

# NetBrain Instant Trial

## Essential Features Walkthrough



## Contents

1. Dynamic Mapping .....	3
1.1 Search and Map .....	3
1.2 Use Map as a Single Glass of Pane .....	7
1.3 Map an Application Flow (A/B Path) .....	13
1.4 Map as Collaboration Medium .....	16
2. Executable Runbooks .....	20
2.1 Monitor Network Operational Status .....	20
2.2 Troubleshoot Repetitive Problems such as a Slow Application .....	26
2.3 Proactively guard against misconfigurations .....	29
2.4 Diagnosis a problem when it is happening .....	31
Additional Questions? .....	34



# 1. Dynamic Mapping

---

NetBrain dynamic map provides the following key benefits compared with the static Visio maps:

- Can be created instantly
- Provides the full visibility of the network such as L3 and L2 topology, network design and operational status.
- Is always updated
- Record user actions and results

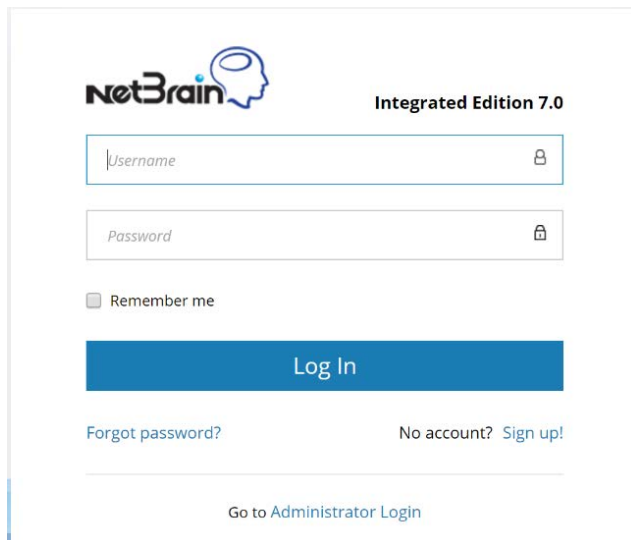
## 1.1 Search and Map

With NetBrain, your entire network becomes a searchable database. You can search an IP address, hostname, vendor/model, or a part of a configuration file such as routing protocol. You can find exactly what you're looking for instantly, and then generate a new (or open an existing) network map, directly from the search results.


This module will introduce how to search for a device by its hostname, and create a new map from the search result.

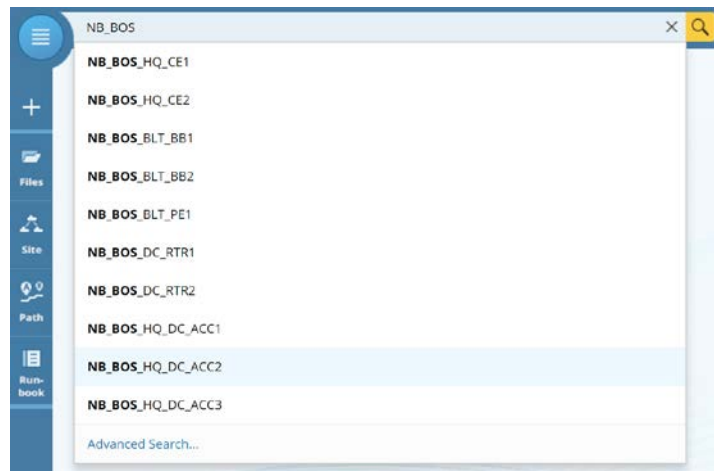
### Instructions:

1. To get started, login to NetBrain ITE web page (<https://ite.netbraintech.com>). Enter the username and password. If you do not have the username, go to the page <https://www.netbraintech.com/try-netbrain-now/> to register yourself. The registration can be done in one minute.

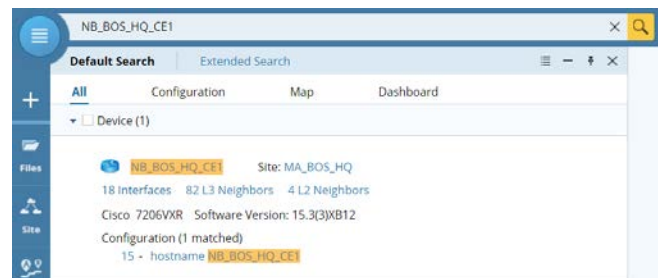
The image shows the login interface for NetBrain Integrated Edition 7.0. At the top left is the NetBrain logo, which consists of the word "netBrain" in a sans-serif font with a stylized brain icon to its right. To the right of the logo, the text "Integrated Edition 7.0" is displayed. Below the logo and text are two input fields: the first is labeled "Username" and the second is labeled "Password". Both fields have a small lock icon on the right side. Below these fields is a checkbox labeled "Remember me". A large blue button with the text "Log In" is positioned below the checkbox. At the bottom of the login area, there are two links: "Forgot password?" on the left and "No account? Sign up!" on the right. At the very bottom of the page, there is a link that says "Go to Administrator Login".

- Search a device: Type hostname **NB\_BOS\_HQ\_CE1** into the **Search** box and press **Enter** key.


 **Tip:** if you do not remember the full hostname, just type in the first part of letters and select the device from the pulldown menu.

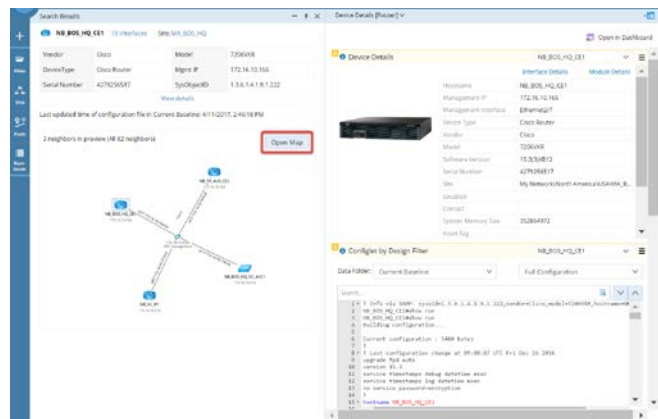



- The Search Results are organized by **All (devices)**, **Configurations**, **Map** and **Dashboard**. Click the hostname **NB\_BOS\_HQ\_CE1** to view the device detail.



- Device detail information such as vendor, model, software version as well as configurations, route table and CDP tables are displayed. A preview map with 3 of its neighbors are shown. Click **Open Map** link to create a new map.

 **Tip:** you can also close the Device Detail page to return the search results page. From the search results drag and drop a device icon to open a new map just for this device without its neighbors.

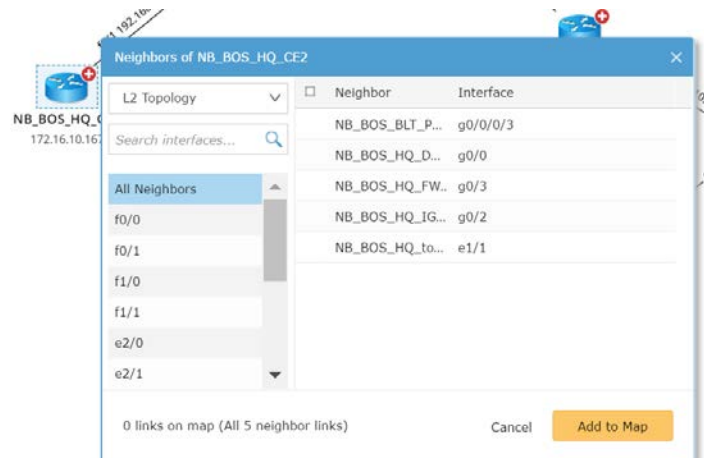
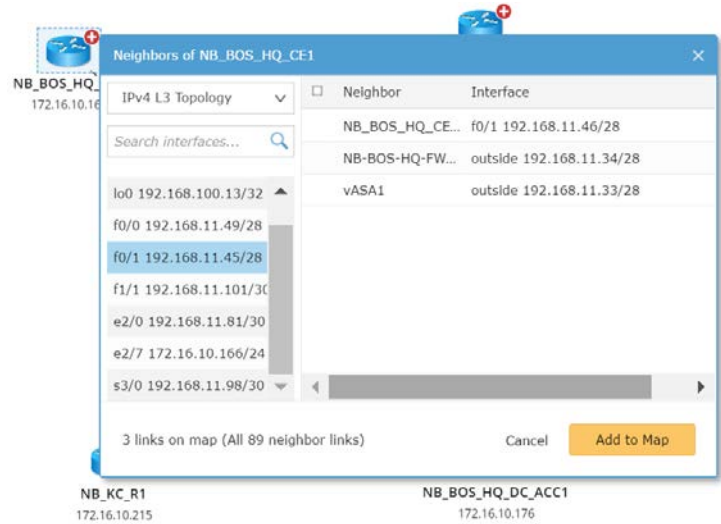


- Extend L3 neighbors: Click the  attached to a device icon to add the neighbor devices to the map. In the **Neighbors** window, you can view all neighbor devices or filter neighbor by the interfaces and type of topology. For example, select the interface **f0/1** of the device **NB\_BOS\_HQ\_CE1** to view three devices connected to this interface. Double click a neighbor device to select a neighbor and click **Add to Map** button to draw it. You can select multiple devices.

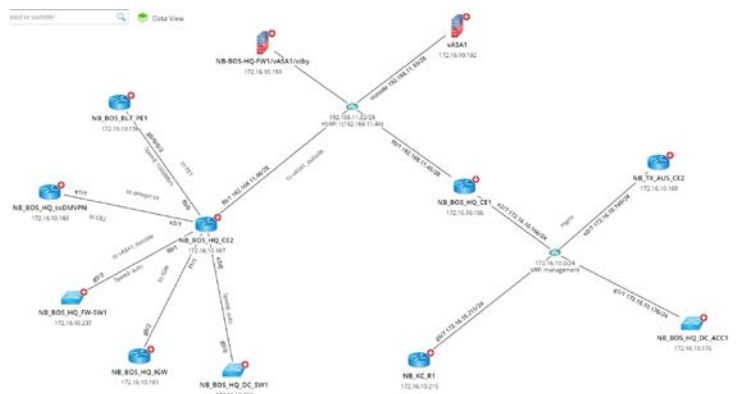


**Tip:** Double click an interface to draw all neighbor devices connected to that interface in the map. You can also double-click **All Neighbors** to draw all neighbors on the map.

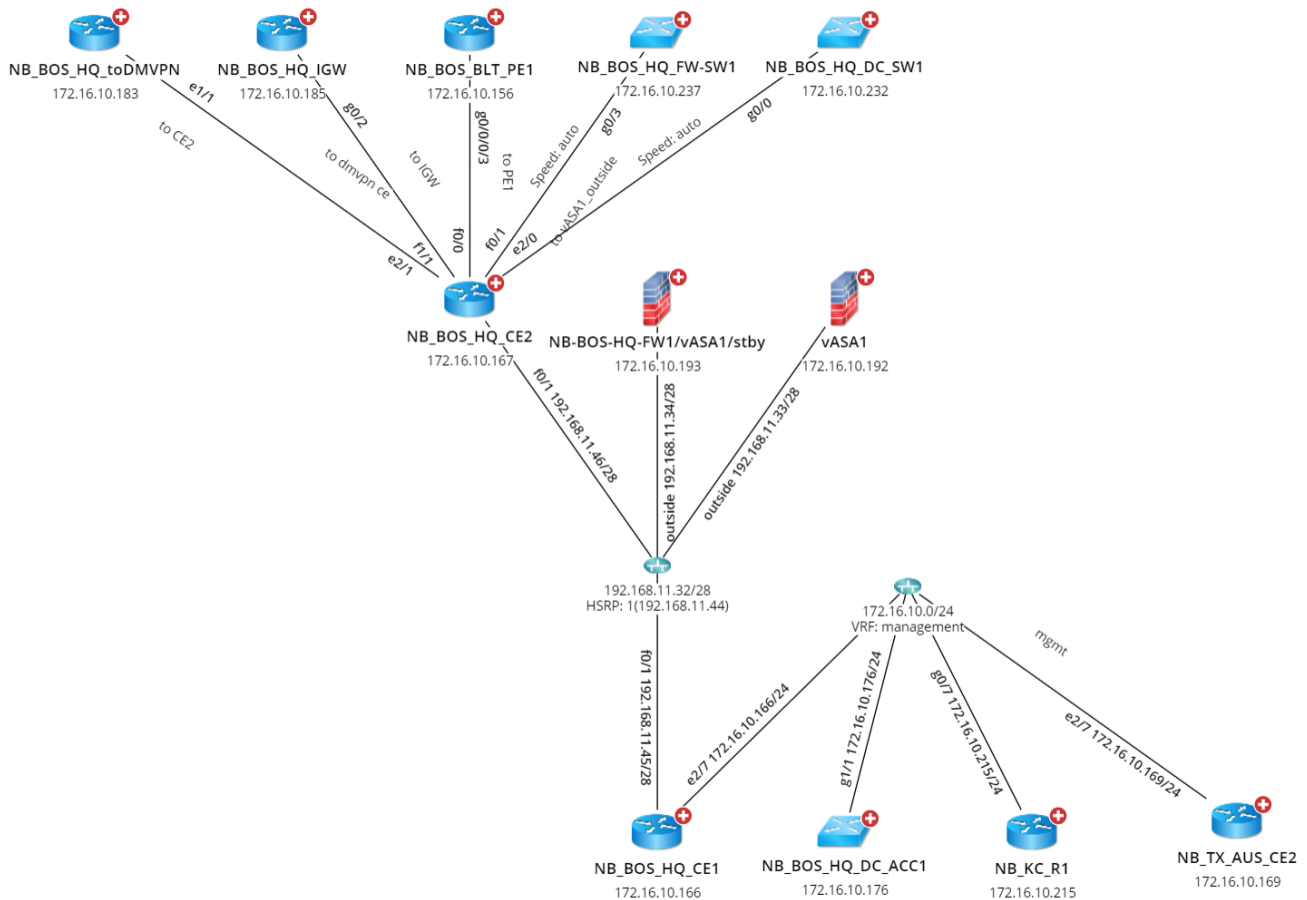
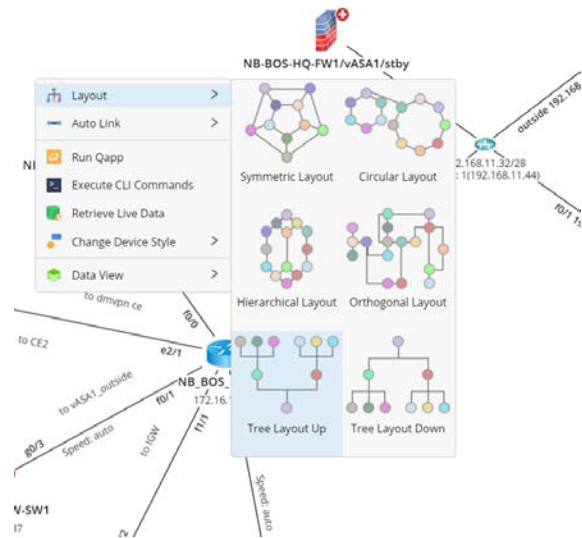
- Extend L2 neighbors: In the **Neighbors** window, select **L2 Topology** from the pulldown menu of the topology and add L2 neighbors to the map. For example, for the device **NB\_BOS\_HQ\_CE2**, select **L2 Topology** and double click **All Neighbors** to add all its neighbors in the map.



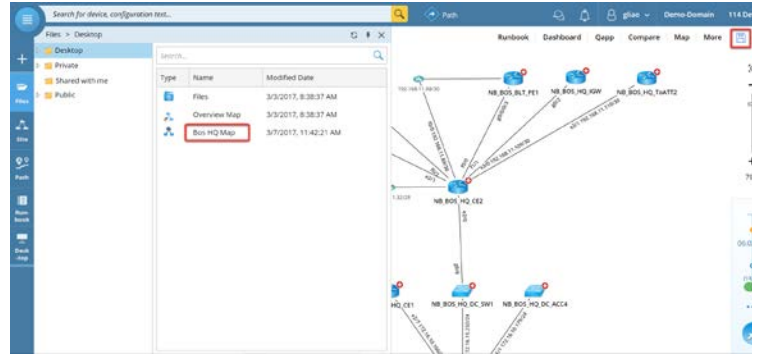
- Repeat the step 5 and 6 till you have all devices you are interested in the map.



8. Auto layout: Right click the map and select one of layout algorithms such as **Tree Layout Up** for a better layout for the map. You can then drag any object on the map to adjust its positions.



- You can save the map in the server for future reference. For example, you can save it in the **Desktop** directory.



## 1.2 Use Map as a Single Glass of Pane

NetBrain dynamic map versus the static network Visio Map is like Google Map versus a printed street map. Different layers of rich data can be displayed in the map such as the data from configurations, CLI commands or from 3<sup>rd</sup> party system. The map can be used as a collaboration media. Automatically updated Data Views replace different sheets in a Visio document.

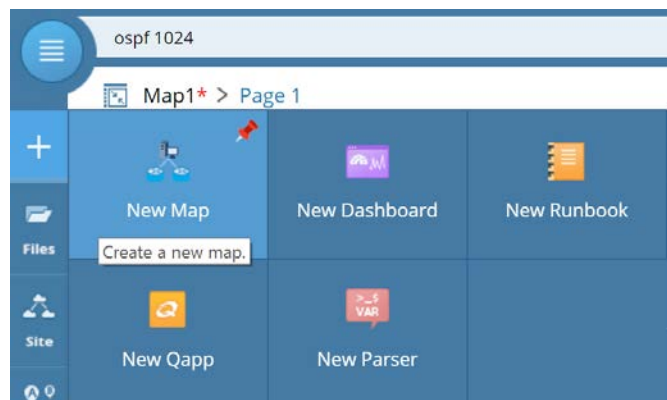
This module will teach you how to use the NetBrain map as a single glass of pane.

### Instructions:

- Click “+” button in the left side menu bar and select **New Map** to create a new map.



**Tip:** if no map is created please check the browser setting to allow the pop-ups from [ite.netbraintech.com](http://ite.netbraintech.com).



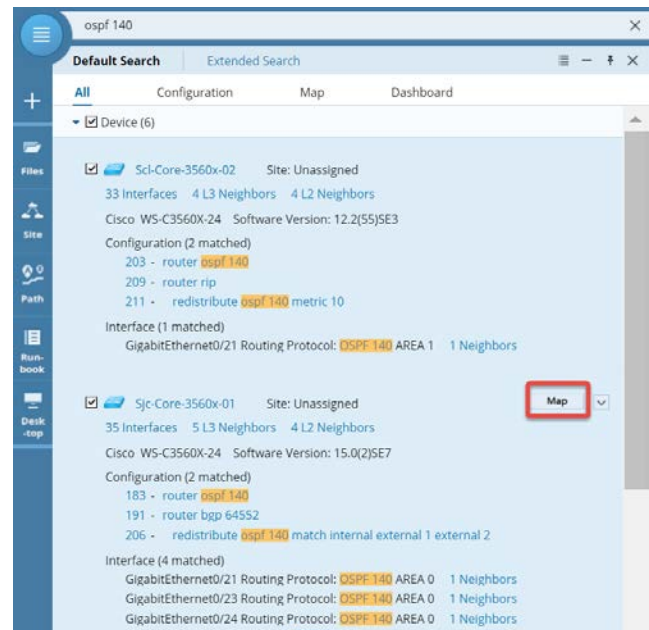
- Type the configuration string **ospf 140** into the **Search** box and press **Enter** key.



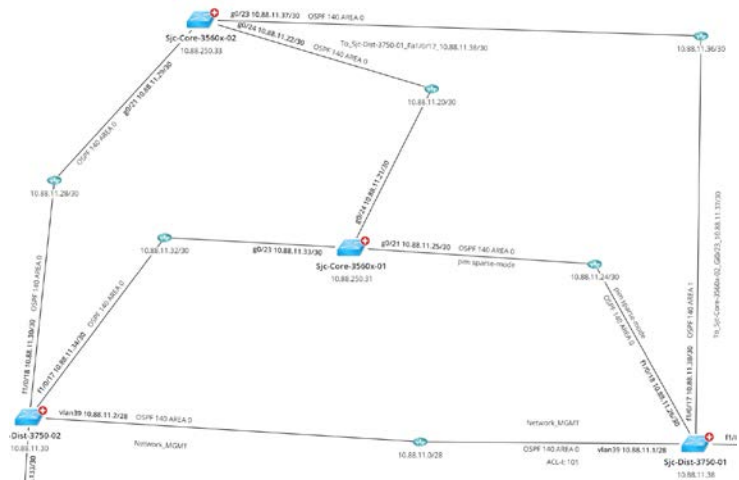
**Tip:** You can search **ospf** first which may return too many devices. And then you can look through the matched configurations in the search result and narrow down by a more specific string such as **ospf 140** or **area 0**.



3. All devices with **OSPF 140** configured are displayed in the search results. Check the checkbox besides **Device(6)** to select all 6 devices in the search result. Then click **Map** button to draw all devices in the map.

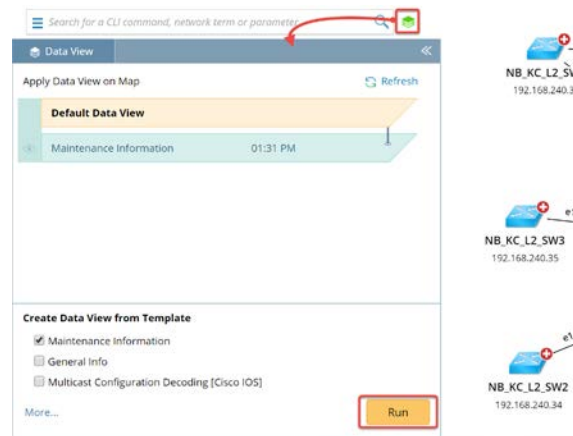


4. Scroll the wheel of your mouse to zoom in the map to view the detail interface data such as the routing protocol.




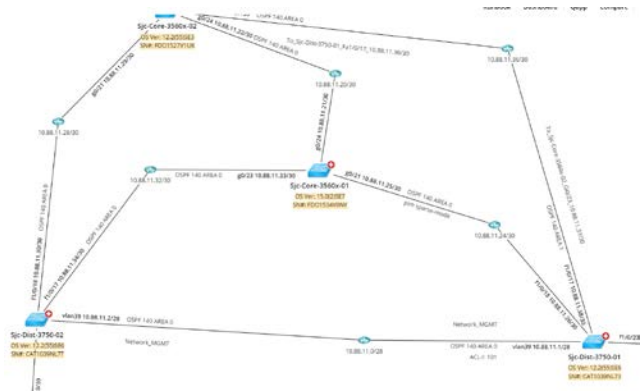


- View different layers of data: Click the green **Data View** sign at the top of the map to open the Data View pane. A data view displays a certain type or layer of data in the map such as basic maintenance info, design and operation status. The data view can be created from the template or an application in scheduled benchmark or on demand. Click one data view such as **Maintenance Information**.





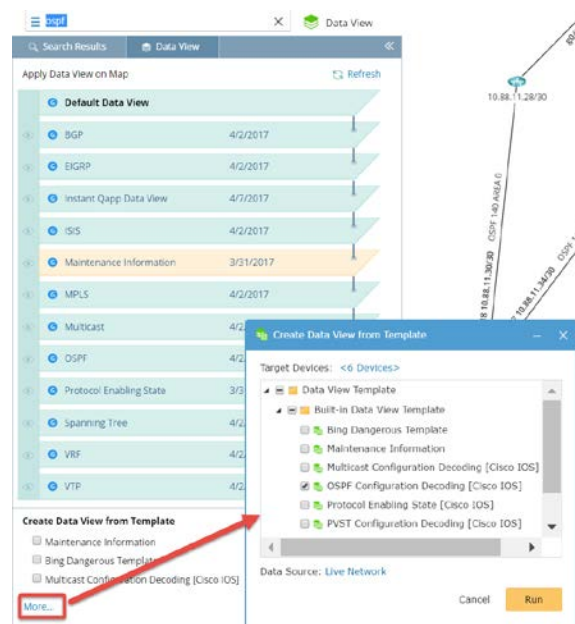
- The maintenance information such as **software version** and **serial number** are displayed under the device.


 **Tip:** zoom in to see the maintenance information if they are not visible under a device.

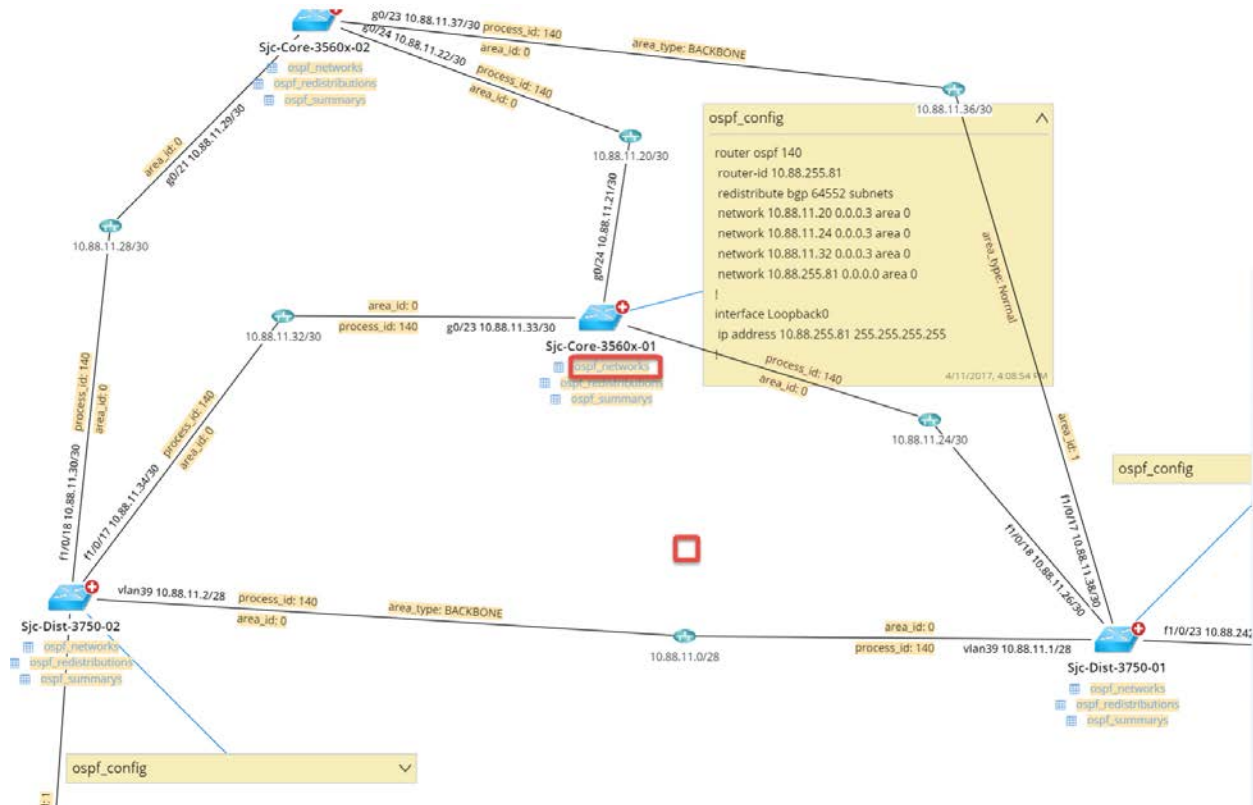


- View OSPF info: at the bottom of data view pane select Data View Template **OSPF Configuration Decoding [Cisco IOS]** (if the template is not visible, click **More...** and select the template in the pop up window). Click **Run** button.


 **Tip:** You can view the definition of a data view template from **Data View Template Manager** which can be opened by clicking the icon  at the top left of the page.

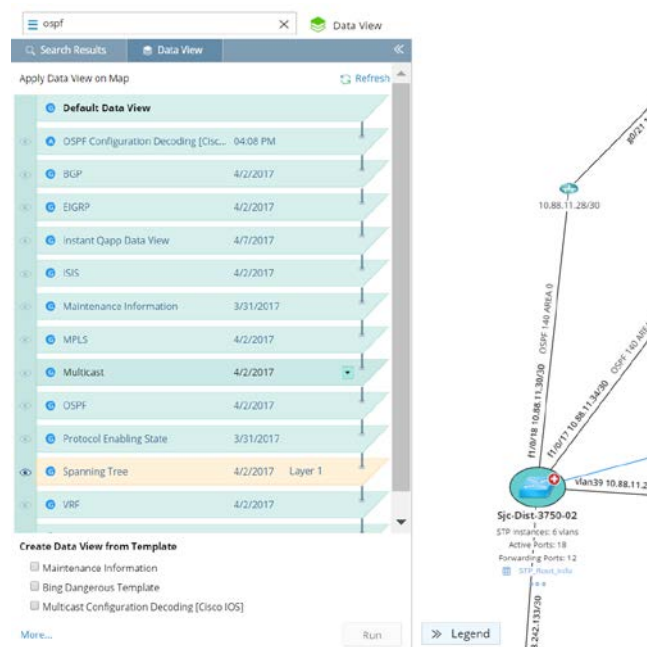


8. A new data view is created and displayed in the map. The OSPF configurations are displayed as a device note. You can click  to expand the note. The table data such as **ospf\_networks** are displayed under the device icon. Click it to show the table data.

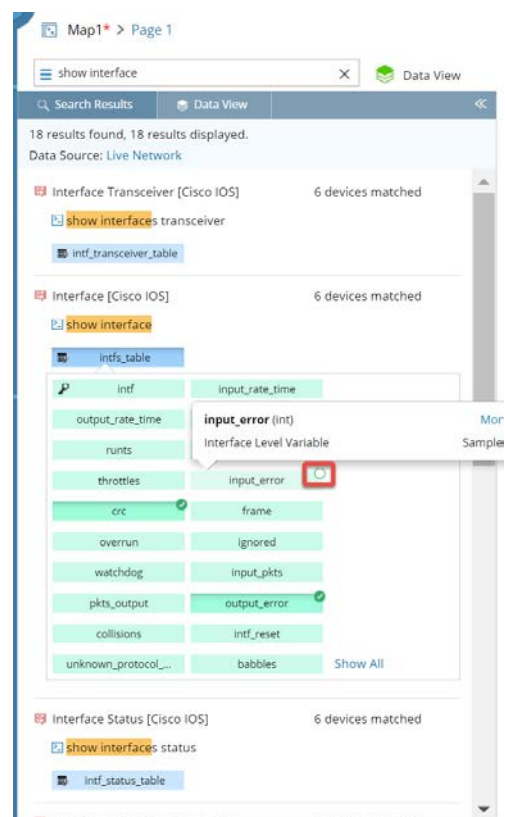


- Switch data views: In the **Data View** pane, click a data view or click the eye shaped icon of the data view to display its data in the map.

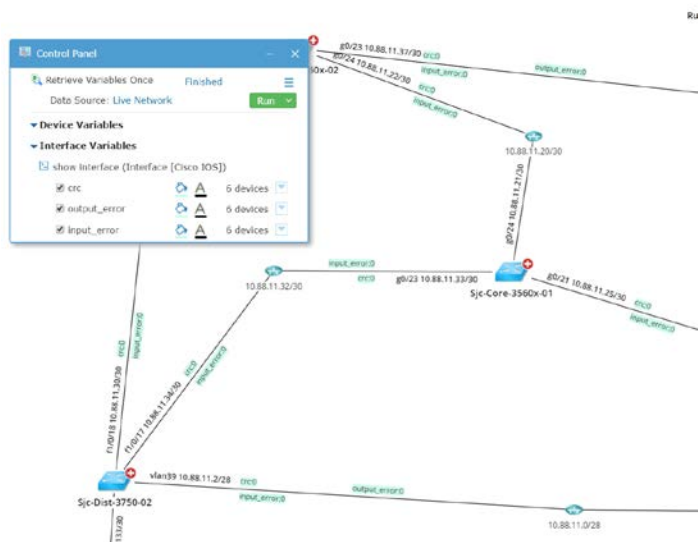
 **Tip:** You can display multiple data views in the map. Just click the eye shaped icon of an invisible data view to display its data in the map besides other data view already visible in the map.




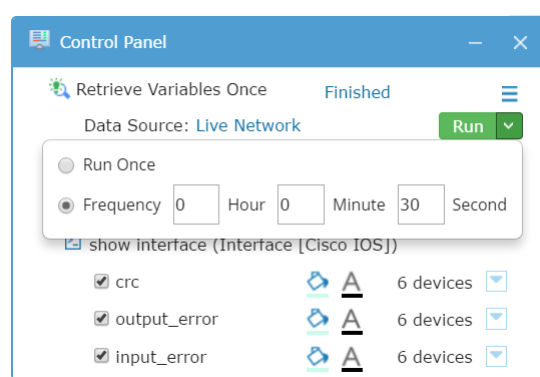
- Search and view the variables from CLI commands: in the search box within the map, you can enter any CLI command you are interested such as **show interface**. Double-click the table named **intfs\_table** to expand the table. Select a variable such as **crc**, and click the **circle** icon to select it. You can select multiple variables.

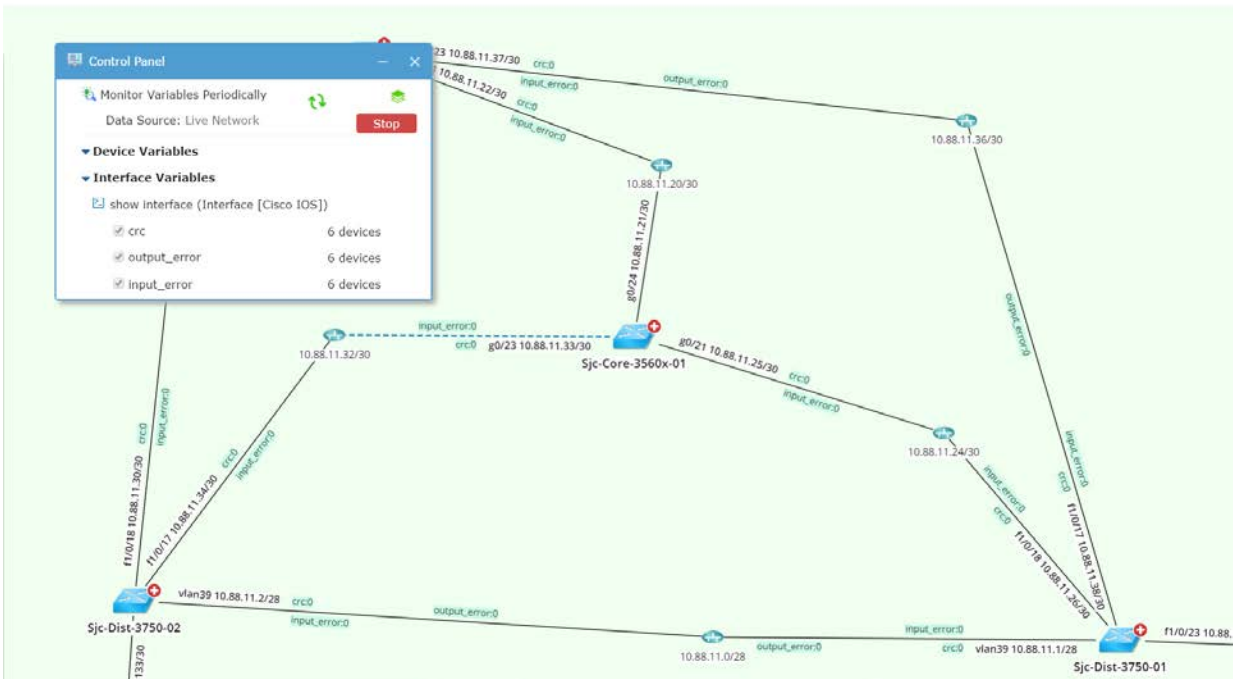


11. Drag and drop the selected variables onto the map. The system starts retrieving the variables from the live network and the results are displayed in the map.



12. Monitor the variables frequently: click  in the **Control Panel** and select **Frequency**. Set the frequency such as every 30 seconds. Click **Run** button. Save the map if prompted. The map turns into the monitored mode.





## 1.3 Map an Application Flow (A/B Path)

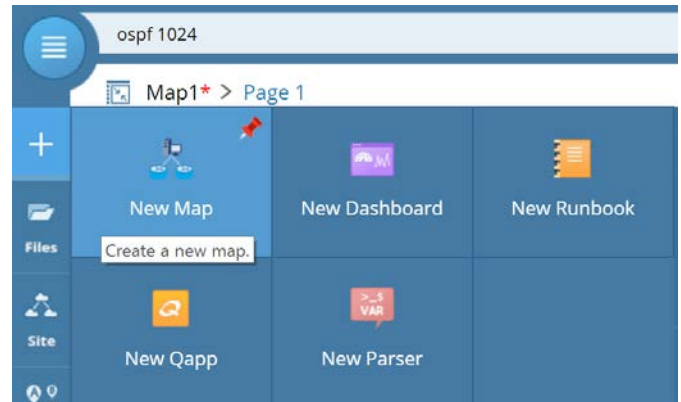
Given the source and destination address of any application, NetBrain can map out both live and historical application paths. NetBrain emulates real packet forwarding to analyze how traffic flows across the network and takes account of the deep network protocol analysis (e.g. routing, ACLs, PBR, NAT, VRF).

This module will introduce how to create a map of an application flow between two endpoints.

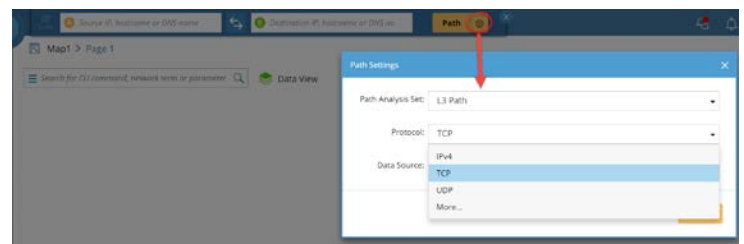
### Instructions:



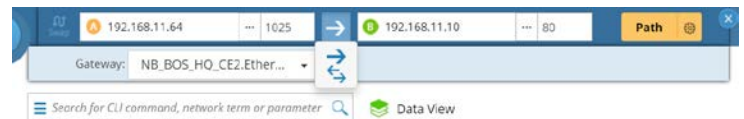
1. Click “+” button in the left side menu bar and select **New Map** to create a new map.




2. Click the **Path** icon at the top of map and then **Path Setting** icon. In **Path Setting** window keep the default path analysis set **L3 Path** and select **TCP** protocol.




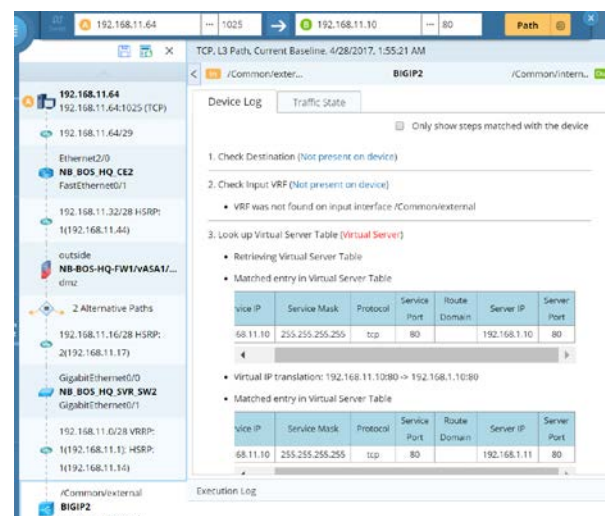
3. Enter the source IP and port as **192.168.11.64 ...1025** and destination IP and port **192.168.11.10 ... 80**. Select the path direction as **→**. Click the **Path** button to calculate the path.



 **Tip:** you can select the gateway device from the pulldown. The correct gateway should be **NB\_BOS\_HQ\_CE2** for this source IP.

4. The path pane shows the devices along the path, the technologies being evaluated (ACL, NAT, PBR, VRF, MPLS, etc.) and the execution log. Selects a device to view the technologies evaluated on this device.

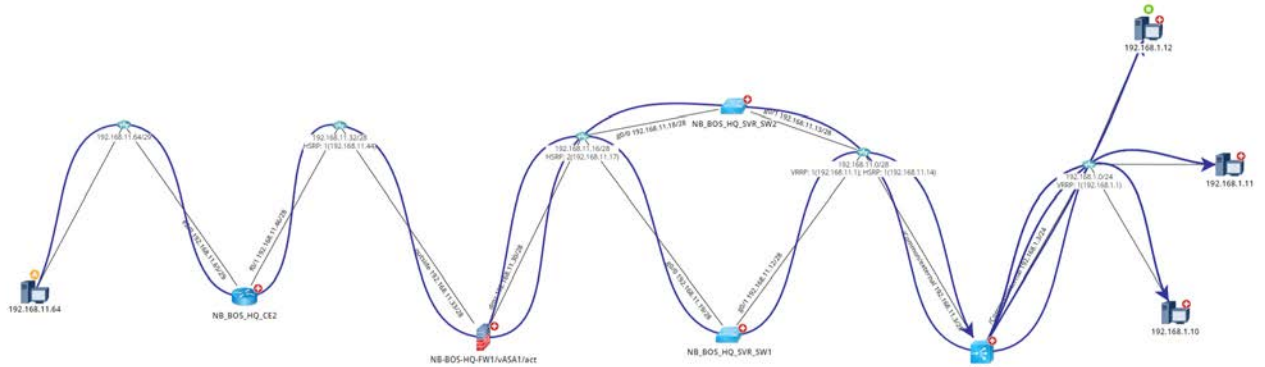
 **Tip:** Uncheck **Only show steps matched with the device** checkbox to view all steps evaluated.



5. Close the path detail pane to view the map. Zoom into the map to view the details along the path.



 **Tip:** Click the path curve and then the **View Detail** button to bring back the path detail pane.



- Click the **Path Setting** icon. In Path Setting select the **Live Network** option.

Path Settings

Path Analysis Set: L3 Path

Protocol: TCP

Data Source: Live Network

☒ Use configuration in Current Baseline

Cancel OK

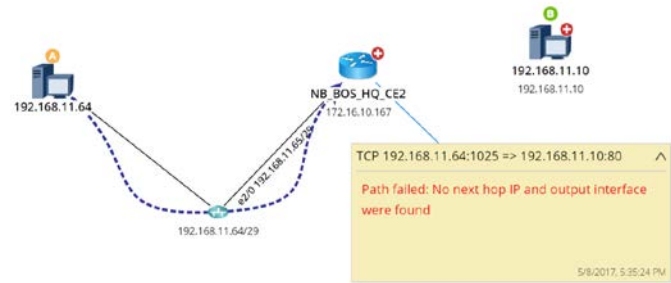
7. Add a new map page: Click **Page 1** link and then **Add Page** button. The map is switched to **Page 2**.

The screenshot shows the AWS CLI interface. At the top, there are two input fields: one with '192.168.11.117' and a blue arrow button, and another with '192.168.2.10' and a green circle button. Below these, a search bar contains the text 'asymmetric path\*' followed by a red box containing 'Page 1'. The search results show a blue box with a white wavy line diagram and the text 'Page 1'. Below this, there is a red box containing '+ Add Page'. At the bottom left, there is a small diagram of a network path with a red circle and a plus sign, and the text '192.168.11.117'.

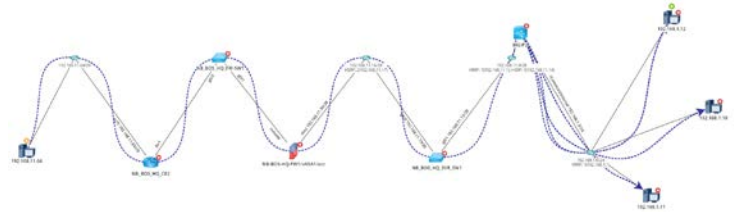




- Click the **Path** button to discover the live path. The result shows the path failed at the device **NB\_BOS\_HQ\_CE2** with the device note explaining why the path failed.



- Map L2 path: Select the **L2 Path** option from **Path Setting**, create a new page and map the L2 path in Page 3.




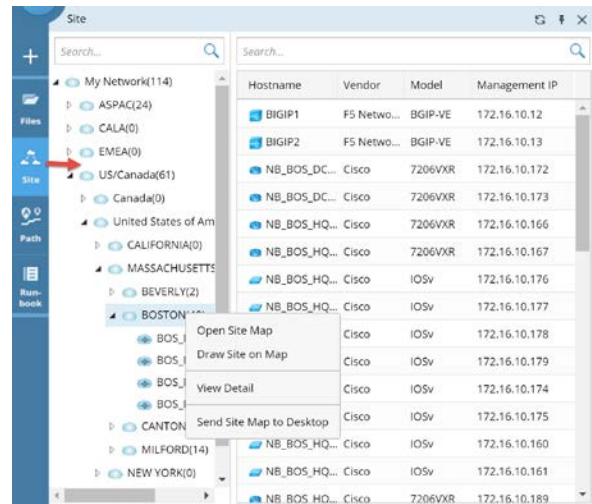
## 1.4 Map as Collaboration Medium

NetBrain map contains not only the rich data but also the action logs (A-logs) performed by different users in this map. Network teams can operate off a common map such as site maps and seamlessly share data and notes for collaborative tasks. This module will introduce site maps and how to use them as a collaboration medium.

### Instructions:

- Open a site map: Click **Site** at the left menu bar and browse through the site **US/Canada > United State of America > MASSACHUSETTS > BOSTON**. Right click the site and select **Open Site Map** menu.

 **Tip:** the number attached to a site is the number of devices belonging to this site. A device can only belong to a leaf site which does not have a child site.

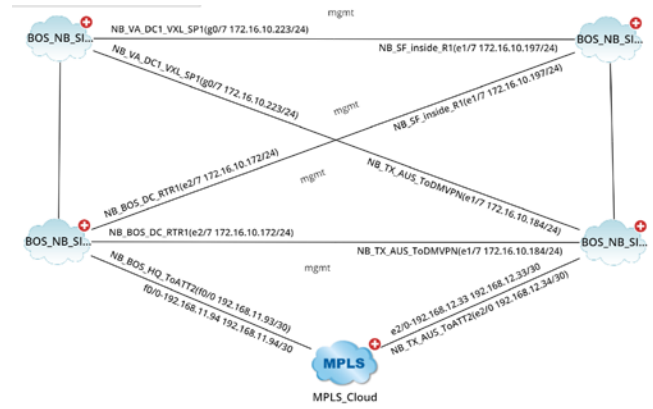




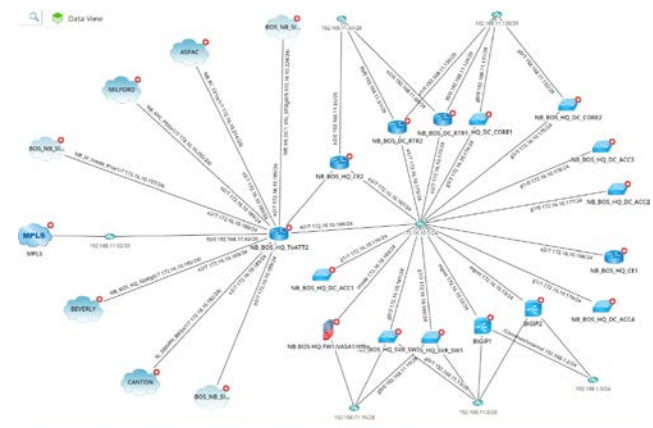
- The site map of a parent site shows how its child sites are connected. Zoom in to view more connection details.



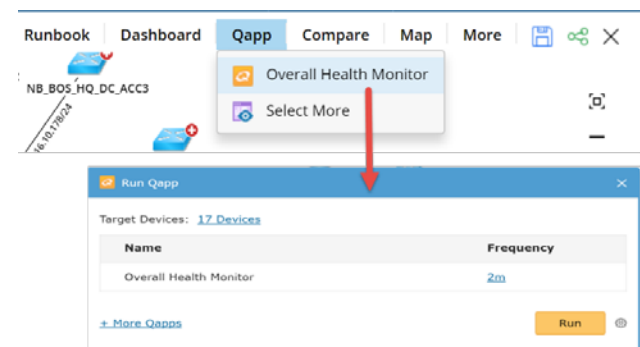
**Tip:** a parent site has one or multiple child sites. Its site map shows the connections of its child sites. The site map of a leaf site shows the connections of its network devices besides the connections between its network devices and neighbor sites.




- Right click the leaf site **BOS\_NB\_SITE1** from the site tree or from **BOSTON** site map to open its site map. The site map draws all devices belonging to this site and their IPv4 connections.

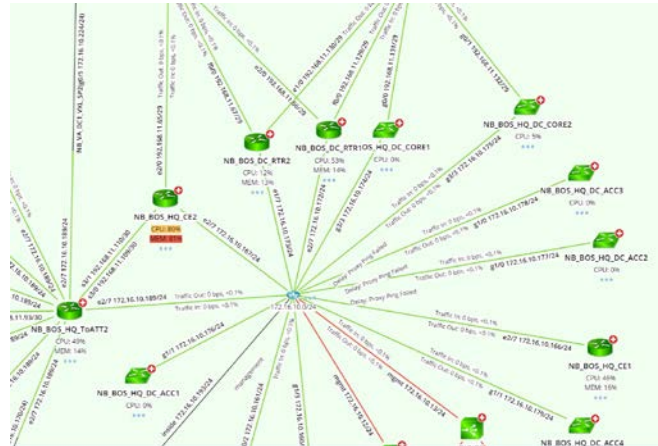


- Run **Over Health Monitor**: from the map menu bar select **Qapp > Overall Health Monitor**. In Run Qapp window, click **Run** button.




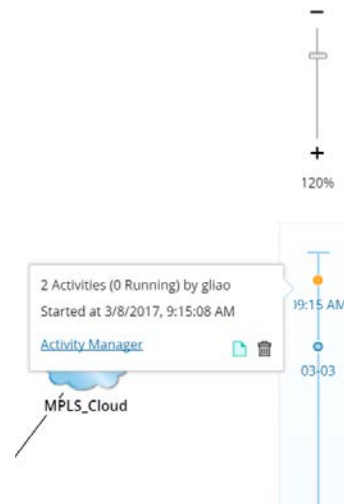
- The map turns into the monitored mode. Zoom in to see more detail data such as interface traffic and errors.


 **Tip:** A data view is created when a Qapp is executed in the map. For example, the **Overall Health Monitor** data view is added in the data view pane. You can turn the monitored data on and off from Data View pane.

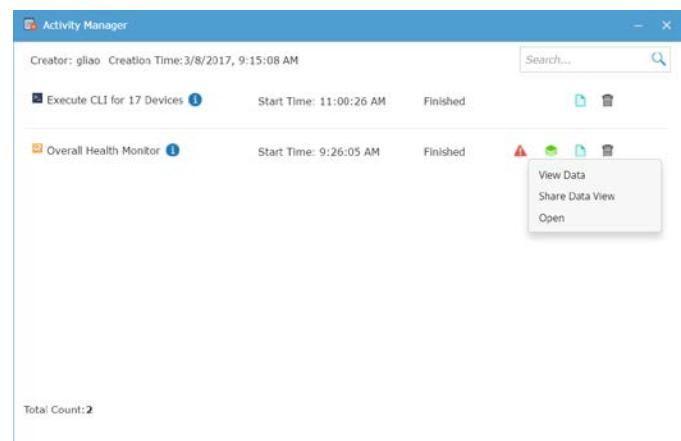


- View the action log: The user actions on a map are presented as a time line on the right side of the map. Click one of nodes in this time line to view the activities and click **Activity Manager** to view the details.

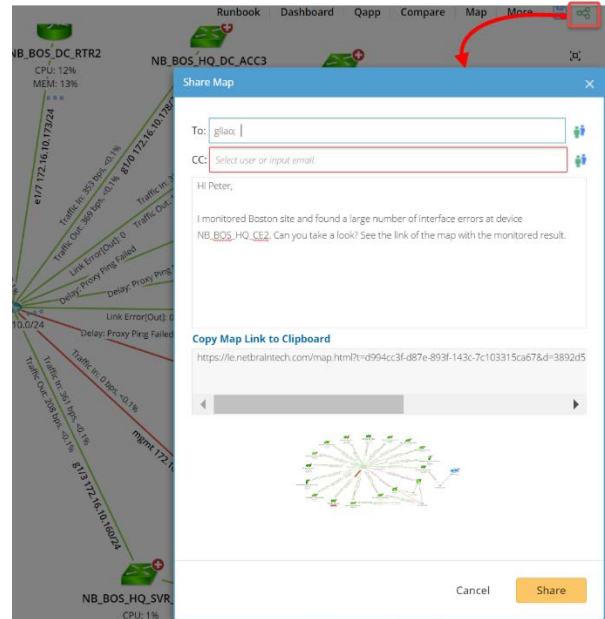
 **Tip:** you can search activities and filter the activities of a user by click ... button at the bottom of time line.



- In Activity Manager window click  to see the description of this activity. Select an activity you can view the data of this activity.



8. Share a map via email: Click the **Share Map** icon in the map menu bar. Select the users you want to share the map and notes. Click the **Share** button to send the email with the map link to the users.



9. The note, the map link and a map image are contained in the email. The link will bring the user directly to the NetBrain map so they can continue working on the same map with all existing data.

Hi Peter, I monitored Boston site and found a large number of interface errors at device NB\_BOS\_HQ\_CE2. Can you take a look? See the link of the map with the monitored result.

<https://ie.netbraintech.com/map.html?t=d994cc3f-d87e-893f-143c-7c103315ca67&d=3892d51a-dec6-476e-99b8-5275995a150b&id=f4c33b5e-c67b-4ca9-ae54-6fbc361f46d3>



## 2. Executable Runbooks

An Executable Runbook is an active flow chart. Each node of the chart corresponds to a step of a network task and can take the form of an executable application (Qapp), a built-in function (Ping or trace route) or just a description. The runbook takes the map as the input and the results are displayed in the map.

This section will walk you through how to use runbooks to automate different type of network tasks:


- Monitor the network operational status
- Troubleshoot a repetitive network problem such as a slow application
- Proactively guard against misconfigurations such as security vulnerabilities over time
- Trigger the diagnosis based on an alert as the event is happening

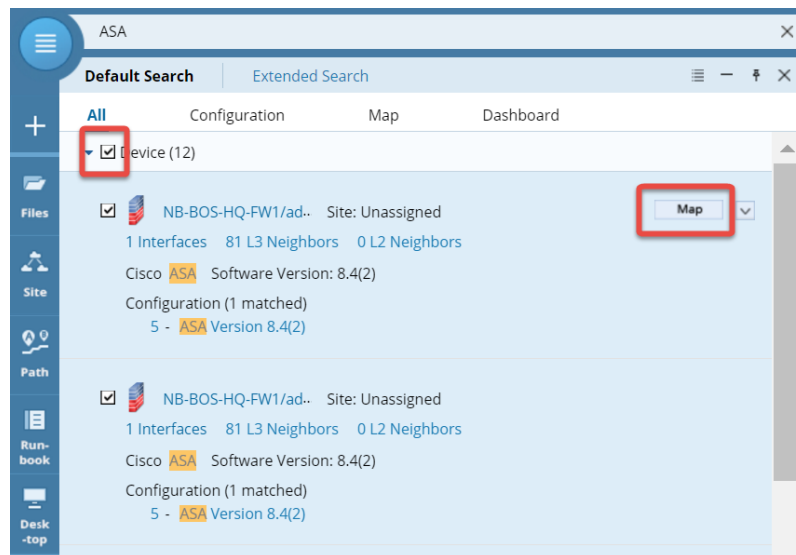
### 2.1 Monitor Network Operational Status

NetBrain runbooks enable you to monitor any common issues or problem areas of your network. Any abnormal status will be highlighted in the map. This module will use ASA firewall failover as an example to teach how to execute a runbook.

#### Instructions:

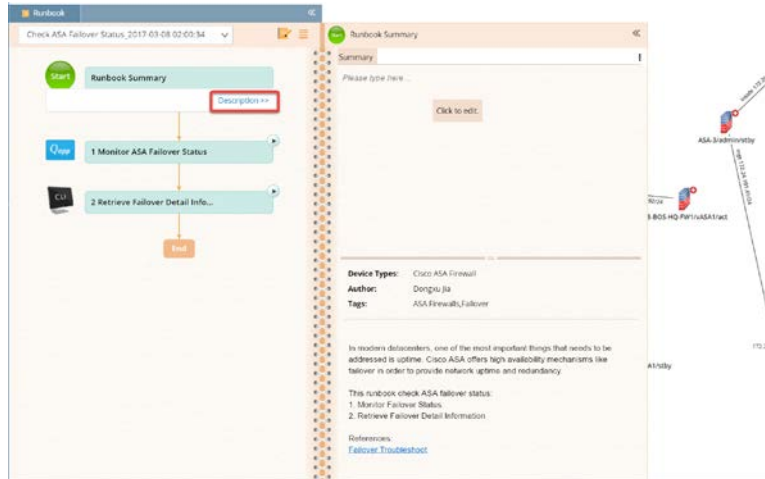
1. Map ASA firewalls: enter **ASA** in the search box. In search result pane select all devices and create a new map.


 **Tip:** refer to step 1-4 of section 1.2 for details on how to map multiple devices at once.

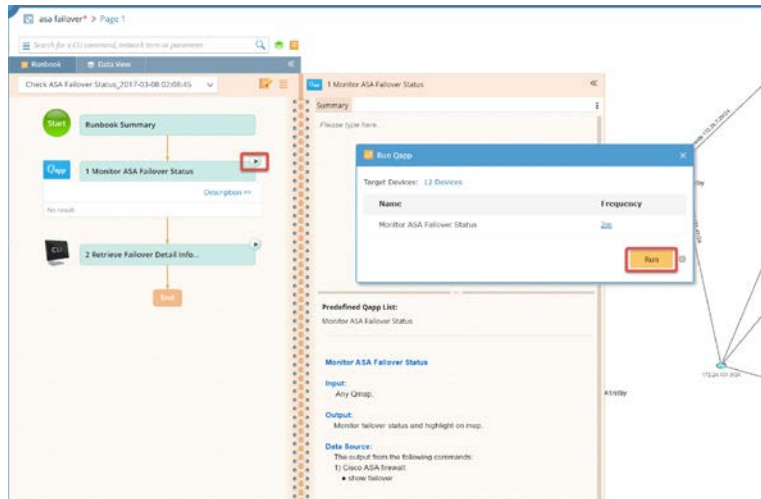





4. Select node **Runbook Summary** and click **Description>>** to read the summary. Pay attention to the field **Device Types** this runbook is applicable to.



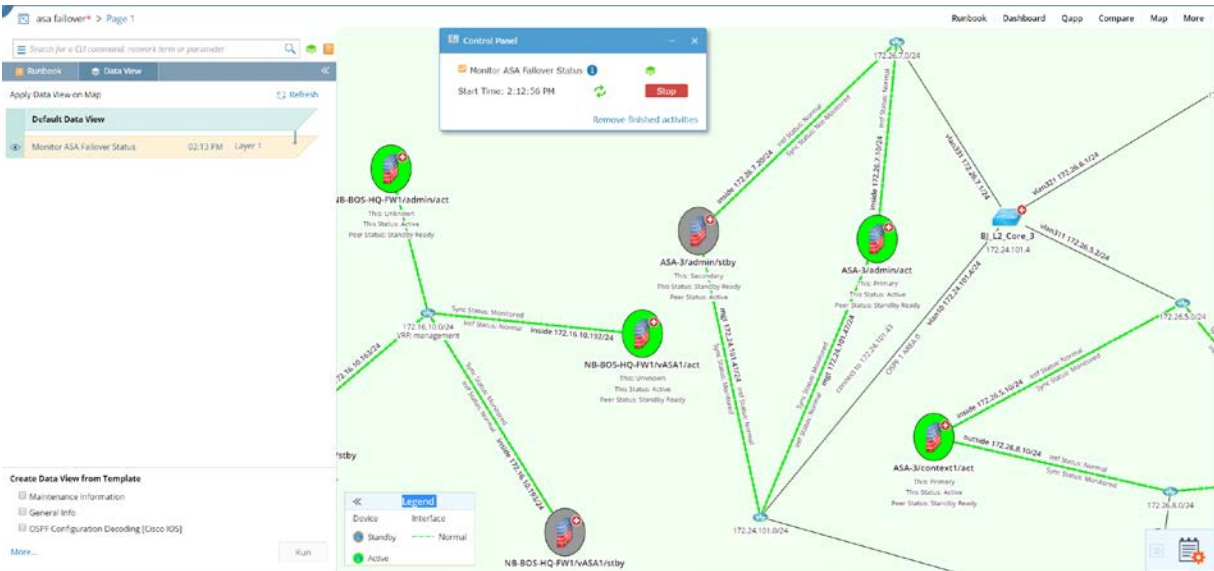
5. Run Qapp node: Select the first node, **Monitor ASA Failover Status** and click the  icon at the top right of the node. Save the map if prompted to do so. Click the **Run** button to run the Qapp.





6. The active or standby state are displayed in the map as well as the sync status of the interface. Zoom in on the map to see interface status if necessary. Click the **Stop** button in **Control Panel** to stop Qapp.

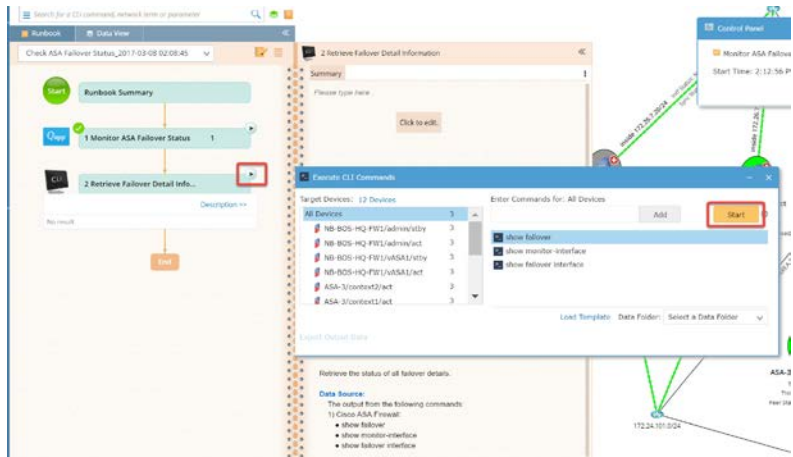
 **Tip:** A data view called **Monitor ASA Failover Status** is created. Check or uncheck this data view to switch the map between the monitored and normal state.





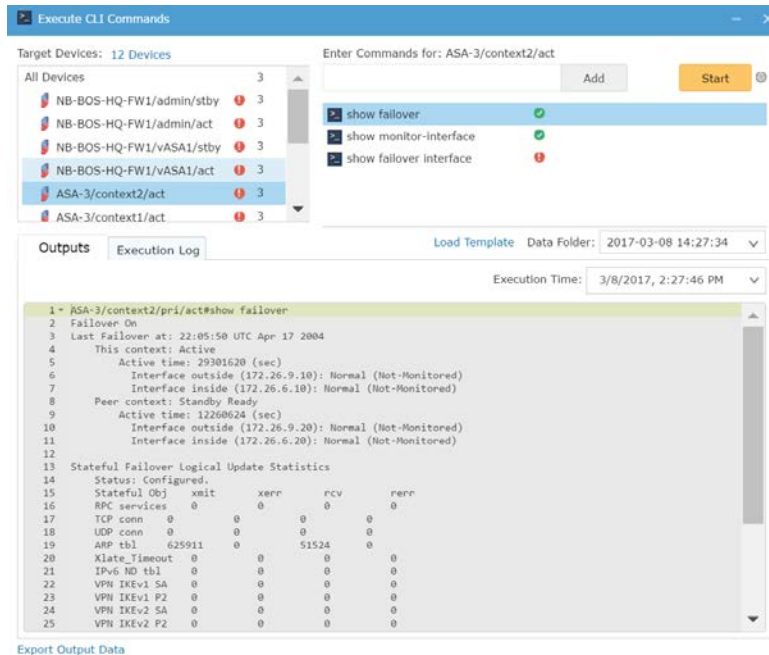
- Run CLI commands: Select the second node, **Retrieve Failover Detail Info** and click the  icon to start. In the **Execute CLI commands** window, click the **Start** button to retrieve three CLI commands.

 **Tip:** if a runbook is not visible in the map, click >> at the left side of the map to expand it. You can toggle between Runbook and Data View.

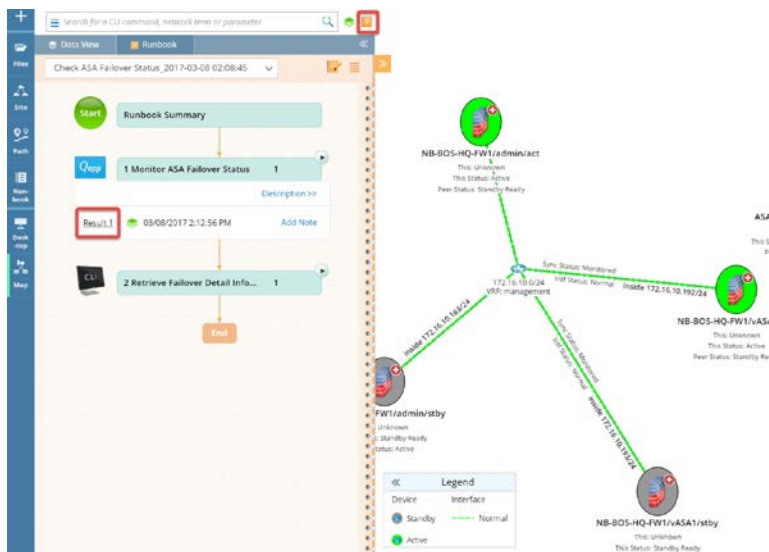




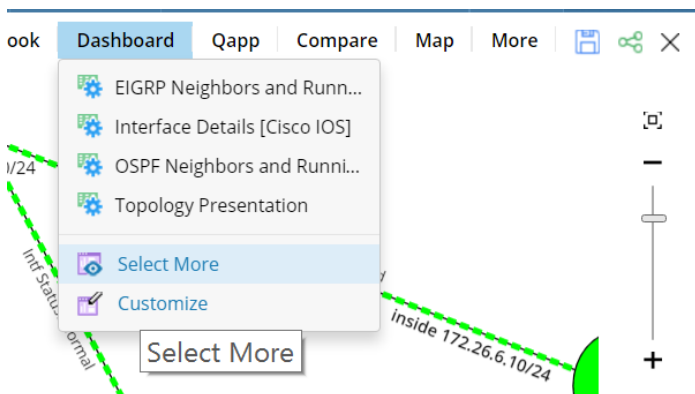
8. Select one device to view the show command status. Select one command to view the output results.



9. Save the map. The Runbook and its execution results are embedded inside the map. To verify this, you can close the map, reopen it and then select one of executable notes and you can view the results such as **Result 1**.

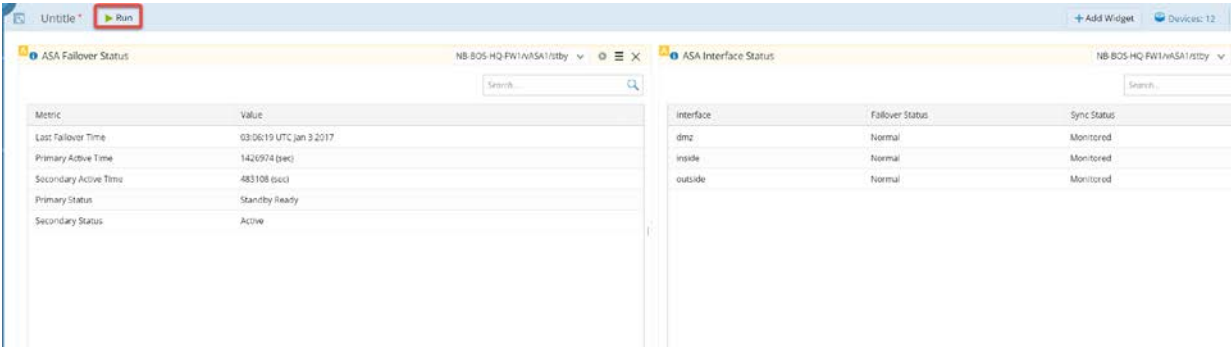


10. Run Dashboard to view the failover status for a device: From the map menu bar select **Dashboard > Select More**. Select **Built-in Templates > High Availability > Failover [Cisco ASA Firewall]**.





11. Click **Run** button to retrieve ASA status from the live network for all devices in the map. You can switch the device from pulldown menu.



The screenshot shows the NetBrain interface with two widgets displayed. The top bar includes a 'Run' button highlighted with a red box, and a 'Devices: 12' indicator. The left widget, titled 'ASA Failover Status', shows a table with metrics and values for a specific device. The right widget, titled 'ASA Interface Status', shows a table with interface details and their respective statuses.

Metric	Value
Last Failover Time	03:06:19 UTC Jan 3 2017
Primary Active Time	1426974 (sec)
Secondary Active Time	483108 (sec)
Primary Status	Standby Ready
Secondary Status	Active

Interface	Fallover Status	Sync Status
dmz	Normal	Monitored
inside	Normal	Monitored
outside	Normal	Monitored



## 2.2 Troubleshoot Repetitive Problems such as a Slow Application

The majorities of network problems are due to common network issues such as misconfigurations and bad cables. Troubleshooting these common issues can still take hours or days. For each common network problem NetBrain can help you create a runbook to automate troubleshooting process and reduce the time to fix the issue.

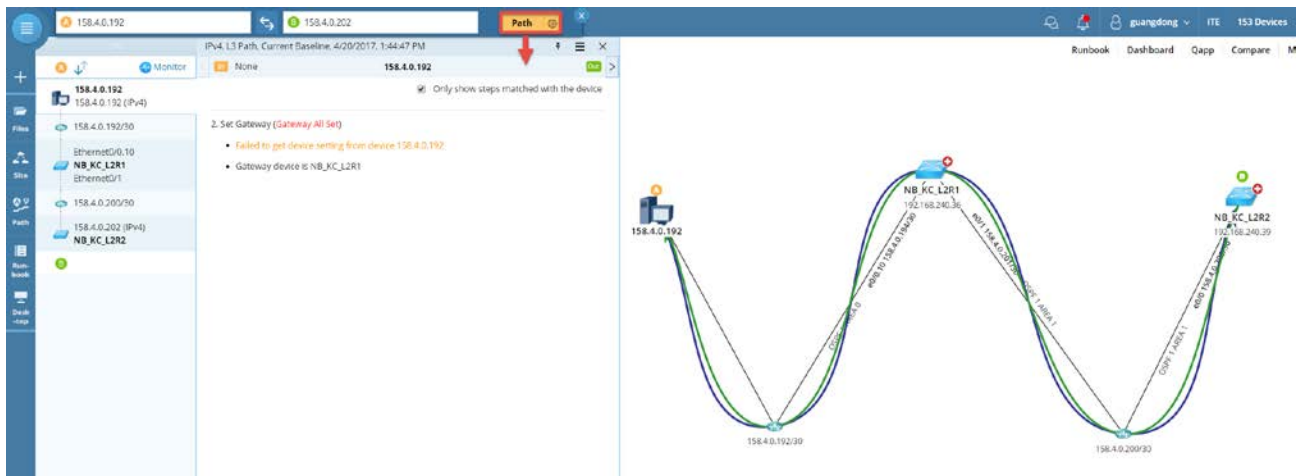
This module uses a slow application as an example to demonstrate how the built-in workbook can help troubleshooting.

### Instructions:

1. Create a new map and map the path from **158.4.0.192** to **158.4.0.202**. In **Path Setting** select **L3 Path** and **IPv4** protocol. You may also select **NB\_KC\_L2R1** as default gateway.




**Tip:** Refer to the section 1.3 for details on how to map the path.

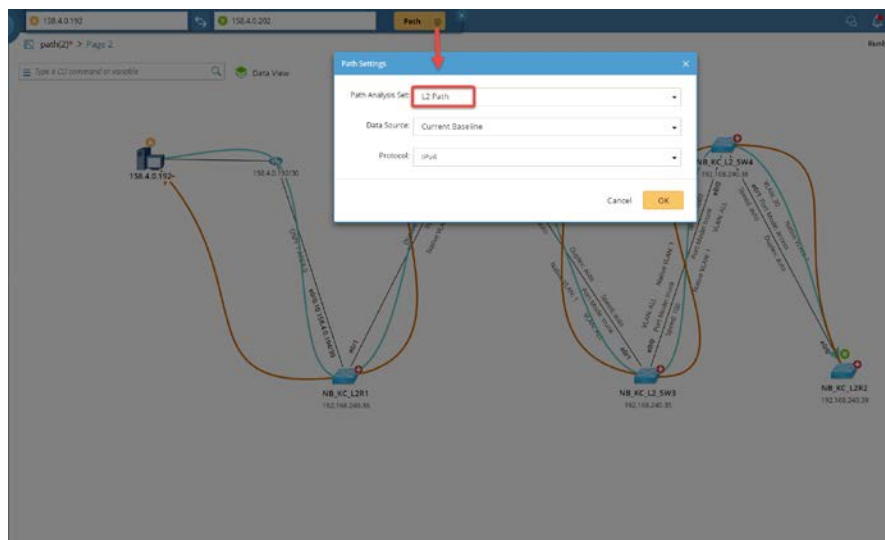


2. Run **General Health Monitor Qapp**: From the map menu bar select **Qapp > Overall Health Monitor**. In the Run Qapp window, click the **Run** button. Check the device status and interface data for any abnormalities.




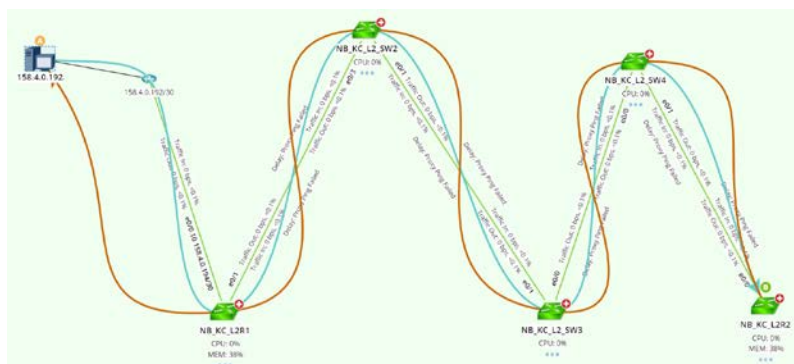
3. Create a new page and map the L2 path for the same set of IP addresses.

 **Tip:** refer to section 1.3 for details.

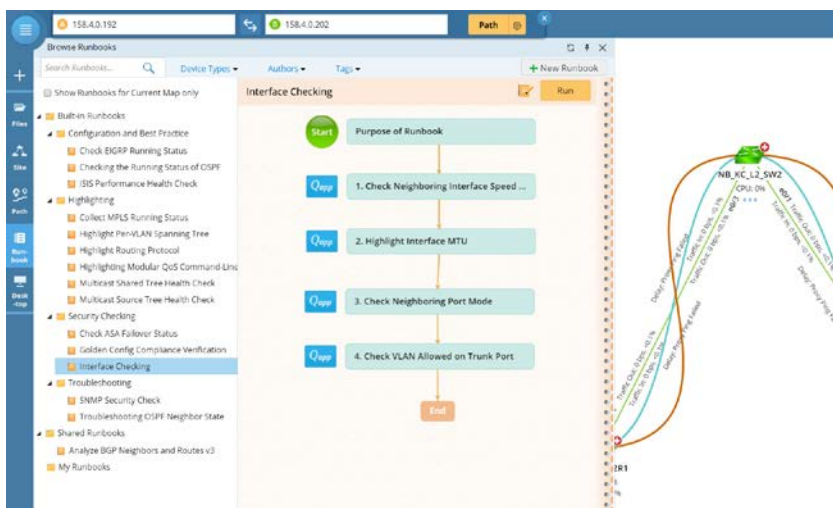



4. Run **General Health Monitor** Qapp again along L2 path. Check the device status and interface data for any abnormalities.


 **Tip:** Click ... below the interface or under the device to view more data not visible in the map.

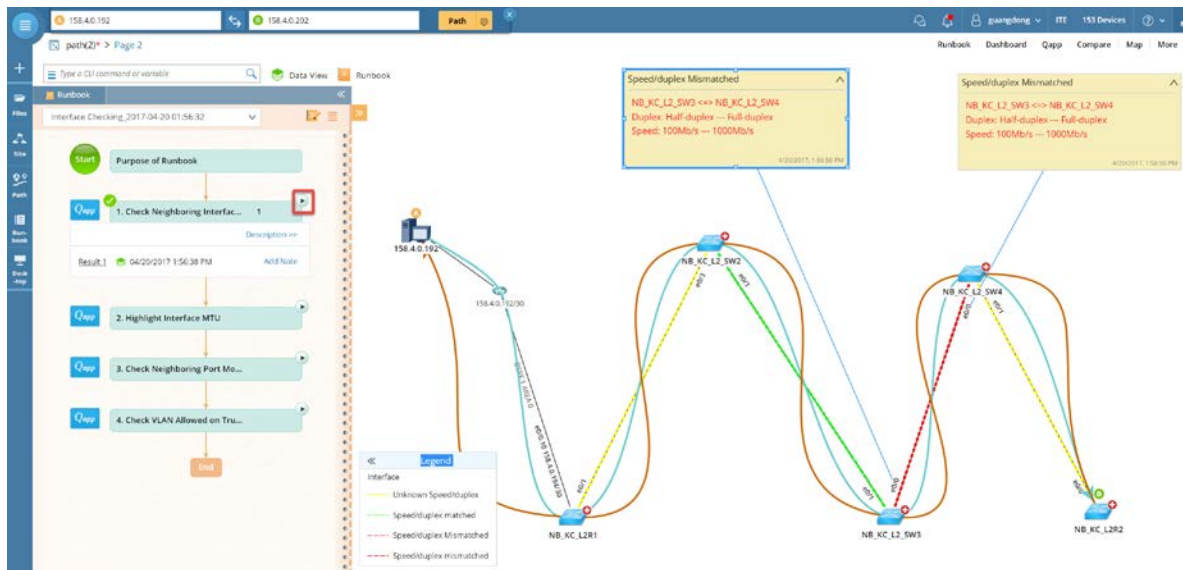


5. Browse the Runbooks to select and run the **Interface Checking** runbook.




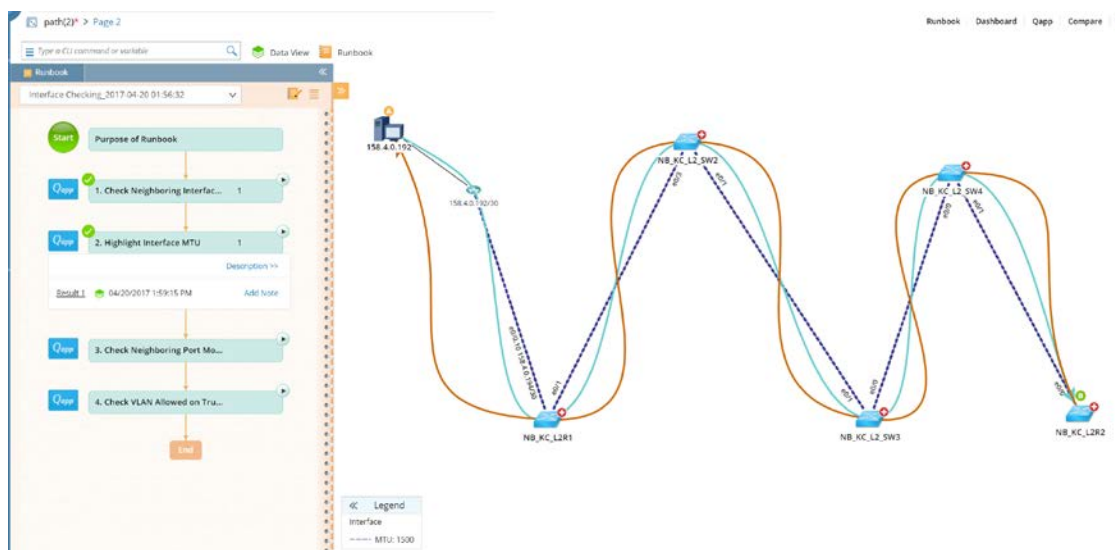
- Select the first node, **Check Neighbor Interface Speed and Duplex** and click icon  at the top right of the node to run the Qapp. Any speed or duplex mismatching is highlighted and interface notes are added for details.

 **Tip:** A Qapp can be run once or repeatedly. If the Qapp checks the configuration, running once is enough. If the Qapp monitors the operational status, it should be run for a period of time to allow deltas to be computed, and intermittent issues to be seen.



- Run other nodes of **Interface Checking** to check interface MTU, port modes and VLAN allowed on trunk modes.

 **Tip:** You can execute any node of a runbook in any order.



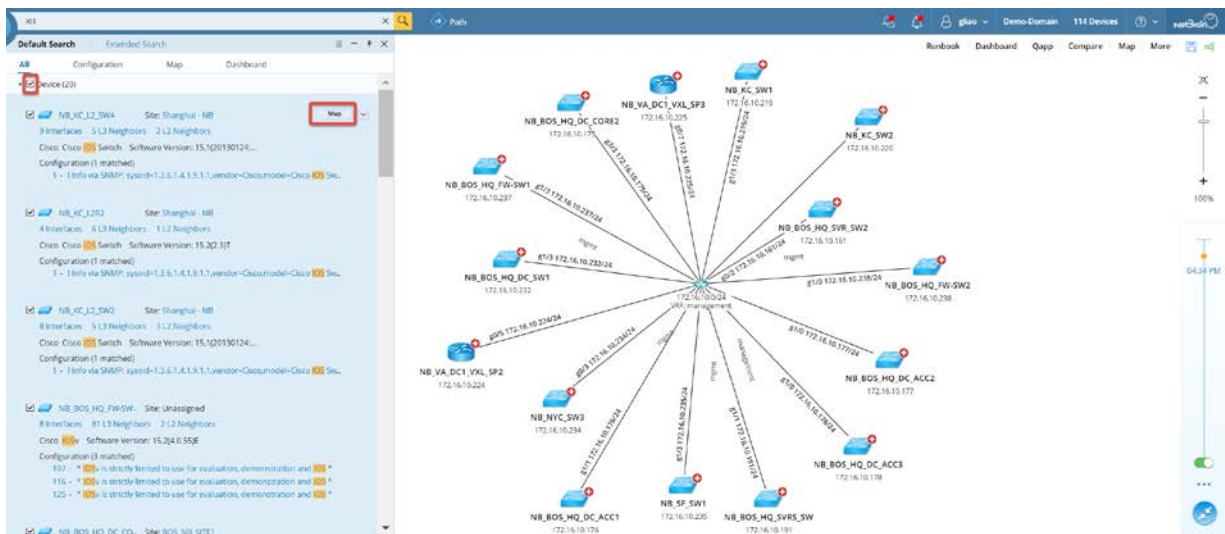
## 2.3 Proactively guard against misconfigurations

NetBrain Runbooks can be used to enforce configuration compliance. For example, a Runbook can be created to check configurations against a set of rules (sometimes called Golden Rules). Additionally, a logging system can be integrated with NetBrain to trigger this runbook analysis to validate any configuration change.

This module shows how to use Runbooks to check configurations for security vulnerabilities.

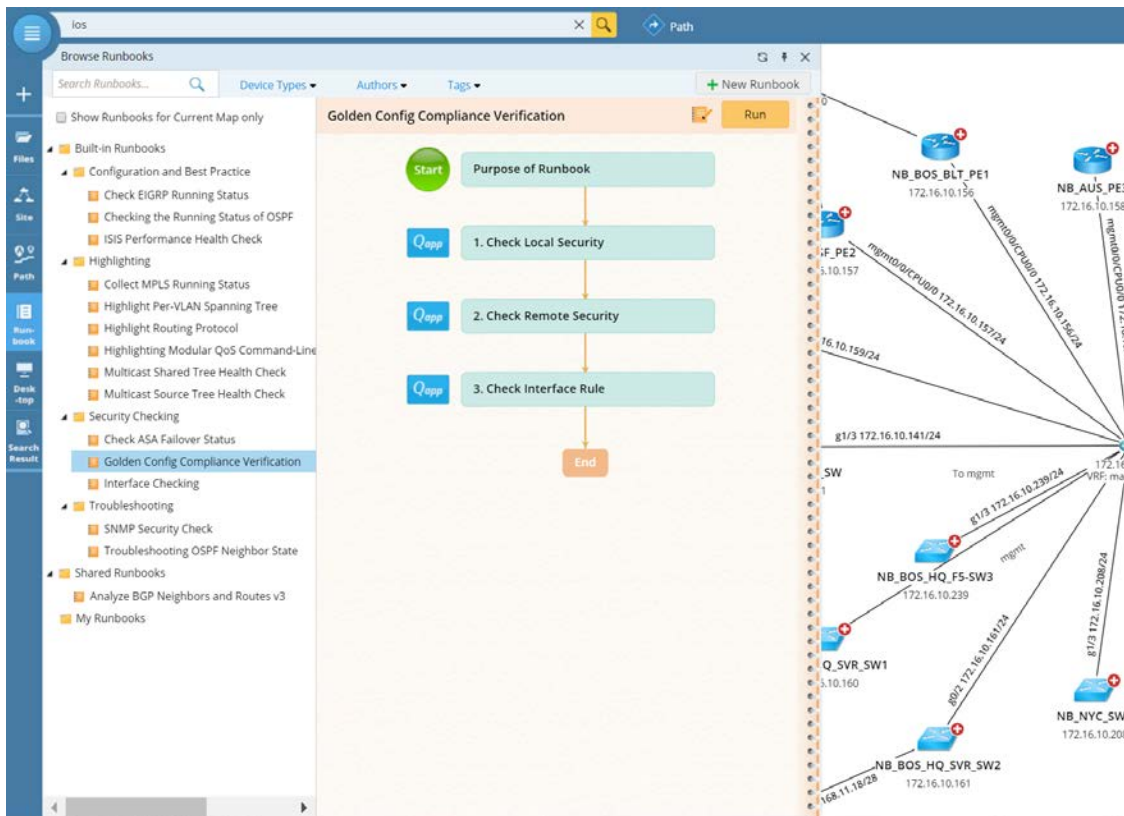
### Instructions:


1. Map cisco IOS devices: Create a new map. Enter **ios** in search field and map all devices in the search field.

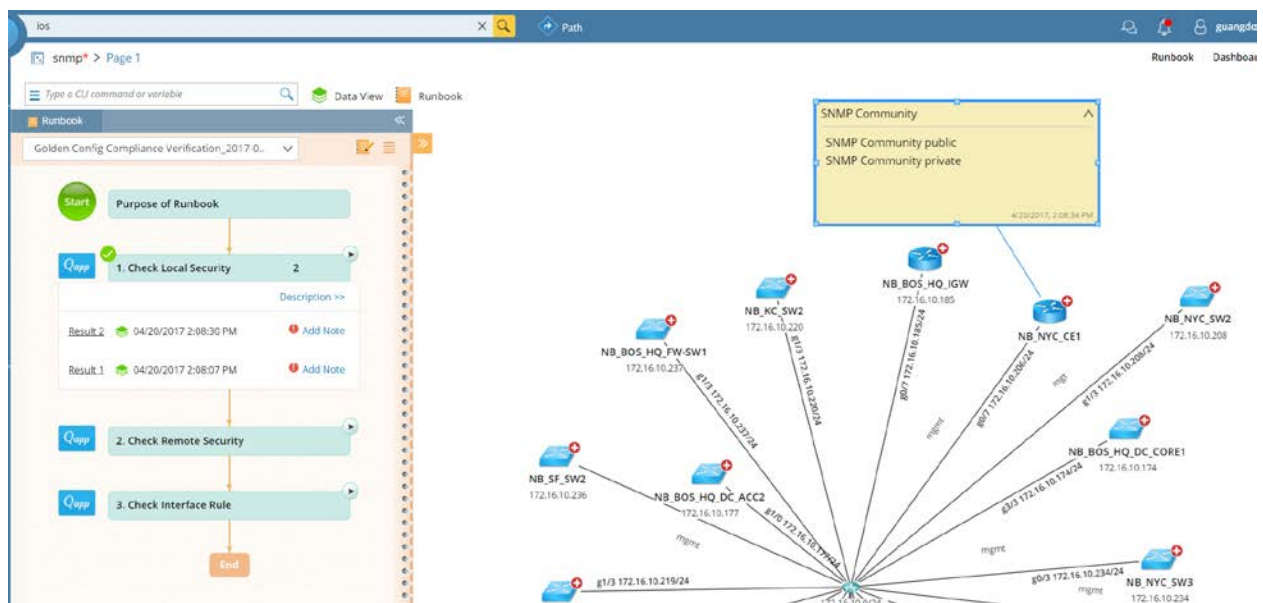


2. Open and run the Runbook Security Vulnerability: Click **Runbook** in the left side menu bar and select **Built-in Runbooks > Security Checking > Golden Config Compliance Verification**. Click the **Run** button.





3. Select the node, **Check Local Security** and click icon  at the top right of the node to run the Qapp. The devices with the default SNMP string are attached with a device note showing the detail configurations.





4. Run other nodes to check remote security and interface rule.

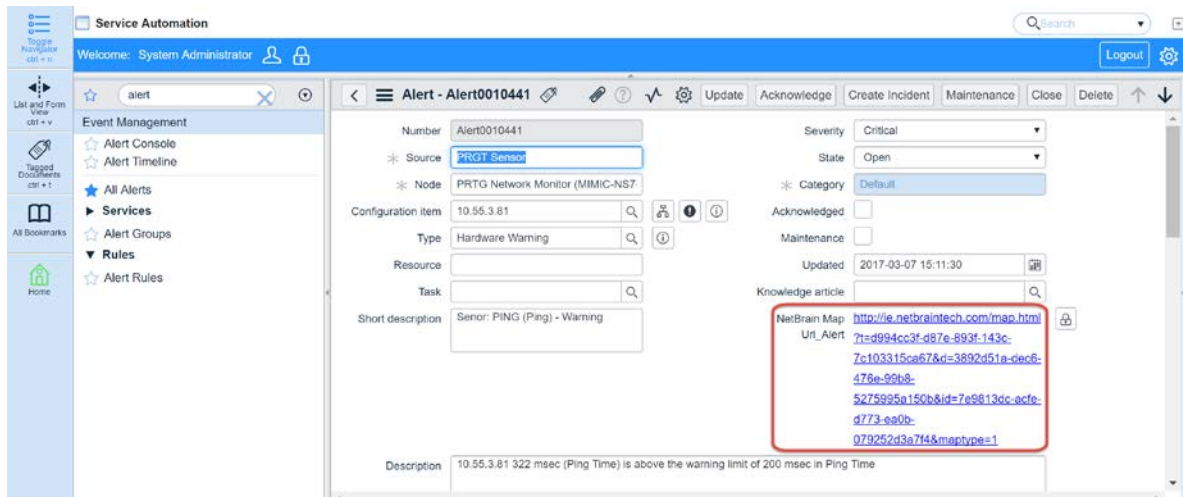
## 2.4 Diagnosis a problem when it is happening


NetBrain provides a set of RESTful APIs and a framework which enables the flexible integration with 3<sup>rd</sup> party system. One example is the integration with the ticket system such as Service Now. When a new ticket is created in ServiceNow indicating a slow application, ServiceNow auto-triggers an API call to NetBrain which maps the application and automatically executes a Runbook inside NetBrain collecting relevant data to the problem while it is happening. No human intervention required.

### Instructions:

*The instructions here illustrate how NetBrain functions can be auto triggered from ServiceNow. You can contact NetBrain support for the integration request.*

1. Login to the Service Now web page and view an alert or an event. Service Now has been setup to trigger an API call to NetBrain for each alert. A URL is added into every alert. Click the URL to open the map created by that API inside NetBrain.



**Tip:** You can define the methods to create the map and Runbooks to run for different types of alert. NetBrain provides a page for you to define them. This page is located under **System Automation Manager > API Stub Manager** (clicking the icon  at the top left of the page to open it).







The screenshot displays the NetBrain interface with a Runbook workflow on the left and the 'Execute CLI Commands' window on the right.

**Runbook Workflow:**

- Start** (Green circle)
- Runbook Info** (Green box)
- CLI Command 1** (Green box with '1' in a circle)
- Overall Healthy Monitor 1** (Green box with a heart icon and '1' in a circle)
- End** (Orange box)

**Execute CLI Commands Window:**

- Target Devices:** 4 Devices (PA-2, NB\_CA\_SF\_CEL, NB\_CA\_SF\_PES, NB\_BOS\_BLT\_BB2)
- Enter Commands for: NB\_CA\_SF\_PES**
  - ☒ show interface
- Outputs:**

```

1> NB_CA_SF_PES#show interface
2 FastEthernet0/0 is up, line protocol is up
3 Hardware is DEC21140, address is ca0a.0e2f.0000 (bia ca0a.0e2f.0000)
4 Description: to_BB2
5 Internet address is 10.55.3.82/30
6 MTU 1500 bytes, BW 1000000 Kbits/sec, DLY 100 usec,
7 reliability 255/255, txload 1/255, rxload 1/255
8 Encapsulation ARPA, loopback not set
9 Keepalive set (10 sec)
10 Full-duplex, 10000/s, 1000baseTX/100
11 ARP type: ARPA, ARP Timeout 04:00:00
12 Last input 00:00:03, output 00:00:00, output hang never
13 Last clearing of "show interface" counters never
14 Input queue: 0/75/408/407 (size/max/drops/flushes); Total output drops: 0
15 Queueing strategy: Class-based queueing
16 Output queue: 0/1000/0 (size/max total/drops)
17 5 minute input rate 3000 bits/sec, 2 packets/sec
18 5 minute output rate 6000 bits/sec, 2 packets/sec
19 5127224 packets input, 3713704208 bytes
20 Received 3473316 broadcasts (0 IP multicasts)
21 0 runs, 0 giants, 377 throttles
22 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
23 0 watchdog
24 0 input packets with dribble condition detected
25 7959124 packets output, 489803880 bytes, 0 underruns
          
```
- Execution Log:** (Empty)
- Load Template:** Data Folder: 2017-03-03 08:20:00
- Execution Time:** 3/3/2017, 8:20:10 AM
- Export Output Data:** (Link)

4. Click the **General Health Monitor** node to view the monitor results in the map.

The screenshot displays the NetBrain interface with the map view on the right and the Runbook workflow on the left.

**Map View:**

- Legend:**
  - Device:** Error (Red), Warning (Yellow), No Alerts (Green)
  - Interface:** Error (Red), Warning (Yellow), No Alerts (Green)
  - Data Unit:** Error (Red), Warning (Yellow), No Alerts (Green)
- Map:** Shows a network topology with nodes and links. The node **NB\_CA\_SF\_PES** is highlighted with a green circle and a tooltip showing its IP address: **192.168.121.10 ~ 10.55.3.81**.
- Time:** 09:07 AM, 03/03
- Scale:** 280N



# Additional Questions?

---

If you have additional questions, please contact us.

Support questions:	Training questions:
+1 800.605.7964 <a href="mailto:support@netbraintech.com">support@netbraintech.com</a>	+1 800.605.7964 <a href="mailto:education@netbraintech.com">education@netbraintech.com</a>

