# Požadované technické parametry dodávky

Předmětem dodávky jsou aktivní síťové prvky dle technických podmínek uvedených níže.

- Bezdrátový přístupový bod typ A (100 ks).
- Bezdrátový přístupový bod typ B (50 ks).
- Přístupový stohovatelný gigabitový přepínač s možností napájení po Ethernetu typ A (2 ks).
- Přístupový stohovatelný gigabitový přepínač s možností napájení po Ethernetu typ B (6 ks).
- Přístupový stohovatelný gigabitový přepínač s možností napájení po Ethernetu s 10Gb uplink porty (1 ks).

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

## Tabulka povinných požadavků pro bezdrátový přístupový bod typ A (požadováno 100 ks)

| Požadavek na funkcionalitu | Minimální požadavky | Splňuje ANO/NE |
|---|---|---|
| **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 | 1 | |
| 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 | |
| **Výkonnostní parametry** | | |
| Fyzická přenosová rychlost bezdrátové části | 867 Mb/s | |
| **Protokoly fyzické vrstvy** | | |
| IEEE 802.11a/b/g/n/ac | ano | |
| MIMO (Multiple Input Multiple Output) | 3x3:2 | |
| IEEE 802.11n Maximal ratio combining (MRC) | ano | |
| Agregace rámců A-MPDU a A-MSDU | ano | |
| Dynamický výběr volné frekvence DFS | ano | |
| Podpora 20MHz a 40 MHz kanálů pro IEEE 802.11n | ano | |
| Podpora 80 MHz 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 | |
| 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 odchytáváním provozu a jeho zasíláním do analyzátoru (například Wireshark) | ano | |

## Tabulka povinných požadavků pro bezdrátový přístupový bod typ B (požadováno 50 ks)

| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje ANO/NE** |
|---|---|---|
| **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 | 1 | |
| Podpora IEEE 802.3at napájení z přepínače nebo injektoru | ano | |
| Typ antén | integrované pro obě pásma | |
| Montáž | na strop | |
| Podpora stávajících centralizovaných řadičů bezdrátové sítě | ano | |
| **Výkonnostní parametry** | | |
| Fyzická přenosová rychlost bezdrátové části | 1,3 Gb/s | |
| **Protokoly fyzické vrstvy** | | |
| IEEE 802.11a/b/g/n/ac | ano | |
| MIMO (Multiple Input Multiple Output) | 3x4:3 | |
| 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 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 odchytáváním | ano | |

| | | |
|---|---|---|
| provozu a jeho zasíláním do analyzátoru (například Wireshark) | | |

## Tabulka povinných požadavků pro přístupový stohovatelný gigabitový přepínač s možností napájení po Ethernetu typ A (požadovány 2 ks)

| Požadavek na funkcionalitu | Minimální požadavky | Splňuje ANO/NE |
|---|---|---|
| **Základní vlastnosti** | | |
| Třída zařízení | L2 přepínač | |
| Formát zařízení | fixní konfigurace, rozšiřitelný na stohování, 1RU | |
| Stohovatelný | ano, modulem | |
| Délka stohovacího kabelu | 50 cm | |
| Stohování požadováno | ano | |
| Počet RJ-45 portů 10/100/1000 | 48 | |
| Podpora PoE (IEEE 802.3af, 15,4W/port) | ano | |
| Podpora PoE+ (IEEE 802.3at, 30W/port) | ano | |
| Dostupný výkon pro napájení PoE portů | 740W | |
| Počet uplink portů 1GE a jejich typ | 2, SFP | |
| Požadovaný počet a typ transceiverů | 2, 1000BASE-T, SFP | |
| Možnost připojit externí redundantní zdroj | ano | |
| **Výkonnostní parametry** | | |
| Propustnost přepínacího subsystému | 200 Gbit/s | |
| Paketový výkon přepínače | 100 milionů paketů/vteřinu | |
| Rychlost stohovacího propojení | 80 Gbit/s | |
| **Vlastnosti stohování** | | |
| Vzájemné stohování všech modelů stejné řady s 1GE/10GE uplinky | ano | |
| Počet přepínačů ve stohu | 8 | |
| Automatická kontrola a sjednocení verze software přepínačů ve stohu | ano | |
| Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením | ano | |
| Seskupování portů (IEEE 802.3ad) mezi různými prvky stohu | ano | |
| Kterýkoli prvek ve stohu může být řídícím prvkem stohu (1:N redundance) | ano | |
| **Protokoly fyzické vrstvy** | | |
| IEEE 802.3-2005 | ano | |
| IEEE 802.3ad | ano | |
| Podpora "jumbo rámců" | ano | |
| **Protokoly spojové vrstvy** | | |
| IEEE 802.1D | ano | |
| IEEE 802.1Q | ano | |
| Počet aktivních VLAN | 1000 | |
| 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 - počet vnitřních front | 4 | |
| Per VLAN Rapid Spanning Tree (PVRST+) nebo ekvivalentní | ano | |
| Detekce protilehlého zařízení | ano | |

| | | |
|---|---|---|
| Detekce parametrů protilehlého zařízení | ano | |
| Protokol pro definici šířených VLAN | ano | |
| Detekce jednosměrnosti optické linky | ano | |
| STP root guard | ano | |
| STP loop guard | ano | |
| Možnost autorecovery po chybovém stavu | 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 | ano | |
| QoS i na stohovacím spoji | ano | |
| DHCP relay | ano | |
| **Protokol IPv6** | | |
| Podpora IPv6 ACL | ano | |
| Podpora IPv6 services ( DNS, Telnet, SSH, Syslog, ICMP) | ano | |
| Podpora IPv6 MLDv2 snooping | ano | |
| Podpora IPv6 Port ACL | ano | |
| Podpora IPv6 First Hop Security RA guard | ano | |
| Podpora IPv6 First Hop Security DHCPv6 guard | ano | |
| Podpora IPv6 First Hop Security IPv6 Binding Integrity Guard | ano | |
| **Směrování multicastu** | | |
| IGMPv2 snooping | ano | |
| IGMPv3 snooping | ano | |
| IPv6 MLDv1 & v2 snooping | ano | |
| **Bezpečnost** | | |
| 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 | |
| Podpora zabezpečení a analýzy DHCP protokolu | ano | |
| Podpora ochrany ARP protokolu | ano | |
| Podpora ochrany podvrženého mapování IP/MAC adresy | 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 | |
| **Podpora koncových zařízení** | | |
| Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury | ano | |
| Podpora IEEE 802.3az | ano | |

| | | |
|---|---|---|
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů | ano | |
| **Management** | | |
| CLI rozhraní | ano | |
| SSHv2 | ano | |
| SSHv2 over IPv6 | ano | |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ano | |
| SNMPv2 | ano | |
| SNMPv3 | ano | |
| Konzolová linka | ano | |
| DNS klient | ano | |
| NTP klient s MD5 autentizací | ano | |
| RADIUS klient pro AAA (autentizace, autorizace, accounting) | ano | |
| TACACS+ klient | ano | |
| Port mirroring | ano | |
| Vzdálený port mirroring | ano | |
| Syslog | ano | |
| Měření zakončení a délky metalického kabelu (TDR) | 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 | ano | |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ano | |

## Tabulka povinných požadavků pro přístupový stohovatelný gigabitový přepínač s možností napájení po Ethernetu typ B (požadováno 6 ks)

| Požadavek na funkcionalitu | Minimální požadavky | Splňuje ANO/NE |
|---|---|---|
| **Základní vlastnosti** | | |
| Třída zařízení | L2 přepínač | |
| Formát zařízení | fixní konfigurace, rozšiřitelný na stohování, 1RU | |
| Stohovatelný | ano, modulem | |
| Délka stohovacího kabelu | 50 cm | |
| Stohování požadováno | ano | |
| Stohování kompatibilní s přístupovým stohovatelným gigabitovým přepínačem s možností napájení po Ethernetu s 10Gb uplink porty požadovaným v této ZD | ano | |
| Počet RJ-45 portů 10/100/1000 | 48 | |
| Podpora PoE (IEEE 802.3af, 15,4W/port) | ano | |
| Podpora PoE+ (IEEE 802.3at, 30W/port) | ano | |
| Dostupný výkon pro napájení PoE portů | 350W | |
| Počet uplink portů 1GE a jejich typ | 2, SFP | |
| Možnost připojit externí redundantní zdroj | ano | |
| **Výkonnostní parametry** | | |
| Propustnost přepínacího subsystému | 200 Gbit/s | |
| Paketový výkon přepínače | 100 milionů paketů/vteřinu | |
| Rychlost stohovacího propojení | 80 Gbit/s | |

| **Vlastnosti stohování** | | |
|---|---|---|
| Vzájemné stohování všech modelů stejné řady s 1GE/10GE uplinky | ano | |
| Počet přepínačů ve stohu | 8 | |
| Automatická kontrola a sjednocení verze software přepínačů ve stohu | ano | |
| Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením | ano | |
| Seskupování portů (IEEE 802.3ad) mezi různými prvky stohu | ano | |
| Kterýkoli prvek ve stohu může být řídícím prvkem stohu (1:N redundance) | ano | |
| **Protokoly fyzické vrstvy** | | |
| IEEE 802.3-2005 | ano | |
| IEEE 802.3ad | ano | |
| Podpora "jumbo rámců" | ano | |
| **Protokoly spojové vrstvy** | | |
| IEEE 802.1D | ano | |
| IEEE 802.1Q | ano | |
| Počet aktivních VLAN | 1000 | |
| 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 - počet vnitřních front | 4 | |
| Per VLAN Rapid Spanning Tree (PVRST+) nebo ekvivalentní | ano | |
| Detekce protilehlého zařízení | ano | |
| Detekce parametrů protilehlého zařízení | ano | |
| Protokol pro definici šířených VLAN | ano | |
| Detekce jednosměrnosti optické linky | ano | |
| STP root guard | ano | |
| STP loop guard | ano | |
| Možnost autorecovery po chybovém stavu | 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 | ano | |
| QoS i na stohovacím spoji | ano | |
| DHCP relay | ano | |
| **Protokol IPv6** | | |
| Podpora IPv6 ACL | ano | |
| Podpora IPv6 services ( DNS, Telnet, SSH, Syslog, ICMP) | ano | |
| Podpora IPv6 MLDv2 snooping | ano | |
| Podpora IPv6 Port ACL | ano | |
| Podpora IPv6 First Hop Security RA guard | ano | |
| Podpora IPv6 First Hop Security DHCPv6 guard | ano | |
| Podpora IPv6 First Hop Security IPv6 Binding Integrity Guard | ano | |
| **Směrování multicastu** | | |
| IGMPv2 snooping | ano | |
| IGMPv3 snooping | ano | |
| IPv6 MLDv1 & v2 snooping | ano | |

| **Bezpečnost** | | |
|---|---|---|
| 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 | |
| Podpora zabezpečení a analýzy DHCP protokolu | ano | |
| Podpora ochrany ARP protokolu | ano | |
| Podpora ochrany podvrženého mapování IP/MAC adresy | 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 | |
| **Podpora koncových zařízení** | | |
| Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury | ano | |
| Podpora IEEE 802.3az | ano | |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů | ano | |
| **Management** | | |
| CLI rozhraní | ano | |
| SSHv2 | ano | |
| SSHv2 over IPv6 | ano | |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ano | |
| SNMPv2 | ano | |
| SNMPv3 | ano | |
| Konzolová linka | ano | |
| DNS klient | ano | |
| NTP klient s MD5 autentizací | ano | |
| RADIUS klient pro AAA (autentizace, autorizace, accounting) | ano | |
| TACACS+ klient | ano | |
| Port mirroring | ano | |
| Vzdálený port mirroring | ano | |
| Syslog | ano | |
| Měření zakončení a délky metalického kabelu (TDR) | 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 | ano | |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ano | |

# Tabulka povinných požadavků pro přístupový stohovatelný gigabitový přepínač s možností napájení po Ethernetu s 10Gb uplink porty (požadován 1 ks)

| Požadavek na funkcionalitu | Minimální požadavky | Splňuje ANO/NE |
|---|---|---|
| **Základní vlastnosti** | | |
| Třída zařízení | L2 přepínač | |
| Formát zařízení | fixní konfigurace, rozšiřitelný na stohování, 1RU | |
| Stohovatelný | ano, modulem | |
| Délka stohovacího kabelu | 1 m | |
| Stohování požadováno | ano | |
| Stohování kompatibilní s přístupovým stohovatelným gigabitovým přepínačem s možností napájení po Ethernetu typ B požadovaným v této ZD | ano | |
| Počet RJ-45 portů 10/100/1000 | 48 | |
| Podpora PoE (IEEE 802.3af, 15,4W/port) | ano | |
| Podpora PoE+ (IEEE 802.3at, 30W/port) | ano | |
| Dostupný výkon pro napájení PoE portů | 350W | |
| Počet uplink portů 1GE a jejich typ | 2, SFP+ | |
| Požadovaný počet a typ transceiverů | 2, 10GBase-LR, SFP+ | |
| Možnost připojit externí redundantní zdroj | ano | |
| **Výkonnostní parametry** | | |
| Propustnost přepínacího subsystému | 200 Gbit/s | |
| Paketový výkon přepínače | 100 milionů paketů/vteřinu | |
| Rychlost stohovacího propojení | 80 Gbit/s | |
| **Vlastnosti stohování** | | |
| Vzájemné stohování všech modelů stejné řady s 1GE/10GE uplinky | ano | |
| Počet přepínačů ve stohu | 8 | |
| Automatická kontrola a sjednocení verze software přepínačů ve stohu | ano | |
| Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením | ano | |
| Seskupování portů (IEEE 802.3ad) mezi různými prvky stohu | ano | |
| Kterýkoli prvek ve stohu může být řídícím prvkem stohu (1:N redundance) | ano | |
| **Protokoly fyzické vrstvy** | | |
| IEEE 802.3-2005 | ano | |
| IEEE 802.3ad | ano | |
| Podpora "jumbo rámců" | ano | |
| **Protokoly spojové vrstvy** | | |
| IEEE 802.1D | ano | |
| IEEE 802.1Q | ano | |
| Počet aktivních VLAN | 1000 | |
| 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 - počet vnitřních front | 4 | |

| | | |
|---|---|---|
| Per VLAN Rapid Spanning Tree (PVRST+) nebo ekvivalentní | ano | |
| Detekce protilehlého zařízení | ano | |
| Detekce parametrů protilehlého zařízení | ano | |
| Protokol pro definici šířených VLAN | ano | |
| Detekce jednosměrnosti optické linky | ano | |
| STP root guard | ano | |
| STP loop guard | ano | |
| Možnost autorecovery po chybovém stavu | 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 | ano | |
| QoS i na stohovacím spoji | ano | |
| DHCP relay | ano | |
| **Protokol IPv6** | | |
| Podpora IPv6 ACL | ano | |
| Podpora IPv6 services ( DNS, Telnet, SSH, Syslog, ICMP) | ano | |
| Podpora IPv6 MLDv2 snooping | ano | |
| Podpora IPv6 Port ACL | ano | |
| Podpora IPv6 First Hop Security RA guard | ano | |
| Podpora IPv6 First Hop Security DHCPv6 guard | ano | |
| Podpora IPv6 First Hop Security IPv6 Binding Integrity Guard | ano | |
| **Směrování multicastu** | | |
| IGMPv2 snooping | ano | |
| IGMPv3 snooping | ano | |
| IPv6 MLDv1 & v2 snooping | ano | |
| **Bezpečnost** | | |
| 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 | |
| Podpora zabezpečení a analýzy DHCP protokolu | ano | |
| Podpora ochrany ARP protokolu | ano | |
| Podpora ochrany podvrženého mapování IP/MAC adresy | 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 | |
| **Podpora koncových zařízení** | | |
| Měření a ovládání spotřeby energie připojených koncových zařízení a | ano | |

| | | |
|---|---|---|
| infrastruktury | | |
| Podpora IEEE 802.3az | ano | |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů | ano | |
| **Management** | | |
| CLI rozhraní | ano | |
| SSHv2 | ano | |
| SSHv2 over IPv6 | ano | |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ano | |
| SNMPv2 | ano | |
| SNMPv3 | ano | |
| Konzolová linka | ano | |
| DNS klient | ano | |
| NTP klient s MD5 autentizací | ano | |
| RADIUS klient pro AAA (autentizace, autorizace, accounting) | ano | |
| TACACS+ klient | ano | |
| Port mirroring | ano | |
| Vzdálený port mirroring | ano | |
| Syslog | ano | |
| Měření zakončení a délky metalického kabelu (TDR) | 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 | ano | |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ano | |

## Struktura technické části nabídky

Technická část nabídky musí obsahovat:

- Podrobný popis technických a funkčních parametrů nabízeného řešení formou vyplnění tabulky mandatorních požadavků, 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

### 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 síření 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/HTPS 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).

## Nástroje používané pro správu sítě ZČU

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

### *Správa konfigurací*

Zálohování konfigurací všech aktivních komunikačních prvků Cisco je prováděno centrálně automaticky pomocí systému RANCID[1] s webovou nadstavbou Subversion (pro přehledné zobrazování změn) periodicky alespoň jednou denně. Archivace (změn) historie konfigurací je udržována minimálně po dobu jednoho roku. Navíc jsou paralelně zálohovány konfigurace (a jejich přehledných sumárních změny) všech aktivních komunikačních prvků Cisco pomocí systému NeDi[2] periodicky alespoň jednou denně. Archivace (změn) historie konfigurací je opět v systému NeDi udržována minimálně po dobu jednoho roku.
Pro hromadné konfigurace skupin zařízení se využívají systémy Netmanager[3], umožňující paralelní vykonávání příkazů, a NeDi.

### *Správa bezdrátové sítě*

[1] http://www.shrubbery.net/rancid/
[2] http://nedi.ch/
[3] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

Na ZČU je provozována bezdrátová síť eduroam[4], 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 freeRADIUS[5]. Pro správu a konfiguraci bezdrátových přístupových bodů je využíváno centralizované řešení. Jako centrální prvky jsou použity tři bezdrátové řadiče[6] pracující v režimu active/standby, které jsou schopny současně spravovat až 1100 AP. K udržení konzistentní konfigurace obou bezdrátových řadičů je používán specializovaný software[7].

### *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 Sauron[8] v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet[9] 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 Netdisco[10] 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, 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.

### *Monitorování provozu*

#### Provozní trendy

Pro sledování non-stop dostupnosti na úrovni služeb se používá systém Nagios[12], který je současně také využíván pro monitorování dostupnosti všech aktivních komunikačních prvků a služebních/management serverů, včetně konfigurace automatického upozorňování/eskalace e-mailem při detekci problémové/chybové situace.

Pro sledování non-stop dostupnosti na úrovni služeb pro systém VoIP ZČU se používá systém Nagios[13], který je využíván pro monitorování dostupnosti všech aktivních komunikačních prvků a služebních/management serverů systému VoIP ZČU, včetně konfigurace automatického upozorňování/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 Dude[14].

---

4 http://www.eduroam.cz

5 http://freeradius.org

6 Dva bezdrátové řadiče Cisco Wireless LAN Controller (WLC) 5520 pro 600 AP, dva bezdrátové řadiče Cisco Wireless LAN Controller (WLC) 5508 pro 400 AP a Cisco WLC 4404 pro 100 AP.

7 Cisco Prime Infrastructure verze 3.1 pro 1100 AP ve virtualizovaném prostředí.

8 http://sauron.jyu.fi/

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

10 http://www.netdisco.org/

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

Pro non-stop historii sledování základních L2 provozních charakteristik aktivních komunikačních prvků všech prostředí pomocí SNMP[15] (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 Cricket[16] a Torrus[17] 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 (kolejní extranet) a specializované FlowMon[18] sondy (kolejní intranet) se zpracovávají jednak nevzorkované pomocí produkčního IPv4 software Caligare Flow Inspector/CFI[19] a jednak vzorkované 1:10 pomocí testovacího IPv4/IPv6 software FTAS[20].
Pro monitorování historie latence/jitteru/ztrátovosti paketů (typicky VoIP subsystému) se používá aktivní nástroj Smokeping[21].
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 Core[22] pro inteligentní korelaci trapů.
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 OSSEC[23] 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 ARPwatch[24].
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 nejblíže místu svého vzniku podle typu komunikačního prvku) je řízeno pomocí nástroje NetSpy[25]. 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 pouze[26] 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,

---

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

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.

pokud tuto vlastnost podporují. AAA auditní informace o administrátorských přístupech ke konfigurovaným zařízením je k dispozici na TACACS+ serverech CIV ZČU.