

# BLOX FEST

Infoblox 



# Best Practices for Network Device Discovery Using Network Insight and NetMRI

**Dave Signori**

Senior Director, Product Management

Network Insight and NetMRI

**Marty Adkins**

NetCraftsmen

**John Belamaric**

Software Architect

Cloud and Network Automation



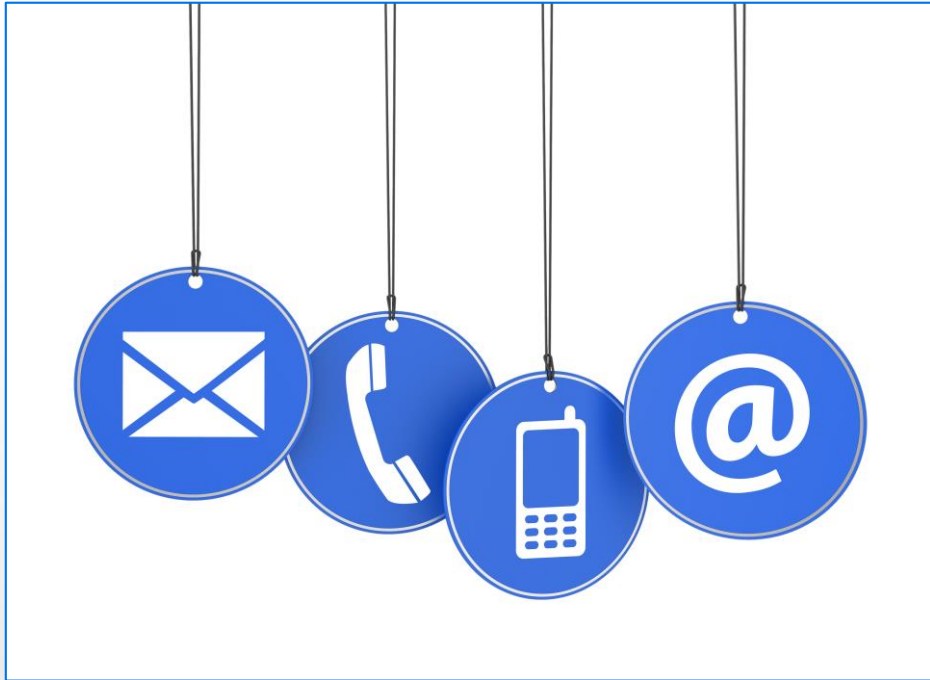
# Agenda

- Customer events
- The value of discovery
- Upcoming discovery enhancements
- How discovery works
- NetMRI tips and tricks
- Network Insight tips and tricks
- VRF environments



# NetMRI Monthly Technical Overview

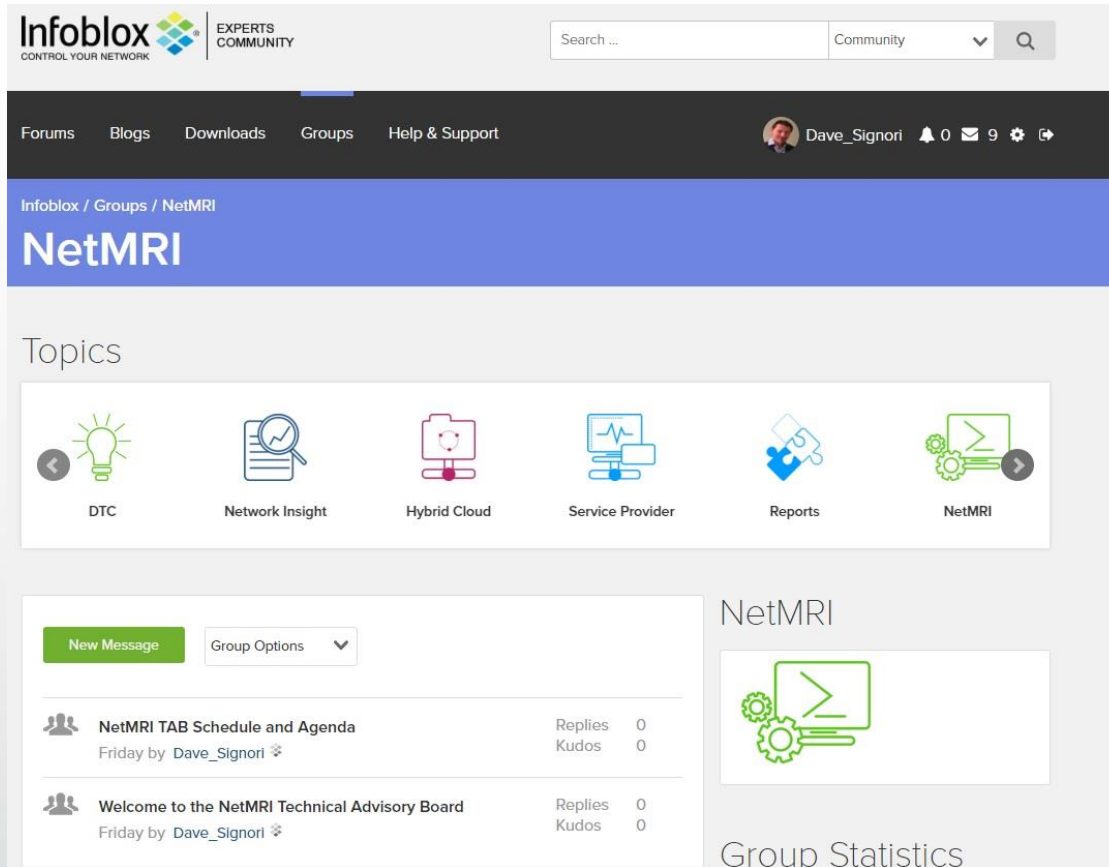
## Customer Facing



- Regularly scheduled 1-hour customer facing WebEx from Product Management, Product Marketing and Virtual Team
- Audience:
  - Customers for review to expand on use cases
  - Prospects
  - Infoblox sales for enablement
- Includes technical sales presentation and demo

# Customer Participation Opportunities

## Technical Advisory Boards



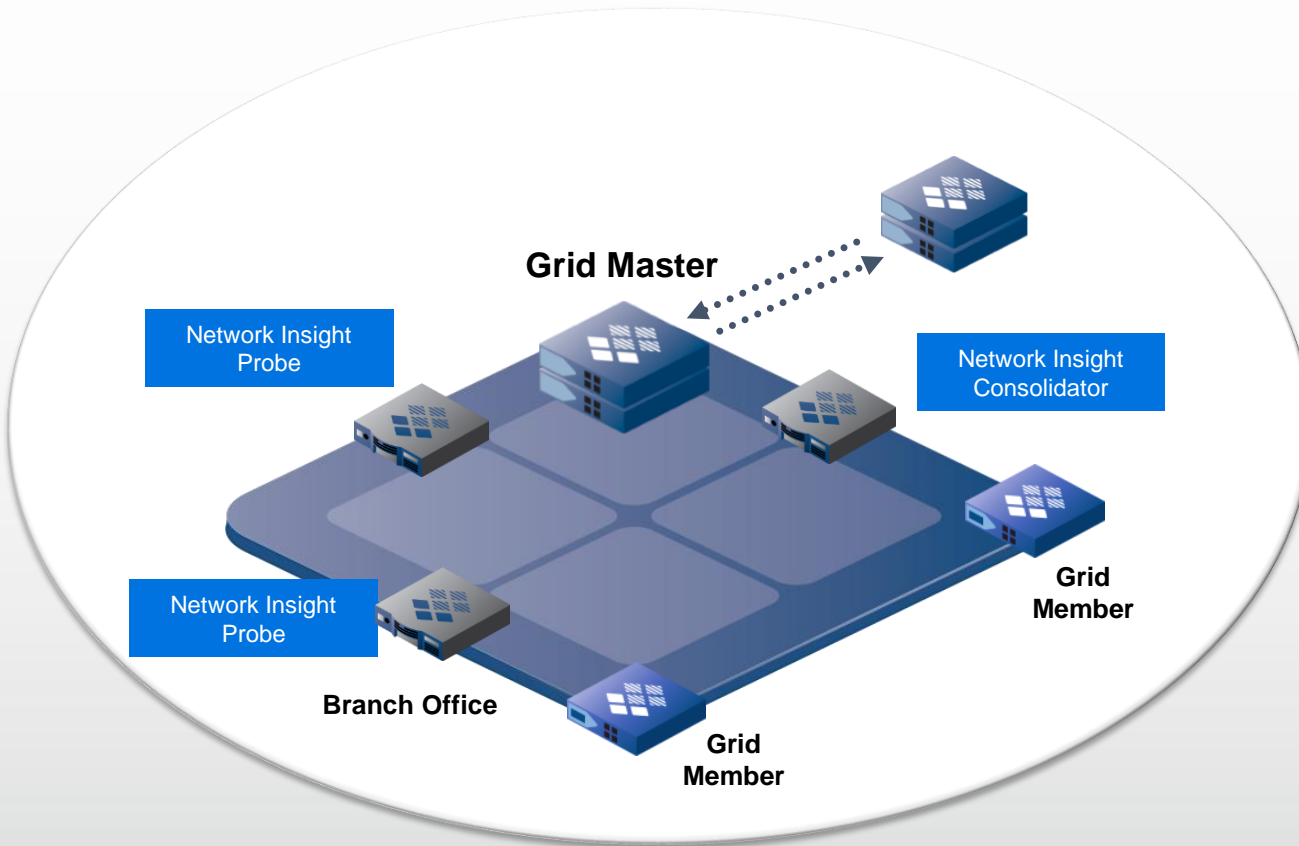
The screenshot shows the Infoblox Experts Community interface. At the top, there's a search bar and a 'Community' dropdown. Below this is a navigation bar with links to Forums, Blogs, Downloads, Groups, and Help & Support. The main header area displays 'Infoblox / Groups / NetMRI' and the group name 'NetMRI'. Under 'Topics', there are six icons representing different areas: DTC, Network Insight, Hybrid Cloud, Service Provider, Reports, and NetMRI. On the left, a 'New Message' button and 'Group Options' dropdown are visible. Below this, a list of messages is shown, including 'NetMRI TAB Schedule and Agenda' and 'Welcome to the NetMRI Technical Advisory Board', both posted by Dave\_Signori. On the right, there's a 'NetMRI' section with a gear icon and a 'Group Statistics' section.

- 10 TABs including NetMRI and Network Insight
- Roadmap and early look at pre-released features
- Input for future enhancements
- Best practices
- First NetMRI session held on May 12th
- Request membership at the Infoblox Community Site



# Infoblox Network Insight

## Discovery and Authoritative IPAM



Integrated with Grid

Enhances and ensures accurate IPAM

Deep discovery of network devices, end hosts, and relationships

Over 60 vendors supported and extensible





# Discovery

## Mapping to IPAM

The screenshot displays the Infoblox NIOS 7.3.4 IPAM interface. The top navigation bar includes the Infoblox logo, a search bar, and tabs for Master Grid, Dashboards, Data Management, Cloud, Smart Folders, Reporting, Grid, and Administration. The main navigation bar shows Company 1 (default) and various IPAM-related tabs: IPAM, Devices, Network Users, DHCP, DNS, Traffic Management, File Distribution, Security, and Threat Analytics.

The left sidebar contains a Finder section with Smart Folders and Unmanaged IP ranges. The main content area shows the IPAM Home view for the 10.66.21.0/28 IPv4 Network. It includes a Quick Filter dropdown set to None, a Filter On button, and a Show Filter link. Below this is a Go to input field and a Go button. The main table displays the IP map with columns for IP Address, Name, Discovered Name, Discoverer, First Discovered, Last Discovered, and MAC Address.

IP Address	Name	Discovered Name	Discoverer	First Discovered	Last Discovered	MAC Address
10.66.21.0						
10.66.21.1	wan-br		gm1p1.infoblox.com	2014-01-10 19:2...	2016-04-23 14:40:04 EDT	
10.66.21.2	branch5		gm1p1.infoblox.com	2014-01-10 19:2...	2016-04-23 10:08:14 EDT	
10.66.21.3						
10.66.21.4						
10.66.21.5						
10.66.21.6						
10.66.21.7						
10.66.21.8						
10.66.21.9						
10.66.21.10						
10.66.21.11						
10.66.21.12						
10.66.21.13						
10.66.21.14						
10.66.21.15						

The right sidebar contains a Toolbar with various actions: Add, Open, Edit, Lease Details, Reclaim, Extensible Attributes, Permissions, Resolve Conflict, Convert, Clear, vDiscovery, Multi-Ping, Ping, Discovery Status, Discovery Diagnostic, Exclusion, Discover Now, Restart Services, CSV Import, CSV Job Manager, and IDN Converter.



# How Discovery Works

## Overview

- Discovery is based on mining of collected data from SNMP and the CLI of a device.
- **Preferred** method to start discovery is from one or more seed routers.
- Discovery does not rely on ping sweeps.
  - Smart Ping sweeps can be configured for discovery of subnets where a router hasn't been found yet.
  - Periodic ping sweeps can be configured per configured discovery range to aid network discovery.
- Performing traceroutes helps seed discovery.
- There is no concept of scheduling discovery or knowing when discovery is complete. Discovery continually mines collected data and data collection processes are continuously running.
- Discovery uses SNMP to complete the discovery process of each device to identify the type of device, vendor, model, and OS version.
- Discovery associates all discovered IP addresses for a device to a single instance and selects a management IP address for the device (prefers loopback).
- Discovery looks at collected SNMP data from the device, along with knowledge from Nmap, traceroute, and CDP/LLDP to determine the device type.
- Discovery can be configured to use Nmap to help identify end-hosts which typically won't have SNMP enabled.





# How Discovery Works

## Stages of discovery

### Device existence

- Through mining collected data (i.e. tables) and active polling
- Possible sources of discovery data:
  - ARP tables
  - CDP / LLDP
  - Path collection (traceroute)
  - Route tables
  - Seed routers provided
  - Static IP addresses provided
  - Subnet scan

#### Note:

- In NetMRI, see E column in Network Explorer → Discovery for the source of discovery



# How Discovery Works

## Stages of discovery

### Active Polling - Path Collection (traceroute)

- Possibly all the active polling you'll need
- Steps:
  - Traceroute to first, second, middle, and last addresses in range.
  - Traceroute to hints provided (NetMRI only)
  - IP addresses found are added to database if they fall within discovery range
  - IP addresses in middle of traceroute are started as a low probability router and given priority in credential guessing
  - If no IP addresses are found in range, the range is split and half and the process started again
  - The range will be split up to 4 times
  - Traceroutes will also be performed on discovered subnets if they fall within the discovery range
  - Traceroutes run every 24 hours
  - Traceroute is Unix UDP type

#### Note:

- The discovery ranges in NI are the Networks and Containers you've defined.



# How Discovery Works

## Stages of discovery

### Active Polling – Ping Sweep

- Optional Periodic Ping Sweeps can be enabled per range
- Frequency configurable. Default is 24 hours
- Not available for IPv6

### Active Polling - Smart Subnet Ping Sweep

- Runs when discovery has not found a router in an included range or subnet
- Optional sweep that can be configured globally
- Frequency is 24 hours
- Not available for IPv6



# How Discovery Works

## Stages of discovery

### Fingerprint

- Nmap is used to make a guess at the device and to check for open ports
- Frequency is 24 hours
- Port scanning with optional finger printing (NI calls it “Profile Device”)
- You can define the port list

#### NI Notes:

- NI has two options for scan technique: SYN and CONNECT
- Configured globally and can be overridden at network level
- See Discover Status, column Fingerprint Status

#### NetMRI Notes:

- Configured globally or per device group
- See **P** column in Network Explorer → Discovery for finger print status





# How Discovery Works

## Stages of discovery

### Reachability

- Status of whether Discovery has received an actual packet from the device
- Could be the result of SNMP requests, ping sweep, or fingerprinting.
- Discovery will always attempt an ICMP ping after failing to collect any SNMP credentials from the device

#### NI Note:

- See Discover Status, column Reached Status

#### NetMRI Note:

- See R column in Network Explorer -> Discovery for reach status or method of reach.

IP Address	Network View	Name	E	P	R	S	SC	C	CC	G	DB	CB	Type	Last Timestamp	Last Action	Last Seen	First Seen
10.66.21.17	Network 1	branch5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch-Rou...	2016-05-16 19:01:25	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:58:29	2015-07-09 16:...
10.66.22.251	Network 1	bld1.infoblox.com	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch	2016-05-16 19:01:23	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:57:25	2015-07-09 17:...
10.66.22.252	Network 1	bld2.infoblox.com	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch	2016-05-16 19:01:19	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:56:52	2015-07-09 17:...
172.16.10.4	Network 1	swr-c-04	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Router	2016-05-16 19:01:06	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:59:57	2014-10-16 10:...
10.66.21.81	Network 1	branch7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch-Rou...	2016-05-16 19:01:04	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:59:54	2014-10-16 10:...
10.66.35.1	CEO	VRF-NetMRI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Router	2016-05-16 19:00:58	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:55:58	2014-10-30 18:...
10.66.21.49	Network 1	branch6	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch-Rou...	2016-05-16 19:00:51	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:59:06	2014-10-16 10:...
10.66.22.206	Network 1	fl6.infoblox.com	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch	2016-05-16 19:00:40	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:56:16	2015-07-09 17:...
10.66.20.193	Network 1	branch54	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch-Rou...	2016-05-16 19:00:37	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:59:38	2014-10-16 10:...
10.66.30.97	CEO	CEO-4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch-Rou...	2016-05-16 19:00:37	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:58:39	2014-11-05 10:...
172.16.20.6	Network 1	swr-c-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch	2016-05-16 19:00:35	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:55:34	2015-07-09 04:...
10.66.21.113	Network 1	branch8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch-Rou...	2016-05-16 19:00:27	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:59:58	2015-07-09 16:...
10.66.100.53	Network 1	Campus1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Router	2016-05-16 19:00:24	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:59:50	2014-10-16 10:...
10.66.30.130	CEO	CEO-9	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch-Rou...	2016-05-16 19:00:21	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:59:00	2014-11-02 10:...
10.66.22.200	Network 1	fl1.infoblox.com	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch	2016-05-16 19:00:13	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:58:36	2015-07-09 17:...
10.66.30.99	CEO	CEO-12	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch-Rou...	2016-05-16 19:00:09	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:58:42	2016-04-16 14:...
172.16.10.3	Network 1	swr-c-03	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Router	2016-05-16 19:00:08	SNMP Credentials: Successfully authenticated / Version: SNMPv2c	2016-05-16 18:56:34	2014-10-16 10:...
10.66.30.131	CEO	CEO-10	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch-Rou...	2016-05-16 19:00:03	Device Groups: Successfully assigned to device groups	2016-05-16 18:58:20	2014-11-05 10:...
10.66.30.98	CEO	CEO-11	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch-Rou...	2016-05-16 19:00:03	Device Groups: Successfully assigned to device groups	2016-05-16 18:59:15	2014-11-04 11:...
10.66.30.96	investment-banking	investment5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch-Rou...	2016-05-16 19:00:03	Device Groups: Successfully assigned to device groups	2016-05-16 18:58:32	2014-11-02 11:...
10.66.100.54	Network 1	Campus2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Router	2016-05-16 19:00:03	Device Groups: Successfully assigned to device groups	2016-05-16 18:58:02	2014-10-16 10:...
192.168.168.1	Network 1	tae-demo.infoblox	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch-Rou...	2016-05-16 19:00:03	Device Groups: Successfully assigned to device groups	2016-05-16 18:59:06	2015-07-27 14:...
10.120.25.145	Network 1	dev7k-dev7k-FP-1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Switch-Rou...	2016-05-16 19:00:03	Device Groups: Successfully assigned to device groups	2016-05-16 18:59:22	2014-10-19 19:...

Page: 1 of 1 | Displaying 1 - 40 of 40

Entire Network Totals  
Network Devices: 51  
Licensed Devices: 41

IP Addresses: Classified 105 Reached 124 Identified 144



# How Discovery Works

## Stages of discovery

### SNMP Credential and Data Collection

- SNMP Credentials are required to identify and manage devices
- When a device has been identified and in a discovery range, its credentials will try to be determined
- Credentials are attempted in order of configured priority
- Once valid credentials have been established, Discovery will no longer check the remaining credentials unless SNMP fails for some time, then guessing is repeated.
- Functioning SNMP collection is needed to complete the discovery of a device (i.e. sysUpTime, sysDescr, sysContact, sysLocation, sysName, sysObjectID, sysServices, and ipForwarding) and to help discover other devices on the network

The screenshot shows the Infoblox Network Explorer interface. At the top, the 'Discovery Status' window is open, showing a table of discovered devices. The 'S' and 'SC' columns are highlighted with red boxes. Below this, the main interface shows a table of discovered devices with columns for IP Address, Name, Type, Overall Status, Reached Status, SNMP Collection Enabled, SNMP Credential Status, and SNMP Collection Status. The 'S' and 'SC' columns are also highlighted with red boxes. The table lists various devices, including switches, routers, and servers, with their respective IP addresses, names, and discovery status.

IP Address	Name	Type	Overall Status	Reached Status	SNMP Collection Enabled	SNMP Credential Status	SNMP Collection Status
10.66.21.17	Network 1	branch5	✓	✓	✓	✓	✓
10.66.22.251	Network 1	bid1.infoblox.com	✓	✓	✓	✓	✓
10.66.22.252	Network 1	bid2.infoblox.com	✓	✓	✓	✓	✓
172.16.10.4	Network 1	svr-c-04	✓	✓	✓	✓	✓
10.66.21.81	Network 1	branch7	✓	✓	✓	✓	✓
10.66.35.1	CEO	VRF-NetMRI	✓	✓	✓	✓	✓
10.66.21.49	Network 1	branch6	✓	✓	✓	✓	✓
10.66.22.206	Network 1	f66.infoblox.com	✓	✓	✓	✓	✓
10.66.20.193	Network 1	branch54	✓	✓	✓	✓	✓
10.66.30.97	CEO	CEO-4	✓	✓	✓	✓	✓
172.16.20.6	Network 1	svr-c-02	✓	✓	✓	✓	✓
10.66.21.113	Network 1	branch8	✓	✓	✓	✓	✓
10.66.100.53	Network 1	Campus1	✓	✓	✓	✓	✓
10.66.30.130	CEO	CEO-9	✓	✓	✓	✓	✓
10.66.22.209	Network 1	f11.infoblox.com	✓	✓	✓	✓	✓
10.66.30.99	CEO	CEO-12	✓	✓	✓	✓	✓
172.16.10.3	Network 1	svr-c-03	✓	✓	✓	✓	✓
10.66.30.131	CEO	CEO-10	✓	✓	✓	✓	✓
10.66.30.98	CEO	CEO-11	✓	✓	✓	✓	✓
10.66.30.66	investment-banking	investment5	✓	✓	✓	✓	✓
10.66.100.54	Network 1	Campus2	✓	✓	✓	✓	✓
192.168.168.1	Network 1	tae-demo.infoblox	✓	✓	✓	✓	✓
10.120.25.145	Network 1	dev7k-dev7k-FP-1	✓	✓	✓	✓	✓

### NetMRI Note:

- See **S** and **SC** columns in Network Explorer → Discovery for SNMP credential and data collection status



# How Discovery Works

## Stages of discovery

### CLI Credential and Data Collection

- CLI Credentials are required to identify and collect certain types of data and manage devices
- When a device has been identified and in a discovery range, its credentials will try to be determined
- Credentials are attempted in order of configured priority
- Once valid credentials have been established, Discovery will no longer check the remaining credentials unless it fails for some time, then guessing is repeated.

#### NI Note:

- See Discover Status, columns: SNMP Credential Status, SNMP Collection Status
- Credentials can be overridden to the device level

#### NetMRI Note:

- See **C** and **CC** columns in Network Explorer → Discovery for SNMP credential and data collection status



# How Discovery Works

## Device Type Assurance – NetMRI only

- When NetMRI initially discovers a device, if no data is currently available to provide clues to the type of device, NetMRI will assign it to the "unknown" device group with a 0% assurance.
- Should initial discovery provide some sort of hint as to the device type, NetMRI will start that device with that type and a 20% assurance.
- As NetMRI collects information about a given device such as SNMP or data from Nmap, the device assurance will increase.
- NetMRI will not raise device assurance above 75% for any device for which SNMP data is not collected.
- Additionally NetMRI will not raise device assurance above 75% for any device for which NetMRI can't determine the difference between two or more possible device types for a given device.
- Executing a discovery diagnostic against such a device will reveal the device types being considered and aid as a debugging tool to the device support team to help resolve such issues.





# How Discovery Works

## Collection Intervals

Operation	Interval
Path collection (traceroute)	24 hours
Ping Sweep	Configurable (default = 24 hours)
Smart Ping Sweep	24 hours
Fingerprinting (Nmap)	24 hours
Switch Polling	Configurable (default = 30 minutes)
SNMP	Depends (See Setup -> Setup -> Device Collection Status)

# NetMRI – Common Discovery Issues

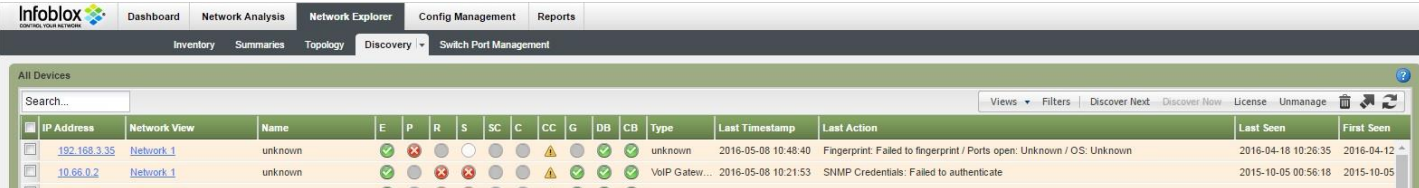
- Device IP not within included Discovery range
- Next hop router NetMRI-facing interface IP not within included Discovery range
- A policy device (firewall) blocks access from NetMRI for some protocols (SNMP, SSH)
- Unwanted (“Unknown”) devices being discovered - adjust Discovery Settings Include/Exclude ranges (Excludes always override Includes)
- Devices and Device Groups can be set to disable SNMP (Unmanage).
- SPM will learn all end host IP/MAC and their L3/L2 location without requiring to manage them



# NetMRI Discovery Aids

## Tools for troubleshooting

- Network Explorer → Discovery → Problems
  - Use Tool Tips
  - Sort by problems (i.e. license problems)
  - Multi-select – discover now, unmanage, delete
  - Sorting, searching, last action, etc ...



The screenshot shows the Infoblox NetMRI Network Explorer interface. The 'Discovery' tab is selected, displaying a table of discovered devices. The table has columns for IP Address, Network View, Name, and various status indicators (E, P, R, S, SC, C, CC, G, DB, CB, Type). The 'Last Action' column shows details of the discovery process, including timestamps and error messages like 'Fingerprint: Failed to fingerprint / Ports open: Unknown / OS: Unknown' and 'SNMP Credentials: Failed to authenticate'.

IP Address	Network View	Name	E	P	R	S	SC	C	CC	G	DB	CB	Type	Last Timestamp	Last Action	Last Seen	First Seen
192.168.3.35	Network 1	unknown	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	unknown	2016-05-08 10:48:40	Fingerprint: Failed to fingerprint / Ports open: Unknown / OS: Unknown	2016-04-18 10:26:35	2016-04-12
10.66.0.2	Network 1	unknown	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	VoIP Gatew...	2016-05-08 10:21:53	SNMP Credentials: Failed to authenticate	2015-10-05 00:56:18	2015-10-05
10.66.0.120	Network 1	unknown	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	VoIP Gatew...	2016-05-08 10:22:00	SNMP Credentials: Failed to authenticate	2016-04-01 16:06:10	2016-04-01

### Interpreting Discovery Table Data

The Recent Activity, License Management, Problems and Non-Detected IPs tables organize information in the following columns:

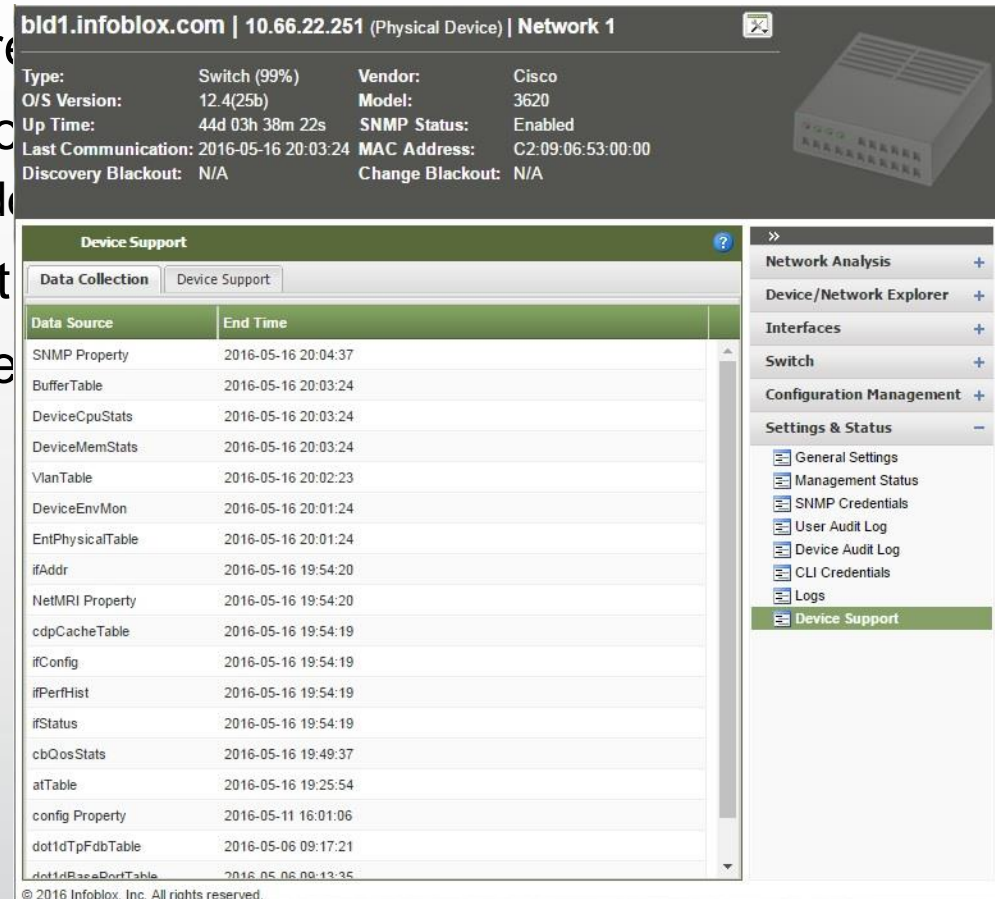
E (Existing Status)	The listed IP address exists in the network. All devices will receive this status to indicate where Network Automation first discovered the address.
P (Fingerprint Status)	If Network Automation is configured to use fingerprinting, device fingerprint status is listed in this column.
R (Reached Status)	Shows whether Network Automation has sent a packet to the device and received a reply, establishing that the device is reachable. Devices are typically tested for reachability through SNMP and the CLI, usually with an ICMP Ping operation.
S (SNMP Credentials Status)	Indicates status of the SNMP credential guessing process.
SC (SNMP Collection Status)	Shows status of SNMP data collection for the device. Success indicates that a device successfully allows data collection through SNMP. If this is not successful, check the S field to see whether the correct credential is given.
C (CLI Credentials Status)	Displays status of the CLI credential guessing process.
CC (Config Collection Status)	indicates whether a device supports command-line connectivity and whether configuration collection is successful. If this is not successful, check the C field to see whether the correct credential is given.
G (Device Group Status)	Shows status of the device group generation process. Success indicates that a device has been assigned to at least one group.



# NetMRI Discovery Aids

## Built-In Tools

- SNMP Credential Test - tries each of the known ones in priority order
- SNMP Walk - specify community string / v3 credentials
- CLI Credential Test - tries each of the known credentials
  - Check "Unknown Password" issue for failing devices
- SSH/Telnet - have NetMRI attempt an interactive session
- Device Viewer -> Settings & Status -> CLI Credentials
- Device Viewer -> Settings & Status -> Device Settings (animate)



The screenshot displays the NetMRI interface for a physical device. The top header shows the device ID 'bld1.infoblox.com', IP '10.66.22.251', and 'Network 1'. Below this, a table lists device properties: Type (Switch 99%), O/S Version (12.4(25b)), Up Time (44d 03h 38m 22s), Vendor (Cisco), Model (3620), SNMP Status (Enabled), Last Communication (2016-05-16 20:03:24), MAC Address (C2:09:06:53:00:00), Discovery Blackout (N/A), and Change Blackout (N/A). A small image of a switch is shown to the right. The main content area is titled 'Device Support' and contains a table with two columns: 'Data Source' and 'End Time'. The table lists various data sources and their corresponding end times. A sidebar on the right contains a navigation menu with options like Network Analysis, Device/Network Explorer, Interfaces, Switch, Configuration Management, Settings & Status, and Device Support.

Data Source	End Time
SNMP Property	2016-05-16 20:04:37
BufferTable	2016-05-16 20:03:24
DeviceCpuStats	2016-05-16 20:03:24
DeviceMemStats	2016-05-16 20:03:24
VlanTable	2016-05-16 20:02:23
DeviceEnvMon	2016-05-16 20:01:24
EntPhysicalTable	2016-05-16 20:01:24
ifAddr	2016-05-16 19:54:20
NetMRI Property	2016-05-16 19:54:20
cdpCacheTable	2016-05-16 19:54:19
ifConfig	2016-05-16 19:54:19
ifPerfHist	2016-05-16 19:54:19
ifStatus	2016-05-16 19:54:19
cbQosStats	2016-05-16 19:49:37
atTable	2016-05-16 19:25:54
config Property	2016-05-11 16:01:06
dot1dTpFdbTable	2016-05-06 09:17:21
dot1dBasePortTable	2016-05-06 09:13:35

© 2016 Infoblox, Inc. All rights reserved.

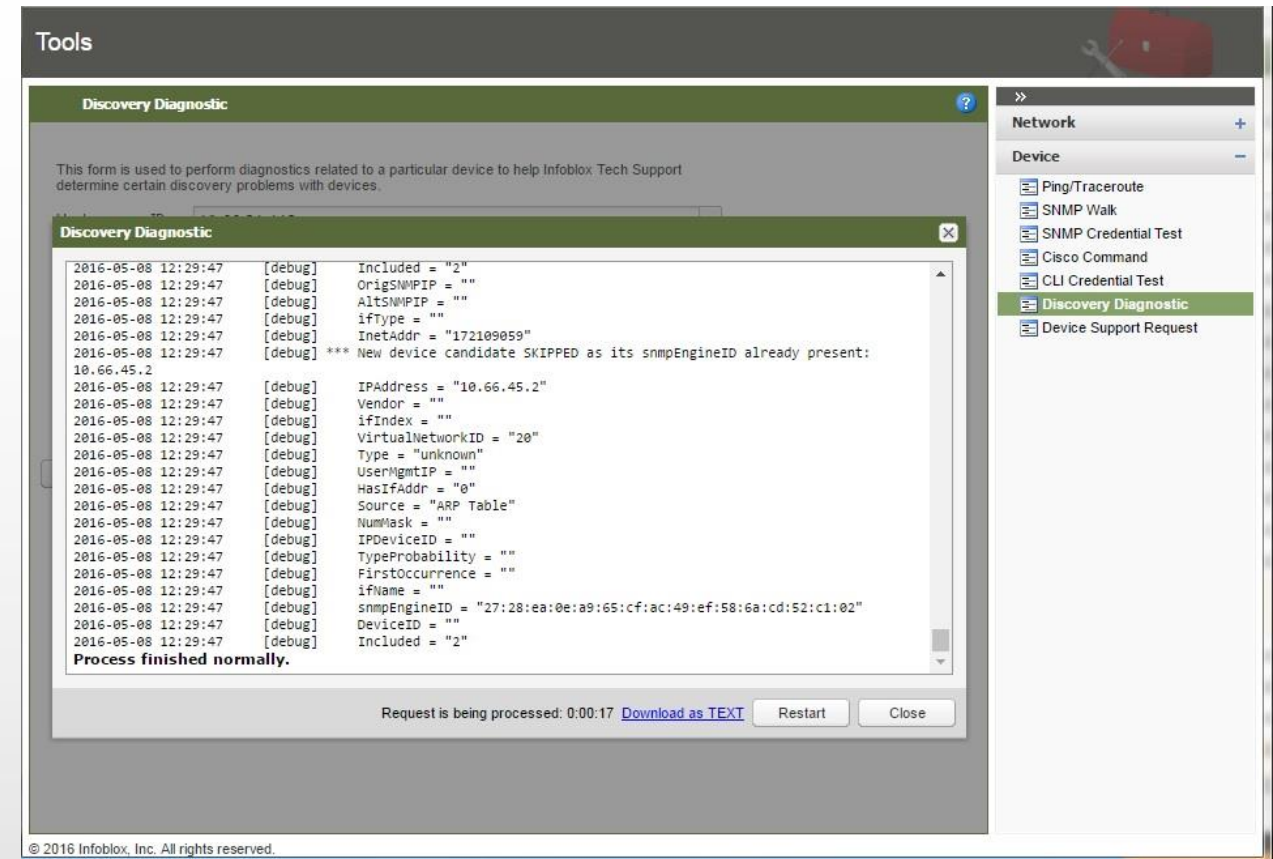




# NetMRI Discovery Aids

## Tools for troubleshooting

- Discovery Diagnostic
  - Tools → Discovery Diagnostic
  - Device getting mis-identified
  - Gives you a chance to manually try some SNMP strings
  - Support will ask for it



# NetMRI Discovery Aids

## Tools for troubleshooting

- Device Audit Log
  - Log of devices coming and going
  - Reason why

Settings

Device Audit Log

Device Events seen

Search...

Views Filters

Time	Type	Message
2016-05-07 15:40:03	LicenseDelete	Device 10.66.100.48 no longer licensed as a result of device group processing.
2016-05-07 15:40:03	LicenseDelete	Device 10.66.20.177 no longer licensed as a result of device group processing.
2016-05-07 15:36:02	LicenseAdd	Device 10.66.100.48 licensed as a result of device group processing.
2016-05-07 15:36:02	LicenseAdd	Device 10.66.20.177 licensed as a result of device group processing.
2016-05-07 15:32:25	DiscoveryDelete	Device 10.66.21.129 deleted due to the reason: duplicate snmpEngineID: similar to device 24765
2016-05-07 15:30:24	DiscoveryDelete	Device 10.66.21.129 deleted due to the reason: duplicate snmpEngineID: similar to device 24765
2016-05-07 15:30:24	DiscoveryDelete	Device 10.66.20.177 deleted due to the reason: MGMT_DUPLICATE
2016-05-07 15:30:03	LicenseAdd	Device 10.66.20.145 licensed as a result of device group processing.
2016-05-07 15:30:03	LicenseAdd	Device 10.66.100.48 licensed as a result of device group processing.
2016-05-07 15:30:03	LicenseAdd	Device 10.66.20.177 licensed as a result of device group processing.
2016-05-07 15:16:17	DiscoveryDelete	Device 10.66.21.129 deleted due to the reason: duplicate snmpEngineID: similar to device 24765
2016-05-07 15:14:16	DiscoveryDelete	Device 10.66.21.129 deleted due to the reason: duplicate snmpEngineID: similar to device 24765
2016-05-07 14:54:03	LicenseAdd	Device 10.66.20.177 licensed as a result of device group processing.
2016-05-07 14:50:03	LicenseAdd	Device 10.66.100.48 licensed as a result of device group processing.
2016-05-07 14:40:03	LicenseDelete	Device 10.66.100.48 no longer licensed as a result of device group processing.
2016-05-07 14:40:03	LicenseDelete	Device 10.66.20.177 no longer licensed as a result of device group processing.
2016-05-07 14:36:03	LicenseAdd	Device 10.66.100.48 licensed as a result of device group processing.
2016-05-07 14:36:03	LicenseAdd	Device 10.66.20.177 licensed as a result of device group processing.
2016-05-07 14:33:56	DiscoveryDelete	Device 10.66.21.129 deleted due to the reason: duplicate snmpEngineID: similar to device 24765
2016-05-07 14:31:55	DiscoveryDelete	Device 10.66.21.129 deleted due to the reason: duplicate snmpEngineID: similar to device 24765
2016-05-07 14:30:02	LicenseAdd	Device 10.66.100.48 licensed as a result of device group processing.
2016-05-07 14:30:02	LicenseAdd	Device 10.66.20.177 licensed as a result of device group processing.

Page 1 of 11 | Displaying 1 - 200 of 2113

Updated at 2016-05-08 12:21:10

© 2016 Infoblox, Inc. All rights reserved.

User Admin  
Setup  
Issue Analysis  
Notifications  
System Health  
Hardware Status  
Subscriptions  
Sent Notifications  
Background Tasks  
System Settings  
System Messages  
Device Audit Log  
General Settings  
Database Settings



# NetMRI Best Practices

## Device Groups

- OOTB defines only generic Switching, Routing, Security, Voice, Wireless, etc.
- Create more based on your needs: topo, geo, orgs, vendor, model
- Devices in higher ranking groups (top of list) are first to be licensed
- Take advantage of sibling and child nesting
- Device can belong to more than one group



# NetMRI Tips and Tricks

**Q:** There's a new device on the network -- how can I speed its discovery?

**A:**

- If the device has been discovered but has a low assurance level:
  - Device Viewer -> Management -> Discover Now
  - Separately use built-in tools
- If the device isn't showing up at all but is within Discovery ranges:
  - Global Settings -> Setup -> Discovery Settings
  - Temporarily add it as a Seed Router -> select Discover Now

**Q:** Device config was changed 10 minutes ago but NetMRI is not showing a new revision.

**Q:** NetMRI shows a new revision but the change was made by "unknown".

**A:**

- Check device configured list of syslog servers -- include NetMRI?
- Good: logging host <\$NetMRI\_ipaddress>
- Better: logging discriminator OnlyConf mnemonics includes CONFIG
  - logging host <\$NetMRI\_ipaddress> discriminator OnlyConf
- Extra Credit: create a policy and remediation script to detect and correct this. :)





# Network Insight Tips and Tricks

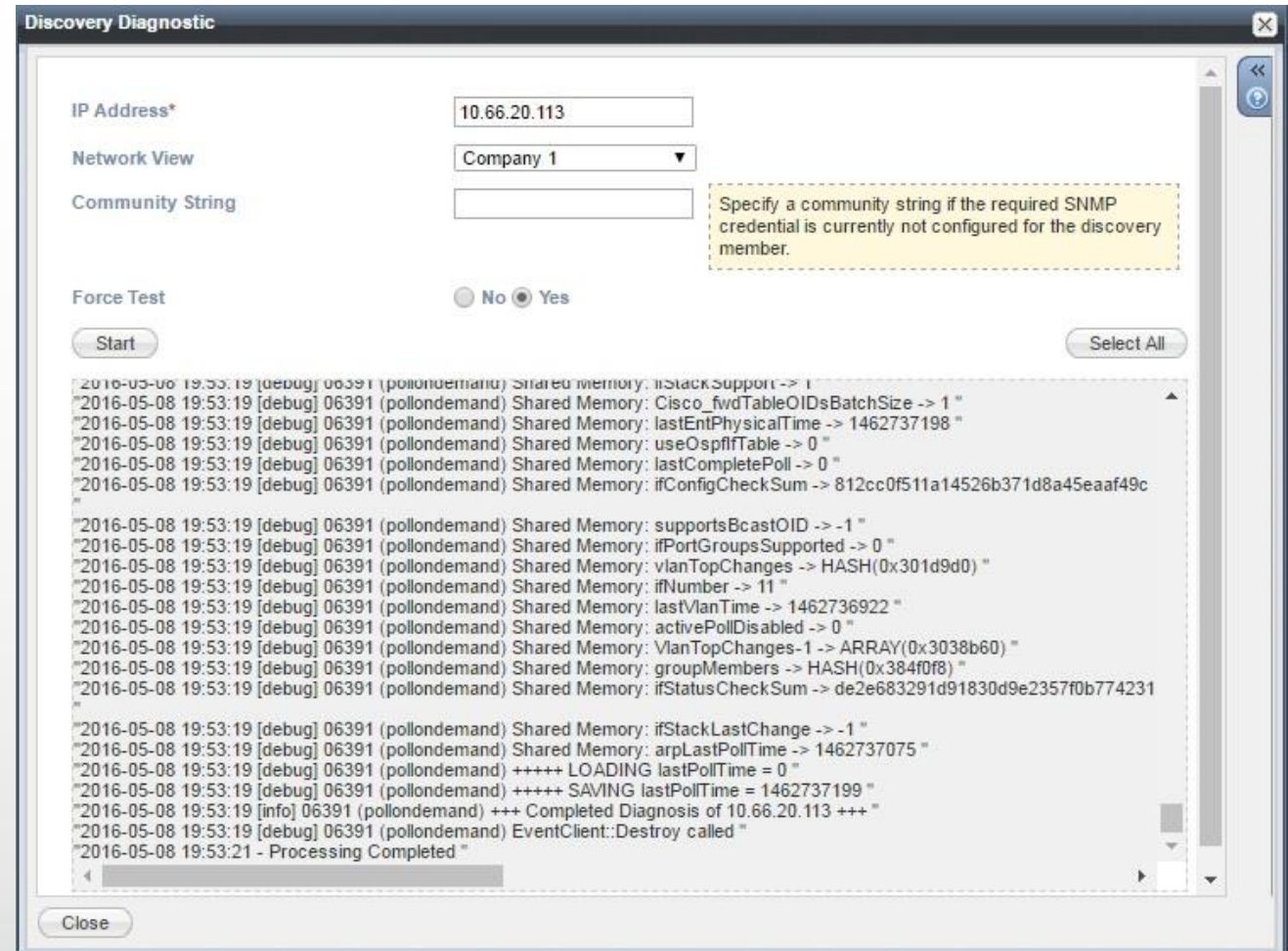
- Best practice:
  - Start troubleshooting with devices, not IPAM
    - If end hosts aren't showing up, check the switch/router they're on
    - Check if device has model, OS, etc ... correct
    - Once you've checked the device, now it's time to run a discovery diagnostic
  - All references to "ranges" in prior slides is a "Network" in NI. In other words, adding a Network in NI is like adding a Range in NetMRI
  - Take advantage of Seed Routers
  - When troubleshooting credentials, note that you can override credentials all the way to the network device level. You can also specify in Discovery Diagnostics
  - Use the Discovery Status feature



# Network Insight Tips and Tricks

## Tools for troubleshooting

- Discovery Diagnostic



# Network Insight Tips and Tricks

## Tools for troubleshooting

- Discovery Status
  - Status or Reached, SNMP collection, CLI collection, Fingerprinting, Last Action, etc ...

Discovery Status

Off Filter On | Show Filter

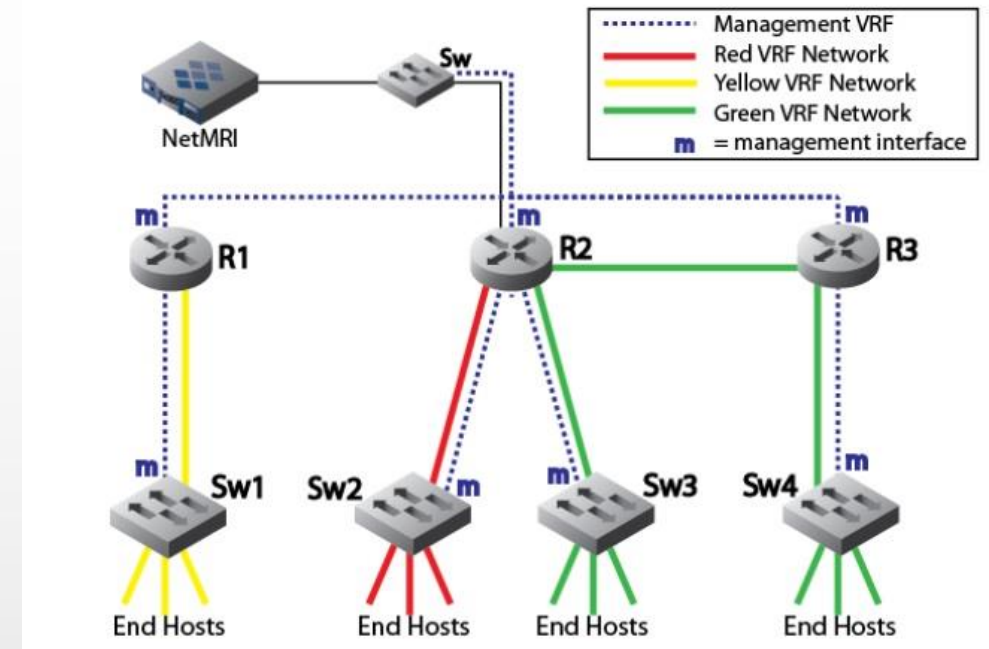
<input type="checkbox"/>	IP Address ▲	Name	Type	Overall Status	Reached Status	SNMP Collection Enabled	SNMP Credential Status	SNMP Collection Status	CLI Credential Status	CLI Collection E
<input type="checkbox"/>	3.1.1.1	unknown	Router	Failed	Failed	Yes	Failed			No
<input type="checkbox"/>	10.66.20.113	wan-br	Switch-Router	Failed	Passed	Yes	Passed	Failed	Failed	Yes
<input type="checkbox"/>	10.66.20.129	branch2	Switch-Router	Failed	Passed	Yes	Passed	Failed	Failed	Yes
<input type="checkbox"/>	10.66.20.161	branch3	Switch-Router	Failed	Passed	Yes	Passed	Failed	Failed	Yes
<input type="checkbox"/>	10.66.20.193	branch54	Switch-Router	Failed	Passed	Yes	Passed	Failed	Failed	Yes
<input type="checkbox"/>	10.66.21.17	branch5	Switch-Router	Failed	Passed	Yes	Passed	Failed	Failed	Yes
<input type="checkbox"/>	10.66.21.49	branch6	Switch-Router	Failed	Passed	Yes	Passed	Failed	Failed	Yes
<input type="checkbox"/>	10.66.21.81	branch7	Switch-Router	Failed	Passed	Yes	Passed	Failed	Failed	Yes
<input type="checkbox"/>	10.66.21.113	branch8	Switch-Router	Failed	Passed	Yes	Passed	Failed	Failed	Yes
<input type="checkbox"/>	10.66.21.145	branch9	Switch-Router	Failed	Passed	Yes	Passed	Failed	Failed	Yes
<input type="checkbox"/>	10.66.22.200	fl1.infoblox.com	Switch	Failed	Passed	Yes	Passed	Passed	Failed	Yes
<input type="checkbox"/>	10.66.22.201	fl2.infoblox.com	Switch	Failed	Passed	Yes	Passed	Passed	Failed	Yes
<input type="checkbox"/>	10.66.22.203	fl3.infoblox.com	Switch	Failed	Passed	Yes	Passed	Passed	Failed	Yes
<input type="checkbox"/>	10.66.22.204	fl4.infoblox.com	Switch	Failed	Passed	Yes	Passed	Passed	Failed	Yes
<input type="checkbox"/>	10.66.22.205	fl4.infoblox.com	Switch	Failed	Passed	Yes	Passed	Passed	Failed	Yes

Close

# Network Insight VRF Support

## NIOS 7.3

- VRF (Virtual Networks) are discovered, modeled and assigned network views
- Overlapping IP addresses with single probe
- VRF support for Cisco IOS, Cisco NX-OS, and Juniper JunOS
- Includes Discovery Engine sync with NetMRI
  - Latest device support
  - Write device support bundles once for both NI and NetMRI
- Configuration:
  - Support several configurations, this one is the most common ...
  - SNMP access to MGMT VRF or MGMT interface on physical device
  - CLI access for gathering VRF information.
  - NI using a scan port for each Network View
  - Multiple VRF assignment per Network View
    - VRF Assignment Rules (7.3.200)





# BLOX FEST

Infoblox 