PORTrockIT Out-of-Path Setup Guide

Eli-v6.2.20

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

1 Introduction

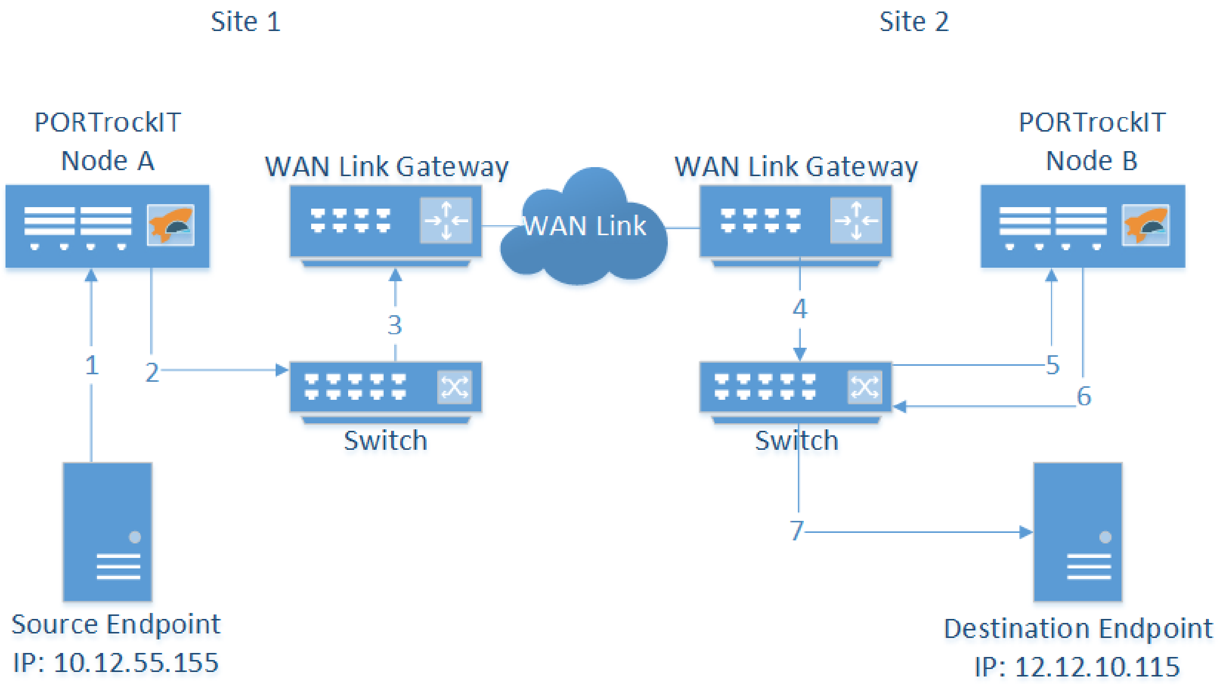
The following document is intended to guide a user through using Bridgeworks PORTrockIT technology. Network infrastructure changes from company to company - if you are in doubt, or this guide does not cover your scenario, please contact support at support@4bridgeworks.com.

Table of Contents

2 Getting Started

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 either a PORTrockIT or WANrockIT Node to accelerate your desired traffic. These Nodes can be either physical hardware appliances, virtual machine images for popular platforms or Amazon Machine Images (AMIs).

This PORTrockIT guide gives an overview of the best way to improve the bandwidth utilisation of supported protocols. The following diagram shows a basic example of how the PORTrockIT Nodes could be deployed.



In this topology *Node A* is in the “Bridged Physically-In-Path” mode of operation and *Node B* is in the “Out-of-Path” mode of operation. The “Out-of-Path” mode can only be used when you are looking to accelerate traffic in a client/server relationship, such as object storage or FTP, and can only be used on the server site.

Node A is set up to intercept traffic leaving the *Source Endpoint* (client), accelerating any data that matches the protocol across the WAN Link to *Node B*. The traffic then continues normally to the *Destination Endpoint* (server).

Depending on the specific protocol you wish to accelerate and your existing network setup, the exact topology you need will vary.

2.1 Prerequisites

In order to use PORTrockIT technology you must have the following:

- Two PORTrockIT Appliances or Virtual Instances - it is permissible to mix both appliances and virtual instances on the same connection.
- A valid Bridgeworks licence for the application you wish to accelerate.

3 Guide Layout

This guide is divided into a series of ordered steps that should be followed through in order. If at any point you run into trouble with a step please refer to the Useful Links section at the end of this document.

It is recommended to print this list of steps out and check off each step as you complete them.

☐ Step 1. Initial Setup of your Bridgeworks Node

☐ Step 2. Configuring IPsec

☐ Step 3. Establishing a Link Between Nodes

☐ Step 4. Configuring PORTrockIT Acceleration

4 Initial Setup of your Bridgeworks Node

4.1 Finding Management IP addresses

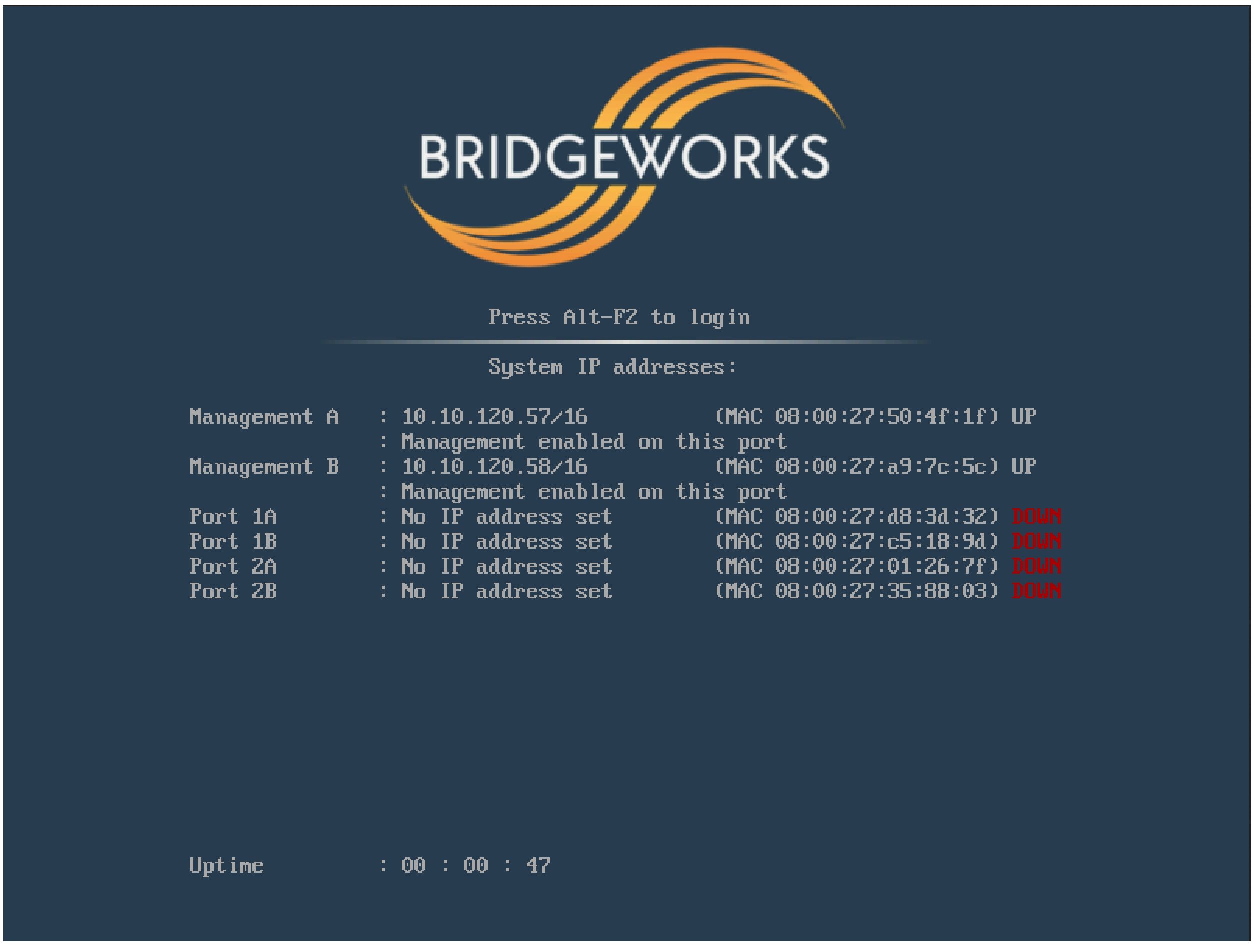
The default management interfaces on hardware appliances will be named Management A and Management B, and both will have DHCP enabled by default.

By default, virtual instances have management capabilities enabled on all network interfaces, but only Port 1 will have DHCP enabled.

You can enable or disable management capabilities on a per-port basis using the Port Mappings page, see Port Mappings ( ) for more information.

If the PORTrockIT unit successfully connects to your DHCP server, and DNS resolution is enabled on your network, you can access the PORTrockIT's web interface from the default hostname by navigating to: `https://bridgeworks/`

To find the IP addresses of management interfaces easily, it is recommended to use the VGA or virtual console as shown below.

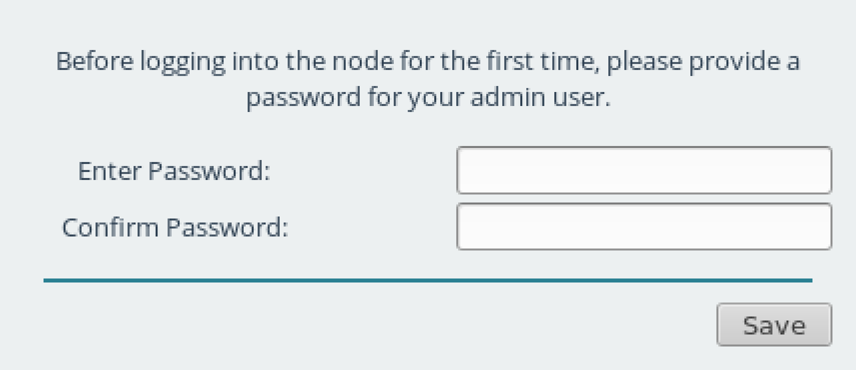


```
                         Press Alt-F2 to login
                         System IP addresses:

Management A    : 10.10.120.57/16         (MAC 08:00:27:50:4f:1f) UP
                : Management enabled on this port
Management B    : 10.10.120.58/16         (MAC 08:00:27:a9:7c:5c) UP
                : Management enabled on this port
Port 1A         : No IP address set       (MAC 08:00:27:d8:3d:32) DOWN
Port 1B         : No IP address set       (MAC 08:00:27:c5:18:9d) DOWN
Port 2A         : No IP address set       (MAC 08:00:27:01:26:7f) DOWN
Port 2B         : No IP address set       (MAC 08:00:27:35:88:03) DOWN




Uptime          : 00 : 00 : 47
```

4.2 First Time Login

Proceed to the web interface of the Node by entering the IP address of one of the Management enabled interfaces in to the address bar of your web browser.

On first access, the web interface displays an initial login page that requires a password to be set for the admin user account of the Node.



Before logging into the node for the first time, please provide a password for your admin user.

Enter Password:

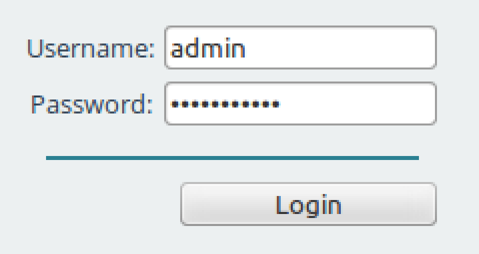
Confirm Password:

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.

The passwords typed in to the two provided fields must match. Passwords must be a minimum of 5 characters and a maximum of 64 characters in length.

4.3 Logging into the Node

When a valid password is submitted, you are redirected to the login screen. To access the *Node Management Console*, enter the login credentials with the admin username and the password set previously.

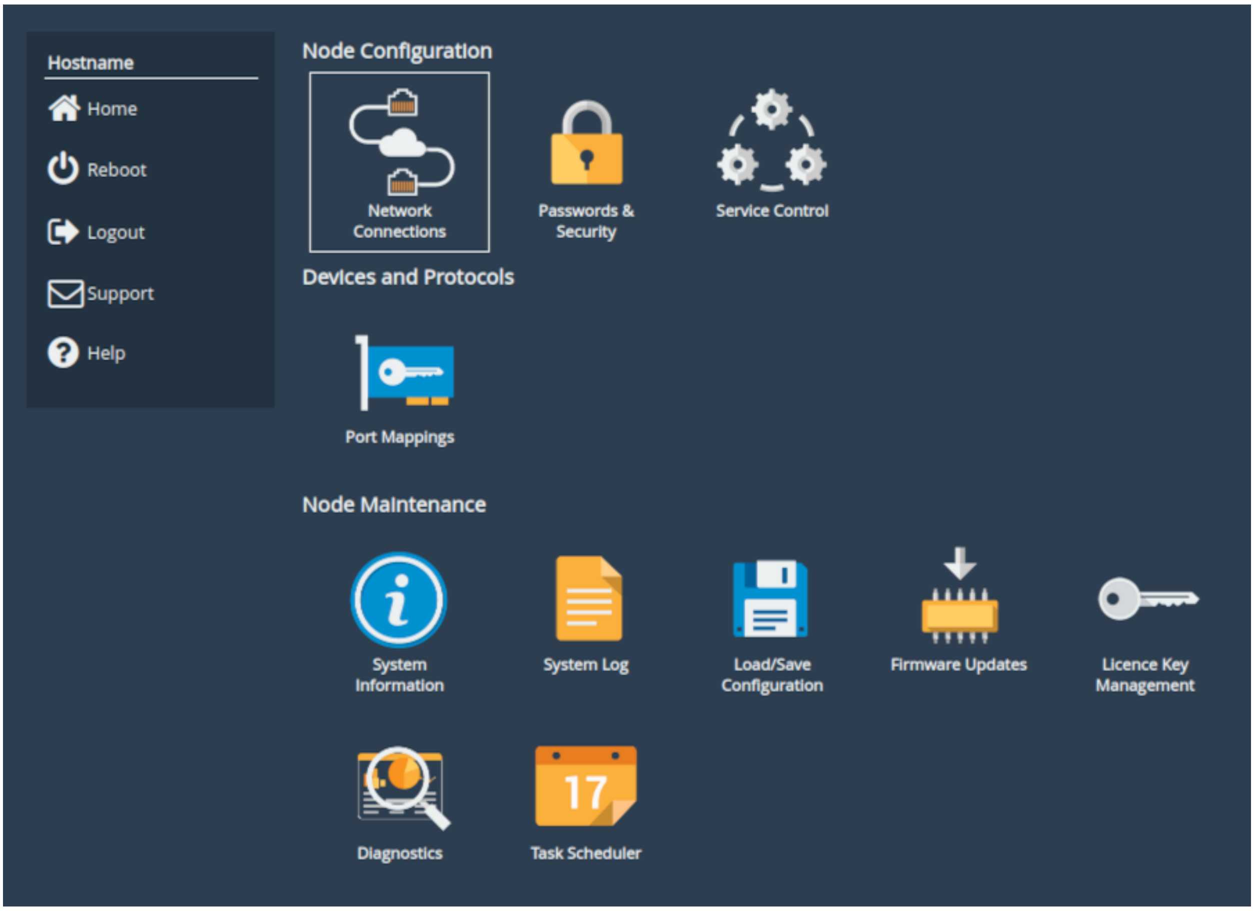


Username: admin

Password: ••••••••••••

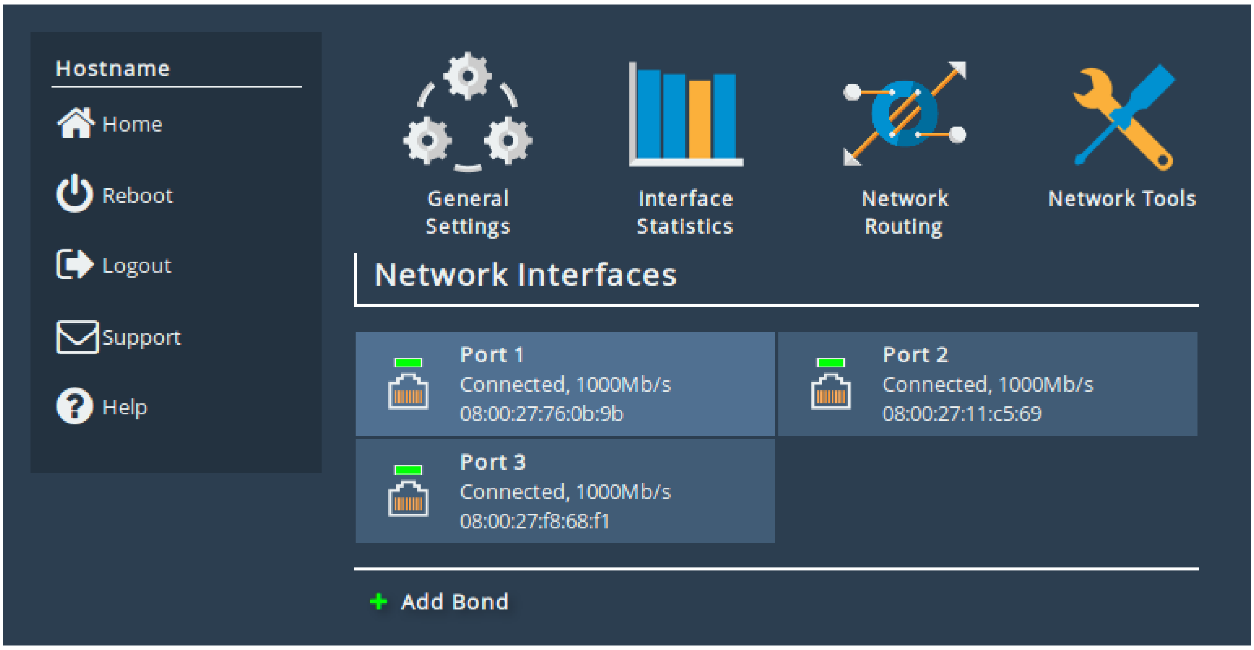
4.4 Network Connections ( )

The *Network Connections* page allows for the configuration of static IP addresses, and changing the hostname of the Node. To change the settings click the *Network Connections* icon as shown below.



4.4.1 Setting the Hostname/Node Name

Click on the *General Settings* icon on the *Network Connections* page as shown below.

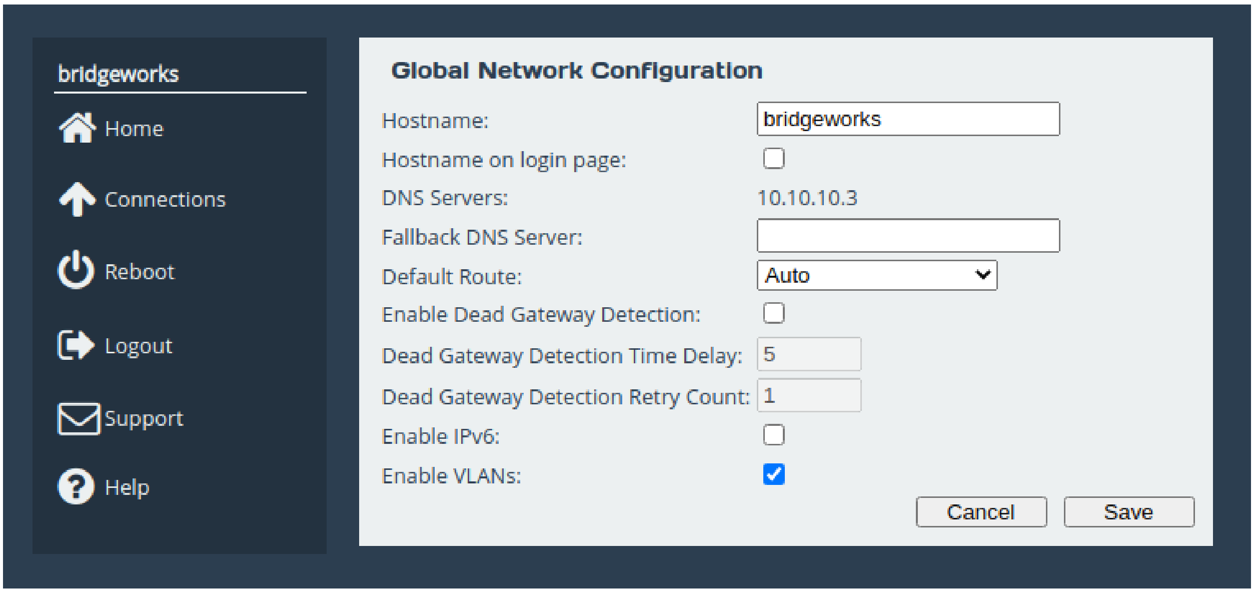


Port 1
Connected, 1000Mb/s
08:00:27:76:0b:9b

Port 2
Connected, 1000Mb/s
08:00:27:11:c5:69

Port 3
Connected, 1000Mb/s
08:00:27:f8:68:f1

The hostname of the Node can be changed by replacing the default name bridgeworks with a name of your choice. This name is also the alias name used for identifying your Nodes under the *Node Management* section.



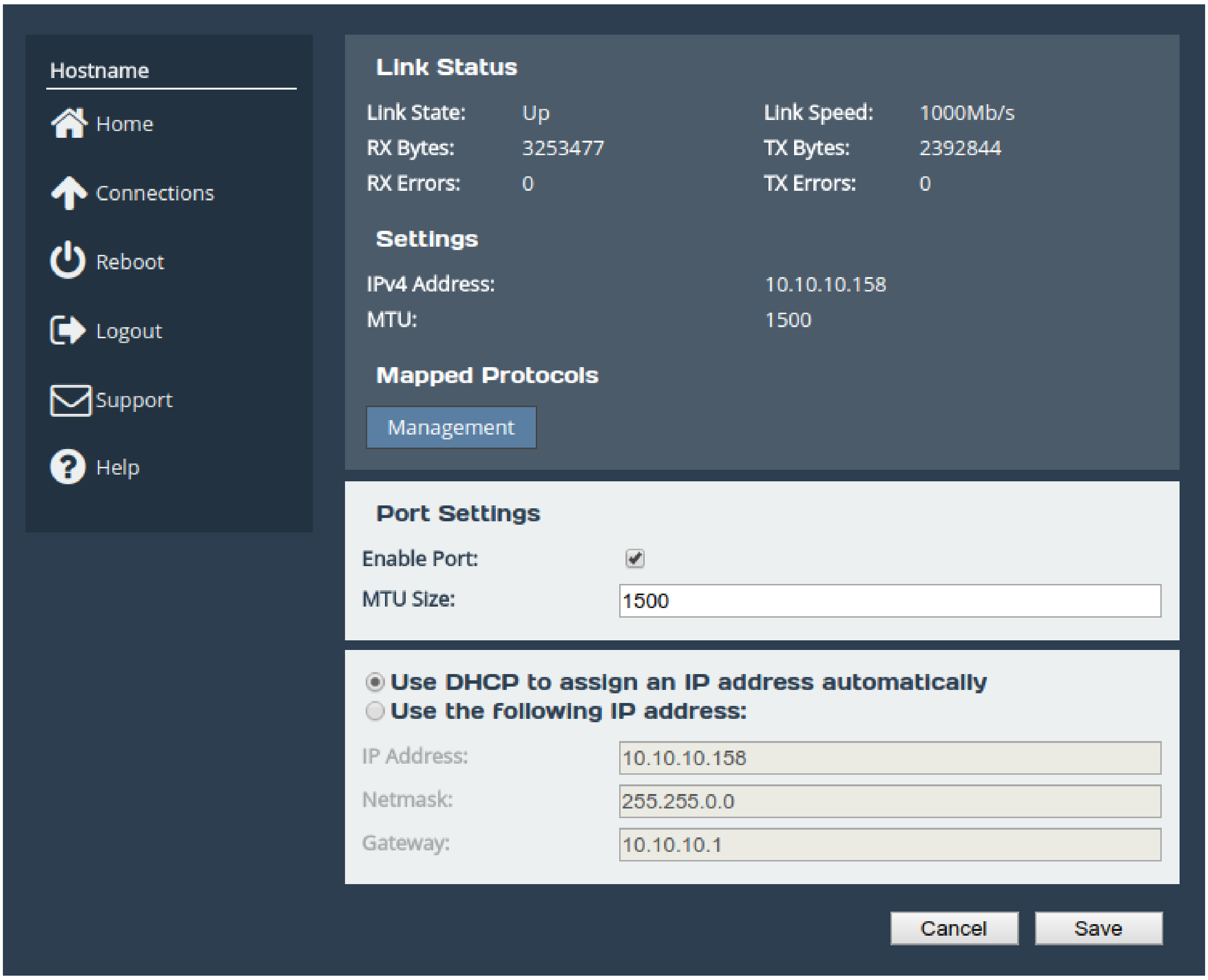
Global Network Configuration

Hostname:	bridgeworks
Hostname on login page:	□
DNS Servers:	10.10.10.3
Fallback DNS Server:	
Default Route:	Auto
Enable Dead Gateway Detection:	□
Dead Gateway Detection Time Delay:	5
Dead Gateway Detection Retry Count:	1
Enable IPv6:	□
Enable VLANs:	☑

When you have changed the hostname, click the *Save* button; A reboot is required for the change to take effect.

4.4.2 Changing IP Addresses

Icons representing each port are displayed underneath the *Network Interfaces* heading, alongside a summary of its current state. Clicking on a port leads to the port settings page.



Link Status

Link State:	Up	Link Speed:	1000Mb/s
RX Bytes:	3253477	TX Bytes:	2392844
RX Errors:	0	TX Errors:	0

Settings

IPv4 Address:	10.10.10.158
MTU:	1500

Mapped Protocols

Port Settings

Enable Port: ☑

MTU Size: 1500

● Use DHCP to assign an IP address automatically

○ Use the following IP address:

IP Address: 10.10.10.158

Netmask: 255.255.0.0

Gateway: 10.10.10.1

A disabled port will initially need to be enabled by selecting the *Enable Port* checkbox. This will bring the port online and allow you to edit its settings.

To manually assign an IP address to a port, select the radio button *Use the following IP address*. The fields *IP Address*, *Netmask* and *Gateway* are now available to be filled in. When all fields are complete, click the *Save* button. A reboot is required for the changes to take effect.

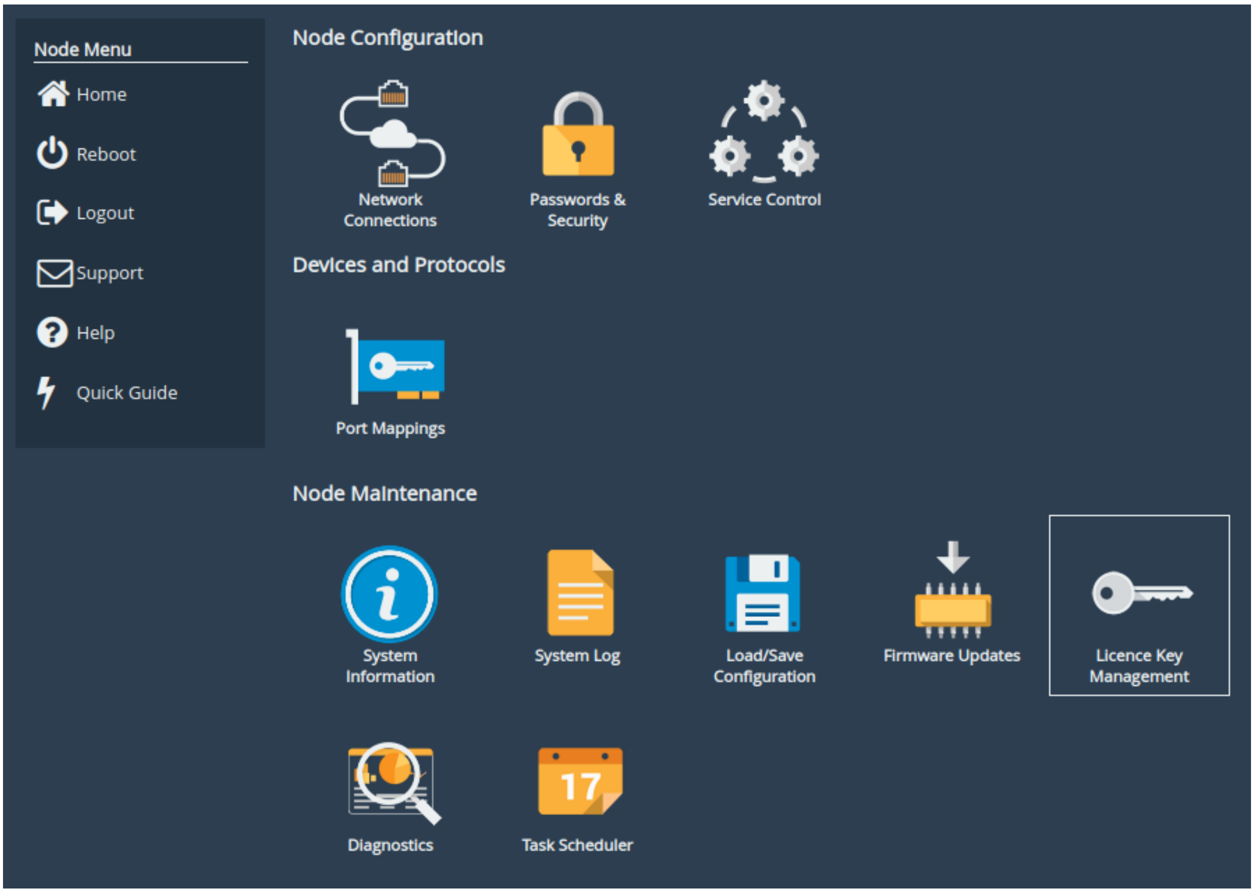
4.5 Licence Keys

All PORTrockIT and WANrockIT products require a licence key in order to unlock the acceleration features of the product.

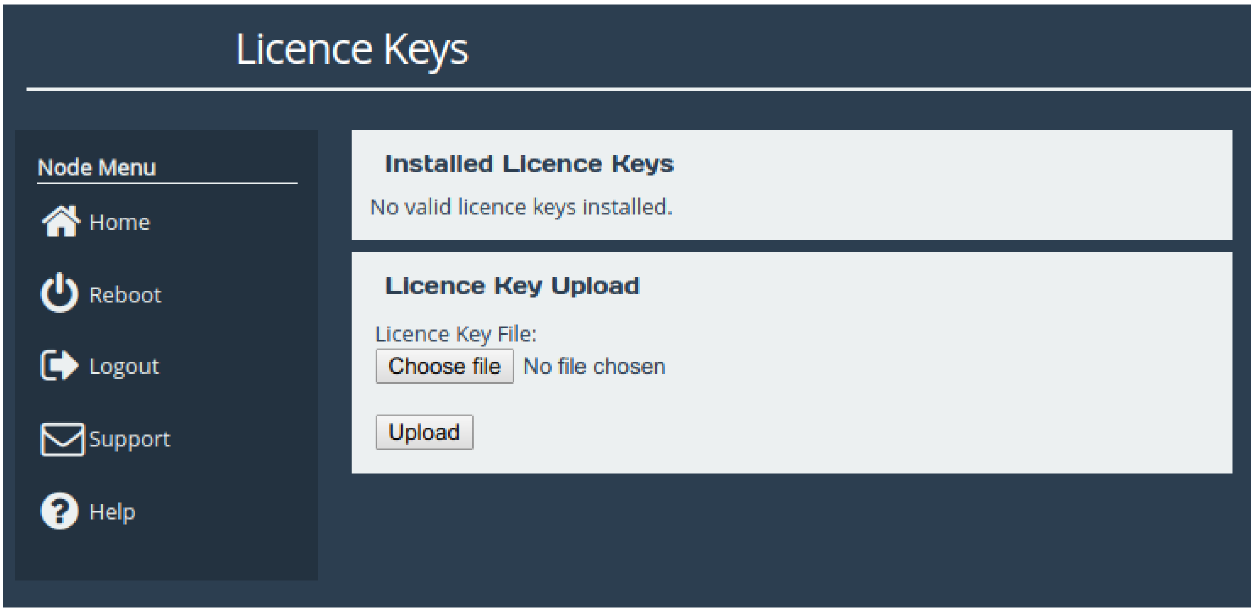
To determine whether there is a valid licence key, log into the Node and navigate to the *Licence Key Management* page. If the page displays *No valid licence keys installed* then you must obtain a licence key to unlock the Node's features. If you do not have a licence key or can no longer locate your key, please contact support@4bridgeworks.com.

4.5.1 Uploading a Licence Key

Once you have received the licence key, log into the web interface of the Node and go to the *Licence Key Management* page.



Click the *Choose file* button and select the licence key to upload.



Licence Keys

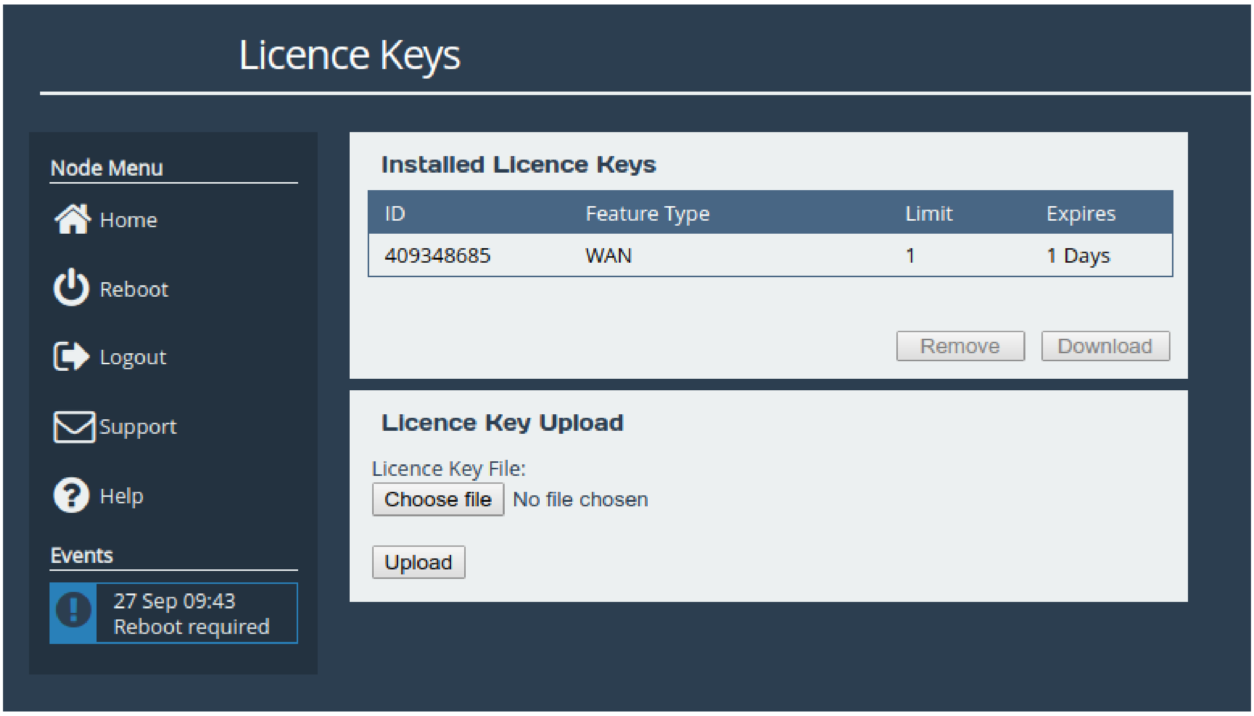
Installed Licence Keys

No valid licence keys installed.

Licence Key Upload

Licence Key File: No file chosen

Click the *Upload* button. The licence key will appear in the table along with the length of time it will remain active.



27 Sep 09:43
Reboot required

Installed Licence Keys

ID	Feature Type	Limit	Expires
409348685	WAN	1	1 Days

Licence Key Upload

Licence Key File: No file chosen

A reboot is required for the licence key to take effect.

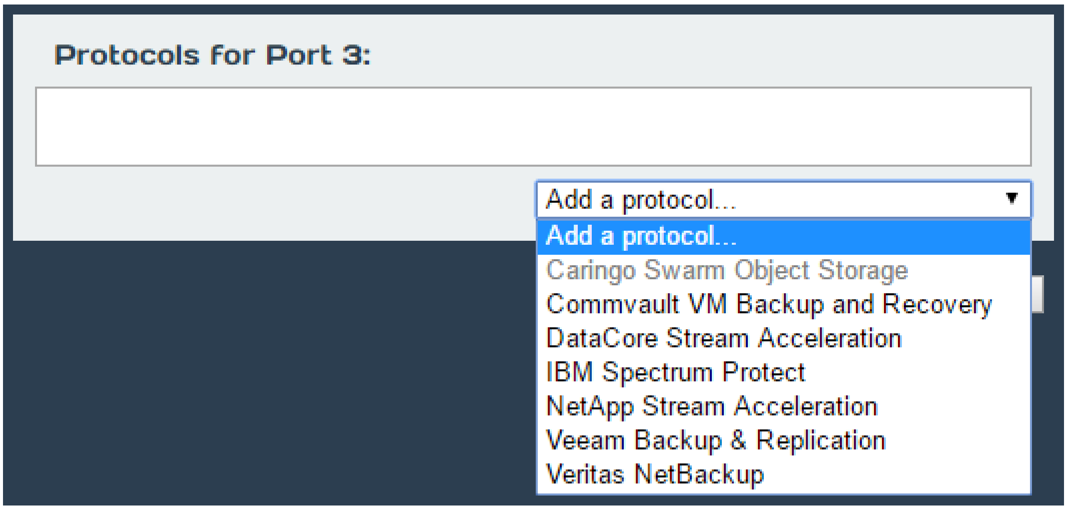
4.6 Port Mappings ( )

4.6.1 Overview

Port Mappings allows for the assignment of protocols to network interfaces. For example, adding *WAN* to a port will allow WAN connections and acceleration from that network port. Except for the WAN protocol, protocols are related to the types of traffic to be accelerated on that port.

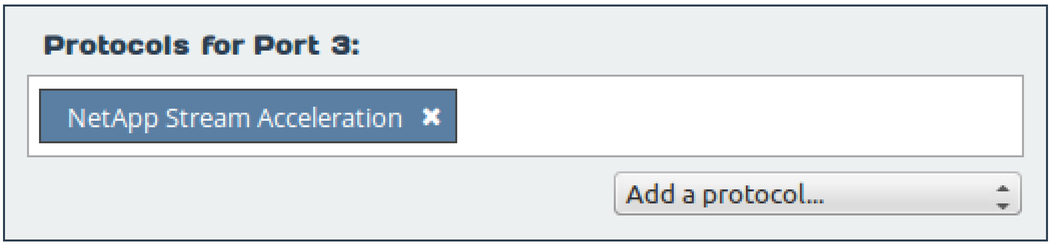
4.6.2 Setting Port Mappings

To assign a protocol to a network interface, select the desired protocol from the drop-down list underneath the port to which it should be assigned. Note that the protocol options will vary between PORTrockIT and WANrockIT Nodes.



Protocols for Port 3:
Add a protocol...
Add a protocol...
Caringo Swarm Object Storage
Commvault VM Backup and Recovery
DataCore Stream Acceleration
IBM Spectrum Protect
NetApp Stream Acceleration
Veeam Backup & Replication
Veritas NetBackup

After selecting a valid protocol from the drop-down list, the name of the protocol appears within a blue box underneath the port.



A mapping can be removed by clicking on the `X` next to the name of the protocol.

Once the configuration is complete, click on the *Save* button. A reboot is required for the changes to take effect.

5 Configuring IPsec

5.1 Introduction

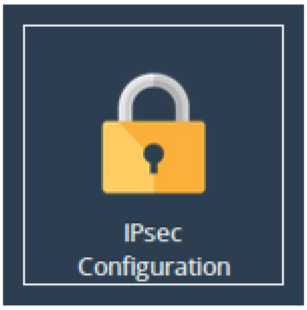
This step will guide you through how to configure IPsec to encrypt traffic between two Bridgeworks Nodes. Using IPsec ensures the integrity, confidentiality and authentication of data communications over an IP network. This step should be done before performing the step Establishing a Link Between Nodes. If you are already connecting your Nodes over an existing VPN link, or a private direct connection then this step is not necessary as your traffic will already be protected.

5.2 Important Notes

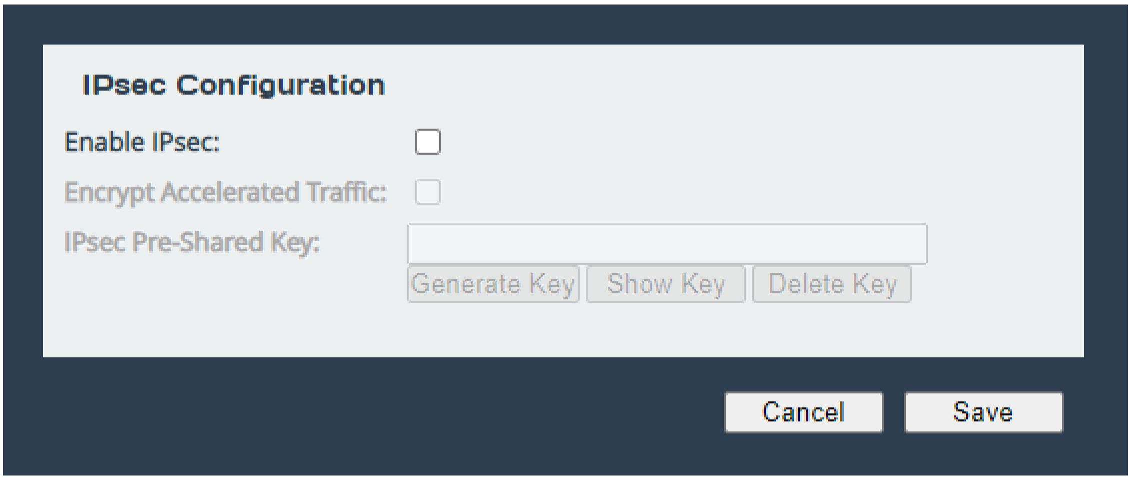
- Nodes with IPsec configured to *Encrypt Accelerated Traffic* will only allow connections from other IPsec-enabled Nodes with the same pre-shared key and settings enabled.
- It is recommended to only enable *Encrypt Accelerated Traffic* when data transfer is stopped as WAN communication will be broken until IPsec configuration has been completed on both Nodes.
- It is recommended that HTTPS is enabled (by default it will already be enabled) before configuring IPsec as this ensures that the Pre-Shared Key is transmitted securely between the Node and web browser.

5.3 Enabling IPsec

From the Node's web interface, navigate to the *Node Management* page, then to the *IPsec Configuration* page by clicking the corresponding icon in the top menu.



The IPsec service is disabled by default, so the Node's IPsec Configuration options will be disabled until the *Enable IPsec* checkbox is selected.



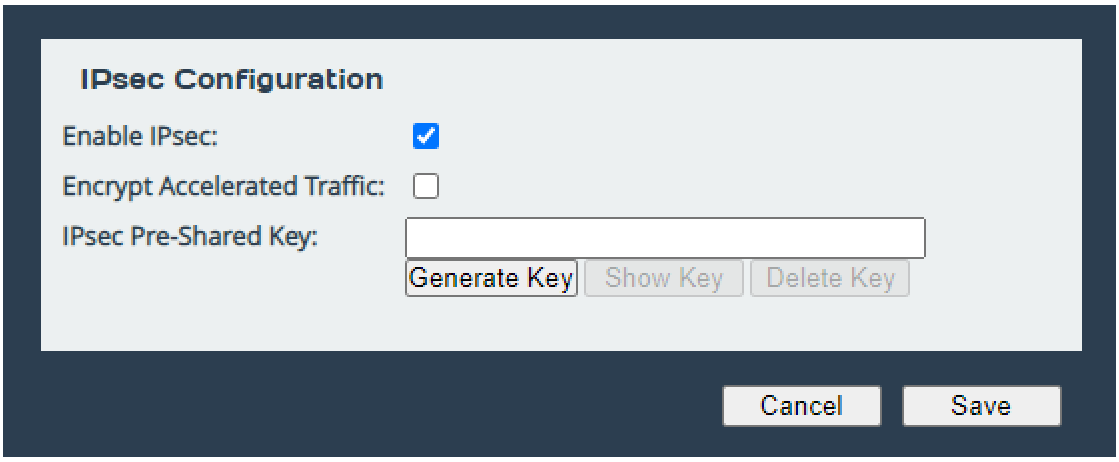
IPsec Configuration

Enable IPsec: ☐

Encrypt Accelerated Traffic: ☐

IPsec Pre-Shared Key:

Select the *Enable IPsec* checkbox and the section will be enabled as shown below:



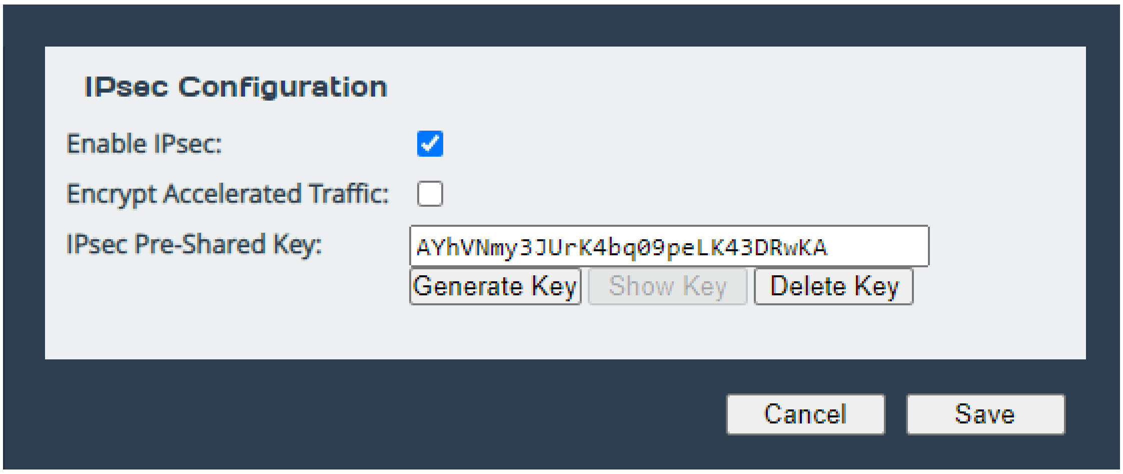
IPsec Configuration

Enable IPsec: ☑

Encrypt Accelerated Traffic: ☐

IPsec Pre-Shared Key:

You can either enter in your own Pre-Shared Key or use the IPsec key generator by clicking *Generate Key*, which will fill in the *IPsec Pre-Shared Key* field as shown below:



IPsec Configuration

Enable IPsec: ☑

Encrypt Accelerated Traffic: ☐

IPsec Pre-Shared Key: AYhVNmy3JUrK4bq09peLK43DRwKA

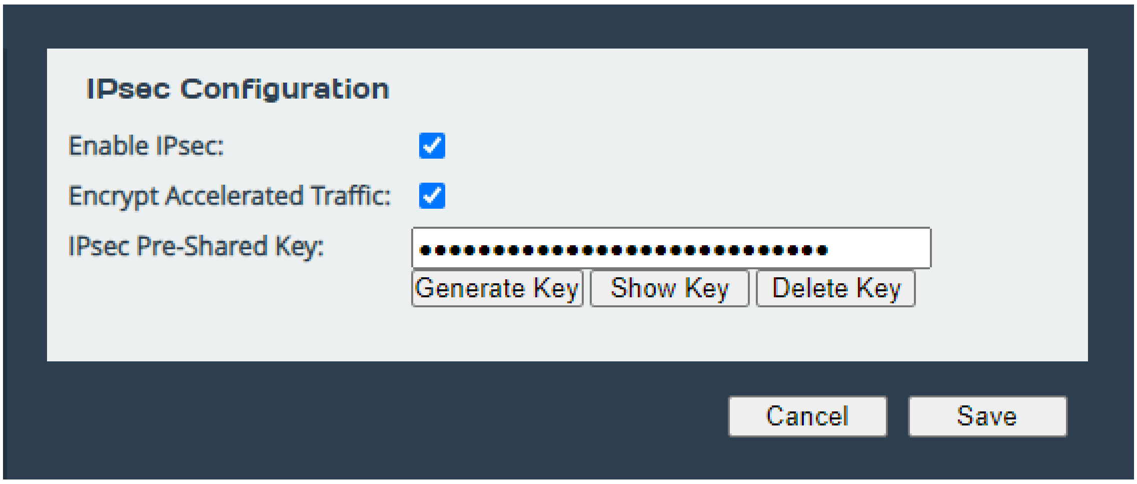
If the *Encrypt Accelerated Traffic* option is desired then tick the corresponding checkbox. This option will encrypt all WAN links between the two Nodes affecting all accelerated data being passed through them.

If only the VPN functionality is required, i.e. only unaccelerated traffic is required to be encrypted, the *Encrypt Accelerated Traffic* option can be left blank.

Click *Save* to store the IPsec configuration. This will become active straight away and, if *Encrypt Accelerated Traffic* is selected, any existing WAN connections will break unless they already have IPsec enabled with the same pre-shared key and settings.

5.4 Copying the Pre-Shared Key to other Bridgeworks Nodes

Return to the *IPsec Configuration* page. The PSK should now be hidden as shown:



IPsec Configuration

Enable IPsec: ☑

Encrypt Accelerated Traffic: ☑

IPsec Pre-Shared Key: ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

Click *Show Key* to display the stored pre-shared key. Select and copy this key to your clipboard. Please note that if HTTPS is not enabled then the Pre-Shared key will be sent to your web browser in plain text format.

From the web interface of any Bridgeworks Nodes you wish to connect to, follow this section again, but paste in the key from your clipboard instead of generating a new one.

6 Establishing a Link Between Nodes

6.1 Introduction

The following section demonstrates how to connect an On-Premise Node to an Off-Premise Node. The examples below illustrate the WAN connection of two Nodes labelled *Node A* and *Node B*. Establishing a WAN link from *Node A* to *Node B* is required in order to allow hosts/endpoints connected to *Node A* to access target devices or endpoints connected to *Node B*. This process will have to be repeated to establish a connection in the reverse direction if you want the hosts/endpoints at *Node B* to connect to targets connected to *Node A*. If you are using the PORTrockIT product range, it is recommended that you establish a connection both ways unless you are certain one way is sufficient.

There are different types of connection possible, depending on your network infrastructure. Throughout the following example topologies, the Nodes are referred to as *Node A* and *Node B* with a summary of which example IP addresses are used. These examples should be kept in mind through the remaining sections of this guide.

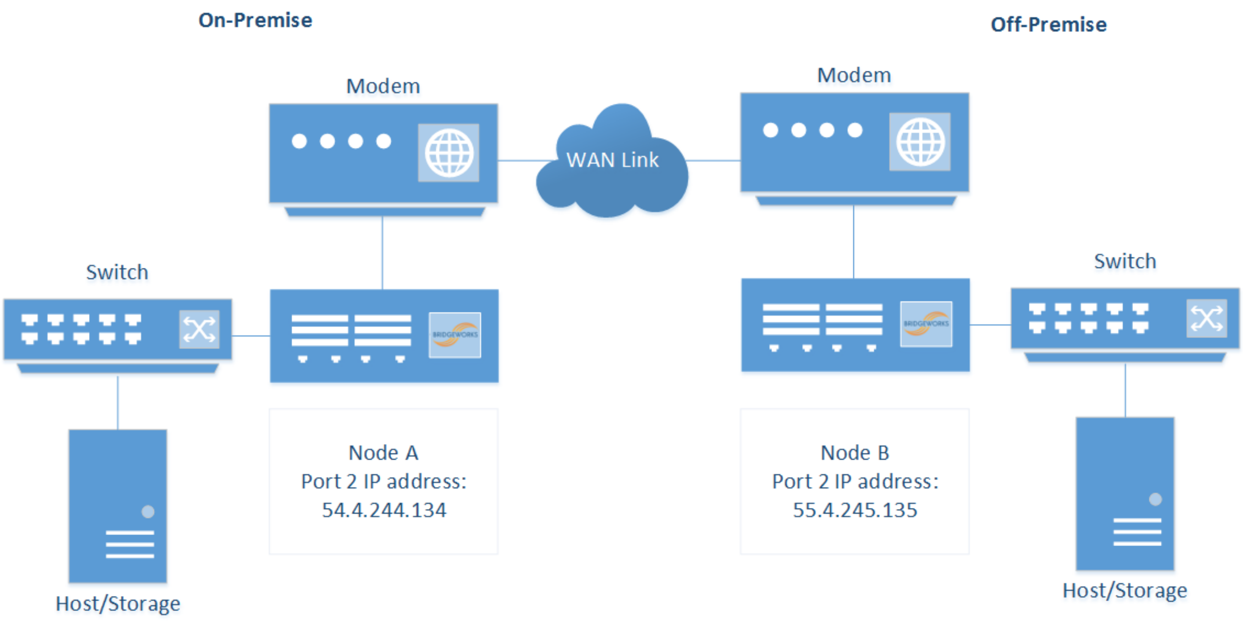
6.2 Firewall

If the WAN link being established is behind a firewall then the following firewall ports will have to be open in both the outbound and inbound direction.

Protocol/Port	Description
TCP 16665	WANrockIT/PORTrockIT main transfer port
UDP 4500	IPsec, used for encrypting WANrockIT/PORTrockIT traffic
UDP 500	IPsec, used for encrypting WANrockIT/PORTrockIT traffic
ESP	IPsec, used for encrypting WANrockIT/PORTrockIT traffic

6.3 Topology 1: Connecting Bridgeworks Nodes which have Public IP addresses

To connect to Bridgeworks Nodes, a public IP address can be assigned directly to the WAN interfaces (by default, *Port 2*) of both Nodes, as shown below. In this case, the WAN port is directly connected into a modem and faces directly out on to a WAN link with a public IP address.

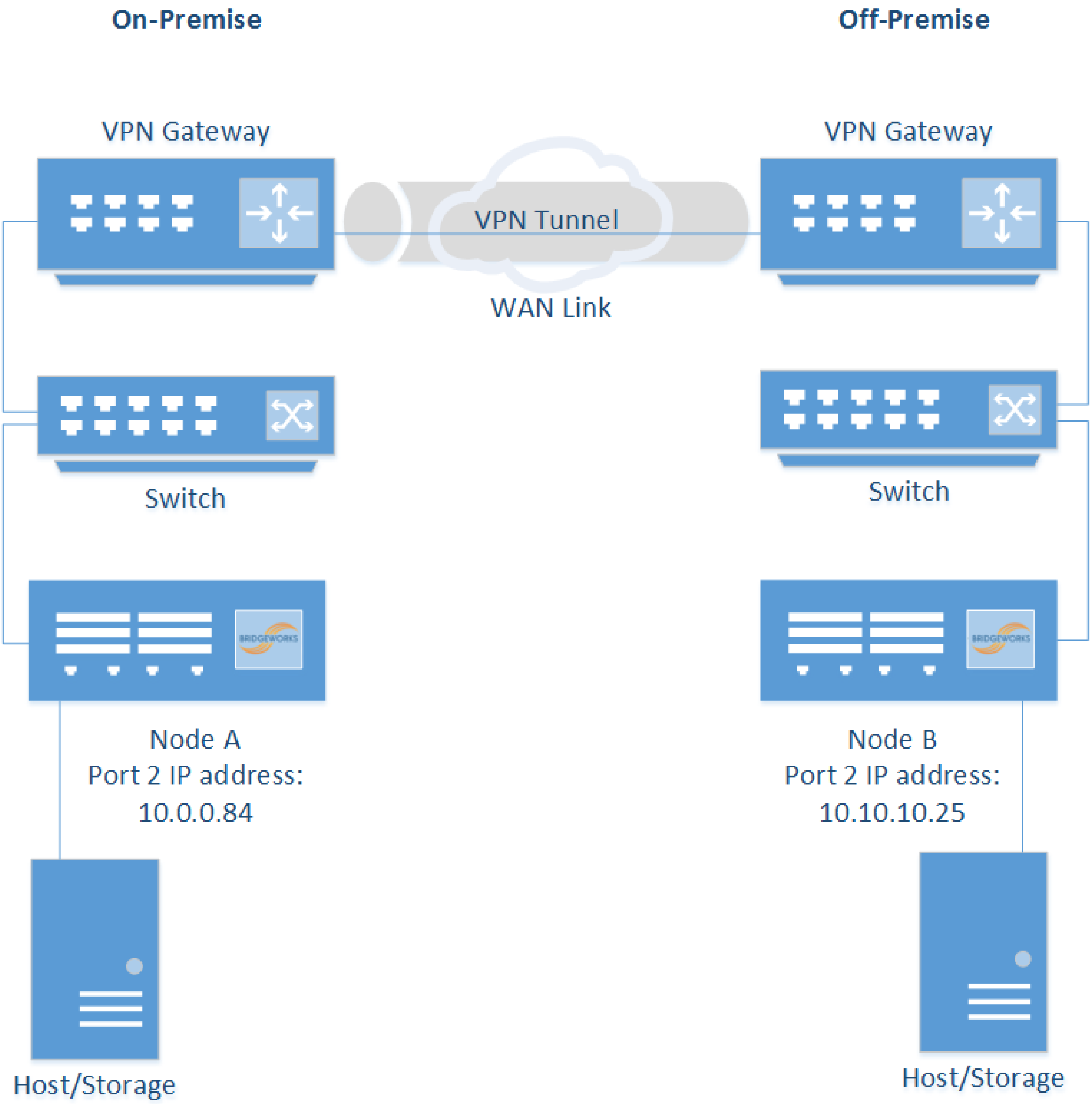


In this example the IP addresses for establishing a Nodal link are the public IP addresses assigned to *Port 2* on the Bridgeworks Nodes:

- Node A: 54.4.244.134
- Node B: 55.4.245.135

6.4 Topology 2: Connecting Bridgeworks Nodes joined via an external VPN

If the On-Premise and Off-Premise sites that will be connected via the Bridgeworks Nodes are already connected via a VPN connection, as per the diagram below, then communication between the private IP addresses on the WAN interface (by default, *Port 2*) of the Bridgeworks Nodes should already be possible.



In this example the IP addresses for establishing a Nodal link are the private IP addresses assigned to *Port 2* on the Bridgeworks Nodes:

- Node A: 10.0.0.84
- Node B: 10.10.10.25

6.5 Topology 3: Connecting Bridgeworks Nodes Using 2 Site NAT

It is possible to connect Bridgeworks Nodes which are behind a NAT, where a router, computer or firewall sits between an internal network and the WAN connection.

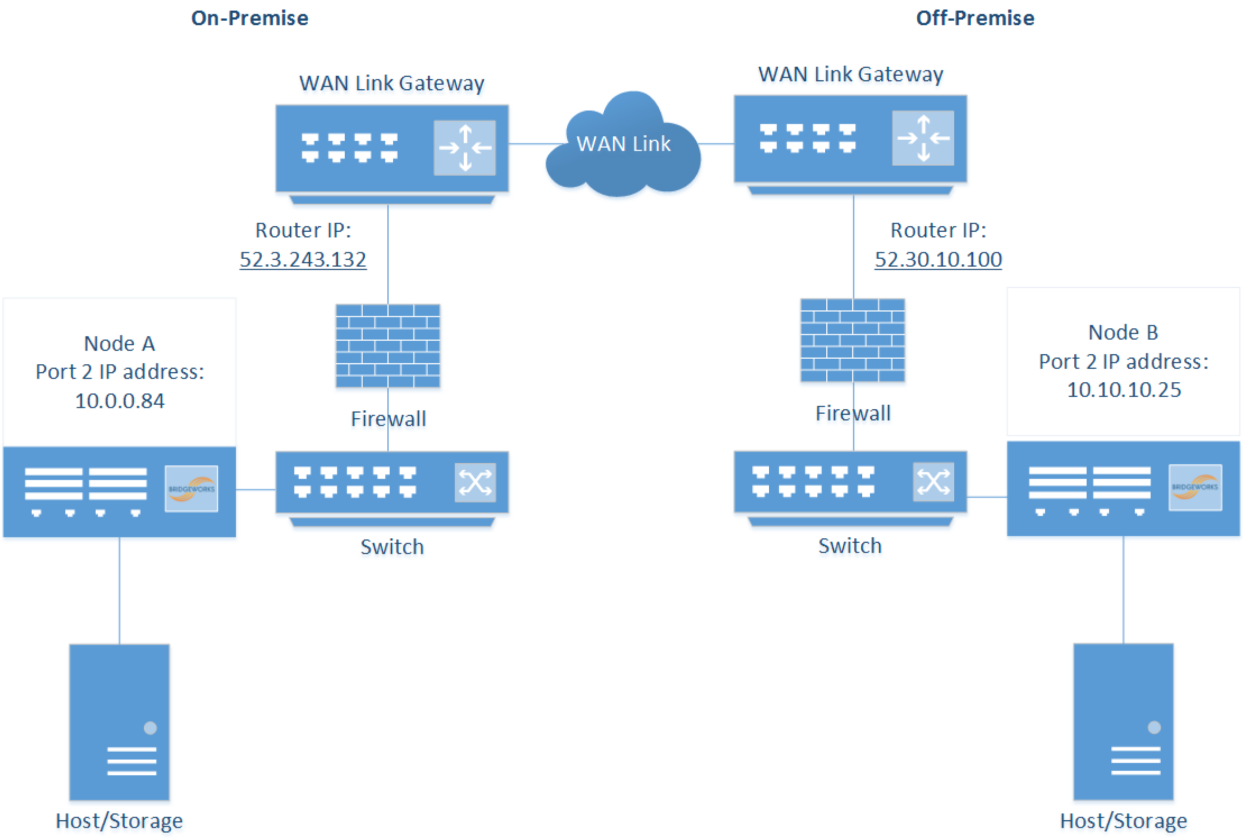
The firewall must be configured with the following sets of NAT port forwarding rules:

Protocol: TCP
Destination Port Range: 16665
Redirect Target IP: <IP addresses of WAN port of the Bridgeworks Node>
Redirect Target Port: 16665

Protocol: UDP
Destination Port Range: 4500
Redirect Target IP: <IP addresses of WAN port of the Bridgeworks Node>
Redirect Target Port: 4500

Protocol: UDP
Destination Port Range: 500
Redirect Target IP: <IP addresses of WAN port of the Bridgeworks Node>
Redirect Target Port: 500

For further assistance with configuring your NAT, please contact your local network administrator. The following diagram gives an overview of an example NAT setup and where the Bridgeworks Nodes would be placed.

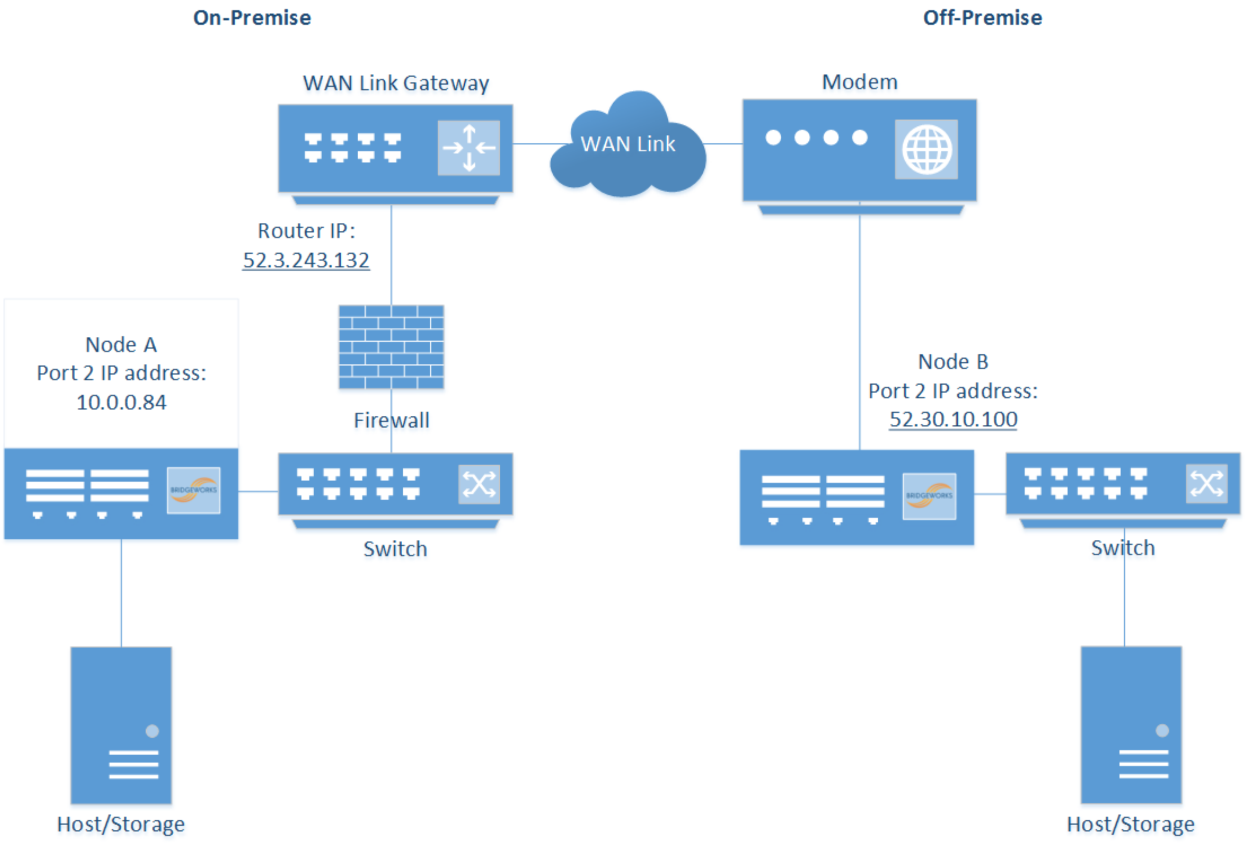


In this example the IP addresses for establishing a Nodal link are the IP addresses of the router, in this case:

- Node A: 52.3.243.132
- Node B: 52.30.10.100

6.6 Topology 4: Connecting to a Bridgeworks Node with a NAT on one site

An alternative to the above topology is for one Bridgeworks Node to be behind a NAT (where a router, computer, or firewall sits between an internal network and the WAN connection), and the second to be accessible through a public IP address. This is useful if you are unable to set any additional firewall policies.



In this example the IP addresses for establishing a Nodal link are the IP address of the router connected to Node A, and the public IP address of Node B.

- Node A: 52.3.243.132
- Node B: 52.30.10.100

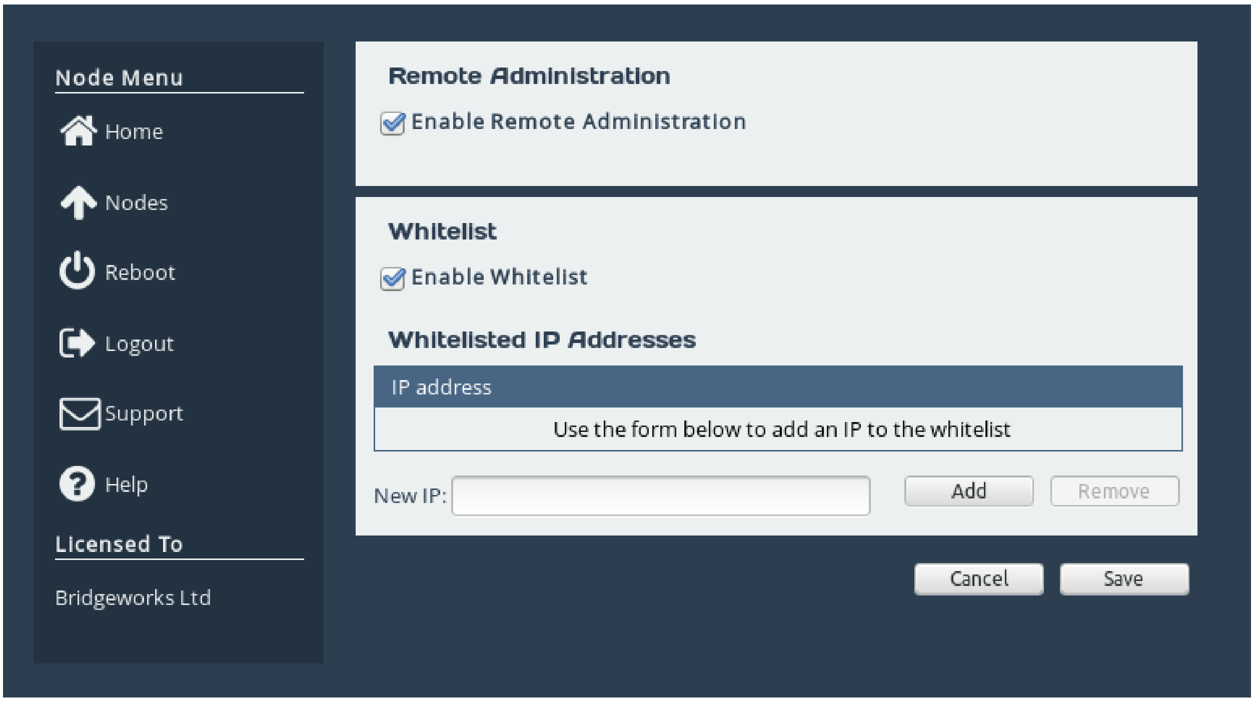
For a successful connection in this example without setting any firewall policies, Node A must first connect to Node B.

6.7 Access Control

Throughout the following sections which refer to *Node A* and *Node B*, use the IP address types found in the previous examples.

Navigate to the *Access Control* page of Node B by going to *Node Management* and clicking on the corresponding icon.

Ensure that under the heading *Whitelist* the *Enable Whitelist* checkbox is ticked. By default this should be the case.



Bridgeworks Ltd

Remote Administration

☑ Enable Remote Administration

Whitelist

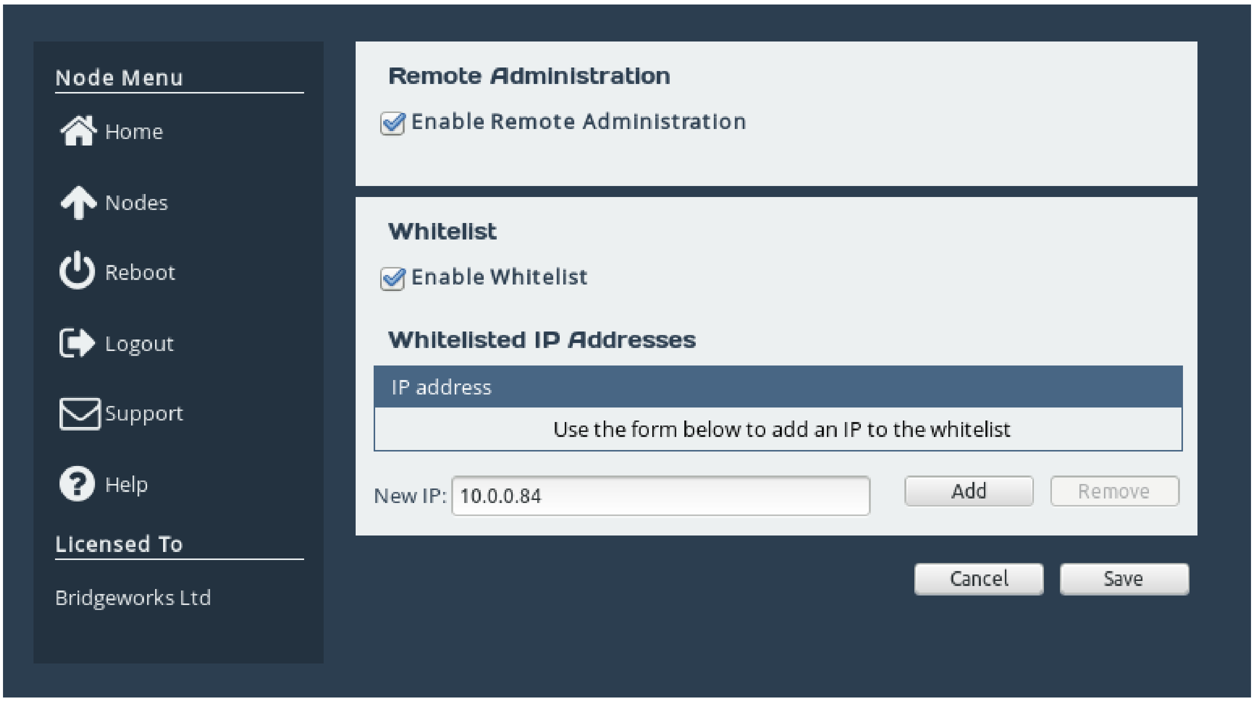
☑ Enable Whitelist

Whitelisted IP Addresses

IP address
Use the form below to add an IP to the whitelist

New IP:

Under *New IP*, enter the IP address of the WAN port of Node A in the entry box, and click the *Add* button.



Remote Administration

☑ Enable Remote Administration

Whitelist

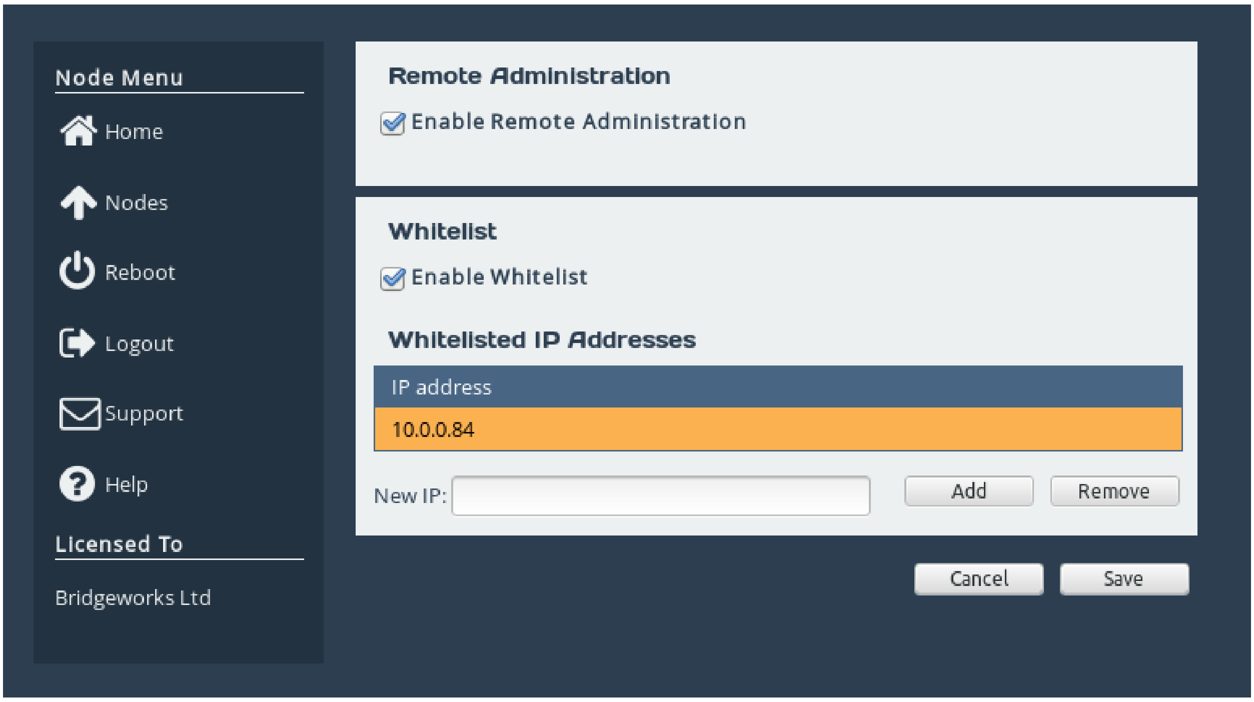
☑ Enable Whitelist

Whitelisted IP Addresses

IP address
Use the form below to add an IP to the whitelist

New IP: 10.0.0.84

When this has been added successfully you will see the IP address entry added to the list, as shown below.



Remote Administration

☑ Enable Remote Administration

Whitelist

☑ Enable Whitelist

Whitelisted IP Addresses

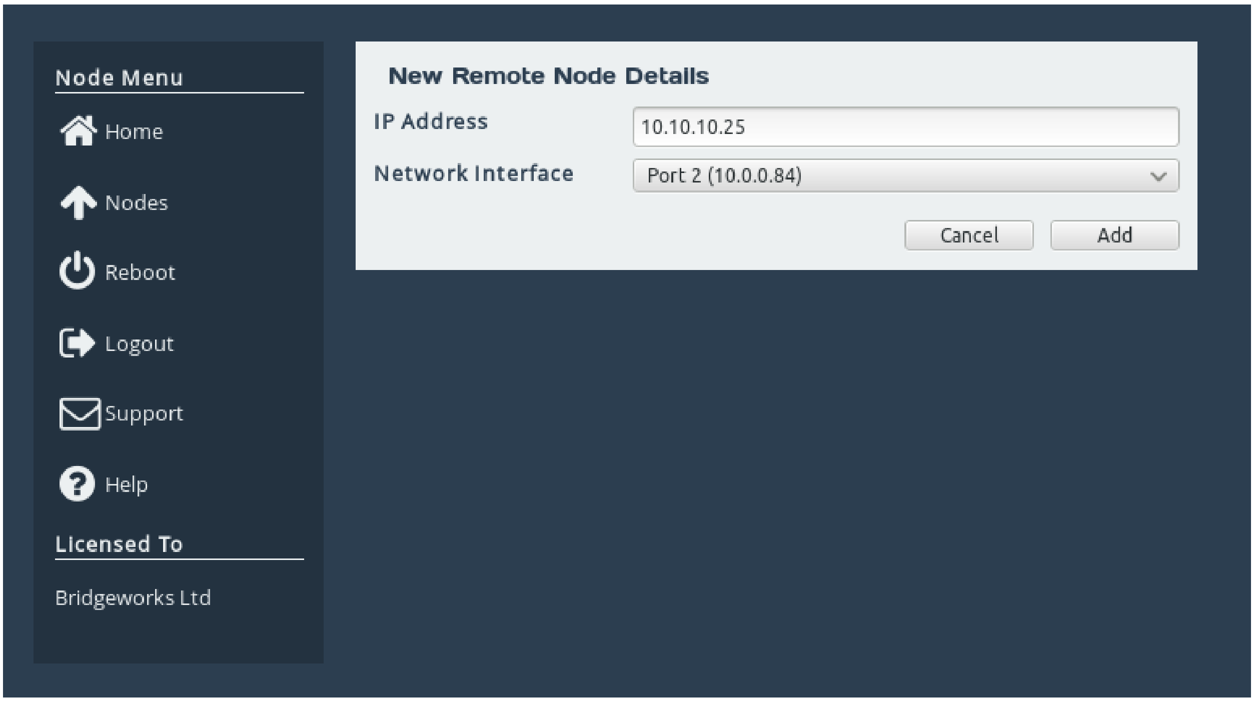
IP address
10.0.0.84

New IP:

Important: If Node B is not behind a NAT, repeat this process on Node A to add the IP address of Node B to the whitelist of Node A.

6.8 Node Management

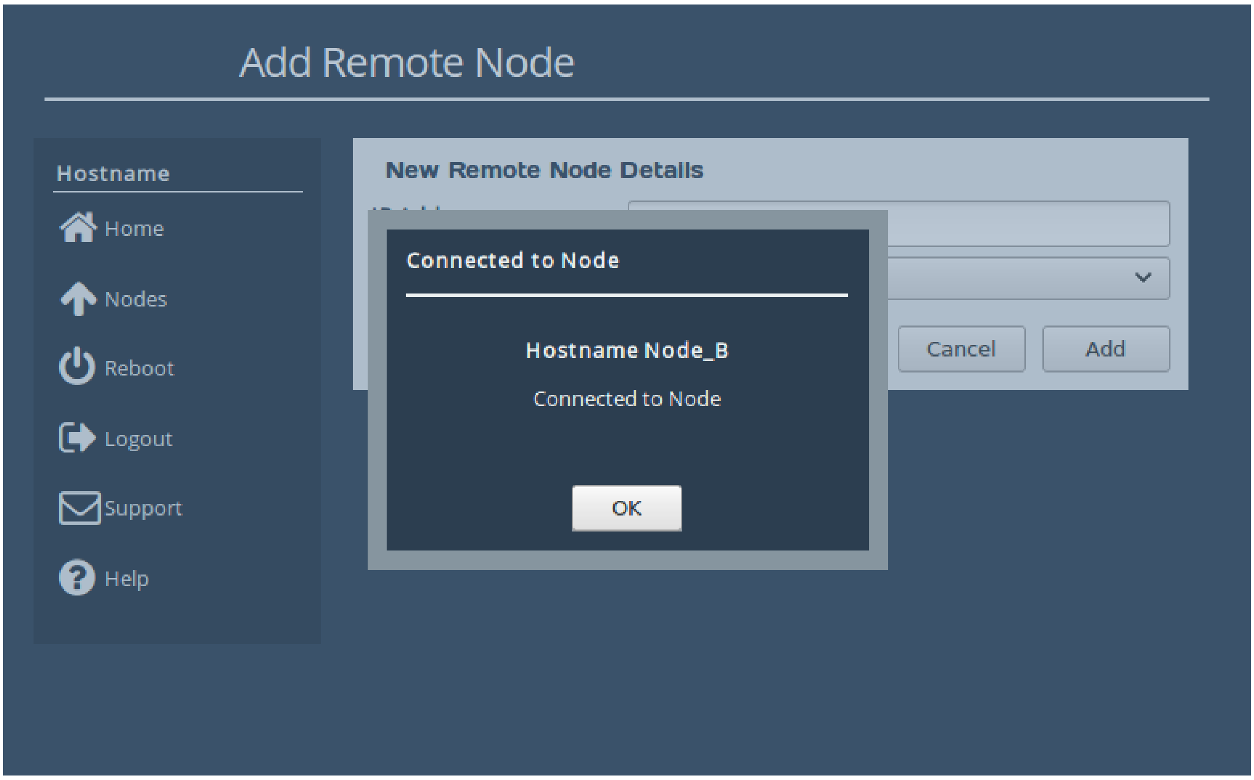
The next stage is to perform the Node Discovery on the WAN link. From the *Node Management* page of Node A, click the *Add Remote Node* icon to navigate to the *Add Remote Node* page. Enter the IP address of Node B’s WAN port in the address field. The *Network Interface* drop-down allows you to change the interface from which you wish to connect. Multiple options will be present if WAN is mapped to multiple network interfaces. Click *Add*, and a connection will be negotiated between the Nodes.



IP Address: 10.10.10.25

Network Interface: Port 2 (10.0.0.84)

When the connection has been established, a dialog will show the hostname of the remote Node.

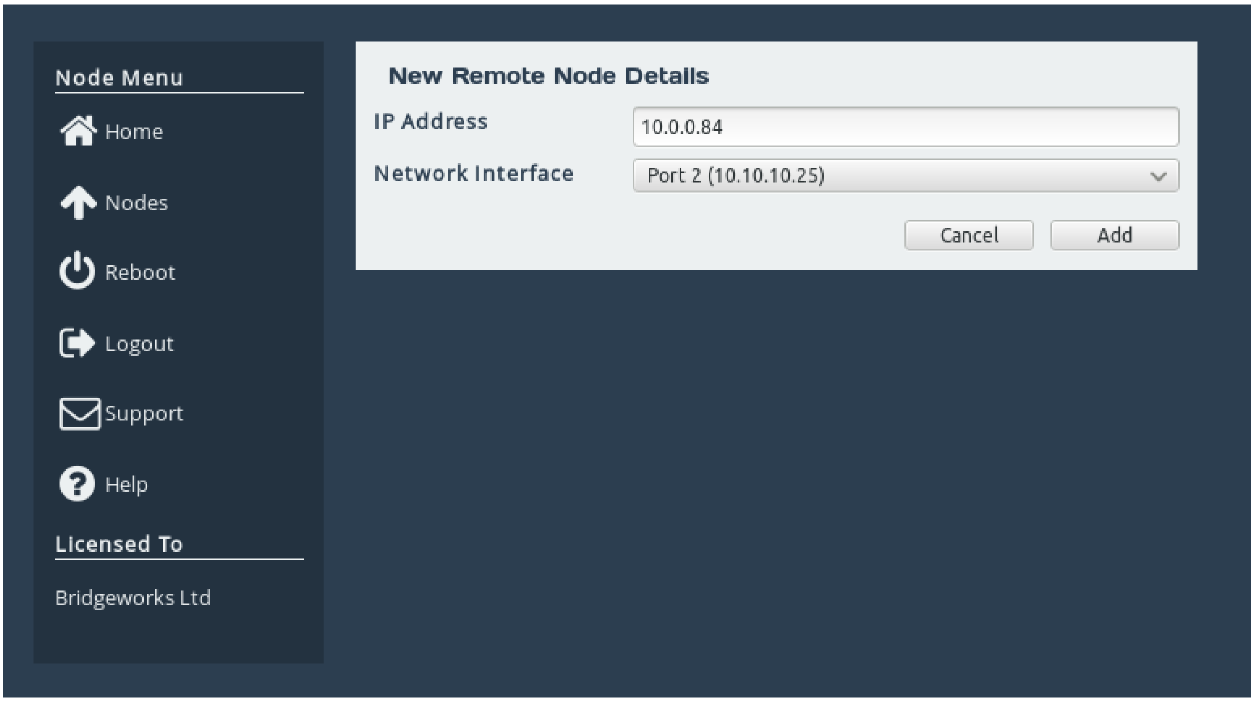


Connected to Node

Hostname Node_B

Connected to Node

The next stage is to perform Node discovery in the other direction. From the *Node Management* of Node B, click the *Add Node* button to bring up a dialog box, and enter the IP address of the WAN port of Node A. Click *Add* to negotiate a connection between the Nodes.



New Remote Node Details

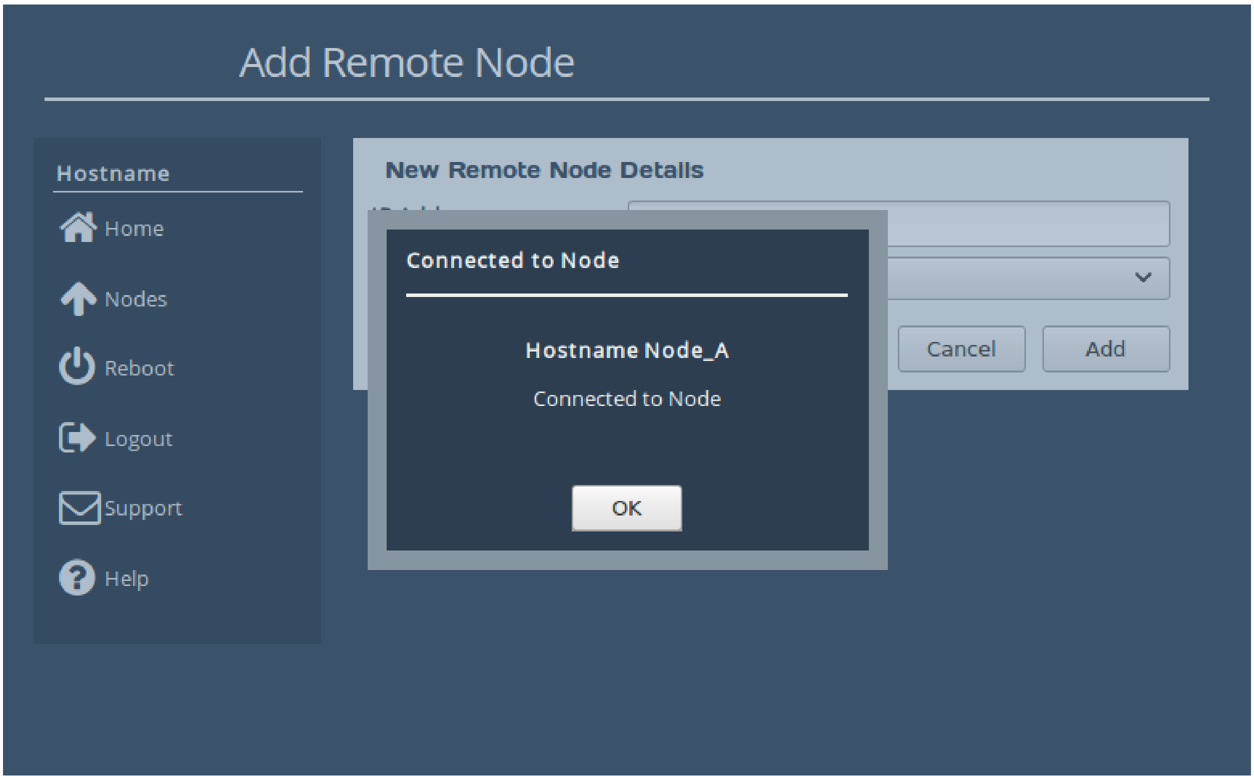
IP Address: 10.0.0.84

Network Interface: Port 2 (10.10.10.25)

Licensed To

Bridgeworks Ltd

When the connection has been established, a dialog will appear.



Connected to Node

Hostname Node_A

Connected to Node

Congratulations, you have successfully set up a connection between your Nodes.

7 Configuring PORTrockIT Acceleration

7.1 Introduction

This section will guide you through how to configure your PORTrockIT Nodes to sit in between the two Endpoints you wish to accelerate.

7.2 Prerequisites

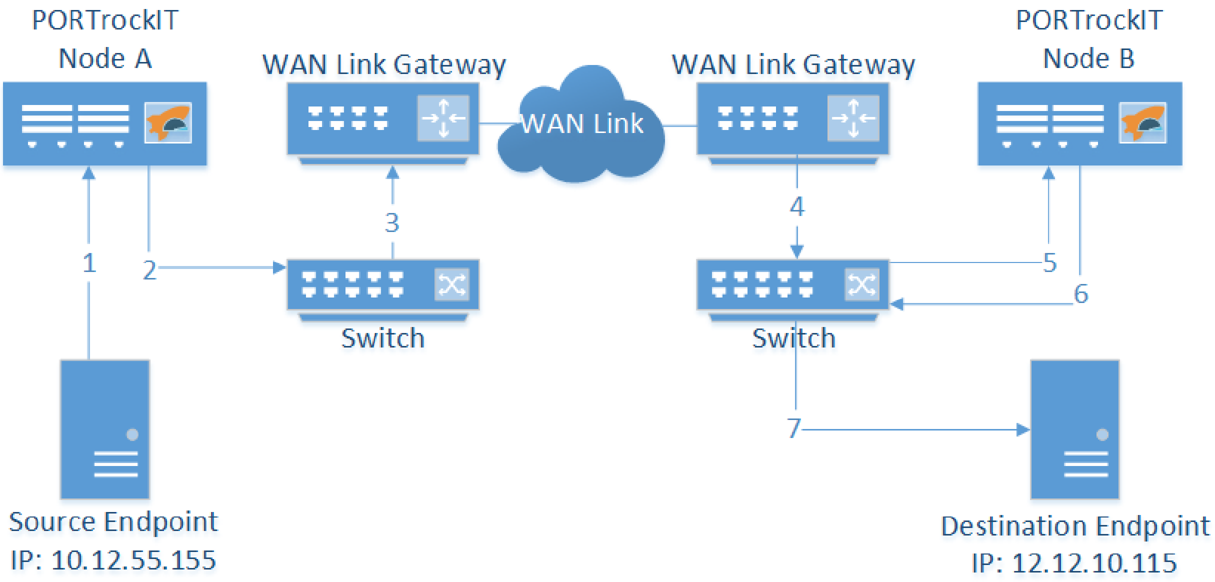
In order to configure PORTrockIT acceleration you must have the following:

- Two PORTrockIT appliances or virtual instances - it is permissible to mix both appliances and virtual instances on the same connection.
- A WAN and PORTrockIT protocol mapping applied.
- A WAN link established between the two PORTrockIT Nodes.

7.3 Adding Services

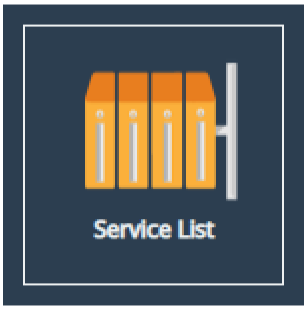
A service defines a part of the local topology, including all information the PORTrockIT Node needs to connect to a target server.

For this section, only the Address will need to be specified to create the service. The topology being used for this example is displayed below.

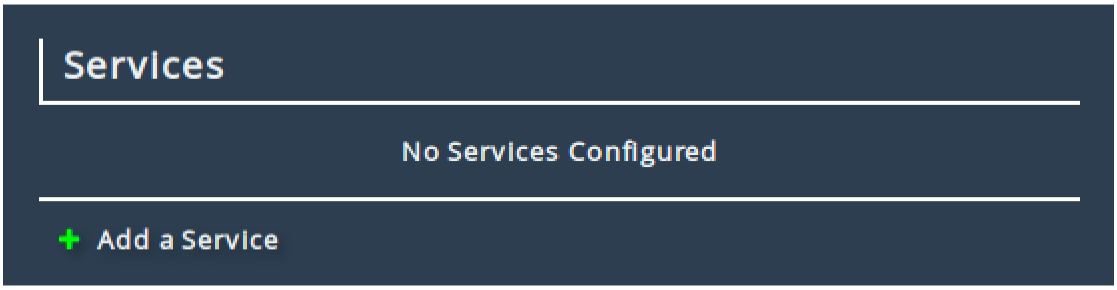


The following instructions only need to be carried out for *Node B*.

To access service configurations, click on the *Service List* icon, under the PORTrockIT section on the home screen.



This is where services are displayed and configured.

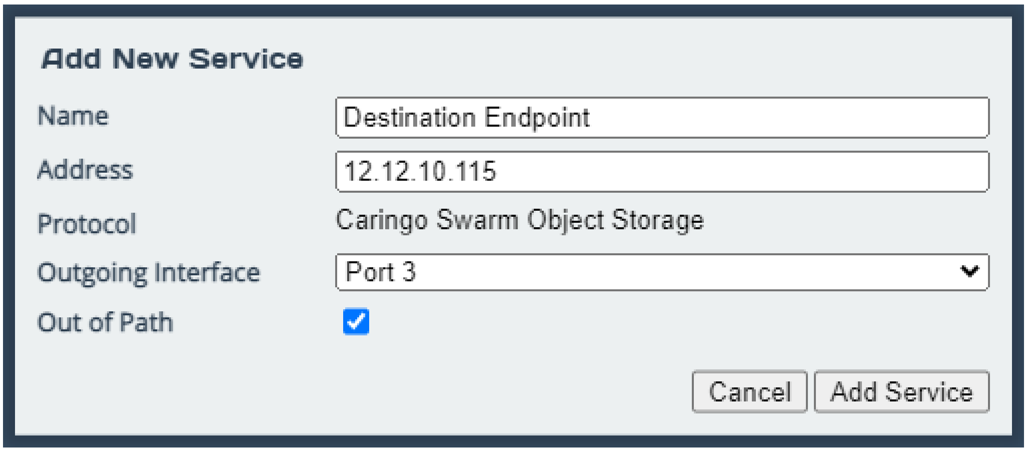

Services

No Services Configured

+ Add a Service

To add a service, click on the *Add a Service* button. This will show a dialog box where local server details can be added. The *Name* field can be changed to something more descriptive if desired. Add the address of the local service into the *Address* field. Options for the address are IPv4, CIDR or a resolvable DNS address. Then select the *Out of Path* checkbox.

Configuration for Node B


Add New Service

Name	Destination Endpoint
Address	12.12.10.115
Protocol	Caringo Swarm Object Storage
Outgoing Interface	Port 3
Out of Path	☑

The above dialog may look different depending on the settings on the *Port Mappings* page. More details on the available settings are in the Bridgeworks user manuals, please refer to the Useful Links section.

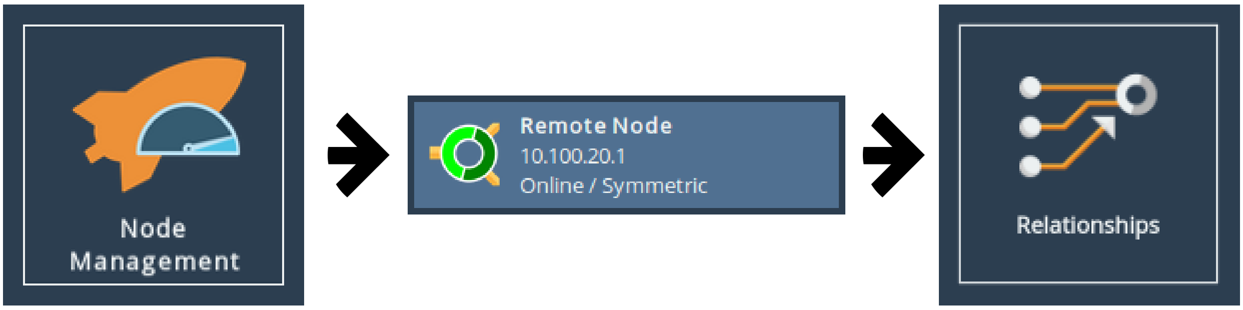
Clicking on the *Add Service* button finishes the creation of the service. The service will now be available to remote Nodes for creating a relationship.

7.4 Establishing Relationships

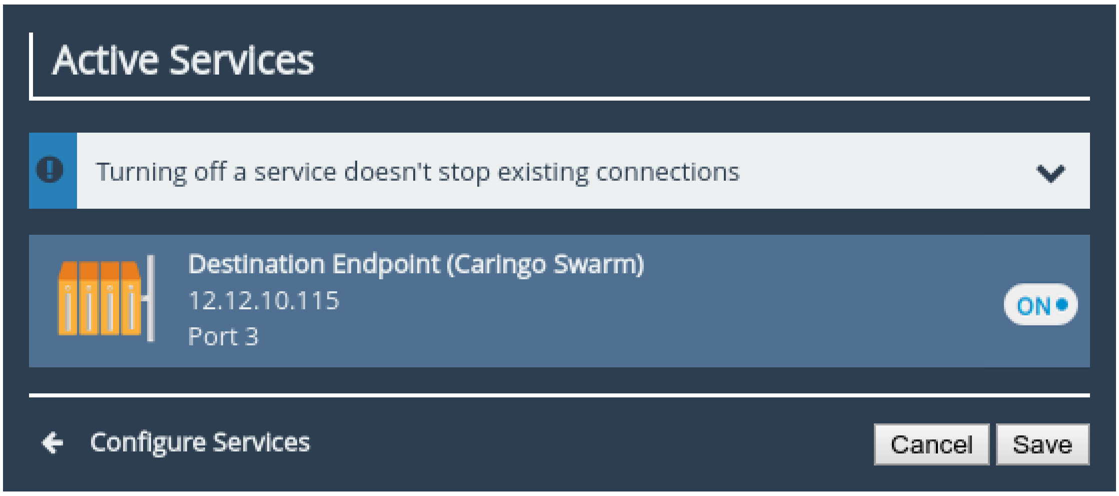
Once a service has been created, it is ready to be associated with one or more remote Nodes. This association between a service and a remote Node is referred to as a relationship. Once the relationships have been created, the PORTrockITs will be ready to accelerate traffic.

These steps will need to be carried out using the GUI of *Node B*.

To create the relationship, navigate to the *Node Management* page which is on the main page under the *PORTrockIT* section. From the list of remote Nodes, click on the button for the Node you would like to make a relationship for. From the *Remote Node Management* page the *Relationships* icon can be found under *Applications & Utilities*.



The *Relationships* page will display the service configured in the previous section. If the service is missing or incorrect click on the *Configure Services* button and follow the steps in Adding Services.



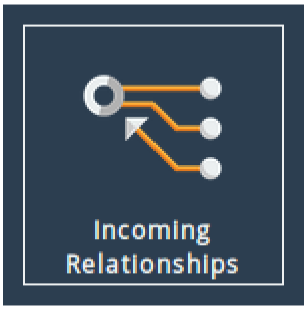
Active Services

Turning off a service doesn't stop existing connections

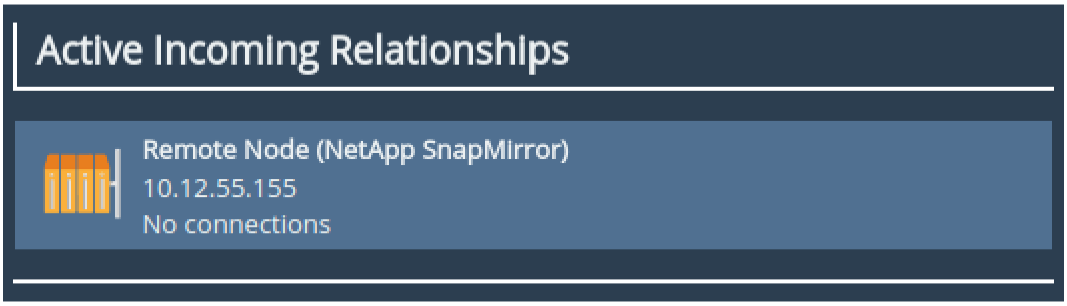
Destination Endpoint (Caringo Swarm)
12.12.10.115
Port 3

To create the relationship, toggle the switch next to the desired service to the ”on” position and save the page.

The relationship should now be visible on the remote Node under the *Incoming Relationships* page accessible from the main page under the *PORTrockIT* section.



After navigating to the *Incoming Relationships* page you will be presented with the following:



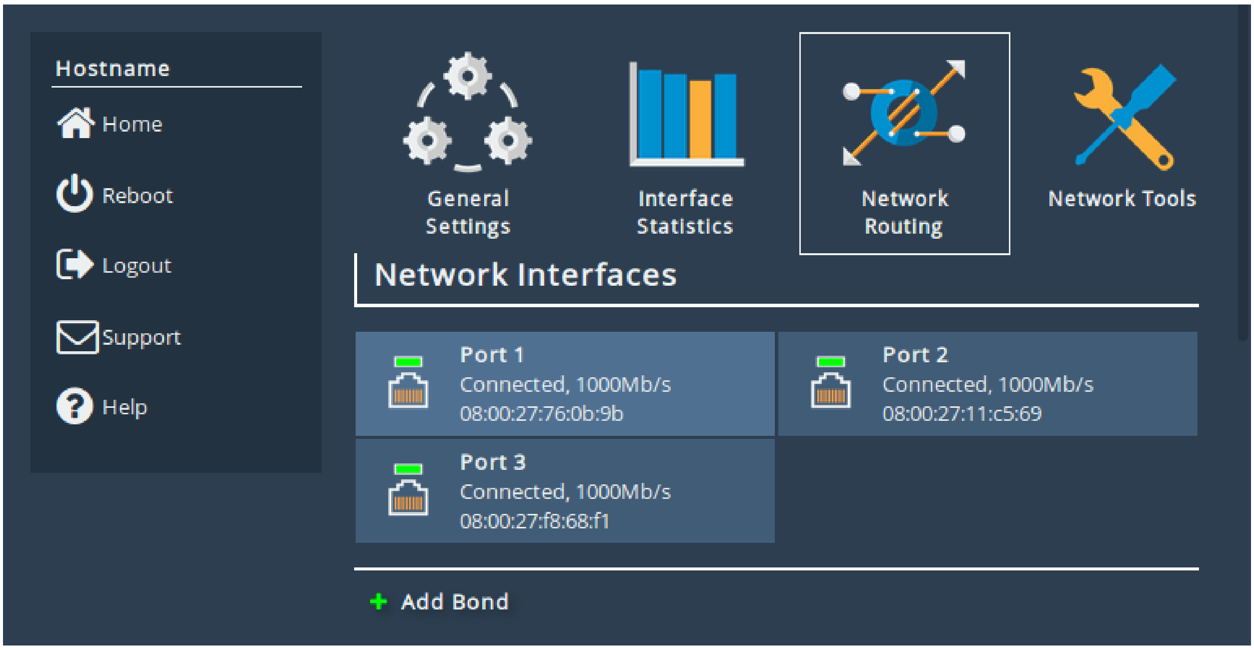
Active Incoming Relationships

Remote Node (NetApp SnapMirror)
10.12.55.155
No connections

If the relationship is displayed in the *Active Incoming Relationships* list then the relationship was successfully created. After this, the software configuration required for accelerating traffic between PORTrockITs is complete.

7.5 Routing for Relationships

In certain configurations, additional routing will have to be set on the PORTrockIT Node for network traffic to know how to reach its destination. In order to add routing rules, navigate to the *Routing* page, which can be found on the Network Connections ( ) page as shown below.



Network Interfaces

Port 1
Connected, 1000Mb/s
08:00:27:76:0b:9b

Port 2
Connected, 1000Mb/s
08:00:27:11:c5:69

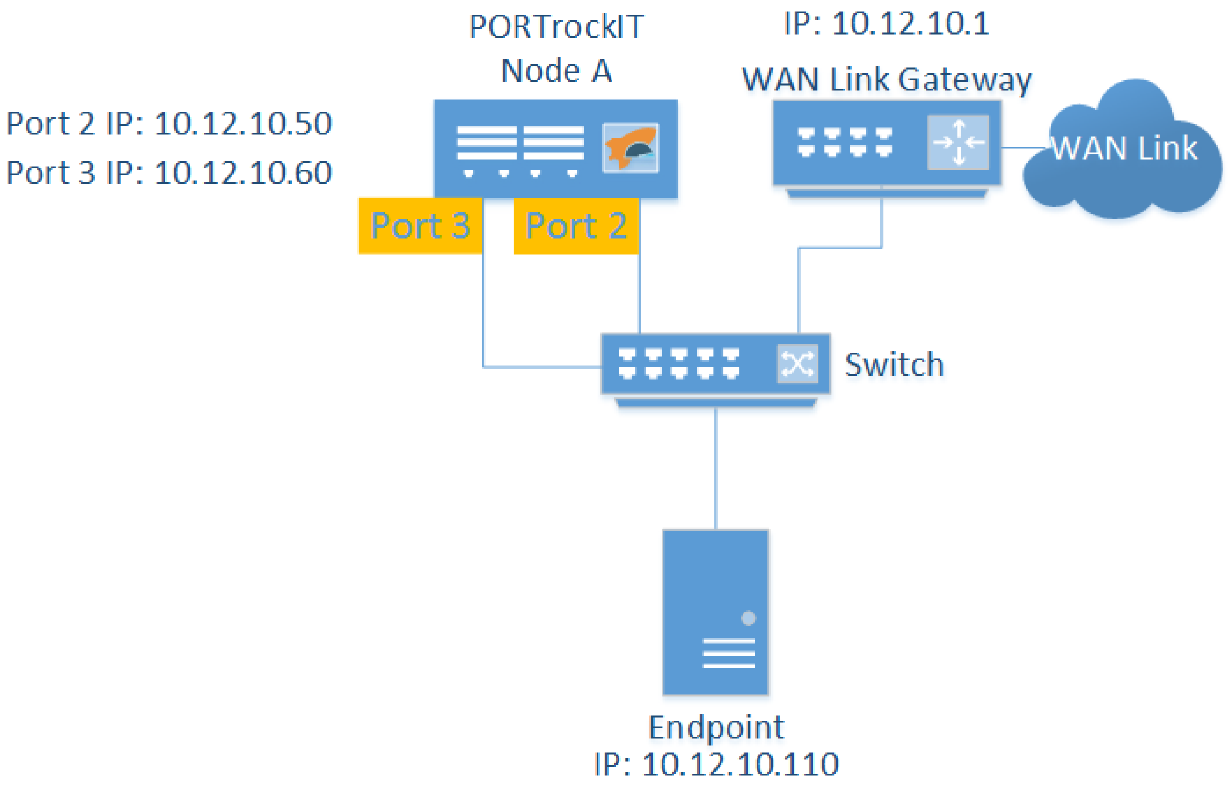
Port 3
Connected, 1000Mb/s
08:00:27:f8:68:f1

Important: Routes created automatically by the system are added with a metric of 1, allowing you to override defaults by using a metric of 0.

The following section contains example topologies with routing rules. Please substitute the IP addresses in the examples with your own. If your use case is not explained, or you need further assistance please contact support@4bridgeworks.com.

7.5.1 Example 1 - WAN and LAN on the same subnet

In this example the PORTrockIT Node has two interfaces on the same subnet where one is the WAN interface (*Port 2*) and the other as the LAN interface (*Port 3*). By default, traffic destined for anything on the subnet will be sent out of *Port 2*, so a routing rule is necessary to use *Port 3* for sending network traffic to the endpoint.



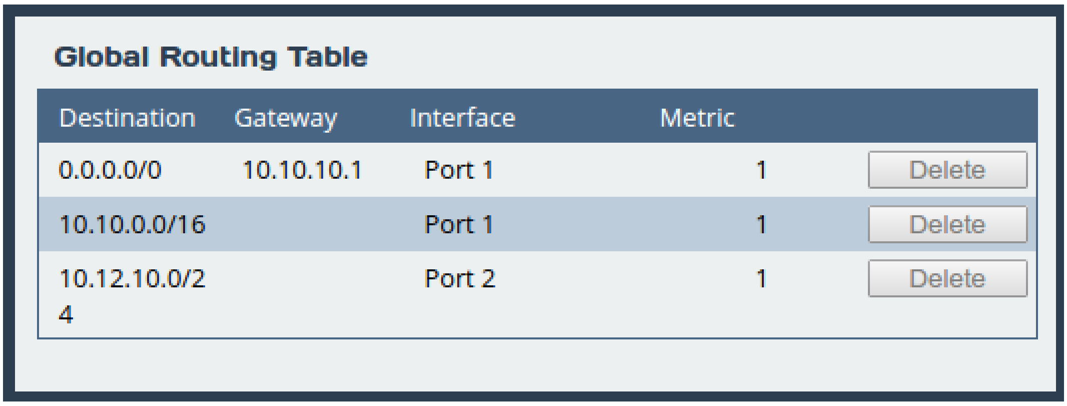
This example explains the routing needed on *Node A*, which has the following 3 ports:

Port 1 Management interface and default route

Port 2 WAN interface (`10.12.10.50`)

Port 3 LAN interface (`10.12.10.60`)

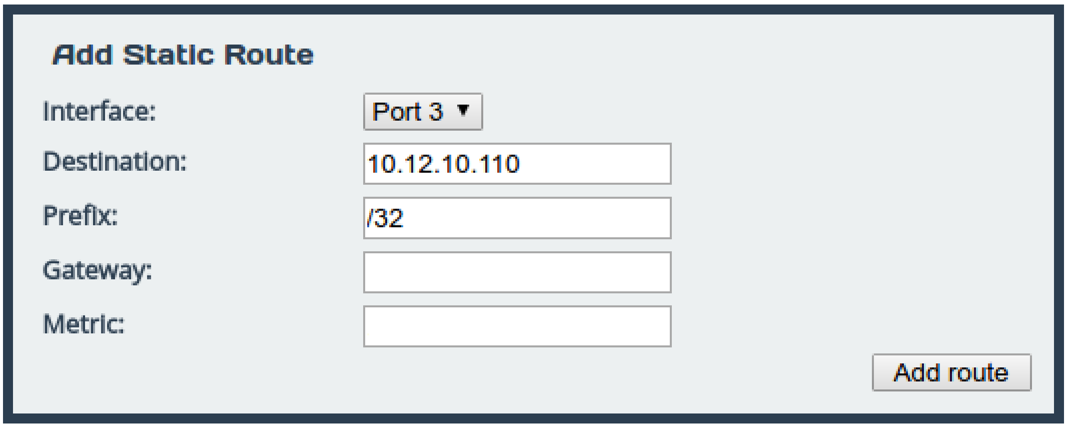
The default routing for *Node A* is shown below.



Global Routing Table

Destination	Gateway	Interface	Metric	
0.0.0.0/0	10.10.10.1	Port 1	1	Delete
10.10.0.0/16		Port 1	1	Delete
10.12.10.0/24		Port 2	1	Delete

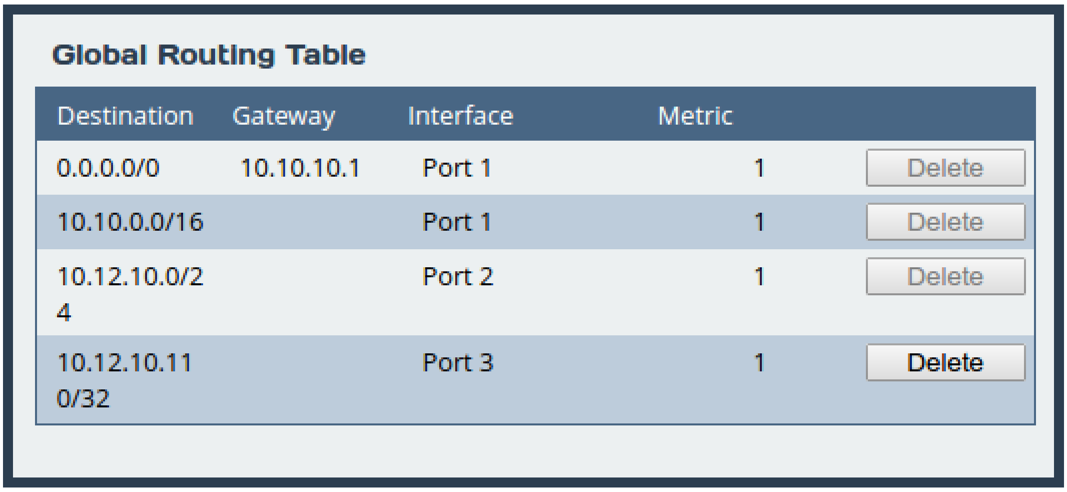
Currently *Node A* will be sending traffic destined for the *Endpoint* from *Port 2* instead of *Port 3*. To resolve this, a static route needs to be added.



Add Static Route

Interface:	Port 3 ▼
Destination:	10.12.10.110
Prefix:	/32
Gateway:	
Metric:	

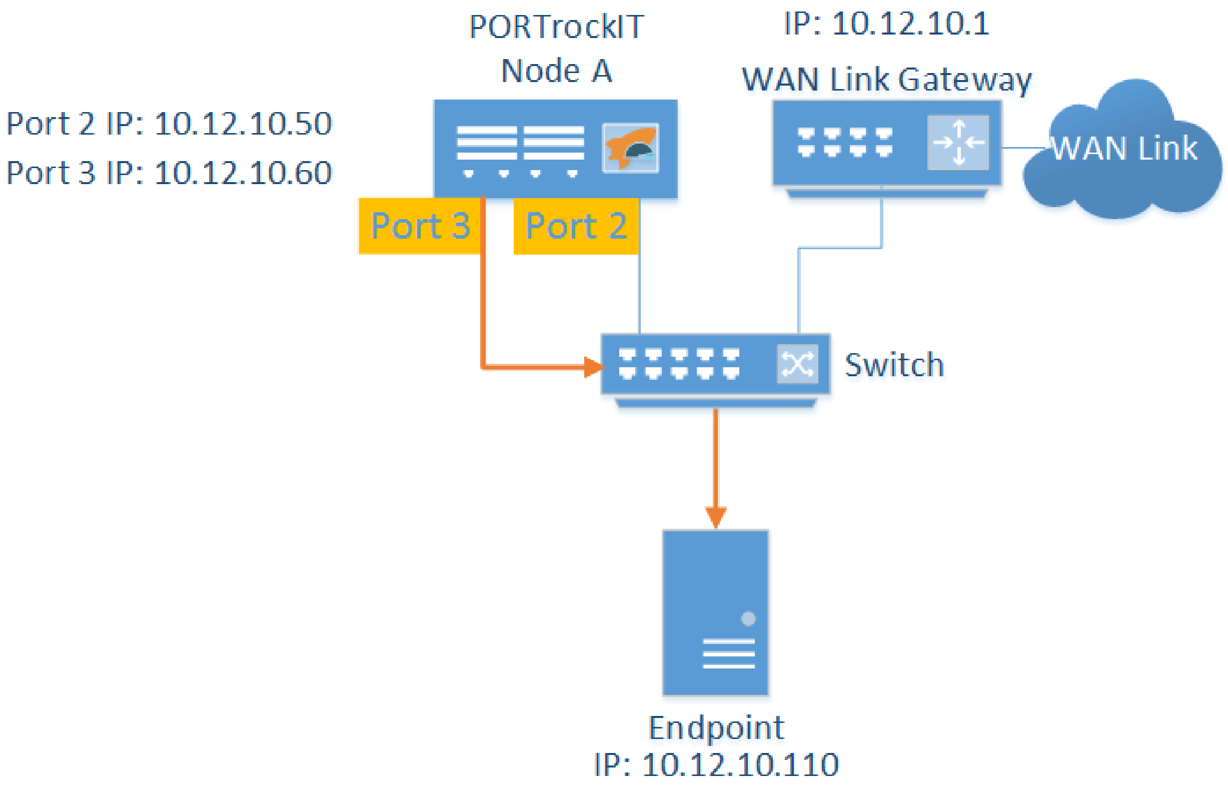
Clicking *Add route* will add the route and it will now be displayed in the *Global Routing Table* as shown below.



Global Routing Table

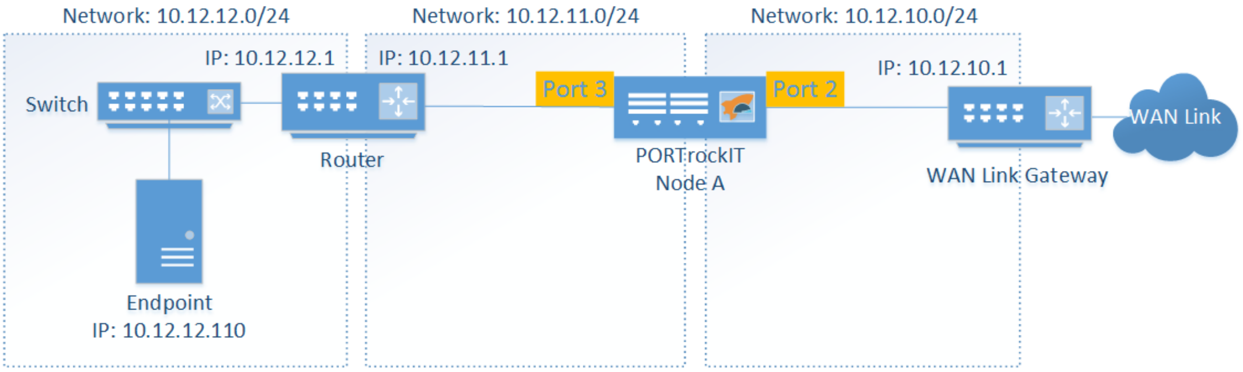
Destination	Gateway	Interface	Metric	
0.0.0.0/0	10.10.10.1	Port 1	1	Delete
10.10.0.0/16		Port 1	1	Delete
10.12.10.0/24		Port 2	1	Delete
10.12.10.110/32		Port 3	1	Delete

Network traffic for the *Endpoint* will now go through *Port 3*.



7.5.2 Example 2 - Endpoint on different subnet to LAN interface

In this example the PORTrockIT Node does not know how to send traffic to the `10.12.12.0/24` subnet. Routing rules need to be configured so the Node knows to send traffic to the router and not the WAN link gateway.



This example explains the routing needed on *Node A*, which has the following 3 ports:

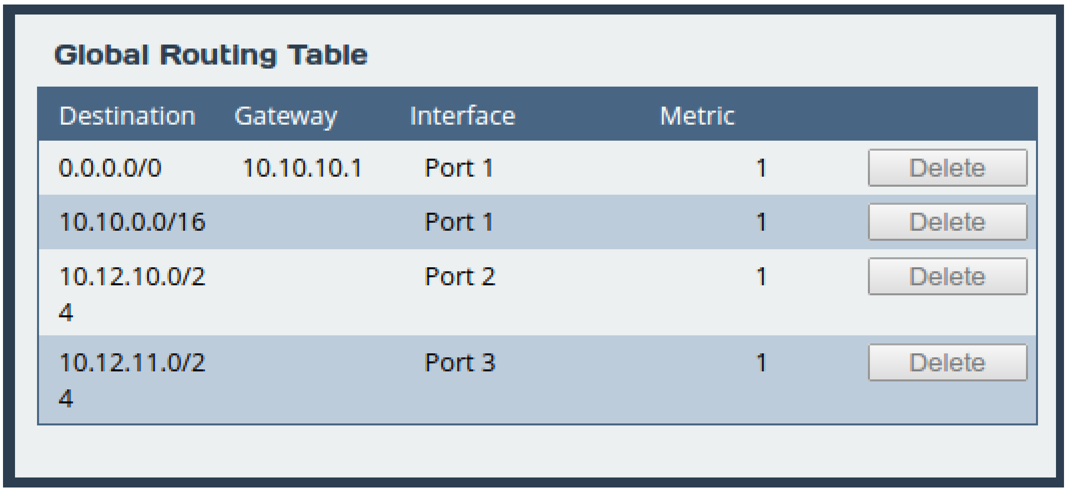
Port 1 Management interface and default route

Port 2 WAN interface on the `10.12.10.0/24` network

Port 3 LAN interface on the `10.12.11.0/24` network

The router, between *Node A* and the switch attached to the *Endpoint*, has two ports with IPs `10.12.11.1` and `10.12.12.1`, and knows how to route traffic between the 2 subnets on either side.

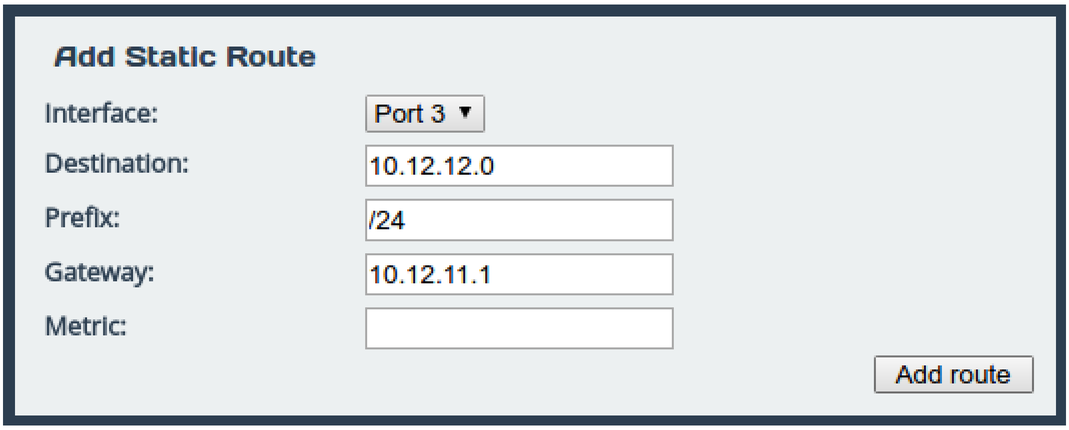
The default routing for *Node A* is shown below.



Global Routing Table

Destination	Gateway	Interface	Metric	
0.0.0.0/0	10.10.10.1	Port 1	1	Delete
10.10.0.0/16		Port 1	1	Delete
10.12.10.0/24		Port 2	1	Delete
10.12.11.0/24		Port 3	1	Delete

Currently *Node A* doesn't know how to reach the `10.12.12.0/24` network so traffic for the *Endpoint* will be lost. To resolve this, a static route needs to be added.



Add Static Route

Interface: Port 3 ▼

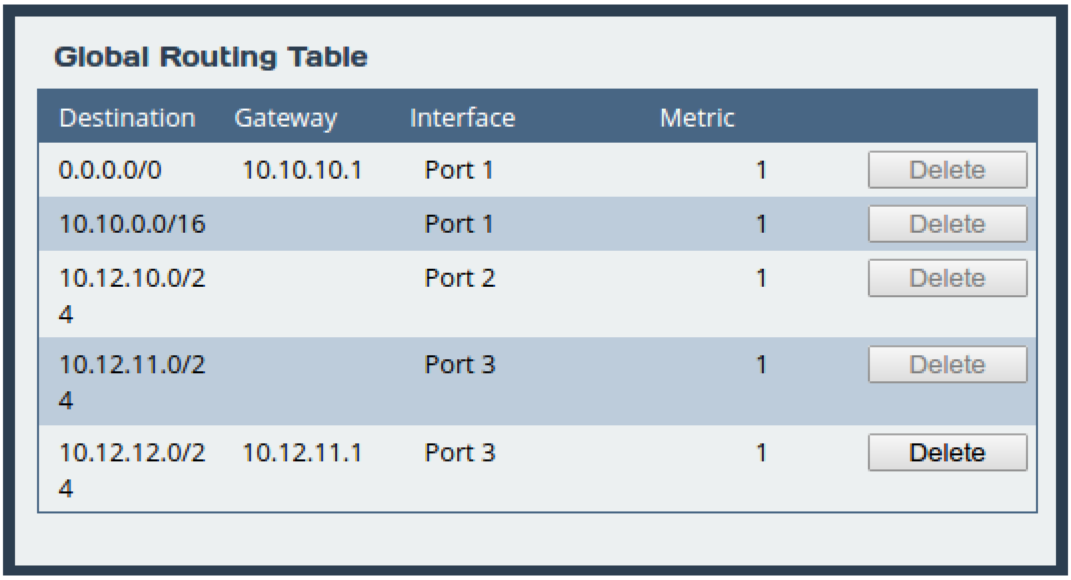
Destination: 10.12.12.0

Prefix: /24

Gateway: 10.12.11.1

Metric:

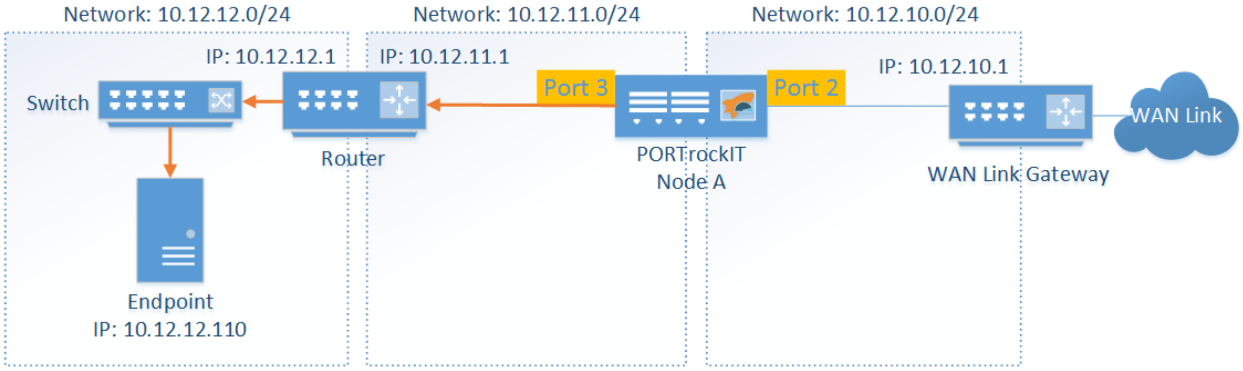
Clicking *Add route* will add the route and it will now be displayed in the *Global Routing Table* as shown below.



Global Routing Table

Destination	Gateway	Interface	Metric	
0.0.0.0/0	10.10.10.1	Port 1	1	Delete
10.10.0.0/16		Port 1	1	Delete
10.12.10.0/24		Port 2	1	Delete
10.12.11.0/24		Port 3	1	Delete
10.12.12.0/24	10.12.11.1	Port 3	1	Delete

Network traffic for the *Endpoint* will be sent from *Port 3* and be directed through the router.



If you require any further assistance with your physical network topology please contact Bridgeworks support team at support@4bridgeworks.com.

8 Accelerating a Windows Hosts traffic with a guest Hyper-V PORTrockIT

8.1 Introduction

When using Hyper-V it is possible to take network traffic from the host and accelerate it through a virtual instance of a PORTrockIT running as a guest. This type of configuration is applicable for DFSR and Live Migration of VMs.

In order to do this the virtual networking must allow direct communication between the host and the guest PORTrockIT.

There are two solutions to allow a Hyper-V host to communicate with its guest through a virtual network connection:

- Allow the host to tap into existing VNets the PORTrockIT is using for the LAN link. This would expose the host to all traffic on that VNet.
- Add an additional *internal* VNet specifically to connect the host to the PORTrockIT. This would create a private connection between the host and the PORTrockIT. In addition, this connection could be removed without impeding the existing LAN connection for other accelerated traffic.

> Note: The guide here discusses the Host system and Hyper-V Manager. Different terms are used between them. ’vEthernet’, ’Virtual Switch’ and ’VNet’ all refer to the same Virtual Network Connection.

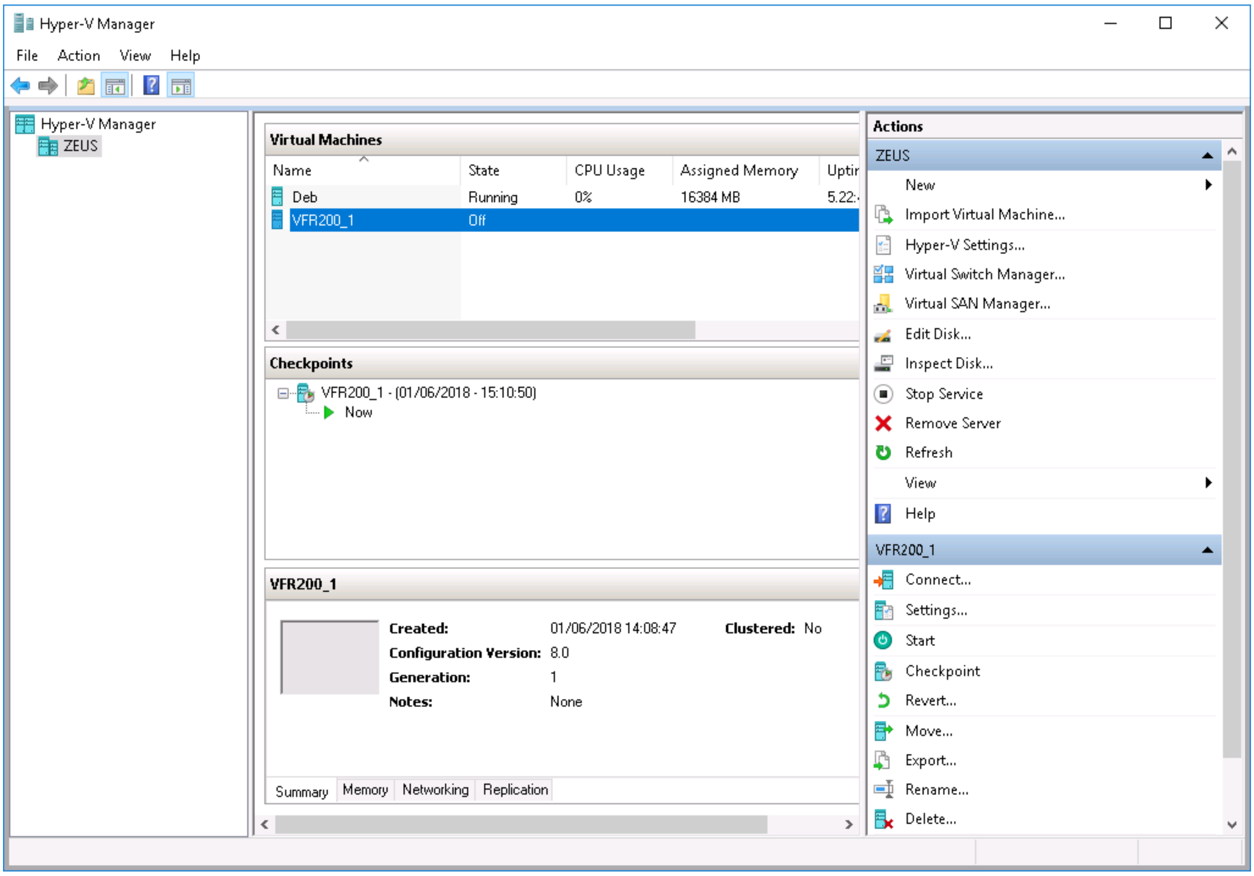
8.2 Connecting host to existing VNet

Setting up a PORTrockIT involves having a WAN and LAN port; if the PORTrockIT was setup to accelerate connections that exist outside of the host, then it should already have the LAN port tied to a physical network connection.

To attach the PORTrockIT to a physical network connection, an *external* network adapter will be required.

To allow the host to connect to the existing external LAN port the settings for that network adapter need to be set.

In the *Virtual Switch Manager* the settings for the desired external switch need to be checked.



Name	State	CPU Usage	Assigned Memory	Uptir
Deb	Running	0%	16384 MB	5.22:
VFR200_1	Off			

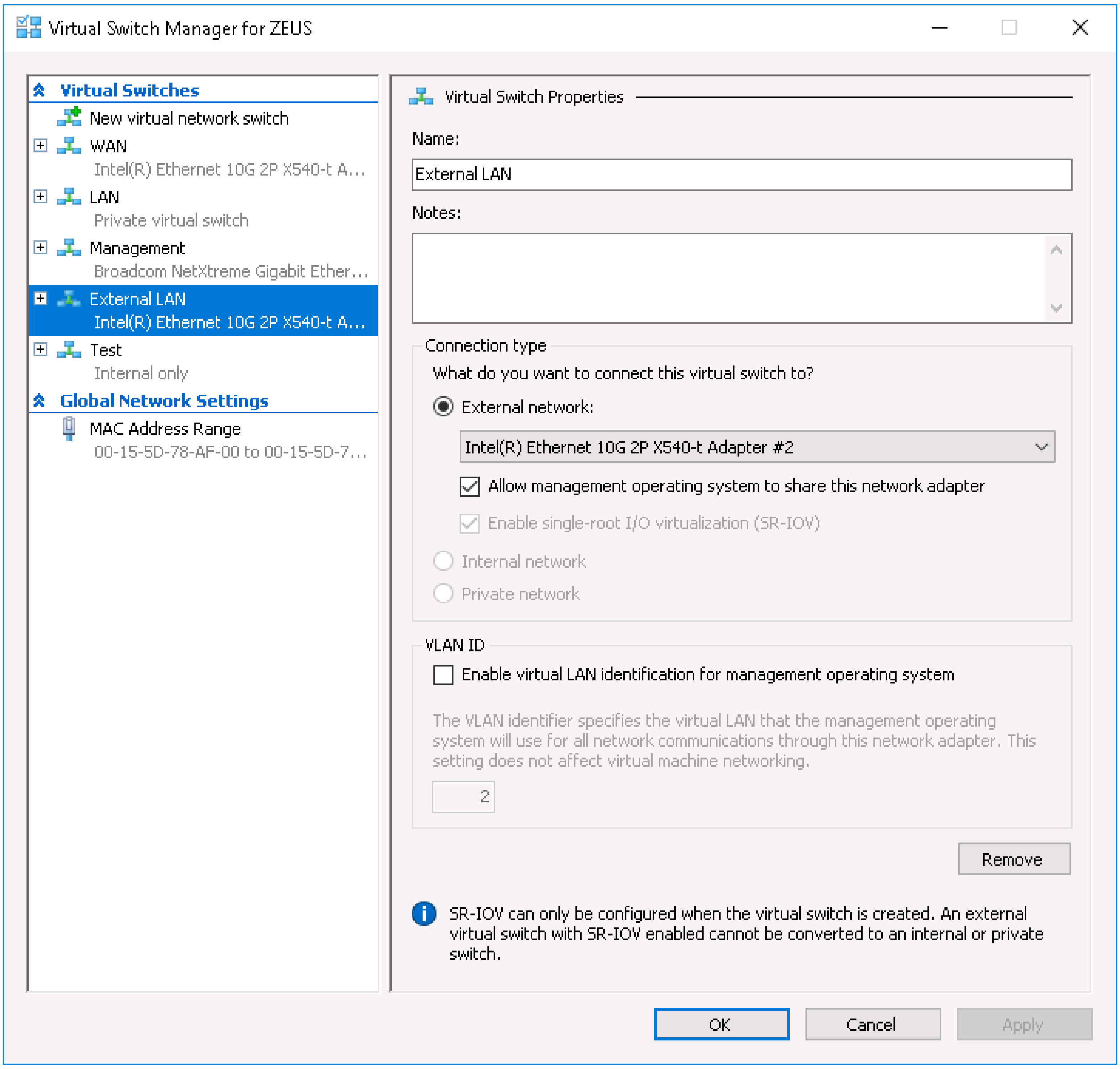
VFR200_1 - (01/06/2018 - 15:10:50)
Now

Created: 01/06/2018 14:08:47 **Clustered:** No
Configuration Version: 8.0
Generation: 1
Notes: None

Select the network connection that is used for the PORTrockIT LAN port.

	Note: Network connections can be checked by accessing the *Settings* option for the PORTrockIT by right clicking its name in the Hyper-V manager main window and selecting *Settings*. The left hand column will include all network connections that are attached to that PORTrockIT.

In the *Virtual Switch Properties* the *Connection type* will be set to *External network* and have an associated physical network connection.



- New virtual network switch
- WAN — Intel(R) Ethernet 10G 2P X540-t A...
- LAN — Private virtual switch
- Management — Broadcom NetXtreme Gigabit Ether...
- External LAN — Intel(R) Ethernet 10G 2P X540-t A...
- Test — Internal only
- MAC Address Range — 00-15-5D-78-AF-00 to 00-15-5D-7...

Name: External LAN

Notes:

Connection type

What do you want to connect this virtual switch to?

● External network:

Intel(R) Ethernet 10G 2P X540-t Adapter #2

☑ Allow management operating system to share this network adapter

☑ Enable single-root I/O virtualization (SR-IOV)

○ Internal network

○ Private network

VLAN ID

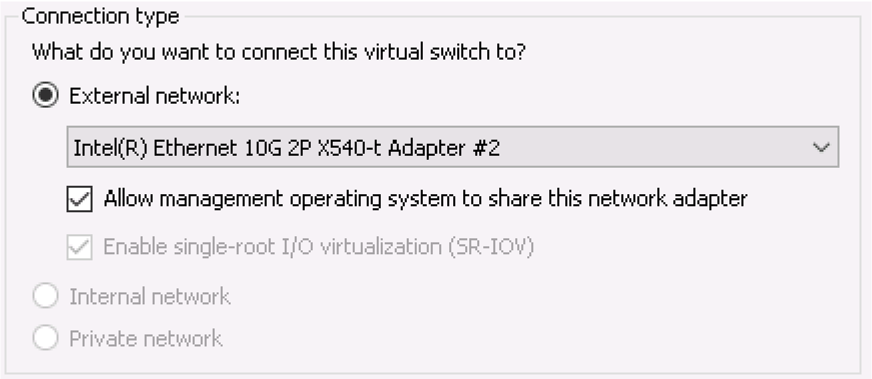
□ Enable virtual LAN identification for management operating system

The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

2

SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.

Ensure that the checkbox labeled *Allow management operating system to share this network adapter* beneath the physical network connection dropdown menu is checked.



Connection type

What do you want to connect this virtual switch to?

● External network:

Intel(R) Ethernet 10G 2P X540-t Adapter #2

☑ Allow management operating system to share this network adapter

☑ Enable single-root I/O virtualization (SR-IOV)

○ Internal network

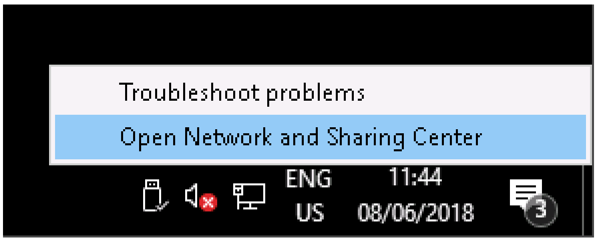
○ Private network

Click *Apply* and then *OK*.

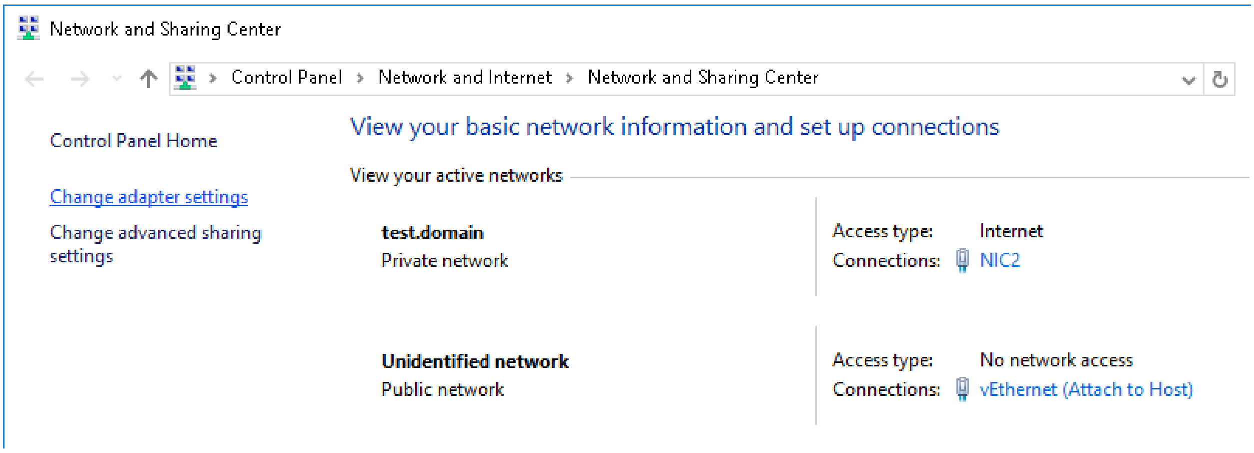
At this stage the virtual switch is now exposed to the host, this can be confirmed by bringing up the

Network Connections in the host system.

To access the *Network Settings*, right click on the network icon at the bottom right of the screen and select *Open Network and Sharing Center*.



In the new window select *Change adapter settings* in the column on the left.


Network and Sharing Center
Control Panel › Network and Internet › Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings

View your basic network information and set up connections

View your active networks

test.domain Private network	Access type: Internet Connections: NIC2
Unidentified network Public network	Access type: No network access Connections: vEthernet (Attach to Host)

In the *Network Connections* window there will be a vEthernet with the same name given in the *Virtual Switch Manager*.

If the vEthernet is present then the PORTrockIT LAN port is exposed to the host and can be used to accelerate host data.

Note: Please ensure that the application requiring acceleration is using the PORTrockIT LAN port for its connection and that appropriate services are setup on the PORTrockIT. See Section 7.5: Routing for Relationships.

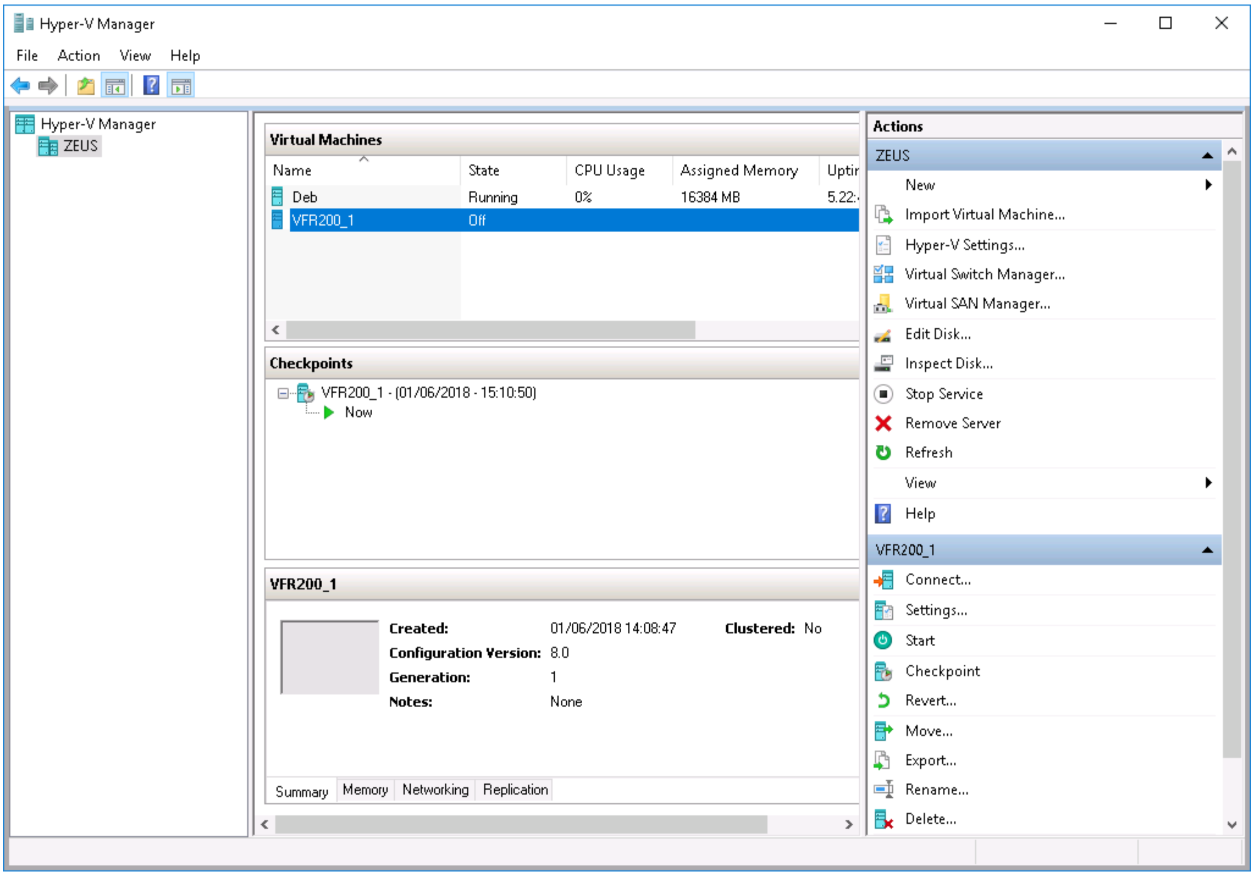
8.3 Adding a dedicated connection

When it is not desirable to have a physical LAN connection to the PORTrockIT, a private network connection can be used to restrict communication to internal guests only.

At this point the host would be unable to connect to the private LAN port of the PORTrockIT.

To enable acceleration of the host data another LAN connection needs to be setup.

In the Hyper-V manager open the *Virtual Switch Manager*, located in the *Actions* column on the right.



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptir
Deb	Running	0%	16384 MB	5.22:·
VFR200_1	Off			

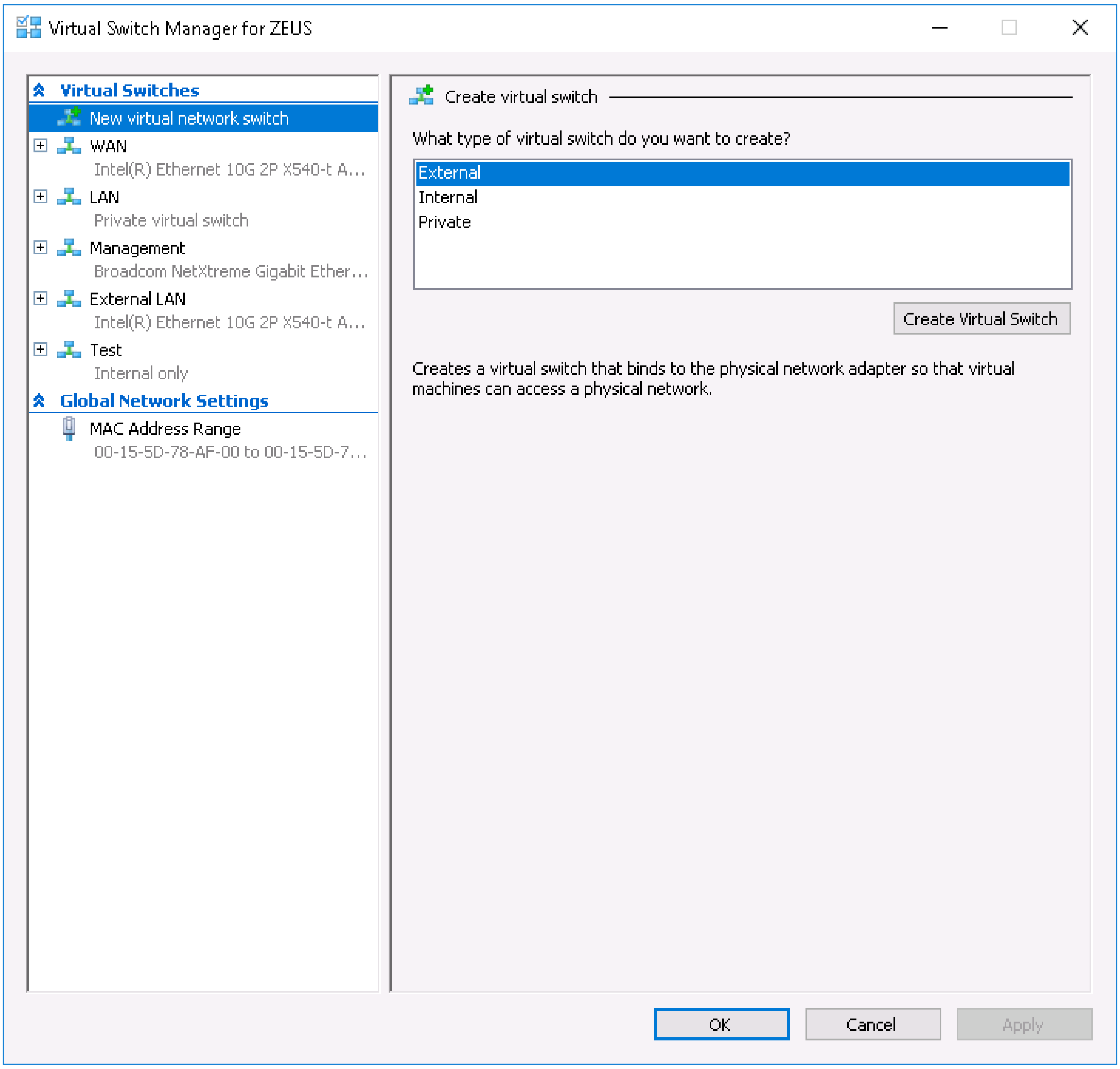
Checkpoints

VFR200_1 - (01/06/2018 - 15:10:50)
Now

VFR200_1

Created:	01/06/2018 14:08:47	**Clustered:**	No
Configuration Version:	8.0		
Generation:	1		
Notes:	None		

In the *Virtual Switch Manager*, select *New virtual network switch*.



Virtual Switch Manager for ZEUS

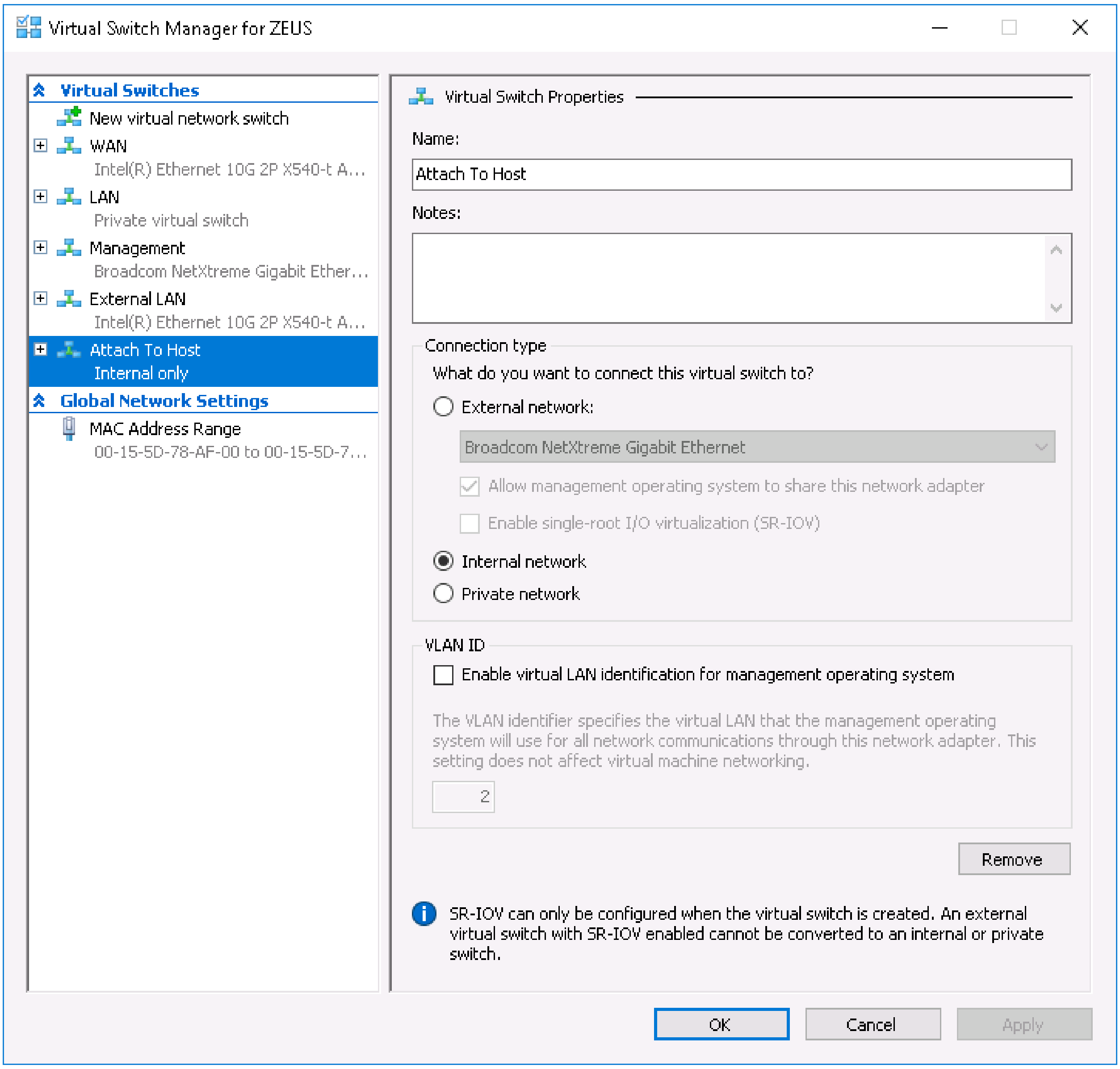
Virtual Switches
New virtual network switch
WAN
Intel(R) Ethernet 10G 2P X540-t A...
LAN
Private virtual switch
Management
Broadcom NetXtreme Gigabit Ether...
External LAN
Intel(R) Ethernet 10G 2P X540-t A...
Test
Internal only
Global Network Settings
MAC Address Range
00-15-5D-78-AF-00 to 00-15-5D-7...
Create virtual switch

What type of virtual switch do you want to create?

External
Internal
Private

Creates a virtual switch that binds to the physical network adapter so that virtual machines can access a physical network.

Choose the option to create an *Internal* connection, then click the *Create Virtual Switch* button.


Virtual Switch Manager for ZEUS
Virtual Switches
New virtual network switch
WAN
Intel(R) Ethernet 10G 2P X540-t A...
LAN
Private virtual switch
Management
Broadcom NetXtreme Gigabit Ether...
External LAN
Intel(R) Ethernet 10G 2P X540-t A...
Attach To Host
Internal only
Global Network Settings
MAC Address Range
00-15-5D-78-AF-00 to 00-15-5D-7...
Virtual Switch Properties
Remove
OK
Cancel
Apply

Name: Attach To Host

Notes:

Connection type

What do you want to connect this virtual switch to?

○ External network:

Broadcom NetXtreme Gigabit Ethernet

☑ Allow management operating system to share this network adapter

□ Enable single-root I/O virtualization (SR-IOV)

● Internal network

○ Private network

VLAN ID

□ Enable virtual LAN identification for management operating system

The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

2

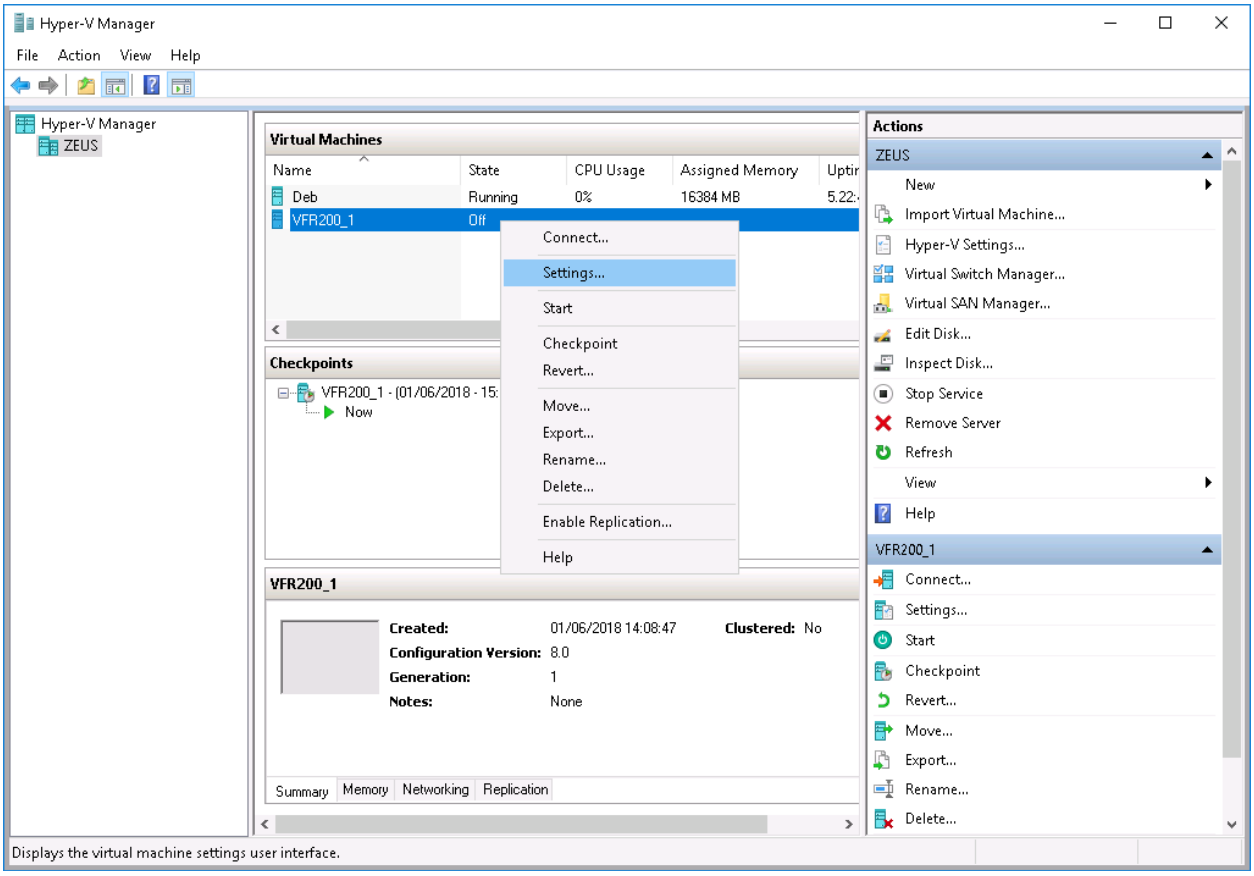
SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.

In the new properties section select a name for the network connection.

Click on *Apply*, then *OK* at the bottom of the *Properties* page.

The next stage is to close the *Virtual Switch Manager* and bring up the *Settings* page for the PORTrockIT.

Note: The PORTrockIT needs to be powered off to add or remove network connections.



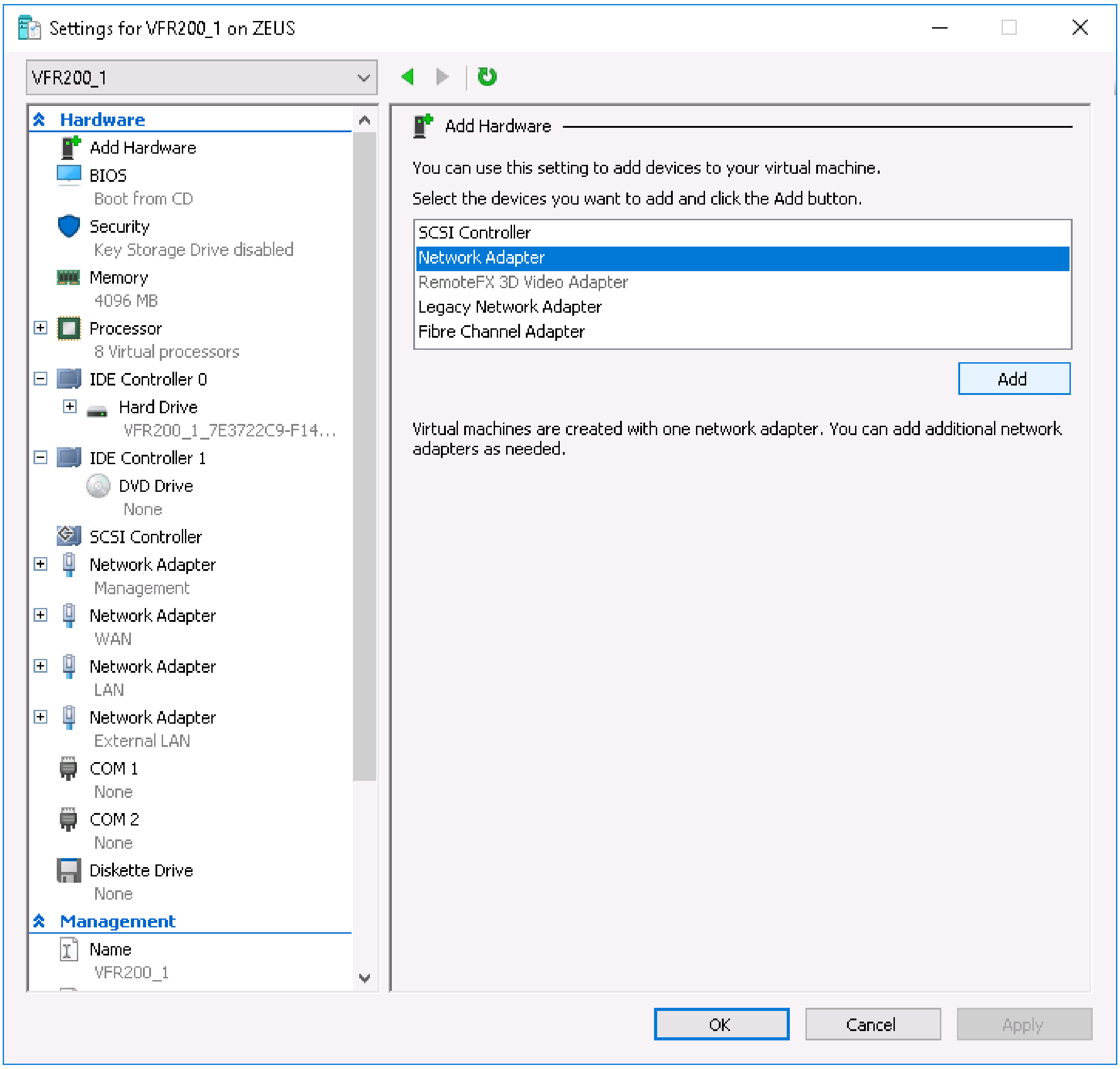
Name	State	CPU Usage	Assigned Memory	Uptir
Deb	Running	0%	16384 MB	5.22:
VFR200_1	Off			

VFR200_1

Created: 01/06/2018 14:08:47 **Clustered:** No
Configuration Version: 8.0
Generation: 1
Notes: None

Displays the virtual machine settings user interface.

In the *Hardware* column on the left of the new window, select *Add Hardware* at the top, then select the *Network Adapter* and click on *Add*.



Settings for VFR200_1 on ZEUS

VFR200_1

Hardware

- Add Hardware
- BIOS
  Boot from CD
- Security
  Key Storage Drive disabled
- Memory
  4096 MB
- Processor
  8 Virtual processors
- IDE Controller 0
  - Hard Drive
    VFR200_1_7E3722C9-F14...
- IDE Controller 1
  - DVD Drive
    None
- SCSI Controller
- Network Adapter
  Management
- Network Adapter
  WAN
- Network Adapter
  LAN
- Network Adapter
  External LAN
- COM 1
  None
- COM 2
  None
- Diskette Drive
  None

Management

- Name
  VFR200_1

Add Hardware

You can use this setting to add devices to your virtual machine.

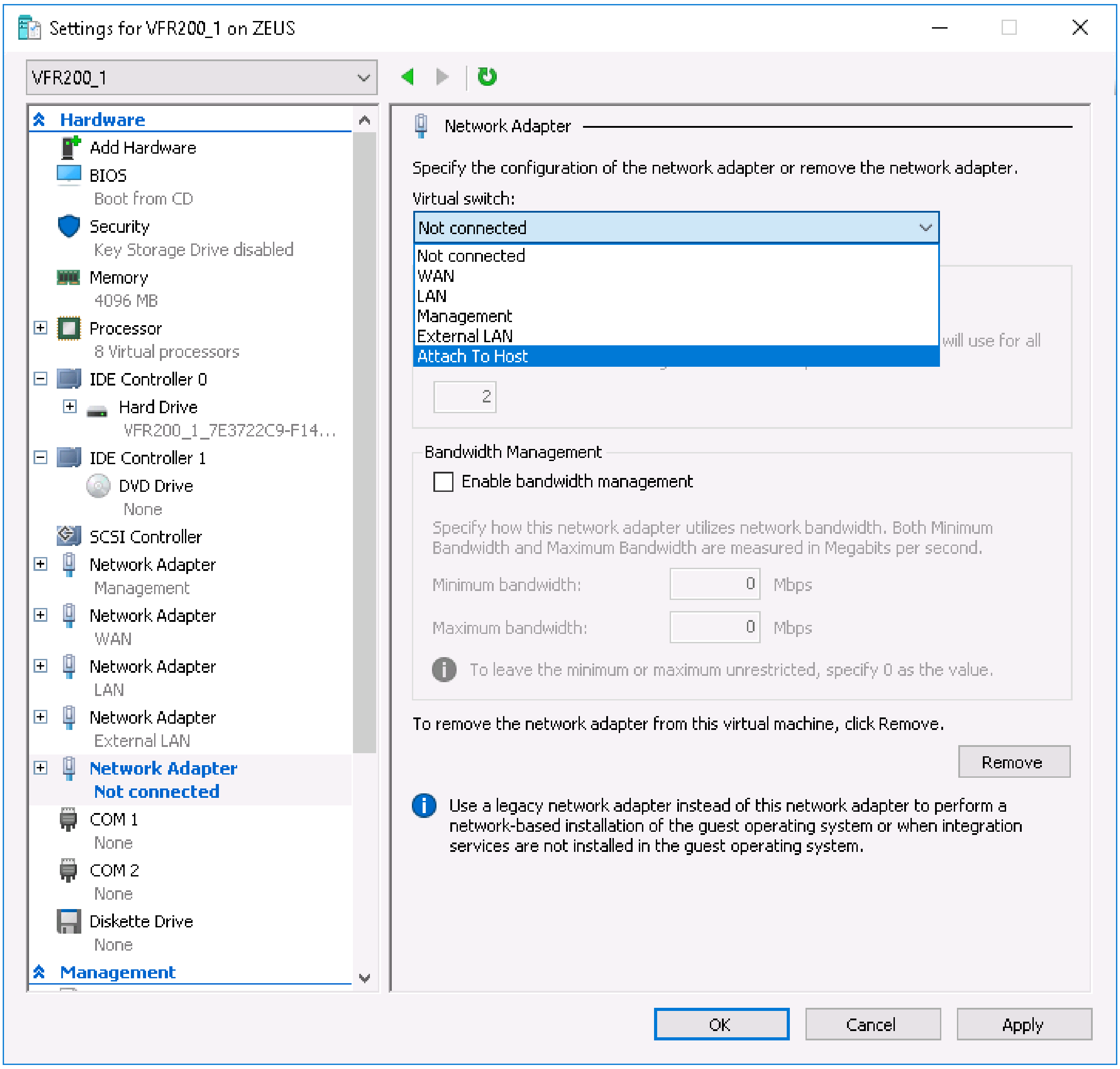
Select the devices you want to add and click the Add button.

- SCSI Controller
- Network Adapter
- RemoteFX 3D Video Adapter
- Legacy Network Adapter
- Fibre Channel Adapter

Add

Virtual machines are created with one network adapter. You can add additional network adapters as needed.

At this point an empty Virtual Switch is displayed. Choose the newly created internal switch from the dropdown menu.



Settings for VFR200_1 on ZEUS

VFR200_1

Hardware

- Add Hardware
- BIOS
  - Boot from CD
- Security
  - Key Storage Drive disabled
- Memory
  - 4096 MB
- Processor
  - 8 Virtual processors
- IDE Controller 0
  - Hard Drive
    - VFR200_1_7E3722C9-F14...
- IDE Controller 1
  - DVD Drive
    - None
- SCSI Controller
- Network Adapter
  - Management
- Network Adapter
  - WAN
- Network Adapter
  - LAN
- Network Adapter
  - External LAN
- **Network Adapter**
  - **Not connected**
- COM 1
  - None
- COM 2
  - None
- Diskette Drive
  - None

Management

Network Adapter

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch:

Not connected

- Not connected
- WAN
- LAN
- Management
- External LAN
- Attach To Host

will use for all

2

Bandwidth Management

□ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth:	0	Mbps
Maximum bandwidth:	0	Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

To remove the network adapter from this virtual machine, click Remove.

Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

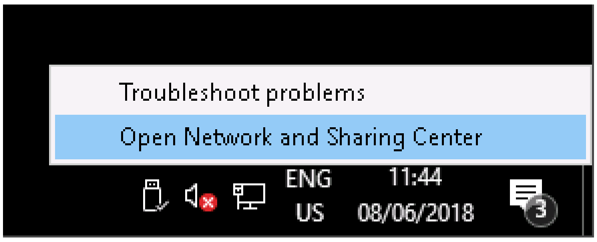
Click *Apply* and then *OK*.

The connection between the Host and PORTrockIT is now available.

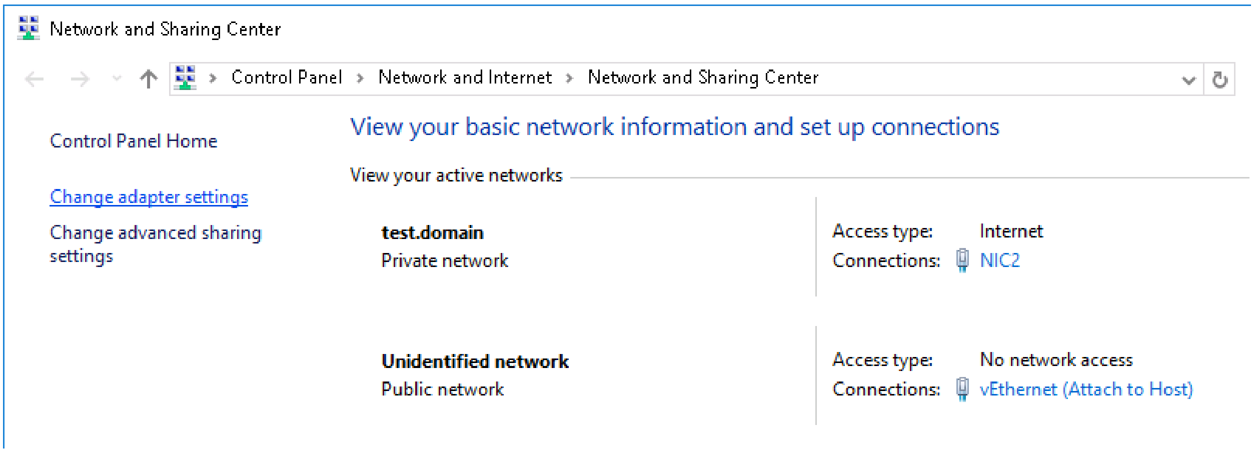
At this stage the PORTrockIT needs to be started and the new port will need a static IP added.

The host will also need a static IP to establish the connection. Bring up the *Network Settings* in the Host and open the settings for the new vEthernet that has been setup. The new Virtual Switch will have same name found in the *Virtual Switch Manager* in the *Hyper-V Manager*.

To access the *Network Settings*, right click on the network icon at the bottom right of the screen and select *Open Network and Sharing Center*.



Then in the new window select *Change adapter settings* in the column on the left.


Network and Sharing Center

Control Panel › Network and Internet › Network and Sharing Center

Control Panel Home

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connections

View your active networks

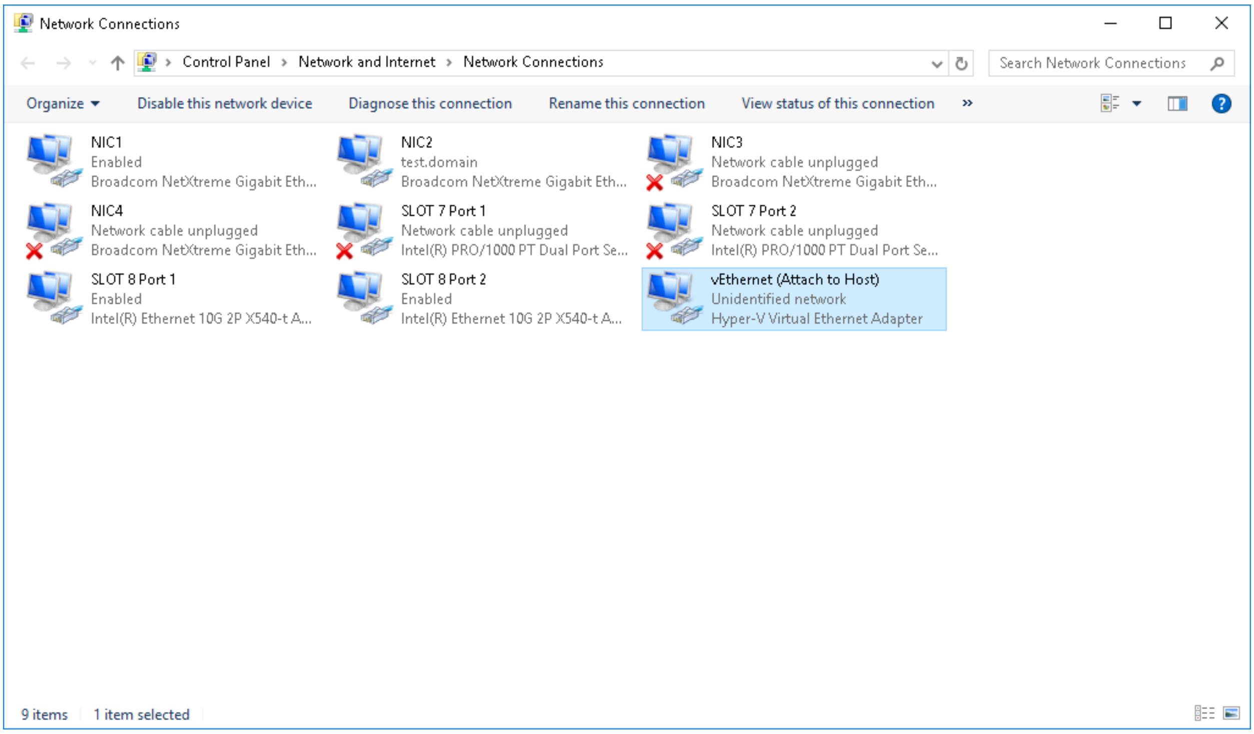
test.domain
Private network

Access type: Internet
Connections: NIC2

Unidentified network
Public network

Access type: No network access
Connections: vEthernet (Attach to Host)

In the *Network Connections* window right click on the internal vEthernet, then click on *properties* from the context menu.


Network Connections

Control Panel › Network and Internet › Network Connections

Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
»

NIC1
Enabled
Broadcom NetXtreme Gigabit Eth...

NIC2
test.domain
Broadcom NetXtreme Gigabit Eth...

NIC3
Network cable unplugged
Broadcom NetXtreme Gigabit Eth...

NIC4
Network cable unplugged
Broadcom NetXtreme Gigabit Eth...

SLOT 7 Port 1
Network cable unplugged
Intel(R) PRO/1000 PT Dual Port Se...

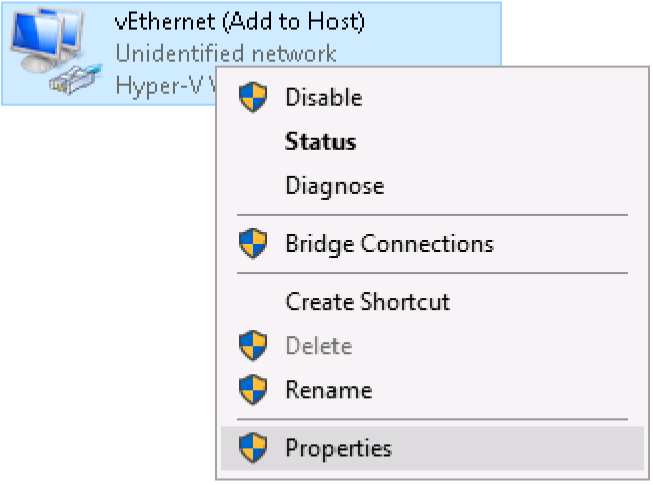
SLOT 7 Port 2
Network cable unplugged
Intel(R) PRO/1000 PT Dual Port Se...

SLOT 8 Port 1
Enabled
Intel(R) Ethernet 10G 2P X540-t A...

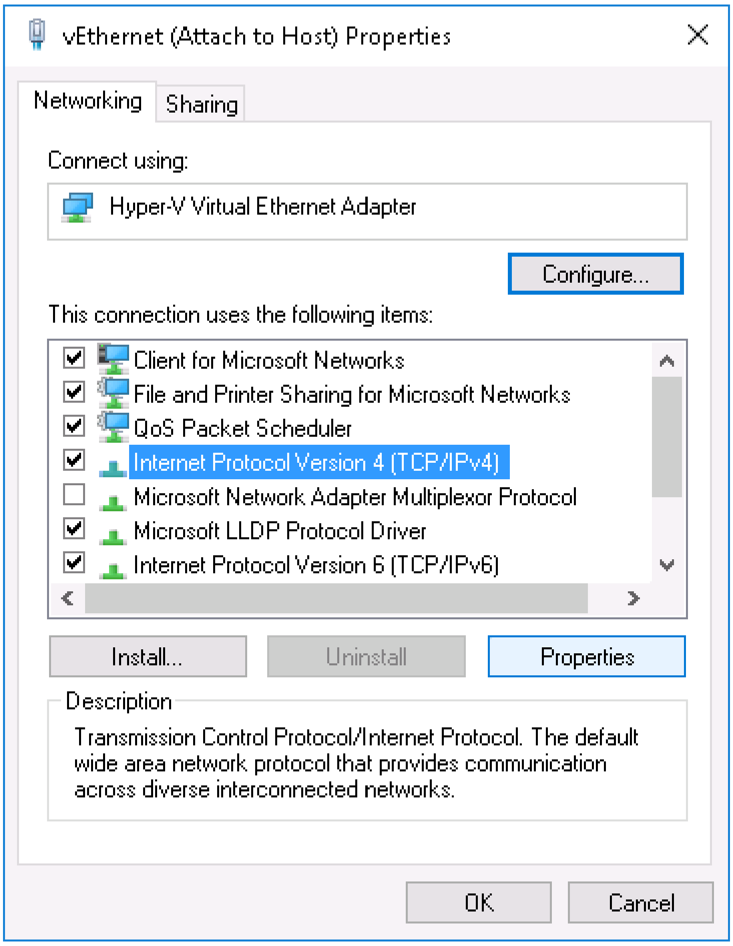
SLOT 8 Port 2
Enabled
Intel(R) Ethernet 10G 2P X540-t A...

vEthernet (Attach to Host)
Unidentified network
Hyper-V Virtual Ethernet Adapter

9 items 1 item selected



In the properties window, left click on *Internet Protocol Version 4 (TCP/IPv4)* and then left click on the *Properties* button.


vEthernet (Attach to Host) Properties

Networking | Sharing

Connect using:

Hyper-V Virtual Ethernet Adapter

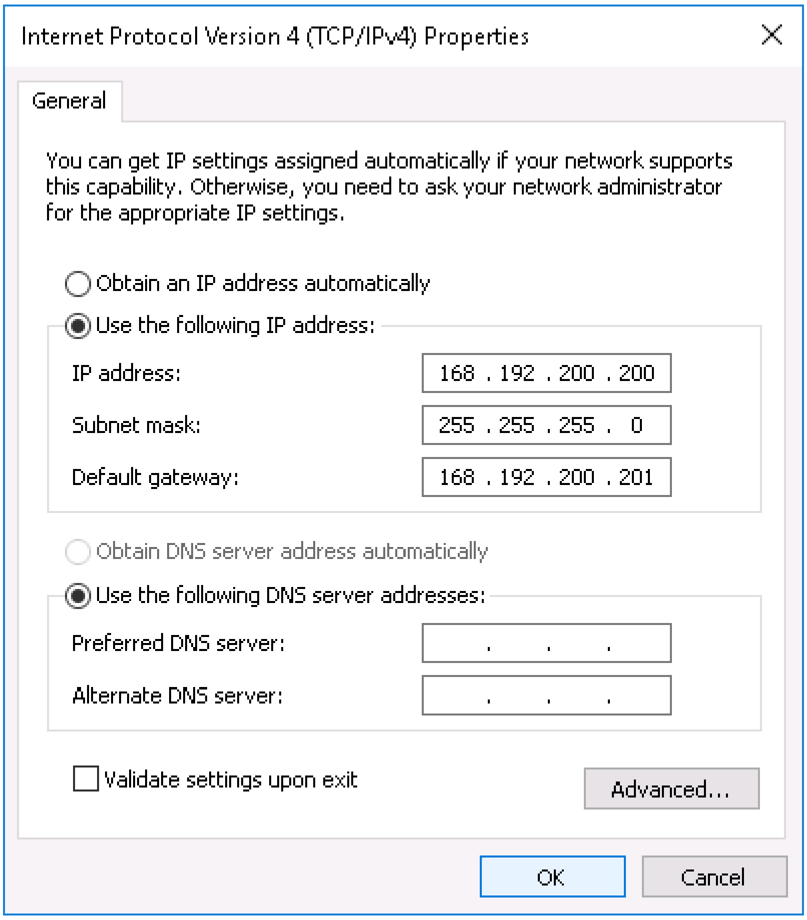
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

In the new properties window change the radio option to *Use the following IP address*.



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:	168 . 192 . 200 . 200
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	168 . 192 . 200 . 201

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

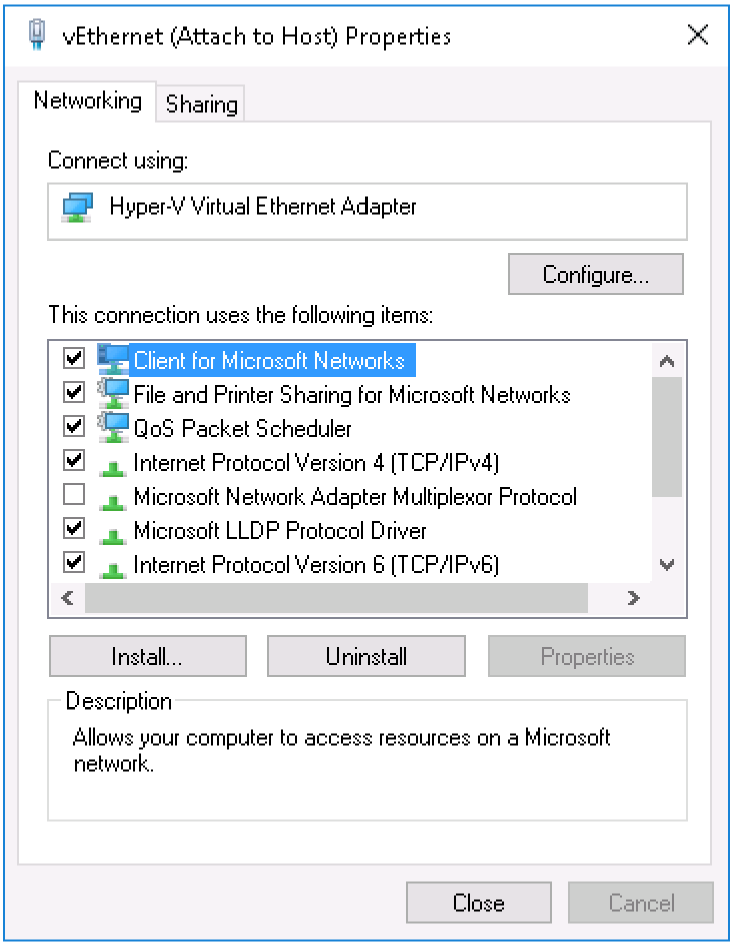
Preferred DNS server:	. . .
Alternate DNS server:	. . .

□ Validate settings upon exit

Enter the IP address and subnet mask to allow it to communicate with the settings that are used for the same Virtual Switch on the PORTrockIT.

The *Default Gateway* should be set to use the IP of the PORTrockIT.

Click *OK* to close this window, then click *close* in the remaining *Properties* window.



Connect using:

Hyper-V Virtual Ethernet Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Allows your computer to access resources on a Microsoft network.

At this stage the host should now have access to communicate with the PORTrockIT.

Note: New port mappings and/or relationships on the PORTrockIT web interface may need to be setup if a new virtual connection was created to connect the host. See Section 7.5: Routing for Relationships.

9 Useful Links

The following section contains links to other guides and FAQs. Support is available through our website: `https://support.4bridgeworks.com/`

The following resources are available online:

- User Manuals
- Installation Guides
- General FAQ
- AWS FAQ

If your question is not answered in our documentation, please submit a ticket through our website.