# Aktivní Prvky, provozní monitoring LAN a WLAN

## Instalace a konfigurace aktivních síťových prvků LAN

Tato kapitola řeší specifikaci požadavků na vybavení počítačové sítě aktivními síťovými prvky dle nově navržené struktury UKS (univerzální kabelážní systém), a které tvoří síťovou LAN infrastrukturu. Návrh designu počítačové sítě je rozdělen do tří vrstev – přístupová (access), jádro (core) a datacentrová (DC).

**Přístupová vrstva (přístupové switche) včetně agregační akt. prvků**

Stávající prvky přístupové sítě jsou morálně zastaralé, s nevyhovující propustností, heterogenní, plně nepodporují důležitý protokol 802.1x. Požadována je generační výměna a rozšíření přístupové vrstvy sítě s cílem homogenizace aktivních prvků. Je požadováno nasazení L2 přístupových switchů dle níže uvedeného schématu na obr. 1 různých typů. Dodávané switche musí podporovat PoE+ (802.3bt) pro napájení přístupových bodů bezdrátové sítě (AP). Pokud bude v datovém rozvaděči více než jeden switch, musí být zapojeny do stohu speciálním stohovacím modulem.

Jako přístupové switche budou také využity některé switche, ve vlastnictví nemocnice, které jsou aktuálně využívané ve stávající infrastruktuře. Tyto stávající switche musí být vždy v rámci rozvaděče sestohovány s nově navrženými prvky tak, aby tvořili jeden logický prvek. Jejich umístění včetně uvedení typu switche je uvedeno na obr. 1 a v tabulce.

**Jádro sítě (core switche)**

Je požadována nově bude zbudována core vrstva, nasazením dvou L3 core switchů do prostředí dvou IT serveroven (Serverovna 1 a 2), v konfiguraci do jedné logické entity viz obr. 1. K této core vrstvě budou duálně připojeny všechny podružné rozvaděče, datacentrové prvky, firewally, kontrolery bezdrátové sítě, atd.

**Datová centra (DC switche)**

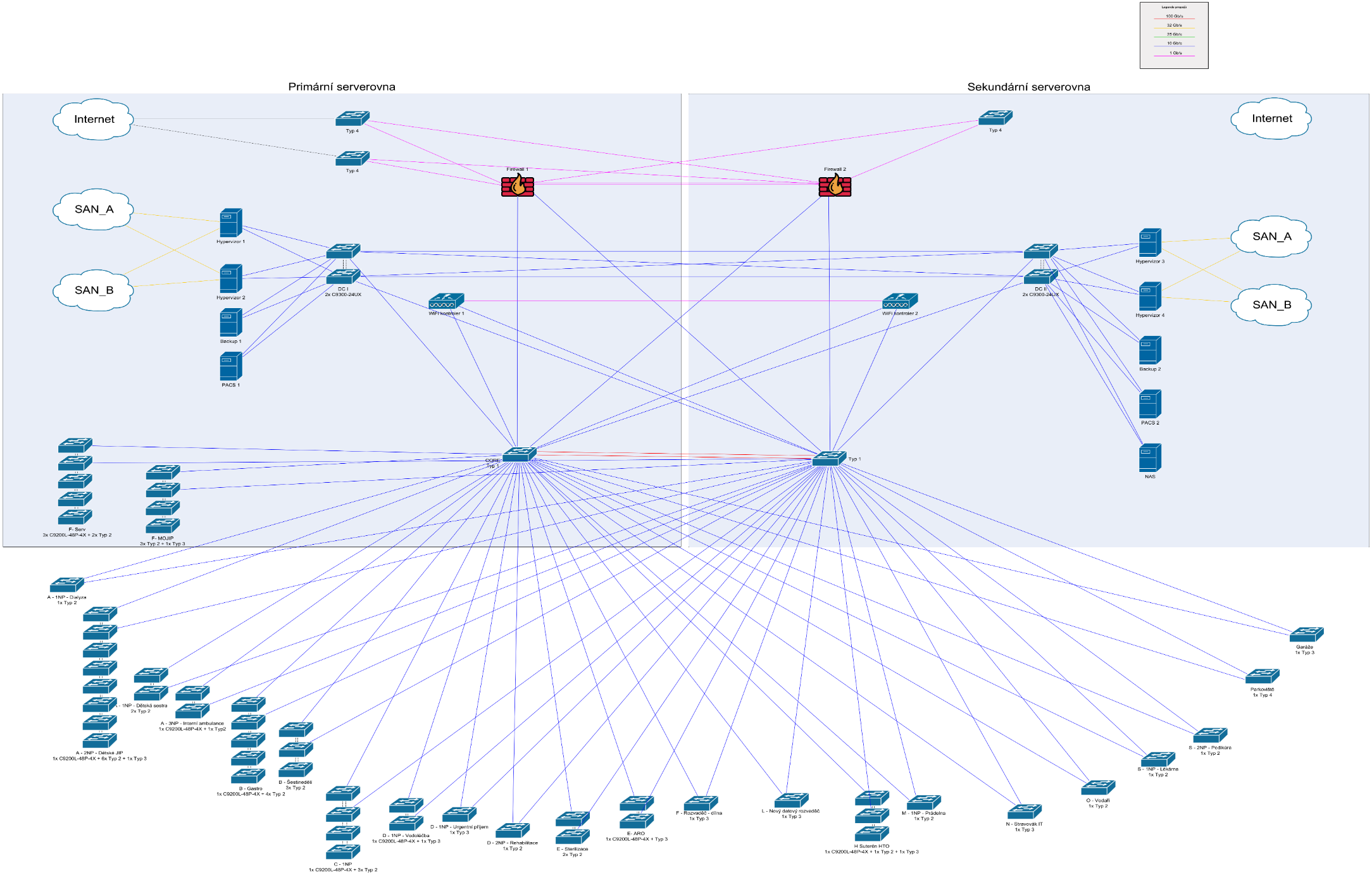
Je požadována datacentrová infrastruktura tvořená dvěma páry aktivních prvků typů C9300-24UX.V každé serverovně bude umístěn jeden pár, jenž vždy tvoří jednu logickou entitu, jenž poskytuje redundantní konektivitu pro jednotlivé servery. Tato infrastruktura se již nyní nachází ve vlastnictví nemocnice a svými parametry je výkonově i morálně dostačující. S ohledem na ochranu investic musí být v rámci projektu využita výše uvedeným způsobem.

Přehledové síťové schéma na obr. 1 detailně zobrazuje zapojení akt. prvků po jednotlivých datových rozvaděčích včetně vazby na související technologické části (virtualizační prostředí, zálohování, externí konektivita). Všechny navrhované switche musí být vybaveny příslušnými moduly pro připojení do počítačové sítě a to včetně připojovacích kabelů a stohovacích modulů, pokud je požadováno jejich sestohování v rámci datového rozvaděče viz obr. 1. Součástí dodávky musí být i všechny potřebné moduly (SFP, SFP+, QSSP, DAC, atd.) včetně nutného množství optických a metalických patchcordů tak, aby bylo dosaženo požadovaného cílového stavu infrastruktury zachyceném na obrázku 1. Počty aktivních prvků, v jednotlivých lokalitách, dle jejich typu, jsou uvedeny v následující tabulce.

Na všechny dodávané aktivní prvky je požadována záruka v rozsahu minimálně 5 let a po tuto dobu musí být výrobcem garantována podpora dodaných prvků.

**Tabulka rozmístění akt. prvků v jednotlivých lokalitách dle typu**

|  |  |  |
| --- | --- | --- |
| Datový rozvaděč | Typ akt. prvku | Počet kusů |
| Primární serverovna | FW 1 | 1 |
|  | WiFi kontrolér 1 | 1 |
|  | 1 | 1 |
|  | 2 | 5 |
|  | 3 | 1 |
|  | 4 | 2 |
|  | C9300-24UX | 2 |
|  | C9300L-48P-4X | 3 |
| Sekundární serverovna | FW 2 | 1 |
|  | WiFi kontrolér 2 | 1 |
|  | 1 | 1 |
|  | 4 | 1 |
|  | C9300-24UX | 2 |
| A – 1NP - Dialyza | 2 | 1 |
| A – 1NP – Dětská sestra | 2 | 2 |
| A – 2NP – Dětské JIP | 2 | 7 |
|  | 3 | 1 |
| A – 3NP – Interní ambulance | 2 | 1 |
| B - Gastro | 2 | 4 |
| B - Šestinedělí | 2 | 3 |
| C – 1NP | 2 | 3 |
| D – 1NP - Vodoléčba | 1 | 1 |
|  | 3 | 1 |
| D – 1NP – Urgentní příjem | 3 | 1 |
| D – 2 NP - Rehabilitace | 2 | 1 |
| E - Sterilizace | 2 | 2 |
| E - ARO | 3 | 1 |
| F – Rozvaděč dílna | 3 | 1 |
| H – Suterén HTO | 2 | 1 |
|  | 3 | 1 |
| L – Nový datový rozvaděč | 3 | 1 |
| M – 1NP - Prádelna | 2 | 1 |
| N – Stravovák IT | 3 | 1 |
| O – Vodaři | 2 | 1 |
| S – 1NP – Lékárna | 2 | 1 |
| S – 2NP – Pedikůra | 2 | 1 |
| Parkoviště | 4 | 1 |
| Garáže | 3 | 1 |



Obr. 1: Topologie řešení počítačové sítě (viz také soubor „Topologie řešení počítačové sítě.png“)

## Monitoring aktivních prvků LAN a bezdrátové sítě (WLAN)

Požadovanou součástí projektu je instalace a konfigurace provozního monitoringu, který v sobě bude integrovat monitoring poptávaných a stávajících aktivních prvků LAN (viz výše uvedená tabulka a obr.) a WLAN. Tento SW nástroj bude provozován jako cloudové řešení.

Součástí implementace bude nastavení pravidel hodnocení shromážděných dat, prahových hodnot (alertů), nastavení notifikací na odpovědné pracovníky (min. e-mailové notifikace), eskalace notifikací a tvorba reportů.

## Specifikace minimálních požadavků technického řešení

### Aktivní síťové prvky LAN

#### TYP aktivního prvku 1

|  |  |
| --- | --- |
| **Požadovaná funkcionalita** | **Specifikace minimálních požadavků** |
| Typ přepínače | L2/L3 přepínač |
| Minimální počet neblokovaných portů 1/10/25GE s volitelným fyzickým rozhraním typu SFP28 | 48 |
| Uplink porty | 4x 40/100GE QSFP28 |
| Interní redundantní napájecí zdroj | ANO |
| Min. velikost sdíleného systémového bufferu | 36MB |
| Velikost MAC address tabulky | 80000 |
| Min. počet IPv4 routes | 100000 |
| Min. počet IPv6 routes | 100000 |
| Min. počet konfigurovatelných security ACL | 27000 |
| Flexibilní alokace SRAM a TCAM zdrojů | ANO |
| IEEE 802.3ad (Link Aggregation - LAG) | ANO |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | ANO |
| ISSU | ANO |
| Minimální počet aktivních VLAN | 4000 |
| IEEE 802.1w - Rapid Spanning Tree Protocol | ANO |
| Podpora instance spanning-tree protokolu per VLAN | ANO |
| Podpora jumbo rámců (min. 9198 bytes) | ANO |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | ANO |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | ANO |
| OSPFv2, OSPFv3 | ANO |
| EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868) | ANO |
| ISIS | ANO |
| BGPv4 | ANO |
| VXLAN s BGP EVPN | ANO |
| Graceful Insertion and Removal | ANO |
| IP Multicast ( PIM SSM, PIM SM) | ANO |
| Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF) | ANO |
| Min. počet oddělených (nezávislých) směrovacích tabulek | 10 |
| MPLS VPN | ANO |
| MPLS VPN - 6VPE | ANO |
| First Hop Redundancy Protokol (např. VRRP, HSRP) pro IPv4 i IPv6 | ANO |
| Reverse path check (uRPF) | ANO |
| Minimální počet HW QoS front | 8 |
| QoS - Strict Priority Queue | ANO |
| QoS classification – ACL, DSCP, CoS based | ANO |
| QoS marking - DSCP, CoS | ANO |
| QoS Policing | ANO |
| QoS-Hierarchical QoS | ANO |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | ANO |
| IPv6 First Hop Security (RA guard, DHCPv6 guard, IPv6 source guard) | ANO |
| Port ACL, VLAN ACL | ANO |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | ANO |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů | ANO |
| HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů | ANO |
| Podpora SUDI  (IEEE 802.1AR) autentizace | ANO |
| IPv6 Port ACL, VLAN ACL | ANO |
| IEEE 802.1AE na všech portech | ANO |
| IEEE 802.1ae (AES-GCM-256) na všech portech | ANO |
| Source-Group Tag Exchange Protocol nebo ekvivalentní | ANO |
| IGMPv2/v3 snooping | ANO |
| MLD snooping | ANO |
| Multicast DNS (mDNS) gateway | ANO |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | ANO |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | ANO |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | ANO |
| SSHv2 | ANO |
| CLI rozhraní | ANO |
| Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu | ANO |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | ANO |
| Python scripting | ANO |
| Linux shell | ANO |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | ANO |
| Application hosting | ANO |
| Aplikace softwarových záplat, nikoli povyšování celého firmware | ANO |
| Streaming telemetrie prostřednictvím NETCONF/XML | ANO |
| SNMPv2/v3 | ANO |
| Inventarizovatelnost komponent integrovanou RFID identifikací | ANO |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | ANO |
| Vzdálený port mirroring (ERSPAN) | ANO |
| NTPv3 server | ANO |

#### TYP aktivního prvku 2

|  |  |
| --- | --- |
| **Požadovaná funkcionalita** | **Specifikace minimálních požadavků** |
| Typ přepínače | L2/L3 přepínač |
| Formát přepínače | Stohovatelný |
| Stohování požadováno | ANO |
| Počet dedikovaných stohovacích portů | 2 |
| Minimální počet zařízení ve stohu | 8 |
| Minimální kapacita sběrnice stohu | 80 Gb/s |
| Stateful Switch Over v rámci stohu | ANO |
| Možnost instalovat interní redundantní napájecí zdroj | ANO |
| Redundantní ventilátory | ANO |
| Interní redundantní napájecí zdroj požadován | NE |
| Datový stohovací kabel požadován | ANO |
| Minimální PoE budget | 740 W |
| Počet portů 10/100/1000 Base-TX s PoE+ napájením | 48 |
| Uplink porty | 4x10GE SFP+ |
| Min. velikost sdíleného systémového bufferu | 6MB |
| Velikost MAC address tabulky | 16000 |
| Min. počet IPv4 routes | 3000 |
| Min. počet IPv6 routes | 1500 |
| Min. počet konfigurovatelných security ACL | 1000 |
| IEEE 802.3ad (Link Aggregation) | ANO |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | ANO |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | ANO |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 48 |
| IEEE 802.1Q | ANO |
| Minimální počet aktivních VLAN | 1000 |
| IEEE 802.1x | ANO |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | ANO |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | ANO |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | ANO |
| RADIUS CoA | ANO |
| Podpora instance spanning-tree protokolu per VLAN | ANO |
| IEEE 802.1w - Rapid Spanning Tree Protocol | ANO |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | ANO |
| Podpora jumbo rámců (min. 9198 bytes) | ANO |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | ANO |
| Směrování protokolů IPv4 a IPv6 v hardware | ANO |
| OSPFv2 | ANO |
| OSPFv3 | ANO |
| ISIS | ANO, povýšením firmware |
| IP Multicast ( PIM SSM, PIM SM) | ANO, povýšením firmware |
| First Hop Redundancy Protokol (např. VRRP, HSRP) | ANO, povýšením firmware |
| Reverse path check (uRPF) pro IPv4 i IPv6 | ANO |
| IGMPv2, IGMPv3 | ANO |
| IGMP snooping | ANO |
| MLD snooping | ANO |
| DHCP relay | ANO |
| Minimální počet HW QoS front | 8 |
| QoS classification – ACL, DSCP, CoS based | ANO |
| QoS marking - DSCP, CoS | ANO |
| QoS - Strict Priority Queue | ANO |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | ANO |
| QoS Policing | ANO |
| QoS-Hierarchical QoS | ANO, min. 2 úrovně |
| First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP) | ANO |
| IPv6 services (SSH, Syslog) | ANO |
| IPv6 QoS | ANO |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | ANO |
| IPv6 Port ACL, VLAN ACL | ANO |
| Možnost definovat povolené MAC adresy na portu | ANO |
| PACL, VACL | ANO |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | ANO, povýšením firmware |
| IEEE 802.1ae na uplink portech | ANO |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | ANO |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | ANO |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | ANO |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů | ANO |
| HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů | ANO |
| Podpora SUDI (IEEE 802.1AR) autentizace | ANO |
| Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače | ANO |
| Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení | ANO |
| IEEE 802.3az | ANO |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | ANO |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | ANO |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | ANO |
| SSHv2 | ANO |
| CLI rozhraní | ANO |
| Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu | ANO |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | ANO |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | ANO |
| Streaming telemetrie prostřednictvím NETCONF/XML | ANO |
| SNMPv2/v3 | ANO |
| Podpora network boot (iPXE) | ANO |
| Inventarizovatelnost komponent integrovanou RFID identifikací | ANO |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | ANO |
| NTPv3 server | ANO |

#### TYP aktivního prvku 3

|  |  |
| --- | --- |
| **Požadovaná funkcionalita** | **Specifikace minimálních požadavků** |
| Typ přepínače | L2/L3 přepínač |
| Formát přepínače | Stohovatelný |
| Stohování požadováno | ANO |
| Počet dedikovaných stohovacích portů | 2 |
| Minimální počet zařízení ve stohu | 8 |
| Minimální kapacita sběrnice stohu | 80 Gb/s |
| Stateful Switch Over v rámci stohu | ANO |
| Možnost instalovat interní redundantní napájecí zdroj | ANO |
| Redundantní ventilátory | ANO |
| Interní redundantní napájecí zdroj požadován | NE |
| Datový stohovací kabel požadován | ANO |
| Minimální PoE budget | 370 W |
| Počet portů 10/100/1000 Base-TX s PoE+ napájením | 24 |
| Uplink porty | 4x10GE SFP+ |
| Min. velikost sdíleného systémového bufferu | 6MB |
| Velikost MAC address tabulky | 16000 |
| Min. počet IPv4 routes | 3000 |
| Min. počet IPv6 routes | 1500 |
| Min. počet konfigurovatelných security ACL | 1000 |
| IEEE 802.3ad (Link Aggregation) | ANO |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | ANO |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | ANO |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 48 |
| IEEE 802.1Q | ANO |
| Minimální počet aktivních VLAN | 1000 |
| IEEE 802.1x | ANO |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | ANO |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | ANO |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | ANO |
| RADIUS CoA | ANO |
| Podpora instance spanning-tree protokolu per VLAN | ANO |
| IEEE 802.1w - Rapid Spanning Tree Protocol | ANO |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | ANO |
| Podpora jumbo rámců (min. 9198 bytes) | ANO |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | ANO |
| Směrování protokolů IPv4 a IPv6 v hardware | ANO |
| OSPFv2 | ANO |
| OSPFv3 | ANO |
| ISIS | ANO, povýšením firmware |
| IP Multicast ( PIM SSM, PIM SM) | ANO, povýšením firmware |
| First Hop Redundancy Protokol (např. VRRP, HSRP) | ANO, povýšením firmware |
| Reverse path check (uRPF) pro IPv4 i IPv6 | ANO |
| IGMPv2, IGMPv3 | ANO |
| IGMP snooping | ANO |
| MLD snooping | ANO |
| DHCP relay | ANO |
| Minimální počet HW QoS front | 8 |
| QoS classification – ACL, DSCP, CoS based | ANO |
| QoS marking - DSCP, CoS | ANO |
| QoS - Strict Priority Queue | ANO |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | ANO |
| QoS Policing | ANO |
| QoS-Hierarchical QoS | ANO, min. 2 úrovně |
| First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP) | ANO |
| IPv6 services (SSH, Syslog) | ANO |
| IPv6 QoS | ANO |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | ANO |
| IPv6 Port ACL, VLAN ACL | ANO |
| Možnost definovat povolené MAC adresy na portu | ANO |
| PACL, VACL | ANO |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | ANO, povýšením firmware |
| IEEE 802.1ae na uplink portech | ANO |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | ANO |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | ANO |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | ANO |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů | ANO |
| HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů | ANO |
| Podpora SUDI (IEEE 802.1AR) autentizace | ANO |
| Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače | ANO |
| Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení | ANO |
| IEEE 802.3az | ANO |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | ANO |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | ANO |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | ANO |
| SSHv2 | ANO |
| CLI rozhraní | ANO |
| Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu | ANO |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | ANO |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | ANO |
| Streaming telemetrie prostřednictvím NETCONF/XML | ANO |
| SNMPv2/v3 | ANO |
| Podpora network boot (iPXE) | ANO |
| Inventarizovatelnost komponent integrovanou RFID identifikací | ANO |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | ANO |
| NTPv3 server | ANO |

#### TYP aktivního prvku 4

|  |  |
| --- | --- |
| **Požadovaná funkcionalita** | **Specifikace minimálních požadavků** |
| Typ přepínače | L2/L3 přepínač |
| Formát přepínače | Fixní konfigurace |
| Bezventilátorový | ANO |
| Počet portů 10/100/1000 Base-TX s PoE+ napájením | 8 |
| Minimální PoE budget | 240W |
| Uplink porty | 2x10/100/1000 + 2x10GE SFP+ |
| Min. velikost sdíleného systémového bufferu | 6MB |
| Velikost MAC address tabulky | 32000 |
| Min. počet IPv4 routes | 600 |
| Min. počet IPv6 routes | 300 |
| Min. počet konfigurovatelných security ACL | 1500 |
| IEEE 802.3ad (Link Aggregation) | ANO |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | ANO |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | ANO |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 48 |
| IEEE 802.1Q | ANO |
| Minimální počet aktivních VLAN | 512 |
| IEEE 802.1x | ANO |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | ANO |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | ANO |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | ANO |
| RADIUS CoA | ANO |
| Podpora instance spanning-tree protokolu per VLAN | ANO |
| IEEE 802.1w - Rapid Spanning Tree Protocol | ANO |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | ANO |
| Podpora jumbo rámců (min. 9198 bytes) | ANO |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | ANO |
| Směrování protokolů IPv4 a IPv6 v hardware | ANO |
| OSPFv2 | ANO |
| OSPFv3 | ANO |
| EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868) | ANO, povýšením firmware |
| ISIS | ANO, povýšením firmware |
| IP Multicast ( PIM SSM, PIM SM) | ANO, povýšením firmware |
| Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF) | ANO, povýšením firmware |
| First Hop Redundancy Protokol (např. VRRP, HSRP) | ANO |
| Reverse path check (uRPF) pro IPv4 i IPv6 | ANO |
| IGMPv2, IGMPv3 | ANO |
| IGMP snooping | ANO |
| MLD snooping | ANO |
| DHCP relay | ANO |
| Minimální počet HW QoS front | 8 |
| QoS classification – ACL, DSCP, CoS based | ANO |
| QoS marking - DSCP, CoS | ANO |
| QoS - Strict Priority Queue | ANO |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | ANO |
| QoS Policing | ANO |
| QoS-Hierarchical QoS | ANO, min. 2 úrovně |
| First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP) | ANO |
| IPv6 services (Telnet, SSH, Syslog, DHCP) | ANO |
| IPv6 QoS | ANO |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | ANO |
| IPv6 Port ACL, VLAN ACL | ANO |
| Možnost definovat povolené MAC adresy na portu | ANO |
| PACL, VACL | ANO |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | ANO, povýšením firmware |
| IEEE 802.1ae na uplink portech | ANO |
| IEEE 802.1ae (AES-GCM-256) na uplink portech | ANO |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | ANO |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | ANO |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | ANO |
| Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-10 nebo funkčně ekvivalentní). | ANO |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů | ANO |
| HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů | ANO |
| Podpora SUDI (IEEE 802.1AR) autentizace | ANO |
| IEEE 802.3af | ANO |
| IEEE 802.3at | ANO |
| Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače | ANO |
| Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení | ANO |
| IEEE 802.3az | ANO |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |
| Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur) | ANO, povýšením firmware |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | ANO |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | ANO |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | ANO |
| SSHv2 | ANO |
| CLI rozhraní | ANO |
| Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu | ANO |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | ANO |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | ANO |
| Aplikace softwarových záplat, nikoli povyšování celého firmware | ANO, povýšením firmware |
| Streaming telemetrie prostřednictvím NETCONF/XML | ANO |
| SNMPv2/v3 | ANO |
| Podpora network boot (iPXE) | ANO |
| Inventarizovatelnost komponent integrovanou RFID identifikací | ANO |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | ANO |
| NTPv3 server | ANO |

### Provozní monitoring LAN a WLAN

|  |  |
| --- | --- |
| **Požadovaná funkcionalita** | **Specifikace minimálních požadavků** |
| Centrální systém monitorování sítě musí umožnit zabezpečené vzdálené monitorování pro všechny poptávané komponenty sítě (přepínače, WiFi kontrolery a bezdrátové přístupové body) a to prostřednictvím jednotného integrovaného webového rozhraní. | ANO |
| Centrální systém monitorování sítě musí být schopen zobrazit všechny klientská zařízení připojená k síti během minimálně posledních 10 dnů. Výpis by měl obsahovat minimálně následující informace:   * Uživatelské jméno * IP a MAC adresa zařízení   Objem uživatelem / zařízením přenesených dat za dané období s rozpadem na jednotlivé rozpoznané aplikace | ANO |
| Systém musí být schopen zobrazit seznam top uživatelů, kteří za dané období v síti přenesli nejvíce dat. | ANO |
| Systém musí být schopen zobrazit polohu a stav všech síťových zařízení v systému v geografické mapě a také graficky zobrazit reálnou fyzickou topologii sítě. | ANO |
| Systém musí být schopen zobrazit polohu všech klientských zařízení v závislosti na způsobu jejich připojení a to buď přímo v plánech jednotlivých podlaží, v geografické mapě nebo v kontextu portu příslušného LAN přepínače. | ANO |
| Systém musí být provozován v režimu vysoké dostupnosti. | ANO |
| Základní konektivita a přístup do Internetu musí být pro klienty zachován i v případě, že je Centrální systém monitorování sítě dočasně nedostupný. | ANO |
| Systém musí umožnit rozdělení administrátorů do skupin s různými právy přístupu. | ANO |
| Pro autentizaci administrátora přistupujícího přes webové rozhraní musí systém podporovat minimálně RADIUS protokol, SAML a dvoufaktorovou autentizaci. | ANO |
| Systém musí být schopen odesílat správcům emailové zprávy o důležitých systémových událostech. | ANO |
| Systém musí být schopen odesílat zprávy na vzdálený SYSLOG server. | ANO |
| Systém musí podporovat SNMP protokol pro vzdálenou správu a monitorování. | ANO |
| Systém musí podporovat XML API pro integraci s navazujícími systémy poskytující informace o připojených komponentách sítě a také klientských zařízeních. | ANO |
| Systém musí sledovat změny konfigurace systému, min. pro a zahrnutých WLAN síťových komponent – Informace musí minimálně obsahovat:   * položku konfigurace * uživatelské jméno administrátora, který změnu provedl   novou hodnotu proměnné, v které ke změně došlo | ANO |
| Systém musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 24 měsíců. | ANO |
| Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 24 měsíců a to včetně všech aktualizací softwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce.  Systém musí být v době prodeje výrobcem plně podporován a na žádnou jeho část nesmí být vyhlášeno ukončení prodeje. | ANO |