

Požadované technické parametry dodávky

Předmětem dodávky jsou aktivní síťové prvky a optické SFP+ moduly dle technických podmínek uvedených níže:

- Přístupový/agregační přepínač (1 ks),
- Přístupový stohovatelný 48 portový gigabitový přepínač s 10Gb uplink portem (8 ks),
- Přístupový stohovatelný 48 portový gigabitový přepínač s 1Gb uplink portem (17 ks),
- Bezdrátový přístupový bod (45 ks),
- Optické SFP+ moduly (16ks).

Tabulka povinných požadavků pro přístupový/agregační přepínač (požadován 1 ks)

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Typ zařízení	L3 přepínač
Formát zařízení	1RU, fixní konfigurací, s rozšiřujícím slotem uplink modulu
Počet portů	16x SFP+, podporujících i SFP moduly
Počet rozšiřujících slotů	1
Uplink moduly vyměnitelné za chodu (hot swap)	ano
Typ uplink modulu	8x SFP+, podporujících i SFP moduly
Uplink modul požadován	ano
Redundantní AC zdroje	ano
Napájecí zdroje vyměnitelné za chodu	ano
Proudění chladicího vzduchu zepředu dozadu (front-to-back)	ano
Změna směru proudění chladicího vzduchu pouhou výměnou ventilátorů a zdrojů	ano
Redundantní ventilátory (výpadek jednoho nemá vliv na funkci přepínače), vyměnitelné za chodu	ano
Podpora Non-Stop Forwarding NSF se zachováním stavových informací	ano, ve dvojici
Podpora upgrade software za provozu (ISSU)	ano, ve dvojici
Statické směrování IPv4	ano
Dynamické směrování IPv4	ano
Podpora IPv4, IPV6 v hardware	ano
Výkonnostní parametry	
Celková propustnost řídicích modulů (IPv4/IPv6)	240/120 Mp/s
Celková potenciální propustnost přepínacího subsystému	480 Gbit/s
Minimální počet záznamů ve směrovací tabulce - IPv4 unicast	32000
Minimální počet záznamů ve směrovací tabulce - IPv6 unicast	24000
Minimální počet záznamů ve směrovací tabulce - IPv4 multicast	12000
Minimální počet záznamů ve směrovací tabulce - IPv6 multicast	6000
Počet MAC adres	32000
Protokoly fyzické vrstvy	

IEEE 802.3-2005	ano
IEEE 802.3ad	ano
IEEE 802.3ad přes více přepínačů	ano
Podpora "jumbo rámců"	ano
Protokoly linkové vrstvy	
IEEE 802.1D	ano
IEEE 802.1Q	ano
Minimální počet aktivních VLAN	4000
Tunelování 802.1Q v 802.1Q	ano
IEEE 802.1X - Port Based Network Access Control	ano
IEEE 802.1s - multiple spanning trees	ano
IEEE 802.1w - Rapid Tree Spanning Protocol	ano
IEEE 802.1p	ano
Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní	ano
Detekce protilehlého zařízení (např. CDP)	ano
Protokol pro definici šířených VLAN (např. VTP)	ano
Detekce jednosměrnosti optické linky (např. UDLD)	ano
STP root guard nebo ekvivalentní	ano
STP loop guard nebo ekvivalentní	ano
Možnost automatického zotavení po chybovém stavu (UDLD, root guard, loop guard)	ano
Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ano
Protokol IP	
IP alias (více IP sítí na jednom rozhraní)	ano
QoS dle DiffServ	ano
DHCP relay	ano
Router redundancy protokol (např. VRRP, HSRP)	ano
Protokol IPv6	
Certifikace IPv6 ready logo – Phase II	ano
Podpora HSRP nebo VRRP pro IPv6	ano
Podpora IPv6 ACL	ano
Podpora IPv6 QoS dle DiffServ	ano
Podpora IPv6 services (DNS, Telnet, SSH, Syslog, ICMP, DHCP)	ano
Podpora IPv6 Multicast (MLDv1 & v2)	ano
Podpora IPv6 Multicast (PIM SSM)	ano
Podpora IPv6 Multicast (PIM SM)	ano
Podpora OSPFv3	ano
Podpora MP BGP	ano
Podpora IS-IS pro IPv4 a IPv6	ano
Podpora IPv6 MLDv2 snooping	ano
Podpora IPv6 First Hop Security (IPv6 Port ACL, RA guard)	ano
Podpora IPv6 SLA	ano
Podpora IPv6 Tunneling: ISATAP Tunnel	ano
Podpora DHCPv6 Relay	ano
Směrovací protokoly	
BGPv4	ano
OSPF	ano
OSPF s MD5 a NSSA	ano

RIPv2	ano
Policy-based routing podle ACL	ano
Statické směrování	ano
Směrování multicastu	
PIM (dense i sparse mód)	ano
Source-Specific Multicast (SSM)	ano
IGMPv2	ano
IGMPv3	ano
IGMPv3 snooping	ano
IPv6 MLDv1 & v2 snooping	ano
Bezpečnost	
Podpora reverse path check (uRPF)	ano
ACL pro IP	ano
IPv6 ACL	ano
Možnost definovat povolené MAC adresy na portu	ano
Možnost definovat maximální počet MAC adres na portu	ano
Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	ano
Podpora zabezpečení a analýzy DHCP protokolu (např. DHCP snooping)	ano
Podpora ochrany ARP protokolu (např. Dynamic ARP inspection)	ano
Podpora ochrany podvrženého mapování IP/MAC adresy (např. IP source guard)	ano
Podpora šifrování na L2 dle IEEE 802.1AE	ano
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ano
Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)	ano
Vynucení IEEE 802.1x ověřování i na externím připojeném přepínači	ano
HW ochrana centrálního procesoru (control plane) před útoky typu DoS	ano
Virtualizace	
Virtualizace směrovače (například Multi-VRF)	ano
Zjednodušená, zautomatizovaná konfigurace virtualizace směrovačů a jejich propojů	ano
Virtualizace dvou fyzických přepínačů do jednoho virtuálního, jedné síťové entity z pohledu L2 i L3	ano
Podpora koncových zařízení	
Měření a ovládání spotřeby energie do LAN připojených koncových zařízení	ano
Management	
CLI rozhraní (příkazová řádka)	ano
Konfigurace zařízení v člověku čitelné textové formě	ano
Možnost povýšení operačního software zařízení po síti pomocí protokolů TFTP, FTP a HTTP	ano
Možnost nahrání/zálohování textové konfigurace zařízení po síti pomocí protokolů TFTP, FTP a HTTP	ano
Podpora vzdáleného přístupu pomocí SSHv2	ano
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
SNMPv2	ano
SNMPv3	ano
Interpretace uživatelských CLI a Tcl skriptů a jejich aktivace asynchronní událostí v systému zařízení	ano
USB port pro datové úložiště a zavádění operačního systému	ano
Sériová konzolová linka	ano

10/100/1000 out-of-band management port	ano
DNS klient	ano
NTP klient s MD5 autentizací	ano
NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955)	ano
Detailní flexibilní definice "flow" dle L2/L3/L4 parametrů	ano
Export statistik "flow" selektivně na více kolektorů	ano
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano
TACACS+ klient	ano
Zrcadlení portů, alespoň 4 paralelní obousměrné relace	ano
Vzdálené zrcadlení portů, alespoň 4 paralelní obousměrné relace	ano
Syslog	ano
Možnost rozšiřování o další funkce licenčními klíči bez nutnosti výměny firmware	ano
Nástroje pro měření odezvy v síti (například IP SLA nebo ekvivalentní)	ano
Nástroje pro pasivní monitorování i aktivní testování odezvy provozovaných aplikací (např. IP SLA Video Operation, performance monitor nebo ekvivalentní)	ano
Možnost v software přepínače integrovat další aplikace (například WireShark, profilování koncových zařízení, ...)	ano
Automatická konfigurace portu dle připojeného zařízení	ano
Proaktivní autodiagnostika HW zařízení při startu i běhu zařízení, konfigurovatelná.	ano
Služby	
Podpora NTP	ano
Zrcadlení portů, alespoň 4 paralelní obousměrné relace	ano

Tabulka povinných požadavků pro přístupový stohovatelný 48 portový gigabitový přepínač s 10Gb uplink portem (požadováno 8 ks)

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Typ zařízení	L2 přepínač
Formát zařízení	1RU
Stohovatelný bez snížení počtu ethernetových portů	ano
Stohování v rámci stohu požadováno	ano
PoE (IEEE 802.3af)	ano
PoE+ (IEEE 802.3at, 30W/port)	ano
Minimální dostupný výkon pro napájení PoE portů pro každého člena stohu	350W
Osazení transeivery	
Možnost volby 1Gbit/s nebo 10Gbit/s rychlosti uplink portu vhodným rozšiřujícím modulem a transeiverem	ano, transeiverem
Možnost připojit redundantní zdroj	ano
Výkonnostní parametry	
Propustnost přepínacího subsystému pro každého člena stohu	200 Gbit/s
Paketový výkon přepínače každého člena stohu	120 milionů paketů/vteřinu
Rychlost stohovacího propojení mezi členy stohu	80 Gbit/s
Počet MAC adres každého člena stohu	15 000
Vlastnosti stohování	
Vzájemné stohování všech modelů členů stohu s 10/100 s 10/100/1000 s 1Gbit/s uplinky s 10Gbit/s uplinky	ano
Počet přepínačů/členů ve stohu	8
Automatická kontrola a sjednocení verze software přepínačů ve stohu	ano
Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením	ano
Seskupení portů (IEEE 802.3ad) mezi různými prvky stohu	ano
Kterýkoli prvek ve stohu může být řídicím prvkem stohu (1:N redundance)	ano

Požadavek na funkcionalitu	Minimální požadavky
Podporované funkce	
IEEE 802.3-2005	ano
IEEE 802.3ad	ano
Hardwarová podpora dlouhých ethernetových rámců, tzv. „jumbo frames“	ano
IEEE 802.1D	ano
IEEE 802.1Q	ano
Počet aktivních VLAN každého přepínače ve stohu	1 000
IEEE 802.1X - Port Based Network Access Control	ano
IEEE 802.1s - multiple spanning trees	ano
IEEE 802.1w - Rapid Tree Spanning Protocol	ano
Per VLAN rapid spanning tree nebo ekvivalentní	ano
IEEE 802.3az	ano
Detekce protilehlého zařízení (např. LLDP)	ano
Detekce parametrů protilehlého zařízení (např. LLDP-MED)	ano
Protokol pro definici šířených VLAN (např. MVRP)	ano
Detekce jednosměrnosti optické linky	ano
STP root guard	ano
STP loop guard	ano
Možnost autorecovery po chybovém stavu (root guard, loop guard)	ano
Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ano
IP alias (více IP sítí na jednom rozhraní)	ano
QoS	ano
QoS i na stohovacím propoju	ano
DHCP relay	ano
Certifikace IPv6 ready logo – Phase II	ano
IPv6 ACL	ano
IPv6 QoS	ano
IPv6 services (DNS, Telnet, SSH, Syslog, ICMP)	ano
HTTP, SNMP over IPv6	ano
RADIUS, TACACS+ over IPv6	ano
IPv6 MLDv2 snooping	ano
IPv6 Port ACL	ano
IPv6 First Hop Security RA guard	ano
IPv6 First Hop Security DHCPv6 guard	ano
IPv6 First Hop Security IPv6 Binding Integrity Guard	ano
IGMPv2 snooping	ano
IGMPv3 snooping	ano
IPv6 MLDv1 & v2 snooping	ano
ACL na rozhraní in/out	ano
ACL pro IP	ano
ACL pro ethernetové rámce	ano
IPv6 ACL	ano
Možnost definovat povolené MAC adresy na portu	ano
Možnost definovat maximální počet MAC adres na portu	ano
Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	ano
DHCP snooping	ano
Dynamic ARP inspection (DAI)	ano
Verifikace mapování IP-MAC (např. IP source guard)	ano
IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu	ano
IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači, sdílení ověření koncových stanic	ano
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ano

Požadavek na funkcionalitu	Minimální požadavky
Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)	ano
Detekce parametrů připojovaného koncového zařízení a jejich sdílení s policy serverem	ano
PoE (IEEE 802.3af)	ano
PoE+ (IEEE 802.3at, 30W/port)	ano
Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury	ano
CLI rozhraní	ano
SSHv2	ano
SSHv2 over IPv6	ano
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
SNMPv2	ano
SNMPv3	ano
USB konzolová linka	ano
Sériová konzolová linka	ano
10/100 management out-of-band port	ano
DNS klient	ano
NTP klient s MD5 autentizací	ano
IPFIX RFC 3917, RFC 3955 (např. jFlow, NetFlow)	ano
Sběr dat pro IPFIX (např. jFlow, NetFlow) export z každého portu přepínače.	ano
Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů	ano
Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb	ano
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano
TACACS+ klient	ano
Port mirroring (SPAN)	ano
Port mirroring 1 -> 1	ano
Port mirroring N -> 1	ano
Port mirroring ACL (mirroruje pouze definované toky)	ano
Vzdálený port mirroring (RSPAN)	ano
Syslog	ano
Měření zakončení a délky metalického kabelu (TDR)	ano
Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů)	ano
Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute)	ano
Přepínač si může automaticky zazálohovat a obnovit firmware včetně konfigurace z nadřazeného směrovače nebo přepínače	ano
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ano
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ano

Tabulka mandatorních požadavků pro přístupový stohovatelný 48 portový gigabitový přepínač s 1Gb uplink portem (požadováno 17 ks)

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Typ zařízení	L2 přepínač
Formát zařízení	1RU
Stohovatelný bez snížení počtu ethernetových portů	ano
Stohování v rámci stohu požadováno	ano
PoE (IEEE 802.3af)	ano
PoE+ (IEEE 802.3at, 30W/port)	ano
Minimální dostupný výkon pro napájení PoE portů pro každého člena stohu	350W
Osazení transeivery	

Požadavek na funkcionalitu	Minimální požadavky
Možnost volby 1Gbit/s rychlosti uplink portu vhodným rozšiřujícím modulem a transceiverem	ano, transceiverem
Možnost připojit redundantní zdroj	ano
Výkonnostní parametry	
Propustnost přepínacího subsystému pro každého člena stohu	200 Gbit/s
Paketový výkon přepínače každého člena stohu	120 milionu paketů/vteřinu
Rychlost stohovacího propojení mezi členy stohu	80 Gbit/s
Počet MAC adres každého člena stohu	15 000
Vlastnosti stohování	
Vzájemné stohování všech modelů členů stohu s 10/100 s 10/100/1000 s 1Gbit/s uplinky s 10Gbit/s uplinky	ano
Počet přepínačů/členů ve stohu	8
Automatická kontrola a sjednocení verze software přepínačů ve stohu	ano
Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením	ano
Seskupení portů (IEEE 802.3ad) mezi různými prvky stohu	ano
Kterýkoli prvek ve stohu může být řídicím prvkem stohu (1:N redundance)	ano
Podporované funkce	
IEEE 802.3-2005	ano
IEEE 802.3ad	ano
Hardwarová podpora dlouhých ethernetových rámců, tzv. „jumbo frames“	ano
IEEE 802.1D	ano
IEEE 802.1Q	ano
Počet aktivních VLAN každého přepínače ve stohu	1 000
IEEE 802.1X - Port Based Network Access Control	ano
IEEE 802.1s - multiple spanning trees	ano
IEEE 802.1w - Rapid Tree Spanning Protocol	ano
Per VLAN rapid spanning tree nebo ekvivalentní	ano
IEEE 802.3az	ano
Detekce protilehlého zařízení (např. LLDP)	ano
Detekce parametrů protilehlého zařízení (např. LLDP-MED)	ano
Protokol pro definici šířených VLAN (např. MVRP)	ano
Detekce jednosměrnosti optické linky	ano
STP root guard	ano
STP loop guard	ano
Možnost autorecovery po chybovém stavu (root guard, loop guard)	ano
Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ano
IP alias (více IP sítí na jednom rozhraní)	ano
QoS	ano
QoS i na stohovacím propoji	ano
DHCP relay	ano
Certifikace IPv6 ready logo – Phase II	ano
IPv6 ACL	ano
IPv6 QoS	ano
IPv6 services (DNS, Telnet, SSH, Syslog, ICMP)	ano
HTTP, SNMP over IPv6	ano
RADIUS, TACACS+ over IPv6	ano
IPv6 MLDv2 snooping	ano
IPv6 Port ACL	ano
IPv6 First Hop Security RA guard	ano
IPv6 First Hop Security DHCPv6 guard	ano
IPv6 First Hop Security IPv6 Binding Integrity Guard	ano
IGMPv2 snooping	ano
IGMPv3 snooping	ano

Požadavek na funkcionalitu	Minimální požadavky
IPv6 MLDv1 & v2 snooping	ano
ACL na rozhraní in/out	ano
ACL pro IP	ano
ACL pro ethernetové rámce	ano
IPv6 ACL	ano
Možnost definovat povolené MAC adresy na portu	ano
Možnost definovat maximální počet MAC adres na portu	ano
Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	ano
DHCP snooping	ano
Dynamic ARP inspection (DAI)	ano
Verifikace mapování IP-MAC (např. IP source guard)	ano
IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu	ano
IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači, sdílení ověření koncových stanic	ano
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ano
Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)	ano
Detekce parametrů připojovaného koncového zařízení a jejich sdílení s policy serverem	ano
PoE (IEEE 802.3af)	ano
PoE+ (IEEE 802.3at, 30W/port)	ano
Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury	ano
CLI rozhraní	ano
SSHv2	ano
SSHv2 over IPv6	ano
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
SNMPv2	ano
SNMPv3	ano
USB konzolová linka	ano
Sériová konzolová linka	ano
10/100 management out-of-band port	ano
DNS klient	ano
NTP klient s MD5 autentizací	ano
IPFIX RFC 3917, RFC 3955 (např. jFlow, NetFlow)	ano
Sběr dat pro IPFIX (např. jFlow, NetFlow) export z každého portu přepínače.	ano
Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů	ano
Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb	ano
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano
TACACS+ klient	ano
Port mirroring (SPAN)	ano
Port mirroring 1 -> 1	ano
Port mirroring N -> 1	ano
Port mirroring ACL (mirroruje pouze definované toky)	ano
Vzdálený port mirroring (RSPAN)	ano
Syslog	ano
Měření zakončení a délky metalického kabelu (TDR)	ano
Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů)	ano
Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute)	ano
Přepínač si může automaticky zazálohovat a obnovit firmware včetně konfigurace z nadřazeného směrovače nebo přepínače	ano
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ano

Požadavek na funkcionalitu	Minimální požadavky
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ano

Tabulka povinných požadavků pro bezdrátový přístupový bod (požadováno 45 ks)

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Typ zařízení	bezdrátový přístupový bod
Rádiové rozhraní pro pásmo 2,4 GHz	ano
Rádiové rozhraní pro pásmo 5 GHz	ano
Počet portů 10/100/1000	2
Podpora IEEE 802.3at napájení z přepínače nebo injektoru	ano
Typ antén	integrované pro obě pásma
Montáž	na betonový strop
Podpora stávajících centralizovaných řadičů bezdrátové sítě	ano
Podpora centralizovaného řadiče poptávaného v této ZD	ano
Výkonnostní parametry	
Fyzická přenosová rychlost bezdrátové části	1,3 Gb/s
Protokoly fyzické vrstvy	
IEEE 802.11a/b/g/n/ac	ano
Podpora standardu IEEE 802.11ac Wave2	ano
MIMO (Multiple Input Multiple Output)	4x4:3
Podpora Multiuser Multiple-Input Multiple-Output (MU-MIMO)	ano
IEEE 802.11n Maximal ratio combining (MRC)	ano
Agregace rámců A-MPDU a A-MSDU	ano
Dynamický výběr volné frekvence DFS	ano
Podpora 20 MHz a 40 MHz kanálů pro IEEE 802.11n	ano
Podpora 80 MHz a 16MHz kanálů pro IEEE 802.11ac	ano
Optimalizace fáze vysílaného bezdrátového signálu směrem k 802.11a/g/n klientům (Beam Forming)	ano
Podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma	ano
Hardwarová podpora spektrální analýzy (detekce zdroje rušivého signálu – interferencí)	ano
Hardwarová podpora rozpoznání zdroje rušivého signálu podle signatur	ano
Podpora výpočtu závažnosti dopadu interference na kvalitu radiového signálu bezdrátové sítě	ano
Minimální počet inzerovaných SSID (BSSID)	8/rádiové rozhraní
Nastavitelný DTIM interval pro jednotlivé bezdrátové sítě	ano
Bezpečnost	
Certifikát s lokální platností pro nasazení PKI	ano
Fyzické zabezpečení/zamknutí k okolním pevným částem	ano
Management	
CLI rozhraní	ano
SSHv2	ano
Konzolová linka	ano
Detekce a monitorování problémů bezdrátové sítě odchyťováním provozu a jeho zasíláním do analyzátoru (například Wireshark)	ano

Tabulka povinných požadavků pro optické SFP+ moduly (požadováno 16ks):

Požadavek na funkcionalitu	Minimální požadavky
Rozhraní 10Gb/s	
Požadovaný počet transceiverů 10GE SFP+	10GBase-LR

Požadavky na záruku a servis dodávky

Všechny poptávané aktivní síťové prvky a optické SFP+ moduly musí být z důvodů ochrany stávajících investic a minimalizace celkových nákladů na vlastnictví a provoz počítačové sítě ZČU kompatibilní se všemi již používanými zařízeními, komunikačními protokoly a systémy správy sítě.

Požadovaná záruční doba na dodaná Zařízení činí 60 měsíců.

Další požadované související plnění:

- Dodávka Zboží do místa plnění.
- Technická dokumentace (v elektronické podobě, čeština nebo angličtina).
- Uchazeč poskytne Zadavateli po dobu trvání záruky všechny relevantní verze operačního software nabízené výrobcem tak, aby dodané řešení fungovalo bez závad. Dodavatel se současně zavazuje informovat Zadavatele o nových softwarových verzích a funkcích, které mohou rozšiřovat dodané řešení. Dodavatel se zavazuje získat potřebné softwarové produkty legálním způsobem za podmínek stanovených výrobcem zařízení.
- Uchazeč zajistí Zadavateli přístup k dokumentaci výrobce zařízení a znalostní bázi, pokud ji výrobce v rámci své podpory koncovým uživatelům poskytuje.
- Veškeré zákonem vyžadované dokumenty potřebné pro provoz nabízených zařízení na území České republiky (prohlášení o shodě apod.)
- Uchazeč je povinen zajistit dostupnost nových originálních náhradních dílů od výrobce pro dodané řešení za podmínek specifikovaných Zadavatelem v režimu 8h x 5d x NBD (počet hodin dostupnosti servisu uchazeče x počet dní v týdnu dostupnosti servisu dodavatele x doba pro doručení náhradního dílu Zadavateli do místa plnění).
- Výše specifikovanou záruční lhůtu, servis a dostupnost náhradních dílů Zadavatel požaduje po dobu 60 měsíců.

Struktura technické části nabídky

Technická část nabídky musí obsahovat:

- **Podrobný popis technických a funkčních parametrů** nabízeného řešení, z něhož bude jasně patrné splnění jednotlivých položek technických a funkčních požadavků technického zadání.
- **Podrobný popis servisních a záručních podmínek**, z něhož bude jasně patrné splnění jednotlivých položek servisních a záručních požadavků zadání.
- **Podrobnou položkovou specifikaci** nabízených zařízení (např. typů šasi, jednotlivých modulů, operačního software, napájecích zdrojů apod.).

Popis prostředí počítačové sítě ZČU

1. Používané komunikační protokoly a podpůrné vlastnosti aktivních prvků sítě ZČU

V akademické síti ZČU WEBnet jsou v současné době používány následující komunikační protokoly a další podpůrné vlastnosti aktivních prvků, s nimiž musí být poptávaná zařízení kompatibilní:

- Podpora IEEE 802.1Q/p (minimálně 1000 VLAN, konfigurační možnosti statického omezování šíření VLAN), IEEE 802.1s/w (RSTP/MSTP), IEEE 802.3ad, IGMPv2/v3, MLDv1/v2 a vlastnické L2 protokoly VTPv3, PVRSTP+, CDPv2, UDLD.
- Možnosti ochrany spanning tree protokolu vůči zneužití (filtrace BPDU rámců na jednotlivých rozhraních, kontrola přípustnosti BPDU apod.).
- Podpora agregace linek (LACP nebo PAgP).
- Podpora privátních VLAN (logická izolace jednotlivých rozhraní nebo skupin rozhraní v rámci téže VLAN).
- Podpora omezení (procentuálního poměru) broadcastového a multicastového provozu na rozhraní.
- Duální podpora IPv4 a IPv6 unicast i multicast (možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, dual-stack).
- Podpora směrovacích protokolů BGPv4, OSPFv2, OSPFv3, PIM-SMv2, RIP, statického směrování a možnosti redistribuce směrovacích informací mezi jednotlivými protokoly, rozkládání zatížení na L3 paralelních cestách, možnosti vytváření logicky oddělených instancí virtuálních směrovacích tabulek v rámci téhož L3 přepínače (podpora virtuálních směrovacích instancí).
- Podpora HSRP nebo VRRP pro zajištění redundance výchozí brány koncovým stanicím/serverům.
- Podpora GRE tunelů.
- Podpora IGMPv2, IGMPv3 a hardwarová podpora omezování zbytečného šíření multicastových rámců/paketů na rozhraní bez explicitních příjemců (IGMPv2/v3 a MLDv1/v2 snooping).
- Možnost definovat povolené MAC adresy na portu, jejich maximální počet na portu a definování různého chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy).
- Hardwarová podpora bezstavové bezpečnostní filtrace provozu podle L2/L3/L4 atributů na úrovni linkové/síťové/transportní vrstvy aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní (VLAN).
- Vzdálený management aktivních prvků (typicky pomocí protokolů Telnet, SSH, HTTP/HTTPS nebo SNMPv2/v3).
- Implementace čítačů přenesených bytů/paketů pro jednotlivé relevantní entity síťových informací (typicky rozhraní, filtry apod.) přístupné přes příkazovou řádku a SNMP.
- Možnost nastavení omezení distribuce IP multicastu ve VLAN.
- Možnost ochrany proti útokům na úrovni síťové a linkové vrstvy (IP DHCP Snooping, Dynamic ARP Inspection, IP Source Guard).
- Hardwarová podpora zajištění kvality služby (QoS) podle L2/L3/L4 atributů umožňující implementaci QoS podle modelu rozlišovaných služeb (DiffServ).

2. Nástroje používané pro správu sítě ZČU

Pro správu sítě ZČU jsou používány následující nástroje síťového managementu, s nimiž musí být poptávaná zařízení kompatibilní.

2.1. Správa konfigurací

Zálohování konfigurací všech aktivních komunikačních prvků je prováděno centrálně automaticky pomocí systému RANCID¹ s webovou nadstavbou Subversion (pro přehledné zobrazování změn). Archivace (změn) historie konfigurací je udržována minimálně po dobu jednoho roku. Navíc jsou paralelně zálohovány konfigurace (a jejich přehled sumárních změn) všech aktivních komunikačních prvků pomocí systému NeDi².

Pro hromadné konfigurace skupin zařízení se využívají systémy Netmanager³, umožňující paralelní vykonávání příkazů, a NeDi.

2.2. Správa bezdrátové sítě

Na ZČU je provozována bezdrátová síť eduroam⁴, která podporuje IP mobilitu a roaming uživatelů v rámci české sítě národního výzkumu a vzdělávání. Kromě toho je provozována síť zcu-mobile, která mobilitu a roaming nepodporuje. Pro její provoz byl vyvinut vlastní systém založený na open-source řešení. Obě řešení jsou navázána na AAA infrastrukturu založenou na ověřovacím serveru freeRADIUS⁵. Pro správu a konfiguraci bezdrátových přístupových bodů je využíváno centralizované řešení. Jako centrální prvky jsou použity dva bezdrátové řadiče⁶ pracující v režimu active/active, které jsou schopny současně spravovat až 200 AP. K udržení konzistentní konfigurace obou bezdrátových řadičů je používán specializovaný software⁷.

2.3. Inventarizace síťových zařízení

Pro inventarizaci veškerých síťových zařízení (typicky aktivních komunikačních prvků a koncových zařízení jako jsou uživatelská PC, notebooky, servery a síťové tiskárny) se využívají dva druhy nástrojů:

- registrační systém Sauron⁸ v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet⁹ v prostředí kolejní sítě (včetně funkce řízení přístupu oprávněných uživatelů do sítě na základě konfigurace kolejních DHCP/DNS serverů a pravidel na centrálním kolejním firewallu)
- on-line systémy Netdisco¹⁰ a NeDi, které na základě periodicky získávaných informací z aktivních komunikačních prvků pomocí protokolů SNMP a CDP poskytují informace o zařízeních připojených do sítě (např. počty, typy a verze OS aktivních prvků, informace o topologii sítě, VLAN, IP podsítích, bezdrátových SSID, mapování MAC adres na IP adresy, připojení MAC/IP adres za konkrétními fyzickými porty jednotlivých přepínačů,

¹ <http://www.shrubbery.net/rancid/>

² <http://nedi.ch/>

³ Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

⁴ <http://www.eduroam.cz>

⁵ <http://freeradius.org>

⁶ Bezdrátový řadič Cisco Wireless LAN Controller (WLC) 5508 pro 100 AP a Cisco WLC 4404 pro 100 AP.

⁷ Cisco Prime Infrastructure verze 1.3 pro 200 AP.

⁸ <http://sauron.jyu.fi/>

⁹ Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

¹⁰ <http://www.netdisco.org/>

informace o SMB atd.¹¹) s možností pokročilého vyhledávání (např. nalezení fyzického připojení zařízení s danou IP/MAC adresou, nalezení duplicitních MAC/IP adres apod.), včetně uchovávání stavové historie.

2.4. Monitorování provozu

2.4.1. Provozní trendy

Pro sledování non-stop dostupnosti na úrovni služeb se používá systém Nagios¹², který je současně také využíván pro monitorování dostupnosti všech aktivních komunikačních prvků a služebních/management serverů, včetně konfigurace automatického upozornění/eskalace e-mailem při detekci problémové/chybové situace.

Pro sledování non-stop dostupnosti na úrovni služeb pro systém VoIP ZČU se používá systém Nagios¹³, který je využíván pro monitorování dostupnosti všech aktivních komunikačních prvků a služebních/management serverů systému VoIP ZČU, včetně konfigurace automatického upozornění/eskalace e-mailem při detekci problémové/chybové situace.

Pro sledování non-stop dostupnosti všech aktivních komunikačních prvků včetně IP telefonů se používá systém Mikrotik The Dude¹⁴.

Pro non-stop historii sledování základních L2 provozních charakteristik aktivních komunikačních prvků všech prostředí pomocí SNMP¹⁵ (typicky zatížení CPU, obsazení operační paměti, stav napájecích zdrojů, teplota, počet BGP prefixů a stavové informace jednotlivých portů/rozhraní jako počet přenesených bytů/rámců/paketů, chybovost portů/rozhraní atd.) se používá optimální konfigurace dvojice nástrojů Cricket¹⁶ a Torrus¹⁷ pracujících nad RRD databázemi.

Pro sledování provozu na úrovni L3/L4 datových toků se využívá technologie NetFlow v9. NetFlow informace exportované ze směrovačů, linuxových firewallů (kolejně extranet) a specializované FlowMon¹⁸ sondy (kolejně intranet) se zpracovávají jednak nevzorkované pomocí produkčního IPv4 software Caligare Flow Inspector/CFI¹⁹ a jednak vzorkované 1:10 pomocí testovacího IPv4/IPv6 software FTAS²⁰.

Pro monitorování historie latence/jitteru/ztrátovosti paketů (typicky VoIP subsystému) se používá aktivní nástroj Smokeping²¹.

Pro monitorování problémových provozních stavů se používá standardní mechanismus zpracování nevyžádaných deníkových zpráv generovaných aktivními prvky na bázi protokolu Syslog a SNMP trap, přičemž se navíc využívá i nadstavba Zenoss Core²² pro inteligentní korelaci trapů.

¹¹ Z bezpečnostních důvodů se však záměrně nevyužívají integrované služby manipulace se stavy portů přepínačů vyžadující SNMP přístup pro zápis.

¹² <http://www.nagios.org/>

¹³ <http://www.nagios.org/>

¹⁴ <http://www.mikrotik.com/thedude.php>

¹⁵ Konfigurace aktivních prvků pouze v režimu pro čtení s povolenými IP adresami management stanic dle

ACL.

¹⁶ <http://cricket.sourceforge.net/>

¹⁷ <http://torrus.org/>

¹⁸ <http://www.invea.cz/produkty-sluzby/flowmon/flowmon-sondy>

¹⁹ <http://www.caligare.com/>

²⁰ <http://www.cesnet.cz/doc/techzpravy/2004/ftas-arch/>,

<http://www.cesnet.cz/doc/techzpravy/2006/ftas-interface/>,

<http://www.cesnet.cz/akce/2009/zazemi-pro-cert-csirt/p/sledovani-provozu.pdf>

²¹ <http://oss.oetiker.ch/smokeping/>

²² <http://www.zenoss.com/solution/network-monitoring>

2.4.2. Bezpečnostní monitorování

Pro monitorování síťové bezpečnosti se jednak využívají standardní nástroje Syslog a SNMP trapy, které mohou být ještě dále inteligentně předzpracovány/filtrovány, korelovány a reportovány SIEM systémem zpracování Syslog hlášení z aktivních prvků OSSEC²³ a pro SNMP trapy systémem Zenoss Core.

Přehled o anomáliích na úrovni automatické detekce podezřelých IPv4 datových toků podle analýzy NetFlow dat poskytuje software Caligare Flow Inspector/CFI.

Automatický přehled o (změnách) mapování aktivních MAC adres na IP adresy pro všechna zařízení připojená do vybraných/důležitých podsítí zajišťuje software ARPwatch²⁴.

Vynucování bezpečnostní síťové přístupové politiky umožňující centralizované systémové zablokování přístupu problémových uživatelů do sítě či síťových služeb (blacklist) zejména na úrovni L2 VACL nebo L3 ACL případně ještě s kombinací vypnutí daného portu na přístupovém prvku (typicky nejbližší místu svého vzniku podle typu komunikačního prvku) je řízeno pomocí nástroje NetSpy²⁵. Tento vlastní nástroj také poskytuje další potřebné podpůrné administrátorské funkce jako např. automatickou detekci neregistrovaných zařízení, vyhledání různých konfliktních síťových stavů, management VLAN/IP podsítí atd.

Vzdálený administrátorský přístup ke všem aktivním síťovým prvkům je zajištěn pouze²⁶ pomocí SSH protokolu s autentizací/autorizací protokolem TACACS+ z předdefinovaných povolených bezpečných podsítí/IP adres. Management rozhraní L2 přepínačů je umístěno ve vyhrazené IP podsíti chráněné firewallem. Pro L3 přepínače/směrovače je konfigurována ochrana Control Plane Policing/CoPP, pokud tuto vlastnost podporují. AAA auditní informace o administrátorských přístupech ke konfigurovaným zařízením je k dispozici na TACACS+ serverech CIV ZČU.

²³ <http://www.ossec.net/>

²⁴ <http://www.securityfocus.com/tools/142>

²⁵ Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

²⁶ S výjimkou menšího počtu zastaralých přepínačů, které SSH nepodporují a jsou postupně podle finančních možností nahrazovány.