Modernizace síťové infrastruktury Matiční gymnázium Ostrava, příspěvková organizace

1. Cíle projektu

Tento dokument je studie zpracovaná jako podklad pro zadání veřejné zakázky, nikoli realizační projektová dokumentace. Uvedené počty, rozmístění prvků a parametry představují návrh a minimální požadavky zadavatele; konkrétní řešení a konfigurace budou upřesněny během realizace.

Studie se zabývá návrhem modernizace a výstavby aktivní části síťové infrastruktury, která navazuje na komplexní modernizaci strukturované kabeláže v objektech Matičního gymnázia v Ostravě. Cílem je zajistit dostatečně výkonnou datovou síť pro výuku, administrativu a další provoz školy. Nově navržené komponenty sítě budou pokrývat jak pevná připojení v učebnách a kancelářích, tak bezdrátovou konektivitu ve všech prostorách školy. Hlavním důvodem projektu je zvýšený požadavek na digitální infrastrukturu školy, který souvisí se změnami ve výuce, nárůstem počtu zařízení, hybridní výukou, provozem informačních systémů, online testováním a obecně potřebou vysoké dostupnosti a stability připojení pro pedagogy, studenty i hosty.

Síťová infrastruktura bude navržena s ohledem na oddělení provozu různých skupin uživatelů, centrální správu, bezpečnostní pravidla a zálohované napájení. Důraz bude kladen na využití prověřených a spolehlivých síťových technologií, škálovatelnost a dlouhodobou udržitelnost.

Cíle projektu jsou následující:

- Vybudování jednotné a spravovatelné školní LAN a Wi-Fi infrastruktury.
- Pokrytí celé budovy bezdrátovou sítí Wi-Fi 6 pomocí centrálně řízených access pointů.
- Nasazení centrálního firewallu s funkcemi směrování, filtrování a segmentace provozu.
- Integrace služby eduroam s ověřením uživatelů přes stávající školní doménu (Active Directory) a RADIUS.

2. Stávající stav

Stávající síťová infrastruktura v objektu je nevyhovující a nesplňuje požadavky na spolehlivý a centralizovaně řízený provoz. Pokrytí bezdrátovým signálem Wi-Fi je nedostatečné a nerovnoměrné, což způsobuje výpadky připojení a snižuje komfort uživatelů. V jednotlivých částech budovy jsou nasazeny směrovače a přístupové body různých výrobců, bez jednotného systému správy a bez možnosti centrální konfigurace nebo dohledu.

Síť není připravena na připojení Eduroam, která je standardem ve školském a akademickém prostředí. Chybí potřebné prvky jako je správné oddělení VLAN, podpora RADIUS autentizace, a bezpečné řízení přístupových práv. Celkově je infrastruktura roztříštěná a neumožňuje efektivní správu, škálování ani zajištění dostatečné úrovně bezpečnosti.

3. Návrh řešení

Navrhované řešení spočívá v nahrazení stávajících nevyhovujících síťových prvků jednotným systémem správy aktivních zařízení. Stávající směrovače a přístupové body různých značek budou demontovány a nahrazeny centralizovaně řízeným systémem složeným z kompatibilních přístupových bodů (AP), switchů a řídicího kontroléru (WLC).

Přístupové body budou rozmístěny s ohledem na pokrytí všech prostor budovy stabilním Wi-Fi signálem, včetně přetížených nebo problematických míst. Celý systém bude spravován z jednoho rozhraní, což umožní vzdálený dohled, aktualizace firmware, přidělování VLAN a centralizovanou autentizaci.

Síť bude zároveň připravena pro nasazení eduroam, včetně podpory 802.1X autentizace pomocí externího RADIUS serveru a integrace s adresářovou službou (např. Microsoft Active Directory). Navržené řešení výrazně zvýší bezpečnost, stabilitu a správu sítě, a současně zajistí připravenost pro budoucí rozšiřování.

Realizace je rozdělena do etap. V první etapě se osazují budovy A a B s celkem 50 přístupovými body a kompletní páteřní, agregační a napájecí infrastrukturou. Aktivní prvky (přepínače, agregační switch, kontrolér) a napájení jsou dimenzovány na cílový stav cca 80 AP, aby druhá etapa (budova C a doplnění pokrytí, plánovaná na následující rok) znamenala pouze doplnění přístupových bodů a jejich licencí bez zásahu do páteřní infrastruktury. Pokrytí v první etapě odpovídá 50 AP; plné pokrytí dle původního návrhu se doplní ve druhé etapě.

Poznámka: V této první fázi (etapě) se neosazuje budova C (rozvaděč DR3). Budova C je součástí druhé etapy plánované na následující rok.

3.1.Datové rozvaděče

V rámci rekonstrukce školní sítě budou v budově využity čtyři datové rozvaděče, označené jako DR1 až DR4. Každý rozvaděč bude vybaven aktivními síťovými prvky dle umístění a požadavků na konektivitu v dané části budovy. Rozvaděče budou mezi sebou propojeny pomocí páteřních optických tras 10 Gbit/s do centrálního agregačního switche, který bude umístěn v rozvaděči DR2 společně se serverem, úložištěm NAS a perimetrickým firewallem. Toto uspořádání odpovídá skutečnému těžišti datového provozu a odstraňuje závislost celé sítě na jediném přístupovém přepínači.

3.1.1.DR1 – místnost č.04

V datovém rozvaděči bude instalován 48portový PoE+ switch (PoE budget min. 740 W) pro připojení Wi-Fi AP připojených z tohoto DR. Pro potřeby účastnických zásuvek v kancelářích 2.NP a třídách připojených z DR1 budou dále instalovány dva 48portové switche dle specifikace. Všechny switche v DR1 budou do centrálního agregačního switche v DR2 napojeny páteřní optickou trasou 10 Gbit/s (SFP+). Zálohované napájení (UPS) je centralizováno v rozvaděči DR2; při delším výpadku napájení nejsou aktivní prvky v DR1 zálohovány.

3.1.2.DR2 – serverovna UPS

DR2 je centrálním agregačním uzlem sítě. Bude v něm instalován agregační switch s porty 10 Gbit/s (SFP+ i metalické), do kterého se sbíhají páteřní optické trasy z DR1, DR3 a DR4 a uplinky přístupových switchů v DR2. Agregační switch zajišťuje L3 směrování mezi VLAN běžného provozu; perimetrický firewall řeší přechod do internetu a pravidla mezi bezpečnostními zónami. Dále bude v DR2 instalován 48portový PoE+ switch (PoE budget min. 740 W) pro připojení Wi-Fi AP z tohoto DR a dva 48portové switche pro účastnické zásuvky budovy B dle specifikace. V tomto rozvaděči je ukončena stávající optická konektivita poskytovatele. Stávající virtualizační server je technicky vyhovující, bude doplněn o rozšíření paměti RAM, dvouportovou 10Gb síťovou kartu a provozní HDD. Nově bude instalováno úložiště NAS 4×8 TB dle specifikace. Rozvaděč bude vybaven UPS o výkonu minimálně 2200 VA pro zálohování instalovaných zařízení.

3.1.3.DR3 – místnost č. 1.15

Rozvaděč DR3 obsluhuje budovu C, která je součástí druhé etapy. V první etapě se DR3 neosazuje aktivními prvky; budova C bude řešena v následujícím roce (viz kapitola Návrh řešení). Připravená optická trasa 10 Gbit/s (SFP+) do DR2 zůstává pro budoucí napojení.

3.1.4.DR4 – místnost č. 308

V datovém rozvaděči bude instalován 48portový switch pro připojení stávajících PC v učebně. Konektivita do jádra v DR2 bude provedena páteřní optickou trasou 10 Gbit/s (SFP+).

4. Technická specifikace

Dodavatel je povinen dodat zařízení s níže uvedenými minimálními technickými parametry. Jsou přípustná i zařízení s vyššími parametry, pokud splňují plnou kompatibilitu a funkcionalitu v rámci navrženého řešení.

4.1. Přístupové body Wi-Fi AP

- Provedení: vnitřní, stropní nebo nástěnná montáž
- Standardy: IEEE 802.11a/b/g/n/ac/ax (Wi-Fi 6)
- Frekvenční pásma: 2,4 GHz a 5 GHz (dual-band)
- Minimální počet streamů: 2x2 MIMO v každém pásmu
- Agregovaná datová propustnost: min. 1,2 Gbps
- Podpora: 802.3af/at (PoE), WPA3, VLAN, 802.1X
- Centrální správa: podpora ovládání přes bezdrátový kontrolér (WLC) nebo cloudový management
- Minimálně 1x 1 Gbps ethernet port (uplink)
- Podpora roamingu, mesh sítí a aplikační vrstvy řízení
- Včetně montážního příslušenství

4.2.Agregační switch

- Porty: min. 12x 10 Gbit/s SFP+; alespoň 4 porty kombo (SFP+/10GBASE-T) pro připojení serveru, NAS a firewallu metalicky
- Kapacita: neblokující propustnost pro všechny porty současně, min. 240 Gbit/s
- Vrstva: plně řízený L2/L3 switch – statické směrování a směrování mezi VLAN (inter-VLAN routing), SVI
- Funkce: VLAN 802.1Q, QoS, STP/RSTP/MSTP, LACP, LLDP, IGMP snooping, SNMPv3, syslog
- Bezpečnost: ACL, DHCP snooping, Dynamic ARP Inspection, 802.1X
- Vysoká dostupnost: podpora stohování nebo redundantních uplinků; napájení s možností zálohy
- Montáž: 19" rack, včetně příslušenství
- Umístění: rozvaděč DR2

4.3. Switche 48 portů PoE+

- Porty: min. 48x 10/100/1000 Mbps RJ-45 + 4x SFP/SFP+ uplink
- PoE standard: min. IEEE 802.3at (PoE+), celkový PoE budget min. 740 W
- Správa: plně řízený switch (L2/L3), podpora VLAN, QoS, STP, LLDP, SNMPv3
- Bezpečnost: podpora ACL, DHCP snooping, 802.1X autentizace

- Redundance: podpora LACP, možnost záložního napájení (RPS nebo interní redundance)
- Montáž: 19" rack, včetně úchytů
- Ventilace: tichý provoz nebo inteligentní řízení otáček ventilátoru

4.4. Switche 48 portů

- Porty: min. 48x 10/100/1000 Mbps RJ-45 + 2x SFP
- PoE: není požadováno
- Správa: plně řízený switch, s VLAN, QoS, SNMP
- Montáž: 19" rack, včetně příslušenství

4.5.Moduly SFP+ 10 Gbps

- Typ: optický transceiver modul pro singlemode duplexní komunikaci
- Přenosová rychlost min. 10Gbps (SFP+)
- Typ přenosu: Dvouvláknový Full-duplex
- Typ konektoru: LC duplex
- Dosah min. 1 km
- Kompatibilní s nasazenými přepínači (MSA, plná funkčnost bez omezení); u aktivních prvků se nepřipouští typové vázání na jednoho výrobce

DAC kabely 10 Gbps (twinax)

- Typ: pasivní přímé propojení SFP+ na SFP+ (Direct Attach Copper, twinax)
- Přenosová rychlost: 10 Gbps, délka 1 m (propoje uvnitř rozvaděče DR2)
- Kompatibilita: plná kompatibilita s dodávanými přepínači na SFP+ portech; bez typového vázání na jednoho výrobce

4.6. Server doplnění

4.6.1.Modul paměti ECC Registered DDR4, 16 GB, 2933 MHz, pro server

- Typ: ECC Registered (RDIMM)
- Kapacita modulu: 16 GB
- Frekvence: 2933 MHz
- Kompatibilita: odpovídající serverovému slotu, podporuje interleaving / vícekanálový provoz
- Rozložení ranků (1Rx8 / 2Rx8) podle stávajících modulů
- Možnost výměny při běhu (pokud server podporuje hot-swap)

4.6.2.Síťová karta 10 Gb/s, dvouportová, RJ-45 / SFP+, PCIe, pro server

- Typ: duální 10 Gb/s síťový adaptér
- Rozhraní: PCI Express (např. x8 nebo x16)
- Porty: 2 × 10G (RJ-45 nebo SFP+)
- Podpora IEEE standardů: 10GBASE-T nebo SFP+ 10G
- Podpora offload funkcí: TCP offload (TOE), Large Send Offload (LSO), Jumbo Frames
- Kompatibilita s operačním systémem serveru
- Podpora pro bonding / teaming / LACP
- Výrobce konfigurace: možnost řízené správy portů / diagnostiky
- Kompatibilita s ovladači stávajícího operačního systému a serverového firmwaru

4.6.3. Pevný disk 2 TB, SATA, 2.5", hot-plug, pro server

- Typ disku: (HDD) určený pro non-critical serverové nasazení (archiv, zálohy, datové úložiště)
- Kapacita: 2 TB
- SATA III 6 Gb/s
- 2.5" SFF (Small Form Factor)
- Hot-plug kompatibilní
- Kompatibilita se stávajícím serverem a řadičem
- Možnost zařazení do RAID polí 0, 1, 5, 6, 10 apod.
- Doporučeno pro prostředí s nižší zátěží na IOPS – např. zálohování, sekundární uložiště, přístup k logům apod.

4.7.Wireless LAN Controller

- Licencování: možnost správy min. 80 přístupových bodů
- Provedení: fyzické zařízení, virtualizovaná instance nebo cloudová platforma výrobce – dle možností nabízené platformy
- Funkce: centralizovaná správa Wi-Fi sítě, dynamická alokace kanálů, roaming, přidělení SSID a VLAN, monitoring
- Podpora protokolu RADIUS (eduroam)
- Šifrování: WPA2, WPA3 Enterprise
- Monitoring: webové rozhraní, SNMP, syslog
- Aktualizace: možnost centrální aktualizace firmware AP

4.8. NAS úložiště

- Počet disků: min. 4 pozice, osazeno 4× HDD 8 TB
- Funkce: RAID1 nebo RAID5, SMB/NFS, zálohování, přístupové role
- Podpora: Active Directory integrace, snapshoty, vzdálený přístup
- Připojení: min. 2× 1 Gbps RJ-45 (10 GbE výhodou vzhledem k 10G páteři v DR2), podpora agregace
- Montáž: 19" rack, včetně příslušenství

4.9. Perimetrický firewall

Referenční výrobek: Fortinet FortiGate FG-90G včetně bezpečnostního předplatného Unified Threat Protection (UTP) na 60 měsíců, nebo rovnocenné řešení splňující níže uvedené parametry. Uvedení referenčního výrobku slouží pouze k upřesnění požadované úrovně a funkčnosti; uchazeč může nabídnout jakékoli rovnocenné řešení.

- Typ: hardware firewall
- Průchodnost firewallu (Firewall throughput): min. 1 Gbps (NGFW), min. 500 Mbps při zapnutém DPI (Deep Packet Inspection)
- VPN: podpora min. 100 současných VPN tunelů (IPSec, SSL), možnost připojení k eduVPN
- Připojení: min. 5x RJ-45 1 Gbps port (WAN, LAN, DMZ, HA apod.), SFP port výhodou
- Montáž: včetně příslušenství pro montáž do 19" rozvaděče (rack mount tray/vana)
- Bezpečnost: Stateful Inspection, DoS ochrana, GeoIP filtr, aplikační kontrola (Layer 7), IDS/IPS. Bezpečnostní předplatné (bundle) na dobu min. 5 let (60 měsíců) zahrnující: IPS, ochranu proti malware (Advanced Malware Protection), aplikační kontrolu, filtrování

URL/DNS/videa, antispam a odpovídající úroveň výrobní podpory (výměna vadného HW, přístup k aktualizacím)
- Správa: webové GUI, CLI, podpora SNMP, možnost zálohy konfigurace
- Autentizace: podpora RADIUS, LDAP, MS Active Directory
- Segmentace: podpora VLAN, interních zón, směrování mezi sítěmi
- Provozní režimy: NAT, transparentní bridge, routing
- Další požadavky: možnost vytvoření pravidel pro eduroam, přístupovou politiku pro hosty, logování událostí
- Montáž: 19" rack, včetně příslušenství

4.10. UPS 2200 VA / 1980 W, line-interactive, 2U rack, čistý sinus, síťový monitoring

- Záložní napájecí zdroj line-interactive s výstupním výkonem minimálně 2200 VA / 1980W
- Konstrukce rack/tower, vhodná pro montáž do 19"
- Čistý sinusový výstup
- Integrovaný AVR
- LCD displej s informacemi o napětí, zátěži, stavu baterie a provozních parametrech
- Komunikační rozhraní USB a možnost síťového SNMP monitoringu
- Výměnné baterie a modulární konstrukce
- Minimálně 6 výstupních zásuvek IEC C13, některé s možností řízení
- Možnost řízeného vypnutí systémů a provozu skrze přibalený SW nebo SNMP

4.11. Licence, podpora a provozní požadavky

Bezpečnostní funkce firewallu a správa Wi-Fi vyžadují softwarové licence a předplatné, která jsou nedílnou součástí dodávky. Přístupové a agregační přepínače jsou navrženy jako řešení bez licenčních poplatků (bezlicenční řada), aby se snížily provozní náklady školy. Uchazeč je ocení jako samostatné položky s uvedením doby platnosti. Není přípustné dodat hardware bez licencí nutných k požadované funkčnosti.

- Wi-Fi kontrolér zajišťuje centrální správu přístupových bodů. Provedení může být fyzické (samostatné zařízení), virtuální (instance na virtualizační platformě objednatele) nebo cloudové – dle nabídky uchazeče a možností nabízené platformy. Virtuální provedení je podmíněno dostupnou virtualizační platformou a volnou kapacitou na serveru objednatele; jinak uchazeč navrhne fyzické nebo cloudové řešení. Nasazení kontroléru je součástí dodávky. Kapacita min. 80 AP (cílový stav po dobudování). V první etapě se osazuje 50 AP; do 50 AP se předpokládá provoz kontroléru bez závislosti na registraci u výrobce (dle zvoleného řešení). Při rozšíření nad 50 AP (2. etapa) může být podle zvoleného řešení nutná registrace licencí/účtu objednatele u výrobce – s tím je třeba počítat. Řešení nesmí být pro základní provoz Wi-Fi závislé na trvalém připojení k internetu ani na platnosti cloudové služby
- Licence a předplatné AP: pro každý přístupový bod veškeré licence a předplatné nutné k plné funkčnosti (centrální správa, 802.1X/RADIUS, eduroam) po dobu min. 5 let. Konkrétní skladba licencí je věcí uchazeče dle nabízené platformy; u řešení bez licenčních poplatků je požadavek splněn dodávkou bez dalších nákladů

- Perimetrický firewall: bezpečnostní předplatné (IPS/IDS, antivirus, kontrola aplikací L7, filtrování obsahu) po dobu min. 5 let – bez něj nelze naplnit požadavky čl. Perimetrický firewall
- Certifikát: pro RADIUS/EAP se požaduje serverový certifikát důvěryhodné veřejné certifikační autority; obnova po dobu životnosti řešení
- Veškeré licence a účty pro správu (např. výrobcem vyžadované licenční či cloudové účty) registrovány na objednatele; dodavatel může mít delegovaný přístup pro správu

4.12. Připojení do eduroam a logování

Škola není členem české eduroam federace. Připojení k federaci je administrativní úkon objednatele vůči sdružení CESNET a musí probíhat souběžně s realizací. Realm uživatelů bude odvozen od stávající domény školy.

- Autentizace 802.1X přes RADIUS s napojením na stávající doménu (Active Directory)
- Pro snadné nastavení klientských zařízení se nasadí nástroj eduroam CAT / geteduroam
- Provoz eduroam vyžaduje uchovávání provozních údajů (čas autentizací, přidělení IP/MAC) po dobu min. 6 a max. 12 měsíců; řešení zajistí úložiště logů (RADIUS, DHCP, kontrolér) s automatickou rotací a mazáním po uplynutí lhůty
- Úložiště logů bude dimenzováno na uvedenou dobu retence (lze využít NAS v DR2)

4.13. Segmentace a směrování

Síť bude rozdělena do VLAN dle skupin uživatelů (např. administrativa, pedagogové, studenti, hosté, kamerový systém, správa aktivních prvků). Směrování běžného provozu mezi VLAN zajišťuje agregační switch hardwarově; perimetrický firewall řeší přechod do internetu a pravidla mezi citlivými zónami. Součástí dodávky je adresní plán, tabulka VLAN s rozsahy a branami a matice povolené komunikace, předané v provozní dokumentaci.

5. Závěr

Tato dokumentace je vypracována POUZE ve stupni studie a nejedná se o realizační projektovou dokumentaci. Slouží jako podklad pro zadání veřejné zakázky. Případný dodavatel je povinen respektovat veškeré právní předpisy České republiky, stejně jako vyhlášky a normy související s předmětem této PD. Dokumentace odpovídá stavu na objektech v době provádění PD, změny, které budou provedeny po odevzdání dokumentace již nemohou být její součástí a PD tyto změny s dopady do navrženého řešení postihnout.

Tato studie slouží jako podklad pro zadání veřejné zakázky. Uvedené rozmístění aktivních prvků, počty portů a konkrétní konfigurace (VLAN, směrování, pravidla firewallu, nastavení kontroléru) jsou návrhové a budou upřesněny a odsouhlaseny s objednatelem během realizace podle skutečného stavu na objektech a podle nabídnutého řešení uchazeče.