
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

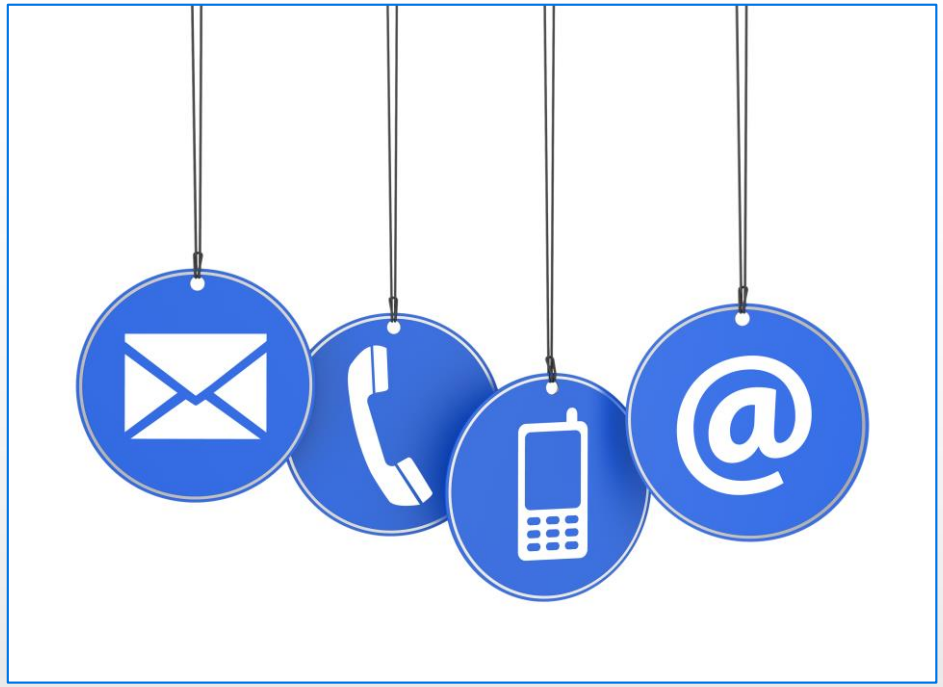
Cloud and Network Automation

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

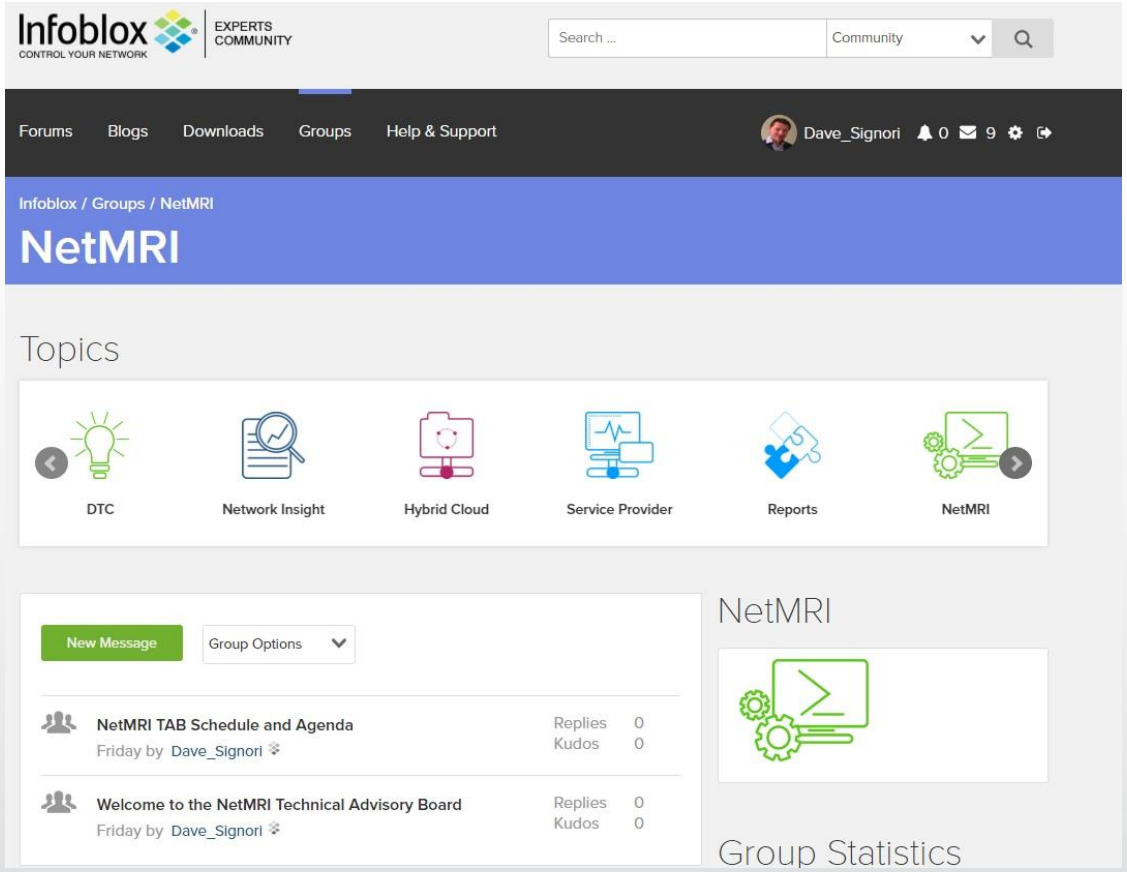
Customer Facing



- 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

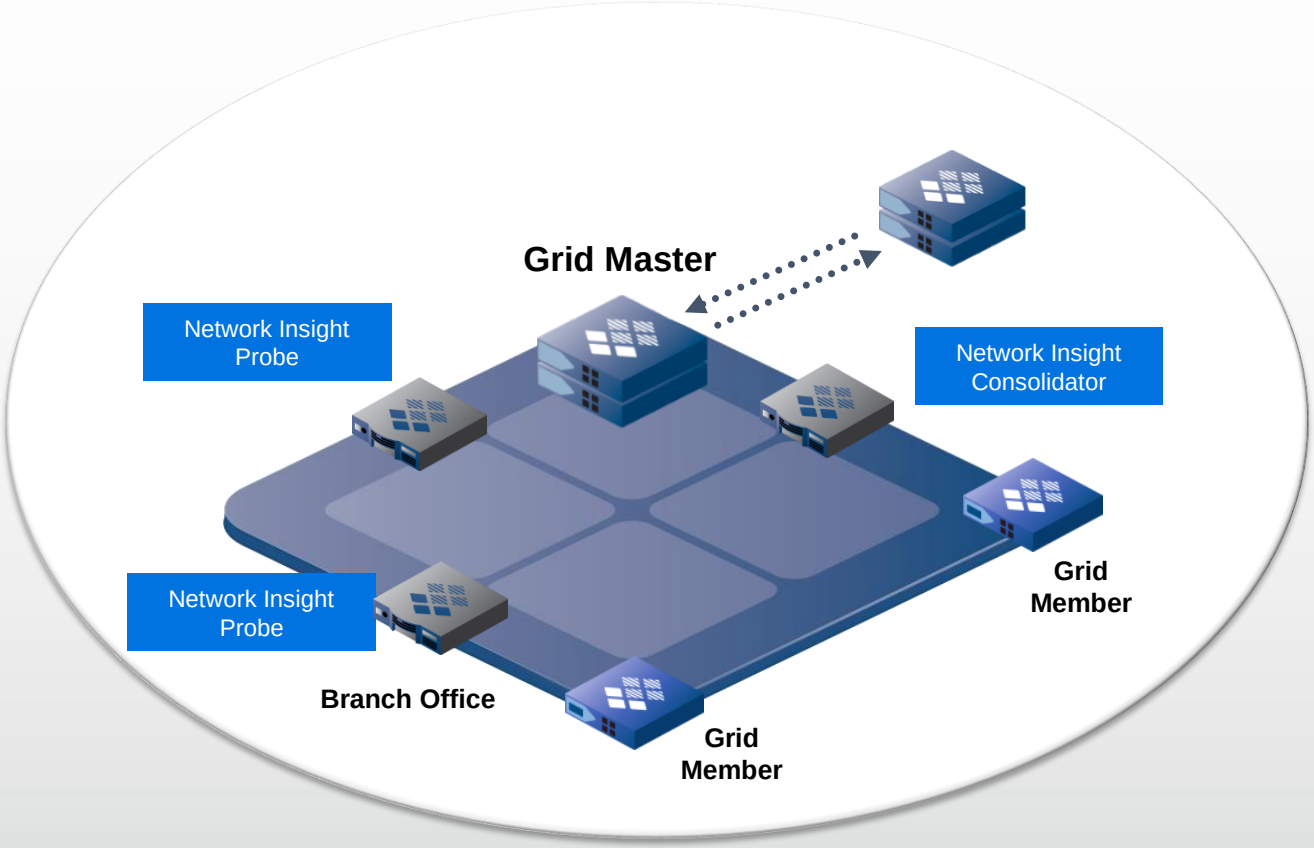
Technical Advisory Boards



- 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

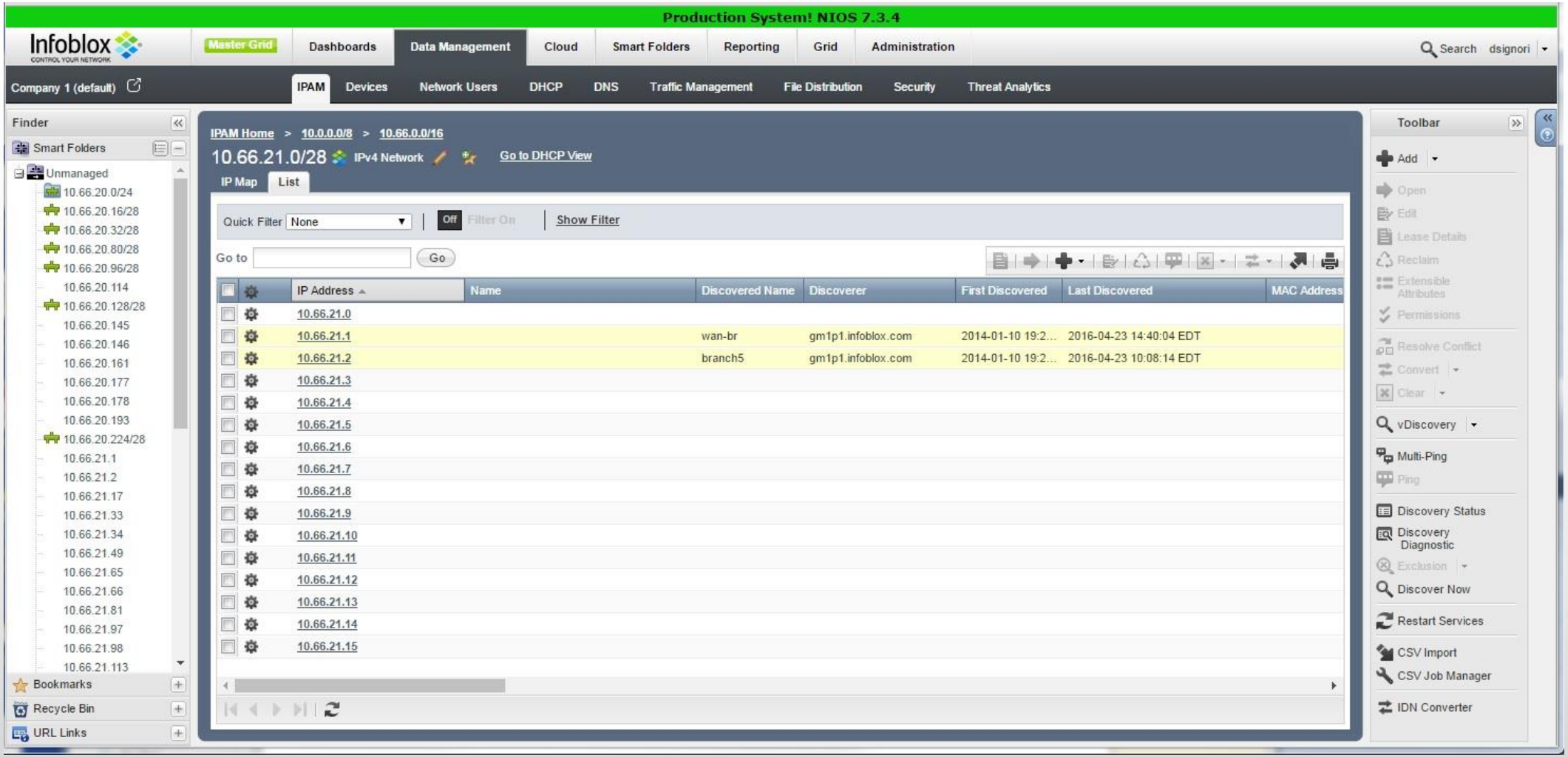
Discovery and Authoritative IPAM



- 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



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

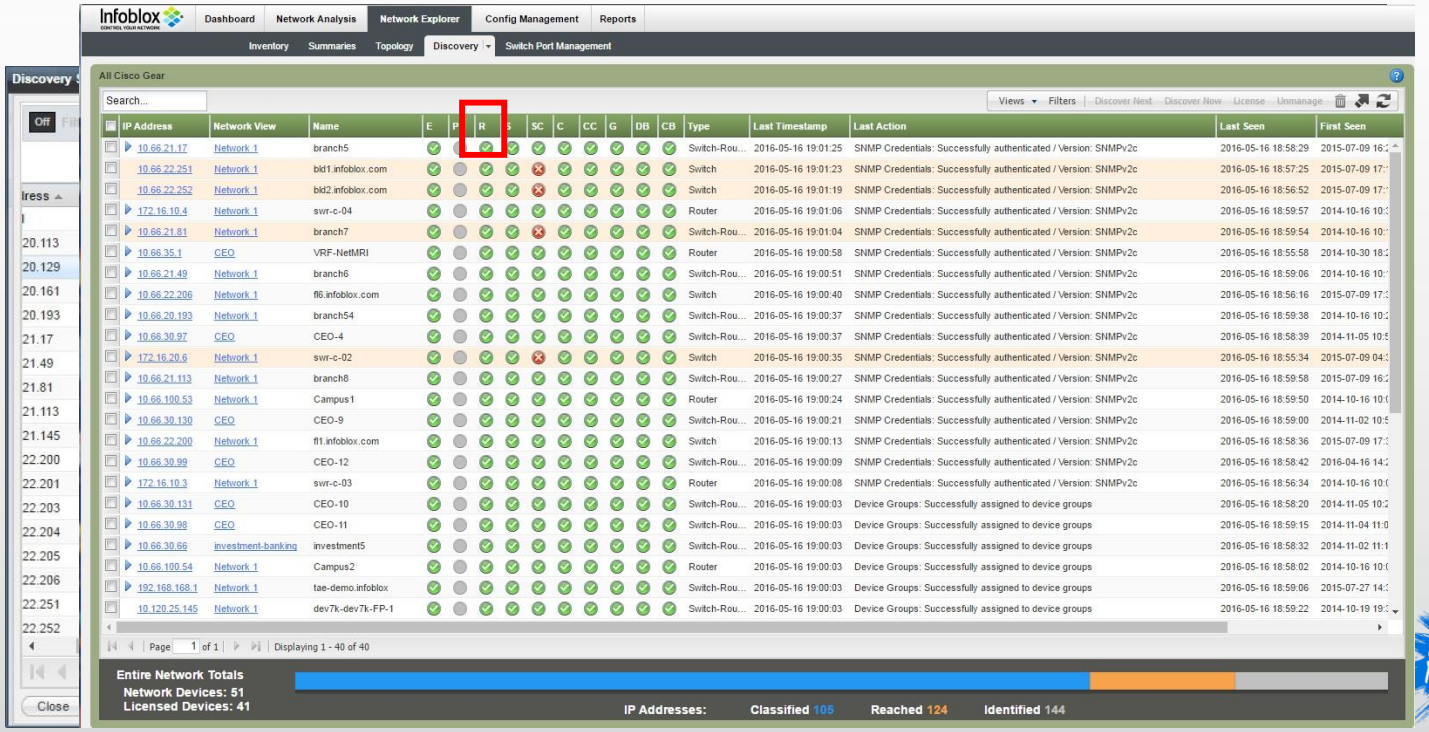
Stages of discovery

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.

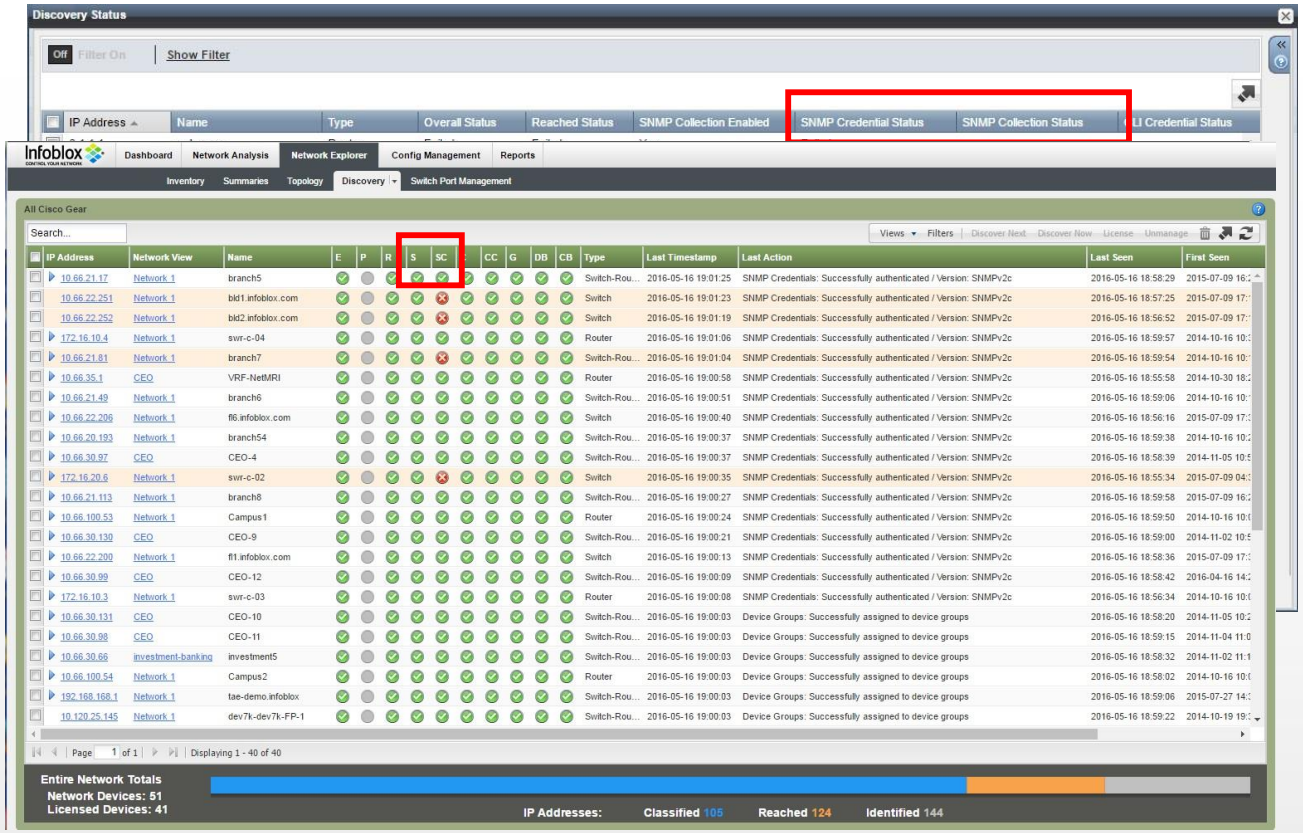


How Discovery Works

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



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)

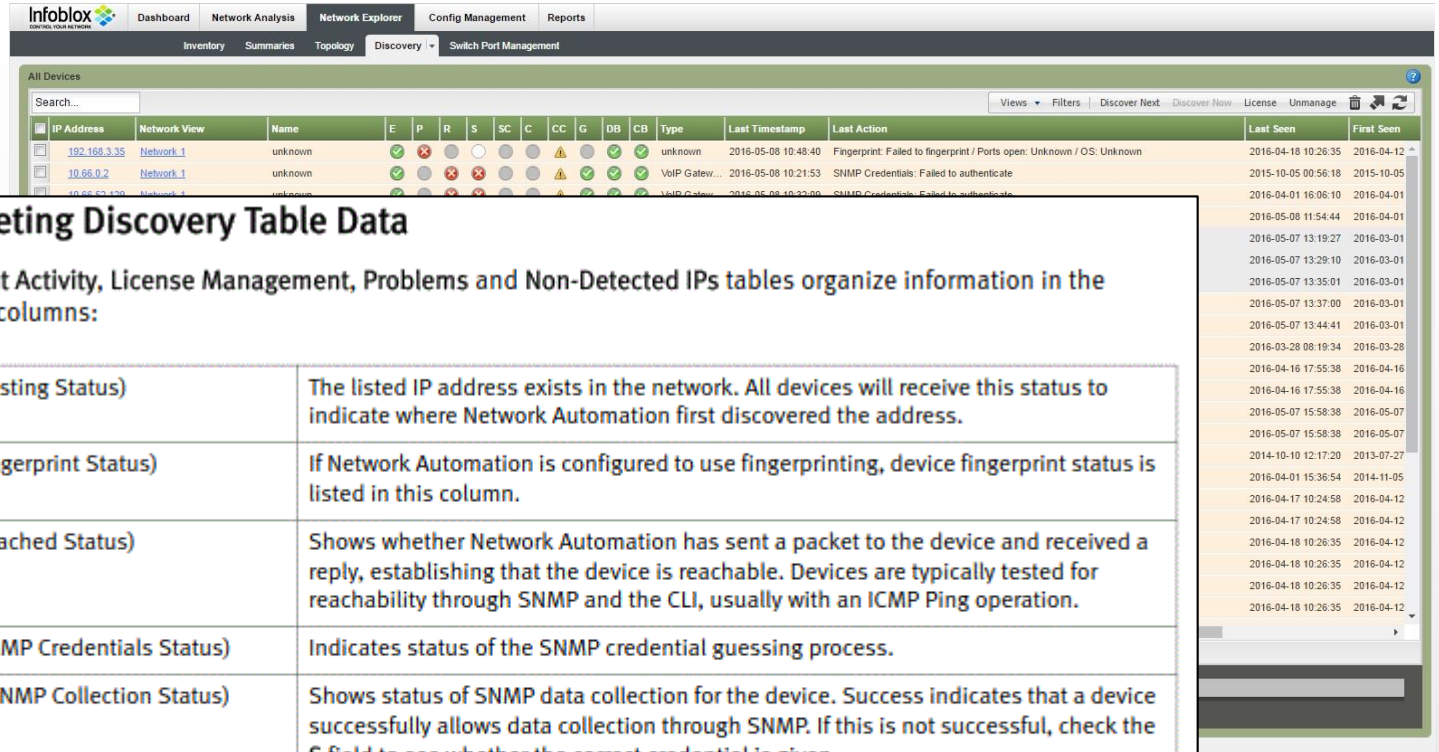
NetMRI – Common Discovery Issues

- 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 …



Interpreting Discovery Table Data

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

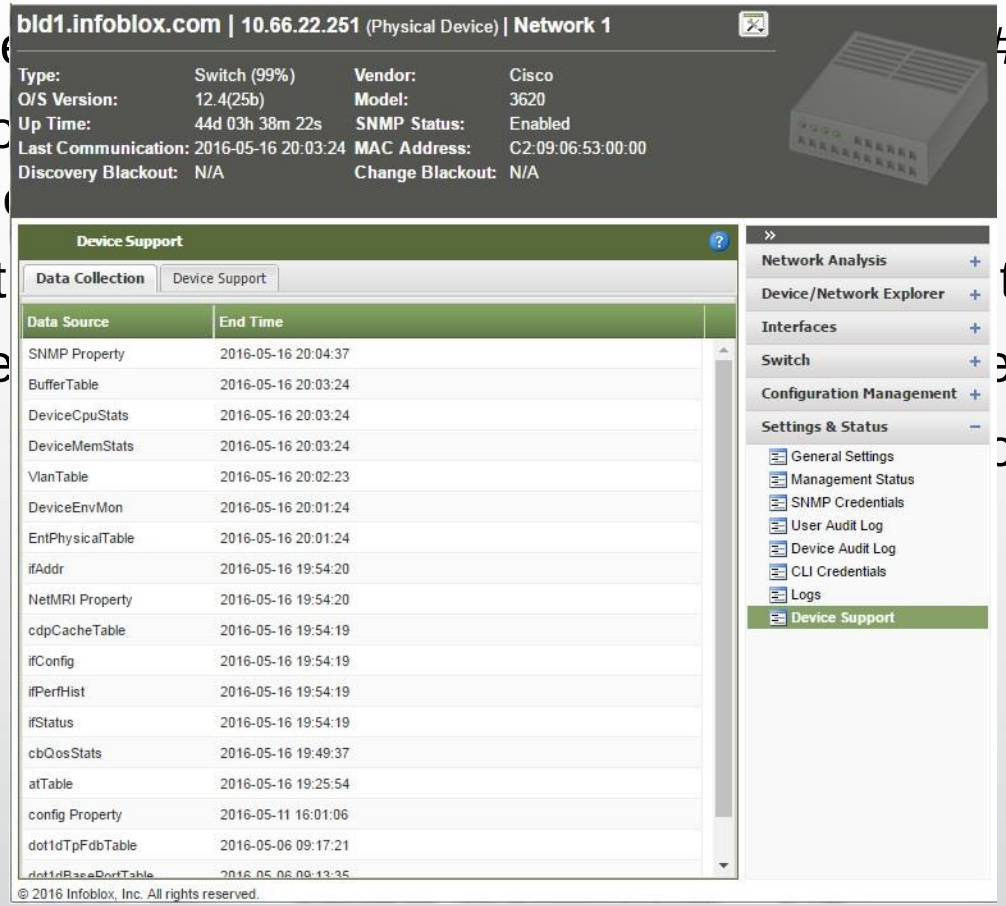
E (Existing Status)	The listed IP address exists in the network. All devices will receive this status to indicate where Network Automation first discovered the address.
P (Fingerprint Status)	If Network Automation is configured to use fingerprinting, device fingerprint status is listed in this column.
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.

BLOX FEST

NetMRI Discovery Aids

Built-In Tools

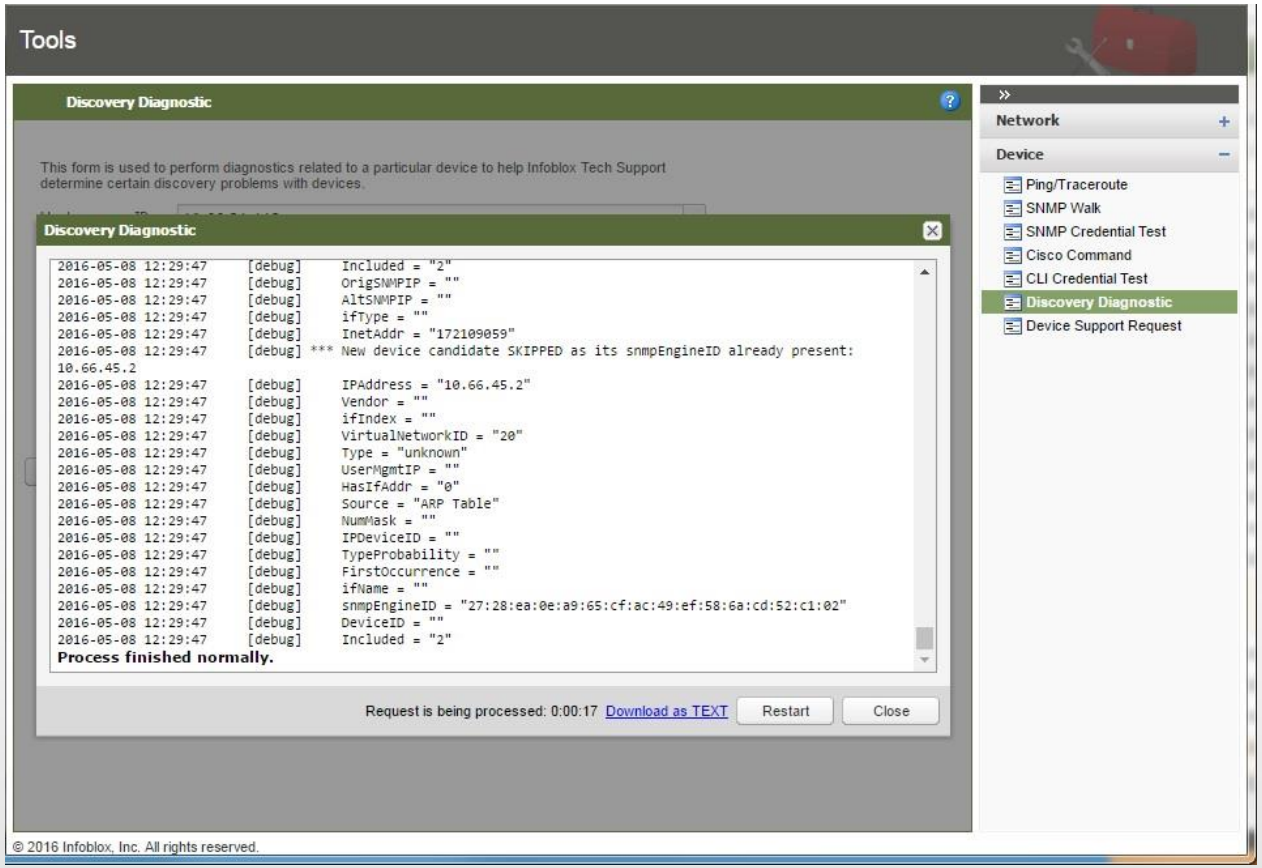
- SNMP Credential Test - tries each of the known ones in priority order
- SNMP Walk - specify community string / v3 cre
- CLI Credential Test - tries each of the known c
  - Check "Unknown Password" issue for failing d
- SSH/Telnet - have NetMRI attempt an interact
- Device Viewer -> Settings & Status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



NetMRI Discovery Aids

Tools for troubleshooting

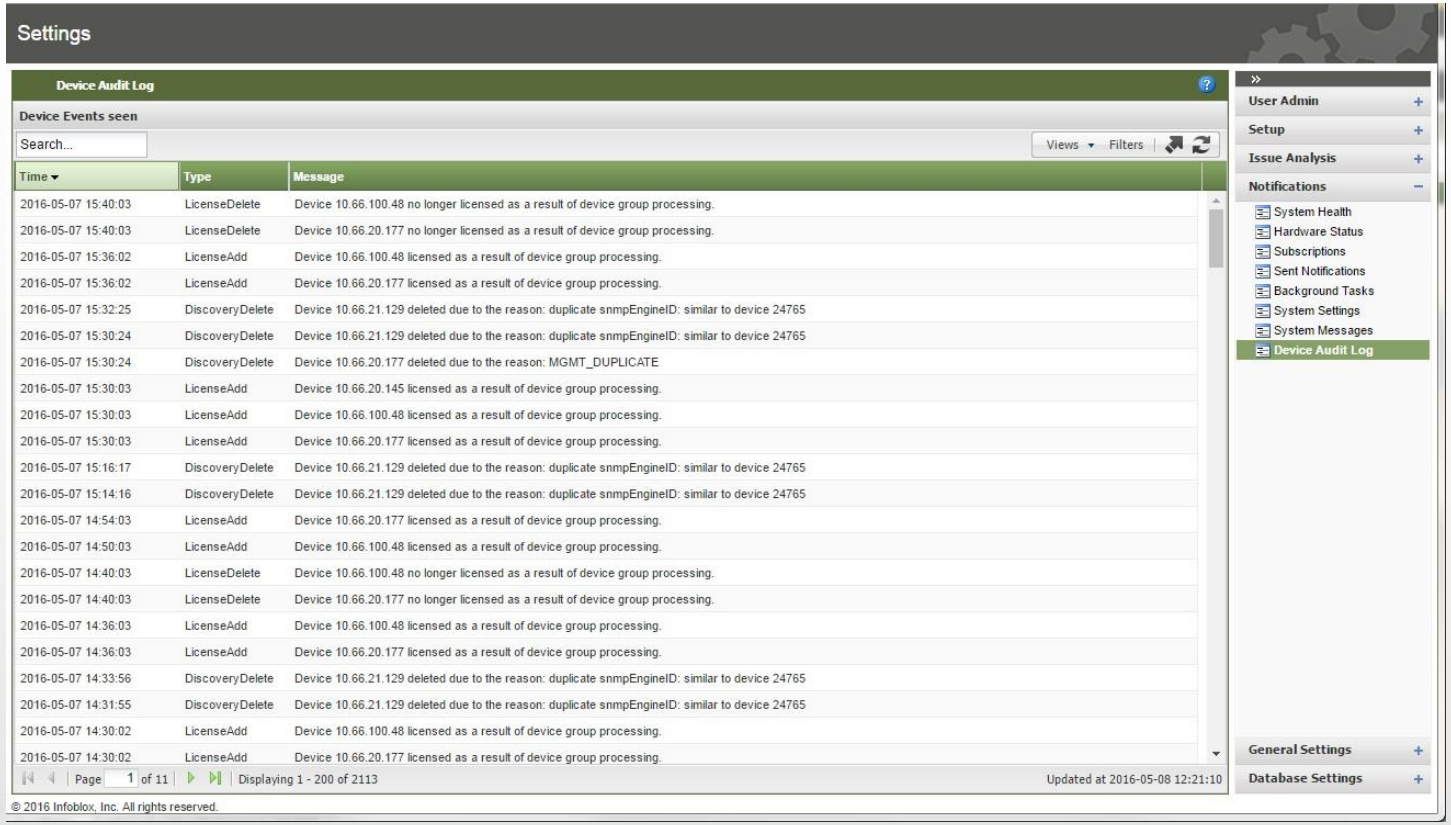
- Discovery Diagnostic
  - Tools → Discovery Diagnostic
  - Device getting mis-identified
  - Gives you a chance to manually try some SNMP strings
  - Support will ask for it



NetMRI Discovery Aids

Tools for troubleshooting

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



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. :)

BLOX FEST

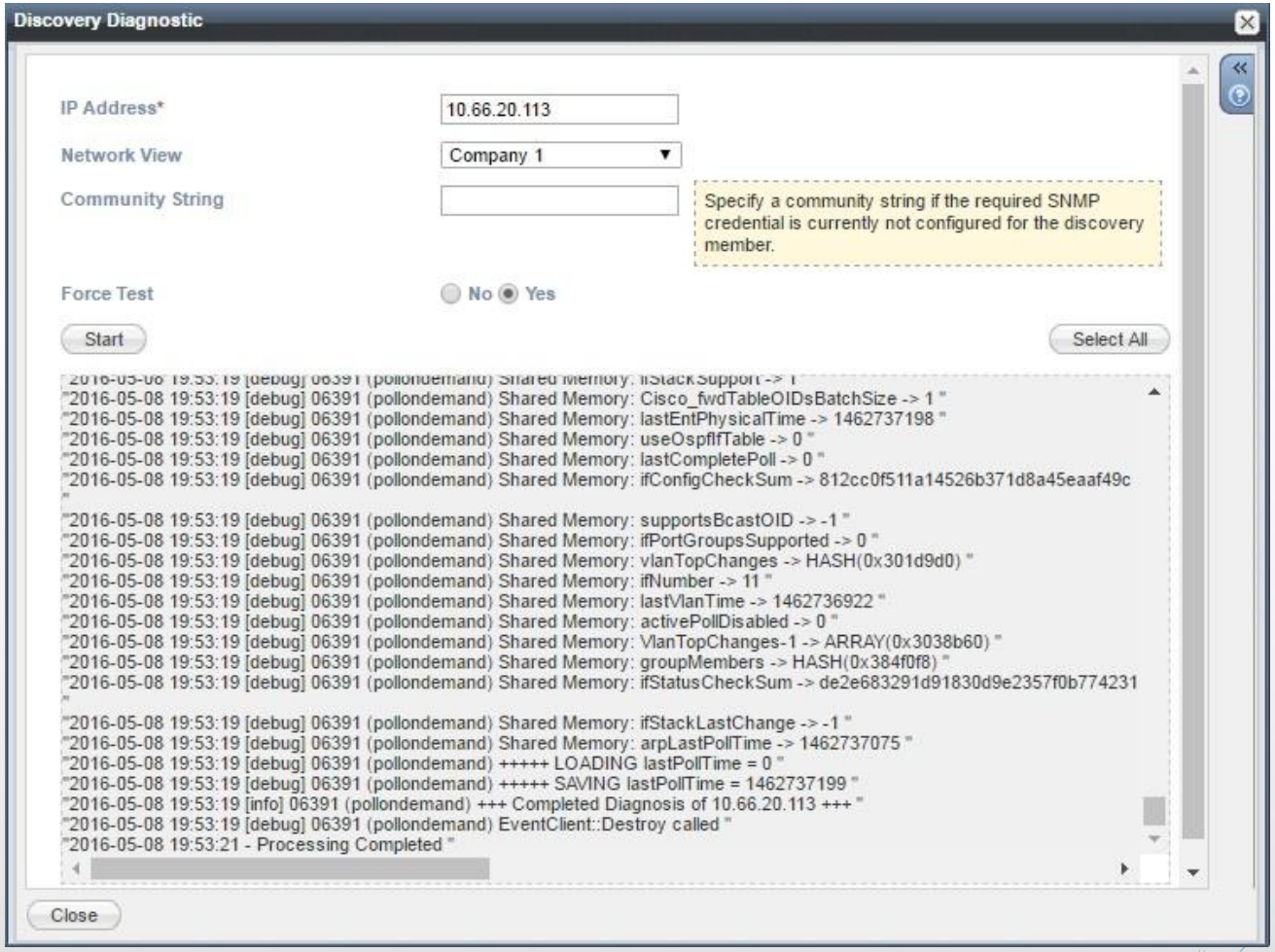
Network Insight Tips and Tricks

- 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

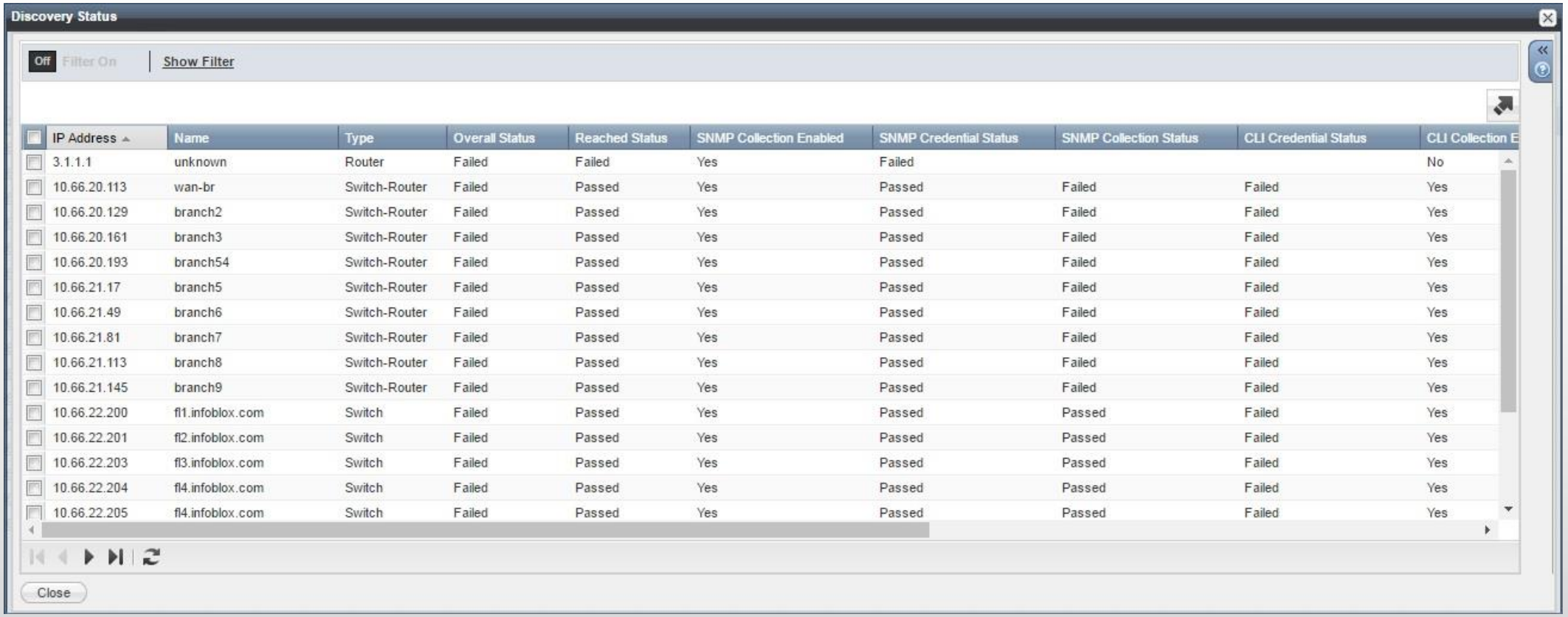
- Discovery Diagnostic



Network Insight Tips and Tricks

Tools for troubleshooting

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



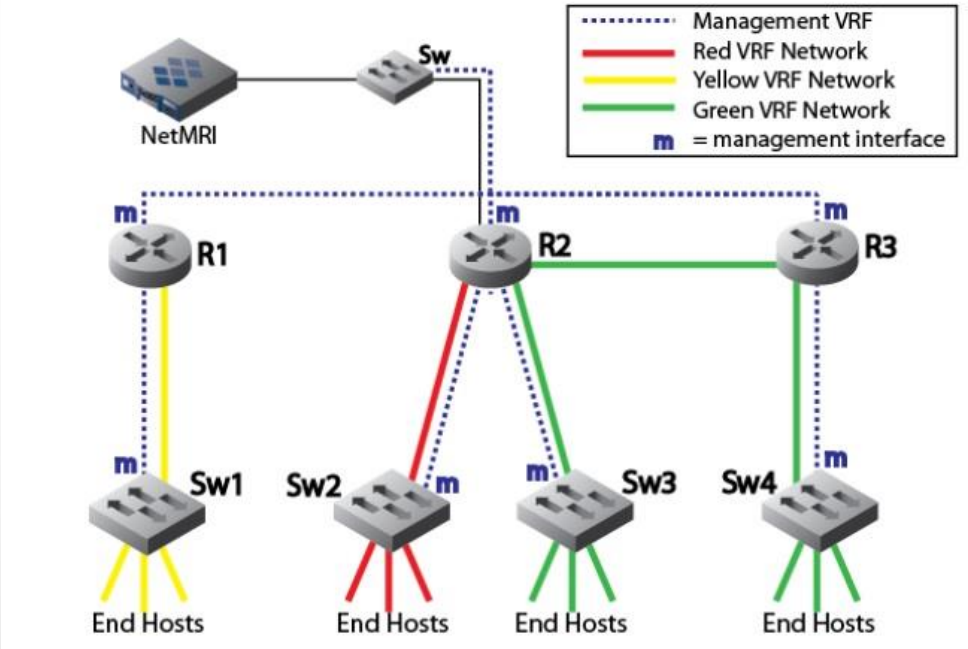
IP Address	Name	Type	Overall Status	Reached Status	SNMP Collection Enabled	SNMP Credential Status	SNMP Collection Status	CLI Credential Status	CLI Collection E
3.1.1.1	unknown	Router	Failed	Failed	Yes	Failed			No
10.66.20.113	wan-br	Switch-Router	Failed	Passed	Yes	Passed	Failed	Failed	Yes
10.66.20.129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

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