

August 19th 2016

GÉANT & Microsoft ExpressRoute Request and Configuration manual

Deliverable is part of GN4-2 JRA1-T3

Contractual Date:01-01-2015Version0.04Authors:Migiel de Vos (SURFnet), Borjan Bonsen (SURFnet)

© GÉANT Limited on behalf of the GN4-2 project.

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

Abstract

Future programmable networks must be highly agile and dynamic allowing end-users to control their traffic. While providing on-demand connectivity, they must also be scalable and elastic. For these purposes, the zero touch provisioning concept needs to be extended to a multi-domain network level where the process of automation can be based primarily on NFV.



Document Revision History

Version	Date	Description of change	Person
0.01	2016-07-01	Very first draft based on SURFnet's version 0.98 – will need to check and change a lot more details	Migiel de Vos
0.02	2016-08-09	Input from first tests with direct MS ExpressRoute via GÉANT	Migiel de Vos
0.03	2016-08-19	Review by Gerben van Malenstein	Migiel de Vos
0.04	2016-08-06	Minor changes, still very drafty	Migiel de Vos





Table of Contents

1	Introdu	uction		4
2	Preconditions			6
3	Requesting an ExpressRoute via GÉANT			
Appen	ppendix A Examples		9	
	A.1	Reques	esting ExpressRoute via the Microsoft Portal	
		A.1.1 circuit	Opening the Microsoft Portal to request an ExpressRc 9	oute
		A.1.2	Requesting an S-Key	10
	A.2	Configu	uring an ExpressRoute peering	12
		A.2.1	Configuring an ExpressRoute peering in the Azure portal	13
	A.3	Configu	uring a Virtual Network with Gateway	14
		A.3.1	Configuring a Virtual Network via the Azure portal	14
		A.3.2	Configuring a Virtual Network Gateway via the Azure portal	15
		A.3.3	Attach Virtual Network with gateway to ExpressRoute	16
	A.4	Local n	etwork configuration	17
		A.4.1	Ethernet layer (L2)	17
		A.4.2	IP layer (L3)	19
	A.5	BGP co	nfiguration	19
		A.5.1	Configuring the BGP peering	20
		A.5.2	Configuring the local preference and metric	21
		A.5.3	Prefix list	23

Error! No text of specified style in document.





1 Introduction

GÉANT provides the opportunity to deliver direct connectivity from institutions via the NRENs and GÉANT to Microsoft. Microsoft calls this ExpressRoute; a service that can be delivered on top of point-to-point Layer2 connectivity.

A Microsoft ExpressRoute lets an institution extend their on-premises network into the Microsoft cloud platform, Microsoft Azure, over a dedicated connection. ExpressRoute connections bypass the public internet and enable the institution to use institutional IP address space for the infrastructure hosted at Microsoft. ExpressRoutes are carried over private L2 connections on top of which the institution sets up IP connectivity between the on-premises network and the network hosted at Microsoft. External BGP is used as the routing protocol.

This manual can be (adjusted and) handed over to institutions to setup their ExpressRoute via their NREN to Microsoft. The picture below shows schematically, how connectivity is provided between the institution and Microsoft.

Introduction





Figure 1: schematic overview of an ExpressRoute connection via GÉANT



Microsoft ExpressRoute has direct connectivity (via NetherLight) to GÉANT in Amsterdam and direct connectivity (via NetherLight) to GÉANT in London. Via these connections redundant services can be provided to all NRENs and their connected institutions in Europe.

The default for delivering ExpressRoute connectivity is by providing two double tagged services (IEEE 802.1ad) between Microsoft and the institution. In this case the outer tag with its payload will be transparently transported between the institution and Microsoft. This means that the NREN, GÉANT and NetherLight will only care about transporting packets between the institution and Microsoft based on the outer tag. Both Microsoft and the institution will handle the inner and outer tags, including the payload for both services (primary and secondary). By default, the primary and secondary VLAN tags are identical. Microsoft recommends to use two customer devices to terminate each of the services.

There are many other solutions available for providing ExpressRoutes to customers. Examples are:

- Accepting the double VLAN tagged from Microsoft as is (described above)
- Stripping the outer tag facing the institution, so that only the inner tag(s) remain
- Retagging VLAN tag(s) such that both services can be terminated on the same institution port/device
- Creating a VRF per ExpressRoute/institution

These options are not discussed in this manual.

This technical manual describes how a system and/or network manager from an institution and/or NREN can request and setup the Microsoft ExpressRoute services via their NREN and GÉANT.

2 **Preconditions**

To be able to request and setup an ExpressRoute connection via GÉANT institutions should consider the following conditions and requirements:

- You must have a valid Microsoft account with an active Azure subscription
- You must have connectivity to an NREN that is connected to GÉANT
- You need a device that is capable of handling double tagged VLANs (IEEE 802.1ad)¹
- You must have a router that runs BGP

¹ Other options are possible, but not discussed in the manual



3 Requesting an ExpressRoute via GÉANT

Microsoft and the NREN require the necessary information for setting up the ExpressRoute service. Most information comes from numbering plans and background information of the institution itself, other information such as the Microsoft s-key follows from the application process.

As a guideline for delivering the service we adhere to the following schedule:

	Responsible party	Exp. time
Check availability at your local NREN (optional but recommended)	Institution	1 week
This first check is performed to see whether the preconditions are met to quickly set up the connection. If the conditions are met, the Microsoft s-key can be requested.		
Request s-key at Microsoft *	Institution	1 hour
Fill the application form and send it to your NREN	Institution	1 hour
Determine request and configure end-to-end service	NREN (and GÉANT)	1 week
Configure layer3 connectivity with Microsoft	Institution	1 day
Test connectivity with the Azure platform	Institution	1 day

* note that Microsoft starts billing for the ExpressRoute connectivity as soon as you receive the s-key

The first check at your NREN can be used to speed up the next steps in the procedure. It is wise to use this first check, such that your NREN is able to verify if your institution is ready to request an ExpressRoute. Please send an email to your contact at the NREN with the following information:

- Port name(s)/number(s) where the ExpressRoute service should be delivered
- Preferred bandwidth to Azure

The NREN will confirm whether your institution is ready to start-up the next phase, which is requesting a so-called "S-key" at Microsoft.

The application for requesting an ExpressRoute can be done by using the table/form on the next page. This table contains some fields that are required by GÉANT, Microsoft and your NREN. Only the red fields need to be filled.



Table 1, required information for requesting an ExpressRoute

Azure ExpressRoute GÉANT information:			
NREN Details			
NREN name			
Customer Contact Details			
Customer name			
Technical/Operations Contact name			
Technical contact e-mail			
Technical contact phone number			
GÉANT Service Provider			
Azure	Amsterdam ¹		
AWS Account ID or Azure S-Key	xxxxxxx-xxxx-xxxx-xxxx-xxxxx		
Requested ExpressRoute bandwidth (Gbps)			
Type of service	Redundant		
Customer port details			
Primary port details			
Secondary port details (only in case of two ports)			

Please forward this table with the required details to your NREN. The NREN will ask GÉANT to configure the service from ExpressRoute to your NREN, such that the NREN is able to complete the part towards the institution.

After the above is completed, the institution can setup VLAN and BGP configuration and test the connectivity to Azure.



Appendix A **Examples**

A.1 Requesting ExpressRoute via the Microsoft Portal

To be able to request an s-key you'll need:

- A Microsoft account with an active Azure subscription

A.1.1 Opening the Microsoft Portal to request an ExpressRoute circuit

Use your favorite browser to go to https://portal.azure.com/ and login with your Microsoft Account with Azure subscription. Once logged in click "Browse >", search for "ExpressRoute-circuits" and click on it.







A.1.2 Requesting an S-Key

Click on "Add" to request an S-Key.

Enter the details as shown in the picture and modify values to your own needs.

Create ExpressRo — 🗖 🗙	* Billing model Unlimited Metered
	Allow classic operations 0
Create new or import from classic 🖤	* Coloriation
Create new Import	 Subscription
* Circuit name	Azure ExpressRoute pilot
GEANT_test_circuit	* Resource group 🖲
* Provider 0	Create new Use existing
GEANT 🗸	GEANT-TEST 🗸
* Peering location 0	* Location
Amsterdam 🗸	West Europe 🗸 🗸
* Bandwidth 🖲	
10Gbps 🗸	
* SKU 🛛	Pin to dashboard
Standard Premium	Create

Please note that the peering location will be Amsterdam, but GÉANT will provision the service via Amsterdam and London to other locations in Europe. This is done to create resiliency for the ExpressRoute services.

When you are ready click on "Create". Please note that Microsoft starts billing from this moment. In the next screen you'll find the Service Key. Using this key you should be able to fill the application for requesting an ExpressRoute and send this to your NREN.

ExpressRoute-circ * -	GEANT_test_circuit	* _ ¤ ×
+ Add ≣≣ Columns ひ Refresh	🔅 Settings 🟛 Delete	
Subscriptions: Azure ExpressRoute pilot	i Initiate the provisioning process with	your service provider.
Filter items	Essentials 🔨	CL 48 🖉
NAME	Resource group GEANT-TEST	Provider GEANT
💪 GEANT_test_circuit	Circuit status Enabled	Provider status Not provisioned
	Location West Europe	Peering location Amsterdam
	Subscription name Azure ExpressRoute pilot	Bandwidth 50 Mbps
	Subscription ID 488a471a-8625-4815-aa55-bf1ebac0551e	Service key 39bd834f-e6fb-479b-ba57-feac5245ceae
		All settings 🔿
GÉANT & Microsoft ExpressRoute Request and Configuration manual		

Error! No text of specified style in document.





A.2 Configuring an ExpressRoute peering

In order to start using ExpressRoute, at least two BGP peerings need to be configured, one per geographical path. Microsoft offers three types of peering services:

- Azure private: Azure compute services, namely virtual machines (IaaS) and cloud services (PaaS), that are deployed within a virtual network can be connected through the private peering domain. The private peering domain is considered to be a trusted extension of your own core network into Microsoft Azure.
- Azure public: services such as Azure Storage, SQL databases and Websites are offered on public IP addresses. You can privately connect to services hosted on public IP addresses, including VIPs of your cloud services, through the public peering routing domain.
- Microsoft; connectivity to all other Microsoft online services (such as Office 365 services) will be through private peering.



A.2.1 Configuring an ExpressRoute peering in the Azure portal

In the Azure portal click on the peering for which you'd like to enter the settings. Note that the VLAN ID entered here is the inner tag used for this peering.

Settings Delete Essentials ^ Resource group Provider GEANT-TEST GEANT Circuit status Provider status Enabled Provisioned Location Peering location West Europe Amsterdam Subscription name Bandwidth Azure ExpressRoute pilot 50 Mbps Subscription ID Service key 488a471a-8625-4815-aa55-bf1ebac0551e 39bd834f-e6fb-479b-ba57-f	신 유 ()	Save Discard Delete * Peer ASN • 65000 * Primary subnet • 192.168.168.0/30 * Secondary subnet • 192.168.168.4/30 * VLAN ID • *	✓✓
Essentials A Provider GEANT-TEST GEANT Circuit status Provider status Enabled Provisioned Location Peering location West Europe Amsterdam Subscription name Bandwidth Azure ExpressRoute pilot 50 Mbps Subscription ID Service key 488a471a-8625-4815-aa55-bf1ebac0551e 39bd834f-e6fb-479b-ba57-f	(쇼) 8억 🔇	 * Peer ASN • 65000 * Primary subnet • 192.168.168.0/30 * Secondary subnet • 192.168.168.4/30 * VLAN ID • 	~ ~ ~
Resource group Provider GEANT-TEST GEANT Circuit status Provider status Enabled Provisioned Location Peering location West Europe Amsterdam Subscription name Bandwidth Azure ExpressRoute pilot 50 Mbps Subscription ID Service key 488a471a-8625-4815-aa55-bf1ebac0551e 39bd834f-e6fb-479b-ba57-f	fear5245reae	65000 * Primary subnet 192.168.168.0/30 * Secondary subnet 192.168.168.4/30 * VLAN ID	_ < _ < _ <
	icacoz roccae	500	~
	All settings •	Shared key	
Peerings TYPE ^ STATUS ^ PRIMARY SUBNET ^ SECONDARY SUB	Add tiles (-	+)	
Azure private Disabled			
Azure public Disabled			
Microsoft Disabled			

Click "save" when you're finished.



A.3 Configuring a Virtual Network with Gateway

A virtual network can be used as a network for your virtual machines. This network can be announced via the ExpressRoute peering to your local premises.

A.3.1 Configuring a Virtual Network via the Azure portal

In the portal click on "Browse >" and search for "Virtual Networks" and click on it. To add a virtual network click on "Add".

Create virtual net $ \square$ \times
* Name
GEANTTEST 🗸
* Address space 🛛
10.15.20.0/24 🗸
10.15.20.0 - 10.15.20.255 (256 addresses)
* Subnet name
GEANT 🗸
* Subnet address range 0
10.15.20.0/24 🗸
10.15.20.0 - 10.15.20.255 (256 addresses)
* Subscription
Azure ExpressRoute pilot 🗸
 ★ Resource group ● ○ Create new ● Use existing
GEANT-TEST V
* Location
West Europe 🗸 🗸

Enter the necessary details and click on "Create".



A.3.2 Configuring a Virtual Network Gateway via the Azure portal

In the portal click on "Browse >" and search for "Virtual network gateways" and click on it. To add a virtual network gateway click on "Add".

* Name	
GEANT_Gateway	~
* Virtual network 🛛	>
GEANT_TEST	
* Gateway subnet address range 0	
10.15.20 16/28	~
10.15.20.16 - 10.15.20.31 (16 add	dresses)
* Public IP address 0	<u>\</u>
(new) GEANT_Gateway	
Gateway type 0	
VPN ExpressRoute	
* Subscription	
Azure ExpressRoute pilot	~
Resource group 0	
GEANT-TEST	
* Location 🛛	
West Europe	~

Enter the necessary details and click on "Create". Provisioning a virtual network gateway may take up to 45 minutes.





A.3.3 Attach Virtual Network with gateway to ExpressRoute

Go back to your ExpressRoute and in the settings menu click on "Connections". Then click on "Add", fill the required details and click on "OK".

Settings — GEANT_test_circuit		Connections GEANT_test_struit	* _ ¤ ×	GEANT_test_circuit — — — X
		>> Search connections		* Name
SUPPORT + TROUBLESHOOTING		NAME ^ STATUS ^ CONNECTION TYPE ^	PEER ^	GEANT Connection type
💥 Diagnose and solve problems	>	No results		ExpressRoute 🗸
Activity logs	>			* Virtual network gateway 0
New support request	>			GEANT_Gateway
GENERAL				* ExpressRoute circuit GEANT_test_circuit
Properties	>			Subscription 0
🚔 Configuration	>			Azure ExpressRoute pilot 🗸 🗸
⊗ Connections	>			Resource group 0
Peerings	>			GEANT-TEST
SETTINGS				Create new
Billing tags	>			Location 🖲 🗸 Vest Europe



A.4 Local network configuration

A.4.1 Ethernet layer (L2)

Cisco Router A1	Juniper Router A1
<pre>#configure terminal (config)#vlan <customer a1="" tag="" vlan=""> (config-vlan)# name Azure</customer></pre>	set interfaces <interface a=""> vlan- tagging</interface>
(config-vlan)# state active (config-vlan)# no shutdown (config)#interface <interface a1=""></interface>	set interfaces <interface a=""> unit <unit-id a1=""> vlan-id <customer vlan<br="">tag A1></customer></unit-id></interface>
(config-if) #switchport trunk encapsulation dot1q	
<pre>(config-if)#switchport trunk allowed vlan <customer a1="" tag="" vlan=""></customer></pre>	
<pre>(config-if)#switchport mode trunk (config-if)#switchport nonegotiate (config-if)#no cdp enable (config-if)#no vtp</pre>	
(config-if)#spanning-tree portfast trunk	
(config-if)#spanning-tree bpdufilter enable	



Cisco Router A2

```
#configure terminal set inte
(config)#vlan <customer vlan tag A2> tagging
(config-vlan)# name Azure
(config-vlan)# state active set inte
(config-vlan)# no shutdown <unit-ic
(config)#interface <interface A2> tag A2>
```

(config-if) #switchport trunk
encapsulation dotlq

(config-if)#switchport trunk allowed vlan <customer vlan tag A2>

(config-if)#switchport mode trunk (config-if)#switchport nonegotiate (config-if)#no cdp enable (config-if)#no vtp (config-if)#spanning-tree portfast trunk

(config-if)#spanning-tree bpdufilter
enable

Juniper Router A2

set interfaces <interface A2> vlantagging

set interfaces <interface A2> unit
<unit-id A2> vlan-id <customer vlan
> tag A2>

A.4.2 IP layer (L3)

For each VLAN (inner tag) an IPv4 interface needs to be configured.

Cisco Router A1	Juniper Router A1
<pre>#configure terminal</pre>	set interfaces <interface a1=""> unit</interface>
(config)#interface vlan <customer vlan tag A1></customer 	<pre><unit-id al=""> lamily inet address <bgp address="" al="" customer="" peer=""></bgp></unit-id></pre>
(config-if)#ip address <bgp peer<br="">address customer A1> <subnetmask></subnetmask></bgp>	
(config-if)#no shutdown	
Cisco Router A2	Juniper Router A2
#configure terminal	set interfaces <interface a2=""> unit <unit-id a2=""> family inet address</unit-id></interface>
(config)#interface vlan <customer vlan tag A2></customer 	<bgp a2="" address="" customer="" peer=""></bgp>
(config-if)#ip address <bgp peer<br="">address customer A2> <subnetmask></subnetmask></bgp>	
(config-if)#no shutdown	

It should be possible to ping the Microsoft addresses on the other side.

Cisco	Juniper
#ping <microsoft address="" b1="" ip=""></microsoft>	ping <microsoft address="" b1="" ip=""></microsoft>
#ping <microsoft address="" b2="" ip=""></microsoft>	ping <microsoft address="" b2="" ip=""></microsoft>

A.5 BGP configuration

Microsoft uses the routing protocol BGP to advertise and receive network prefixes configured in the Azure cloud and institution environment respectively. Therefor an institution should setup BGP sessions with Microsoft. The necessary details required to setup an peering with Microsoft Azure via ExpressRoute are provided by Microsoft in the portal in the "ExpressRoute circuit" menu. These details are provided by the institution, see section A.2.1.



A.5.1 Configuring the BGP peering

Cisco Router A1	Juniper Router A1
#configure terminal (config)#router bgp <customer as=""></customer>	set protocols bgp group azure- private type external
(config-router)#network a.b.c.d !eigen IP-apace, classful	set protocols bgp group azure- private neighbor <bgp address<br="" peer="">TC B1> description "Azure A1"</bgp>
(config-router)#neighbor <bgp peer<br="">address TC A1> remote-as 15830</bgp>	set protocols bgp group azure- private neighbor <bgp address<br="" peer="">TC B1> peer-as 15830</bgp>
Cisco Router A2	Juniner Bouter A2
	Jumper Router Az
#configure terminal (config)#router bgp <customer as=""></customer>	set protocols bgp group azure- private type external
<pre>#configure terminal (config)#router bgp <customer as=""> (config-router)#network a.b.c.d !eigen IP-apace, classful (config-router)#netickhon (DCD D)</customer></pre>	<pre>set protocols bgp group azure- private type external set protocols bgp group azure- private neighbor <bgp address<br="" peer="">TC B2> description "Azure A2"</bgp></pre>

Check if the BGP sessions are UP.

Cisco	Juniper
#show bgp summary	show bgp summary

Check which routes are being distributed from Microsoft to you. You can configure these networks in the Azure portal or via the Azure APIs.

Cisco	Juniper
#show ip bgp neighbor <bgp peer<="" td=""><td>show route receive-protocol bgp <</td></bgp>	show route receive-protocol bgp <
address TC A1> routes	BGP Peer address TC B1>
#show ip bgp neighbor <bgp peer<="" td=""><td>show route receive-protocol bgp <</td></bgp>	show route receive-protocol bgp <
address TC A2> routes	BGP Peer address TC B2>



A.5.2 Configuring the local preference and metric

For example to prefer the connection on router A1 above the connection of router A2.

Cisco Router A1

```
#configure terminal
(config)#router bgp <Customer AS>
```

```
(config-router)#bgp default local-
preference 100*)
```

(config-router)#neighbor <BGP Peer
address TC A1> remote-as weight
500*)

Juniper Router A1

```
set policy-options policy-statement
azure-A1-in then local-preference
100
```

set protocols bgp group azureprivate neighbor <Microsoft IP Address B1> import azure-A1-in

Juniper Router A2

set policy-options policy-statement
azure-A2-in then local-preference
200

set protocols bgp group azureprivate neighbor <Microsoft IP Address B2> import azure-A2-in



Ask Microsoft to do the same.

	Juniper Router A1
	set policy-options policy-statement azure-A-out then metric 10
	set protocols bgp group azure- private neighbor <microsoft ip<br="">Address B1> export azure-A-out</microsoft>
Cisco Router A2	Juniper Router A2
<pre>#configure terminal (config)#route-map localonly permit 10</pre>	set policy-options policy-statement azure-B-out then metric 20
(config-route-map)#match as-path 10	set protocols bgp group azure- private neighbor <microsoft ip<br="">Address B2> export azure-B-out</microsoft>
(config-route-map)#set as-path prepend <customer as=""> <customer as=""></customer></customer>	
(config-route-map) #exit (config-ip) #exit	
<pre>(config)# router bgp <customer as=""> (config-router)#neighbor <microsoft address="" b2="" ip=""> route-map localonly out</microsoft></customer></pre>	



A.5.3 Prefix list

in

To filter incoming prefixes.

Cisco Router A1	Juniper Router A1
<pre>#configure terminal (config)#ip prefix-list azure-in seq 5 permit <a.b.0.0 z=""></a.b.0.0></pre>	set policy-options prefix-list azure-in <ip mask="" range=""></ip>
(config)#router bgp <customer as=""></customer>	set protocols bgp group azure- private neighbor <bgp address<br="" peer="">TC B1> import azure-in</bgp>
<pre>(config-router)#neighbor <microsoft address="" b1="" ip=""> prefix-list azure-in in</microsoft></pre>	
Cisco Router A2	Juniper Router A2
#configure_terminal	
<pre>(config)#ip prefix-list azure-in seq 5 permit <a.b.0.0 z=""></a.b.0.0></pre>	set policy-options prefix-list azure-in <ip mask="" range=""></ip>
<pre>(config)#ip prefix-list azure-in seq 5 permit <a.b.0.0 z=""> (config)#router bgp <customer as=""></customer></a.b.0.0></pre>	<pre>set policy-options prefix-list azure-in <ip mask="" range=""> set protocols bgp group azure- private neighbor <bgp address="" b2="" peer="" tc=""> import azure-in</bgp></ip></pre>



To filter outgoing prefixes.

Cisco Router A1	Juniper Router A1
<pre>#configure terminal (config)#ip as-path access-list 10 permit ^\$</pre>	set policy-options prefix-list azure-out <ip mask="" range=""></ip>
(config-ip)#route-map azure-out permit 10	set protocols bgp group azure- private neighbor <bgp address<br="" peer="">TC B1> export azure-out</bgp>
(config-route-map)#match as-path 10 (config-router)#neighbor <microsoft IP address B1> route-map azure-out out</microsoft 	
Cisco Router A2	Juniper Router A2
<pre>Cisco Router A2 #configure terminal (config)#ip as-path access-list 10 permit ^\$</pre>	<pre>Juniper Router A2 set policy-options prefix-list azure-out <ip mask="" range=""></ip></pre>
<pre>Cisco Router A2 #configure terminal (config)#ip as-path access-list 10 permit ^\$ (config-ip)#route-map azure-out permit 10</pre>	Juniper Router A2 set policy-options prefix-list azure-out <ip mask="" range=""> set protocols bgp group azure- private neighbor <bgp address<br="" peer="">TC B2> export azure-out</bgp></ip>