



# **Avaya Visualization Performance and Fault Manager — Discovery Best Practices**

2.3  
NN48014-105  
01.02  
June 2011

## Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

## Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

## Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

## Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

## Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

## Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

## Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

## Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

## Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: <http://support.avaya.com>.

## Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://support.avaya.com>.

# Contents

|   |           |
|---|-----------|
| <b>Chapter 1: New in this release</b> .....             | <b>5</b>  |
| Features.....   | <b>5</b>  |
| Avaya VPFM discovery philosophy.....                    | <b>5</b>  |
| Plan your discovery.....                                | <b>6</b>  |
| Discover your network.....                              | <b>6</b>  |
| MIB tables required to discover a device.....           | <b>6</b>  |
| Device clusters.....                                    | <b>6</b>  |
| Discovery of the Switched Firewall.....                 | <b>6</b>  |
| Query of the private ARP cache.....                     | <b>7</b>  |
| Discovery of the Wireless Security Switch.....          | <b>7</b>  |
| Discovery of links.....                                 | <b>7</b>  |
| Device circuits.....                                    | <b>7</b>  |
| Discovery of the Avaya VPN Gateway.....                 | <b>7</b>  |
| Discovery of voice application.....                     | <b>8</b>  |
| Discovery of third party devices.....                   | <b>8</b>  |
| Analysis of Avaya VPFM logs.....                        | <b>8</b>  |
| <b>Chapter 2: Introduction</b> .....                    | <b>9</b>  |
| <b>Chapter 3: Avaya VPFM discovery philosophy</b> ..... | <b>11</b> |
| <b>Chapter 4: Plan your discovery</b> .....             | <b>13</b> |
| <b>Chapter 5: Discover your network</b> .....           | <b>15</b> |
| Supplying credentials for a discovery.....              | <b>15</b> |
| Configuring a seed for a discovery.....                 | <b>17</b> |
| Excluding a device from discovery.....                  | <b>18</b> |
| MIB tables for a device discovery.....                  | <b>19</b> |
| Discovery of clusters.....                              | <b>20</b> |
| Switched Firewall discovery.....                        | <b>21</b> |
| Discovering devices behind the Switched Firewall.....   | <b>22</b> |
| Wireless Security Switch discovery.....                 | <b>23</b> |
| Discovery of links.....                                 | <b>23</b> |
| Device circuits in Avaya VPFM.....                      | <b>24</b> |
| Avaya VPN Gateway discovery.....                        | <b>24</b> |
| Voice application discovery.....                        | <b>25</b> |
| Discovery of third party devices.....                   | <b>26</b> |
| Analyzing Avaya VPFM logs.....                          | <b>26</b> |



# Chapter 1: New in this release

The following section details what's new in *Avaya Visualization Performance and Fault Manager Discovery Best Practices* (NN48014–105) for release 2.2.

---

## Features

See the following sections for information about features.

- [Avaya VPFM discovery philosophy](#) on page 5
- [Plan your discovery](#) on page 6
- [Discover your network](#) on page 6
- [MIB tables required to discover a device](#) on page 6
- [Device clusters](#) on page 6
- [Discovery of the Switched Firewall](#) on page 6
- [Query of the private ARP cache](#) on page 7
- [Discovery of the Wireless Security Switch](#) on page 7
- [Discovery of links](#) on page 7
- [Device circuits](#) on page 7
- [Discovery of the Avaya VPN Gateway](#) on page 7
- [Discovery of voice application](#) on page 8
- [Discovery of third party devices](#) on page 8
- [Analysis of Avaya VPFM logs](#) on page 8

---

## Avaya VPFM discovery philosophy

Review the best practices philosophy for Avaya Visualization Performance and Fault Manager (Avaya VPFM) discovery, including an overview of the standards that Avaya VPFM offers for a best-in-class discovery and monitoring solution for your network. For more information, see [Avaya VPFM discovery philosophy](#) on page 11.

---

## Plan your discovery

Before you start your discovery, it is important to plan your discovery with Avaya VPFM. For more information, see [Plan your discovery](#) on page 13.

---

## Discover your network

To accurately discover your network with Avaya VPFM, there is a sequence of procedures to follow. For more information, see [Supplying credentials for a discovery](#) on page 15, [Configuring a seed for a discovery](#) on page 17, and [Excluding a device from discovery](#) on page 18.

---

## MIB tables required to discover a device

To discover a device, Avaya VPFM requires three standard Management Information Bases (MIB) tables. For more information, see [MIB tables for a device discovery](#) on page 19 .

---

## Device clusters

Avaya VPFM can discover more than one hardware unit that make up a device cluster, which is managed with a single Management IP. For more information, see [Discovery of clusters](#) on page 20.

---

## Discovery of the Switched Firewall

For Avaya VPFM to discover the Switched Firewall, Simple Network Management Protocol (SNMP) configurations are required. For more information, see [Switched Firewall discovery](#) on page 21.

---

## Query of the private ARP cache

Avaya VPFM can discover devices behind the Switched Firewall by performing a query of the private Address Resolution Protocol (ARP) cache of the Switched Firewall device. For more information, see [Discovering devices behind the Switched Firewall](#) on page 22.

---

## Discovery of the Wireless Security Switch

Avaya VPFM can discover multiple Internet Protocol (IP) addresses belonging to a device to create one element for the device. For more information, see [Wireless Security Switch discovery](#) on page 23.

---

## Discovery of links

Avaya VPFM uses three protocols to discover links. For more information, see [Discovery of links](#) on page 23.

---

## Device circuits

Avaya VPFM creates device circuits, that contain other devices and end notes, to complete your network topology map. For more information, see [Device circuits in Avaya VPFM](#) on page 24.

---

## Discovery of the Avaya VPN Gateway

After the management station IP address is provided as an SNMP manager to the device, Avaya VPFM can discover Virtual Private Network (VPN) routers. For more information, see [Avaya VPN Gateway discovery](#) on page 24.

---

## Discovery of voice application

Avaya VPFM discovers IP deskphones by querying the open ports on the required devices after an IP address does not respond to SNMP. For more information, see [Voice application discovery](#) on page 25.

---

## Discovery of third party devices

Avaya VPFM discovers and manages any device that responds to ping and SNMP if the device implements standard MIBs. For more information, see [Discovery of third party devices](#) on page 26.

---

## Analysis of Avaya VPFM logs

You can view logs related to a discovery on the Discovery Problem Reports page. For more information, see [Analyzing Avaya VPFM logs](#) on page 26.



# Chapter 2: Introduction

*Avaya Visualization Performance and Fault Manager Discovery Best Practices* (NN48014–105) is a new document. This document describes the best practices guidelines for discovery using Avaya Visualization Performance and Fault Manager (Avaya VPFM) to discover your network.

*Avaya Visualization Performance and Fault Manager Discovery Best Practices* (NN48014–105) contains information on the following topics:

- [Avaya VPFM discovery philosophy](#) on page 11
- [Plan your discovery](#) on page 13
- [Discover your network](#) on page 15



# Chapter 3: Avaya VPFM discovery philosophy

This chapter describes the philosophy of Avaya Visualization Performance and Fault Manager (Avaya VPFM) discovery.

## **Heterogeneous**

Avaya VPFM is a best-in-class discovery and monitoring solution for networks consisting of Avaya devices, and devices from various vendors.

## **Standards based**

To achieve heterogeneity, Avaya VPFM is completely standards based in its approach to discovery. That is, VPFM uses MIB-2 Management Information Bases (MIB) as opposed to enterprise specific MIBs whenever possible. For more information, see [MIB tables for a device discovery](#) on page 19.

## **Easy segregation and management**

Avaya VPFM uses domains to contain the topology and monitoring data for a discovery. You can create multiple domains in VPFM, which permits you to discover and manage portions of your network independent of other portions.

## **Adapting to your network**

If devices do not implement standard link discovery protocols, Avaya VPFM uses a weighted algorithm for inferring links. The more traffic that is present between these devices, which equates to more entries in the neighboring switches Forwarding database (FDB) tables, the better the accuracy with which VPFM performs the inference.



# Chapter 4: Plan your discovery

To achieve the best results from Avaya Visualization Performance and Fault Manager (Avaya VPFM), it is important to plan your discovery before starting a discovery with Avaya VPFM.

The following is a list of points to consider when planning a discovery.

- Decide on the parts of the network you want to discover.
- Choose a seed router, any layer-3 device, from which all parts of your network are reachable either directly or indirectly.
- If a subnet does not have any layer-3 device, provide the subnet itself as a seed.
- Avaya VPFM can perform WAN crawls across the supported devices; for example, Contivity devices and Avaya Secure Routers. But, if the connectivity is across a service provider network, then you must provide a seed device from the remote networks, in addition to the seed you have already specified.
- Specify how far you want the discovery to reach out to by providing subnet limits.
- If there are any device types or specific devices you want to exclude from discovery, specify these in the exclusions criteria.
- Make sure that autotopology, such as SynOptics Network Management Protocol (SONMP) and Cisco Discovery Protocol (CDP), is enabled on all the devices that support these protocols.
- If you have an out-of-band network setup for management, ensure that the devices Address Resolution Protocol (ARP) cache reflects the out-of-band addresses. Otherwise, VPFM tries to access the devices using the in-band addresses, if these are present in the ARP cache.

Plan your discovery

# Chapter 5: Discover your network

To accurately discover your network with Avaya Visualization and Fault Manager (Avaya VPFM) at a high level, perform the following procedures in the order they appear.

- Provide the Simple Network Management Protocol (SNMP) and Telnet device credentials in Avaya Unified Communications Management (Avaya UCM). For more information, see [Supplying credentials for a discovery](#) on page 15.
- Create a discovery domain and provide the discovery seed. For more information, see [Configuring a seed for a discovery](#) on page 17.
- Configure the subnet limits and any exclusions. For more information, see [Excluding a device from discovery](#) on page 18.

For other information relevant to discovering your network, see the following sections.

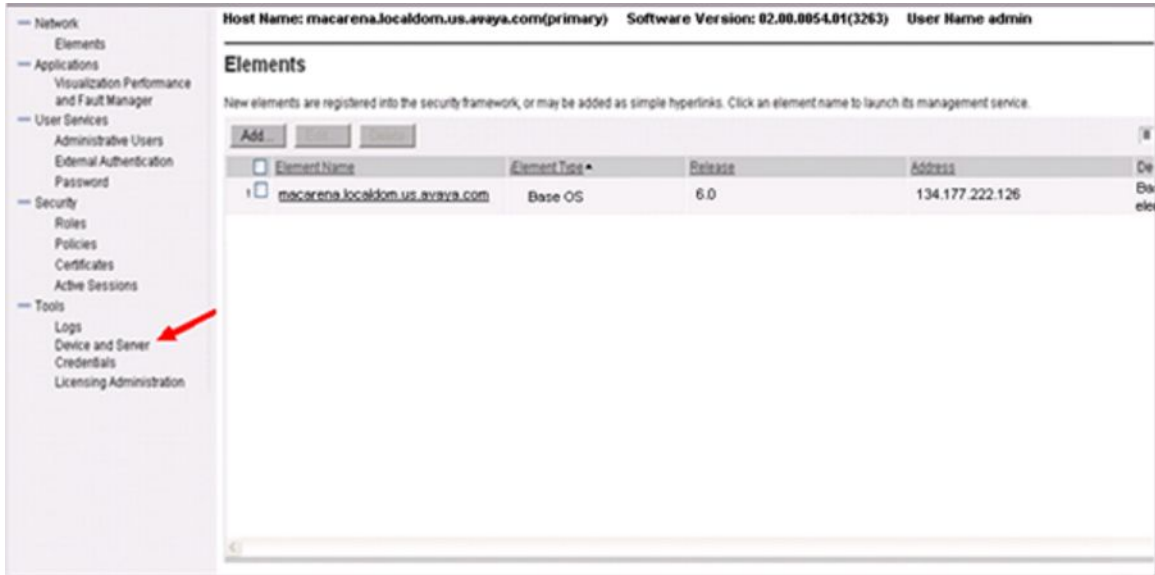
- [MIB tables for a device discovery](#) on page 19
- [Discovery of clusters](#) on page 20
- [Switched Firewall discovery](#) on page 21
- [Discovering devices behind the Switched Firewall](#) on page 22
- [Wireless Security Switch discovery](#) on page 23
- [Discovery of links](#) on page 23
- [Device circuits in Avaya VPFM](#) on page 24
- [Avaya VPN Gateway discovery](#) on page 24
- [Voice application discovery](#) on page 25
- [Discovery of third party devices](#) on page 26
- [Analyzing Avaya VPFM logs](#) on page 26

---

## Supplying credentials for a discovery

Before starting a discovery, you must supply SNMP, and in some cases, Telnet credentials for all the devices that you are required to discover and manage using Avaya VPFM.

To supply credentials for a discovery, navigate to the Avaya UCM Device Credentials page, as shown in the following figure.



**Note:**

Avaya VPFM uses a seed to begin the search for devices within your network, using an Address Resolution Protocol (ARP) cache, and communicates with all these devices to discover their properties and connectivity. Therefore you must supply credentials for your discovery seed, and for all devices within your network that you are required to discover and manage with VPFM.

No credentials are provided by default (for example, SNMP v1/v2c credentials of public/private for \*.\*.\* must be entered).

To enable an SNMP v3 based discovery, make sure that you provide only the SNMP v3 credentials for the device. If you provide SNMP v1 credentials, VPFM uses only the v1 credentials during discovery.

Avaya VPFM requires SNMP (v1, v2c, and v3) credentials to discover most devices in your network. In some cases, VPFM goes beyond SNMP and uses other protocols such as, Telnet, Common Information Model (CIM), Port Scanning, and Windows logon credentials for a more accurate discovery.

Avaya VPFM uses Telnet for discovering and associating Internet Protocol (IP) deskphones to their registered Avaya Communication Server 1000 (Avaya CS 1000) Signaling Servers. Avaya VPFM uses the CIM for associating IP deskphones to their registered Avaya Business Communications Manager (Avaya BCM) systems. For discovery of Wireless Local Area Network (WLAN) access points and IP deskphones, VPFM scans for open ports on those devices. For more information, see [Voice application discovery](#) on page 25.

For discovering Windows servers, VPFM uses the Windows logon credentials provided.



## Configuring a seed for a discovery

To discover your network with Avaya VPFM, provide the seed routers or seed subnets that VPFM uses to contact the devices requiring discovery. The discovery seeds can accompany any exclusions that are provided in the Discovery Configuration page as shown in the following figure.

| Element Type | Prev. | Last | Merged |
|--------------|-------|------|--------|
| Device       | 0     | 6    | 6      |
| Manageable   | 0     | 6    | 6      |
| Router       | 0     | 0    | 0      |
| Switch (L2)  | 0     | 0    | 0      |
| Switch (L3)  | 0     | 6    | 6      |
| Server       | 0     | 0    | 0      |
| Other        | 0     | 0    | 0      |
| Unmanageable | 0     | 0    | 0      |
| Phone        | 0     | 0    | 0      |
| Interface    | 0     | 283  | 283    |

### \* Note:

Avaya recommends that you do not use overly large subnet seeds for discovery.

Avaya recommends that you use router seeds, and only use subnet seeds in situations when they are the actual LAN in the network or when a layer-3 device is not present in the network to be discovered.

If you specify more than one subnet-based seed, some of subnet-based seeds are ignored if one of the seeds results in the discovery of a router which has routing interfaces in the other subnets.

For example: The subnet seeds specified are 10.127.1.0/24, 10.127.2.0/24 and 10.127.3.0/24. If the first seed results in the discovery of a router, such as 10.127.1.1 which also has an interface 10.127.3.1, then the 10.127.3.0/24 is ignored. Avaya VPFM discovers the network using the routing interface ARP entries.

You must specify a subnet-based seed or provide other router seeds for the subnets you want discovered.

The following table outlines the recommended seeds based on the network topology.

| Topology  | Recommended seed  |
|---|---|
| Layered topology containing Core, Distribution and Access Switches                            | One of the core or distribution switches (must be a layer-3 switch or a router)         |
| Pure Layer-2 network (no layer-3 device)  | Provide the entire subnet as the seed; for example, 10.127.22.0/24                      |
| Remote networks without supported WAN routers (like Avaya Secure Router or Avaya VPN Gateway) | In addition to the seed for the main office, provide a seed in the remote site as well. |

## Excluding a device from discovery

In some situations, certain devices may need to be excluded from discovery. Reasons to exclude a device from discover include, bad SNMP agents that cause loops during discovery, devices that send incomplete traps that cause issues with the Avaya VPFM trap browser, and multiple Virtual Router Redundancy Protocol (VRRP) addresses showing up as unmanaged causing clutter on the Network Browser.

To exclude devices from discovery, in the Discovery Configuration page, provide the IP addresses of the devices, as shown in the following figure.

The screenshot shows the 'Network Discovery' configuration page. On the left, there are sections for 'Seeds' (containing 10.127.233.2), 'Limit to Subnets' (containing 10.127.233.0/24), 'Exclusions' (highlighted with a red arrow), and 'Options' (with checkboxes for Wide Area Crawl, VPN Crawl, DNS Lookup, and Avaya Only Discovery). On the right, there is a 'Discovery Status Summary' table and a 'Campuses' table.

| Field           | Value                                 |
|-----------------|---------------------------------------|
| As of           | 22:51:55                              |
| Discovery State | Completed                             |
| Discovery Level | Initial Discovery                     |
| Start Time      | Friday, September 04, 2009 5:04:17 PM |
| End Time        | Friday, September 04, 2009 5:04:33 PM |

| Element Type | Prev. | Last | Merged |
|--------------|-------|------|--------|
| Device       | 0     | 6    | 6      |
| Manageable   | 0     | 6    | 6      |
| Router       | 0     | 0    | 0      |
| Switch (L2)  | 0     | 0    | 0      |
| Switch (L3)  | 0     | 6    | 6      |
| Server       | 0     | 0    | 0      |
| Other        | 0     | 0    | 0      |
| Unmanageable | 0     | 0    | 0      |
| Phone        | 0     | 0    | 0      |
| Interface    | 0     | 283  | 283    |

To exclude a device from discover, all the IP interfaces of the device must be in the exclusion list. If you do not enter all the interfaces in the exclusion list, a device intended for exclusion may be discovered if any of the other interfaces fall in the discovery range.

To prevent device circuits, containing VRRP IP addresses and other unmanaged devices, from appearing in the topology, specify Unmanaged Devices as an exclusion criteria for discovery.

## MIB tables for a device discovery

For Avaya VPFM to discover a device completely and reach out to other devices within the subnet, VPFM requires the following Management Information Bases (MIB) tables to be implemented on each device.

Avaya VPFM requires the following standard (MIB-2) MIB tables for a device discovery.

### Interfaces Table (ifTable)

Avaya VPFM uses the Interfaces Table (ifTable) for discovering physical interfaces (ports) of a device.

The following figure is an example of an Interfaces Table.

| .mgmt.mib-2.interfaces.ifTable.ifEntry |         |                             |                   |       |         |                   |               |              |                    |            |               |
|--|---------|-----------------------------|-------------------|-------|---------|-------------------|---------------|--------------|--------------------|------------|---------------|
| ifIndex                                | ifIndex | ifDescr                     | ifType            | ifMtu | ifSpeed | ifPhysAddress     | ifAdminStatus | ifOperStatus | ifLastChange       | ifInOctets | ifInUcastPkts |
| .64                                    | 64      | 10/100BaseTX Port 1/1 Name  | ethernetCsmacd(6) | 1950  | 0       | 00:e0:7b:b0:48:00 | up(1)         | down(2)      | 0 days, 0:00:17.00 | 0          | 0             |
| .65                                    | 65      | 10/100BaseTX Port 1/2 Name  | ethernetCsmacd(6) | 1950  | 0       | 00:e0:7b:b0:48:01 | up(1)         | down(2)      | 0 days, 0:00:17.00 | 0          | 0             |
| .66                                    | 66      | 10/100BaseTX Port 1/3 Name  | ethernetCsmacd(6) | 1950  | 0       | 00:e0:7b:b0:48:02 | up(1)         | down(2)      | 0 days, 0:00:17.00 | 0          | 0             |
| .67                                    | 67      | 10/100BaseTX Port 1/4 Name  | ethernetCsmacd(6) | 1950  | 0       | 00:e0:7b:b0:48:03 | up(1)         | down(2)      | 0 days, 0:00:17.00 | 0          | 0             |
| .68                                    | 68      | 10/100BaseTX Port 1/5 Name  | ethernetCsmacd(6) | 1950  | 0       | 00:e0:7b:b0:48:04 | up(1)         | down(2)      | 0 days, 0:00:17.00 | 0          | 0             |
| .69                                    | 69      | 10/100BaseTX Port 1/6 Name  | ethernetCsmacd(6) | 1950  | 0       | 00:e0:7b:b0:48:05 | up(1)         | down(2)      | 0 days, 0:00:17.00 | 0          | 0             |
| .70                                    | 70      | 10/100BaseTX Port 1/7 Name  | ethernetCsmacd(6) | 1950  | 0       | 00:e0:7b:b0:48:06 | up(1)         | down(2)      | 0 days, 0:00:17.00 | 0          | 0             |
| .71                                    | 71      | 10/100BaseTX Port 1/8 Name  | ethernetCsmacd(6) | 1950  | 0       | 00:e0:7b:b0:48:07 | up(1)         | down(2)      | 0 days, 0:00:17.00 | 0          | 0             |
| .72                                    | 72      | 10/100BaseTX Port 1/9 Name  | ethernetCsmacd(6) | 1950  | 0       | 00:e0:7b:b0:48:08 | up(1)         | down(2)      | 0 days, 0:00:17.00 | 0          | 0             |
| .73                                    | 73      | 10/100BaseTX Port 1/10 Name | ethernetCsmacd(6) | 1950  | 0       | 00:e0:7b:b0:48:09 | up(1)         | down(2)      | 0 days, 0:00:17.00 | 0          | 0             |
| .74                                    | 74      | 10/100BaseTX Port 1/11 Name | ethernetCsmacd(6) | 1950  | 0       | 00:e0:7b:b0:48:0a | up(1)         | down(2)      | 0 days, 0:00:17.00 | 0          | 0             |
| .75                                    | 75      | 10/100BaseTX Port 1/12 Name | ethernetCsmacd(6) | 1950  | 0       | 00:e0:7b:b0:48:0b | up(1)         | down(2)      | 0 days, 0:00:17.00 | 0          | 0             |

### IP Addresses Table (ipAddrTable)

Avaya VPFM uses the IP Addresses Table (ipAddrTable) for discovering all the IP interfaces of a device. In conjunction with the ifTable, VPFM uses the ipAddrTable to map IP addresses to actual physical interfaces (by using an index value in both tables).

Any mismatches or inability to associate an IP interface with a physical interface could result in inconsistent discoveries.

The following figure is an example of an IP Addresses Table.

| .mgmt.mib-2.ip.AddrTable.ipAddrEntry |              |                |                |                  |                     |
|--------------------------------------|--------------|----------------|----------------|------------------|---------------------|
| ipAdEntAddr                          | ipAdEntAddr  | ipAdEntIfIndex | ipAdEntNetMask | ipAdEntBcastAddr | ipAdEntReasmMaxSize |
| .8.8.8.1                             | 8.8.8.1      | 2051           | 255.255.255.0  | 1                | 1500                |
| .10.4.20.12                          | 10.4.20.12   | 320            | 255.255.255.0  | 1                | 1500                |
| .10.127.22.12                        | 10.127.22.12 | 2049           | 255.255.255.0  | 1                | 1500                |

### ARP Cache (ipNetToMediaTable)

The ARP Cache (ipNetToMediaTable), is queried on all routing interfaces to find all IP addresses within a routing interface subnet (Layer-2). Avaya VPFM then tries to discover this set of IP addresses.

Address Resolution Protocol (ARP) cache entries are dynamic in nature and expire routinely if certain elements (mostly end nodes) are not discovered consistently.

The following figure is an example of an ARP Cache Table.

| .mgmt.mib-2.ip.ipNetToMediaTable.ipNetToMediaEntry |                     |                         |                        |                  |
|--|---------------------|-------------------------|------------------------|------------------|
| ipNetToMediaIfIndex, ipNetToMediaNetAddress        | ipNetToMediaIfIndex | ipNetToMediaPhysAddress | ipNetToMediaNetAddress | ipNetToMediaType |
| .2049.10.127.22.1                                  | 402720769           | 00:80:2d:c7:1a:15       | 10.127.22.1            | dynamic(3)       |
| .2049.10.127.22.2                                  | 402720769           | 00:e0:7b:88:9a:00       | 10.127.22.2            | dynamic(3)       |
| .2049.10.127.22.3                                  | 402720769           | 00:80:2d:ac:9a:00       | 10.127.22.3            | dynamic(3)       |
| .2049.10.127.22.12                                 | 2049                | 00:e0:7b:b0:4a:00       | 10.127.22.12           | other(1)         |
| .2049.10.127.22.13                                 | 402655233           | 00:e0:7b:c9:5e:00       | 10.127.22.13           | dynamic(3)       |
| .2049.10.127.22.90                                 | 402720769           | 00:01:02:74:0e:59       | 10.127.22.90           | dynamic(3)       |
| .2049.10.127.22.102                                | 402720769           | 00:e0:7b:a8:9a:00       | 10.127.22.102          | dynamic(3)       |
| .2049.10.127.22.103                                | 402720769           | 00:01:81:28:7e:00       | 10.127.22.103          | dynamic(3)       |
| .2049.10.127.22.112                                | 402720769           | 00:04:38:96:a2:00       | 10.127.22.112          | dynamic(3)       |
| .2049.10.127.22.113                                | 402720769           | 00:0e:40:03:92:00       | 10.127.22.113          | dynamic(3)       |
| .2049.10.127.22.122                                | 402655233           | 00:01:02:74:14:1f       | 10.127.22.122          | dynamic(3)       |
| .2049.10.127.22.133                                | 403572737           | 00:01:02:73:fe:60       | 10.127.22.133          | dynamic(3)       |
| .2049.10.127.22.255                                | 2049                | ff:ff:ff:ff:ff:ff       | 10.127.22.255          | other(1)         |
| .2051.8.8.8.1                                      | 2051                | 00:e0:7b:b0:4a:01       | 8.8.8.1                | other(1)         |
| .2051.8.8.8.2                                      | 402655235           | 00:e0:7b:c9:5e:01       | 8.8.8.2                | dynamic(3)       |
| .2051.8.8.8.255                                    | 2051                | ff:ff:ff:ff:ff:ff       | 8.8.8.255              | other(1)         |

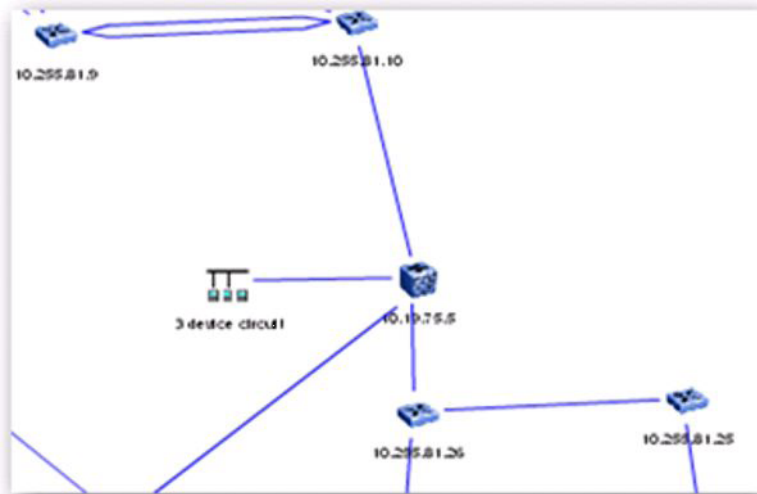
## Discovery of clusters

Avaya VPFM 2.3 discovers device clusters as single devices. Device clusters are typically comprised of more than one hardware unit, managed with a single Management IP. Traps from device clusters are handled correctly, as long as they are received from the same management IP that was discovered. This is true even if a failover happens after discovery.

Because clusters are not discovered as separate components, links to the multiple components may not be fully and correctly discovered.

Some examples of such clusters are the Switched Firewall cluster (comprised of director and accelerator appliances) and Secure Network Access clusters. In the case of the Switched Firewall cluster, only links to the Master accelerator component are discovered.

In the following figure, the firewall device 10.19.75.5 is connected to 10.255.81.10 and 10.255.81.26. In the network, the firewall device is connected to 10.255.81.25 and 10.255.81.9 as well, but VPFM shows the connectivity only to the switches connected to the master accelerator.




---

## Switched Firewall discovery

To discover the Switched Firewall discovery device successfully, you must configure the following SNMP configuration options on the device:

- `/cfg/sys/adm/snmp/adv/allinfy`

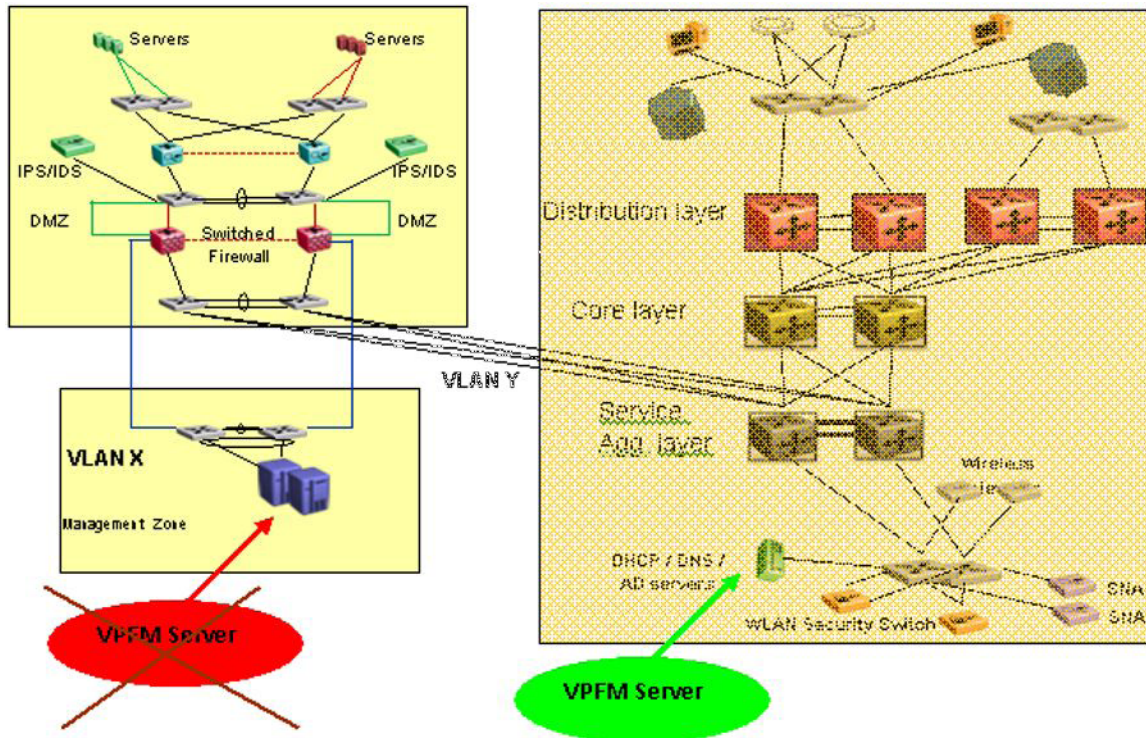
Ensures that the Switched Firewall can respond to SNMP requests sent to any of its IP addresses.

- `/cfg/sys/adm/snmp/adv/getsrcip auto`

Sets the source IP of the SNMP response to that of the outgoing interface. You must ensure that the IP address of the Switched Firewall that Avaya VPFM sends the SNMP request to, is the outgoing interface through which the SNMP response is sent. For this purpose, Avaya recommends that you place the server hosting the VPFM service appropriately with respect to the Switched Firewall device.

The following diagram demonstrates an Switched Firewall discovery.





In the preceding diagram, the VPFM Server is placed in Virtual Local Area Network (VLAN) X with the Switched Firewall interface (the VPFM Server default gateway). After VPFM learns the IP address of the firewall in VLAN Y from the routers in the Distribution (Core or Service Aggregation) layer—one of these was selected as the seed route), VPFM attempts to send SNMP requests to the VLAN Y interface of the firewall. The firewall responds to the VPFM server through the VPFM outgoing interface in VLAN X. A mismatch in the destination and source IP addresses in the SNMP request and response occurs, and VPFM ignores the responses from the Switched Firewall and does not discover the device.

To correct the mismatch in the destination and source IP addresses in the SNMP request and response, choose one of the following options:

- Place the VPFM server in VLAN Y.
- Provide a seed router from VLAN X (if available) so that VPFM learns about the Switched Firewall VLAN X interface.

## Discovering devices behind the Switched Firewall

To discover the devices behind the firewall, Avaya VPFM queries the private ARP cache of the Switched Firewall device. To ensure that the SNMP query does not time out (causing the non-discovery of some of the devices), the Switched Firewall device must operate software 4.2.6.0 or later. You can obtain the latest Switched Firewall image from the Avaya Support Web Site: <http://www.avaya.com/support>.

---

## Wireless Security Switch discovery

Avaya VPFM discovers each of the IP addresses of the Wireless Security Switch (WSS) device as a separate element, because the WSS device does not implement the ipAddrTable MIB (IP Address Table). Avaya VPFM requires the ipAddrTable MIB to identify multiple IP addresses belonging to a device and to create only one element for the device. In the absence of the ipAddrTable MIB, VPFM is unable to identify the IP addresses as belonging to a single device and ends up creating multiple elements.

Avaya VPFM may not discover the links between the WSS and the switch that WSS is connected to, because the WSS device does not provide forwarding database (FDB) information through SNMP. Avaya VPFM attempts to use only the FDB information from the connected switch to draw the link, but the operational state of the WSS interfaces may prevent VPFM from drawing the link.

Avaya VPFM can still manage and monitor the device.

---

## Discovery of links

Avaya VPFM discovers links using the following three protocols:

- Avaya SONMP (s5EnMsTopNmmEosTable MIB)
- LLDP (802.1ab)
- FDB inference (dot1dTpFdbTable MIB)

The following table outlines the Avaya devices that support SONMP and LLDP (802.1ab).

| Device type                  | SONMP | LLDP (802.1ab) |
|------------------------------|-------|----------------|
| ERS 25xx                     | Yes   | Yes            |
| ERS 45xx                     | Yes   | Yes            |
| ERS 55xx                     | Yes   | Yes            |
| ERS 56xx                     | Yes   | Yes            |
| ERS 16xx                     | Yes   | No             |
| ERS 83xx                     | Yes   | Yes            |
| ERS 86xx                     | Yes   | No             |
| Wireless LAN Security Switch | No    | No             |

| Device type                         | SONMP | LLDP (802.1ab) |
|-------------------------------------|-------|----------------|
| Secure Network Access Switch (SNAS) | Yes   | No             |

For devices that do not implement SynOptics Network Management Protocol (SONMP) or Link Layer Discovery Protocol (LLDP), VPFM uses the FDB table to infer the links. For switches, both the devices FDB tables must have an entry for each other. For links between a switch and an end-node, the switch FDB entries are sufficient.

To accurately discover links with the FDB table inference algorithm, VPFM depends on the presence of traffic on the links, and uses a weighted algorithm; the more traffic that is present (which equates to more entries in the neighboring switches FDB tables), the better the accuracy with which VPFM can perform the inference.

## Device circuits in Avaya VPFM

On a regular basis, Avaya VPFM creates device circuits; objects that contain other devices and end-nodes.

Device circuits complete your network topology map. Avaya VPFM uses device circuits to ensure that all discovered devices are available in the topology map, and places the device circuits in the correct network.

Device circuits are created when there is no logical information (SONMP, LLDP, or FDB entries) to connect a device or end-node to a switch. Device circuits are created based on routing interface ARP information, which is why device circuits are always attached to a layer-3 device and never to a layer-2 switch.

If there is more than one routing interface for the subnet, there is no definite way to know which routing interface the device circuits are attached to.

 **Note:**

If devices have multiple VRRP addresses, VPFM discovers some of the addresses separately as unmanaged devices that end up in device circuits. To remove unwanted device circuits, add Unmanaged devices to the exclusion list in your discovery seed configuration.

## Avaya VPN Gateway discovery

For discovery of Virtual Private Network (VPN) routers, ensure that the management station IP address is provided as an SNMP manager to the device (by using the Business Element



Manager), and that SNMP MIBs (specifically the Tunnel MIB) are enabled in the Business Element Manager.

The following figure is an example of the Avaya VPN Gateway Business Element Manager page.

**SNMP IDENTITY**

|             |                             |
|-------------|-----------------------------|
| sysDescr    | CES V04_85.120              |
| sysObjectid | 01.03.06.01.04.01.2505.1100 |
| sysName     | CES 1100                    |
| sysContact  | ENSM LAB                    |
| sysLocation | SC100-03 Rack-E10           |

**SNMP-GET HOST**

| Enable                              | Host Name or IP Address | Community Name | Status      |
|-------------------------------------|-------------------------|----------------|-------------|
| <input checked="" type="checkbox"/> | 134.177.222.158         | public         | Operational |
| <input checked="" type="checkbox"/> | 134.177.222.220         | public         | Operational |
| <input checked="" type="checkbox"/> | 134.177.222.33          | public         | Operational |
| <input checked="" type="checkbox"/> | 10.127.10.165           | public         | Operational |
| <input checked="" type="checkbox"/> | 134.177.222.145         | public         | Operational |
| <input checked="" type="checkbox"/> | 10.127.10.144           | public         | Operational |

**MIBs**

| Enable                              | MIB Name  | Description                          |
|-------------------------------------|-----------|--------------------------------------|
| <input checked="" type="checkbox"/> | IP Tunnel | (RFC2667) Tunnel statistics          |
| <input checked="" type="checkbox"/> | RIPV2     | (RFC1724) RIPV2 statistics           |
| <input checked="" type="checkbox"/> | OSPF      | OSPF Statistics                      |
| <input checked="" type="checkbox"/> | VRRP      | VRRP Statistics                      |
| <input checked="" type="checkbox"/> | IPX       | IPX Statistics                       |
| <input checked="" type="checkbox"/> | RIPSAP    | RIPSAP Statistics                    |
| <input checked="" type="checkbox"/> | DSU/CSU   | DSU/CSU Configuration and Statistics |

## Voice application discovery

Avaya VPFM discovers Avaya IP deskphones by querying open ports on the IP deskphones, not SNMP.

After an IP address does not respond to SNMP, VPFM queries the device to check if certain ports are open.

You can identify Avaya IP deskphones by the following open ports: 5000, and 5001.

The Avaya Secure Router 4134 (Avaya SR 4134) can include a VoIP module. To ensure that VPFM discovers and lists the VoIP module as a Voice Application in VPFM, enter telnet

credentials for the Avaya SR 4134 on the Avaya Unified Communications Manager (Avaya UCM) credentials page.

To associate the discovered IP deskphones with their respective Avaya Communication Server 1000 (Avaya CS 1000) systems, ensure that you enter the telnet credentials for the Signaling Server in the Avaya UCM credentials page.

To associate the discovered IP deskphones with their respective Avaya Business Communications Manager (Avaya BCM) systems, make sure that the CIM credentials are entered for the Avaya BCM in the Avaya UCM credentials page.

---


## Discovery of third party devices

Avaya VPFM discovers and manages any device that responds to ping and SNMP. The only requirement is that third party devices implement standard MIBs (also called MIB-2 MIBs) to ensure that VPFM accurately discovers and connects the third party devices in the topology.

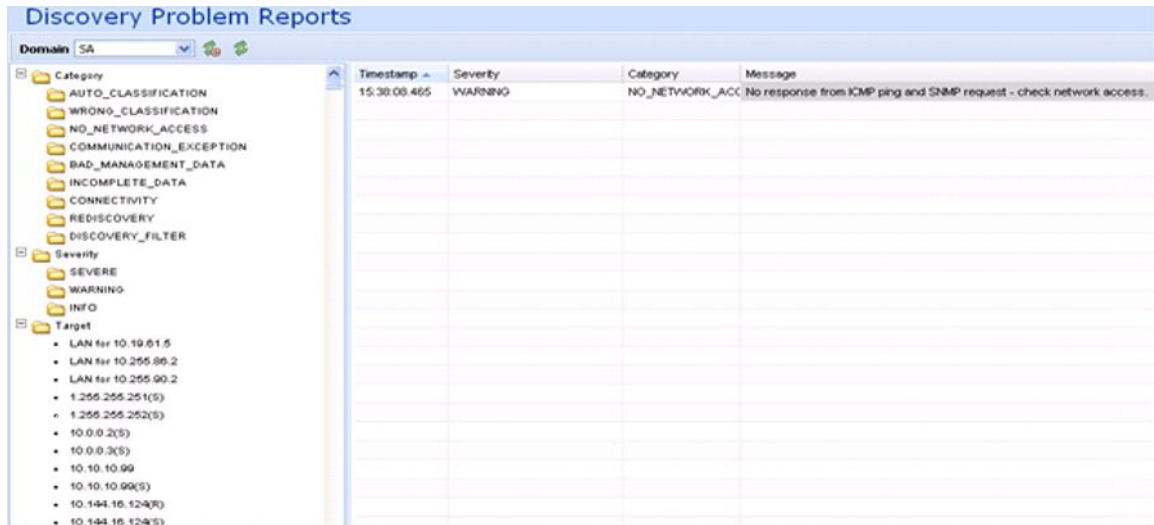
Because of various differences in the way certain configurations, such as clustering, are implemented in different devices, the devices are exposed through enterprise MIBs (non-standard MIBs). There is no guarantee that VPFM can accurately discover and visualize these configurations in the VPFM topology maps.

---

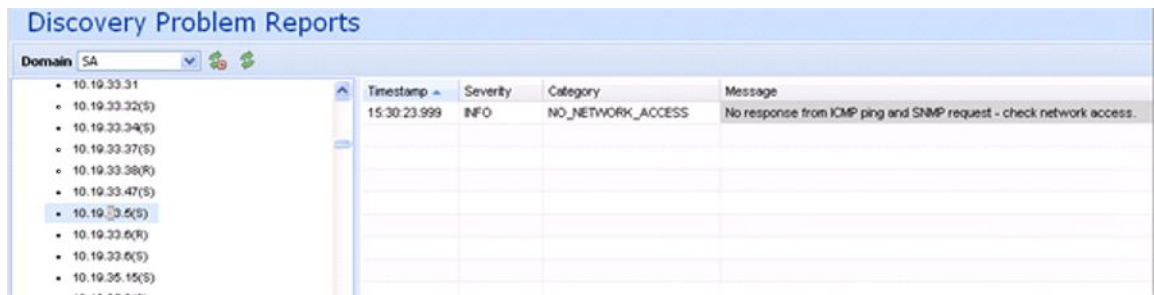
## Analyzing Avaya VPFM logs

To view logs related to a discovery, on the toolbar of the Network Discovery page, click on the  button. A Discovery Problem Reports page appears.

The following is an example of a Discover Problem Reports page.



The left hand navigation pane on the Discovery Problem Reports page organizes log messages based on category, severity, and IP address.



To troubleshoot why a particular IP address is not discovered or is discovered as unmanaged, locate the IP address in the left navigation pane.

One common reason for not discovering a device is the lack of response from the device from ping or SNMP requests sent from Avaya VPFM. In this case, check the UCM device credentials to make sure they are correct.

If the credentials are correct, then check for SNMP access using the SNMP MIB browser.

Some of the common messages that you encounter in the logs are as follows:

- Device did not respond to SNMP or ICMP

If the device does not respond to SNMP or ICMP, then perform the following procedures:

- Check if the device responds to ping.
- Check if the device responds to SNMP from the VPFM MIB browser.
- Check with Wireshark to determine if the device is sending back a response.
- If all of the above is occurring, check UCM credentials and rerun the discovery
- Potential managed device was excluded from discovery

If the potential managed device is excluded from discovery, then perform the following procedures:

- Check discovery constraints to ensure that the device IP is not excluded by subnet limits or other constraints
- You may also see this message, or a similar message, if the topology table of one device includes this device, but this device is not found in the ARP table of any of the routers in that subnet. In this case, check the ARP table of the routers and fix any related issues. Avaya VPFM discovers a device only if the device is found in the ARP table.
- There is no log entry for an undiscovered device
  - Make sure that UCM credentials exist for that IP and that they are correct
  - Make sure that the device's IP address is present in the ARP tables of one or more discovered layer-3 devices in your network.