Where networks meet

DE-CIX MICROSOFT AZURE PEERING SERVICE TECHNICAL SERVICE DESCRIPTION

I. GENERAL PROVISIONS

1. Overview, scope of application

This document contains the Technical Service Description (TSD) for Microsoft Azure Peering Service (hereinafter referred to only as “Azure Peering Service”). This TSD is part of the DE-CIX contractual framework.

This TSD shall apply only to Azure Peering Services. Azure Peering Services may, however, be a prerequisite for other DE-CIX services. This document contains only technical specifications and documentation. Please consult the Microsoft Azure Peering Service Special Service Level Agreement (Special SLA) for service levels.

2. Amendment

This document may be revised and amended at any time pursuant to the provisions of the DE-CIX Agreement.

3. Definitions

Azure Peering Services are layer 2 services for the exchange of (layer 2) frames between Microsoft and customers to gain privileged access to Microsoft. Azure Peering Service is a networking service that enhances customer connectivity to Microsoft cloud services such as Microsoft 365, Dynamics 365, software as a service (SaaS) services, Azure, or any Microsoft services accessible. DE-CIX and Microsoft have partnered to provide reliable and high-performing public connectivity with optimal routing from the customer to the Microsoft network. Public connectivity is optimized for high reliability and minimal latency from cloud services to the end-user location. Route reflectors deployed by DE-CIX enable BGP peering.

Microsoft operates a global backbone1 with multiple edge PoP locations and Azure Cloud regions spread through different countries worldwide. We advise customers of Azure Peering Service to provision local Azure Peering Service instances per geographical location and

[1] https://azure.microsoft.com/en-us/global-infrastructure/global-network/

consider in advance, which prefixes would be announced on a certain instance of an Azure Peering Service. Ideally, enterprises with multiple office locations in (e.g. Central Germany, Southern Europe, and East US), should have one dedicated prefix per bigger branch, office location, or country.

4. Product prerequisites

Azure Peering Services require the following DE-CIX product for its normal operation:

- DE-CIX Access (see Master SLA and DE-CIX Technical Access Description (TAD)) at any data center location that allows a local or remote connection to the respective Azure Peering Services location.

5. Applicable standards

Members' use of the DE-CIX network shall at all times conform to the relevant standards as laid out in STD0001 and associated Internet STD documents.

II. DATA LINK-LAYER CONFIGURATION (ISO/OSI LAYER 2)

1. Bandwidth

Bandwidth of Azure Peering Services must be explicitly configured if the agreed bandwidth for Azure Peering Services differs from the bandwidth of the access or bundle of aggregated access, on which the Azure Peering Service is used.

2. Frame types

The following general policies shall apply:

Frame type (ethertypes)	Policy	Enforcement
0x0800 – IPv4 0x0806 – ARP	**Allow**	-
All other types	**Discard**	Strict – all frames other than allowed types are dropped

3. MAC address configuration

All frames forwarded to Azure Peering Services shall have the same source MAC address.

4. Broadcast/Multicast Traffic

The following policies shall apply to broadcast/multicast traffic

Protocol	Policy	Enforcement
Broadcast ARP (excluding proxy ARP)	**Allowed, but rate limited to 1,000kbps**	-
All other types, i.e. including, but not limited to: - IRDP - ICMP redirects - IEEE802 Spanning Tree - Vendor proprietary discovery protocols (e.g. CDP) - Interior routing protocol broad/multicasts (e.g. OSPF, IS-IS, IGRP, EIGRP) - BOOTP/DHCP - PIM-SM - PIM-DM - DVMRP	**Discard**	Discarded, unless specifically allowed

III. IP LAYER CONFIGURATION (ISO/OSI LAYER 3)

1. Interface configuration

Interfaces connected to DE-CIX ports shall only use IP addresses and netmasks (prefix lengths) assigned to them by DE-CIX. The assignment will be provided in writing (e.g. email) during the provisioning process. In particular:

Parameter	Policy	Remarks
IP addresses (IPv4), including subnet mask for your interfaces	**IPv4 required**	At least the IPv4 address has to be configured
IP address of route reflectors	**Required for credit claim**	Configure at least one BGP session to one route reflector to be able to claim credits for Azure Peering Services. Advertising routes are not a requirement.

2. Additional configuration parameters

Parameter	Policy	Remarks
Standard MTU	**Fixed size**	Standard IP MTU size must be explicitly set to 1,500 Bytes, unless explicitly agreed in writing.

3. Routing configuration

The customer system's routing configuration shall include the following policies/settings:

Parameter	Policy	Remarks
BGP Version	**v. 4 only**	-
AS numbers	**Public only**	No AS numbers allowed from ranges reserved for private use across the entire DE-CIX network.
Multiple ASN	**Allow**	Members may use more than one ASN for their DE-CIX service, provided that each ASN presented shares the same NOC and peering contact details.
Route advertising	**Maximum aggregation**	All routes advertised shall be aggregated as far as possible.
Route advertising – target IP	**Advertising router only**	All routes advertised across the Azure Peering Service must point to the router advertising it, unless an agreement has been made in advance in writing by DE-CIX and the members involved.
Route advertising – registration	**Public registration required**	All routes to be advertised across DE-CIX must be registered in the RIPE database or another public routing registry.
IP-address space advertising	**With permission only**	IP address space assigned to DE-CIX peering LAN shall not be advertised to other networks without explicit permission of DE-CIX.
DE-CIX advertised routes	**Accept**	You can safely accept any routes announced by us, as all incoming advertisements are filtered according to the configured policies.

4. Route Reflector

The DE-CIX route reflector system consists of two reflectors running BGP.

4.1 Configuration

In order for Azure Peering Services to function, a session to every route reflector must be set up with the following parameters:

Parameter	Policy	Remarks
connection mode	**Active**	DE-CIX Side is configured as passive
bgp enforce-first-as	**Not allowed**	Enabled by default, must be disabled manually
AS-Set	**Required**	DE-CIX needs the customer AS-Set to build the filter rules
martians/bogons	**Will be discarded**	

4.2 BGP announcement validation

BGP announcement provided by the customer to the DE-CIX route reflectors are validated for security reasons. Databases might be used for the route validation (e.g. RADB).

4.3 Optional: communities

In addition to the one route reflector minimum configuration, the Customer may elect to control outgoing routing information directly on the DE-CIX route reflector by joining communities. Communities are processed by the DE-CIX route reflector. A list of all supported communities on DE-CIX conventional route servers/reflectors is provided here:
https://www.de-cix.net/de/resources/route-server-guides/operational-bgp-communities
Of particular interest for Azure Peering Service are (referring to the website above):

- BGP Communities NO_EXPORT and NO_ADVERTISE (not on a per-peer basis)
- AS Path Prepending
- Graceful BGP Session Shutdown

IV. MICROSOFT AZURE PORTAL CONFIGURATION (OPTIONAL)

1. AS registration, Prefix-Key generation

After the BGP sessions are established with DE-CIX Route Reflectors, DE-CIX will register the Customers ASN and generate a Prefix-Key within the Azure portal. DE-CIX will provide the Prefix-Key to the Customer. Based on this, the Customer is able to create a "Peering Service" within his Azure subscription to access telemetry services.

2. Azure portal

Customers will be able to create this "Peering Service" in the Azure subscription, only after BGP sessions with DE-CIX Route Reflectors are established and after DE-CIX forwards prefixes towards Microsoft.

Details can be found here:
https://docs.microsoft.com/en-us/azure/peering-service/azure-portal

DE-CIX assumes no responsibility for the representations within the Microsoft Azure portal.