

***Projektová dokumentace***

***„Vybudování JCE IB SOŠ INFORMATIKY A SPOJŮ A SOU  
KOLÍN - zpracování projektové dokumentace“***

***TECHNOLOGICKÁ ČÁST JCE IB***

***D.1.4.9. Technologie a řešení JCE IB***

***D.1.4.9.02. BEZDRÁTOVÁ INFRASTRUKTURA (WLAN)***

**Zpracoval:**

Petr Lacina

## 2 BEZDRÁTOVÁ INFRASTRUKTURA (WLAN)

---

### 2.1 INSTALACE A KONFIGURACE BEZDRÁTOVÉ POČÍTAČOVÉ SÍŤE (WiFi)

Rozsah této části projektu spočívá ve vykrytí celé školy včetně domova mládeže bezdrátovým signálem, prostřednictvím bezdrátových přístupových bodů (AP) se zajištěním centrálního řízení této WiFi sítě. V rámci tohoto projektu dojde k instalaci AP splňující standard 802.11ax (WiFi 6).

Návrh technologie WLAN se skládá z vlastních přístupových bodů a centrálního systému (kontrolér), v redundantním režimu, pro řízení a konfigurování bezdrátové sítě.

Dodavatel provede instalaci AP včetně kabelážního systému do příslušných datových rozvaděčů v jednotlivých částech budovy, na základě projektu fyzické infrastruktury s rozmístěním jednotlivých přístupových bodů, který je nedílnou součástí tohoto projektu. Všechny kabelové trasy (datové TP trasy) budou poměřeny certifikovaným, měřicím přístrojem a bude vyhotoven měřicí protokol prokazující validitu tohoto kabelového propoje.

Dále bude provedena konfiguraci kontrolérů a AP včetně vytvoření 3 SSSID a jejich propagaci, pomocí VLAN, do LAN. Nedílnou součástí konfigurační práce je implementace segmentace prostřednictvím VLAN a protokolu 802.1x vycházející z bezpečnostních pravidel konfigurovaných v LAN (drátové poč. síti)

Dodávka, instalace a konfigurace řešení pro WiFi sestává z následujících částí:

- Přístupové body bezdrátové sítě – celkem 60 kusů
  - Etapa 1. – 44 kusů
  - Etapa 2. – 16 kusů
- Fyzický kontrolér – 2ks
  - oba kontroléry budou nainstalovány v etapě 1.

## 2.2 SPECIFIKACE MINIMÁLNÍCH POŽADAVKŮ TECHNICKÉHO ŘEŠENÍ

### 2.2.1 Přístupové body bezdrátové sítě (AP)

Požadovaná funkcionalita	Specifikace minimálních požadavků
Access Point určený pro instalaci na strop/podhled	PODPORUJE
Typ antén	Integrované pro obě pásma
Tři rádia pracující v režimu 2.4 + 5 + 6 GHz pro standardní prostředí	PODPORUJE
Samostatné rádio pro monitorování 2.4, 5 a 6 GHz RF spektra – detailní spektrální analýza, detekce útoků na bezdrátovou síť, lokalizace klientů	PODPORUJE
Podpora standardů 802.11a/b/g/n/ac/ax a Wi-Fi6E	PODPORUJE
Podpora minimálně 2x2 pro 2.4 GHz	PODPORUJE
Podpora minimálně 4x4 pro 5 a 6 GHz	PODPORUJE
Podpora MIMO, MU-MIMO, UL/DL OFDMA, TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax	PODPORUJE
Minimální počet inzerovaných SSID (BSSID) per radio	16
Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 n/ac/ax klientům (Tx Beam Forming)	PODPORUJE
Podpora mechanismu pro přepojení klientů z 2.4GHz do 5GHz pásma	PODPORUJE
Podpora mechanismu pro přepojení klientů z 2.4GHz a 5GHz do 6GHz pásma	PODPORUJE
Access Pointy obsahují X.509 certifikát s lokální platností pro nasazení PKI	PODPORUJE
Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x suplikant	PODPORUJE

Podpora detekce a monitorování problémů WLAN odchyťáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark)	PODPORUJE
Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí Telnet a SSH	PODPORUJE
Hardwarová podpora spektrální analýzy s podporou 160 MHz kanálů (detekce zdroje rušivého signálu – interference) pro 2.4, 5 a 6 GHz	PODPORUJE
Podpora rozpoznání zdroje rušivého signálu podle signatur 2.4, 5 a 6 GHz	PODPORUJE
Access Point obsahuje radio podporující BLE 5.1 a USB 2.0 port s podporou napájení minimálně 4.5W	PODPORUJE
Access Point podporuje kontejnerové prostředí pro běh aplikací	PODPORUJE
1 x 100/1000/2500 Mbit/s RJ45 ethernet rozhraní kompatibilní s 802.3bz	PODPORUJE
Možnost 802.3af/at/bt PoE napájení AP z přepínače nebo injectoru. Plná funkce obou rádií AP i při použití 802.3at, tj. 2x2 + 4x4 + 4x4 MIMO bez sníženého vysílacího výkonu	PODPORUJE
Možnost napájení z DC zdroje	PODPORUJE
AP uzavřené konstrukce bez větracích otvorů a ventilátoru	PODPORUJE
Součástí AP je plechový úchyt pro instalaci na strop nebo stěnu	PODPORUJE
AP je fyzicky zabezpečitelné/zamknutelné k okolním pevným částem.	PODPORUJE
Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanismy pro ochranu SW a HW proti útokům	PODPORUJE
SW a HW podpora po dobu minimálně 5 let	PODPORUJE

## 2.2.2 Centrální řídicí systém pro WiFi - kontrolér

Požadovaná funkcionalita	Specifikace minimálních požadavků
Požadovaný formát zařízení	Fyzické zařízení
Minimální počet Ethernet portů per kontroler.	2x 1/10G
Minimální propustnost pro data Gb/s	10 Gb/s
Licence dle počtu nově pořizovaných AP, možnost upgradu až na minimálně 250 registrovaných AP	PODPORUJE
Podpora stávajících AP řady 9115, které má Zadavatel nasazený ve své infrastruktuře, a nově pořizovaných AP	PODPORUJE
Minimální počet současně připojených klientů	5000
Redundance na úrovni kontrolerů a jejich portů, výpadek aktivního kontroleru v redundantním páru nemá žádný dopad na provoz již připojených klientů (tj. bez potřeby reautentizace)	PODPORUJE
Lokální síť - možnost tunelování uživatelských dat z AP až na kontroler, možnost šifrování těchto uživatelských dat bez výrazného vlivu na propustnost	PODPORUJE
Mesh síť - podpora mesh sítí, současné připojení normálních a mesh AP k jednomu kontroleru	PODPORUJE
Vzdálené lokality - možnost lokálního bridgování uživatelských dat per SSID přímo na příslušném AP	PODPORUJE
Šifrovaná řídicí komunikace AP-kontroler	PODPORUJE
Současná funkčnost AP pro přenos dat, analýzu spektra a detekci bezpečnostních incidentů	PODPORUJE
<b>Bezpečnost a Guest Access</b>	

Podpora 802.11i, respektive jeho implementace WPA2 včetně enterprise variant autentizace/šifrování	PODPORUJE
Podpora WPA3 – WPA3 Enterprise, WPA3 SAE, WPA3 OWE	PODPORUJE
PSK autentizace vč. možnosti různých PSK klíčů pro různé klienty v rámci jednoho SSID	PODPORUJE
Podpora standardu „802.11w“ pro ochranu řídicích rámců na AP a klientovi	PODPORUJE
Podpora standardu „802.11u“ pro výběr SSID a autentizaci klienta	PODPORUJE
Integrované řešení návštěvnického přístupu s možností webové autentizace (včetně nativních IPv6 klientů), bezpečné oddělení od zaměstnaneckého provozu, funkční i v módu lokálního bridgování uživatelských dat přímo na AP	PODPORUJE
Podpora řešení návštěvnického přístupu pro klienty bezdrátové i drátové sítě	PODPORUJE
Možnost omezit počet klientů per SSID	PODPORUJE
Lokální profilování zařízení – per uživatel a per zařízení	PODPORUJE
Integrovaný IDS systém pro detekci cizích AP (Rogue AP) a klientů v AdHoc režimu, možnost vynuceného odpojení klientů od cizích AP	PODPORUJE
Podpora Flexible NetFlow a exportu záznamů (dle RFC 3954) o datových tocích uživatelů (vč. zdrojové a cílové IP adresy, portů, WLAN ID, počtu paketů a objemu přenesených dat) směrem k externímu kolektoru	PODPORUJE
Podpora pro analýzu šifrovaného provozu	PODPORUJE
Podpora integrace pro ochranu protokolu DNS	PODPORUJE
<b>Rychlý roaming</b>	
Podpora standardu „802.11r“ pro rychlý roaming klientů mezi AP, možnost selektivního	PODPORUJE

využití 802.11r na sdíleném SSID pouze pro zařízení, které tento standard podporují	
Podpora standardu „802.11k“ pro optimalizaci roamingu	PODPORUJE
Podpora standardu „802.11v“ pro optimalizaci připojení klienta	PODPORUJE
<b>QoS a řízení provozu v bezdrátové síti</b>	
Podpora 802.11e/WMM	PODPORUJE
Diferenciace úrovní QoS pro různé služby a skupiny uživatelů (zaměstnance a návštěvníky), možnost obousměrného omezení propustnosti per klient.	PODPORUJE
Mechanismy řízení přístupu (Call Admission Control) pro hasový i video provoz. Konfigurovatelné parametry max. zátěže a šířky pásma.	PODPORUJE
Podpora Video-streamingu se spolehlivým multicastem	PODPORUJE
Optimalizace multicast provozu v bezdrátové síti (IGMP snooping)	PODPORUJE
Aplikační inspekce přenášeného provozu (DPI na 7. vrstvě ISO/OSI na základě aplikačních signatur) umožňující rozpoznání jednotlivých aplikací, grafické zobrazení statistik a možnost řízení QoS per rozpoznaná aplikace	PODPORUJE
<b>Správa frekvenčního pásma, konfigurační profily</b>	
Automatizovaná centrální správa frekvenčního pásma	PODPORUJE
Monitoring rádiového spektra vč. 20/40/80/160 MHz kanálů, možnost okamžité automatické centralizovaně řízené reakce (změna kanálu nebo jeho šířky, změna vysílacího výkonu), grafické vyobrazení informací o kvalitě signálu	PODPORUJE
Automatické zvýšení vysílacího výkonu okolních AP při výpadku AP („self healing“)	PODPORUJE

Automatické přepínání rádií mezi 2,4 a 5 Ghz jednotlivých AP	PODPORUJE
Možnost detekce rušivých signálů (interference) a identifikace zdrojů interference na základě signatur	PODPORUJE
Mesh síť – automatický výběr vhodného kanálu pro backhaul, automatické sestavení optimálního mesh stromu, monitorování všech kanálů na pozadí s rychlou konvergencí v případě výpadku primárního nadřazeného AP	PODPORUJE
Troubleshooting radiového signálu a automatické řešení problému rušivého signálu, generování alarmů na základě překročení prahových hodnot kvality signálu	PODPORUJE
Možnost definovat různé konfigurační profily a ty následně přiřadit vybraným AP (např. dle umístění AP, bezpečnostních pravidel atd.).	PODPORUJE
Možnost vytvořit různé rádiové profily (nastavení kanálů, rychlostí) a ty následně přiřadit vybraným AP.	PODPORUJE
<b>Podpora IPv6</b>	
Podpora IPv6 – management kontroleru (vč. Syslog, radius)	PODPORUJE
Podpora IPv6 – komunikace AP-kontroler	PODPORUJE
Podpora IPv6 – Guest Access i pro nativní klienty vč. webové autentizace pro IPv6 klienty	PODPORUJE
Podpora IPv6 – IPv6 multicast, MLD snooping	PODPORUJE
Podpora IPv6 – bezpečnost (RA Guard, IPv6 Source Guard, DHCPv6 Server Guard, ACL)	PODPORUJE
Podpora IPv6 – ND cache na kontroleru, optimalizace přenosu ND zpráv, rate-limiting pro RA	PODPORUJE
<b>Dohled a správa kontroleru, zabezpečení HW/SW</b>	
Centrální administrace správců s granularitou přístupových práv	PODPORUJE



Podpora správy přes serial CLI nebo přes IP pomocí SSH/telnet a https web GUI, SNMP	PODPORUJE
RJ45 konzolový port a/nebo USB konzolový port, dedikovaný ethernetový RJ45 management port	PODPORUJE
Podpora API rozhraní pro plnou konfiguraci kontroleru pomocí NETCONF, RESTCONF za použití YANG data modelů. Podpora exportu provozních dat z kontroleru.	PODPORUJE
Možnosti využití vestavěného Python API pro automatizovanou správu	PODPORUJE
Důvěryhodný HW/SW – kontroler používá bezpečný zavaděč OS, ověřování podpisu SW komponent, kontrolu autentičnosti HW a mechanismy pro ochranu SW a HW proti útokům	PODPORUJE
Možnost rozšíření o lokalizační a analytické služby připojených klientů	PODPORUJE
SW a HW podpora po dobu minimálně 5 let	PODPORUJE