DE-CIX CLOSED USER GROUPS TECHNICAL SERVICE DESCRIPTION

I. GENERAL PROVISIONS

1. Overview, scope of application

This document contains the Technical Service Description (TSD) for Closed User Groups (CUG) Services. This TSD is part of the DE-CIX contractual framework.

This TSD shall apply only to CUG Services. Closed User Groups Services may, however, be a prerequisite for other DE-CIX services. This document contains only technical specifications and documentation. Please consult the CUG 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

3.1. CUG Service Definition: CUG are layer 2 point to multipoint services for the exchange of (layer 2) frames between customers, a CUG Owner and Members, of the specific service to enable connectivity and gain privileged access to the specific services offered by the Owner. CUG offer a dedicated and secure environment to exchange IP traffic for special use cases and services amongst each other. This controlled environment and the well-defined set of participants within the CUG, technically based on an E-TREE setup, enables bandwidth guarantees, secure routing, and follows highest standards in terms of redundancy.

3.2. CUG Owner: ISP, Cloud Services Provider or Enterprise using logically separated services based and built on the DE-CIX Apollon platform.

3.3. CUG Member: User of CUG Services

4. Product prerequisites

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

- <u>DE-CIX Access</u> (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 CUG 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](STD0001) and associated Internet STD documents.

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

1. Bandwidth

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

2. Frame types

The following general policies shall apply:

Frame type (ethertypes)	Policy	Enforcement
0x0800 – IPv4 0x0806 – ARP 0x86dd – IPv6	**Allow**	-
All other types	**Discard**	Strict – all frames other than allowed types are dropped

3.   MAC address configuration

All frames forwarded to CUG 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), multicast IPv6 Neighbor Discovery (ND)	**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, IPv6), 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 CUG Services. Advertising routes are not a requirement.

2. Additional configuration parameters

Parameter	Policy	Remarks
IPv6 addresses (link-local & global scope)	**No auto-configuration**	All IPv6 addresses must be explicitly configured
IPv6 address (site-local)	**Not allowed**	IPv6 site-local addresses must not be used
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 peering, 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 CUG 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 in a peering session 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 CUG 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 CUG 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