Základní škola Slatiňany, okres Chrudim

ZŠ Slatiňany – modernizace datové a síťové infrastruktury

Technický podklad pro aktivní prvky

Zadavatel:

Základní škola Slatiňany, okres Chrudim
T.G. Masaryka 136
538 21 Slatiňany
IČO: 750 16 460
DIČ: CZ75016460

Veřejná zakázka: ZŠ Slatiňany – modernizace datové a síťové infrastruktury

Obsah

1. POPIS ZAKÁZKY 3
2. ROZSAH PROJEKTU 3
3. TECHNICKÉ POŽADAVKY 4
3.1 Centrální správa a jednotná platforma 4
3.2 Výkon a kapacita 4
3.3 Síťové funkce a segmentace 4
3.4 Bezpečnostní požadavky 5
3.5 Standardy a kompatibilita 5
3.6 Spolehlivost a dostupnost 5
4. AKTIVNÍ PRVKY - NEXTGEN FIREWALL 6
5. AKTIVNÍ PRVKY - CORE SWITCH 7
5.1 Hardwarové požadavky 7
5.2 Výkonové parametry 7
5.3 L3 a síťové funkce 7
5.4 Bezpečnostní funkce 8
5.5 Správa a monitoring 8
5.6 Redundance a rozšiřitelnost 8
5.7 Logická segmentace sítě 8
6. AKTIVNÍ PRVKY - DISTRIBUČNÍ SWITCHE 9
6.1 Hardwarové požadavky 9
6.2 Výkonové požadavky 9
6.3 Síťové funkce 9
6.4 Bezpečnostní funkce 10
6.5 Správa a monitoring 10
6.6 Napájení a PoE 10
6.7 Rozšiřitelnost 10
7. WIFI INFRASTRUKTURA 11
7.1 Počet a rozmístění zařízení 11
7.2 Technické požadavky na přístupové body 11
7.3 Kapacita a provoz 12
7.4 Pokročilé funkce 12
7.5 Bezpečnost a řízení přístupu 12
7.6 Správa a controller 13
8. ZÁLOŽNÍ ZDROJE 14
8.1 UPS pro hlavní rozvaděč 14
8.2 UPS pro vedlejší rozvaděče 14
9. POŽADAVEK NA KOMPATIBILITU 15
9.1 Správa a monitoring 15
9.2 Kompatibilita koncových zařízení 15
9.3 Řízení přístupů 15

1. Popis zakázky

Zadavatel požaduje komplexní modernizaci síťové infrastruktury Základní školy Slatiňany za účelem zajištění spolehlivého, bezpečného a výkonného síťového připojení pro všechny prostory školní budovy. Současná síťová infrastruktura již neodpovídá požadavkům moderního vzdělávacího procesu ani potřebám digitalizace školství.

Předmětem plnění je dodávka, instalace, konfigurace a zprovoznění aktivních prvků datové sítě, které budou tvořit jednotný, plně funkční a centrálně spravovatelný celek. Navržené řešení musí zajistit dlouhodobě stabilní provoz, vysokou úroveň bezpečnosti a dostatečnou kapacitu pro současné i budoucí potřeby školy.

Zadavatel klade důraz na použití kvalitních komponent určených pro profesionální nasazení, odbornou instalaci provedenou kvalifikovanými techniky a předání kompletní dokumentace, včetně zaškolení správce IT. Řešení musí být navrženo jako škálovatelné a rozšiřitelné bez nutnosti zásadních zásahů do infrastruktury.

Dodané řešení musí splňovat všechny příslušné technické normy a standardy pro síťové infrastruktury v budovách a musí být realizováno v souladu s požadavky na strukturovanou kabeláž dle norem řady ISO/IEC 11801.

Součástí plnění je rovněž integrace dodaného řešení do stávající IT infrastruktury zadavatele, zajištění jeho plné funkčnosti a ověření provozu v reálných podmínkách.

2. Rozsah projektu

Předmětem této části veřejné zakázky je dodávka, instalace, konfigurace a zprovoznění aktivních prvků datové sítě v objektu ZŠ Slatiňany.

Řešení navazuje na realizaci pasivní infrastruktury (strukturovaná kabeláž a optické spoje) a tvoří její funkční nadstavbu zajišťující přenos dat, přístup k síťovým službám, připojení k internetu a bezpečný provoz ICT prostředí školy.

Součástí projektu je zejména:

- dodávka centrálního bezpečnostního prvku (Next-Generation firewall),
- dodávka centrálního přepínače (core switch) s podporou L3 funkcionality,
- dodávka distribučních a přístupových přepínačů,
- dodávka a implementace bezdrátové sítě (WiFi),
- zajištění záložního napájení (UPS),
- implementace centrální správy všech aktivních prvků.

Bezdrátová síť musí zajistit pokrytí celé školní budovy, včetně učeben, chodeb a společných prostor, s dostatečnou kapacitou pro současné připojení většího počtu zařízení.

Řešení musí umožňovat logické členění sítě prostřednictvím VLAN segmentace, a to minimálně pro oddělení provozu administrativy, pedagogických pracovníků, žáků a hostů. Komunikace mezi jednotlivými segmenty musí být řízena a zabezpečena prostřednictvím definovaných bezpečnostních politik.

Dodavatel je povinen dodat řešení jako plně funkční celek („na klíč“), včetně veškerých potřebných licencí, konfigurace, otestování a uvedení do provozu.

3. Technické požadavky

Technické řešení musí být navrženo jako profesionální, škálovatelné a centrálně spravovatelné. Všechny aktivní prvky musí tvořit jednotný funkční celek umožňující centralizovanou konfiguraci, monitoring a správu.

Řešení musí být určeno pro provoz ve veřejných institucích a musí být dlouhodobě podporováno výrobcem, a to minimálně po dobu 5 let od dodání. Zadavatel **nepřipouští řešení** určená primárně **pro domácí nebo SOHO segment.**

3.1 Centrální správa a jednotná platforma

Zadavatel požaduje, aby všechny aktivní prvky (firewall, přepínače a bezdrátová infrastruktura) byly spravovatelné prostřednictvím jednotné management platformy jednoho výrobce.

Správa musí umožňovat:

- centrální konfiguraci zařízení,
- monitoring provozních stavů a výkonu,
- správu uživatelů a oprávnění (RBAC),
- vzdálený přístup ke konfiguraci,
- zálohování a obnovu konfigurací,
- evidenci událostí a logů.

3.2 Výkon a kapacita

Navržené řešení musí být dimenzováno s dostatečnou rezervou pro budoucí rozšíření a zvýšení počtu připojených zařízení.

Aktivní prvky musí splňovat:

- dostatečný switching výkon bez vzniku úzkých hrdel,
- dostatečnou kapacitu MAC adresních tabulek,
- dostatečnou velikost packet bufferu,
- podporu vysokorychlostních uplinků (min. 10 Gbit/s),
- schopnost obsluhy vysokého počtu současných klientů (zejména v případě WiFi).

3.3 Síťové funkce a segmentace

Řešení musí podporovat standardní síťové funkce nezbytné pro bezpečný, stabilní a efektivní **provoz školní infrastruktury**. Síťová segmentace je požadována jako důležité bezpečnostní opatření pro oddělení jednotlivých skupin uživatelů a zařízení, omezení nežádoucí komunikace a snížení rizika šíření bezpečnostních incidentů. Zároveň umožní lépe řídit přístupová oprávnění a uplatňovat rozdílné bezpečnostní politiky podle typu provozu a uživatelské role.

Řešení musí podporovat:

- VLAN (IEEE 802.1Q),
- řízení provozu mezi VLAN (inter-VLAN routing),
- QoS pro prioritizaci provozu,
- Link Aggregation (LACP),
- Spanning Tree (RSTP/MSTP),
- IGMP snooping.

Síť musí být logicky rozdělena minimálně na:

- administrativní síť,
- síť pedagogických pracovníků,
- síť žáků.

3.4 Bezpečnostní požadavky

Aktivní prvky musí podporovat pokročilé bezpečnostní mechanismy odpovídající provozu ve školním prostředí a požadavkům na ochranu interních systémů a uživatelských dat. Bezpečnostní funkce musí umožňovat prevenci neoprávněného přístupu, omezení šíření síťových incidentů a zvýšení celkové odolnosti infrastruktury.

Podpora pokročilých bezpečnostních mechanismů:

- řízení přístupu (ACL),
- DHCP snooping,
- ochranu proti ARP spoofingu (Dynamic ARP Inspection),
- ochranu proti neoprávněnému přístupu (např. port security, 802.1X nebo ekvivalent),
- ochranu proti síťovým smyčkám a broadcast stormům,
- oddělení managementu (management VLAN).

Přístup ke správě zařízení musí být zabezpečen a umožněn pouze prostřednictvím šifrovaných protokolů (HTTPS, SSH).

3.5 Standardy a kompatibilita

Všechna zařízení musí podporovat standardizované síťové protokoly a rozhraní pro zajištění interoperability a snadné správy infrastruktury. Řešení musí být navrženo tak, aby umožňovalo bezproblémovou integraci s běžnými nástroji pro monitoring, správu a dohled nad sítí.

Zadavatel požaduje:

- SNMP v3,
- SSH,
- HTTPS,
- Syslog (včetně možnosti šifrovaného přenosu),
- IPv4/IPv6 dual-stack.

3.6 Spolehlivost a dostupnost

Řešení musí být navrženo s důrazem na vysokou dostupnost a spolehlivost provozu. Součástí návrhu musí být opatření umožňující rychlou identifikaci poruchy, omezení jejího dopadu a obnovení plné funkčnosti infrastruktury.

Zadavatel požaduje:

- stabilní provoz bez výpadků,
- možnost rychlé obnovy konfigurace,
- minimalizaci dopadů poruch,
- možnost diagnostiky a vzdáleného řešení problémů.

4. Aktivní prvky - NEXTGEN firewall

Zadavatel uvádí, že v infrastruktuře školy je již provozován centrální bezpečnostní prvek typu Next-Generation firewall, který není předmětem dodávky v rámci této části veřejné zakázky. Firewall bude i nadále sloužit jako hlavní bezpečnostní prvek pro řízení komunikace mezi školní sítí, internetem a vybranými síťovými segmenty.

Dodavatel je povinen navrhnout, dodat a nakonfigurovat ostatní aktivní prvky tak, aby byly plně **provozně kompatibilní** se stávajícím **firewallem** zadavatele. Řešení musí umožnit napojení na stávající firewall, respektovat jeho síťové nastavení, VLAN segmentaci, bezpečnostní politiky, způsob routování, VPN služby a pravidla pro přístup k internetu.

Součástí plnění je koordinace konfigurace dodávaných aktivních prvků se stávajícím firewallem, zejména v oblasti VLAN, IP adresace, routingu, DHCP/DNS návazností, přístupových pravidel a případného logování. Dodavatel je povinen před zahájením konfigurace ověřit aktuální stav firewallu a projednat potřebné změny se zadavatelem nebo správcem IT infrastruktury.

Dodavatelem dodané aktivní prvky musí využívat standardní síťové protokoly a rozhraní a musí být plně interoperabilní se stávajícím firewallem zadavatele. Kompatibilita musí být zajištěna zejména v oblasti síťové komunikace, VLAN segmentace, routingu, QoS, autentizace a logování.

Použití **proprietárních nebo uzavřených řešení**, která by znemožňovala plnohodnotnou integraci se stávajícím firewallem nebo omezovala budoucí rozšiřitelnost infrastruktury, **není přípustné.**

Dodavatel nenese odpovědnost za technický stav, výkon ani licenční vybavení stávajícího firewallu, pokud tyto části nejsou předmětem jeho dodávky. Je však povinen zajistit, aby jím dodané aktivní prvky byly do stávající infrastruktury začleněny funkčním a bezpečným způsobem.

5. Aktivní prvky - Core switch

Zadavatel požaduje dodání centrálního přepínače (core switch), který bude tvořit hlavní agregační a směrovací prvek celé síťové infrastruktury. Core switch musí být plně integrován do jednotné platformy pro správu aktivních prvků a musí zajišťovat vysoký výkon, spolehlivost a bezpečnost.

Zadavatel požaduje dodání celkem **1 ks** core switche. Přesné členění a umístění je uvedeno ve slepém rozpočtu, který tvoří součást zadávací dokumentace. Dodávka musí zahrnovat veškeré licence, podporu a aktualizace firmware potřebné pro plnohodnotný provoz zařízení po dobu minimálně 36 měsíců od předání. **Záruka** na hardware musí být minimálně **36 měsíců.**

5.1 Hardwarové požadavky

Hardwarové provedení core switche musí odpovídat jeho **roli centrálního prvku** infrastruktury. Zařízení musí poskytovat dostatečný počet vysokorychlostních portů a flexibilitu pro připojení optických i metalických tras.

Minimálně požadavky:

- minimálně 10× SFP+ port (10 Gbit/s) pro optické propojení
- minimálně 2× 10GBase-T (RJ45) port pro metalické 10G připojení
- kombinace optických a metalických rozhraní
- instalace do 19" racku
- redundantní nebo zálohované napájení (výhodou)

Optické transceivery typu SFP+ musí být plně podporované výrobcem dodaných switchů a musí být dodány jako originální příslušenství daného výrobce. Použití OEM, neoriginálních nebo pouze deklarovaně kompatibilních modulů není přípustné.

5.2 Výkonové parametry

Core switch musí být dimenzován tak, aby zvládal provoz celé sítě bez vzniku úzkých hrdel. Požadované parametry musí zajistit plynulý provoz při plném zatížení a dostatečnou rezervu do budoucna.

Core switch musí splňovat:

- switching capacity min. 220 Gbps
- forwarding rate odpovídající plnému vytížení portů (line-rate switching)
- packet buffer min. 2 MB
- MAC address table min. 32 000 záznamů

5.3 L3 a síťové funkce

Core switch musí podporovat pokročilé síťové funkce nezbytné pro řízení provozu a segmentaci sítě. Tyto funkce zajistí efektivní směrování, prioritizaci a stabilní provoz celé infrastruktury.

Core switch musí podporovat:

- L3 routing (inter-VLAN routing)
- statické i dynamické routování (min. OSPF nebo ekvivalent)
- VLAN (802.1Q)
- QoS (prioritizace provozu)
- Link Aggregation (LACP)
- Spanning Tree (RSTP/MSTP)
- IGMP Snooping

5.4 Bezpečnostní funkce

Core switch musí podporovat bezpečnostní mechanismy pro ochranu vnitřní sítě a omezení neoprávněného přístupu. Požadované funkce musí přispívat ke zvýšení bezpečnosti a stability provozu.

Zařízení musí podporovat:

- ACL (IPv4 i IPv6)
- DHCP snooping
- Dynamic ARP Inspection
- IP Source Guard nebo ekvivalent
- ochranu proti smyčkám (loop protection, BPDU guard)
- oddělení managementu (management VLAN)

5.5 Správa a monitoring

Core switch zajišťuje efektivní správu, monitoring a diagnostiku provozu sítě. Správa je centralizovaná a umožňuje rychlou identifikaci a řešení provozních problémů.

Zařízení musí podporovat:

- centrální správu v rámci jednotné management platformy
- správu prostřednictvím webového rozhraní i CLI
- monitoring portů, provozu a klientů
- SNMP v3
- syslog (včetně šifrovaného přenosu)
- vzdálenou diagnostiku
- zálohování a obnovu konfigurace
- zero-touch provisioning

5.6 Redundance a rozšiřitelnost

Řešení zajišťuje vysokou dostupnost a budoucí rozšiřitelnost infrastruktury. Core switch podporuje mechanismy pro minimalizaci dopadů poruch a snadné rozšíření kapacity.

Zařízení musí umožňovat:

- stohování (stacking) nebo ekvivalentní technologii
- vysokou dostupnost (HA) nebo rychlou obnovu provozu
- budoucí rozšíření bez nutnosti výměny zařízení

5.7 Logická segmentace sítě

Core switch zajišťuje logické členění sítě s důrazem na bezpečnost a oddělení jednotlivých typů provozu. Segmentace musí zajistit přehledné řízení komunikace a omezení nežádoucích přístupů.

Síť musí být rozdělena minimálně na:

- administrativní síť
- síť pedagogických pracovníků
- síť žáků
- hostovskou síť

Komunikace mezi jednotlivými VLAN musí být řízena bezpečnostními politikami, a to buď na úrovni core switchů (ACL), nebo prostřednictvím firewallu.

6. Aktivní prvky - distribuční switche

Zadavatel požaduje dodání distribučních a přístupových přepínačů určených pro připojení koncových zařízení v jednotlivých částech budovy (učebny, kabinety, kanceláře a technologické prostory). Tyto přepínače musí být plně integrovány do **jednotné platformy** pro správu aktivních prvků a musí umožňovat centrální konfiguraci, monitoring a správu. Přesný počet požadovaných zařízení je uveden ve slepém rozpočtu, který tvoří součást zadávací dokumentace.

Zadavatel požaduje dodání celkem **5 ks** distribučních switchů. Přesné členění a umístění je uvedeno ve slepém rozpočtu, který tvoří součást zadávací dokumentace.

Dodávka musí zahrnovat veškeré licence, podporu a aktualizace firmware potřebné pro plnohodnotný provoz zařízení po dobu minimálně 36 měsíců od předání. **Záruka** na hardware musí být minimálně **36 měsíců.**

6.1 Hardwarové požadavky

Hardwarové provedení distribučních switchů musí odpovídat jejich nasazení v jednotlivých částech budovy. Zařízení musí poskytovat dostatečný počet portů, PoE kapacitu a uplink konektivitu pro spolehlivý provoz připojených zařízení.

Minimální požadavky na distribuční switche:

- minimálně **52× 10/100/1000Base-T portů** dle potřeby instalace
- podpora napájení PoE+ (IEEE 802.3af/at)
- minimální celkový PoE budget **min. 370 W**
- minimálně **4× SFP+ (10 Gbit/s)** uplink porty
- instalace do 19" racku
- aktivní chlazení (ventilátor) nebo ekvivalentní řešení

6.2 Výkonové požadavky

Distribuční switche musí být dimenzovány pro současné připojení většího počtu zařízení bez negativního dopadu na výkon. Požadované parametry musí zajistit plynulý provoz i při plném zatížení.

Switch musí splňovat:

- switching capacity odpovídající plnému využití portů (non-blocking switching)
- forwarding rate odpovídající line-rate provozu
- MAC address table min. **15 000 záznamů**

Zařízení musí být schopno obsluhovat vysoký počet současně připojených zařízení bez degradace výkonu.

6.3 Síťové funkce

Distribuční switche musí podporovat základní síťové funkce pro řízení provozu a segmentaci sítě. Tyto funkce musí zajistit stabilní a efektivní provoz připojených zařízení.

Switch musí podporovat minimálně:

- VLAN (IEEE 802.1Q)
- QoS (prioritizace provozu)
- Link Aggregation (LACP)
- Spanning Tree (RSTP)
- IGMP snooping

Výhodou je podpora základních L3 funkcí (např. statické routování).

6.4 Bezpečnostní funkce

Zařízení musí podporovat bezpečnostní mechanismy pro ochranu přístupové vrstvy sítě. Požadované funkce musí omezovat neoprávněný přístup a zvyšovat celkovou bezpečnost infrastruktury.

Switch musí podporovat:

- ACL (řízení přístupu)
- DHCP snooping
- ochranu proti ARP spoofingu (Dynamic ARP Inspection) nebo ekvivalent
- ochranu proti smyčkám (loop protection, BPDU guard)
- port security nebo ekvivalentní mechanismus

6.5 Správa a monitoring

Distribuční switche podporují centrální správu a monitoring v rámci celé infrastruktury. Správa musí být přehledná a umožňovat rychlou diagnostiku provozních problémů.

Zařízení musí podporovat:

- centrální správu v rámci jednotné management platformy
- správu prostřednictvím webového rozhraní
- monitoring portů a připojených zařízení
- SNMP v3
- syslog
- vzdálenou diagnostiku
- zálohování konfigurace

6.6 Napájení a PoE

Distribuční switche musí zajišťovat napájení připojených zařízení prostřednictvím technologie PoE v souladu se standardy minimálně IEEE 802.3af a IEEE 802.3at. PoE kapacita musí být dimenzována s ohledem na současné i budoucí požadavky provozu.

Switch musí být schopen napájet připojená zařízení, zejména:

- WiFi access pointy,
- IP telefony,
- kamery,
- další síťová zařízení.

PoE budget musí odpovídat požadavkům uvedeným v kapitole 6.1 a musí být navržen s dostatečnou rezervou pro současný i budoucí provoz.

6.7 Rozšiřitelnost

Síťové řešení umožní budoucí rozšiřování infrastruktury bez nutnosti zásadních změn. Distribuční switche musí podporovat propojení do vyšších vrstev sítě a integraci do centrální správy.

Zařízení musí umožňovat:

- propojení do vyšší topologie prostřednictvím 10G uplinků
- integraci do centrálně řízené infrastruktury
- budoucí rozšíření bez nutnosti výměny zařízení

7. WiFi infrastruktura

Zadavatel požaduje doplnění a rozšíření stávající bezdrátové infrastruktury na hlavní budově školy tak, aby bylo zajištěno plnohodnotné a kapacitně odpovídající pokrytí všech požadovaných prostor školní budovy, zejména učeben, kabinetů, chodeb a společných prostor.

Zadavatel uvádí, že ve škole jsou již v provozu bezdrátové přístupové body, které budou i nadále součástí výsledného řešení. Předmětem této části zakázky je proto zejména dodávka, instalace, konfigurace a zprovoznění dalších přístupových bodů za účelem rozšíření stávající WiFi infrastruktury.

Nově dodané přístupové body musí být navrženy tak, aby bylo možné zajistit **centrální správu**, konfiguraci a monitoring všech přístupových bodů (stávajících i nově dodaných) v rámci **jednotné management platformy** pro správu bezdrátové infrastruktury. Řešení musí zajistit **plnohodnotnou integraci** stávajících přístupových bodů **bez nutnosti jejich výměny**.

Není přípustné řešení, které by vedlo k oddělené správě více nezávislých WiFi infrastruktur.

Zadavatel požaduje dodání celkem **8 ks** WiFi access pointů. Přesné členění a umístění je uvedeno ve slepém rozpočtu, který tvoří součást zadávací dokumentace. Dodávka musí zahrnovat veškeré licence, podporu a aktualizace firmware potřebné pro plnohodnotný provoz zařízení po dobu minimálně 36 měsíců od předání. **Záruka** na hardware musí být minimálně **36 měsíců.**

7.1 Počet a rozmístění zařízení

Počet a rozmístění přístupových bodů musí zajistit plnohodnotné pokrytí všech prostor budovy a dostatečnou kapacitu pro připojená zařízení. Návrh musí zohledňovat charakter jednotlivých prostor a očekávané zatížení sítě.

Rozmístění přístupových bodů musí být navrženo dodavatelem tak, aby bylo zajištěno:

- dostatečné pokrytí signálem,
- dostatečná kapacita pro vysoký počet klientů,
- minimalizace rušení a překryvů.

Dodavatel je povinen provést návrh rozmístění přístupových bodů na základě odborného návrhu pokrytí (site survey), případně doložit výpočtem nebo měřením, že navržené řešení zajistí požadované pokrytí a kapacitu.

7.2 Technické požadavky na přístupové body

Přístupové body musí podporovat minimálně standard IEEE 802.11be (WiFi 7) a provoz v pásmech 2,4 GHz, 5 GHz a 6 GHz. Zařízení musí být určena pro provoz ve školním prostředí s vyšší hustotou klientů a podporovat centrální správu v rámci jednotné management platformy.

Přístupové body musí splňovat minimálně:

- podporu standardů IEEE 802.11ax a IEEE 802.11be,
- provoz v pásmech 2,4 GHz, 5 GHz a 6 GHz,
- podporu šířky kanálu 20/40/80 MHz, výhodou 160 MHz,
- podporu MIMO minimálně 2×2, výhodou 4×4 pro vybrané lokality,
- agregovanou bezdrátovou kapacitu odpovídající standardu WiFi 7,
- podporu napájení PoE+ (IEEE 802.3at),
- minimálně 1× 2,5 Gbit/s nebo vyšší uplink port,
- podporu centrální správy v rámci jednotné management platformy.

7.3 Kapacita a provoz

WiFi infrastruktura musí být navržena s ohledem na **vysoký počet** současně připojených zařízení a jejich typické využití ve školním prostředí. Řešení musí zajistit plynulý provoz bez významné degradace výkonu.

Každý přístupový bod musí být schopen **obsloužit minimálně:**

- 50 současně připojených klientů bez významné degradace výkonu

Návrh musí zohledňovat:

- vysokou hustotu zařízení
- využití online výukových aplikací

7.4 Pokročilé funkce

Přístupové body musí podporovat funkce zajišťující efektivní provoz bezdrátové sítě a kvalitní uživatelský komfort. Tyto funkce musí být plně funkční v rámci celé infrastruktury.

Přístupové body musí podporovat:

- band steering
- load balancing
- seamless roaming
- fast roaming (802.11r/k/v)

Tyto funkce musí být aktivně využitelné v rámci celé infrastruktury.

7.5 Bezpečnost a řízení přístupu

WiFi infrastruktura zajišťuje bezpečné řízení přístupu a oddělení jednotlivých skupin uživatelů. Řešení chrání interní systémy před neoprávněným přístupem a umožňuje kontrolu využívání síťových zdrojů. Důraz je kladen na oddělení provozu, autentizaci uživatelů a uplatnění odpovídajících bezpečnostních politik.

Zařízení musí podporovat:

- vytvoření více SSID pro různé uživatelské skupiny
- mapování SSID na VLAN
- zabezpečení pomocí WPA2-Enterprise a WPA3
- integraci s RADIUS serverem
- oddělení provozu jednotlivých skupin uživatelů

Minimálně musí být vytvořeny sítě pro:

- zaměstnance školy
- žáky

7.6 Správa a controller

WiFi infrastruktura musí být spravována centrálně prostřednictvím controlleru nebo ekvivalentního systému správy, který zajistí jednotnou konfiguraci, monitoring a správu celé sítě. Správa musí být přehledná a dostupná vzdáleně.

Řešení musí být plně kompatibilní se stávající bezdrátovou infrastrukturou zadavatele a musí umožňovat jednotnou správu všech přístupových bodů v rámci jedné management platformy. Zadavatel připouští cloudové, on-premise nebo hybridní řešení, pokud splňuje požadavek jednotné správy a plné integrace stávajících zařízení.

Požadována je zejména:

- centrální konfigurace všech AP,
- monitoring provozu a klientů,
- správa SSID a bezpečnostních politik,
- vzdálený přístup,
- aktualizace firmware.

Systém správy musí být součástí jednotné management platformy společné pro ostatní aktivní prvky.

8. Záložní zdroje

Zadavatel požaduje dodání a instalaci záložního napájecího systému (UPS) pro zajištění kontinuity provozu aktivních prvků síťové infrastruktury při výpadku elektrické energie. UPS systémy musí být navrženy s ohledem na rozdělení infrastruktury do hlavního a vedlejších rozvaděčů.

Zadavatel požaduje dodání celkem **3 ks** záložních zdrojů UPS. Přesné členění a umístění je uvedeno ve slepém rozpočtu, který tvoří součást zadávací dokumentace.

8.1 UPS pro hlavní rozvaděč

UPS pro hlavní rozvaděč musí zajistit nepřerušený provoz klíčových prvků síťové infrastruktury při výpadku napájení. Řešení musí umožňovat bezpečné překlenutí krátkodobých výpadků a řízené odstavení systémů při delším přerušení dodávky elektrické energie.

Pro hlavní síťový rozvaděč je požadována UPS splňující minimálně:

- výkon minimálně 3000 VA / 2700 W,
- provedení rackmount (19"),
- topologii minimálně line-interactive,
- vybavení síťovou management kartou (SNMP),
- podporu SNMP v3,
- možnost e-mailových notifikací,
- možnost integrace do centrálního monitoringu,
- podporu automatického bezpečného vypnutí připojených zařízení při výpadku napájení,
- záložní komunikační rozhraní (USB nebo sériové rozhraní).

UPS musí být schopna zajistit napájení následujících zařízení:

- firewall,
- core switch,
- distribučních switchů v hlavním racku,
- serveru,

a to po dobu minimálně 15 minut při plném zatížení.

Zařízení musí být vybaveno:

- displejem pro zobrazení provozních stavů
- funkcí automatického testování baterií
- signalizací poruch a nutnosti výměny baterií

Baterie musí mít minimální životnost 3 roky a musí být **vyměnitelné za provozu (hot-swap)**.

8.2 UPS pro vedlejší rozvaděče

UPS pro vedlejší rozvaděče musí zajistit základní zálohování napájení pro aktivní prvky umístěné mimo hlavní rozvaděč. Jejich úkolem je zejména překlenutí krátkodobých výpadků napájení a omezení dopadů poruch na provoz jednotlivých částí infrastruktury.

Pro vedlejší síťové rozvaděče zadavatel požaduje UPS splňující:

- výkon minimálně 1500 VA
- provedení rackmount nebo tower dle umístění
- topologie minimálně line-interactive
- podpora základního managementu (USB nebo sériové rozhraní)
- podpora signalizace stavu a základní diagnostiky

9. Požadavek na kompatibilitu

Dodané řešení musí být **plně kompatibilní se stávající IT infrastrukturou** zadavatele a musí umožňovat integraci s budoucími technologiemi a systémy. Veškeré aktivní prvky musí podporovat standardní síťové protokoly a rozhraní pro zajištění interoperability a omezení závislosti na proprietárních řešeních.

Síťová infrastruktura musí být navržena s důrazem na:

- dlouhodobou rozšiřitelnost,
- možnost implementace nových služeb,
- snadnou integraci dalších zařízení a systémů.

9.1 Správa a monitoring

Aktivní síťové prvky musí podporovat správu a monitoring prostřednictvím standardních protokolů a rozhraní, aby bylo možné zajistit jejich dlouhodobý dohled, správu a diagnostiku. Řešení musí být kompatibilní s běžnými nástroji pro síťový monitoring a správu.

Aktivní síťové prvky musí podporovat zejména:

- SNMP v3
- SSH
- HTTPS
- syslog (včetně možnosti šifrovaného přenosu)
- konfigurace všech zařízení musí být zálohovatelná a exportovatelná

9.2 Kompatibilita koncových zařízení

WiFi infrastruktura musí být kompatibilní se širokým spektrem klientských zařízení a musí podporovat i starší standardy pro zajištění zpětné kompatibility.

- notebooky
- tablety
- smartphony

Přístupové body musí podporovat i starší (legacy) standardy pro zajištění zpětné kompatibility.

9.3 Řízení přístupů

Centrální management musí umožňovat víceúrovňová oprávnění na principu RBAC (Role-Based Access Control), aby bylo možné oddělit jednotlivé role správy a omezit přístup jednotlivých administrátorů pouze na vymezenou část infrastruktury.