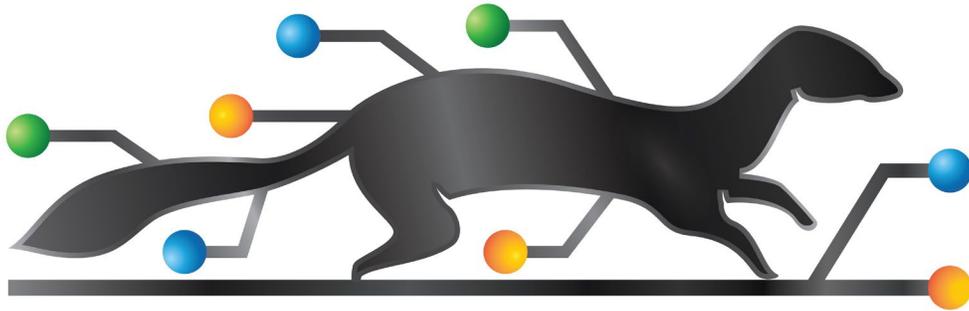


Network Ferret™

MIB Dump Manager

V18



Contents

1: What Is MIB Dump Manager	1
NMS Shops Collect Dumps	1
How To Make Sense Of It All	1
What Questions Can MDM Answer?	1
2: Quick Start.....	2
Installation	2
Sample Database.....	2
Start MDM	2
See The Features In The Dump	3
Which Dumps Have The IPv6 table	3
How Do Two or More Dumps Compare	3
View The Dump Data.....	4
Do The First Scan	4
3: Scanning	5
nfMIBDumpManager.def	5
Set The Default nfMIBDumpManager.def File	6
Set The Root Directory	6
Scan Everything	6
Save The Database.....	7
Scan For New Dumps	7
Scan For A Random OID	7
Scan A Random File	8
4: Definition File.....	9
Section 1 - Substitutions.....	9
Section 2 - Features	10
Section 3 - Vendors.....	11
Section 4 – MIB Simulator.....	12
Section 5 – Extensions.....	13
XML Files.....	13
Section 6 – Ignore	14
5: Filters.....	15
Features Filter	15
Containing Filters	15
Notes Filter	15
No Translated Vendor	15
6: Dump Actions	16
Compare Dump Features	16
View The Dump Data	18
Extract Features From A Dump.....	19
Open the Dump File in a Text Editor	19
Various Copy Actions	20
Which Project Use This Dump.....	20
Generate Simulator Devices	20



7: Feature Actions	21
Which Dumps Have This Feature.....	21
Which Dumps DO NOT Have This Feature.....	21
Open MIB Analysis.....	22
8: Notes	23
Adding/Editing/Deleting A Note	23
Who Has Notes	23
9: Simulator Integration	24
Setting the Simulator	24
Viewing Projects.....	24
Project <-> Dump Relationship.....	25



1: What Is MIB Dump Manager

NMS Shops Collect Dumps

Any NMS shop whether it is a product shop or a consulting shop is going to collect SNMP MIB Dumps. It is unavoidable.

Dumps are collected to load into a MIB Simulator and test NMS software. Dumps are collected to plan out new features. Dumps are collected when customers have bugs.

How To Make Sense Of It All

Dumps contain a lot of information, most of which is not relevant to a particular problem being solved. MDM allows you to define the tables and variables (Features) that are important to you. MDM then scans all of your dumps and catalogs which dumps contain which features.

MDM allows you to attach Notes to dumps and dump folders to track things like which customer this dump is for or which trouble ticket number this dump is related to.

Use MDM in conjunction with Network Ferret MIB Analysis, to have a powerful toolset to quickly investigate issues.

What Questions Can MDM Answer?

- What Features (tables/variables) are included in this dump?
- Which dumps contain a selected set of features?
- How do the features compare between multiple dumps?
- Which SNMP simulator projects contains this dump?
- Show which dumps are in a simulator project.
- Which dumps match for this sysOID, sysDescr, file name or notes?
- Scan for a random OID and show which dumps contain it.
- How much file space are the dumps taking?
- A dump was just received from a customer, quickly scan it and show what Features (tables/variables) it has.



2: Quick Start

Installation

Unzip the distribution and follow the instructions in the readme. It is necessary to know where the machine's Java installation is.

Sample Database

The distribution comes with a subfolder called dumps which contains a few MIB Dumps and a pre-scanned database.

The database was scanned using the nfMIBDumpManager.def file located in the root directory of the distribution.

Start MDM

Start MDM and do File->Set Root Directory... to the dumps directory in the distribution. MDM consists of two panes. The left pane shows the folder hierarchy of dumps that were scanned. The right pane shows the features defined in nfMIBDumpManager.def.

Select the first Brocade dump on the left.

The screenshot shows the Network Ferret - MIB Dump Manager application. The left pane displays the MIB Dump Hierarchy with the following data:

Folder/Dump Name	N	#F	Size(MB)	Type	Vendor	SysOID	SysDescr
C:\amt_tools\dumps		32	8				
Brocade_1.xml		32	3	XML	Brocade	1991.1.3.55.3.2	Brocade MLXe (System Mode: ...
Brocade_2.xml		20	2	XML	Brocade	1588.3.3.1.164	Brocade VDX Switch, BR-VDX69...
paloAlto.txt		6	1	txt	1.3.6.1.4.1.25461...	25461.2.3.18	Palo Alto Networks PA-3000 ser...
Vyatta.xml		8	2	XML	unknown	30803	

The right pane displays the Features list with the following data:

Feature Name	OID	OID Short
Basic Features		
sysServices	1.3.6.1.2.1.1.7.0	mibII .1.7.0
Interfaces		
ifNumber	1.3.6.1.2.1.2.1.0	mibII .2.1.0
Interfaces	1.3.6.1.2.1.2.2.1	mibII .2.2.1
InterfacesExtended	1.3.6.1.2.1.31.1.1.1	mibII .31.1.1.1
IPAddresses		
IPAddressV4	1.3.6.1.2.1.4.20.1	mibII .4.20.1
IPAddressV6	1.3.6.1.2.1.4.34.1	mibII .4.34.1
IPAddressV6.55	1.3.6.1.2.1.55.1.8.1.2	mibII .55.1.8.1.2
ARP		
ARPv4	1.3.6.1.2.1.4.22.1.2	mibII .4.22.1.2
ARPv6	1.3.6.1.2.1.4.35.1	mibII .4.35.1
ifStack	1.3.6.1.2.1.31	mibII .31
Entity MIB		
V1	1.3.6.1.2.1.47.1.1.1.1.2	mibII .47.1.1.1.1.2
V2	1.3.6.1.2.1.47.1.1.1.1.9	mibII .47.1.1.1.1.9
IF Alias	1.3.6.1.2.1.47.1.3.2.1	mibII .47.1.3.2.1
Virtual IP		
VRRP	1.3.6.1.2.1.68	mibII .68
HSRP	1.3.6.1.4.1.9.9.106.1.2.1.1	private .9.9.106.1.2.1.1
Discovery Protocols		



See The Features In The Dump

The features pane on the right will highlight in green all of the features found in the selected dump.

For example, the dump has the IPv6 table but not the older IPv4 table nor the newer IPv6 table in the .55 branch.

It can also be seen that the device has the VRRP feature but not the HSRP feature.

Which Dumps Have The IPv6 table

Hit the **Clear Selection/Filter button** at the top of the left pane.

Right-click on the IPAddresssv6 row in the Features pane on the right and select **Which Dumps Have This Feature**.

The screenshot shows the Network Ferret - MIB Dump Manager interface. The left pane displays a table of dumps with columns: Folder/Dump Name, N, #F, Size(MB), Type, Vendor, SysOID, and SysDescr. The right pane displays a list of features with columns: Feature Name, OID, and OID Short.

Folder/Dump Name	N	#F	Size(MB)	Type	Vendor	SysOID	SysDescr
▼ C:\amt_tools\dumps	32	8					
Brocade_1.xml	32	3		XML	Brocade	1991.1.3.55.3.2	Brocade MLXe (System Mode: ...
Brocade_2.xml	20	2		XML	Brocade	1588.3.3.1.164	Brocade VDX Switch_BR-VDX69...
paloAlto.txt	6	1		txt	1.3.6.1.4.1.25461...	25461.2.3.18	Palo Alto Networks PA-3000 ser...
Vyatta.xml	8	2		XML	unknown	30803	

Feature Name	OID	OID Short
▼ Basic Features		
sysServices	1.3.6.1.2.1.1.7.0	mibll .1.7.0
▼ Interfaces		
ifNumber	1.3.6.1.2.1.2.1.0	mibll .2.1.0
Interfaces	1.3.6.1.2.1.2.2.1	mibll .2.2.1
InterfacesExtended	1.3.6.1.2.1.31.1.1.1	mibll .31.1.1.1
▼ IPAddresses		
IPAddressV4	1.3.6.1.2.1.4.20.1	mibll .4.20.1
IPAddressV6	1.3.6.1.2.1.4.34.1	mibll .4.34.1
IPAddressV6.55	1.3.6.1.2.1.55.1.8.1.2	mibll .55.1.8.1.2
▼ ARP		
ARPV4	1.3.6.1.2.1.4.22.1.2	mibll .4.22.1.2
ARPV6	1.3.6.1.2.1.4.35.1	mibll .4.35.1
ifStack	1.3.6.1.2.1.31	mibll .31
▼ Entity MIB		
V1	1.3.6.1.2.1.47.1.1.1.1.2	mibll .47.1.1.1.1.2
V2	1.3.6.1.2.1.47.1.1.1.1.9	mibll .47.1.1.1.1.9
IF Alias	1.3.6.1.2.1.47.1.3.2.1	mibll .47.1.3.2.1
▼ Virtual IP		
VRRP	1.3.6.1.2.1.68	mibll .68
HSRP	1.3.6.1.4.1.99.106.1.2.1.1	private .99.106.1.2.1.1
▼ Discovery Protocols		

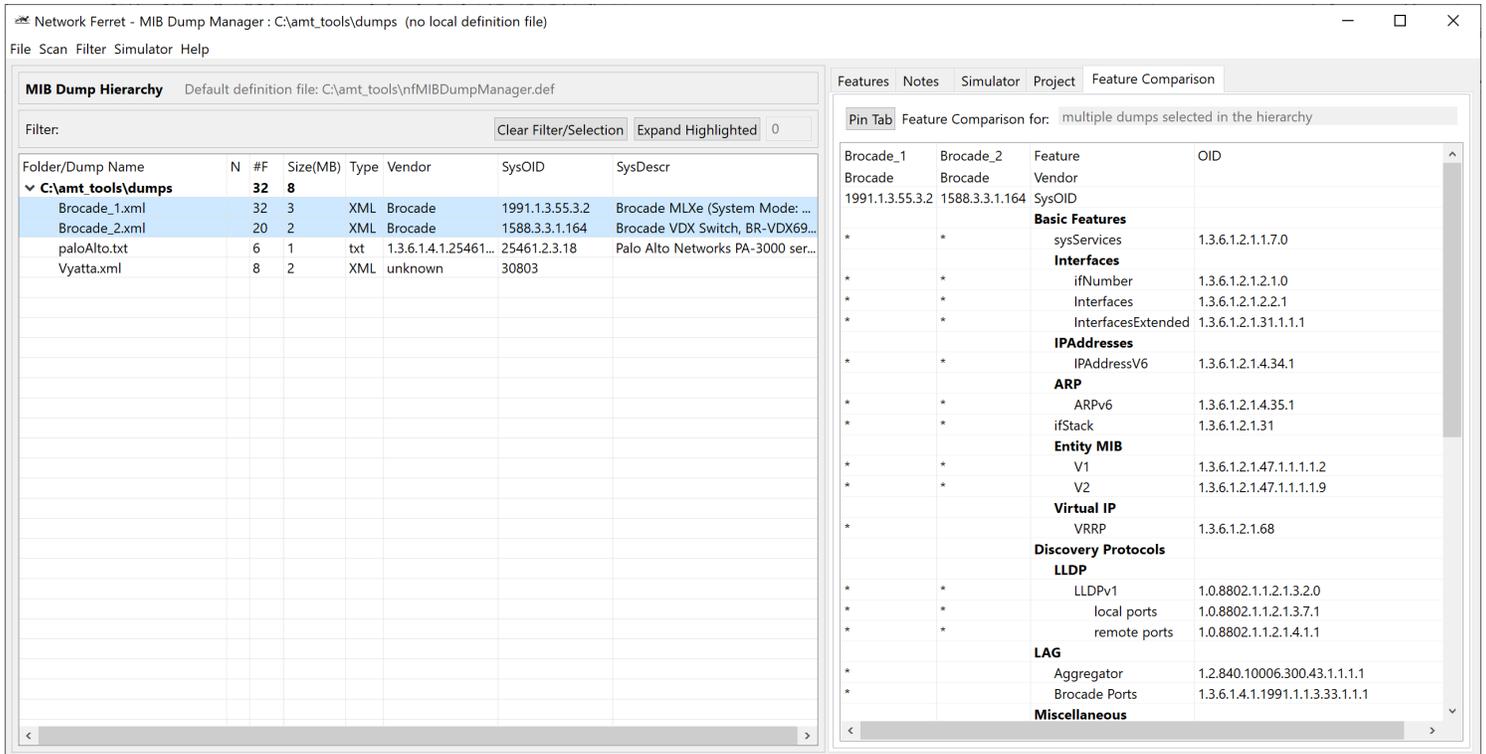
MDM shows that three of the four dumps contain the IPv6 table.

How Do Two or More Dumps Compare

Hit the **Clear Selection/Filter button** at the top of the left pane.

Use CTRL-click to select the two Brocade dumps. Right-click and choose **Compare features between dumps**.





The Feature Comparison tab will activate on the right. This will only show features that at least one dump has.

The example, shows that one Brocade device has the VRRP and LAG features while the other does not.

This is very useful in a situation where a client sends multiple dumps of a network and says, “You are not hooking up everything correctly”. A quick comparison of the features will show which devices have the switch data and the investigation can start there.

View The Dump Data

Right-click on a dump and select **Open File in MIB Analysis**. This will open the Network Ferret – MIB Analysis Tool. This is essentially a MIB Browser on a dump file rather than a running device or simulation.

Of course, MIBs will need to be scanned first or the AMT MIB database can be downloaded.

Do The First Scan

Those are the four main features of MDM. Now you are ready to do your first scan. All of the other features will be discussed later.



3: Scanning

nfMIBDumpManager.def

This is an XML formatted file. Two small parts of this file define what files to scan and what files NOT to scan. The file is in the root directory of the distribution.

Edit the file in any text editor and scroll to the bottom. You can also select **File->Set External Editor** and open the file directly from MDM.

One section defines the file extensions to scan. The other section defines folders and files to ignore.

```
<Extensions>
  <Extension name=".xml"> </Extension>
  <Extension name=".txt"> </Extension>
  <Extension name=".wlk"> </Extension>
</Extensions>

<Ignore>
  <Directory name="OLD"> </Directory>
  <Directory name="mibs"> </Directory>
  <FileName contains="copy"> </FileName>
</Ignore>
```

The rest of the document will be explained later.

The .def file included in the distribution is the actual .def file used at AMT. Network Ferret is a topology discovery engine and that is reflected in the features that are defined.



Set The Default nfMIBDumpManager.def File

Select **File->Set Default Definition File** and select the file in the root of the distribution. This will be remembered between runs of MDM.

The default file can be located anywhere. Any directory that is scanned can also have its own version of this file for purposes of scanning features different from the default.

Set The Root Directory

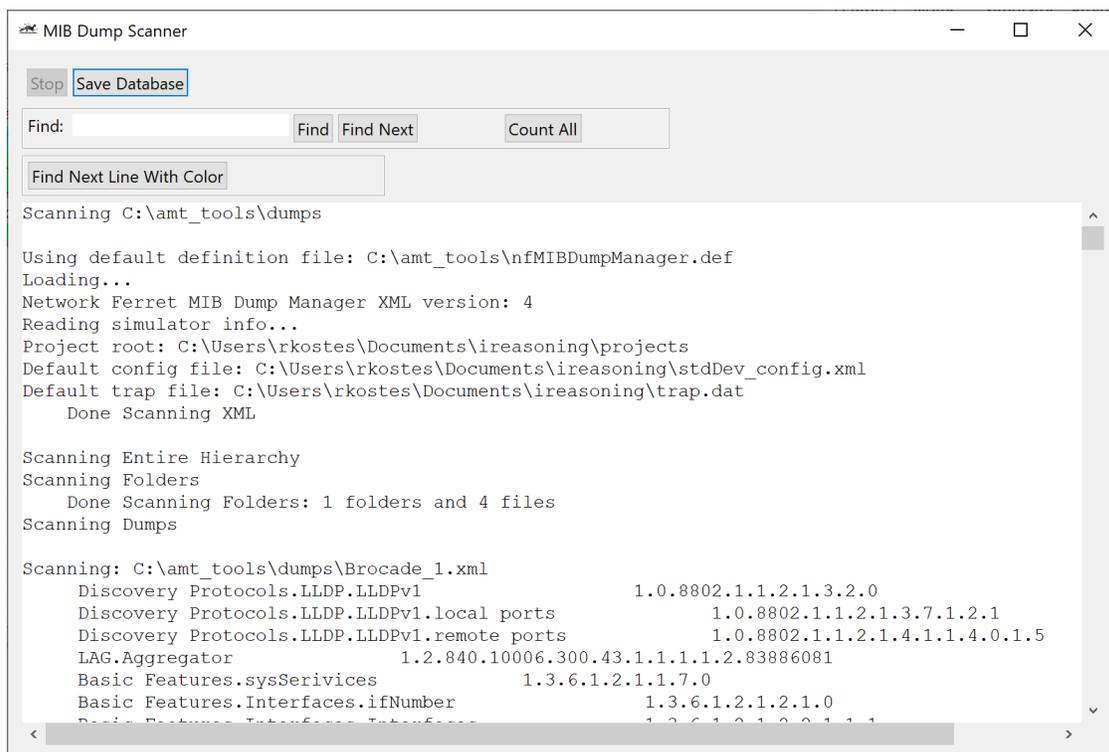
The root directory is where three of the four scan options will work from.

Select **File->Set Root Directory** and choose the directory to be scanned. If a database already exists in that directory, it will be loaded.

Scanning will recursively traverse the directory hierarchy.

Scan Everything

Select **File->Scan All**. The Scanner window open and scanning will commence.



```
MIB Dump Scanner
Stop Save Database
Find: Find Find Next Count All
Find Next Line With Color
Scanning C:\amt_tools\dumps
Using default definition file: C:\amt_tools\nfMIBDumpManager.def
Loading...
Network Ferret MIB Dump Manager XML version: 4
Reading simulator info...
Project root: C:\Users\rkostas\Documents\ireasoning\projects
Default config file: C:\Users\rkostas\Documents\ireasoning\stdDev_config.xml
Default trap file: C:\Users\rkostas\Documents\ireasoning\trap.dat
Done Scanning XML
Scanning Entire Hierarchy
Scanning Folders
Done Scanning Folders: 1 folders and 4 files
Scanning Dumps
Scanning: C:\amt_tools\dumps\Brocade_1.xml
Discovery Protocols.LLDP.LLDPv1 1.0.8802.1.1.2.1.3.2.0
Discovery Protocols.LLDP.LLDPv1.local ports 1.0.8802.1.1.2.1.3.7.1.2.1
Discovery Protocols.LLDP.LLDPv1.remote ports 1.0.8802.1.1.2.1.4.1.1.4.0.1.5
LAG.Aggregator 1.2.840.10006.300.43.1.1.1.1.2.83886081
Basic Features.sysServices 1.3.6.1.2.1.1.7.0
Basic Features.Interfaces.ifNumber 1.3.6.1.2.1.2.1.0
Basic Features.Interfaces.Interface...
```



The scanner window puts out a lot of information. Errors will be in **red**. Warnings will be in **yellow**. Progress/Category will be in **cyan**. The final line will, hopefully, be in **green**. Use the **Find Next Line With Color** button to quickly move through these lines.

Use the Find, Find Next and Count All widgets to do standard text searching.

Save The Database

If satisfied with the scan, hit the Save Database button and close the Scanner window. The database file, **nfMIBDumpManager.dat**, will be placed in the Root Directory that was scanned.

Note that there is nothing in the database that was not scanned from a dump file. So if the database is corrupted, simply delete the file and rescan.

The database file can be moved elsewhere to be browsed. Scans will fail since the database is no longer located with the actual dumps. Notes will function as long as the machine browsing the database has access to the hierarchy containing the dumps.

Scan For New Dumps

Select **File->Scan For New**. The Scanner window open and scanning will commence.

The scanner will look for new files only. It is NOT looking for changes in existing files nor is it looking for files that are no longer there.

The Scan Window will display the results. If **Save Database** is chosen, the hierarchy in the main window will highlight the new files.

Scan For A Random OID

Select **File->Scan Random OID**. Enter the OID to scan for. The Scanner window open and scanning will commence.

Use this option when you quickly want to see which dumps have a Feature (table/variable) that you have not defined in the .def XML file.

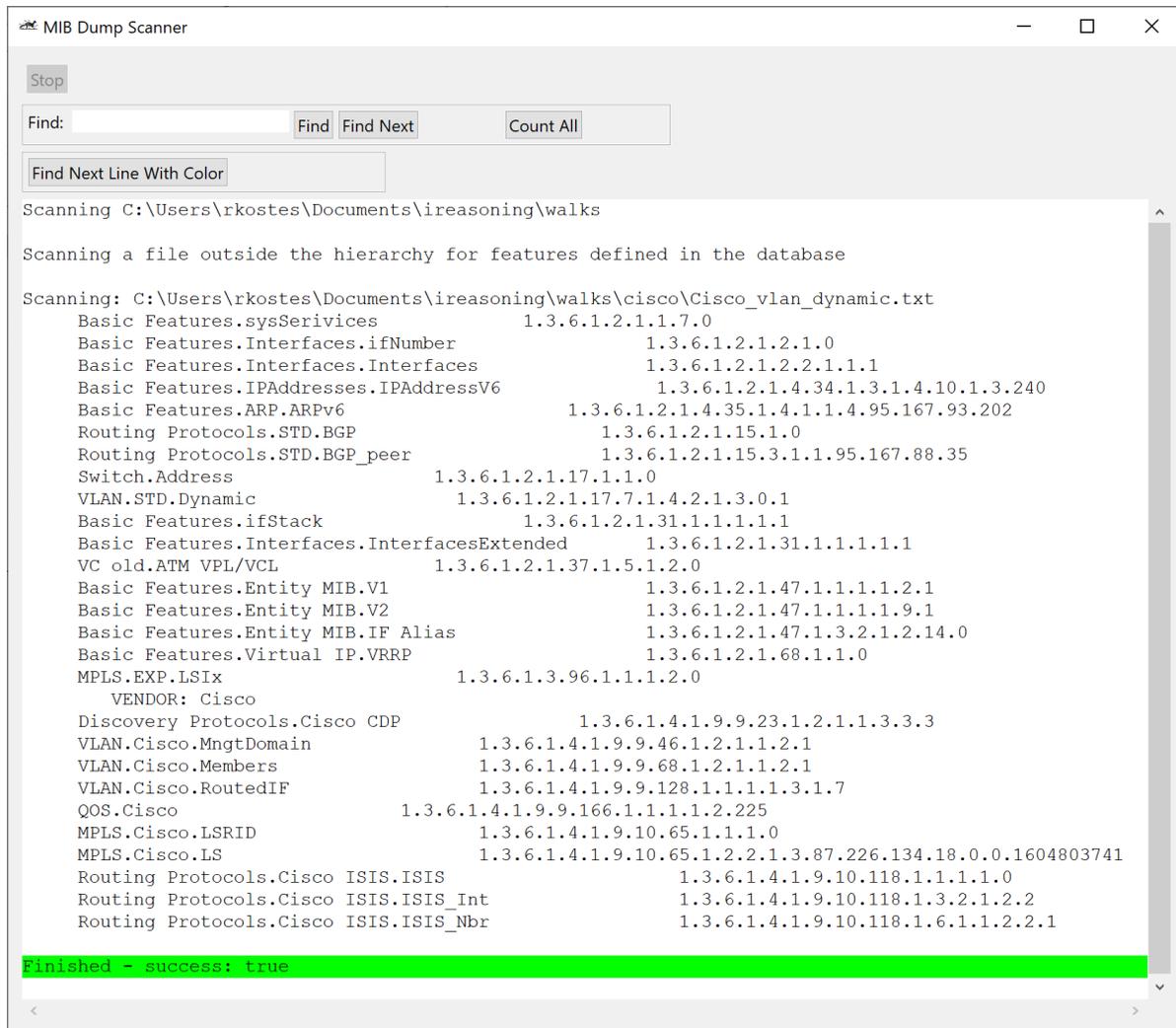
The Scan Window will display the results. There is no Save option. The hierarchy in the main window will highlight any dumps that contain the OID.



Scan A Random File

Select **File->Scan Random File**. Select the file to scan. This file can be anywhere in the system.

The Scanner Window will open and the file will be scanned. There is no option to update the database. The Scanner Window will show the Features (tables/variables) that were found in the file.



The screenshot shows the MIB Dump Scanner application window. At the top, there is a 'Stop' button and a search bar with 'Find', 'Find Next', and 'Count All' buttons. Below the search bar is a 'Find Next Line With Color' button. The main area displays the scan results for the file 'C:\Users\rkostes\Documents\ireasoning\walks\cisco\Cisco_vlan_dynamic.txt'. The results are listed as follows:

```
Scanning C:\Users\rkostes\Documents\ireasoning\walks
Scanning a file outside the hierarchy for features defined in the database
Scanning: C:\Users\rkostes\Documents\ireasoning\walks\cisco\Cisco_vlan_dynamic.txt
Basic Features.sysServices 1.3.6.1.2.1.1.7.0
Basic Features.Interfaces.ifNumber 1.3.6.1.2.1.2.1.0
Basic Features.Interfaces.Interfaces 1.3.6.1.2.1.2.2.1.1.1
Basic Features.IPAddresses.IPAddressV6 1.3.6.1.2.1.4.34.1.3.1.4.10.1.3.240
Basic Features.ARP.ARPv6 1.3.6.1.2.1.4.35.1.4.1.1.4.95.167.93.202
Routing Protocols.STD.BGP 1.3.6.1.2.1.15.1.0
Routing Protocols.STD.BGP_peer 1.3.6.1.2.1.15.3.1.1.95.167.88.35
Switch.Address 1.3.6.1.2.1.17.1.1.0
VLAN.STD.Dynamic 1.3.6.1.2.1.17.7.1.4.2.1.3.0.1
Basic Features.ifStack 1.3.6.1.2.1.31.1.1.1.1.1
Basic Features.Interfaces.InterfacesExtended 1.3.6.1.2.1.31.1.1.1.1.1
VC old.ATM VPL/VCL 1.3.6.1.2.1.37.1.5.1.2.0
Basic Features.Entity MIB.V1 1.3.6.1.2.1.47.1.1.1.1.2.1
Basic Features.Entity MIB.V2 1.3.6.1.2.1.47.1.1.1.1.9.1
Basic Features.Entity MIB.IF Alias 1.3.6.1.2.1.47.1.3.2.1.2.14.0
Basic Features.Virtual IP.VRRP 1.3.6.1.2.1.68.1.1.0
MPLS.EXP.LSIX 1.3.6.1.3.96.1.1.1.2.0
VENDOR: Cisco
Discovery Protocols.Cisco CDP 1.3.6.1.4.1.9.9.23.1.2.1.1.3.3.3
VLAN.Cisco.MngtDomain 1.3.6.1.4.1.9.9.46.1.2.1.1.2.1
VLAN.Cisco.Members 1.3.6.1.4.1.9.9.68.1.2.1.1.2.1
VLAN.Cisco.RoutedIF 1.3.6.1.4.1.9.9.128.1.1.1.1.3.1.7
QOS.Cisco 1.3.6.1.4.1.9.9.166.1.1.1.1.2.225
MPLS.Cisco.LSRID 1.3.6.1.4.1.9.10.65.1.1.1.0
MPLS.Cisco.LS 1.3.6.1.4.1.9.10.65.1.2.2.1.3.87.226.134.18.0.0.1604803741
Routing Protocols.Cisco ISIS.ISIS 1.3.6.1.4.1.9.10.118.1.1.1.1.0
Routing Protocols.Cisco ISIS.ISIS_Int 1.3.6.1.4.1.9.10.118.1.3.2.1.2.2
Routing Protocols.Cisco ISIS.ISIS_Nbr 1.3.6.1.4.1.9.10.118.1.6.1.1.2.2.1
```

Finished ~ success: true



4: Definition File

nfMIBDumpManager.def is an XML format file that defines what MDM will scan for. It has 6 sections. These sections MUST stay in order in the file.

The file in the distribution is the actual file used at AMT. Network Ferret is a topology discovery engine so you will probably need to edit this file heavily to define the Features (tables/variables) that are important to your application.

Section 1 - Substitutions

The substitutions section defines human readable names to replace OID strings. It is important to put the **dot** (.) on the end of the name and the OID.

```
<Substitutions>
  <Substitution name="mib2."          oid="1.3.6.1.2.1.">      </Substitution>
  <Substitution name="exp."          oid="1.3.6.1.3.">      </Substitution>
  <Substitution name="private."      oid="1.3.6.1.4.1.">    </Substitution>
  <Substitution name="mpls."        oid="1.3.6.1.2.1.10.166."> </Substitution>
</Substitutions>
```

Substitutions are used to make Feature definitions easier to read.

```
<Feature name="sysServices"          oid="mib2.1.7.0">      </Feature>
```



Section 2 - Features

Features represent MIB tables or individual variables that are important to your application. This is what is looked for during scanning.

```
<Feature name="Switch">
  <Feature name="Address"          oid="mib2.17.1.1">          </Feature>
  <Feature name="Ports"           oid="mib2.17.1.4.1">       </Feature>
  <Feature name="Forwarding DB"    oid="mib2.17.4.3.1">       </Feature>
  <Feature name="Forwarding DB New" oid="mib2.17.7.1.2.2.1">   </Feature>
  <Feature name="Spanning Tree">
    <Feature name="STD"           oid="mib2.17.2.15.1">      </Feature>
    <Feature name="Huawei"        oid="Huawei.5.25.42.4.1.20"> </Feature>
  </Feature>
</Feature>
```

Logical Features can be created to better organize things. For example, **Switch** and **Spanning Tree** are logical features above. Essentially, folders of Features.

A Logical Feature is permitted to have an OID as well. See the LLDPv1 and LLDPv2 sections of the definition file shipped with the distribution.

Note that **Huawei** above is an example of a Vendor substitution which is explained below.

The top level features will be sorted alphabetically in the MDM window. All other features will appear in the same order as defined in the file.

The graphic below shows how the Feature definition appears in the MDM window.

▼ Switch		
Address	1.3.6.1.2.1.17.1.1	mibll .17.1.1
Ports	1.3.6.1.2.1.17.1.4.1	mibll .17.1.4.1
Forwarding DB	1.3.6.1.2.1.17.4.3.1	mibll .17.4.3.1
Forwarding DB New	1.3.6.1.2.1.17.7.1.2.2.1	mibll .17.7.1.2.2.1
▼ Spanning Tree		
STD	1.3.6.1.2.1.17.2.15.1	mibll .17.2.15.1
Huawei	1.3.6.1.4.1.2011.5.25.42.4.1.20	private .2011.5.25.42.4.1.20



Section 3 - Vendors

This section defines a mapping between a vendor's name and their number in the private branch of the MIB tree.

These names can be used in the Features definition section above. These names will also be used in the Vendor column in the left pane of MDM.

Folder/Dump Name	N	#F	Size(MB)	Type	Vendor	SysOID
> lag_operKeys		22	9			
▼ lldp_onlyOneEnd		33	4			
Cisco_unknown_10.10.10.2.txt		23	2	txt	Cisco	9.1.832
Juniper_Virtual_10.10.10.1.txt		20	2	txt	Juniper	2636.1.1.1.2.31

Below is a sample from the file in the distribution.

```
<Vendors>
  <Vendor name="Brocade"      oid="1588">
  <Vendor name="Brocade"      oid="1991">
  <Vendor name="Cisco"        oid="9">
  <Vendor name="Dell"         oid="674">
  <Vendor name="DLink"        oid="171">
  <Vendor name="Ericsson"     oid="193">
  <Vendor name="Extreme"     oid="1916">
  <Vendor name="Huawei"       oid="2011">
  <Vendor name="Juniper"     oid="2636">
  <Vendor name="Juniper"     oid="4874">
  <Vendor name="NEC"          oid="119">
  <Vendor name="QTech"        oid="27514">
  <Vendor name="SNMPResearch" oid="99">
  <Vendor name="Timetra"     oid="6527">
  <Vendor name="Viptela"     oid="41916">
  <Vendor name="VMWare"      oid="6876">
</Vendors>
```

We consciously did NOT include a line for the many thousands of vendor numbers defined.



Section 4 – MIB Simulator

The purpose of this section is to allow MDM to integrate with MIB Simulators and help to generate config/project file definitions.

This capability will evolve as we get more experience with other simulators. AMT uses iReasoning so MDM ships with a plugin for that product.

```
<!-- Plugin to work with MIB simulators -->
<!-- Currently, the only possible names to use are ireasoning or none -->
<Simulator name="none" root="C:\Users\rkostas\Documents\ireasoning">
  <ireasoning>
    <!-- These are all relative to the root -->
    <projectsRoot      name="projects">      </projectsRoot>
    <defaultConfigFile name="stdDev_config.xml"> </defaultConfigFile>
    <defaultTrapFile   name="trap.dat">      </defaultTrapFile>
  </ireasoning>
</Simulator>
```

If you use iReasoning, change **Simulator name=** to ireasoning and modify the various folders and files.

See the Simulator chapter for a description of what you can do in MDM with iReasoning.



Section 5 – Extensions

The file extensions to be scanned. Network Ferret generates both txt and XML files for each device dump created at a customer site.

The XML files are more verbose so if duplicate files are found and one has a .xml extension, the other file will be scanned. Also, the text files are easier for humans to read if one is opened.

```
<Extensions>
  <Extension name=".xml">           </Extension>
  <Extension name=".txt">          </Extension>
  <Extension name=".wlk">         </Extension>
</Extensions>
```

MDM has a File Size column in the left pane. Each folder adds up the files contained in it. But keep in mind that this may not be an accurate account of the space being taken on disk. Remember that if both a txt and XML version of a file exist, the text version will be scanned and the XML version will not be in the database and thus not counted.

XML Files

MDM expects XML files to use the tags used by iReasoning. If there are other XML formats for dumps, please send us a sample and we will incorporate it.

Technically, MDM is not building the XML object tree when scanning. It is scanning the file looking for three things:

```
<?xml - on the first line of the file
```

```
Lines with oid="someOid"
```

```
<![CDATA[value ]> when trying to extract the
sysDescriptor and sysOID. If the character data is
split across lines, it will not be extracted.
```

Since MIB Analysis needs to extract the values as well as the OIDs, it will build the XML object tree when it loads a dump to be analyzed. It has more specific requirements for the XML format. See that documentation.



Section 6 – Ignore

Directories and files to be ignored. Case does not matter.

```
<Ignore>
  <Directory name="OLD">          </Directory>
  <Directory name="mibs">        </Directory>
  <!-- <FileName contains="" or startsWith="" or endsWith=""> </FileName> -->
  <FileName contains="copy">     </FileName>
</Ignore>
```



5: Filters

MDM provides many filters that will highlight sections of the dump hierarchy.

Features Filter

This is the most powerful filter in MDM. It is set by selecting Features in the right pane (CTRL-click to multiselect), right-clicking and selecting

Which dumps have this feature
or
Which dumps DO NOT have this feature

The dump hierarchy on the left will highlight all of the dumps that contain the feature(s).

Selecting a Feature Folder will include all of the features in that folder and there is an implicit AND operation.

Containing Filters

There are four filters that will do a text search. These are found in the main window menu under Filter. They search against:

The dump file name
The sysDescriptor
The sysOID
Notes – this search is case sensitive

Any dumps passing the search will be highlighted.

Notes Filter

This filter will highlight any dumps/folders that have Notes defined. It does not matter what the Note contains. This Filter is found in the main window menu under Filter.

No Translated Vendor

This filter will highlight any dumps that do not have a Vendor translation in the definition file. This Filter is found in the main window menu under Filter.



6: Dump Actions

The dump hierarchy in the left pane of MDM reflects the file system where the dumps were scanned. There are several things you can do with a single dump or a collection of dumps.

Compare Dump Features

This is a very powerful feature that allows you to quickly analyze a situation and make a plan of action.

Suppose a client sends you a collection of dumps, tells you that things are not hooked up properly and gives you a list of links that should be there. We apologize for all of our examples being about topology but that is what we know here at AMT!

Rather than simply loading the dumps into your simulator and running your application, first scan the dumps into MDM and do a feature analysis.

Right-click on a folder or multi-select specific dumps and select **Compare features between dumps**.

The example below is a big comparison between 10 dumps. It is very easy to see what data is there and what data is missing. This allows you to quickly come up with an investigation plan.

See graphic on next page



View The Dump Data

MDM only handles the OIDs that are in a dump. It knows nothing about the data. But MDM works with the Network Ferret MIB Analysis tool. MA is essentially a MIB Browser on a dump file. Please see that documentation.

Right-click on a MIB Dump and select **Open File in MIB Analysis**.

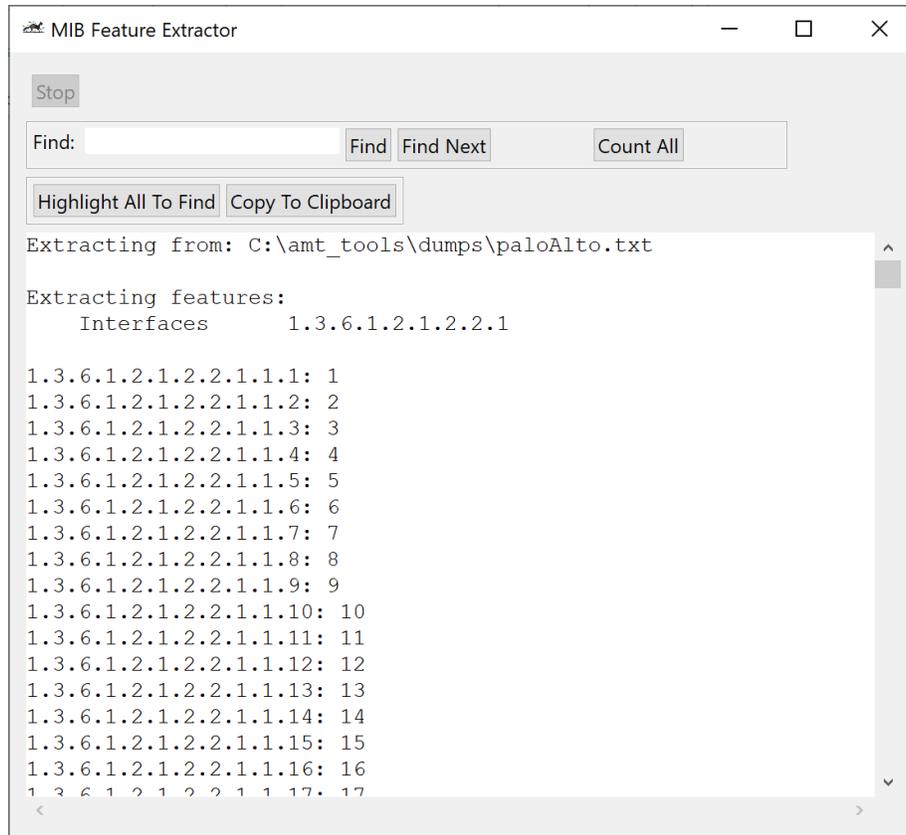
The screenshot shows the Network Ferret - MIB Analysis application. The left pane displays a tree view of MIB databases. The right pane shows a table view for the selected 'ifTable' MIB, displaying details for various interfaces.

Index	ifIndex	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress
1	1	100GigabitEthernet1/1	6	1548	4294967295	0xCC 0x4E 0x24 0x99 0xD1 0x00
2	2	100GigabitEthernet1/2	6	1548	4294967295	0xCC 0x4E 0x24 0x99 0xD1 0x01
65	65	GigabitEthernet2/1	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x30
66	66	GigabitEthernet2/2	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x31
67	67	GigabitEthernet2/3	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x32
68	68	GigabitEthernet2/4	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x33
69	69	GigabitEthernet2/5	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x34
70	70	GigabitEthernet2/6	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x35
71	71	GigabitEthernet2/7	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x36
72	72	GigabitEthernet2/8	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x37
73	73	GigabitEthernet2/9	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x38
74	74	GigabitEthernet2/10	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x39
75	75	GigabitEthernet2/11	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x3A
76	76	GigabitEthernet2/12	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x3B
77	77	GigabitEthernet2/13	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x3C
78	78	GigabitEthernet2/14	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x3D
79	79	GigabitEthernet2/15	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x3E
80	80	GigabitEthernet2/16	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x3F
81	81	GigabitEthernet2/17	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x40
82	82	GigabitEthernet2/18	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x41
83	83	GigabitEthernet2/19	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x42
84	84	GigabitEthernet2/20	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x43
85	85	GigabitEthernet2/21	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x44
86	86	GigabitEthernet2/22	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x45
87	87	GigabitEthernet2/23	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x46
88	88	GigabitEthernet2/24	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x47
129	129	GigabitEthernet3/1	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x60
130	130	GigabitEthernet3/2	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x60
131	131	GigabitEthernet3/3	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x62
132	132	GigabitEthernet3/4	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x63
133	133	GigabitEthernet3/5	6	1548	1000000000	0xCC 0x4E 0x24 0x99 0xD1 0x64



Extract Features From A Dump

After setting a Features Filter by selecting Features in the right pane and then choosing **Which dumps have this feature**, you can right-click on a text dump (not XML) and choose **Extract features from file** to extract those tables/variables from the MIB Dump. Remember that you can always use Network Ferret – MIB Analysis to load the dump and browse all the data.



Open the Dump File in a Text Editor

Sometimes you want to browse the actual dump file. Although Network Ferret – MIB Analysis is much easier.

First, select **File->Set External Editor** to set the editor on your machine.

Second, optionally, select **File->Set File Size Warning**. Dump files can be very large and many times we have sat there and waited while our editor choked on an 80MB text file. Setting this value > 0 will



generate an “Are You Sure” dialog when you try to open a file larger than the warning value.

Right-click on a dump and select **Open file in editor**.

Various Copy Actions

There are various Copy actions to make it easy to add some information to emails or documents. Things like the sysOID or device names, lists of IP addresses, etc.

Which Project Use This Dump

Generate Simulator Devices

See the Simulator chapter for details.



7: Feature Actions

The Feature hierarchy in the right pane of MDM reflects the Features defined in the XML definition file. There are several things you can do with a single feature or a collection of features.

Which Dumps Have This Feature

Suppose a client reports a bug in how your product handles table X. MDM allows you to quickly see which of your dumps has table X so you can start investigating/testing.

Select one or more Features in the features pane, right-click and select **Which dumps have this feature**. Several things will happen:

- 1 – A Feature Filter will be applied to the Dump Hierarchy on the left.
- 2 – The text box to the right of the Expand Highlighted button will show how many dumps pass the filter.
- 3 – Folders and dumps will be highlighted in the Dump Hierarchy.

Optionally, hit the Expand Highlighted button to expand the tree to show every dump that passes the filter.

The screenshot shows the Network Ferret - MIB Dump Manager interface. The left pane displays the 'MIB Dump Hierarchy' with a filter applied: 'Features(1) Discovery Protocols.LLDP.LLDPv1'. The hierarchy shows a folder 'C:\amt_tools\dumps' expanded, with sub-items 'Brocade_1.xml', 'Brocade_2.xml', 'paloAlto.txt', and 'Vyatta.xml'. The right pane shows a list of features with columns for 'Feature Name', 'OID', and 'OID Short'. The 'LLDP' feature is expanded, showing sub-features like 'LLDPv1', 'local ports', 'remote ports', 'LLDPv2', and 'Timetra LLDP'. The 'Hardware' feature is also expanded, showing 'LAG' and 'Aggregator' sub-features.

Folder/Dump Name	N	#F	Size(MB)	Type	Vendor	SysOID	SysDescr
C:\amt_tools\dumps		32	8				
Brocade_1.xml	32	3		XML	Brocade	1991.1.3.55.3.2	Brocade ...
Brocade_2.xml	20	2		XML	Brocade	1588.3.3.1.164	Brocade V...
paloAlto.txt	6	1		txt	1.3.6.1.4.1.25461...	25461.2.3.18	Palo Alto ...
Vyatta.xml	8	2		XML	unknown	30803	

Feature Name	OID	OID Short
Cisco CEF	1.3.6.1.4.1.9.9.492.1.2.2.1	private .9.9.492.1.2.2.1
Extreme EDP	1.3.6.1.4.1.1916.1.13.2.1	private .1916.1.13.2.1
Foundry FDP	1.3.6.1.4.1.1991.1.1.3.20.1.2.1.1	private .1991.1.1.3.20.1.2.1.1
LLDP		
LLDPv1	1.0.8802.1.1.2.1.3.2.0	
local ports	1.0.8802.1.1.2.1.3.7.1	
remote ports	1.0.8802.1.1.2.1.4.1.1	
LLDPv2	1.3.111.2.802.1.1.13.1.3.1.0	
Timetra LLDP		
Hardware		
LAG		
Aggregator	1.2.840.10006.300.43.1.1.1.1	
Aggregator Ports	1.2.840.10006.300.43.1.2.1.1	
Aggregator Ports - ALT	1.2.840.10006.300.43.1.1.2.1	

Which Dumps DO NOT Have This Feature

The inverse of the above filter. Sometimes it is interesting to see which dumps don't have a common Feature such as the Interface Table.



Open MIB Analysis

This is another integration with Network Ferret – MIB Analysis. Right-click on a Feature and select **Open MIB Analysis to this OID**.

This is useful when you need to refresh your memory regarding specific variable definitions/descriptions or enumeration values.

The screenshot shows the Network Ferret - MIB Analysis application window. The left pane displays a tree view of MIB files, with the 'ifTable' entry selected. The right pane shows the details for the selected entry, including its name, OID, type, and index, along with a list of table entries and their descriptions.

Id	Name	MIB Name	File
> 1	iso		
▼ 2	mgmt		
▼ 1	mib-2		
> 1	system	RFC1213-MIB	rfc1213_MIBII.txt
▼ 2	interfaces	IF-MIB	rfc2863.txt
1	ifNumber	IF-MIB	rfc2863.txt
▼ 2	ifTable	IF-MIB	rfc2863.txt
> 1	ifEntry	IF-MIB	rfc2863.txt
> 3	at	RFC1213-MIB	rfc1213_MIBII.txt
> 4	ip	IP-MIB	rfc4293-newIP.txt
> 10	transmission	RFC1213-MIB	rfc1213_MIBII.txt
> 11	snmp	RFC1213-MIB	rfc1213_MIBII.txt
> 14	ospf	RFC1253-MIB	rfc1253-OSPF.txt
> 15	bgp	BGP4-MIB	rfc1657v1.mib.txt
> 17	dot1dBridge	BRIDGE-MIB	rfc4188-bridgeMIBNew.txt
> 31	ifMIB	IF-MIB	rfc2863.txt
> 35	etherMIB	EtherLike-MIB	IETF_ETHERLIKE.mib.txt
> 37	atmMIB	ATM-MIB-v1	ATM-MIB-V1SMI.mib.txt
> 47	entityMIB	ENTITY-MIB	IETF_ENTITY.mib.txt
> 53	vgRptrMIB	DOT12-RPTR-MIB	rfc2266.mib.txt
> 55	ipv6MIB	IPV6-MIB	mib-rfc2465.txt
> 68	vrrpMIB	VRRP-MIB	VRRP-MIB.txt
> 75	fcFeMIB	FIBRE-CHANNEL-FE-MIB	V4_0FE.mib.txt
76	inetAddressMIB	INET-ADDRESS-MIB	IETF_INET_ADDRESS.mib.txt
> 79	ptopoMIB	PTOPO-MIB	rfc2922_physical_topology.txt
> 83	ipMRouteStdMIB	IPMROUTE-STD-MIB	rfc2932-MRoute.txt
84	ianaRtProtoMIB	IANA-RTPROTO-MIB	IANA_RTPROTO.mib.txt
> 85	igmpStdMIB	IGMP-STD-MIB	rfc2933-IGMP.txt
> 100	transportAddressMIB	TRANSPORT-ADDRESS-M...	mib-rfc3419.txt
103	ipv6FlowLabelMIB	IPV6-FLOW-LABEL-MIB	mib-IPV6-FLOW-LABEL-MIB.txt

MIB Detail | Dump Content | Table View

Table variable view options

Show Descriptions Show Full OID Show Type Detail

File name: rfc2863.txt
MIB name: IF-MIB

Variable name: ifEntry
OID: 1.3.6.1.2.1.2.2.1
Type: ENTRY
Index: ifindex }

Table Entries:
=====

Variable name: [1] ifIndex
Type: InterfaceIndex -> Integer32 -> INTEGER
Description: A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."

Variable name: [2] ifDescr
Type: DisplayString -> OCTET STRING
Description: A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the interface hardware/software."

Variable name: [3] ifType
Type: IANAifType -> INTEGER
Description: The type of interface. Additional values for ifType are



8: Notes

If working in a team environment, it is useful to be able to attach notes to Folders or Dumps to indicate things like what trouble ticket is this dump associated with, or what test scenario is this folder associated with or maybe something special about the dump like the data in table X is not formatted to the standard in the MIB definition.

Notes are NOT in the database. Notes are separate files in the file system. Each Note is stored in the same folder as the dump. If your database gets corrupted and a rescan must be done, no Note data is lost because it is not there.

Adding/Editing/Deleting A Note

Adding/Editing a Note is easy. Select a Folder or Dump in the Dump Hierarchy. Select the Notes tab in the Features pane and start typing.

There is no right-click menu but the standard CTRL-X, C and V are available.

Who Has Notes

From the main window menu select **Filter->Dumps with notes** to highlight all of the dumps with Notes.

There is also a Filter for Notes containing a search phrase. This search **is case sensitive**.

The N column in the Dump Hierarchy will have an * for any folder or dump that has a note.



9: Simulator Integration

AMT uses ireasoning as its SNMP Simulator. Since we do topology, we have no need for complex simulations with changing values. We have used Gambit Communications MIMIC in the past and it is also a fine product.

The simulator integration with MDM involves scanning project files, generating project files and understanding what dumps are in which project.

Setting the Simulator

See the Definitions chapter to see how to tell MDM about your simulator location and files.

Viewing Projects

Select the Projects tab in the Features pane on the right. A tree view of the project hierarchy disk will be displayed.

The screenshot shows the Network Ferret - MIB Dump Manager interface. The main window title is "Network Ferret - MIB Dump Manager : C:\Users\rkostos\Documents\ireasoning\walks (no local definition file)". The interface is divided into two main panes. The left pane, titled "MIB Dump Hierarchy", shows a list of folders and dumps with columns for "Folder/Dump Name", "N", "#F", "Size(MB)", "Type", and "Vend". The right pane, titled "Features", has tabs for "Features", "Notes", "Simulator", "Project", and "Feature Comparison". The "Simulator" tab is active, displaying a tree view of project folders and files with columns for "Project Folder/Name", "# Devices", and "# Dups".

Folder/Dump Name	N	#F	Size(MB)	Type	Vend
> ADVA_LAG		15	5		
> brocade		37	26		
> cisco		68	260		
> ConnectionDiscovery		69	88		
> dell_iDRAC		10	2		
> dlink		24	12		
> eltex		16	72		
> ericsson_mw		17	6		
> HP		23	8		
> huawei		48	120		
> huawei_lag		22	4		
> huawei_vlan		17	6		
> ISIS_juniper_cisco		24	2		
> ISIS_juniper_huawei		36	25		
> isisExperimental		24	40		

Project Folder/Name	# Devices	# Dups
> projects		
> cisco		
> Huawei		
> juniper		
isis_inferred.prj	3	
ISIS_STD.prj	2	
Juniper_BGP_NetConf.prj	2	
Juniper_Huawei_LAG_via_LLDP	1	
Juniper_ISIS_NetConf.prj	2	
Juniper_LAG_operKeys.prj	2	
Juniper_LAGMissingPorts.prj	2	
Juniper_misc.prj	13	
Juniper_VLAN_trunks.prj	2	
> timetra		
aaSandbox.prj	1	
ADVA_LAG.prj	1	
Brocade_lab.prj	10	

Double-click on a project and the Project tab will activate with the contents of the project file. The file can be edited here.



Project <-> Dump Relationship

Right-click on a Project and select **Which dumps are in this project**. The Dump Hierarchy on the left will have a project filter applied and all of the dumps in the project will be highlighted. In this case, it is clear that we gave the same name to the simulator project and the folders holding the dumps for the project.

Network Ferret - MIB Dump Manager : C:\Users\rkostas\Documents\ireasoning\walks (no local definition file)

File Scan Filter Simulator Help

MIB Dump Hierarchy Default definition file: C:\amt_tools\nfMIBDumpManager.def

Filter: Simulator Project: Brocade_lab.prj Clear Filter/Selection Expand Highlighted 10

Folder/Dump Name	N	#F	Size(MB)	Type	Vend
> ADVA_LAG		15	5		
> brocade		37	26		
> brocade_lab	*	34	20		
Brocade_172.16.10.10.txt		32	3	XML	Broca
Brocade_172.16.10.11.txt		30	3	XML	Broca
Brocade_172.16.10.2.txt		18	2	XML	unkn
Brocade_172.16.10.51.txt		18	1	XML	Broca
Brocade_172.16.10.52.txt		18	1	XML	Broca
Brocade_172.16.10.53.txt		23	2	XML	Broca
Brocade_172.16.10.54.txt		23	2	XML	Broca
Brocade_172.16.10.56.txt		20	2	XML	Broca
Brocade_172.16.10.59.txt		20	2	XML	Broca
Vyatta_172.16.10.1.txt		8	2	XML	unkn
> fdp		16	6		
> cisco		68	260		

Features Notes Simulator Project Feature Comparison

Project Folder/Name	# Devices	# Dups
> projects		
> cisco		
> Huawei		
> juniper		
isis_inferred.prj	3	
ISIS_STD.prj	2	
Juniper_BGP_NetConf.prj	2	
Juniper_Huawei_LAG_via_LLDP	1	
Juniper_ISIS_NetConf.prj	2	
Juniper_LAG_operKeys.prj	2	
Juniper_LAGMissingPorts.prj	2	
Juniper_misc.prj	13	
Juniper_VLAN_trunks.prj	2	
> timetra		
aaSandbox.prj	1	
ADVA_LAG.prj	1	
Brocade_lab.prj	10	

Conversely, in the Dump Hierarchy, right-click on a dump and select **Which Projects use this dump**.

Network Ferret - MIB Dump Manager : C:\Users\rkostas\Documents\ireasoning\walks (no local definition file)

File Scan Filter Simulator Help

MIB Dump Hierarchy Default definition file: C:\amt_tools\nfMIBDumpManager.def

Filter:

Folder/Dump Name	N	#F	Size(MB)	Type	Vend
> fdp		16	6		
> cisco		68	260		
> CDP_basic	*	42	3		
> CDP_unknownType		23	9		
> CEF_ARP		48	9		
> CFM_TrafficPolicers		23	19		
> CiscoFEX_HPBlade	*	22	17		
> ciscoNX		30	30		
CiscoNX_dualVLANMember.txt		22	3	txt	1.3.6.
CiscoNX_WITH_FEXSerials.txt		27	21	XML	Cisco
CiscoNX_WO_FEXSerials.txt		22	6	XML	Cisco
> ENCS		29	5		
> LAG_inferredFromCDP		48	74		
> LLDP		24	2		
> routedVLAN		20	2		

Features Notes Simulator Project Feature Comparison

Project Folder/Name	# Devices	# Dups
> projects		
> cisco		
Cisco_LAG_EtherChannel.prj	1	
Cisco_LLDP.prj	2	
Cisco_misc.prj	1	
Cisco_TTI_India.prj	26	
CiscoCDP_basic.prj	3	
CiscoCDP_unknownType.prj	1	
CiscoCEF_ARP.prj	2	
CiscoCFM_TrafficPolicers.prj	2	
CiscoENCS.prj	3	
CiscoFEX_HPBlade.prj	4	
CiscoNX_FEXSerials.prj	3	
CiscoRoutedVLAN.prj	2	
test.prj	0	
> Huawei		
> juniper		

