Service Description

Universal Access

September 2024 | Document Version 1.3

Contents

1. Universal Access – Description 7

1.1. Cloud Interconnect 7

1.1.1 Main characteristics 7
1.1.2 Network topologies supported 7
1.1.3 NTT Data Points of Presence 8
1.1.4 Technical Environment and Termination Capabilities 8
1.1.5 Prerequisites 8
1.1.6 Bandwidth requirements 9
1.1.7 Connectivity types 9
1.1.8 Facility Services 9
1.1.9 Noteworthy limitations 12

1.2 Remote SBC Management 13

1.2.1 Available topologies for UCaaS connectivity 13
1.2.2 Specific UCaaS features compatibility 14
1.2.3 List of compatible devices 14
1.2.4 SBC remote maintenance and firmware updates 14
1.2.5 SBC vendor(s) escalations 14
1.2.6 24/7 monitoring and alerts 15
1.2.7 Remote SBC Management pre-requisites and specifications 15

1.3 Cloud Endpoints Registration 17

1.3.1 Description 18
1.3.2 Requirements 18
1.3.3 Limitations 18

2. Service Operations 19

2.1. Service Management 19

2.2. Global Integrated Operations Centre (GIOC) service-desk 19

2.3. High Availability 19

2.3.1 In-DC N+1 redundant design 19
2.3.2 Geo-Redundancy 19

2.4. Service Monitoring 19

2.5. Incident Management 20

2.5.1 Incident priority definition 20
2.5.2 Incident priority matrix 20

2.6. Monthly Service Availability Service Level Agreement (SLA) 20

2.6.1 Description 20
2.6.2 Scope 21

The Monthly Service Availability is calculated on a per subscription basis (per Universal Access option element, i.e. per registered endpoint) 21

For example, should Client have 10 Service Numbers and the service becomes unavailable for 1 Service Number during 100 minutes, Then 100 minutes would be counted as Valid

Downtime and withdrawn from the Total Monthly Minutes of 43 920 x 10 = 439 200 minutes. 21
2.7. Patch Management.....21
2.8. Data Management.....21
2.9. Data security policies.....21
2.9.1 Datacenter security policies.....21
2.9.2 Remote access to Cloud Voice network management layer.....21
2.9.3 Vulnerability scanning and penetration testing.....21
2.9.4 Traffic encryption.....21
2.9.5 At-rest data encryption.....22
2.9.6 Backup policies.....22
2.9.7 Limitations and Exclusions.....22
2.10. Personnel Security.....22
3. Security and fraud management.....23
3.1. Main fraud schemes managed.....23
3.1.1 Toll-Free fraud/Toll-Free traffic-pumping.....23
3.1.2 Call transfer fraud.....23
3.1.3 Telecom denial-of-service (TDOS).....23
3.1.4 Wangiri fraud.....23
3.1.5 Revenue sharing fraud.....23
3.2. Security and Fraud management mechanisms.....23
3.2.1 SIP Proxy: Real-time traffic patterns monitoring.....23
3.2.2 Central Black and White-lists management system.....24
3.2.3 SIP Analytics.....24
3.2.4 IP White-listing.....24
3.2.5 STIR/SHAKEN.....24
3.3. Client Obligations.....24
4. Reporting and QoS.....25
4.1. Mean Opinion Score (MOS).....25
4.2. NTT MOS Degradation.....25
4.3. Post Dialling Delay (PDD).....25
5. Billing.....26
5.1. Standard Charges types.....26
5.2. Billing Cycles.....26
5.3. One-Time Charges.....26
5.4. Monthly Recurring Charges.....26
5.4.1 Cloud Interconnect charges.....26
5.4.2 Remote SBC Management charges.....27
5.4.3 Cloud Endpoints Registration – Per Endpoint.....27
5.5. Minimum Monthly Commitment.....27

(Insert appropriate disclaimer if required)

5.6. Other charges 27

5.7. Billing and Invoicing capabilities 27

(Insert appropriate disclaimer if required)

List of abbreviations

Abbreviation	Meaning
Business-Hours	NTT Data Business-Hours are from Monday to Friday between 7AM and 7PM (GMT for EMEA, CDT for Americas and SGT for APAC)
CLI	Calling Line Identifier: The phone number used by a calling party using the PSTN
Contract	Means the agreement concluded between NTT Data and Client pursuant to which NTT Data provides Client with the Services described in this Service Description
Client	Means the Party contracting with NTT Data for purchasing the Service(s) described in this Service Description
Datacenter	A Datacenter is a facility used to house computer systems and associated components, such as telecommunications and storage systems
DDI	Stands for “Direct Dial In” and means the PSTN E.164 numbers as supplied by NTT Data as part of its Calling Plans Service
Emergency Maintenance Window	Exceptional maintenance operation required to react to a critical issue that need to be remedy promptly. Occurs during non-Business-Hours.
PSTN	Public Switched Telephone Network
Scheduled Maintenance Window	Maintenance operations scheduled in advance by NTT Data to implement a specific change on the NTT Data infrastructure. Occurs during non-Business-Hours.
Service-Desk	Service-Desk means a single point of contact (SPOC) for communication between NTT Data and its clients and business partners.
Self-Care	Self-Care means the provisioning portal which permits Client to administrate its solution and its options
SIP	Means “Session Initiation Protocol” and is a signaling protocol used for initiating, maintaining, and terminating real-time sessions
SKU	Stands for Stock Keeping Unit and is a distinct type of item for sale
SOF	Stands for Service Order Form
Tenant	A Tenant is a group of Users who share a common access with specific privileges.
UCaaS	Means Unified Communications as a Service, a cloud-based UC solution permitting end-users to use features such as Instant Messaging, Meetings and Calling
User	Means a Client’s employee, partner or another person having an account declared on a UCaaS platform or any communication platform connected to Cloud Voice services. This is sometimes referred to as “end-User”.
WAN	Wide Area Network is a telecommunications network that extends over a large geographic area for the primary purpose of computer networking.

Document history

Issue	Date	Comments
1.0	April 1st, 2020	- Initial document
1.1	July 31st, 2020	- Added Remote SBC Management solution
1.2	January 31st, 2021	- Added Cloud Endpoints Registration solution
1.2.1	July 15th, 2023	- Updated Cisco WBX CC platform integration locations
1.3	September 15th, 2024	- New NTT Data formatting - Update of SLA section - Update of Billing section

(Insert appropriate disclaimer if required)

1. Universal Access – Description

Universal Access is a set of standard options to access NTT's Cloud Voice services in a more Client-specific context.

Universal Access options complement the other Cloud Voice services and can notably be used along with the Universal Calling Plans and/or Cloud voice for CX services.

1.1. Cloud Interconnect

Cloud Interconnect gives Client the ability to consume Cloud Voice services through a dedicated interconnection between NTT Data' Data-Center(s) and Client's private network (WAN).

Such interconnection relies on one or more IP private circuit(s) and is a stable and secure way for Client to access Cloud Voice services.

Cloud Interconnect is available in several worldwide locations and NTT Data provides a global coverage with IP Carrier Neutral Points of Presence (POP).

1.1.1 Main characteristics

- L2 and L3 VPN compatibility: Interconnect using L2 or L3 VPN extension with or without hosting client router at NTT Data colocation facilities.
- Bandwidth reservation: Bandwidth is reserved and dedicated for the sole purpose of Cloud Voice services. Cloud Interconnect reduces the numbers of hops compared to public internet, providing better latency and reducing the point of failures
- DSCP tagging: Cloud Interconnect is compatible with the Differentiated Service Code Point (DSCP) technology for Quality of Service (QoS) management via traffic prioritization. By default, NTT CC does not apply DSCP tagging to packets but will do so upon Client request. Differentiated DSCP tags based on packet types can also be implemented if required (i.e. EF tag to voice-media RTP packets and CS5 to SIP signaling packets).
- Scalability: Cloud Interconnect allows you to scale your bandwidth up to 1Gbps
- Security: Client traffic doesn't transit through Public Internet. It stays securely between NTT Data and Client.

1.1.2 Network topologies supported

Client is expected to extend its private network directly into NTT Data' Data-Centers. The following topologies are made available:

Single Cloud Interconnect access in one DC

This direct access topology will provide a main connection using Cloud Interconnect.

An alternate back-up path can be setup along with it, most likely a public network: PSTN or INTERNET) if the main connection is unavailable.

Should the Internet back-up be chosen, then dedicated link is preferred when is available, NTT Data relies on BGP as a routing protocol to advertise a list of host routes matching key Voices services components.

Those host routes must be made visible all the way to Client's infrastructures by the ISP providing extended IP VPN connectivity to NTT Data' Voice Services Data Centers.

Usually the ISP would not be in charge of any onsite Internet access solution, this is why the end Client should know about those BGP host routes. Otherwise, they will not be informed on any failure of the dedicated link solution.

Although this falls into Client's area of responsibility, and NTT Data cannot be held responsible for this, it is our duty to provide all party with the same level of information.

As such, we would recommend a setup where the ISP has BGP peering session in place with a Client managed device aware of both NTT Data private routes and public routes pointing to a local Internet access to be used as a backup access solution.
Client switch/firewall/router will know about the failure and make a decision to use the local Client direct Internet access, based on any routing method in place (STATIC/BGP).

Dual Accesses in one DC with High Availability Active/Passive

The Dual Accesses service option will provide a built-in protection for application traffic, ensuring both availability and quality of service for users at all times.
The Dual Accesses options will point at two physically separate edge routers on NTT Data side.

1.1.3 NTT Data Points of Presence

NTT Data is able to enable Cloud Interconnect from the below list of IP PoPs:

Label	Company	Address	Country
US Equinix (USATL)	Equinix	USA East: NTT Data at Equinix AT3 56 Marietta Street NW - Atlanta, GA 30303 - USA	US
US TelX (USCHI)	TelX	USA Central: NTT Data at TelX 350 E. Cermak Road Chicago, IL 60616 – USA	US
FR Equinix (FRPA2)	Equinix	NTT Data in NTTC Space at Equinix PA2 114 rue Ambroise Croizat – 93200 Saint-Denis - France	FR
UK Equinix (UKLD4)	Equinix	NTT Data at Equinix LD4 2, Buckingham Avenue, Slough Trading Estate – Slough, SL1 4NB - UK	UK
DE NTT (DETAU)	NTT	NTT Data at Equinix/NTT Borsencenter Unit – Taubenstrasse 7-9 ,D-60313 Frankfurt, Germany	DE
SG NTT (SGNTT)	NTT	NTT Data at NTT Com 51 Serangoon North Ave 4 Singapore 555858	SG
AU NTT (AUPYR)	NTT	NTT Data at NTT Com 400 Harris Street, Ultimo NSW 2007 – Australia	AU

1.1.4 Technical Environment and Termination Capabilities

NTT Data technical environment incorporates a fully resilient design that can process thousands of concurrent sessions.
Cloud Interconnect allows Client to connect a CPE to our edge switches with one of the following types of 1Gbps connections:

- 1000-BaseT [RJ-45 Copper]
- 1000-BaseSX [SMF/MMF] LC/SC
- 1000-BaseLX/LH [SMF/MMF] LC/SC
- 1000-BaseZX [SMF] LC/SC
- DWDM [LH/DWDM]

1.1.5 Prerequisites

To benefit from the Cloud Interconnect solution, the following prerequisites must be met:

- Client is responsible for ordering the Dedicated Access Link(s) from a Network Service Provider(s) of their choice. Sizing and other relevant QoS related options of the Access Link(s) are under Client's responsibility.
- Client is expected to run at least one BGP process instance to be able to peer with NTT Data network routers.

- Client must comply with the prerequisites as provided by NTT Data in its Statement of Work
- Client will have to cover the cost of all cabling to the demarcation point with NTT Data

1.1.6 Bandwidth requirements

- If bandwidth requirements exceed 50Mbps, a capacity check will be carried out by the NTT Data teams in charge of implementing the service. An implementation date will be communicated to Client-facing team in return (delays may result).
- The expected bandwidth is specified by Client in the Cloud Interconnect Service Order Form.

The available bandwidth will be limited on the interconnection facility between Client's network and Cloud Voice platforms.

1.1.7 Connectivity types

Cloud Interconnect allows two types of connectivity to the Cloud Voice platforms: With or without a Hosted CPE in NTT Data premises.

Specifics for connection with Hosted CPE

- NTT Data uses [password protected] BGP as a routing protocol between Client's CPE and its managed infrastructure
- Client must provide NTT Data with the BGP private AS number used on their CPE(s)
- The bandwidth contracted by Client to their Network Service Provider should be shared with NTT Data
- Client/carrier must communicate to NTT Data the total number of Rack-Units (RU) necessary to host the CPE(s)
- Standard Hosted CPE prices apply for up to 2 Rack-Units CPEs. Additional RU will need to be quoted.
- Client/carrier should provide CPE Power plugs adapted to the standards of the local Datacenter as specified by NTT Data
- NTT Data uses BGP AS number 53550
- Static routing is not supported
- Equipment requiring Direct Current power is not supported
- Standard 19-inch rack mounted equipment is recommended, any equipment without mounting brackets will be charged for an additional RU

Specifics for connection without a CPE hosted in NTT Data premises

- NTT Data uses [password protected] BGP as a routing protocol between Client CPE and its managed infrastructure
- Client must provide NTT Data with the BGP private AS number used on their CPE(s)
- The bandwidth contracted by Client to their ISP should be communicated to NTT Data' project manager

1.1.8 Facility Services

Access

Access to Premises and Licensed Area

NTT Data shall provide Client access to the Premises and Licensed Area (the area within NTT CC's DC where Client's equipments are hosted) consistent this service description.

Client's Authorized Personnel shall be permitted to enter onto the Premises and shall have access to the Licensed Area to perform the work or services permitted by this Agreement, by prior arrangement with NTT Data, and on up to four occasions per calendar year. Accesses should be arranged as far as possible in advance, and in any case 5 business days in advance. If more than four accesses are required in a calendar year, NTT Data reserves the right to charge for time and materials to support such additional accesses. NTT

(Insert appropriate disclaimer if required)

Data may require Client to provide photographic identification according to the physical access and security requirements at the facility and may require Client’s Authorized Personnel to be supervised while they access the premises.

Power

NTT Data shall provide DC power and/or AC power to the Licensed Area as per the allotment specified in the applicable Service Order. NTT Data shall be responsible for repairing and maintaining the electrical system of the Premises

Facility Maintenance Services

NTT Data shall maintain the Premises (but shall not have an obligation to maintain the Licensed Area) and shall provide maintenance services in a professional workmanlike manner consistent with telecommunications industry standards

Interconnection/Cross-Connect Services

Upon acceptance of a Client-executed SOF, NTT Data shall provide Interconnection Services at the pricing and rates provided in the applicable SOF. Unless otherwise agreed to by NTT Data, all Interconnection Services shall be performed in the Meet-Me-Area. In the event a conduit build is required for the purpose of extending connectivity to termination points outside of the Premises or the Meet-Me-Area (e.g. to other carriers within the Building not in the Meet-Me-Area), such conduit build-outs shall be on mutually agreed terms and shall be set forth on the applicable Service Order.

Air Conditioning

NTT Data shall provide air conditioning service to the Premises consistent with telecommunications industry standards and shall be responsible for repairing and maintaining the air conditioning equipment.

Fire Suppression

NTT Data shall supply a fire suppression system for the Premises consistent with telecommunications industry standards and shall be responsible for repairing and maintaining the fire suppression system in compliance with telecommunications industry standards.

Lighting

NTT Data shall provide common overhead lighting for the Premises and shall be responsible for repairing and maintaining the common overhead lighting system.

Equipment-Installation/Removal

Installation

Any delivery, installation, replacement or removal work with respect to Client's Equipment shall be subject to review and approval by NTT Data, such approval not to be unreasonably withheld or delayed. From time to time NTT Data may request and Client shall promptly provide information regarding Client's Equipment, systems, proposed rack/cabinet layout and interconnections/cross-connect diagrams, and the identification of Client's suppliers or contractors. All Equipment and Equipment installations shall strictly adhere to the "Equipment Specifications" section of the Facility Rules. Approval by NTT Data is not an endorsement of Client's supplier or contractor, and Client will remain solely responsible for the selection of the supplier or contractor and all payments for construction work.

Client shall not make, or cause to be made, any construction changes or material alterations to the interior or exterior portions of the Premises or Licensed Area, including any cabling or power supplies for the Equipment, without obtaining NTT Data' written approval for Client to have the work performed and otherwise complying with the terms of this Agreement. NTT Data shall have no responsibility for any loss or damage to Client's

Equipment, except to the extent caused by NTT Data' or its subcontractor's gross negligence or wilful misconduct.

Removal

Client agrees that, upon the expiration or termination of the License, Client shall promptly remove, at Client's sole cost and expense, all cable, wiring, connecting lines, and other installations, equipment or property installed or placed by or for Client in the Premises, and restore those portions of the Premises damaged by such removal to their condition immediately prior to the installation or placement of such items, ordinary wear and tear excepted. If Client fails to promptly remove all such items, NTT Data may, at Client's expense, remove and store such items and restore those portions of the Premises damaged by such removal to their condition immediately prior to the installation or placement of such items, ordinary wear and tear excepted. Any Client Equipment not claimed by Client within 60 days of the expiration or termination of the License shall be deemed abandoned and ownership of such equipment shall automatically transfer to NTT Data. Notwithstanding anything to the contrary contained in this Agreement, Client shall not be permitted to remove any Client Equipment from the Licensed Area at a time when Client is delinquent in meeting its undisputed payment obligations or is in breach of any material term under this Agreement. In the event that Client is restricted in accessing the Licensed Area due to non-payment of undisputed payment obligations and NTT Data seizes Client's Equipment as a result of such non-payment, NTT Data shall apply the fair market value of the seized Equipment against Client's unpaid balance.

Cross-Connections

Only upon the prior express written consent of NTT Data may Client cross-connect its Equipment with equipment or services of any other Client or tenant of NTT Data, including any sub-tenant/sub- licensee within the Premises. Failure to obtain the prior written consent of NTT Data shall constitute a material breach of this Agreement and NTT Data may pursue any legal or equitable remedy available to it, including immediate removal of such impermissible cross-connects and/or the immediate termination or suspension of the License granted by this Agreement without any liability. All installation and other work relating to the establishment of cross-connections with any party for which NTT Data gives explicit written permission shall be established under the control and direction of NTT Data and shall be carried out in the Meet-Me-Area.

Licensed Area Relocation

NTT Data shall not unreasonably, arbitrarily or discriminatorily require Client to relocate the Equipment to a relocated Licensed Area; however, NTT Data shall have the right to relocate the Licensed Area within the Premises upon thirty (30) days' advance written notice to Client or, in the event of an emergency, as determined by NTT Data in its sole discretion, with such notice as NTT Data may deem reasonable under the circumstances. In such case, NTT Data shall reimburse Client its reasonable costs incurred in moving Client's Equipment to the new Licensed Area.

Compliance with Laws

Facility Rules & Regulations. Each of NTT Data and Client, at its sole cost and expense, shall comply with (a) all laws, ordinances, orders, rules and regulations of state, federal, municipal or other agencies or bodies having jurisdiction relating to its specific use or manner of use of the Licensed Area, and (b) all industry standards, practices and procedures. Client's use of the Licensed Area, installation of Equipment and access to the Premises shall at all times be subject to and conditioned upon the strict adherence to the Facility Rules.

Inspections

NTT Data may conduct reasonable inspections of the Equipment and Licensed Area as NTT Data deems necessary or appropriate. NTT Data will use commercially reasonable efforts to give Client reasonable notice of such inspection, but under no circumstances will NTT Data be required to notify Client or obtain Client's consent before entering the Licensed Area.

Eminent Domain

In the event of a taking by eminent domain of all or any portion of the Premises so as to prevent, in NTT Data' sole reasonable judgment, the utilization by Client of the Licensed Area, the License shall terminate as of the date of such taking or conveyance with respect to the Licensed Area which is affected by such taking or conveyance, and the MRC to be paid by Client shall be adjusted accordingly. Client shall have no claim against NTT Data for the value of the unexpired Term of this Agreement or the applicable Service Order affected thereby (or any portion thereof) or any claim or right to any portion of the amount that might be awarded to the landlord of the Premises or NTT Data as a result of any such payment for condemnation or damages.

Damage to Premises

If the Premises are damaged by fire or other casualty, NTT Data shall give notice to Client of such damage as quickly as practicable under the circumstances. NTT Data shall have the option to terminate the License due to damage or destruction of the Premises and the License shall terminate as of the date of such exercise or decision as to the affected Licensed Area, and the MRC to be paid by Client shall be adjusted accordingly. If NTT Data does not exercise the right to terminate, then NTT Data shall restore the Premises to substantially the same condition it was in prior to the damage, completing the same with reasonable speed considering all of the facts and circumstances. In no event shall NTT Data have any obligation to repair or replace Equipment unless the Equipment is damages as a sole result of NTT Data' gross negligence or willful misconduct. In the event that NTT Data shall fail to complete the repair within a reasonable time period under the circumstances, Client shall thereupon have the option to terminate the relevant License and applicable Service Order(s) with respect to the affected Licensed Area, which option shall be the sole remedy available to Client against NTT Data under this Agreement relating to such failure. If the Licensed Area or any portion thereof shall be rendered unusable by reason of such damage, the MRC for such Licensed Area shall proportionately abate, based on the amount of square footage of the Licensed Area which is rendered unusable, for the period from the date of such damage to the date when such damage shall have been repaired for the portion of the Licensed Area rendered

1.1.9 Noteworthy limitations

- The demarcation points between Client and NTT Data is at the NTT Data edge switch port.
- NTT Data shall not be held responsible for any incident occurring between Client’s network and NTT Data’ edge switch port.
- This item does not include the costs of the last mile within NTT Data’ Datacenters (i.e. Leased-line, local loop, etc.).
- Cloud Interconnect service is provided "as is", without warranties or guarantees whatsoever. NTT Data excludes and disclaims to the fullest extent permitted by law all representations, warranties, guarantees, conditions and terms express, implied, statutory or otherwise including, without limitation, the warranties of merchantability, fitness for a particular purpose, and non-infringement of proprietary and intellectual property rights. NTT Data makes no warranty or guarantee that the Cloud Interconnect service will be uninterrupted, available at all times, timely, secure, error-free, fault-free or omission-free or that NTT Data can prevent fraud or fraudulent access, malware, phishing attacks or hacking of the Cloud Interconnect service. NTT Data accepts no liability for any service outage other than in the circumstances described herein (service level agreement).
- Information transmitted using the Cloud Interconnect service will pass over third-party communications networks. NTT Data accepts no liability if the Cloud Interconnect service is not accessible due to failure of equipment, systems, connections or services not provided by NTT Data including, but not limited to network connectivity problems caused by third party network service provider or other user network connectivity issues; end user’s firewall software, hardware or security settings; user’s configuration of anti-virus software or anti-spyware or malware software, or any other third party software or equipment.
- NTT Data accepts no responsibility or liability (i) for any equipment hosted by NTT Data and supplied by Client or by any third party in the name of and on Client’s behalf or (ii) for any action or omission by Client or by any third party acting in the name and on Client’s behalf, including when installing or removing the equipment in NTT Data’ (or its subcontractors’) premises.

- It is Client's responsibility to retrieve its equipment within two (2) months after the expiry of the Agreement, failing which NTT Data shall be entitled to destroy the equipment in the name of and on Client's behalf.
- Access to the premises and licensed area will be granted only if Client is current in its payment obligations and has not breached any material term under this Agreement,
- Client shall be liable for the actions of any Authorized Personnel accessing the premises and the licensed area. Authorized Personnel must carry photo-identification for presentation to NTT Data or NTT Data' agents, employees or representatives when entering the Premises. Client shall designate one person as the primary account contact and shall provide the name and contact information for the primary account contact on the Contact Information page appended to the end of this Agreement. Client shall ensure at all times that the primary account contact information is accurate and complete. In no event shall Client or any agent, representative, contractor or invitee of Client, including without limitation, Authorized Personnel, have the right to access any portion of the Premises, other than the common areas and the Licensed Area.
- NTT Data shall have the right to refuse access to the Premises and Licensed Area to anyone in its reasonable sole discretion if it determines that such person presents a hazard or security threat to NTT Data or its other Client or if the License granted hereunder has been suspended or terminated.

1.2 Remote SBC Management

With the Remote SBC Management service, Cloud Communications remotely manages a selection of Session Border Controller (SBC) models to enable specific use-cases including:

- On-premises connectivity of analog endpoints (built-in analog ports or using an Analog Telephone Adaptor separate device)
- On-premises connectivity of IP-PBX equipment

For some territories, terminating or originating PSTN calls outside the country, or avoiding local PSTN tolls by using cloud services is not permitted. It is Client's responsibility to ensure compliance with any such local regulations, consulting with Cloud Communications' Advanced Services teams as necessary.

N.B. The Remote SBC Management service does not include the monitoring of endpoints or other hardware elements placed beyond the SBC(s) of Client.

1.2.1 Available topologies for UCaaS connectivity

Cloud Communications' standard deployment topology of SBCs is based on the "Upstream" design. In this design, the SBC is positioned in-between the PSTN carrier leg and the Client's legacy on-premises equipment (i.e. legacy IP-PBX), if any.
This design is very well suited for smooth and progressive migration of end-users from legacy to Cloud-based solutions.

Direct SBC connectivity to UCaaS solutions

By default, the Remote SBC Management service is connecting directly to the available UCaaS platforms via Internet using SIPS/SRTP encryption (TLS1.2).
The solution is also compatible with Cloud Interconnect.

Indirect SBC Connectivity to UCaaS solutions

At present, this type of connectivity using the Cloud Voice network to reach targeted UCaaS platform(s) is not supported.

Customer's carrier connectivity (BYOC)

Client can connect its own carrier to the solution using any of the below technologies:

- SIP trunking
- ISDN

- Analog lines

1.2.2 Specific UCaaS features compatibility

Media Bypass

The Remote SBC Management service is compatible with Media ByPass technology and works as defined by the UCaaS vendors Cloud Voice is enabled for.
Media Bypass is a feature that lets voice media packets flow directly between end-users and their defined SBC. This notably avoids sending voice traffic over the internet to the vendor's cloud and may be more suited to Client's needs in some specific topologies.
Since the configuration of Media Bypass relies on WebRTC, end-users need to have access to the public IP address of their SBCs and this generally requires specific firewall configuration.
N.B. Media-Bypass is not yet available for Cisco Webex Calling

1.2.3 List of compatible devices

Audiocodes

The following Audiocodes devices are supported for Remote SBC Management service:

- The Remote SBC Management service is compatible with all Mediant series, including the Virtual Edition (VE)
- MediaPack (MP) 1288

Cisco Cube and IOS gateway

All models amongst below device types defined compatible with Webex Calling by vendor (Cisco) are supported:

- Cisco® Unified Border Element (CUBE) for IP-based connectivity
- Cisco IOS® gateway for TDM-based connectivity

1.2.4 SBC remote maintenance and firmware updates

Remote maintenance

As part of this service, Cloud Communications provides remote maintenance services to fix issues and bugs occurring on the SBC device(s).
A "Management Jump Box" is used by Cloud Communications Engineering teams to remotely and centrally access management protocols of the SBCs (HTTP, HTTPS, SSH). It also allows logs collection of the SBC(s) and serve as a NTP server.

Firmware updates

Cloud Communications provides firmware update management for critical or major vendor firmware updates.
Firmware updates will be provided inclusive of non-regression testing only for scenario listed as standard in this Service Description document.
Any regression testing for bespoke setup can be done using Cloud Communications Advanced Services.

1.2.5 SBC vendor(s) escalations

As part of this service, Cloud Communications manages escalation to SBC vendor(s) on behalf of Client.

1.2.6 24/7 monitoring and alerts

Cloud Communications provides 24/7 monitoring via its Central Monitoring infrastructure and receives live alerts on the health of the systems.

24/7 monitoring teams

Managed SBCs are monitored by our 24/7 monitoring teams. Cloud Communications monitoring teams will initiate investigations and engage Cloud Communications support teams if any issue is raised by monitoring tool.
Cloud Communications support teams will connect to the remote SBC(s) in order to perform any required troubleshooting or maintenance tasks.

1.2.7 Remote SBC Management pre-requisites and specifications

The Remote SBC Management service requires Client to comply with below pre-requisites and specifications.

Hardware maintenance contract

For Cloud Communications to effectively provide maintenance and vendor escalation services, Client is responsible for having a valid Hardware maintenance contract in place for the duration of the Remote SBC Management service.
Such Hardware maintenance contract must also cover for Hardware replacement in case of physical damage impacting the SBC.
In the event of a defective hardware SBC, Cloud Communications does not provide on-site support. It is Client's responsibility to un-rack the faulty unit, rack the replacement unit and configure the initial IP parameters. Cloud Communications support teams will then remotely connect to the replacement SBC and push the backup configuration.

Remote connectivity requirements

Client can choose between two solutions to enable Cloud Communications for remotely accessing to the SBC(s):

- Site-to-site VPN connectivity
- Monitoring Probe through SBC's public IP@

Cloud Communications recommends using the Site-to-Site VPN connectivity solution described below as it permits an easier configuration and does not require to expose SBC management ports on the Internet.

Site-to-site VPN connectivity (Appliance or Windows VM based)

This option is based on the creation of a Site-to-Site VPN Connectivity between a VPN Equipment on Client side and a VPN Concentrator on Cloud Communications side. Monitoring (SNMP, Syslog) and Management (HTTP, HTTPS, SSH) protocols between the SBC and Cloud Communications Servers are tunneled through VPN link.
This solution requires Client to either:

1. Purchase and install an appliance as per Cloud Communications guidance, or
2. Provide a Windows VM to install the OpenVPN software

The solution should be connected in same subnet/VLAN as the SBC Management Interface on one side and should be provided with an Internet access on the other side.
The following network flow should be authorised between the VPN Equipment and Cloud Communications infrastructure on the Internet.

Service	Traffic	Source	Source Port	Destination	Destination Port

Management	OpenVPN	Netgate appliance Or VPN VM	any	VPN Concentrator Public IP	TCP 443

Monitoring Probe through SBC's public IP@

This option involves management of HTTP, HTTPS and SSH streams over the Internet using the SBC's public IP address.

A VM needs to be setup as a monitoring probe in Client's environment. This monitoring probe will communicate with the SBC (SNMP, Syslog, NTP) locally on Client's network and monitoring data will be forwarded securely over the Internet to Cloud Communications.

Remote management of the VM is performed thanks to an OpenVPN client installed on the VM allowing RDP connection from the Management Jump Box to the Monitoring probe.

The Monitoring VM should be connected in the same VLAN as the SBC private management interface and should be provided with an Internet access.
The following network flows should be authorised between Cloud Communications infrastructure on the Internet and the SBC Public IP Address:

Service	Traffic	Source	Source Port	Destination	Destination Port
Management	HTTPS	NTT Public Ips	any	SBC Public IP Address	TCP 443
Management	HTTP	NTT Public IPs	any	SBC Public IP Address	TCP 80
Management	SSH	NTT Public IPs	any	SBC Public IP Address	TCP 22
Monitoring	SCOM Gateway	Monitoring VM	any	Central Monitoring infrastructure IP@	TCP 5723
Management	OpenVPN	Monitoring VM	any	VPN Concentrator Public IP	TCP 443

The public IP assigned to the Monitoring VM when connecting to the Internet (can be over NAT) should be a static IP. This public IP should be communicated to Cloud Communications' engineering teams for authorization on the central infrastructure (white-listing).

Protocol requirements

The following protocols need to be available between Cloud Communications and the SBC hosted on customer premises:

SNMP (Monitoring)

3. Connection from NTT to the SBC (poll)
4. Connection from the SBC to NTT (trap)

Syslog (Monitoring)

5. Connection from the SBC to NTT

NTP (Time Synchronization)

6. Connection from the SBC to NTT

SCOM Agent (Monitoring) => when using Option B (see 7.3.2)

7. Connection from the Monitoring VM to NTT

HTTP (Management)

8. Connection from NTT to the SBC
9. By default, HTTP will be disabled on the SBC, still this protocol will be activated on-demand by UC Engineering Ops/Support on a regular basis in order to successfully perform the update of the SSL Certificate

HTTPS (Management)

10. Connection from NTT to the SBC

SSH (Management)

11. Connection from NTT to the SBC

Firewall requirements

Depending on the chosen remote connectivity scenario Client may be required to open several interfaces on its Firewall(s), as per NTT Cloud Communications indications.

Technical specifications

Network connectivity assessment to UCaaS platform(s)

A network assessment is recommended to validate the sustainability of the solution. The below criteria should be checked as per ITU-T recommendations for VoIP applications:

- Max RTD: 300 ms (recommended)
- Jitter 50-80 ms
- Packet loss ratio < 1%

Public Certificates requirements

Each SBC deployed must have a public certificate from a supported Public CA:

- When generating the CSR, the private key size should be at least 2048
- Do not try to use onmicrosoft.com domain for certificates
- The SBC FQDN (example “sbc.directrouting.com”) must be in the subject, common name, or subject alternate name fields.
- A wildcard certificate *.mycompany.com

Cloud Communications requires that the certificates are generated from one of the root certificates providers certified by the chosen UCaaS solution vendor. Not conforming with this will prevent the solution to effectively communicate with the UCaaS platform(s).

1.3 Cloud Endpoints Registration

The Cloud Endpoints Registration service allows Client's end-users to consume Universal Calling Plans directly on legacy endpoints without the need to deploy Client-hosted SBCs.

(Insert appropriate disclaimer if required)

1.3.1 Description

The Cloud Endpoints Registration offers Client to register endpoints on NTT CC's cloud-based SIP registration platforms.
The solution is designed to be plug and play and secured with SIPS and SRTP encryption.

1.3.2 Requirements

Internet-based and Private network-based accesses

Whether Client is using Public Internet based access or using Private network-based access (Cloud Interconnect or NTT Global Networks access), a static public IP address is required per Client's network exit point(s) and the solution will use UDP port 5099 NATed with a private IP.

List of compatible devices

Client must use one of the following Analog Telephone Adapter (ATA) devices to connect analog endpoints to our Cloud Voice services:

- MediaPack 20X (2 to 4 FXS ports)
- MediaPack 1XX (2 to 24 FXS ports)
- MediaPack 5XX (4 to 8 FXS ports)
- MediaPack 1288 (up to 288 FXS ports)

Once an ATA device is installed and validated, it is Client's responsibility to save its full configuration (ini.file) and store it to be able to restore the service in case of hardware failure.

1.3.3 Limitations

This service is limited to registration of analog endpoints.
Please be mindful that the implementation of encryption may impact
This service does not include the maintenance of Client's ATA(s). NTT CC recommends keeping spare ATA devices on sites with critical analog endpoints.

2. Service Operations

2.1. Service Management

Support for Customer’s own communication platform (e.g. IPPBX, Contact-center, UCaaS solutions) is not included when the Customer only subscribes to the Universal Access products set.
The scope of the support provided as part of Cloud Voice for CX is limited to the elements under NTT’ control. These elements include:

- NTT’ backbone network
- NTT’ voice infrastructures
- NTT’ connectivity to partner carriers
- NTT’ connectivity to standard CX platforms listed in this Service Description

2.2. Global Integrated Operations Centre (GIOC) service-desk

The NTT Global Integrated Operations Centre operates currently as a single virtual team with engineers based in Barcelona (Spain) and South Africa.
The NTT Global Integrated Operations offers English language support on a 24hours/365 days basis.
The NTT Global Integrated Operations Centre is responsible for:

- Being the first point of contact for Customer Authorized Administrator
- Tracking, managing and completing Services and Incident Requests
- Responding to phone calls and service portal requests
- Manage requests with other vendors and internal escalation teams.

N.B. Service requests and incidents must be raised by a Customer Authorized Administrator.
Customer Authorized Administrators are one or more named individuals or a named Service Desk that are authorized to log cases to NTT.

2.3. High Availability

Conscious of the importance of providing a highly reliable Cloud Voice service, NTT has made strong investments in effectively deploying a highly redundant Cloud Voice network relying on a fully meshed high-speed L2VPN backbone network.

2.3.1 In-DC N+1 redundant design

The Cloud Voice network relies on high availability clusters: Our VoIP platforms are all made on-site redundant. These clusters offer high availability service delivery with stateful failover which allows preservation of calls in-progress in many failover scenarios.

2.3.2 Geo-Redundancy

In case of a full DC outage, our Cloud Voice network platforms provide alternate routes via different locations to reach a destination, notably thanks to multi-homing of upstream carriers’ connectivity, and multi-homing of connectivity to Cloud Voice platforms.

2.4. Service Monitoring

The Cloud Voice network is monitored on a 24/7 basis by our globally distributed NOC/L2/L3 teams.
SIP service state is monitored using SIP Options requests.
In case of standalone deployments (i.e. on-premises platforms), Client must answer to SIP Options request to benefit from this monitoring service. As per Failover implementation, SIP service will continue even if one network link is down.

(Insert appropriate disclaimer if required)

In the case of Cloud Interconnect or NTT Global Network services type of accesses are used, then BGP-peering state is monitored.

2.5. Incident Management

Incidents are defined as “unplanned interruption to service or reduction in the quality of service provided”. When it comes to Universal Access Product, the below specifics apply.

2.5.1 Incident priority definition

Incidents are prioritized according to the below matrix table:

	Large scale	Medium scale	Small scale
High impact	P1	P1	P3
Medium impact	P2	P2	P3
Low impact	P2	P3	P3

Request for Information (RFI) are classified as P4

Large scale: Entire Site impacted / Several groups of end-users. A site is a company business office.
Medium scale: Group of several end-users. Can be a business department, a site floor, several users in different sites.
Small scale: A couple of users or Remote Workers.

High impact: Service not available (i.e. no calling / one-way audio)
Medium impact: Service partially available (i.e. Unable to reach some PSTN destinations, some outbound calls are failing, etc.)
Low impact: Poor service quality (i.e. Voice quality is not good, Ringback tone is strange, etc.)

2.5.2 Incident priority matrix

Incident priorities are defined according to the below matrix table:

Incident Priority	Response Target (Auto)	Ticket Status Update	Time to Restore
P1	15 mins	2 Hours	4 Hours
P2	30 Mins	4 Hours	12 Hours
P3	4 Hours	24 Hours	72 Hours
P4	N/A	N/A	N/A

2.6. Monthly Service Availability Service Level Agreement (SLA)

2.6.1 Description

NTT Cloud Voice Monthly Service Availability SLA applies from within Cloud Voice service boundaries (notably the NTT Cloud Voice network, its connectivity to our ingress PSTN carriers and the interconnection with standardized CX cloud platforms). Any outage outside of this perimeter will not be taken into account to compute this SLA (i.e. the terminating operator’s network or the Client’s real-time communication platform).

Monthly Service Availability is computed using the following formula:
MSA = (Total Monthly Minutes – Valid Downtime)/Total Monthly Minutes

Valid downtime includes, and is limited to the below events:

- End-user is unable to receive PSTN calls (IN)

- End-user is unable to place domestic PSTN calls (OUT)[1]

Valid Downtime excludes downtime linked to Standard, Emergency and Scheduled Maintenance Windows. Downtime linked to these events shall be excluded from the calculation of the Monthly Service Availability. Downtime starts from the point at which a relevant priority incident is logged to the Service-Desk and ends when Client is notified that the incident has been resolved.

2.6.2 Scope

The Monthly Service Availability is calculated on a per subscription basis (per Universal Access option element, i.e. per registered endpoint).

For example, should Client have 10 Service Numbers and the service becomes unavailable for 1 Service Number during 100 minutes, Then 100 minutes would be counted as Valid Downtime and withdrawn from the Total Monthly Minutes of 43 920 x 10 = 439 200 minutes.

Resulting MSA would be 99.98%.

2.7. Patch Management

NTT implements critical and security patches in a maximum 30-days timeframe from the release of the vendor.

2.8. Data Management

Data Management specifics are detailed in the NTT Fact Sheet for the Universal Access product.

2.9. Data security policies

2.9.1 Datacenter security policies

NTT hosts its platforms in 3rd party Datacenters where a set of certifications such as SSAE16 (Statement on Standards for Attestation Engagements) and ISO 27001 are available. This guarantees the implementation of a rigorous set of global standards covering physical, logical, process, and management controls.

2.9.2 Remote access to Cloud Voice network management layer

Remote access to Cloud Voice network management layer is prohibited. Accesses are only permitted from within the NTT CC’s internal network and secure remote access facilities with multi-factor authentication.

2.9.3 Vulnerability scanning and penetration testing

NTT performs external and internal vulnerability scanning on a monthly basis. Risk based reviews are performed based on scan results and are addressed in accordance with NTT Group policy. In addition, annual penetration tests are performed to evaluate the security of the NTT’ external cloud footprint. The penetration tests are scoped to include all identified external IP ranges and align with testing based on industry standard methodology.

2.9.4 Traffic encryption

For Internet-based accesses to the service, NTT TLS encryption settings are the below ones:

- TLS version 1.2

- TLS Key: 2048 bits
- Encryption algorithm: AES-256 (256 bit key, 128 bit block)

Authentication mode: encrypted credentials (login/password) and SSL Certificate.

2.9.5 At-rest data encryption

All at-rest Personal Data stored by NTT for a period over 1 hour are encrypted using the AES-256 (256 bit key, 128 bit block) algorithm.

2.9.6 Backup policies

NTT operates and maintains a data protection infrastructure to prevent loss of data and permit timely restoration of services in the case of a disaster or catastrophic system failure.

2.9.7 Limitations and Exclusions

NTT’s data protection infrastructure is NOT meant to maintain a versioned history of data.

Restoration of Client data shall be at Client’s sole cost and expense, unless the need for the restoration was due solely to a failure or error of NTT.
NTT shall delete all information related to a User from its databases as soon as a User is deleted by Client on the Self-Care.

2.10. Personnel Security

NTT implements a security policy framework influenced by ISO/IEC 27001. The security policies are communicated and made available for all NTT’ employees. The policies are reviewed by the Security Officer on a yearly basis

3. Security and fraud management

Our Cloud Voice product is fully featured with state-of-the-art Fraud Management systems to protect our clients against the main voice fraud schemes.

3.1. Main fraud schemes managed

Amongst the various fraudulent activities which may occur in voice networks, the below listed ones are usually quite impactful for enterprises. Our solution is designed to prevent such frauds.

3.1.1 Toll-Free fraud/Toll-Free traffic-pumping

Toll-Free fraud involves making multiple calls to a Toll-Free number—and staying on the call as long as possible, often navigating the automated IVR prompts and avoiding connecting to a live operator.

3.1.2 Call transfer fraud

In this scenario, the fraudster hacks into a PBX and uses that PBX's services to make free long-distance calls. By instructing the compromised PBX to transfer the call to the hacker's own phone service, subscribers to the fraudster's phone service can speak to their international destinations through the hacked PBX.

3.1.3 Telecom denial-of-service (TDOS)

Telecom denial-of-service (TDoS) attacks are typically made of a huge number of phone calls to one organization's set of User Number(s), keeping them up for long durations, and overwhelming the capacity of an organization's phone network.

3.1.4 Wangiri fraud

Wangiri, in Japanese, means "one and cut." That is, one ring and a cut off phone call. A Wangiri phone fraud scheme relies on this single ring method. A fraudster will set up a computer to dial many phone numbers at random. Each rings just once, then hangs up. This leaves a number as a missed call on the recipients' phone. Users often see the missed call and believe a legitimate call was cut off, or are simply curious as to who called, so they dial the missed number. The number turns out to be a premium rate number.

3.1.5 Revenue sharing fraud

Revenue share fraudulent activities are those which abuse carrier interconnect agreements. The fraudster's goal is to pair up with a destination that can charge high rates, and then inflate traffic to his numbers at little or no cost to himself. It often involves compromising a PBX or an auto-attendant system.
These types of schemes can occur within a country, or across international borders.

3.2. Security and Fraud management mechanisms

Several mechanisms have been put in place to prevent fraudulent activities such as the ones described above.

3.2.1 SIP Proxy: Real-time traffic patterns monitoring

Traffic patterns are monitored in real-time with call attempts, call minutes and costs compared to thresholds to detect fraudulent activities.
In case of an unusually high volume of calls to a destination, within a short period of time, or an unusually high call duration for calls to a destination, can be detected in real-time and may result in calls to that destination

being suspended temporarily (60 minutes by default on a per destination-basis – can be customized on a per Client-basis as a PS engagement).

3.2.2 Central Black and White-lists management system

NTT subscribes to live fraud protection data, updated multiple times per day, which dynamically adjusts blacklists and whitelists with high-risk phone numbers compiled from research, industry sources, and national numbering plans.
NTT also maintains its blacklists and whitelists based on monitoring telephony services across its network.
Lastly, the 24/7 NOC and support teams are able to make changes to this in near real-time when appropriate based on reports from the outbound routing system, and incidents.

3.2.3 SIP Analytics

The SIP Analytics technology permits to detect and automatically block telecom fraud attacks without impacting legitimate calls. By analyzing SIP messages before the call is set up, the system can quickly detect an attack—much faster than other systems that use call detail records (CDRs), which are typically created after calls are completed.
SIP Analytics include the following tools:

- TDoS mechanisms
- SIP normalization and protocol validation
- Back-to-Back User Agent (B2BUA)

3.2.4 IP White-listing

At IP level, all SBC public interfaces are configured with white-listing of trusted peers.

3.2.5 STIR/SHAKEN

These acronyms stand for:

- STIR: Secure Telephony Identity Revisited. A framework for authenticating and verifying caller ID.
- SHAKEN: Secure Handling of Asserted information using toKENs. A specific framework built on top of the STIR framework that details how tokens should be used.

In a nutshell, this technology allows for verification that calls are coming from a real caller ID instead of a spoofed or fake caller ID .
STIR/SHAKEN is actively being used by NTT in USA and Canada.

3.3. Client Obligations

Although NTT makes every effort to detect and block fraudulent calls on its network, Client must always:

- Ensure that only authorized people use the Cloud Voice connected phone system to make and receive calls
- Take sensible precautions regarding security and access to systems, such as enforcing the use of strong passwords and PINs where applicable, to prevent unauthorized usage.

Additionally, NTT requires that Client use a valid CLI in the FROM or P-Asserted Identity headers on outbound calls. Generally, this CLI must be one of the User Number DDIs provided by NTT and presented in E.164 format. If Client originates outbound calls without a valid CLI, or with a CLI which is not among Client’s assigned User Numbers, NTT may block the call as this scenario may be considered by PSTN carriers as an attempt to “spoof” a CLI. It may be possible to present a different CLI, by arrangement with NTT.

4. Reporting and QoS

By default, Client gets access to a set of online reporting elements on NTT's selfcare portal via the "Digital Collaboration Services" app.
Here-below are the main reporting elements provided with current release:

- Usage, Consumption and Quality of Service dashboards
- Custom reports (with ability to generate and download these reports)

NTT also measures several KPIs to track QoS, including the below:

4.1. Mean Opinion Score (MOS)

NTT measures the quality of speech by monitoring calls placed on the Cloud Voice network. This measurement provides a qualitative indicator between 1 (lowest perceived quality) and 4.5 (highest perceived quality possible). The maximum values obtained highly depend on the Codec being used for the call. For example PSTN calls using the G.711 codec (most commonly used codec for PSTN calls) have a maximum value for MOS of 4.4.
The Mean Opinion Score (MOS) will be measured as the average of all qualitative indicators for the calls placed on the Cloud Voice Network during the month.

The targeted Mean Opinion Score (MOS) for Cloud Voice (G.711) is ≥4.1

4.2. NTT MOS Degradation

The NTT MOS Degradation is a KPI measuring the impact of NTT Cloud Voice network on the end-to-end Mean Opinion Score of a PSTN phone-call.
This KPI is computed on a per-CDR basis and covers the call path between the NTT Cloud Voice ingress SBC to the NTT Cloud Voice egress SBC.
The targeted NTT MOS Degradation score for Cloud Voice is <0.4.

4.3. Post Dialling Delay (PDD)

Post Dial Delay ("PDD") is the time interval between the end of user or terminal equipment dialling and the reception of the appropriate network response.
Post Dialling Delay can be influenced by Client dialling behaviour and/or the types of network, e.g. variable number lengths, that are interconnected, and in some cases, by the type of service that is being carried on the end-to-end telecommunication networks.
NTT measures the average monthly PDD on its Cloud Voice network.
NTT commits on an **average PDD ≤4 seconds**

5. Billing

5.1. Standard Charges types

The Cloud Voice Service as described in this document is structured with the flowing SKU's:

SKU name	Description	Charge type
Cloud Interconnect – Single Access setup	Single Access Cloud Interconnect solution (includes cross-connect charges)	Monthly Recurring Charges
Cloud Interconnect – Dual Access setup	Dual Access Cloud Interconnect solution (includes cross-connect charges)	Monthly Recurring Charges
Remote SBC Management - Single Gateway	Remote management, monitoring and firmware updates of one cluster of one SBC	Monthly Recurring Charges
Remote SBC Management - Dual Gateway (HA)	Remote management, monitoring and firmware updates of one cluster of two SBCs	Monthly Recurring Charges
Cloud Endpoints Registration – Per Endpoint	Monthly add-on fee for endpoints registration into Cloud Voice. Comes as an add-on to underlying Universal Calling Plan.	Monthly Recurring Charges

List of billing charges

5.2. Billing Cycles

NTT billing cycles start on the first calendar day of the month and ends on the last calendar day of the month. Monthly Recurring Charges (i.e. Universal Calling Plans) and overage per-minute pay-as-you-go communication charges are computed on the last calendar day of the Month for invoicing (i.e. Communications of December 2023 are rated on December 31st and invoiced by mid-January 2024).
NTT does not provide pro-rated charges but rather full month rating and invoicing.

5.3. One-Time Charges

One-Time Charges are to be charged only once and following conditions described in the SOF or in the SoW if Professional Services (PS) activities are also included.
In case of the latter, the detailed description of what is covered by such charges shall be described in the PS Statement of Work.

5.4. Monthly Recurring Charges

5.4.1 Cloud Interconnect charges

Cloud Interconnect charges are Monthly Recurring Charges and are chargeable in arrears on a per-Cloud Interconnect cluster basis, with a charge depending on whether this is a single or dual Cloud Interconnect cluster.

5.4.2 Remote SBC Management charges

Remote SBC Management charges are Monthly Recurring Charges and are chargeable in arrears on a per-SBC cluster basis, with a charge depending on whether this is a single or dual SBC cluster.

5.4.3 Cloud Endpoints Registration – Per Endpoint

Cloud Endpoints Registration – Per Endpoint is a metered monthly charge for each endpoint directly registered into Cloud Voice. This charge comes as add-on to the underlying Universal Calling Plan (and phone number) assigned to this endpoint.

5.5. Minimum Monthly Commitment

Client understands and agrees that NTT is entitled to charge a Minimum Monthly Commitment (MMC) as defined in the Service Order Form (SOF).
Said MMC shall only be charged should the total amount of Monthly Recurring Charges and the Per-minute overage consumption due over a monthly period be inferior to this MMC amount. In such case the MMC only will be charged to Client superseding the sum of the other Cloud Voice charges (excluding One-Time charges). The MMC is computed at the Billing Account level.

5.6. Other charges

For all charges not listed in SOF, Client must refer to its NTT Account Manager. Should the provisioning of services not listed in the SOF be effective, NTT shall charge such services using its standard Price-List, available on-demand from Client's Account Manager.

5.7. Billing and Invoicing capabilities

By default, NTT will invoice Client centrally in-country as initially agreed between the two parties.

Specifics

Billing is not available in all countries, nor in all currencies. Feasibility must be checked upfront.
Invoicing of China Calling Plans must be done outside of China.