ПРИЛОЖЕНИЕ 1 – Технически спецификации и технически условия за изпълнение на поръчката към Заявка за стартиране на процедура с предмет

Доставка на комуникационно оборудване за изграждане на опорна телекомуникационна мрежа между поделенията на Дружеството използвайки изградената по фонд „Козлодуй“оптична свързаност.

1. *Технически спецификации и технически условия за изпълнение на поръчката:*

Всички продукти да са напълно съвместими със съществуващата инфраструктура в „Мини Марица-изток“ ЕАД

Позиция 1. Комутатор 24 open SFP slots, окомплектован с 12 бр. 1G SFP RJ45 T и 6 бр. 1G SFP LC LX Transceivers.

Основни характеристики

Входно-изходни портове

24 open mini-GBIC (SFP) slots

Да поддържа 4 бр. 10GbE ports, с допълнителен модул.

12 бр. SFP RJ45 IEEE 802.3ab Type 1000BASE-T Transivers, поддържащи 100 Mb/s и 1000 Mb/s

6 бр. SFP LC IEEE 802.3z Type 1000BASE-LX (10 km SM, 550 m MM) Transivers

Производителност

Throughput	да постига 75.7 million pps
Routing/Switching capacity	мин. 101.8 Gb/s
Switch fabric speed	мин. 105.6 Gb/s
Routing table size	мин. 10000 entries (IPv4)

Захранване

Автоматично регулиране на входно напрежение между 100-127 и 200-240 V с честота 50 или 60 Hz.

Монтаж

Да се монтира в стандартен EIA 19“ telco rack

Поддържани протоколи и стандарти

BGP
- RFC 1997 BGP Communities Attribute
- RFC 2918 Route Refresh Capability
- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
- RFC 5492 Capabilities Advertisement with BGP-4

Device management
- RFC 1591 DNS (client)
- HTML and telnet management

General protocols
- IEEE 802.1ad Q-in-Q
- IEEE 802.1AX-2008 Link Aggregation

IEEE 802.1D MAC Bridges
IEEE 802.1p Priority
IEEE 802.1Q VLANs
IEEE 802.1s Multiple Spanning Trees
IEEE 802.1v VLAN classification by Protocol and Port
IEEE 802.1w Rapid Reconfiguration of Spanning Tree
IEEE 802.3ad Link Aggregation Control Protocol (LACP)
IEEE 802.3x Flow Control
RFC 768 UDP
RFC 783 TFTP Protocol (revision 2)
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 TELNET
RFC 868 Time Protocol
RFC 951 BOOTP
RFC 1058 RIPv1
RFC 1350 TFTP Protocol (revision 2)
RFC 1519 CIDR
RFC 1542 BOOTP Extensions
RFC 2030 Simple Network Time Protocol (SNTP) v4
RFC 2131 DHCP
RFC 2453 RIPv2
RFC 2548 (MS-RAS-Vendor only)
RFC 3046 DHCP Relay Agent Information Option
RFC 3576 Ext to RADIUS (CoA only)
RFC 3768 VRRP
RFC 4675 RADIUS VLAN & Priority
RFC 5798 VRRP (exclude Accept Mode and sub-sec timer)
UDLD (Uni-directional Link Detection)

IP multicast
RFC 3376 IGMPv3 (host joins only)
RFC 3973 PIM Dense Mode
RFC 4601 PIM Sparse Mode

IPv6
RFC 1981 IPv6 Path MTU Discovery
RFC 2375 IPv6 Multicast Address Assignments
RFC 2460 IPv6 Specification
RFC 2464 Transmission of IPv6 over Ethernet Networks
RFC 2710 Multicast Listener Discovery (MLD) for IPv6
RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only)
RFC 3019 MLDv1 MIB
RFC 3315 DHCPv6 (client and relay)
RFC 3484 Default Address Selection for IPv6
RFC 3587 IPv6 Global Unicast Address Format
RFC 3596 DNS Extension for IPv6
RFC 3810 MLDv2 for IPv6

RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC 4022 MIB for TCP
RFC 4087 IP Tunnel MIB
RFC 4113 MIB for UDP
RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers
RFC 4251 SSHv6 Architecture
RFC 4252 SSHv6 Authentication
RFC 4253 SSHv6 Transport Layer
RFC 4254 SSHv6 Connection
RFC 4291 IP Version 6 Addressing Architecture
RFC 4293 MIB for IP
RFC 4294 IPv6 Node Requirements
RFC 4419 Key Exchange for SSH
RFC 4443 ICMPv6
RFC 4541 IGMP & MLD Snooping Switch
RFC 4861 IPv6 Neighbor Discovery
RFC 4862 IPv6 Stateless Address Auto-configuration
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
RFC 5340 OSPF for IPv6
RFC 5453 Reserved IPv6 Interface Identifiers
RFC 5519 Multicast Group Membership Discovery MIB (MLDv2 only)
RFC 5722 Handling of Overlapping IPv6 Fragments

MIBs
IEEE 802.1ap (MSTP and STP MIB's only)
RFC 1213 MIB II
RFC 1493 Bridge MIB
RFC 1724 RIPv2 MIB
RFC 1850 OSPFv2 MIB
RFC 2021 RMONv2 MIB
RFC 2096 IP Forwarding Table MIB
RFC 2613 SMON MIB
RFC 2618 RADIUS Client MIB
RFC 2620 RADIUS Accounting MIB
RFC 2665 Ethernet-Like-MIB
RFC 2668 802.3 MAU MIB
RFC 2674 802.1p and IEEE 802.1Q Bridge MIB
RFC 2737 Entity MIB (Version 2)
RFC 2787 VRRP MIB
RFC 2863 The Interfaces Group MIB
RFC 2925 Ping MIB
RFC 2933 IGMP MIB

Network management
IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
RFC 2819 Four groups of RMON: 1 (statistics), 2 (history), 3 (alarm) and 9 (events)
RFC 3176 sFlow
ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED)
SNMPv1/v2c/v3
XRMON

OSPF
- RFC 2328 OSPFv2
- RFC 3101 OSPF NSSA
- RFC 5340 OSPF for IPv6

QoS/CoS
- RFC 2474 DiffServ Precedence, including 8 queues/port
- RFC 2597 DiffServ Assured Forwarding (AF)
- RFC 2598 DiffServ Expedited Forwarding (EF)

Security
- IEEE 802.1X Port Based Network Access Control
- RFC 1492 TACACS+
- RFC 2865 RADIUS (client only)
- RFC 2866 RADIUS Accounting
- RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)
- Secure Sockets Layer (SSL)
- SSHv2 Secure Shell

Поддържани функционалности

Software-defined networking

OpenFlow — supports OpenFlow 1.0 and 1.3 specifications to enable SDN by allowing separation of the data (packet forwarding) and control (routing decision) paths

Quality of Service (QoS)

Advanced classifier-based QoS — classifies traffic using multiple match criteria based on Layer 2, 3, and 4 information; applies QoS policies such as setting priority level and rate limit to selected traffic on a per-port or per-VLAN basis

Layer 4 prioritization — enables prioritization based on TCP/UDP port numbers

Traffic prioritization — allows real-time traffic classification into eight priority levels mapped to eight queues

Bandwidth shaping —

Port-based rate limiting — provides per-port ingress-/egress-enforced increased bandwidth

Classifier-based rate limiting — uses an access control list (ACL) to enforce increased bandwidth for ingress traffic on each port

Reduced bandwidth — provides per-port, per-queue egress-based reduced bandwidth

Class of Service (CoS) — sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ

Management

Remote intelligent mirroring — mirrors selected ingress/egress traffic based on ACL, port, MAC address, or VLAN to a local or remote HP 8200 zl, 6600, 6200 yl, 5400 zl, or 3500 Switch located anywhere on the network

RMON, XRMON, and sFlow — provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events

IEEE 802.1AB Link Layer Discovery Protocol (LLDP) — advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications

Command authorization — leverages RADIUS to link a custom list of CLI commands to an individual network administrator's login; an audit trail documents activity

Friendly port names — allows assignment of descriptive names to ports

Dual flash images — provides independent primary and secondary operating system files for backup while upgrading

Multiple configuration files — stores easily to the flash image

Uni-Directional Link Detection (UDLD) — monitors a cable between two switches and shuts down the ports on both ends if the cable is broken, turning the bidirectional link into a unidirectional one; this prevents network problems such as loops

Management simplicity — provides common software features and CLI implementation across all ProVision-based switches (including the zl and yl switches)

Comware CLI —

Comware-compatible CLI — bridges the experience of HP Comware CLI users who are using the HP ProVision software CLI

Display and fundamental Comware CLI commands — are embedded in the switch CLI as native commands; display output is formatted as on Comware-based switches, and fundamental commands provide a Comware-familiar initial switch setup

Configuration Comware CLI commands — when Comware commands are entered, CLI help is elicited to formulate the correct ProVision software CLI command

Connectivity

Jumbo frames — on Gigabit Ethernet and 10-Gigabit Ethernet ports, jumbo frames allow high-performance remote backup and disaster-recovery services

IPv6 —

IPv6 host — enables switches to be managed in an IPv6 network

Dual stack (IPv4 and IPv6) — transitions from IPv4 to IPv6, supporting connectivity for both protocols

MLD snooping — forwards IPv6 multicast traffic to the appropriate interface

IPv6 ACL/QoS — supports ACL and QoS for IPv6 network traffic

IPv6 routing — supports static and OSPFv3 routing protocols

6in4 tunneling — supports encapsulation of IPv6 traffic in IPv4 packets

Performance

High-speed, high-capacity architecture — 105.6 Gbps crossbar switching fabric provides intramodule and intermodule switching with 75.7 million pps

Selectable queue configurations — allows for increased performance by selecting the number of queues and associated memory buffering that best meet the requirements of the network applications

Resiliency and high availability

Virtual Router Redundancy Protocol (VRRP) — allows groups of two routers to dynamically back each other up to create highly available routed environments in IPv4 and IPv6 networks

IEEE 802.1s multiple Spanning Tree Protocols — provides high link availability in multiple VLAN environments by allowing multiple spanning trees; encompasses IEEE 802.1D Spanning Tree Protocol and IEEE 802.1w Rapid Spanning Tree Protocol

IEEE 802.3ad Link Aggregation Control Protocol (LACP) and HP port trunking — support up to 144 trunks, each with up to eight links (ports) per trunk

Distributed trunking — enables loop-free and redundant network topology without using Spanning Tree Protocol; allows a server or switch to connect to two switches using one logical trunk for redundancy and load sharing

Uplink Failure Detection — provides active-standby network path redundancy for servers that are configured for active-standby NIC teaming

NEW SmartLink — provides easy-to-configure link redundancy of active and standby links

Layer 2 switching

IEEE 802.1ad Q-in-Q — increases the scalability of an Ethernet network by providing a hierarchical structure; connects multiple LANs on a high-speed campus or metro network

HP switch meshing — dynamically load balances across multiple active redundant links to increase available aggregate bandwidth

VLAN support and tagging — supports complete IEEE 802.1Q standard and 2,048 VLANs simultaneously

IEEE 802.1v protocol VLANs — isolate select non-IPv4 protocols automatically into their own VLANs

GARP VLAN Registration Protocol — allows automatic learning and dynamic assignment of VLANs

Rapid Per-VLAN Spanning Tree (RPVST+) — allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+

Layer 3 services

User Datagram Protocol (UDP) helper function — allows UDP broadcasts to be directed across router interfaces to specific IP unicast or subnet broadcast addresses and prevents server spoofing for UDP services such as DHCP

Loopback interface address — defines an address in Routing Information Protocol (RIP) and Open Standard Path First (OSPF), improving diagnostic capability

Route maps — provide more control during route redistribution; allow filtering and altering of route metrics

Layer 3 routing

Static IP routing — provides manually configured routing for both IPv4 and IPv6 networks

Routing Information Protocol (RIP) — provides RIPv1 and RIPv2 routing

OSPF — provides OSPFv2 for IPv4 routing and OSPFv3 for IPv6 routing

Border Gateway Protocol (BGP) — provides IPv4 Border Gateway Protocol routing, which is scalable, robust, and flexible

Security

Switch CPU protection — provides automatic protection against malicious network traffic trying to shut down the switch

Virus throttling — detects traffic patterns typical of worm-type viruses and either throttles or entirely prevents the virus from spreading across the routed VLANs without requiring external appliances

ICMP throttling — defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic

Multiple user authentication methods —

IEEE 802.1X users per port — provides authentication of multiple IEEE 802.1X users per port

Web-based authentication — authenticates from Web browser for clients that do not support IEEE 802.1X supplicant

MAC-based authentication — authenticates client with the RADIUS server based on client's MAC address

Concurrent IEEE 802.1X, Web, and MAC authentication schemes per port — switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications

Access control lists (ACLs) — provide filtering based on the IP field, source/destination IP address/subnet, and source/destination TCP/UDP port number on a per-VLAN or per-port basis

Identity-driven ACL — enables implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user

DHCP protection — blocks DHCP packets from unauthorized DHCP servers, preventing denial-of-service attacks

STP BPDU port protection — blocks Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks

Dynamic IP lockdown — works with DHCP protection to block traffic from unauthorized hosts, preventing IP source address spoofing

Dynamic ARP protection — blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data

Detection of malicious attacks — monitors 10 types of network traffic and sends a warning when an anomaly that potentially can be caused by malicious attacks is detected

Port security — allows access only to specified MAC addresses, which can be learned or specified by the administrator

MAC address lockout — prevents particular configured MAC addresses from connecting to the network

Source-port filtering — allows only specified ports to communicate with each other

RADIUS/TACACS+ — eases switch management security administration by using a password authentication server

Secure shell — encrypts all transmitted data for secure remote CLI access over IP networks

Secure Sockets Layer (SSL) — encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch

Secure FTP — allows secure file transfer to and from the switch; protects against unwanted file downloads or unauthorized copying of a switch configuration file

Management Interface Wizard — helps secure management interfaces such as SNMP, telnet, SSH, SSL, Web, and USB at the desired level

Secure management access — delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3

Switch management logon security — helps secure switch CLI logon by optionally requiring either RADIUS or TACACS+ authentication

Security banner — displays customized security policy when users log in to the switch

STP root guard — protects the root bridge from malicious attacks or configuration mistakes

Convergence

IP multicast routing — includes PIM Sparse and Dense modes to route IP multicast traffic

IP multicast snooping (data-driven IGMP) — prevents flooding of IP multicast traffic

LLDP-MED (Media Endpoint Discovery) — defines a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones

Auto VLAN configuration for voice —

RADIUS VLAN — uses a standard RADIUS attribute and LLDP-MED to automatically configure a VLAN for IP phones

CDPv2 — uses CDPv2 to configure legacy IP phones

Local MAC Authentication — assigns attributes such as VLAN and QoS using locally configured profile that can be a list of MAC prefixes

Гаранции и поддръжка

Доживотна гаранция

Свободно и безплатно изтегляне на софтуерни версии от интернет портал на производителя

2. ***Изисквания към потенциалните контрагенти и съпровождащи изпълнението на поръчката документи:***

- ✓ Участникът да има внедрена система за управление на качеството (доказва се с валиден сертификат ISO 9001 или еквивалентен);
- ✓ Участникът да притежава валиден партньорски договор с производителя на изделията, предмет на настоящата процедура;
- ✓ Участникът да е оторизиран сервиз на производителя на предложената техника;
- ✓ Всички изделия да са произведени от един производител – доказва се с декларация и разпечатка от Интернет;
- ✓ Участникът да притежава офис и/или сервизна база с посочване на стационарен телефон и лице за контакти. Доказва се със заверено копие на документ за собственост или документ за наем на офиса и/или сервизната база. Да има назначени в този офис и/или сервизна база минимум двама сертифицирани от производителя на предлаганата техника специалисти за поддръжка и ремонт на изделията. Доказва се със заверени копия на трудовите договори и валидни сертификати от производителя;
- ✓ Участникът да има изградена интегрирана сервизна информационна система – Helpdesk/Servicedesk предлагаща различни комуникационни канали за приемане на заявки за сервизно обслужване: телефон, факс, e-mail, web интерфейс;

ИЗГОТВИЛ:

инж. Динко Вълчев
Аналитик КК, отдел ИТ

инж. Георги Георгиев
Р-л на ОП „ИТ“