**Popis současného stavu, technická specifikace dodávky vč. minimálních technických požadavků**

nadlimitní veřejná zakázka na dodávky s názvem

## **„Modernizace síťové infrastruktury Fakulty architektury ČVUT“**

## **OBNOVA PŘÍSTUPOVÉ SÍTĚ FAKULTY ARCHITEKTURY ČVUT V PRAZE**

Pro budoucí rozvoj a zkvalitnění funkcí síťové infrastruktury je nutné provést obnovu stávající sítě LAN. Obnova musí přinést nejen navýšení propustnosti sítě, ale též nasazení nejnovějších bezpečnostních standardů, které vyžaduje kybernetická bezpečnost. Většina aktuálně používaných aktivních prvků LAN je více jak 10 let stará a je za koncem své technické životnosti. To znamená, že pro ně výrobce již neposkytuje aktualizaci softwaru ani opravu případných bezpečnostních chyb či zranitelností. Stávající řešení dále nepodporuje autorizaci přístupu do LAN, dynamickou segmentaci a k dispozici nejsou ani pokročilé software nástroje pro dynamickou karanténu zařízení v případě zjištění bezpečnostní hrozby. Používání stávající technologie již není pro Zadavatele ekonomické ani bezpečné.

## **POPIS STÁVAJÍCÍHO STAVU**

Topologie LAN má charakter dvojité hvězdy se zdvojenými propoji. Hvězda je zdvojena z důvodu redundance, tj. v případě výpadku jednoho z centrálních přepínačů je možné nalézt v síti náhradní cestu. Centrální přepínače Cisco 6500E jsou logicky sdruženy do jednoho virtuálního přepínače pomocí technologie VSS (Virtual Switching System). V případě výpadku jednoho z centrálních přepínačů funkci vypadnuvšího převezme přepínač druhý. Jednotlivé spoje mezi přístupovými přepínači a páteřními přepínači jsou realizovány jako optické spoje o kapacitě 2x10Gb/s do každého z core přepínačů. Optické spoje jsou na obou koncích ukončeny v optických modulech jednotlivých přepínačů. Přístupové přepínače jsou realizovány pomocí modelových řad Cisco Catalyst 4500E a Cisco Catalyst 3560E. K centrálním přepínačům jsou připojeny i servery v datovém centru. Pro připojení koncových zařízení jako jsou PC, notebooky, kamery, přístupové body je použito portů nabízejících maximálně 1000Mbps. Aktuální PoE standard je IEEE 802.3af. Stávající bezdrátová síť je založena na přístupových bodech Aruba AP-325. Přístupové body jsou spravovány centrálním bezdrátovým kontrolérem Aruba 7210. V současné době je v budově použito cca 160 přístupových bodů.

## **FYZICKÁ TOPOLOGIE LAN**



## **POŽADOVANÝ BUDOUCÍ STAV**

Předkládaná obnova se zaměřuje na vysokou ochranu investice a dlouhodobou udržitelnost bez nutnosti dodatečných investic. Po architektonické stránce je kladen důraz na unifikaci, vysokou technickou vyspělost nabídnutých zařízení a možnou míru provázanosti všech komponent včetně možnosti funkčního provázání se stávajícími technologiemi. Z pohledu provozu je kladen důraz na automatizaci správy, rychlost nasazení a minimalizaci operační složitosti. Mezi důležité rysy budoucího stavu patří redundance centrálních přepínačů, navýšení propustnosti páteře, implementace moderních způsobů segmentace sítě, unifikace a centralizace uživatelských politik. Nové přepínače musí nabízet dostatek portů pro připojení koncových zařízení a současně umožnit jednoduché rozšíření nebo rychlostní upgrade páteře. Předpokládaná rychlost páteře je minimálně 25Gbps. Důraz je kladen na vysokou dostupnost všech kritických komponent, které musí zároveň umožňovat upgrade za provozu. Přístupové přepínače musí umožnit připojení koncových zařízení minimálně rychlostí 1Gbps včetně podpory nejnovějších PoE napájecích standardů. Každý přístupový přepínač bude připojen do obou centrálních přepínačů. Propojení mezi centrálními a přístupovými přepínači bude vždy zdvojené a obě linky budou nastaveny v linkové agregaci, tak aby byly využívány současně a nedocházelo k jejich blokování. Všechny přístupové přepínače musí podporovat mikro-segmentaci, kdy provoz/komunikace mezi zařízeními ve stejné VLAN síti je buď úplně blokován nebo vždy prochází kontrolou na stavovém firewallu, kde bude rozhodnuto, zda je komunikace zakázána nebo povolena.

Součástí nového řešení musí být i autentizační server (AAA), který zabezpečí autentizaci a autorizaci vybraných zařízení do sítě. AAA server musí být možné integrovat s databází uživatelů Microsoft Active Directory či LDAP. Autentizační server bude centrálním bodem bezpečnostní politiky sítě a všechny nabízené aktivní prvky musí umožňovat integraci s autentizačním serverem. Všechny uživatelské profily se budou definovat na centrálním autentizačním serveru a uživatelům přiřazovat na základě autentizace do sítě. Autentizace do sítě definuje, zda bude zařízení komunikovat přímo do sítě, nebo zda jeho komunikace bude procházet kontrolou na interním segmentačním firewallu. Autentizační server musí být možné integrovat se stávajícím firewallem pro sdílení uživatelských rolí.

## **PŘEDMĚT PLNĚNÍ A POŽADOVANÝ ROZSAH PLNĚNÍ**

Předmětem veřejné zakázky je dodávka aktivních prvků LAN (zařízení), software autentizační platformy a souvisejících služeb pro postupnou obnovu LAN Zadavatele. Zadavatel požaduje dodání následujících aktivních prvků a software:

- Přepínač TYP1-Core 2 ks

- Přepínač TYP2-Access 11 ks

- Přepínač TYP3-Access 2 ks

- Přepínač TYP4-Access 2 ks

- Autentizační platforma 2 ks

- Příslušenství výčet položek uveden dále

Součástí dodávky je migrace, dokumentace a školení v rozsahu 2 dnů, když podrobnosti stanoví Kupní smlouva.

Všechna zařízení a software musí splňovat požadavky definované v části “**Minimální technické požadavky**”. Všechna zařízení, software, operační systémy, licence a subscripce musí být od stejného výrobce a musí být garantovaná plná interoperabilita všech nabízených zařízení. Všechny licence pro požadované funkce musí být součástí zařízení. V případě, že je licence časově omezena (subscription), musí být minimálně na 7 let.

Po dodání všech zařízení bude podepsán akceptační protokol, který bude podkladem pro fakturaci. Fakturace bude dílčí, když konečnou fakturu je možno vystavit až po kompletním dodání a předání celého předmětu plnění. U každého dodávaného zařízení uchazeč uvede v nabídce jeho přesnou specifikaci, obchodní název, výrobce a produktové číslo (product number), popř. též internetový odkaz (link) na nabízení produkt.

Na všechny části dodávané síťové infrastruktury je vyžadována záruka a záruční servisní podpora následujícího rozsahu:

* Záruka a záruční podpora výrobce v úrovni 8x5xNBD, zadavatel se může obrátit přímo na podporu výrobce zařízení. Délka trvání min. 60 měsíců.
* Součástí záruky musí být přímý přístup k technické podpoře výrobce zařízení. Délka trvání min. 60 měsíců.
* Přístup k bezpečnostním opravám SW a HW po dobu životnosti dodaných prvků. Délka trvání min. 60 měsíců.
* Záruční podpora musí zahrnovat i nárok na aktualizace software a firmware pro dodané prvky po dobu životnosti dodaných prvků. Délka trvání min. 60 měsíců.
* Zadavatel musí mít možnost si sám legálně stahovat nové verze software přímo ze stránek výrobce. Délka trvání min. 60 měsíců.
* Zadavateli musí být umožněn přístup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje. Délka trvání min. 60 měsíců.
* Rozšířená servisní podpora na software Autentizační platformy garantovaná přímo výrobcem zařízení v režimu 24x7. Možnost otevírat servisní požadavky přímo u výrobce. Délka trvání min. 60 měsíců.

## **MINIMÁLNÍ TECHNICKÉ POŽADAVKY**

1. **PŘEPÍNAČE TYP1, TYP2, TYP3**

Zadavatel primárně specifikuje společné vlastnosti všech uvedených přepínačů, když následně jsou stanoveny další požadavky vztahující se k jednotlivému přepínači.

**Společné vlastnosti pro přepínače TYP1-Core, TYP2-Access a TYP3-Access**

|  |
| --- |
| **Požadovaná funkcionalita/vlastnost** |
| Typ zařízení: L3 přepínač |
| Všechny ethernet porty na dodávaných zařízeních aktivní bez nutnosti dokupování licence |
| 2x Interní AC hot-swap napájecí zdroje |
| Redundantní hot-swap ventilátory |
| Podpora originálních transceiverů výrobce: 10GBASE-T SFP+ |
| Podporovaný počet přepínačů ve stohu: 2 |
| Stoh z přepínačů podporuje distribuované přepínání paketů |
| Redundance řídícího prvku v rámci stohu |
| Seskupení portů IEEE 802.3ad mezi různými prvky stohu (MC-LAG) |
| Podpora stohování na vzdálenost minimálně 100 m |
| Podpora jumbo rámců včetně velikosti 9198 Byte |
| Podpora linkové agregace IEEE 802.1AX |
| Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4 |
| Protokol pro definici šířených VLAN: MVRP |
| Minimálně 4000 aktivních VLAN podle IEEE 802.1Q |
| VLAN translace - swap 802.1Q tagů na trunk portu |
| Podpora zařazování do VLAN podle standardu 802.1v |
| Private VLAN včetně primary, secondary a community VLAN |
| IEEE 802.1s - Multiple Spanning Tree a IEEE 802.1w |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) |
| Podpora ERPS (ITU G.8032) pro rychlou konvergenci do 100ms v kruhových sítích |
| Detekce protilehlého zařízení pomocí LLDP, včetně LLDP over OoB management port |
| Detekce jednosměrnosti optické linky (např. UDLD nebo ekvivalentní) |
| DHCP server a relay pro IPv4 a IPv6 včetně podpory VRF |
| Podpora zapouzdření: GRE over IPv4 |
| Podpora NTPv4 client pro IPv4 a IPv6 včetně VRF a MD5 autentizace, podpora NTP server |
| Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subnety |
| Podpora L3 routed port včetně L3 sub-interface - nadřazené L3 rozhraní lze rozdělit |
| Dynamické směrování: RIP, RIPng, OSPFv2 včetně HMAC-SHA-384, OSPFv3, BGP, MP-BGP |
| Funkce BGP konfederace a route reflector pro IPv4 a IPv6 |
| Podpora BGP MD5 autentizace a BGP TTL security |
| Podpora police based routing |
| Podpora VRRPv2 a VRRPv3 |
| Podpora route map |
| ECMP včetně možnosti konfigurace rozkládání zátěže podle L3 a L4 |
| Podpora minimálně 256 virtuálních směrovacích instancí (VRF) |
| IGMP v2 a v3, IGMP snooping |
| MLD v1 a v2, MLD snooping |
| Směrování multicast: PIM-DM, PIM-SM, IPv6 PIM-SM, PIM-SSM, IPv6 PIM-SSM, MSDP |
| Hardware podpora IPv4 a IPv6 ACL |
| ACL klasifikace na úrovni zdroj./cílová MAC adresa, zdroj./cílová IPv4/IPv6 adresa, číslo zdroj./cílového portu, protokol, TTL hodnota, číslo VLAN |
| HW ochrana proti zahlcení portu (broadcast/multicast/unicast) nastavitelná na kbps a pps |
| 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) |
| Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675 |
| 802.1X s podporou odlišných Preauth VLAN, Fail VLAN, Critical VLAN a Critical voice VLAN |
| Uživatelské role definované lokálně v přepínači, jejich aplikace dle výsledku autorizace |
| Uživatelské role dynamicky stahovatelné z RADIUS, jejich aplikace dle výsledku autorizace  |
| Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC |
| BPDU guard a Root guard |
| Podpora service insertion včetně technologie VXLAN |
| Podpora static a dynamic VXLAN s využítím BGP-EVPN |
| Podpora Group based policy pro VXLAN (VXLAN GBP) |
| Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU |
| Vynucení zadat heslo administrátora a nastavitelná politika komplexity hesla přímo na přepínači |
| Možnost instalace vlastního certifikátu včetně podpory Enrollment over Secure Transport (EST) |
| TACACS+ a RADIUS klient pro AAA (autentizace, autorizace, accounting) |
| Aktivní monitoring dostupnosti RADIUS a TACACS+ přednastaveným jménem a heslem |
| Podpora Radius over TLS (RadSec) |
| CLI formou 1x USB-C console port |
| Bezdrátová sériová konzole pomocí Bluetooth |
| Konfigurace zařízení v člověku čitelné textové formě |
| OoB management formou portu RJ45 s podporou ethernetu |
| USB port pro přenos konfigurace a firmware |
| Podpora IPv4 a IPv6 management: SSHv2 server, HTTPS server, SFTP a SCP klient |
| Podpora RSA s délkou klíče minimálně 4096 bitů |
| Podpora SNMPv2c a SNMPv3 |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL |
| Lokálně vynucené RBAC na úrovni přepínače |
| Dualní flash image - podpora dvou nezávislých verzí operačního systému |
| Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler) |
| TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více SYSLOG serverů |
| Automatické i manuální snapshoty systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby |
| Podpora standardního Linux Shellu (BASH) pro debugging a skriptování |
| Podpora skripování v jazyce Python – lokální interpret jazyka v přepínači |
| Možnost vytváření vlastních diagnostických a korelačních skriptů a jejich grafických interpretací v jazyce Python (korelace libovolných událostí a hodnot v podobě grafů) |
| Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů - možnost vynášení stavu monitorovaných metrik do grafů atp. |
| Root cause analysis v grafickém rozhraní – možnost návratu ke konkrétní funkční konfiguraci a stavu protokolů v čase |
| Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní) |
| Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události |
| Interní uložistě dat pro sběr provozních dat a pokročilou dignostiku zařízení: min. 30 GB |
| Analýza provozu sFlow podle RFC 3176 nebo Neflow pro oba směry ingress a egress |
| Ochrana proti nahrání modifikovaného SW prostřednictvím image signing a secure boot, ověřující autentičnost a integritu OS prostřednictvím TPM chipu |
| SPAN a ERSPAN port mirroring, alespoň 4 různé obousměrné session |
| IP SLA pro měření dostupnosti a zpoždění provozu VoIP - režim responder i probe |
| Podpora integrace s automatizačními nástroji (Ansible, NAPALM) |
| Podpora REST API v režimech read-only a read-write pro automatizaci nastavení |
| Podpora Cloud based management |
| Podpora Zero Touch Provisioning (ZTP) |
| Je plně kompatibilní se stávajícím nástrojem správy zadavatele zajišťujícím monitoring a dohled aktivních prvků. |
| Podpora na přepínač dle specifikace „záručních podmínek“ |
| Všechny licence k výše uvedeným funkcím musí být součástí přepínače. V případě, že je licence časově omezena musí být minimálně na 7 let |
| Kryptografie musí být v souladu s požadavky § 26 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti a doporučením NÚKIB pro kryptografickou ochranu. Kryptografie obecně musí umožnit použití takových algoritmů, které jsou v souladu s doporučenými algoritmy NÚKIB. Nesmí se jednat o algoritmy označované jako „dožívající“ v doporučení NÚKIB. |

**Tabulka A – Přepínač TYP1-Core**

|  |
| --- |
| **Požadovaná funkcionalita/vlastnost** |
| Velikost zařízení: 1U |
| Počet SFP28 interface: 32x 10/25Gbps portů s volitelným fyzickým rozhraním |
| Počet QSFP interface: 4x 40/100Gbps portů s volitelným fyzickým rozhraním |
| Podpora rozdělení 40GE portů na 4x10GE a 100GE portů na 4x25GE |
| Směr proudění vzduchu zařízením: předo-zadní |
| Přepínací výkon: 2,4 Tbps |
| Paketový výkon: 1100 Mpps |
| Paketový buffer: 32 MB |
| Maximální přípustná hloubka přepínače: 45 cm |
| Kapacita stohovacího propojení: 400 Gbps |
| Upgrade OS ve stohu bez narušení provozu (ISSU/Live upgrade) |
| Automatizace upgrade OS ve stohu bez narušení provozu přes REST API |
| Minimální počet záznamů v tabulce MAC adres: 210 000 |
| Minimální počet záznamů v tabulce ARP: 140 000 |
| Minimální počet IPv4 záznamů ve směrovací tabulce: 600 000 |
| Minimální počet IPv6 záznamů ve směrovací tabulce: 600 000 |
| Minimální počet LACP skupin/linek ve skupině: 48/16  |
| Podpora Data Center Bridging (PFC 802.1Qbb, ETS 802.1Qaz) |
| IP Explicit Congestion Notification (ECN) |
| Podpora RoCEv2 |
| HW a SW podpora MACSec |

**Tabulka B – Přepínač TYP2-Access**

|  |
| --- |
| **Požadovaná funkcionalita/vlastnost** |
| Velikost zařízení: modulární chassis |
| Maximální velikost zařízení: 10U |
| Počet SFP28 interface: 8x 10/25Gbps portů s volitelným fyzickým rozhraním |
| Počet multigigabit interface: 48x 100Mbit/1Gbit/2,5Gbit/5Gbit RJ45 metalických portů |
| Počet gigabit interface: 96x10/100/1000Mbit RJ45 metalických portů |
| Při výpadku libovolné linkové karty zůstává aktivní minimálně polovina 25GE interface  |
| Všechny dostupné ethernet interface jsou plně propustné – neblokující porty |
| 2 volné sloty plné šířky pro osazení rozšiřujícími linkovými kartami |
| Možnost rozšíření o linkové karty s podporou 40GE QSFP interface |
| Možnost rozšíření o linkové karty s podporou 10GBASE-T SFP+ portů |
| Možnost rozšíření o další napájecí zdroje pro vyšší míru redundance nebo vyšší PoE výkon |
| Možnost rozšíření o redundantní management jednotku/supervisor |
| Podpora PoE+ dle standardu 802.3at a Enhanced PoE dle standardu 802.3bt |
| Dostupný výkon pro PoE+ napájení: 4800 W |
| Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače |
| Podpora Energy Efficient Ethernet (802.3az) |
| Přepínací výkon: 13 Tbps |
| Paketový výkon: 5 Bpps |
| Paketový buffer: 8 MB per linková karta |
| Maximální přípustná hloubka přepínače: 45 cm |
| Minimální kapacita stohovacího propojení: 100 Gbps |
| Upgrade OS ve stohu bez narušení provozu (ISSU/Live upgrade) |
| Automatizace upgrade OS ve stohu bez narušení provozu přes REST API |
| Počet záznamů v tabulce MAC adres: 32 000 |
| Počet záznamů v tabulce ARP: 45 000 |
| Počet IPv4 záznamů ve směrovací tabulce: 60 000 |
| Počet IPv6 záznamů ve směrovací tabulce: 60 000 |
| Počet LACP skupin/linek ve skupině: 256/8  |
| ACL definice na základě skupiny fyzických portů |
| Podpora LLDP-MED |
| DHCP snooping pro IPv4 a IPv6 |
| Uživatelské role definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely |
| Tunelování uživatelského provozu do L2 GRE tunelů - schopnost izolovat více koncových zařízení na jednom portu do unikátních tunelů |
| Přiřazení koncového zařízení do tunelu na základě výsledku autorizace |
| Podpora bezpečného transportu Dynamic ACL během 802.1X, např. pomocí SSL  |
| Podpora IPv6 RA Guard |
| IP source guard / dynamic IP lockdown |
| Ochrana ARP protokolu (Dynamic ARP protection nebo funkčně ekvivalentní) |
| Podpora RADIUS CoA (RFC3576) |
| 802.1x autentizace přepínače vůči nadřazenému přepínači pomocí EAP-TLS a EAP-MD5 |
| Podpora selektivního tunelování provozu koncových zařízení per port do stávajícího bezdrátového kontroléru |

**Tabulka C – Přepínač TYP3-Access**

|  |
| --- |
| **Požadovaná funkcionalita/vlastnost** |
| Velikost zařízení: 1U nebo modulární chassis |
| Počet multigigabit interface: 48x 100Mbit/1Gbit/2,5Gbit/5Gbit RJ45 metalických portů |
| Počet SFP28 interface: 4x 10/25 Gbps portů volitelným fyzickým rozhraním |
| Podpora PoE+ dle standardu 802.3at a Enhanced PoE dle standardu 802.3bt |
| Dostupný výkon pro PoE+ napájení: 1440W |
| Schopnost poskytovat PoE napájení připojeným zařízením i během restartu přepínače |
| Možnost rozšíření o napájecí zdroj s vyšším výkonem pro PoE |
| Podpora Energy Efficient Ethernet (802.3az) |
| Minimální přepínací výkon: 800 Gbps |
| Minimální paketový výkon: 650 Mpps |
| Minimální paketový buffer: 8 MB |
| Maximální přípustná hloubka přepínače: 40 cm |
| Kapacita stohovacího propojení: 100 Gbps |
| Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor) |
| Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF |
| Počet záznamů v tabulce MAC adres: 32 000 |
| Počet záznamů v tabulce ARP: 45 000 |
| Počet IPv4 záznamů ve směrovací tabulce: 60 000 |
| Počet IPv6 záznamů ve směrovací tabulce: 60 000 |
| Počet LACP skupin/linek ve skupině: 256/8  |
| ACL definice na základě skupiny fyzických portů |
| Podpora LLDP-MED |
| DHCP snooping pro IPv4 a IPv6 |
| Uživatelské role definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely |
| Tunelování uživatelského provozu do L2 GRE tunelů - schopnost izolovat více koncových zařízení na jednom portu do unikátních tunelů |
| Přiřazení koncového zařízení do tunelu na základě výsledku autorizace |
| Podpora bezpečného transportu Dynamic ACL během 802.1X, např. pomocí SSL  |
| Podpora IPv6 RA Guard |
| IP source guard / dynamic IP lockdown |
| Ochrana ARP protokolu (Dynamic ARP protection nebo funkčně ekvivalentní) |
| Podpora RADIUS CoA (RFC3576) |
| 802.1x autentizace přepínače vůči nadřazenému přepínači pomocí EAP-TLS a EAP-MD5 |
| Podpora selektivního tunelování provozu koncových zařízení per port do stávajícího bezdrátového kontroléru |

1. **PŘEPÍNAČ TYP4**

**Tabulka D – Přepínač TYP4-Access**

|  |
| --- |
| **Požadovaná funkcionalita/vlastnost** |
| Typ zařízení: L2 switch |
| Velikost zařízení: 1U |
| Počet 1Gbit/s metalických portů: 24×RJ45 |
| Počet 10Gbit/s SFP+ optických portů s volitelným fyzickým rozhraním: 4×SFP+ |
| 10GE interface zpětně kompatibilní s 1Gbit/s transceivery |
| Všechny ethernet porty jsou dostupné zepředu |
| Interní AC napájecí zdroj |
| Podpora PoE+ dle standardu 802.3at a Enhanced PoE dle standardu 802.3bt |
| Dostupný výkon pro PoE+ napájení: 240 W |
| Podpora Energy Efficient Ethernet (802.3az) |
| Přepínací výkon: 128 Gbps |
| Paketový výkon: 95 Mpps |
| Paketový buffer: 12 MB |
| Maximální přípustná hloubka přepínače: 31 cm |
| Bez ventilátoru |
| Stupeň krytí IP30 |
| Rozsah provozních teplot -30° až +60°C |
| Podpora "jumbo rámců" včetně velikosti 9198 Byte |
| Podpora linkové agregace IEEE 802.3ad  |
| Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4 |
| Minimální počet LACP skupin/linek ve skupině: 8/8 |
| Protokol pro definici šířených VLAN: MVRP |
| Podpora VLAN podle IEEE 802.1Q |
| IEEE 802.1s - Multiple Spanning Tree |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED |
| Detekce jednosměrnosti optické linky (např. UDLD) |
| NTP pro IPv4 a IPv6 včetně MD5 autentizace |
| Statické směrování IPv4 a IPv6 |
| IGMP v2 a v3 a MLD v1 a v2 |
| Hardware podpora IPv4 a IPv6 ACL |
| ACL definice na základě skupiny fyzických portů |
| ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN |
| BPDU guard a Root guard |
| DHCP snooping pro IPv4 a IPv6 |
| Uživatelské role definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely |
| Tunelování uživatelského provozu do L2 GRE tunelů - schopnost izolovat více koncových zařízení na jednom portu do unikátních tunelů |
| HW ochrana proti zahlcení (broadcast/multicast/unicast) nastavitelná na kbps |
| Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port |
| Konfigurovatelná kombinace pořadí postupného ověřování na portu (IEEE 802.1x, MAC adresou) |
| 802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN a Critical voice VLAN |
| Dynamické zařazování do VLAN |
| Ochrana ARP protokolu (Dynamic ARP protection nebo funkčně ekvivalentní) |
| Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC |
| Ochrana proti flapování linek s možností konfigurace citlivosti a akce při překročení |
| Uplink failure detection – detekce výpadku uplink a automatický shutdown navázaných downlink portů |
| Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU |
| Podpora instalace vlastního certifikátu včetně Enrollment over Secure Transport (EST) |
| Podpora IPv4 a IPv6 QoS |
| 802.1x autentizace přepínače vůči nadřazenému přepínači pomocí EAP-TLS a EAP-MD5 |
| CLI formou 1x USB-C console port |
| Konfigurace zařízení v člověku čitelné textové formě |
| USB port pro diagnostiku, přenos konfigurace a firmware |
| Podpora managementu přes IPv4 i IPv6 |
| Podpora SSHv2 server, HTTPS server, SFTP a SCP klient |
| Podpora SNMPv2c a SNMPv3 |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL |
| Lokálně vynucené RBAC na úrovni přepínače |
| Dualní flash image - podpora dvou nezávislých verzí operačního systému |
| TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logování na více serverů |
| Podpora SYSLOG over TLS |
| Měření zakončení a délky metalického kabelu (např. TDR nebo ekvivalentní) |
| Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby |
| Podpora standardního Linux Shellu (BASH) pro debugging a skriptování |
| Podpora RADIUS, RADIUS CoA (RFC3576), RADIUS IPSec |
| Podpora TACACS+ včetně command authorization |
| Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler) |
| Aktivní monitoring dostupnosti RADIUS a TACACS+ přednastaveným jménem a heslem |
| Interní uložistě dat pro sběr provozních dat a pokročilou dignostiku zařízení: min. 15 GB |
| Analýza síťového provozu sFlow podle RFC 3176 |
| Port mirroring (SPAN), alespoň 4 různé obousměrné session |
| Podpora Zero Touch Provisioning (ZTP) |
| Podpora REST API v režimech read-only a read-write pro automatizaci nastavení |
| Automatická konfigurace portu podle připojeného zařízení |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů  |
| Podpora na přepínač dle specifikace „záručních podmínek“ |
| Všechny licence k výše uvedeným funkcím musí být součástí přepínače. V případě, že je licence časově omezena musí být minimálně na 7 let |

1. **AUTENTIZAČNÍ PLATFORMA**

**Tabulka E – Autentizační platforma**

|  |
| --- |
| **Požadovaná funkcionalita/vlastnost** |
| Autentizační platforma (AAA) pro řízení přístupu uživatelů a zařízení do LAN a WiFi |
| On-premise appliance, nepřipouští se cloud řešení |
| Virtuální appliance bez nutnosti dodatečných licencí např. pro OS nebo database |
| Podporované hypervisory: VMware (.OVA formát), Hyper-V, KVM |
| Plná kompatibilita s infrastrukturou zadavatele na které bude probíhat ověřování |
| Podpora 802.1X autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN |
| Podpora minimálně pro 500 současně autentizovaných zařízení (pomocí 802.1X), licence pro 500 zařízení |
| Možnost vytváření active-active clusterů. Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality a umožňovat navýšení počtu podporovaných uživatelů přidáním další instance |
| Podpora minimálně následujících autentizačních metod: PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, Tunnel Extensible Authentication Protocol (TEAP), MAC autentizace |
| Platforma musí umožňovat úplné oddělení autentizace a autorizace, např. autentizace proti službě Active Directory, ale autorizace proti externí SQL databázi |
| Autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, typ zařízení, osobní profil či členství ve skupině v Active Directory |
| Podpora dalších způsobů autentizace a autorizace. Minimálně: LDAP, MS AD, Token, MAC auth, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta) |
| Podpora změny autorizačního stavu zařízení bez nutnosti změny definice autorizační politiky, např. pro odpojení nebo karanténu koncových zařízení |
| Podpora RADIUS CoA podle RFC3576 a RadSec (RADIUS over TLS) |
| Možnost autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. za účelem omezení celkového času online či objemu přenesených dat za delší časové období |
| Sběr dodatečných informací o připojených zařízeních (profilování) jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace lze využít pro doplňkové ověření přístupu zařízení do sítě. Licence pro 500 profilovaných zařízení |
| Sběr dodatečných informací o připojených IoT zařízeních (profilování), pomocí aktivních metod jako jsou: SNMP, WMI a NMAP scan. Tyto informace lze využít pro doplňkové ověření přístupu zařízení do sítě |
| Platforma obsahuje funkci otestovani autentizační politiky, včetne flexibilní volby typu autentizace, atributů klienta, atd. |
| Podpora REST API pro většinu základních úkonů AAA platformy. Podpora REST volání vyvolaného autentizační či autorizační událostí (pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.) |
| Zpracovávání SYSLOG hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení. |
| Možnost vlastní tvorby parseru/integrace SYSLOG hlášení pro možnost uživatelské integrace s libovolnými systémy třetích stran. |
| Podpora SYSLOG podle RFC 5424. |
| Možnost registrace zařízení pomocí MAC adresy pro non-IT uživatele - omezená funkce administračního rozhranní, se zařazením zařízení do skupiny s definovanou politikou přístupu. |
| Podpora protokolu TACACS+ pro možnost řízení přístupu administrátorů na síťová zařízení |
| Možnost aktivace služby TACACS+ bez nutnosti instalace dalšího systému nebo SW |
| Možnost integrace s MDM (Mobile Device Management) platformami třetích stran (minimálně AirWatch, Citrix, MobileIron, JAMF). |
| Možnost rozšíření o nadstavbovou software komponentu pro koncové stanice jako trvalý či dočasný NAC agent, který zajišťuje ochranu formou posture assessments a health checks. NAC agent podporuje v návaznosti na autentizační proces kontrolu systémových procesů, aplikací , klíčů registru, použití USB zařízení, přítomnost anti-viru, firewallu. |
| Podpora HTTP a HTTPS web autentizace (Captive portál). |
| Podpora autentizace hostů pomocí účtů sociálních sítí: Google, Google Plus, Facebook, Facebook WIFI, Twitter, LinkedIn, Microsoft. |
| Podpora autentizace lokálními účty v rámci portálu, ověření pomocí jméno+heslo, autentizační kód. |
| Možnost samoobslužné registrace hosta do sítě se SMS a email ověřením. |
| Přístup zdarma pouze s akceptací podmínek užití. |
| Tarify lze omezit časově, z hlediska rychlosti připojení či objemu přenesených dat. |
| Vynucení odpojení zařízení ihned po naplnění jakéhokoliv z limitů. |
| Perzistence autentizace/registrace s využitím MAC cache a zobrazení jen uvítacích stránek s osobním oslovením hosta při opakovaných návštěvách. Konfigurovatelné hodnoty trvání MAC cache pro různé hosty v rámci jedné služby (např. jedno SSID). |
| Možnost vytváření účtů samoobslužnou registrací. |
| Možnost provozovat více graficky i obsahově unikátních portálů v rámci jedné instalace. |
| Redakční systém pro plnou grafickou a obsahovou úpravu jednotlivých captive portálů umožňuje:* Uprava barev, fontů, pozadí a loga.
* Úprava registračních formulářů – přidávání a odebírání polí pro vstupní data formuláře včetně validace vkládaného obsahu.
* Možnost vkládání animací, videí a dalšího dynamického obsahu.
* Vytváření specifických stránek pro různé typy zařízení a operačních systémů (např. pro efektivní navedení do specifického app store).
 |
| HTTPS rozhraní s podporou konfiguračních průvodců a předkonfigurovaných šablon. |
| Appliance podporuje šifrování disku nebo souborů. |
| Appliance podporuje CLI přístup a umožňuje v něm konfiguraci základních nastavení. |
| Diagnostika problemů (systémová, údaje o chybách přihlašování, TCP dump, packet capture) |

1. **PŘÍSLUŠENSTVÍ**

**Tabulka F – Příslušenství:**

|  |  |
| --- | --- |
| **Požadované příslušenství** | **Počet ks** |
| linková karta 48x10/100/1000Mbit RJ45 s PoE - 100% kompatibilní s přepínačem TYP2 | **7 ks** |
| supervisor/management modul - 100% kompatibilní přepínačem TYP2 | **2 ks** |
| 40Gbit QSFP+ LC BiDi MM originální opt. převodník výrobce, nepřipouští se OEM verze | **2 ks** |
| 25Gbit SR SFP28 originální opt. převodník výrobce, nepřipouští se OEM verze | **48 ks** |
| 10Gbit SR SFP+ kompatibilní opt. převodník, nepřipouští se připouští se OEM verze | **14 ks** |
| 1Gbit SFP RJ45 T originální převodník výrobce, nepřipouští se OEM verze | **14 ks** |
| 1Gbit LX SFP originální opt. převodník výrobce, nepřipouští se OEM verze | **2 ks** |
| 100GE DAC kabel, délka minimálně 3m, nepřipouští se OEM verze | **2 ks** |
| 40Gbit QSFP+ LC BiDi MM orig. převodník výrobce kompatibilní s HPE 6125XLG, nepřipouští se OEM verze | **2 ks** |
| LC-LC OM4 MM kabel, délka 3 m | **58 ks** |
| LC-LC OM4 MM kabel, délka 5 m | **2 ks** |

**SPECIFIKACE DODAVATELEM NABÍZENÉHO PLNĚNÍ[[1]](#footnote-1)**

|  |
| --- |
| **Přepínač typ1-Core** |
| **Výrobce:** |  |
| **Produktové číslo, typ, specifikace:** |  |
| **Jednotková cena bez DPH za 1 ks** |  |
|  |
| **PŘEPÍNAČ TYP2-ACCESS** |
| **Výrobce:** |  |
| **Produktové číslo, typ, specifikace:** |  |
| **Jednotková cena bez DPH za 1 ks** |  |
|  |
| **PŘEPÍNAČ TYP3-ACCESS** |
| **Výrobce:** |  |
| **Produktové číslo, typ, specifikace:** |  |
| **Jednotková cena bez DPH za 1 ks** |  |
|  |
| **PŘEPÍNAČ TYP4-ACCESS** |
| **Výrobce:** |  |
| **Produktové číslo, typ, specifikace:** |  |
| **Jednotková cena bez DPH za 1 ks** |  |
|  |
| **AUTENTIZAČNÍ PLATFORMA** |
| **Výrobce:** |  |
| **Produktové číslo, typ, specifikace:** |  |
| **Jednotková cena bez DPH za 1 ks** |  |
|  |
| **PŘÍSLUŠENSTVÍ** |
| **POŽADOVANÉ PŘÍSLUŠENSTVÍ** | **PRODUKTOVÉ ČÍSLO** | **Jednotková cena za 1 ks bez DPH** |
| linková karta 48x10/100/1000Mbit RJ45 s PoE - 100% kompatibilní s přepínačem TYP2 |  |  |
| supervisor/management modul - 100% kompatibilní přepínačem TYP2 |  |  |
| 40Gbit QSFP+ LC BiDi MM originální opt. převodník výrobce, nepřipouští se OEM verze |  |  |
| 25Gbit SR SFP28 originální opt. převodník výrobce, nepřipouští se OEM verze |  |  |
| 10Gbit SR SFP+ kompatibilní opt. převodník, nepřipouští se připouští se OEM verze |  |  |
| 1Gbit SFP RJ45 T originální převodník výrobce, nepřipouští se OEM verze |  |  |
| 1Gbit LX SFP originální opt. převodník výrobce, nepřipouští se OEM verze |  |  |
| 100GE DAC kabel, délka minimálně 3m, nepřipouští se OEM verze |  |  |
| 40Gbit QSFP+ LC BiDi MM orig. převodník výrobce kompatibilní s HPE 6125XLG, nepřipouští se OEM verze |  |  |
| LC-LC OM4 MM kabel, délka 3 m |  |  |
| LC-LC OM4 MM kabel, délka 5 m |  |  |

**CELKOVÁ VÝŠE NABÍDKOVÉ CENY ZA NABÍZENÉ PLNĚNÍ - SHRNUTÍ[[2]](#footnote-2):**

|  |  |
| --- | --- |
| Celková cena bez DPH za nabízené plnění Přepínač TYP1-Core (celkem 2 ks): |   |
| Celková cena bez DPH za nabízené plnění Přepínač TYP2-Access (celkem 11 ks): |   |
| Celková cena bez DPH za nabízené plnění Přepínač TYP3-Access (celkem 2 ks): |   |
| Celková cena bez DPH za nabízené plnění Přepínač TYP4-Access (celkem 2 ks): |   |
| Celková cena bez DPH za nabízené plnění Autentizační platforma (celkem 2 ks) |   |
| Celková souhrnná cena bez DPH za nabízené plnění příslušenství (v rozsahu dle počtu jednotlivých kusů uvedených výše – viz tabulka F - Příslušenství) |  |
| Celková cena bez DPH za nabízené plnění instalace, konfigurace, zaškolení a související činnosti (kompletní provedení činností) |  |
| **Celková výše nabídkové ceny bez DPH:**  |   |

1. Ve vztahu ke všem požadovaným plněním doplní dodavatel do připravené tabulky specifikaci dle skutečně nabízeného plnění. [↑](#footnote-ref-1)
2. Dodavatel uvede dílčí hodnoty ceny nabízeného plnění a uvede celkovou výši nabídkové ceny bez DPH, která odpovídá součtu dílčích hodnot nabídkové ceny, kterou uvede rovněž na krycím listu nabídky a do návrhu kupní smlouvy. [↑](#footnote-ref-2)