

PORTrockIT Logical-In-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

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	5
	2.1	Prerequisites	5
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	8
	4.4	Network Connections ()	8
		4.4.1 Setting the Hostname/Node Name	9
		4.4.2 Changing IP Addresses	10
	4.5	Licence Keys	11
		4.5.1 Uploading a Licence Key	12
	4.6	Port Mappings (🔄)	13
		4.6.1 Overview	13
		4.6.2 Setting Port Mappings	13
5	Con	figuring IPsec	15
	5.1	Introduction	15
	5.2	Important Notes	15
	5.3	Enabling IPsec	15
	5.4	Copying the Pre-Shared Key to other Bridgeworks Nodes	17
6	Esta	ablishing a Link Between Nodes	18
	6.1		18
	6.2	Firewall	18

	6.3	Topolo	ogy 1: Connecting Bridgeworks Nodes which have Public IP addresses	18
	6.4	Topolo	ogy 2: Connecting Bridgeworks Nodes joined via an external VPN	19
	6.5	Topolo	bgy 3: Connecting Bridgeworks Nodes Using 2 Site NAT	20
	6.6	Topolo	bgy 4: Connecting to a Bridgeworks Node with a NAT on one site	22
	6.7	Acces	s Control	22
	6.8	Node	Management	25
7	Con	figurin	g PORTrockIT Acceleration	28
	7.1	Introdu		28
	7.2	Prerec	quisites	28
	7.3	Adding	g Services	28
		7.3.1	Adding Services with NAT Preservation	30
	7.4	Client	NAT Preservation Mappings	33
	7.5	Establ	ishing Relationships	36
	7.6	Routin	g for Relationships	38
		7.6.1	Example 1 - WAN and LAN on the same subnet	38
		7.6.2	Example 2 - Endpoint on different subnet to LAN interface	41
	7.7	Routin	g Policies	43
		7.7.1	Routing at the Host	43
			7.7.1.1 Adding Routes on Windows	43
			7.7.1.2 Adding Routes on Linux	45
		7.7.2	Routing at the Gateway	46
			7.7.2.1 Adding Routes on a Cisco Router	46
			7.7.2.1.1 Static Routes	46
			7.7.2.1.2 Route-Maps	46
			7.7.2.2 Adding Routes on a pfSense Firewall/Router	46
			7.7.2.2.1 Gateways	47
			7.7.2.2.2 Rules	47
8	Acc	eleratir	ng a Windows Hosts traffic with a guest Hyper-V PORTrockIT	49
	8.1	Introdu	uction	49

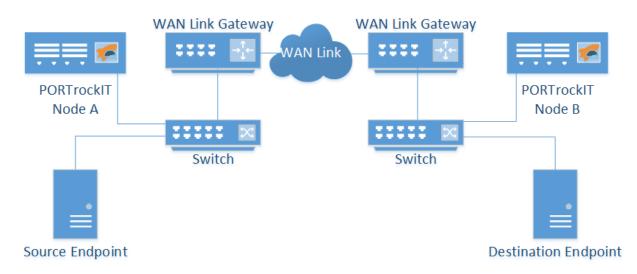
8.2	Connecting host to existing VNet	49
8.3	Adding a dedicated connection	52

9 Useful Links

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

This basic setup can be extended to work in both directions allowing a bidirectional link between the two *Endpoints*.

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

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.

	BRIDGEWORKS
	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 Port 1B Port 2A Port 2B	: 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

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:
	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

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.

password this way, you will be directed to the login screen.

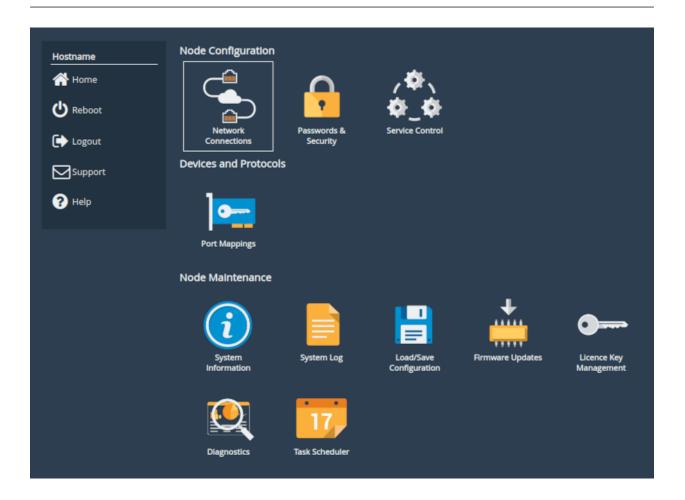
4.3 Logging into the Node

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:	••••••	
	Login	

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.



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.

	Hostname:	bridgeworks
삼 Home		
	Hostname on login page:	
The Connections	DNS Servers:	10.10.10.3
	Fallback DNS Server:	
U Reboot	Default Route:	Auto 🗸
	Enable Dead Gateway Detection:	
🕞 Logout	Dead Gateway Detection Time Dela	y: 5
	Dead Gateway Detection Retry Cou	nt: 1
Support	Enable IPv6:	
? Help	Enable VLANs:	
		Cancel Save

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.

_						
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					
V Rebool	IPv4 Address:			10.10.10.158		
🕞 Logout	MTU:			1500		
	Mapped P	rotocols				
Support	Managemen	ıt				
? Help				_	_	
	Port Settir	ngs				
	Enable Port:					
	MTU Size:		1500			
						_
	 Use DHC Use the f 			dress autom	atically	
	IP Address:	_	10.10.10.158			
	Netmask:		255.255.0.0			
	Gateway:		10.10.10.1			
					Cancel	Save

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.

Node Menu	Node Configuration				
Home		P	,¢∖ ¢_¢		
↓ Logout	Network Connections	Passwords & Security	Service Control		
Support	Devices and Protocols				
 Help Quick Guide 					
	Port Mappings				
	Node Maintenance				
	System Information	System Log	Load/Save Configuration	Firmware Updates	Licence Key Management
	Diagnostics	177 Task Scheduler			

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

Licen	ce Keys
Node Menu	Installed Licence Keys No valid licence keys installed.
Creboot	Licence Key Upload Licence Key File: Choose file No file chosen
? 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			
삼 Home	ID	Feature Type	Limit	Expires	
U Reboot	409348685	WAN	1	1 Days	
🕞 Logout			Remove	Download	
Support	Licence Key	Upload			
? Help	Licence Key File: Choose file	o file chosen			
Events 27 Sep 09:43 Reboot required	Upload				

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.

Protocols for Port 3:		
NetApp Stream Acceleration 🗙		
	Add a protocol	*

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:	
	Generate Key Show Key Delete Key
	Cancel Save

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:]
	Generate Key Show Key Delete Key	
	Cancel	Save

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		
	Generate Key Show Key Delete Key		
	Cancel Save		

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:

•••••
Generate Key Show Key Delete Key
Cancel Save

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.

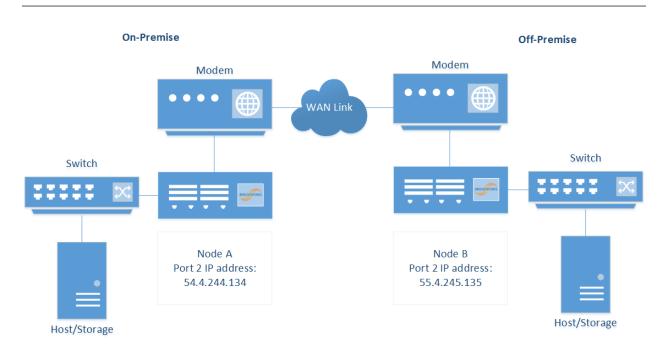
6.2 Firewall

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.

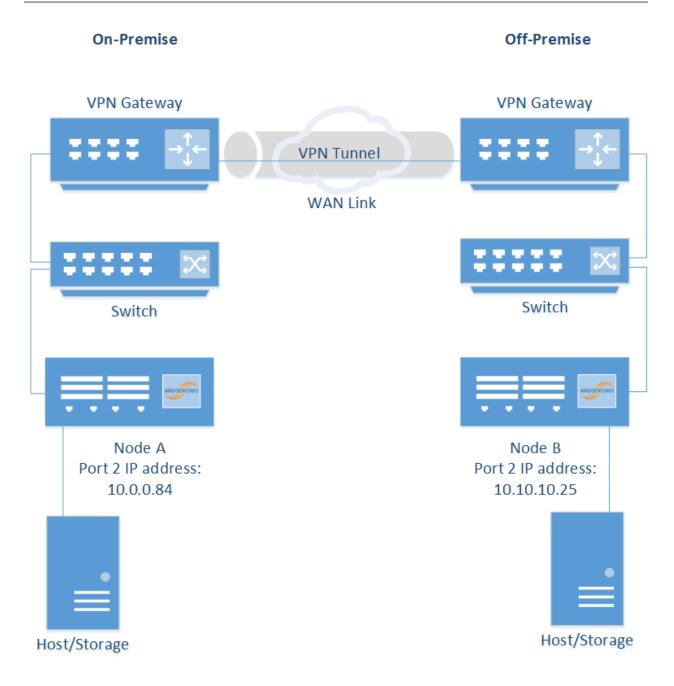


In this example the IP addresses for establishing a Nodal link are the public IP addresses assigned to *Port 2* on the Bridgeworks Nodes:

- 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.

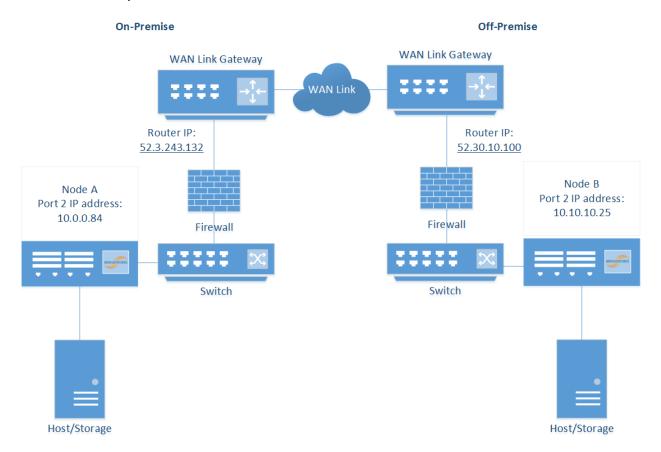
The firewall must be configured with the following sets of NAT port forwarding rules:

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.

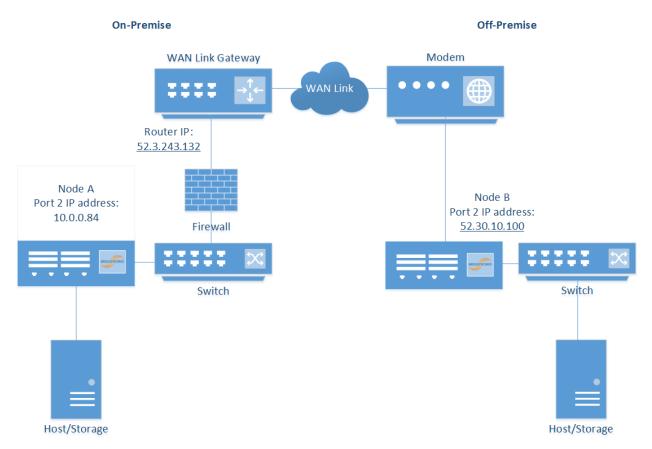


In this example the IP addresses for establishing a Nodal link are the IP addresses of the router, in this case:

- 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.

Node Menu	Remote Administration
♠ Nodes ♣ Reboot	Whitelist
➡ Logout	Whitelisted IP Addresses IP address
? Help	Use the form below to add an IP to the whitelist New IP: Add Remove
Licensed To 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
🕞 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	Whitelist
U Reboot	✓ Enable Whitelist
🕩 Logout	Whitelisted IP Addresses
Support	IP address 10.0.084
? Help	New IP: Add Remove
Licensed To Bridgeworks Ltd	Cancel Save



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.

Node Menu	New Remote Nod	e Details	
合 Home	IP Address	10.10.25	
♠ Nodes	Network Interface	Port 2 (10.0.0.84)	~
U Reboot			Cancel Add
🕩 Logout			
Support			
? Help			
Licensed To			
Bridgeworks Ltd			

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

Ad	d Remote Node	
Hostname	New Remote Node Details	
☆ Home ▲ Nodes	Connected to Node	_
Reboot	Hostname Node_B Connected to Node	Cancel Add
➡ Logout	ок	
PHelp		-

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 Node Details			
삼 Home	IP Address	10.0.84		
1 Nodes	Network Interface	Port 2 (10.10.10.25)		
U Reboot			Cancel Add	
🕞 Logout				
Support				
? Help				
Licensed To				
Bridgeworks Ltd				

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

Hostname	New Remote Node Details	
☆ Home Nodes	Connected to Node	
C Reboot	Hostname Node_A Connected to Node	Cancel Add
🗭 Logout		
Support	ОК	

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

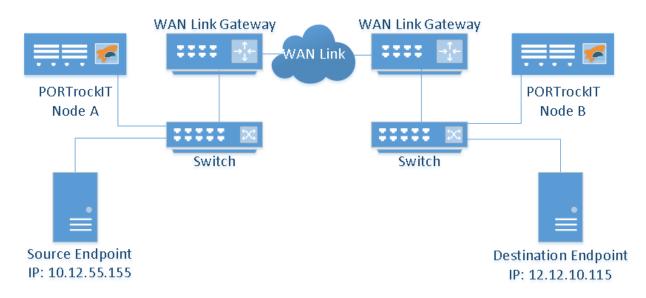
In order to configure PORTrockIT acceleration you must have the following:

- 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

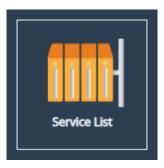
A service defines a part of the local topology, including all information the PORTrockIT Node needs to connect to a target server.

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 instructions will need to be carried out using the GUI for both *Node A* and *Node B* to allow for bidirectional connections.

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.

Configuration for Node A

Add New Service		
Name	Source Endpoint	
Address	10.12.55.155	
Protocol	NetApp SnapMirror	
Outgoing Interface	Port 3	T
		Cancel Add Service

Configuration for Node B

Add New Service	•
Name	Destination Endpoint
Address	12.12.10.115
Protocol	NetApp SnapMirror
Outgoing Interface	Port 3
	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.

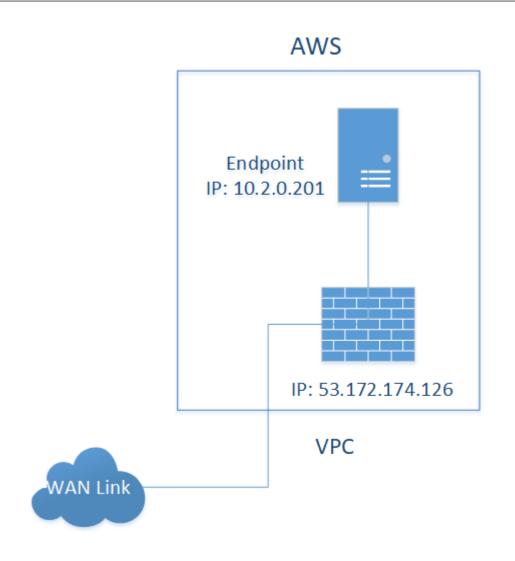
7.3.1 Adding Services with NAT Preservation

Currently setting up a NAT preservation configuration is only available if you have a WANdisco Fusion licence and are using a Cloud environment.

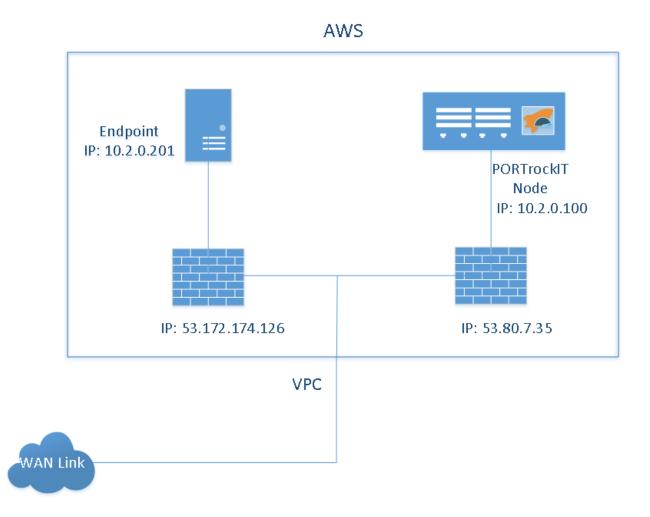
The following section explains how to set up a service when a previously used NAT IP address needs to be preserved. Client NAT preservation is also required for a complete set up, which is explained in the Client NAT Preservation Mappings section.

When a target server resides behind a firewall which is performing NAT forwarding and the PORTrockIT is also placed behind a firewall, a NAT service is required. NAT services allow the PORTrockIT to translate the public IP address of the server to its private IP address when connecting.

The set up before the PORTrockIT is introduced can be seen in the following topology diagram.



The changes to the system after the PORTrockIT has been added can be seen in the topology diagram displayed below.



To add a service with NAT preservation, click on the *Add a Service* button on the *Service List* page below. 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.



To enable NAT preservation for a service, click the *Enable NAT* switch so that it says 'On'. Enter the public and private IPs of the local server being connected to into the *Public IP* and *Private IP* fields and click *Add Service* to finish the creation of this service. The configuration for this example is shown below.

Add New Service	e
Name	Service 1
Enable NAT	
Public IP	53.172.174.126
Private IP	10.2.0.201
Address	IPv4 Address / CIDR / Hostname
Protocol	WANdisco Fusion
Outgoing Interface	Port 1
	Cancel Add Service

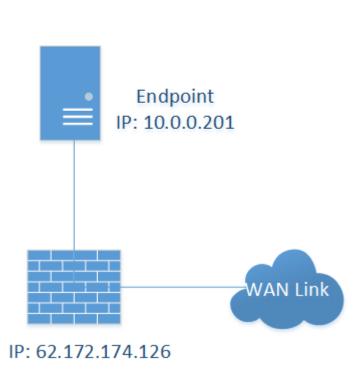
7.4 Client NAT Preservation Mappings

Currently setting up a NAT preservation configuration is only available if you have a WANdisco Fusion licence and are using a Cloud environment.

Client NAT preservation mappings are used for services which have been previously connected through a NAT firewall and are required to keep the existing source IP addresses in order for your endpoints' previous configuration to require no modification.

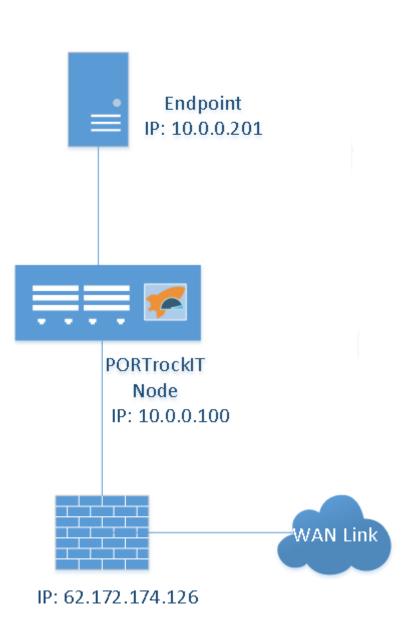
The previous connection set up through the NAT firewall can be seen in the topology diagram below.

Site 1



The addition of the PORTrockIT to the system can be seen in the following topology diagram.

Site 1



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

Client NAT Preservation

To establish a new mapping, enter the public and private IP pair of the client into the input boxes

and click *Add*. The mapping for this example is shown below.

Clier	nt NAT Preservatior	1
Node Menu	Client NAT IP Address	es
삼 Home	Private IP address	Public IP address
U Reboot	10.0.0.201 Private IP address:	62.172.174.126
🕞 Logout	Private IP address:	
Support	rabie ir address.	Add Remove
? Help		Cancel Save

Once entries have been added to the table they need to be saved to ensure that they take effect, which can be done by pressing the *Save* button.

7.5 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.

The following steps will have to be completed on both Node A and 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.

Hostname	Active Services	
Home	Source Endpoint (NetApp SnapMirror) 10.12.55.155 Ports: 3	010
C Reboot	← Configure Services Cancel	Save
► Logout		
? Help		

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:

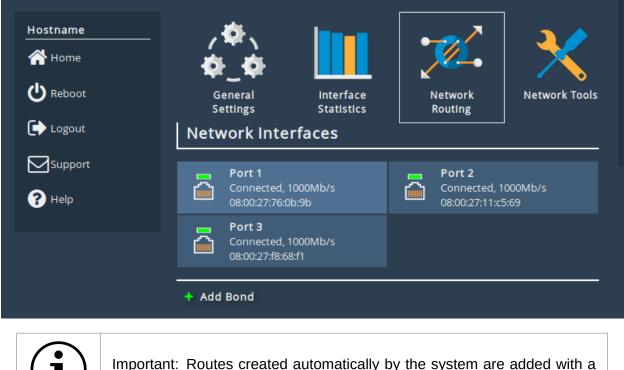
Activ	e Incoming Relationships
m	Remote Node (NetApp SnapMirror) 10.12.55.155 No connections

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.

7.6 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.

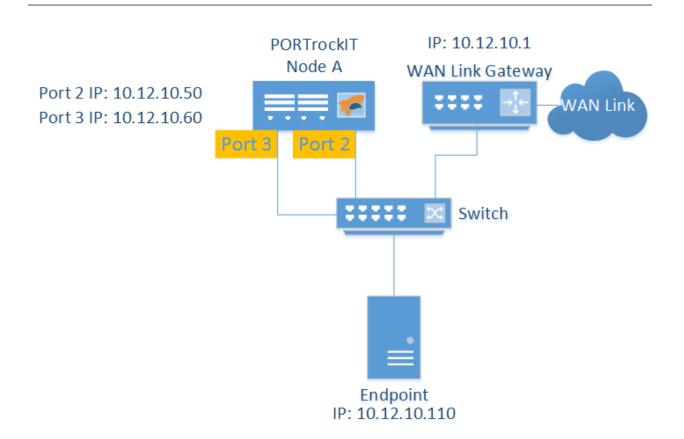


Important: Routes created automatically by the system are added with a metric of 1, allowing you to override defaults by using a metric of 0.

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.

7.6.1 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 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

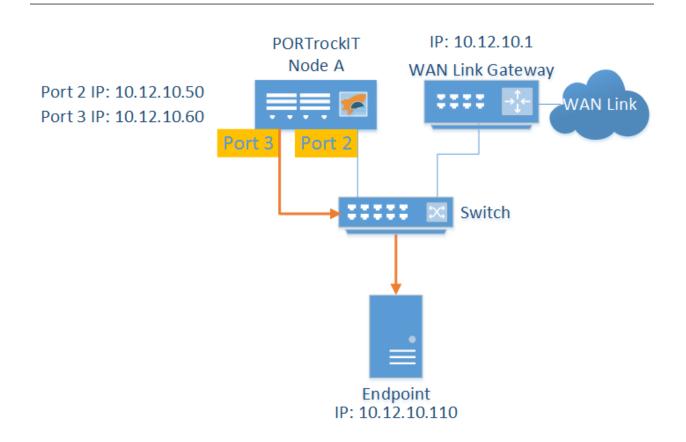
Currently *Node A* will be sending traffic destined for the *Endpoint* from *Port 2* instead of *Port 3*. To resolve this, a static route needs to be added.

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

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

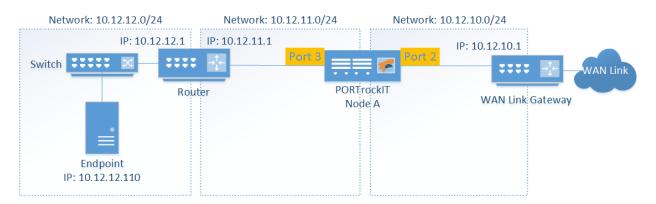
0.0.0.0/0 10.	eway Interface	Metric	
	.10.10.1 Port 1		
		1	Delete
10.10.0.0/16	Port 1	1	Delete
10.12.10.0/2 4	Port 2	1	Delete
10.12.10.11 0/32	Port 3	1	Delete

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



7.6.2 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.

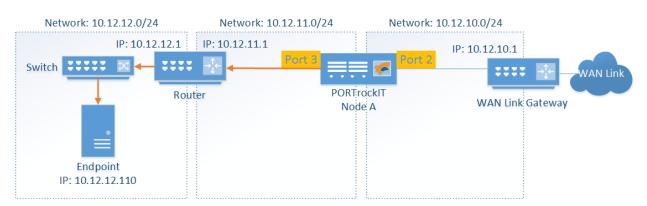
DestinationGatewayInterfaceMetric0.0.0.0/010.10.10.1Port 11Delete10.10.0.0/16Port 11Delete10.12.10.0/2Port 21Delete4Port 31Delete	Global Rou	ting Table			
10.10.0.0/16 Port 1 1 Delete 10.12.10.0/2 Port 2 1 Delete 4 10.12.11.0/2 Port 3 1 Delete	Destination	Gateway	Interface	Metric	
10.12.10.0/2 Port 2 1 Delete 4 10.12.11.0/2 Port 3 1 Delete	0.0.0/0	10.10.10.1	Port 1	1	Delete
4 10.12.11.0/2 Port 3 1 Delete	10.10.0.0/16		Port 1	1	Delete
			Port 2	1	Delete
			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 V	
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

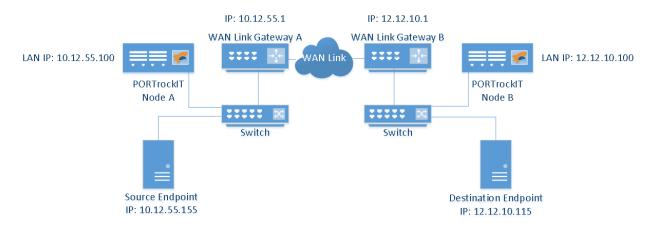


Network traffic for the *Endpoint* will be sent from *Port 3* and be directed through the router.

7.7 Routing Policies

Now that the PORTrockIT software configuration is complete, you must configure your network's routing policy to route the traffic to be accelerated to the LAN IP address of the PORTrockIT unit to complete the set up.

This section provides some examples of how to route traffic, which is to be accelerated, into a PORTrockIT unit for the following topology.



7.7.1 Routing at the Host

In this configuration, routing rules are added to the host to make the IP address of the PORTrockIT's LAN port the gateway for either a specific Endpoint or the default gateway.

The routing covered here will be from the point of view of the *Source Endpoint* wanting to accelerate data transfer to the *Destination Endpoint*.

7.7.1.1 Adding Routes on Windows

This example uses a Windows host for the *Source Endpoint*. It has a single network interface with a static IP configuration of 10.12.55.155 and a default gateway of 10.12.55.1. The route will be added on the command line using Command Prompt.

Current IPv4 routes can be displayed using route print -4. Below shows the command being used on the Windows host.

Administrator: Comm	and Prompt		_		×
1	 7f 23vmxne Softw	t3 Ethernet Adapt are Loopback Inte soft ISATAP Adapt	rface 1		
IPv4 Route Table Active Routes:					
Network Destinatio	n Netmask	Gateway	Interface	Metric	
0.0.0.0	0.0.0.0	10.12.55.1	10.12.55.155	271	
10.12.55.0	255.255.255.0	On-link	10.12.55.155	271	
10.12.55.155	255.255.255.255	On-link	10.12.55.155	271	
10.12.55.255	255.255.255.255	On-link	10.12.55.155	271	
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331	
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331	
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331	
224.0.0.0	240.0.0.0	On-link	127.0.0.1	331	
224.0.0.0	240.0.0.0	On-link	10.12.55.155	271	
255.255.255.255	255.255.255.255	On-link	127.0.0.1	331	
255.255.255.255	255.255.255.255	On-link	10.12.55.155	271	
Persistent Routes:					
Network Address	Netmask	Gateway Address	Metric		
0.0.0.0	0.0.0	10.12.55.1	Default		
				======	

A persistent route can be added to Windows using the route command. For this example, a route is added to direct traffic for *Destination Endpoint* through *PORTrockIT Node A* using its LAN IP address.

Administrator: Command Prompt	—	\times
c:\>route add -p 12.12.10.115 mask 255.255.255.255 10.12.55.100 OK!		Â

The route is then added to the routing table and appears in the *Persistent Routes* section as shown below.

Administrator: Command Prompt

c:\>route print -4				· · · · · · · · · · · · · · · · · · ·
1	7f 23vmxne Softw	t3 Ethernet Adapt are Loopback Inte soft ISATAP Adapt	rface 1	
IPv4 Route Table				
Active Routes:				
Network Destinatio	n Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	10.12.55.1		271
	255.255.255.0	On-link	10.12.55.155	271
10.12.55.155	255.255.255.255	On-link	10.12.55.155	271
10.12.55.255	255.255.255.255	On-link	10.12.55.155	271
12.12.10.115	255.255.255.255	10.12.55.100	10.12.55.155	16
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-link	10.12.55.155	271
255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
255.255.255.255	255.255.255.255	On-link	10.12.55.155	271
Persistent Routes:			==================	======
Network Address	Netmask	Gateway Address	Metric	
0.0.0.0	0.0.0.0	10.12.55.1		
12.12.10.115	255.255.255.255	10.12.55.100	1	
	======================	===================	=====================	

_

 \times

7.7.1.2 Adding Routes on Linux

These instructions apply to Red Hat Enterprise Linux (RHEL).

This example uses a Linux host for the *Source Endpoint*. It has a single network interface named **eth0** with a static IP configuration of 10.12.55.155 and a default gateway of 10.12.55.1. The route will be added on the command line.

Current IPv4 routes can be displayed using ip -4 route show. Below shows the command being used on the Linux host.

```
# ip -4 route show
default via 10.12.55.1 dev eth0 proto static metric 100
10.12.55.0/24 dev eth0 proto kernel scope link src 10.12.55.155 metric 100
```

A route can be added to Linux using the ip -4 route command. For this example, a route is added to direct traffic for *Destination Endpoint* through *PORTrockIT Node A* using its LAN IP address.

ip -4 route add 12.12.10.115 via 10.12.55.100 dev eth0

The route is then added to the routing table as shown below.

```
# ip -4 route show
default via 10.12.55.1 dev eth0 proto static metric 100
10.12.55.0/24 dev eth0 proto kernel scope link src 10.12.55.155 metric 100
12.12.10.115 via 10.12.55.100 dev eth0
```

In order to make the route persistent, it must be added to the file /etc/sysconfig/network-scripts/route-eth0 as shown below.

echo '12.12.10.115 via 10.12.55.100 dev eth0' >> /etc/sysconfig/network-scripts/route-eth0

7.7.2 Routing at the Gateway

In this configuration, routing rules are added to a firewall or gateway to redirect traffic that is subject for acceleration to the PORTrockIT's LAN port.

The routing covered here will be from the point of view of the gateway of the *Source Endpoint* wanting to accelerate data transfer to the *Destination Endpoint*.

7.7.2.1 Adding Routes on a Cisco Router

7.7.2.1.1 Static Routes

To add a static routing rule on a Cisco Router from the command line, the configuration mode must be entered with the command:

conf t

Then the route can be added that redirects all traffic for the *Destination Endpoint* through the PORTrockIT unit, by entering the following command:

ip route 12.12.10.115 255.255.255.255 10.12.55.100

7.7.2.1.2 Route-Maps

A route-map allows more specific redirection by specifying both the IP and port of the source and destination.

To setup a route-map, the configuration mode must be entered with the command:

conf t

For this example an access-list is required, which specifies the traffic is to be redirected. The following command adds an access-list that matches traffic on TCP port 11104 from the *Source Endpoint* going to the *Destination Endpoint*.

access-list 101 permit tcp host 10.12.55.155 host 12.12.10.115 eq 11104

Using this access-list as a matching criteria, the route-map can be created using the following command:

route-map portrockit permit 10

Then the route-map can be configured to use the access-list to match traffic and to redirect that traffic into the PORTrockIT with the following commands:

match ip address 101 set ip next-hop 10.12.55.100

7.7.2.2 Adding Routes on a pfSense Firewall/Router

These instructions have been tested with pfSense 2.3.4 Community Edition.

7.7.2.2.1 Gateways

In order for pfSense to redirect traffic to be accelerated to a PORTrockIT unit, the unit must be added as a gateway.

On WAN Link Gateway A, the LAN IP address of PORTrockIT Node A must be added as a gateway:

Edit Gateway		
Interface	LAN v Choose which interface this gateway applies to.	
Address Family	IPv4 v Choose the Internet Protocol this gateway uses.	
Name	PORTrockIT Gateway name	
Gateway	10.12.55.100 Gateway IP address	

Similarly, on WAN Link Gateway B, the LAN IP address of PORTrockIT Node B must be added as a gateway.

7.7.2.2.2 Rules

Now that the PORTrockIT units have been added as gateways, firewall rules can be added that redirect traffic to be accelerated to the PORTrockIT units.

On WAN Link Gateway A, add a new firewall rule. This rule covers accelerated traffic from the *Source Endpoint* to the *Destination Endpoint*. The following fields must be modified:

- Destination: 12.12.10.115
- Destination Port Range: 11104–11105
- State type: Sloppy
- Gateway: PORTrockIT

In this example, TCP traffic from the *Source Endpoint* to the *Destination Endpoint* will be accelerated if its destination port is either 11104 or 11105:

Destination			
Destination	Invert match.	Single host or alias	▼ 12.12.10.115 / ▼
Destination Port	(other) 🔻	11104 (other)	▼ 11105
Range	From	Custom To	Custom
	Specify the destination	port or port range for this rule. The "To"	field may be left empty if only filtering a single port.

Advanced Option	IS	
State type	Sloppy	Y
	Sloppy: works with all IP protocols	
Gateway	PORTrockIT - 10.12.55.100	T
	Leave as 'default' to use the system routing t	able. Or choose a gateway to utilize policy based routing.

On WAN Link Gateway B, add a new firewall rule. This rule covers accelerated return traffic from the Destination Endpoint to the Source Endpoint. The following fields must be modified:

- Source: 12.12.10.115
- Source Port Range: 11104–11105
- TCP Flags: SYN+ACK out of SYN+ACK
- State type: Keep
- Gateway: PORTrockIT

In this example, return TCP traffic from the *Destination Endpoint* to the *Source Endpoint* will be accelerated if its source port is either 11104 or 11105:

Source											
Source	Invert mat	ch.	3	Single	host or	alias			T	12.12.10.115	/ •
	🔅 Hide Advan	ced									
	The Source P this setting m							ndom and almo	ost nev	er equal to the destinati	on port. In most cases
Source Port Range	(other)	•	1	1104			(other)	•	11105	
j	From		Cu	istom			То			Custom	
	Specify the sc	urce po	ort or po	ort ran	ge for t	this rule	e. The	"To" field may b	e left e	empty if only filtering a s	single port.
Advanced Option	S										
TCP Flags	FIN	SYN	RST	PSH	ACK	URG	ECE	CWR			
	set 🔲	v									
	out of 📃	1			√						
	out of 📃 🗖	•			¥		_	_			
	Any flags.	_			_	_		_	to mate	ch.	
State type	Any flags. Use this to ch	_			_	_			to mate	ch.	
State type	Any flags.	oose TC	CP flag	s that r	_	_		ed for this rule t	to mate	ch.	
	Any flags. Use this to ch Keep Keep: works v	oose TC vith all II	CP flag: P proto	s that r	_	_		ed for this rule t	to mat	ch.	
State type Gateway	Any flags. Use this to ch Keep Keep: works v PORTrockIT	vith all II	CP flags P proto 10.100	s that r ocols	must b	e set o	clear	ed for this rule t		ch. tilize policy based routin	

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.

📲 Hyper-V Manager						- 0	×
File Action View Help							
🗢 🔿 🙍 🖬							
🚻 Hyper-V Manager	/irtual Machines				_	Actions	
2EU3	~					ZEUS	<u> </u>
	Name Deb	State	CPU Usage 0%	Assigned Memory 16384 MB	Uptir 5.22:-	New	•
	VFR200_1	Running Off	0%	16384 MB	5.22:	🚯 Import Virtual Machine	
		0				📑 Hyper-V Settings	
						🚼 Virtual Switch Manager	
						🛃 Virtual SAN Manager	
	c					🚅 Edit Disk	
	Checkpoints					Inspect Disk	
	B-R VFR200_1 - (01/06/2018 - 15:10:50)					Stop Service	
	Now	````				X Remove Server	
						D Refresh	
						View	-
						Help	
						VFR200_1	•
	/FR200_1					📲 Connect	
		Created:	01/06/2018 14:08:4	47 Clustered: N		📷 Settings	
		Creaced: Configuration Version:		tiusterea: N	0	🕲 Start	
		Generation:	1			🔂 Checkpoint	
		Notes:	None			5 Revert	
						B→ Move	
						Export	
	Summary Memory	Networking Replication	1			🗐 Rename	
<					>	Delete	
					-	, 	

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 Switch Manager for ZEUS	- 🗆 X
 Virtual Switches New virtual network switch New virtual network switch New virtual network switch New virtual switch 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 	Virtual Switch Properties Name: External LAN Notes: Connection type What do you want to connect this virtual switch to? 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 Allow management operating system to share this network adapter Allow management operating system to share this network adapter Number of the VLAN identification for management operating system Number of the VLAN identification for management operating system Number of all network communications through this network adapter. This setting does not affect virtual machine networking. 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.
	OK Cancel Apply

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

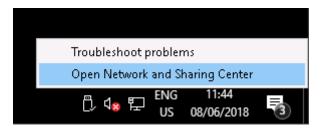
Connection type What do you want to connect this virtual switch to? External network:	
Intel(R) Ethernet 10G 2P X540-t Adapter #2	~
Allow management operating system to share this network ada	apter
Enable single-root I/O virtualization (SR-IOV)	
 Internal network 	
O Private network	

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.

🗧 🔶 🕤 🛧 💆 🕨 Control	Panel > Network and Internet > Network and	Sharing Center	\sim
Control Panel Home	View your basic network inform	ation and set up connections	
Change adapter settings	View your active networks		
Change advanced sharing settings	test.domain Private network	Access type: Internet Connections: I NIC2	
	Unidentified network	Access type: No network access	

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 7.6: 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.

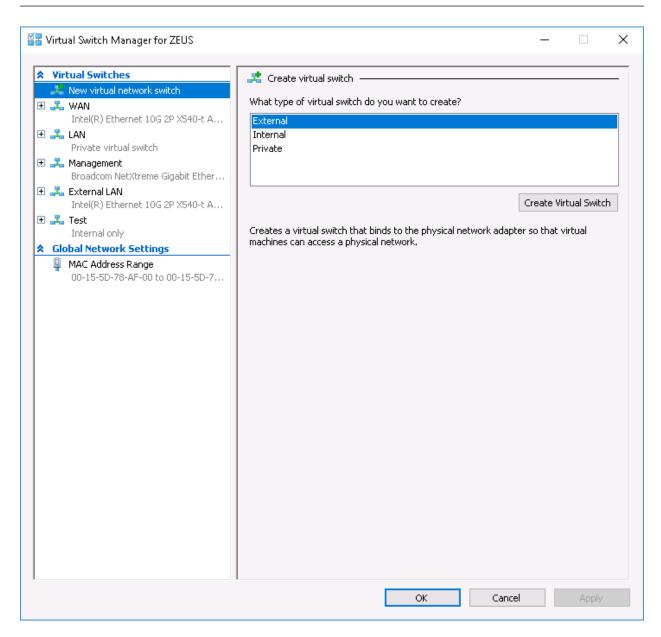
At this point the host would be unable to connect to the private LAN port of the PORTrockIT.

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.

📲 Hyper-V Manager						– 🗆 ×
File Action View Help						
🗢 🔿 🙍 🖬						
📑 Hyper-V Manager						Actions
E ZEUS	Virtual Machines					ZEUS 🔺 🛆
	Name	State	CPU Usage	Assigned Mem		New
	Deb VFR200_1	Running Off	0%	16384 MB	5.22:	🐚 Import Virtual Machine
						🔄 Hyper-V Settings
						🚰 Virtual Switch Manager
						🛃 Virtual SAN Manager
	<					🚄 Edit Disk
	Checkpoints					🔄 Inspect Disk
		· (01/06/2018 · 15:10:50)				Stop Service
	Now					🗙 Remove Server
						🖏 Refresh
						View
						👔 Help
					VFR200_1	
	VFR200_1					📲 Connect
						🛐 Settings
		Created: Configuration Version:	01/06/2018 14:08:4	7 Cluster	ed: No	🕲 Start
		-	1			🔂 Checkpoint
		Notes:	None			5 Revert
						🖶 Move
						🛐 Export
	Summary Memory	Networking Replication	1			🛒 Rename
	<				>	🕞 Delete 🗸

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



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

🚰 Virtual Switch Manager for ZEUS	– 🗆 X
 Virtual Switch Manager for ZEUS Virtual Switches New virtual network switch New virtual network switch New virtual network switch New virtual switch An Private virtual switch Anagement 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 Name: Attach To Host Notes: Connection type What do you want to connect this virtual switch to? 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 VLAN ID Charles VLAN ID Charles VLAN ID Charles VLAN ID Charles Allow the thermate operating system Allow the the management operating system Allow the thermate opera
	Remove 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. OK Cancel Apply

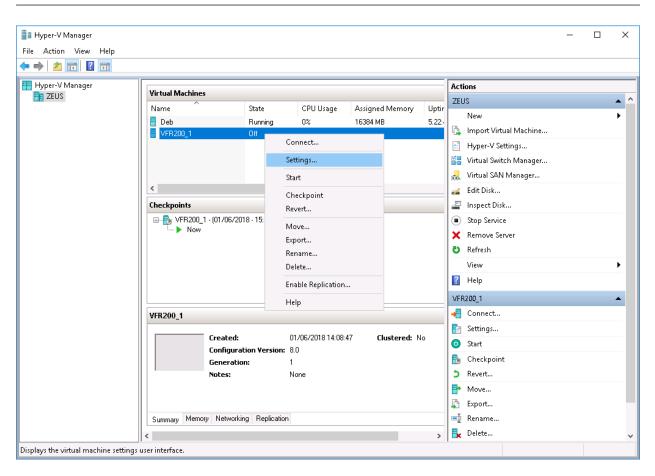
In the new properties section select a name for the network connection.

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

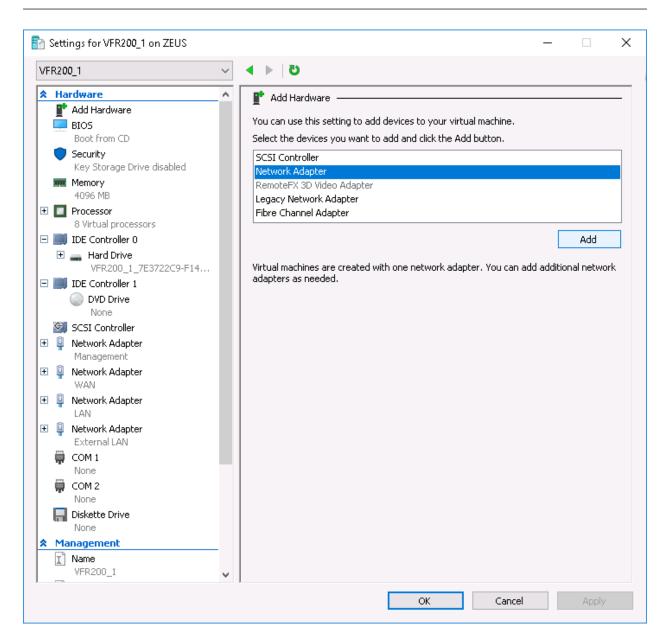
The next stage is to close the *Virtual Switch Manager* and bring up the *Settings* page for the PORTrockIT.



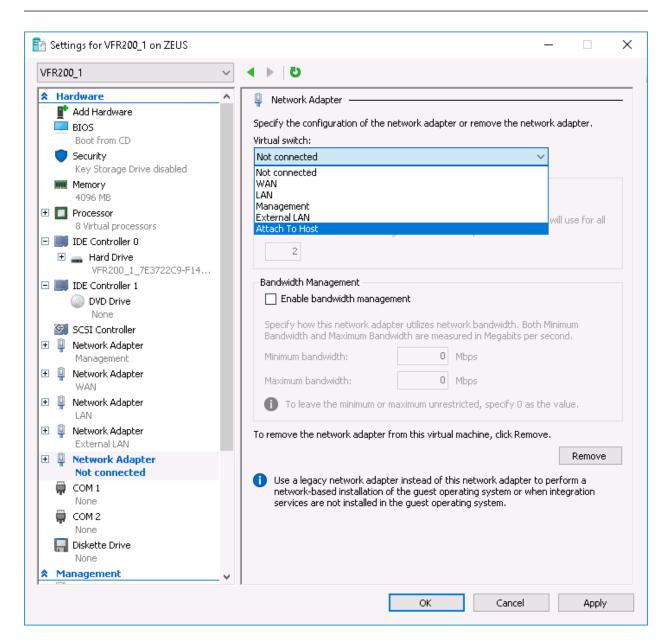
Note: The PORTrockIT needs to be powered off to add or remove network connections.



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*.



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



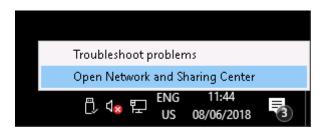
Click Apply and then OK.

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*.

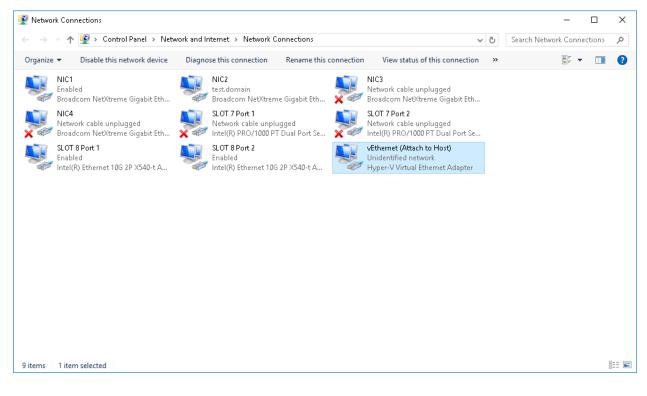
To access the *Network Settings*, right click on the network icon at the bottom right of the screen and select *Open Network and Sharing Center*.



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

🔶 🐳 👻 🛧 🕎 > Control I	Panel > Network and Internet > Network and	Sharing Center	~ Č
Control Panel Home	View your basic network inform	ation and set up connections	
Change adapter settings	View your active networks		
Change advanced sharing	test.domain	Access type: Internet	
settings	Private network	Connections: 📱 NIC2	
	Unidentified network	Access type: No network acces	ss
	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.



vEthernet Unidentifi			
Hyper-V \	•	Disable	
		Status	
		Diagnose	
	•	Bridge Connections	
		Create Shortcut	
	•	Delete	
	•	Rename	
	•	Properties	

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 Client for Microsoft Networks Client 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							
• 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.

ļ,	/Ethernet (Attach to I	Host) Properties		×	
Net	working Sharing				
Co	onnect using:				
ļ	🕎 Hyper-V Virtual Eth	iernet Adapter			
			Configure		
Tł	nis 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.					
		Cle	ose Can	cel	

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 7.6: 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.