



NetBrain[®] Integrated Edition 10.0

Domain Setup Guide

1. Setup Overview	4
2. Logging in.....	6
3. Creating a Domain.....	7
4. Configuring Share Policy	8
5. Configuring Network Settings	9
6. Discovering Network Devices	12
7. Cleaning Up Domain Issues	18
8. Creating Sites	20
8.1. Creating a Site Hierarchy by Importing a Spreadsheet	21
8.2. Adding a Container Site.....	23
8.3. Adding a Leaf Site.....	24
9. Creating MPLS Clouds.....	26
10. Adding Internet Clouds.....	30
11. Adding Generic Devices.....	33
12. Resolving Duplicated IPs	35
13. Scheduling Benchmark Tasks	37
14. Scheduling Discovery Tasks.....	39
15. Scheduling Data View Template/Parser Task.....	41
16. Scheduling Qapp Tasks.....	42
17. Defining Device Access Policy.....	44
18. Creating a Layout Style	46
19. Viewing Domain Health Report	48

1. Setup Overview

Before end users start to experience NetBrain Integrated Edition, the following preparations must be done to set up your domain:

1. [Log in](#) and [Create a domain](#).
2. [Configure share policy](#).
3. Perform the following actions:

Category	Task	Expected Result
Discovery	Configure Network Settings	<ul style="list-style-type: none">▪ All Front Servers are connected▪ All network credentials are configured
	Discover Network Devices	<ul style="list-style-type: none">▪ All managed network devices are discovered
Fine Tune	Clean Up Domain Issues	Resolve all managed devices under the following categories: <ul style="list-style-type: none">▪ Unknown IP▪ Missed Devices▪ Discovered by SNMP▪ Unknown SNMP sysObjectID▪ Unclassified Network Devices▪ Hostname-Changed Devices
	Create MPLS Clouds	<ul style="list-style-type: none">▪ MPLS Clouds are created based on a full list of CE devices with CLI access
	Add Internet Cloud	<ul style="list-style-type: none">▪ All paths between boundary devices and the Internet are visible and can be calculated successfully
	Add Generic Device	<ul style="list-style-type: none">▪ Devices that cannot be accessed are manually added to the domain
	Resolve Duplicated IPs	<ul style="list-style-type: none">▪ No conflicted IP
Site & System Tasks	Create Sites	<ul style="list-style-type: none">▪ All sites are created▪ No unassigned devices
	Schedule Benchmark Tasks	<ul style="list-style-type: none">▪ Benchmark task is enabled and executed successfully▪ Update Site Maps is enabled
	Schedule Discovery Task (Optional)	<ul style="list-style-type: none">▪ Discovery task is enabled and executed successfully

Category	Task	Expected Result
	Schedule Data View Template/Parser Task	<ul style="list-style-type: none"> All applicable built-in DVTs are enabled and executed successfully
	Schedule Qapp Tasks (Optional)	<ul style="list-style-type: none"> Target tasks are enabled at a proper frequency
Advanced Tasks	Define Device Access Policy (Optional)	<ul style="list-style-type: none"> Users are assigned to corresponding policies as required
	Create Layout Style (Optional)	<ul style="list-style-type: none"> All sites are associated with customized layout
	View Domain Health Report	<ul style="list-style-type: none"> All issues reflected in the report are resolved

2. Logging in

1. In your web browser, navigate to **http(s)://<Hostname or IP address of NetBrain Application Server>/**. For example, **https://10.10.3.142/** or **http://10.10.3.142/**.
2. In the login page, enter your username or email address, and password.

Note: If you are using SSO (Single Sign-On), click the hyperlink of the SSO server to redirect to the login page of your Identity Provider. After your credentials are verified, you will be directly logged in to the system and you can skip step 3.

3. Click **Log In**.
4. Please update the initial password if it is your first-time login.

3. Creating a Domain

1. In the pop-up dialog, select the target tenant and click **New Domain**. The Create Domain Wizard is launched to guide you through the mandatory steps to create a domain.
2. Select the target tenant, enter the basic information for the new domain, and then click **Finish**.

4. Configuring Share Policy

Share Policy refers to the mechanism of authorizing roles and privileges to all users within a tenant. Users can access multiple domains concurrently with different roles assigned.

1. Click the domain name from the quick access toolbar and then click **Domain Management**.
2. In the Domain Management page, select **Operations > Share Policy** from the quick access toolbar. The **Share Policy** tab lists all users who have access to the current tenant.
3. Select a user to assign domain access and more privileges by role. See [Roles and Privileges](#) for more details regarding privilege division.
4. Click **Apply**.

BEFORE YOU CONTINUE:

- If you are migrating from NetBrain Enterprise Edition (version 6.x), refer to [Legacy Data Migration Guide](#) for more details. Then continue with [Scheduling Benchmark Task](#).
- If you are building the domain from scratch, please continue with the following steps.

5. Configuring Network Settings

NetBrain Network Settings collects all the credentials used to access live devices and retrieve device data. Only the users who have the privilege to manage the domain can configure and share the Network Settings.

Desired Outcome: All Front Servers are connected, and all network credentials are configured.

1. In the Domain Management page, select **Operations > Discover Settings > Network Settings** from the quick access toolbar.
2. On the **Network Settings** tab, enter all available credentials of your network devices and jumpbox server information in the corresponding tabs.
 - [Private Key](#)
 - [Jumpbox](#)
 - [Telnet/SSH Login](#)
 - [Privilege Login](#)
 - [SNMP String](#)

Configuring Private Key

The following SSH private key types are supported in the system to access your network devices:

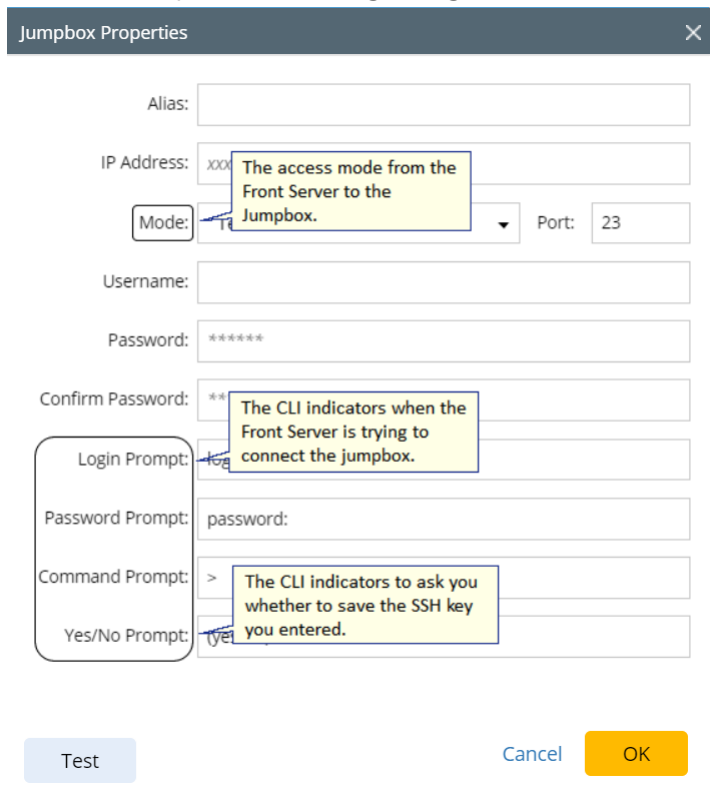
- SSHv1 RSA key
 - SSHv2 RSA key
 - SSHv2 DSA key
- 1) Click the **Private Key** tab.
 - 2) Click **Add** to open the **Private Key Settings** dialog box.
 - 3) Enter an alias and click **Browse** to import your SSH private key file.
 - 4) Enter a passphrase twice if your private key is encrypted.
 - 5) Click **OK**.

Repeat step 2) ~ 5) to add more entries if required.

Configuring Jumpbox

If NetBrain Front Server cannot access your live network directly, you can configure a Jumpbox. The Front Server accesses the Jumpbox first and then retrieve live data via the Jumpbox.

- 1) Click the **Jumpbox** tab.
- 2) Click **Add** to open the following dialog box and enter the required information.



- 3) If your network devices require special commands to access via Telnet or SSH, or require an additional set of credentials, you can click **Advanced** to configure more settings.
- 4) Click **Test** to check whether the connection between the Jumpbox and the Front Server is working. In the pop-up dialog box, you can click **Refresh** to retest the connections.
- 5) Click **OK**.

Configuring Telnet/SSH Login

- 1) Select the **Telnet/SSH Login** tab.
- 2) Click **Add** to open the **Telnet/SSH Login** dialog box.
- 3) Select the authentication method, enter or select the non-privilege login credentials, and click **OK**.

Repeat step 2) and step 3) to add more entries if required.

Configuring Privilege Login

The privilege login credentials refer to the passwords used to enter the enable mode. With these credentials, the system can issue CLI commands on live devices.

- 1) Click the **Privilege Login** tab.
- 2) Click **Add** to open the **Privilege Login** dialog box.
- 3) Enter the access credentials and click **OK**.

Repeat step 2) and step 3) to add more entries if required.

Configuring SNMP Read-Only Community String

- 1) Click the **SNMP String** tab.
- 2) Click **Add** to open the **SNMP Setting** dialog box.
- 3) Select the version of SNMP and enter the required credentials, and then click **OK**.

Repeat step 2) and step 3) to add more entries.

Best Practice:

- [How to Optimize Discovery Performance When Many Front Servers and Network Credentials Exist](#)
- [How to Telnet/SSH Directly from NetBrain](#)

6. Discovering Network Devices

The live network discovery function enables you to discover your network devices and provides a granular view of your network infrastructure.

Desired Outcome: All managed network devices are discovered.

The system provides the following two ways to discover your network.

- [Discovering Network via Seed Routers](#)
- [Discovering Network by Scanning IP Range](#)

Note: Before discovering your network devices, you need to make sure that the connections between NetBrain Front Servers and your live network are working, and all available credentials are configured in the [Network Settings](#) to access your devices.

Note: The time to finish the discovery process depends on your network scale. To narrow down the discovery scope, you can exclude devices by adding them to the [Do-Not-Scan List](#).

Note: [Network Definition](#) is recommended as a workaround if SNMP is not accessible on specific devices temporarily when discovering a network. During the discovery, the system uses the settings in the Network Definition to discover a device when the SNMP of this device fails.

Note: After the discovery, the system will add the newly discovered devices to your domain and perform additional operations, including building Layer 3 topology, synchronizing with sites, and updating the CE devices of the BGP MPLS cloud.

Discovering Network via Seed Routers

A seed router is the starting point where the discovery begins. With the seed router method, all the discovered neighbor devices will be treated as new seeds, until all devices matching the defined [Discovery Depths](#) are discovered. The system enables you to discover all the neighbor devices from the route tables, NDP tables, and SNMP routing protocol neighbors.

1. In the Domain Management page, click **Discover** on the Start Page or select **Operations** > **Discover** from the quick access toolbar.

2. On the **Discover** tab, the method **Discover via Seed Routers** is selected by default. Select one of the following ways to enter one or multiple seed routers:

Domain Management Tenant: BVT_DB1TEN_viuw0M Domain: BVT_DB1DOM_6UeH80 Operations

Start Page **Discover** ✕

Discover View Historical Result: [Select](#)

Discover Devices via **SNMP/CLI** [Network Settings](#)

Method: ☒ Discover via Seed Routers ☐ Scan IP Range Access Mode: **SNMP and SSH/Telnet** ? Discovery Depth:

IP/Hostname: [Import IP List](#) ▼

Discover Devices via **API** [+ Select API Servers](#)

API Servers:

[Advanced Options](#) ▼ [Start Discovery](#)

- Enter seed IP addresses directly in the blank field, separated by semicolons. The live network discovery starts from these IP addresses.
- If you already have any devices discovered in your domain, click **Select Devices**.
- Import a **.csv** or a **.txt** file by clicking **Import IP list**. Here is a sample list for your reference:

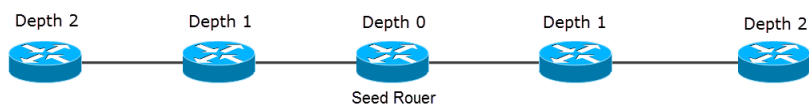
	A	B	C	D	E	F	G
1	192.168.0.1						
2	192.168.10.1						
3	192.168.20.1						
4	10.10.0.1						
5	10.10.10.1						

3. Select one of the following options from the **Access Mode** drop-down list.
- **SNMP and Telnet** — retrieve vendor and model information via SNMP first, and then log in to devices by using Telnet to retrieve live data.
 - **SNMP and SSH** — retrieve vendor and model information via SNMP first, and then log in to devices by using SSH to retrieve live data.
 - **SNMP and Telnet/SSH** — retrieve vendor and model information via SNMP first, and then log in to devices by using Telnet to retrieve live data; if Telnet doesn't work, then use SSH.
 - **SNMP and SSH/Telnet** — retrieve vendor and model information via SNMP first, and then log in to devices by using SSH to retrieve live data; if SSH doesn't work, then use Telnet.
 - **SNMP Only** — retrieve live data via SNMP only.

Note: The data retrieved via SNMP only might be incomplete.

4. Set the discovery depth by entering a value between 0 and 255.
- It refers to how deep you want the discovery to go. That is, how many levels of neighbors are explored from the seed

router (the neighbors can include NDP neighbors, routing protocol neighbors, and next-hops in route tables, which depend on your [configurations](#)). Here is a sample for discovery depth.



5. Click **Advanced Options** to configure more settings:

- **Run additional operations after discovery** — choose to whether to run the additional operations for the discovery, including updating MPLS Cloud CE list, building IPv4 L3 topology, sites and so on. It is recommended to keep this option checked, otherwise the discovered devices will not be ready until the benchmark task finishes.
- **Retrieve device/module/interface information** — choose to whether to retrieve the device/module/interface information for certain discovery (for example, AWS discovery to merge the multi-source devices and Juniper discovery for complete MIB information).
- **CLI Forced Timeout** — the time limit of each CLI command to retrieve live data from a device. The default value is 600 seconds.
- **Use NDP to discover neighbor devices** — discover neighbor devices by looking up an NDP table.
- **Find routing protocol neighbor via SNMP** — retrieve routing protocol (such as BGP, EIGRP, and OSPF) neighbors via SNMP.
- **Use CLI routing table to discover next-hops** — discover neighbor devices from route tables retrieved by CLI commands.
- **Scan destination subnets** — continue to scan all destination subnets in the route tables of the devices that are discovered in the last depth.

Note: The option is only available when the **Use CLI routing table to discover next-hops** option is selected.

- **Scan all connected subnets** — continue to scan all directly connected subnets of the devices that are discovered in the last depth.
 - **Minimum mask bits** — scan subnets with mask exceeding the threshold. The default value is 24 and can be configured between 22 and 32.

6. Click **Start Discovery**.

- When the discovery task is finished, the discovered devices are automatically added to the current domain.

Device Type	Count
Cisco Router	20
Cisco IOS Switch	54
Cisco ASA Fire...	10
Cisco Catalyst S...	1
Juniper EX Switch	2
Arista Switch	2
Extreme Switch	1
Cisco PIX Firewall	1
Avaya Switch	2
HP ProCurve Sw...	1
Juniper SRX Fire...	1
NetScreen Fire...	1
End System	65
Cisco WLC	1
3Com Switch	1
Cisco Nexus Swi...	8
Unclassified De...	1
Cisco WAP	1
Aruba WLC	1
Aruba IAP	1
Dell Sonicwall	1
Dell Force10 Sw...	1

You can click **Discovery Report** to view the access log of discovered devices or click **Execution Log** to view the execution log of the entire discovery process.

Discovering Network by Scanning IP Range

The scanning method only discovers devices in the specified IP range or subnet. It is recommended to use this method to discover a large-scale network, which is divided into subnets and each of which occupies a range of IP addresses.

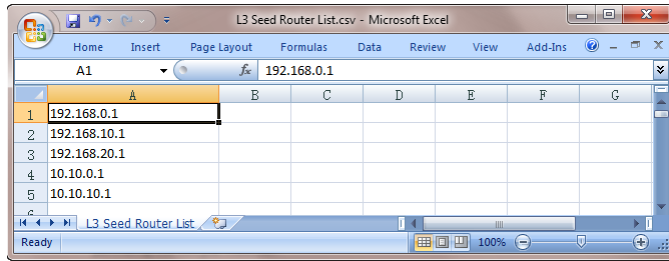
- Click **Discover** on the Start Page or select **Operations** > **Discover** from the quick access toolbar.
- On the **Discover** tab, select **Scan IP Range** and use one of the following ways to specify the IP range:

Device Type	Count
Cisco Router	20
Cisco IOS Switch	54
Cisco ASA Fire...	10
Cisco Catalyst S...	1
Juniper EX Switch	2
Arista Switch	2
Extreme Switch	1
Cisco PIX Firewall	1
Avaya Switch	2
HP ProCurve Sw...	1
Juniper SRX Fire...	1
NetScreen Fire...	1
End System	65
Cisco WLC	1
3Com Switch	1
Cisco Nexus Swi...	8
Unclassified De...	1
Cisco WAP	1
Aruba WLC	1
Aruba IAP	1
Dell Sonicwall	1
Dell Force10 Sw...	1

- Enter an IP range directly in the blank field, separated by semicolons. For example, enter **192.168.2.1** as a single IP address; enter **10.10.10.1/24** as a segment address; enter **10.10.10.1-10.10.10.6** as an IP range.

Note: Under the premise of meeting the requirements, it is highly recommended to enter a segment address as small as enough to ensure a smooth discovery process.

- Import a **.csv** or a **.txt** file by clicking Import IP list. Here is a sample list for your reference:

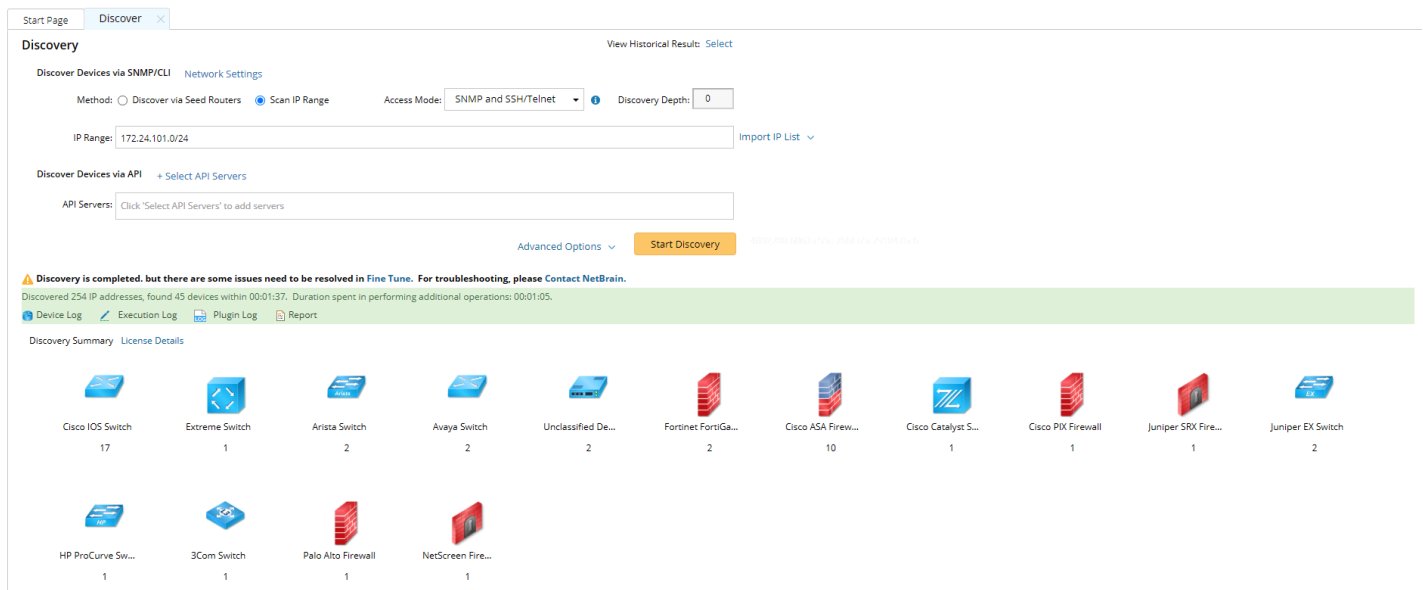


3. Select one of the following options from the drop-down list of the **Access Mode** field.

- **SNMP and Telnet** — retrieve vendor and model information via SNMP first, and then log in to devices by using Telnet to retrieve live data.
- **SNMP and SSH** — retrieve vendor and model information via SNMP first, and then log in to devices by using SSH to retrieve live data.
- **SNMP and Telnet/SSH** — retrieve vendor and model information via SNMP first, and then log in to devices by using Telnet to retrieve live data; if Telnet doesn't work, then use SSH.
- **SNMP and SSH/Telnet** — retrieve vendor and model information via SNMP first, and then log in to devices by using SSH to retrieve live data; if SSH doesn't work, then use Telnet.
- **SNMP Only** — retrieve live data via SNMP only.

Note: The data retrieved via SNMP only might be incomplete.

4. To specify the proxies and credentials to be used in the discovery, click **Network Settings** to adjust.
5. Click **Start Discovery**.
6. When the discovery task is finished, the discovered devices are automatically added to the current domain.



You can click **Discovery Report** to view the access log of discovered devices or click **Execution Log** to view the execution log of the entire discovery process.

Best Practice:

- [How to Discover a Network from an IP Address or Subnet List](#)
- [How to Discover Devices without SNMP Access](#)
- [How to Increase Telnet/SSH Timeout Value When Discovery Times Out](#)
- [How to Prevent NetBrain from Discovering Certain Devices](#)

7. Cleaning Up Domain Issues

Creating and maintaining a domain with all devices properly discovered is the key to keep system data up-to-date to guarantee data accuracy and further utilize advanced features, such as path and map.

Fine Tune provides an overview of how devices are discovered, where you can get started to fix all the access issues. The devices listed in each category are updated as soon as a discovery task is completed, including both the on-demand discovery and the scheduled discovery. It's recommended to check and maintain in the Fine Tune at least once a week or whenever a discovery task is completed.

1. In the Domain Management page, click **Fine Tune** on the Start Page or select **Operations > Fine Tune** from the quick access toolbar.
2. Resolve the issues under the following categories:
 - **[SNMP-Only Devices](#)** — the devices accessed by SNMP but failed to be accessed via Telnet/SSH.
 - **Desired Outcome:** Fix Telnet/SSH access issues on all devices in this list that use these protocols. This list should only contain devices that are SNMP-only.
 - **[Missed Devices](#)** — the devices existing in the current domain but failed to be verified during a discovery.
 - **Desired Outcome:** Fix device access issues or remove decommissioned devices in this list to bring the number of devices down to 0.
 - **[Unknown SNMP SysObjectID](#)** — the devices whose SysObjectIDs are not defined in the Vendor Model table.
 - **Desired Outcome:** Add all unknown OIDs in this list to the vendor model table to decrease the number down to 0.
 - **[Unknown IP](#)** — the IP addresses that cannot be accessed via Telnet/SSH and SNMP in the **Discover via Seed Routers** method during a discovery.
 - **Desired Outcome:** Fix all known IPs with correct Telnet/SSH/SNMP in this list.
 - **[SSH Fingerprint Check Failed](#)** — the devices whose current fingerprint keys are different with the latest ones retrieved during live access.
 - **Desired Outcome:** All devices with SSH fingerprint check failed are resolved.
 - **[Hostname-Changed Device](#)** — the device whose hostname is changed and exists with more than one hostname in a domain.
 - **Desired Outcome:** All devices with hostname change are detected and the desired ones remain in the domain.

Tip: You can click [Discovered Devices](#) to view the devices discovered successfully.

Best Practice:



- [How to Remove Devices from Domain](#)
- [How to Identify a List of Devices That Have Lost Access for Certain Days in the System](#)
- [How to Manage Devices with Inconsistent Hostnames Retrieved via SNMP and CLI](#)

8. Creating Sites

Site is a geographical grouping of network devices, which can be used as device scopes, asset filters, and map/topology views. For example, you can divide your network into a hierarchy of sites based on country, state, city, region, and office location.

Desired Outcome: All sites are created and there is no device listed in the **Unassigned** node.

There are two types of sites in the system:

- **Container Site** () — a parent site that contains leaf sites and other container sites. No devices are directly nested under a container site.
- **Leaf Site** () — a child site that contains devices. The devices can be added manually or searched dynamically.

Site Manager is used to manage and maintain the sites in your domain. You can use either of the following ways to create or maintain a site hierarchy:

- [Create a Site Hierarchy by Importing a Spreadsheet](#)
- Manually create sites:
 - [Create a Container Site](#)
 - [Create a Leaf Site](#)

8.1. Creating a Site Hierarchy by Importing a Spreadsheet

1. Prepare a spreadsheet with the table headers organized as follows to set the site hierarchy. Here is an [example](#):

Site Name (Office)\City\State\Country\Region\Device Hostname

	A	B	C	D	E	F	G
1	Site	City	State	Country	Region	Device Hostname	Device IP Address
	BJ	CANTON	MASSACHUSETTS	United States of America	US_Canada	BJ_Acc_SW1 BJ_Acc_SW6 BJ_Acc_SW4 BJ_Dis_SW1 BJ_Dis_SW2 BJ_L2_Core_3 BJ_L2_Core_4 BJ_L2_test_1 BJ_core_3550	
2	Canton_NB2	CANTON	MASSACHUSETTS	United States of America	US_Canada	sw2960-130 sw3560-123 sw3560-127 sw3560-128 sw3850-102 sw3850-103	
3	BOS	BOSTON	MASSACHUSETTS	United States of America	US_Canada	BST BST,POP1 BSTX.Core	
4	NY	BOSTON	MASSACHUSETTS	United States of America	US_Canada	NY-core-bak NY_Core NY_DIS NY_POPP NY_Router	
5	BOS_NB_SITE2	BOSTON	MASSACHUSETTS	United States of America	US_Canada	EX2200-1 EX2200-2 GW2Lab LA.DIS,1 LA_POP	
6							
7	Beverly_NB1	BEVERLY	MASSACHUSETTS	United States of America	US_Canada		

Note: Only the **.csv**, **.xls**, and **.xlsx** formats are supported. You can add more column headers or leave some columns blank based on your network distribution.

Note: The site name cannot contain any special characters, such as `\ / : * ? " < > | . $`

Note: The values in the **Device Hostname** column must be the same as those in the domain so that the devices can be identified and added to the corresponding leaf sites.

Note: The value in the **Device IP Address** column will be set as the criteria to search for site members. Only one IP address is supported in each row. You can leave it blank if not required.

2. In the Domain Management page, click **Site** on the Start Page or select **Operations > Site Manager** from the quick access toolbar.
3. In the Site Manager, click **Import from File** to select the prepared file, and click **Open**.
4. Configure the following settings.

- 1) On the **Define Site Hierarchy** tab, select table headers for each level to define the site hierarchy. By default, five levels are provided, and you can add more levels. In this example, you can define the site hierarchy as follows:

The screenshot shows a dialog box titled "Import File to Create Site" with a close button (X) in the top right corner. It has three tabs: "Define Site Hierarchy" (selected), "Add Site Properties", and "Add Site Identification". Under the "Define Site Hierarchy" tab, there is a section titled "Assign column name for each site level:". Below this, there are five rows, each with a label "Level 1:" through "Level 5:", a dropdown menu, and a blue "X" button to its right. The dropdowns are set to "Region", "Country", "State", "City", and "Site" respectively. Below these rows is another dropdown menu labeled "Add a New Level". At the bottom of the dialog, there is a checkbox labeled "Recreate Site Hierarchy" which is unchecked, and two buttons: "Cancel" and "OK".

- 2) On the **Add Site Properties** tab, select the table headers to set the site properties for each level.
- 3) On the **Add Site Identification** tab, select the table headers for the following site identification fields:
 - **Device Hostname** — select the **Device Hostname** table header from the list for device identification.
 - **Device IP Address** — select the **Device IP Address** table header from the list. Leave it blank if this column is not in the imported spreadsheet.

- Click **OK**. The site nodes are created in the site tree.

The screenshot shows the Site Manager interface with the Site Definition tab selected. The left sidebar displays a hierarchical tree of site nodes, with 'BOS(3)' selected. The main panel contains the following sections:

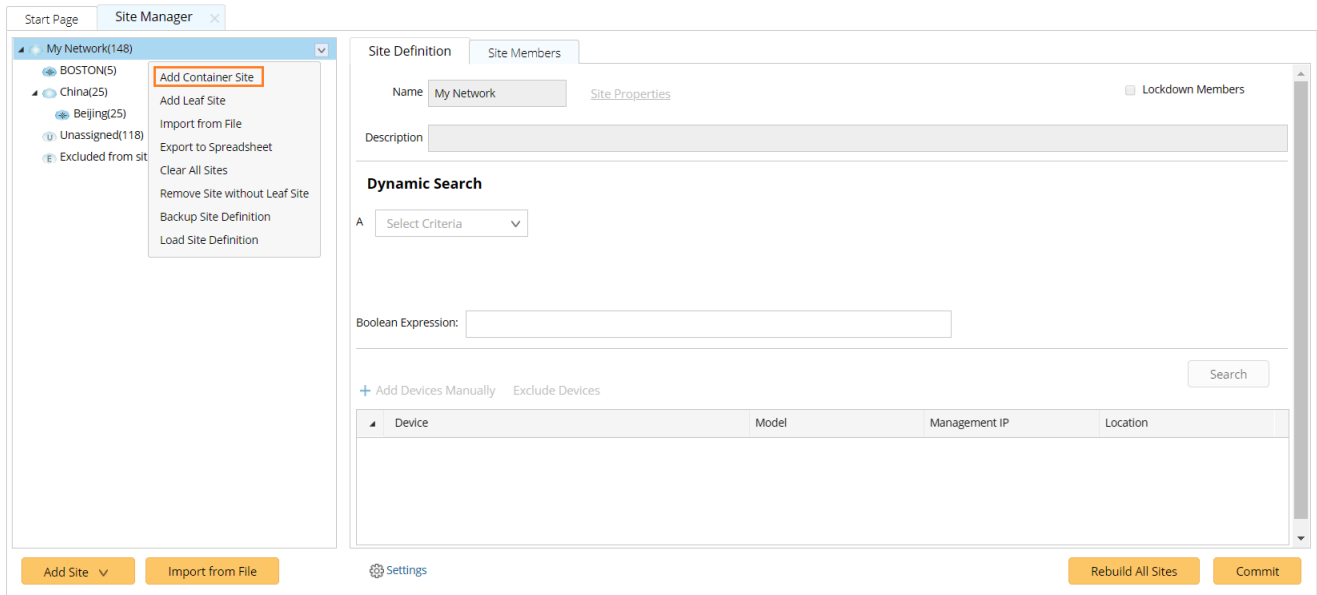
- Site Definition** tab: Includes a 'Name' field with 'BOS', a 'Description' field, and a 'Lockdown Members' checkbox.
- Dynamic Search** section: Contains three rows (A, B, C) for defining search criteria. Row A and B are set to 'IPv4 Address' and 'Matches' with the value '172.24.10.250;172.24.32.2;172.24.32.'. Row C is set to 'Select Criteria'. A 'Boolean Expression' field shows 'A or B'.
- Search** button: A yellow button to execute the search.
- Table**: A table with columns 'Device', 'Model', 'Management IP', and 'Location'. It lists three manually added devices: 'BST' (Model 2514, IP 172.24.10.250), 'BST_POP1' (Model 2500, IP 172.24.255.7), and 'BSTX.Core' (Model 2621, IP 172.24.255.5).
- Buttons**: 'Add Site', 'Import from File', 'Settings', 'Rebuild All Sites', and 'Commit'.

- Click **Rebuild All Sites** to rebuild the site topology. The **Site Members** tab opens automatically, listing the device members in the currently selected site.
- Click **Commit** to commit the site changes.

8.2. Adding a Container Site

- In the Domain Management page, click **Site** on the Start Page or select **Operations > Site Manager** from the quick access toolbar.

2. In the Site Manager, right-click the **My Network** root node in the site tree and then select **Add Container Site**.



3. On the **Site Definition** tab, enter the site name and click **Site Properties** to set the site properties.
4. Click **OK**.

Tip: You can add one or more container sites or leaf sites to a container site. However, you cannot assign any devices to a container site directly.

8.3. Adding a Leaf Site

1. In the Site Manager, right-click the **My Network** root node in the site tree and then select **Add Leaf Site**.
2. On the **Site Definition** tab, enter the leaf site name and click **Site Properties** to set the site properties.
3. Add devices to the leaf site by using either of the following ways.
 - **Dynamic Search** — specify search criteria and a boolean expression and then click **Search**.
 - **Manually Add** — click **Add Devices Manually** and then pick out devices from a device group, a site, or a device type.

Tip: A device can only be assigned to one leaf site.

4. Click **Rebuild All Sites** to rebuild the site topology.

Tip: To exclude specific device types from being involved in any site build or topology build, click **Settings** in the bottom of the **Site Manager** pane to select target device types.

5. Click **Commit** to commit the site changes.

Best Practice:

- [How to Keep Site Maps Up-to-Date](#)

9. Creating MPLS Clouds

Generally, geographically dispersed networks are connected through the MPLS VPN network of an Internet Service Provider (ISP). The system introduces a concept called MPLS Cloud to simulate the MPLS functions by following the rules of forwarding labeled packets. In the system, an MPLS Cloud is taken as a device and uses a virtual routing table to calculate A-B paths across the MPLS.

Desired Outcome: All MPLS clouds that are created based on a full list of CE devices are with CLI access.

Adding an MPLS Cloud

1. In the Domain Management page, click **Fine Tune** on the Start Page or select **Operations > Fine Tune** from the quick access toolbar.
2. On the **Fine Tune** tab, select **Cloud Manager** in the left pane and click **Add** in the right pane.
3. In the **Cloud Definition** dialog box, follow the steps below to define an MPLS Cloud.
 - 1) Enter a name for the cloud.
 - 2) Keep the default Cloud Type **MPLS L3 VPN**.
 - 3) Enter a description of the MPLS cloud.
 - 4) Add MPLS edge devices to the MPLS Cloud by either of the following ways:

▼ Dynamic Search

- 1) Click **Dynamic Search Interface**.
- 2) In the pop-up dialog, select **By BGP AS** (autonomous system) to add edge devices and interfaces based on BGP AS number and VRF.

Dynamic Search Interface by BGP AS

Input remote AS# or BGP neighbor. Use semicolon to separate multiple items.

BGP AS#:

VRF name:

Exclude Device

Define criteria to make your search result more accurate.

A

Select Criteria

Boolean Expression:

Search Result:

Search

Device Name	Interface
SanJose_Core	FastEthernet0/1.1

Auto update searched device and interface

Cancel

OK

- 3) Enter BGP AS number and VRF name.

Tip: VRF is used to establish the correct connections if some devices have duplicated IP addresses. You can enter multiple VRF names and use semicolons (;) to separate them. Interfaces that have the matched VRF names will be searched out. If you don't want to use the VRF name as a condition to filter interfaces, left it empty; if you want to search interfaces without VRF configured, enter 'global' (single quotes must be included).

Tip: Through a specified BGP AS number, a device that meets all the following conditions will be added as a CE device:

- The devices not only configured with EBGP Neighbor but also pointing to the defined AS number.
- The non-loopback interface in the same network segment with EBGP Neighbor IP configured on the device.
- The neighbor IP of CE devices does not exist in the domain.

- 4) Click **Search**.

5) Review the search result, click **OK**.

▼ Manually Add

1) Click **Static Interface**.

2) In the pop-up dialog, specify the properties of the CE device.

a) Click **Browse** to select the CE device.

The screenshot shows the 'Add Static Interface' dialog box. It contains the following fields and values:

- * CE Device: BJ_Acc_SW1 (with a 'Browse' button)
- * CE Interface: FastEthernet0/1 (dropdown menu)
- VRF on Interface: (empty text box)
- CE Interface Description: (empty text box)
- * IP of PE Interface: 172.168.1.1
- * PE Interface: PE_INT
- VPN: 1

Buttons at the bottom: Close, OK.

b) Select the interface of the CE device connected to the PE device.

c) Enter the VRF name of the CE interface if it has been configured with a VRF.

d) Enter the description of the CE interface.

e) Enter the IP address of the PE interface that the CE interface connects to.

f) Enter the name of the PE interface. The PE interface name can be any strings, and you can name it based on your needs.

g) Enter a VPN value for the CE device.

Note: Assign the same VPN value to those CE devices in different sites that have communications with each other. When the system builds a routing table for an MPLS cloud, CE devices with the same VPN value will be added to one virtual routing table. If the VPN field is left empty, the system will determine that all CE devices in an MPLS cloud communicate with each other.

3) Add more CE devices to the MPLS Cloud by following step 2.

4) Click **OK**.

5. (Optional) Click **Exclude** to select CE devices or interfaces that you want to exclude from the MPLS cloud.

6. Click **OK**.

Tip: To make the MPLS cloud participate in path calculation, go to the **Additional Operations after Benchmark** tab to build the topology and NCT. See [Benchmark Task Settings](#) for more details.

Best Practice:

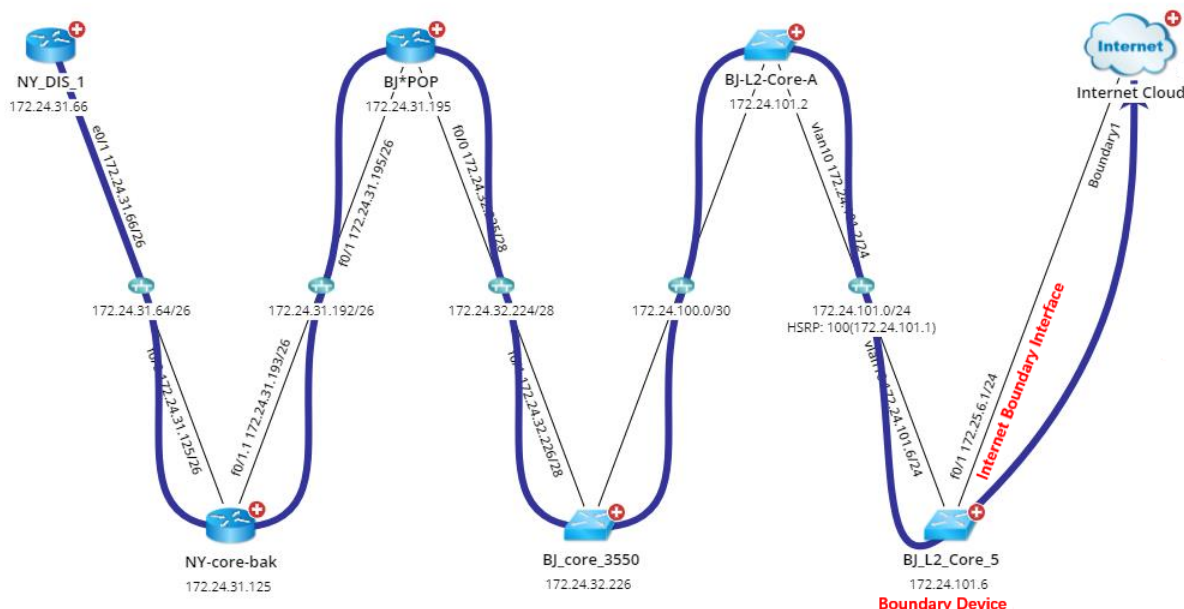
- [How to Create MPLS Cloud if PE-CE Is Not Running BGP](#)
- [How to Create Multiple MPLS Clouds with the Same AS Number](#)

10. Adding Internet Clouds

Internet Cloud refers to the Internet that the boundary device connects to. In general, an Internet Cloud is considered as a device, and it can be assigned an interface either manually or automatically. With the Internet Cloud, you can view the path between the Internet and the boundary device on a map.

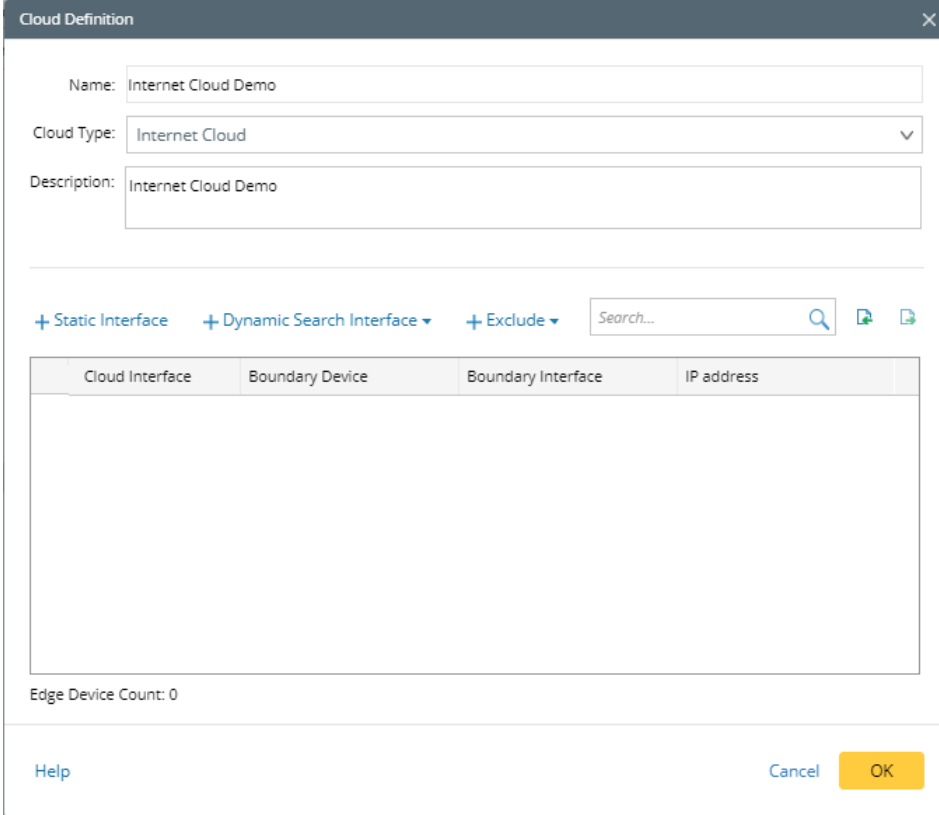
Desired Outcome: All paths between boundary devices and the Internet are visible and can be calculated successfully.

Here is an example of a path through the Internet.



1. In the Domain Management page, click **Fine Tune** on the Start Page or select **Operations > Fine Tune** from the quick access toolbar.
2. On the **Fine Tune** tab, select **Cloud Manager** in the left pane and click **Add** in the right pane.
3. In the **Cloud Definition** dialog box, follow the steps below to define an Internet Cloud.
 - 1) Enter a name for the cloud.
 - 2) Change the Cloud Type to **Internet Cloud**.

3) Enter a description of the Internet cloud.



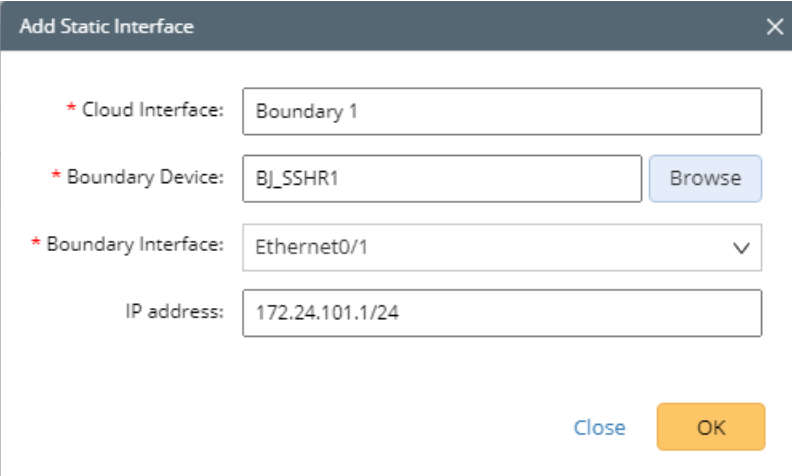
The 'Cloud Definition' dialog box is shown. It has a title bar with a close button. Inside, there are three input fields: 'Name' with the value 'Internet Cloud Demo', 'Cloud Type' with a dropdown menu showing 'Internet Cloud', and 'Description' with the value 'Internet Cloud Demo'. Below these fields is a horizontal separator. Under the separator, there are three buttons: '+ Static Interface', '+ Dynamic Search Interface', and '+ Exclude'. To the right of these buttons is a search bar with the placeholder text 'Search...'. Below the buttons and search bar is a table with four columns: 'Cloud Interface', 'Boundary Device', 'Boundary Interface', and 'IP address'. The table is currently empty. Below the table, it says 'Edge Device Count: 0'. At the bottom of the dialog, there are three buttons: 'Help', 'Cancel', and 'OK'.

4) Add Internet Cloud and boundary device information by either of the following ways:

▼ **Manually Add**

1) Click **Static Interface**.

2) In the pop-up dialog, specify the properties of the cloud and boundary device.



The 'Add Static Interface' dialog box is shown. It has a title bar with a close button. Inside, there are four input fields: '* Cloud Interface' with the value 'Boundary 1', '* Boundary Device' with the value 'BJ_SSHR1' and a 'Browse' button to its right, '* Boundary Interface' with a dropdown menu showing 'Ethernet0/1', and 'IP address' with the value '172.24.101.1/24'. At the bottom right, there are two buttons: 'Close' and 'OK'.

a) Enter a cloud interface name.

b) Click **Browse** to select the boundary device.

c) Select a boundary interface from the drop-down list.

- d) Enter the IP address of the cloud.
- 3) Add more boundary devices to the Internet Cloud by following step 2).
- 4) Click **OK**.

▼ Dynamic Search

- 1) Click **Dynamic Search Interface**.
- 2) In the pop-up dialog, select **By Advanced Search** to find the boundary devices and interfaces.

Dynamic Search Interface by Advanced Search

Search Scope: All Devices

Device Criteria:

A Device Main Type Router, L3 Switch, Firewall

B Select Criteria

Boolean Expression: A

Interface Criteria:

A IPv4 Address Matches 172.24.101.1

B Select Criteria

Boolean Expression: A

Search

Search Result:

Device Name	Interface
-------------	-----------

Cancel OK

- a) Specify Device Criteria.
- b) Specify Interface Criteria.
- c) Click Search.
- 3) Add more boundary devices to the Internet Cloud by following step 2).
- 4) Review the search result, click **OK**.

5. Click **OK**.

Tip: It is required to manually perform benchmark task or build topology after adding Internet Clouds.

Tip: You can also click **Exclude** to select boundary devices or interfaces that you want to exclude from the connection with internet cloud.

11. Adding Generic Devices

When the system attempts to discover devices from a real network, there may be some devices that you don't have live access. You can manually add such devices to your domain.

Desired Outcome: Devices that cannot be accessed are manually added to the domain.

Complete the following steps to manually add a device to your domain:

1. In the Domain Management page, click **Fine Tune** on the Start Page or select **Operations > Fine Tune** from the quick access toolbar.
2. On the **Fine Tune** tab, click **Generic Device** in the left pane.
3. Click **Add** and define the generic device information.
 - 1) In the **Add Generic Device** pane, enter the hostname and management IP, and select the device type from the drop-down list. The device driver is automatically selected based on the device type.
 - 2) Click **Add** in the **L3 Interface Information** area to define the L3 interface properties according to the actual situation, such as interface name and VRF name. Then click **OK**.

The screenshot shows the 'Add Generic Device' dialog box. In the background, the 'Add Generic Device' pane has fields for '*Hostname:' (endsystem-generic), '*Management IP:' (10.12.122.41), and 'Device Type:' (End System). Below these are sections for 'L3 Interface Information' and 'L2 Interface Information', each with a '+ Add' button. An orange arrow points from the '+ Add' button in the 'L3 Interface Information' section to the 'Add Interface Properties' sub-dialog box in the foreground.

The 'Add Interface Properties' sub-dialog box contains the following fields:

- Interface Type: Physical (dropdown menu)
- *Interface Name: port1
- MAC Address: FFFF:345E:CC44
- IPv4 Address: 10.12.122.41/24
- IPv6 Address: 2001::1/64
- IPv6 Link Local Address: fe80::d1df:1f75:cb93:18de/16
- VRF Name: VRF1
- Description: (empty text area)

At the bottom of the sub-dialog are 'Cancel' and 'OK' buttons. The main dialog also has 'Cancel' and 'OK' buttons at the bottom right.

- 3) Click **Add** in the **L2 Interface Information** area to define the L2 interface properties according to the actual situation. Then click **OK**.

Add Generic Device

*Hostname: endsystem-generic *Management IP: 10.12.122.41

Device Type: End System Device Driver: End System

L3 Interface Information + Add

Interface Name	MAC Address	IPv4 Address	IPv6 Address	VRF	Interface Type
port1		10.12.122.41/24		VRF1	Physical

L2 Interface Information + Add

Port Name

Add Port Properties

*Port Name: port2

Mode: access

VLAN: 10

Note: You can input multi-VLAN under trunk or multiple modes, e.g. All, 1, 3-10

Cancel OK

4. Click **OK**.

Tip: To make the added device participate in path calculation, right-click the target device entry, and manually create a fix-up route table for it.

5. To find the added device, click **Site** on the taskbar, then input the device name **endsystem-generic** in the device search bar and press the **Enter** key on your keyboard.

Prerequisite: Rebuild the L3 topology in Topology Link Manager.

NetBrain Search for device, configuration text... Path

Site

Search... endsystem

Hostname	Vendor	Model	Management ...
endsystem-generic			10.12.122.41

12. Resolving Duplicated IPs

The duplicate IPs refer to the interfaces configured with the same IPv4 addresses.

During the live network discovery, the system parses the VRF and IPv4 address for each interface and deals with the interfaces of duplicated IPs as follows:

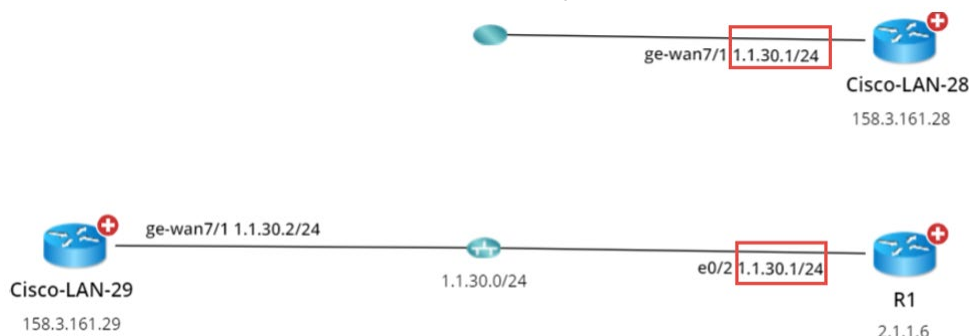
- If two interfaces are configured with the same IP address, but with different VRFs, then two zones named after the VRFs will be created automatically after the IPv4 L3 topology is built, and these two interfaces will be moved to the corresponding zone according to its configured VRF. The system automatically performs this operation by default. To disable it, go to the **Domain Management** page, click **Operations**, point to **Domain Settings**, select **Advanced Settings**, and uncheck the **Automatically create zones and assign VRF interface based on VRF names** option.
- If two interfaces are configured with the same IP address, but without VRFs configured, these two interfaces will be moved to the Default Zone. To separate the two interfaces, you must create a zone manually, then move one of the interfaces and its neighbor interfaces into the created zone, and finally rebuild the IPv4 L3 topology.

Tip: The Default Zone is auto-generated in each domain by the system to store interfaces in IPv4 L3 topology by default. It can neither be renamed nor deleted.

After the interfaces of duplicated IPs being moved into different zones, all duplicated IPs can be involved in IPv4 L3 topology link calculations. When you extend IPv4 L3 neighbors, all calculated links can be displayed on the same map page. Leaving duplicated IPs unresolved will lead to no L3 links on the interfaces with duplicated IP.

Desired Outcome: All interfaces of duplicated IPs are moved into different zones. No interfaces are listed with **Yes** in the **IP Conflicted** column.

Example: Devices "R1" and "Cisco-LAN-28" are configured with the same IP address, but without VRF configured. The device "Cisco-LAN-29" in a real network should be connected to the device "Cisco-LAN-28", but now it is wrongly connected to the device "R1" because of the duplicated IP issue.



1. In the Domain Management page, click **Fine Tune** on the Start Page and then click **Duplicated IP and Subnet Manager** on the left pane. All subnets that contain duplicate IPs in the **Default Zone** are listed by default.

2. Create a zone.
 - 1) Click **New zone**.
 - 2) Enter the zone name, for example, **Zone1** and press **Enter**.
3. Move the interface of duplicated IP and its neighbor interface that can be connected correctly to the **Zone1** and rebuild the IPv4 L3 topology.
 - 1) Select the interface of duplicated IP and its neighbor interfaces that you want to establish the topology link, and then right-click to select **Move to**. In this example, select the **GE-WAN7/1** interface of the **Cisco-LAN-29** device and the **GE-WAN7/1** interface of the **Cisco-LAN-28** device, and then right-click to select **Move to**.

Subnet	Device Name	Interface Name	IP Address	IP Conflicted	VRF	Interface Description
1.1.30.0/24 - (Default Zone) (3)	Cisco-LAN-29	GE-WAN7/1	1.1.30.1/24	Yes		
	R1	Move to	1.1.30.1/24	Yes		
	Cisco-LAN-28	GE-WAN7/1	1.1.30.2/24	No		

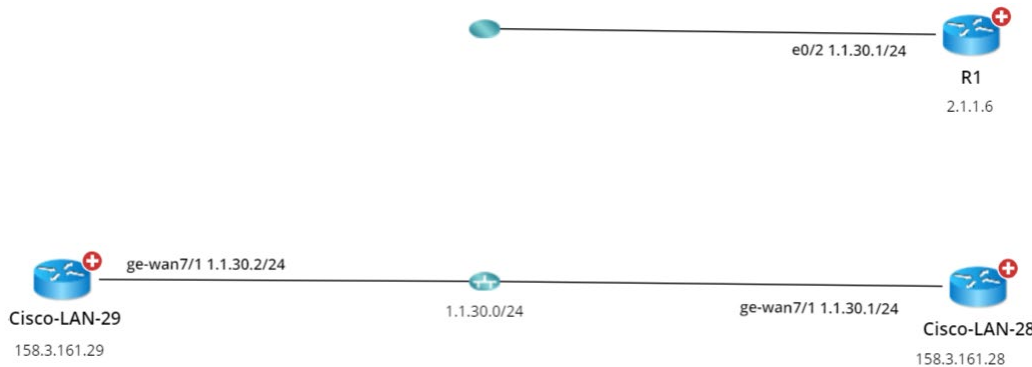
Tip: If a lot of duplicated subnets are detected in the Default Zone, you can quickly search them within the **Search bar**. Use semicolons to separate the multiple items.

- 2) Select **Zone1** that you created and click **OK**.

Note: The **Move to** operation will delete all the manually added topology links of this interface.

- 3) Click **Yes** in the pop-up dialog box to rebuild the IPv4 Layer 3 topology.

After the system finishes building the topology, the topology links are correctly connected.



Best Practice:

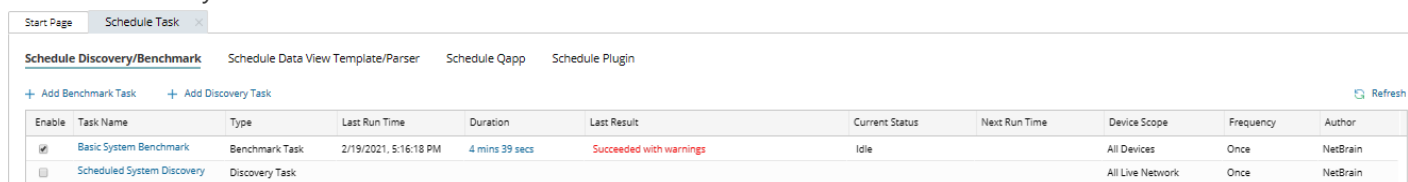
- [How to Manually Build or Change L3/L2 Topology Links on Demand](#)

13. Scheduling Benchmark Tasks

Basic System Benchmark task can regularly collect live data as baselines to build topology, and calculate paths, device groups, sites, and MPLS Virtual Route Tables. The network data to be retrieved are predefined in the task, and the task will be executed on all your domain devices by default.

Desired Outcome: System benchmark is scheduled with **Update Site Maps** enabled.

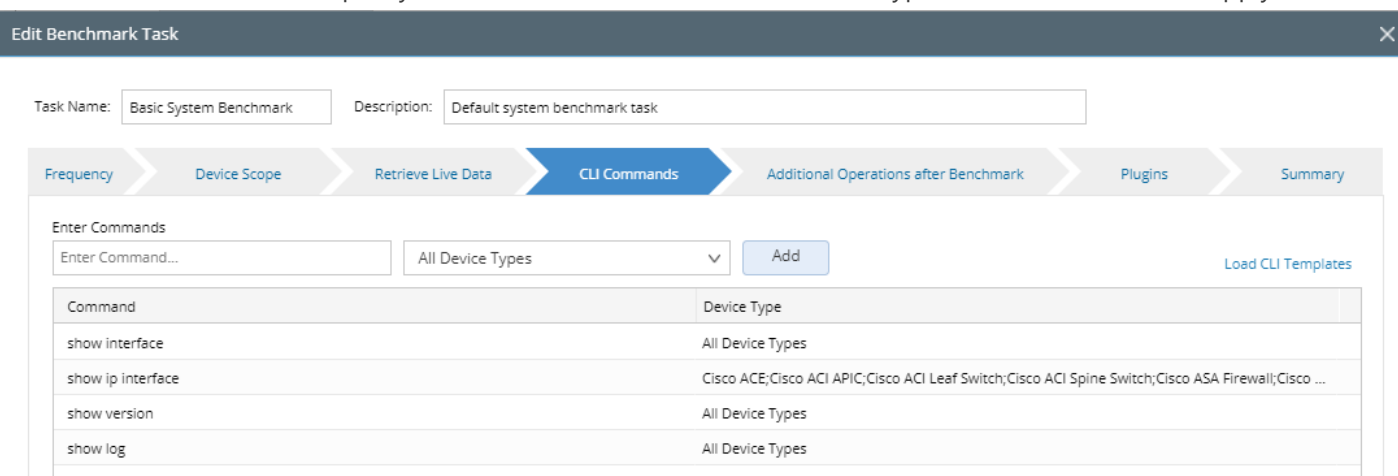
1. In the Domain Management page, select **Operations > Schedule Task** from the quick access toolbar.
2. On the **Schedule Task > Schedule Discovery/Benchmark** tab, select the **Enable** check box for the **Basic System Benchmark** entry.



The screenshot shows the 'Schedule Task' page with the 'Schedule Discovery/Benchmark' tab selected. A table lists the tasks:

Enable	Task Name	Type	Last Run Time	Duration	Last Result	Current Status	Next Run Time	Device Scope	Frequency	Author
<input checked="" type="checkbox"/>	Basic System Benchmark	Benchmark Task	2/19/2021, 5:16:18 PM	4 mins 39 secs	Succeeded with warnings	Idle		All Devices	Once	NetBrain
<input type="checkbox"/>	Scheduled System Discovery	Discovery Task						All Live Network	Once	NetBrain

3. Click **Basic System Benchmark** to configure the task settings.
 - 1) On the **Frequency** tab, specify the task execution frequency.
 - 2) On the **Device Scope** tab, add the target devices for this task. You can also exclude unwanted devices by clicking the **Exclude Device Group** area.
 - 3) On the **Retrieve Live Data** tab, select the target data to be retrieved.
 - 4) On the **CLI Commands** tab, specify CLI commands and select which device types these commands can apply to.



The screenshot shows the 'Edit Benchmark Task' configuration page, specifically the 'CLI Commands' tab. It includes a table of predefined CLI commands and their applicable device types.

Command	Device Type
show interface	All Device Types
show ip interface	Cisco ACE;Cisco ACI APIC;Cisco ACI Leaf Switch;Cisco ACI Spine Switch;Cisco ASA Firewall;Cisco ...
show version	All Device Types
show log	All Device Types

- 5) On the **Additional Operations after Benchmark** tab, specify the operations, such as building topology and updating maps, after the benchmark task. See [Benchmark Task Settings](#) for more details.
 - **Update Cloud** — select the Cloud related operations to perform after the latest data is retrieved.
 - **Build Topology** — select the target topology to build after the latest data is retrieved.
 - **System Operations** — select the target objects to update after the latest data is retrieved.

- **Rebuild Visual Space** — select the target templates to rebuild for SDN networks after the latest data is retrieved.
- **Parse Configuration Files** — select the target parsers to parse specific data from configuration files.
- **Update Maps** — select the target maps to update after the latest data is retrieved.

Note: It is highly recommended to enable **Update Site Maps** to keep site maps up-to-date. You can select to back up the original map files in case a rollback is required.

- **Auto Set Golden Path** — enable this function to auto set the paths which have no change during the defined consecutive time period as golden paths.
 - **Application Verification** — select the target application and path to verify.
 - **Run Scheduled Tasks after Benchmark** — select the scheduled tasks to run after the benchmark task is finished, such as data view template and scheduled Qapp task.
 - **Email Alerts** — enable the email alert function for task execution failures or configuration retrieval failures.
- 6) (Optional) On the **Plugins** tab, add plugins to resolve the inaccuracy of path and topology. See [Plugin Manager](#) for more details.
- 7) On the **Summary** tab, review all the settings you have configured for this task.
4. Click **Submit**.
5. To view the task result, see [Verify Benchmark/Discovery Results](#) for more details.

Best Practice:

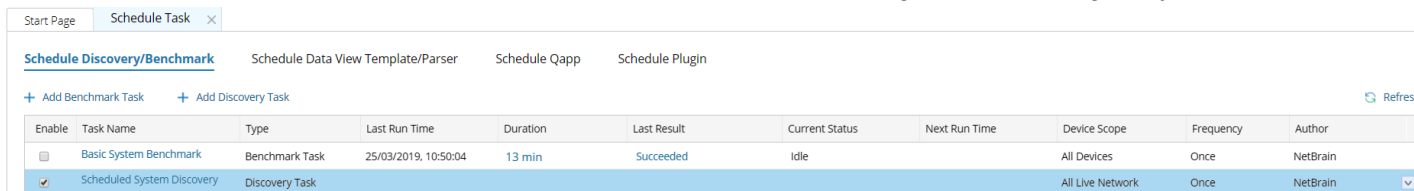
- [How to Export Visio Map](#)
- [How to Run A Benchmark for A Subset of Devices](#)
- [How to Separate Tasks to Gather Large-size Tables](#)
- [How to Set Up and Optimize Multi-thread Tasks](#)
- [How to Utilize System Benchmark to Capture More Frequent A/B Path Snapshots](#)

14. Scheduling Discovery Tasks

Discovery tasks can be scheduled regularly to discover new devices from a live network and automatically add the newly discovered devices to your domain. By default, the task takes all devices in your current domain as seed devices to expand the discovery.

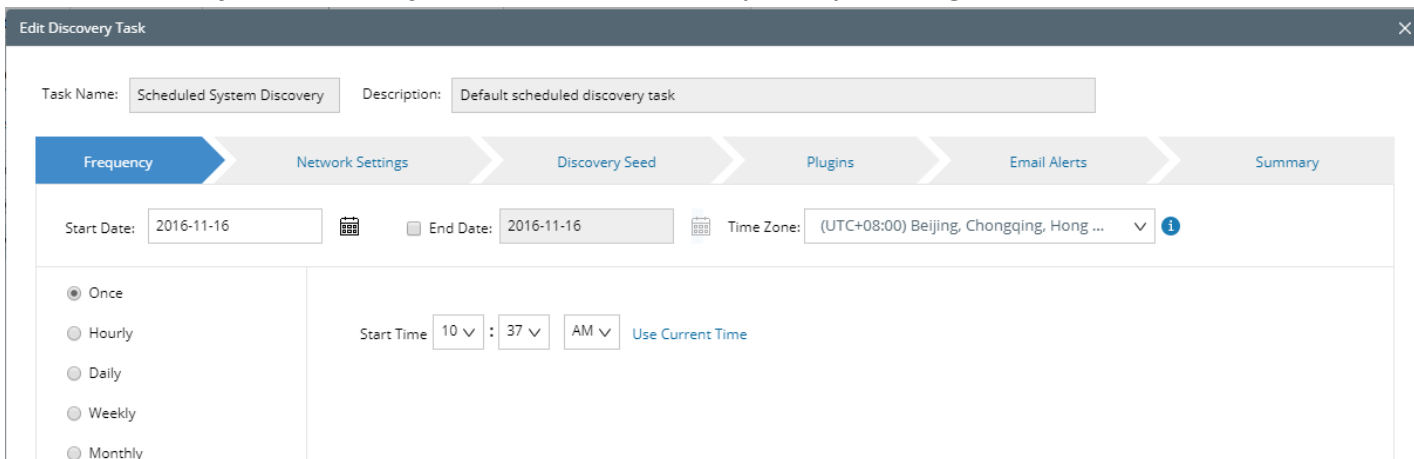
Desired Outcome: System discovery is scheduled with proper frequency and discovery depth.

1. In the Domain Management page, click **Schedule Task** on the Start Page or select **Operations > Schedule Task** from the quick access toolbar.
2. On the **Schedule Task** tab, select the **Enable** check box for the **Scheduled System Discovery** entry.



Start Page Schedule Task X										
Schedule Discovery/Benchmark Schedule Data View Template/Parser Schedule Qapp Schedule Plugin										
+ Add Benchmark Task + Add Discovery Task Refresh										
Enable	Task Name	Type	Last Run Time	Duration	Last Result	Current Status	Next Run Time	Device Scope	Frequency	Author
<input type="checkbox"/>	Basic System Benchmark	Benchmark Task	25/03/2019, 10:50:04	13 min	Succeeded	Idle		All Devices	Once	NetBrain
<input checked="" type="checkbox"/>	Scheduled System Discovery	Discovery Task						All Live Network	Once	NetBrain

3. Click **Scheduled System Discovery**, and then edit the discovery task by following the wizard.



Task Name: Scheduled System Discovery Description: Default scheduled discovery task

Frequency Network Settings Discovery Seed Plugins Email Alerts Summary

Start Date: 2016-11-16 End Date: 2016-11-16 Time Zone: (UTC+08:00) Beijing, Chongqing, Hong ...

Once (selected) Hourly Daily Weekly Monthly

Start Time: 10 : 37 AM Use Current Time

- **Frequency** — specify the execution frequency for the task. By default, it is **once**.
 - **Network Settings** — specify the proxies and credentials to be used to access devices in the discovery.
 - **Discovery Seed** — by default, the **Discover All Live Network** method is selected, which means taking all devices in the domain as seeds to discover new devices by neighbor spreading until the discovery depth is reached.
 - **Plugins** — add plugins to resolve the inaccuracy of path and topology. See [Plugin Manager](#) for more details.
 - **Email Alerts** — enable the email alert function for task execution failures or new devices discovered.
 - **Summary** — check your settings.
4. Click **Submit** to save your settings.

Tip: After the discovery task is executed, the system will automatically rebuild IPv4 Layer 3 topology and synchronize new devices to sites. To view the task result, see [Verify Benchmark/Discovery Results](#) for more details.

Best Practice:

- [How to Set up Schedule Discovery](#)
- [How to Use Schedule Discovery to Discover Limited Scope of Devices](#)
- [How to Validate Schedule Discovery Result and Discovered Devices](#)

15. Scheduling Data View Template/Parser Task

To instantly visualize the values of concerned parser variables in a data view template, you can schedule a Data View Template/Parser task to retrieve and parse network data regularly. Once scheduled, the task is auto-enabled, and can also be triggered through Benchmark.

Desired Outcome: All applicable built-in DVTs are enabled and executed successfully.

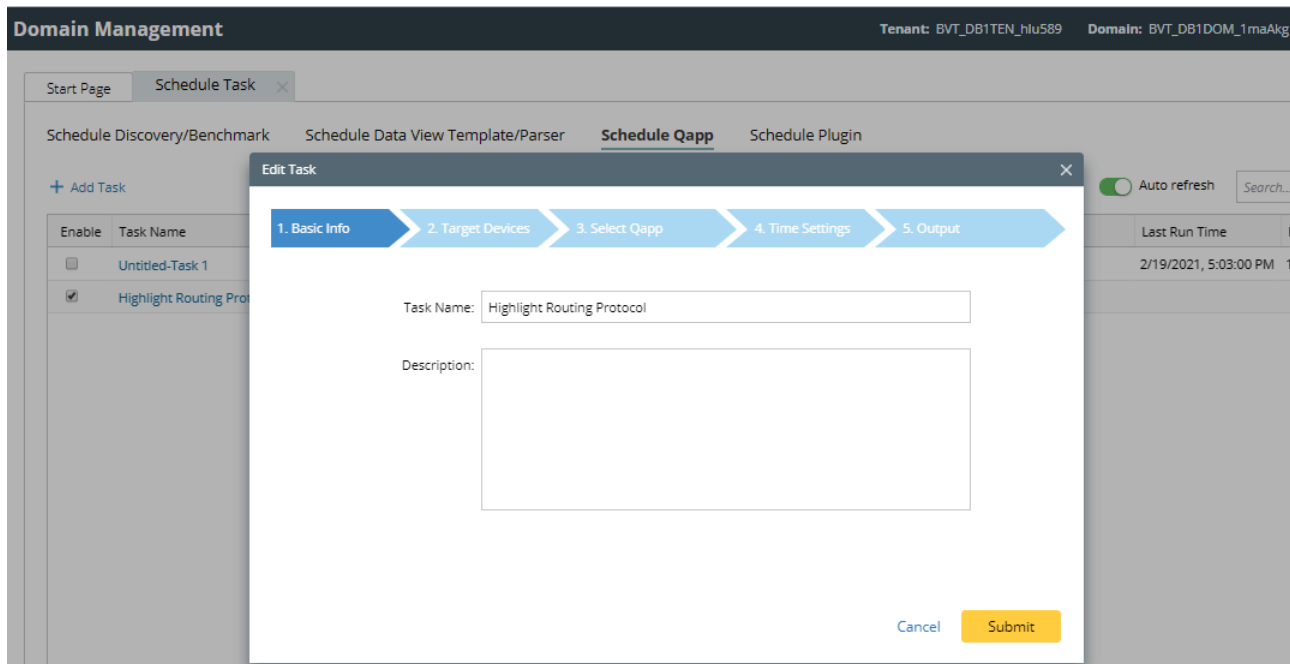
1. In the Domain Management page, click **Schedule Task** on the Start Page or select **Operations > Schedule Task** from the quick access toolbar.
 2. On the **Schedule Data View Template/Parser** tab, click **Add Task**.
 - 1) Specify a run time and a frequency to run the task.
 - 2) Specify a device scope. Both traditional devices and logic nodes can be added to a task.
 - 3) Specify the parsers to retrieve and parse data via two methods:
 - Select data view templates to apply all referenced parsers inside. You can also select them by folder so that folder content change can be synced.
 - Select parsers directly from Parser Library.
- Note:** The **Max Command Instances for one Parser** field is used to limit the generated CLI command instances for each device included in this task. By default, the value is **32**. If the parsers you select or refer have parameters, you can assign a smaller value to avoid devices overloaded due to the execution of too many CLI commands.
- 4) Specify who will receive alerts generated during the task execution.
3. Click **Submit**.

16. Scheduling Qapp Tasks

The system provides a built-in scheduled Qapp task to create a static data view.

Desired Outcome: The built-in task is enabled at a proper frequency.

1. In the Domain Management page, click **Schedule Task** on the Start Page or select **Operations > Schedule Task** from the quick access toolbar.
2. On the **Schedule Qapp** tab, enable the built-in task **Highlight Routing Protocol**.
By default, the built-in Qapp task will auto-generate a static data view.
3. Click the task name to edit the Qapp task by the following wizard.



- 1) On the **Basic Info** tab, view the task name.
- 2) On the **Target Devices** tab, view the selected devices.
- 3) On the **Select Qapp** tab, keep the Qapp **Highlight Routing Protocol** selected.

- 4) On the **Time Settings** tab, set a proper execution time and frequency. For example, set the frequency to **Daily**.

Edit Task

1. Basic Info 2. Target Devices 3. Select Qapp 4. Time Settings 5. Output

☐ Once

☐ Continually

☒ Daily ⓘ

☐ Weekly

Start: 2021-02-19 📅

Execute at: 06 ▾ : 04 ▾ PM ▾

Frequency: ☒ Once a day

☐ Repeat every 2 minutes for a duration of 1 hours

End: 2022-02-20 📅

Time Zone: (UTC-08:00) Pacific Time (US & Canada) ▾ ⓘ

Cancel Submit

- 5) On the **Output** tab, click **Submit**.

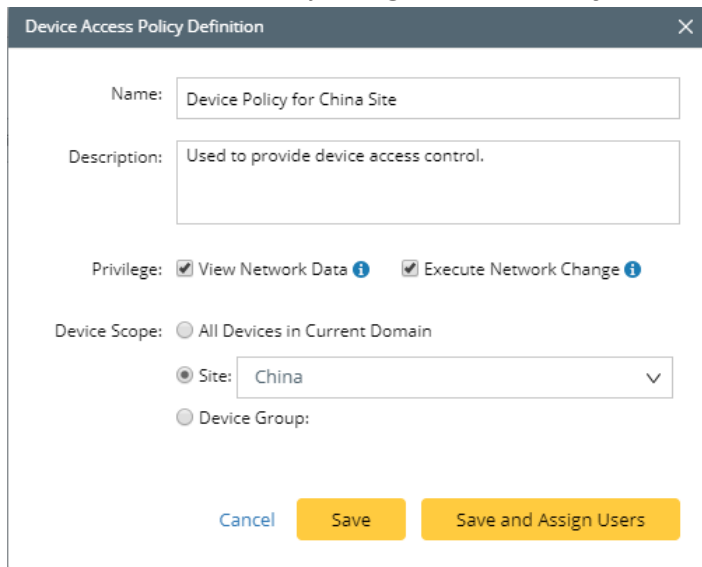
17. Defining Device Access Policy

Device Access Policy provides precise control of access to devices. You can assign specified users to specific policies to determine which users can access which devices.

Desired Outcome: All users are assigned to corresponding policies as required.

Prerequisite: To define and apply the device access policy, go to **System Management > Advanced Settings** to enable the Device Access Policy Control.

1. In the Domain Management page, select **Operations > Device Access Policy** from the quick access toolbar.
2. In the Device Access Policy dialog, click **Add Policy** to define the device access policy.



The screenshot shows the 'Device Access Policy Definition' dialog box. It has a title bar with a close button. The form contains the following fields and controls:

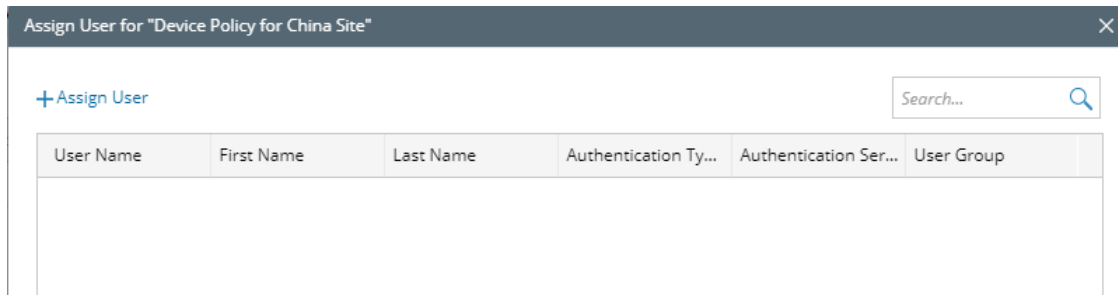
- Name:** A text input field containing 'Device Policy for China Site'.
- Description:** A text area containing 'Used to provide device access control.'
- Privilege:** Two checked checkboxes: 'View Network Data' and 'Execute Network Change', each with an information icon.
- Device Scope:** A radio button selected for 'All Devices in Current Domain'.
- Site:** A dropdown menu with 'China' selected and a downward arrow.
- Device Group:** An unselected radio button.
- Buttons:** 'Cancel' (blue), 'Save' (yellow), and 'Save and Assign Users' (yellow).

- 1) Enter a unique name **Device Policy for China Site** and a brief description.
- 2) In the **Privilege** area, select at least one check box.

Note: In order to execute network change tasks successfully, make sure the privilege **Access to Live Network** and **View Network Change** are assigned to users.

- 3) In the **Device Scope** area, select the **Site** check box and click the  icon to select **China**.

3. Click **Save and Assign Users**.



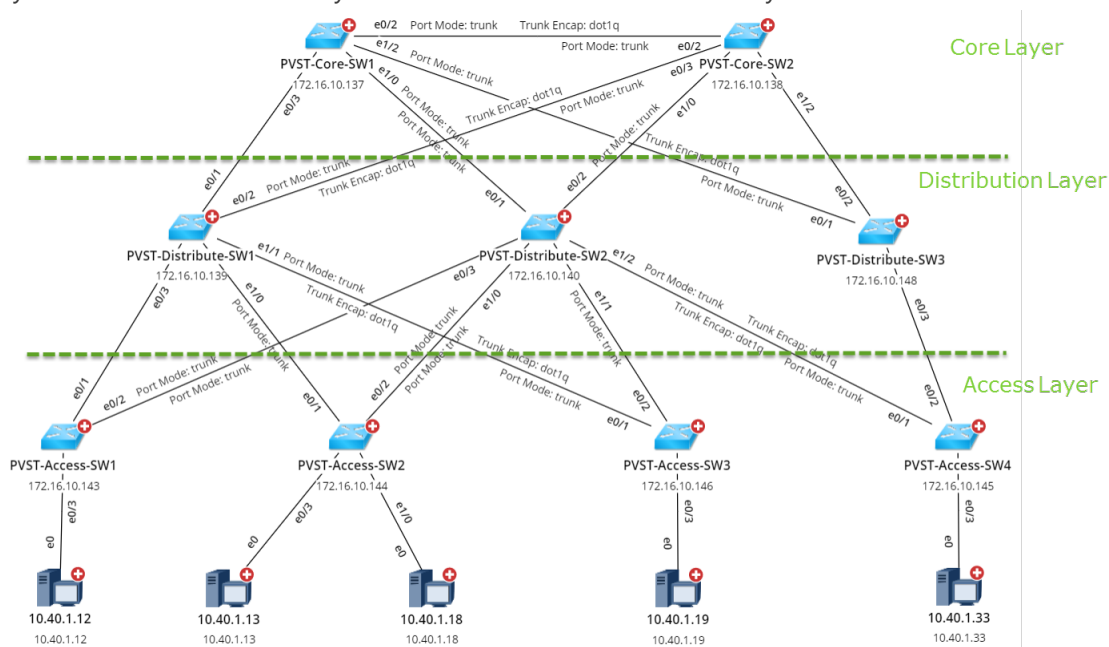
The screenshot shows a dialog box titled "Assign User for 'Device Policy for China Site'". Inside the dialog, there is a button labeled "+ Assign User" and a search bar with the placeholder text "Search...". Below these elements is a table with the following columns: "User Name", "First Name", "Last Name", "Authentication Ty...", "Authentication Ser...", and "User Group". The table is currently empty.

- 1) Click **Assign User**.
- 2) Select the user to assign the policy.
- 3) Click **OK**.


Note: A relogin for the selected user accounts is required to apply a policy.

18. Creating a Layout Style

To reflect a real network infrastructure, you can create a map layout to organize devices. For example, the following layout is divided into three layers to reflect network hierarchical layers.

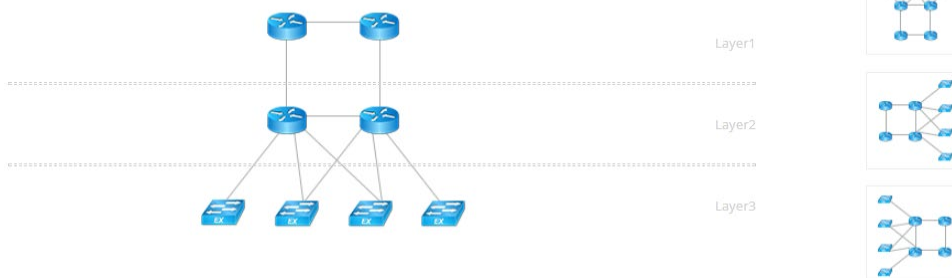


Desired Outcome: All sites are associated with the above customized layout.


1. Click the start menu  and then select **Map Layout Manager**.
2. On the **Layout Style** tab, right-click the **Layout Styles** node, and then select **New Folder**.
3. Right-click the new folder and then select **New Layout Style**. Enter a style name **My Style**.
4. In the **Layout Style** area, click **Change Layout Type** to select a layout type suitable for your three-layer network.

Layout Style

[Change Layout Type](#)









Tip: To change the layout direction, click a thumbnail next to the selected layout type diagram.

5. In the **Layout Tags** area, add tags to the layout type. Tags are used to mark devices and layout layers to identify which layout layer a device belongs to.
 - 1) For each layer, click the  icon to create a layout tag. Enter **core**, **distribution**, and **access** as tag names respectively. The tags will be used to associate layout layers with devices.

Layout Tags

[+ Add Layer](#)

Layer	Associated Tags	Maximum Displayed Devices per Row	Device Icon Size
Layer 1	core 	8	Medium(100%) 
Layer 2	distribution 	8	Medium(100%) 
Layer 3	access 	8	Medium(100%) 

- 2) Set the maximum device number in each row of a layer and device icon size.
 - 3) Click **Save**.
6. On the **Assign Tags** tab, assign layout tags to devices based on their role in your network. For example, if a device is in the core layer, assign the layout tag **core** to the device.

Map Layout Manager

Layout Style

Assign Tags

Layout Association


By Device Group

By Search Term

Import Device Tags


Search Devices:

PVST-Core-SW1




Tag:

core




Assign Tag

1 Devices in #BGP 100

 Delete All Tags

<input checked="" type="checkbox"/>	Device Name	Layout Tags
<input checked="" type="checkbox"/>	PVST-Core-SW1	Core

Tip: To delete tags from devices, you can click **Delete All Tags** to remove all tags, or point to the target tag in the **Layout Tags** column and click the  icon to delete the tag one by one.

7. On the **Layout Association** tab, associate the layout style with site maps.
 - 1) Click **Refresh** to display the newly created layout style. In the **Site Maps** column, expand the site tree from the **My Network** node.
 - 2) Select the site names you want to associate with the layout created above.

Note: Only the maps of leaf sites () can be associated.

- 3) Click **Select** to select **My Style** from the drop-down list.

19. Viewing Domain Health Report

Domain Health Report records the key factors about domain health. You can get a quick overview of the current domain status with this report.

Desired Outcome: All issues reflected in the report are resolved.

1. In the Domain Management page, select **Operations > Domain Health Report** from the quick access toolbar.
2. In the **Domain Health Report** tab, click **Create Health Report** to generate a report.
3. View the highlighted area to get an overview.

Domain Management Tenant: BVT_DB1TEN_C8gk7 Domain: BVT_DB1DOM_SPx1Ku Operations kang netBrain

Start Page Domain Health Report

Report Generated Time: 2/10/2021 05:18:49 PM Refresh

Create Health Report

Basic Network Settings: 5 need attention Discovery Status: 4 need attention Path: 0 failed Others: 11 need attention Export

Driver Associated Device:

23 Driver Applied, 212 Devices, 5448 Interfaces

Device Driver	Associated Device Count
Cisco IOS Switch	94
Cisco Router	85
Cisco Nexus Switch	6
Arista Switch	2
Aruba WLC	2
Avaya Switch	2
Avaya VSP	2
Juniper EX Switch	2
Juniper Router	2
Viptela vEdge	2

Basic Network Settings Completeness:

Attention	Index	Count
	Front Server (defined)	2
	Front Server (unused)	0
	Front Server (with over 5000 devices)	0
	Private Key (defined)	6

4. Check the following areas to get more information. See [Viewing Domain Health Report](#) for more details.
 - Driver Associated Device
 - Basic Network Settings Completeness
 - Discovery Status
 - Site Definition Completeness
 - Benchmark Task Health
 - Cloud Health
 - Path Calculation Health
 - Disk Management Settings Completeness
 - Map Layout Settings Completeness