



PORTrockIT Software Manual Eli-v6.5.391

Bridgeworks

Unit 1, Aero Centre, Ampress Lane,
Ampress Park, Lymington,
Hampshire SO41 8QF
Tel: +44 (0) 1590 615 444
Email: support@4bridgeworks.com

Table of Contents

1	Introduction	9
1.1	Overview	9
1.2	Manual Layout	10
1.3	Definitions	10
1.3.1	Node	10
1.3.2	Endpoint	10
2	Initial Setup and Operation	11
2.1	Browsers	11
2.2	Connecting to the Web Interface	11
2.2.1	Connecting using a dynamically assigned IP address	11
2.2.2	Connecting without a dynamically assigned IP address	12
2.3	Initial screen	13
2.4	Network Setup via CLI	14
2.5	Management Console (Home screen)	17
3	Node Configuration Reference	19
3.1	Network Connections	19
3.1.1	Network Interfaces	20
3.1.2	Add Bond	20
3.1.3	General Settings	20
3.1.3.1	Hostname	21
3.1.3.2	Hostname on login page	21
3.1.3.3	DNS Servers	21
3.1.3.4	Default Route	21
3.1.3.5	Dead Gateway Detection	22
3.1.3.6	Enable IPv6	23
3.1.3.7	Enable VLANs	24

3.1.4	Interface Statistics	24
3.1.4.1	Data Transmission Rate	25
3.1.4.2	Data Reception Rate	25
3.1.4.3	Legend	26
3.1.5	Network Routing	26
3.1.5.1	Add Static Route	26
3.1.6	LLDP	28
3.1.6.1	LLDP Settings	29
3.1.7	Network Tools	29
3.1.7.1	Ping	30
3.1.7.2	Traceroute	31
3.1.8	Port Settings	32
3.1.8.1	Linked Interfaces	34
3.1.8.2	Enable Port	35
3.1.8.3	Setting the MTU	35
3.1.8.4	Enable Forwarding	35
3.1.8.5	Bridged Physically-In-Path Mode	36
3.1.8.6	Configuring Spanning Tree Parameters	37
3.1.8.7	LLDP Port Settings	39
3.1.8.8	LLDP Neighbours	39
3.1.8.9	LLDP Statistics	40
3.1.8.10	LLDP Settings	40
3.1.8.11	Setting the IP Address	40
3.1.8.12	Bonding Options	41
3.1.8.13	Adding VLANs	43
3.1.8.14	Committing the Changes	44
3.2	Passwords & Security	44
3.2.1	System Password	45
3.2.2	Password Reset Options	45
3.2.2.1	Password Reset via Email	45

3.2.2.1.1	Setup	45
3.2.2.1.2	Using Password Reset via Email	46
3.2.2.2	Password Reset via Local Console or SSH	48
3.2.2.2.1	Setup	48
3.2.2.2.2	Using Password Reset via Local Console or SSH	49
3.2.3	Secure Connection	51
3.2.3.1	Generate new Certificate Signing Request	51
3.2.4	User Settings	52
3.2.4.1	Session Timeout	52
3.2.4.2	Unit Display Format	52
3.2.5	Secure Shell (SSH)	52
3.2.5.1	Managing Public Keys	53
3.2.5.2	Using SSH	54
3.3	Service Control	54
3.3.1	Network Time Protocol (NTP)	56
3.3.2	Simple Network Management Protocol (SNMP)	58
3.3.2.1	System Information	59
3.3.2.2	SNMP Trap Sinks	59
3.3.2.3	Add SNMP Trap Sink	59
3.3.2.4	Download MIB Files	60
3.3.3	Email	61
3.3.4	Event Notification Email	62
3.3.5	Remote System Log	62
3.3.5.1	Editing or Deleting a Connection	64
4	PORTrockIT Configuration	65
4.1	Node Management	65
4.1.1	Remote Nodes	66
4.1.1.1	Configured Nodes	68
4.1.1.2	Non-Configured Nodes	68

4.1.1.3	Orphaned Nodes	68
4.1.2	Add Remote Node	69
4.1.3	Transfer Statistics	70
4.1.3.1	Data Transfer Rate	71
4.1.3.2	Download 24 Hour Transfer History	72
4.1.4	Access Control	72
4.1.4.1	Remote Administration	73
4.1.4.2	Whitelist	73
4.1.5	IPsec	73
4.1.5.1	Enabling IPsec service	74
4.1.5.2	Encrypting Accelerated Traffic	74
4.1.5.3	Adding a PSK (Pre-Shared Key)	75
4.2	PORTrockIT Node Page	75
4.2.1	Node Status	76
4.2.2	Node Configuration	77
4.2.3	Applications & Utilities	77
4.2.4	Path Configuration	77
4.2.4.1	Setting Primary and Failover Paths	78
4.2.4.2	Filtering options	79
4.2.4.3	Configuring a Node's Bandwidth	79
4.2.5	Node Specific Transfer Statistics	80
4.2.5.1	Data Transfer Rate	80
4.2.5.2	Download 24 Hour Transfer History	81
4.2.6	Remove Node	81
4.2.7	Relationships	82
4.2.7.1	Prerequisites	82
4.2.8	Services Table	83
4.2.9	Toggling a Relationship	83
4.2.10	Configure Services	84
4.2.11	Cancel	84

4.2.12	Save	84
4.2.13	Disabled Services	84
4.2.14	VPN Configuration	85
4.2.15	WCCPv2	86
4.2.15.1	Prerequisites	87
4.2.15.2	Configuring a Service Group	87
4.2.15.3	Monitoring a Service Group	89
4.2.15.4	WCCPv2 Service Group	89
4.2.16	Remote Control	90
4.2.17	Learn	92
4.2.17.1	Data Transfer Rate	93
4.3	Service List	93
4.3.1	Service Table	94
4.3.2	Remove Service	94
4.3.3	Add Service	94
4.3.3.1	Name	96
4.3.3.2	Address	96
4.3.3.3	Public IP - Only available if NAT has been enabled	97
4.3.3.4	Private IP - Only available if NAT has been enabled	97
4.3.3.5	Protocol	97
4.3.3.6	Outgoing Interface	97
4.3.3.7	Out of Path	97
4.3.3.8	Cancel	97
4.3.3.9	Add Service	97
4.3.4	Disabled Services	97
4.4	Incoming Relationships	98
4.4.0.1	Active Incoming Relationships	98
4.4.1	Incoming Relationship	99
4.4.1.1	Nodes	100
4.4.1.2	Connections	100

4.5	Client NAT Preservation	100
4.5.1	Client NAT IP Addresses Table	102
5	Port Mappings	103
5.1	Setting Port Mappings	104
5.2	Removing a Port Mapping	104
5.3	Saving Port Mappings	104
5.4	Available Port Mappings	104
6	Node Maintenance	106
6.1	System Information	106
6.2	System Log	107
6.3	Load/Save Configuration	108
6.3.1	Loading a Saved Configuration	109
6.3.2	Saving the Configuration to Disk	109
6.3.3	Restoring to Factory Defaults	110
6.4	Firmware Updates	110
6.4.1	Updating Firmware Manually	111
6.5	Licence Key Management	112
6.5.1	Uploading a Licence Key	113
6.5.2	Removing a Licence Key	113
6.5.3	Downloading a Licence Key	114
6.6	Diagnostics	114
6.7	Task Scheduler	115
6.7.1	Adding Tasks	116
6.7.2	Removing/Editing Tasks	116
6.7.3	Task Wizard	118
6.7.3.1	Action - Email Performance Statistics	118
6.7.3.2	Action - PORTrockIT Bandwidth Limit	119
6.7.3.3	Trigger	120
6.7.3.4	Start Date	121

6.7.3.5	End Date	121
6.7.3.6	Summary	122
7	Troubleshooting	123
7.1	Network Connectivity Problems	123
7.2	Network Performance Problems	123
7.3	Recovery Wizard	124
7.3.1	Factory Restore	125
7.3.2	Delete Configuration	127
A	IP Protocols and Port Numbers	130
A.1	Inbound LAN Protocols and Port Numbers	130
A.2	Outbound LAN Protocols and Port Numbers	130
A.3	WAN Protocols and Port Numbers	131
A.4	PORTrockIT TCP Port Numbers	131
A.4.1	Caringo Swarm Object Storage	131
A.4.2	Commvault VM Backup and Recovery	131
A.4.3	HTTP	131
A.4.4	HTTPS	132
A.4.5	IBM Spectrum Protect	132
A.4.6	NetApp SnapMirror	132
A.4.7	NetApp StorageGRID Client	132
A.4.8	NetApp StorageGRID Combined	133
A.4.9	NetApp StorageGRID Intercluster	134
A.4.10	NFS	134
A.4.11	PeerGFS	135
A.4.12	S3	135
A.4.13	SecuritEase	135
A.4.14	Veeam Backup & Replication	135
A.4.15	Veritas NetBackup	136
A.4.16	WANDisco Fusion	136

A.4.17 Web	136
B Accessing the Node from Windows using a static IP Address	137
C PORTrockIT Series Comparisons	141
C.1 Node Limits	141
D Transfer Statistics Graphing Instructions for Excel 2010	142
E Useful Links	153

1 Introduction

Thank you for purchasing the Bridgeworks PORTrockIT Node.

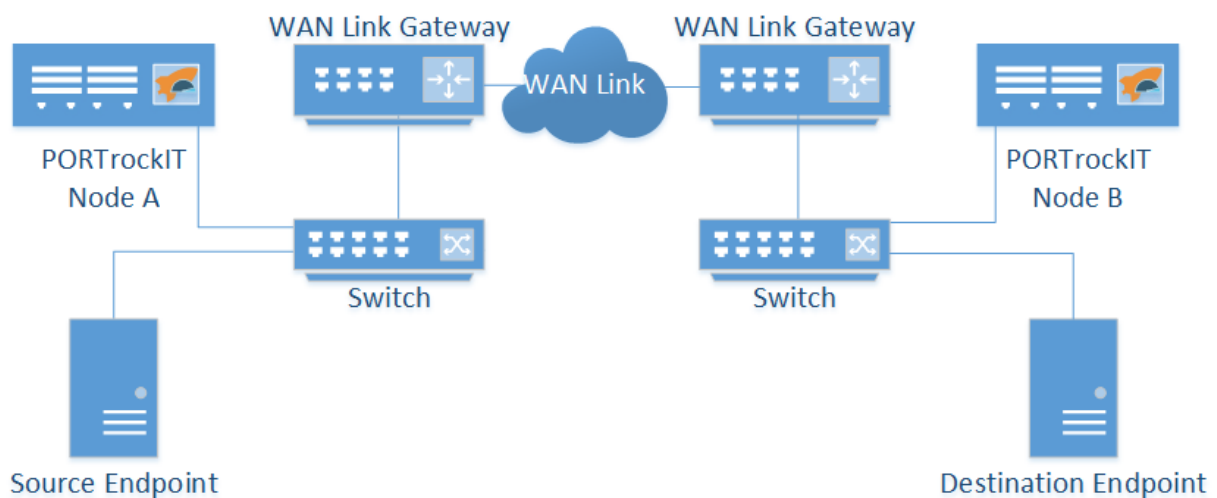
The PORTrockIT Node has been designed to ensure that in the majority of installations it will require minimal setup before use. However, we suggest you read the following section which will guide you through setting up your Node.

This Manual contains information for setting up all feature cards that may be installed in your PORTrockIT Node. Therefore, some sections may refer to a feature card that may not be installed in your particular Node.

1.1 Overview

Bridgeworks latency mitigating technology allows you to accelerate your network traffic between two different sites. These sites may include data centres, your business centres and the Amazon Web Services (AWS) cloud. Each site will require a PORTrockIT Node to accelerate your desired traffic. PORTrockIT nodes can be either physical hardware appliances, virtual machine images for popular platforms or Amazon Machine Images (AMIs).

The following diagram shows a basic example of how the PORTrockIT Nodes could be deployed.

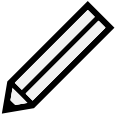




In this case data is accelerated from the *Source Endpoint* to the *Destination Endpoint*. *Node A* is set up to intercept traffic leaving the *Source Endpoint*, accelerating any data that matches the protocol across the *WAN Link* to the connected *Node B*. The traffic then continues on normally to its intended destination.

This basic setup can be extended to work in both directions allowing a bidirectional link between the two *Endpoints*. Depending on the specific protocol you wish to accelerate and your existing network setup, the exact topology you need will vary.

1.2 Manual Layout

Throughout the manual, symbols will be used to quickly identify different pieces of information.

	This icon represents a note of interest about a step or section of information.
	This icon represents an important piece of information.
	This icon represents a warning. Care must be taken and the warning should be read thoroughly.

1.3 Definitions

Throughout this manual, selected terms will be used to describe pieces of equipment and concepts. This section provides an explanation of those terms.

1.3.1 Node

A Node refers to a PORTrockIT unit.

1.3.2 Endpoint

A host machine sending/receiving protocol data to be accelerated by PORTrockIT technology, as well as possibly other, non-accelerated data.

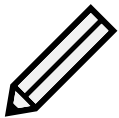
2 Initial Setup and Operation

The primary method for configuring any option is through the web interface. The following section highlights the requirements needed to access the web interface of the Node.

2.1 Browsers

This Node supports the following browsers:

- Microsoft Edge¹
- Mozilla Firefox¹
- Google Chrome¹
- Safari¹

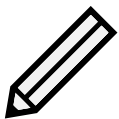


Note: JavaScript must be enabled within the web browser to use the web interface.



Important: If you choose to use a browser that is not in the list of supported browsers, Bridgeworks cannot guarantee the behaviour of the Node's functionality.

2.2 Connecting to the Web Interface



Note:

- DHCP is enabled by default on the management interface.
- The default hostname is `bridgeworks`.

For help locating management interfaces on hardware appliances, please refer to your hardware manual.

2.2.1 Connecting using a dynamically assigned IP address

You can find the Node IP address on the server/router assigning the dynamic IP address, virtual console if you are using a virtual machine, or by attaching a monitor to the Node.

¹Latest version as of release



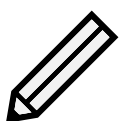
The image above represents something similar to what you would find when attaching a monitor to the Node.

If the Node is successfully assigned a dynamic IP address, and DNS resolution is enabled on your network by default, you can easily access the Node's web interface from the default hostname by navigating to: <http://bridgeworks/>

2.2.2 Connecting without a dynamically assigned IP address

Without a dynamically assigned IP address you will need to set up a static IP using the CLI, in order to access the web interface. To accomplish this, you will need to connect a keyboard and monitor to the Node. For virtual machines use the corresponding virtual keyboard and mouse.

Refer to Section [2.4: Network Setup via CLI](#) for the initial CLI setup.



Note: The hardware manual for the device includes details of where the ports are located. See Appendix [E: Useful Links](#) for information on how to access the manuals.



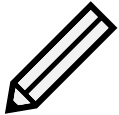
Important: Only US-International and compatible keyboards are supported.

2.3 Initial screen



Important: Your host will likely need to be directly-connected to the Node if DHCP is not enabled, and its subnet set appropriately. See [Appendix B: Accessing the Node from Windows using a static IP Address](#) for help with accessing the Node web interface without DHCP.

From within your web browser, connect to the Node's web interface using the default hostname or IP address of a connected management interface.



Note: If you have already configured the initial password via the CLI (Section [2.2.2: Connecting without a dynamically assigned IP address](#)) you can skip the following step on how to set up your password.

Once you have connected to the web interface on the Node you will be provided with the Bridgeworks End User License Agreement (EULA) which must be accepted before you are able to access the Node. Ensure you read this agreement thoroughly. To proceed, you must accept the agreement by clicking the **Accept** button.

End User License Agreement

Software License Agreement

This Bridgeworks, Ltd. SOFTWARE LICENSE AGREEMENT (this "Agreement") forms a binding legal agreement by and between Bridgeworks and you, or if you are entering into this Agreement on behalf of another entity or organization, that entity or organization (in either case, "Licensee").

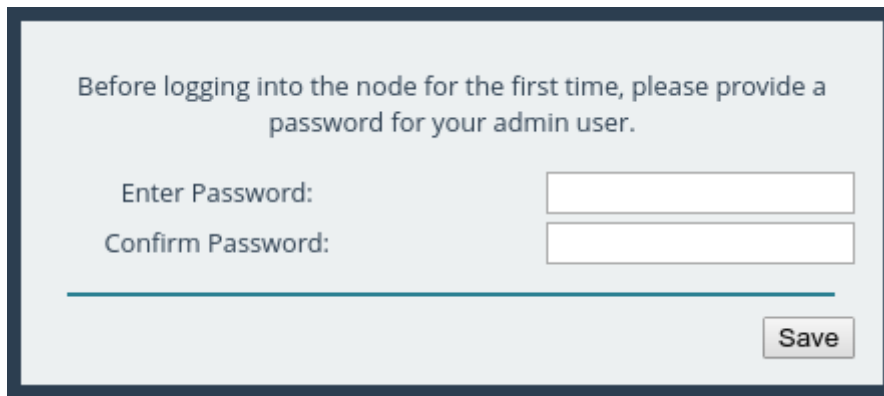
Licensee desires to obtain a license to certain software developed and offered by Bridgeworks, Ltd. ("Bridgeworks"). Licensee has completed one or more orders referencing this Agreement (whether completed online or in another form accepted by Bridgeworks, each an "Order") specifying such software (the "Software"). This Agreement establishes the terms and conditions under which Bridgeworks is willing to provide Licensee with a limited right to access and use the version of such Software set forth in each Order under this Agreement for Licensee's own internal business purposes. Bridgeworks is willing to make available the Software to Licensee on the condition that Licensee agrees to be bound by the terms and conditions of this Agreement.

Accept



Important: If you accepted the Bridgeworks EULA during the deployment of your Node, you will not need to accept it again.

You will then see the entry page shown below:

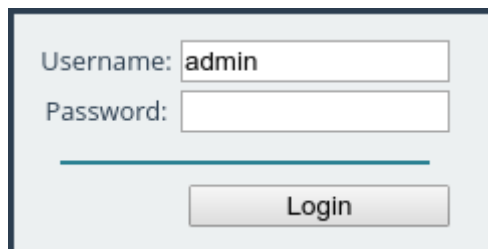


Important: AWS Nodes will require the instance ID and Azure Nodes will require the subscription ID to be able to set the initial password.



Important: During deployment of Azure Nodes you are able to set the initial password if you choose to use password authentication. If you set up your password this way, you will be directed to the login screen.

Enter and confirm the new web interface password to be presented with the login screen. The password must be between 5 and 64 characters and should contain both symbols and numbers.



To access the web interface a username and password must be used. The default username is *admin*.



Important: On Azure nodes, you will need to enter the username that you chose during deployment.

2.4 Network Setup via CLI



Important: If your Node is hosted on a cloud platform, you will not be able to access the CLI, and must configure it via the platform's interface.

If you are initially unable to access the web interface, you may need to perform some initial setup

via the CLI.

On the Node's interface, press Alt+F2 to enter the CLI.

If this is your first time logging into the Node, you will have to set a password.

```
Bridgeworks Management Interface
No password configured - Enter new password: _
```

You can now log into the Node using the default username *admin*, and the password you set.

Within the CLI, you can select an option by entering the number next to it. Navigate to *Network Connections* using *1*, then select the port you will be using to manage your Node.

```
=====
Network Port                                Bridgeworks WANrockIT
=====
1 Enable Port                               : Yes
2 MTU Size                                  : 1500
3 Enable Forwarding                         : No
4 Use DHCP to assign an IP address          : Yes
5 DNS Registration                          : Yes
6 Use the following IP address              : No
7 IP Address                               : 10.10.64.60
8 Netmask                                   : 255.255.0.0
9 Gateway                                   : 10.10.10.1

s Save
x Cancel
=====
```

Ensure this port is enabled by checking the *Enable Port* option. If this says *No* next to it, select it, then press *y* to enable it.

DHCP will be enabled by default. If you need to set a static IP address for your Node, select *Use the following IP address*, this will disable DHCP automatically.

Next, set your IP address by selecting *IP Address* and entering a valid IPv4 address. You may also need to adjust the netmask and default gateway.

When you are done modifying your port settings, press *s* to save.

If you need to set your default route, you can navigate to *Network Connections*, then *General Settings*, then *Default Route*, and select the port you configured. Then press *s* again to save.

Once you have saved all your settings, press *r* to reboot your Node to apply them.

Once the Node has finished rebooting, you should see the status screen. If the port is working, you should see an IP address, and *UP*.

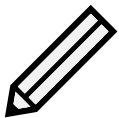
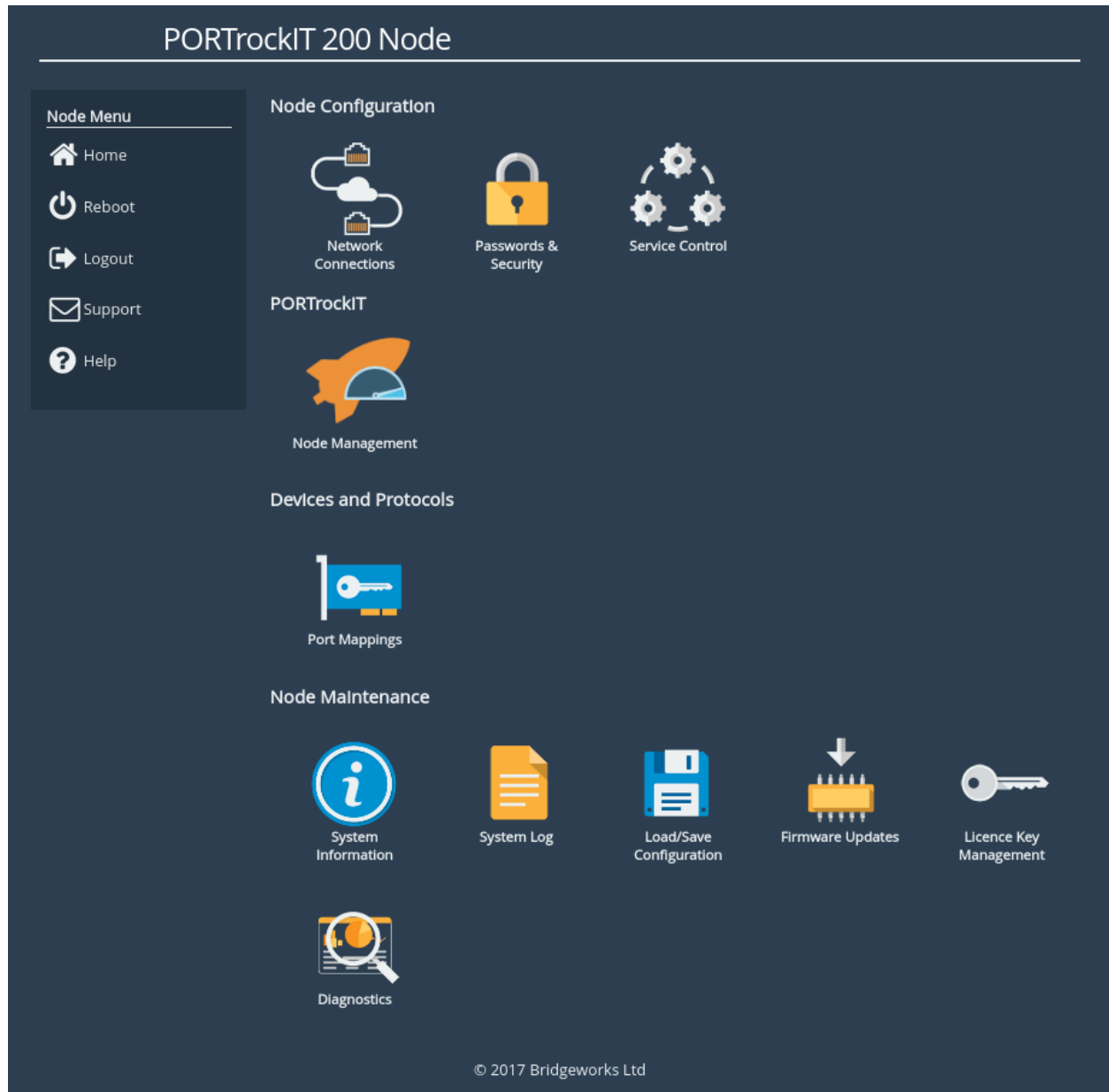


If you want to return to this screen without rebooting, you can do so with Alt+F1.

Once your port is set up correctly, you should be able to access the Node via a web browser as described in Section [2.2: Connecting to the Web Interface](#).

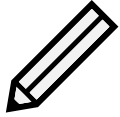
2.5 Management Console (Home screen)

The web interface will now display the Console Home screen as shown below:



Note: The web interface may have different icons to the ones shown above depending on the configuration you have purchased.

The web interface is split into two sections. The left hand *Node Menu* panel typically remains constant wherever you are within the web interface. It allows you to reboot or logout of the web interface. The Home link may be used from any page to return to the Home screen.



Note: Whenever a Reboot command is issued, it may take several minutes for the Node to become accessible again.

The Support link will open up a new tab in your browser at the Bridgeworks website support page.

The Help will provide you with information relevant to the display and configuration data.



Note: To quickly get started with the setup of your PORTrockIT, we recommend referring to the Chapter 4: [PORTrockIT Configuration](#) section. This section provides comprehensive instructions on how to properly configure your machine.

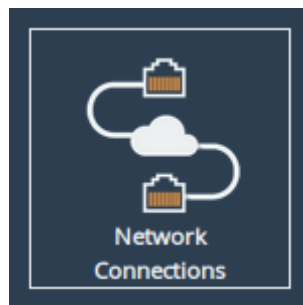
3 Node Configuration Reference

This section details the configuration of the Node's basic network and service settings.

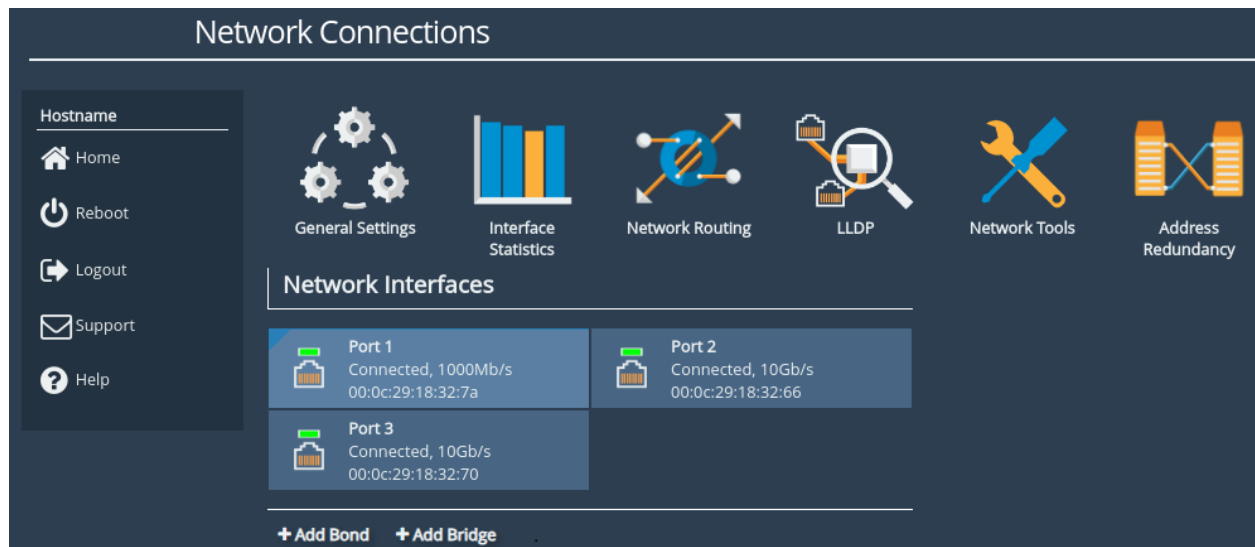
3.1 Network Connections

This configuration page allows the administrator to configure network interface settings and view network statistics.

From the Home screen, select the *Network Connections* icon under the *Node Configuration* section.



The web interface will display a screen similar to the following (Not all options are available on some products):



Options at the top of the page allow you to access various network settings and tools. More information for these options can be found in the following sections:

- Section [3.1.3: General Settings](#)
- Section [3.1.4: Interface Statistics](#)
- Section [3.1.5: Network Routing](#)
- Section [3.1.6: LLDP](#)
- Section [3.1.7: Network Tools](#)

3.1.1 Network Interfaces

This section displays each network port present on the Node, along with its current status/link speed, and hardware identifier (MAC address).

Clicking on a particular interface will navigate to a bespoke configuration page for that particular interface. More information on the different interface settings is available in [Section 3.1.8: Port Settings](#).

3.1.2 Add Bond

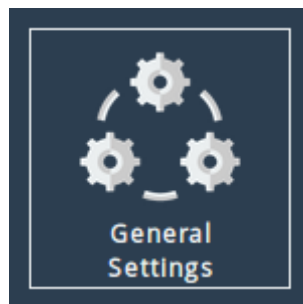
This button will add a new network *Bond* to the system (also known as Link Aggregation/Bundling, Port Trunking, or NIC Teaming). This allows two or more *Network Interfaces* to be combined together, providing potential load balancing as well as greater levels of fault tolerance.

Once a new *Bond* has been created, click on it to access its settings and add the desired interfaces. More information on *Bond* settings is available in [Section 3.1.8: Port Settings](#).

3.1.3 General Settings

This configuration page allows the administrator to configure general network settings for the Node.

From the *Network Connections* page, select the *General Settings* icon.



When selected, you will be presented with the following screen.

3.1.3.1 Hostname

In the *Hostname* field, enter the name you wish to use to address this Node. It is a good idea to make the name relevant to the Node's location and/or purpose.

You can then access the web interface from this hostname in future, from any DHCP-enabled management interface.

3.1.3.2 Hostname on login page

Selecting the *Hostname on login page* checkbox enables the display of the system hostname, and if available the DHCP domain name on the login page. This may be useful to identify which device you are logging in to.

3.1.3.3 DNS Servers

Setting a DNS server enables the use of DNS names when configuring network services.

The *DNS Servers* field lists the DNS servers that are currently in use by the Node. If DHCP is enabled on an interface and returns DNS servers, then these will be displayed in the list, otherwise the *Fallback DNS Server* will be used.

3.1.3.4 Default Route

The *Default Route* is the interface that the Node will use to route packets when no specific interface has been specified.



Important: The selected interface must have a gateway configured for this to take effect.

In addition to being able to select a specific interface for the *Default Route* it is also possible to select the interface automatically with the *Auto* option. In this case, an interface which has both *Management* mapped to it and a default gateway configured will be set as the default route. This

operation is performed at startup only.

If the user requires no *Default Route* it is possible to set *None*. It should be noted that if a bond interface is assigned to be the default route and the bond is deleted, the default route will automatically be set to *None*. The factory default value for this setting is *Auto*.

3.1.3.5 Dead Gateway Detection

Selecting the *Enable Dead Gateway Detection* checkbox will allow the Node to detect dead gateways and remove network routes that specify those gateways. When the dead gateways are reachable again, the routes are restored. This provides a level of failover in the event that the gateways become unreachable.

Dead Gateway Detection Time Delay refers to the time in seconds between requests being sent to the gateway to see whether that gateway is still reachable.

Dead Gateway Detection Retry Count refers to the number of times an unreachable gateway will be contacted before being set as a dead gateway and removed.

The status of each gateway is displayed on the *Routing* page. The status of the gateways for an individual port are also shown on the *Port Settings* pages. Refer to Section [3.1.5: Network Routing](#) for information on viewing and modifying network routes. An icon next to each gateway indicates its state:



Live Gateway Represents a gateway that responds to ICMP echo



Dead Gateway Represents a gateway that no longer responds to ICMP echo requests; it is dead



Important: Dead gateway detection functions by sending periodic ICMP echo requests to each gateway. Please ensure that the gateways can respond to such requests; if they're blocked by a firewall, dead gateway detection will always consider the gateways to be dead.

Hostname

Home

Connections

Reboot

Logout

Support

Help

Default routes should not be added here

Routing Tables

VLAN:

None

Destination	Gateway		Interface	Metric	
0.0.0.0/0	10.10.10.1	✓	Port 1	1	🔒
10.10.0.0/16			Port 1	1	🔒
192.168.1.0/24			Port 2	1	
192.168.2.0/24	192.168.1.1	✗	Port 2	1	
192.168.2.0/24	192.168.1.100	✓	Port 2	2	

Delete route

Add Static Route

Interface:

Port 1

VLAN:

None

Destination:

192.168.2.0

Prefix:

/24

Gateway:

192.168.1.100

Metric:

2

Add route

In this example, dead gateway detection has been enabled and multiple redundant routes to 192.168.2.0/24 have been added with different gateways (192.168.1.1 and 192.168.1.100) and different metrics (1 and 2, respectively).

The gateway with the IP address of 192.168.1.1 isn't responding to ICMP echo requests, so it's deemed to be dead. The corresponding route has been removed, so any traffic to 192.168.2.0/24 will now go via 192.168.1.100 instead.

When the gateway with the IP address of 192.168.1.1 starts to respond to ICMP echo requests again, the icon next to it will change from the red cross to the green tick and its route will be restored. Any traffic to 192.168.2.0/24 will go via 192.168.1.1.

3.1.3.6 Enable IPv6

Selecting the *Enable IPv6* checkbox will enable the Node to use IPv6 addresses. As with IPv4, you can either choose automatic address assignment or assign a static IPv6 address.

3.1.3.7 Enable VLANs

When the *Enable VLANs* checkbox is selected, VLANs (IEEE 802.1Q) will be configurable for network interfaces on their respective port configuration page. Section [3.1.8: Port Settings](#)

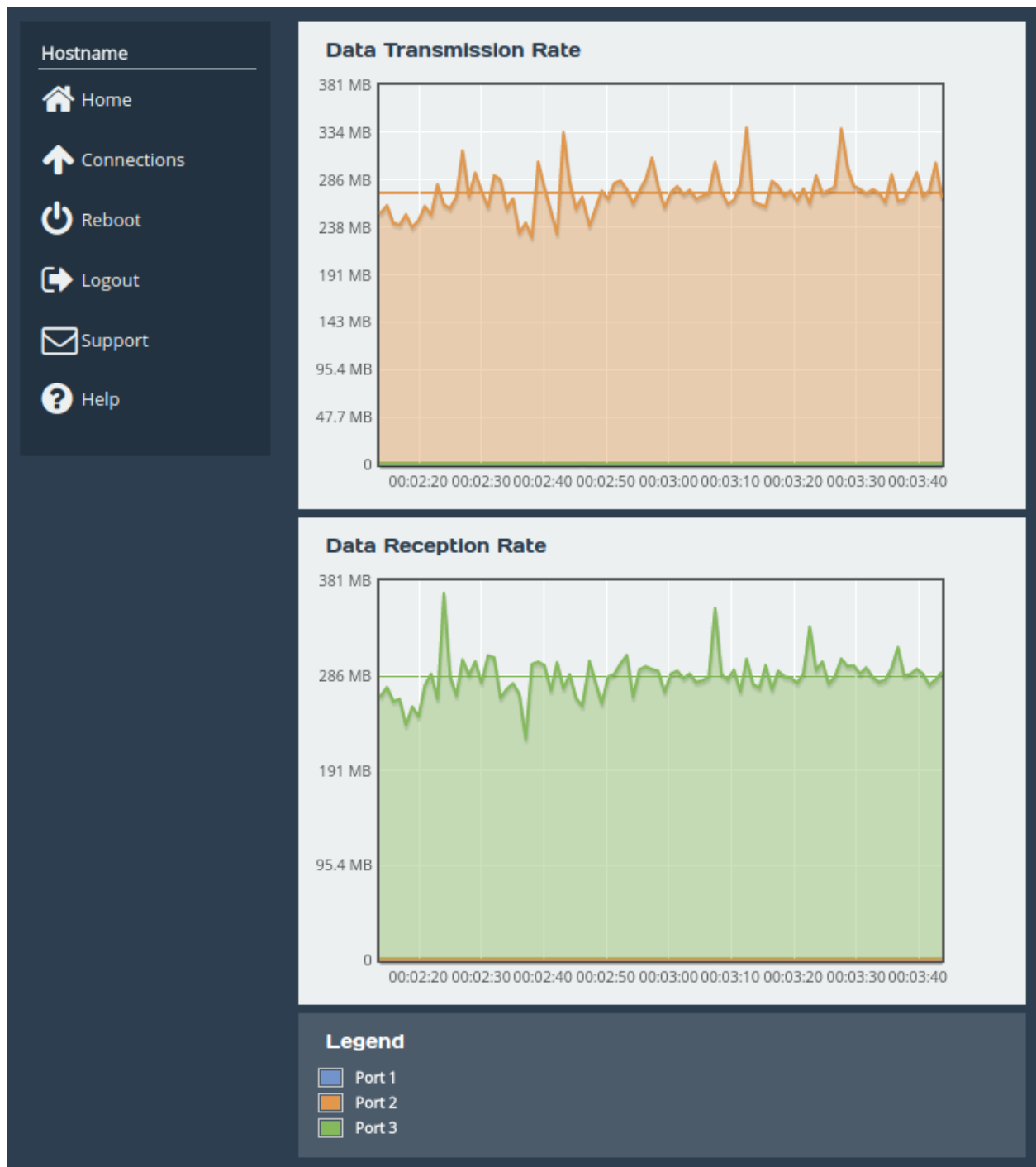
3.1.4 Interface Statistics

This page displays live network interface data rate statistics.

From the *Network Connections* page, select the *Interface Statistics* icon.



When selected, you will be presented with the following screen.



3.1.4.1 Data Transmission Rate

This section displays a graph, representing the data transmission rate for each network interface over the last 90 seconds. Each interface is displayed using a unique colour specified in the *Legend*. The average transmission rate over the last 90 seconds is displayed by a horizontal line for each interface.

3.1.4.2 Data Reception Rate

This section displays a graph, representing the data reception rate for each network interface over the last 90 seconds. Each interface is displayed using a unique colour specified in the *Legend*. The

average reception rate over the last 90 seconds is displayed by a horizontal line for each interface.

3.1.4.3 Legend

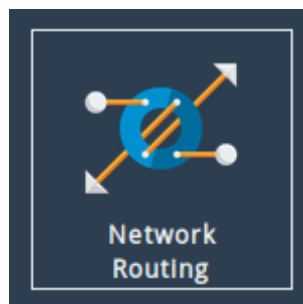
Each base network interface and each bond will be displayed using a unique colour for the data rate graphs. Each interfaces colour will be displayed alongside the ports name here.

Statistics for VLANs are included in the statistics for their parent interface.

3.1.5 Network Routing

This configuration page allows the user to view, add and remove network routes on the Node. Routes auto generated by the Node to support IP address and gateway configuration settings are read-only on this page. These are indicated by a padlock symbol against the route. User added routes may have a warning triangle shown after them indicating that the route is inactive. This occurs in situations where the configured route can't be applied due to conflicting configurations. Two likely causes of this are the gateway no longer being in the same subnet as the port, or the port having no valid IP address.

From the *Network Connections* page, select the *Network Routing* icon.



Routes are only displayed for the selected VLAN. Using the *VLAN* dropdown at the top of the page will change which VLAN is selected. This also affects which VLAN a route is added to using the *Add Static Route* form. To view and add routes without a VLAN select *None*.

Routing Tables		
VLAN:		None ▾
		None
Destination	Gateway	10
0.0.0.0/0	10.1	20
10.10.0.0/16		25
192.168.1.0/24		30
192.168.2.0/24		40
		50
		60

3.1.5.1 Add Static Route

To add a route, fill in the following fields and click on the *Add route* button:

Interface The network interface to which the route applies.

VLAN The VLAN on which the route applies. Selectable with the *VLAN* dropdown at the top of the page.

Destination The IP address component of the CIDR block to which the route applies, e.g. 192.168.5.0.

Prefix The prefix length component of the CIDR block to which the route applies, e.g. /24.

Gateway Route traffic via the gateway with this IP address. Optional.

Metric Metric (priority) of the route. Optional; defaults to 1.

Hostname

Home

Connections

Reboot

Logout

Support

Help

Default routes should not be added here

Routing Tables

VLAN:

None

Destination	Gateway	Interface	Metric	
0.0.0.0/0	10.10.10.1	Port 1	1	🔒
10.10.0.0/16		Port 1	1	🔒
192.168.1.0/24		Port 3	1	⚠️
192.168.2.0/24		Port 2	1	
192.168.4.0/24	192.168.2.3	Port 2	2	

Delete route

Add Static Route

Interface:

Port 2

VLAN:

None

Destination:

192.168.5.0

Prefix:

/24

Gateway:

192.168.2.4

Metric:

3

Add route

In this example, a route is being added to 192.168.5.0/24 via the gateway at 192.168.2.4 on Port 2. The route has a metric of 3.

To remove an existing route, click on the *Delete* button next to it.



Important: Routes created automatically by the system cannot be removed.

When dead gateway detection is enabled, each gateway in the table will have an icon next to it indicating its current status (live or dead). Refer to Section 3.1.3.5: [Dead Gateway Detection](#) for more information.

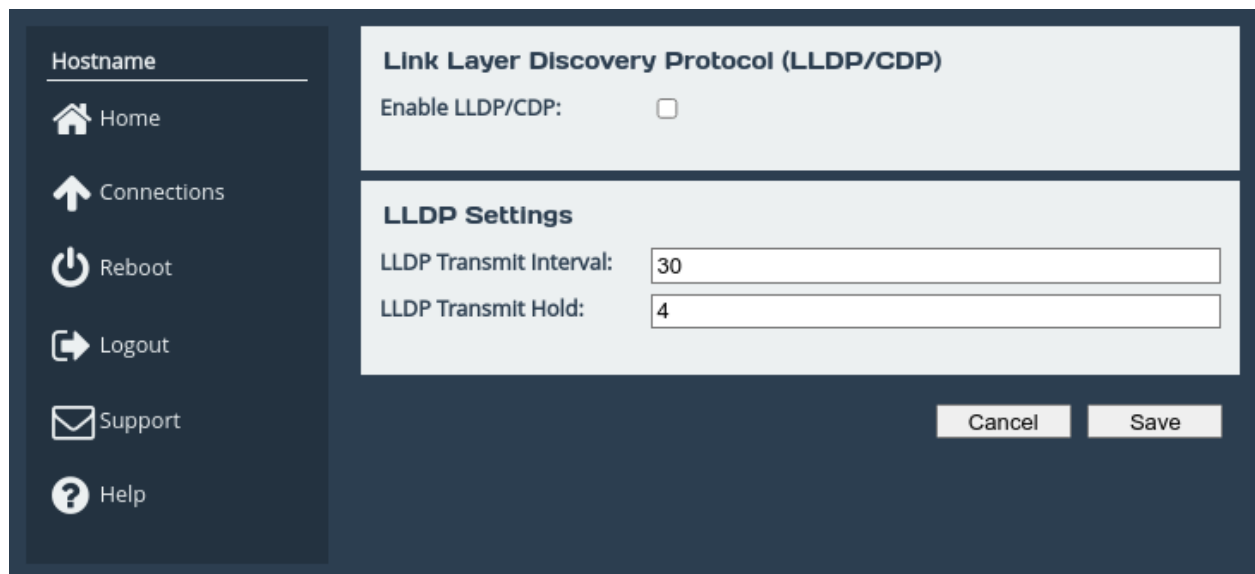
3.1.6 LLDP

This page allows an administrator to configure Link-Layer Discovery Protocol (LLDP) system settings. LLDP is a layer 2 protocol used for discovering and advertising a system's identity, capabilities, and neighbours.

From the *Network Connections* page, select the *LLDP* icon.



When selected, you will be presented with the following screen.

The screenshot shows a web interface with a dark blue sidebar on the left and a main content area on the right. The sidebar contains a 'Hostname' field and several menu items: 'Home' (house icon), 'Connections' (upward arrow icon), 'Reboot' (power icon), 'Logout' (logout icon), 'Support' (envelope icon), and 'Help' (question mark icon). The main content area has a title 'Link Layer Discovery Protocol (LLDP/CDP)' and a checkbox labeled 'Enable LLDP/CDP:'. Below this is a section titled 'LLDP Settings' containing two input fields: 'LLDP Transmit Interval:' with the value '30' and 'LLDP Transmit Hold:' with the value '4'. At the bottom right of the main content area are two buttons: 'Cancel' and 'Save'.

Checking the *Enable LLDP/CDP* checkbox will enable LLDP on all ports and show the LLDP Chassis Status section.

Hostname

Home

Connections

Reboot

Logout

Support

Help

LLDP Chassis Status

Name: Hostname
Description: PORTrockIT Hostname Eli.v6.05.297 (Nov 22 2024 06:29:41)
Chassis ID: mac 00:0c:29:e3:cb:e8
Capabilities: Router

Link Layer Discovery Protocol (LLDP/CDP)

Enable LLDP/CDP: ☒

LLDP Settings

LLDP Transmit Interval:
LLDP Transmit Hold:

Cancel

Save

LLDP Chassis Status The LLDP Chassis Status section displays the chassis information to be advertised to neighbours. This includes the system's name, description, chassis ID, and capabilities. These will be automatically created and updated by the Node when LLDP is enabled.

Enable LLDP/CDP When the *Enable LLDP/CDP* checkbox is selected, LLDP will be enabled and by default all ports will start to advertise device information from the Node whilst also discovering neighbouring device information. To view discovered neighbour information, navigate to any port on the *Network Connections* page.

3.1.6.1 LLDP Settings

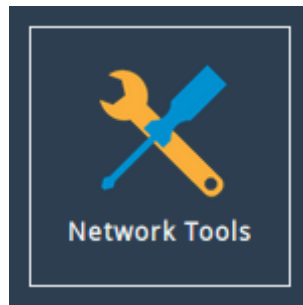
LLDP Transmit Interval The transmit interval is the time in seconds between LLDP packet transmissions. The total time-to-live (TTL) for LLDPDU's are the product of the transmit interval and transmit hold. Default is 30.

LLDP Transmit Hold The transmit hold is a multiplier for transmit interval used to determine the total TTL.

3.1.7 Network Tools

The PORTrockIT product provides some network tools that can be used for verifying network connectivity and behaviour between the Node and network hosts.

From the *Network Connections* page, select the *Network Tools* icon.



This opens the network tools page, this is a tabbed interface where you may select from the available tools.

3.1.7.1 Ping

The screenshot shows a web interface with a dark blue sidebar on the left and a main content area. The sidebar contains a "Hostname" header and several menu items: "Home" (house icon), "Connections" (upward arrow icon), "Reboot" (power icon), "Logout" (right arrow icon), "Support" (envelope icon), and "Help" (question mark icon). The main content area has two tabs: "Ping" (active) and "Traceroute". The "Ping" tab contains a form with the following fields: "Host:" (text input), "Payload Size:" (text input), "Count:" (text input with "5" entered), "VLAN:" (dropdown menu with "None" selected), and "Network Interface:" (dropdown menu with "Default selection" selected). A "Ping" button is located at the bottom right of the form. Below the form is a section titled "Ping Output" which contains a large, empty rectangular box for displaying results.

Ping can be used to verify the connectivity between the Node and a network host.

To test connectivity, fill in the following fields and click on the *Ping* button:

Host The IP address of the network host.

Payload Size The ping payload size. Leave blank to default to 56 bytes.

Count The number of ping attempts that you wish the Node to perform. Setting the count to 0 will send pings indefinitely, until the page is navigated away from, or another ping/traceroute operation is initiated.

VLAN The VLAN that the ping will be sent on. Changing this option will filter the interfaces in the *Network Interface* option.

Network Interface The interface that you want to ping from. If you are checking the routing on the unit, leave this option set to

Default selection. Only interfaces with the selected VLAN will be displayed.

On a successful ping, the *Output* box will fill with text similar to that below.

```
PING Address (Address): 56 data bytes
64 bytes from Address: seq=0 ttl=64 time=0.600 ms
64 bytes from Address: seq=1 ttl=64 time=0.129 ms
64 bytes from Address: seq=2 ttl=64 time=0.096 ms
64 bytes from Address: seq=3 ttl=64 time=0.143 ms
64 bytes from Address: seq=4 ttl=64 time=0.094 ms

--- Address ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.094/0.212/0.600 ms
```



Note: *Address* is replaced with the IP address that you entered.

3.1.7.2 Traceroute

Hostname

Home

Connections

Reboot

Logout

Support

Help

Ping

Traceroute

Traceroute Protocol:

UDP

Host:

Packet Size:

Destination Port:

Set Don't Fragment Bit:

☐

VLAN:

None

Network Interface:

Default selection

Traceroute

Traceroute Output

Traceroute can be used to determine the route packets take from the Node to a network host.

To test the routing, fill in the following fields and click on the *Traceroute* button:

Traceroute Protocol The type of protocol you wish to use: UDP, ICMP or TCP. UDP is the default option, ICMP can be used if firewalls block UDP datagrams. TCP is useful for testing access lists and firewall protocol rules.

Host The IP address of the network host.

Packet Size The traceroute payload size. Leave blank to default to 46 bytes for IPv4 or 72 bytes for IPv6.

Destination Port The destination port can be selected. This may be useful, alongside TCP probes, when testing policy based routing; or for testing specific ports, especially Dynamic Ports (also known as Private or Ephemeral Ports). It is disabled when using ICMP.

Set Don't Fragment Bit Select to set the don't fragment (DF) bit on the traceroute packets. This can be used to diagnose MTU issues on your network.

VLAN The VLAN that the traceroute will be sent on. Changing this option will filter the interfaces in the *Network Interface* option.

Network Interface The interface that traceroute packets will be sent from. Leave as *Default selection* for the interface to be selected according to the routing table.

Only interfaces with the selected VLAN will be displayed.

The result from traceroute will appear in the *Output* box.

3.1.8 Port Settings

Clicking on an interface will navigate to a bespoke settings page for that particular interface. Depending on the type of interface that was selected and the current options that are enabled, different settings will be presented.

Hostname

Home

Connections

Reboot

Logout

Support

Help

Link Status

Link State: Up

Link Speed: 10Gb/s

RX Bytes: 272846

TX Bytes: 753281

RX Errors: 0

TX Errors: 0

Settings

IPv4 Address: 10.10.10.95 /16

MTU: 1500 (user config) Max: 9000

Gateway: Global default via 10.10.10.1

Mapped Protocols

Management

This management interface is currently in use

Port Settings

Enable Port: ☒

MTU Size:

☒ Use DHCP to assign an IP address automatically

☒ Register this system's hostname on this interface
 ☒ Override configured MTU when supplied by DHCP

☐ Use the following IP address:

IP Address:

Netmask:

Gateway:

Cancel

Save

When dead gateway detection is enabled, each gateway on the port will have an icon next to it indicating its current status (live or dead). Refer to Section 3.1.3.5: [Dead Gateway Detection](#) for more information.

The following is a list of all possible interface types, and the settings available for each.

	Linked Interfaces	Enable Port	MTU	Enable Forwarding	STP Bridge Configuration*	STP Port Configuration*	LLDP Settings*	IPv4	IPv6	VLANs*	Bonding Options
Basic Interface		✓	✓	✓			✓	✓	✓	✓	
Bridged Interface (master)	✓	✓	✓		✓			✓	✓	✓	
Bridged Interface (slave)		✓				✓	✓				
Bond Interface (master)	✓		✓	✓				✓	✓	✓	✓
Bonded Interface (slave)		✓					✓				
VLAN Interface			✓	✓				✓	✓		



Important: STP Bridge Configuration will only be displayed if the interface is the bridge master of a bridge with STP enabled.



Important: STP Port Configuration will only be displayed if the interface is a bridge slave that is part of a bridge with STP enabled.



Important: LLDP Settings will only be displayed if LLDP/CDP is enabled from the LLDP page.



Important: IPv6 Options will only be displayed if IPv6 has been enabled (see Section 3.1.3: [General Settings](#)).



Important: VLANs will only be displayed if VLANs have been enabled (see Section 3.1.3: [General Settings](#)).

3.1.8.1 Linked Interfaces

Displays all Interfaces which are linked to make up a Bridge or Bond. Additional interfaces can be added by clicking the *Add Interface* button, or deleted by clicking the *X* button on a particular interface and then clicking *Delete*.

Changes to the *Linked Interfaces* will be queued until the page is saved. This includes both adding

and deleting of interfaces.



Important: Protocol mappings on a Bond are acquired by inheriting only the common mappings of the bonded interfaces.



Important: Protocol mappings on a Bridge are acquired by inheriting all of the mappings of the bridged interfaces.

3.1.8.2 Enable Port

An interface may be enabled or disabled by toggling this option.

3.1.8.3 Setting the MTU

The maximum transmission unit (MTU) may be adjusted from the default of 1500 bytes. Lower values are sometimes required for best performance with some types of network VPN equipment. However, it is recommended to leave this value unchanged, unless advised by documentation for any external VPN equipment used in conjunction with the Node.

Enabling larger frames on a jumbo frame-capable network can improve your network throughput. Jumbo frames are Ethernet frames that contain more than 1500 bytes of payload (MTU).

Before enabling jumbo frames, ensure that all the devices/hosts located on the network support the jumbo frame size that you intend to use to communicate with the Node. If you experience network-related problems while using jumbo frames, use a smaller jumbo frame size. Consult your networking equipment documentation for additional instructions.



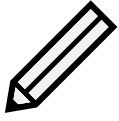
Important: Some networking switches require you to specify the size of the jumbo frame (MTU) when enabling, as opposed to a simple enable command. On these switches, it might be required to add the necessary bytes needed for the frame header to the MTU size you specify in the Node's port configuration. Typical header size is 28 bytes, so a 9000 byte MTU could translate to a 9028-byte total size. Refer to your switch documentation to understand what the maximum frame size settings are for your switch.

3.1.8.4 Enable Forwarding

Firewall rules exist to block any traffic that is not destined for the PORTrockIT. Enabling this option will remove the firewall rules, allowing traffic to freely pass through the interface.

By default this option is enabled on LAN interfaces, but disabled on WAN interfaces. This will allow accelerated traffic through, but will block any unaccelerated traffic from leaving the Node. If required traffic is passing through the Node that is not being accelerated, this option should be enabled on all relevant interfaces.

3.1.8.5 Bridged Physically-In-Path Mode

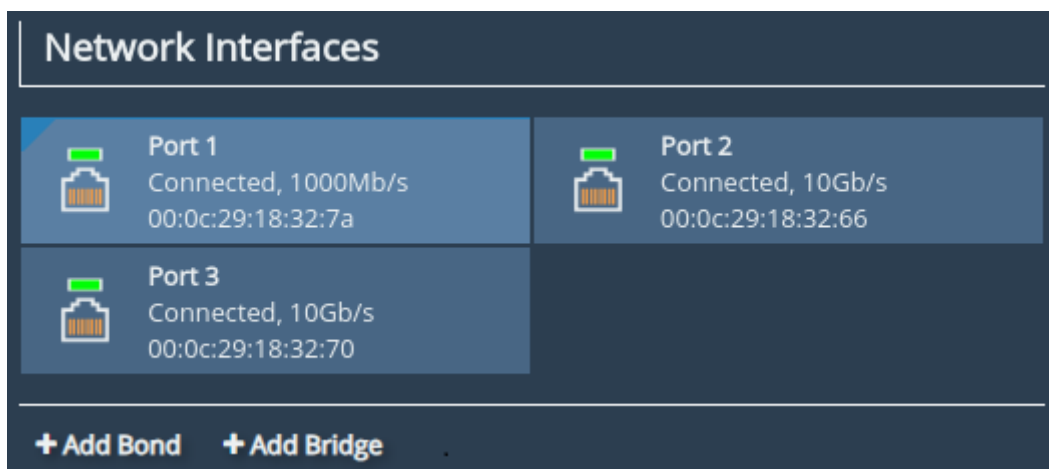


Note: You may skip reading this section if you wish to deploy your Node in the *Logical-In-Path* or *Out-of-Path* topologies.

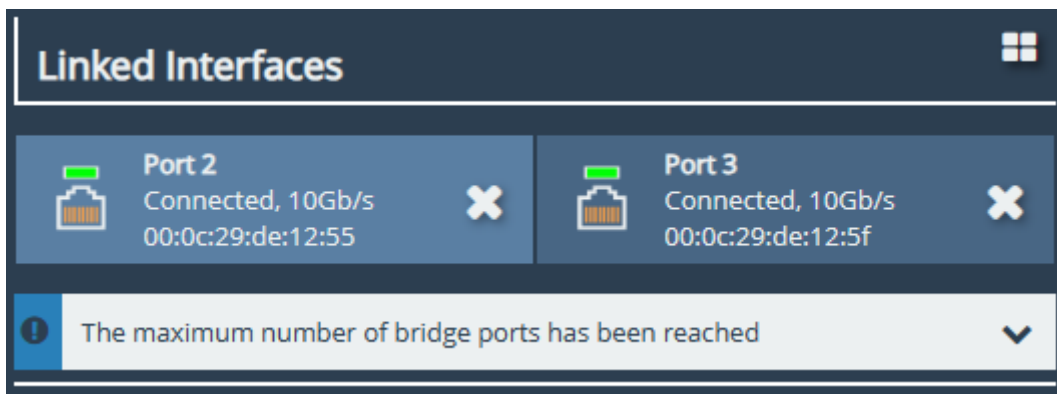


Important: Bridged Physically-In-Path Mode is unavailable on AWS, Azure and Hyper-V Nodes.

In order for the PORTrockIT acceleration to pass traffic through the network, a Bridge port must be created and two interfaces added to it.



The port that has a PORTrockIT protocol mapped to it (such as IBM Spectrum Protect or NetApp) must be added to the Bridge along with the WAN port used to establish the leading WAN link between the two units.



Please ensure these Nodes are not connected to the same Ethernet segment. To help protect against network issues, the PORTrockIT unit participates in STP (Spanning Tree Protocol) by default to ensure that network loops are not created. However this will prevent the PORTrockIT unit from operating as an acceleration device if it has to disable its bridging to protect the network.

In rare circumstances STP may need to be disabled. Clearing the *Enable Spanning Tree* checkbox on the Bridge will disable STP.

Once the changes are complete click **Save**. A reboot of the PORTrockIT Node will be required for the change to become active. This should be completed on both PORTrockIT Nodes before continuing.

3.1.8.6 Configuring Spanning Tree Parameters

In order to configure and fine-tune Spanning Trees, ensure that Spanning Tree Protocol (STP) is enabled and the unit has been rebooted.



Important: The current implementation of Spanning Trees available on this PORTrockIT unit is equivalent to the revision of STP introduced in IEEE 802.1D.

The following statistics will become visible on the Bridge port:


Spanning Tree Status			
Bridge ID:	32768-00:0c:29:de:12:73	Hello Time:	2
Root Bridge:	32768-00:0c:29:de:12:73	Max Age:	20
Root Port:	None	Forward Delay:	15

Root Bridge The bridge or switch with the lowest bridge priority in the network. In the case where there are 2 bridges with the same priority, the MAC address is used as the tie-breaker to determine the root bridge.

Root Port The port which has the lowest cost path pointing to the root bridge. If the bridge is the root bridge, then there will be no local root port, and this section will display "none".

Spanning Tree Bridge Settings

Bridge Priority:

 The following Spanning Tree timers will only take effect if the bridge being configured is the root bridge of the network.

Forward Delay:

Hello Time:

Max Age:

Bridge Priority The bridge with the lowest bridge priority in the network will become the root bridge. The bridge priority must be a value between 0 and 61440 in increments of 4096. We do not recommend making the PORTrockIT the root bridge, as any changes which require a reboot will re-elect the next lowest priority bridge as the root bridge, and, as a result of STP convergence, may cause network instability for upwards of 30 seconds.

Forward Delay The forward delay defines the time in seconds which ports belonging to this STP instance will spend in a listening and learning state. This must be a value between 2 and 30.

The forward delay will only take effect if the bridge being configured is the root bridge of the network.

Hello Time The hello time determines the interval in seconds where a BPDU is forwarded from the bridge. This must be a value between 1 and 10. The hello time will only take effect if the bridge being configured is the root bridge of the network.

Max Age The max age determines the maximum amount of time in seconds before the bridge saves its configuration BPDU information. This must be a value between 6 and 40. The max age will only take effect if the bridge being configured is the root bridge of the network.



Important: Altering STP timers from the default values could negatively impact network performance.

Similarly the following statistics will become visible on each of the slave ports:

Spanning Tree Status			
State:	Forwarding	Cost:	20
Priority:	20		

State The current STP specific state of a port. The following states are possible.

- *Blocking* This state will occur during root port elections, and also after the election if the port is not a root port, or a designated port. The port will not forward frames, and will discard received frames.
- *Listening* This state will occur on root ports and designated ports after the blocking state. During this state, received bridge protocol data units (BPDU) are accepted by the port, but any other received frames are discarded. The port will also start to process user frames and update the MAC address table.
- *Learning* This state will occur after being in a listening state for 15 seconds. For the duration of this state, the port is listening for, and processing BPDUs. After 15 seconds have passed, the port will switch to a forwarding state.
- *Forwarding* This state will occur after the learning state has finished. Ports in a forwarding state will forward frames, process BPDUs, and update their MAC address table. This is the normal operational state.
- *Disabled* This state will only occur if the port is administratively down and will not forward or receive any frames.

Spanning Tree Port Settings	
Port Priority:	<input type="text" value="20"/>
Port Cost:	<input type="text" value="20"/>


Port Priority The port priority is the final choice STP will use as a tie-breaker in the root port elections to decide which port becomes root. Changing the port priority will affect the *neighbouring* port and not the local interface; the interface with the lowest port priority will cause the neighbouring interface to become the root port. This must be a value between 0 and 31.

Port Cost The port cost is the first choice STP uses as a tie-breaker on a non root bridge device during root port elections to decide which port becomes root. A local interface with the lowest cost will become the root port for the bridge. This must be a value between 1 and 65535. Generally setting the local interface with the largest bandwidth path to the root port as the lowest costing interface is best practice.

Once the changes are complete click **Save**. This will not require a reboot.

3.1.8.7 LLDP Port Settings

To configure LLDP settings on ports, first ensure that LLDP has been enabled from the LLDP page.



Important: The different LLDP protocols compatible with your Node are LLDP and CDP (Cisco Discovery Protocol.)

After enabling LLDP, the following statistics and configuration boxes will become visible.

LLDP Neighbours
System Name: Hostname
System Description: PORTrockIT Hostname Eli.v6.05.297 (Nov 22 2024 06:29:41)
Management IP: 10.10.10.10
System Capabilities: Router
Ports: port3

LLDP Statistics

LLDPDU's Transmitted:	34	LLDPDU's Received:	33
------------------------------	----	---------------------------	----

3.1.8.8 LLDP Neighbours

System Name The system name of the neighbour device.

System Description The description set for the neighbour device. This will usually contain information such as: kernel name, node name, kernel version, build date, architecture. Your Node will advertise a combination of product name, host name, firmware version.

Management IP The management IP address of the neighbour device.

System Capabilities A list of capabilities the neighbouring device has enabled. This can be any of the following: Bridge, Router, Station, Telephone, WLAN Access Point, Repeater, DOCSIS Cable Device, Other.

Ports A list of port descriptions from the connecting ports on the neighbouring device.

3.1.8.9 LLDP Statistics

LLDPDU's Transmitted Total LLDPDU's sent from this port.

LLDPDU's Received Total LLDPDU's received from this port.

3.1.8.10 LLDP Settings



LLDP Mode Set the operation of LLDP on this port. The following options are available.

- *Disabled* LLDP will not run on this port, and therefore will not send or receive LLDPDU's. This option is useful if you want the port to remain anonymous to neighbouring machines using LLDP.
- *Only Listen* This port will receive LLDPDU's, however will not forward any. Use this if you want the port to remain anonymous to neighbouring machines whilst retaining the ability to view LLDP data from neighbours.
- *Only advertise* This port will send LLDPDU's, however will not receive any. Use this if you want the port to only advertise itself to neighbouring machines.
- *Advertise and Listen* This port will send and receive LLDPDU's, which will both allow the discovery of neighbouring machines and the advertisement of itself to neighbouring ports. This is the default setting.

Port Description Set a custom alphanumeric string to advertise from this port.

3.1.8.11 Setting the IP Address

There are two possibilities when configuring the IP address of a network port:

DHCP The Node will seek out your network's DHCP server and obtain an IP address for this port each time it boots.

If the server is not found, this port will fall back to its saved static IP settings.

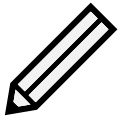
When DHCP is selected, the option to register the system's hostname with DNS is made available, this is enabled by default on management interfaces. Additionally, the option to override the configured MTU becomes available. When this option is applied and DHCP supplies the MTU, this will show as (DHCP) rather than (user config).

Static IP The IP address, netmask and gateway set in the corresponding fields will be used for this port.

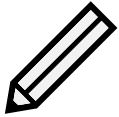
The gateway field may be left blank.

The IPv4 netmask field must be specified in dot-decimal form, e.g. 255.255.255.0.

If IPv6 is enabled from the *Network Connections* page, you can choose to use automatic address assignment to assign an IPv6 address, or you can set a static IPv6 address.



Note: DHCP is enabled by default on management interfaces.



Note: If DHCP is enabled, we recommend that your DHCP server is set to automatically update the DNS server.

3.1.8.12 Bonding Options

The *Bonding Options* define the behaviour of a network Bond. Depending on the *Mode* selected, different options will be available. The following is a list of all modifiable options.

Aggregation Mode:

Specifies which bonding policy the bond will operate under.

- *'Balance Round Robin' (default)* - Packets will be sent out of each bonded interface in turn (Round-Robin). Has both fault tolerance and load balancing.
- *'Active Backup'* - Traffic will be sent out of only one of the bonded interfaces. If that interface goes down another active bonded interface is used. Has fault tolerance.
- *'Broadcast'* - Traffic will be sent out of all bonded interfaces simultaneously. Has fault tolerance.
- *'LACP (IEEE 802.3ad)'* - Bonded interfaces will be grouped in to link aggregation groups (LAGs) with other interfaces in the bond that share the same speed and duplex settings. Only one LAG is active at any time. Traffic will be sent out of bonded interfaces in the active LAG based on the result of an XOR function performed on the MAC address of each packet. Has both fault tolerance and load balancing.

For more information about the different network bonding modes please refer to the *Bonding Guide*.

LAG Selection (compatible Modes - LACP):

Specifies which logic to use when selecting the active 802.3ad LAG.

- *'Highest Bandwidth (Stable)' (default)* - The LAG with the largest bandwidth is selected. LAG re-selection happens when all interfaces in the LAG are down.
- *'Highest Bandwidth (Always)'* - The LAG with the largest bandwidth is selected. LAG re-selection happens when:
 - Interfaces are added or removed from the bond.
 - An interface changes LAG.
 - The state of any of the interfaces in the bond changes.

-
- The state of the bond changes to up.
 - *'Highest Port Count (Always)'* - The LAG with the most interfaces is selected. LAG re-selection happens when:
 - Interfaces are added or removed from the bond.
 - An interface changes LAG.
 - The state of any of the interfaces in the bond changes.
 - The state of the bond changes to up.

Down Delay (compatible Modes - All):

Specifies the time to wait when a link failure is detected on a bonded interface before treating the interface as disabled. Down delay is measured in milliseconds, and should be a multiple of 100. The default is set to 0.

MAC Sharing (compatible Modes - Active Backup):

Specifies what the MAC addresses of the bonded interfaces should be set to.

- *'All Interfaces Copy Bond'* (default) - All bonded interfaces share the MAC address of the first interface in the bond.
- *'Bond Copies Active Interface'* - All bonded interfaces will retain their normal MAC address. The bond will take the MAC address of the active interface.
- *'Active Interface Copies Bond'* - All bonded interfaces will retain their normal MAC address when in fail over mode (not active). When an interface becomes active it will take the MAC address of the bond. The bond will take the MAC address of the first interface in the bond.

LACP Keep Alive Frequency (compatible Modes - LACP):

Specifies how frequently to transmit Link Aggregation Control Protocol Data Unit (LACPDU) 'keep alive' packets.

- *Slow (default)* - Every 30 seconds.
- *Fast* - Every 1 second.

Minimum Active Interfaces (compatible Modes - LACP):

Specifies the number of bonded interfaces that must be up in at least one LAG before the bond is reported as up. The default is set to 0. It should be noted that 0 has the same affect as 1.

Packets Per Interface (compatible Modes - Balance Round Robin):

Specifies how many packets should be sent via a bonded interface before the next interface is used. When set to 0 a random interface will be selected for each packet. The default is set to 1. There is a minimum value of 0, and a maximum value of 65535.

Primary Interface Re-Selection (compatible Modes - Active Backup):

Specifies the logic to use when selecting the active interfaces when the primary interface comes back up. The primary interface is the first interface in the bond.

-
- *As Soon As Possible (default)* - The primary interface becomes active whenever it comes back online.
 - *Only If Better Than Current* - The primary interface becomes active if the speed and duplex is better than the currently active interface.
 - *When Current Goes Down* - The primary interface becomes active if the currently active interface goes down.

If no interfaces are active, the first interface to come back up is selected as the active interface.

Up Delay (compatible Modes - All):

Specifies the time to wait when a link recovery is detected on a bonded interface before treating the interface as enabled. Up delay is measured in milliseconds, and should be a multiple of 100. The default is set to 0.

IGMP Membership Reports (compatible Modes - Balance Round Robin/Active Backup):

Specifies how many IGMP membership reports are sent when the active bonded interface changes. Membership reports are sent with 200ms intervals. Specifying a value of 0 prevents any reports being sent when the active interface changes. The default is set to 1. There is a minimum value of 0, and a maximum value of 255.

Transmit Port Selection (compatible Modes - LACP):

Specifies the policy by which the system selects the transmit interface for any given packet. Please note, the reception interface for traffic is controlled by the upstream switch.

- *Hash of MAC addresses only* - Using layer 2 information only, this policy will place all traffic to a layer 2 adjacent peer on the same interface.
- *Hash of MAC and IP addresses* - Using a combination of layer 2 and layer 3 information, this policy will place all traffic to a single destination IP on the same interface.
- *Hash of IP address and port numbers* - Combining layer 3 and layer 4 information, this policy will place different streams on different interfaces, but may result in out of order delivery. Note, this method is not fully 802.3ad compliant and may not work with all switches.

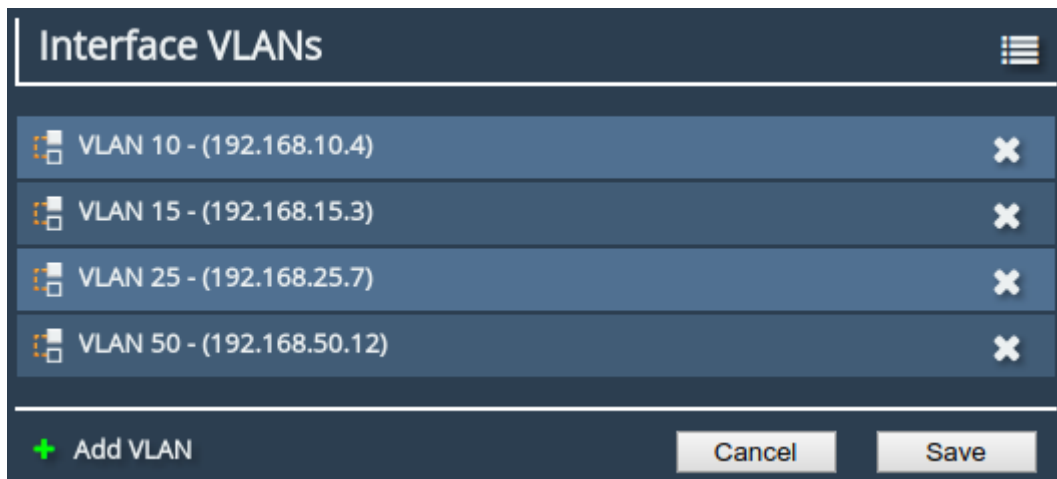
More information on these options can be found in the official Linux documentation:

<https://www.kernel.org/doc/Documentation/networking/bonding.txt>

3.1.8.13 Adding VLANs

If VLANs are enabled on the PORTrockIT they will be listed at the bottom of the port page. For each VLAN the ID and IP address are shown.

Refer to Section [3.1.3: General Settings](#) for information about enabling VLANs on the PORTrockIT.



VLANs can be added to an interface by pressing the *Add VLAN* button. When the button is pressed an *Add VLAN* dialogue will appear. A VLAN can be created with an ID between 1 and 4094. A maximum of 64 different VLANs can be added to the PORTrockIT. To queue the VLAN for addition, press the *OK* button. The VLAN will not be added to the interface until the changes are committed. If the *Cancel* button is pressed or the page is navigated away from, the VLAN will not be added.

VLANs can be deleted by pressing the *X* to the right of the VLAN and selecting the *Delete* button. The VLAN will not be removed from the interface until the changes are committed. If the *Cancel* button is pressed or the page is navigated away from, the VLAN will not be removed.

The configuration page for a VLAN can be accessed by selecting the VLAN in the VLANs list. From the VLANs configuration page the IP address settings can be changed. See Section [3.1.8.11: Setting the IP Address](#).

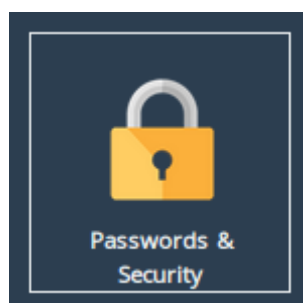
3.1.8.14 Committing the Changes

Click the *Save* button to save these parameters, then reboot the Node to apply them.

3.2 Passwords & Security

This configuration page allows the administrator to change the security settings of the Node.

From the Home screen, select the *Passwords & Security* icon under the *Node Configuration* section.



3.2.1 System Password

This section allows the administrator to change the access password for the web interface. The new password must be between 5 and 64 characters and should contain both symbols and numbers.



The 'System Password' form contains three input fields: 'Old Password:', 'New Password:', and 'Retype New Password:'. A 'Change Password' button is located at the bottom right of the form.

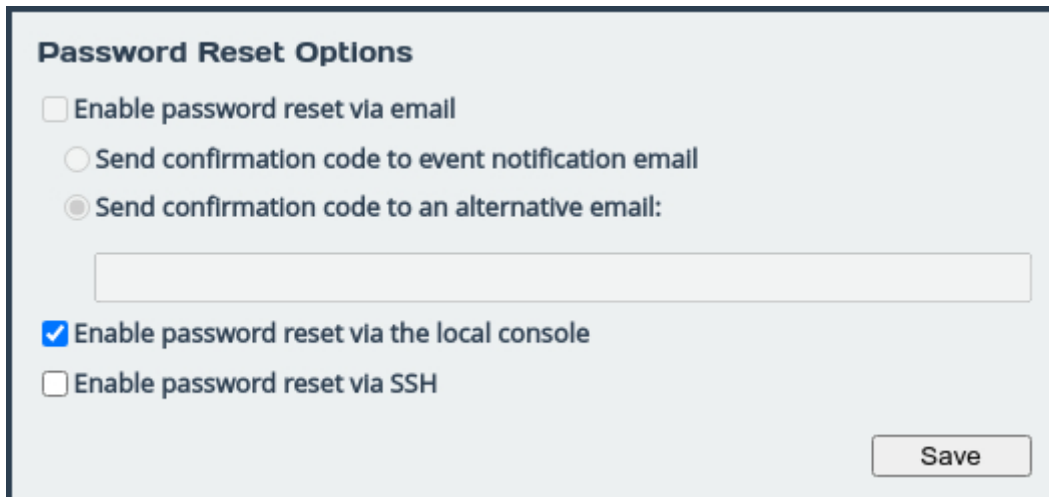


Important: The word “RESET” is reserved by the system and cannot be used as a password.

Enter the existing password into the *Old Password* field; then enter the desired new password into the two following fields. Then click *Change Password*.

3.2.2 Password Reset Options

This section allows the administrator to enable and disable different methods of password reset on the Node.



The 'Password Reset Options' form includes several settings: 'Enable password reset via email' (unchecked), 'Send confirmation code to event notification email' (radio button), 'Send confirmation code to an alternative email:' (radio button selected with an empty text field below it), 'Enable password reset via the local console' (checked), and 'Enable password reset via SSH' (unchecked). A 'Save' button is at the bottom right.

3.2.2.1 Password Reset via Email

3.2.2.1.1 Setup

This method of password reset allows a user that is authorised to access a pre-configured email address to reset the password of any user account on the Node.

When a user forgets their password, they will be able to click on the *Forgot your password?* link on the login page to reset their password.

To successfully reset your password using this method, a confirmation code will be sent to an email address previously configured in the web interface. This code will have to be obtained by the user and entered into the password reset wizard to complete the password reset procedure.



Important: Resetting a password will log out any current sessions under that user name.

To enable password reset via email, SMTP settings will have to be configured first to allow the Node to send emails. Navigate to the *Service Control* page and enter your SMTP settings under the *Simple Mail Transfer Protocol (SMTP)* section. Refer to Section 3.3.3: [Email](#) for information on SMTP configuration.

Next, navigate to the *Passwords & Security* page and tick the *Enable password reset via email* checkbox. You must then select whether you wish to have the confirmation code sent to the “event notification email” which is configured on the *Service Control* page, or to an alternative email which can be entered in the text box underneath.

Refer to Section 3.3.4: [Event Notification Email](#) for information on setting an event notification email. You will be required to enter an email address into the *alternative email* text box if an event notification email has not been set.

3.2.2.1.2 Using Password Reset via Email

To reset the password of a user account using the email method, navigate to the login page of the Node you wish to reset the password for. If password reset via email is enabled, there will be a “Forgot your password?” link underneath the login button as shown:

The screenshot shows a login form with two input fields: 'Username:' and 'Password:'. Below these fields is a horizontal line, followed by a 'Login' button. Underneath the 'Login' button is a link that says 'Forgot your password?'.



Important: If the “Forgot your password?” link is not present, then password reset via email has not been enabled on the Node.

Enter the username you wish to reset the password for and complete the captcha challenge by entering the characters in the image into the *Answer* text box. Then click *Next* to continue.

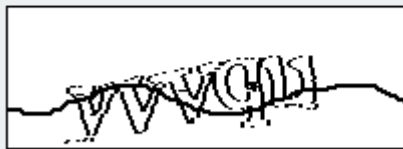
Reset Your Password

This wizard will guide you in resetting your password.

Please note that to verify that you are an authorized user of this node, an email containing a confirmation code will be sent to the system administrator. You will be required to obtain this confirmation code from the system administrator before you are able to reset your password.

To begin the password reset process, please enter your username and enter the characters shown in the image into the "Answer" field.

Username:



Answer:

Cancel

Next



Important: You can try a different captcha challenge by refreshing the web page.

An email containing a confirmation code will be sent to the email address set in the *Passwords & Security* page. Enter the confirmation code sent in the email to the *Confirmation Code* text box.

Enter your new password into the *New Password* and *Confirm Password* text fields and press the *Next* button.

Reset Your Password

An email containing a 16-digit confirmation code has been sent to the system administrator of this Node.

Enter the confirmation code and your new password below. Please note that you will not be able to reset your password if the confirmation code is incorrect.

Confirmation Code:

New Password:

Confirm Password:

If password reset was successful, a message will be displayed and you will be able to log in with your new password.


Password reset was successful.
Please login with your new password.

Username:

Password:

[Forgot your password?](#)

3.2.2.2 Password Reset via Local Console or SSH

	<p>Important: Password reset via local console is unavailable on AWS or Azure Nodes due to the absence of a real console.</p>
---	---

3.2.2.2.1 Setup

These methods of password reset allow any user that either has access to the local console or remote access via SSH to reset the password of any user account on the Node.



Warning: These methods of password reset should be disabled if unauthorised users may either have access to the local console or remote access via SSH.



Important: Resetting a password will log out any current sessions under that user name.

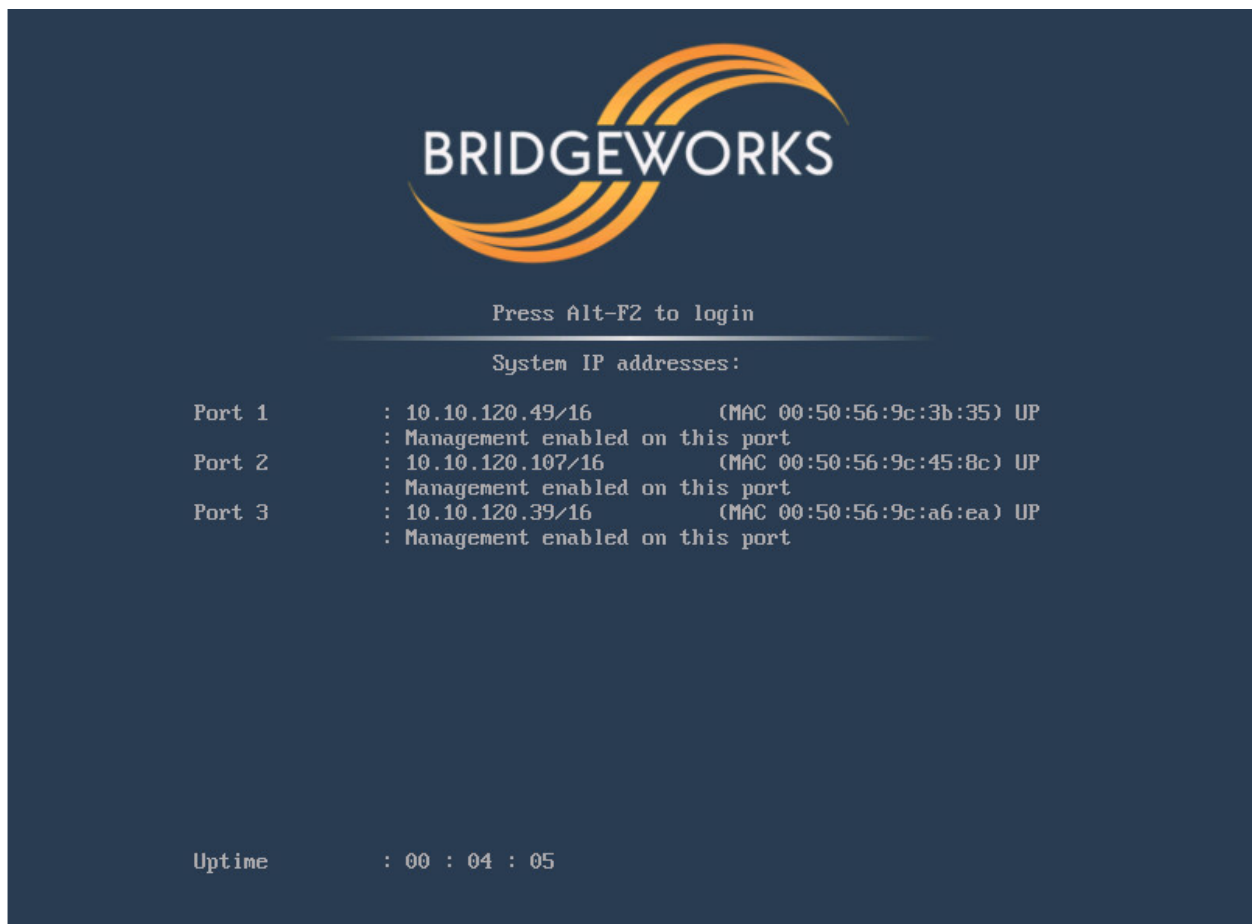
To enable password reset via local console, tick the *Enable password reset via the local console* checkbox or to enable via SSH, tick the *Enable password reset via SSH* checkbox. Then click Save.



Important: Password reset via local console is enabled by default.

3.2.2.2.2 Using Password Reset via Local Console or SSH

To reset the password of a user account using the local console method, connect a keyboard and monitor to the Node. You will see the following screen:



Press the “Alt” and “F2” keys at the same time to get access to the login prompt as shown:

```
Bridgeworks Management Interface
Username: _
```

To reset the password of a user account using the SSH method, connect to the Node via SSH to access the login prompt.

Enter the username you wish to reset the password for, such as “admin”. Then enter the password as “RESET”. Both the username and password are case-sensitive.

You will then be asked whether you wish to continue resetting the password. Press the “y” key then press the “Enter” key. Entering any other key will abort the password reset process.

```
Bridgeworks Management Interface
Username: admin
Password:
Are you sure you want to reset your password? y/n
_
```

Next, enter the new password you wish to set for the user selected. You will then be asked to enter the password again.



Important: If the two passwords do not match, or you are attempting to set the password as “RESET”, then password reset will fail.

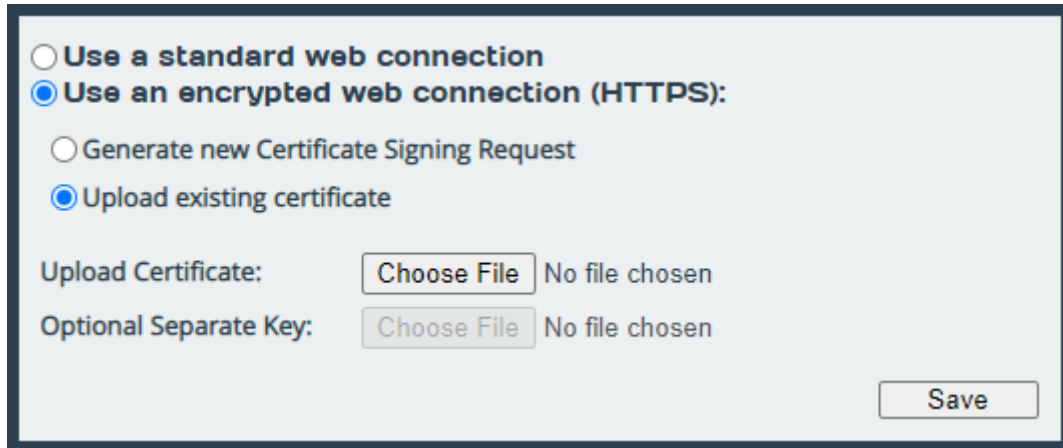
If your new password is accepted, the “Password set successfully” message will appear as shown:

```
Password set successfully
Bridgeworks Management Interface
Username: _
```

You will now be able to log into the web interface using your username and new password.

3.2.3 Secure Connection

To enable HTTPS, select the *Use an encrypted web connection (HTTPS)* radio button, then *Upload existing certificate*, and click Save.



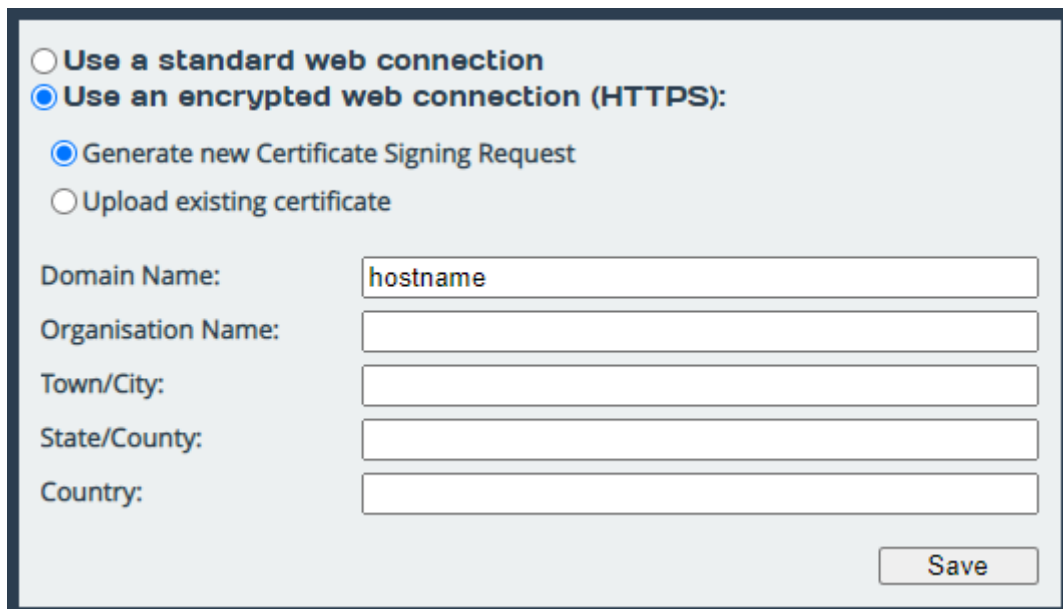
The screenshot shows a web interface for configuring a secure connection. At the top, there are two radio buttons: 'Use a standard web connection' (unselected) and 'Use an encrypted web connection (HTTPS):' (selected). Below the selected option, there are two more radio buttons: 'Generate new Certificate Signing Request' (unselected) and 'Upload existing certificate' (selected). Under 'Upload existing certificate', there are two rows. The first row is 'Upload Certificate:' with a 'Choose File' button and the text 'No file chosen'. The second row is 'Optional Separate Key:' with a 'Choose File' button and the text 'No file chosen'. At the bottom right, there is a 'Save' button.

If you simply click Save without uploading any files for the certificate or key, a self-signed certificate will be automatically generated by the Node.

Alternatively, You can use your own certificate & key pair by selecting files to upload with the file-picker buttons. You may upload the key pair as two separate files, or one combined file.

You will be logged out of the Node's web interface, and further transactions with the web interface will use SSL/TLS encryption.

3.2.3.1 Generate new Certificate Signing Request



The screenshot shows the same web interface as before, but with the 'Generate new Certificate Signing Request' radio button selected under the 'Use an encrypted web connection (HTTPS):' option. Below this, there are five text input fields with labels: 'Domain Name:' (containing 'hostname'), 'Organisation Name:', 'Town/City:', 'State/County:', and 'Country:'. At the bottom right, there is a 'Save' button.

If you need a certificate signed by an external certificate authority, you may use the *Generate new Certificate Signing Request* option to do so. Select *Use an encrypted web connection (HTTPS)*, then *Generate new Certificate Signing Request* to open the form.

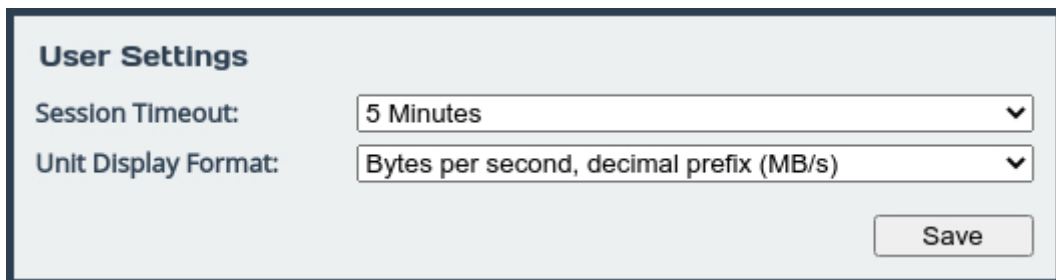
The fields which appear below this option when selected should be filled in with the details you want to appear on the certificate. The *Domain Name* field should be filled in with the IP address or fully qualified domain name which you use to access your Node. The following four fields should identify your company or organisation. Note that the *Country* field should contain a two-letter country code (ISO 3166-1 alpha-2), not a full country name.

Clicking *Save* will then download a CSR file. You should then send this file to your certificate authority, who should send you back a signed certificate file.

You can then upload this signed certificate file to the Node, using the *Upload existing certificate* option, leaving the *Optional Separate Key* field empty.

3.2.4 User Settings

Settings in this section allow you to change parameters for the user interface.



The screenshot shows a 'User Settings' panel. It contains two configuration options, each with a dropdown menu. The first option is 'Session Timeout', which is currently set to '5 Minutes'. The second option is 'Unit Display Format', which is currently set to 'Bytes per second, decimal prefix (MB/s)'. A 'Save' button is positioned at the bottom right of the settings panel.

3.2.4.1 Session Timeout

After not interacting with the interface for a certain period of time, you will automatically be logged out. The Session Timeout setting allows you to adjust the length of time that must pass before you are logged out.

3.2.4.2 Unit Display Format

To allow a user to view system graphs in a unit that is applicable to their use case, the system may be switched to display in one of 6 different unit scales:

- Bits per second, decimal prefix (Mbit/s)
- Bytes per second, decimal prefix (MB/s)
- Bits per second, binary prefix (Mibit/s)
- Bytes per second, binary prefix (MiB/s)
- Bytes per hour, decimal prefix (TB/h)
- Bytes per hour, binary prefix (TiB/h)

3.2.5 Secure Shell (SSH)

Secure Shell (SSH) is a protocol that allows for secure access to a Node's configuration console.

To enable SSH on network interfaces with the “Management” protocol mapped, tick the *Enable SSH* checkbox and click *Save*.

Note: At least one public key must be uploaded, as described below, before SSH can be enabled.

3.2.5.1 Managing Public Keys

To log on to a Node’s configuration console using SSH, a public key is required to be uploaded first. Users connecting to the Node without having uploaded the corresponding public key to the Node first will be refused access.

To upload a public key, click on the *Add Public Key* button. The *Add Public Key* dialog box will appear. Click on the *Browse* button to select a public key file.

Note: Only RSA keys in the OpenSSH or RFC4716 format are supported.

Click on the *Add* button to upload the selected public key file. The public key should then appear in

the *List of Public Keys*.

To delete a public key, click on the public key to delete in the *List of Public Keys* and then click on the *Remove Public Key* button.



Important: Open SSH connections will not be closed when a public key is removed, or if SSH is disabled. Only new SSH connections will be rejected.

3.2.5.2 Using SSH

To connect to a Node which has a management port with an IP address of 192.168.0.20 using the OpenSSH SSH client, use the command:

```
ssh admin@192.168.0.20
```

You will then be prompted for the username and password of the Node to log into the configuration console.

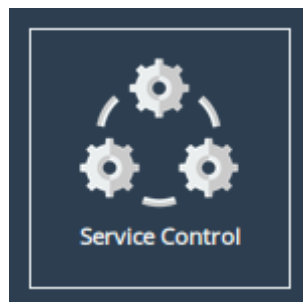
You will be denied entry to the configuration console if you have not uploaded a public key to the Node prior to connecting via SSH. A valid username and password for the Node are also required to log in using SSH.



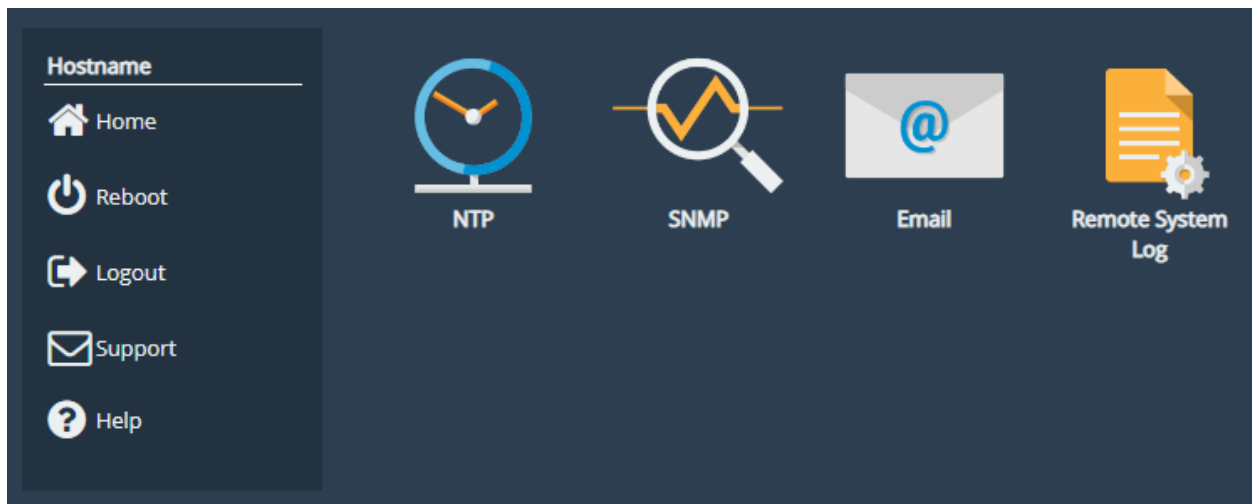
Important: Logging in as root user is disabled on SSH.

3.3 Service Control

This configuration page allows the administrator to configure network services for the Node. From the Home screen, select the *Service Control* icon under the *Node Configuration* section.



The web interface will display the following:



Each link leads to a different service.

The *NTP* (Network Time Protocol) page allows you to configure various settings available for NTP on the Node.

The *SNMP* (Simple Network Management Protocol) page allows you to configure various settings available for SNMP on the Node.

The *Email* page allows you to configure various settings available for Email alerts on the Node.

The *Remote System Log* page allows you to configure various settings available for remote logging on the Node.

3.3.1 Network Time Protocol (NTP)

SNTP Status

Current server: 62.149.2.7 (USER)

Last Receive: Jan 25, 2023 15:12:25 UTC

Server Priority List:

- 1 : USER 62.149.2.7
- 1 : USER 193.192.36.3
- 1 : USER 185.209.85.222
- 1 : USER 80.74.64.2
- 2 : DHCP 80.87.128.222 (port2)
- 2 : DHCP 80.87.128.222 (port4)
- 3 : DHCP 185.103.117.60 (port2)
- 3 : DHCP 185.103.117.60 (port4)

SNTP Settings

Enable SNTP: ☒

NTP Server:

Priority:

Time synchronization between the host machine and the guest VM is only enabled when NTP is disabled.

SNTP is a protocol for synchronising the clock of computer systems. This feature is critical if you are planning on using the scheduler or useful when viewing the logs to determine when an event occurred. Refer to Section 6.2: [System Log](#) for more information.

SNTP may be configured by specifying either a hostname or IP address in the *NTP Server* field, or alternatively this can be left blank and the NTP servers may be obtained via DHCP or DHCPv6. In the case that a hostname is specified a DNS lookup will be performed to obtain the addresses of the NTP servers.

Servers received from all sources are placed into a prioritised list which can be ordered based on the user preference as specified in the *Priority* field. For servers received via DHCP they will be prioritised using the same mechanism as used for selecting the DNS, that is to say ports with the default route or management on them will be higher priority. The order in which the server appears in the list supplied by DHCP is also taken into account. For user specified servers the request will automatically take the optimal route to the destination so is not associated with any particular port.

The *Enable SNTP* checkbox is used to enable/disable SNTP and clicking the *Save* button will save all the SNTP settings.

When SNTP is enabled the *SNTP Status* is displayed showing the following information:

-
- Current Server: The currently selected NTP server.
 - Last Receive: The last time a valid response was received.
 - Server Priority List: The ordered list of servers with highest priority at the top of the list. Each entry specifies if it is USER defined, or has been obtained via DHCP. In the case of DHCP provided servers it also shows which network port received the details from DHCP.

If the current server fails to provide a valid response after 5 attempts it will be deemed as failed and will have its priority temporarily lowered for a period of 10 minutes. If it becomes the highest priority server again and the first request is successful it will be considered fully functional again, if this request fails it will immediately be deemed failed again.

3.3.2 Simple Network Management Protocol (SNMP)

☐ **SNMP v2c Agent**
Community Name:
[Save](#)

☐ **SNMP v3 Agent**
Username:
Auth Type:
Auth Password:
Privacy Type:
Privacy Password:
[Save](#)

System Information
System Location:
System Contact:
[Save](#)

SNMP Trap Sinks

Address	Port	Version	Community/User
No SNMP trap sinks configured			

[Delete Sink](#) [Add Sink](#)

Download MIB Files
[Click Here to Download](#)

Two versions of SNMP are supported, 2c and 3. V3 is recommended as it has everything 2c has plus vastly superior security.

To enable SNMPv2c, check the box in the top left of the *SNMP v2c Agent* box, enter a *Community Name* and click *Save*.

To enable SNMPv3, check the box in the top left of the *SNMP v3 Agent* box, then enter a *Username*. Authentication verifies the sender of data while privacy protects the data. *SHA1* and *AES-128* are the superior and recommended hash function and encryption protocol respectively. Once done configuring the security settings, click *Save*.

3.3.2.1 System Information

The information configured here is accessible over SNMP.

System Location is the location of this Node. The value of this property should provide enough information for an administrator to locate this Node.

System Contact is the contact information for the person or department responsible for managing this Node. Click *Save* to save changes to System Information.

3.3.2.2 SNMP Trap Sinks

The Node notifies all configured *Trap Sinks* when a system event occurs. This means your SNMP manager can be notified should the Node encounter an error.

Click *More Info* link to view more information about a specific sink.

To add a new sink, click the *Add Sink* button to open the Add SNMP Trap Sink dialog.

3.3.2.3 Add SNMP Trap Sink

Address is the IP Address of the trap sink. Must be a valid IP address. Reserved and multicast addresses are not supported.

Port is the port of the trap sink.

Version is the version of SNMP the sink uses. It is recommended to use SNMPv3 where possible since it allows for authentication and privacy. The following versions are supported:

- v1: SNMPv1 (not recommended)
- v2c: SNMPv2c allows acknowledged traps
- v3: SNMPv3 allows privacy and authentication, making it more secure than SNMPv1 and SNMPv2c. (recommended)

Type is the type of notification sent to the trap sink. It is recommended to use the *Inform* notification type since it is acknowledged and therefore the notification is less likely to be unintentionally lost.

- Trap: Unacknowledged message
- Inform: Acknowledged message, not supported with SNMPv1

Community is the community string to use for the trap sink. Supported in SNMPv1 and SNMPv2c. Cannot contain spaces.

Username is the SNMPv3 unique identifier to associate these security details with. Must be 1-32 characters in length, and cannot contain spaces.

Engine ID is the SNMPv3 Engine ID of the trap sink. The Node should automatically discover the engine ID if this is left blank. If an Engine ID is provided, it must be 5-32 characters in length, and cannot contain spaces.

Authentication is the SNMPv3 authentication hash function used by the trap sink. Authentication allows only SNMP engines with the correct authentication password to connect to the trap sink. It is recommended to use authentication where available. It is not recommended to use the MD5 hash function since it suffers from vulnerabilities.

- SHA1: Uses the SHA1 hash function (recommended)
- MD5: Uses the MD5 hash function (not recommended)
- None: Authentication Disabled (not recommended)

Auth Password is the authentication password used to log in to the trap sink. An authentication password must be provided if *Authentication* is not set to *None*.

Privacy is the SNMPv3 privacy type used by the trap sink. *Authentication* must be enabled to use privacy. Privacy allows SNMP engines to communicate privately using encrypted messages. It is recommended to use privacy where available. It is not recommended to use the DES cipher function since it is cryptographically weak.

- AES-128: Uses the AES-128 cipher function (recommended)
- DES: Uses the DES cipher function (not recommended)
- None: Privacy Disabled (not recommended)

Privacy Password is the privacy password used to communicate privately with the trap sink. A privacy password must be provided if *Privacy* is not set to *None*. If the sink has privacy enabled but doesn't have a specific privacy password, then the privacy password is likely the same as the authentication password.

3.3.2.4 Download MIB Files

Several Management Information Bases (MIBs) are available for querying on this unit using SNMP and these MIBs can be accessed using unique Object Identifiers (OIDs).

MIB	OID
System	1.3.6.1.2.1.1
Interfaces	1.3.6.1.2.1.2
IP	1.3.6.1.2.1.4
ICMP	1.3.6.1.2.1.5
TCP	1.3.6.1.2.1.6
UDP	1.3.6.1.2.1.7
Bridgeworks Node Management Statistics	1.3.6.1.4.1.49599.11
Bridgeworks Service Statistics	1.3.6.1.4.1.49599.12

The MIBs describing data within the Bridgeworks' OID can be downloaded by clicking [Click Here to Download](#). A MIB file can be imported into an SNMP manager in order to provide useful information about data returned by the SNMP agent or sent in an SNMP trap.

3.3.3 Email

Simple Mail Transfer Protocol (SMTP)

SMTP Server:

SMTP Server Port:

Sender Email Address:

SMTP Username:

SMTP Password:

Save

Event Notification Email

Enable Email Alerts: ☐

Recipient Email Address:

System Event Level:

System Log Level:

Test Save

This section allows an SMTP server to be configured, to send emails on behalf of the Node.

The fields in this subsection are:

SMTP Server To enable an SMTP server, enter its IP address or hostname in this field.

The server must be reachable from the Node's Management interface (or whichever port the default route is set to) on this address. Refer to Section [3.1.3.4: Default Route](#) for information on setting the default route.

SMTP Server Port Enter the port number of the SMTP server. If no port number is specified, it will use the default port (25).

Sender Email Address The address from which emails will be sent. This needn't be a previously in-use address; it can be anything your SMTP server will allow. This can be used to identify the emails from this Node.

Must be of the form: @.

SMTP Username Username credential to be used to send emails from the SMTP server. May be blank, depending on your server's configuration.

SMTP Password Password credential to be used to send emails from the SMTP server. May be blank, depending on your server's configuration.

Click **Save** to apply any changes made to the SMTP configuration.

3.3.4 Event Notification Email

The Node can notify a systems administrator when events of a certain urgency occur in the Node log. Before this can be done, SMTP settings must be configured. Refer to Section 3.3.3: [Email](#) for information on SMTP settings.

To enable email alerts on the Node, select the *Enable Email Alerts* checkbox. The two following fields should then be completed:

Recipient Email Address The email address/addresses to which the emails will be sent. Multiple email addresses can be specified, separated by a semicolon, e.g.:
`office@example.com; home@example.com.`

Trigger Event Log Level The minimum log level to trigger an email. Events of higher urgency than the selected level will also trigger an email. The available levels are, in descending order of urgency:

Critical Example: The Node is running at non-recommended temperatures.

Error Example: A device attached to the Node has been disconnected.

Warning Example: An invalid configuration file was uploaded.

Confirm these settings by clicking **Save**.

The *Test* button will send a test email to the recipient email address/addresses to confirm that the email configuration is working correctly.

3.3.5 Remote System Log

This section is about remote system logging, which allows the user to store the node's logs in a centralised external system. Each node can send its logs to a maximum of 10 different servers by completing the form below.

Add Remote Log Host

Syslog Server:

Port:

Protocol:

TCP Framing:

Enable Encryption: ☐

Certificate Authority: No file chosen

Authorisation Mode:

Peer Name:

Syslog Server The IP address or hostname of the local server being accessed.

Port The port number to use when connecting to the log host. This defaults to 514 if not changed.

Protocol The type of protocol to use for forwarding: TCP or UDP. Only one protocol can be defined per remote log host.

TCP Framing When sending system log messages to TCP hosts there are two forms of message framing, traditional sends new line characters after each log, while octet-counted sends the message length ahead of the log entry. Select the method which is most compatible with your system log server.

Enable Encryption This section allows the log host connection to be encrypted. If you do not wish to encrypt your system log, leave the Enable Encryption checkbox unchecked.

Certificate Authority When encryption has been selected a Certificate Authority certificate must be provided using the file upload field. This should match the certificate authority used on your remote log host as it will be used to verify the connection.

Authorisation Mode There are two supported authorisation modes: Name and Anon. Name is the default option as it is the most secure.

Name Uses certificate validation and subject name authentication.

Anon Uses anonymous authentication. This mode checks for certificates, however they aren't validated.

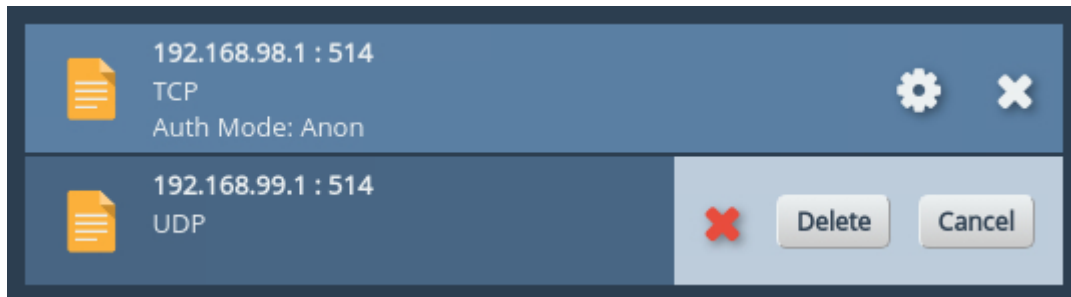
Peer Name This is the name of the remote peer on your client's certificate. This is only relevant when Name Authorisation is selected.

Once all the desired fields have been completed, click the *Add* button at the bottom right of the form.

3.3.5.1 Editing or Deleting a Connection

Once a connection has been created, the information can be updated by clicking the *gear* symbol. Any aspect of the connection can be edited from the address to type of encryption it uses. If a certificate authority has previously been uploaded for that connection, editing also means that this can be removed and a new one uploaded if desired.

Additionally, a host can be deleted by clicking the *X* icon on the main remote logging host page. Deleting a host will immediately remove the connection as well as the Certificate Authority linked to that connection, if applicable.



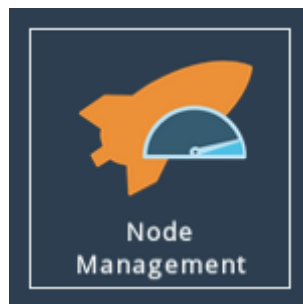
4 PORTrockIT Configuration

The *PORTrockIT* section of the web interface allows the administrator to configure different aspects of the PORTrockIT Node.

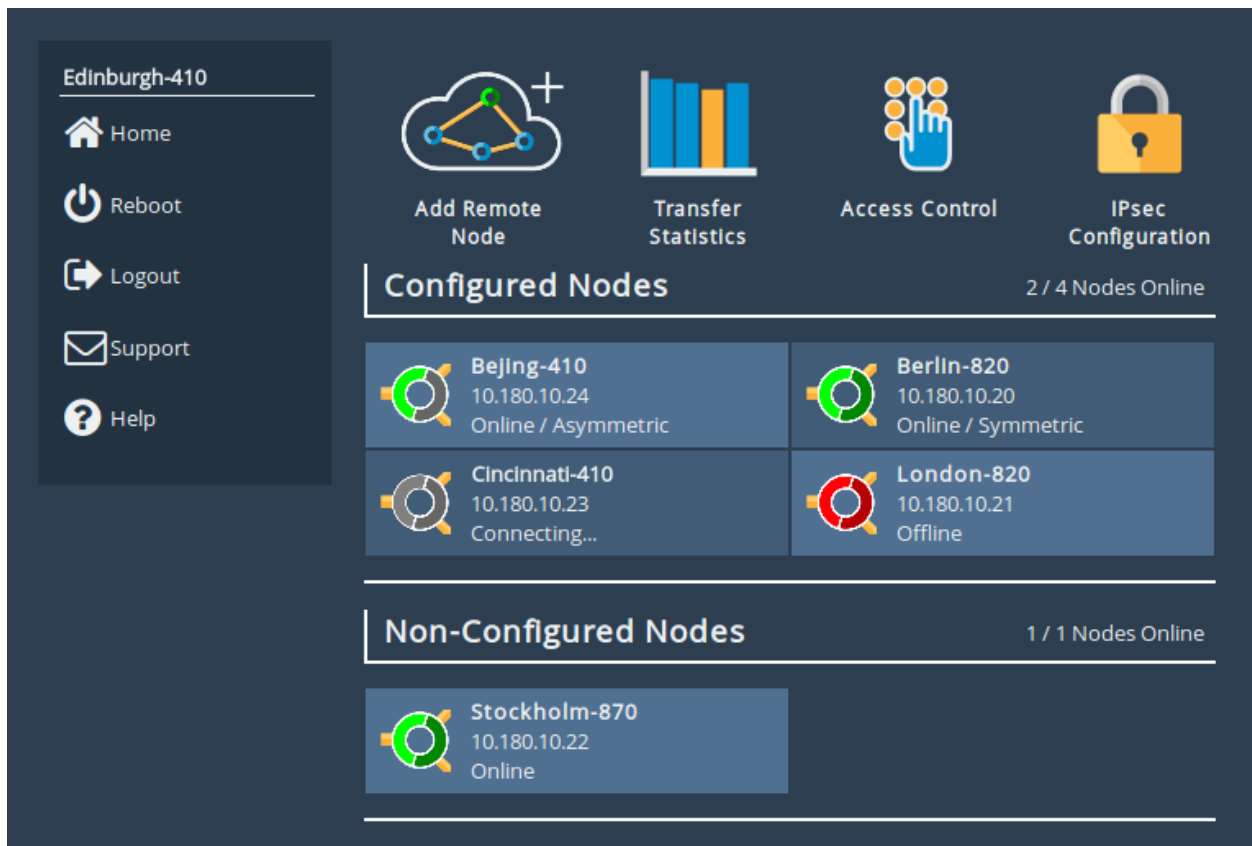
4.1 Node Management







The *Node Management* page has all the tools necessary to connect to remote Nodes, set security options, view transfer statistics and configure your linked Nodes.


From the Home screen, select the *Node Management* icon under the *PORTrockIT* section.



The web interface will now display the following:



Configured Nodes		2 / 4 Nodes Online
	Beijing-410 10.180.10.24 Online / Asymmetric	
	Berlin-820 10.180.10.20 Online / Symmetric	
	Cincinnati-410 10.180.10.23 Connecting...	
	London-820 10.180.10.21 Offline	

Non-Configured Nodes		1 / 1 Nodes Online
	Stockholm-870 10.180.10.22 Online	

Options at the top of the page allow you to configure settings for your current Node. More information for these options can be found in the following sections:

- Section [4.1.2: Add Remote Node](#)
- Section [4.1.3: Transfer Statistics](#)
- Section [4.1.4: Access Control](#)
- Section [4.1.5: IPsec](#)

4.1.1 Remote Nodes

This section details the Nodes that have been configured with your appliance.

The screenshot displays a web interface with two main sections: 'Configured Nodes' and 'Non-Configured Nodes'. The 'Configured Nodes' section is titled 'Configured Nodes' and shows '2 / 4 Nodes Online'. It contains four entries, each with a circular status icon, a hostname, an IP address, and a connection status. The entries are: Beijing-410 (10.180.10.24, Online / Asymmetric), Berlin-820 (10.180.10.20, Online / Symmetric), Cincinnati-410 (10.180.10.23, Connecting...), and London-820 (10.180.10.21, Offline). The 'Non-Configured Nodes' section is titled 'Non-Configured Nodes' and shows '1 / 1 Nodes Online'. It contains one entry: Stockholm-870 (10.180.10.22, Online).

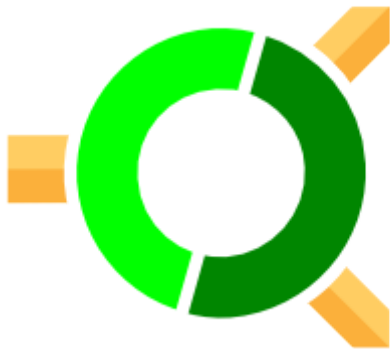
Configured Nodes		2 / 4 Nodes Online	
	Beijing-410 10.180.10.24 Online / Asymmetric		Berlin-820 10.180.10.20 Online / Symmetric
	Cincinnati-410 10.180.10.23 Connecting...		London-820 10.180.10.21 Offline

Non-Configured Nodes		1 / 1 Nodes Online	
	Stockholm-870 10.180.10.22 Online		

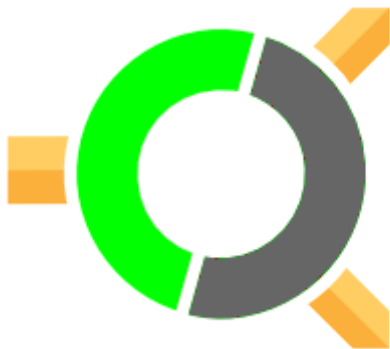
Each Node can be identified by the Node's hostname. The hostname of each Node can be configured on its own Web interface under the *Hostname* field of the *Network Connections* page.

In addition to the hostname, the leading IP address will be displayed. This is the Node's primary path address, which will by default be the IP address which was used to add the Node on the *Add Remote Node* page.

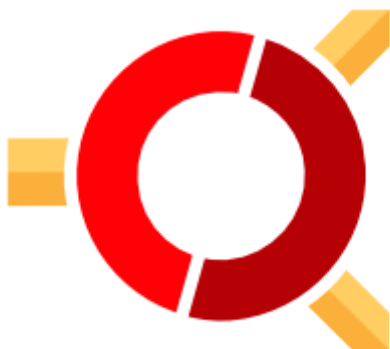
Finally the current status of the Node is displayed alongside an icon. The connection to the Node can be in one of four states:



Connection Active (Symmetric) Node is active with connected paths. Node also has a fully configured connection back.



Connection Active (Asymmetric) Node is active with connected paths. Node does not have a fully configured connection back. Note that acceleration will still work as normal with a Node in this state.



Connection Inactive Connection can not be made to a previously available Node. You may still remove the remote Node as usual.



Connecting Remote Node is configured with this device and is waiting upon a connection to be made. You may still remove the remote Node configuration as usual.

Clicking on the icon for a remote Node will take you to the management page for the remote Node.

4.1.1.1 Configured Nodes

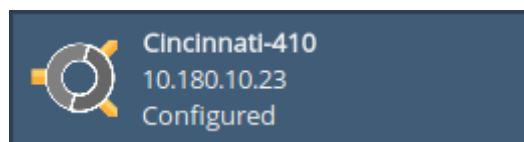
This list represents Nodes that have been directly added. Nodes in this list have additional configuration options available for them.

4.1.1.2 Non-Configured Nodes

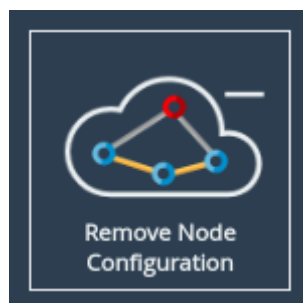
This list represents Nodes that have made an inbound connection, but have not been directly added. *Relationships* and *VPN* tunnels can still be created for Nodes in this state and acceleration can still be performed. A *Non-Configured Node* can become a *Configured Node* by performing the *Add Remote Node* operation on it; doing so will enable additional configuration options.

4.1.1.3 Orphaned Nodes

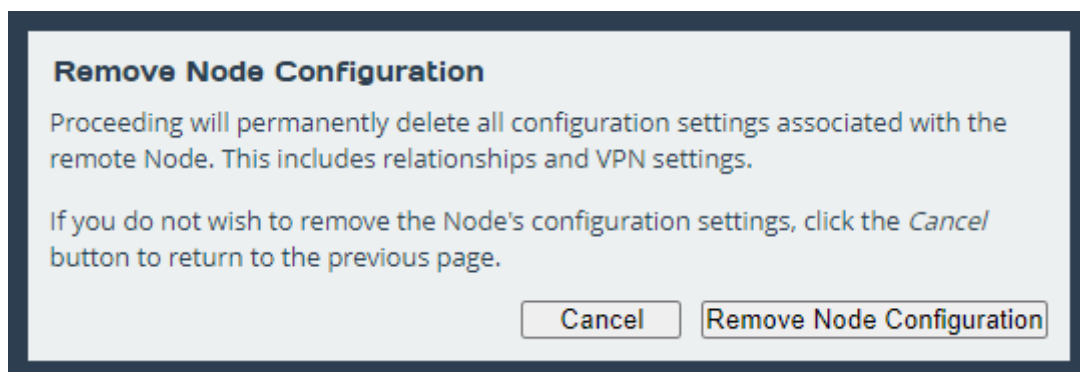
An orphaned Node is a remote Node which has configuration settings, hasn't been directly connected, and hasn't established the inbound connection to this Node. These Nodes will be displayed in the *Configured Nodes* list and look like the following example.



These configuration settings can be deleted by first clicking on the orphaned Node and then clicking on *Remove Node Configuration*.



This takes you to the Remove Node Configuration page as shown below.



Click on the *Remove Node Configuration* button and confirm the removal to delete the saved

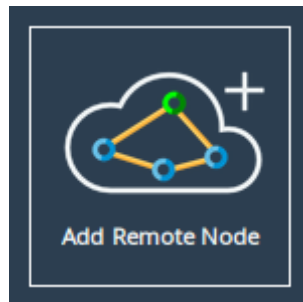
configuration settings.

4.1.2 Add Remote Node



Important: If you want to encrypt accelerated traffic, this step should be done after configuring [IPsec](#).

To add a remote Node, click on the *Add Remote Node* icon on the Node Management page.



The following page will allow you to add a remote Node using the *IP Address*.

This page allows a remote Node to be added to the list of connected Nodes. The *IP Address* field takes input of the IP address of the remote Node. The *Network Interface* drop-down menu allows for the selection of the WAN interface on this Node to be used to initiate the connection to the remote Node, if this Node has WAN capabilities mapped to more than one. See [Chapter 5: Port Mappings](#) for information on adding and removing WAN capabilities to network interfaces.

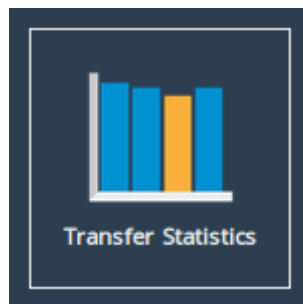
To add a remote Node, enter the IP address of a WAN port on the remote Node which is visible to this Node, and click the *Add* button. If the remote Node is behind a NAT connection, the public IP address for the NAT connection should be used.

A dialog box will appear indicating the connection attempt to the remote Node, and will alert you to the success or failure of the Node connection. Any remote Node connection that has been added to the local Node in this way will be automatically saved, and will restore on reboot until the Node is removed.

4.1.3 Transfer Statistics

This configuration page will allow you to monitor, in real time, the performance of a link over the span of a minute and download the performance data between the local and the remote Node over the last 24 hours.


From the Node Management screen, select the *Transfer Statistics* icon.





The web interface will now display the following window:


Transfer Statistics


Node Menu


 Home

 Nodes

 Reboot

 Logout

 Support

 Help

Licensed To

Bridgeworks Ltd

Remote Nodes

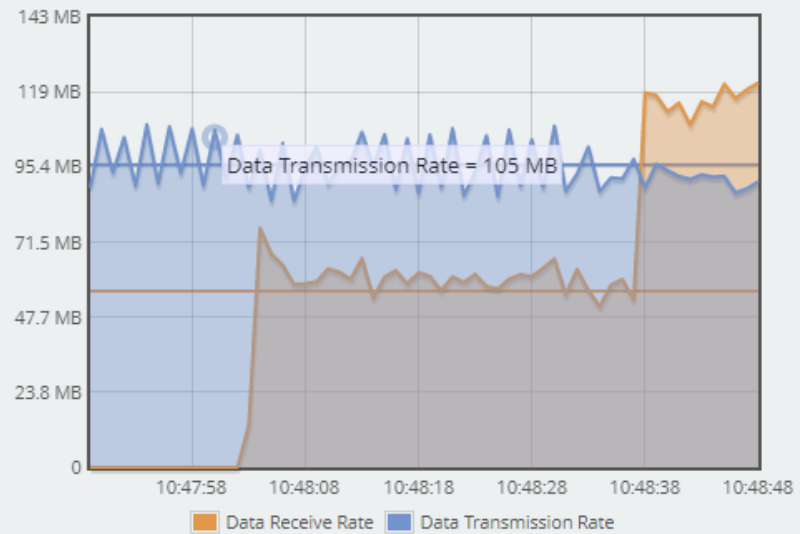
Select a Node from the list below to view transfer information.

Remote Node Name

Berlin-800

Stockholm-200: (Offline)

Data Transfer Rate



[Download 24 Hour CSV File](#)

To view a remote Node's transfer rate, click on the name of the Node from the *Remote Node Name* list, and graphing will start automatically.

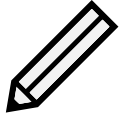
A remote Node will be shown as offline if the link to it has not been re-established after a system restart. You cannot start monitoring performance data to a remote Node until the link has been re-established. An offline Node is indicated if the name of the Node has *Offline* next to it, as shown.



Important: If there are no remote Nodes online then you will not be able to see the *Data Transmission Rate* graph or the *24 Hour Transfer History* button.

4.1.3.1 Data Transfer Rate

This section shows both the *transmission* and the *receive* rate for the Node. The transmission rate is in blue and the receive rate is in orange.



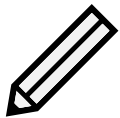
Note: Because these parameters are always in a state of continual monitoring by the AI, clicking to view these figures will not affect the performance of the data transfer.

The solid, horizontal, blue and orange lines across the graph show the average *transmission* and *receive* rates respectively over the displayed one minute period.

Hovering the mouse over any of the *transmission* or *receive* data points will display the exact value at that point.

4.1.3.2 Download 24 Hour Transfer History

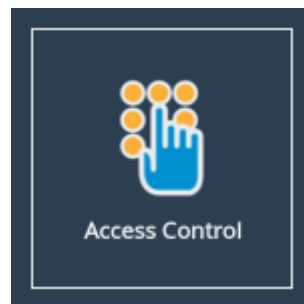
You are able to download the transfer rate statistics of the previous 24 hours by clicking on the *Download 24 Hour CSV File* button. The downloaded file is in .csv format and can be viewed in a compatible program. See Appendix D: [Transfer Statistics Graphing Instructions for Excel 2010](#) for information on viewing this file.



Note: The 24 hour statistics are cleared on reboot.

4.1.4 Access Control

To configure access control settings, click on the *Access Control* icon on the Node Management page.



The following page will be displayed:

The screenshot shows the 'Access Control' configuration page. On the left is a 'Node Menu' with links to Home, Nodes, Reboot, Logout, Support, and Help, and a 'Licensed To' section for Bridgeworks Ltd. The main content area has two sections: 'Remote Administration' with a checked 'Enable Remote Administration' checkbox, and 'Whitelist' with a checked 'Enable Whitelist' checkbox. Below the whitelist section is a table titled 'Whitelisted IP Addresses' with one header 'IP address' and one row containing the text 'Use the form below to add an IP to the whitelist'. Below the table is a 'New IP:' label, a text input field, and 'Add' and 'Remove' buttons. At the bottom right are 'Cancel' and 'Save' buttons.

4.1.4.1 Remote Administration


The *Enable Remote Administration* checkbox allows for the disabling or enabling of remote access of this Node. You can start a Remote Access session from the Node Management page of the remote Node, see Section 4.2.16: [Remote Control](#).

4.1.4.2 Whitelist

By default, the *Enable Whitelist* checkbox will be selected, which stops incoming PORTrockIT connections from IP addresses not explicitly specified. Clearing the checkbox will instead allow all incoming PORTrockIT connections.

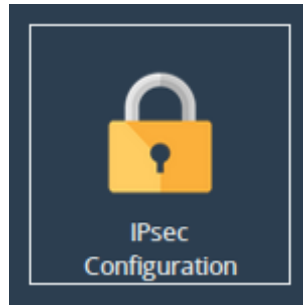
To allow a new connection from a remote Node, enter the IP address of the remote Node's WAN interface in to the *New IP* field and click *Add*. Multiple addresses can be added for each connected remote Node, and are required for multiple paths.

To delete a listing, select the entry in the *Whitelisted IP Addresses* table and then click *Remove*.

	<p>Important: Adding or removing entries from the whitelist will not take effect until the Save button is clicked.</p>
---	--

4.1.5 IPsec

IPsec can be enabled on all WAN connections, using AES encryption. To configure IPsec, click on the *IPsec Configuration* icon found at the top of the Node Management page.



The web interface will now display the following window:



Important: Additional UDP ports must be open on any firewalls between the Node and the external WAN connection before configuring IPsec. For more information on which ports need to be opened, please see [Appendix A: IP Protocols and Port Numbers](#)

4.1.5.1 Enabling IPsec service

Checking the *Enable IPsec* checkbox will allow the IPsec encryption service to start after clicking the Save button. Traffic moving through the Node will not be encrypted at this point. Unchecking this box will stop the IPsec service without removing any of the configurations on this page.

4.1.5.2 Encrypting Accelerated Traffic

Accelerated traffic can be encrypted using the *Encrypt Accelerated Traffic* checkbox as long as the service has been started and a PSK has been set.



Important: A pre-shared key is necessary for both VPN connections, and WAN link encryption.

4.1.5.3 Adding a PSK (Pre-Shared Key)

In the *IPsec Pre-Shared Key* field, enter a value or use the *Generate Key* button to set the PSK. If the *Generate Key* button was used to create the key, copy and paste it to the *IPsec Configuration* page of each connected Node.



Important: A matching pre-shared key must be entered on all connected Nodes.



Important: The PSK must be at least 16 characters and at most 256 characters.

The pre-shared key will not display automatically when returning to this page. If you need to copy it to another Node, click the *Show Key* button.



Important: A warning will appear when configuring IPsec over an unsecured connection (i.e. HTTP rather than HTTPS). To ensure your pre-shared key cannot be intercepted over your network connection, enable HTTPS before configuring IPsec as explained in Section [3.2.3: Secure Connection](#).

The entered pre-shared key is saved in a secure configuration store, and is not removed automatically when IPsec is disabled. To delete your pre-shared key, click *Delete Key*. This will disable any VPN connections, and WAN link encryption, if either is enabled.

4.2 PORTrockIT Node Page

The *PORTrockIT Node* page has all the configuration settings and applications used to set up a specific remote Node. Clicking on any *Remote Node* icon on the *Node Management* page will take you to the equivalent *PORTrockIT Node* page for that remote Node.

Once loaded, the following page should be displayed:

PORTrockIT Node - Hostname

Hostname

Home

Nodes

Reboot

Logout

Support

Help

Node Status

State:

Online

Model:

100

TX/RX:

0 KB/s / 0 KB/s

Active Paths:

1 / 1

Negotiated Bandwidth:

119 MB/s

Remote Configuration:

Present

Node Configuration

Path Configuration

Transfer Statistics

Remove Node

Applications & Utilities

Relationships

WCCPv2

VPN

Remote Control

Learn

Note: Available configuration options and applications shown will vary based on the specific *Product Type* of the remote Node.

Note: Available configuration options and applications are limited if the selected remote Node is considered *Non-Configured*.

4.2.1 Node Status

This section contains information about the remote Node:

State The current connection state for the remote Node. Potential values include: *Online*, *Connecting* or *Offline*.

Active Paths Both the total number of available paths to the remote Node as well as the number that are currently active.

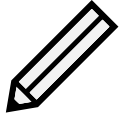
Model Model number of the remote Node.

Negotiated Bandwidth Maximum licensed bandwidth limit between the two Nodes.

TX/RX Current transfer and receive statistics to and from the remote Node respectively.

Remote Configuration *Present* or *Not Present* indicating whether or not the remote Node has a full configuration back to this Node. This value may take a few seconds to update after a configuration change.

76



Note: Some status elements may appear as *Unknown* if the selected remote Node is considered *Non-Configured*.

4.2.2 Node Configuration

All settings specific to this remote Node are located here. More information for these options can be found in the following sections:

- Section [4.2.4: Path Configuration](#)
- Section [4.2.5: Node Specific Transfer Statistics](#)
- Section [4.2.6: Remove Node](#)

4.2.3 Applications & Utilities

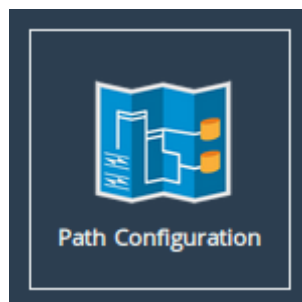
Any available *Applications* or *Utilities* are displayed here. More information for these options can be found in the following sections:

- Section [4.2.7: Relationships](#)
- Section [4.2.14: VPN Configuration](#)
- Section [4.2.16: Remote Control](#)
- Section [4.2.17: Learn](#)

4.2.4 Path Configuration

The PORTrockIT Node will always attempt to get the best performance possible for the data it is transferring. Upon establishing a connection between two PORTrockIT Nodes, an automatic check for other connections through their WAN ports will occur.

To view and modify link settings between two Nodes, navigate to the *Path Configuration* page from the management page of the remote Node.



A table will be displayed showing all paths between the current Node and the remote Node.

Path Configuration - bridgeworks

Hostname

Home

Nodes

Reboot

Logout

Support

Help

Path Configuration

Filtering options: Hide Unavailable Paths

	Local Address/ Remote Address	Path State	Bandwidth Limit	Path Type	Failover Target / ID
	10.10.64.205/ 10.10.64.144	✓	<input type="checkbox"/> 0 MB/s	Primary	Any
	10.10.64.205/ 10.10.64.94	✓	<input type="checkbox"/> 0 MB/s	Failover	Path 2
	10.10.64.205/ 10.10.64.142	✓	<input type="checkbox"/> 0 MB/s	Failover	Path 3
	10.10.64.205/ 10.10.64.143	✓	<input type="checkbox"/> 0 MB/s	Failover	Path 4
	10.10.64.205/ 10.10.64.153	✓	<input type="checkbox"/> 0 MB/s	Failover	Path 5


Refresh

Cancel

Save

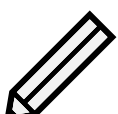
4.2.4.1 Setting Primary and Failover Paths

A path is a connection between two IP addresses when you establish a link between two PORTrockIT Nodes. Once the “primary” path is established, the Nodes will then automatically check for other available connections to each other through their WAN ports. Any additional connections that are found will automatically be set as ‘failover’ paths. A failover path will not be used unless the primary path fails. You can also select a *Primary Failover* path which will be the first used in the event of a failure with the primary path. To choose a Primary Failover path, select the path that you wish to use from the *Failover Target/ID* drop down box on the far right of the path table.



Note: The order in which failover paths are used, after any initial Primary Failover path, is set automatically and cannot be manually changed.

To change the primary path, click on the *Path Type* drop-down of the primary path and select *Failover* from the drop down list. Click on the *Path Type* drop box of the path that you wish to set as the new primary path and select *Primary* from the drop down list. Click on *Save* to save your changes.



Note: Multiple links can be assigned as “primary paths”; the PORTrockIT Node will automatically attempt to use all available primary links simultaneously. There must be at least one primary path designated at any time.

An icon in the *Path State* box will indicate the state of each path:



Link Up Represents a known link that is up.



Known Link Down Represents a known link that is down.



Unavailable Link Represents a possible link that has not been connected to.

4.2.4.2 Filtering options

By default, this page will hide unavailable paths. In order to show unavailable paths, select *None* from the *Filtering options* drop-down.

4.2.4.3 Configuring a Node's Bandwidth

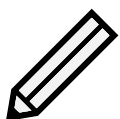
If there is other traffic on your network that needs to access a share of your bandwidth, you can limit the bandwidth between your Nodes. The limit is applied on a per path basis.

To set a limit on a connection, select the *Bandwidth Limit* checkbox next to the connection that you wish to limit. This will enable the bandwidth limit field next to the checkbox. Enter a value in megabytes per second and click the *Save* button.



Note: The minimum bandwidth limit you can set is 1 MB/s.

To remove a *Bandwidth Limit* untick the *Bandwidth Limit* checkbox on the desired connection, and click *Save*. The limit will then be lifted. A bandwidth limit of 0MB/s indicates that no restriction is being applied.

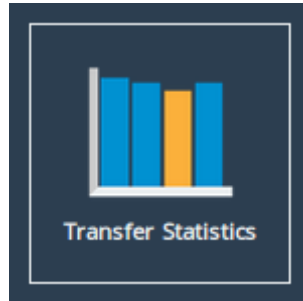


Note: Any changes to the bandwidth limit will become effective immediately on pressing *Save*.

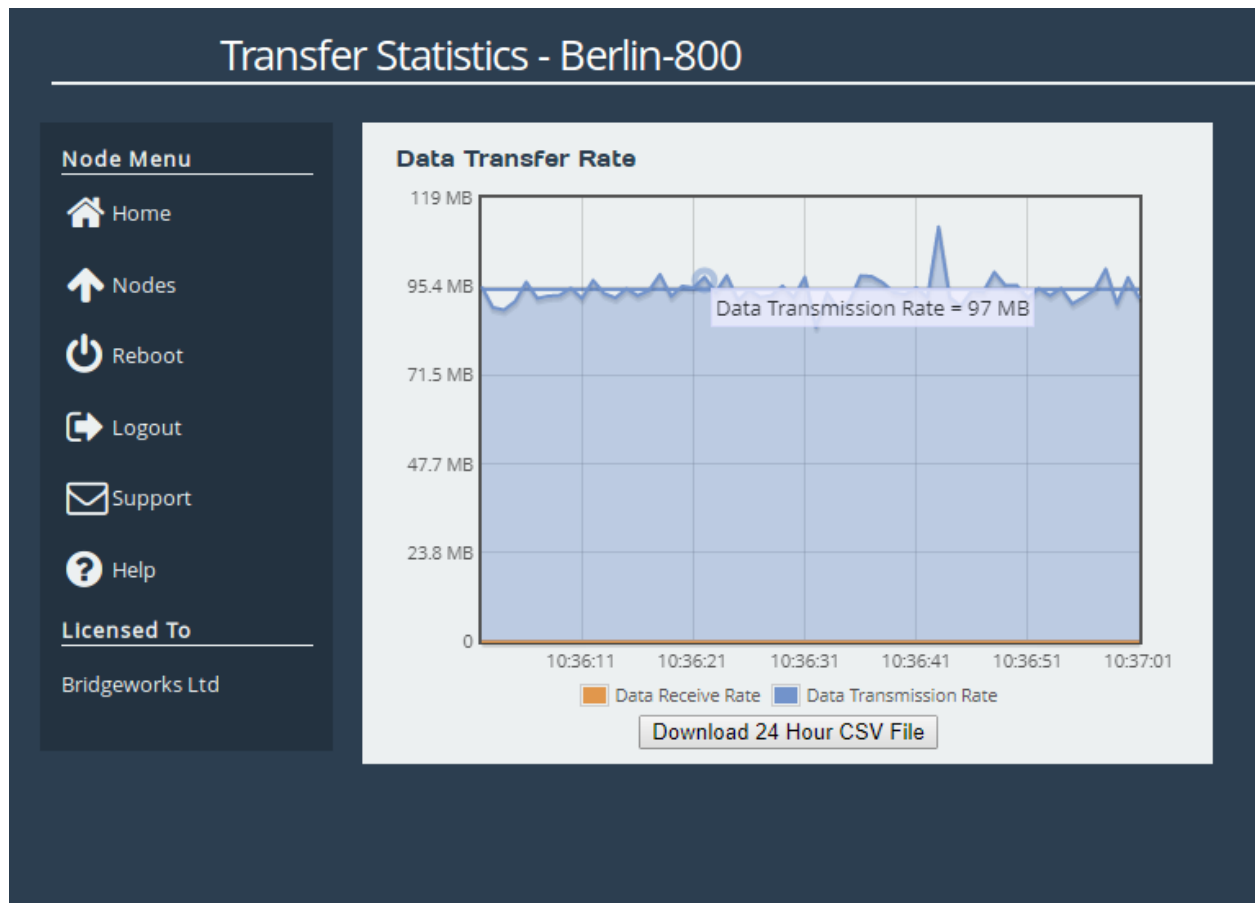
4.2.5 Node Specific Transfer Statistics

This page allows you to monitor, in real time, the performance of the link between your Node and a remote Node.

Navigate to the management page of the remote Node and click the *Transfer Statistics* icon.

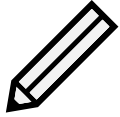


The web interface will then display the following window:



4.2.5.1 Data Transfer Rate

This section shows both the *transmission* and the *receive* rate for the Node. The transmission rate is in blue and the receive rate is in orange.



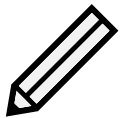
Note: Because these parameters are always in a state of continual monitoring by the AI, clicking to view these figures will not affect the performance of the data transfer.

The solid, horizontal, blue and orange lines across the graph show the average *transmission* and *receive* rates respectively over the displayed one minute period.

Hovering the mouse over any of the *transmission* or *receive* data points will display the exact value at that point.

4.2.5.2 Download 24 Hour Transfer History

You are able to download the transfer rate statistics of the previous 24 hours by clicking on the *Download 24 Hour CSV File* button. The downloaded file is in .csv format and can be viewed in a compatible program. See Appendix D: [Transfer Statistics Graphing Instructions for Excel 2010](#) for information on viewing this file.



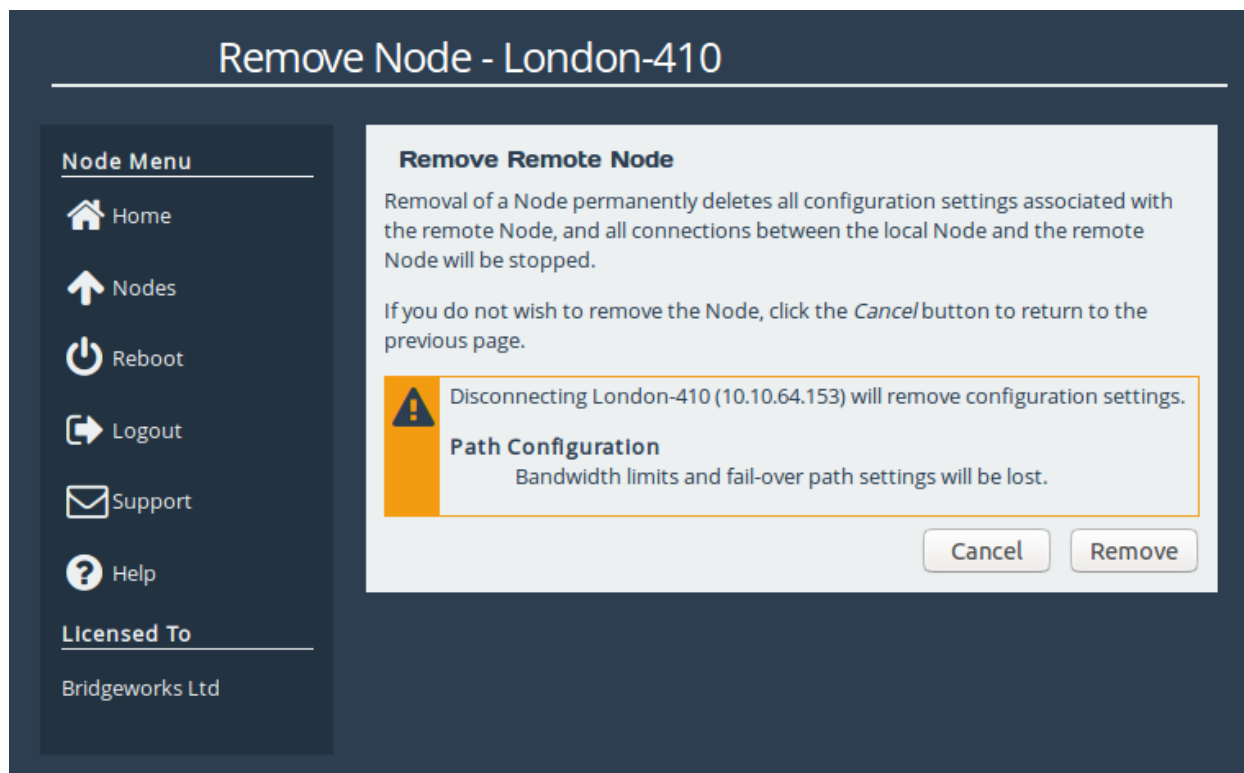
Note: The 24 hour statistics are cleared on reboot.

4.2.6 Remove Node

To remove outgoing configurations for a remote Node, navigate to the management page of the remote Node and click the *Remove Node* icon.



The following page will be displayed:



This page allows the administrator to disconnect from a remote Node, removing it from the list of connected Nodes and permanently deleting all outgoing configurations to that Node. To disconnect from a remote Node, click the *Remove* button.

	<p>Important: Removing a Node will not terminate existing transfers unless both Nodes have removed each other and been rebooted together.</p>
--	---

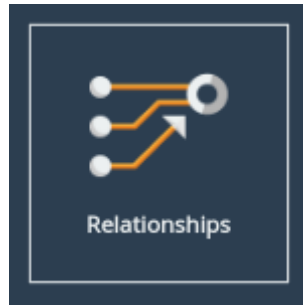
4.2.7 Relationships

The *Relationship* between two Nodes dictates which traffic is accelerated by a remote Node. This is done by linking one of the pre-configured services (see Section 4.3: [Service List](#)) to a remote Node. The remote Node will then recognise any traffic that matches the service and accelerate it.

4.2.7.1 Prerequisites

In order to establish an acceleration link you must have an officially supported appliance or application which PORTrockIT has been verified to accelerate.

To configure the *Relationships* for any remote Node, navigate to the management page of the remote Node you wish to configure and click the *Relationships* icon.



4.2.8 Services Table

The page will display a table with all of the currently configured services listed as shown below.

A screenshot of a web interface titled "Relationships - Belle". On the left is a "Node Menu" with links: Home, Nodes, Reboot, Logout, Support, and Help. The main area is titled "Active Services" and contains a table with three rows. Each row has an icon of four orange books, a text description of the service, its IP address and port, and a toggle switch labeled "OFF". At the bottom, there is a "Configure Services" link with a left arrow, and "Cancel" and "Save" buttons.

Active Services			
	Development (IBM Spectrum Protect)	192.168.1.5 Port 5	<input type="checkbox"/> OFF
	Service 2 (Carlingo Swarm)	192.168.1.3 Port 4	<input type="checkbox"/> OFF
	Service 3 (Carlingo Swarm)	192.168.1.0/24 Port 3	<input type="checkbox"/> OFF

Each service has a summary including the designated *Name* and *Protocol* - some may include the port ranges of the service, followed by the given *Address* of that service and the *LAN Interface* that can be used to connect to that address.

4.2.9 Toggling a Relationship

Services have a switch on the right edge of the table item. This will toggle the relationship off or on as shown.



The page must be saved for any changes to take effect.

4.2.10 Configure Services

This link will navigate directly to the *Service List* page, allowing new services to be configured if they have not already been set up.

4.2.11 Cancel

Returns to the *Node Specific* page discarding any changes.

4.2.12 Save

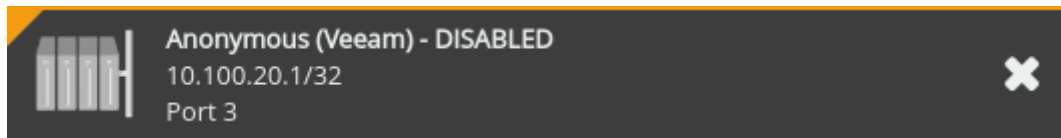
Commits any changes made, setting up *Relationships* for any services that have been linked to this remote Node.

4.2.13 Disabled Services

Disabled services occur due to:

- Modifications to the licences and their association to a network interface
- An active interface, bond, or VLAN being deleted
- An active interface being bonded

If changes are made in this way, any active services that are no longer valid for the new configuration will be marked as disabled.



Any associated relationship configurations are immediately removed when a service is disabled resulting in potential disruption of traffic. Equally, it is not possible to activate a relationship using a disabled service.

In order to re-enable the service, the correct interface must be made available and mapped with the corresponding protocol licence as defined by the service listed (see Chapter 5: [Port Mappings](#)). Alternatively, the disabled service can be erased from the configurations (see Section 4.3.2: [Remove Service](#)).

4.2.14 VPN Configuration

Connected PORTrockIT Nodes can set up a *VPN Tunnel* across the WAN link. This can be helpful if the PORTrockIT Nodes represent the only viable path between the two Endpoints, allowing non-accelerated traffic to pass through a dedicated link.

To begin setting up a VPN tunnel to a remote Node, navigate to the *VPN* page from the management page of the remote Node.



The following page should be displayed.

VPN - Edinburgh-410

Node Menu

Home

Nodes

Reboot

Logout

Support

Help

Licensed To

Bridgeworks Ltd

VPN Configuration

Note that you must also configure the remote VPN settings by navigating to the remote Node or starting a [remote session](#) before the VPN will activate.

Enable VPN:

☒

Local Subnet:


10.180.10.1 / 32


Cancel


Save

VPN settings can be enabled by ticking the *Enable VPN* checkbox.

The tunnel will require a CIDR block representing the *Local Subnet* to be entered into the *Local Subnet* input box.

- 

Important: The *VPN tunnel* will only initialise once the *Local Subnet* has been configured in this way on **both** the local and remote Nodes.
- 

Important: The *VPN tunnel* requires IPsec to be configured and running to the remote Node before it can be activated. See Section [4.1.5: IPsec](#) for more details on configuring IPsec.
- 

Important: The *VPN tunnel* cannot be activated if any of the Node's Interfaces are configured to act as a *Network Bridge*.

4.2.15 WCCPv2

WCCPv2 allows traffic between two Nodes to be accelerated without any configuration at the endpoints. The web interface allows for configuration of a service group for each Node, as well as viewing the status of connected web-caches and routers.

To begin setting up a *WCCPv2* connection with a remote Node, navigate to the *WCCPv2* page from

the management page of the remote Node.



The following page will be displayed.

Service Group Status

State:	Usable	Uptime:	03:16
Forwarding:	L2	Return Method:	L2
Connected Routers:	1 / 1		

More Info

WCCPv2

Enabled:	<input checked="" type="checkbox"/>
Router Address:	<input type="text" value="10.10.136.14"/>
Service ID:	<input type="text" value="70"/>
Password:	<input type="text"/>

Show Advanced

Clear Configuration

Cancel

Save

4.2.15.1 Prerequisites

In order to establish WCCPv2 acceleration you must have two PORTrockIT Appliances or Virtual Instances, with a WAN link established between them, and licensed TCP acceleration protocols. For more information on establishing a WAN link, see Chapter 4: [PORTrockIT Configuration](#).

4.2.15.2 Configuring a Service Group

Details for a service group configured on a compatible Cisco router should be entered on this page in order for the Node to join the service group. Fields are available under the *WCCP* heading.

Service ID Service ID for this service group. This should be a number between 0 and 255 which matches the service ID value set on all routers in the service group.

Enabled Whether this Node should join the service group.


Router Address The address(es) used to communicate with the routers in the service group. This

can be: a single router IP address; a comma-separated list of router addresses; or a single multicast address on which all routers in the service group must be configured to listen.

Password An optional password, up to eight characters long, used for MD5 authentication when joining a service group. This should match the WCCP security setting used on routers in the service group. This field can be left blank to disable MD5 authentication.

The above settings should be sufficient to begin WCCPv2 acceleration with most configurations. In the event of differing needs for specific hardware configurations, further settings are available under the *Advanced* heading. Click the *Show Advanced* button to display this section.

Advanced Settings

 These options do not need adjustment for most configurations. Consider your use case before altering these settings.

Priority:

240

Weight:

100

Disable Router Address Check:

☐

Packet Assignment Method:

Negotiate Automatically ▼

Assignment Hash:

☒ Source IP

☐ Destination IP

☒ Source Port

☐ Destination Port

Assignment Mask:

Source IP Mask

0x1741

Destination IP Mask

Source Port Mask

Destination Port Mask

The settings available for further configuration are listed below.

Priority The priority with which packets for redirection are matched against those from other service groups. Valid inputs are 0 to 255, with 0 representing the lowest priority.

Weight The priority of the web-cache in relation to others in the service group, with 0 representing the lowest weight. Valid inputs are 0 to 65,535. Default value is 100.

Disable Router Address Check This option allows negotiation with a router if it replies to the Node from an IP address other than that specified under *Router Address*. Selecting this option should only be done when absolutely necessary. It is not necessary if a multicast address is specified under *Router Address*.

Packet Assignment Method Method with which packets are allocated across routers within the service group. *Automatic* negotiates with the router to decide a method. If using the *Automatic*

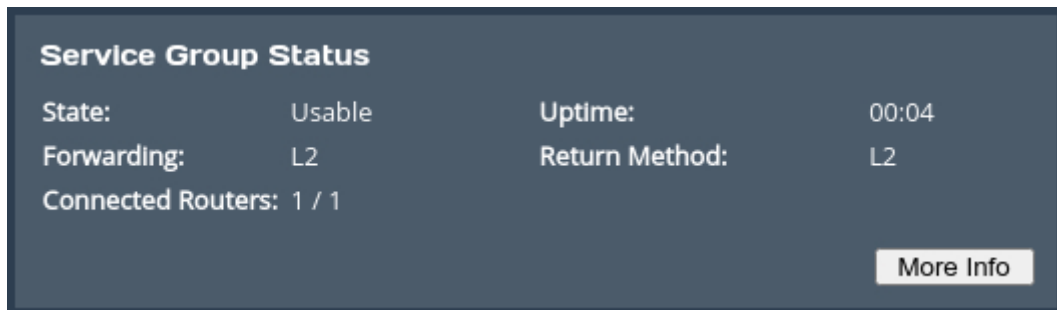
method, fields can be optionally filled in to be used in the case of negotiating to either *Hash* or *Mask* assignment. If a Packet Assignment Method is chosen, input fields are only available for the selected assignment method.

Assignment Hash Assignment Hash checkboxes represent elements of the packet to be used when the Packet Assignment Method is set to *Hash Assignment*.

Assignment Mask Assignment Mask fields take in a hexadecimal value of up to eight characters, in the format 0x00000000. The values represent binary bitmasks used by routers to distribute traffic when the Packet Assignment Method is set to *Mask Assignment*. The maximum number of total high bits across all masks combined should be no more than 7.

4.2.15.3 Monitoring a Service Group

The status of the service group can be observed with the field under the *Service Group Status* heading. The fields display basic information about an established service group.



Clicking the *More Info* button in the *Service Group Status* field on the WCCPV2 page leads to the *Service Group Status* page. This page allows for more in-depth monitoring of a service group, and shows information for each connected router.

4.2.15.4 WCCPV2 Service Group

The *Service Group* page allows you to observe the state of a service group, and ensure that it is working as expected.

The *Service Group Status* section shows negotiated settings and current information for the service group.

Service Group 70 Status	
Enabled	Yes
Priority	240
Weight:	100
Router Address Type	Unicast
Router Addresses	10.10.136.14
Forwarding Method	L2
Return Method	L2
Active Paths:	1 / 2

Enabled Whether the service group is currently active.

Priority Priority of the web cache against other web caches connected to a router.

Weight The priority of the web-cache in relation to others in the service group.

Router Address Type Whether the router(s) are connected through unicast addresses or a multicast address.


Router Addresses Multicast address, or list of individual router addresses, which are visible to the Node in the service group.

Forwarding Method Negotiated forwarding method across all routers.

Return Method Negotiated return method across all routers.

Active Paths The number of active and total paths to the specified routers.

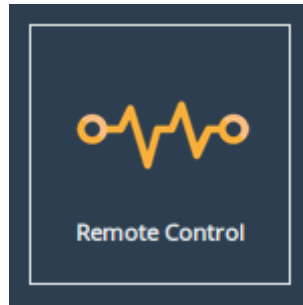
The *Routers* heading lists all known routers and an overview of their state.

Routers				1 of 1 active
	State:	Usable	Forward:	L2
	Identity IP:	10.10.136.14	Return:	L2
	Uptime:	00:31		

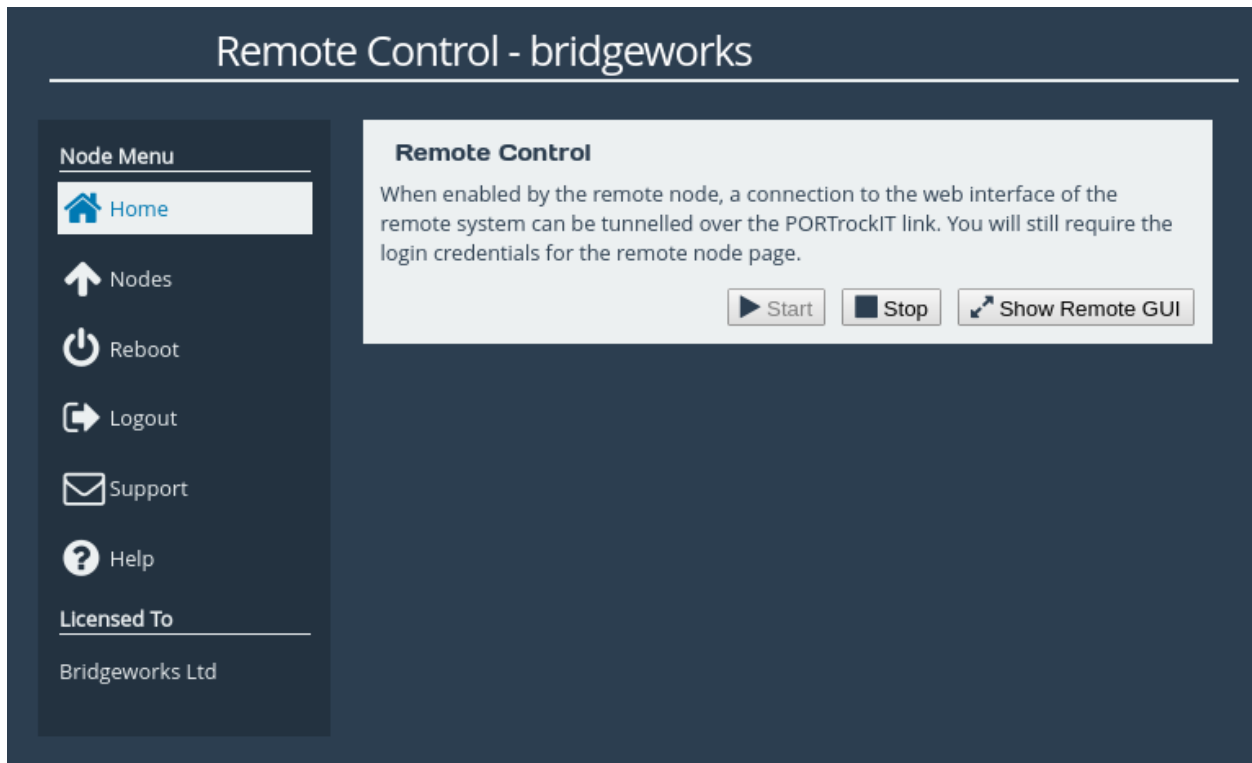
4.2.16 Remote Control

This page allows remote web interface access to a Node, which is useful when it is not possible to directly access the web interface of a remote Node.

To use remote control functionality, go to the management page of the remote Node and select the *Remote Control* icon.



To enable remote control, click the *Start* button.



The web interface will appear in a new window or tab, displaying the login screen of the remote Node. At the top of the web page will be a yellow bar displaying the name of the remote Node you are connected to. The rest of the page will display the login screen of the remote Node. You can log in with the remote Node's usual credentials.



Important: Your web browser may prevent the new window from appearing. Consult your web browser's documentation for information on how to allow the new window.

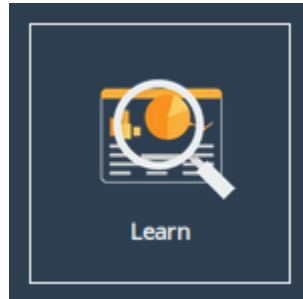
Remote Control Link - "hostname"

If you close the remote Node window with an HTTP connection, the session will continue to run. You may resume an HTTP remote session at any time by returning to the remote Node page and clicking the *Show Remote GUI* button. An HTTPS remote session to a Node will require reauthorisation if the session is left. To stop a remote Node session, click the *Stop* button.

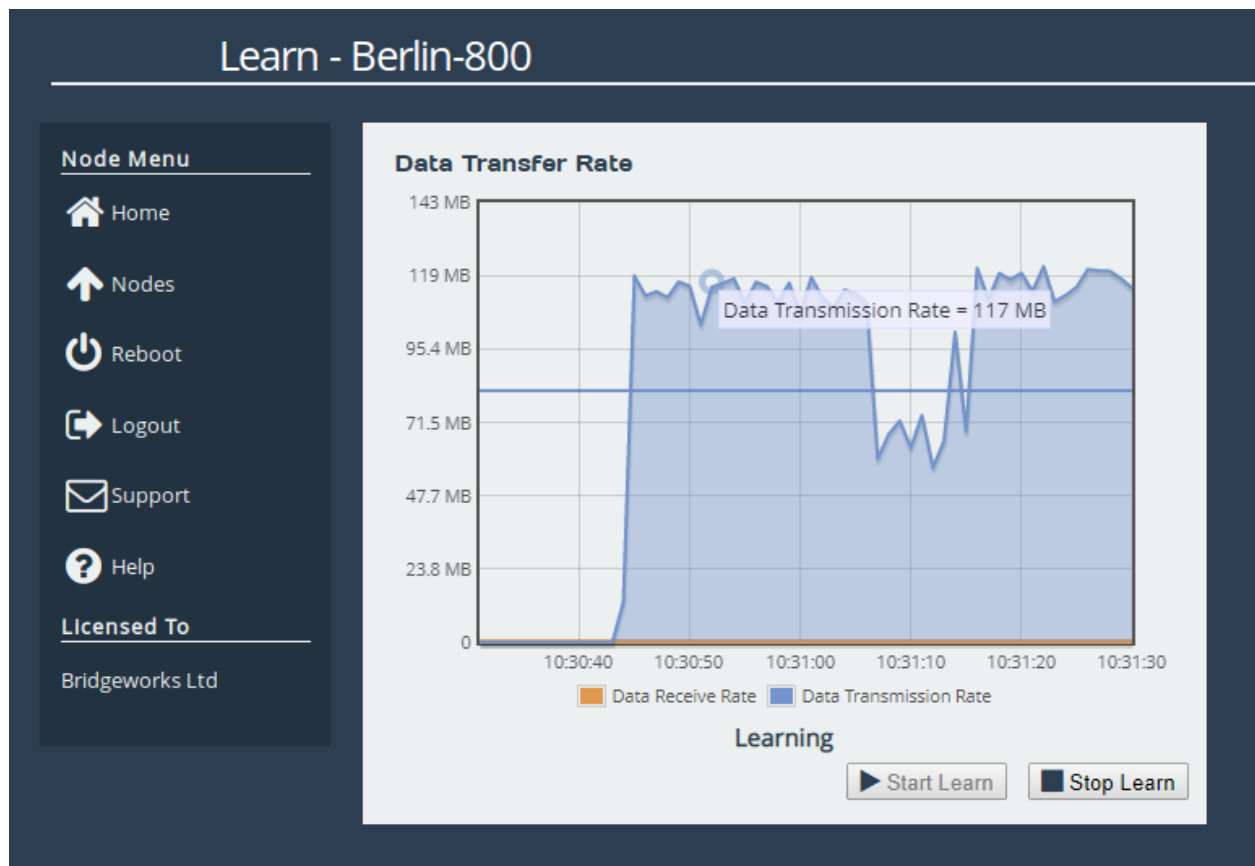
4.2.17 Learn

The learn procedure will initiate the *Artificial Intelligence* module, analysing the characteristics of the link network. Once it has completed, it will store these values to improve future data transfers.

A learn can be started by navigating to a Node's management page and selecting the *Learn* icon.



Clicking the *Start Learn* button will begin the learn procedure. A graph of the data transferred during the process will be displayed:



The learn process will take approximately five minutes. Navigating away from this page will not terminate the learn. The learn procedure can be run concurrently for multiple Nodes.

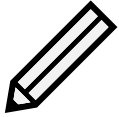


Important: Running a Learn operation uses large amounts of data between this Node and the remote Node, and thus may incur data charges.

Once the learn procedure is complete, the status message below the graph will read *Learn Successful*. A learn can be terminated before completion by clicking the *Stop Learn* button.

4.2.17.1 Data Transfer Rate

This section shows both the *transmission* and the *receive* rate for the Node. The transmission rate is in blue and the receive rate is in orange.



Note: Because these parameters are always in a state of continual monitoring by the AI, clicking to view these figures will not affect the performance of the data transfer.

The solid, horizontal, blue and orange lines across the graph show the average *transmission* and *receive* rates respectively over the displayed one minute period.

Hovering the mouse over any of the *transmission* or *receive* data points will display the exact value at that point.

4.3 Service List

The *Service List* page contains all the tools necessary to set up local services. A service defines a part of the local topology, including all information the PORTrockIT Node needs to connect to a target server.

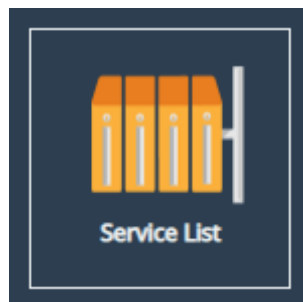
These are linked to remote Nodes to define what traffic types are accelerated from which remote Nodes, to which target servers.

Preserving the IP addresses the endpoints previously connected with whilst traversing a NAT is required to prevent any re-configuration on your Endpoints. In this scenario the *Service List* page is able to set up local services within a previously established NAT environment. For complete NAT set up NAT mapping configuration is also needed.



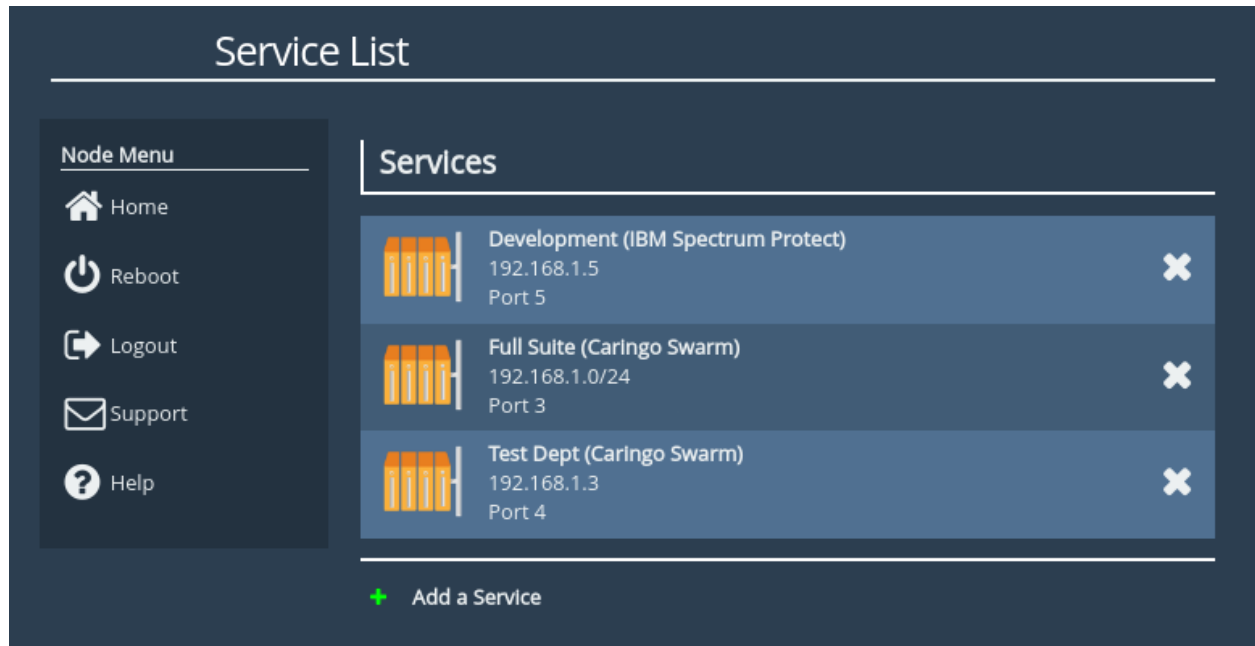
Important: A WANdisco Fusion licence and a Cloud platform set up are currently required to establish a NAT preservation connection. For more information on NAT preservation mappings see Section 4.5: [Client NAT Preservation](#).

From the Home screen, select the *Service List* icon under the *PORTrockIT* section.



4.3.1 Service Table

The page will display a table with all of the currently configured services listed as shown below.



Each service will give a summary including the designated *Name* and *Protocol*, followed by the given *Address* of that service and the *LAN Interface* that can be used to connect to that address.

Some relationships will also show the port ranges the service is configured on.

4.3.2 Remove Service

A service can be removed by clicking the 'X' icon on the right edge of the relevant table item. Confirmation will be required before the service is removed.

	Important: Removing a service will also remove all <i>Relationships</i> that use that service.
--	--

4.3.3 Add Service

Clicking the *Add a Service* button will show a dialog which is used to configure a new service.

If a NAT preservation configuration has not been established for this PORTrockIT then the following box will be shown.

Add New Service

Name
Service 1

Address
IPv4 Address / CIDR / Hostname

Protocol
Select Protocol...

Outgoing Interface
Select Interface...

Out of Path
☐

Cancel
Add Service

If NAT preservation is required on this system then an option to disable or enable NAT preservation for this service will be available.

Clearing the *Enable NAT* checkbox will disable endpoint NAT preservation and display the following dialog box.

Add New Service

Name
Service 1

Enable NAT
☐

Address
IPv4 Address / CIDR / Hostname

Private IP
Private IP Address

Protocol
WANdisco Fusion

Outgoing Interface
Port 3

Out of Path
☐

Cancel
Add Service

Selecting the *Enable NAT* checkbox will enable endpoint NAT preservation and display the following dialog box.

Add New Service

Name
Service 1

Enable NAT
☒

Public IP
Public IP Address

Private IP
Private IP Address

Protocol
WANDisco Fusion

Outgoing Interface
Port 3

Out of Path
☐

Cancel
Add Service

Other protocols may also introduce different fields to determine what port or port range is to be used during a data transfer. An example of this type of dialog box can be seen below where *Control Port* and *Data Port* are the port or port range a transfer will run on.

Add New Service

Name
Service 1

Address
IPv4 Address / CIDR / Hostname

Protocol
Data Transfer

Control Port
Port / Low Port-High Port

Data Port
Port / Low Port-High Port

Outgoing Interface
Port 3

Out of Path
☐

Cancel
Add Service



Note: Available configuration options will vary depending on the exact mappings and protocols available to the PORTrockIT unit.

4.3.3.1 Name

A unique identifier used to differentiate between services. Must be between 1 and 45 characters long.

4.3.3.2 Address

The address of the local server being accessed. This can be either an IPv4 value, a CIDR block value, or a resolvable hostname.

4.3.3.3 Public IP - Only available if NAT has been enabled

The public IP of the local server being connected to. This must be a valid IPv4 address.

4.3.3.4 Private IP - Only available if NAT has been enabled

The private IP of the local server being connected to. This must be a valid IPv4 address.

4.3.3.5 Protocol

A selection of all currently mapped protocols. Used to define which specific traffic type this service will use. A protocol must be mapped to an interface using the *Port Mappings* page before it will appear as a selection. Only one protocol can be defined per service.

4.3.3.6 Outgoing Interface

A list of all interfaces with a valid PORTrockIT mapping. Only interfaces with the currently selected protocol mapped to them will be available for selection. This interface will be used for outgoing connections irrespective of global routing rules.

4.3.3.7 Out of Path

If the selected protocol does not require a two way connection, the exact topology determines this setting as follows:

- **Out-of-Path** - Out-of-Path enables the acceleration of traffic where the PORTrockIT Node is located in a different routing domain to the server. It achieves this using non-transparent addressing, and can only accelerate incoming connections to the server.
- **Bridged Physically-In-Path** - The PORTrockIT Node is placed directly in-path between the server and WAN such that no additional routing rules are required for local traffic. The Node must be configured to act as a network bridge to use this topology.
- **Logical-In-Path** - The PORTrockIT Node is placed logically in-path between the server and WAN. Routing rules must be set up to ensure that traffic is passed through the Node on the local site.

4.3.3.8 Cancel

Closes the dialog, discarding all current progress.

4.3.3.9 Add Service

Completes the dialog, immediately setting up the service and updating the service list.

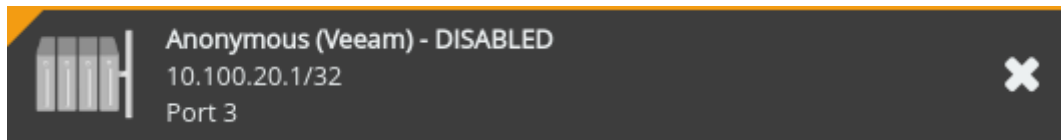
4.3.4 Disabled Services

Disabled services occur due to:

- Modifications to the licences and their association to a network interface

- An active interface, bond, or VLAN being deleted
- An active interface being bonded

If changes are made in this way, any active services that are no longer valid for the new configuration will be marked as disabled.



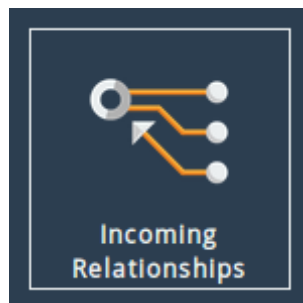
Any associated relationship configurations are immediately removed when a service is disabled resulting in potential disruption of traffic. Equally, it is not possible to activate a relationship using a disabled service.

In order to re-enable the service, the correct interface must be made available and mapped with the corresponding protocol licence as defined by the service listed (see Chapter 5: [Port Mappings](#)). Alternatively, the disabled service can be erased from the configurations (see Section 4.3.2: [Remove Service](#)).

4.4 Incoming Relationships

The *Incoming Relationships* page contains a list of service relationships that have been created by remote nodes.

From the Home screen, select the *Incoming Relationships* icon under the *PORTrockIT* section.



4.4.0.1 Active Incoming Relationships


The page will display a table with all of the currently configured service relationships that have been enabled for this node by remote nodes, as seen below.



For each incoming relationship the following is displayed:

- Node hostname
- Service Protocol
- Service Address
- Number of connections using the service

Some relationships will also show the port ranges the service is configured on.



Note: All connections originating from the same IP address will be displayed as a single connection.

4.4.1 Incoming Relationship

Selecting an *Active Incoming Relationship* on the *Incoming Relationships* page will show the *Incoming Relationship* page.

Dublin

Home

Incoming Relationships

Reboot


Logout

Support

Help

Incoming Relationship: 178.32.62.54 (NetApp SnapMirror)

Nodes



London

178.32.62.9

Online - Active

Connections

From: 17.64.12.18 - 1 Stream	In: 144 MB/s	Out: 212 MB/s
From: 17.64.12.21 - 1 Stream	In: 42 MB/s	Out: 144 MB/s
From: 17.64.13.144 - 1 Stream	In: 2 MB/s	Out: 289 MB/s

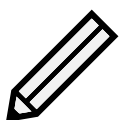
4.4.1.1 Nodes

This section will display the remote node that initiated the service relationship.

4.4.1.2 Connections

This section will show all connections that are currently using this service relationship. For each connection the following is displayed:

- Origin IP Address
- Incoming transfer rate
- Outgoing transfer rate

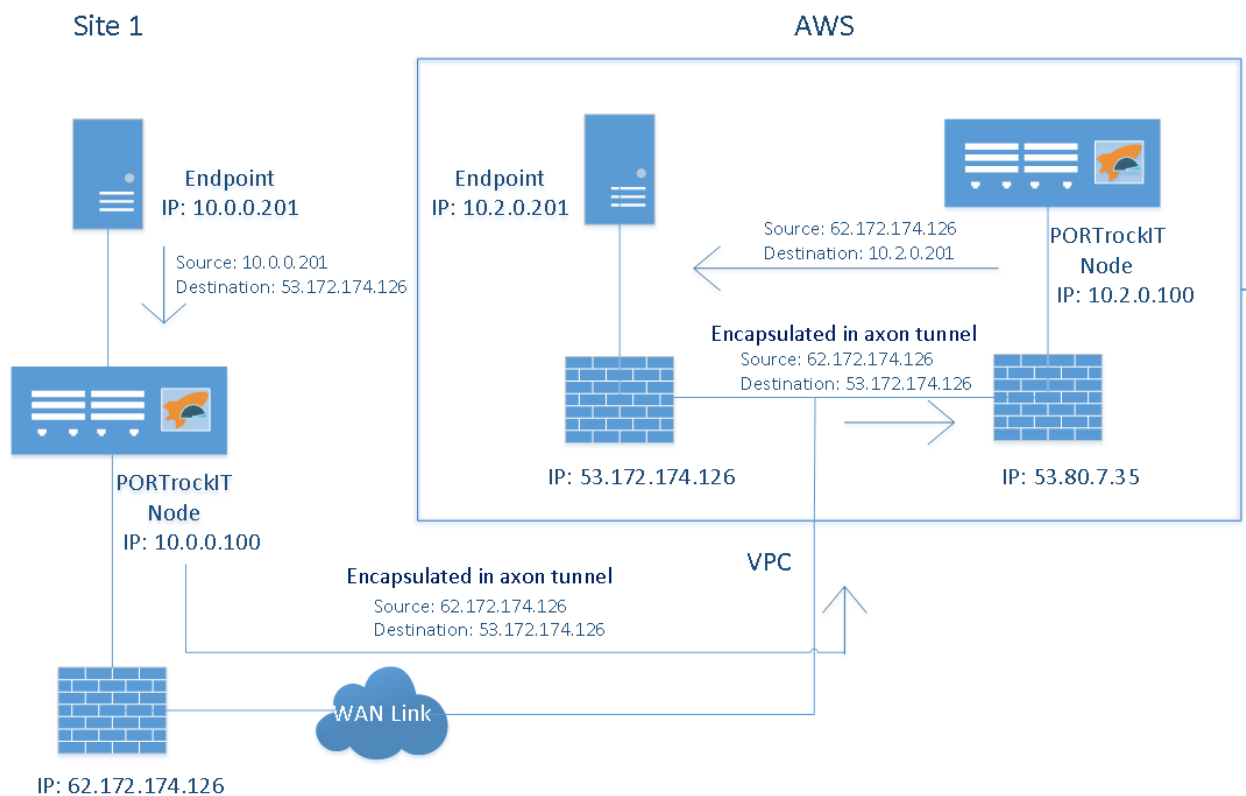


Note: All connections originating from the same IP address will be displayed as a single connection.

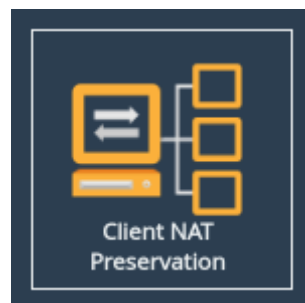
4.5 Client NAT Preservation

Client NAT preservation mappings are used for services that have been previously connected through a NAT, allowing the Endpoints to continue communicating without needing to modify their configuration. They map the Endpoints' old, public IP addresses to their new, private IP addresses.

The following diagram shows how this IP mapping works, demonstrating the source and destination addresses of traffic to be accelerated going between endpoints.



To configure client NAT preservation mappings, click on the *Client NAT Preservation* icon under the *PORTrockIT* section of the Home screen.



The following page will be displayed:

Client NAT Preservation

Node Menu

Home

Reboot

Logout

Support

Help

Client NAT IP Addresses

Private IP address	Public IP address
10.0.0.201	62.172.174.176

Private IP address:

Public IP address:

Add

Remove


Cancel

Save

4.5.1 Client NAT IP Addresses Table

To establish a new mapping, enter the public and private IP pair into the table and click *Add*. Each IP must be a valid IPv4 address and the private IP must be unique.

To delete a listing, select the entry in the *Client NAT IP Addresses* table and then click *Remove*.



Important: Adding or removing entries from the table will not take effect until the *Save* button is clicked.

102

5 Port Mappings

Port Mappings allow you to configure which network ports will have support for which protocols. Navigate to the *Port Mappings* page from the main page of the web interface.



The web interface will display the following:

Port Mappings

Hostname
[Home](#)
[Reboot](#)
[Logout](#)
[Support](#)
[Help](#)

Instructions
Select which protocols should be active on each network interface. After saving changes, reboot the product for the new configuration to take effect.

Licensed Adapters

Feature Type	Limit	Assigned
Management	Unlimited	3
WAN	3	1

Protocols for Port 1:

Management ✕

Add a protocol... ▾

Protocols for Port 2:

Management ✕ WAN ✕

Add a protocol... ▾

Protocols for Port 3:

Management ✕

Add a protocol... ▾

[Cancel](#) [Save](#)

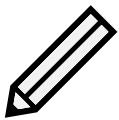
Hardware appliances have dedicated management ports, but can have the Management protocol assigned to additional ports.

Virtual instances will assign the Management protocol to all network ports on first load. The number of ports with the Management protocol assigned can be reduced, but at least one port must have it assigned.

5.1 Setting Port Mappings

To set up protocols on a network port, select an option from the corresponding *Add a protocol...* drop down box.

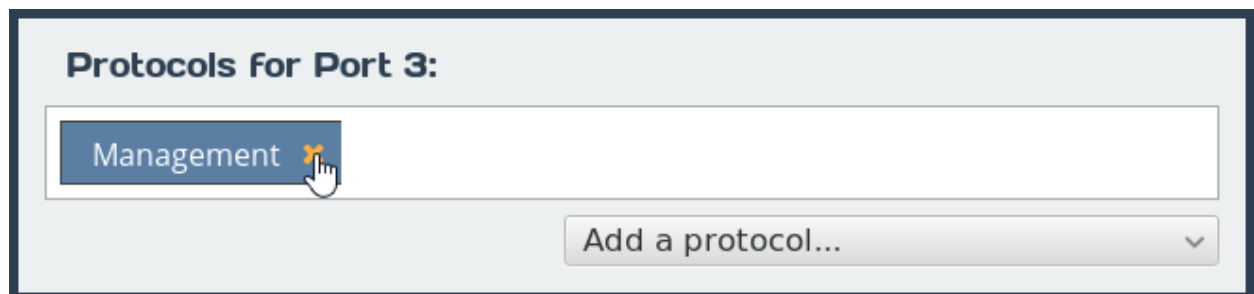
When a protocol has been applied to a port, a blue box corresponding to the protocol will appear under the port.



Note: Hardware appliances will apply some mappings to the PCI slot instead of individual ports, enabling the protocol for all ports on the card in that slot.

5.2 Removing a Port Mapping

To remove a mapping, click on the “X” next to the protocol as shown below.



5.3 Saving Port Mappings

To save the Port Mapping configuration, press the Save button at the bottom of the page. This will return you to the Home screen.



Important: Saving the Port Mappings configuration will require a reboot to take effect.

5.4 Available Port Mappings

Licences are required before mappings can be applied. Licences may have speed restrictions, limiting which ports the licence can be mapped to; these licences have an additional suffix after the

protocol name. An example licence is *WAN 10 Gb* which can only be applied to ports capable of 10Gb speeds. See Section [6.5: Licence Key Management](#) for help managing and uploading new licence keys.

A summary of licences is displayed in the *Licensed Adapters* table.

Provided the matching licences have been purchased and the product has the appropriate cards for the mapping, the following protocols can be added to an available port:



Important: Certain platforms have restrictions on available license mappings.

Management

The Management mapping is required to access the Web interface of the Node, and also allows SSH and SNMP connections.

PORTrockIT TCP Protocols

The list of licences supported by Bridgeworks is updated frequently. Supported licences include Commvault VM Backup and Recovery and Veeam Backup & Replication.

WAN

The WAN port mapping allows this PORTrockIT node to connect to another node.

Please contact Bridgeworks support for a full list of available licences.



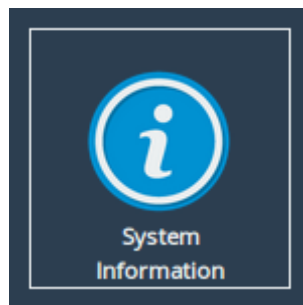
Important: If intending to configure a PORTrockIT protocol in the *Bridged Physically-In-Path* topology, two separate ports will be required; one with the PORTrockIT protocol mapped and the other with WAN mapped.

6 Node Maintenance

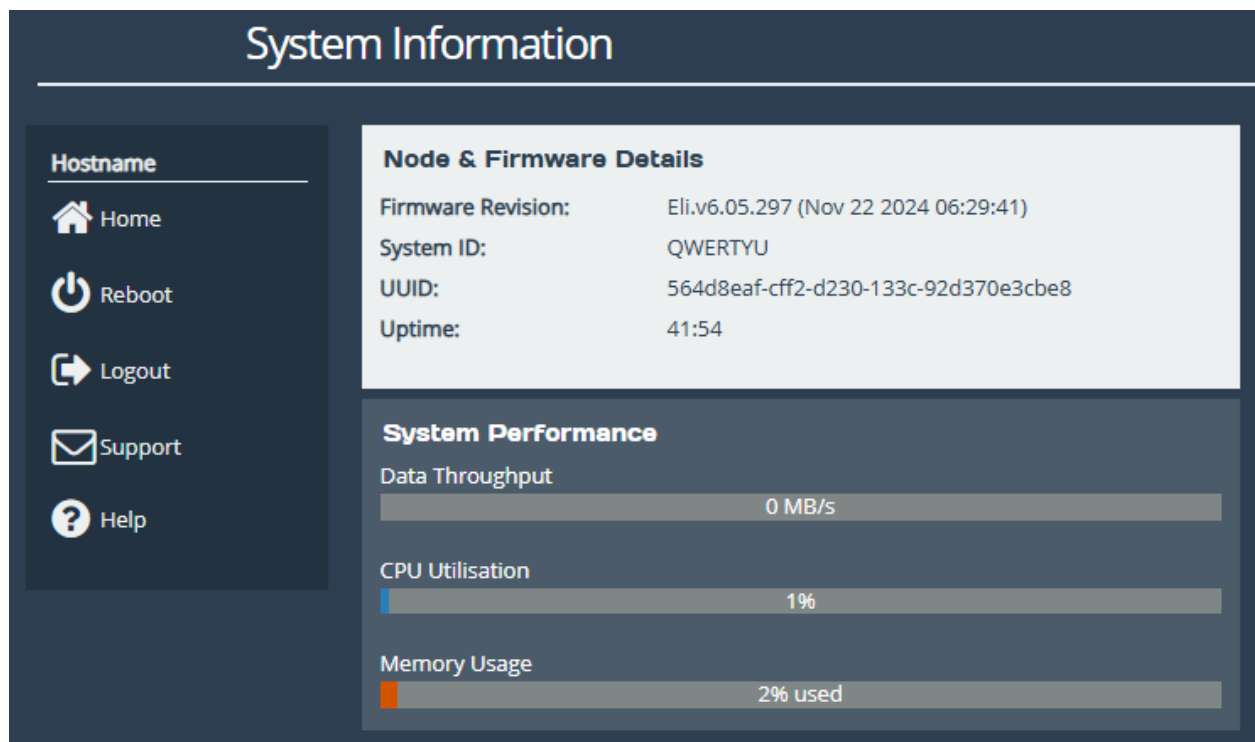
The following section describes the various pages that are available to the administrator to monitor performance and maintain the Node.

6.1 System Information

This page allows the administrator to view the performance of the Node. From the Home screen, select the *System Information* icon from the *Node Maintenance* section.



The following page will be displayed:



In the *Node & Firmware Details* section, the following information is displayed:

Firmware Revision is the installed firmware revision level.

Serial Number/UUID is the unique identifier of that specific PORTrockIT Node.

Uptime is the amount of time the PORTrockIT Node has been powered on for.

The *System Performance* section contains three meters which provide an approximation of the following performance parameters:

Data Throughput This indicates the current performance in MB/s.

CPU Utilisation This indicates the percentage of the time the CPU is occupied undertaking the management and scheduling the transfer of data between the two interfaces.

Memory Usage This indicates the percentage of memory used by all processes.

On hardware appliances, the following section will also appear on this page:

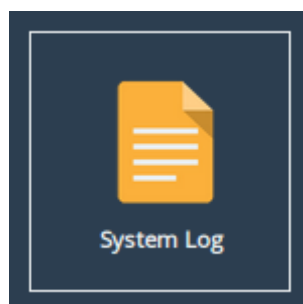
Inventory	
Component	Description
Chassis	Model a004
PCI Slot 1	Intel X540 T2 10 Gigabit Network Connection
PCI Slot 2	Emulex Lancer-G6 LPe31002-M6-D Fibre Channel Host Adapter

The *Inventory* section shows the hardware your Node is running on, including the board and any cards installed in it.

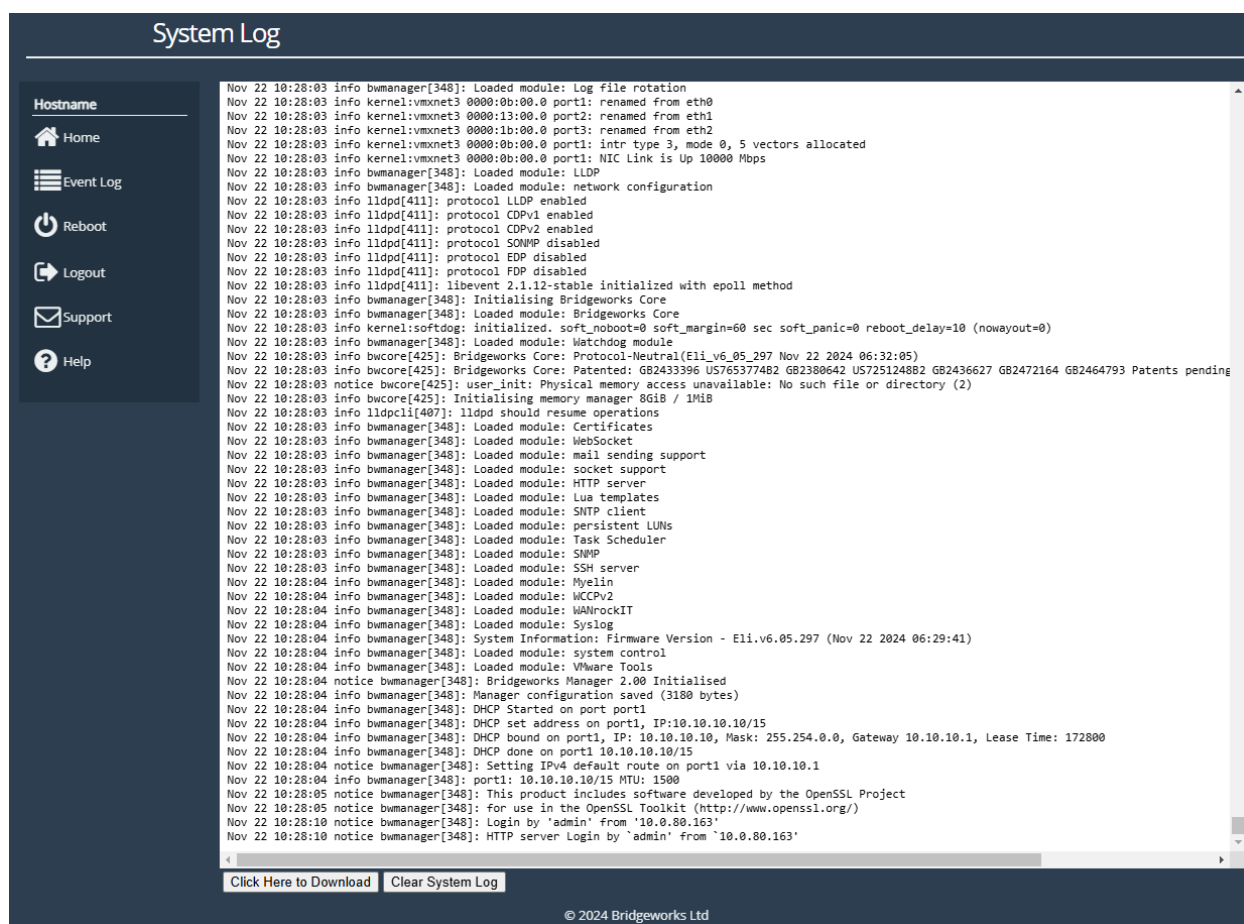
6.2 System Log

This page displays the system log, useful for diagnosing problems with the Node, attached devices and connections.

From the Home screen, select the *System Log* icon from the *Node Maintenance* section.



The web interface will now display the following:



Below the log display pane are two options:

Click Here to Download This will download the log file to your local machine.

Clear System Log This will clear all logs within the Node.

For information on troubleshooting your Node, see Chapter 7: [Troubleshooting](#).

6.3 Load/Save Configuration

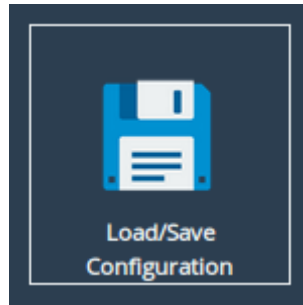


Important: Loading/Saving configuration is unavailable on certain platforms.

The configuration Load/Save feature allows you to save a copy of the Node's configuration to a file and optionally restore back to that configuration at a later time.

Once you have finished configuring your Node we recommend that you save your configuration data to a local disk. By doing so you could save valuable time if the Node requires replacement or if configuration is lost during upgrades.

From the Home screen, select the *Load/Save Configuration* icon from the *Node Maintenance* section.



The following page will be displayed:

Load/Save Configuration

Hostname

- Home
- Reboot
- Logout
- Support
- Help

Import Configuration

! HTTPS and IPsec certificates and keys will need to be restored manually after uploading a saved configuration.

Choose File No file chosen

Upload

Export Configuration


Click Here to Download

Restore Defaults

Restore Factory Defaults

6.3.1 Loading a Saved Configuration

To reload a configuration, click the *Choose file* button and locate the configuration file to upload to the Node. Once located, click the *Upload* button and the new configuration data will be uploaded.



Important: Once a valid configuration file is uploaded, a reboot will automatically occur.

6.3.2 Saving the Configuration to Disk

To save the configuration data, click the *Click Here to Download* button. Then choose to save the file.

The Node will now download an encoded file that contains all of its configuration settings.

109

6.3.3 Restoring to Factory Defaults

To restore the Node to factory defaults, click the *Restore Factory Defaults* button. This resets all configuration parameters including the hostname, IP addresses and passwords. This option is useful to protect sensitive information if a Node appliance is ever returned for maintenance.

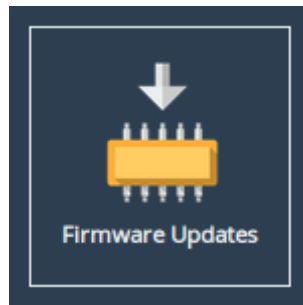


Important: After clicking the *Restore Factory Defaults* button, a reboot will automatically occur.

6.4 Firmware Updates

From time to time it may be necessary to upgrade the firmware within the Node. New versions contain resolutions to known issues as well as new features and improvements to the functionality of the Node.

The *Firmware Updates* page allows the administrator to load new firmware onto the Node. From the Home screen, select the *Firmware Updates* icon from the *Node Maintenance* section.



The following page will be displayed:

Firmware Updates

Hostname

Home

Reboot

Logout

Support

Help

Automatic Firmware Update

Check For Updates Automatically: ☐

Save

Check Now

Note: No information regarding your bridge is sent during the check for firmware updates.

Firmware Upload

Firmware Revision:

Eli.v6.05.207 (Aug 6 2024 06:13:19)

Firmware Image:

Choose file


No file chosen

Update

After clicking update please wait for this page to change before proceeding.


You can now manually upload and update to a firmware version of your choosing.

6.4.1 Updating Firmware Manually



Important: Manual firmware updating is unavailable on Cloud nodes.

Contact Bridgeworks support at support@4bridgeworks.com providing the serial number of your product to receive the latest version of the firmware.



Warning: Do not load on a firmware which has an earlier release revision unless you have been instructed to by the Bridgeworks support team. Always ensure that you have the correct firmware for your product.

If in any doubt, please contact Bridgeworks support. See [Appendix E: Useful Links](#) for contact information.

Once you have downloaded the new firmware to your local machine:

1. Click on the *Choose file* button to locate the file you have downloaded from the Bridgeworks website.
2. Click on the *Update* button to start. A progress bar labelled *Uploading* will appear showing the progress in uploading the new firmware on to the PORTrockIT Node.
3. When the label above the progress bar changes to *Progress*, you can navigate away from this page and the installation will continue.

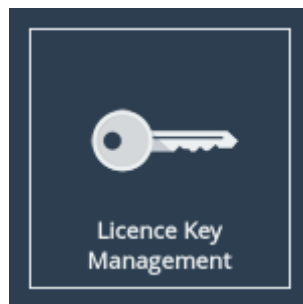
111

Updating the firmware will take a few minutes. After the update is complete, a notification will appear under the *Node Menu*, indicating that a system reboot is necessary. To reboot the Node, click on the *Reboot* button located in the *Node Menu* at the left side of the web interface.

6.5 Licence Key Management

This page allows you to view, upload, download or remove licence keys installed on the Node. Licence keys are required to enable features on installed feature cards. See Chapter 5: [Port Mappings](#) for information on assigning licence keys to interfaces.

From the Home screen, select the *Licence Key Management* icon from the *Node Maintenance* section.



The following page will be displayed:

Licence Keys

Node Menu

- Home
- Reboot
- Logout
- Support
- Help

Installed Licence Keys

ID	Feature Type	Limit	Expires
315953172	Fibre Channel	1	Expired
777490233	Fibre Channel	1	5 Days
2018560049	WAN	8	N/A
	iSCSI	8	
	SAS	8	
2125412457	Fibre Channel	8	N/A

Some of your licence keys have expired. Functionality may be missing from your node as a result. Please remove the expired licence keys.

RemoveDownload

Licence Key Upload

Licence Key File:

Choose file No file chosen

Upload

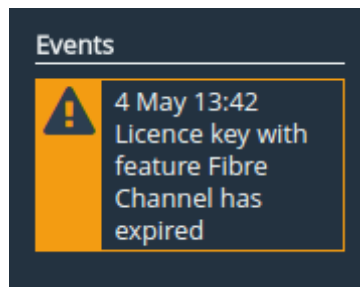
The *Installed Licence Keys* table displays the installed licence keys with the following information:

Feature Type The feature that the licence key enables.

Limit The number of interfaces that the feature may be mapped to.

Expires The amount of time left until a temporary licence key expires. If *N/A* is in this column, it indicates the licence key is not temporary.

When a temporary licence key has expired, there will be a warning on the page and the *Expires* field will say *Expired* as shown in the image above. At the point of expiration, an event will be displayed below the *Node Menu* similar to the one shown below.

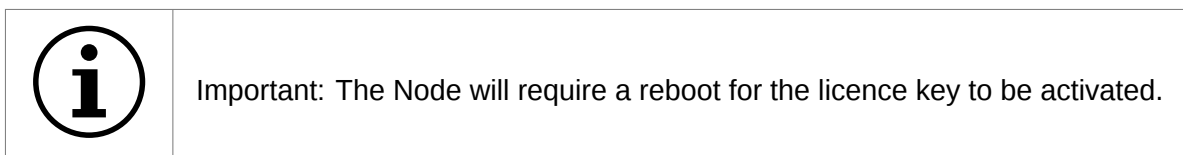


6.5.1 Uploading a Licence Key

To upload a licence key:

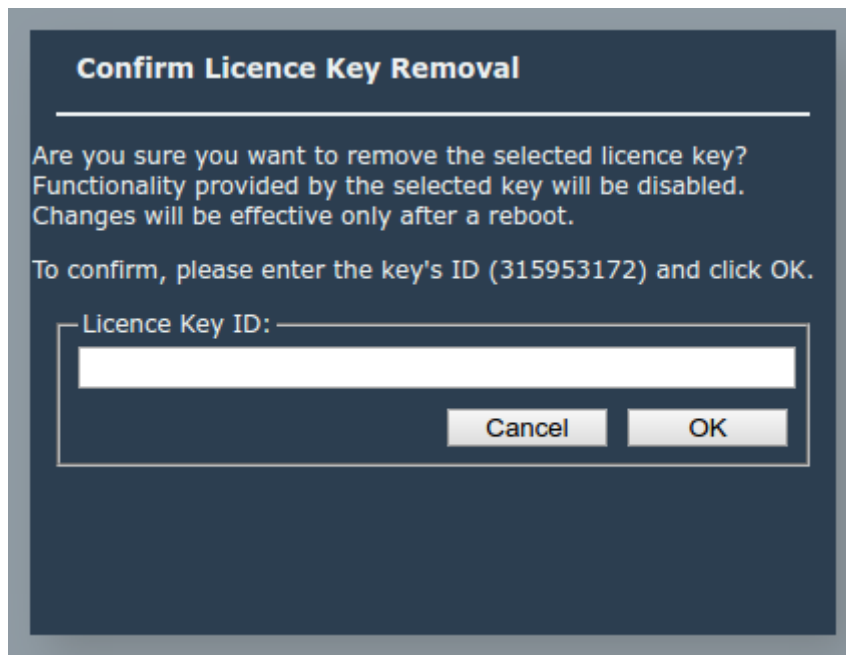
1. Click the *Choose file* button in the *Licence Key Upload* section.
2. Locate and select the licence key to upload.
3. Click the *Upload* button.

After the upload completes, a valid licence key will appear in the *Installed Licence Keys* table.



6.5.2 Removing a Licence Key

To remove a licence key, select the licence key from the *Installed Licence Keys* table, then click the *Remove* button. This will open a dialog box, as shown below.





Copy the licence key ID into the *Licence Key ID* field and click *OK*. The licence key will be removed from the Node and will no longer be displayed in the *Installed Licence Keys* table.

6.5.3 Downloading a Licence Key

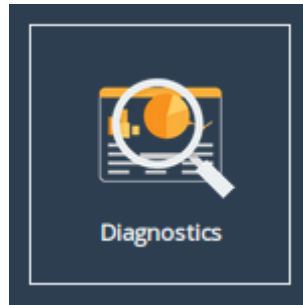
To download a licence key, select the licence key from the *Installed Licence Keys* table, and click *Download*.

6.6 Diagnostics

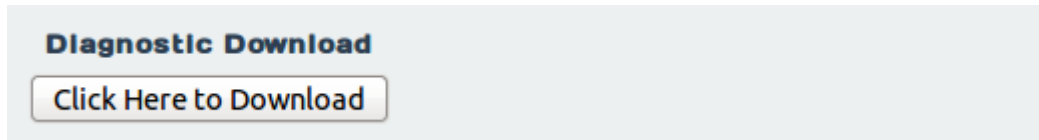
In the unlikely event that a problem arises with your PORTrockIT Node, you may be requested by Bridgeworks Support to provide a diagnostic file.

	<p>Important: If an issue arises with your PORTrockIT Node, check Chapter 7: Troubleshooting for information on how the issue may be resolved.</p>
	<p>Note: The following instructions are demonstrated in the Bridgeworks Support Video "WANrockIT: Downloading Diagnostic Information" found at https://www.youtube.com/watch?v=8RZXFGCy3ZU.</p>

To download the diagnostic file, click on the *Diagnostics* icon on the Home screen:



Then click on the *Click Here to Download* button.



This will cause the PORTrockIT Node to collect data regarding various modules and store them in a single file. Once this process is complete, a download for “diagnostics.bin” will begin.

6.7 Task Scheduler



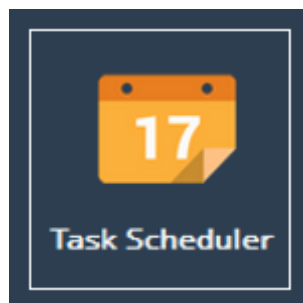
Important: Before configuring the Task Scheduler SNTP must be setup as described in Section [3.3.1: Network Time Protocol \(NTP\)](#).

This page allows the administrator to schedule tasks with the following actions:

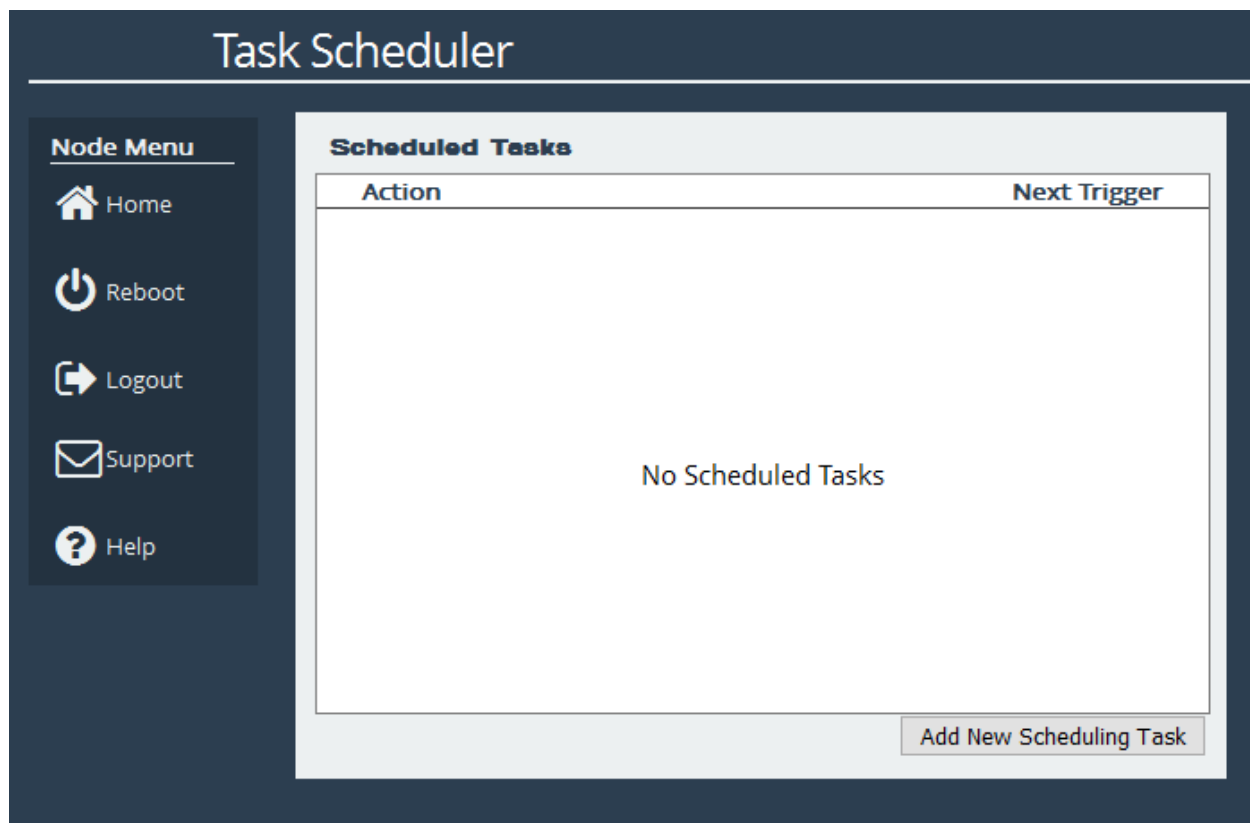
Email Performance Statistics This will email the log of the throughput rate to a given email address(es).

PORTrockIT Bandwidth Limit This will restrict the PORTrockIT transmission rate to a given number of Megabytes per second.

From the Home screen, select the *Task Scheduler* icon from the *Node Maintenance* section.



The web interface will now display the following:

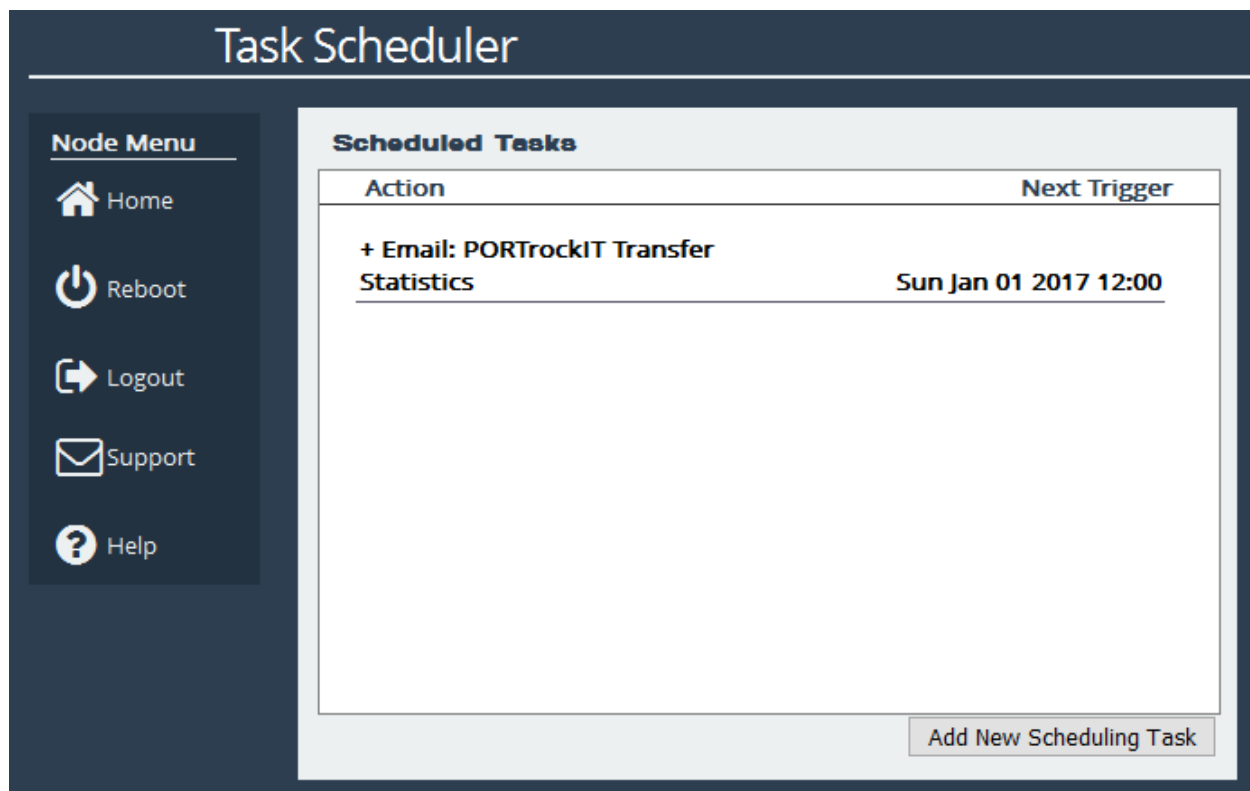


6.7.1 Adding Tasks

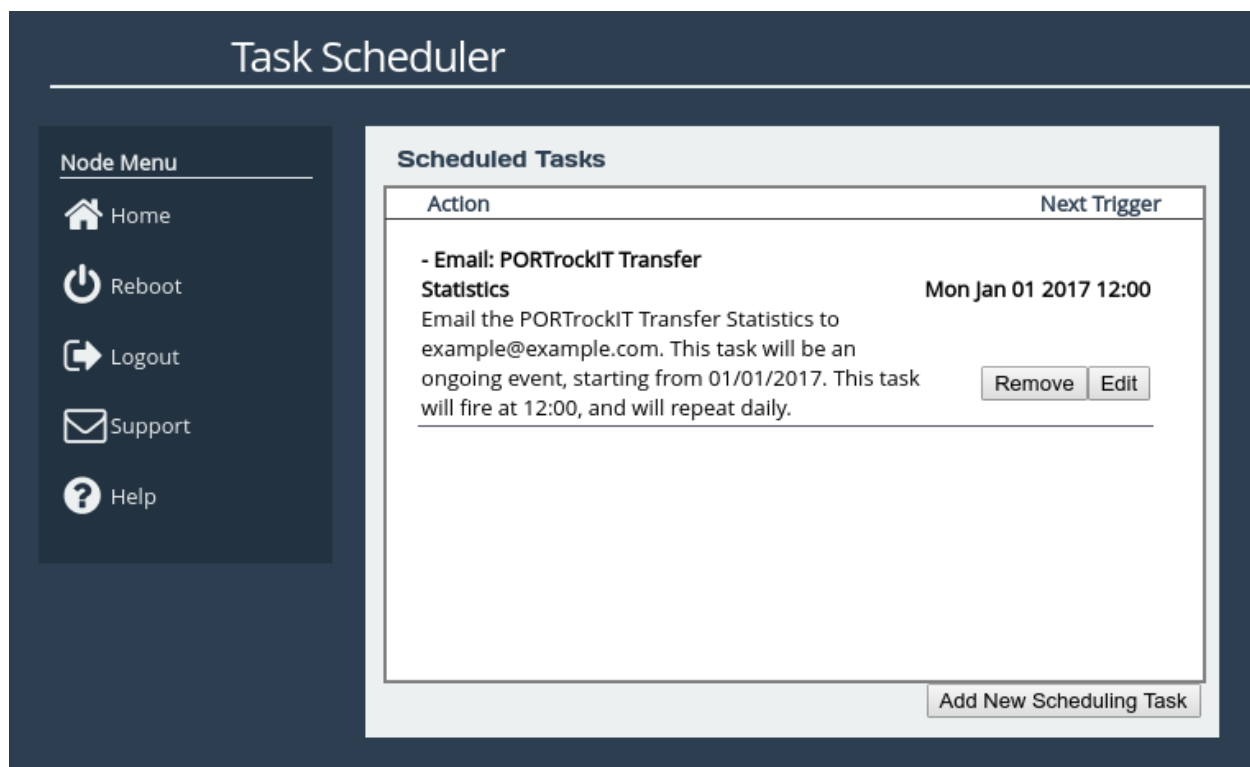
Tasks can be added by clicking on the *Add New Scheduling Task* button, which will start the task wizard.

6.7.2 Removing/Editing Tasks

If you already have some tasks added, they will be listed in the Scheduled Tasks window as shown:



Clicking on a task will expand it as shown:



Clicking the *Remove* button will remove the task from the task scheduler. Clicking the *Edit* button will start the task wizard for the task, allowing it to be edited.

6.7.3 Task Wizard

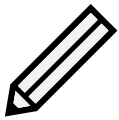
The task wizard will guide you through the adding or editing of scheduled tasks. There are a few common buttons across the individual sections of the wizard:

Help Clicking this button will display the Online Help page for the Task Scheduler.

Cancel Clicking this button will discard the changes being made to the task and close the wizard.

Next If present, this button will navigate you to the next section of the wizard.

Previous If present, this button will navigate you to the previous section of the wizard.



Note: The currently active section of the wizard will be highlighted in orange on the left-hand side.

6.7.3.1 Action - Email Performance Statistics

The screenshot shows the 'Adding New Scheduler Task' wizard. On the left, a vertical list of sections is shown: '1 - Action' (highlighted in orange), '2 - Trigger', '3 - Start Date', '4 - End Date', and '5 - Summary'. The main content area is for the 'Action' section, showing 'Function: Email Performance Statistics' and 'Recipient Email(s):' with an empty text box. At the top right is a 'Help' button, and at the bottom right are 'Next' and 'Cancel' buttons.

On the Action section of the wizard, enter the recipient email(s), separating multiple emails with semi-colons.



Important: If you see the following image, click on the yellow box to be taken to the Service Control page where SMTP can be set up. See Section [3.3.3: Email](#).

Adding New Scheduler Task		Help
1 - Action	Function: Email Performance Statistics ▼	
2 - Trigger	<div>Please setup SMTP Settings before scheduling this function. Click here to take you straight to the setup page.</div>	
3 - Start Date		
4 - End Date		
5 - Summary		
		Next Cancel

6.7.3.2 Action - PORTrockIT Bandwidth Limit

Adding New Scheduler Task		Help
1 - Action	Function: PORTrockIT Bandwidth Limit ▼	
2 - Trigger	PORTrockIT Bandwidth Limit (MB/s): 0	
3 - Start Date	Unlimited Bandwidth: <input type="checkbox"/>	
4 - End Date	Node: All ▼	
5 - Summary		
		Next Cancel

On the Action section of the wizard, enter a bandwidth limit in Megabytes per second to apply a limit or select the *Unlimited Bandwidth* checkbox to remove a limit. Then select which Node and Path should be affected by the bandwidth limit. This limit will remain in place until another task overwrites it.

6.7.3.3 Trigger

Adding New Scheduler Task Help

1 - Action

2 - Trigger

3 - Start Date

4 - End Date

5 - Summary

How often would you like it to trigger? Daily

Previous Next Cancel

On the Trigger section of the wizard, you can pick the frequency of the event. The options are:

Once This means the action will be performed at the specified time and not repeat.

Daily This means the action will be performed every day at the specified time.

Weekly This means the action will be performed on specified days every week at the specified time. When selecting this option, you will be able to pick which days to trigger the action by selecting checkboxes. Each day will have its own checkbox, as shown:

Adding New Scheduler Task Help

1 - Action

2 - Trigger

3 - Start Date

4 - End Date

5 - Summary

How often would you like it to trigger? Weekly

Select days to trigger on:

Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Previous Next Cancel

6.7.3.4 Start Date

The screenshot shows the 'Adding New Scheduler Task' wizard with five steps: 1 - Action, 2 - Trigger, 3 - Start Date (highlighted in orange), 4 - End Date, and 5 - Summary. The main content area displays the instruction 'Please select start date for new task:' and a time input field 'Time for the first trigger:' set to '12:00'. A calendar for October 2019 is shown, with the 8th of the month selected and marked with a red 'X'. The calendar grid is as follows:

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		X	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Below the calendar is a 'Display today' button. At the bottom of the wizard are 'Previous', 'Next', and 'Cancel' buttons.

On the Start Date section of the wizard, you can pick the starting date and time for the new task. Enter a time into the *Time for the first trigger* box and select your start date using the calendar. The selected date will be marked with a red cross.

6.7.3.5 End Date

The screenshot shows the 'Adding New Scheduler Task' wizard with five steps: 1 - Action, 2 - Trigger, 3 - Start Date, 4 - End Date (highlighted in orange), and 5 - Summary. The main content area displays the instruction 'Please select end date for new task:' and a checkbox for 'Ongoing Event' which is checked. A calendar for September 2019 is shown, with the 17th of the month selected. The calendar grid is as follows:

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	2	3	4	5	6	
	9	10	11	12	13	
	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

Below the calendar is a 'Display today' button. At the bottom of the wizard are 'Previous', 'Next', and 'Cancel' buttons.

On the End Date section of the wizard, you can pick the end date for the new task. You can either select the *Ongoing Event* checkbox for a task that should run until cancelled, or select a date using the calendar. The selected date will be marked with a red cross.

6.7.3.6 Summary

The screenshot shows a wizard window titled "Adding New Scheduler Task". On the left is a vertical sidebar with five steps: "1 - Action", "2 - Trigger", "3 - Start Date", "4 - End Date", and "5 - Summary". The "5 - Summary" step is highlighted in orange. The main area of the wizard displays the title "Summary" followed by a description: "Email the PORTrockIT Transfer Statistics to example@example.com. This task will be an ongoing event, starting from 01/10/2019. This task will fire at 12:00, and will repeat daily." At the bottom of the wizard, there are three buttons: "Previous" on the left, "Save" in the center, and "Cancel" on the right. A "Help" button is located in the top right corner of the window.

On the Summary section of the wizard, a brief description of the task will be displayed. If you are happy with this task, click the Save button to add the task to the task scheduler. Saving will automatically close the wizard.

7 Troubleshooting

7.1 Network Connectivity Problems

Under normal operation, you should be able to “ping” the network address of the Node and receive a response. If this fails, run through the following list to identify and solve the problem.

- Ensure the Node is powered on. This can be verified on hardware appliances by checking that the power LED is illuminated.
- Ensure that the Ethernet cable is plugged in at both ends.
- For hardware appliances, ensure the *Link indicator* LED of the Ethernet connector is illuminated. If it is not, check with your Network Administrator. Refer to the *Visual Indicators* appendix within the relevant hardware manual for help identifying the LED.
- If you are using a Node with two Management ports and only one network cable, try using the other network address and/or the other Management port.
- If the Node is transferring large amounts of data, then the response from the web interface may seem slower than usual as the process that controls the web interface has the lowest priority for Network and CPU resources.
- If you can “ping” the Node but the web interface fails to appear, check the settings within the web browser you are using. If you are directly connected to the Node then any proxy settings will require adjustment and may require you to contact your Network Administrator.
- Ensure you are using the correct network address and netmask. See Appendix B: [Accessing the Node from Windows using a static IP Address](#).

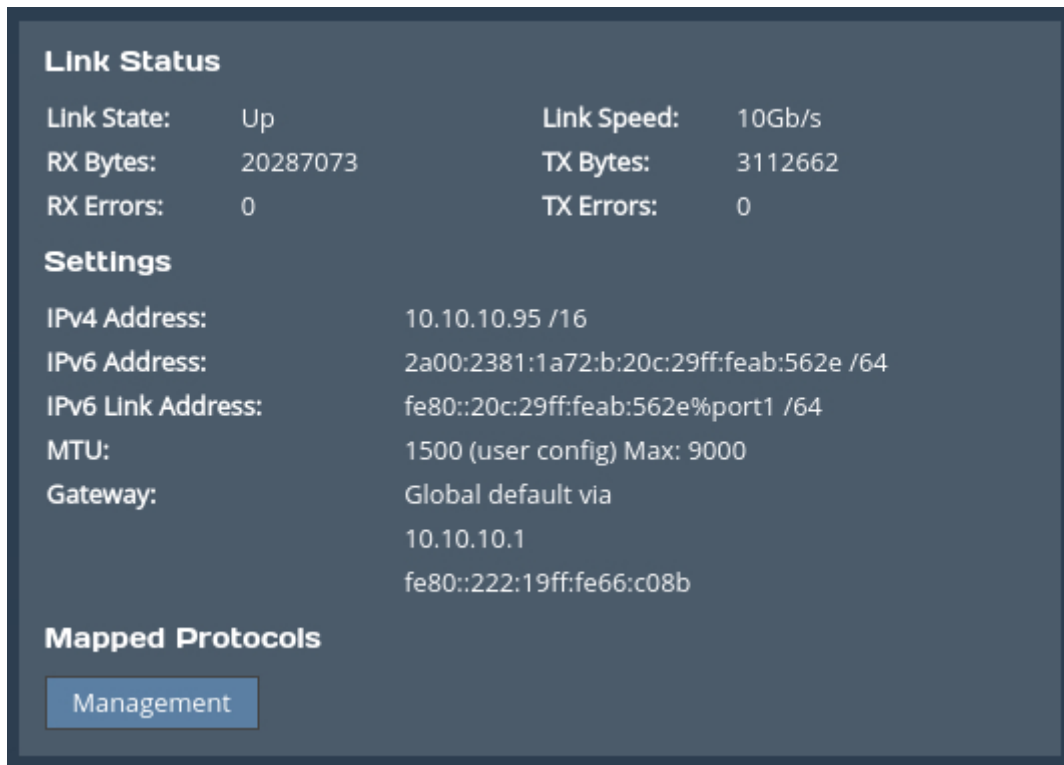
If none of the above resolves your problem, then after consulting with your Network Administrator, please contact support. See Appendix E: [Useful Links](#) for information on how to contact Bridgeworks Support.

7.2 Network Performance Problems

Poor network performance can be caused by many differing reasons. The following list is provided as a guide to where you may find ways to improve performance.

- Ensure that the entire network cabling between the network and the Node is of the correct standard.
- Ensure your network and Node are communicating at the fastest possible network speed. Current link speeds can be found next to each interface on the *Network Connections* page. The link speed should be *1000Mb/s* on a 1 Gigabit network link. If it is 10 or 100Mb/s, this will limit the performance dramatically. See Section 3.1: [Network Connections](#) for help finding the *Network Connections* page.
- Packet loss can be a cause of poor performance. Within the *Link Status Box* check the number of TX and RX errors for relevant network interfaces that are displayed on each *Network Port*

page. This should be zero or a very small number. If these are showing large numbers of errors, check the connections between the Node and the network. See Section [3.1.8: Port Settings](#) for help finding the *Network Port* page.



The screenshot displays a network configuration interface with three main sections: Link Status, Settings, and Mapped Protocols. The Link Status section shows the link is up at 10Gb/s with no errors. The Settings section lists IPv4 and IPv6 addresses, MTU, and gateway information. The Mapped Protocols section has a 'Management' button.

Link Status	
Link State:	Up
RX Bytes:	20287073
RX Errors:	0
Link Speed:	10Gb/s
TX Bytes:	3112662
TX Errors:	0

Settings	
IPv4 Address:	10.10.10.95 /16
IPv6 Address:	2a00:2381:1a72:b:20c:29ff:feab:562e /64
IPv6 Link Address:	fe80::20c:29ff:feab:562e%port1 /64
MTU:	1500 (user config) Max: 9000
Gateway:	Global default via 10.10.10.1 fe80::222:19ff:fe66:c08b

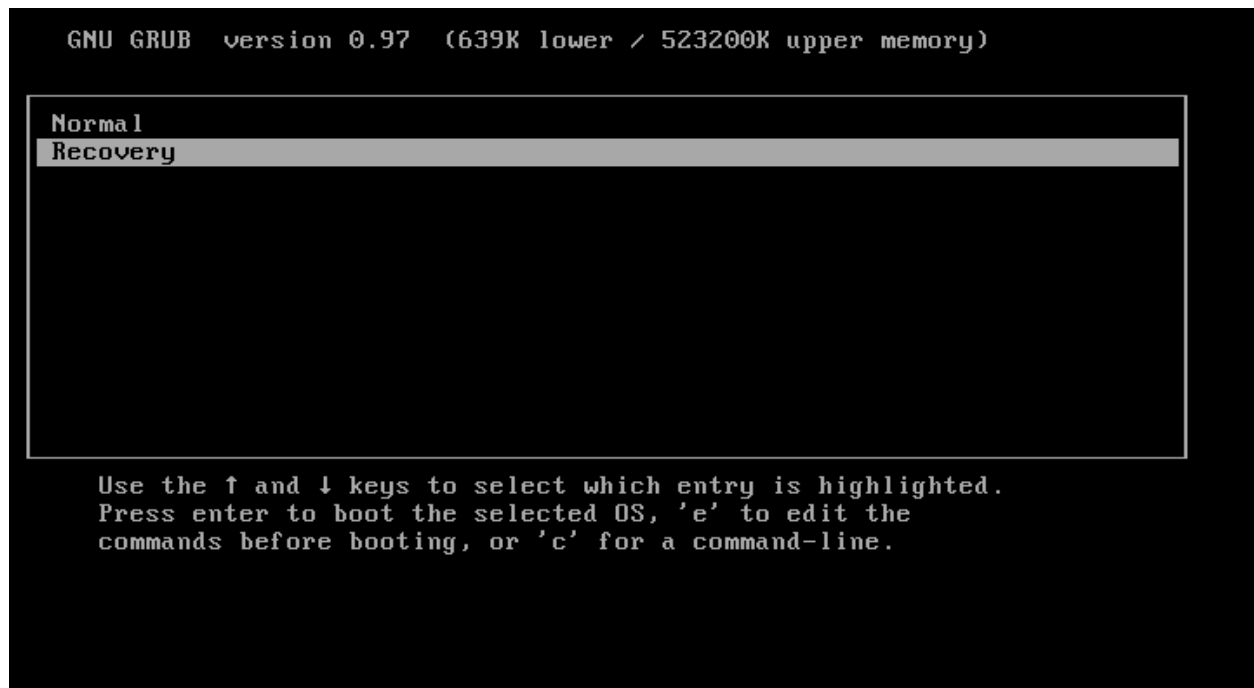
Mapped Protocols	
<button>Management</button>	

If none of the above resolves your problem, then after consulting with your Network Administrator, please contact support. See Appendix [E: Useful Links](#) for information on how to contact Bridgeworks Support.

7.3 Recovery Wizard

If access to the system is being disrupted because of problems with the configuration file then, in consultation with Bridgeworks support, the following procedures can be used to recover your system.

To access the Recovery Wizard press the *Esc* key during the unit's boot sequence as soon as you see the message "GRUB loading, please wait..." Select the *Recovery* option on the menu that follows.



The Recovery Wizard provides two options for system recovery: restoring your unit to factory defaults, and deleting your configuration file.

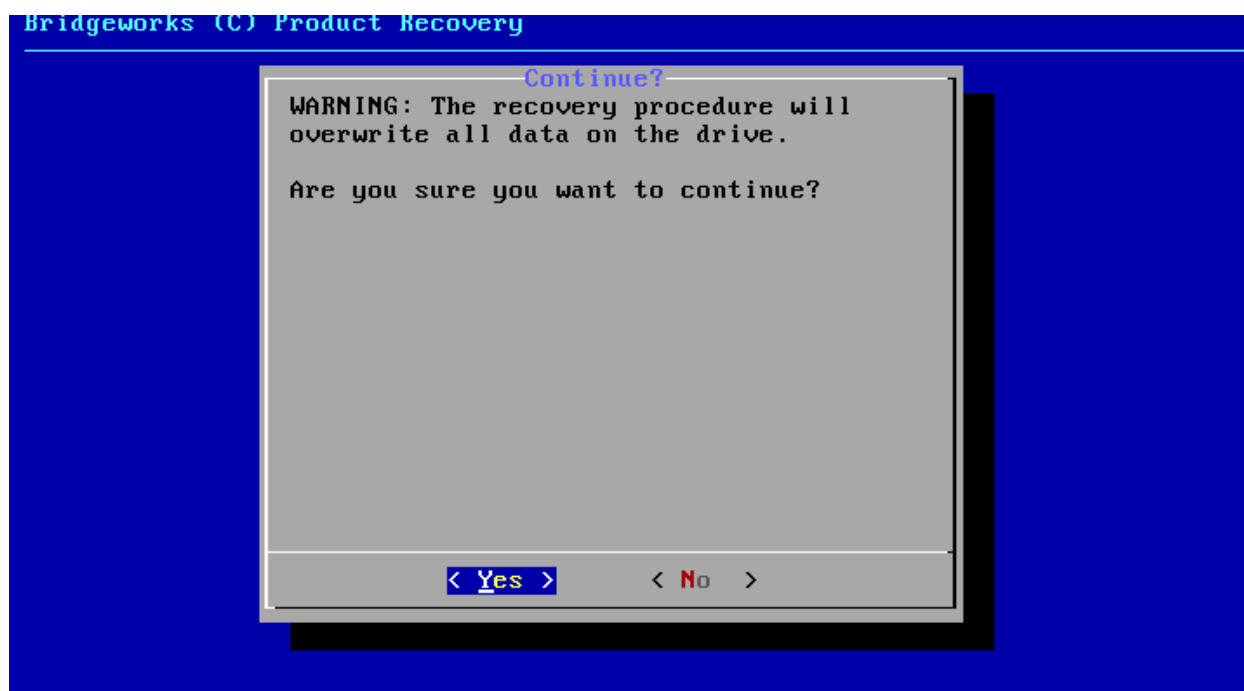
7.3.1 Factory Restore

This option will restore your unit to its factory defaults, removing any current configuration on your system including your current firmware and licence keys.

To restore your unit to defaults, ensure that the *Factory Restore* option is highlighted in the Recovery Wizard menu and press the *Space Bar* to select it. Press the *Enter* key to start the factory restore process.



This procedure cannot be undone once complete; only continue if you are sure that you wish to do so. You will be asked to confirm that you wish to proceed. Choosing Yes will restore your unit to defaults and No will exit the Recovery Wizard menu and drop to the shell.



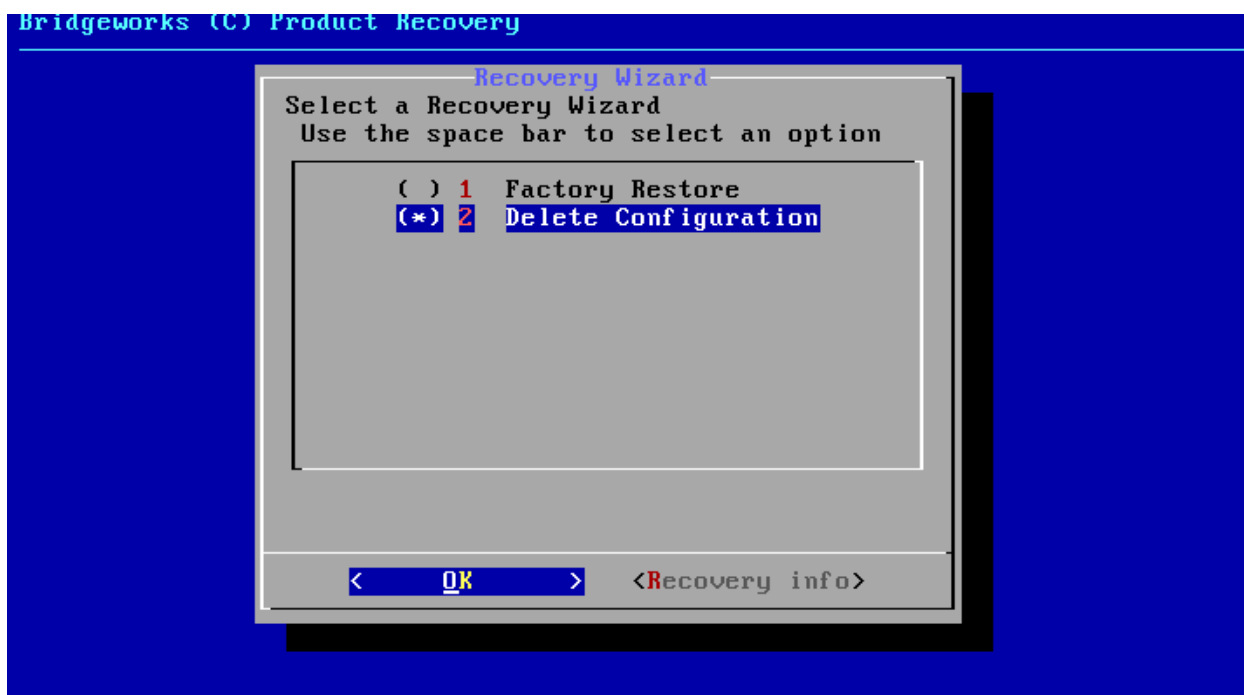
Once the factory restore procedure has completed successfully you will need to reboot your system.



7.3.2 Delete Configuration

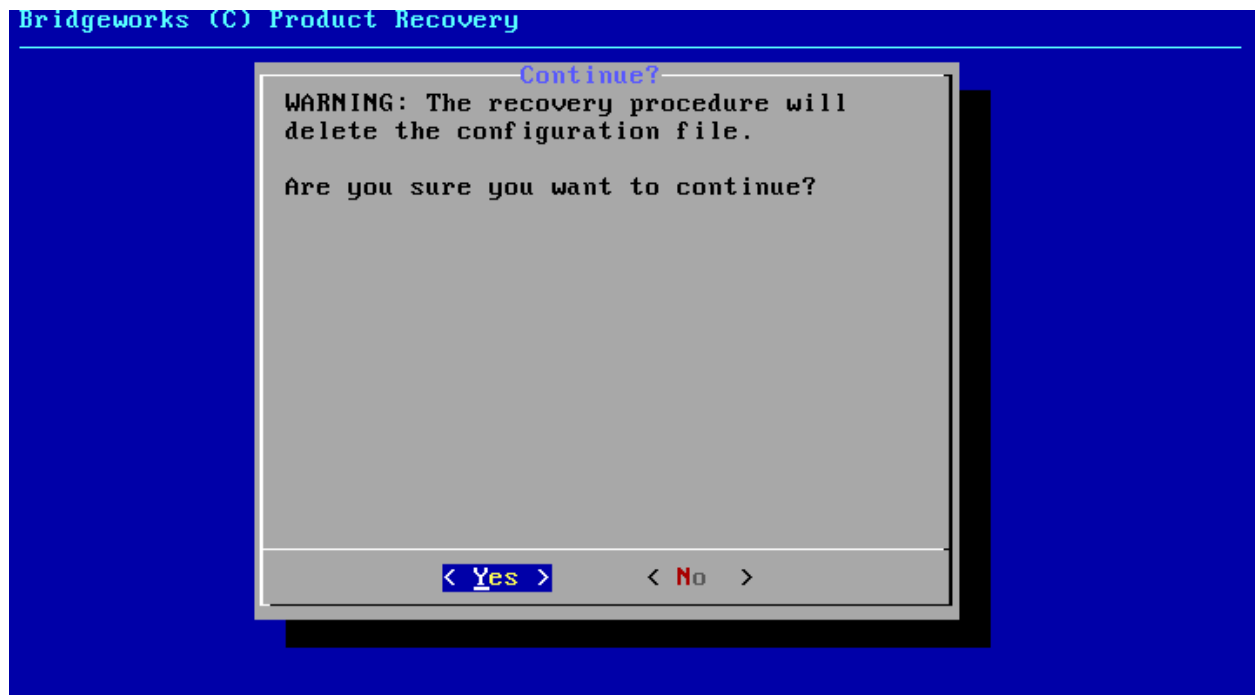
This option will delete your configuration file, removing any current configuration on your system but keeping your current firmware and licence keys.

To delete your configuration file, ensure that the *Delete Configuration* option is highlighted in the Recovery Wizard menu and press the *Space Bar* to select it. Press the *Enter* key to start the deletion process.

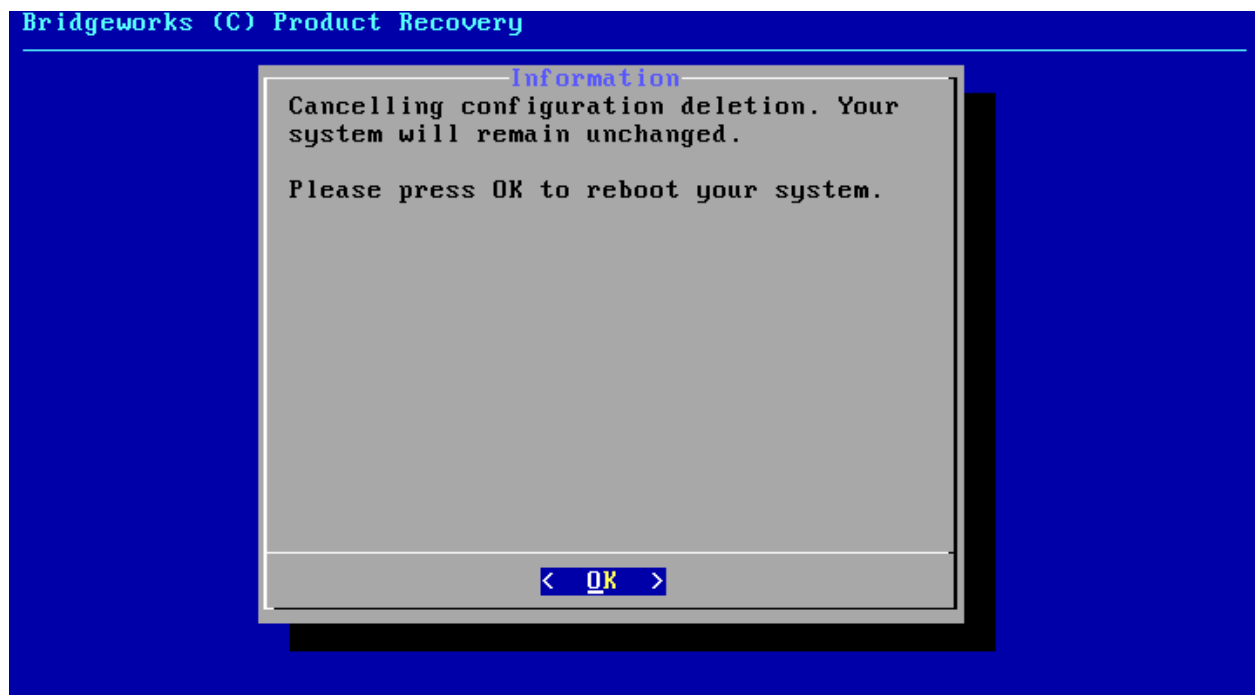


This procedure cannot be undone once complete; only continue if you are sure that you wish

to do so. You will be asked to confirm that you wish to proceed. Choosing Yes will delete your configuration file and No will cancel the configuration deletion wizard.

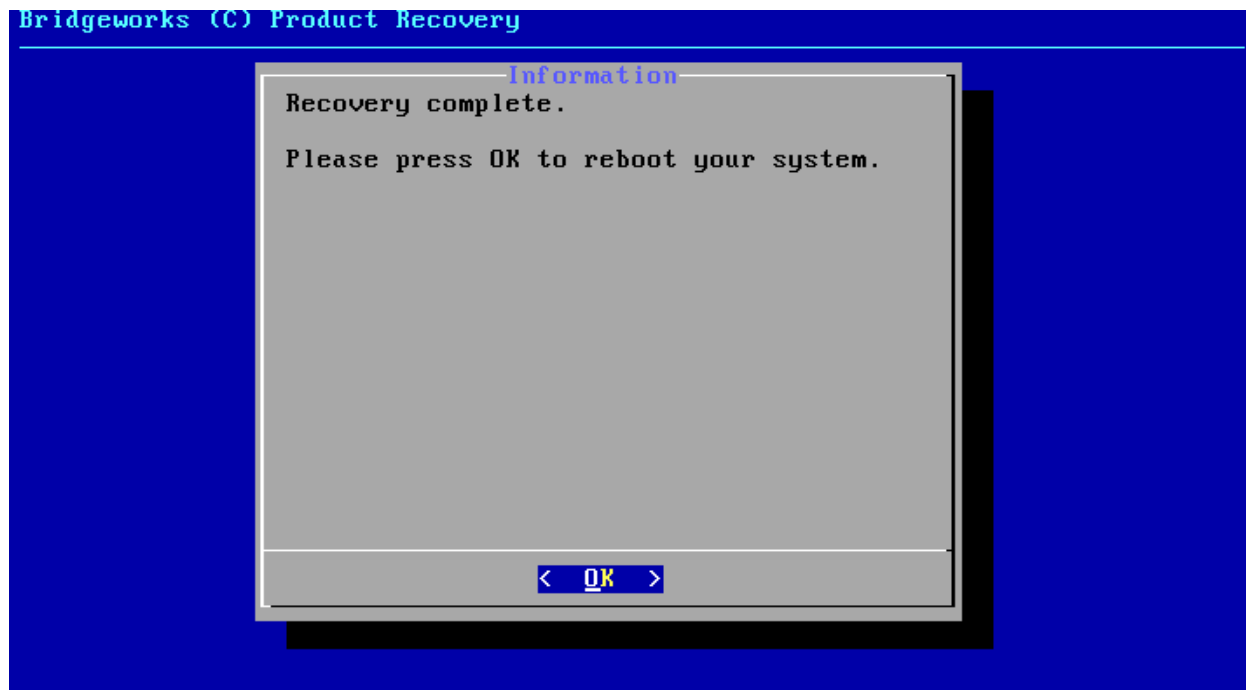


If you cancel the deletion wizard at this point nothing on your system will be affected.



Once the delete configuration procedure has completed successfully you will need to reboot your system.

Bridgeworks (C) Product Recovery



When the Recovery Wizard completes and you connect to the web interface of your unit, it will be reset to its original configuration. For help re-establishing your setup see [Section 2.2: Connecting to the Web Interface](#).

Appendix A: IP Protocols and Port Numbers

For the Node to be able to communicate with other network hosts, it may be necessary to contact your network administrator to ensure that the required IP protocols & port numbers are available.

A.1 Inbound LAN Protocols and Port Numbers

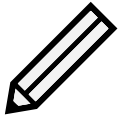
Protocol/Port	Name	Description
TCP 22	SSH	Required to access the configuration console through management interfaces when SSH is enabled. See Section 3.2.5: Secure Shell (SSH) .
TCP 80	HTTP	Required to access the web interface through management interfaces when HTTP is enabled.
TCP 443	HTTPS	Required to access the web interface through management interfaces when HTTPS is enabled.
TCP 8002		Required to access the remote web interface using Remote Control when HTTP is enabled on the controlling Node. See Section 4.2.16: Remote Control .
TCP 8082		Required to access the remote web interface using Remote Control when HTTPS is enabled on the controlling Node.
UDP 161	SNMP	Required for management interfaces to respond to Simple Network Management Protocol requests, see Section 3.3.2: Simple Network Management Protocol (SNMP) .

A.2 Outbound LAN Protocols and Port Numbers

Protocol/Port	Name	Description
TCP 25	SMTP	Simple Mail Transfer Protocol, see Section 3.3.3: Email .
UDP 123	NTP	Network Time Protocol, see Section 3.3.1: Network Time Protocol (NTP) .
UDP 2048	WCCP	Web Cache Communication Protocol. Allows accelerated traffic between nodes without endpoint configuration, see Section 4.2.15: WCCPv2 .
ICMP		Internet Control Message Protocol. Required by dead gateway detection (see Section 3.1.3.5: Dead Gateway Detection) and network debugging tools (see Section 3.1.7: Network Tools).

A.3 WAN Protocols and Port Numbers

Protocol/Port	Name	Description
TCP 16665	axon-tunnel	Reliable multipath data transport for high latencies
UDP 4500	ipsec-nat-t	IPsec NAT-Traversal
UDP 500	isakmp	Internet Security Association and Key Management Protocol
ESP		IP Encapsulating Security Payload



Note: Only TCP Port 16665 is required if not using IPsec encryption or VPN functionality on the PORTrockIT product.

A.4 PORTrockIT TCP Port Numbers

Depending on the licences being used on the device, different TCP ports will need to be open for communication between the PORTrockIT Node and local Endpoint.

A.4.1 Caringo Swarm Object Storage

TCP Port/range	Description
80	Caringo Swarm Communication and Data Transfer

A.4.2 Commvault VM Backup and Recovery

TCP Port/range	Description
8400	Commvault Communications Service (GxCVD)
8401	Commvault Server Event Manager (GxEvMgrS)
8402	Commvault Client Event Manager (GxEvMgrC)
8403	Commvault Tunnel Communication
8408	Commvault CommServe Communication
32768 - 65535	IANA standard Ephemeral port range

A.4.3 HTTP

TCP Port/range	Description
80	HTTP data transfer

A.4.4 HTTPS

TCP Port/range	Description
443	HTTPS data transfer

A.4.5 IBM Spectrum Protect

TCP Port/range	Description
1500	Inbound Client, server, admin
1501	Classic Scheduler listener for PROMPTED
1581	Web Client Listener

A.4.6 NetApp SnapMirror

TCP Port/range	Description
10565 - 10569	NetApp Data Transfer
11104	NetApp Intercluster Communication
11105	NetApp Intercluster Data Transfer

A.4.7 NetApp StorageGRID Client

TCP Port/range	Description
8082	S3-related external traffic to API Gateway Nodes (HTTPS)
8083	Swift-related external traffic to API Gateway Nodes (HTTPS)
8084	S3-related external traffic to API Gateway Nodes (HTTPS)
8085	Swift-related external traffic to API Gateway Nodes (HTTPS)
18082	S3-related external traffic to Storage Nodes (HTTPS)
18083	Swift-related external traffic to Storage Nodes (HTTPS)
18084	S3-related external traffic to Storage Nodes (HTTPS)
18085	Swift-related external traffic to Storage Nodes (HTTPS)

A.4.8 NetApp StorageGRID Combined

TCP Port/range	Description
1139	LDR replication
1501	ADC service connection
1502	LDR service connection
1503	CMS service connection
1506	SSM service connection
1509	ARC service connection
1511	DDS service connection
7000	Cassandra inter-node cluster communication
7001	Cassandra SSL inter-node cluster communication
8082	S3-related external traffic to API Gateway Nodes (HTTPS)
8083	Swift-related external traffic to API Gateway Nodes (HTTPS)
8084	S3-related external traffic to API Gateway Nodes (HTTPS)
8085	Swift-related external traffic to API Gateway Nodes (HTTPS)
9042	Cassandra CQL Native Transport Port
9080	Used by all grid nodes to communicate with the primary Admin Node to coordinate when services are started
9081	StorageGRID Webscale Installer
9999	Metrics exporter
11139	ARC replication
18000	Account service connection
18001	Identity service connection
18002	Internal HTTP API connections from Admin Nodes and other Storage Nodes
18003	Platform services configuration service connections from Admin Nodes and other Storage Nodes
18017	Used for internal HTTPS communications among Storage Nodes and between Storage Nodes and Admin Nodes
18080	HTTP query/retrieve and ingest
18082	S3-related external traffic to Storage Nodes (HTTPS)
18083	Swift-related external traffic to Storage Nodes (HTTPS)
18084	S3-related external traffic to Storage Nodes (HTTPS)
18085	Swift-related external traffic to Storage Nodes (HTTPS)
18200	Additional statistics about client requests
19000	Keystone service internal traffic

A.4.9 NetApp StorageGRID Intercluster

TCP Port/range	Description
1139	LDR replication
1501	ADC service connection
1502	LDR service connection
1503	CMS service connection
1506	SSM service connection
1509	ARC service connection
1511	DDS service connection
7000	Cassandra inter-node cluster communication
7001	Cassandra SSL inter-node cluster communication
9042	Cassandra CQL Native Transport Port
9080	Used by all grid nodes to communicate with the primary Admin Node to coordinate when services are started
9081	StorageGRID Webscale Installer
9999	Metrics exporter
11139	ARC replication
18000	Account service connection
18001	Identity service connection
18002	Internal HTTP API connections from Admin Nodes and other Storage Nodes
18003	Platform services configuration service connections from Admin Nodes and other Storage Nodes
18017	Used for internal HTTPS communications among Storage Nodes and between Storage Nodes and Admin Nodes
18080	HTTP query/retrieve and ingest
18082	S3-related external traffic to Storage Nodes (HTTPS)
18200	Additional statistics about client requests
19000	Keystone service internal traffic

A.4.10 NFS

TCP Port/range	Description
111	NFS Service
2049	NFS Service

A.4.11 PeerGFS

TCP Port/range	Description
61616	PeerGFS data transfer
61617	PeerGFS encrypted data transfer

A.4.12 S3

TCP Port/range	Description
80	S3 data transfer
443	S3 encrypted data transfer

A.4.13 SecuritEase

TCP Port/range	Description
80	
443	
12000	
12001	

A.4.14 Veeam Backup & Replication

TCP Port/range	Description
902	Veeam Data Transmission to ESXi
2500 - 5000	Veeam Data Transmission
6160	Veeam Installer Service
6161	Veeam vPower NFS Service
6162	Veeam Data Mover Service

A.4.15 Veritas NetBackup

TCP Port/range	Description
1556	Symantec Private Branch Exchange Service
10082	NetBackup Deduplication Engine (spold)
10102	NetBackup Deduplication Manager (spad)
13722	Authorization Service (nbazd)
13724	NetBackup Network Service
13783	Authentication Service (nbatd)

A.4.16 WANdisco Fusion

TCP Port/range	Description
7000 - 7999	Data Transfer between Fusion Server and IHC servers
9000 - 9999	HTTP server that exposes JMX metrics from IHC servers

A.4.17 Web

TCP Port/range	Description
80	HTTP data transfer
443	HTTPS data transfer

Appendix B: Accessing the Node from Windows using a static IP Address

This appendix describes how to configure a Windows host to access the Node's web interface from its default static IP address, if DHCP is not enabled on the Node.

These instructions apply to Windows Vista, 7, 8, 10 and to Windows Server 2008, 2012, 2016, 2019 and their respective R2 versions.



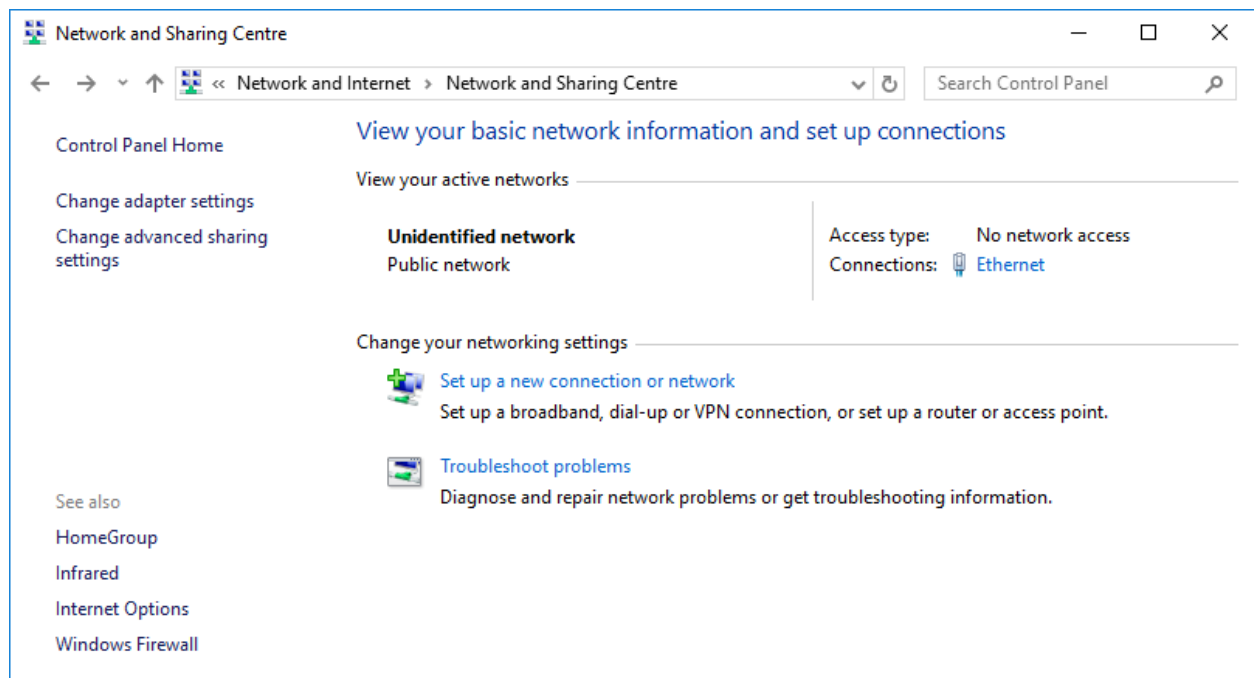
Warning: Administrative privileges may be required to modify network device settings.

From the Start menu, select *Control Panel*.

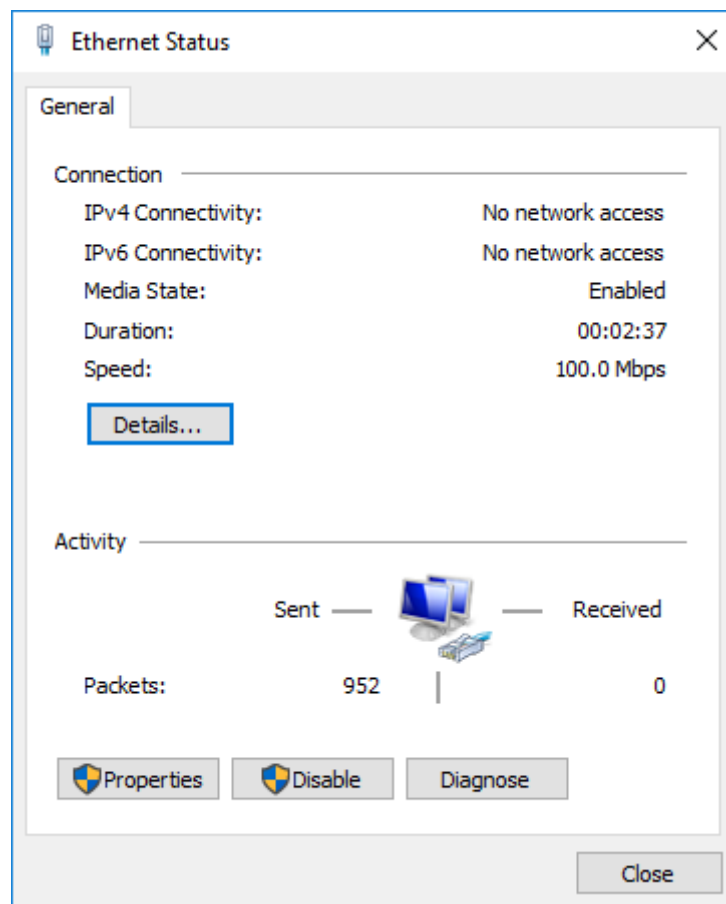


Important: It may be required to search for "Control Panel" in the Start menu before it appears as an entry.

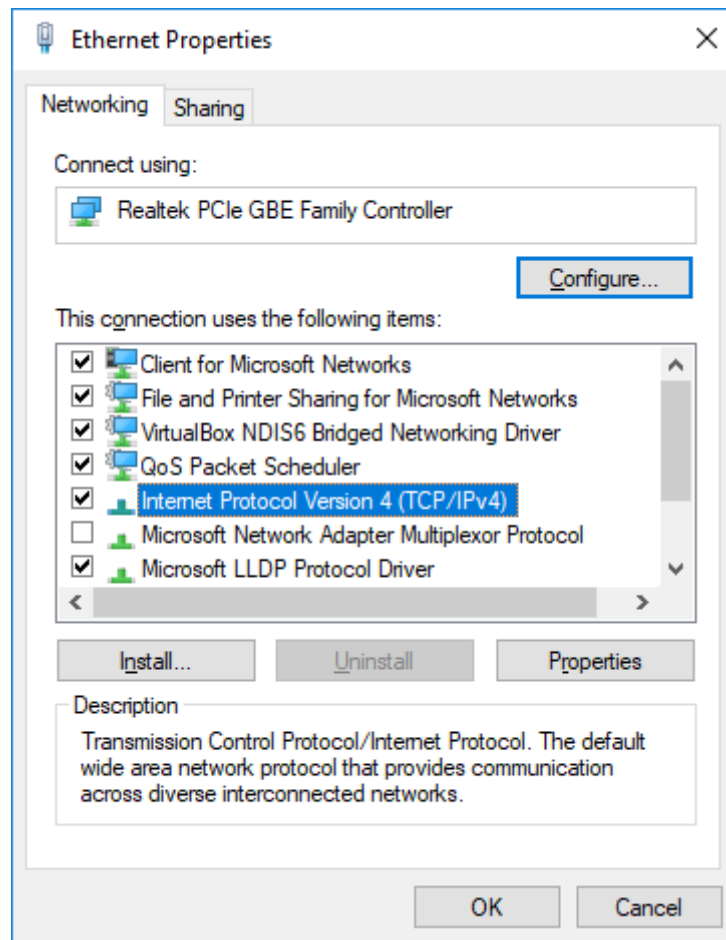
From the Control Panel select the *Network and Internet* link, followed by the *Network and Sharing Centre* link. Click on the link next to "Connections" for your respective network. This is named "Ethernet" in the screenshot below.



A general status page will be displayed. From within this page select *Properties*.

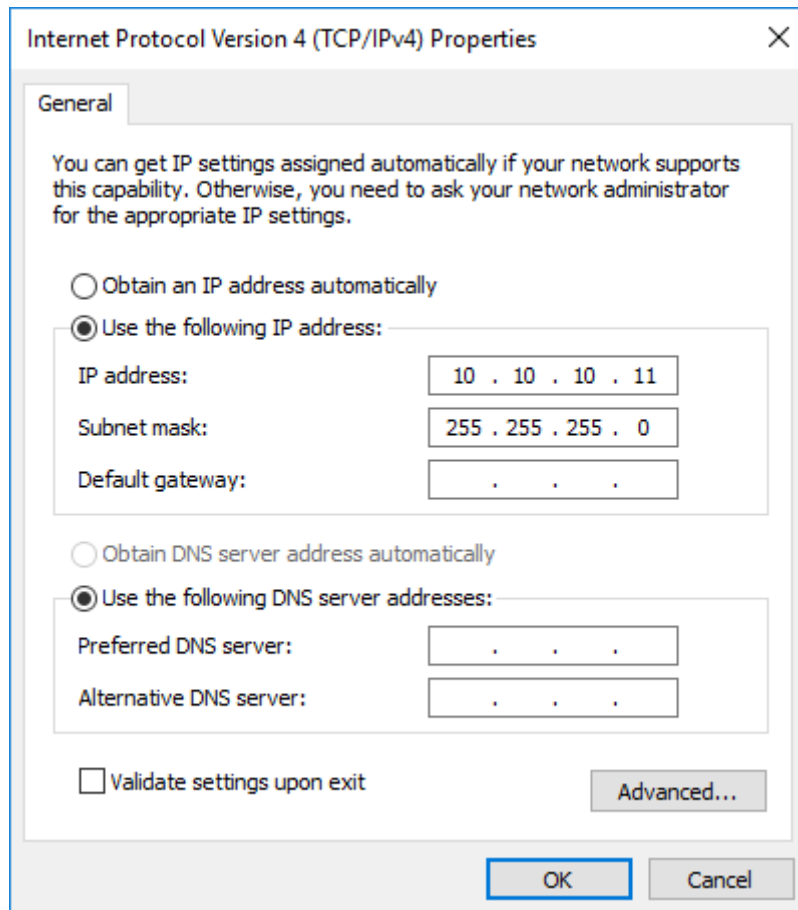


Select the *Internet Protocol Version 4 (TCP/IPv4)* entry and then *Properties*.



Before continuing, make a note of your current configuration as it will be modified. Afterwards,

1. Click *Use the following IP Address*.
2. Enter *10.10.10.11* into the *IP Address* field.
3. Enter *255.255.255.0* into the *Subnet Mask* field.
4. Finally click the *OK* button.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 10 . 10 . 10 . 11

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternative DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel



Note: Once you have completed the initial set up of the Node, return your computer to the original settings and reconnect to the Node.

Appendix C: PORTrockIT Series Comparisons

C.1 Node Limits

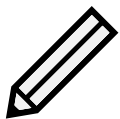
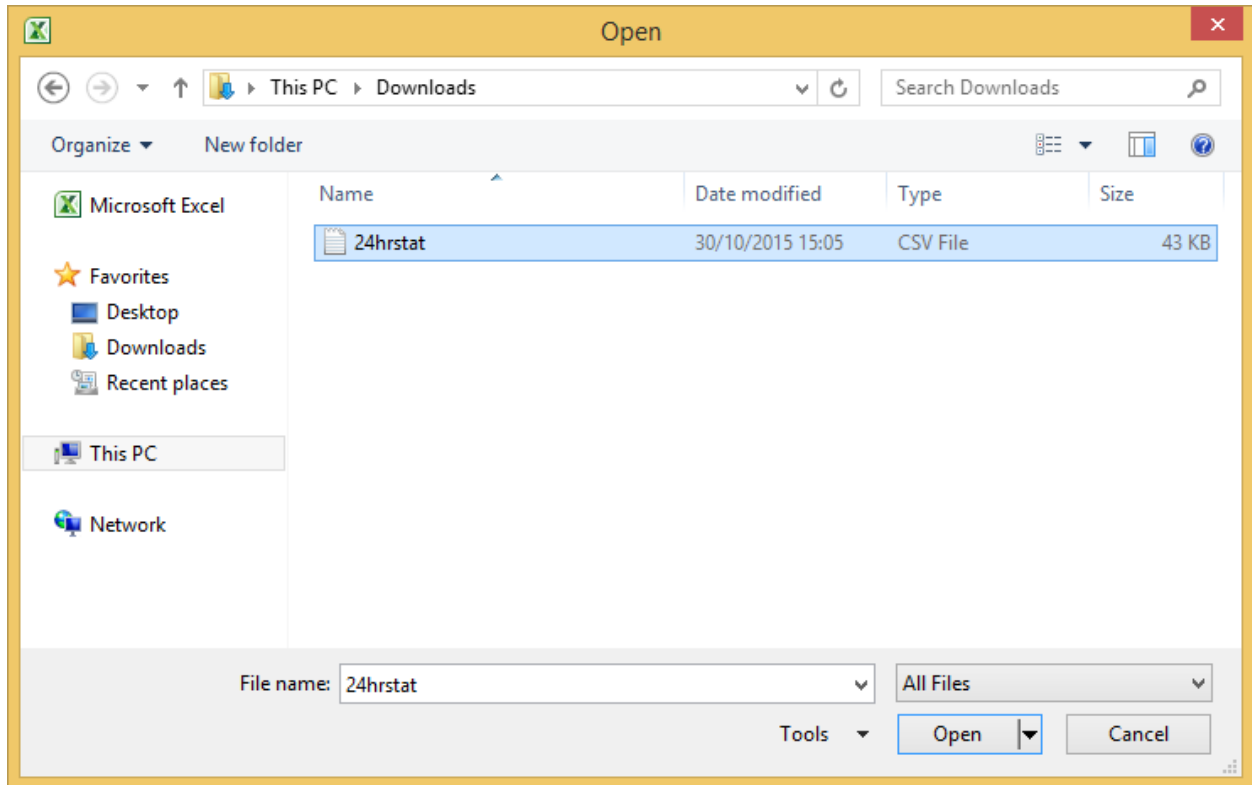
Series	Bandwidth	Maximum Connected Nodes
50	500 Mb/s	1
100	1 Gb/s	1
200	2 Gb/s	4
400	10 Gb/s	10
600	20 Gb/s	20

Bandwidth The bandwidth limit applied to accelerated transfers.

Maximum Connected Nodes The maximum number of Nodes that a Node may connect to.

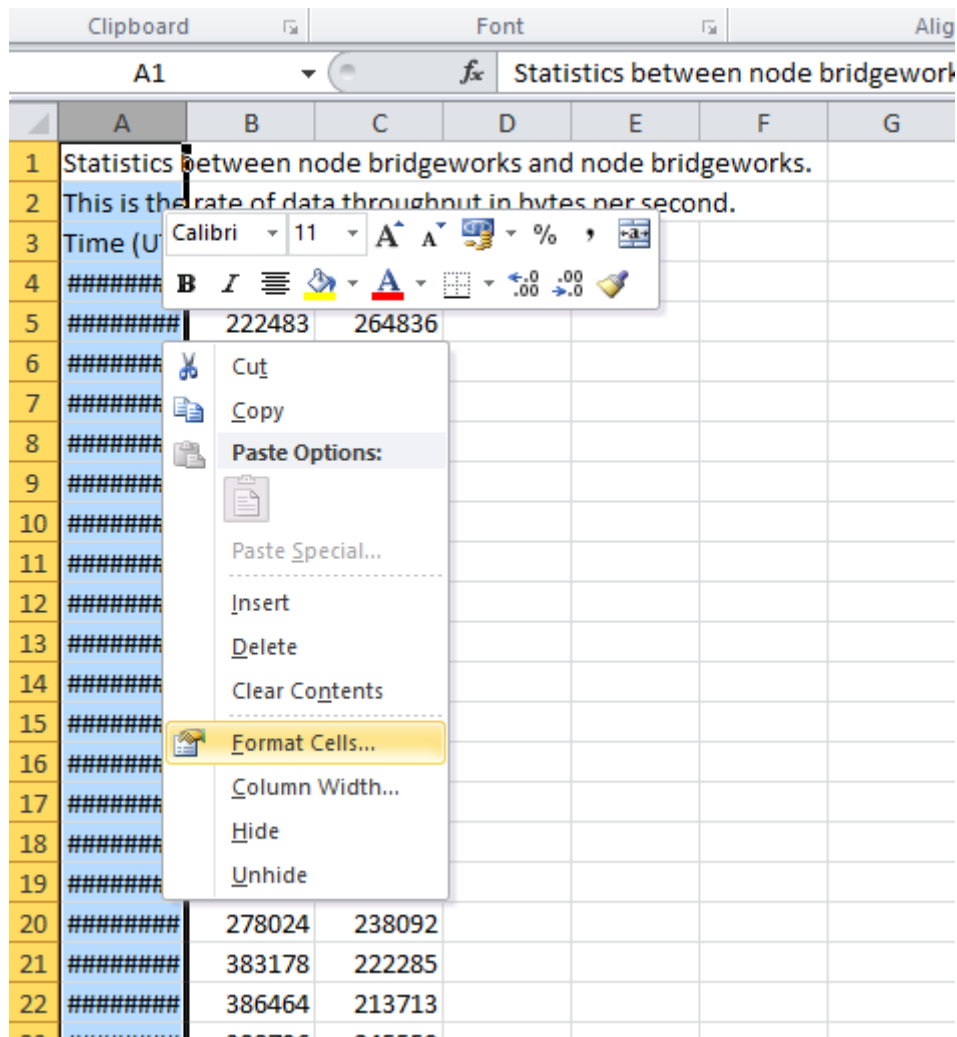
Appendix D: Transfer Statistics Graphing Instructions for Excel 2010

Open Microsoft Excel 2010. From the *Open* dialog box, navigate to the download location for the transfer statistics. Open the file type drop down box and select the transfer statistics .csv file as shown:

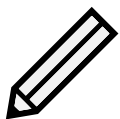


Note: For information on obtaining transfer statistics from your PORTrockIT Node, see Section [4.1.3.2: Download 24 Hour Transfer History](#).

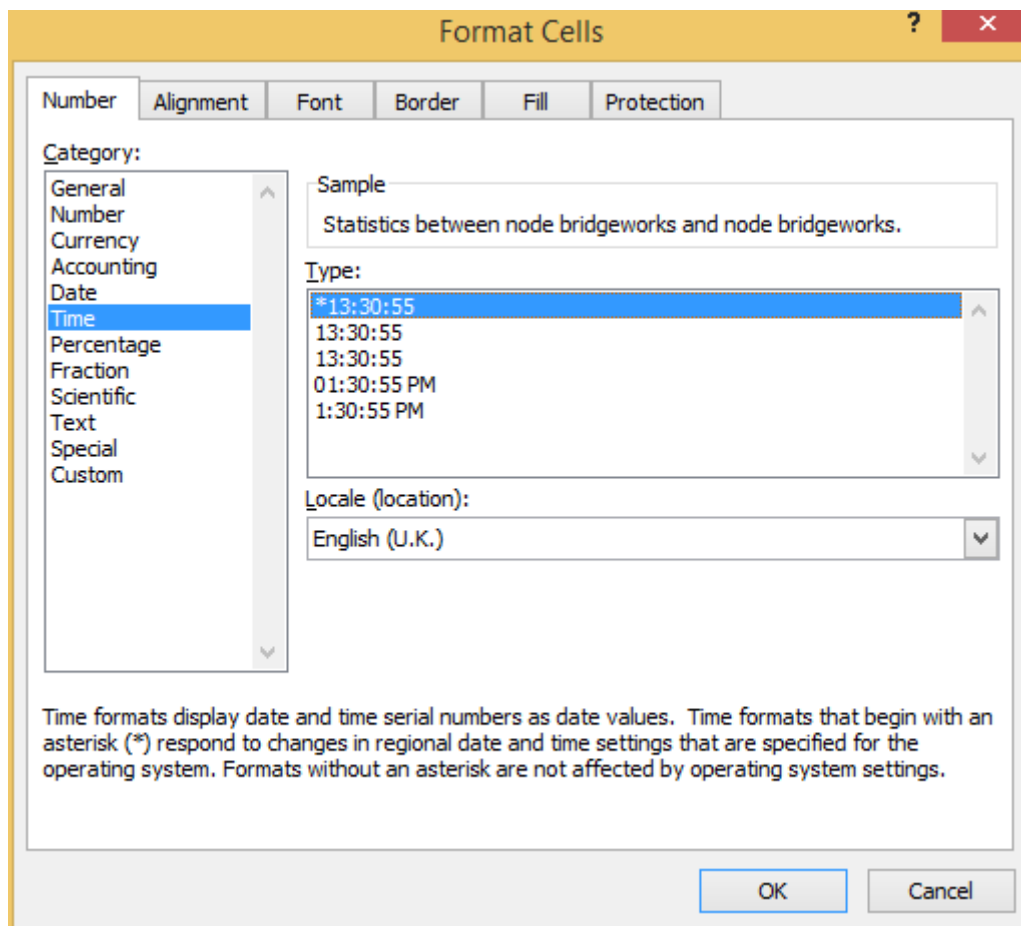
Select the A column of the newly generated worksheet, right-click, and select *Format Cells*.



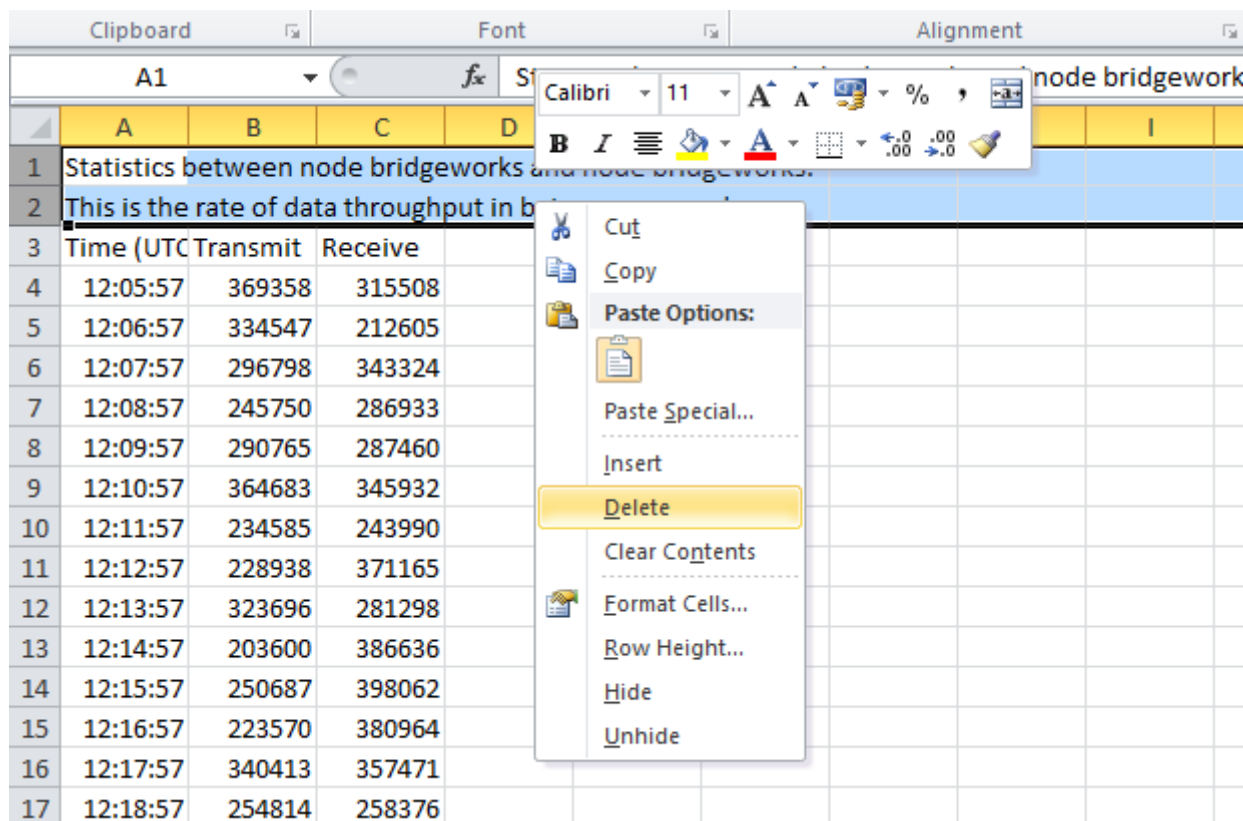
From the *Number* tab, select the *Time* category, and select the option *13:30:55 as shown below then click *OK*.



Note: The time format chosen here is not the format in which the time will be displayed in the final graph.



Select the first two rows (row 1 and row 2) then right-click and select *Delete*.



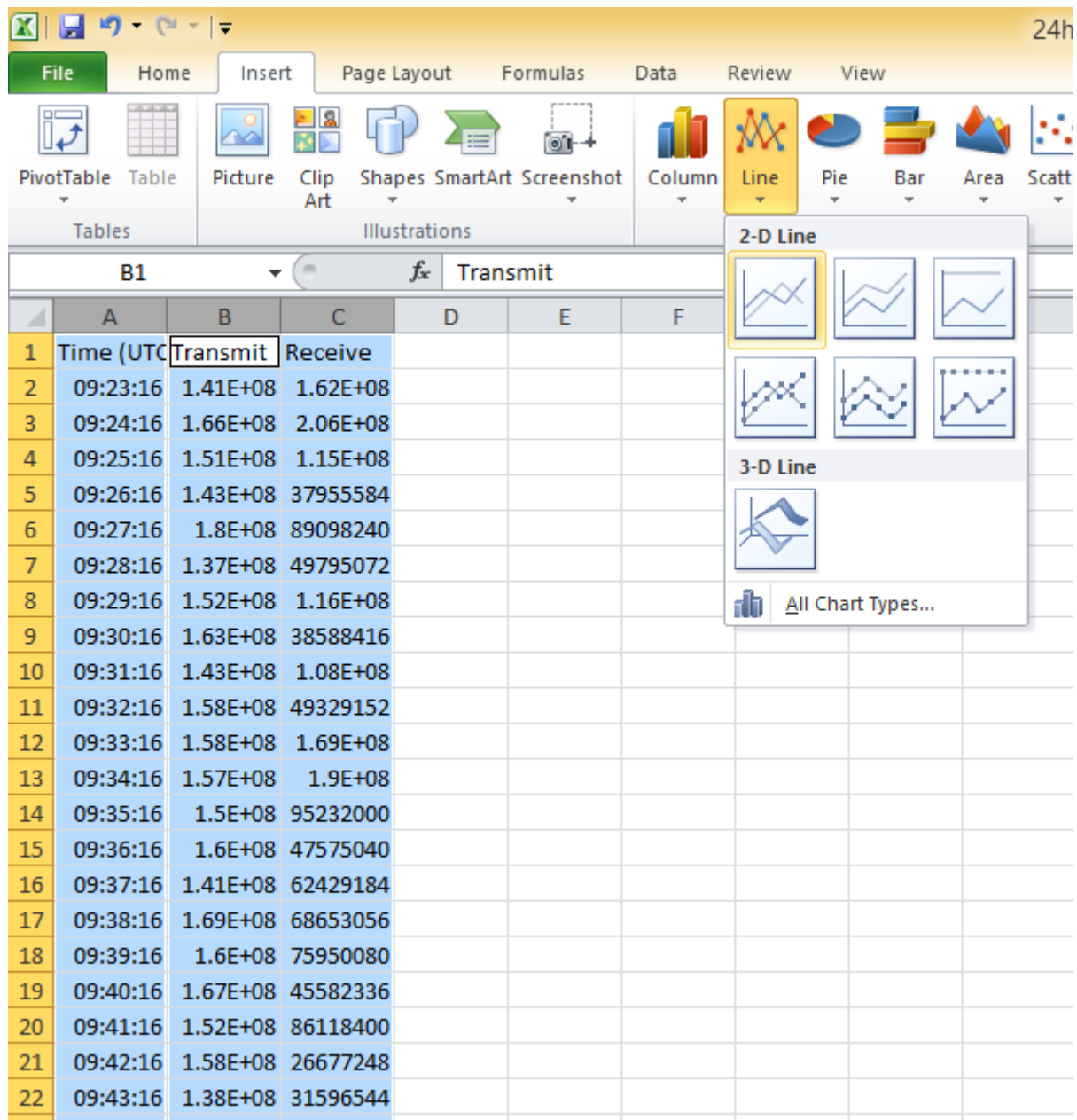
Select the first column by clicking on A. Then, hold down the **Ctrl** key on the keyboard and select the columns *B* and *C*. The three columns should now be selected as shown below:

	A	B	C	D	E	F
1	Time (UTC)	Transmit	Receive			
2	09:23:16	1.41E+08	1.62E+08			
3	09:24:16	1.66E+08	2.06E+08			
4	09:25:16	1.51E+08	1.15E+08			
5	09:26:16	1.43E+08	37955584			
6	09:27:16	1.8E+08	89098240			
7	09:28:16	1.37E+08	49795072			
8	09:29:16	1.52E+08	1.16E+08			
9	09:30:16	1.63E+08	38588416			
10	09:31:16	1.43E+08	1.08E+08			
11	09:32:16	1.58E+08	49329152			
12	09:33:16	1.58E+08	1.69E+08			
13	09:34:16	1.57E+08	1.9E+08			
14	09:35:16	1.5E+08	95232000			
15	09:36:16	1.6E+08	47575040			
16	09:37:16	1.41E+08	62429184			
17	09:38:16	1.69E+08	68653056			
18	09:39:16	1.6E+08	75950080			

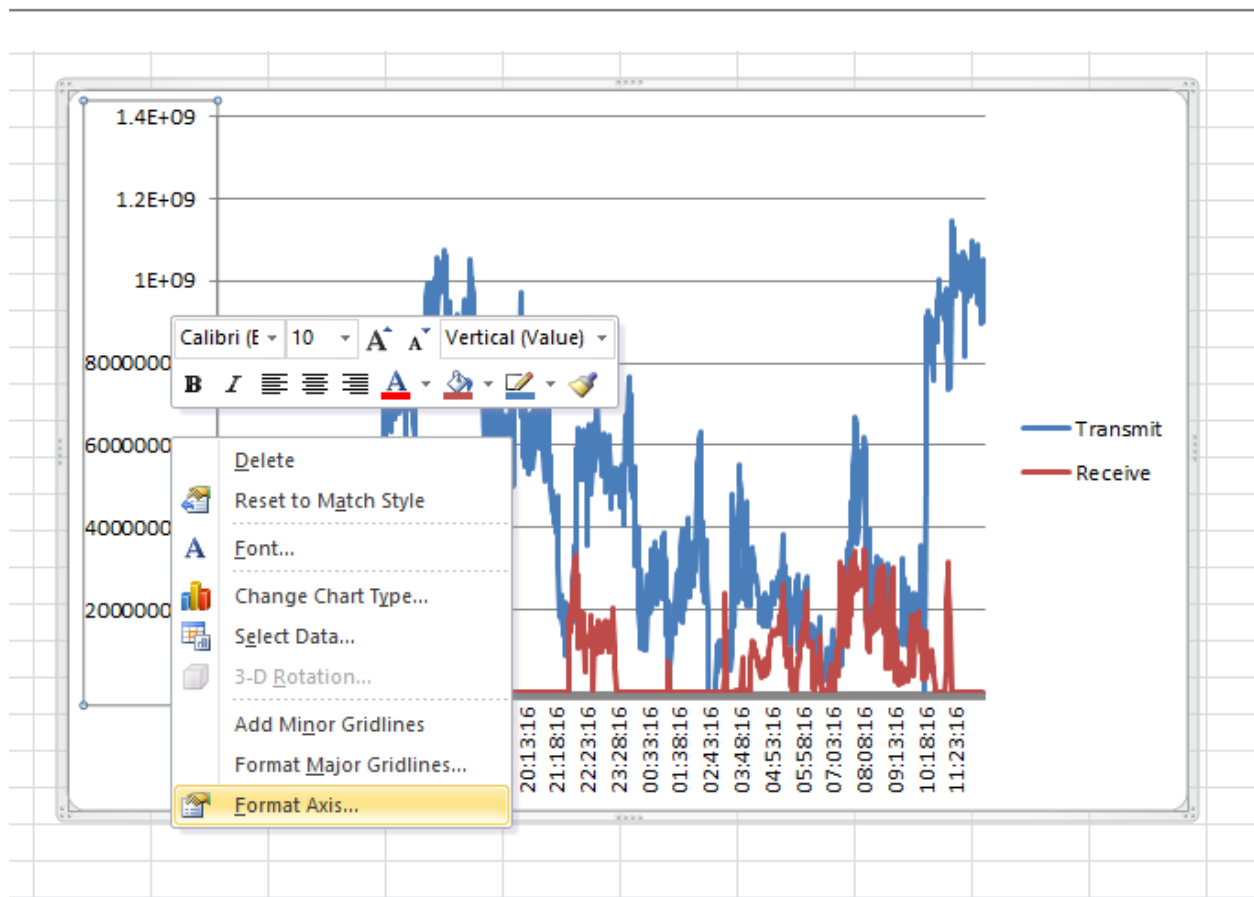


Warning: Selecting all three columns at the same time may cause errors in generating the graph in the following steps. Remember to select column *A* first and then the other two columns with the **Ctrl** key held down.

On the *Insert* tab, in the *Charts* group, select the *Line* chart type and then the first icon shown.

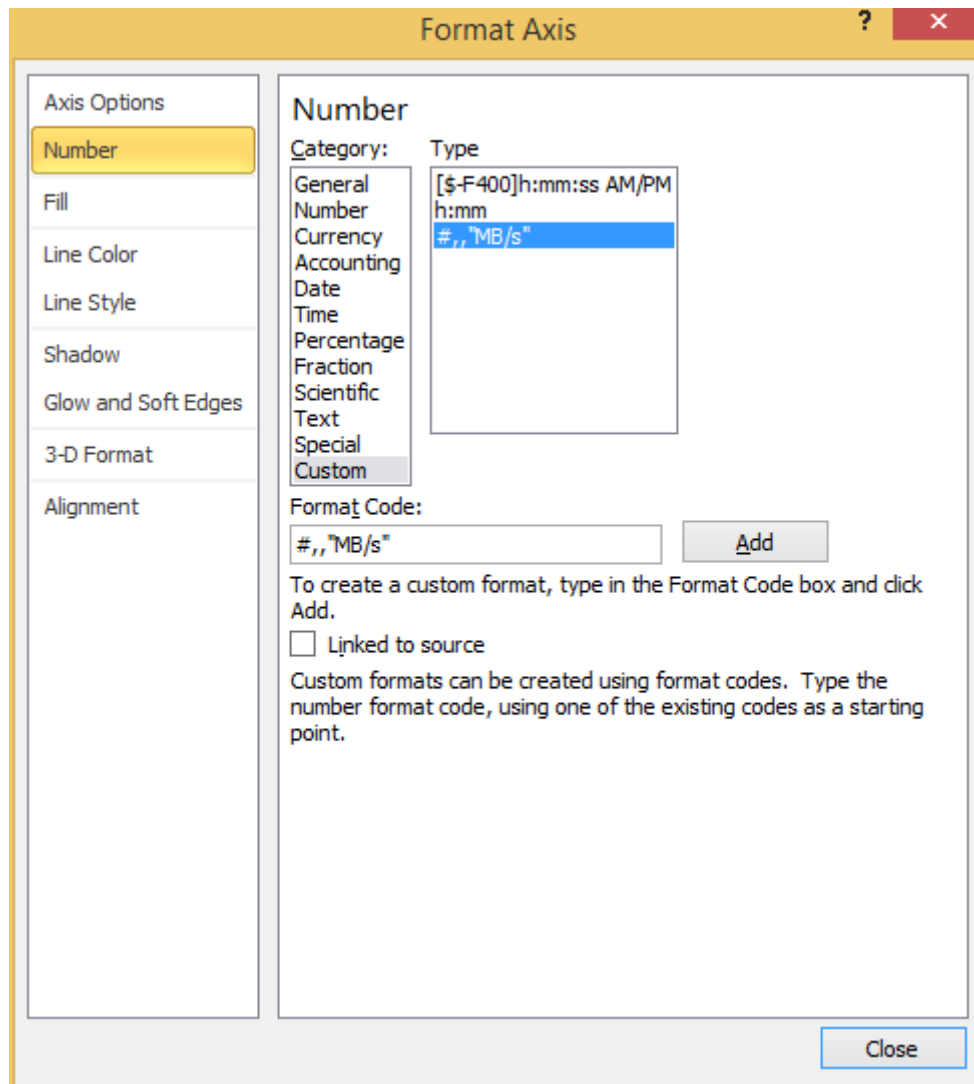


A new chart will be created. Right click the vertical axis on this chart and select *Format Axis*.



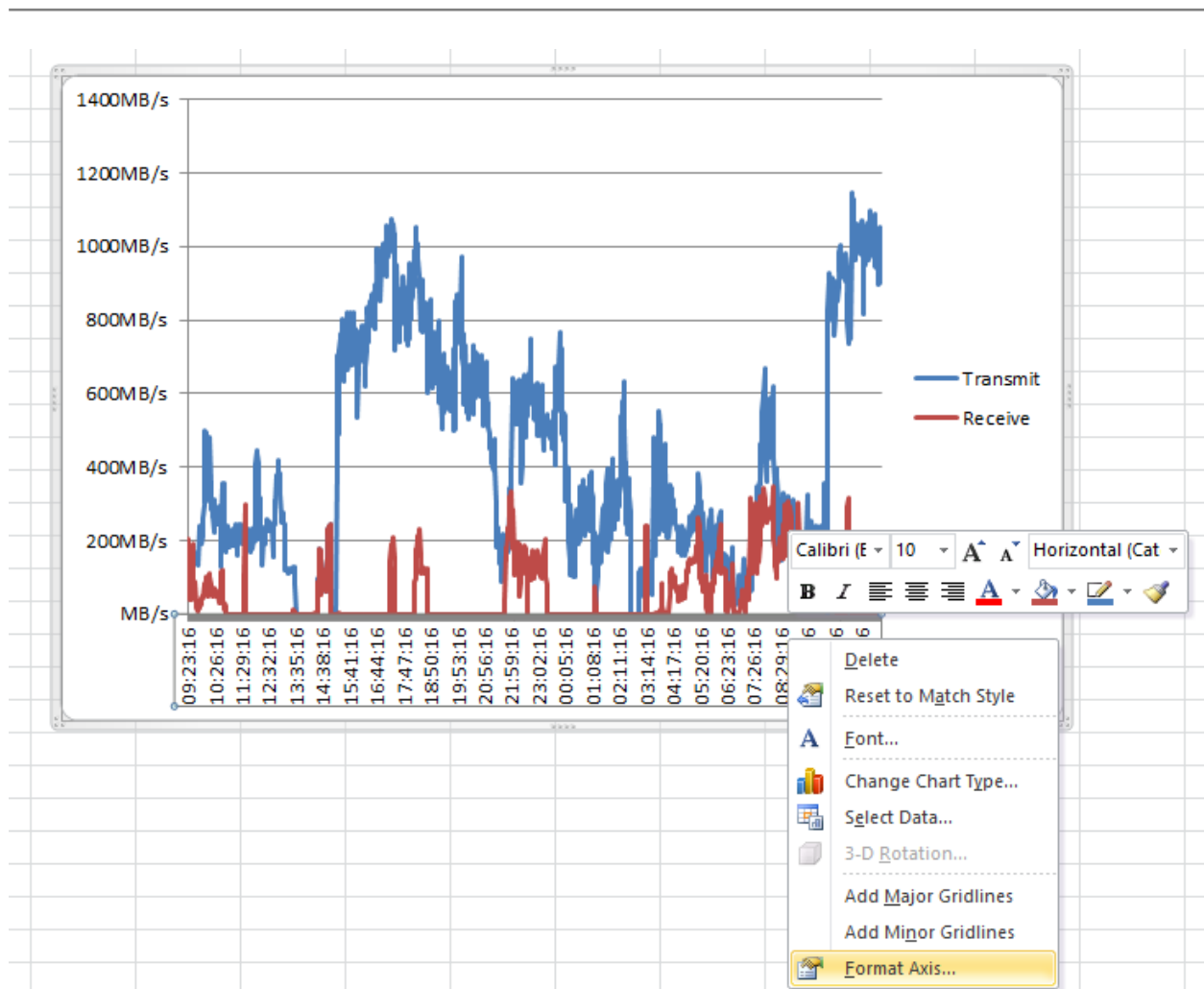
From the *Number* tab, select the *Custom* category. Enter the following in the *Format Code* field:

#,,"MB/s"

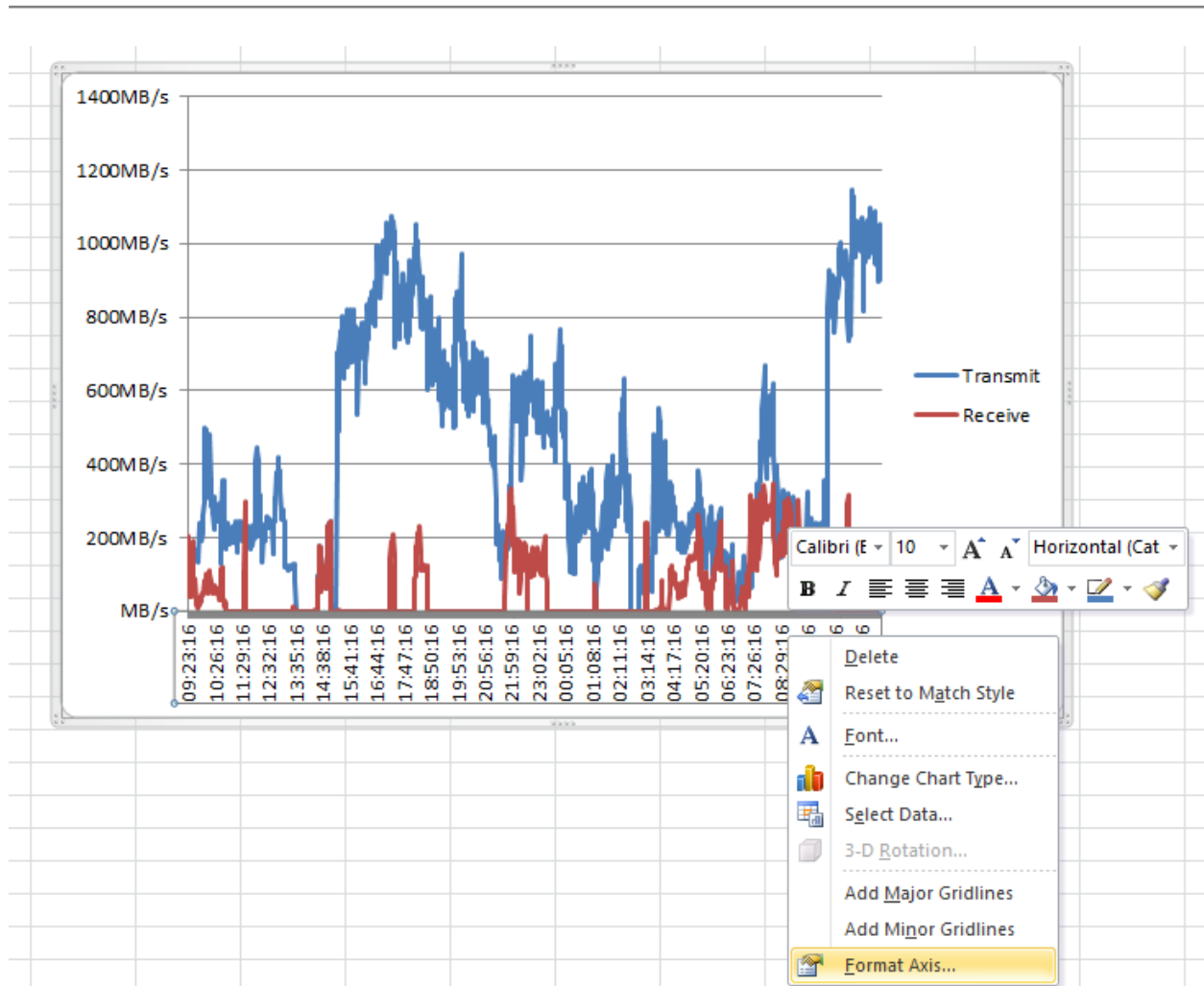


Click *Add*, then *Close*.

Now right click the horizontal axis and select *Format Axis*.

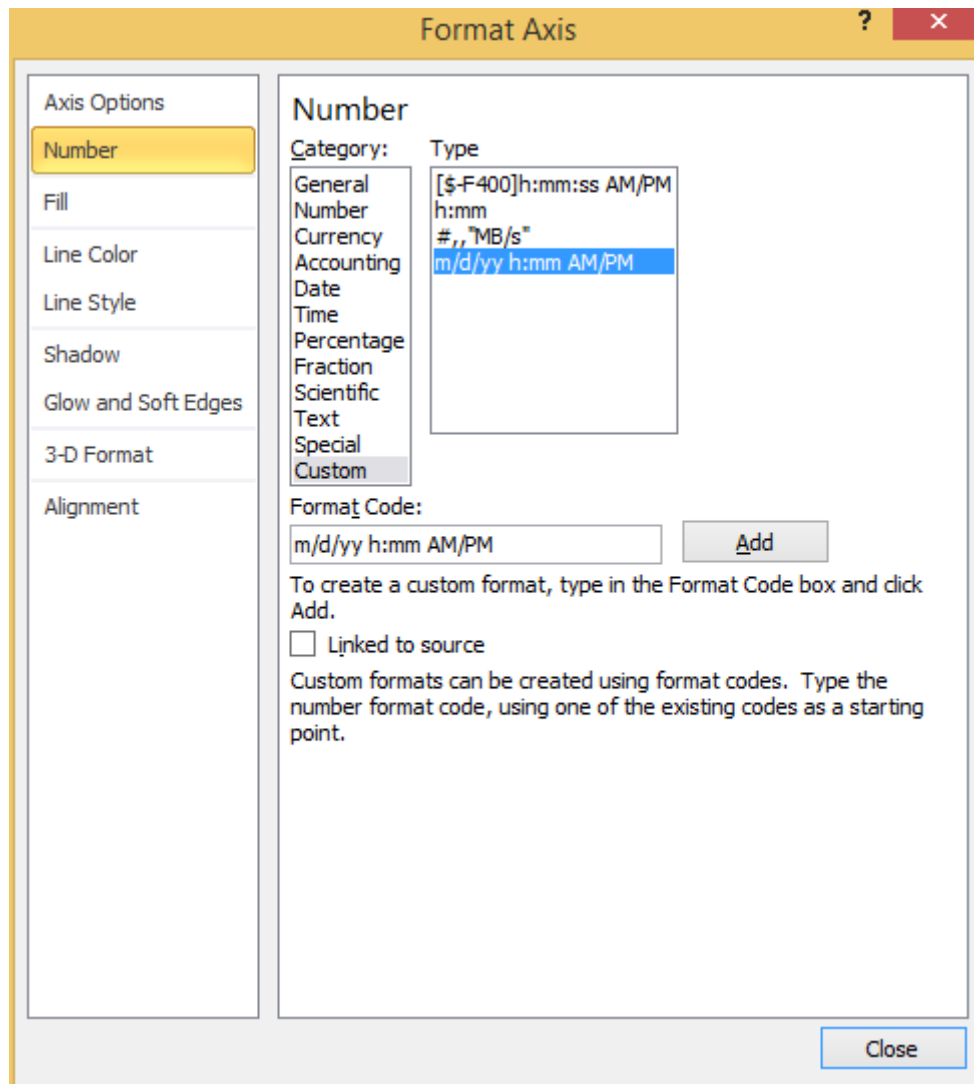


From the *Number* tab, select the *Time* category. Select the format you wish for the time to be displayed.

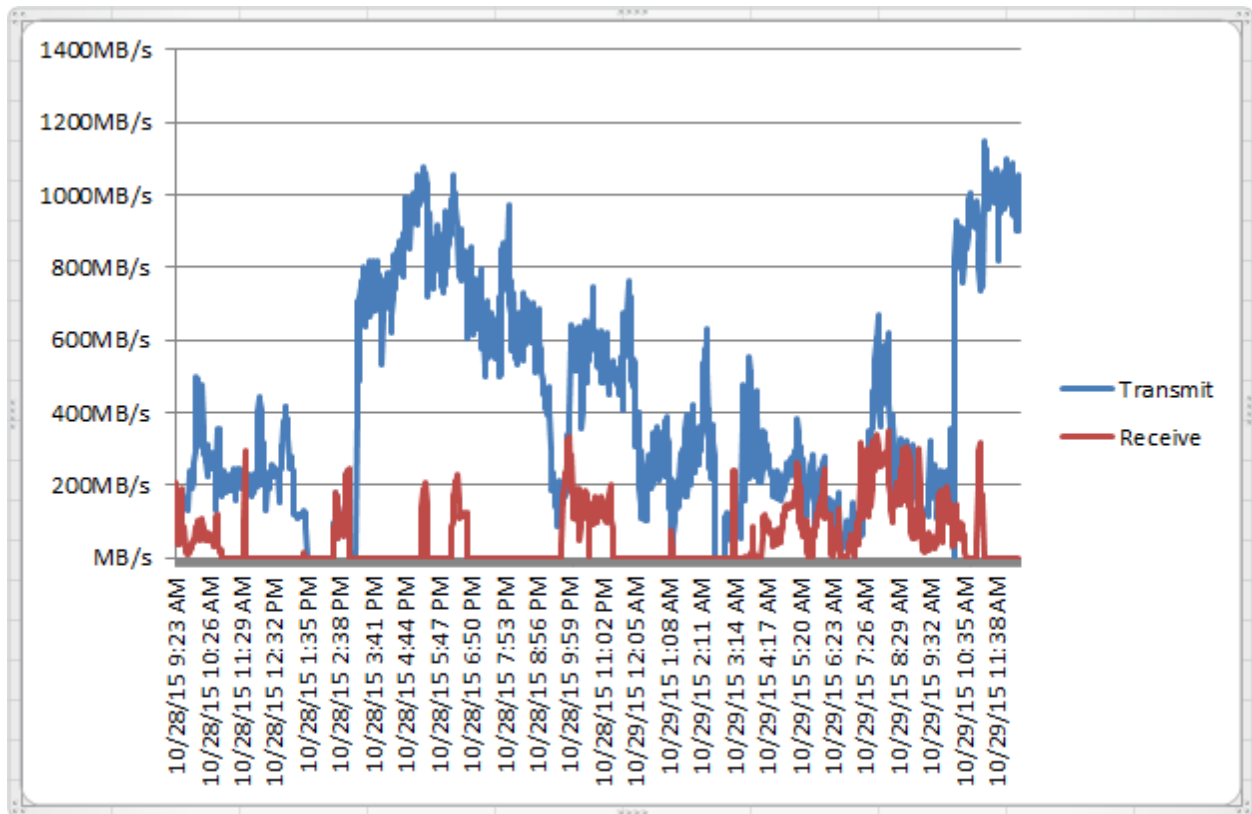


Alternatively, you can use a custom format for the date. In this case, select the *Custom* category, and enter your custom format in to the *Format Code* text field. The following is an example of a format code:

m/d/yy h:mm AM/PM



Click *Add* and then *Close*. Your chart should now look like the following:



Appendix E: Useful Links

Further documentation and support is available through our website: <https://support.4bridgeworks.com/>

If your question is not answered in our documentation, please submit a ticket: <https://support.4bridgeworks.com/contact/>