DE-CIX GLOBEPEER TECHNICAL SERVICE DESCRIPTION	ОПИС ТЕХНІЧНИХ ПОСЛУГ DE-CIX GLOBEPEER
I. GENERAL PROVISIONS	**I. ЗАГАЛЬНІ ПОЛОЖЕННЯ**
1. Overview, scope of application	**1. Огляд, сфера застосування**
This document contains the Technical Service Description (TSD) for the GlobePEER product. This TSD is part of the DE-CIX contractual framework.	Даний документ містить опис технічних послуг (TSD) продукту DE-CIX GlobePEER. Даний опис технічних послуг є частиною договірної бази DE-CIX.
This TSD shall apply only to the GlobePEER product. The GlobePEER product may, however, be a prerequisite for other DE-CIX services. This document contains only technical specifications and documentation. Please consult the GlobePEER Special Service Level Agreement (Special SLA) for service levels.	Даний опис технічних послуг використовується виключно для продукту DE-CIX GlobePEER. Проте, продукт DE-CIX GlobePEER може бути попередньою умовою для інших послуг DE-CIX. Цей документ містить лише технічні характеристики й документацію. Інформація про рівні послуг викладена в Спеціальній угоді про рівні послуг для GlobePEER.
2. Amendment	**2. Доповнення**
This document may be revised and amended at any time pursuant to the provisions of the DE-CIX Agreement.	Даний документ може бути переглянутий і доповнений в будь-який час відповідно до положень Угоди DE-CIX.
3. Product prerequisites	**3. Діючі попередні умови для продукту**
The GlobePEER Product requires the following DE-CIX products for its normal operation:	Для нормального функціонування продукту GlobePEER необхідні наступні продукти DE-CIX:

• DE-CIX Access (see Master SLA and DE-CIX Technical Access Description (TAD)) at any data center location that allows a local or remote[1] connection to the respective GlobePEER region.	• DE-CIX Access (див. Основну угоду про рівень послуг і Опис технічного доступу DE-CIX (TAD)) в будь-якому місцезнаходженні центру обробки даних, який забезпечує локальний і віддалений[1] зв'язок з відповідного регіону GlobePEER.
4. Applicable standards	**4. Діючі стандарти**
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.	При використанні мережі DE-CIX учасники завжди повинні дотримуватися відповідних стандартів, викладених у STD0001, і відповідної документації по стандартах.
II. DATA LINK-LAYER CONFIGURATION (ISO/OSI LAYER 2)	**II. КОНФІГУРАЦІЯ РІВНЯ ПЕРЕДАЧІ ДАНИХ (ISO/OSI РІВЕНЬ 2)**
1. Bandwidth	**1. Смуга пропускання**
Bandwidth of the GlobePEER product must be explicitly configured if the agreed bandwidth for GlobePEER differs from the bandwidth of the access or bundle of aggregated access, on which the GlobePEER product is used.	Смуга пропускання продукту GlobePEER повинна мати встановлену конфігурацію, якщо узгоджена смуга пропускання для GlobePEER відрізняється від смуги пропускання доступу або пучка агрегованого доступу, на яких

[1] Some Exchange locations of DE-CIX are interconnected. At those locations customers can book the access to the GlobePEER region at the remote locationas an additional service, e.g., customers of DE-CIX New York region can order the access to the DE-CIX GlobePEERFrankfurt region. / Деякі замінювані місцезнаходження DE-CIX взаємопов'язані. У таких місцях розташування користувачі можуть резервувати доступ до регіону GlobePEER з віддаленого місцезнаходження як додаткову послугу, наприклад, користувачі регіону DE-CIX Нью-Йорк можуть замовити доступ до регіону DE-CIX GlobePEER Франкфурт.

	використовується продукт GlobePEER.
2. Frame types	**2. Типи рамок**
The following general policies shall apply:	Застосовуються наступні політики:

Frame type (ethertypes) / Тип рамки (ethertypes)	**Policy / Політика**	**Enforcement / Виконання**
0x0800 – IPv4 0x0806 – ARP 0x86dd – IPv6	**Allow / Дозволити**	-
All other types / Всі інші типи	**Discard / Не враховувати**	Strict – all frames other than allowed types are dropped / Строго — відкидаються всі кадри, за винятком дозволених

3. MAC address configuration	**3. Конфігурація MAC-адреси**
All frames forwarded to the GlobePEER service shall have the same source MAC address.	Всі рамки, направлені на послугу GlobePEER, повинні мати ту ж вихідну MAC-адресу.
4. Broadcast/Multicast Traffic	**4. Широкомовний/Багатоадресний трафік**
The following policies shall apply to broadcast/multicast traffic	Наступні політики використовуються для широкомовного/багатоадресного трафіку

Protocol / Протокол	**Policy / Політика**	**Enforcement / Виконання**
Broadcast ARP (excluding proxy ARP), multicast IPv6 Neighbor Discovery (ND) / Широкомовний ARP-протокол (за винятком проксі- ARP), багатоадресний протокол IPv6 Neighbor Discovery (ND)	**Allowed, but rate limited to 1,000kbps / Дозволено, але з обмеженням швидкості до 1 000 кБ/с**	-

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 / Всі інші типи, тобто в тому числі, але не обмежуючись ними: - IRDP - ICMP, перепризначення - IEEE802, зв'язуюче дерево - Ліцензійні (пропрієтарні) протоколи виявлення Постачальника (наприклад, CDP) - Внутрішні протоколи маршрутизації, широкомовні/багатоадресні (наприклад, OSPF, IS-IS, IGRP, EIGRP) - BOOTP/DHCP - PIM-SM - PIM-DM - DVMRP- PIM-DM - DVMRP	**Discard / Не враховувати**	Discarded, unless specifically allowed / Не враховується, якщо окремо не дозволені

III. IP LAYER CONFIGURATION (ISO/OSI LAYER 3)	III. КОНФІГУРАЦІЯ IP-РІВНЯ (ISO/OSI РІВЕНЬ 3)
1. Interface configuration	**1. Конфігурація інтерфейсу**
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:	Інтерфейси, приєднані до портів DE-CIX, використовують виключно IP-адреси й маски мережі (довжина префіксів), призначені їм DE-CIX. Призначення надається в письмовій формі (наприклад, по електронній пошті) в процесі ініціалізації. Зокрема:

Parameter / Параметр	**Policy / Політика**	**Remarks / Примітки**
IP addresses (IPv4, IPv6), including subnet mask for your interfaces / IP-адреси (IPv4, IPv6), включаючи маску підмережі для Ваших інтерфейсів.	**IPv4 required / Необхідна IPv4**	At least the IPv4 address has to be configured / Як мінімум, необхідно налаштувати адресу IPv4
IP address of route servers / IP-адреса серверів маршрутизації	**Required for credit claim / Необхідна для претензії по кредиту**	Configure at least one BGP session to one route server to be able to claim credits for the GlobePEER service. Advertising routes are not a requirement. / Налаштувати як мінімум один сеанс BGP для одного сервера маршрутизації для забезпечення претензій по кредитах для послуги GlobePEER. Анонсуючі маршрути не обов'язкові.

2. Additional configuration parameters	**2. Додаткові параметри конфігурації**

Parameter / Параметр	**Policy / Політика**	**Remarks / Примітки**
IPv6 addresses (link-local & global scope) / Адреси IPv6 (внутрішньоканальна й глобальна область)	**No auto-configuration / Відсутність автоматичної конфігурації**	All IPv6 addresses must be explicitly configured / Всі адреси IPv6 повинні бути чітко налаштовані
IPv6 address (site-local) / Адреса IPv6 (локальна адреса для мережевого вузла)	**Not allowed / Не дозволено**	IPv6 site-local addresses must not be used / Локальні адреси IPv6 для мережевого вузла не повинні використовуватися
Standard MTU / Стандартний MTU	**Fixed size / Визначений розмір**	Standard IP MTU size must be explicitly set to 1,500 Bytes, unless explicitly agreed in writing. / Розмір IP-адреси стандартного MTU повинен бути чітко визначений на 1 500 байт, якщо інше не погоджено письмово.

3. Routing configuration	**3. Конфігурація маршрутизації**
The customer system's routing configuration shall include the following policies/settings:	Конфігурація маршрутизації системи користувача включає наступні політики/ налаштування:

Parameter / Параметр	**Policy / Політика**	**Remarks / Примітки**
BGP Version / Версія BGP	**v. 4 only / тільки v.4**	-
AS numbers номери AS	**Public only / Тільки публічно**	No AS numbers allowed from ranges reserved for private use across the entire DE-CIX network. / Немає дозволених номерів AS в діапазонах, збережених для приватного використання в усій мережі DE-CIX.
Multiple ASN / Кілька ASN	**Allow / Дозволити**	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. / Учасники можуть використовувати більше одного ASN для взаємодії в мережі DE-CI за умови, що кожен представлений ASN використовує той же NOC і обмінюється контактними даними.
Route advertising / Анонсирование маршрута	**Maximum aggregation / Максимальное агрегирование**	All routes advertised shall be aggregated as far as possible. / Усі анонсовані маршрути агрегуються до максимального рівня.

Route advertising – target IP / Анонсування маршруту — цільова IP-адреса	**Advertising router only / Тільки маршрутизатор анонсування**	All routes advertised across the DE-CIX network must point to the router advertising it, unless an agreement has been made in advance in writing by DE-CIX and the members involved. / Усі анонсовані маршрути по мережі DE-CIX повинні вказувати на маршрутизатор, що анонсує їх, за винятком випадків, коли компанією DE-CIX у письмовій формі й завчасно було укладено угоду із залученням учасників.
Route advertising – registration / Анонсування маршруту — реєстрація	**Public registration required / Необхідна публічна реєстрація**	All routes to be advertised in a peering session across DE-CIX must be registered in the RIPE database or another public routing registry. / Усі маршрути, які підлягають анонсуванню в сеансі взаємодії по DE-CIX, повинні реєструватися в базі даних RIPE або в іншому відкритому реєстрі маршрутизації.
IP-address space advertising / Анонсування простору IP-адреси	**With permission only / Тільки за згодою**	IP address space assigned to DE-CIX peering LAN shall not be advertised to other networks without explicit permission of DE-CIX. / Простір IP-адреси, призначений DE-CIX для взаємодії з мережею LAN, не анонсується для інших мереж без відповідного дозволу DE-CIX.
DE-CIX advertised routes / Анонсовані маршрути DE-CIX	**Accept / Прийняти**	You can safely accept any routes announced by us, as all incoming advertisements are filtered according to the configured policies. / Ви можете без вагань приймати всі маршрути, анонсовані нами, так як всі вхідні оголошення фільтруються відповідно до налаштованої політики.

4. Traffic forwarding	**4. Переадресація трафіку**
Traffic shall only be forwarded to a DE-CIX member, if permission has been given by the receiving member either:	Трафік переадресовується тільки учаснику DE-CIX, якщо учасник, який приймає, отримав дозвіл або:
• by advertising a route across the DE-CIX network (directly or via the route server)	• шляхом анонсування маршруту по мережі DE-CIX (прямо або через сервер маршрутизації),
• or explicitly in writing	• або в письмовій формі
5. Route server feature	**5. Функція сервера маршрутизації**
The DE-CIX route server system consists of two servers running BGP. For normal operation, only one is needed.	Система сервера маршрутизації DE-CIX складається з двох серверів, що функціонують по протоколу BGP. Для нормальної роботи необхідний тільки один.
5.1 Minimum configuration	**5.1 Мінімальна конфігурація**
In order for the DE-CIX measurements of the route server feature to function, and thus for a customer to be eligible for any credits, at least one connection to one route server must be set up with the following parameters:	Щоб забезпечити функціонування вимірювань сервера маршрутизації DE-CIX і, таким чином, забезпечити право користувача на кредит, як мінімум має бути налагоджене одне підключення до одного сервера маршрутизації з наступними параметрами:

Parameter / Параметр	**Policy / Політика**	**Remarks / Примітки**
connection mode / режим підключення	**Active / Активний**	DE-CIX Side is configured as passive / Сторона DE-CIX налаштована як пасивна
bgp enforce-first-as	**Not allowed / Не дозволено**	Enabled by default, must be disabled manually / Активується по замовчуванню, деактивується вручну
AS-Set	**Required / Вимагається**	DE-CIX needs the customer AS-Set to build the filter rules / DE-CIX вимагає, щоб користувач AS-Set створив свої правила фільтрації
martians/bogons	**Will be discarded / Буде відхилено**	

5.2 BGP announcement validation	**5.2 Валідація оголошення BGP**
BGP announcement provided by the customer to the DE-CIX route server are validated for security reasons. Databases might be used for the route validation (e.g. RADB).	Валідація оголошення BGP, наданого користувачем для сервера маршрутизації DE-CIX, здійснюється з метою безпеки. Для валідації маршрутизації можуть використовуватися бази даних (наприклад, RADB).
5.3 Optional: communities	**5.3 Додатково:групи**
In addition to the one route server minimum configuration, the Customer may elect to control outgoing routing information directly on the DE-CIX route server by joining communities. Communities are processed by the DE-CIX route servers by the following set	Крім мінімальної конфігурації одного сервера маршрутизації, Користувач може вибрати управління вихідною інформацією про маршрутизацію безпосередньо на сервері маршрутизації DE-CIX шляхом об'єднання груп. Групи обробляються

of filter rules:	серверами маршрутизації DE-CIX за наступним набором правил фільтрації:

# / №	**Action дія**	**Community / група**	**Local Preference / Локальна перевага**
1	block announcement of a route to a certain peer / блочне повідомлення про маршрут до певного вузла	0:<peer-as>	50
2	announcement of a route to a certain peer / повідомлення про маршрут до певного вузла	<route-server-as>:<peer-as>	
3	block announcement of a route to all peers (monitoring only session) / блочне повідомлення про маршрут до всіх вузлів (тільки контроль сеансу)	0:<route-server-as>, no advertise, no-export	0
4	announcement of a route to all peers / повідомлення про маршрут до всіх вузлів	<route-server-as>:<route-server-as> (default if nothing set) / <route-server-as>:<route-server-as> (за замовчуванням, якщо не встановлено інше)	100

The number and list of available communities may vary between GlobePEER regions and locations. Customers are kindly asked to consult the location-specific documentation	Число й перелік доступних груп може змінюватися в залежності від регіонів і розташування GlobePEER. Просимо користувачів звертатися до документації,

of existing communities, made available upon request.	призначеної для конкретного місцезнаходження існуючих груп, яка надається за запитом.
6. Blackholing	**6. Блекхолінг**
Blackholing means diverting the flow of data to a different next hop (the “Blackhole”) where the traffic is discarded. The result is that no traffic reaches the original destination and hence hosts located within the "blackholed" prefix are protected from massive distributed denial of service (DDoS) attacks congesting the connection from the customer to DE-CIX. Thus blackholing is an effective way of mitigating the effects of DDoS attacks etc.	Блекхолінг — це переадресація потоку даних на іншу, наступну транзитну ділянку («Чорну діру»), де відбувається скидання трафіку. В результаті трафік не досягає вихідної точки призначення, і тому хости, які мають префікс блекхолінгу, захищені від розподіленої атаки типу «відмова в обслуговуванні» (DDoS), перевантажуючи лінію зв'язку від користувача до DE-CIX. Таким чином, блекхолінг — ефективний спосіб пом'якшення наслідків атак DDoS і т.д.
DE-CIX provides the technical infrastructure to allow Blackholing to be set up and used by customers. However, whether a certain customer accepts “Blackholed” prefixes or not is out of the control of DE-CIX.	DE-CIX забезпечує технічну інфраструктуру, яка дозволяє налаштувати блекхолінг з метою його використання користувачами. Однак, прийняття або неприйняття префіксів блекхолінгу певним користувачем не входить в зону контролю DE-CIX.
6.1 Basic principle	**6.1 Базовий принцип**
6.1.1 In standard conditions	**6.1.1 У стандартних умовах**
Customers advertise their prefixes with a Next Hop IP address belonging to their AS:	Користувачі анонсують свої префікси з IP-адресою наступної транзитної ділянки, що належить їх номеру AS:

• IPv4: /8 <= and <= /24 • IPv6: /19 <= and <= /48	• IPv4:/8 <= и <= /24 • IPv6:/19 <= и <= /48
6.1.2 In case of DDoS	**6.1.2 У випадку з DDoS**
Customers advertise their prefixes with a unique DE-CIX-provided Blackhole next hop IP address (BN):	Користувачі анонсують свої префікси з унікальною, наданою DE-CIX IP-адресою наступної транзитної ділянки для блекхолінгу (BN):
• IPv4: /8 <= up to = /32 (if and only if the BN is set)	• IPv4:/8 <= до = /32 (якщо і виключно при установці BN)
• IPv6: /19 <= up to = /128 (if and only if the BN is set)	• IPv6:/19 <= до = /128 (якщо і виключно при установці BN)
The standard announcement checks still apply.	При цьому здійснюється стандартна перевірка повідомлення.
6.2 L2 filtering	**6.2 Фільтрація L2**
• Blackhole next hop (BN) has a unique MAC address (determined by ARP for the BN IP address) e.g. de:ad:be:ef:66:95	• Наступна транзитна ділянка для блекхолінгу/Blackhole next hop (BN) має унікальну MAC-адресу (визначається ARP-протоколом для BN IP-адреси), наприклад:de:ad:be:ef:66:95
• ARP resolving for the Blackhole IP next hop is currently served by the host buoy.	• ARP-протокол, який використовується для Blackhole IP next hop, на даний момент обслуговується буєм хоста.
• All edge nodes have a static entry for the unique MAC address	• Усі граничні вузли мають статичний вхід для унікальної MAC-адреси

• Attack traffic is forwarded from the customer to the service with the static MAC address, traffic is denied ingress. This results in attack traffic not leaving the node through which it enters the GlobePEER service and it is discarded locally.	• Трафік атаки переадресовується від користувача до сервісу із статичною MAC-адресою, трафік відхиляється. Це призводить до того, що трафік атаки не проходить вузол, через який він входить у сервіс GlobePEER і відхиляється локально.
6.3 Result	**6.3 Результат**
As a result, all traffic to the attacked and "blackholed" IP prefix is already discarded on the incoming switch, and hence the victim's resources (e.g. connection from customer to DE-CIX) are protected.	В результаті всі трафіки з IP-префіксами атаки і блекхолінгу відхиляються вже на вході і, таким чином, захищаються ресурси потерпілого (наприклад, з'єднання від користувача до DE-CIX).