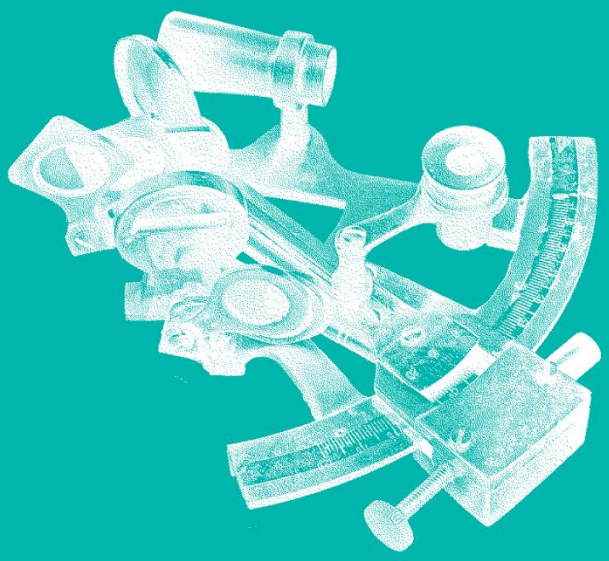
Zajištění konektivity do škol - projektová dokumentace – aktivní prvky

Střední průmyslová škola Hronov



ALEF NULA, a.s., U Plynárny 1002/97, 101 00 Praha 10, Česká republika
Obchodní rejstřík u Městského soudu v Praze, oddíl B, vložka 2727
Tel +420 225 090 111 • **Fax** +420 225 090 112 • cz-recepce@alef.com
IČO 61858579 • **DIČ** CZ61858579

Obsah

Úvod

Projektová dokumentace je zpracována pro SPŠ Hronov, sídlící na adrese Hostovského 910, Hronov. Projekt se týká budovy Hostovského 910, Hronov a budovy Vrchlického 538, Hronov. Cílem je ověřit a vydefinovat, jak je splněno zadávání výzvy č. 32/33 v oblasti Standardu konektivity škol.

Zpracování proběhlo v souladu s vyhláškou č. 499/2006 Sb., o dokumentaci staveb, v platném znění. Součástí díla je:

A. Průvodní zpráva
B. Souhrnná technická zpráva
C. Situační výkresy
D. Dokumentace objektů a technických a technologických zařízení
E. Dokladová část

Věcné a časové vazby:

- Práce budou zahájeny až po schválení projektové dokumentace majitelem objektu.
- V průběhu prací budou dodrženy podmínky stanovené majitelem.
- Práce budou zahájeny po výběru dodavatele stavby investorem stavby

A. Průvodní zpráva

A.1 Identifikační údaje

A.1.1 Údaje o stavbě

Název objektu: **Střední průmyslová škola Hronov**
Dotčené objekty:

- objekt Hostovského – Hostovského 910, Hronov, katastrální území Hronov, parcelní číslo 363
- objekt Vrchlického – Vrchlického 538, Hronov, katastrální území Hronov, parcelní číslo 148

A.1.2 Údaje o stavebníkovi

Královehradecký kraj, IČ 708 89 546, Pivovarské náměstí 1245, 500 03 Hradec Králové

A.1.3 Údaje o zpracovateli projektové dokumentace

Zpracovatel: **ALEF NULA, a.s., IČ 61858579, U Plynárny 1002/97, 101 00 Praha 10**
Hlavní projektant: Ing. Kosta Prandžev, evidenční číslo 36956, autorizovaný inženýr v oboru technologická zařízení staveb a evidenční číslo 36957, autorizovaný technik v oboru technika prostředí staveb, specializace elektrotechnická zařízení

A.2 Seznam vstupních podkladů

Projektová dokumentace vznikla na základě těchto podkladů:

- Informace o současném stavu
- Technická specifikace aktivních i pasivních prvků
- Půdorysné plány budov

A.3 Údaje o území

Objekt	Katastrální území
Objekt Hostovského – Hostovského 910, Hronov	katastrální území Hronov, parcelní číslo 363
Objekt Vrchlického – Vrchlického 538	katastrální území Hronov, parcelní číslo 148

B. Souhrnná technická zpráva

Technická zpráva popisuje projekt „Standard konektivity škol“, dle výzvy č. 33.

B.1 Výchozí stav

Ve škole je aktuálně 300 žáků a 100 počítačů. Konektivita pro celou školu je 25 Mbit/s pro příchozí a 5 Mbit/s pro odchozí směr internetového provozu bez agregace a bez FUP. Poskytovatelem internetového připojení je N-SYS s.r.o. Přidělené IP adresy jsou v současné době pouze IPv4.

Ve škole se využívá centrální databáze identit Microsoft Active Directory pro přístup žáků a zaměstnanců do školních systémů.

Na perimetru sítě je umístěn Mikrotik router, lokální síť je tvořena přepínači Cisco SG300. Bezdrátová síť je realizována na přístupových bodech Mikrotik.

B.2 Nedostatky infrastruktury dle výzvy č. 33

Dle výše popsaného výchozího stavu je třeba navýšit přenosovou rychlost internetového připojení. Dle výzvy je třeba zajistit přenosovou rychlost odpovídající 128 kbit/s pro každého žáka. Z celkového počtu žáků 300 je potřeba zajistit internetové připojení alespoň 39 Mbit/s pro oba směry provozu.

V aktuální řešení chybí implementace RADIUS serveru, který je třeba nasadit pro bezpečný přístup žáků do lokální sítě. Zároveň provést konfiguraci a integraci do systému Eduroam pro mobilitu žáku a učitelů.

Největší problémy jsou s nedostatečnou výpočetní kapacitou serverů, chybějícím propojením budov Hostovského a Vrchlického.

Poskytovatel internetového připojení přiděluje pouze IPv4 adresy, ale nebude problém s rozšířením o IPv6 adresy.

B.3 Technické řešení projektu

Níže je v jednotlivých částech popsán technický návrh řešení projektu.

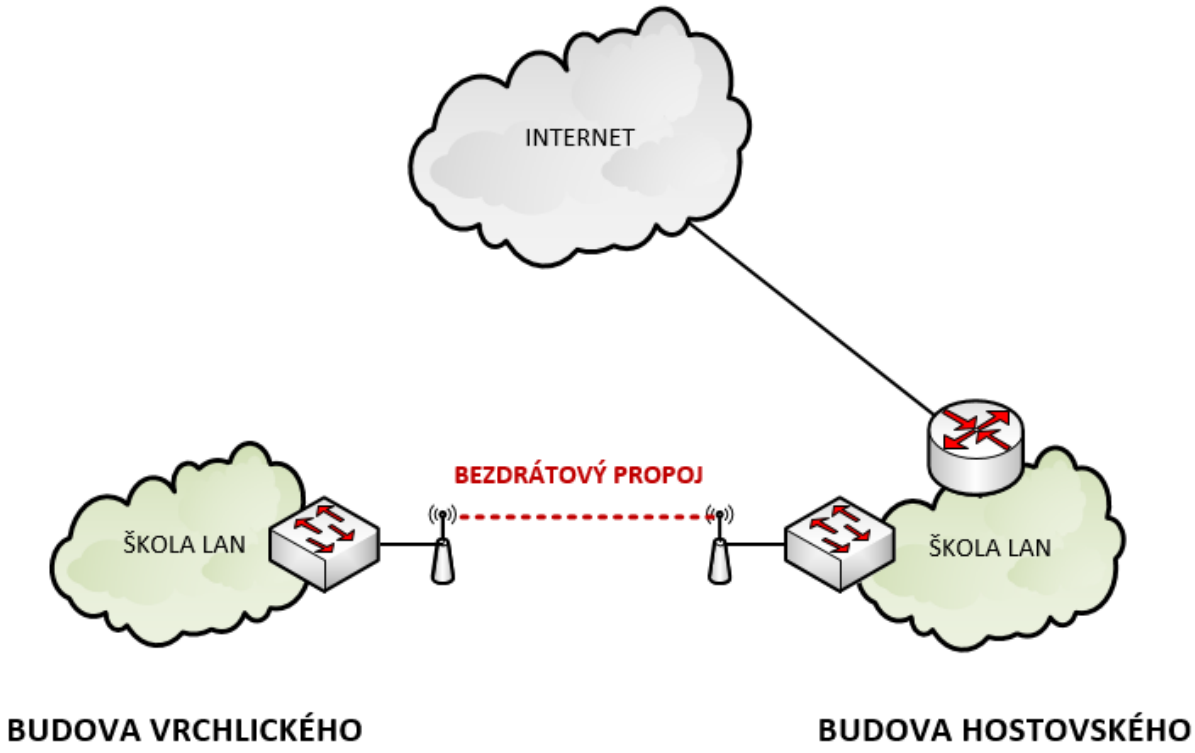
B.3.1 Konektivita k Internetu

Konektivita k Internetu musí splňovat kapacitní nároky. Dle výzvy je třeba zajistit přenosovou rychlost odpovídající 128 kbit/s pro každého žáka. Z celkového počtu žáků 300 je potřeba zajistit internetové připojení alespoň 39 Mbit/s pro oba směry provozu. Škola plánuje rozšíření na přenosové rychlosti na 50 Mbit/s pro oba směry provozu, což by mělo být dostatečné i s plánem navýšení počtu žáku do budoucna.

Dle výzvy musí být poskytovatel internetu součástí bezpečnostního projektu FÉNIX nebo alespoň splňovat jeho technické požadavky. Hlavní výhody pro školu jsou takové, že poskytovatel internetu provozuje redundantní a nepřetížené linky do nejméně dvou uzlů NIX.CZ. Má dohledové středisko fungující v režimu 24x7, tedy v případě problémů s připojením jsou neustále k dispozici. Součástí služby poskytovatele je také CERT/CSIRT tým, který je zodpovědný za řešení bezpečnostních incidentů.

B.3.2 Propojení budov

Na obrázcích níže je požadovaná topologie LAN i WAN sítě pro obě budovy školy. V budově Hostovského je zřízeno připojení do internetu. Propojení mezi budovami bude realizováno bezdrátově. Propojení musí být realizován v licencovaném pásmu.



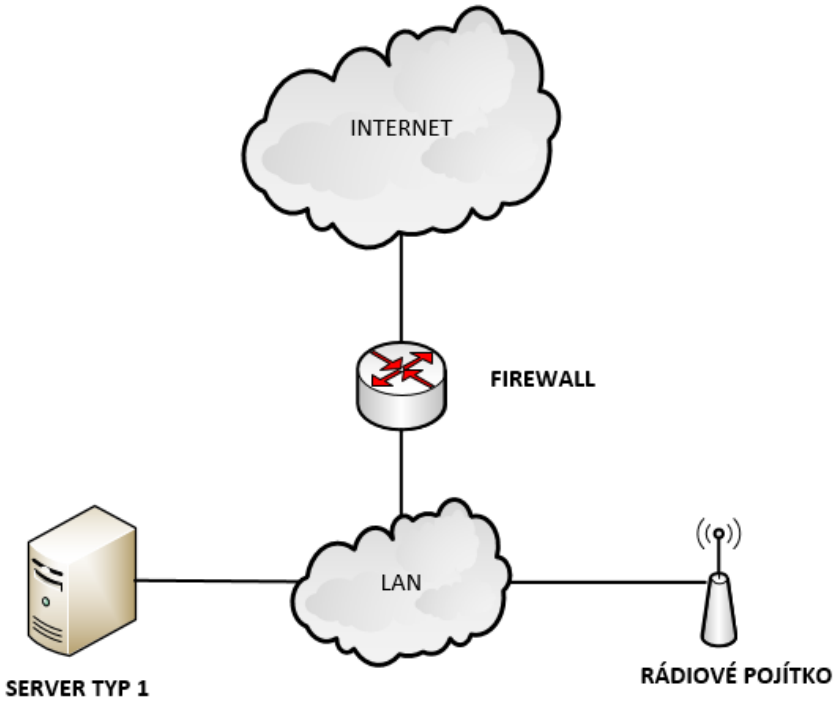
Obr. 1 Blokové schéma propojení budov

B.3.3 Interní LAN

Navržená infrastruktura se skládá z následujících částí:

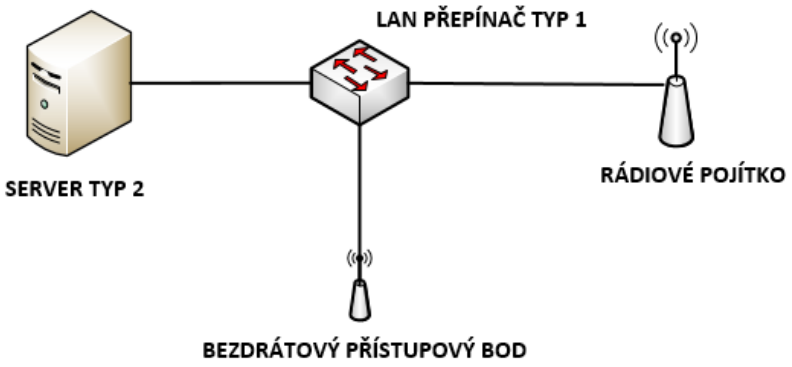
- Firewall
- LAN přepínače
- Bezdrátové přístupové body
- Sonda
- Servery
- UPS
- Rádiová pojítka

Na perimetru sítě je zamýšlen firewall, do kterého bude připojena stávající LAN síť tvořena přepínači, které budou zajišťovat připojení serveru a rádiového pojítka.



Obr. 2 Budova Hostovského - blokové schéma sítě

V budově Vrchlického bude LAN síť tvořena dvěma LAN přepínači typu 1, které se budou starat o připojení serveru typu 2 a rádiového pojítka, dále budou zajišťovat připojení bezdrátových přístupových bodů a jejich napájení přes PoE.



Obr. 3 Budova Vrchlického - blokové schéma sítě

B.3.4 Analýza síťového provozu

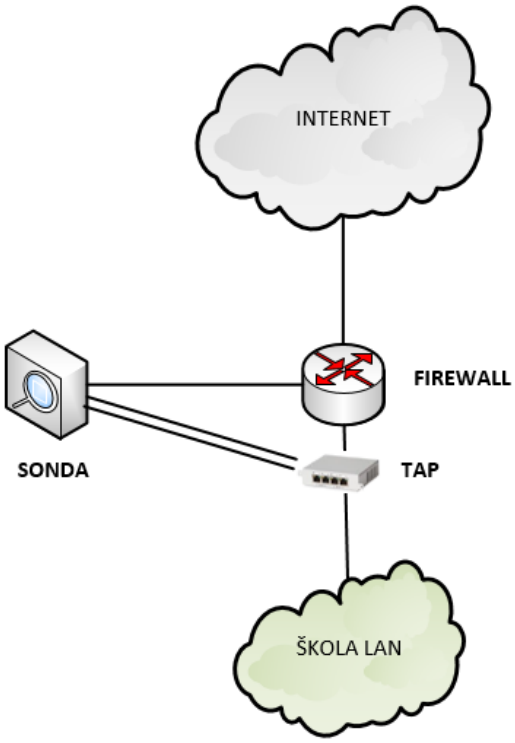
Analýza síťového provozu je kompletní řešení pro analýzu a bezpečnost počítačových sítí na základě IP toků od 10 Mb/s do 100 Gb/s. Řešení poskytuje nástroje pro sledování provozu a zabezpečení sítě, řešení

problémů v síti, monitorování aktivit uživatelů a aplikací, správu a optimalizaci síťového provozu, splnění zákonných požadavků, sledování výkonových parametrů sítě (Network Performance Monitoring) a aplikací (Application Performance Monitoring), analýzu chování sítě (NBA – Network Behavior Analysis) a další.

Řešení zahrnuje následující komponenty:

- Sondy – výkonná autonomní zařízení, která monitorují provoz na počítačové síti, vytváří o něm statistiky v podobě IP toků a zasílají (exportují) je k uložení a další analýze na kolektor
- Kolektory – výkonná zařízení pro sběr, zobrazení, analýzu a dlouhodobé uložení síťových statistik ze zařízení podporující technologii flow (switche, routery), sond či jiných zdrojů. Všechny kolektory jsou vybaveny monitorovacím centrem – aplikaci pro detailní analýzu dat ve formě grafů, tabulek, výpisů komunikací a mnoho dalšího. To poskytuje kompletní přehled o dění v síti včetně dlouhodobých grafů s různými perspektivami, top N statistik, uživatelsky nastavených profilů, možnosti zobrazení dat až na úroveň komunikací a další.
- Moduly – softwarové moduly, které rozšiřují funkcionalitu sond a kolektorů.

Návrh počítá s firewallem, který bude propojen jedním metalickým propojem směrem do Internetu a jedním metalickým propojem směrem ke stávajícímu LAN přepínači. Monitoring linek bude prováděn pomocí metalického TAPu, kdy toto zařízení bude umístěno přímo na lince a bude zrcadlit provoz do sondy. Tato sonda bude provádět sběr dat a bude na vyžádání generovat reporty o překladu adres a uživatelské aktivitě v čase.

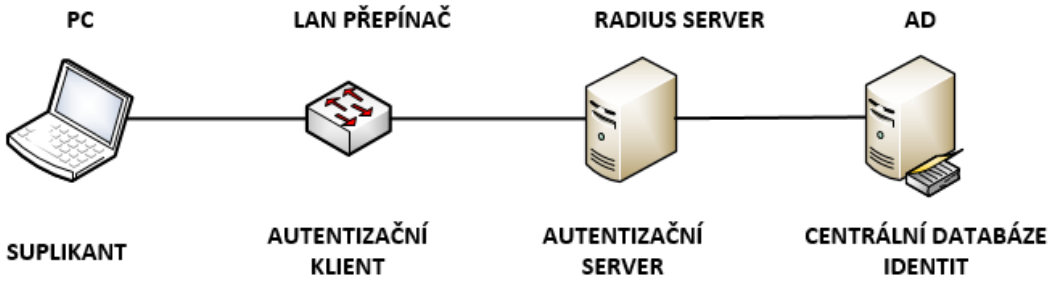


Obr. 4 Blokové schéma pro analýzu síťového provozu

B.3.5 Zabezpečení přístupu do vnitřní sítě (LAN i WLAN)

Uživatelské účty budou uloženy v centrální databázi identit, kde musí být rozděleny do skupin – žáci, učitelé, případně další skupiny. Tato centrální databáze identit bude pak použita pro autentizaci uživatelů do sítě LAN i WLAN, tedy drátové i bezdrátové. Díky tomu bude možné identifikovat uživatele a jeho zařízení v síti a škola bude mít jistotu, že se do sítě nepřipojí nikdo cizí.

Architektura pro zabezpečení přístupu využije 802.1x frameworku, který se skládá z následujících komponent:



Obr. 5 Blokové schéma 802.1x autentizace

- **Suplikant**
  - Software, který běží na koncovém zařízení uživatele a v dnešní době je součástí všech nejrozšířenějších operačních systémů (Microsoft, Apple, Android).
- **Autentizační klient**
  - Síťové zařízení - centrální bezdrátový kontrolér, bezdrátový přístupový bod nebo LAN přepínač, který přeposílá autentizační požadavky od suplikanta na autentizační server a na základě vyhodnocení přístupových údajů povolí nebo zakáže suplikantovi přístup do sítě.
- **Autentizační server**
  - Server, který zpracovává autentizační požadavky a dotazuje se centrální databáze identit na konkrétní uživatelské účty.
- **Centrální databáze identit**
  - Server, nebo služba, která uchovává veškeré informace o všech uživatelských účtech a jejich rozřazení do jednotlivých skupin.

Vzhledem k tomu, že škola již vlastní centrální databázi identit (systém Microsoft Active Directory), je bezesporu doporučeno použít toto řešení.

Jelikož škola již vlastní prostředí postavené na systémech Microsoft, řešení bude rozšířeno o autentizační server založený na službě NPS (Network Policy Server), který bude nainstalován na serveru se systémem MS Windows Server a který plně podporuje protokol RADIUS.

Roli autentizačních klientů budou zastávat všechny síťové prvky, které slouží k přístupu do sítě, tedy LAN přepínače a bezdrátové přístupové body. Tato zařízení podporují protokol RADIUS a umí reagovat na odpovědi od autentizačního serveru.

Jako suplikant bude použit samotný operační systém klientů, není tedy potřeba žádný doplňkový SW. Pro připojení síťových zařízení, které nepodporují funkci suplikanta, se využije MAC bypass autentizace. Do RADIUS serveru se zanese MAC adresa zařízení, která se použije pro 802.1x autentizaci (využívá se například pro IP telefony, tiskárny, kamery, atd.).

Konfigurace NPS

NPS služba bude přijímat požadavky od autentizačních klientů:

- všechny LAN přepínače, které slouží k připojení koncových stanic do sítě
- centrální řídící bezdrátový přístupový bod, který spravuje ostatní přístupové body

NPS bude obsahovat pravidla:

1. V případě, že poskytnuté přihlašovací údaje patří do skupiny „žáci“, NPS jako odpověď vrátí číslo 802.1Q VLAN, do které mají být zařazena všechna žákovská koncová zařízení. Autentizační klient koncové zařízení přiřadí do této VLAN.
2. V případě, že poskytnuté přihlašovací údaje patří do skupiny „učitelé“, NPS jako odpověď vrátí číslo 802.1Q VLAN, do které mají být zařazena všechna učitelská koncová zařízení. Autentizační klient koncové zařízení přiřadí do této VLAN.
3. U zařízení, které nepodporují 802.1X autentizaci, NPS služba ověří jejich MAC adresu. V případě, že tato adresa má být vpuštěna do sítě, NPS vrátí úspěšnou odpověď a autentizační server přiřadí koncové zařízení do VLAN vyhrazené pro tento typ zařízení.
4. Při neúspěšné autentizaci koncového zařízení (špatné přihlašovací údaje, neplatná MAC adresa), autentizační klient nevpustí zařízení do vnitřní sítě školy.

V rámci celé sítě budou na distribučním přepínači nasazena pravidla omezující provozy mezi jednotlivými 802.1Q VLAN.

B.3.6 Zapojení do systému Eduroam

Dle znění výzvy č. 32. je třeba zapojení do federovaného systému Eduroam pro zajištění národní i mezinárodní mobility žáků a učitelů. Eduroam funguje na základě zabezpečeného přístupu do sítě 802.1x (princip popsán výše).

Implementovaný lokální RADIUS server, který autentizuje lokální uživatele, v případě cizích uživatelů předá autentizační požadavek na nadřazený RADIUS server, který spravuje organizace CESNET.

Pro připojení školy do systému Eduroam je nutné definovat správce zodpovědné za RADIUS servery a uživatele. Komunikace mezi RADIUS servery je zabezpečená přes protokoly RadSec nebo IPsec. Pro RadSec nebo IPsec musí správci připojované školy získat certifikát od uznávané CA (certifikační autority). Doporučený je certifikát TCS od firmy DigiCert. Po splnění těchto podmínek budou organizací CESNET dodány další detaily ohledně integrace do sítě Eduroam (např. IP adresy RADIUS serverů).

B.3.7 DNSSEC

DNSSEC (zkratka pro Domain Name System Security Extensions) je v informatice sada IETF specifikací, které umožňují zabezpečit informace poskytované DNS systémem v IP sítích proti podvržení a úmyslné manipulaci. Klient (resolver) může pomocí elektronického podpisu ověřit původ dat, jejich integritu (neporušenost) nebo platnost neexistence záznamu.

Jako rekurzivní DNS server doporučujeme použití Microsoft DNS serveru, který je možné provozovat současně s Active Directory rolí. Microsoft DNS server podporuje nativní resolving DNSSEC domén. Zároveň je možné použít tento DNS server pro interní doménu školy.

DNS server bude nasazený na každém doménovém kontroleru.

B.3.8 Změny potřebné pro úplné splnění výzvy

Pro plné splnění Standardu konektivity školy navrhujeme následující úpravy:

- Navýšit počet bezdrátových přístupových bodů ze 2 na 4 pro dostatečné pokrytí Wi-Fi v budově Vrchlického
- Je třeba, aby aktuální poskytovatel internetového připojení provedl úpravu stávající služby a poskytl subjektu IPv6 adresy
- Zřízení RADIUS serveru a integrace do federovaného systému Eduroam
- Konfigurace DNSSEC resolveru na stávajícím DNS serveru

B.3.9 Počty zařízení v jednotlivých objektech

Počet zařízení, které budou umístěny v budově Hostovského je uveden v tab. 1.

Název	Počet
Firewall	1
Server typ 1	1
Sonda	1
Metalický TAP	2
UPS	1
Rádiové pojítko	1

Tab. 1 Počet zařízení v budově Hostovského

Firewall bude umístěn v místnosti sekretariátu č. 203 ve 3.NP ve stávající rackové skříni. Server typ 1 (Logovací a poštovní server) spolu s UPS bude umístěn v místnosti č. 016 v 1.NP. Rádiové pojítko bude umístěno na střeše budovy na anténním stožáru a bude směrováno na budovu Vrchlického.

Počet zařízení, které jsou zamýšleny pro budovu Vrchlického je shrnut v tab. 2.

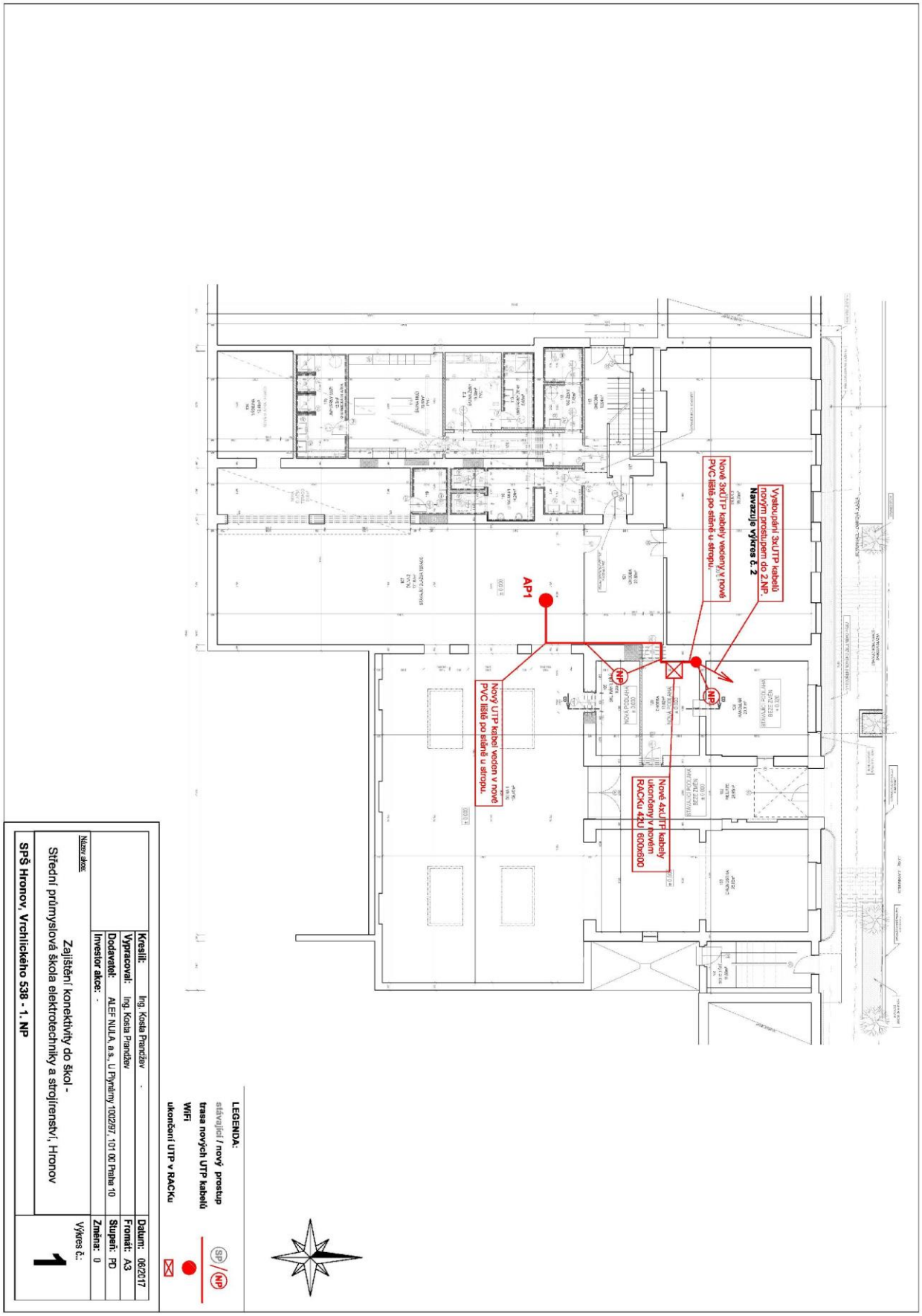
Název	Počet
Bezdrátový přístupový bod	4
LAN přepínač typ 1	2
Server typ 2	1
UPS	1
Rádiové pojítko	1

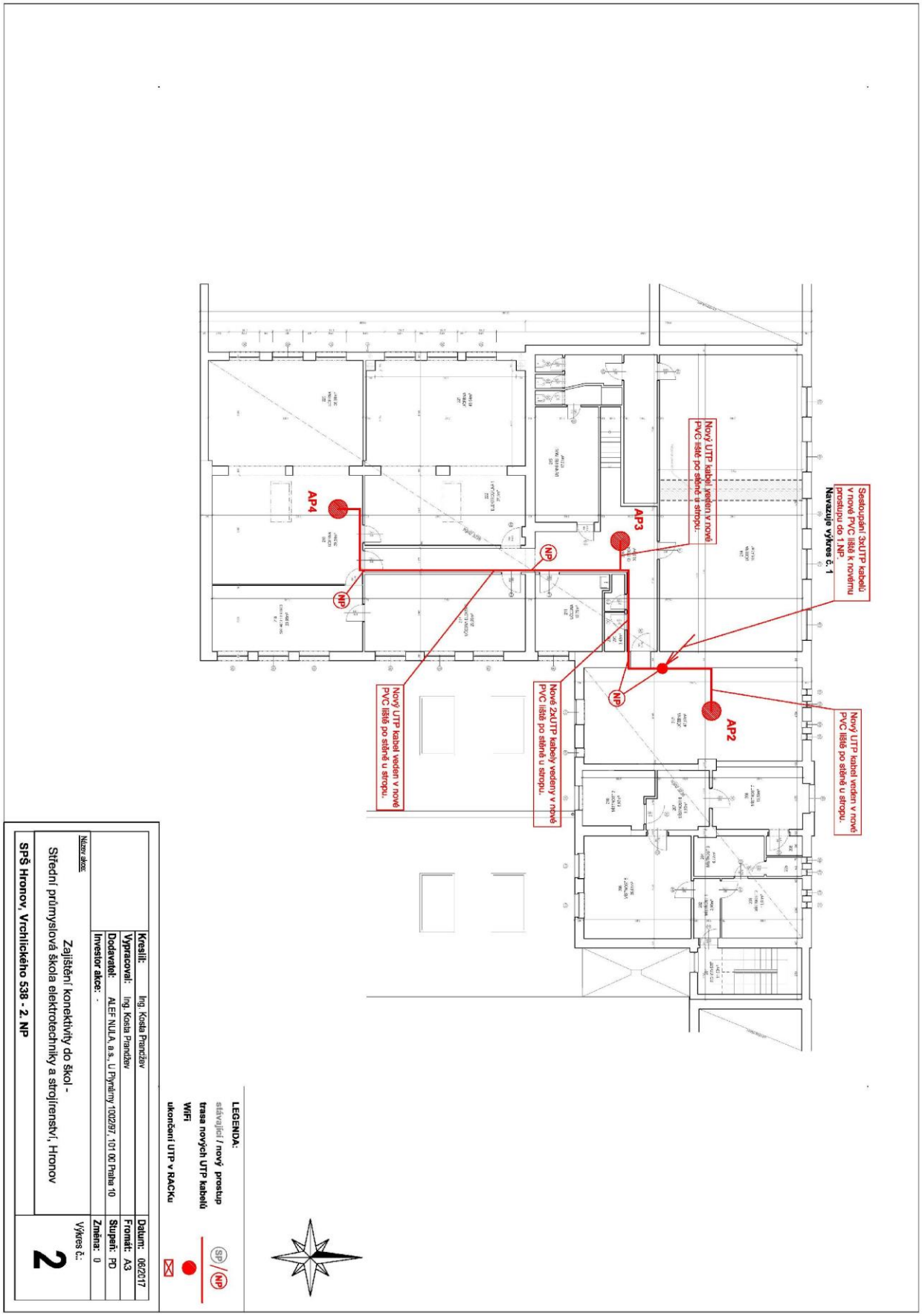
Tab. 2 Počet zařízení v budově Vrchlického

Server typ 2, jeden LAN přepínač typ 1 a UPS budou umístěny v rackové skříni v rohu chodbu č. 120 v 1.NP (vpravo ode dveří, kterými se prochází do chodby č. 121). Druhý LAN přepínač typ 1 bude umístěn v učebně PCV Vrchlického, kde nahradí stávající přepínač.

C. Situační výkresy

Na situačních výkresech níže je zobrazeno rozmístění bezdrátových přístupových bodů a vedení strukturované kabeláže. Rozmístění bezdrátových přístupových bodů bylo určeno na základě simulace šíření Wi-Fi signálu v softwaru Ekahau Site Survey Pro 8.7.2. Výstupy ze simulace jsou zobrazeny v příloze na konci projektové dokumentace.


Vystoupání 3xUTP kabelů novým prostupem do 2.NP.
Navazuje výkres č. 2
Nové 3xUTP kabely vedeny v nové PVC liště po stěně u stropu.
AP1
Nový UTP kabel veden v nové PVC liště po stěně u stropu.
Nové 4xUTP kabely ukončeny v novém RACKu 42U 600x600
NP
LEGENDA:
stávající / nový prostup
trasa nových UTP kabelů
WiFi
ukončení UTP v RACKu
Kreslil: Ing. Kosta Pramžav -
Vypracoval: Ing. Kosta Pramžav
Dodavatel: ALEF NULA, a.s., U Plynárny 1002/97, 101 00 Praha 10
Investor akce: -
Název akce:
Zajištění konektivity do škol -
Střední průmyslová škola elektrotechniky a strojírenství, Hronov
SPŠ Hronov, Vrchlického 538 - 1. NP
Datum: 06/2017
Formát: A3
Stupeň: PD
Změna: 0
Výkres č.:
1


Sestoupání 3xUTP kabelů v nové PVC liště k novému prostupu do 1.NP.
Navazuje výkres č. 1
Nový UTP kabel veden v nové PVC liště po stěně u stropu.
Nový UTP kabel veden v nové PVC liště po stěně u stropu.
Nové 2xUTP kabely vedeny v nové PVC liště po stěně u stropu.
Nový UTP kabel veden v nové PVC liště po stěně u stropu.
AP4
AP3
AP2
NP
LEGENDA:
stávající / nový prostup
trasa nových UTP kabelů
WiFi
ukončení UTP v RACKu
Kreslil: Ing. Kosta Prančáev
Vypracoval: Ing. Kosta Prančáev
Dodavatel: ALEF NULA, a.s., U Plynárny 1002/97, 101 00 Praha 10
Investor akce: -
Název akce:
Zajištění konektivity do škol -
Střední průmyslová škola elektrotechniky a strojírenství, Hronov
SPŠ Hronov, Vrchlického 538 - 2. NP
2
Výkres č.:
Datum: 06/2017
Formát: A3
Stupeň: PD
Změna: 0

D. Dokumentace objektů a technických a technologických zařízení

D.1 Základní technická kritéria školní síťové infrastruktury

Zadavatelem je vyžadováno splnění následujících základních technických kritérií a to jak v části projektu týkající se připojení školy ke službám veřejného Internetu, tak v části o vnitřní konektivitě školy.

D.1.1 Firewall (povinné minimální parametry)

- 1x UTM firewall (bezpečnostní brána) vč. služeb
- 8 x Gb RJ45 port
- 64 GB solid state storage
- možnost vysoce dostupného zapojení dvou firewallů
- minimálně 500 Gateway-to-Gateway IPSec VPN Tunelů
- minimálně 270 client-to-Gateway IPSec VPN Tunelů
- Funkce Load Balancing – možnost rozdělování zátěže
- Bezdrátový kontrolér, podpora vytváření inteligentní bezdrátové sítě
- Podpora silné autentizace uživatelů
- Integrace do sandboxingu
- Podpora IPV6 – NAT46, 66, 64
- integrovaná centrální správa endpoint security klientů z GUI firewallu s možností rozšíření počtu spravovaných klientů, možnost rozšíření o antivirovou funkčnost
- sdílení bezpečnostních informací mezi endpointy a firewallem, automatická pravidla firewallu v závislosti na stavu endpoint klienta
- Integrovaná ochrana emailů (antispam, antivir) včetně podpory šifrování emailů do PDF (automaticky či dle volby uživatele), DLP, uživatelský samoobslužný portál pro přístup k šifrovaným emailům)
- Hardwarová zařízení pro bezkonfigurační VPN na pobočkách. VPN musí být Layer 2, Propustnost VPN min. 90 Mbps.Integrovaný reporting (řádově stovky připravených reportů)
- možnost integrace 2faktorové autentizace klientů VPN či administrátorů firewallu bez nutnosti koupě a/nebo instalace dalšího backend či management software
- bezpečnostní brána a její nadstavby a služby budou zahrnuty v ceně na celou dobu trvání projektu a musí dále splňovat všechny podmínky požadované ve výzvě č. 33 - standard konektivity škol (WAN i LAN)
- součástí bude kompletní konfigurace a nastavení dle potřeb zákazníka a podmínek specifikovaných ve výzvě č. 33 - standard konektivity škol (WAN i LAN)

D.1.2 Server typ 1 (povinné minimální parametry)

- logovací a poštovní server
- rack mount, maximální velikost 2U, přístup ke všem komponentám serveru bez použití nářadí
- 2 sockety pro CPU
- 2 procesory – 8 jader, základní frekvence 2,4 GHz, max. frekvence 3,2 GHz, 20MB Cache
- Min. 48 GB RAM (min. 8GB moduly 2133MHz)
- Min. 2x 8GB (flash či netočící médium) v raid 1 pro hypervizor
- 2x 4TB SATA HDD
- 2x 2TB SATA HDD

- 2x 300GB SAS HDD
- Windows Server 2012 Standard
- HW řadič s podporou raid 0, 1
- Min. 4x 1Gbit ethernet síťové porty s podporou IPv4, IPv6
- Min. 2x 12Gbit SAS porty pro připojení diskového pole včetně 2x 2M kabelů
- DVDROM
- Management serveru nezávislý na operačním systému s dedikovaným USB či SD úložištěm o min. kapacitě 8GB (data na úložišti musí být dostupná i v případě výpadku interních disků či flash pro hypervisor)
- Adresa IP pro vzdálený management musí být na serveru jednoduše nastavitelná a zjistitelná bez potřeby připojování klávesnice a monitoru (z předního ovládacího panelu chassis nebo nahráním dávky z USB paměti)
- Server musí být přístupný v režimu KVM-over-IP s možností připojení remote médií (CDROM, USB, ISO), včetně podpory remote boot z takto připojených prostředků
- Možno použít 2 redundantní síťové napájecí zdroje min. 750W
- Rackové ližiny a rameno na kabeláž na zadní straně serveru
- Certifikace pro VMware 5 a 6, Windows Server 2008 R2, Windows Server 2012 R2 včetně podpory Hyper-V, Red Hat Enterprise a Xen
- Zařízení musí být možné napojit na dohledové centrum výrobce se schopností automaticky generovat servisní události (tzv. proaktivní podpora)

D.1.3 Server typ 2 (povinné minimální parametry)

- server pro budovu Vrchlického
- rack mount, maximální velikost 2U, přístup ke všem komponentám serveru bez použití nářadí
- 2 sockety pro CPU
- 2 procesory – 8 jader, základní frekvence 2,4 GHz, max. frekvence 3,2 GHz, 20MB Cache
- Min. 48 GB RAM (min. 8GB moduly 2133MHz)
- Min. 2x 8GB (flash či netočící médium) v raid 1 pro hypervizor
- 2x 4TB SATA HDD
- 2x 2TB SATA HDD
- 2x 300GB SAS HDD
- Windows Server 2012 Standard
- HW řadič s podporou raid 0, 1
- Min. 4x 1Gbit ethernet síťové porty s podporou IPv4, IPv6
- Min. 2x 12Gbit SAS porty pro připojení diskového pole včetně 2x 2M kabelů
- DVDROM
- Management serveru nezávislý na operačním systému s dedikovaným USB či SD úložištěm o min. kapacitě 8GB (data na úložišti musí být dostupná i v případě výpadku interních disků či flash pro hypervisor)
- Adresa IP pro vzdálený management musí být na serveru jednoduše nastavitelná a zjistitelná bez potřeby připojování klávesnice a monitoru (z předního ovládacího panelu chassis nebo nahráním dávky z USB paměti)
- Server musí být přístupný v režimu KVM-over-IP s možností připojení remote médií (CDROM, USB, ISO), včetně podpory remote boot z takto připojených prostředků
- Možno použít 2 redundantní síťové napájecí zdroje min. 750W

- Rackové ližiny a rameno na kabeláž na zadní straně serveru
- Certifikace pro VMware 5 a 6, Windows Server 2008 R2, Windows Server 2012 R2 včetně podpory Hyper-V, Red Hat Enterprise a Xen
- Zařízení musí být možné napojit na dohledové centrum výrobce se schopností automaticky generovat servisní události (tzv. proaktivní podpora)

D.1.4 Software pro server typ 1 (poštovní server)

- Software pro poštovní server pro 50 uživatelů s jednoduchou správou s pokročilými funkcemi a s ohledem na navrhovaný hardware
- Možnost uchovávat e-mail v rámci řešení on-premise (vlastní hardware), případně v cloudu
- Administrační rozhraní prostřednictvím web prohlížeče
- Intuitivní prostředí v českém jazyce včetně technické podpory

D.1.5 UPS záložní zdroj (povinné minimální parametry)

- 2x UPS pro zálohu napájení obou serverů

D.1.6 LAN přepínač typ 1 (povinné minimální parametry)

- 2x síťový přepínač
- Velikost 1U do racku 19“
- Vrstvy L2 a L3 light switch (pracuje na 2. a 3. vrstvě modelu OSI), plně spravovatelný
- Počet portů min. 48 RJ-45 100/1000 Mb/s
- Podpora logování provozu v síti
- Podpora řízení datových toků
- výrobcem podporované plnohodnotné CLI rozhraní pro konfiguraci a řešení problémů
- IPv4 routing s možností definice až 512 statických cest na až 128 IP rozhranní (VLAN)
- definice ACL s podporou až 512 pravidel
- podpora časově závislých ACL
- podpora IPv6 – včetně IPV6 QoS a ACL
- podpora dvou image na flash – pro možnost jednoduchého návratu k předchozí verzi v případě problémů po upgrade
- Podpora 802.1X
- Podpora QoS

D.1.7 Bezdrátový přístupový bod (povinné minimální parametry)

- 4x bezdrátový přístupový bod (AP)
- AP musí splňovat specifikaci 802.11a/b/g/n/ac
- Každé AP bude mít dvě samostatná rádia - jedno pro frekvenci 2,4GHz a druhé pro frekvenci 5GHz
- MIMO konfigurace rádií minimálně 2x2 v pásmu 2,4GHz a 5GHz
- Podpora centralizovaného automatického plánování kanálů a síly signálu
- Podpora automatického roamingu 802.1x autentizovaných klientů na další AP
- Podpora lokálního i externího guest captive portálu
- AP musí podporovat QoS a VOIP služby
- AP musí umět pracovat v topologii Bridge a Mesh včetně algoritmu pro výběr cesty v rámci MESH stromu

- Podpora napájení přes PoE standardu 802.3af nebo 802.3at
- AP bude možno SW nastavením provozovat v módu:
    - AP plně řízené kontrolérem tunelující všechna uživatelská data směrem ke kontroléru
- Až 8 možných vysílaných BSSID na jednu radiovou část
- AP obsahuje HW pro spektrální analýzu (detekce zdroje rušivého signálu – interference)
- Jednotlivá AP musí mít plnohodnotnou WIFI-Alliance certifikaci
- WIFI AP musí mít možnost být automaticky nastaveno (zero touch provisioning) externím management SW
- Součástí dodávky AP musí být instalační sada pro pevnou instalaci na povrch v bílé barvě
- Bezdrátové prvky musí splňovat všechny podmínky požadované ve výzvě č. 33 - standard konektivity škol (LAN)
- součástí dodávky bude kompletní konfigurace a nastavení dle potřeb zákazníka a podmínek specifikované ve výzvě č. 33

D.1.8 Sonda pro monitorování síťového provozu (povinné minimální parametry)

- Počet monitorovacích portů: min. 2 x 10/100/1000 Mbps (metalika - RJ45)
- Management port: 1x 10/100/1000 Mbps metalický
- Minimální výkon na každém monitorovacím portu: 1 200 000 paketů za sekundu
- Možnost nastavení rychlosti monitorované linky 10/100/1000Mb/s na metalických rozhraních
- Pasivní zapojení bez vlivu na monitorovanou síť: zapojení pomocí TAPů
- Nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích, nesmí docházet k ovlivňování chování sítě
- Nezávislý autonomní zdroj Flow statistik, podpora IPv4, IPv6, VLAN, MPLS, GRE
- Podpora monitorování MAC adres, http URL a DNS dotazu
- Podpora standardizovaných protokolů pro výměnu dat o IP tocích: NetFlow v5, v9 - RFC3954, IPFIX
- Detekce aplikací, monitorování a analýza HTTP provozu a VoIP statistik
- Zabezpečená vzdálená správa, dohled a konfigurace: HTTPS (GUI), SSH
- Kolektor pro dočasné ukládání Flow statistik (zajištění redundance) obsahuje uživatelsky definovaný dashboard, automatickou tvorbu reportů, detekci aktivních zařízení a detailní analytické možnosti
- Úložná kapacita kolektoru min. 500 GB
- Možnost doplnit o další moduly, např. behaviorální analýza, monitoring výkonu webových aplikací
- Časová synchronizace zařízení proti centrálnímu zdroji času na síti
- Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména
- Správa uživatelů a přístupových práv na zařízení
- Podpora vzdálené autentizace uživatelů LDAP (Active Directory)

E. Příloha

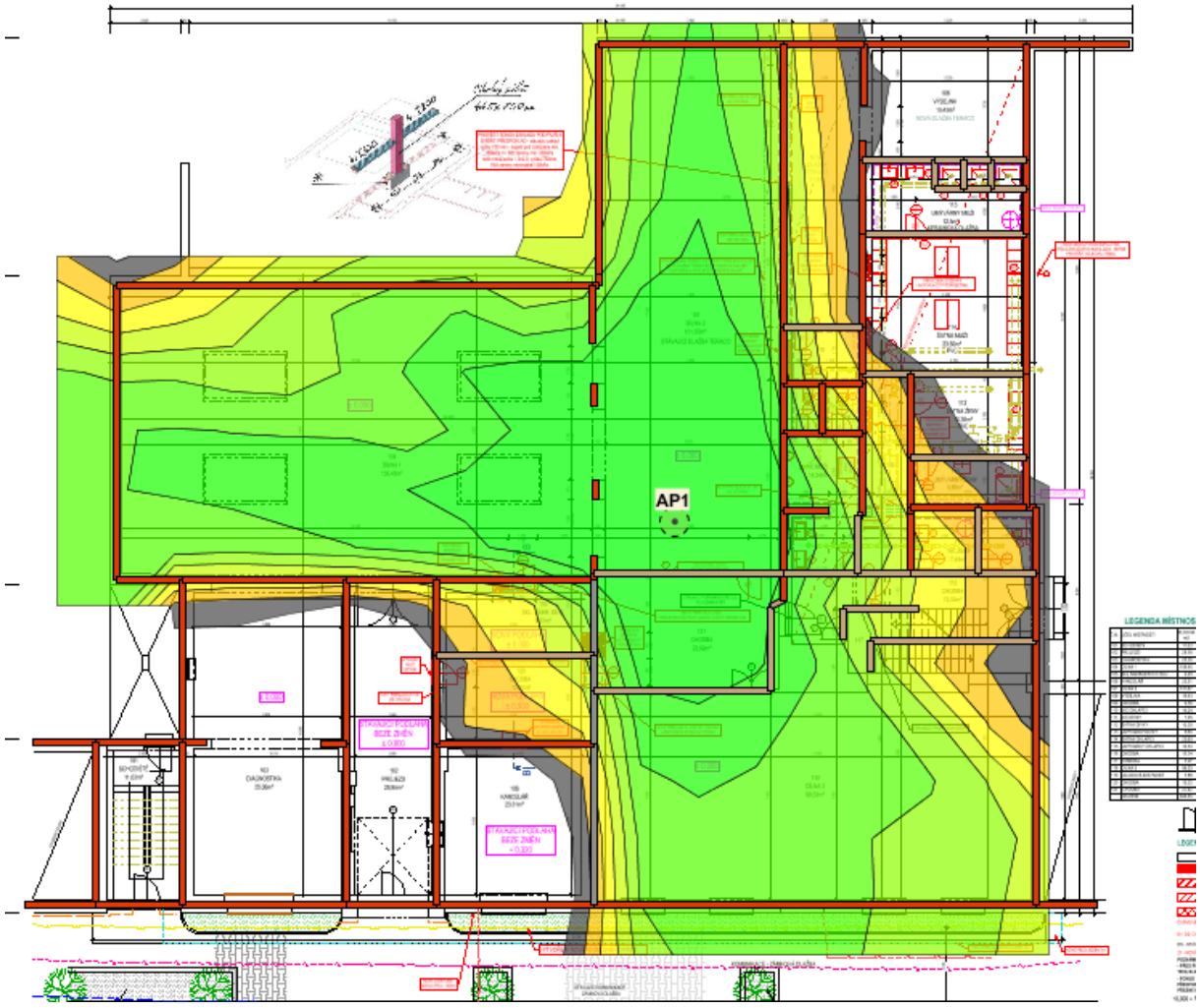
E.1 Simulace šíření Wi-Fi signálů

Na obrázcích níže je výstup ze simulace šíření Wi-Fi signálu pro pásmo 2,4 i 5GHz. Je zobrazena síla signálu v jednotkách dBm.

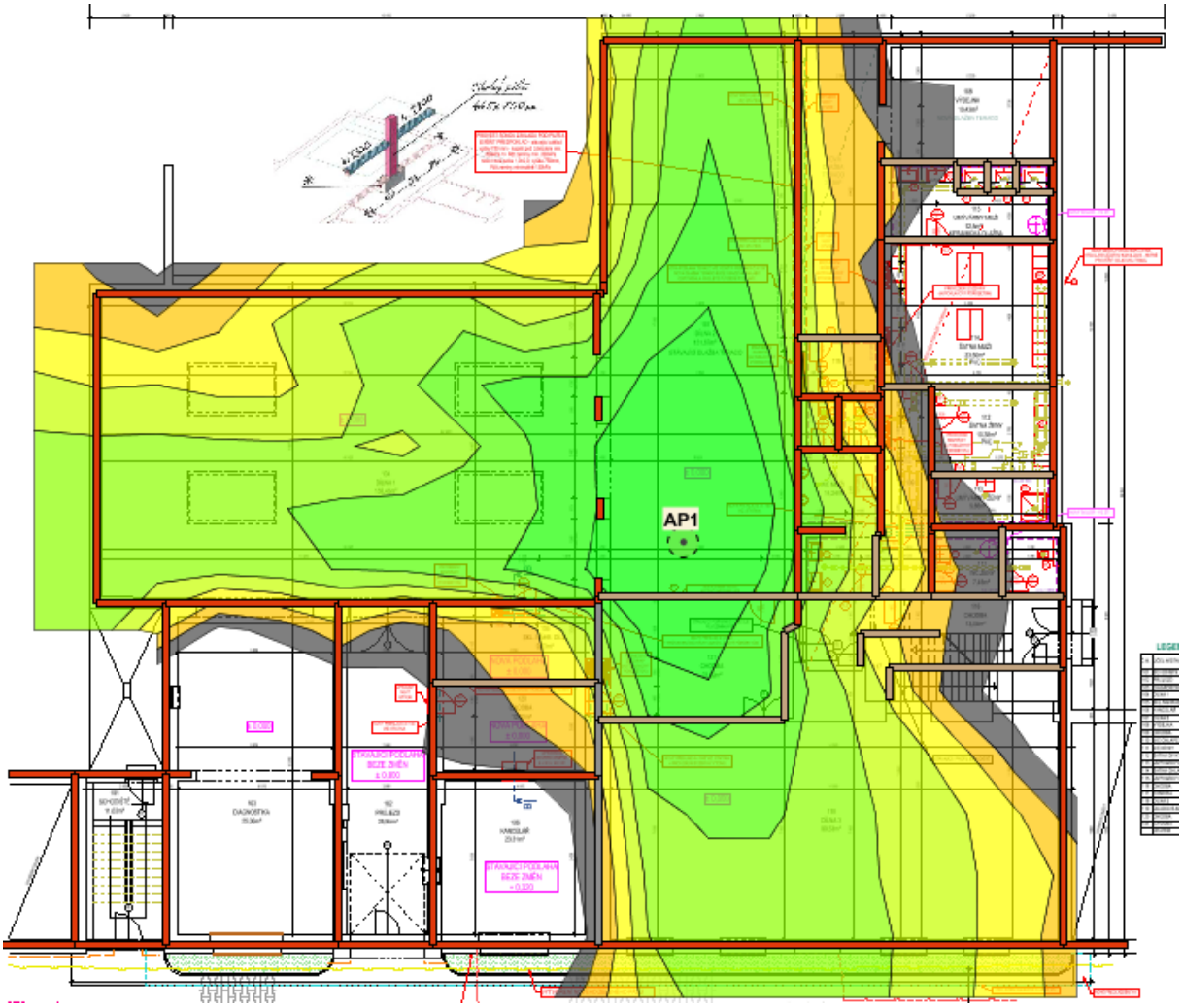
Pro účely simulace byli zvoleny následující hodnoty

- Typ bezdrátového přístupového bodu: Meraki MR32
- Vysílací výkon: 25mW
- Útlum zdiva:
  - Červená – 10dB
  - Hnědá – 3dB
- Ořez síly signálu (znázorněn šedivou barvou): -75dBm

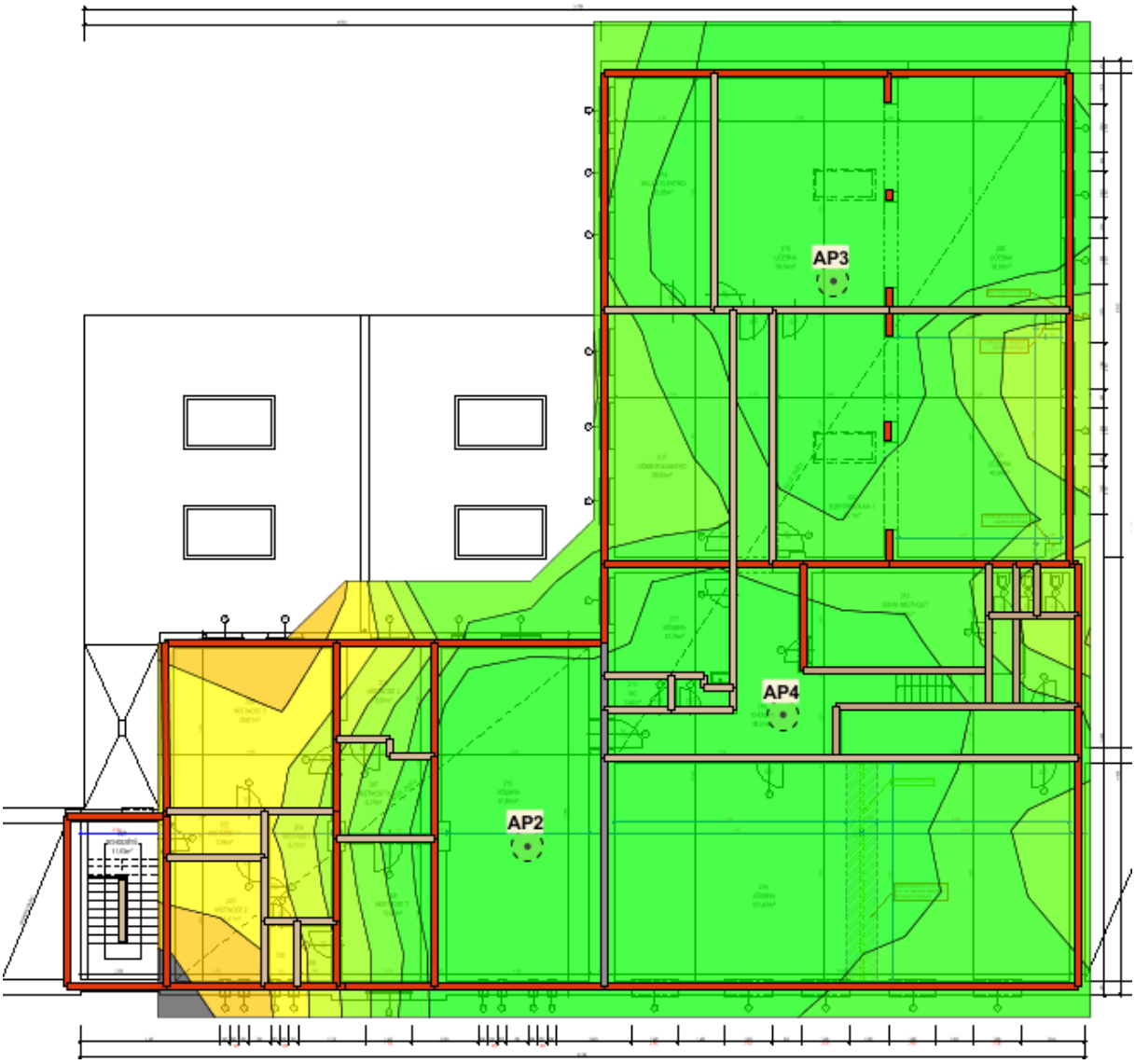
Obr. 6 Legenda síly signálu RSSI



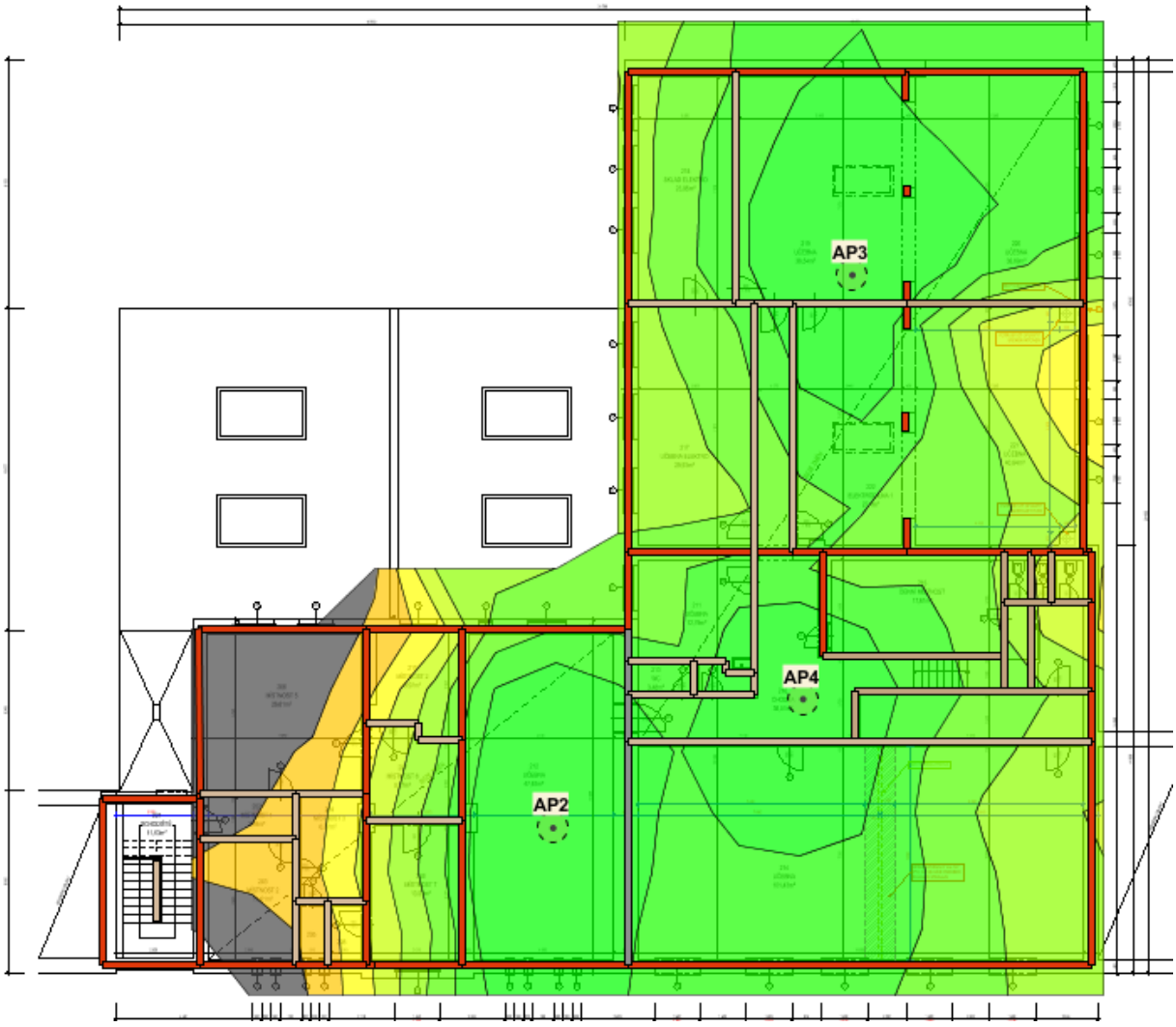
Obr. 7 Budova Vrchlického – 1.NP – síla signálu RSSI pro 2,4GHz



Obr. 8 Budova Vrchlického – 1.NP – síla signálu RSSI pro 5GHz



Obr. 9 Budova Vrchlického – 2.NP – síla signálu RSSI pro 2,4GHz



Obr. 10 Budova Vrchlického – 2.NP – síla signálu RSSI pro 5GHz