

PORTrockIT Out-of-Path Setup Guide Eli-v5.03.148

Bridgeworks

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

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

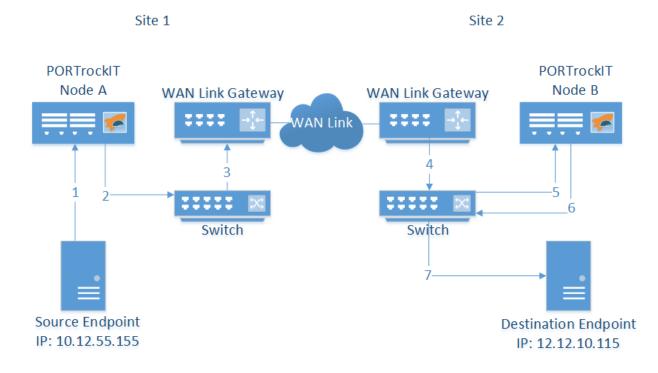
1	Intro	oduction	1	
2	Gett	ting Started	4	
	2.1	Prerequisites	4	
3	Gui	de Layout	6	
4	Initia	al Setup of your Bridgeworks Node	7	
	4.1	Finding Management IP addresses	7	
	4.2	First Time Login	8	
	4.3	Logging into the Node	9	
	4.4	Network Connections (9	
		4.4.1 Setting the Hostname/Node Name	10	
		4.4.2 Changing IP Addresses	11	
	4.5	Licence Keys	12	
		4.5.1 Uploading a Licence Key	12	
	4.6	Port Mappings (📴)	14	
		4.6.1 Overview	14	
		4.6.2 Setting Port Mappings	14	
5	Con	figuring IPsec	17	
	5.1	Introduction	17	
	5.2	Important Notes	17	
	5.3 Enabling IPsec			
	5.4	Copying the Pre-Shared Key to other Bridgeworks Nodes	19	
6	Esta	ablishing a Link Between Nodes	21	
	6.1	Introduction	21	
	6.2	Firewall	21	

	6.3	Topology 1: Connecting Bridgeworks Nodes which have Public IP addresses \ldots	21		
	6.4	Topology 2: Connecting Bridgeworks Nodes joined via an external VPN \ldots	22		
	6.5	Topology 3: Connecting Bridgeworks Nodes Using 2 Site NAT	23		
	6.6	Topology 4: Connecting to a Bridgeworks Node with a NAT on one site	24		
	6.7	Access Control	25		
	6.8	Node Management	27		
7	Con	figuring PORTrockIT Acceleration	30		
	7.1	Introduction	30		
	7.2	Prerequisites	30		
	7.3	3 Adding Services			
	7.4	Establishing Relationships			
	7.5	Routing for Relationships	33		
		7.5.1 Example 1 - WAN and LAN on the same subnet	34		
		7.5.2 Example 2 - Endpoint on different subnet to LAN interface	37		
8	Acc	elerating a Windows Hosts traffic with a guest Hyper-V PORTrockIT	40		
	8.1	Introduction	40		
	8.2	Connecting host to existing VNet	40		
	8.3	Adding a dedicated connection	43		
9	Use	ful Links	52		

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 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.

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.

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

Initial Setup of your Bridgeworks Node

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/

If DHCP fails, then the fallback IP addresses are:

Management A/Port 1 10.10.10.10

Management B 10.10.10.12

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

	BRIDGEWORKS Press Alt-F2 to login
Management A Management B Port 1A Port 1B Port 2A Port 2B	System IP addresses: 10.10.120.57/16 (MAC 08:00:27:50:4f:1f) UP Management enabled on this port 10.10.120.58/16 (MAC 08:00:27:a9:7c:5c) UP Management enabled on this port No IP address set (MAC 08:00:27:d8:3d:32) DOUN No IP address set (MAC 08:00:27:c5:18:9d) DOUN No IP address set (MAC 08:00:27:01:26:7f) DOUN No IP address set (MAC 08:00:27:35:88:03) DOUN
Uptime	: 00 : 00 : 47

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 password for you	
Enter Password: Confirm Password:	
	Save



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

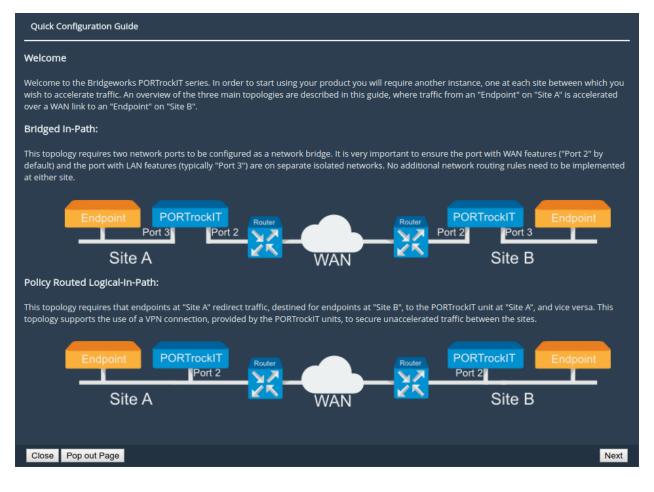
characters and a maximum of 64 characters in length.

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:	••••••
	Login

When you have logged in, the *Quick Configuration Guide* is presented. This gives an overview of a typical setup, as well as key areas that will need to be configured.



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

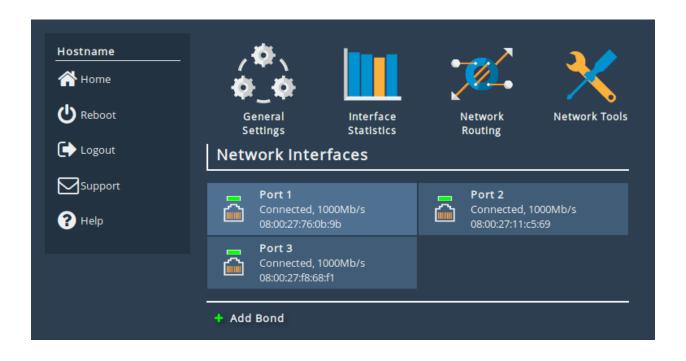
below.



Setting the Hostname/Node Name

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.



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.

Hostname	Link Statu	S				
A Home	Link State:	Up		Link Speed:	1000Mb/s	
••	RX Bytes:	3253477		TX Bytes:	2392844	
1 Connections	RX Errors:	0		TX Errors:	0	
U Reboot	Settings					
U Kebool	IPv4 Address:			10.10.10.158		
🕞 Logout	MTU:			1500		
	Mapped Pr	otocols				
Support	Managemen	t				
? Help				_	_	_
	Port Settin	igs				
	Enable Port:		v			
	MTU Size:		1500			
						_
	Use DHCI			dress autom	atically	
	IP Address:	Showing	10.10.10.158			
	Netmask:		255.255.0.0			
	Gateway:		10.10.10.1			
					Cancel	Save
					Januer	Cave

The port settings page allows the IP address of a port to be manually assigned. To do so, 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.

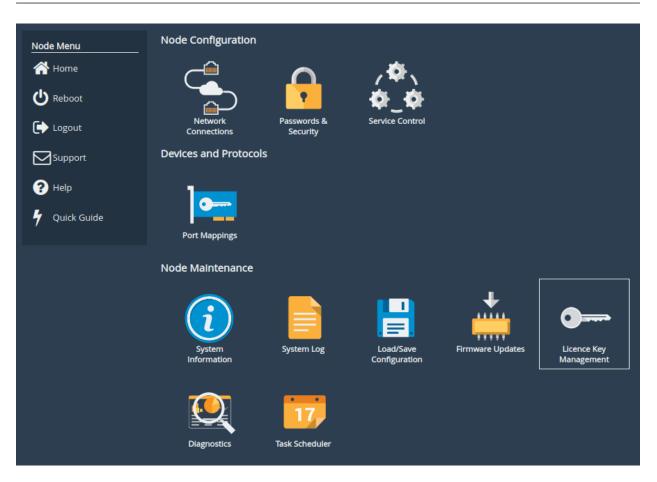
Licence Keys

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.

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.

Licen	ice Keys
Node Menu	Installed Licence Keys
Home	No valid licence keys installed.
🕑 Reboot	Licence Key File: Choose file No file chosen
Support	Upload
? Help	

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

Licence Keys				
Node Menu	Installed Lice	ence Keys		
🕂 Home	ID	Feature Type	Limit	Expires
C Reboot	409348685	WAN	1	1 Days
🕞 Logout			Remove	Download
Support	Licence Key	Upload		
? Help	Licence Key File: Choose file No	o file chosen		
Events	Upload			
27 Sep 09:43 Reboot required				

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



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.

Virtual instances can have mappings applied to any number of ports, however the number of unique protocols that can be applied is dependent the on the product range.

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.

Node Menu	Instructions
삼 Home	Select which protocols should be active on each network interface. After saving changes, reboot the product for the new configuration to take effect.
U Reboot	
Ŭ	Protocols for Port 1:
Logout	Management
	Management
	Add a protocol
? Help	Protocols for Port 2:
Licensed To	
	WAN X
	Add a protocol
	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.

_	
Node Menu	Instructions
삼 Home	Select which protocols should be active on each network interface. After saving changes, reboot the product for the new configuration to take effect.
U Reboot	
C	Protocols for Port 1:
🕞 Logout	Management
Support	Add a protocol 🗘
? Help	Protocols for Port 2:
	WAN 🗙
	Add a protocol 🗘
	Protocols for Port 3:
	NetApp Stream Acceleration 🗶
	Add a protocol 🗘
	Cancel
	WAN X

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.

Configuring IPsec

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.

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.

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.

Node Menu	PORTrockIT IPsec	Configuration
🕋 Home	Enable IPsec:	
1 Nodes	Encrypt Accelerated Traffic:	
U Reboot	IPsec Pre-Shared Key:	Generate Key Show Key Delete Key
🕞 Logout		Save
Support		
? Help		
Licensed To		
Bridgeworks Ltd		

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

Node Menu	PORTrockIT IPsec 0	PORTrockIT IPsec Configuration		
谷 Home	Enable IPsec:			
← Nodes	Encrypt Accelerated Traffic:			
U Reboot	IPsec Pre-Shared Key:	Generate Key Show Key Delete Key		
🕞 Logout		Save		
Support				
? Help				
Licensed To	-			
Bridgeworks Ltd				

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:

Node Menu	PORTrockIT IPsec	Configuration
A Home	Enable IPsec:	
▲ Nodes	Encrypt Accelerated Traffic:	
C Reboot	IPsec Pre-Shared Key:	VHFldWTfkQU_ZIzDTIG4F5xtDhX8
C Reboot		Generate Key Show Key Delete Key
🕞 Logout		Save
Support		
? Help		
Licensed To		
Bridgeworks Ltd		

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.

Copying the Pre-Shared Key to other Bridgeworks Nodes

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

Node Menu	PORTrockIT IPsec (Configuration
삼 Home	Enable IPsec:	
1 Nodes	Encrypt Accelerated Traffic:	
U Reboot	IPsec Pre-Shared Key:	Generate Key Show Key Delete Key
Logout		Save
Support		
? Help		
Licensed To		
Bridgeworks Ltd		

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.

Establishing a Link Between Nodes

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.

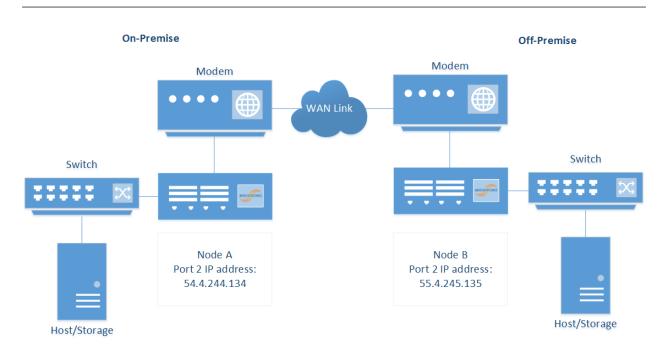
Firewall

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

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.

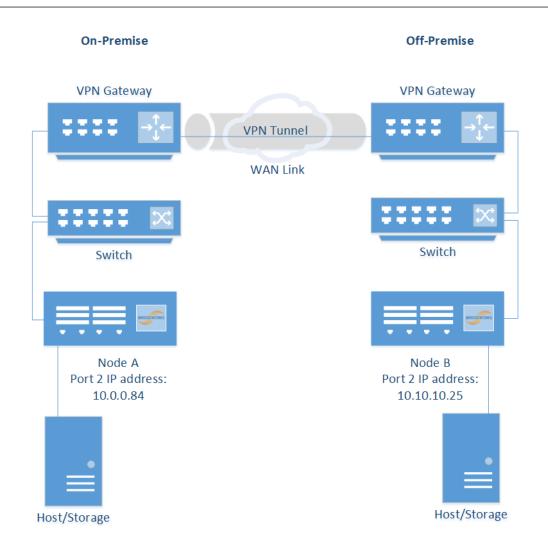


In this example the IP addresses for establishing a Nodal link are the public IP addresses assigned to *Port 2* on the Bridgeworks Nodes:

- Node A: 54.4.244.134
- Node B: 55.4.245.135

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

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:

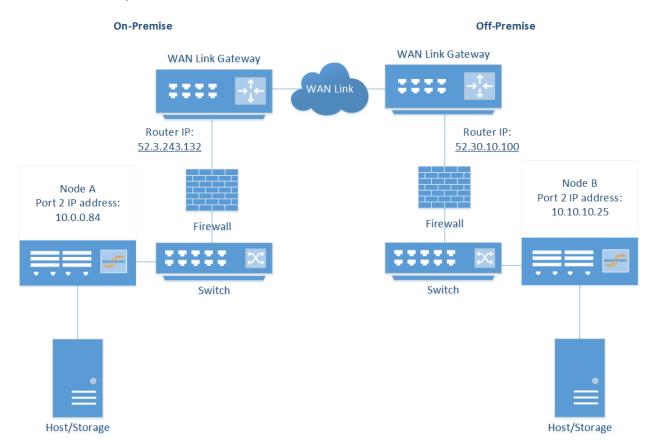
Protocol: TCP Destination Port Range: 16665 Redirect Target IP: <IP addresses of WAN port of the Bridgeworks Node> Redirect Target Port: 16665

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.

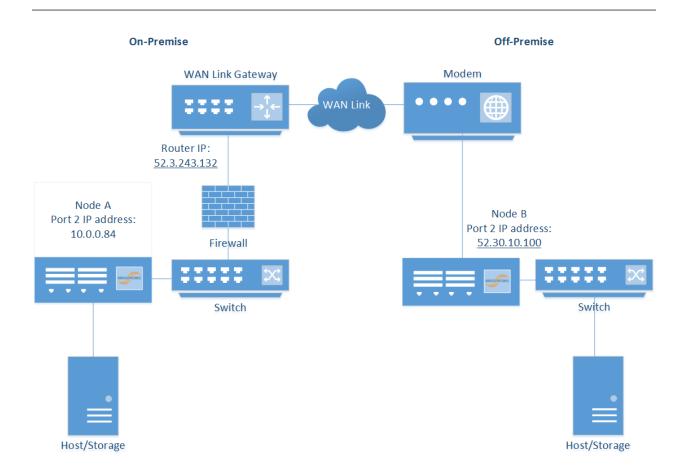


In this example the IP addresses for establishing a Nodal link are the IP addresses of the router, in this case:

- Node A: 52.3.243.132
- Node B: 52.30.10.100

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.

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.

Node Menu	Remote Administration
♠ Nodes ♦ Reboot	Whitelist
➡ Logout	Whitelisted IP Addresses IP address Use the form below to add an IP to the whitelist
Help	New IP: Add Remove
Bridgeworks Ltd	Cancel Save

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

Node Menu	Remote Administration
♠ Nodes ♣ Reboot	Whitelist
C→ Logout	Whitelisted IP Addresses
Support	Use the form below to add an IP to the whitelist
? Help	New IP: 10.0.0.84 Add Remove
Licensed To Bridgeworks Ltd	Cancel Save

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

Node Menu	Remote Administration
♠ Nodes ● Reboot	Whitelist
➡ Logout	Whitelisted IP Addresses
PHelp	10.0.0.84 New IP: Add
Bridgeworks Ltd	Cancel Save

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 Node* icon to navigate to the *Add 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.

Node Menu	New Remote Nod	e Details	
🕋 Home	IP Address	10.10.10.25	
♠ Nodes	Network Interface	Port 2 (10.0.0.84)	∼ Cancel Add
U Reboot			
🕞 Logout			
Support			
? Help			
Licensed To	_		

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

Hostname	New Remote Node Details	
🖀 Home	Connected to Node	~
▲ Nodes ④ Reboot	Hostname Node_B Cancel	Add
🔶 Logout	Connected to Node	
Support	ОК	

The IP address of Node B is automatically added to the *Access Control* list of Node A when a discovery is initiated. This allows a reverse WAN connection to be made - from *Node B* to *Node A* - if your topology requires it.

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.

Node Menu	New Remote Nod	e Detalls	
삼 Home	IP Address	10.0.0.84	
♠ Nodes	Network Interface	Port 2 (10.10.10.25)	Cancel Add
U Reboot			Cancer
🕞 Logout			
Support			
? Help			
Licensed To	_		
Bridgeworks Ltd			

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

lostname	New Remote Node Details	
😭 Home	Connected to Node	
♠ Nodes		-
U Reboot	Hostname Node_A	Cancel Add
🗭 Logout	Connected to Node	
Support	ок	
? Help		
_	ОК	

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

Configuring PORTrockIT Acceleration

Introduction

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

Prerequisites

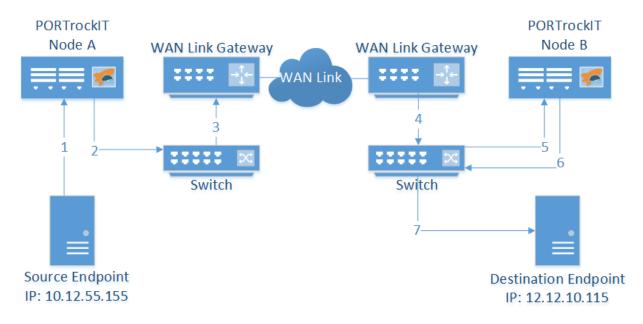
In order to configure PORTrockIT acceleration you must have the following:

- 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.

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 *PORTrockIT 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 *Out-of-Path* from the *Topology* dropdown.

Configuration for Node B

Add New Service	
Name	Destination Endpoint
Address	12.12.10.115
Protocol	Caringo Swarm Object Storage
Outgoing Interface	Port 3
Topology	Out-of-Path 🔻
	Cancel Add Service

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.

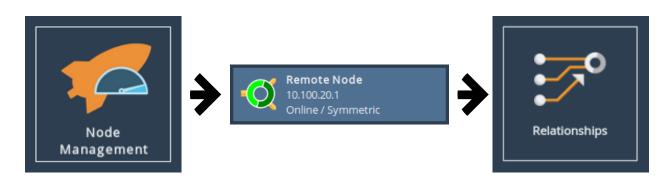
Clicking on the *Add Service* button finishes the creation of the service. The service will now be available to remote Nodes for creating a relationship.

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.

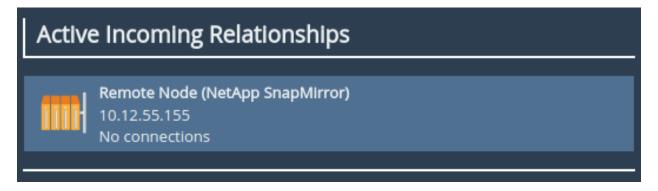
Active	Services	
• Turnin	g off a service doesn't stop existing connections	~
	Destination Endpoint (Caringo Swarm) 12.12.10.115 Port 3	ON•
← Configure Services		Cancel Save

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:

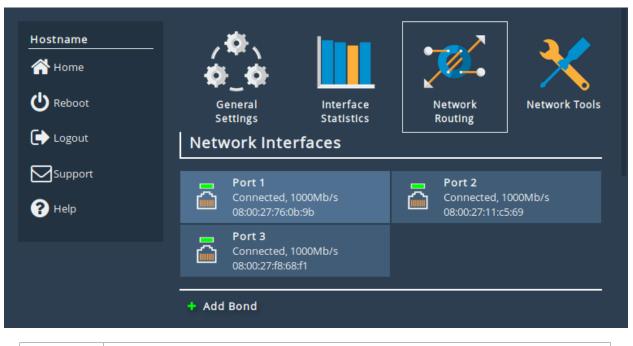


If the relationship is displayed in the *Active Incoming Relationships* list then the relationship was successfully created. After this, the software configuration required for accelerating traffic between PORTrockITs is complete.

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.



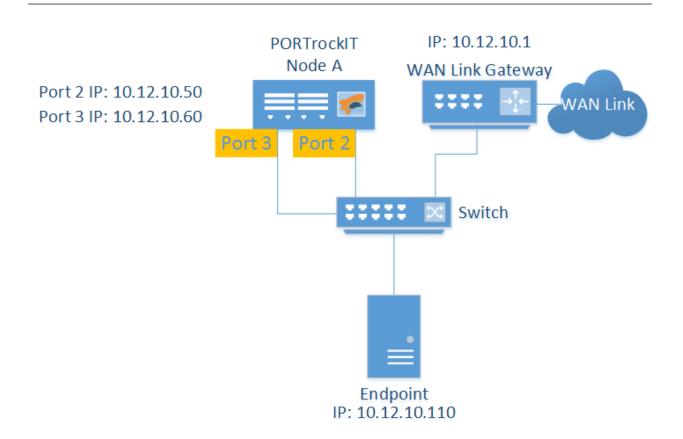


Important: Routes created automatically by the system are added with a metric of 1, allowing you to override defaults by using a metric of 0.

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.

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	10.10.10.1	Port 1	1	Delete		
10.10.0.0/16		Port 1	1	Delete		
10.12.10.0/2 4		Port 2	1	Delete		

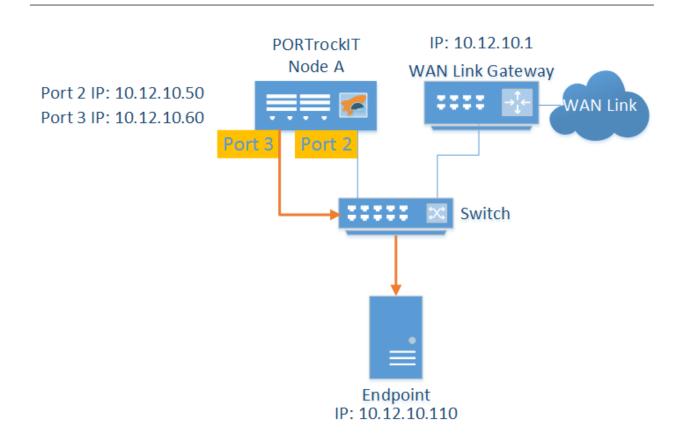
Currently *Node A* will be sending traffic destined for the *Endpoint* from *Port 2* instead of *Port 3*. To resolve this, a static route needs to be added.

Add Static Rou	ite	
Interface:	Port 3 🔻	
Destination:	10.12.10.110	
Prefix:	/32	
Gateway:		
Metric:		
		Add rou

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

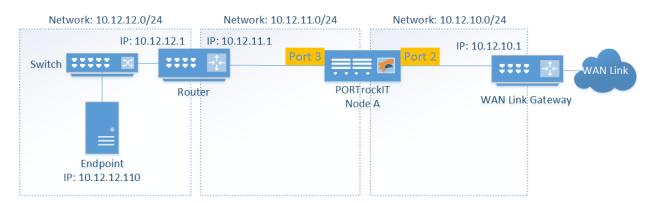
Global Rou	ting Table			
Destination	Gateway	Interface	Metric	
0.0.0/0	10.10.10.1	Port 1	1	Delete
10.10.0.0/16		Port 1	1	Delete
10.12.10.0/2 4		Port 2	1	Delete
10.12.10.11 0/32		Port 3	1	Delete

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



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 Rou	ting Table			
Destination	Gateway	Interface	Metric	
0.0.0/0	10.10.10.1	Port 1	1	Delete
10.10.0.0/16		Port 1	1	Delete
10.12.10.0/2 4		Port 2	1	Delete
10.12.11.0/2 4		Port 3	1	Delete

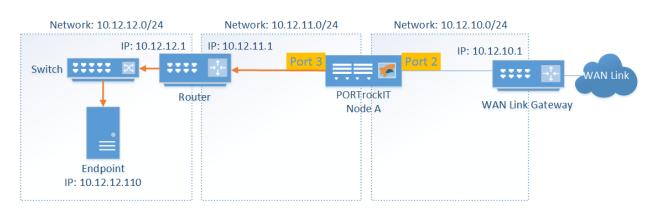
Currently *Node A* doesn't know how to reach the 10.12.12.0/24 network so traffic for the *Endpoint* will be lost. To resolve this, a static route needs to be added.

Add Static Route		
Interface:	Port 3 T	
Destination:	10.12.12.0	
Prefix:	/24	
Gateway:	10.12.11.1	
Metric:		
		Add route

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

Global Rou	ting Table			
Destination	Gateway	Interface	Metric	
0.0.0/0	10.10.10.1	Port 1	1	Delete
10.10.0.0/16		Port 1	1	Delete
10.12.10.0/2 4		Port 2	1	Delete
10.12.11.0/2 4		Port 3	1	Delete
10.12.12.0/2 4	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.

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

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.

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.

📲 Hyper-V Manager) X
File Action View Help							
🗢 🔿 🙍 🖬 🚺 🖬	In View Help Internet						
📰 Hyper-V Manager					_	Actions	
TEUS						ZEUS	<u>^</u>
			-			New	•
			0%	16384 MB	5.22:	🛝 Import Virtual Machine	
	VIII200_1	01					
	 ✓ ✓						
	Checkpoints						
	-	6/2018 - 15:10:50)					
		, , , , , , , , , , , , , , , , , , ,					
						1	
						-	
						👔 Help	
						VFR200_1	-
	VFR200_1					📲 Connect	
						📷 Settings	
				7 Clustered: N	0	🙂 Start	
						🔂 Checkpoint	
						5 Revert	
						➡ Move	
						Export	
	Summaru Memory Net	working Replication					
		2				-	
					>		~

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.

 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 Notes: External LAN Notes: Connection type What do you want to connect this virtual switch to? External network: Intel(R) Ethernet 10G 2P X540-t A External only Global Network Settings MAC Address Range 00-15-5D-78-AF-00 to 00-15-5D-7 Allow management operating system to share this network adapted 	~ ~
 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 Management operating system to share this network adapted 	~ ~
Intel(R) Ethernet 10G 2P X540-t A	
 Private virtual switch Management Broadcom NetXtreme Gigabit Ether External LAN Intel(R) Ethernet 10G 2P X540-t A Connection type Global Network Settings MAC Address Range 00-15-SD-78-AF-00 to 00-15-SD-7 Mac Address Range On 15-SD-78-AF-00 to 00-15-SD-7 Allow management operating system to share this network adapted 	~
	~
Broadcom NetXtreme Gigabit Ether External LAN Intel(R) Ethernet 10G 2P X540-t A E Test Internal only Connection type What do you want to connect this virtual switch to? MAC Address Range 00-15-5D-78-AF-00 to 00-15-5D-7 Intel(R) Ethernet 10G 2P X540-t Adapter #2 Allow management operating system to share this network adapted	~
Intel(R) Ethernet 10G 2P X540-t A Connection type Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What do you want to connect this virtual switch to? Connection type What	~
Internal only Connection type Global Network Settings What do you want to connect this virtual switch to? MAC Address Range External network: Intel(R) Ethernet 10G 2P X540-t Adapter #2 Allow management operating system to share this network adapted	
Internal only What do you want to connect this virtual switch to? Image: Global Network Settings Image: Global Network Settings Image: MAC Address Range Image: Global Network Settings Image: Optimized Settings Image: Global Network Settings <tr< td=""><td></td></tr<>	
Global Network Settings MAC Address Range 00-15-5D-78-AF-00 to 00-15-5D-7 Allow management operating system to share this network adapted	
MAC Address Range 00-15-5D-78-AF-00 to 00-15-5D-7 MAC Address Range Intel(R) Ethernet 10G 2P X540-t Adapter #2 Allow management operating system to share this network adapted	
Allow management operating system to share this network adapter	
	~
	r
Enable single-root I/O virtualization (SR-IOV)	
O Internal network	
O Private network	
VLAN ID	
Enable virtual LAN identification for management operating system	
The VLAN identifier specifies the virtual LAN that the management operatin system will use for all network communications through this network adapt setting does not affect virtual machine networking,	
SR-IOV can only be configured when the virtual switch is created. An exvirtual switch with SR-IOV enabled cannot be converted to an internal o 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	\sim
Allow management operating system to share this network adapter	
Enable single-root I/O virtualization (SR-IOV)	
O Internal network	
O Private network	

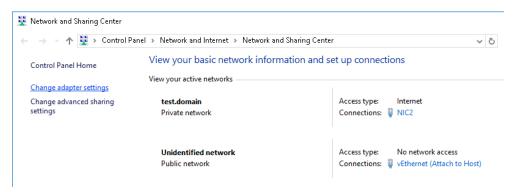
Click Apply and then OK.

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.



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.

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.

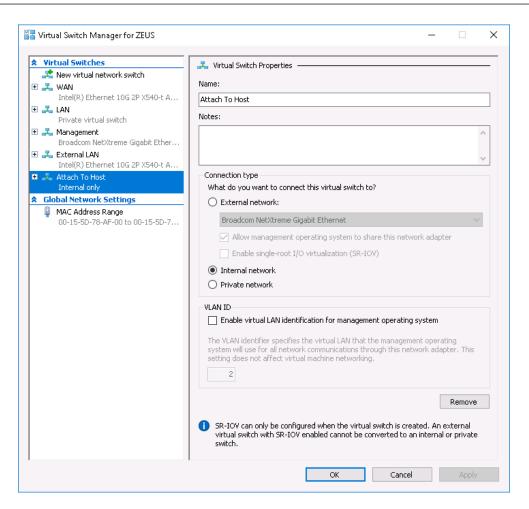
In the Hyper-V manager open the *Virtual Switch Manager*, located in the *Actions* column on the right.

📳 Hyper-V Manager						- 0	\times
File Action View Help							
		Actions					
ZEUS		-				ZEUS	^
			-			New	•
			U%	16384 MB	5.22:	强 Import Virtual Machine	
		0.1				Hyper-V Settings	
	<						
	Checkpoints					-	
	-	/06/2018 - 15:10:50)					
						- · ·	
						-	<u> </u>
							•
							-
	VFR200_1					-	
	Gree	ated	01/06/2018 14:09:4	7 Clustered: N		Settings	
				clustered. N	°	🕲 Start	
	Ger	neration:	1			🔂 Checkpoint	
	Not	es:	None			5 Revert	
						Move	
						Export	
	Summary Memory N	etworking Replication	1			=] Rename	
						E. Delete	

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

Virtual Switches	Create virtual switch
🥕 New virtual network switch	
E 🛃 WAN	What type of virtual switch do you want to create?
Intel(R) Ethernet 10G 2P X540-t A	External Internal
E 🛃 LAN Private virtual switch	Private
🗄 🚑 Management	
Broadcom NetXtreme Gigabit Ether	
External LAN Intel(R) Ethernet 10G 2P X540-t A	Create Virtual Switch
Intel(K) Ethemet 10G 2P X540-t A	
Internal only	Creates a virtual switch that binds to the physical network adapter so that virtual
Global Network Settings	machines can access a physical network.
	OK Cancel Apply

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



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.

Hyper-V Manager						- 1	⊐ ×
File Action View Help							
🗢 🏟 🙇 🖬 📓 🖬							
📰 Hyper-V Manager					_	Actions	
E ZEUS			001111		11.12	ZEUS	<u>^</u> ^
			-		1.1	New	•
	VFR200_1	Off	0%	10304 MB	5.22.	🚯 Import Virtual Machine	
			Connect			Hyper-V Settings	
			Settings		Actions ZEUS New B 5222. Hyper-V Settings Virtual SAN Manager Virtual SAN Manager Virtual SAN Manager City Virtual SAN Manager Virtual SAN Manage		
			Start			🔬 Virtual SAN Manager	
	<		Checknoint			🚄 Edit Disk	
	Checkpoints		Revert			🔄 Inspect Disk	
		- (01/06/2018 - 15:	Move			 Stop Service 	
	- Now					🗙 Remove Server	
			Rename			🖏 Refresh	
			Delete			View	•
	View Help Start Start View View Service Move Esport Esport Inspect Disk Pholo View Uital Manager View Help View Uital Manager View Help Start View Uital Manager Start Delete Esport Esport Start View Uital Manager Start View Uital Manager Start Created: 01/05/2018 14:08:47 Clustered: No Start						
						VFR200_1	•
	VER200_1		neip			- Connect	
	111200_1					Settings	
				7 Clustered: 1	٩o		
		-				🔂 Checkpoint	
						➡ Move	
	Summary Memory	Networking Replicatio	on				
	<				>	Delete	~
Displays the virtual machine setting	1				,		Ţ

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*.

/FR200_1	\sim	ଓ ∢ ▶			
Hardware	^	P Add Hardware			
📑 Add Hardware					
BIOS		You can use this setting to add devices to your virtual machine.			
Boot from CD		Select the devices you want to add and click the Add button.			
Security		SCSI Controller			
Key Storage Drive disabled		Network Adapter			
Memory 4096 MB		RemoteFX 3D Video Adapter			
Processor		Legacy Network Adapter Fibre Channel Adapter			
8 Virtual processors					_
IDE Controller 0				Add	
🗄 👝 Hard Drive					
VFR200_1_7E3722C9-F14		Virtual machines are created with one network adapter. You can	add additio	nal networ	rk
🛛 🧾 IDE Controller 1		adapters as needed.			
DVD Drive					
None					
🗐 SCSI Controller					
🞯 SCSI Controller E 🃮 Network Adapter					
SCSI Controller Viework Adapter Management					
SCSI Controller Wanagement Wetwork Adapter Management Network Adapter					
SCSI Controller Network Adapter Management Network Adapter WAN					
SCSI Controller Vetwork Adapter Management Vetwork Adapter WAN					
SCSI Controller Image: Image and the second secon					
SCSI Controller Image: Image					
SCSI Controller Image: Image					
SCSI Controller Image: Image					
SCSI Controller Image: Image					
SCSI Controller Image: Image					
SCSI Controller Image: Image					
SCSI Controller Image: Image					
 SCSI Controller Network Adapter Management Network Adapter WAN Network Adapter LAN Network Adapter External LAN COM 1 None COM 2 None Diskette Drive None 					
SCSI Controller Image: Image					

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

the dropdown menu.

VFR200_1	v < ▶ ŭ		
★ Hardware	Network Adapter		
📑 Add Hardware			
EIOS		network adapter or remove the network adapter	•
Boot from CD	Virtual switch:		
Security	Not connected	~	
Key Storage Drive disabled	Not connected WAN		
Memory 4096 MB	LAN		
Processor	Management		
8 Virtual processors	External LAN Attach To Host	will use fo	r all
🖃 🧱 IDE Controller 0			
🗉 🚃 Hard Drive	2		
VFR200_1_7E3722C9-F			
🖃 🌉 IDE Controller 1	Bandwidth Management		
OVD Drive	Enable bandwidth manager	ment	
None	Specify bow this petwork adap	oter utilizes network bandwidth. Both Minimum	
SCSI Controller	Bandwidth and Maximum Band	lwidth are measured in Megabits per second.	
Network Adapter Management	Minimum bandwidth:	0 Mbps	
Initialized encodes Initialized encodes Initialized encodes			
WAN	Maximum bandwidth:	0 Mbps	
Network Adapter LAN	To leave the minimum or r	maximum unrestricted, specify 0 as the value.	
E I Network Adapter	To remove the network adapter f	from this virtual machine, click Remove.	
External LAN			
🗉 📮 Network Adapter		Rem	ove
Not connected	Use a legacy network adapte	er instead of this network adapter to perform a	
COM 1	network-based installation o	of the guest operating system or when integration	n
None	services are not installed in t	the guest operating system.	
COM 2 None			
Diskette Drive			
None			
Management			

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*.

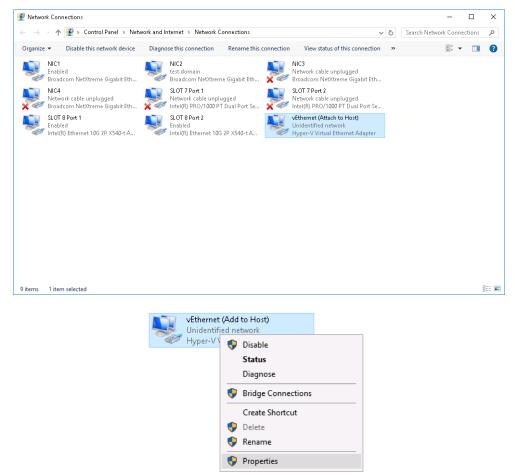
To access the *Network Settings*, right click on the network icon at the bottom right of the screen and select *Open Network and Sharing Center*.

Troubleshoot problems	
Open Network and Sharing Center	
凸 d _☎ 貯 ENG 11:44 US 08/06/2018	3

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

– 🔶 🝸 🛧 🚆 > Control P	anel > Network and Internet > Network and	Sharing Center 🗸 🗸	, (
Control Panel Home	View your basic network inform	ation and set up connections	
Characteristic and the setting of	View your active networks		
Change adapter settings		A l-tt	
Change advanced sharing settings	test.domain Private network	Access type: Internet Connections: II NIC2	
	Fivale network		
	Unidentified network	Access type: No network access	
	Public network	Connections: 🎚 vEthernet (Attach to Host)	

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



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	
Configure	
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)	
< >>	
Install Uninstall Properties	
Description	
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication	
across diverse interconnected networks.	
OK Cancel	

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	
O 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 Advanced	
OK Cancel	

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.

🏺 vEthernet (Attach to Host) Properties	Х
Networking Sharing	
Connect using:	
🚽 Hyper-V Virtual Ethernet Adapter	
Configure	
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) 	~
Install Uninstall Properties	
Description Allows your computer to access resources on a Microsoft network. Close Canc	el

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.

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.