Devices and Interfaces

When NetMRI performs Discovery on devices in the network for the first time, they're organized into Device Groups and Interface Groups, using common-sense networking terms. Device Groups and Interface Groups are the primary organizational units in NetMRI. You can create device groups in a nested structure, with some device groups subordinate to other device groups. You can apply device group membership criteria in the same ways with nested device groups as for device groups from earlier releases of NetMRI, which used a flat data structure and enforced all device groups as existing on the same peer level. You can now create a hierarchical list of device groups, comprised of top-level groups, with child device groups subordinate to them, with child device groups further subordinate to their parent groups. For information, see Creating Device Groups.

NetMRI uses device groups to organize device discovery results, generate separate scorecards, filter issues and to manage polling and processing for each device in the network. Device groups also offer control of Switch Port Management processes, including the ability to immediately carry out Switch Port polling in a device group.

Device groups can also be used for suppression of Issue reporting across sets of devices, and to modify the thresholds used by NetMRI for raising chosen issues. The use of Device Group suppression removes the need for manually suppressing undesirable issue instances and allows for instances that have yet to be raised to be suppressed before they are raised.

You create device groups to organize devices according to business needs. Devices can belong to more than one group, and different sets of groups can be used for different purposes.

For example, you might create a collection of groups named North, South, East and West that organize devices geographically, while creating another set of groups named Accounting, Sales and Engineering that organize devices along departmental lines. This allows you to manage devices across different dimensions, using similar mechanisms. With the groups described above, for instance, you can generate separate scorecards for all devices in the West or all devices used by Engineering. You decide on the organization, and NetMRI properly sorts everything.

The Device Shortcut Menu

Anywhere an IP address appears as a hyperlink in the NetMRI appliance, you can right-click that hyperlink to open a useful shortcut menu.

- **Device Viewer** – Opens the Device Viewer for the selected device associated with the hyperlink;
- **Config Explorer** – Opens the Config Explorer for the device associated with the hyperlink;
- **View Running Config** – Queries the chosen device and displays the contents of its currently running configuration file;
- **Changes** – Displays the device's Network Analysis → Changes page in the Device Viewer.
- **Issue List** – Displays the chosen device's Network Analysis → Issues page in the Device Viewer. See Evaluating Issues in NetMRI for more information about Issues, what they mean and how they work.
- **Policy Compliance** – Opens the chosen device's Network Analysis → Policy Compliance page in the Device Viewer, which shows the status of any Policies deployed against the chosen device;
- **Topology Viewer** – Opens the NetMRI Topology Viewer with the selected device as the central device shown in the map.
- **Schedule Job** – Opens the Job Details window, to set up a job script to run against the chosen device. See Job Management and Automation Change Manager for more information about job features in NetMRI.
- **Execute Command** – Similar to Schedule Job, this option opens an Ad Hoc Command function to allow entry of a single command string to the chosen device. The command syntax needs to be compatible with the selected device: JunOS for Juniper, IOS or CatOS for Cisco, and so on.
- **Open Telnet Session** – Activates the Telnet/SSH proxy to start a new Telnet session with the chosen device.
- **Open SSH Session** – Activates the Telnet/SSH proxy to start a new SSH session with the chosen device.

Telnet and SSH Proxy Operation

**Note:** Before typing, click in the browser-based Telnet or SSH session window after you open a session.

The NetMRI appliance functions as a Telnet and SSH session proxy for users to communicate by command line with devices on the network, including devices that the system sees and can reach, but does not manage. This functionality extends to Telnet or SSH sessions with NetMRI devices themselves. The Telnet/SSH proxy also provides full VT100 emulation for systems and devices that need it. NetMRI provides a hard limit of ten concurrent SSH or Telnet sessions from any NetMRI instance to other devices. (Example: if one user has seven Telnet sessions open on a NetMRI instance, all other users are limited to a total of three additional terminal sessions.)

**Note:** Operations Center Only: The Telnet/SSH proxy works transparently in the OC as a two-tiered proxy to communicate to devices reachable by the individual collectors. The proxy is two-tiered because the OC cannot talk directly to devices–only Collectors can do so. Telnet/SSH operation is transparent and behaves normally when initiating sessions from the OC appliance.
For any Telnet or SSH session, administrative users can define user CLI credentials for other NetMRI user accounts. The location for configuring is Settings icon -> User Admin -> edit User -> CLI Credentials tab. (Accounts that can modify CLI credentials for themselves and other users include SysAdmin, UserAdmin and ChangeEngineer High.) Without User CLI credentials, other users can still log in to devices using their own device-specific credentials. This is particularly handy for devices that are not directly managed by NetMRI, such as Linux systems, but for which a user has a specific account. Some devices that are detected and/or managed by NetMRI may not provide the same level of Telnet or SSH as NetMRI. This is an advantage of the Telnet/SSH proxy.

Some NetMRI user accounts, such as ChangeEngineer Low, will not be able to start terminal configuration sessions using the Telnet/SSH proxy. System credentials can also be used for Telnet/SSH sessions. See Creating Admin and User Accounts for more information.

All session activity is logged. See User Audit Logs for more information.

Note: All Telnet/SSH proxy sessions have an inactivity timeout of five minutes. This value cannot be changed. NetMRI allows only one session to a device from the same NetMRI instance.

To open a Telnet or SSH session with a device, do the following:

1. Right-click on the IP address hyperlink for a device. The shortcut menu appears.
2. From the menu, select Telnet Session or SSH session based on your preferences.

Using CLI Proxy

In addition to using Telnet and SSH sessions as proxies, you can connect to network devices using the CLI proxy. This feature allows users with valid privileges to proxy a connection to network devices through NetMRI. Superusers can grant the following privileges to control user access to the CLI proxy feature:

- **Terminal**: Open Session: This permits users to connect to network devices.
- **Terminal**: User System Creds: This permits users to use the credentials stored on NetMRI to access network devices.

For information about specifying privileges, see Defining and Editing Roles.

To connect to specific devices, users must also have permissions to the corresponding device groups to which the devices belong. Authorized users can use any SSH client to gain proxy connection using their NetMRI credentials, without the need to acquire the credentials for individual devices. With valid privileges, users can use the Connect command to connect to the devices to any SSH client. For information about the command, see Using the Connect Command. The CLI proxy feature connects only through the management interface on the NetMRI appliance. This helps eliminate the need to gain access to the user's computer through various networks, VRFs, and VLANs. Note that all connections and commands issued to any network devices through the CLI proxy are audited and logged. For information about audit logs, see User Audit Logs.

Using the Connect Command

Use the Connect command to connect to network devices from any SSH client. Users only need a connection to the NetMRI Management interface to connect to any managed devices. Users can connect to devices in groups to which they have valid permissions. You can view the audit logs for all events when the users use the Connect command to access network devices.

**Example**

```
Netmriuser > connect {device ip | device name} <Network View>
```

where `<Network View>` is the name of the network view.

Connecting to Managed Devices through the CLI Proxy

To connect to a managed device via the CLI proxy:

1. Connect to the NetMRI Management IP address using an SSH client of your choice.
2. Log in using the same username and password you would use to log in to the NetMRI Web interface.
3. Connect to a device using the Connect command. Example: connect 10.0.1.24. If there are multi-network deployments, you must specify the name of the network view in the Connect command. Example: Connect 10.0.1.24 "Network 1".

Connecting Automatically to Managed Devices

You can configure an SSH connection to automatically connect to a managed device using SSH environment variables. Using this feature, you can save shortcuts to the devices to which you frequently connect.

You can use the following environment variables to set up the automatic connection:

- **CLI_PROXY_HOST**: The IP address or hostname of the device you want to automatically connect to after you log in to NetMRI.
- **CLI_PROXY_NET**: The name of the network view in which the device resides. This is required only for multiple network deployments.

The following example illustrates how to use these environment variables through PuTTY:

1. Start a PuTTY session.
2. In the PuTTY Configuration window, go to the Connection -> Data -> Category section.
3. As illustrated in Figure 14.1, do the following in the Environment variables section:
   - Enter CLI_PROXY_HOST 210.20.20.5.
5. Click Open.

**User Audit Logs**

**Note:** If the contents of an audit log are of interest and must be kept for a longer term, save the log contents into a separate text file, as the log will drop off of the system 30 days after it appears. Audit logs are unique to each device.

Audit logs are an important tool for tracking the following event types:

- Configuration collection logging after discovery.
- CLI Credential guessing and CLI sessions through the Telnet/SSH proxy.
- Connections and commands issued to devices through the CLI proxy.

When you display a single audit log entry, a complete screen dump of the entire session is shown in text format. Session audit logs are kept by the appliance for a rolling 30-day time window. Audit logs are available at two levels: system-wide (under **Settings**), and for individual devices (in the Device Viewer). Error events you see here are normally associated with credential guessing operations by NetMRI and user-initiated SSH/Telnet sessions to individual devices.

For CLI Credential guessing and Telnet/SSH session attempts, you will see messages for the following phenomena:

- **Invalid Credentials** – in which a connection attempt is made through Telnet/SSH, and the login tuple is used but the distant end rejects it. This occurs after NetMRI successfully communicates with the device, and the initial attempts with username/password combinations fail;
- **Connection Closed by Foreign Host** – usually due to enforced telnet or SSH session timeout on the device;
- **Timeout Waiting for Device** – NetMRI's discovery polling or data collection timed out due to lack of response from the device;
- *** No Route to Host** – the device is now not reachable;
- **Bad Secrets for Enable Mode** – an incorrect Enable password was sent by NetMRI and the device rejects the attempt to enter Enable mode.

For configuration collection logging, you may see messages of the following types:

- **Config collection disabled globally** – the current instance of NetMRI has disabled all Config Collection features (go to Settings icon → **Setup** → **Collection and Groups** → **Config Management** side tab to check and enable collection settings);
- **Not Included by Discovery Settings** – The device in question is not part of any IP range, is not specified as a static IP, and does not match any device Hints and is not a seed router. (go to Settings icon → **Setup** → **Discovery Settings** to check values for each of the four setting types. This message appears only for attempts to get configurations from the device);
- **Not Licensed** – Device is not licensed under NetMRI. This message appears only for attempts to get configurations from the device;
- **History Indicates Config not Changed** – No configuration changes have occurred since the previous fetching of configuration data. This message appears only for regular device polling operations on managed devices;
- **CLI credentials unknown** – all attempts at guessing or logging in to a device after discovery are unsuccessful.
To view a device's user audit log, go to Device Viewer→ Settings & Status→ User Audit Log. The audit log appears as a cumulative list for all Telnet/SSH sessions for the individual network device or end host for the last 30 days.

### Using the Device Audit Log

**Note:** The System Administrator and View Audit Log privileges are required in order to view the Device Audit Log.

The Device Audit Log (Device Viewer→ Settings & Status→ Device Audit Log) provides a device-specific list of events related to the device's management by NetMRI. You can expect to see messages such as LicenseAdd, indicating when the device was added to NetMRI management into a Device Group for purposes of Switch Port Management or other licensing requirements; and DiscoveryDelete, a case where a device with a particular management port IP address was removed from NetMRI management due to another device being managed through the same IP.

A second Device Audit Log, in Settings icon→ Notifications→ Device Audit Log, provides a listing for all Discovery and Licensing messages for all devices managed by NetMRI. When devices are removed from the license count for NetMRI or ACM, related event messages will appear.

### Introducing Device Groups

**Note:** NetMRI provides two functional device group categories: Basic device groups and Extended device groups. All default device groups that appear in the Select Device Group pane are Extended device groups, which means that they provide network scores for the NetMRI Dashboard and enable management through user Roles and Privileges. extended device groups also may impose a higher computation load on the appliance. Basic device groups are most useful for large collections of network devices that you know will not be actively managed, such as end-user network segments at the terminating end of Ethernet circuits.

Device groups are a fundamental organizing tool in NetMRI. You use device groups to gather devices with similar attributes and similar categories together, to perform device management tasks, or because you want to organize a set of devices into a group to perform specific processing tasks or to prevent processing tasks from being performed. Device groups are divided into two types: Basic device groups, which provide only basic categorization and processing features to limit processing loads on member devices; and extended device groups, which provide the full set of NetMRI device processing features on member devices (for more information, see Controlling NetMRI with Device Groups).

The default set of device groups in NetMRI appears as a hierarchical list and includes the following:

- **Network Management** — Any devices, including NetMRI appliances, that perform network management tasks;
- **Security** — All firewall, VPN concentrator and security management devices;
- **Network w/o SNMP** — Devices that are discovered, but also discovered to lack support for SNMP protocols. This device group is required for NetMRI operation and cannot be deleted by the administrator;
- **NIOS** — Device group that contains Infoblox NIOS appliances supporting the Grid Manager environment for DNS, DHCP and IPAM and other features, if any are present in the network;
- **Routing** — L3 routing devices that perform no switching or VLAN support;
- **Switch-Router** — L2/L3 switches that support routing protocols and VLANs;
- **Switches** — L2 switches that do not support VLANs;
- **Unknown** — All devices for which identification cannot be determined, perhaps because NetMRI does not provides device support for the devices. This device group is required for NetMRI operation and cannot be deleted by the administrator;
- **Network Management** — All NetMRI appliances and other devices used for network management tasks;
- **Network Pending** — All devices discovered and in processing by NetMRI, but not yet managed by NetMRI. This device group is required for NetMRI operation and cannot be deleted by the administrator;
- **NAME ONLY** — All discovered devices for which only their name can be determined by NetMRI's discovery feature. This device group is required for NetMRI operation and cannot be deleted by the administrator.

### Using the Device Group Selector

The main Dashboard, Network Analysis and Network Explorer pages show the Device Group Selector control on the right. Simply click a device group name in the selector to filter the contents of the main display pane. To edit a device group, right-click any device group name and select Edit Device Group, or click the Edit Device Group icon.

All top-level device groups can act as top-level device groups for nested device groups. Nested device groups can only contain devices from the parent device group. You can nest child device groups up to five levels deep in the tree. By default, child device groups automatically appear in the tree but can be hidden by clicking the (−) symbol next to the parent group.

### Controlling NetMRI with Device Groups

**Note:** For efficient system operation, NetMRI provides an upper limit of 250 Extended device groups and 250 Basic device groups.
All default device groups (including those listed above) in NetMRI are extended device groups, which means that they support extended processing functions. Some types of network devices warrant more processing by NetMRI, such as the collection of performance and environmental data, open ports probing, NetBIOS name probing, collecting of configuration files, analyzing for issues, and other device processing features. Some device types can be quickly excluded from complex processing tasks by simply assigning them to a basic device group. Many end host networks may fall into this category. You can create both basic and extended device groups in your deployment. You can also convert basic device groups to extended device groups, and also the reverse, at any time.

Basic device groups limit their processing options to a minimum. Basic device groups do not contribute to NetMRI Network Scorecard calculations and significantly reduce back-end processing. You can define group membership criteria and use the **Include end hosts** feature for any discovered network segments that match your requirements. An example involves collecting end host network segments into a basic device group to avoid expending system processing cycles on network devices that do not require them. (For more information on group membership criteria, see the section **Understanding Device Group Membership Criteria**.)

Extended device groups provide a substantial collection of settings to determine how the device group processes its information. Along with defining group membership criteria, a number of option switches help determine the level and types of processing performed by the device group:

- **Rank** (for more information, see **Ranking Device Groups**);
- **Switch Port data collection**: Enable this only for device groups with L2/L3 Ethernet switching devices as member. For more information, see **Device Groups and Switch Port Management**;
- **Collect performance and environmental data** Enable or disable performance and environmental information (for more information, see **C handing Performance Data Collection Settings**);
- **Probe for open ports**: Allows NetMRI to probe for open TCP/UDP ports on member devices;
- **Identify device using fingerprinting** (for more information, see **Defining Group Data Collection Settings**);
- **Probe for NetBIOS name**: For more information, see **Defining Group Data Collection Settings**;
- **Analyze for Issues**: For more information, see beginning with **Evaluating Issues in NetMRI**, and the topic **Viewing Device Issues, Configurations and Changes**;
- **Test for default credentials**: Allows NetMRI to test all devices in the group for the presence of vendor default SNMP credentials, which are a potential element for security breaches, but are also used for assistance in collecting device configurations. Credential default testing is also a compliance measure;
- **Collect config files**: For more information, see beginning with **Configuration Management**;
- **Regard configurations as 'Locked'**: Disallows editing of any collection configuration files for members of the device group;
- **Allow script execution**: Allows the execution of Perl and CCS scripts on group member devices.
- **Enable Discovery Blackout**: Define time periods when NetMRI will not communicate with devices or networks for discovery;
- **Enable Change Blackout**: Define blackouts for CLI interaction, scheduled or run-now job executions, Telnet/SSH proxy and port control UI features for all devices in the group. For more information, see **Defining Blackout Periods**.

All settings are further described in the topic **Creating Device Groups**.

### Device Groups and Switch Port Management

Through device groups, switch port management enables you to monitor and analyze the complement of Ethernet trunks and switch ports in their network. Switch port information gathering, or polling, is the key tool for doing this. Device groups can specify unique switch port management polling settings. Not all device groups will use these settings, which are located under Settings icon → **Setup** → **Collection and Groups** → **Groups** tab, take precedence over the global settings defined in the Collection and Groups feature.

A device group can use either Periodic or Scheduled polling, or disable polling for the device group.

**Note:** You can also click **Poll Now** at any time to poll all member devices of the device group.

To poll a device group or create custom settings for polling, do the following:

1. In the Device Group Selector, right-click any desired device group anywhere in the tree and select **Edit Device Group**. (For switch port management, select the **Switching** device group.) The Edit Device Group dialog opens.

   The **Switching** device group is an extended device group that provides several features designed for Ethernet switching devices management.

2. To change polling options for the selected switching device group, open the **Switch Port Data Collection** dropdown. Four switch port data collection options are offered:

   - **Use Global Settings**: Choosing this option enforces use of global settings for device polling on the current device group.
   - **Specify Polling Interval**: Define regular polling time periods. Choose a polling interval of 1 or more **Minutes** or **Hours**, or click **Poll Now** to poll all devices that are members of the Device Group;
   - **Specify Schedule**: Click the radio button and select from the list of schedules in the panel, or click **Add New Schedule** (near the top right of the scheduling pane) to create a schedule for recurrent polling. Select a **Recurrence Pattern** of **Once**, **Hourly**, **Daily**, **Weekly** or **Monthly**: in all cases you must choose an **Execution Time**. Click the **Add** button when finished defining the new schedule. In the same scheduling pane, select the desired schedule from the list. After saving changes, the chosen schedule goes into effect for the device group.
   - **Disable**: Disables device switch port data collection for the selected device group. Disabling switch port data collection prevents NetMRI from collecting VLAN and switch forwarding data. This can affect neighbor topology for the switch and any connected devices to the switch possibly resulting in NetMRI not being able to accurately locate devices on the network. Disabling switch port data collection also prevents analysis of any VLAN-related issues for a disabled switch.

3. Click **Save & Close** or **Save & New** to commit your settings. If you need to change any more extended device group settings, do so before saving.

The settings you define here apply only to the chosen device group.
Ranking Device Groups

For Extended device groups, NetMRI uses Rank settings, defined for each group, to determine how and when each device is processed after it is discovered on the network. The default groups defined by from the same organize devices essentially into “network” and “non-network” devices, based on their type and assurance level. Network devices usually have SNMP and Config collection and analysis enabled, while non-network devices do not. This reduces unnecessary data collection and processing loads, allowing the appliance to work more efficiently for devices that matter most. By selectively enabling and disabling data collection, you can fine-tune NetMRI performance, or ensure that NetMRI processes the most important devices when a Device Limit or Interface Limit, based on licensing, is exceeded. In such cases, the Rank associated with each group is used to determine which devices are within the limits (devices with the highest rank) and which are outside the limits (devices with a lower rank). In this way, the most important devices, as indicated by the group rank, are processed while others are not.

The NAME ONLY and UNKNOWN Groups

Discovery uses two special device groups, NAME ONLY and UNKNOWN, to identify and categorize devices as they are discovered. Newly found devices first appear in the UNKNOWN group, with SNMP collection and port scanning enabled to learn more about them. The NAME ONLY group lists devices for which very little is known, except for their name (which usually comes initially from DNS). If more is learned, such as their SNMP community, devices disappear from these low level groups and appear in higher-level groups, where their process settings change to meet the needs of that group.

The Group Processing Hierarchy

NetMRI controls processing within device groups by a hierarchical collection of settings in the following order:

- Global settings for network polling and configuration management;
- Device group settings;
- Device settings;
- Interface group settings.

If you disable a specific process (such as SNMP collection) at a higher level, then all lower level settings are ignored. This allows administrators to quickly disable all processing of a given type, such as SNMP, without being forced to change individual settings.

Filtering by Device Group

When the Select Device Group panel is available (in the right panel), you can filter the contents of the center panel by device group.

- To filter by device group: In the Select Device Groups panel, click the desired device group.
- To remove device group filtering: In the Select Device Groups panel, click All Devices.
- To edit device groups: Click the Edit Device Groups button to the right of the Select Device Group heading.

The Collection and Groups page opens, showing the Groups -> Device Groups tab (also reachable by Settings icon -> Setup -> Collection and Groups -> Groups tab).

Note: The number in parentheses after a device group name is the number of devices in the group.

Creating Device Groups

The Device Groups page (Settings icon -> Setup section -> Collection and Groups page -> Groups tab -> Device Groups side tab) enables you to create and configure device groups.

As previously noted, you can create two different categories of device groups: Basic and Extended. Both types of device groups also support discovery blackout and change blackout periods (for more information, see Defining Blackout Periods).

Note: Discovery blackout periods and change blackout periods may be defined for any Basic or Extended device group, at the time you create them or when you decide to edit them.

The table in the Device Groups side tab lists all device groups, with default sorting by Rank. Each row shows group configuration settings, with any parent groups appearing as folder icons indicating that child device groups exist as child device groups beneath them in the tree. The device groups table provides a series of columns showing status of various discovery and monitoring features that are enabled or disabled for each group. Tooltips appear when you hover over any icon in the table, including column headers. For example, when you hover over a row’s MC (Membership criteria) column, it displays the complete text of the membership criteria regular expression. Any feature column that is cleared, without a checkmark, for a device group indicates that the given feature is not enabled. (Bear in mind that individual devices of certain types can override group-level settings. For information about device-level settings, see Interpreting Discovery Table Data.) The complete list of data points provided for every device group at all nested levels, includes the following:
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>Indicates whether member devices in the group will have their ARP caches refreshed before collecting discovery data. NetMRI uses ARP cache refresh to control LAN switches from which switch-forwarding data is collected. For information, see Notes on ARP, Switch Data Collection, and End Hosts.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Indicates whether the device group is set to enable SNMP data collection for member devices. SNMP collection can also be enabled/disabled for groups and devices.</td>
</tr>
<tr>
<td>PS</td>
<td>Indicates whether members of the device group will be scanned for open protocol ports. If enabled, NetMRI probes the TCP and UDP ports listed at Settings icon → Setup → Port List, to determine whether they are open. For information, see Defining Group Data Collection Settings.</td>
</tr>
<tr>
<td>FP</td>
<td>Indicates the device group setting to use the Identify device using fingerprinting setting for member devices. (This setting is dependent on the Probe for Open ports feature.) A polling technique to identify each network device based on the response characteristics of its TCP stack. This information is used to determine the device type. In the absence of SNMP access, fingerprinting is usually the only way to identify non-network devices. For information, see Defining Group Data Collection Settings.</td>
</tr>
<tr>
<td>C</td>
<td>Indicates the device group setting to allow config file collection for all members in the group (Collect config files).</td>
</tr>
<tr>
<td>CCS</td>
<td>Indicates the device group setting to allow CCS script file execution for all members in the group (Allow Script Execution).</td>
</tr>
<tr>
<td>DC</td>
<td>Indicates the device group setting for Test for Default Credentials, used to scan for the presence of vendor default credentials for all members in the group.</td>
</tr>
<tr>
<td>A</td>
<td>Indicates the device group setting to allow Issue analysis for all members in the group (Analyze for Issues). For information about Issue analysis, see Viewing Issues in the Network.</td>
</tr>
<tr>
<td>CL</td>
<td>Indicates the device group setting to collect config data but to consider all member device configs a locked and not to be changed through NetMRI (Regard configurations as 'locked'). For information, see Defining Group Data Collection Settings.</td>
</tr>
<tr>
<td>NB</td>
<td>Device polling method to collect the NetBIOS name for endpoint devices in the network. Device groups also enable NetBIOS scanning. For information, see Defining Group Data Collection Settings.</td>
</tr>
<tr>
<td>DB</td>
<td>Indicates the device group setting to impose discovery blackouts. For information, see Defining Blackout Periods.</td>
</tr>
<tr>
<td>CB</td>
<td>Indicates the device group setting to impose configuration change blackouts. For information, see Defining Blackout Periods.</td>
</tr>
<tr>
<td>SPMC</td>
<td>Indicates the device group setting to allow switch port data collection (Switch port data Collection). For information, see Device Groups and Switch Port Management.</td>
</tr>
<tr>
<td>SPMS</td>
<td>Indicates whether the device group provides a polling interval or scheduling for switch port data collection. This setting is dependent on an enabled Switch port data Collection setting for the device group.</td>
</tr>
</tbody>
</table>
Device groups use Rank as a way of determining the actions to take on a device that is a member of more than one group. If a device is a member of two groups, one that is enabled for config collection, and in another that is not, the group with the highest rank determines if the configs should be collected for that device. Ranking for nested device groups in the device group tree is hierarchical. Child groups ranking is always higher than the ranking of its parent, without user input.

Group Ranking is determined by their position in the tree. Should the user want a device group to have a higher ranking, the group must be moved to a higher position in the group tree.

Creating a Top-Level orSibling Device Group

1. Open the Settings icon → Setup → Collection and Groups → Groups tab.
2. Right-click a top-level device group and select Add → Child from the shortcut menu.
   The Add Device Group dialog appears. By default, NetMRI creates new groups as Basic device groups. Two option buttons can be chosen: Basic and Extended. For more information about extended device group settings, see Creating Extended Device Groups.
3. Enter a Name for the new group. (The group name is shown in all group-related displays and reports, so the group name should be meaningful without being too long.)
4. Enter a Membership Criteria regular expression. (Criteria are used for either Basic or Extended device groups.) See Understanding Device Group Membership Criteria for details.
   By default, NetMRI creates new groups as Basic device groups. We assume creation of a Basic device group in this procedure.
5. To define a Discovery Blackout for the new device group, check the Enable Discovery Blackout check box and click its Scheduling icon. The Discovery Blackout Scheduling gadgets open in the dialog. For more information about discovery blackout configuration, see Creating Extended Device Groups.
6. If necessary, select the Enable Change Blackout check box and click its Scheduling icon. The Discovery Blackout Scheduling gadgets appear. For more information about change blackout configuration, see Creating Extended Device Groups.
7. Click Save & Close or Save & New. Clicking Save & New saves your new device group and keeps the dialog box open.

To create a sibling device group, do the following:

1. Open the Settings icon → Setup → Collection and Groups → Groups tab.
2. Right-click a top-level device group and select Add → Sibling Above or Add → Sibling Below from the shortcut menu.
   The effect of creating sibling groups allows you to insert a device group into a position anywhere in the list of device groups, thereby defining the ranking for the new group. By default, new device groups are inserted at the bottom of the list, denoting a lower ranking.
   The Add Device Group dialog appears. By default, NetMRI creates new groups as Basic device groups. Two option buttons can be chosen: Basic and Extended.
3. Follow Steps 4–7 from the previous procedure to create a sibling device group. Note that this process also places the new device group in the ranking position immediately above or below the original group you selected for creating the sibling.

Creating a Nested Device Group

Nested device groups should only contain devices belonging to their parent group. Creating a child device group of the top-level group “Routing” and using a device group criteria regular expression to filter other devices (e.g., firewalls) will result in an empty device group.

The group criteria statements built into each device group, respectively:

$Assurance > 75 and $vendor eq "Cisco" and $type in ["Router","Switch-Router"]

$Assurance > 75 and $vendor eq "Juniper" and $type in ["Router","Switch-Router"]

Note: When you create a nested/child device group for an existing device group, the existing group changes its icon from a Group icon to a folder. That folder icon does not change the essential properties of the parent device group—the parent keeps all of its qualifying devices.

To create a new child device group, do the following:

1. Open the Settings icon → Setup → Collection and Groups → Groups tab.
2. Right-click a top-level device group and select Add → Child from the shortcut menu.
   The Add Device Group dialog appears. By default, NetMRI creates new groups as Basic device groups. Two option buttons can be chosen: Basic and Extended. For more information about extended device group settings, see Creating Extended Device Groups.
3. Enter a Name for the new child group. (The group name is shown in all group-related displays and reports, so the group name should be meaningful without being too long.)
4. Enter a Membership Criteria regular expression. (Criteria are used for either Basic or Extended device groups.) See Understanding Device Group Membership Criteria for details.
5. If you want the device group to include collections of discovered end hosts (an option for basic device groups to prevent end-host computers from occupying valuable licensing space), enable the Include end hosts check box.
   By default, NetMRI creates new groups as Basic device groups. We assume creation of a Basic device group in this procedure.
6. To define a Discovery Blackout for the new device group, check the Enable Discovery Blackout check box and click its Scheduling icon. The Discovery Blackout Scheduling gadgets open in the dialog. For more information about discovery blackout configuration, see Creating Extended Device Groups.
7. If necessary, select the Enable Change Blackout check box and click its Scheduling icon. The Discovery Blackout Scheduling gadgets appear. For more information about change blackout configuration, see Creating Extended Device Groups.

8. Click Save & Close or Save & New. Clicking Save & New saves the device group and keeps the dialog box open.

Note: Nested device groups also operate with Issue Analysis (for information, see Issue Analysis in NetMRI and its subsections). Nested device groups inherit their Issue settings from their parent device groups, and may need editing to suppress Issues that are not relevant to them.

Creating Extended Device Groups

Extended device groups can exist at any level in the device group tree, without restriction. To create an Extended device group with additional features, do the following:

1. Next to Type, click the Extended option.
2. Enter a Name for the group. (The group name is shown in all group-related displays and reports, so the group name should be meaningful without being too long.)
3. Define a Membership Criteria regular expression. (Criteria are used for both Basic and Extended device groups.) See Understanding Device Group Membership Criteria for details.

Note: Infoblox recommends using regular expressions for refining the membership in device groups. The topic Understanding Device Group Membership Criteria provides the information you need to understand and define simple regular expressions for device groups.

4. If you want the device group to include collections of discovered end hosts (a possible option for basic device groups to prevent end-host computers from occupying valuable licensing space), enable the Includeendhosts check box.

5. Under Type, click Extended to create an extended device group with wider choices of device processing options.

Rank: Displays the Ranking value as the default sort order. See Ranking Device Groups for details. Ranking value is used as the default sort order for all group-related tables, with the highest rank shown first. Rank is also used to determine the individual device settings controlling processing for each device.

6. To change Switch Port data collection settings (if necessary), choose from the following:

- **Use Global Settings**: the default, which enables the device group to inherit its switch port data collection settings from the default settings defined for all device groups, including periodic polling and scheduled polling settings (see Global Switch Port Management Polling Settings for related information);
- **Specify Polling Interval**: overrides the global Periodic Polling settings with a polling interval setting that is local to the current device group. Choosing this option displays a Polling Interval setting pair, in which you define the interval in 1-60 Minutes or in 1-24 Hours. You can also click Poll Now to execute polling on the device group when you finish creating it;
- **Specify Schedule**: overrides the global Scheduled Polling settings with a scheduled polling definition that is local to the current device group. Existing schedule sets may appear in the list; or, click Add New Schedule to create a new polling schedule instance. Choose a Recurrence Pattern of Once, Hourly, Daily, Weekly or Monthly; in all cases you must choose an Execution Time and select at least one day of the week check box. You can also click Poll Now to execute polling on the device group when you finish creating it;
- **Disable**: Completely disables device polling for the device group.

7. To change Switch Port data collection settings (if necessary), choose from the following:

- **Collect performance and environmental data** Enable or disable device performance and environmental information for all member devices in the group (for more information, see Changing Performance Data Collection Settings);
- **Probe for open ports**: If enabled, TCP and UDP ports listed at Settings icon → Setup section → Port List are probed to determine whether they are open.
  - **Analyze device using fingerprinting**: If enabled, fingerprinting attempts to identify each device based on the response characteristics of the TCP stack being used.
- **Probe for NetBIOS name** Setting to enable NetMRI to collect the NetBIOS names for endpoint device members in the device group. For more information, see Defining Group Data Collection Settings and is globally disabled by default to prevent unexpected scanning of the network by a new Operations Center Collector;
- **Analyze for Issues**: NetMRI evaluates over 250 discrete Issues, plus custom Issues defined by the admin user. Issues are discovered and reported by NetMRI based on globally set schedules. Disabling this feature for a device group disallows the group from being selectable in the Device Group Selector panel in the main Network Analysis Issues page For more information, see Evaluating Issues in NetMRI and Viewing Device Issues, Configurations and Changes;
- **Test for default credentials**: Allows NetMRI to test all devices in the group for the presence of vendor default SNMP credentials, which are a potential element for security breaches, but are also used for assistance in collecting device configurations. Credential default testing is also a compliance measure;
- **Collect config files**: When enabled, this check box allows NetMRI to collect all present configuration files for devices in the device group, to participate in the Configuration Management feature set, which allows you to view and compare differences between running-config and saved-config configuration files, and edit and manage config files on devices. For more information, see Configuration Management;
  - **Regard configurations as 'Locked'**: Disallows editing of any collection configuration files for members of the device group;
- **Allow script execution**: Allows the execution of Perl and CCS scripts on member devices.
- **Refresh device caches before collecting switch port data** Check box to enable refreshing of ARP caches on switches and switch-routers in the managed network before NetMRI performs polling of switch ports. Enabling this feature will not produce an automatic ping sweep of the managed network (for information on ping sweep, see Defining Group Data Collection Settings). The benefit of this feature is that it enables more accurate detection of all endpoint devices on switches. Without ARP refresh, some endpoint devices may not be detected. This feature is globally disabled by default. With this setting globally enabled, individual device groups can also be set to enable or disable this feature.
8. Select the **Enable Discovery Blackout** check box and click its Scheduling icon. The Discovery Blackout Scheduling gadgets open in the dialog.

**Note:** For more information about discovery blackouts and change blackouts, see *Defining Blackout Periods*.

a. In the **Recurrence Pattern** dropdown, choose how often you want to execute the blackout period. You can select **Once**, **Daily**, **Weekly**, or **Monthly**.

b. If you choose **Once**:
   - Choose an **Execution Time** from the drop-down list.
   - Enter the date of the blackout, in the **Day of** field.
   - Specify the **Duration**: 10 or more Minutes, Hours or Days.

c. If you choose **Daily**, click either **Every Day** or **Every Weekday**.
   - Choose an **Execution Time** from the drop-down list.
   - Specify the **Duration**: 10 or more Minutes, Hours or Days.

d. If you choose **Weekly**, complete the following:
   - Choose an **Execution Time** from the drop-down list.
   - Check the check boxes for one or more days from **Sunday** through **Saturday**.
   - Specify the **Duration**: 10 or more Minutes, Hours or Days.

e. If you choose **Monthly**, complete the following:
   - Choose an **Execution Time** from the drop-down list.
   - **Schedule the day of the month**: A discovery blackout can be executed monthly on a specific day, or blackout instances can be executed more than one month apart on a specific day, in the **Day of every month(s)** field.
   - Specify the **Duration**: 10 or more Minutes, Hours or Days.

9. If necessary, select the **Enable Change Blackout** check box and click its Scheduling icon. The Discovery Blackout Scheduling gadgets appear.

a. Follow steps 14a through 14e to define the change blackout schedule.

**Note:** Some devices in your network may have a locked **Config Change** setting (Device Viewer → **Settings & Status → General Settings**), which means that NetMRI will be disallowed from changing configurations on the device. In these cases, a device-level **Enable Change Blackout** setting is unnecessary. Similarly, each NetMRI device group has a **Regard configurations as 'locked'** setting. If a device group uses this setting, the **Enable Change Blackout** setting is unnecessary. If a device group does not enforce a change blackout, but a device in that group enables the **Regard configurations as 'locked'** setting, the device setting takes precedence.

10. Click **Save & Close**; if you need to create another device group, click **Save & New**.

### Additional Device Group Operations

To view a list of device group members (devices that are included in the device group):

1. Click the Action icon for the group, and choose **View Members** from the shortcut menu. A new browser popup window appears, displaying the list of member devices. Clicking the **IP address** for any device brings up the Device Viewer.

To copy a group (to use as the basis for a new group), do the following:

1. Click the Action icon for the group, and choose **Copy** from the shortcut menu. (The new group is initially named "Copy x of <original name>.")
2. Edit the new group’s name and settings.

To delete a group:

1. Click the Action icon for the group, and choose **Delete** from the shortcut menu.
2. Confirm the deletion.

### Device Groups Action Menu

The **Device Groups** page provides the complete list of top-level device groups, populated with a series of gear icons. Clicking each icon displays a shortcut Actions menu offering group editing features: for device groups, features include the following:

- **The Add** option enables the creation of new device groups at the same level in the group hierarchy as the current group (**Sibling Above** and **Sibling Below**) and provides the **Child Below** option, which allows you to create a nested device group that is subordinate to the group you’ve currently selected.
- **View Members** lists the devices within the group, displaying the list in a separate window;
- **Copy, Edit** and **Delete** perform their respective functions on the selected device group. The **Edit** feature provides all the standard device group editing capabilities, including changing blackout periods, data collection settings, membership criteria and Rank settings.
NetMRI ships with pre-defined device group definitions. These groups are based on device types and assurance levels (the probability that from the same has correctly identified a given device) and are primarily used to see what has been discovered on the network. Default device groups can be used as-is, edited to suit your needs, or removed completely (provided you have admin rights to do so).

Use caution when deleting device groups; the Routing, Switching, NIOS, Optimizers, Security, and many other groups are built-in with NetMRI and should never be removed without first having developed new groups with the desired functionality to take their place.

Default device groups serve as good examples of how selection criteria and process settings can be defined to organize your network devices, but you should learn how to create your own device groups to gain all of the benefits of the device groups feature.

Understanding Device Group Membership Criteria

Note: One good way to understand how you define membership criteria for device groups is to look at existing Extended device groups in the system, including Routing, Switching and Security.

Group membership criteria expressions are simple logical expressions used to determine if a given device or interface should be included in a Device Group or Interface Group based on the properties associated with that device or interface. In other NetMRI contexts, such as Security Management, this process is also called filtering. A device group uses its filtering settings, called membership criteria, to determine which devices discovered by NetMRI will belong to that group.

If the device matches more than one group criteria, it is assigned the rank of the highest matching group and all of the settings for that group.

Device Groups also determine how its member devices will be interacted with by NetMRI. For example, if SNMP Collection or Config Collection are disabled for the highest ranking group containing a given device, then no SNMP data collection or Configuration file collection is performed for that device (beyond the initial collection needed to detect its existence). You use the same processes and settings to define Interface Groups (described in Creating Interface Groups.) The process for Device Groups is straightforward.

An example of a regular expression comprising the membership criteria for a Device Group:

```
$Assurance > 75 and $Type in ["Router","Switch-Router"]
```

This regular expression is used to define the Routing device group. Note the use of Boolean logic and the enclosure of two NetMRI device group types (Router and Switch-Router) in square brackets. Two unique NetMRI variables, $Assurance and $Type, are used as the filtering criteria to define what belongs in the group. Typically, at least two variables must be used to create accurate filtering for a Device Group definition. The $Assurance value is the value attached to every device by NetMRI after it is discovered, to certify the device type is determined correctly. Consider an expression for a custom Device Group definition:

```
$Assurance > 75 and $vendor eq "Juniper" and $type eq "Firewall" and $Access eq "on"
```

The more specific the expression, the more effective and specific that membership can be in the Device Group. The values to be matched against must, of course, be recognized by NetMRI.

Group membership criteria are also used to define the Device-Filter and Section-Filter directives in Configuration Policy Definition (CPD) files, and script-filter directives in Configuration Command Script (CCS) automation scripts. In these cases, if a device matches, then the CPD file or CCS script is used to analyze that device. (You can create custom files or scripts to define new criteria.) You do not need to use CPD files or CCS scripts to create new Device Groups or Interface Groups.

For Interface Groups, the processes are similar with some useful differences in how the regular expressions are defined to filter out interfaces reported in the device configuration.

```
$Type in ["Switch","Switch-Router"] and $ifType like /ether/ and $ifAdminStatus eq "up"
```

The Switch Port interface group uses the same variables to filter membership. The $ifType like /ether/ variable expression indicates how an expression can be interpreted to add Ethernet ports of varying types to the Group, the argument like allows a loose match against any port with the partial phrase ether in its identification. Considering the possibility of separating only 10/100 interfaces into a distinct group, you would use a more-specific expression such as:

```
$ifType like /FastEthernet/
```

Device Group Criteria and Device Custom Fields

Device Groups offer the flexibility to specify custom fields data as matching information against custom fields identification values defined on individual devices. You specify custom fields information in device groups through the Device Group Criteria. Doing so, you can craft devices groups that match specific types of information, such as Business Units, operational function, and so on. Based on the information in the section Defining and Using Custom Fields, you can create device custom fields (“device” is a specific type of custom field that you can create and use for data matching) that are referenced by specific device groups for collection of devices into logically-named groups in NetMRI for asset manageability.

Supporting custom fields in device groups requires some specific Device Group Criteria syntax. Because a custom field can use the same nomenclature as a standard device attribute (for example, the Custom Fields feature does not prevent you from creating a custom field named "Type," "Vendor" or "Model"), the device group criteria uses a convention to prevent conflicts. To do so, you prefix every Device Group Criteria reference to a device custom field with a syntax constant:

```
$custom_
Consider the creation of a device custom field called “business_unit.” (For information on how to create custom fields in NetMRI, see Defining and Using Custom Fields.) Editing the Device Group Criteria field for a device group called “Consumer Banking Group” to support a device custom field, typical syntax is as follows:

\[
\text{Assurance} > 65 \text{ and Type in ["Router","Switch-Router","Switch","Firewall"] and custom_business_unit = "Consumer Banking"}
\]

You preprend the constant $custom_to the value “business_unit” to create the expression $custom_business_unit = “Consumer Banking”. Doing so in the Device Group Criteria ensures that any device that possesses a matching field value will match the “Consumer Banking Group” device group.

### Device Group and Interface Group Criteria for Networks

Because devices are managed as part of one or more network views, you can define device groups or interface groups with criteria based on network membership.

- You use the $Network variable in both Device Groups and Interface Groups:
  - If the variable is applied to a device, it returns the name of the network view to which the device's Management IP belongs;
  - If the variable applied to a device's interface, it returns the name of the network view to which the interface IP address belongs.

  **Example:** $Network = "blue"

- The hasnetwork operator returns a value of true if at least one device interface is part of the specified network views list:

  **Syntax example:** hasnetwork("blue","red","green")

### Device Group/Interface Group Membership and Issue Suppression

Change issue thresholds and suppress issues for device groups in the Settings icon → Issue Analysis → Issue Group Settings icon → by Device Groups and by Interface Groups side tabs. After selecting a group in the left panel, the Issue Settings for Group table lists all issues for the group and shows the current thresholds (if any) in the Criteria column, and whether any listed issue is suppressed. Consult the topics Issue Group Settings and Performing Issue Suppression for more information.

### Creating Interface Groups

After Discovery, you can organize all interfaces discovered on the network into collections of named groups. Similar to device groups, interface groups can be used to organize interfaces for results analysis, troubleshooting, or to manage interface data collection. Interface group membership is determined periodically and stored in the database. Interface Groups have considerably narrower use in NetMRI compared to Device Groups. NetMRI ships with a set of common-sense default interface groups that automatically organize common interfaces, such as switched Ethernet ports, VLANs and Ethernet trunk interfaces. Interface groups can be modified or copied, pasted and edited to create new ones, or you can create entirely new groups (provided you have admin rights to do so).

### Interface Groups Action Menu

The Interface Groups page provides an Actions column, populated with a series of gear icons. Clicking each icon displays a shortcut Actions menu offering group editing features: for interface groups, View Members lists the interfaces within the group; Copy, Edit and Delete perform their respective functions on the selected group.

Use caution when deleting interface groups; the Admin Down, Trunk Ports, Active Router Interfaces and Switch Ports groups are built-in groups with NetMRI and should not be removed without first having developed new groups with the desired functionality to take their place.

You create and configure interface groups in the Interface Groups page (Settings icon → Setup → Collection and Groups → Groups tab → Interface Groups side tab). The benefits of using interface groups include:

- Collect performance data at specific time intervals for particular port types (trunk ports, VLANs of a specific switch, router interfaces of a specific type, or any other arbitrary designation);
- Use regular expressions to strictly define the interfaces that qualify to be part of the group, ensuring accurate group membership;
- Obtain flow connection information.

The table in the Interface Groups side tab lists all interface groups, with default sorting by Rank. Each row shows group configuration settings, with a green check indicating that the option is enabled, and a red X indicating that the option is disabled.

**Rank** determines the process settings for individual interfaces that belong to multiple interface groups. An interface is assigned the process setting associated with the highest ranking group that includes the interface as a member.

**Note:** Interfaces can be a member of one or more interface groups.

To create an interface group, do the following:

1. Go to Settings icon → Setup → Collection & Groups → Interface Groups side tab.
2. Click the Add Group button (below the Interface Groups table). The Add Interface Group dialog appears.
3. Type a Name for the interface group. (The group name is shown in all group-related displays and reports, so it should be meaningful without being too long.)
4. Enter a Rank for the interface group. See Ranking Device Groups for details.
5. Type a Membership Criteria expression. See Understanding Device Group Membership Criteria for more details.
6. Activate the processing options for the group.  
**Performance Statistics Collection:** If enabled, NetMRI collects performance data for interfaces in the group. If disabled, the appliance gathers minimal data for interfaces in the group. (This setting can be overridden for an individual interface in the Interface Viewer -> Settings icon -> General Settings page.)  
**Frequency:** Select the performance statistics collection interval. The default is set as Daily.

**Note:** You can set the Frequency to be more frequent than the default Daily setting.

7. Click the Save & Close button.

   or

   Click the Save & New button to save/close the current group definition and start a new group definition.

   • To view a list of group members: Click the View Members button for the group.
   • To edit a group: Click the Edit button for the group.

To view a list of interface group members:

1. Click the Action icon for the group, and choose View Members from the shortcut menu. A new browser popup window appears, displaying the list of member interfaces. Clicking the Device IP for any device brings up the Device Viewer. Each interface listing provides a link for its respective Interface Viewer and its VLAN Viewer, where applicable.

To copy a group (to use as the basis for a new group), do the following:

1. Click the Action icon for the group, and choose Copy from the shortcut menu. (The new group is initially named “Copy x of <original name>.”)
2. Edit the new group’s name and settings.

To delete a group:

1. Click the Action icon for the group, and choose Delete from the shortcut menu.
2. Confirm the deletion.

Exercise caution when deleting groups, because any associated group settings such as filtering and other attributes will also be deleted. (For related information, see Regular Expressions in Group Definitions.)

### Gathering Performance Data from Interface Groups

Performance data consists of utilization rates, error rates and broadcast levels for the interfaces that are gathered into an interface group. You can also view the same performance data for each interface in the interface viewer.

Performance data includes configured speed, throughput, percent utilization, percent errors, percent broadcasts and percent discards. Additional information can be displayed through selections from the Columns drop-down list available via column header menus.

By default, performance data collection is disabled for most interface groups. NetMRI provides two ways to enable performance data collection:

• To enable performance data collection for an interface group: In the Settings icon -> Setup section -> Collection and Groups page -> Groups tab -> Interface Groups side tab, hover the mouse over the Action icon and choose Edit, and activate the Performance Statistics Collection checkbox.

By default, collection takes place daily. For some interfaces, you may need to collect performance data more frequently. To do so, select a different setting from the Frequency dropdown. Values include Daily (the default), and incremental values from 15 minutes to 2 minutes.

**Note:** You can use more-frequent data collection only on a select number of interfaces: up to 10% of the total interfaces up to the Interface Limit in the managed network, based on the NetMRI license.

• To enable performance data collection for a specific interface: Open the interface in the Interface Viewer. In the Settings section -> General Settings page, enable Performance Statistics Collection by selecting Enabled from the dropdown menu and clicking Update. (This setting overrides the parent interface group's setting.)

Performance data collection uses interface groups to determine the data types to be collected and stored for each monitored interface. Because collection runs continuously, it needs to be informed when interface group definitions have been changed. Notification is done automatically if one or more group definitions have been changed since the last group generation process was performed (either scheduled or manual). If a definition changes while collection is taking place, the changes will not take effect until the next collection run.

At that point, interface data collection resumes collecting limited data for all interfaces to determine which should be further processed, based on the new definitions.

**Note:** Infoblox recommends that interface group definitions be changed only when necessary, or when data collection is disabled. This reduces the workload on the appliance.

Use interface groups for suppression of certain interface related issues and to modify thresholds for their appearance. Interface group issue suppression removes the need to manually suppress undesirable issue instances and allows for instances that have yet to be raised—and to be suppressed — to be suppressed before they are even raised. You can review interface group issue suppression settings at the Settings icon -> Issue Analysis section -> Issue Group Settings page.
Regular Expressions in Group Definitions

Group membership expressions consist of one or more logical sub-expressions (e.g., equals, like, in), acting on a set of variables (e.g., $Name, $Type) evaluated by boolean operators (e.g., and, or, =>, <=). You can specify any logical membership criteria using sub-expression combinations. Some variables are defined only for certain types of criteria expressions.

Device Variables

NetMRI defines the following device variables that are usable in Device Group, Interface Group, Device-Filter and Section-Filter criteria expressions:

- $ID: unique NetMRI ID for device
- $IPAddress: IP address of the device (e.g., 192.168.1.33)
- $Name: name of the device (e.g., rtr1.netcodia.com)
- $Type: type of the device (e.g., Router, Switch, etc.)
- $Assurance: assurance level for the device type
- $Vendor: vendor of the device (e.g., Cisco)
- $Model: model of the device
- $Version: software version of the device
- $Community: SNMP community of the device
- $sysName: SNMP system name (CPD only)
- $sysDescr: SNMP system description (CPD only)
- $sysLocation: SNMP system location
- $sysName: SNMP system name
- $sysDescr: SNMP system description
- $sysContact: SNMP system contact

Note: All device variables and interface variables are case-insensitive.

Interface Variables

The following variables are defined for interfaces and supported in Interface Group criteria expressions:

- $ifIndex: unique SNMP numeric index for the interface
- $ifDescr: interface description defined by user
- $ifName: interface name
- $ifType: interface type defined by SNMP
- $ifMtu: interface MTU
- $ifPhysAddress: interface MAC address (if any)
- $ifSpeed: interface speed
- $ifAdminStatus: interface administrative status ("up"/"down")
- $ifOperStatus: interface operational status ("up"/"down")
- $ifTrunkStatus: interface trunk status ("on"/"off")
- $Network: returns the name of the network view to which the interface IP address belongs.

Comparison Operators

The following comparison operators are supported in all criteria expressions:

- =, ==, !=, <, <=, =
- eq, ne, gt, lt, ge, le
- =~, !~, like, not like
- =~, !~, regular expression (A non-string value on the left side of operator is converted to a string before comparison.)
- in, not in
- memberOf, not memberOf

Determines if the device or interface is a member of one or more other Device Groups and/or Interface Groups.
hasnetwork
determines if the device or interface is a member of a specific Network View.

Examples:

$ID = 30
$Vendor eq "Cisco"
$Version like /^12.1.*/
$Model in ["cat4506", "3725"]
$IPAddress in [10.1.3.56, 10.2.0.0/16]
memberOf ["Router Group", "Switch Group"]
$Vendor eq "Cisco" and ($Model eq "catalyst2912XL" or $Model eq "cat3548XL")

To perform a case-insensitive match, use the regular expression modifier /i.
Example:

$Name like /core/i

The $Model and $IPAddress values work for creating device groups but cannot be used for building Rules with device attributes under Configuration Management -> Policy Design Center -> Rule.

$Model in ["cat4506", "3725"]
$IPAddress in [10.1.3.56, 10.2.0.0/16]

For Rules in the Policy Design Center, simply use a comma-separated format.

Logical Operators

The following logical operators can be used to combine sub-expressions:

and, &, &&
boolean AND
boolean OR
(grouping

Examples:

$Vendor eq "Cisco" and $Type eq "Router"
($Vendor eq "Juniper" and $Type eq "Router")
or ($Vendor eq "Cisco" and $Type in ["Router", "Switch"])
memberOf ["Routing Group"] and $IPAddress in [10.1.0.0/16, 10.2.3.45]

Regular Expressions Usage

NetMRI uses regular expressions similar to those supported by Cisco, JavaScript and Unix programming languages. Regular expressions supported for table filtering consist of a sequence of special symbols, modifiers and normal characters. NetMRI interprets the following single characters and expressions as follows:

^ Matches the beginning of the string
$ Matches the end of the string
. Matches any single character
[... ] A set of matching characters such as [aeiouA-Z]
[^...] A set of non-matching characters
(... ) A sub-pattern to be modified or remembered
(... |...) A set of alternate sub-patterns
\w Matches any word character; same as [a-zA-Z0-9]
\D Matches any non-word character; same as [\^a-zA-Z0-9]}
\s Matches any whitespace character; same as [\tn\r\f\v]
\s Matches any non-whitespace character; same as \[^\s\t\n\r\f\v\]
\d Matches any digit; same as [0-9]
\D Matches any non-digit; same as [^0-9]

To match any of the special characters above, enter the backslash (\) escape character immediately before them. Avoid spurious or excessive matches. To match all IP addresses starting with an initial octet of 10, use /10\./ as the pattern, not /10./ which matches 10., 100., 101, 102, etc. (remember, dot is a special symbol).

Examples:

$Vendor like /Cis.*$/
$Type like /.*Switch.*$/
$IPAddress like /10\.*[/16]/

Note: A common mistake occurs by using the Unix wildcard syntax (*) instead of the regular expression syntax (.*) to match any sequence of characters.

Using Expression Modifiers

With the special symbols above, the following characters are treated as modifiers that can be used to match against a previous sub-pattern zero, one, or more times:

- `(N)` Match the sub-pattern exactly N times
- `(N,)` Match the sub-pattern N or more times
- `(N,M)` Match at least N times and no more than M times
- `?` Match the sub-pattern 0 or 1 times; same as `{0,1}`
- `*` Match the sub-pattern 0 or more times; same as `{0,}`
- `+` Match the sub-pattern 1 or more times; same as `{1,}`

Modifiers can be used to reduce the size of the expression and to specify optional parts of the expression. They are useful when combined with parentheses to designate sub-patterns.

The pattern

/Se(rial)?\d+$/

matches any serial interface designator, either in the short form (Se0/0) or the long form (Serial12/45).

Examples:

$Vendor like /Cis(co)?$/
ifType like /Se(rial)?\d+$/

You use regular expressions to match values selected from a larger database of values. For economy of effort, it is sometimes easier to specify "just enough" of a pattern to obtain the match. For example, though a valid IPv4 address is formatted as "A.B.C.D" where A, B, C and D range from 0 to 255, an expression

/\^\{d(1-3)\.\}3254$/

ensures that the first three octets are in fact defined as numbers with dots in between, but is unnecessary to find all addresses ending with ".254" when a simpler expression

/\..254$/

which checks for the desired suffix will succeed.