Arcstar Universal One Service

User's Guide

Arcstar Universal One Service User's Guide

1. Basic Service

1-1. Core Network Service

Arcstar Universal One Service classifies the service type as below.

Service Types	Description
VPN Type	Other than Internet Type
Internet Type	The Type which is an internet access with managed CPE services
Remarks 1. Internet Type shall be ordered with CPE Service which shall be Managed CPE Option #1 or Managed CPE Option #2. 2. Access Line of VPN Type and Access Line of Internet Type shall not belong to the same VPN Group.	

1-1-1.VPN Type

Service Category	Remarks
MPLS	MPLS service provides the IP Protocol based connection mainly for data communication between Global VPN ports of the Customer. - Routing Protocol: BGP4/ Static - MTU Size: 46-1500 Bytes - Unavailable address: /22 address block (/22 address blocks can be specified by Customer. 10.128.0.0/22 is recommended.) This service includes the service that provides the interconnection port with other carrier's VPN. Available bandwidth indicates logical circuit speed including the header size.
Ethernet	Ethernet service provides the Ethernet frame based connection mainly for data communication between VPN ports of the Customer. - Available number of MAC addresses: 1000 per each VPN - Maximum number of sites: 250 - Multicast: not available - Ethernet frame size: 46-1500 bytes (untagged), 68-1522 bites (802.1q tagged) - Customer VLAN transparency: available - Available Layer 2 Protocol: Limited - Link down transfer: not available Available bandwidth indicates logical circuit speeds including the header size.
DMVPN	DMVPN service provides Internet VPN communications by using DMVPN (Dynamic Multipoint VPN) technology between Customer's pre-specified ports, mainly for the purpose of data communications. - DMVPN enables communications without going through Universal One networks. - In case of limiting communications with Universal One networks, for which VPN Group Representative should request upon applying for the said VPN Group. - As a condition to use DMVPN type, Customer is required to apply for CPE Service (Managed CPE Option #1 or Managed CPE Option#2).

1) The duplication of IP address within the same VPN (including other interconnected VPNs) is not allowed.
2) Company specifies maximum number of routes which can be allowed to use in the same VPN. Service Item is defined by bps (bit per second), and it is the maximum traffic which can be transferred in one Global VPN port. The traffics should be even.
3) The traffic exceeding the Service Item is not secured regardless of whether it is constant or instantaneous (less than 1 second). When the traffic which exceeds the Service Item generated, the traffic may be dropped.
4) Packet loss or frame loss may occur in the following cases depending on traffic condition although the sufficient bandwidth is secured in the section which service is provided.
   A. Asymmetric communication: The traffic which exceeds the Service Item of destination port by micro-burst traffic sent from Customer's CE may be dropped.
   B. Simultaneous packet transmission from multiple sites: The traffic which exceeds the Service Item

of destination port by packets transmitted by multiple sites simultaneously may be dropped based on QoS policy. Customer shall not use the load generation equipment to transmit such unusually large amount of packets. When the act including the cases below is found, Company may stop the Customer's communication immediately.

a. Any act by which Customer transmits a large amount of fragment packets to Universal One network in a unilateral way
b. Any act by which Customer transmits a large amount of packets to Universal One network without waiting acknowledgement in a unilateral way
c. Any act by which Customer transmits packet to addresses which is not described in application form
d. Any other test activities which can affect the performance of Universal One network.

1-1-2. Internet Type

Service Category	Remarks
Internet Services	Internet Services provides internet circuit using managed CPE services. No SLA is provided. Following service menu is available for Internet Services: - Business Portal - SoftMAC - CE Commander - Local Support

1) SLA, network quality assurance, or incident investigation and report is not available for Internet Services.
2) Service area of Internet Services is from Internet to CPE LAN port.
3) The establishment of IPSec tunnel between Managed CPE with encrypted communication by Customer's request and fixed global IP address specified by Customer is as follows:
   A. In case of establishing IPSec tunnel at the same time as activating Internet circuit:
   ・Customer should apply for both Internet circuit and IPSec tunnel.
   ・IPSec tunnel will be established at the same time as activating Internet circuit. Therefore, submission of necessary information to Company and Customer's preparation for establishing IPSec tunnel should be completed by Customer prior to the activation of Internet circuit.
   ・If the preparation is incomplete by Customer, Internet circuit will be activated without establishing IPSec tunnel. In this case, Customer is required to apply for IPSec tunnel separately, which cost will be borne by Customer.
   B. In case of establishing IPSec tunnel after activating Internet circuit:
   ・Customer should apply for IPSec tunnel.
   ・Submission of necessary information to Company and Customer's preparation for establishing IPSec tunnel should be completed by Customer prior to the establishment of IPSec tunnel.
4) Neither monitoring of IPSec tunnel between Managed CPE with encrypted communication by Customer's request and fixed global IP address specified by Customer nor outage notification to Customer will be provided by Company.

1-2. Access Service

Arcstar Universal One Service classifies the Access Line Type as below.

Access Line Type	Description
Dedicated Access (DA)	Dedicated Access is an access line of which the bandwidth is not shared among users.
Dedicated Internet Access (DIA)	Dedicated Internet Access is an access line which goes through Internet and the last one-mile access is not shared among users.
Broadband Internet Access (BIA)	Broadband Internet Access is an access line which goes through Internet and the last one-mile access is broadband access (access line shared among users).

The following Access Line types are available for each UNO product:

UNO Product	Access Line Type availability		
	Dedicated Access (DA)	Dedicated Internet Access (DIA)	Broadband Internet Access (BIA)
MPLS (UNO L3)	Available	Available	Available
VPLS (UNO L2)	Available	Not Available	Not Available
DMVPN (Internet VPN)	Not Available	Available	Available
Internet Services	Not Available	Available	Available

1) The available bandwidth includes IFG. The control range is defined to be the range from preamble of Ethernet frame to frame check sequence and other headers necessary for the technical methodology supported by Ethernet.
2) In case CPE Service is not provided, the Customer shall notify to the Company at the time when the Customer connects Customer managed equipment to Universal One Service. Company will not be able to activate Ping monitoring in case the Customer does not complete connection of the Customer managed equipment or does not make the notification.
3) In case CPE Service is not provided, outage diagnosis by using Customer managed equipment is necessary when Company detects the outage in the section which includes access line and Customer managed equipment.
4) The Customer data communications may be temporarily stopped when significant traffic congestion occurs in the Customer's communication route or when the Company judges it is necessary to do so for the maintenance of the relevant telecommunications equipment. In addition, this service may be temporarily stopped without notice.
5) The other providers VPN services may be used as a part of access service. In such cases, there may be some limitations in the available optional service or its technical specifications. The connection between Customer sites may be made in other carriers' network without passing through the core network service.
6) NTU (DTU) equipment installed in the sites in specified countries including, but not limited to, China or Vietnam should be purchased by Customer. In case of outage of the equipment 1 year after the installation, Customer needs to purchase NTU (DTU) again by Customer's own expense. In such case, local contract and local billing are applicable.
7) DA/DIA may be provided with Ether over Copper (EOC), which uses two or more access lines as one high speed access line by bundling such access lines. Company does not detect an outage which occurs on some part of access lines consisting EoC circuit. In that case, troubleshooting will begin based on the declaration by the Customer.
8) Depending on the service conditions of countries/regions, DA/DIA access section may be provided partially by wireless type access such as fixed wireless or satellite link. Since the condition of wireless communication may vary with time and place, stable bandwidth and transmission quality are not guaranteed.
9) Equipment, place and city in which access line is accommodated may change.
10) Due to tightening of regulations regarding communication on the Internet or VPN in a country/area, where there may be some actions required, requested by agency of such a country/area. The Customer may have to correspond to those requests.
11) Due to tightening of regulations regarding communication on the Internet or VPN in a country/area, although there may be a case, when circuit cannot be activated nor cannot be used by the Customer after activation, delivery related cost shall be borne by the Customer.
12) The T&Cs and important notes for DIA/BIA have effect regardless of the purpose of use. Even when Customer uses Active-Active design by combination with DA, the conditions for BIA/DIA are same as independent use.
13) Only DIA/BIA is available for Internet VPN or Internet Services, which utilizes Cisco's Dynamic Multipoint VPN (DMVPN) technique.
14) CPIA(Customer Provided Internet Access) shall not be used for Internet Services.
15) Internet VPN with MPLS interconnection (Cloud Based Internet VPN) utilizes a DMVPN controller located at NTT Communication's POP. Customer shall have a controller redundancy and order main and back up controllers.
16) Internet VPN without MPLS interconnection (CPE Based Internet VPN) places a DMVPN controller (HUB CPE) at Customer's sites. Customer shall have two HUB CPEs, main and backup controllers (controller redundancy) at their sites.

17) SLA, network quality assurance, or incident investigation and report is not available for Internet VPN or Internet Services.
18) Internet VPN group shall be made within the same region (i.e., America, EMEA and APAC) and shall not be made cross-regionally.
19) If Customer wishes to replace their existing UNO service to Internet VPN or Internet Services, Customer shall terminate the existing UNO service and place a new order for Internet VPN or Internet Services. This restriction applies to changing to/from Cloud Based Internet VPN from/to CPE Based Internet VPN.
20) In case of relocation of Customer's site, Customer shall terminate the existing site and place a new order of new site for Internet VPN or Internet Services.
21) CPE for Internet VPN or Internet Services cannot be shared with MPLS. CPE is respectively required for each Service; MPLS, Internet VPN, and Internet Services.
22) An independent VPN ID (ACG Number) will be assigned to Internet VPN without MPLS interconnection (CPE Based Internet VPN) and Internet Services. This ID is separate from the other NTT Communications MPLS circuits.
23) Internet VPN is not worked only spoke sites. Cloud Hub or Customer's Hub sites need to complete delivery before spoke sites implementation.
24) Internet VPN has a few minutes until establish tunnel of Spoke-Spoke when the communication starts first time. Sometimes Customer needs to tune their time-out value of applications.
25) In Internet VPN, if the site communication that use dynamic tunnel was nothing, the dynamic tunnel will be session timeout after a certain period of time.
26) In the case of countries or service providers which forbid the use of encrypted communication including IPsec, DIA and BIA cannot be provided.
27) Ether OAM technology is used for the circuit monitoring in Japanese internet circuit. Therefore, OAM frame spends a part of bandwidth.
28) Static public IP address that Customer get from other carrier is not allowed for Japanese internet circuit. Customer needs to get them from UNO.
29) DIA/BIA uses an unspecified number of ISPs between CPE and PE. The service cannot control which ISP to choose. The behavior of the ISP section changes at an unpredictable timing due to the usage time zone or the ISP's work. (e.g., packet loss, delay, jitter, throughput, MTU size, handling of fragmented packets, etc.)
30) If Customer uses MTU size of over 1400 byte with DIA/BIA, there is a possibility that traffic may be disrupted.
31) Customer's applications/network design such as MTU settings under Customer's responsibility should be considered for DIA/BIA, since these circuit types may be affected by 3rd party issues e.g. ISP's devices and service conditions that passes through.
32) In the case of the Customer provided internet access (CPIA), the Customer should acknowledge following notes.
    - The Customer should get a global (public) IPv4 address for CPE WAN interface from ISP carrier.
    - Also, there is a possibility that there is a long delay by combination with each ISP carrier.
    - Internet circuit is a Customer responsibility. Our operators cannot handle the issue consistently therefore there is a possibility that the trouble will become longer than ISP Bundle type.

1-3. CPE-Service (Universal One Terminal)

1) CPE Service is the service provided by the combination of following 4 menus.

1)-1 CPE Arrangement

Customer can select from the following three types of CPE Arrangement types.

CPE Arrangement Type	Service Description
Selling	- The difference with rental CPE is payment method and asset. - Customer needs to make a lump-sum payment and it is Customer's asset. - The managed menu is offered for selling type, even if it is selling type.
Rental	- Customer uses Company CPE provided through rental scheme. - Customer makes monthly payment. Company owns CPE as its asset.
Customer Arranged CPE	- Reuse of CPE provided by Customers, is possible. - There is a case that there are conditions of hardware, software, license, and contract contents.

※Manufacturer's EoL equipment or software is not acceptable. (For details of conditions, please refer to Arcstar Universal One Service Service Description.)

※Company ended Selling on February 4th, 2023, with the exception of Selling on a valid quotation made by Company on/before February 3rd, 2023.

1)-2 CPE Management Type

Customer can select from the following four types of CPE Management menu.

CPE Management Type	Service Description
Managed CPE Option #1	Managed CPE Option#1 is the CPE fully managed by Company. Design, installation, configuration change, monitoring(ping and SNMP), 1st level trouble shooting, and on-site maintenance are conducted by Company.
Managed CPE Option #2	Managed CPE Option#2 is CPE which is fully managed by Company as primary management. Customer can check the status of CPE. Design, installation, configuration change, monitoring(ping and SNMP), 1st level trouble shooting , and on-site maintenance as provided in Managed CPE Option #1 are conducted by Company, except for the following two functions: 1. Customer gets SNMP read-only access to CPE routers for status monitoring 2. Customer can execute the predefined commands (such as show command, ping, and traceroute) on CPE through Business portal (CE Commander).
Unmanaged CPE Option #1	Unmanaged CPE Option #1 is the optional menu in which Customer holds the final authority for network configuration changes. The condition to provide this option is as follows. 1. Company gets SNMP read-only access to CPE routers for status monitoring. 2. The loopback interface with global IP address (100.64.0.0/10) assigned by Company should be configured on CPE for alive monitoring and access from terminal. 3. Company asks Customer to execute some privileged commands such as shutdown/no shutdown. 4. Customer is required to setup both username and password in order for Company to remotely access to CPE (login with Read access) for monitoring/troubleshooting purposes. - Username is determined by Company and basically no change can be applied. For password, please use at least 10 or more random characters containing an uppercase letter, a lowercase letter and a number, which are less easily guessed. - Changing the password by Customer requires update on Company's database to keep remote access to CPE, for which please request by SoftMAC (2-7. SoftMAC). 5. Customer Operation Center works with Company Operation Center in real-time over the phone to troubleshoot network problems. 6. The condition for Service User arranged CPE should be also met. Please refer to "Service User Arranged CPE" of CPE Arrangement Type. 7. Configuration of parameters, including VLAN tag as specified by Company, may be required in Customer CPE. In this case, Company will notify VLAN-ID to Customer before service start date. Customer is also responsible to check the negotiation mode of the ethernet access (auto or full-duplex) and configure proper setting in CPE
Unmanaged CPE Option #2	1. Company only sends ping to WAN interface on CPE. 2. Configuration of parameters, including VLAN tag as specified by Company, may be required in Customer CPE. In this case, Company

	will notify VLAN-ID to Customer before service start date. Customer is also responsible to check the negotiation mode of the ethernet access (auto or full-duplex) and configure proper setting in CPE.

※Only Managed CPE Option #1 or Managed CPE Option #2 is available for Internet VPN or Internet Services. Unmanaged CPE Option #1 or Unmanaged CPE Option #2 is not available.

1)-3 Cisco CPE Router Type

Customer can select Chassis, modules, and software from the following three categories.

Category	Service Description
CPE Chassis	Customer can select Cisco's routers, switches, and modules from service provider's lineup. (Company's lineup may be changed without the announcement to the Customers.)
CPE Module	
CPE IOS	[IOS Version] (At the start of service) ・The latest version of IOS recommended by Cisco is basically used. ・An impact analysis on actual customer's network environment will NOT be conducted. ・Specifying IOS version by Customer is possible on condition that Company can confirm no compatibility problem nor bug. However, Company does not guarantee that there is no compatibility problem nor bug. (After the start of service) ・On operation phase after the service is launched, neither impact analysis against bug/vulnerability of Managed CPE nor proactive update of IOS version as preventive maintenance will not be conducted. Although updating IOS version will be charged to customer if requested, complimentary version update may be conducted as a part of maintenance if NTTCom determines it is necessary to solve the outage caused by bug/vulnerability, including prevention of communication trouble/outage possibly caused by such bug/vulnerability. Outage described here means the one recognized/determined by NTTCom's monitoring system. [Technology Package] ・Supported Technology Package is "IP BASE", "SEC" and "UC". ・Customer can specify another license on condition that Company can confirm no compatibility problem nor bug. However, Company does not guarantee that there is no compatibility problem nor bug.

※"CPE IOS" is applicable only for Managed CPE Option #1 or Managed CPE Option #2. With regard to Unmanaged CPE Option #1 or Unmanaged CPE Option #2, in which Customer holds the final authority for network configuration changes, IOS version and technology package shall be managed under Customer's responsibility, taking some risks into consideration (e.g., security breach caused by bugs/vulnerabilities, such as system communication jamming, unauthorized use or information leak).
※Company ended selling of UC license on October 4th, 2022.

1)-4 CPE Design

Customer can select System Design from the following list. Depending on the service, available designs are limited.

Design Item
• Static Route Design (The number of the address is not limited) ※1

• BGP Routing Design (The number of the address is not limited)	
• Tos Mapping Design	
• Access List/NAT(Static, Dynamic, PAT) Design(The number of the address is not limited) ※2	
• DHCP Relay/Server Design	
• MLPPP	
• VRRP/HSRP	
• Load sharing Design	
• Backup Design	
• SNMP Read Only	
• QoS(4Class,6Class) Design	
• LAN Routing Design(OSPF,EIGRP)	※ 1
• Multicast	
• MultiVRF	
• Jumbo Frame	
• IPSec(Except DMVPN)	
• Netflow export setting to Service User's Netflow server	
• LDP/CDP	
• RIPv1,v2	
• ECMP(Equal Cost Multi-path) for LAN	
• Syslog data export setting to Service User's Syslog server	

Default route for Internet

- MPLS (UNO L3) Dedicated Internet Access / Broadband Internet Access and Internet VPN
  - In case of no split tunnel in use, default route setting for Internet will not be implemented in CPEs applied on/after August 1st, 2020. If there is traffic necessary in terms of operation/monitoring purposes for customer and/or ISP/outsourcing company arranged by customer, please specify traffic information upon delivery. In exception with Internet line procured by customer, default route setting will be conducted if requested by customer, as long as ISP or outsourcing company arranged by customer does not disclose information necessary for operation/monitoring purposes. There may be some risks of security breach, such as system communication jamming, unauthorized use or information leak, by abused vulnerability of communicable port from external Internet.
  - There is a case where default route has been set despite of no split tunnel in use in existing CPEs applied before August 1st, 2020. There may be some risks of security breach, such as system communication jamming, unauthorized use or information leak, by abused vulnerability of communicable port from external Internet. ACL setting will be configured by modification order as requested.
- Internet Services
  - Default route setting for Internet will be implemented in CPEs.

※2 Access Control List(ACL) setting

- MPLS(UNO L3) Dedicated Access
  - Customer should apply for Access Control List(ACL) setting to CPE. Unless requested by customer, ACL setting will not be configured and all packets passing through CPE will be allowed, though it is recommended to apply for ACL setting.
  - In case of monitoring by customer's SNMP server, please specify traffic information for SNMP individual ACL setting, which allows traffic only to/from customer's SNMP server. SNMP write permission will not be set up. For SNMP community name, please use at least 10 or more random characters containing an uppercase letter, a lowercase letter and a number, which are less easily guessed.

- MPLS (UNO L3) Dedicated Internet Access / Broadband Internet Access and Internet VPN
  - Customer shall apply for Access Control List(ACL) setting to CPE. Unless requested by customer, deny all packets passing through CPE from external Internet by WAN I/F ACL, except following traffics, for CPEs applied on/after August 1st, 2020:
    A. TCP returning traffic in case of split tunnel in use (TCP Established)
    B. Traffic necessary for UNO service offering
    C. IPsec traffic to UNO Network facility (IPSec GW)

  If there is traffic necessary in terms of operation/monitoring purposes for customer and/or ISP/outsourcing company arranged by customer, please specify traffic information upon delivery. In case of monitoring by customer's SNMP server, please specify traffic information for SNMP individual ACL setting, which allows traffic only to/from customer's SNMP server and SNMP write permission will not be set up. For SNMP community name, please use at least 10 or more random characters containing an uppercase letter, a lowercase letter and a number, which are less easily guessed.
  - For CPEs applied before August 1st, 2020, ACL was not configured unless requested by customer. Depending on combination with other configurations of CPE, there may be some risks of security breach, such as system communication jamming, unauthorized use, or information leak, by abused vulnerability of communicable port from external Internet. ACL setting will be configured by modification order as requested.
- Internet Services
  - Only ACL setting requested by customer will be configured to customer's Internet communication. If not requested, all packets passing through CPE from external Internet will not be denied.

2) Off-site maintenance

2)-1 Company provides 24x7 monitoring, outage reception, outage isolation, outage recovery work and outage recovery notification. Company conducts monitoring using Ping.

2)-2 Maintenance is provided on a 24 hours / 365 days basis.

2-3) CPE remote maintenance is performed via WAN circuit. In the case of outage, Company accesses to CPE via WAN circuit and conducts equipment status checking and isolation. (*)(For details of conditions, please refer to Arcstar Universal One Service Service Description.)

*OOB access for CPE remote maintenance is no longer required effective November 21, 2023.

- Handling of existing OOB access and OOB equipment is as follows:
- Customer may cancel existing OOB access prepared by Customer.
- Company will not remove specifically existing OOB equipment, to be collected during CPE removal work.
- Company will not conduct replacement of existing OOB equipment.
- Regardless of OOB access/equipment type (PSTN/BB/4G) or built-in/external type, reuse of existing OOB equipment (renewal/move of CPE, etc.) is not acceptable.

3) On-site maintenance

Maintenance engineers are sent to an installation site of CPE to implement troubleshooting operations.

3)-1 Maintenance Hours

Maintenance hours is to be "a" basically, but it is to be "b" if 24 hours / 365 days on-site Maintenance service cannot be available.

a. 24 hours / 365 days
b. During business hours (9:00-17:00 on weekday except the national holidays in the relevant countries or areas where CPE is installed.)

3)-2 Operations

The specific work contents are as follows.

- Maintenance engineers aim to arrive at the outage site after the Company judges the necessity of on-site work after the outage site is identified through offsite maintenance.
- Securing substitute CPE if necessary.
- Replacing of a broken equipment with a substitute equipment. Re-setup and testing to confirm normal operations are conducted.

<<Notes>>

- Depending on the country/area where the CPE is installed, the above conditions may not apply.
- Maintenance personnel of the manufacturer, etc., contracted by the Company may be sent to the site in the event of an outage.
- Periodical checking of CPE and power off/on work in the event of power failure at the Customer premise are not included.

- In order to enable router setup / monitoring, Company will set up the router to transit the packets with the designated IP address / port number.
- Router ID and its password will not be provided to the Customer. (The Customer cannot change the router set up.)
- 24 hours / 365 days on-site maintenance service is available only when the engineers can access the Customer premise 24 hours a day.
- Maintenance coverage is based on the applicable Service Description document by each CPE manufacturer. Any accessories or expendable parts are not covered under such Services Description, which requires customers to procure/arrange and furnish the spares

*The conditions differ depending on "CPE Management Type".

4) Others

4)-1 Managed CPE Option #1 and Managed CPE Option #2 are available only when CPE Arrangement Type is Selling or Rental or Customer Arranged CPE which meet conditions of company designated CPE Chassis, CPE Module, CPE IOS and CPE Design menu.

4)-2 In case Customer applies DIA or BIA, Customer shall apply Managed CPE Option #1 or Managed CPE Option #2.

4)-3 Both DIA and BIA are Internet lines. It is imperative for customer to implement security measures for their network besides this service, which does not provide security functions. This will also be applied when Customer Provided Internet Access line (CPIA) is in use for MPLS and Internet VPN.

4)-4 In the circumstances specified below, a separate fee is charged.

a. In case design (change), installation, testing, etc., are newly required as the result of changes in the CPE or network configuration after the start of CPE Service.

b. In case Customer requests for upgrades of the CPE IOS.

4)-5 In the event setup changes, etc., are made by the Customer (other than the installation and maintenance work by the Company), maintenance under this service is not provided, and service maintenance and outage recovery cannot be guaranteed.

4)-6 The Customer is requested to notify the Company of the following events:

a. Installation work which causes blackout of power supply to the CPE

b. Installation work which causes the disconnection of any cables linking the CPE and the Customer facilities or cuts the power of the HUB connected via such cables

4)-7 Company may ask the Customer to undertake simple work for prompt outage recovery.

4)-8 When CPE Service is provided and the Customer installs routers other than the relevant routers within the Customer network, the Customer is requested to provide NTT Com with design information of such routers.

4)-9 This service does not include the site survey. Site survey is provided for extra charge.

4)-10 The service conditions may differ if CPE service is connected with the access line provided by the interconnection with other carrier.

4)-11 In case of using NNI service, Customer basically needs to use Universal One Terminal.

4)-12 If Customer requests to use Customer Router without Universal One Terminal, Customer Router can be acceptable under the following conditions:

a. Customers allow NTT to monitor Customer CPE through sending Ping to router's WAN IF. (The above is not acceptable for "Unmanaged CPE Option #3")

b. Service will commence after ping test using tester on Customer site conducted by service provider is completed. Maintenance will start after NOC confirms ping availability from carrier equipment to Customer router.

c. Maintenance can only be started after necessary information is provided by Customer to sales team 10 days before desired service start date, and Customer has to request to Company on their own to request to NOC for Ping confirmation after CPE installation.

d. In case of trouble, Customer will be required to support troubleshooting between circuit and router.

e. In case that router repair/replacement will be required, Customers will be required to repair/replace router by themselves.

f. There will be possibility that the Time to Repair will be prolonged.

g. In case on-site dispatch of technician is required due to Customer's own reasons during testing and troubleshooting, for circuit/router installation and maintenance, the on-site fee will be beard by Customer.

4)-13 If equipment and software which are used for CPE service are to be EoL, Company may ask Customers to replace them.

4)-14 In case CPE arrangement type is "Rental", Customers shall return the CPE when the CPE service is terminated.

a. UNO Factory shall contact the Customer for scheduling a pick-up date and conduct all the arrangements in regards to collecting CPE, including having a field engineer to conduct actual physical work (removing CPE from the rack, pulling the cable off, packing CPE) as well as to coordinate a transportation company for collection.

b. UNO Factory shall deem CPE to be lost by the Customer if no contacts are made by the Customer over the period of sixty [60] calendar days from the starting date of calculation mentioned above, even though the Customer did find the CPE later on. The Customer shall have responsibilities to dispose the CPE by themselves.

4)-15 If rental CPE (including accessories, etc.) is lost due to the Customer's fault, UNO Factory shall charge of any necessary fees for installation, etc. as a tender.

a. As for equipment fee in tender, 6 months of Service Charge (UO Terminal) will be charged as a standard.

b. The Tender is charged for the lost CPE and if the Customer requests for continuous use of the service, the new order for CPE should be placed to UNO Factory, in the same manner as changing equipment type.

4)-16 End of new order for voice modules was Oct. 4, 2022, in accordance with EoS of OS versions with H.323 call control function, determined by the manufacturer. End of use of existing modules is Sept. 30, 2023, which is the last available date of bug modification program for manufacturer's recommending OS versions' vulnerability/security. After this date, neither setting change nor troubleshooting with regard to the voice function will not be available. Further, the voice function becomes unavailable without notice upon version upgrade as a measure to solve manufacturer-depended failures.

2. Optional Service

NTT Communications makes no guarantees concerning the accuracy of all the data provided under the Service. The provided data may be lost, shows unexpected results or temporarily unavailable due to system maintenance or anything else that affects proper function of the system. NTT Communications shall not be liable to the recovery of lost data, unavailable time including any loss caused by it, nor anything else under any circumstances. NTT Communications does not provide any outage notice, outage report, procedure manual nor work report.

2-1. Priority Control Service (MPLS)

1) Priority Control Service is available only for Dedicated Access.
2) Priority Control Service cannot be provided if using TOS5 for data or using TOS 6 or 7 for the highest priority data.
3) Customer shall assign IP Precedence bits per IP packet.
4) Service conditions for 4 Class are as follows.
   4)-1 4 classes (Voice Class, Premium1 Class, Premium2 Class, Standard Class) can be provided.
   4)-2 The available bandwidth for this service is as follows.

For data only purposes	64 kbps or higher
For voice only or data and voice purposes	128 kbps or higher

   (Note) In case of Ethernet access line, available bandwidth is from 1 Mbps or higher
   4)-3 In case this service is used for voice at 768 kbps or less, CPE Service is need to be applied.
5) Service conditions for 6 Class are as follow.
   5)-1 6 classes (Voice Class, Premium 1 Class, Premium 2 Class, Premium 3 Class, Premium 4 Class, Standard Class) can be provided.
   5)-2 The available bandwidth for this service is 1Mbps or higher
6) Periodical monitoring, quality management, and quality assurance which is specific to Priority Control Service are not provided.
7) In case the traffic exceeding the contracted bandwidth flows to Customer's circuit, the prioritized packet including voice class packet may be dropped by the equipment specification even if the traffic of those prioritized packet is within the contracted bandwidth.
8) Allocation for Voice class is recommended to be up to 33% of contract bandwidth. Otherwise, packet may

be dropped by the equipment specification even if the traffic of those prioritized packet is within the contracted bandwidth.

2-2. Priority Control Service (Ethernet)

1) Priority Control Service (L2) is the service that transfers the frame according to the priority order indicated by the value of ToS (Type of Service) or CoS (Class of Service) and the QoS mapping in L2 VPN backbone given by Customer.

ToS	This service is the service that transfers the IP packet according to the priority given per IP packet by the Customer.
CoS	This service is the service that transfers the frame according to the priority designated by the Customer in CoS field in case the frame is tagged with IEEE802.1q VLAN.

2) Customer shall order either of "ToS", "CoS" or "None" for all the sites if Customer applies this service.
3) 4 classes (Voice Class, Premium1 Class, Premium2 Class, and Standard Class) can be provided.
4) Customer shall assign IP Precedence bits or CoS bits per Ethernet frame.
5) Periodical monitoring, quality control and quality guarantee are not provided for this service.
6) In case the traffic exceeding the contracted bandwidth flows to Customer's circuit, the prioritized packet including voice class packet may be dropped by the equipment specification even if those prioritized packet traffic is within the contracted bandwidth.

2-3. Multi VRF (MPLS)

1) The port set on each VPN is called "VRF Port", and each VRF Port shall belong to different Universal One Groups. The group bundling the VRF Ports is called "Port Group".
2) Customers are to select the Port Group speed and the VRF Port speed.
3) Each VRF Port speed shall be set on the condition that the total speed of each VRF Port does not exceed the Port Group speed.
4) Communication will not be affected by the traffic of other VRF Ports in the same Port Group. However, even if there is unused bandwidth within the Port Group speed, communication exceeding the predefined VRF Port speed is not possible.
5) Priority Control Service 4 Class and 6 Class can be provided per VRF Port, but voice service is not available.
6) The available access types are STM and Ethernet.
7) The number of VRF Ports that can be set per Port Group is from two (2) to ten (10).
8) Contract is per Port Group.
9) As charges are set per Port Group, billing per VRF Port is not available.
10) This service cannot be provided together with some optional services.
11) Provision of service to the Customer starts upon successful completion of implementation test defined by Company.
12) Maintenance will be done per Universal One Group which each VRF Ports belong to. Maintenance for communication among Universal One Groups is not available.

2-4. Multicast

2-4-1. Multicast (MPLS)

1) This service provides multicast function within L3 VPN network (up to Managed CPE), but it does not assure the multicast communication between source terminal and receiver terminal. Required application and equipment (LAN, server, client etc.) supporting multicast communication must be prepared (including design and configuration) by Customer.
2) Multicast is not available when Customer manages CE router (Unmanaged CPE).
3) The multicast design including application and the equipment (router, IOS, platform, memory, PC etc,) configuration in the Customer premises must be made by Customer.
4) This service is available only for Dedicated Access.
5) When the other providers' VPN services are used as a part of access service, multicast is not available.
6) PIM (Sparse-Mode) is available as multicast protocol (PIM mode).
7) Rendezvous Point (RP) is provided at Managed CPE within VPN network. BSR is recommended as RP selection method, but auto-RP is also available.
8) Regarding multicast group, the maximum number of mroute (multicast route) is set at 65.
9) To prevent large data packet from flowing into the backbone network due to micro burst, multicast transmission rate of the source side is restricted at 2M (2,000,000bps). Customer should configure and manage the application and the equipment of Multicast in accordance with this threshold.
10) The service is deemed as available to Customer when PIM neighbor is established between Provided Router (PE) and CPE.
11) In case of trouble isolation, Company is considered to have met its responsibilities when followings are verified: appropriate Multicast setting and confirmation on the establishment of PIM neighbor between PE

and CPE.

12) Trouble isolation for application and equipment (LAN, Server, Client etc.) using multicast communication must be conducted by Customer.

2-4-2. Multicast (Ethernet)

1) Multicast, broadcast and/or Unknown unicast traffic including, without limitation, video delivery or file transfer that causes heavy traffic continuously cannot be used.
2) If the use of multicast is detected within the network, the service provision for Customer may either be suspended or terminated

2-5. Traffic Report Service[Basic],[COS Performance],[Netflow]

1) ID registration on the NTT communications Business Portal shall be required for the use of this function.
2) Traffic Report Service is the service to report traffic status of Customer networks and the performance of the routers (CE) at Customer's site. It needs customer application to order COS performance and Netflow by circuit.
3) Refer Arcstar Network View –Reports user guide as user manual.

2-6. SoftMAC

1) ID registration on the NTT communications Business Portal shall be required for the use of this function.
2) We accept simple setting change requested by our customer via business portal. SoftMAC is a service to provide simple setting change promptly to our customer based on their requests. Because of the reason, we simplify the ordering process as much as possible we can. Please be noted the following points to utilize functions.
   - Simple setting changes will be carried out based on understanding of the nature of the service and technical aspects by our customer. Also we need to check customers' settings have no discrepancy with the contents of the applications. We will conduct an operation under the agreement on both sides.
   - In case of occurring malfunctions by operating simple change setting, NTT Communications shall not be liable to any loss nor anything else caused by those errors or malfunctions. We will place back the setting to the previous conditions upon customer's request. However, it does not guarantee solving the problems caused by malfunctions.
   - There may be a time when simple setting changes cannot be requested due to system maintenance or anything else that affects proper function of the system. NTT Communications shall not be liable to unavailable time including any loss caused by it nor anything else under any circumstances.
   - If requested by Customer, a four-hour window can be specified for simple setting change. Company will conduct the setting change work at any time during the specified time frame. However, the work may not be able to be carried out within the time frame specified by Customer.
   - Company may require Customer to do the remote hand work (including turning CPE on or off, or plugging or unplugging cables, etc.) or the confirmation (checking status of lamps related to CPE) during remote configuration change works by Company.
   - Company does not provide any setting change (the setting change to CPE that has no redundant configuration and can only be connected through a single circuit, or the setting change that has a high possibility of stopping CPE.) which has a high possibility for making communications via WAN circuit(s) unavailable, except in case that Customer do the remote hand work or the confirmation.
   - In case that doing the remote hand work or the confirmation is required for Customer, Company shall not be liable for any damage or detriment to Customer and Third party arising from Customer's omission of doing the remote hand work or the confirmation.
3) This service is only available in English.

2-7. Value Added Services (VAS)

2-7-1. General

1) Customer can use virtual appliance functions which utilize NFV technology provided on LCNC (Local Cloud Network Center; Our facilities with virtual appliance functions) without customer on-premise devices.
2) The following terms are necessary to use this service.
   a. Contract to Arcstar Universal One L3 service for at least 1 circuit.
   b. ID registration from NTT Communications Business Portal is necessary to this service.
3) The Customer can activate/change/deactivate VAS service via VAS portal. VAS Portal can be used as a part of NTT Communications Business Portal. VAS Portal supports English and Japanese.
4) VAS portal administrator will be the same user of NTT Communications Business Portal administrator.
5) Customer can subscribe VAS service by activating/changing/deactivating the services via VAS Portal (self-service). Also, like the circuit services, NTT Communications can activate/change/deactivate VAS service

based on the service order form signed by the customer (service order). Customer can freely choose both ways. (Customer can choose both ways multiple times.)

6) Customer can select from "Pay-per-Use Model", service period of 1 month, 1 day, or 1 hour per unit without advance payment or minimum service period, or "Fixed-Term Model", service period is fixed 1 year, 2 years, or 3 years. (Service periods for part of optional services are included.) For portal (self-service) activation, all service period stated above can be designated. However, for SO-based activation (service order), service period of 1day and 1hour of "Pay-per-Use Model" cannot be designated.
7) Penalty charge of remaining service period will be charged in case of deactivation before service period for "Fixed-Term Model". If the remaining period is less than 1 month, penalty charges equivalent to that remaining period will be charged totally with the last service charges.
8) Customer provided charges will be defined from the price list separately. NTT Communications may change the price list without any notifications in advance due to license fees and foreign exchange fluctuations. (This is exceptional for customer who have different agreement prior with NTT Communications)
9) Customer will be charged from the time service has been activated. The date and time of service activation/deactivation is recorded and calculated based on Coordinated Universal Time. Service charges will be included in the billing of the activated circuits. However, if there is a request in advance, a specific or all of the service charges can be integrated into a specific circuit charge in the same VPN group. If this service is activated before the billing of the circuit has started, the service charges may be charged together with the initial charges of the circuit.
10) If circuits which using VAS services are deactivated, service charges will be integrated into a different circuit in the same site or the same LCNC. If all circuits on the same site or LCNC had been deactivated, service charges will be integrated into different circuit in the same region and into a different circuit in the same VPN group if all circuits in the same region had been deactivated. If there is no circuit in the VPN group to integrate the service charges, VAS services may be forced to deactivate.
11) Due to regulations in some countries, service charges cannot be billed into the corresponding circuit charges. In this case, another circuit must be specified before the service activation. VAS service may be forced to deactivate if no circuits are specified.
12) Following terms are not supported.
    a. From Non Arcstar Universal One MPLS service
    b. From different VPN group
13) Inquiries (regarding to service specification, VAS Portal usage) will be supported by Business portal helpdesk and GOC, Global Operation Center.
14) 24 hours support which NTT Communications provide for this service does not include end users. Customer with service contract is responsible for any support for end users.
15) This service may be changed without notifications in advance. (This includes software updates, deleting part of functions, etc.)
16) Charges will be exempted for one month from initial service activation as a free trial period
    Please use the free trial before regular operations of the service, e.g. service functional test, performance tests, prior preparations, and etc. Optional services such as IPS and URL Filtering are also the target of free trial.

16)-1 Unit and Term for free trial

Unit applied for the free trial differs between each VAS service as below.

Cloud-Based Secure Web Gateway, Cloud-Based SSL VPN, Cloud-Based IPSEC VPN Gateway:

One month from initial activation day of each service per VPN Group

Cloud-Based Application Acceleration Service:

One month from initial activation day of each circuit

"One month": When activated in the beginning of the month, until the end of the same month. When activated in the day except for the beginning of the month, until the day before the corresponding day of the next month. However, if there is no corresponding day in the next month, it will be until the end of the next month.

For example, if activated in Nov. 1st, it will be until Nov. 30th. If activated in Nov. 15th, it will be until Dec. 14th. If activated in Jan. 31st, 2017, it will be until Feb. 28th, 2017.

16)-2 Conditions for free trial

If services are activated under the conditions below, free trial will be applied.

Services will be charged when below conditions are not met even if during free trial period.

- Services are activated as "Pay-per-Use Model (1 month, 1 day, or 1 hour)"
  (Fixed-Term Model (1 year, 2 years, or 3 years) is not subject to the free trial.)
  Besides gateways, contract terms for optional services, e.g. IPS, per site charges, SSL VPN users can be setup from VAS Portal. Please be careful that these contract terms must also be Pay-per-Use Model.

- During free trial period, you can change plans, e.g. 10M to 100M, number of SSL VPN users, and deactivate/re-activate services.

16)-3 Notices

- Expiration date of free trial will not be notified to the Customer.
- There will be charges when free trial period ends after continuous usage.
  If services are going to be used continuously, changing contract terms to Fixed-Term Model (1 year, 2 years, or 3 years) is recommended, which is relatively low in price.
- When contracts terms are changed from Pay-per-Use Model to Fixed-Term Model, there will be charges from the day it was changed.
- When activating/deactivating services from VAS Portal, notification messages confirming charges or penalty charges will be shown. However, if conditions of free trial are applied, charges will be exempted, so please continue the service activation/deactivation process.

17) In the case of countries or service providers which forbid the use of encrypted communication including https, TLS/SSL and IPsec, Cloud-Based Secure Web Gateway (CBSWG), Cloud-Based IPSEC VPN Gateway (CBIPSEC), Cloud-Based SSL VPN (CBSSL) cannot be provided.

2-7-2. Cloud-Based Secure Web Gateway (CBSWG)

1) This service provides Cloud-based Internet breakout from Customer VPN to the Internet with secure gateway.
2) BY choosing a circuit to activate CBSWG, the gateway of LCNC which corresponds to the circuit can be used.
3) Gateway service charges will be applied to the circuit which CBSWG is activated first, and per site charges will be applied to each circuit using CBSWG. Circuits can be chosen from the VAS Portal.
4) 7 standard plans (5M, 10M, 20M, 50M, 100M, 150M, and 200M) are available. Plans can be chosen according to Firewall throughput, maximum number of rules, maximum number of sessions, etc.
5) IPS and URL Filtering can be used as optional services. Also, IPS includes event notifications corresponding to the security levels the customer set up.
6) Firewall and IPS has log transfer feature. The traffic information that passed through the firewall, and the logs related to security incidents detected by IPS could be transferred to the designated log server installed in the relevant VPN network
7) Internet connectivity charges of CBSWG are included. Customer-used Internet connection charges are not included.
8) IP address range of /29 and 1 AS number is necessary to activate CBSWG. These items must be unique in Customer's VPN.
9) When using CBSWG from a specific site, the nearest Secure Web Gateway set up in the same region will be chosen automatically. If there are no gateways in the same region, this service cannot be used from that site.
10) Redundant gateway model can be designed by activating 2 gateways in the same region. Redundant configuration can be between these 2 form: (1) Multiple-primary gateway configuration: multiple primary gateways (gateways activated for usual use) activated within the same region. (2) Primary gateway/ backup gateway configuration: within the same region, one primary gateway (for main usage) and one backup gateway (will only be used when primary gateway is down) activated respectively. To make a complete backup during breakdown, choosing the same plans and optional services (IPS and URL Filtering) are recommended.
11) Communications are managed by default-route routing function. If default-route is set up in Customer VPN, CBSWG may be affected.
12) Security policies can be set up or changed via VAS Portal. Consultation or management support is not included.
13) We will not owe any responsibilities for damages/failures/disadvantages caused by security policies the Customer set up.
14) Due to legal reasons, this service cannot be provided in mainland China.

2-7-3. Application Acceleration Service

2-7-3-1. Cloud-Based Application Acceleration Service (CBAAS)

1) This service provides application acceleration to optimize network traffic in backbone portion (between LCNCs) of customer VPN without customer on-premise devices. The application traffic, between chosen circuits, will be accelerated in full mesh.
2) Customer can choose circuits to apply this service. The minimum menu (2M, 5M, 10M, 20M, 30M, 50M, 100M, 150M, 200M, and 500M) which does not goes under the circuit bandwidth will be automatically

applied.
3) If the circuit bandwidth is accelerated, the menus of this service will also be changed automatically. If the circuit bandwidth is decelerated, the menus of this service will not be changed.
4) Optimized network traffics will be supported up to 500 Mbps per LCNC. Traffics exceeding 500 Mbps will not be optimized.
5) The total circuit bandwidths connected to the same LCNC must be below 500 Mbps.
6) This service may not be fully effective if the round trip delay between Customer site and LCNC exceeds 50 msec.
7) Encrypted traffics, real-time traffics, and Internet-bound traffics will not be accelerated. Not all applications are guaranteed to be accelerated.
8) If the circuit is already congested, the performance of CBAAS may not be fully effective. In this case, upgrading the bandwidth is recommended.
9) SLA of transmission delay time, data transmission rate and jitter are not applied between through otherwise agreed by SLA of Arcstar Universal One Service.

2-7-3-2. On-Premise Application Acceleration Service Hybrid Type

1) CPE service specified by Company (hereinafter referred to as "Specified CPE") shall be provided for Hybrid Type which enables application to accelerate between Specified CPA and Access Points opposite Circuit site.
2) Terms for On-Premise Application Acceleration Service are in addition the Cloud-Based Application Acceleration terms which also apply to On-Premise Application Acceleration unless otherwise noted. But the type of contract period shall be Annual contract and items shall be 2Mb/s, 5Mb/s, 10Mb/s, 20Mb/s or 50Mb/s.
3) Type of Specified CPE shall be "Selling" and "Managed CPE". So to use this service, the customer has to purchase the Specified CPE and choose CPE Managed option #1 or #2 for 1 year, 2 years and 3 years contract.
4) Early termination penalties for the On-Premise Application Acceleration service will be waived as long as the upgraded or extended On-Premise Application Acceleration service has a service period greater than or equal to the remaining service period of the current On-Premise Application Acceleration service.
5) Early termination penalties for the Cloud-Based Application Acceleration service will be waived in the case of an upgrade to On-Premise Application Acceleration if the following conditions are met:

- New On-Premise Application Acceleration service must be for the same customer site that has existing Cloud-Based Application Acceleration service.
- Service period of new On-Premise Application Acceleration must be greater to remaining service period of replaced Cloud-Based Application Acceleration service.
- Service period of new On-Premise Application Acceleration must be a minimum of 1 year.

2-7-4. Cloud-Based SSL VPN (CBSSL)

1) SSL VPN is a remote access VPN which uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security), an encrypted algorism for Web browsers. This service provides secure remote access between the Internet to Customer VPN by using PCs and smart devices.
2) By choosing a circuit to activate CBSSL, the gateway of LCNC which corresponds to the circuit can be used. SSL VPN user ID can be registered from the Business Portal.
3) Internet connectivity charges of CBSSL are included. Customer-used Internet connection charges are not included.
4) The maximum number of users per SSL VPN Gateway is 1,000 users. The total users are the sum of Active users (Related to CBSSL service period) and Monthly users (Not related to CBSSL service period).
5) Service charges are calculated from the number of users which accessed the SSL VPN gateway per month. Since the number of users is counted based on the unique login IDs, so please note that if you connect remotely after changing a login ID, the system will recognize the former ID and the later ID as separate an user account respectively.
6) Split tunneling and host checker is available as optional services. These options are applied to all users.
7) One Realm and one URL (sign-in URL) are used regardless of the number of SSL VPN gateways. During service subscription, the Customer specifies a Realm for user authentication. The Realm will be registered in the system and validated. Also, URL (sign-in URL) to access SSL VPN gateway will be given out when CBSSL is activated.
8) If there are multiple SSL VPN gateways, SSL VPN gateway which is the nearest to the remote access site will be connected. We can achieve redundant configuration by configuring multiple SSL VPN gateways in the same VPN group. Redundant configuration can be between these 2 forms. (1) Multiple primary gateway configuration: activate multiple primary gateways (gateways activated for usual use) in the same VPN group, (2) Primary gateway/ backup gateway configuration: Activating primary gateway (for main usage) and backup gateway (will only be used when primary gateway is down) respectively in the same VPN Group.

a. In (1) Multiple Primary Gateway Configurations", you can specify option service and number of users for each primary gateway. However, if you want to have complete backup when a failure occurs, we recommend you to specify the same optional service and specify the number of users who are supposed to access on the backup side.
b. In "(2) Primary Gateway / Backup Gateway Configuration", the option service specified by the primary gateway and its setting are automatically applied to the backup gateway. Although specifying the number of users is unnecessary for the backup gateway, the number of concurrent connections is not guaranteed when switching to the backup gateway. In order to guarantee the number of concurrent connections, it is necessary to use the configuration of (1).

9) As mentioned in the previous section "(1) Multiple Primary Gateway Configuration", When using the SSL VPN gateway from a certain Internet location, the nearest SSL VPN gateway installed in the same VPN group is automatically selected.
10) Radius authentication is included as a standard service of CBSSL authentication. Not just the registered maximum users, but also address ranges including 8 IP addresses must be assigned.

Ex) 150 users -> 158 IP addresses -> /24 (256 IP addresses)

This address range must be unique in Customer network.

11) The number of users which can simultaneously access a certain gateway is the upper limit of the maximum number of registered users. Access which exceeds this will be denied. Also, even if there are multiple gateways, users will not be transferred to other gateways.

2-7-5. Cloud-Based IPSEC VPN Gateway (CBIPSEC)

1) This service provides gateways to establish IPSEC tunnels to access Customer network from third-party services in the Internet or from IPSEC devices.
2) Internet connectivity charges of CBIPSEC are included. Internet connections to Customer environment are not included.
3) By choosing circuits to activate CBIPSEC, the LCNC gateway corresponding to the chosen circuits can be used.
4) The maximum number of tunnels per LCNC is 10.
5) The throughput of each tunnel must be chosen from the bandwidth menu (2M, 5M, 10M, 20M, 30M, 40M, 50M and 100M※). The communication quality would be provided as best effort within the upper limit of the chosen bandwidth. (※It cannot be selected in South America Region.)
6) This service provides gateways which terminates IPSEC tunnels. Customer must setup CPE terminal devices in Customer sites. Furthermore, routing protocols between CBIPEC and CPE terminal device in Customer network only supports static routing.
7) Tunnels which are terminated in each LCNC are mapped as a part of the Customer's VPN and /30 network address will be delivered to Customer VPN.
8) If Customer uses MTU size of over 1400 byte, there is a possibility that traffic may be disrupted.
9) Customer's applications/Network design such as MTU settings under customer's responsibility should be considered for CBIPSEC, since this service may be affected by 3rd party issues e.g. ISP's devices and service conditions that passed through.

2-7-6. Cloud based SteelHead Appliance type service (CBSH-A)

1) By connecting CBSH-A to the VPN service provided by the service provider, this service provides the following functions to improve the performance of Application.

-Data compression/Reduction
-Cache
-Speed up TCP communication
-Speed up application communication (CIFS, HTTP etc.)

No SLA will be provided to guarantee the performance of these functions.

2) CBSH-A will be provided by the service provider.
3) The product type of CBSH-A to be provided is limited to the product specified by the service provider.
4) This service will be prepared to the CPE management service applied CPE.
5) It is assumed that CBSH-A and CPE are directly connected by cable or connected by other equipment to which service provider provided management service is applied.
6) Depending on the configuration, a CBSH-A off-site maintenance VPN port is required.
7) If there is a change in existing equipment, etc. due to the provision of services, additional costs will be incurred.

8) If there is a change in CBSH-A or network configuration after the start of service provision, and a new design (change), construction, or testing is required, additional costs will be incurred.
9) If the version changes of RiOS (RiOS Riverbed optimization system software) is to be performed after the start of service provision, it will be separately charged. If the version of RiOS is changed due to a bug, it will be handled free of charge as a part of operation.
10) If the setting of CBSH-A is changed by the customer, by customer's own judgement, this service will not be capable to cover by the maintenance, which will be not guaranteed its failure restoration.
11) CBSH-A cannot be monitored or controlled by a customer-owned monitoring device.
12) If customer is performing any insite work that affects the CBSH-A as followed, please inform the service provider in advance.
    a. Construction where power supply interruption occurs to CBSH-A
    b. Construction work that occurs when the cable connecting CBSH-A and the customer's equipment is disconnected and the HUB connected via the cable is powered off
13) Indoor wiring, such as cables and adapters, for connecting this device to customer-owned equipment is not included, so customers should prepare it. In addition, customers should prepare installation environment equipment such as power supply and air conditioning.
14) Select the line of the site to which you want to apply this service. For each selected line, select the menu (2M, 6M, 10M, 20M, 30M, 50M, 100M, 200M, 500M, 1G) with the minimum bandwidth that does not fall below the line bandwidth.
15) In case the circuit bandwidth has been upgraded, and its circuit bandwidth after upgrade is greater than the bandwidth of the installed CBSH-A, CBSH-A will also need to be upgraded. Please note that it does not automatically change. No downgrade service is available.
16) If the port at the customer site is already in congestion, application acceleration performance may not be improved sufficiently. In that case, it is recommended to upgrade the circuit bandwidth.

17) -1 Off-site maintenance
-At the Arcstar Network Operations Center, etc., perform continuous CBSH-A fault monitoring, fault acceptance, fault isolation, fault recovery measures, vendor coordination, and recovery communications.
-The monitoring method of CBSH-A is response confirmation by Ping.
-Monitoring and fault acceptance of CBSH-A will be conducted constantly (24 hours / 365 days).
-The CBSH-A Admin password will not be notified to customers.
(Customer cannot change the settings.)
- Read-Only account privileges will be provided to the customers.

17) -2 Hardware maintenance
Hardware maintenance will be provided according to the contents of the contract with the customer. Hardware maintenance is carried out after fault isolation between service providers and vendors.
After contacting the vendor from the service provider, an engineer from the vendor will be onsite to the customer's site with new device (on-site maintenance). Alternatively, after contacting the vendor from the service provider, the vendor will ship the new device to the customer. (First Out Send Back)
The onsite time for on-site maintenance may be prolonged because it will change significantly depending on the location of the customer's site and the status of equipment arrangements.

<< Contents of Hardware Maintenance Tasks >>
The specific tasks of hardware maintenance are as follows.
-In the case of hardware failure, after the service provider exchanges equipment and sets the IP address, the establishment of communication between the service provider's network operation center and CBSH-A will be checked, After the confirmation, and the latest configuration has been installed, operation will be restored.

<< Cautions >>
-Device replacement will be conducted once the device vender has determined it physical failure.
-Engineers dispatched at the time of failure will be maintenance engineers such as commissioned by the service provider.
-Customers might be asked by service provider to do simple work for quick recovery from failure, so please cooperate in advance.
-Regular inspection of CBSH-A and device power off / on at during and after the power outage at customer

site, are not included.
-The 24-hour / 365-day maintenance period requires that a 24-hour reception system is in place at the customer's home.

17) -3 CBSH-A design and installation
CBSH-A will provide the configuration creation support based on the basic design which was provided by customer. CIF will be used to inform the basic design. Customer onsite for meeting is not included in the service.
17) -4 Service provision start conditions
Service provision start is after when the introduction test is completed by the provider. Application testing after the implementation test is completed will be the customer's responsibility.

2-8. CE Commander

1) CE Commander allows Customer to login and execute command to their NTT managed CPE via NTT Communications business portal to see the real time status.
2) CE Commander is provided to Managed CPE option #2.
3) CE Commander is provided on the web.
4) ID of Business portal is required to use the service.
5) Data is displayed only in English.
6) CE Commander supports UNO standard CPE chassis and IOS only.
7) Set of executable commands is defined by Cisco and the list changes without a prior notice. Some information about password and management cannot be shown.
8) Inquiry about output of command cannot be accepted.
   Inquiry about how to use Cisco commands and the meaning of commands cannot be accepted.
   Inquiry about configuration/design policy and routing cannot be accepted.
9) Maintenance request based on the output of command cannot be accepted. (Trouble shooting is conducted based on the Arcstar standard.

2-9. Multi-Cloud Connect

1) This service is the Arcstar Universal One option service and provides the VPN connectivity to Cloud Service Provider's cloud service from users' VPN.
2) Users must contract the Cloud Service Provider's cloud service separately.
3) The service start date is when NTT Communications confirms the connectivity between VPN and Cloud service is good in the cut-over date.
4) NTT Communications monitors liveliness of the network segments only. When it is suspected any trouble happens in the Cloud Service Provider's segment, it is users' responsibility to escalate to the Cloud Service Provider.
5) Following terms are necessary to use this service.
   i. Contract to Arcstar Universal One L3 service for at least one circuit
6) Minimum contractual period is one month.
7) Penalty charge of remaining service period will be charged in case of deactivation before service period or change of service (change to lower plan or term).
8) The contract price is in USD; however, billing price is in local currency.
9) Billing amount is calculated by converting contract price (USD) into the currency of the contracting country using the exchange rate released by MUFJ Bank as of the 10th day of the month of use. In case that the billing amount has a fractional part after currency conversion, NTT Communications rounds down a fractional part to two decimal places when auxiliary currency can be used for billing, and to the whole number when it cannot.
10) Amazon AWS connection specific conditions:
   i. Maximum number of the advertised routes from VPN to AWS must be less than 100 due to AWS specification. If users have more than the numbers specified above, they must choose the route advertisement pattern from either, default-route only, summarized routes, or selected routes. In case of selected routes, users must list up the routes which requires communicate with the cloud service.
   ii. The user's VPN is connected via AWS Direct Connect connection location to its Cloud Service Platform. Only the Cloud Service Platform in the same region of the Direct Connect location is available.
   iii. One Multi-Cloud Connect connection can be linked with one VPC in the AWS. This is the limitation of the AWS.

iv. If users link Virtual Interfaces with unexpected VGWs, users cannot change links due to the Amazon specification. In case users require the change of the link, they must create another Virtual Interface and place new order of Multi-Cloud Connect.
v. In order to active the Virtual Interfaces, users must authorize the Virtual Interface connection request from NTT Communications via the AWS portal. After authorized, users must notice the NTT Communications' PM in order to proceed with the remaining configuration.
vi. Users will be charged Data transfer fee etc. from Amazon directly. Please check the AWS web pages for more in detail.

11) Microsoft Azure connection specific conditions:
i. Microsoft peering which provides the Office365 connectivity etc. is not necessarily available by any users due to the Microsoft policy. Users must get the authorization from Microsoft in advance.
ii. Maximum number of the advertised routes from VPN to Azure private peering must be less than 4000 due to Azure specification. If users have more than the numbers specified above, they must choose the route advertisement pattern from either, default-route only, summarized routes, or selected routes. In case of selected routes, users must list up the routes which requires communicate with the cloud service.
iii. The user's VPN is connected via Azure ExpressRoute connection location to its Cloud Service Platform. Only the Cloud Service Platform in the same region (GEO) of the ExpressRoute location is available.
iv. Users will be charged Data transfer fee etc. from Microsoft directly. Please check the Microsoft web pages for more in detail.
v. If users use Microsoft peering, the considerable number of global ip addresses of Microsoft will flow into VPN. In a certain condition of the network, those peering connections cannot be used.
vi. When terminating Multi-Cloud Connect connection, users must unlink the VNET and S-key in advance.

12) Price of Multi-Cloud Connect ordered on demand
i. When applying on demand, it may take up to 5 business days for customer's contact information to be reflected on the system, so there is a possibility of delay in reporting when a failure occurs.
ii. If a customer places an on-demand order for Multi-Cloud Connect, the charge is according to the price list below.

(USD)

Cloud	Product Type	Bandwidth	London		San Jose		Washington		Singapore		Sydney	
			MRC	NRC	MRC	NRC	MRC	NRC	MRC	NRC	MRC	NRC
AWS	AWS Base Connection (Best Effort)	100M	1610	1400	1610	1400	1610	1400	2820	1200	3680	1800

2-10. Extended Network Management Service (ENMS)

1) This service is the Arcstar Universal One option service and provides the management services such as equipment monitoring, NW / equipment management, and carrier/ vendor arrangement for Customers procured, designed and implemented NW/ equipment by our NOC single point of contact.
2) ENMS has 3types menu as below.
i. ENMS WAN Vendor Management: Operational management of the circuit carrier, mainly support of troubleshooting and driving them to resolution.
ii. ENMS Device Management: Includes ENMS Device monitoring feature below, incident management and resolution, equipment break/fix, configuration and change management
iii. ENMS Device Monitoring: Fault monitoring, outage notification
3) Carrier/device maintenance vendor that under contract with the Customer must be able to use English.
4) Customer must submit network diagram for any ENMS orders.
5) Prior to taking over the monitoring and/or management of the circuits and devices, Company will review the Customer existing configurations and may conduct service acceptance test as part of the transition and on-boarding process.
6) Delivery support for Customer circuits/device (for example, ordering representative service, device configuration design, circuit and/or device installation work) are out of scope of this service.
7) This service requires Universal One reachability.
8) Management traffic will pass through Customer circuit and hence this service requires some bandwidth of Customer circuit.
9) This service doesn't provide trouble and failure reporting. Maintenance itself is provided by carrier or device maintenance vendor. Therefore, service level of this ENMS depend on the maintenance service level of the carrier or the device maintenance vendor.

10) Customer must apply for RFC order also for this service when the WAN side Universal One CPE moved.
11) If Customer physically disconnect or move circuits/devices without any disconnect or move order, this service may detect the failure and send failure notice to Customer and carrier/vendor.
12) Move order which move to other country is prohibited. Please apply for disconnect order to existing ENMS and then apply for new order to new location.
13) ENMS WAN Vendor Management specific conditions:
    i. Both originating and terminating device must be Company managed. Therefore, bot h device must be Universal One Managed CPE or the device which have ENMS Device Management.
    ii. This service requires maintenance contract between Customer and carrier. Customer needs to provide copy of LOA (Letters Of Authorization) letter for Company to appoint Company as authorized entity to contact with carrier directly for circuit troubleshooting.
14) ENMS Device Management specific conditions:
    i. This service requires maintenance contract between Customer and device maintenance vendor. Customer needs to provide copy of LOA letter for Company to appoint Company as authorized entity to contact with device maintenance vendor directly for troubleshooting/RMA.
    ii. OOB access for CPE remote maintenance is no longer required effective November 21, 2023.
    Handling of existing OOB access and OOB equipment is as follows:
    - Customer may cancel existing OOB access prepared by Customer.
    - Company will not remove specifically existing OOB equipment, to be collected during CPE removal work.
    - Company will not conduct replacement of existing OOB equipment.
    - Regardless of OOB access/equipment type (PSTN/BB/4G) or built-in/external type, reuse of existing OOB equipment (renewal/move of CPE, etc.) is not acceptable.
    iii. Customer needs to transfer device exclusive RW access right to Company during the ENMS Device Management service period.
    iv. Company will make changes to device configuration if Company determines that such changes are necessary for the provisioning of the service
    v. Customer must submit the device license information. If some license information omitted, the license may not available after device replacement as in RMA.
    vi. Company will be proactively applying the vulnerability patch only for the updates which are service impacting and Company determines such patch is necessary. Prior to implementation of any patches, Company will inform Customer as part of the Change Management process.
    vii. Basically, devices, IOS version, and/or feature license designated by manufacturers as End of Life (EoL) cannot be used under ENMS service.
15) ENMS Device Monitoring specific conditions:
    i. Customer needs to configure the device to allow Company to ping monitoring the device.

3. Ordering

3-1. One-Stop Ordering

1) One-Stop Ordering enables a Customer to make centralized applications for the service upon the Customer's request.
2) One-Stop Ordering may not be available in some countries with the equipment provided through the one directly connected to the Universal One VPN.
3) Applications are received in Japanese or English.
   This service will handle all processes for the Customer from installation work arrangements to testing and the work required for service start, including arrangements of other carrier(s).

3-2. Due date of Application Form, Design Requirement Sheet, Maintenance Information and Termination Order

3-2-1. Application Form (Contract)

The deadline for the application form differs depending on the location (country, area) in which the Customer wishes the service to be provided or the network configuration. The application form needs to be submitted by the deadline notified by Company separately. In case the application form is not submitted by the deadline, the provisioning of the service shall be delayed.

3-2-2. Design Requirement Sheet (New or Modification Order)

1) In order to conclude a new or modification contract, Customers must fill in the necessary items of the

Design Requirement Sheet for Universal One Service and submit the sheet to the sales representative by the deadline. In case the Customer is using CPE service (including cases where the Arcstar Company designs the Customer owned router), the sheet must be submitted 20 business days before the requested service start date (if the Customer is subscribing for multiple locations with different requested service start dates, the earliest requested service start date). In case of Customer owned router, the sheet must be submitted 12 days before the requested service start date (if the Customer is subscribing for multiple locations with different requested service start dates, the earliest requested service start date). If the sheet is not submitted by the deadline the provisioning of the service may be delayed.

2) The deadlines for the new orders for Domestic (Japan) Interconnection and IPSEC (Software Type) are different. It must be submitted with the relevant Service Order and Agreement by the following date: Deadline for Domestic (Japan) Interconnection: by "15 business days before the Requested Service Start Date" Deadline for IPSEC Access (Software Type): by "17 business days before the Requested Service Start Date".
3) Please note that in order to modify the setup of Dedicated Internet Access or Broadband Internet Access. Customers must submit the sheet with the relevant Modification Form or Installation Application Form to the sales representative by the date specified separately. If the sheet is not submitted by the deadline the provisioning of the service may be delayed.
4) In case Arcstar Company is to fill in the Design Requirement Sheet on behalf of the Customer by interviewing the Customer, then a separate fee shall be charged.

3-2-3. Design Requirement Sheet (Addition or Modification to addresses registered at the PE router)

In order to add or modify the addresses registered at the PE router, Customers must fill in the necessary items of the Installation Application Form for Universal One Service and the Design Requirement Sheet and submit both to the sales representative by "8 business days before the Requested Service Start Date" (if the Customer is subscribing for multiple locations with different requested service start dates, the earliest requested service start date).

3-2-4. Maintenance Information

Customers must submit the maintenance information to Arcstar Company when Customers submit Design Sheet. Maintenance information is information such as Customer's contact point necessary for the maintenance of the services provided to the Customer by the Arcstar Company. Maintenance is not possible is the Maintenance information is not submitted to the sales representative. Maintenance information must be promptly submitted whenever the maintenance information is changed. If maintenance information is not submitted, there may be difficulties in order to do the maintenance.

3-2-5. Termination Order

Unless otherwise provided, termination order shall be submitted in writing as prescribed by the Company at least 60 days prior (90 days prior, in case the service is provided by Orange Business Services or Myanmar Posts and Telecommunications.) to the end of the contract term, otherwise the contract term shall automatically renew. In case of cancellations during the contract term, equivalent to the remainder of the monthly charge for the month will be imposed as penalty.

4. Provisioning and Maintenance

4-1. Ready for Service and Start of Maintenance (Conditions)

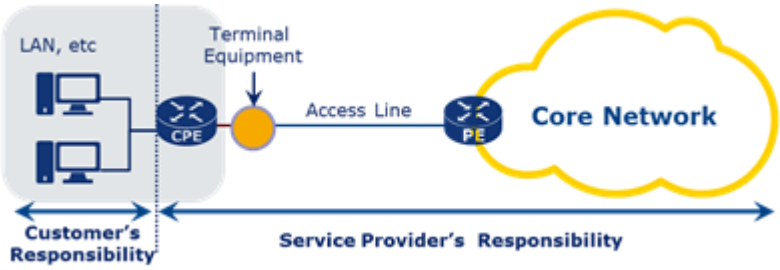
Whether the service is ready for use is determined by the results of the tests done by the Arcstar Company based on Arcstar Company's standards (including network service levels). Depending on the work or network configuration, link down may occur at the relevant location and the other existing locations when implementation work is being conducted.

Note) Tests do not include Customer's LAN side tests. If remote support is needed for Customer's LAN side test, then 3-1-2 3) Customer side remote construction support service must be subscribed.

1) In case CPE Service is provided (including in the case of Customer owned routers designed by Arcstar Company)

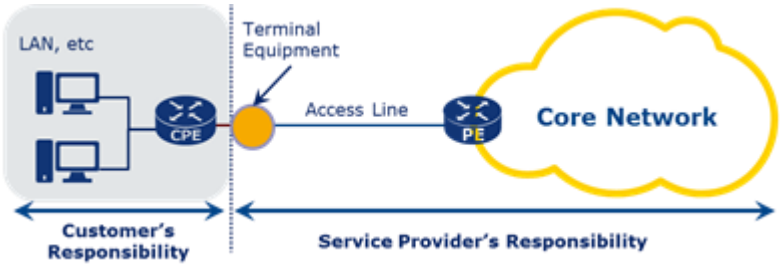
Ready for Service is determined when the result of the ping test done by the Arcstar Company toward

the CPE at Customer's site is successful. Maintenance starts from the Service Start Date with the condition that complete maintenance information is submitted by the Customer to Arcstar's sales representative 10 days before the requested service start date.



(Note) If maintenance information is not submitted or the information is incomplete, then maintenance shall not start even the provisioning of the service has already started.

2) In case CPE Service is not provided (excluding Customer owned router designed by Arcstar Company)
Test terminals are installed at both Arcstar Company's site and Customer's site and Arcstar Company shall perform reachability test between the test terminals. If the result of the test is successful, then the ready for service shall be determined.
Maintenance starts from the Service Start Date with the condition that complete maintenance information is submitted by the Customer to Arcstar's sales representative 10 days before the requested service start date and the ping test performed by the Arcstar Company upon receiving the telephone call from the Customer that the router installation has been completed is successful.



(Note 1) The test does not include the Customer's LAN connectivity test or its onsite or remote support.
(Note 2) The in-house wiring and cabling, and the arrangement of the entrance procedure for the on-site engineer shall be prepared by Customer. Upon activation, Customer's attendance at the sites is required.
(Note 3) If maintenance information is not submitted or the information is incomplete, then maintenance shall not start even the provisioning of the service has already started.
(Note 4) The Service Start Date is either of the date following the order completion date or the Requested Service Start Date, whichever comes later.
(Note 5) In the case of Broadband Internet Access (Customer Provided Internet Access), the internet circuits should be ready before 3 business days in which the CPE is scheduled to be installed. If the circuit is not activated, extra fee related to the delay in implementation work may be incurred.

4-2. Operation and Maintenance

1) One-stop maintenance service is provided by Helpdesk to handle all outages related to Universal One Service. Maintenance is provided on a 24 hours / 365 days basis.
2) This service is supported only in Japanese and English.
3) When Customer makes an inquiry, Customer shall notice its company name, location and Customer ID (begin with W or VR).
4) Company begins operation based on trouble tickets or outage notification by Customer.
5) When outage occurs on the global circuit, Company makes a notification for an outage in English. In such case, Company uses contact information provided by Customer.
6) Company makes the progress notification of operation per approximately 60 minutes in the language

specified by Customer (English or Japanese).

7) Company makes the restoration notification of operation in the language specified by Customer (English or Japanese) when Company judges that the outage has been repaired.
8) Arrangement with other carriers at the time of an outage is also conducted for the Customer. Arrangement with other carriers is subject to each carrier's maintenance conditions.
9) At Customer's request, Company gives the reports the cause of outage for the circuits and CPEs below when the outage applies to the condition below (Report is provided for Dedicated Access only). The report may not be prepared depending on the cause of the incident.
   CPE Management Type: Managed CPE, Unmanaged Option#1
   - condition: outage duration violates SLA.
10) Customer shall declare the outage after confirming the outage is not caused by Customers' equipment or electric power supply. In case on-site maintenance is provided and the outage is found to be occurred in the section under the Customers' responsibility, extra charge may be required.
11) In the case of Dedicated Internet Access or Broadband Internet Access, using Customer Provided Internet Access, Company is not responsible for service degradation (including PDR, delay and jitter), and will not accept any inquiry regarding the traffic status.
12) Prior to call our NOC, the customer must run through the following troubleshooting procedures:
   (12-1) Power Down the Broadband termination device, turn it back on after 30 seconds (do not reboot Cisco / Juniper device)
   a) Wait 5 minutes
   b) If the connectivity is not restored, continue to step #12-2
   (12-2) Re-seat all of the cables connected to the device
   c) Wait 5 minutes
   d) If the connectivity is not restored, continue to step #12-3
   (12-3) Call the our Network Operations Center (NOC)
13) When an alarm is detected and continued for approximately 17 days, Company will suspend Ping monitoring for relevant circuits. In the case of a reason, which is not attributable to Company, the monitoring will be resumed upon customer's request.

4-3. Service Suspension due to Planned Maintenance Work

1) Every Saturday/Sunday from 0:01 a.m. to 6:00 a.m. local time in the area where Access Point is located is considered as "planned maintenance work hours". Disconnection of the Arcstar Universal One service may occur during these hours.
2) For the third party's service and equipment including, but not limited to, Access Service, the maintenance works may be conducted from time to time. Company will use reasonable effort to make a prior notification of the schedule.
3) Company reserves the right to change any notified maintenance times, where necessary, upon prior notice to the Customer.
4) When maintenance work is conducted during the above stated hours, the planned maintenance work date is notified by e-mail two week ahead with the exception of the following cases.
   - The notice is not sent in case the traffic outage due to the maintenance work is less than 1 minute.
   - In case of Dedicated Internet Access or Broadband Internet Access, the notice is not sent by email.
   - In case of urgent maintenance of outage recovery work.
5) However, no request from customer for rescheduling the work date is accepted.

5. Billing

1) At the Customer's request, one-stop billing for the total charge incurred in all countries for Universal One Service can be provided as One-Stop Billing service.
   (Note) One-Stop Billing may not be available in some countries with the equipment provided through the one directly connected to Universal One Service.
2) The mailing address of the bill can be designated per Universal One Service contract. The billing currency will be the currency of the country where the bill is sent. The language used for the statement is English only.
   (Note) The number of billing addresses is not limited as far as on an International Universal One Service contract basis.
3) The calculation of the billing is based on a calendar month, and bills are issued monthly (the installation

work fee and other one-time fees will be included in the bill for the nearest month).

4) Bills will be issued around the 10th of the month following the billing month, and the payment deadline is the end of the month of issue.
   (Note 1) This is not applied to One-Stop Billing including the charges for other services.
   (Note 2) When the charges for Global VPN Service are included in those for another service under a one-stop format, the billing cycle is subject to that of the other service.
5) Applications and / or modifications related to the billing system can be reflected on the current month's statement (issued on the following month) if received by the end of the month.
6) In case of cancellations or bandwidth changes (only in case the billing amount decreases) during the contract term, a penalty will be imposed. (The penalty is equivalent to the remainder of the monthly charge for the month when the cancellation or decrease occurs.)
7) For services that are newly started, cancelled or changed in the middle of the month, the monthly charge is billed on a daily basis. (This is calculated by multiplying the number of days from the service start date to the end of the month in case of newly built, from the first day of the month to the cancel date in case of a cancellation, from the first day of the month to the day before the change date for the old bandwidth, and from the change date to the end of the month for new bandwidth (the latter two are for bandwidth changes) by 1/30th of the monthly charge.)
   However, for some services, the monthly charge will not be billed on a daily basis.
8) When any fractions are generated in the course of discount calculations, daily charge calculations and the exchange rate, such fractions shall be omitted (the adjustments are to be made on the basis of each charge item).
9) In case multiple Services are installed as a result of the change, etc. requested by Customer, Company can charge the monthly charge for at most 30 days (this shall not apply to China or India) concerning each service.
10) Taxes specified under the applicable laws in each country will be added to the billing amount.
11) If Customer cancels all or some parts of the service order form before the commencement date, Customer shall pay termination fees which shall include the full amount of the service charges that Customer would have been charged for the initial order term.
12) As a reference, the billing amount may be converted from local currency to the currency of the contracting country, based on the exchange rate (designated by Arcstar Global Network service carriers) of the 10th of the month before issuing bill.
13) With an application from Customer, if there is any change to Service contents provided to Customer in the middle of the month with no impact to its original billing amount, the change will be reflected on the description of the statement from the following month's bill, which will be issued on the month after the following month.

Arrearage interest is calculated by multiplying the rate specified in the Service Agreement by the number of days from the day after the due date to the day before the payment is made. (However, payments made within 10 days of the day following the due date are not applied to arrearage interest.)

Appendix 1 : Provision related to Service Order Form (SOF)

Table 1 : Standard lead time for relocation (from quotation request up to handover)

Date	APAC	EMEA	SCNA
120 CD	Bangladesh, Cambodia, Hong Kong, New Zealand, Sri Lanka, Thailand		
150 CD	Bhutan, Brunei, Darussalam, China, Fiji, Guam, India, Indonesia, Japan, Korea, Macau, Maldives, Mongolia, Nepal, Pakistan, Singapore, Taiwan, Viet Nam	Albania, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Belgium, Bulgaria, Croatia, Czech, Denmark, Egypt, Estonia, Finland, Georgia, Gibraltar, Hungary, Iraq, Ireland, Israel, Jordan, Kuwait, Kyrgyzstan, Latvia, Lebanon, Libya, Liechtenstein, Lithuania, Luxembourg, Macedonia, Malta, Moldova, Monaco, Oman, Poland, Qatar, Romania, Russia, Saudi Arabia, Serbia, Slovakia, Slovenia, Spain, Switzerland, Tajikistan, Tunisia, Turkmenistan, Ukraine, Uzbekistan, Yemen	Anguilla, Antigua and arbuda, Argentina, Aruba, Bahamas, Barbados, Belize, Bermuda, Chile, Colombia, Costa Rica, Dominican Republic, El Salvador, Guatemala, Honduras, Jamaica, Netherlands, Antilles, Nicaragua, Panama, Peru, Puerto Rico, Uruguay, Venezuela
180 CD	Australia, Malaysia	Germany, Italy, Netherlands, Norway, Portugal, United Arab Emirates, United Kingdom	Bolivia, Bouvet, Island, Canada, Comoros, Ecuador, Guadeloupe, Haiti, Mexico, Paraguay, Saint Helena, Saint Pierre and Miquelon, Trinidad and Tobago, United States, Virgin Islands, Virgin Islands, U.S.

210 CD	Afghanistan, American Samoa, Micronesia, Nauru, New Caledonia, Palau, Papua New Guinea, Philippines, Seychelles, Tonga, Tuvalu, Vanuatu	Algeria, Andorra, Angola, Benin, Bosnia and Herzegovina, Botswana, Burkina Faso, Burundi, Cameroon, Central African Republic, Congo, Cyprus, Djibouti, Equatorial Guinea, Eritrea, Ethiopia, France, Gabon, Gambia, Ghana, Greece, Greenland, Guinea, Guinea-Bissau, Iceland, Isle of Man, Ivory Coast, Kazakhstan, Kenya, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritania, Mauritius, Montserrat, Morocco, Mozambique, Namibia, Niger, Nigeria, Rwanda, Senegal, Sierra Leone, Somalia, South Africa, Swaziland, Sweden, Tanzania, United Republic of Togo, Turkey, Uganda, Zambia, Zimbabwe	Brazil