ສຳນັກງານໃຫຍ່

ເລກທີ: 1844/ທຄຕລ..2024.....
ນະຄອນຫຼວງວຽງຈັນ, ວັນທີ:..17..05..2024.....

ໜັງສືແຈ້ງເຊີນ

ເຖິງ : ບັນດາບໍລິສັດ ຫ້າງຮ้ານຕົວແທນຈຳໜ່າຍເຄື່ອງໄອທີ ໃນນະຄອນຫຼວງວຽງຈັນ.
ເລື່ອງ: ແຈ້ງເຊີນເຂົ້າຮ่วมยื่นซองประมูลราคาเครื่องไอทีอุปกรณ์เครือข่าย (Core Switch Network).

ທະນາຄານການຄ้าต่างประเทดลาว ມະຫາຊົນ ຂໍແຈ້ງມາຍັງບັນດາບໍລິສັດ ແລະ ຫ້າງຮ้ານຕົວແທນຈຳໜ່າຍເຄື່ອງໄອທີ ຊາບວ່າ ທຄຕລ ມີຄວາມຕ้ອງການ ອຸປະກອນໄອທີ ເຄືອຂ่าย Core Switch Network ໃໝ່, ເພື່ອນຳໃຊ້ເຂົ້າໃນວຽກງານວິຊາສະເພາະຂອງ ທະນາຄານ, ຈຶ່ງໄດ້ແຈ້ງເຊີນມາຍັງທ่านเพื่อยื่นซองเข้าร่วมประมูลราคา ດັ່ງມີລາຍລະອຽດข้างล่างนี้:

ລ.ດ	ລາຍການ	ยี่ห้/ລ่ຸນ ເປ้าหมาย	ຈຳນວນ	ข่วงติดตั้ง
1	Core Switch (Spine)	Huawei/Cisco	2	DC
2	Router	Huawei/Cisco	2	DC
3	Aggregation/Distributed Switch (Leaf)	Huawei/Cisco	6	DC
4	Electrical Aggregation/Distributed Switch	Huawei/Cisco	2	DC
5	DR Site Core Switch	Huawei/Cisco	2	DR
6	DR Site Electrical Aggregation/Distributed Switch	Huawei/Cisco	2	DR
7	SDN Controller Server	Huawei/Cisco/Other	3	DC/DR
ການສະໜອງລາຍການทั้งหมด แม่นให้ลวมค่าติดตั้ง, ฝึกอบรมใช้งาน และ ค่าบำลุงรักสา (MA&License) สำลับ 03 ปี **ลายละอองข้อมูนก่องกับสะเป้กัดติดด้านหลัง**				

- **ເງื่อนไขของบໍລິสัด ห้างร้านตัวแทนจำหน่ายเครื่องไอที ที่มีความต้องการยื่นซองประมูลราคาต้องประกอบเอกสารให้ถูกต้องดังลุ่มนี้:**
- **<u>เอกะสาน ชุดที่ 1:</u>**
  1. ประกอบเอกะสานในนามนิติบุกคล ที่ดำเนินทุละกิดจำหน่ายเครื่องอุปะกอนไอที, ดำเนินทุละกิดย่างน้อย 03 ปีขึ้นไป, สำเนาใบทะบียนอิสาหะกิด, ใบยั้งยืนการเสยอากอน ปี 2023 และใบยั้งยืนการเป็นตัวแทนจำหน่ายที่มีใบรับรอง หรือ เป็นโตแทนขายย่างเป็นทางการของผะลิดตะพันดังก่าว.
  2. มีทีมงานที่ชำนาญในการออกแบบ, ติดตั้ง และ ดูแลรองอุปะกอนดังก่าว ที่สามาดให้คำปึกสา และ แก้ไขบันหาทางด้านเตักนิก.
  3. เอกะสานลายละอองสะเป้กสินค้า, การรับประกันสินค้า, ไลยะเอลาการจัดส่งสินค้า และ ข้อมูนต่างๆ ตาม format ที่ติดถัดมาพ้อมนี้.

ເລກທີ 01, ถะหนิน: ปางคำ, เมืองจันทะบูลี, นะคอนหลวงวียงจัน, สปป ลาว. ตู้ ป.น: 2925, โทละสับ: (856-21) 213200-3, 223243-4, 255080-5
Website: http:/www.bcel.com.la, E-mail: bcelhqv@bcel.com.la, SWIFT Code: COEBLALA

4. ເອກະສານຂ້າງເທິງແມ່ນໃຫ້ຍື່ນກ່ອນ **ວັນຈັນ ວັນທີ 03/06/2024 ເວລາ 11:00 ໂມງ** ໂດຍການສົ່ງຟາຍເຂົ້າ **E-mail:** procurement@bcel.com.la **ແລະ** inspect-it@bcel.com.la ເພື່ອໃຫ້ສູນໄອທີໄດ້ກວດສະເປັກ.

ເອກະສານ ຊອງທີ 2: (ປິດຊອງ)

1. ໃບສະເໜີລາຄາ ໃຫ້ລະບຸລາຄາຫົວໜ່ວຍແຕ່ລະລາຍການໃຫ້ລະອຽດ ແລະ ຕ້ອງລວມມູນຄ່າອາກອນທັງໝົດເປັນສະກຸນເງິນກີບໃຫ້ຄົບຖ້ວນ.
2. ຜູ້ສະໜອງຕ້ອງວາງເງິນຄ້ຳປະກັນການປະມູນຕ່ຳສຸດ 2% ຂອງມູນຄ່າທັງໝົດ ໂດຍໜັງສືຄ້ຳປະກັນທີ່ອອກໂດຍທະນາຄານພາຍໃນ **(ວັນໝົດອາຍຸໜັງສືຄ້ຳປະກັນຕ້ອງເຖິງ ວັນທີ 13/09/2024)** ຫຼື ແຊັກທີ່ວີຊ້າແລ້ວ (ທຄຕລ ບໍ່ຮັບເງິນສົດ), ພາຍຫຼັງປະກາດຜົນ ທຄຕລ ຈະສົ່ງໜັງສືຄ້ຳປະກັນຄືນ.
3. **ໃນວັນພະຫັດ ວັນທີ 13/06/2024 ເວລາ 13:30 ໂມງ** ແມ່ນມື້ເປີດຊອງປະມູນ ສະນັ້ນ, ໃຫ້ຜູ້ສະໜອງທີ່ຜ່ານການຄັດເລືອກຈາກເອກະສານຊອງທີ 1 ມາຍື່ນຊອງລາຄາດ້ວຍຕົນເອງ ຫຼື ສົ່ງຜູ້ຕາງໜ້າເຂົ້າຮ່ວມທີ່ຫ້ອງປະຊຸມໃຫຍ່ຊັ້ນ 5 ອາຄານ C ຫ້ອງ 5/2 ສຳນັກງານໃຫຍ່ ທຄຕລ.

ໝາຍເຫດ:

- ທຄຕລ ຂໍສະຫງວນສິດ ປະຕິເສດຜູ້ສະໜອງທີ່ປະກອບເອກະສານ ບໍ່ຄົບຖ້ວນ ຫຼື ບໍ່ຖືກຕ້ອງຕາມການກຳນົດຂ້າງເທິງ.

❖ ເງື່ອນໄຂຂອງສັນຍາລະຫວ່າງ ທຄຕລ ແລະ ຜູ້ສະໜອງທີ່ຊະນະການປະມູນ:

1. ຜູ້ທີ່ຊະນະການປະມູນຈະໄດ້ເຊັນສັນຍາກັບ ທຄຕລ ແລະ ຮັບຜິດຊອບຄ່າທຳນຽມໃນການຈົດທະບຽນສັນຍາ.
2. ຖ້າຜູ້ຊະນະການປະມູນປະຕິເສດການເຊັນສັນຍາ ແມ່ນຕ້ອງຮັບຜິດຊອບຄ່າເສຍຫາຍໃຫ້ແກ່ ທຄຕລ ໃນອັດຕາ 2% ຂອງມູນຄ່າລວມທີ່ສະເໜີປະມູນ.

ການຊຳລະຈະແບ່ງຈ່າຍເປັນ 02 ງວດ ລຸ່ມນີ້:

- **ງວດທີ 1:** ຊຳລະ 90% ຂອງມູນຄ່າ ພາຍໃນ 25 ວັນ ລັດຖະການ ພາຍຫຼັງໄດ້ຮັບເຄື່ອງ ແລະ ກວດກາຄວາມຖືກຕ້ອງຈາກຄະນະກຳມະການຕິດຕາມກວດກາ.
- **ງວດທີ 2:** ຊຳລະ 10% ຂອງມູນຄ່າ ພາຍຫຼັງຄົບກຳນົດການຄ້ຳປະກັນຄຸນະພາບສິນຄ້າ 12 ເດືອນ.

ດັ່ງນັ້ນ, ຈຶ່ງຂໍອະນຸຍາດແຈ້ງເຊີນມາຍັງທ່ານທີ່ມີຄວາມສົນໃຈເຂົ້າຮ່ວມຍື່ນຊອງປະມູນໃນຄັ้งนี้.

ຜູ້ອຳນວຍການ

ທະນາຄານ ການຄ້າຕ່າງປະເທດລາວ ມະຫາຊົນ BANQUE POUR LE COMMERCE EXTERIEUR LAO PUBLIC

ນັນທະລາດ ແກ້ວປະເສີດ

ລາຍການທີ່ຕ້ອງການ ຂອງໂຄງການປັບປຸງລະບົບເຄືອຂ່າຍ ທຄຕລ

ລດ	ລາຍການ	ຍີຫໍ້/ລຸ້ນ ເປົ້າໝາຍ	ຈຳນວນ	ບ່ອນຕິດຕັ້ງ
1	Core Switch (Spine)	Huawei/Cisco	2	DC
2	Router	Huawei/Cisco	2	DC
3	Aggregation/Distributed Switch (Leaf)	Huawei/Cisco	6	DC
4	Electrical Aggregation/Distributed Switch	Huawei/Cisco	2	DC
5	DR Site Core Switch	Huawei/Cisco	2	DR
6	DR Site Electrical Aggregation/Distributed Switch	Huawei/Cisco	2	DR
7	SDN Controller Server	Huawei/Cisco/Other	3	DC/DR
8	ການສະໜອງລາຍການທັງໝົດ ແມ່ນໃຫ້ລວມຄ່າຕິດຕັ້ງ, ເຝິກອົບຮົມໃຊ້ງານ ແລະ ຄ່າບຳລຸງຮັກສາ (MA&License) ສຳລັບ 03 ປີ.			

ລາຍລະອຽດຂອງແຕ່ລະລາຍການ

Table 1-1 Spine/Core Switch Parameter Requirements of Data Center Network solution **(02 Units)**

Core Switch (Spine)	
Specification	**Requirement**
Brand	Huawei/Cisco
Hardware specifications	Number of service slots ≥ 4
	The number of SFU slots must be greater than or equal to 6, and the SFUs must be in N+M redundancy mode.
	Fan tray redundancy design. The number of slots in the fan tray must be greater than or equal to 3.
	A single PSU supports dual inputs and hybrid power supply of AC and HVDC.
	The MPU and SFU are separated from each other. The forwarding performance of the entire system is not affected when the MPU is faulty or replaced.
	The device supports the VOQ capability
	Supports cell switching, inter-board forwarding without packet loss
	Strict front-to-rear airflow.
Performance	Switching capacity not less than 43Tbps
	Packet forwarding rate not less than 11280Mpps
Port Configuration Requirements	Supports 10G/40G/100G line cards. A single slot supports a maximum of 36*100GE ports or 36*40GE line card.
Layer 2 Function	Supports port aggregation and 802.3ad.
	Supports inter-chassis link binding technologies such as M-LAG, vPC
	N:1 mirroring, flow mirroring, and remote port mirroring
Layer 3 Function	Supports IPv4 dynamic routing protocols, such as RIP, OSPF, IS-IS, and BGP.
	Supports IPv6 dynamic routing protocols, such as RIPng, OSPFv3, IS-ISv6, and BGP4+.
	Supports dynamic routing (OSPF/OSPFv3/BGP/BGP4+) access to M-LAG
	Supports routing protocol multi-instance and policy-based routing.
	Supports VRRP/VRRPv3.

	IPv6 ND and PMTU discovery
	Supports IP fragmentation and reassembly
QoS	Supports queue scheduling modes such as PQ, DRR, and PQ+DRR.
	Supports ACL, CAR, and remark actions.
	Supports congestion avoidance mechanisms, such as WRED and tail drop.
	Supports traffic shaping.
Reliability	Bidirectional Forwarding Detection (BFD) with a detection interval of 3.3 ms
	Supports BFD for M-LAG
	Supports the N-to-N-to-N technology for clustering or stacking, allowing multiple devices to be managed on a single interface.
	A cluster or stack supports out-of-band management, direct connection between MPUs, and separate management and forwarding links.
DC features	Supports one-to-many virtualization to virtualize a maximum of 16 logical switches
	VXLAN and BGP EVPN are supported.
	Supports Ethernet Segment Identifier (ESI) multi-homing access
	Supports the statistics of the buffered microburst status
	Supports MAC flapping
	Supports VXLAN over IPv6
	Supports IPv6 VXLAN over IPv4
Security	Supports Layer 2 to Layer 4 ACLs.
	Microsegmentation (IPv4 and IPv6) is supported.
	NSH (IPv4 and IPv6) and third-party test reports
	Supports MACsec.
	BPDU guard
	Supports VXLAN ARP broadcast suppression
	Supports unicast, multicast, and broadcast storm control.
	Supports DHCPv4 server, relay, and snooping.
	Supports IP/ARP/ICMP security.
Multicast	Supports IGMP snooping V1, V2, and V3.
	Supports IGMP proxy.
	Supports PIM-SM and PIM-SSM.
Configuration and maintenance	Supports Telemetry
	Supports enhanced ERSPAN
	Supports VxLAN OAM: VxLAN ping, VxLAN tracert
	Supports IEEE 1588v2
	Supports iPCA
	Supports SNMP V1, V2, V3, Telnet, RMON, and SSH.
	Supports configuration and management through command lines and graphical configuration software.
	The rollback point for one or more configurations is formed through the CLI based on the commit command. The rollback point can be flexibly executed multiple times.
	BootROM upgrade and remote online upgrade
	ZTP technology, automatic configuration delivery

	Supports RADIUS user login authentication.
	Supports automatic Ansible configuration.
Intelligent lossless network features	Adjusts ECN threshold parameters based on the traffic model. Ensures that the port bandwidth usage of RoCE services can reach over 90% and zero packet loss occurs in various traffic models.
	RoCE and TCP traffic can be scheduled in proportion. The scheduling proportion error is controlled within 5% of the bandwidth of the entire port.
	RoCE network KPIs can be visualized, including the number of received and transmitted PFC backpressure frames, number of PFC deadlock monitoring, number of PFC deadlock recovery, and ECN packets.
	Supports PFC deadlock detection and deadlock prevention
	iNOF is supported.
	Supports ECN overlay and applies ECN to VXLAN networks.
Traffic analysis	~~NetStream~~
	Supports sFlow
	Supports intelligent TCP traffic analysis
	Supports intelligent UDP traffic analysis

Table 1-2 Mobile Service Router Parameter Requirements of Data Center Network solution **(02 Units)**

Mobile Service Router	
Specification	**Requirement**
Brand	Huawei/Cisco
Architecture	Support non-blocking switching structure, and provide the official website links and screenshot
	Support Multi-core CPU, at least support 16 cores, and provide the official website links and screenshot.
	Support dual Control Plane and Forwarding Plane in redundancy mode. (request two pieces of forwarding plane board)
Slot	6*WSIC; 4*SIC
Performance	WAN with service performance (IMIX) ≥ 10Gbps.
Fixed interfaces	14 * 10GE SFP+(compatible with GE SFP) +10 * GE RJ45 (All WAN ports can be configured as LAN)
Interface type	WAN interface: Support FE, GE, 10GE
Operating Temperature	0-45 °C
LAN Access	Support IEEE 802.1P, 802.1Q standard.
	Support IEEE 802.1d (STP), 802.1w (RSTP), 802.1s (MSTP) standard.
	Support static MAC address and dynamic MAC address.
	Support MAC address limit, LLDP, Transparent bridge.
WAN Access	Support PPP, MP, PPPoE C/S
	Support PPP, MP, PPPoE C/S
	Support IPv4 and IPv6 PPP, MLPPP.
IP Application	Support NAT, NAT ALG.
	Support DNS Client, DNS proxy/relay, DDNS, DNS6 Client, DNS6 Proxy/Relay.
	Support IPv4 VRRP, VRRP6.
	Support NQA ICMP/UDP/TCP/SNMP/FTP/HTTP UDP jitter test/DHCP/Trace/DNS test.
	Support DHCP Client, DHCP relay, DHCP Server, DHCPv6 Client, DHCPv6 relay and DHCPv6 Server.
IPv6 Tunnel	ISATAP tunnel.

	6 over 4 manual tunnel.
	Supports IPv4 address-compatible automatic tunnel.
	6 over 4 GRE tunnel.
Routing	Support RIPv1/v2, RIPng, OSPFv2, OSPFv3, IS-IS, IS-ISv6, BGP4, BGP4+, MBGP.
	Support Smart Policy Route.
	Support IGMPv1/v2/v3, IGMP Proxy.
	Support PIM-DM, PIM-SM and PIM SSM.
MPLS	Support IPv4 LDP and LDP FRR.
	Support Hub-Spoke VPN, HoVPN, Support MCE, Support manual VPN FRR and VPN Auto FRR.
	Support local CCC, SVC VLL, Martini VLL, and inter-domain Martini VLL.
	Support MPLS TE.
VPN	Support GRE, L2TP, IPsec VPN
	IPsec tunnels ≥6000.
	Support DSVPN or similar VPN.
	Support A2A VPN
Wireless network(AC)	Support AC function without additional hardware. At least support to manage 64 APs.
	Support WEP, WPA, WPA2;
	Support WLAN QoS
Security	Support packet filtering firewall, ASPF, Attack defense, Active/Standby firewall.
	Support Zone-based Stateful FW
	Support 802.1x & MAC authentication
	Support Web authentication, User access management.
	Support ARP packet suppression, ARP spoofing, DAI, Broadcast suppression
	Support ICMP attack defense, uRPF, IPSG, Attach Source Track
	Support IPS, URL filtering & files Filtering
QoS	Support basic IPv4 ACLs, extended IPv4 ACLs, and Ethernet frame header-based Layer 2 ACLs and name ACLs.
	Support CAR, Shaping, WRED
	Support SP/WRR/SP+WRR on LAN port, PQ/CBWFQ on WAN port
	Support sub-interface QOS, FR QoS, IPv6 QoS, ATM QoS and hierarchical QoS.
	Support Smart Application Control (SAC)
	Hardware based QOS
Reliability	All interface cards support hot-swappable.
	Interface card/service card not limited for the slot. (No IO slots limitation)
	Support VRRP
OAM	Support Netstream or other similar features
	Support FTP/TFTP, SSH, Telnet.
	Support SYSLOG, SNMP V1/V2/V3, RMON, Web Management.
	Support NetConf/YANG.
	Support USB drive to configure devices for plug-and-play.
SD-WAN	Support SD-WAN Features.

Certification	Provide CB/NRTL/GS Certificate
	Provide CE certificate

Table 1-3 Leaf/Aggregation/Distributed Switch Parameter Requirements of Data Center Network solution (06 units)

Aggregation/Distributed Switch (Leaf)	
Specification	**Requirement**
Brand	Huawei/Cisco
Hardware Specifications	The height is less than or equal to 1 U, with fixed ports.
	The power modules work in 1+1 backup mode and the fan modules work in 3+1 backup mode.
	The available cache size of the entire system is greater than or equal to 36 MB.
	Front-to-back and rear-to-front air channels
Performance	Switching capacity not less than 2.16Tbps
	Packet forwarding rate not less than 954Mpps
Port Configuration Requirements	40/100 GE optical ports ≥ 6
	The number of 10GE optical ports is greater than or equal to 48
Layer 2 Function	Supports the access, trunk, and hybrid modes.
	Supports QinQ.
	Supports inter-chassis link bundling technologies such as M-LAG, vPC
	Supports DLDP.
	Dynamic, static, and blackhole MAC address entries are supported.
Layer 3 Function	Supports IPv4 dynamic routing protocols, such as RIP, OSPF, IS-IS, and BGP.
	Supports IPv6 dynamic routing protocols, such as RIPng, OSPFv3, IS-ISv6, and BGP4+.
	Supports IP packet fragmentation and reassembly
	Supports BFD for OSPF, BGP, IS-IS, and static routes.
	IPv6 ND and PMTU discovery
QoS	Supports queue scheduling modes such as PQ, DRR, and PQ+DRR.
	Supports traffic classification based on the L2 protocol header, L3 protocol, and L4 protocol.
	Supports bidirectional port rate limiting.
	Provides the broadcast storm suppression function.
	Supports traffic shaping.
Reliability	Supports VRRP, VRRP load balancing, and BFD for VRRP.
	Bidirectional Forwarding Detection (BFD) with a detection interval of 3.3 ms
	Supports the N-to-N-to-N technology for cluster or stacking, allowing multiple devices to be managed on a single interface.
DC Features	VXLAN and BGP EVPN are supported.
	Supports VXLAN over IPv6
	Supports IPv6 VXLAN over IPv4
	QinQ Access VXLAN
	Supports Ethernet Segment Identifier (ESI) multi-homing access
Security	DoS, ARP, and ICMP attacks can be prevented.
	Supports microsegmentation (IPv4 and IPv6)

	Supports NSH (IPv4 and IPv6).
	Binding of IP addresses, MAC addresses, ports, and VLANs
	Supports port isolation.
	Supports user login authentication, such as RADIUS.
	Support RMON
Multicast	Multicast traffic suppression
	IGMP Snooping
	Supports IGMP proxy.
	Supports IGMP, PIM-SM, and MBGP.
Configuration and maintenance	Supports Telemetry
	Supports ERSPAN enhancement
	Supports VxLAN OAM: VxLAN ping, VxLAN tracert
	Supports IPCA
	Supports SNMP V1, V2, V3, Telnet, RMON, and SSH.
	Supports configuration rollback based on the CLI.
	Network-wide path detection is supported.
	Supports the statistics of the buffered microburst status
	Supports BootROM upgrade and remote online upgrade.
	ZTP technology, automatic configuration delivery
	Supports automatic Ansible configuration
Traffic Analysis	NetStream
	Supports sFlow.

Table 1-4 Electrical Leaf/Aggregation/Distributed Switch Parameter Requirements of Data Center Network solution **(02 Units)**

Electrical Aggregation/Distributed Switch	
~~Specification~~	**~~Requirement~~**
Brand	Huawei/Cisco
Hardware Specifications	The height is less than or equal to 1 U, with fixed ports.
	The power modules work in 1+1 backup mode and the fan modules work in 3+1 backup mode.
	The available cache size of the entire system is greater than or equal to 36 MB.
	Front-to-back and rear-to-front air channels
Performance	Switching capacity not less than 2.16Tbps
	Packet forwarding rate not less than 954Mpps
Port Configuration Requirements	40/100 GE optical ports ≥ 6
	The number of 10GE electrical ports is greater than or equal to 48
Layer 2 Function	Supports the access, trunk, and hybrid modes.
	Supports QinQ.
	Supports inter-chassis link bundling technologies such as M-LAG, vPC
	Supports DLDP.

	Dynamic, static, and blackhole MAC address entries are supported.
Layer 3 Function	Supports IPv4 dynamic routing protocols, such as RIP, OSPF, IS-IS, and BGP.
	Supports IPv6 dynamic routing protocols, such as RIPng, OSPFv3, IS-ISv6, and BGP4+.
	Supports IP packet fragmentation and reassembly
	Supports BFD for OSPF, BGP, IS-IS, and static routes.
	IPv6 ND and PMTU discovery
QoS	Supports queue scheduling modes such as PQ, DRR, and PQ+DRR.
	Supports traffic classification based on the L2 protocol header, L3 protocol, and L4 protocol.
	Supports bidirectional port rate limiting.
	Provides the broadcast storm suppression function.
	Supports traffic shaping.
Reliability	Supports VRRP, VRRP load balancing, and BFD for VRRP.
	Bidirectional Forwarding Detection (BFD) with a detection interval of 3.3 ms
	Supports the N-to-N-to-N technology for cluster or stacking, allowing multiple devices to be managed on a single interface.
DC Features	VXLAN and BGP EVPN are supported.
	Supports VXLAN over IPv6
	Supports IPv6 VXLAN over IPv4
	QinQ Access VXLAN
	Supports Ethernet Segment Identifier (ESI) multi-homing access
Security	DoS, ARP, and ICMP attacks can be prevented.
	Supports microsegmentation (IPv4 and IPv6)
	Supports NSH (IPv4 and IPv6).
	Binding of IP addresses, MAC addresses, ports, and VLANs
	Supports port isolation.
	Supports user login authentication, such as RADIUS.
	Support RMON
Multicast	Multicast traffic suppression
	IGMP Snooping
	Supports IGMP proxy.
	Supports IGMP, PIM-SM, and MBGP.
Configuration and maintenance	Supports Telemetry
	Supports ERSPAN enhancement
	Supports VxLAN OAM: VxLAN ping, VxLAN tracert
	Supports IPCA
	Supports SNMP V1, V2, V3, Telnet, RMON, and SSH.
	Supports configuration rollback based on the CLI.
	Network-wide path detection is supported.
	Supports the statistics of the buffered microburst status
	Supports BootROM upgrade and remote online upgrade.
	ZTP technology, automatic configuration delivery

	Supports automatic Ansible configuration
Traffic Analysis	NetStream
	Supports sFlow.

Table 1-5 DR Site Core Switch Parameter Requirements of Data Center Network solution (02 units)

DR Site Core Switch	
Specification	**Requirement**
Brand	Huawei/Cisco
Hardware Specifications	The height is less than or equal to 1 U, with fixed ports.
	The power modules work in 1+1 backup mode and the fan modules work in 3+1 backup mode.
	The available cache size of the entire system is greater than or equal to 36 MB.
	Front-to-back and rear-to-front air channels
Performance	Switching capacity not less than 2.16Tbps
	Packet forwarding rate not less than 954Mpps
Port Configuration Requirements	40/100 GE optical ports ≥ 6
	The number of 10GE optical ports is greater than or equal to 48
Layer 2 Function	Supports the access, trunk, and hybrid modes.
	Supports QinQ.
	Supports inter-chassis link bundling technologies such as M-LAG, vPC
	Supports DLDP.
	Dynamic, static, and blackhole MAC address entries are supported.
Layer 3 Function	Supports IPv4 dynamic routing protocols, such as RIP, OSPF, IS-IS, and BGP.
	Supports IPv6 dynamic routing protocols, such as RIPng, OSPFv3, IS-ISv6, and BGP4+.
	Supports IP packet fragmentation and reassembly
	Supports BFD for OSPF, BGP, IS-IS, and static routes.
	IPv6 ND and PMTU discovery
QoS	Supports queue scheduling modes such as PQ, DRR, and PQ+DRR.
	Supports traffic classification based on the L2 protocol header, L3 protocol, and L4 protocol.
	Supports bidirectional port rate limiting.
	Provides the broadcast storm suppression function.
	Supports traffic shaping.
Reliability	Supports VRRP, VRRP load balancing, and BFD for VRRP.
	Bidirectional Forwarding Detection (BFD) with a detection interval of 3.3 ms
	Supports the N-to-N-to-N technology for cluster or stacking, allowing multiple devices to be managed on a single interface.
DC Features	VXLAN and BGP EVPN are supported.
	Supports VXLAN over IPv6
	Supports IPv6 VXLAN over IPv4
	QinQ Access VXLAN
	Supports Ethernet Segment Identifier (ESI) multi-homing access
Security	DoS, ARP, and ICMP attacks can be prevented.

	Supports microsegmentation (IPv4 and IPv6)
	Supports NSH (IPv4 and IPv6).
	Binding of IP addresses, MAC addresses, ports, and VLANs
	Supports port isolation.
	Supports user login authentication, such as RADIUS.
	Support RMON
Multicast	Multicast traffic suppression
	IGMP Snooping
	Supports IGMP proxy.
	Supports IGMP, PIM-SM, and MBGP.
Configuration and maintenance	Supports Telemetry
	Supports ERSPAN enhancement
	Supports VxLAN OAM: VxLAN ping, VxLAN tracert
	Supports IPCA
	Supports SNMP V1, V2, V3, Telnet, RMON, and SSH.
	Supports configuration rollback based on the CLI.
	Network-wide path detection is supported.
	Supports the statistics of the buffered microburst status
	Supports BootROM upgrade and remote online upgrade.
	ZTP technology, automatic configuration delivery
	Supports automatic Ansible configuration
Traffic Analysis	NetStream
	Supports sFlow.

Table 1-6 DR Site Electrical Aggregation/Distributed Switch Parameter Requirements of Data Center Network solution (02 Units)

DR Site Electrical Aggregation/Distributed Switch	
Specification	**Requirement**
Brand	Huawei/Cisco
Hardware Specifications	The height is less than or equal to 1 U, with fixed ports.
	The power modules work in 1+1 backup mode and the fan modules work in 3+1 backup mode.
	The available cache size of the entire system is greater than or equal to 36 MB.
	Front-to-back and rear-to-front air channels
Performance	Switching capacity not less than 2.16Tbps
	Packet forwarding rate not less than 954Mpps
Port Configuration Requirements	40/100 GE optical ports ≥ 6
	The number of 10GE electrical ports is greater than or equal to 48
Layer 2 Function	Supports the access, trunk, and hybrid modes.
	Supports QinQ.
	Supports inter-chassis link bundling technologies such as M-LAG, vPC

	Supports DLDP.
	Dynamic, static, and blackhole MAC address entries are supported.
Layer 3 Function	Supports IPv4 dynamic routing protocols, such as RIP, OSPF, IS-IS, and BGP.
	Supports IPv6 dynamic routing protocols, such as RIPng, OSPFv3, IS-ISv6, and BGP4+.
	Supports IP packet fragmentation and reassembly
	Supports BFD for OSPF, BGP, IS-IS, and static routes.
	IPv6 ND and PMTU discovery
QoS	Supports queue scheduling modes such as PQ, DRR, and PQ+DRR.
	Supports traffic classification based on the L2 protocol header, L3 protocol, and L4 protocol.
	Supports bidirectional port rate limiting.
	Provides the broadcast storm suppression function.
	Supports traffic shaping.
Reliability	Supports VRRP, VRRP load balancing, and BFD for VRRP.
	Bidirectional Forwarding Detection (BFD) with a detection interval of 3.3 ms
	Supports the N-to-N-to-N technology for cluster or stacking, allowing multiple devices to be managed on a single interface.
DC Features	VXLAN and BGP EVPN are supported.
	Supports VXLAN over IPv6
	Supports IPv6 VXLAN over IPv4
	QinQ Access VXLAN
	Supports Ethernet Segment Identifier (ESI) multi-homing access
Security	DoS, ARP, and ICMP attacks can be prevented.
	Supports microsegmentation (IPv4 and IPv6)
	Supports NSH (IPv4 and IPv6).
	Binding of IP addresses, MAC addresses, ports, and VLANs
	Supports port isolation.
	Supports user login authentication, such as RADIUS.
	Support RMON
Multicast	Multicast traffic suppression
	IGMP Snooping
	Supports IGMP proxy.
	Supports IGMP, PIM-SM, and MBGP.
Configuration and maintenance	Supports Telemetry
	Supports ERSPAN enhancement
	Supports VxLAN OAM: VxLAN ping, VxLAN tracert
	Supports IPCA
	Supports SNMP V1, V2, V3, Telnet, RMON, and SSH.
	Supports configuration rollback based on the CLI.
	Network-wide path detection is supported.
	Supports the statistics of the buffered microburst status
	Supports BootROM upgrade and remote online upgrade.

	ZTP technology, automatic configuration delivery
	Supports automatic Ansible configuration
Traffic Analysis	NetStream
	Supports sFlow.

Table 1-7 SDN Controller Parameter Requirements of Data Center Network solution (03 Units)

SDN Controller	
Specification	**Requirement**
Brand	Huawei/Cisco/Other Server
Product architecture	To ensure high availability, the system supports cluster deployment and load balances services among multiple cluster nodes. When a single node fails, the entire cluster can still run properly. In addition, the system supports flexible capacity expansion to enhance the performance of the entire cluster.
	Based on the Cloud Native architecture, the system uses a service-oriented module design and supports distributed virtualization deployment. By connecting to the cloud platform in the northbound direction, network devices in the southbound direction, and the computing management platform in the east-west direction, the system implements collaborative provisioning of network, computing, and storage resources. In addition, the system can collaborate with the analyzer to build an efficient, simple, and open data center network.
Installation and deployment	To facilitate deployment, the system must provide two installation modes: **factory installation** and **one-click installation using the automatic tool**. The services to be deployed can be selected on the installation page as required, and the controller deployment guide is available.
	To fully utilize server resources, the controller can be deployed on physical machines and VMs in a single-node system or cluster. **A solution test report issued by a third-party authoritative organization must be provided.**
	Installation requirements: 1. **Number of servers or VMs**: Small-scale deployment: one server; cluster deployment: three or more servers 2. **Requirements for x86 servers provided by vendors**: CPU: ≥ 16-core 2.3 GHz; memory: ≥ 128 GB; hard disk: 4 x 1200 GB SAS HDD, RAID 10, 20 MB/s read/write rate for 4-KB blocks; RAID controller card: 9460-8i (2 GB cache) or MSCC SmartRAID 3152-8i (2 GB cache) 3. **Requirements for ARM-based servers provided by vendors**: 2 x Kunpeng 920-24Core@2.6 GHz; memory: ≥ 128 GB; hard disk: 4 x 960 GB SSD, RAID 10, 20 MB/s read/write rate for 4-KB blocks; RAID controller card: 9440-8i 4. **Requirements for third-party servers**: CPU: ≥ 2 x 10 cores, 2.2 GHz; memory: 128 GB or above; hard disk: 4 x 600 GB HDD and 2 x 960 GB SSD, 20 MB/s read/write rate for 4-KB blocks; RAID controller card: super capacitor 5. **Requirements for VMs**: x86 architecture: ≥ 24 vCPUs, 128 GB memory, and 1.2 TB hard disk; ARM architecture: ≥ 64 vCPUs, 128 GB memory, and 1.2 TB hard disk
Performance capacity	A three-node controller cluster (deployed on physical machines or VMs) can manage at least 1.8K NVE nodes. A cluster with the largest number of nodes (deployed on physical machines or VMs) can manage at least 4.2K NVE nodes.
	The small-scale deployment solution (single-node controller) can manage at least 34 NVE nodes, regardless of the deployment mode (on a physical machine or VM).
Open ecosystem	To simplify management, a unified portal is required for device O&M and configuration delivery (including both the overlay and underlay). In addition, SSO can be used to switch to the analyzer for intelligent O&M and analysis.
	The system must provide unified northbound programmable interfaces and implement programmable management through open and standard RESTful APIs. In addition, it can interconnect with mature OpenStack cloud management platforms through standard Neutron APIs.
	The controller can use standard southbound interface protocols, such as OpenFlow, NETCONF, SNMP, and SSH, to interconnect with network devices.
	To maintain compatibility with existing switches on the live network, the system must be able to uniformly manage and deliver configurations to third-party switches. **A solution test report issued by a third-party authoritative organization must be provided.**
	To maintain compatibility with existing VAS devices on the live network, the system must be able to uniformly manage and deliver configurations to third-party VAS devices, including Fortinet firewalls, Palo Alto firewalls, Check Point firewalls, and F5 load balancers. **A solution test report issued by a third-party authoritative organization must be provided.**
	For third-party VAS devices (such as third-party WAFs, firewalls, and load balancers) that cannot be managed, traffic can be diverted to them as dumb devices.

System availability	During system running, to prevent the entire network from being affected by system faults or system offline, the controller does not participate in data forwarding. This ensures that existing network services are not affected after all controller nodes fail. **A solution test report issued by a third-party authoritative organization must be provided.**
	To ensure high reliability, the system must support cluster deployment. Nodes in the cluster work in load balancing mode and provide a unique management IP address for the upper-layer application system and cloud platform. When less than half of the nodes in the cluster are faulty, the cluster can still run properly and the management IP address can be switched from the faulty node to a functioning node, which is not perceived by the upper-layer service system.
	To ensure the DR capability, the system must support remote DR deployment. When the active data center is faulty and services are switched to the standby data center, no data is lost. **A solution test report issued by a third-party authoritative organization must be provided.**
	When geographic redundancy is deployed, the controller supports manual switchover and automatic switchover between the active and standby clusters through a third-party arbitration service. The arbitration service can be provided by the vendor or third-party arbitration software.
	To ensure that a single node in a cluster can be quickly recovered after a fault occurs, the system must support single node replacement.
	To ensure that a cluster can quickly recover from a fault, the system needs to support cluster backup and restoration.
Single-DC networking architecture	To fully utilize devices on the live network, the network must support multiple networking models, such as the combination of the border leaf and spine nodes, the combination of the border leaf and fabric gateway, and the combination of the border leaf, spine, server leaf, service leaf, and fabric gateway. The network can flexibly adapt to all series of GE, 10GE, 25GE, 40GE, 100GE, and 400GE legacy network devices, facilitating device reuse, upgrade, and expansion. **A solution test report issued by a third-party authoritative organization must be provided.**
	To improve network reliability, the multi-spine networking must be supported, where services can still be properly forwarded upon the fault of a single spine node.
	To improve network reliability, leaf nodes can form an M-LAG. If a single link fails, traffic can be switched within 20 ms. **A solution test report issued by a third-party authoritative organization must be provided.**
	To maximize the utilization of legacy network resources and properly schedule traffic, ECMP-based load balancing must be supported between spine and leaf nodes.
Underlay network	To manage links more flexibly, the controller must support automatic discovery and manual creation of links. **A solution test report issued by a third-party authoritative organization must be provided.**
	To improve deployment efficiency, the system must support simplified ZTP to quickly implement automatic configuration of the underlay Layer 3 network and automatic onboarding of devices. The DHCP server can flexibly select the built-in or external DHCP service of the controller. The controller also supports flexible underlay configurations such as spine/RR egress interconnection configuration templates as well as O&M configurations (such as syslogs). **A solution test report issued by a third-party authoritative organization must be provided.**
	To ensure the security and reliability of devices, the controller supports two-way certificate authentication when devices go online through ZTP. In addition, after devices are discovered, the device models can be viewed without additional identifiers. **A solution test report issued by a third-party authoritative organization must be provided.**
	To greatly simplify the underlay network planning and deployment, the system must support intent-based automatic DC fabric underlay network planning and automatic topology generation. The topology configuration can be modified, simulated and verified, and provisioned. **A solution test report issued by a third-party authoritative organization must be provided.**
	To prevent errors after underlay network planning and deployment, the system must support diverse verification mechanisms such as intent-based connectivity verification between underlay VTEPs, VTEP IP address verification, router ID address verification, VTEP MAC address verification, blackhole route verification, and routing loop verification. **A solution test report issued by a third-party authoritative organization must be provided.**
	To improve the efficiency of switch and server capacity expansion and avoid possible errors caused by manual configuration, the system must support intent-based automatic configuration for access switch and server capacity expansion. **A solution test report issued by a third-party authoritative organization must be provided.**
	To eliminate security risks during ZTP, the system must support ZTP in out-of-band management mode to isolate the controller from the service network. **A solution test report issued by a third-party authoritative organization must be provided.**
	To facilitate the evolution from IPv4 to IPv6, underlay IPv6 networking must be supported.
Interconnection with the cloud platform	The controller can interconnect with the OpenStack cloud platform based on the standard model to implement unified management and on-demand scheduling of network resources. The control and forwarding planes use standard protocols and support interconnection status query.

	If OpenStack is interconnected, services can be provisioned based on IPv6 and IPv4, including but not limited to subnet, port, QoS, bare metal server, metadata proxy, security group, security policy, VPC communication, and external network.
	To ensure bare metal server provisioning security, the controller automatically converts security groups in OpenStack to ACLs on server leaf switches and implements security group policies to ensure the same security experience of VMs and bare metal servers. **A solution test report issued by a third-party authoritative organization must be provided.**
	In the OpenStack VXLAN overlay solution, leaf switches (access switches) can be used as VXLAN VTEP devices. The switch hardware encapsulates and decapsulates VXLAN packets, relieving the processing pressure on the host network.
	To ensure secure and reliable interconnection with OpenStack, two-way certificate authentication needs to be supported between the cloud platform plug-in and the controller, including HTTPS, WebSocket, and SAN authentication. **Detailed operation instructions must be provided.**
Container interconnection	Mainstream container software such as open-source K8S, Docker, and CCE Agile can be interconnected through plug-ins to implement collaborative provisioning of container network services.
	Cluster IP addresses are supported. The container plug-in detects the cluster IP address and notifies the controller of the cluster IP address information, which is then saved on the controller.
	Node ports are supported. The container plug-in detects the node port and notifies the controller of node port information, which is then saved on the controller.
	Visualized container network model: The container logical network topology and application network topology are visualized. **A solution test report issued by a third-party authoritative organization must be provided.**
VMware interconnection	The controller can be integrated with the VMware vCenter to push the virtual network configurations to the vSwitch, implementing unified planning of physical and virtual networks. The controller can detect VM online, offline, and migration events to implement on-demand delivery and migration of network configurations. **A solution test report issued by a third-party authoritative organization must be provided.**
	The controller supports interconnection with VMware Fault Tolerance (FT) to provide higher reliability than HA. **A solution test report issued by a third-party authoritative organization must be provided.**
	The controller supports interconnection with multiple vCenters and cross-vCenter VM migration. **A solution test report issued by a third-party authoritative organization must be provided.**
	When the controller interconnects with VMware, the PVLAN mode can be enabled on VMware to isolate traffic of different VMs in a port group by default. In this way, VMs can communicate with each other only through the switch. Microsegmentation rules can be configured on the switch to allow only communication between VMs on the same subnet.
Overlay services	To minimize the impact of flooding on the network, the controller must support the flooding suppression function. The SDN controller or switch must be able to enable or disable this function. When this function is enabled, flooding of broadcast, unknown unicast, and unknown multicast packets can be effectively prevented, minimizing the impact of flooding on the network.
	To inherit the O&M habits on the live network, the system must support both drag-and-drop and CLI-based configuration management. In addition, the lock mechanism must be provided to prevent configuration conflicts. **A solution test report issued by a third-party authoritative organization must be provided.**
	Layer 2 and Layer 3 multicast service deployment in VXLAN scenarios needs to be supported.
	To facilitate the evolution from IPv4 to IPv6, the system must support IPv6/IPv4 VXLAN overlay service networking. **A solution test report issued by a third-party authoritative organization must be provided.**
	To improve the batch configuration efficiency, the system needs to support batch import of static routes, VPCs, external gateways, and SFC rules, batch export of configurations based on VPCs and devices, and batch modification of port names and descriptions, device passwords, and RR configurations on spine nodes. **A solution test report issued by a third-party authoritative organization must be provided.**
	To ensure high availability of the connection between the data center and external network, the controller needs to support multiple groups of egress gateways. If any group of egress gateways is faulty, the egress connectivity can still be ensured. **A solution test report issued by a third-party authoritative organization must be provided.**
	Autonomous driving intent translation: To simplify overlay network deployment and improve service deployment efficiency, the system must automatically identify user intents and intelligently recommend logical network solutions without the need of service orchestration, including application launch, offline, change, and interconnection. **A solution test report issued by a third-party authoritative organization must be provided.**
	Simulation and verification: To ensure the correctness of overlay service delivery and configuration changes, the controller needs to support online minute-level simulation and verification before overlay service provisioning and configuration changes (IPv4 and IPv6). Based on the existing and new configurations of devices, the controller performs modeling and simulation on resources, connectivity, and change impact. The configuration changes to be verified include logical networks, microsegmentation, external networks, and VPC communication. The resources to be verified include

	VRFs, static routes, Layer 2 sub-interfaces, and VNIs/BDs/EVPNs. This prevents incorrect configurations from affecting existing services. **A solution test report issued by a third-party authoritative organization must be provided.**
	To quickly roll back services that do not meet expectations after service deployment, the system needs to support three-level rollback: service-level, tenant-level, and network-wide rollback. **A solution test report issued by a third-party authoritative organization must be provided.**
	To ensure southbound and northbound data consistency, the controller needs to support configuration data consistency verification with the cloud platform in the northbound direction and with switches in the southbound direction. **A solution test report issued by a third-party authoritative organization must be provided.**
Service Function Chaining (SFC)	Security policy resource pools can be constructed to effectively protect east-west access. The controller implements security isolation based on application groups. Application groups are divided based on service requirements and are decoupled from the topology and infrastructure. Terminals in the same IP subnet can be allocated to different application groups. This ensures that communication between terminals in different application groups is controlled and filtered by an inter-group policy even if the terminals are in the same subnet and use the same gateway.
	SFC: To save ACL resources, the system needs to support the IETF standard SFC model, NSH- and PBR-based SFC modes, and IPv4/IPv6 SFC protocols. **A solution test report issued by a third-party authoritative organization must be provided.**
	To meet different service security requirements, the system needs to support orchestration of L4-L7 services such as WAF, NAT, IPsec, and firewall through the SFC, and ensure that service traffic traverses multi-hop service nodes for security protection.
	To meet different service security requirements, the system needs to ensure security for intra-VPN east-west traffic, inter-VPN east-west traffic, inter-fabric east-west traffic, and traffic between tenant services in a fabric and external network users through the SFC.
	SFC bypass: In a multi-hop SFC, if a firewall is faulty, traffic can bypass the faulty node to prevent services from being affected.
Microsegmentation	To provide more fine-grained grouping than subnets for security protection, the system needs to support IPv4/IPv6 microsegmentation and use EPG policies on switches to implement security control and isolation.
	The controller needs to support microsegmentation scenarios where the source and destination EPG members are in different fabrics so that the microsegmentation service can be deployed across fabrics.
Multi-DC	To enable interconnection between different DC equipment rooms, the system needs to support multi-DC interconnection scenarios such as multi-fabric interconnection, edge DC access to the central DC, and remote DC interconnection.
	The system needs to support multi-DC collaborative management across domain controllers. Users can quickly orchestrate cross-domain services through the unified GUI in drag-and-drop mode. Transit fabrics can be created for multi-cloud service orchestration, and transit VPCs can be instantiated in the transit fabric to implement cross-DC communication of multi-tenant VPCs. In addition, DCs can be interconnected through private lines. **A solution test report issued by a third-party authoritative organization must be provided.**
	The controller needs to support collaboration management with public clouds (such as AWS) across domain controllers. The controller invokes public cloud APIs to automatically orchestrate services such as VPCs and restore topologies on the public cloud, without the need to deploy additional virtual network devices on the public cloud. **A solution test report issued by a third-party authoritative organization must be provided.**
	To ensure the correctness of cross-DC service provisioning and configuration changes, the system needs to support pre-event simulation and verification of cross-DC network services. Before service provisioning, the system performs modeling and simulation of resources, connectivity, and change impact to prevent incorrect configurations from affecting existing services. **A solution test report issued by a third-party authoritative organization must be provided.**
	To ensure the deterministic SLA of cross-cloud services, the controller needs to allow inter-DC services to enter different SRv6 tunnels based on users' service requirements.
Network visibility	To better locate devices, configurations, and faults, the system needs to support associated display of applications, logical topologies, and physical topologies as well as display of mapping relationships. **A solution test report issued by a third-party authoritative organization must be provided.**
Anomaly detection	To better detect exceptions on the network, the system needs to be able to detect possible loops and failure points on the VXLAN network and provide the measures to eliminate loops. The system can detect loops on a single interface of a single device, on multiple interfaces of a single device, and between devices. **A solution test report issued by a third-party authoritative organization must be provided.**
Troubleshooting	To better analyze the impact of operations on services during troubleshooting, the system needs to support service impact analysis before device replacement or operations on faults, collect statistics on and display the services (including access, egress, and security services) affected by device replacement or faults, and service details. **A solution test report issued by a third-party authoritative organization must be provided.**
	To quickly remediate faults, the controller needs to be able to collaborate with the analyzer to demarcate faults within 1 minute, locate faults within 3 minutes, and rectify faults within 5 minutes. In addition, the

	controller can remediate at least 20 types of faults through collaboration with the analyzer, including configuration change impact analysis and troubleshooting policy delivery. **A solution test report issued by a third-party authoritative organization must be provided.**
	To quickly restore the mistakenly deleted configurations during emergency troubleshooting, the controller needs to support configuration audit to discover the configurations that are mistakenly deleted from switches supporting both GUI- and CLI-based configuration and one-click restoration of the mistakenly deleted configurations. **A solution test report issued by a third-party authoritative organization must be provided.**
Information display	To help users learn about the network status in a timely manner, the controller needs to display brief information about the device hardware, underlay/overlay network, and controller on the SDN network, as well as related statistics such as logs and alarms. In addition, the controller needs to display detailed information about the physical network, including the configuration and running status of the gateway, and detailed information about the virtual network such as the virtual link layer network, virtual router, virtual port, and virtual subnet.
	To quickly notify users of faults on the live network, the controller needs to be able to automatically notify related personnel by email or SMS upon a fault.
	To help users have an in-depth understanding of the network, the controller needs to support device performance monitoring, including the CPU usage, memory usage, device usage, and daily unreachable rate. The controller also supports unified display of network device entities, panels, electronic labels, and network device interfaces.
Security audit requirements	The controller records the change person, change time, and change content involved in a configuration change of each managed object in detail.
Security control	The controller supports role-based access control to isolate tenants and manage user accounts and permissions.
	The controller supports password-based local authentication and user security authentication such as RADIUS and LDAP authentication.
	The controller allows user addition and password change for existing users.

(ຕົວຢ່າງ) ລາຍລະອຽດເອກະສານການປະມູນ (ກະລຸນາຕື່ມຂໍ້ມູນ ແລະ ເຊັນຢັ້ງຢືນ)

- ອີງຕາມໃບແຈ້ງປະມູນ ສະບັບເລກທີ ……/ທຄຕລ, ລົງວັນທີ ……..

ລ/ດ	ຜູ້ສະໜອງ	ເງື່ອນໄຂ									ໝາຍເຫດ
		ໃບທະບຽນວິສາຫະກິດ	ໃບຢັ້ງຢືນການເສຍອາກອນ 2020	ໃບອະນຸຍາດດຳເນີນທຸລະກິດ 2021	ໄລຍະເວລາໃນການດຳເນີນທຸລະກິດ	ຜົນງານຜ່ານມາ (ເຄີຍສະໜອງໃຫ້ພາກສ່ວນໃດແນ່)	ປະເພດ / ວັດສະດຸ / ຍີ່ຫໍ້ສິນຄ້າ	ປະເທດຜະລິດ	ການຮັບປະກັນສິນຄ້າ	ກຳນົດສົ່ງ (ວັນ)	
1	ບ/ສ……	(xxx/ 02.01.2015)	(xxx/ 02.01.2015)	(xxx/ 02.01.2015)	…. ປີ	(ໃຫ້ລະບຸ)		ປະເທດ.....	…. ປີ	……	

ໝາຍເຫດ: ຂໍ້ມູນທີ່ແຈ້ງຂ້າງເທິງນີ້ ເປັນຄວາມຈິງທຸກປະການ, ຖ້າມີຂໍ້ມູນຜິດພາດ ຂ້າພະເຈົ້າຂໍຮັບຜິດຊອບເອງທຸກປະການ.

ນະຄອນຫຼວງວຽງຈັນ, ວັນທີ .....
ຜູ້ອຳນວຍການບໍລິສັດ

ຜູ້ປະສານງານບໍລິສັດ:
ຊື່:
ໂທ: