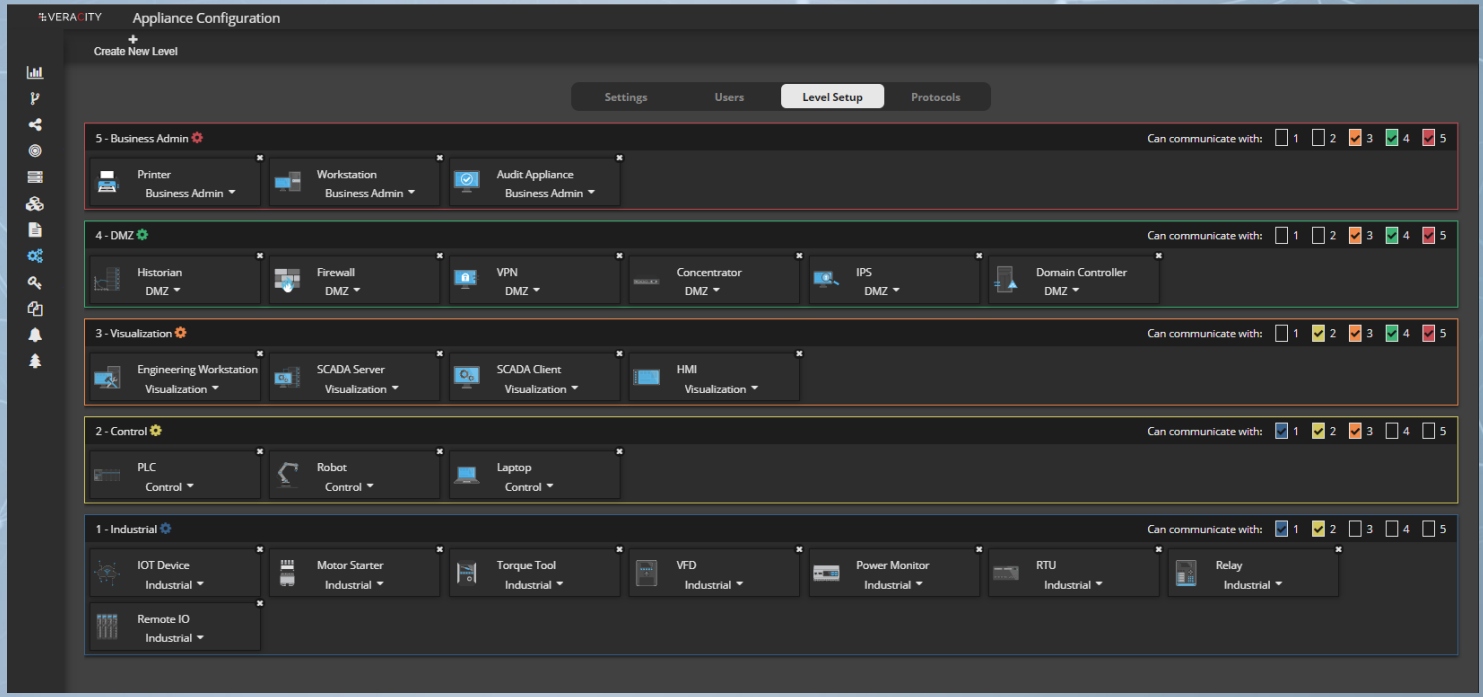
What does that mean to normal people?

When initially configuring the network, or starting the network up at an equipment builder (OEM), just put the network in learn mode and let it write flows to allow whatever traffic is needed without delaying the build and runoff process. You can even put a single switch in learning mode if needed.

NET-OPTIX LEVEL CONFIGURATION

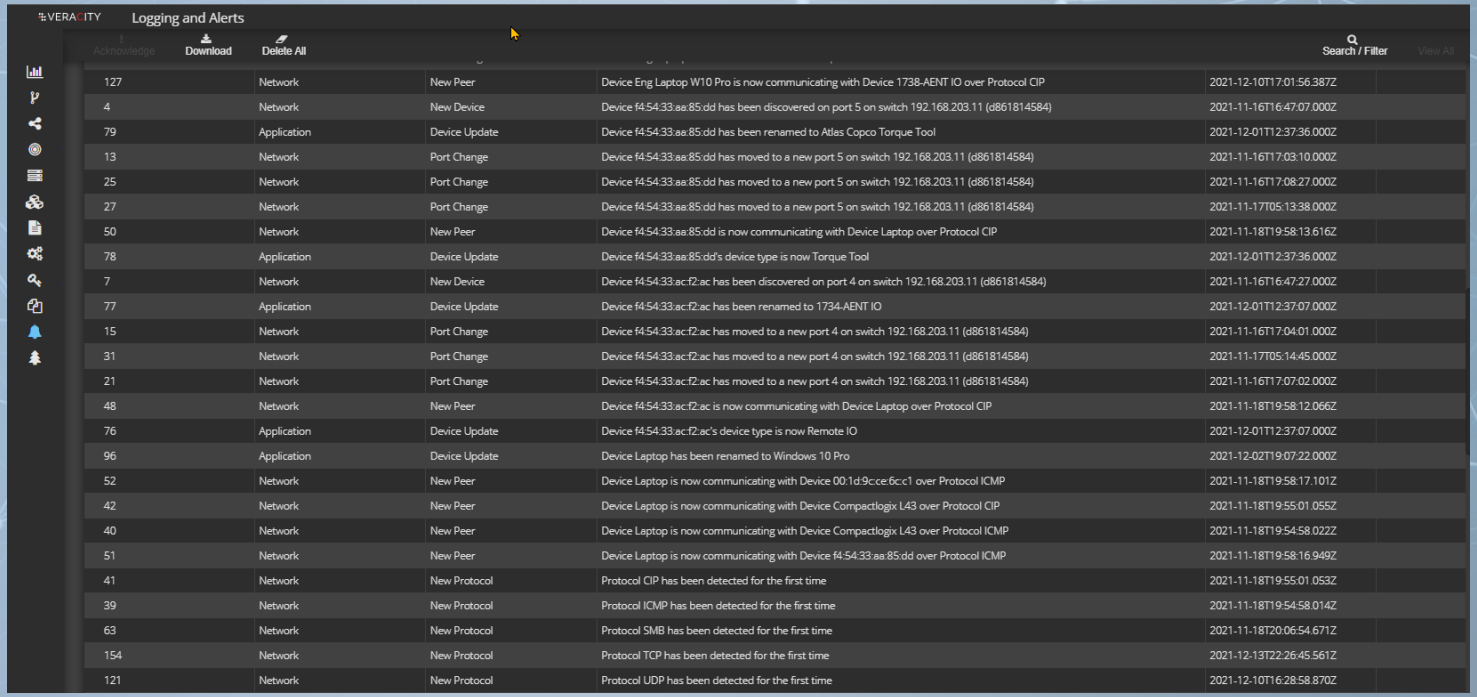
Organize the network using a level approach (pun intended)

Optionally utilize a network structure that matches or is similar to the Purdue Model



NET-OPTIX LOGGING & ALERTS

View changes to the network, by category, and time



127	Network	New Peer	Device Eng Laptop W10 Pro is now communicating with Device 1738-AENT IO over Protocol CIP	2021-12-10T17:01:56.387Z
4	Network	New Device	Device f4:54:33:aa:85:dd has been discovered on port 5 on switch 192.168.203.11 (d861814584)	2021-11-16T16:47:07.000Z
79	Application	Device Update	Device f4:54:33:aa:85:dd has been renamed to Atlas Copco Torque Tool	2021-12-01T12:37:36.000Z
13	Network	Port Change	Device f4:54:33:aa:85:dd has moved to a new port 5 on switch 192.168.203.11 (d861814584)	2021-11-16T17:03:10.000Z
25	Network	Port Change	Device f4:54:33:aa:85:dd has moved to a new port 5 on switch 192.168.203.11 (d861814584)	2021-11-16T17:08:27.000Z
27	Network	Port Change	Device f4:54:33:aa:85:dd has moved to a new port 5 on switch 192.168.203.11 (d861814584)	2021-11-17T05:13:38.000Z
50	Network	New Peer	Device f4:54:33:aa:85:dd is now communicating with Device Laptop over Protocol CIP	2021-11-18T19:58:13.616Z
78	Application	Device Update	Device f4:54:33:aa:85:dd's device type is now Torque Tool	2021-12-01T12:37:36.000Z
7	Network	New Device	Device f4:54:33:ac:f2:ac has been discovered on port 4 on switch 192.168.203.11 (d861814584)	2021-11-16T16:47:27.000Z
77	Application	Device Update	Device f4:54:33:ac:f2:ac has been renamed to 1734-AENT IO	2021-12-01T12:37:07.000Z
15	Network	Port Change	Device f4:54:33:ac:f2:ac has moved to a new port 4 on switch 192.168.203.11 (d861814584)	2021-11-16T17:04:01.000Z
31	Network	Port Change	Device f4:54:33:ac:f2:ac has moved to a new port 4 on switch 192.168.203.11 (d861814584)	2021-11-17T05:14:45.000Z
21	Network	Port Change	Device f4:54:33:ac:f2:ac has moved to a new port 4 on switch 192.168.203.11 (d861814584)	2021-11-16T17:07:02.000Z
48	Network	New Peer	Device f4:54:33:ac:f2:ac is now communicating with Device Laptop over Protocol CIP	2021-11-18T19:58:12.066Z
76	Application	Device Update	Device f4:54:33:ac:f2:ac's device type is now Remote IO	2021-12-01T12:37:07.000Z
96	Application	Device Update	Device Laptop has been renamed to Windows 10 Pro	2021-12-02T19:07:22.000Z
52	Network	New Peer	Device Laptop is now communicating with Device 00:1d:9c:ce:6c:c1 over Protocol ICMP	2021-11-18T19:58:17.101Z
42	Network	New Peer	Device Laptop is now communicating with Device Compactlogix L43 over Protocol CIP	2021-11-18T19:55:01.055Z
40	Network	New Peer	Device Laptop is now communicating with Device Compactlogix L43 over Protocol ICMP	2021-11-18T19:54:58.022Z
51	Network	New Peer	Device Laptop is now communicating with Device f4:54:33:aa:85:dd over Protocol ICMP	2021-11-18T19:58:16.949Z
41	Network	New Protocol	Protocol CIP has been detected for the first time	2021-11-18T19:55:01.053Z
39	Network	New Protocol	Protocol ICMP has been detected for the first time	2021-11-18T19:54:58.014Z
63	Network	New Protocol	Protocol SMB has been detected for the first time	2021-11-18T20:06:54.671Z
154	Network	New Protocol	Protocol TCP has been detected for the first time	2021-12-13T22:26:45.561Z
121	Network	New Protocol	Protocol UDP has been detected for the first time	2021-12-10T16:28:58.870Z

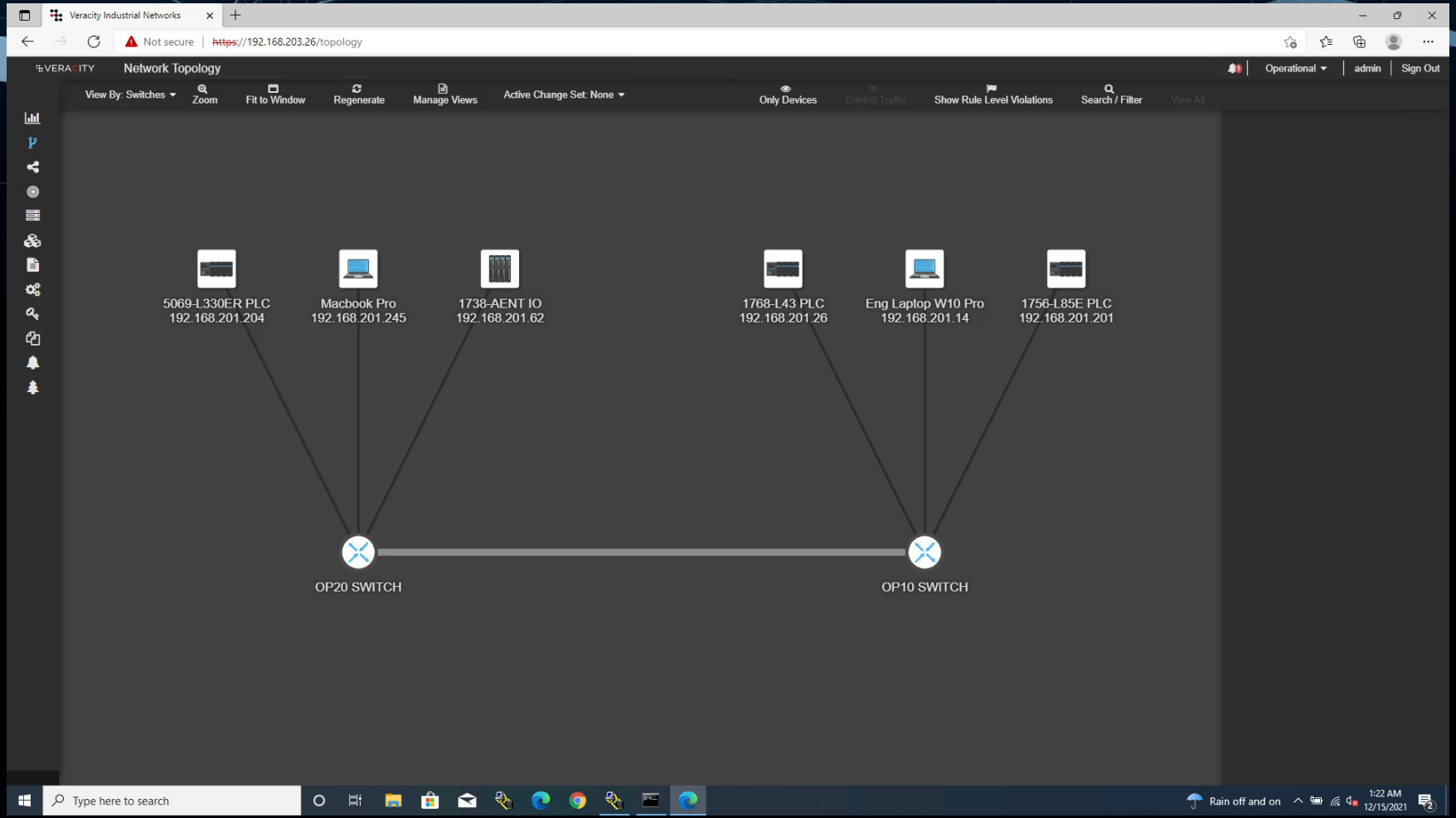
!!! FUN FACT !!!

Net-Optix provides a power-up recovery mode to make sure the controller and the network operations are sync'd.

What does that mean to normal people?

If you lose your controller configuration, for any reason such as a fork truck slams into the controller enclosure, a virtual machine corrupts, etc. Net-Optix allows you to enter "recovery mode" and it will synchronize your controller to your running production network.

DEMO


Veracity Industrial Networks
Not secure
https://192.168.203.26/topology
VERACITY
Network Topology
Operational
admin
Sign Out
View By: Switches
Zoom
Fit to Window
Regenerate
Manage Views
Active Change Set: None
Only Devices
Control Traffic
Show Rule Level Violations
Search / Filter
View All
5069-L330ER PLC
192.168.201.204
Macbook Pro
192.168.201.245
1738-AENT IO
192.168.201.62
1768-L43 PLC
192.168.201.26
Eng Laptop W10 Pro
192.168.201.14
1756-L85E PLC
192.168.201.201
OP20 SWITCH
OP10 SWITCH
Type here to search
Rain off and on
1:22 AM
12/15/2021

jsmith@dynics.com

QUESTIONS?