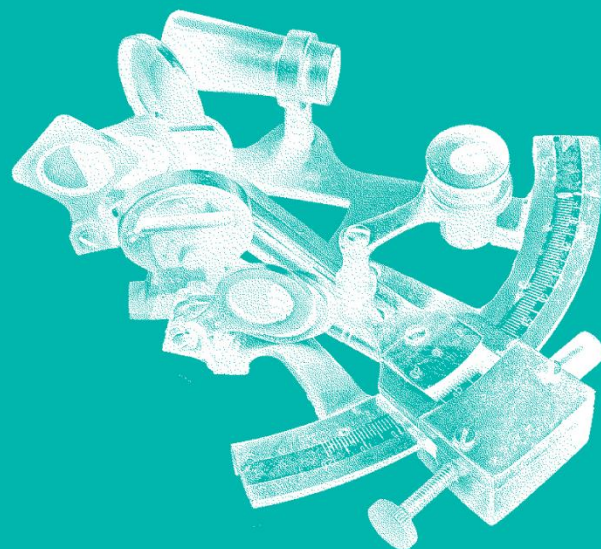


# Zajištění konektivity do škol - projektová dokumentace – aktivní prvky

**Střední škola gastronomie a služeb, Nová Paka**



## Obsah

<b>Úvod</b>	<b>3</b>
<b>A. Průvodní zpráva</b>	<b>4</b>
A.1 Identifikační údaje	4
A.2 Seznam vstupních podkladů	4
A.3 Údaje o území	4
<b>B. Souhrnná technická zpráva</b>	<b>5</b>
B.1 Výchozí stav	5
B.2 Nedostatky infrastruktury dle výzvy č. 32	5
B.3 Technické řešení projektu	5
<b>C. Situační výkresy</b>	<b>12</b>
<b>D. Dokumentace objektů a technických a technologických zařízení</b>	<b>20</b>
D.1 Základní technická kritéria školní síťové infrastruktury	20
<b>E. Příloha</b>	<b>25</b>
E.1 Simulace šíření Wi-Fi signálů	25

## Úvod

Projektová dokumentace je zpracována pro SŠGS Nová Paka, hlavní budova Masarykovo nám. 2 a cukrářská dílna Havlova 403. 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 škola gastronomie a služeb, Nová Paka**  
 Dotčené objekty:

- objekt školy - Masarykovo nám. 2, Nová Paka, katastrální území Nová Paka, parcelní číslo 23
- objekt cukrářů – Havlova 403, Nová Paka, katastrální území Nová Paka, parcelní číslo 3745

#### 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
- Proveden průzkum - šetření na místě stavby

### A.3 Údaje o území

Objekt	Katastrální území
Objekt školy - Masarykovo nám. 2, Nová Paka	katastrální území Nová Paka, parcelní číslo 23
Objekt cukrářů – Havlova 403, Nová Paka	katastrální území Nová Paka, parcelní číslo 3745

## B. Souhrnná technická zpráva

Technická zpráva popisuje projekt „Standard konektivity škol“, dle výzvy č. 32.

### B.1 Výchozí stav

Ve škole je aktuálně 366 žáků a 77 počítačů. Konektivita pro celou školu je 32 Mbit/s pro příchozí i odchozí směr internetového provozu s agregací 1:2 bez FUP. Poskytovatelem internetového připojení je NET2U. Přidělené IP adresy jsou pouze IPv4.

Ve škole se využívá centrální databáze identit Microsoft Active Directory pro přístup do PC v počítačových učebnách.

Na perimetru sítě je umístěn HP server, na kterém běží mimo jiné i firewall. LAN přepínače jsou TP-link, Zyxel a další. Bezdrátová síť je realizována na přístupových bodech Ubiquity.

### B.2 Nedostatky infrastruktury dle výzvy č. 32

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 366 je potřeba zajistit internetové připojení alespoň 47 Mbit/s pro oba směry provozu.

V aktuálním 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 bezdrátovou sítí, která není dimenzovaná na vyšší počet žáků a nezvládá je obsloužit v požadované kvalitě a očekávaném uživatelském komfortu. Dále dochází k vyčerpání kapacity na serveru, pro budoucí růst aplikací je třeba pořídit výkonnější server.

Aktuální poskytovatel internetového připojení neposkytuje IPv6 adresy, není zapojen do bezpečnostního projektu FÉNIX a ani nesplňuje jeho podmínky.

### B.3 Technické řešení projektu

Níže je v jednotlivých částech popsán technický návrh řešení projektu.

#### B.3.1 Konektivita k Internetu

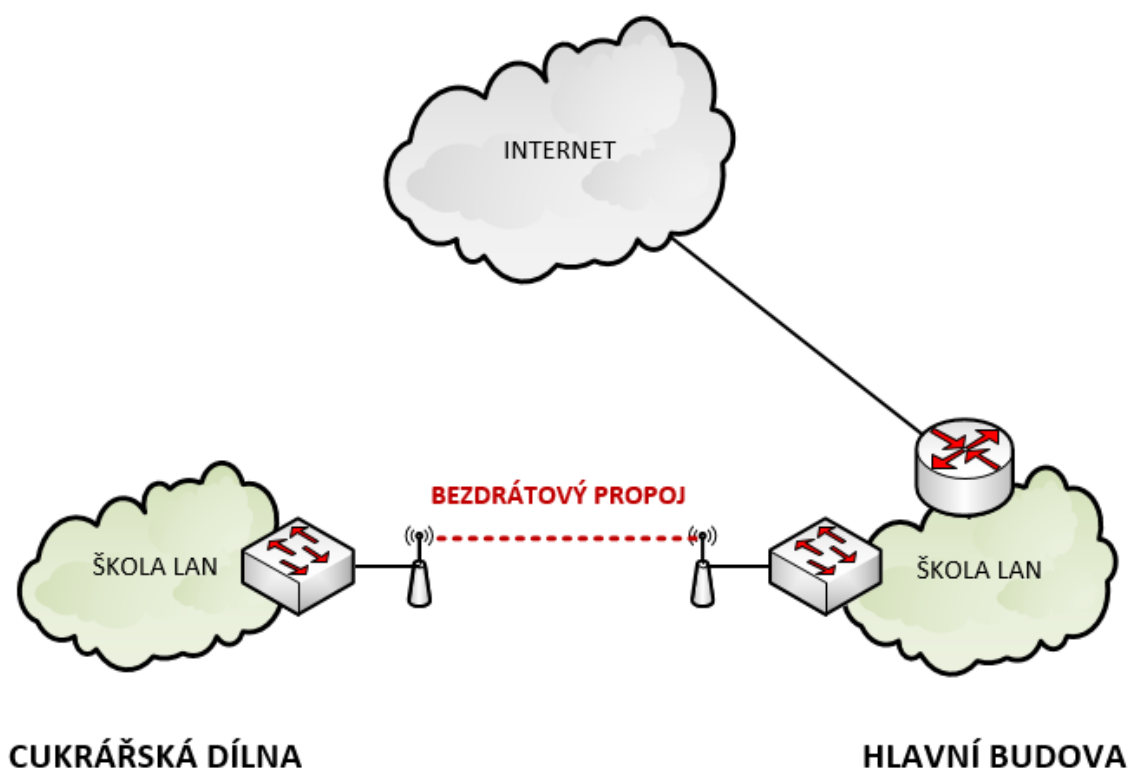
Konektivita k Internetu musí splňovat kapacitní nároky. Dle výzvy je třeba zajistit přenosovou rychlost odpovídající 128 kbit/s pro každého žáka. Z celkového počtu žáků 366 je potřeba zajistit internetové připojení alespoň 47 Mbit/s pro oba směry provozu.

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

V hlavní budově je zřízeno připojení do Internetu. Vzhledem k lokalitě budov, bude propojení mezi hlavní budovou a cukrářskou dílnou realizováno bezdrátovou technologií v licencovaném pásmu.

Propojení zřídí poskytovatel internetového připojení formou služby, proto není součástí projektové dokumentace.



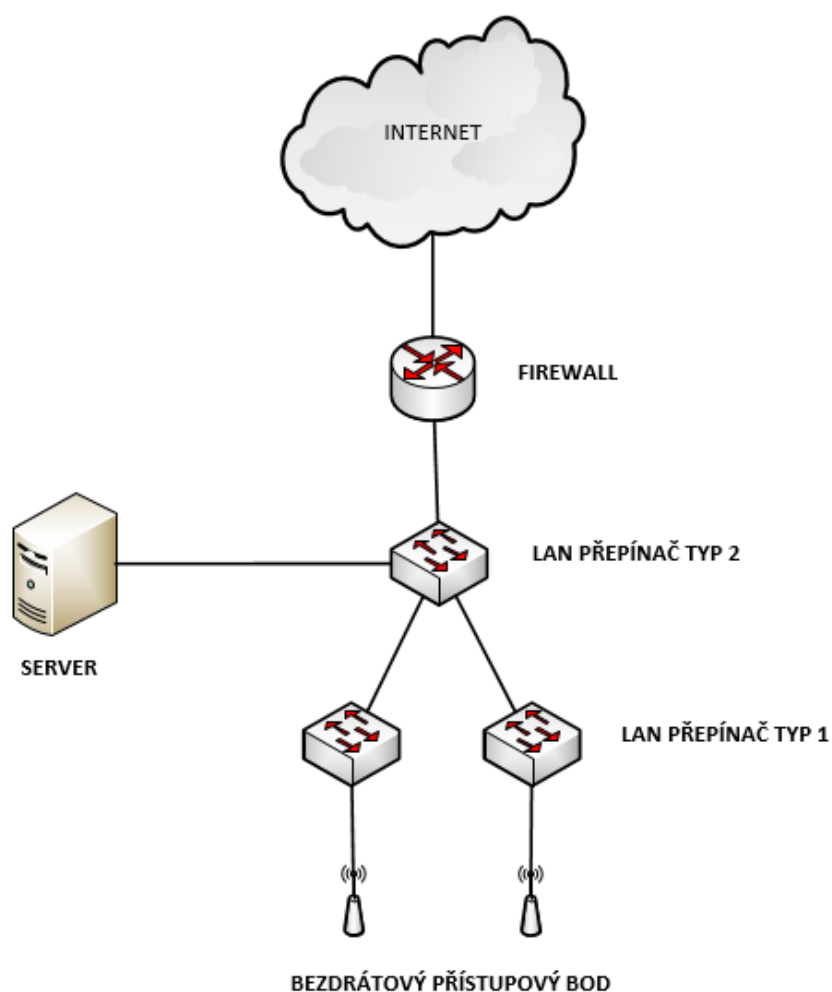
Obr. 1 Blokové schéma propojení budov

### B.3.3 Interní LAN

Navržená infrastruktura se skládá z následujících částí:

- Firewall
- LAN přepínače
- Bezdrátové přístupové body
- PoE injektory
- Sonda
- Server
- USB flash disk
- UPS záložní zdroj

Na perimetru sítě je zamýšlen firewall, do kterého je připojen distribuční LAN přepínač typu 2, který bude provádět směrování VLAN a připojení serveru a přístupových LAN přepínačů typu 1. Bezdrátové přístupové body v hlavní budově budou napájeny z LAN přepínačů typu 1 přes Power-over-Ethernet (PoE).



*Obr. 2 Hlavní budova - blokové schéma sítě*

V budově cukrářské dílny budou dva bezdrátové přístupové body napájeny PoE injektory.



*Obr. 3 Cukrářská dílna - blokové schéma sítě*

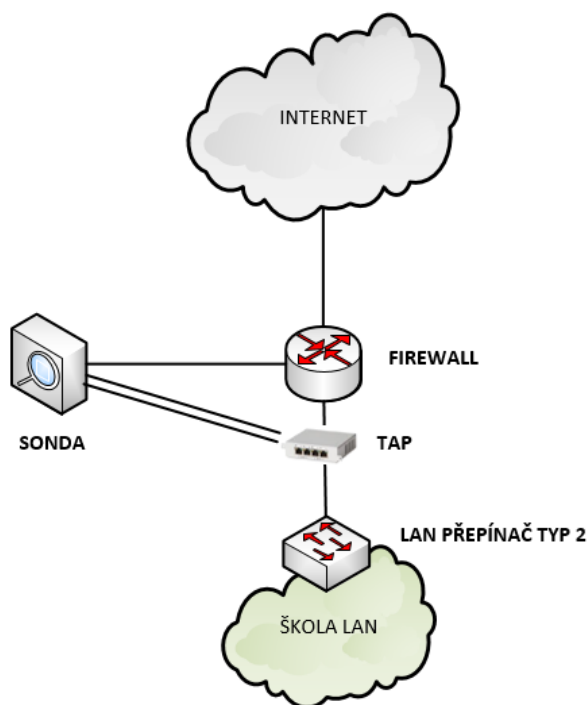
### B.3.4 Analýza síťového provozu

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 – aplikací 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 firewalllem, který bude propojen jedním metalickým propojem směrem do Internetu a jedním metalickým propojem směrem k distribučnímu LAN přepínači typu 2. Monitoring linek bude prováděn pomocí metalického TAPu, kdy toto zařízení bude umístěno přímo na lince a bude zrcadlit provoz do sondy. Sběr dat bude provádět sonda. Tato sonda bude nasbíraná data uchovávat a na vyžádání generovat reporty o překladech adres a uživatelské aktivitě v čase.



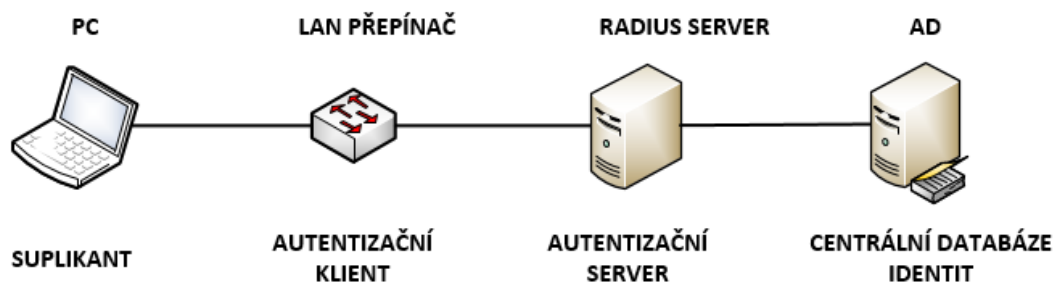
*Obr. 4 Blokové schéma pro analýzu síťového provozu*



### 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 typu 1 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 zanesou MAC adresy zařízení, která se použijí 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 řídicí 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 provoz 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 Počty zařízení v jednotlivých objektech

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

Název	Počet
Firewall	1
LAN přepínač typ 1	2
LAN přepínač typ 2	1
Bezdrátový přístupový bod	15
Server	1
Sonda	1
Metalický TAP	1
USB flash disk	1
UPS záložní zdroj	1

Tab. 1 Počet zařízení v hlavní budově

V učebně č. 6 bude umístěn firewall, jeden LAN přepínač typ 1 a jeden LAN přepínač typ 2. Dále zde bude umístěn server a sonda pro monitorování síťového provozu. Druhý LAN přepínač typ 1 bude umístěn ve sborovně v přízemí. Všechny zmíněné aktivní prvky budou implementovány výměnou za stávající zařízení. Budou použity také stávající LAN propoje mezi učebnou č. 6 a sborovnou.

Počet zařízení, které jsou zamýšleny pro cukrářskou dílnu, je shrnut v tab. 2.

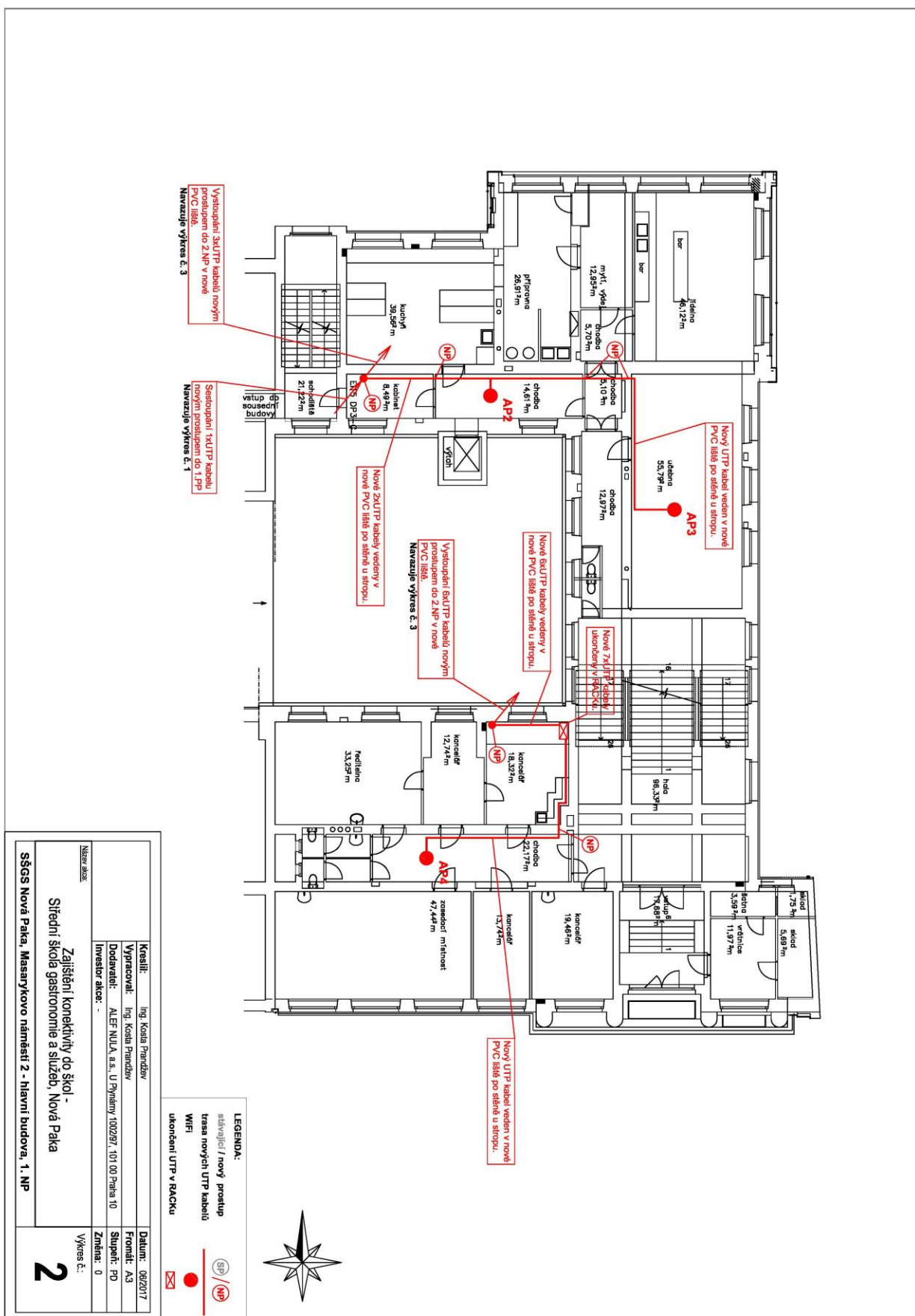
Název	Počet
Bezdrátový přístupový bod	2
PoE injektor	2

Tab. 2 Počet zařízení v cukrářské dílně

## C. Situační výkresy

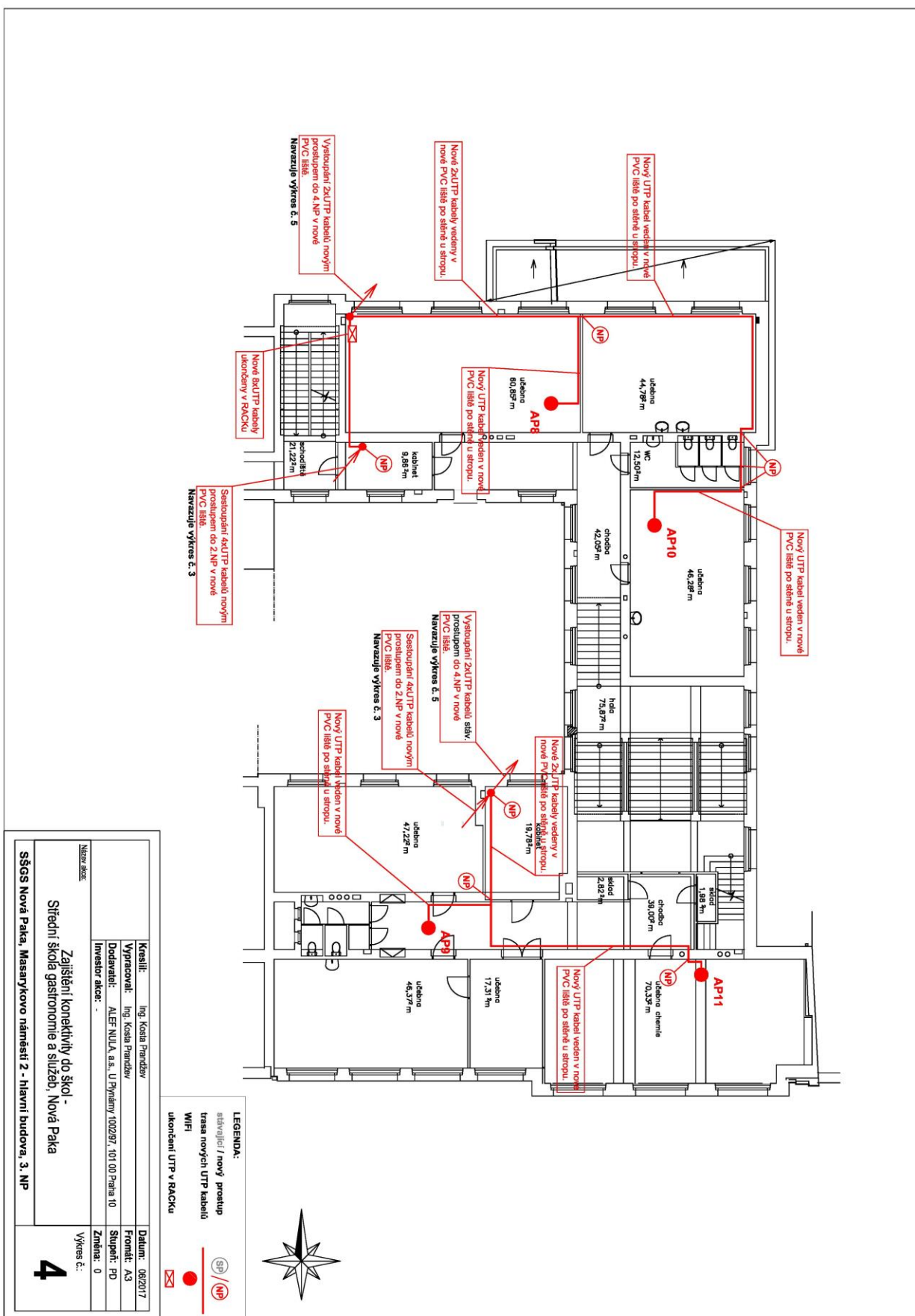
Na situačních výkresech níže je zobrazeno rozmístění bezdrátových přístupových bodů a vedení strukturované kabeláže. Rozmístění bezdrátových přístupových bodů bylo určeno na základě simulace šíření Wi-Fi signálu v softwaru Ekahau Site Survey Pro 8.7.2. Výstupy ze simulace jsou zobrazeny v příloze na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



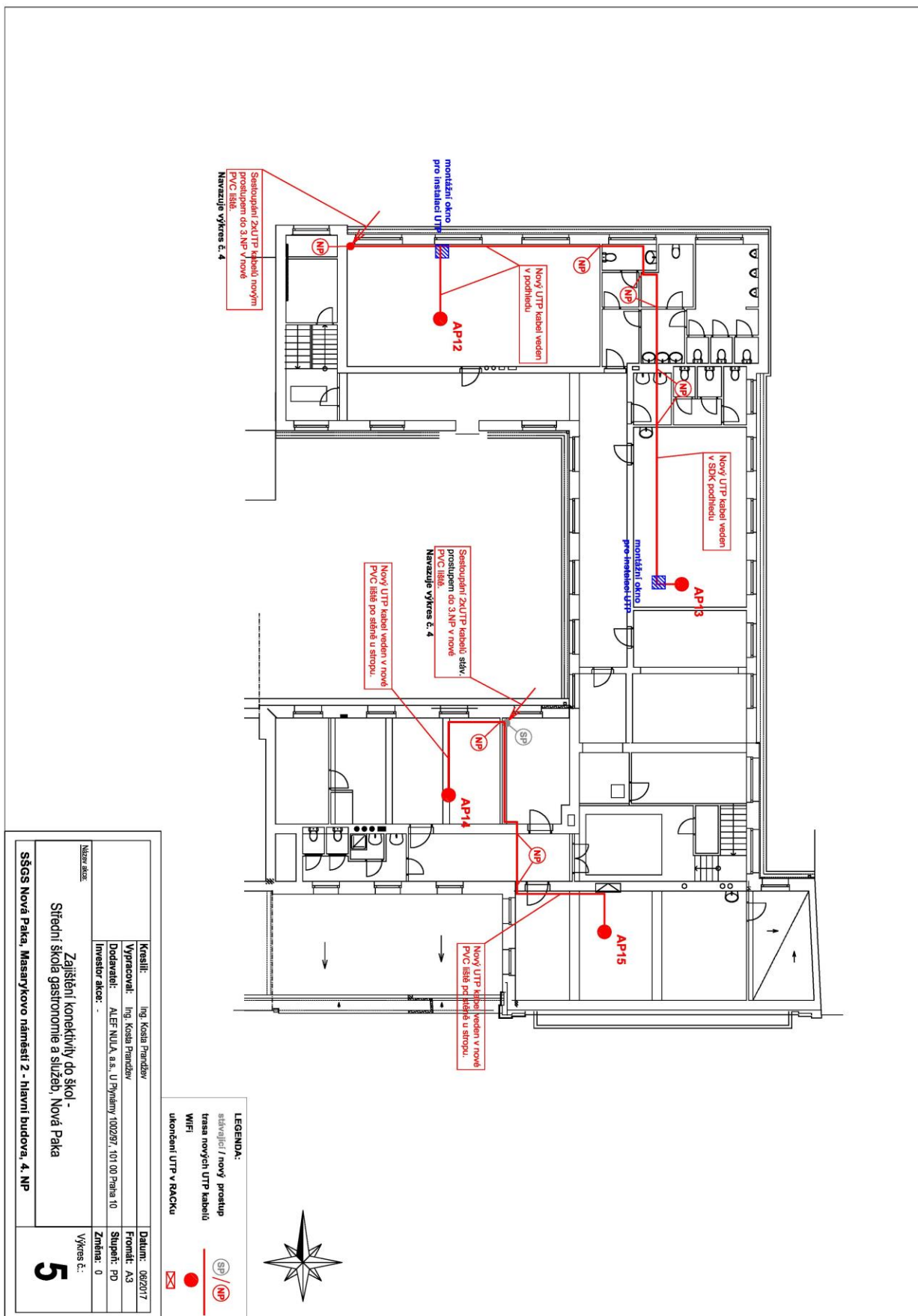


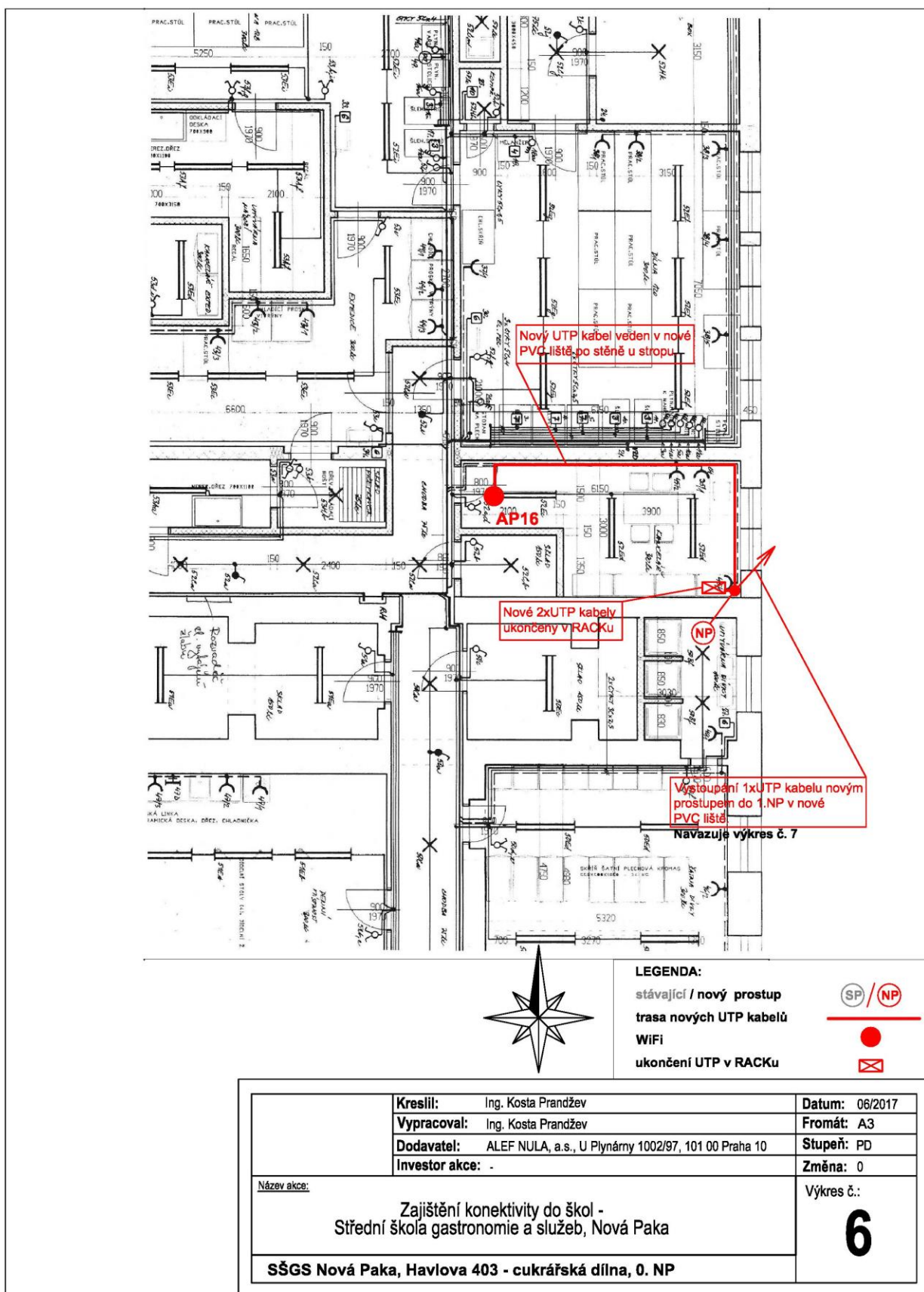


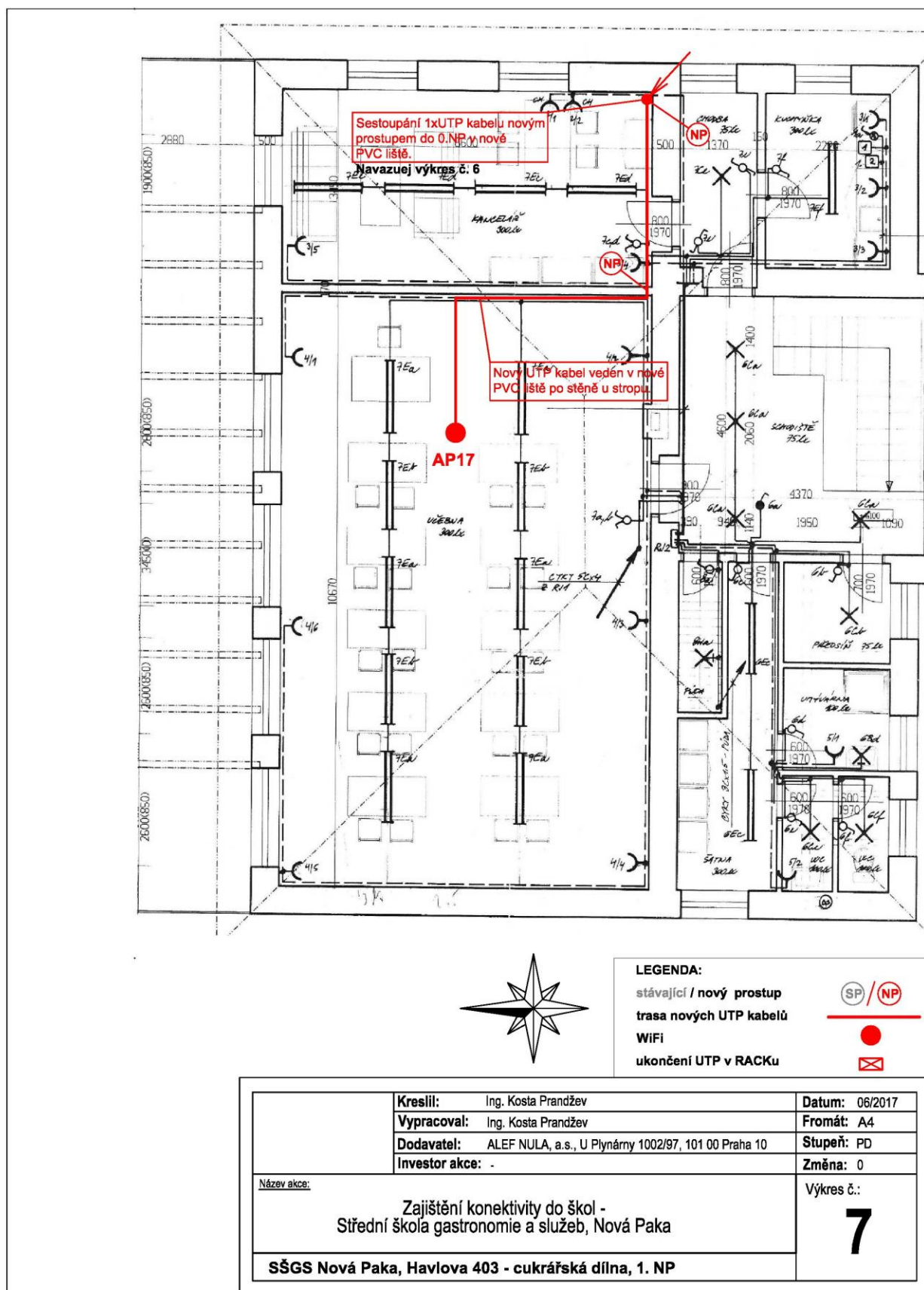












## D. Dokumentace objektů a technických a technologických zařízení

### 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)

- UTM firewall
- funkcionality VPN, IPS, aplikační kontroly (L7), web filtering, antivirus, antispam
- kontrola http a https provozu, kategorizace a selekce obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirová kontrola stahovaného obsahu
- výkon firewallu 2.5Gbps
- výkon IPS 950Mbps
- výkon SSL VPN 300Mbps
- výkon antiviru 300Mbps
- port pro správu (console)
- min. 8x 1Gbps RJ45
- monitoring a logování NAT (RFC 2663)
- integrovaná dvoufaktorová autentizace (HW nebo SW token)
- podpora IPV6 – NAT46, 66, 64
- vnitřní kapacita storage 32GB, možnost logování na lokální disk nebo na logovací server
- logování přístupu uživatelů do Internetu min. IP adresa – čas – uživatel v stávající Microsoft Active Directory
- podpora pro rate limiting, antispoofing a ACL/xACL
- snadná konfigurace ACL/FW na základě identifikovaných útoků přes webové rozhraní
- Management přes SSH, HTTPS
- policy based routing a source based routing
- SSL inspekce
- Podpora virtuálních firewallů s oddělenou správou a konfigurací, min. 5 virtuálních firewallů
- Možnost konfigurace tzv. Guest portálu
- montáž do racku

#### D.1.2 Server (povinné minimální parametry)

- 2x CPU
- Každý CPU schopnost zpracovávat najednou 12 procesů (= 12 fyzických jader, nebo 6 fyzických a 12 virtuálních)
- výkon dle [www.cpubenchmark.net](http://www.cpubenchmark.net) minimálně 9800 (PassMark – CPU Mark), aby bylo možno prokázat výkon procesoru, udělejte v den vytvoření nabídky screenshot jeho aktuálního skóre ve výše uvedené webové stránce. Přiložte ho k nabídce.
- Procesor s podporou virtualizace
- Podpora 2 procesorů
- Alespoň 64GB RAM DDR4 2133MHz RDIMM ECC



- Konektivita 4xLAN 1Gbps
- USB rozhraní na základní desce
- 2x Pevný disk 2,5" – kapacita alespoň 300GB kompatibilní s rozhraním základní desky, 10000rpm
- možnost instalace alespoň dalších 10ks 2,5" disků
- Řadič disku s min. 2GB paměti
- vzdálený management serveru (kvm) přes webový prohlížeč
- HW RAID řadič s minimální podporou raid 0,1,5,6
- SATA DVD RW mechanika
- Podpora instalace redundantního napájecího zdroje
- server musí být kompatibilní s VMware esx poslední verze - <http://www.vmware.com/resources/compatibility/search.php>
- 8 ks Pevný disk 2,5" – kapacita alespoň 1.8TB, rychlost otáček 10tis rpm, podpora hotplug, kompatibilní s rozhraním základní desky
- Redundantní napájecí zdroj k serveru
- KVM vzdálený management serveru s podporou připojení virtuálního media a přenosu grafického obrazu

#### **D.1.3 Implementace serveru**

- Min. v rozsahu kompletní HW serveru, fyzická montáž, aktualizace firmware a ovladačů, konfigurace storage (RAID), konfigurace vzdáleného managementu, konfigurace hypervisoru (ESXi), instalace a základní konfigurace OS Windows 2012 (2016) Serveru, aktualizace OS, konfigurace Active Directory (cca 500 uživatelů), migrace objektů a dat ze stávajícího serveru, migrace oprávnění.
- Konfigurace DNS, DHCP
- Konfigurace DNSSEC resolver
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel
- vazba na UTM FireWall

#### **D.1.4 USB flash disk (povinné minimální parametry)**

- USB 3.0
- rychlost čtení 150MB/s
- kompatibilní s rozhraním serveru
- kapacita alespoň 32GB

#### **D.1.5 UPS záložní zdroj (povinné minimální parametry)**

- výstupní výkon 900W/1500VA, 230V
- USB port
- line interaktivní
- panel pro kontrolu stavu, zvukové upozornění
- přepětová ochrana rázu 459J
- při 100% zátěži doba provozu 4,5min
- při 50% zátěži doba provozu 13min
- výstupní zásuvky 6ks IEC 320 C13

#### **D.1.6 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)

#### **D.1.7 Implementace sondy pro monitorování síťového provozu**

- Montáž ro racku, aktualizace firmware, nastavení management portu (SSL, HTTPS)
- Nasazení ve směru do WAN
- Zrcadlení provozu pomocí TAP
- Konfigurace ukládání Flow data min. na úrovni zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ), která budou archivována min. 2 měsíce.
- Konfigurace NTP

#### **D.1.8 LAN přepínač typ 1 (povinné minimální parametry)**

- Velikost 1U do racku 19"
- Vrstvy L2 (pracuje na 2. vrstvě modelu OSI), plně spravovatelný
- Výkon PoE min. 370W PoE+
- Počet portů min. 48 RJ-45 100/1000 Mb/s
- Počet SFP portů min. 4
- Kapacita přepínání min. 104 Gb/s
- Datový tok min. 77 milionů paketů/s
- Velikost tabulky MAC adres min. 16 000 záznamů
- Počet VLAN 512
- Vlastnosti přepínače:
- SNMP verze 2c a 3.
- Quality of Service (QoS).
- Multiple spanning tree.
- Rapid spanning Tree
- IEEE 802.1p – Min. 4 fronty

- Podpora spanning tree instance per VLAN s 802.1Q tagováním BPDU rámců.
- Monitoring datových toků v síti pomocí sFlow.
- Podpora managementu přes IPv4 i IPv6
- Podpora ACL na protokolu IPv4 a IPv6
- Podpora SSH/SSL
- Podpora filtrování MAC adres
- Podpora IEEE 802.1x

#### **D.1.9 Implementace LAN přepínače typu 1**

- fyzická montáž
- aktualizace firmware
- zapojení do stávající infrastruktury cca 10 přepínačů
- L2 konfigurace
- Konfigurace managementu (SSH, HTTPS, NTP)

#### **D.1.10 LAN přepínač typ 2 (povinné minimální parametry)**

- Velikost 1U do racku 19"
- Vrstvy L2 a L3 (pracuje na 2. a 3. vrstvě modelu OSI), plně spravovatelný
- Výkon PoE min. 370W PoE+
- Počet portů min. 48 RJ-45 100/1000 Mb/s
- Počet SFP portů min. 4
- Kapacita přepínání min. 104 Gb/s
- Datový tok min. 77 milionů paketů/s
- Velikost tabulky MAC adres min. 32 000 záznamů
- Vlastnosti přepínače:
- Podpora plnohodnotné správy přes IPv4 a IPv6 rozhraní.
- Podpora statického L3 směrování mezi VLANnami.
- Podpora dynamického routingu skrze protokoly RIP, OSPFv2 a OSPFv3.
- SNMP verze 2c a 3.
- Quality of Service (QoS).
- Multiple spanning tree.
- Podpora spanning tree instance per VLAN s 802.1Q tagováním BPDU rámců.
- Podpora protokolu MVRP pro administraci a distribuci VLAN.
- Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty.
- Monitoring datových toků v síti pomocí sFlow.
- Software REST API pro automatizaci nastavení sítě.
- Podpora technologie VxLAN
- Podpora standardu 802.1v
- Podpora OpenFlow
- Podpora ACL na protokolu IPv6
- Podpora SSH/SSL
- Podpora filtrování MAC adres
- Podpora IEEE 802.1x
- Podpora aktivního monitorování RADIUS serveru přednastaveným jménem a heslem.

- Podpora RADIUS MAC autentizace, která probíhá před 802.1x autentizací pro případy, že koncové zařízení není softwarově vybaveno pro 802.1x autentizaci.
- Podpora RADIUS Change of Authorization (RFC3576).
- RA guard, DHCPv6 protection
- IPv6 ND snooping.
- Private VLAN.

#### **D.1.11 Implementace LAN přepínače typu 2**

- fyzická montáž
- aktualizace firmware
- zapojení do stávající infrastruktury cca 10 přepínačů
- L3 konfigurace, cca 10 VLAN
- Konfigurace managementu (SSH, HTTPS, NTP)

#### **D.1.12 Bezdrátový přístupový bod (povinné minimální parametry)**

- Současná funkce AP v pásmu 2,4 GHz i 5GHz
- Min. 3x3 MIMO
- izolace klientů
- Podpora 802.11 a/g/n/ac, ac Wave 2
- podpora PoE, VLAN, multi SSID
- ACL pro filtrování provozu
- podpora zabezpečení: WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP nebo AES)
- Podpora 802.1x resp. ověřování Wi-Fi uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD ...)
- Centralizovaná architektura správy wifi sítě (centrální řadič, centrální management, tzv. thin access pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení)
- Minimálně pasivní zapojení do federovaného systému eduroam ([www.eduroam.cz](http://www.eduroam.cz)). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů
- Držák pro uchycení dodaných AP na zeď

#### **D.1.13 Implementace bezdrátových přístupových bodů**

- Návrh topologie Wi-Fi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou ve v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů
- Montáž AP na zeď
- Zapojení, oživení, aktualizace firmware
- Implementace centralizované architektury WiFi řešení
- 5 SSID

#### **D.1.14 PoE injektor (povinné minimální parametry)**

- IEEE 802.3af PoE



## E. Příloha

### E.1 Simulace šíření Wi-Fi signálů

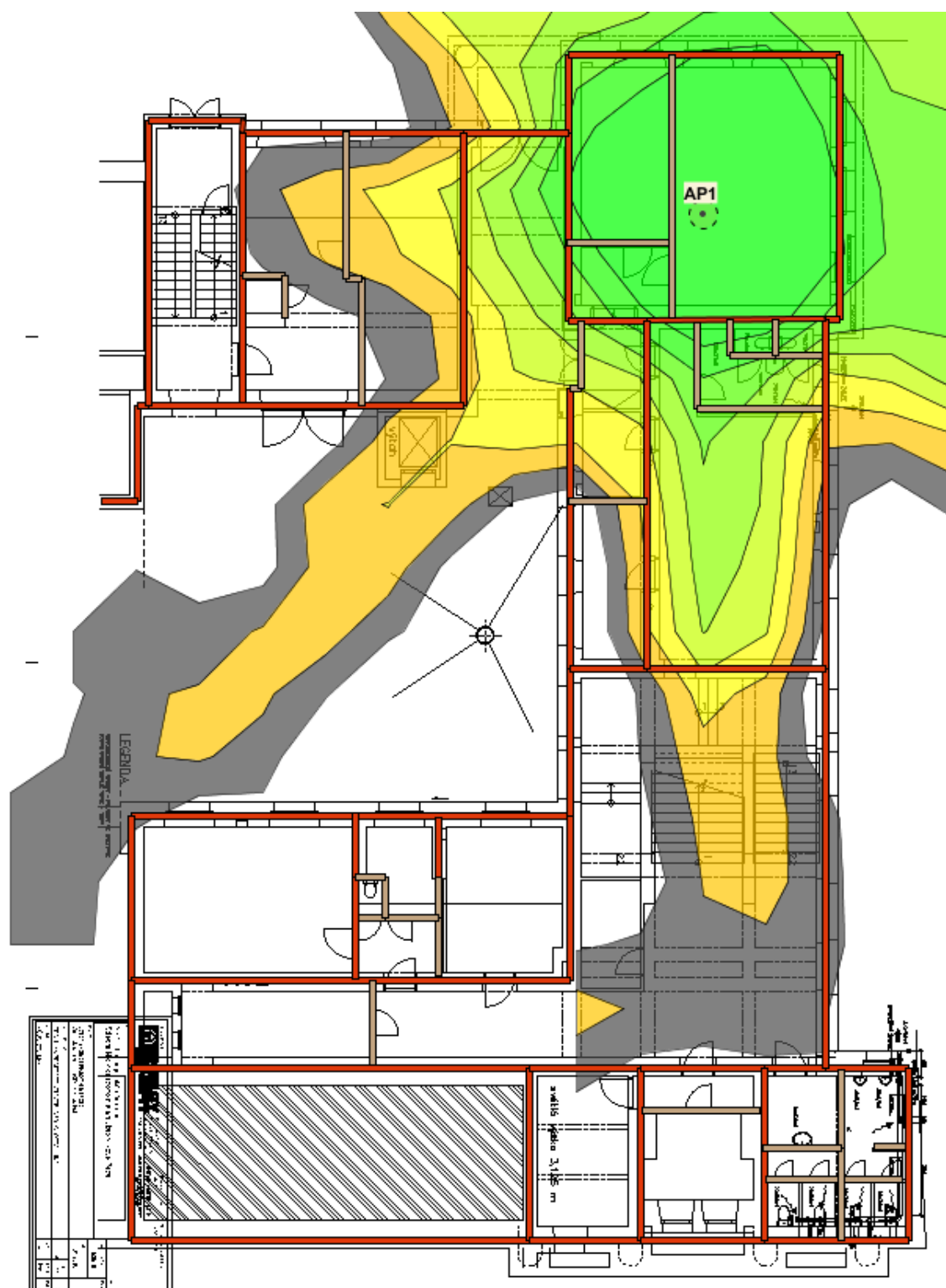
Na obrázcích níže je výstup ze simulace šíření Wi-Fi signálu pro pásmo 2,4 i 5GHz. Je zobrazena síla signálu v jednotkách dBm.

Pro účely simulace byli zvoleny následující hodnoty

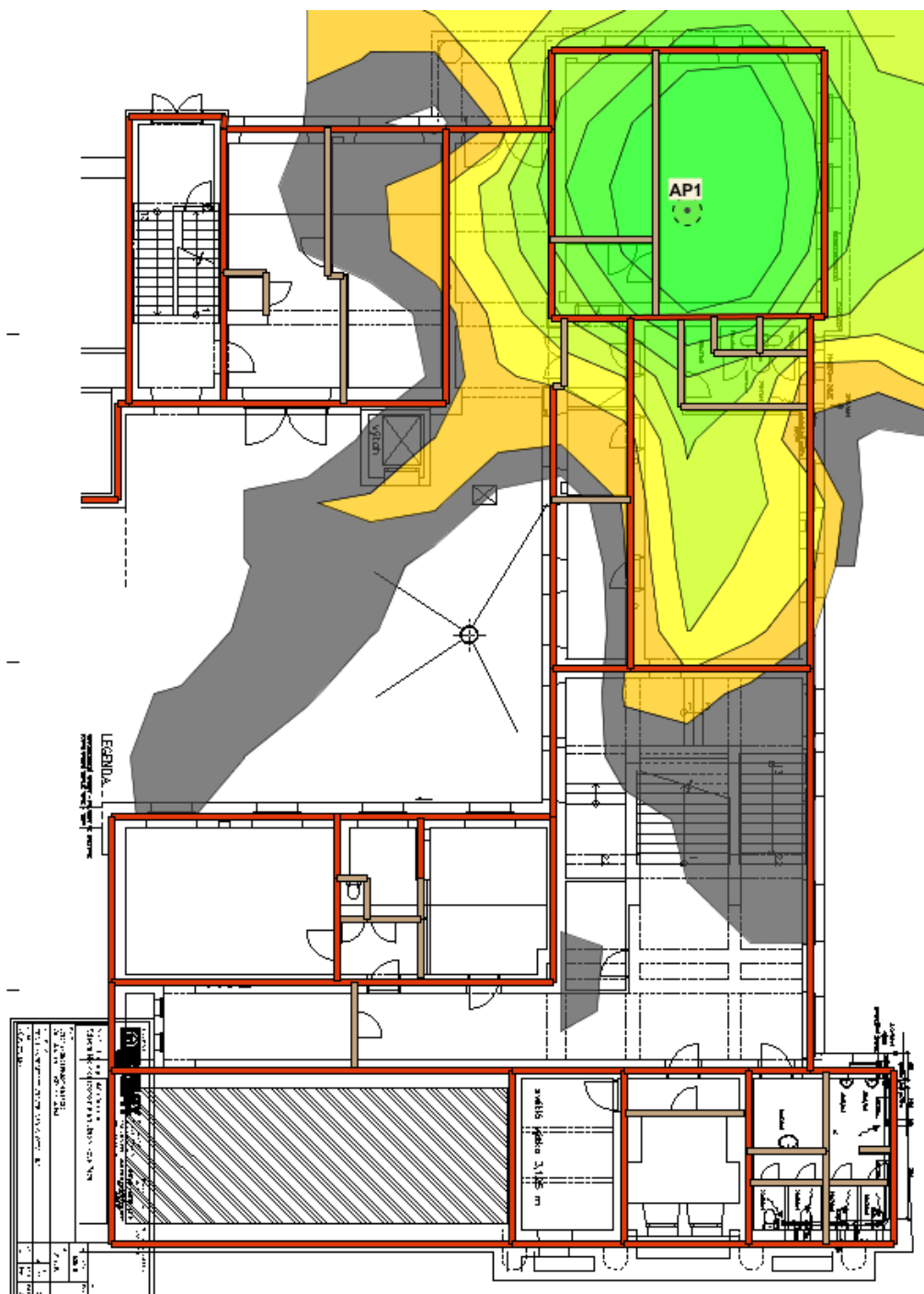
- Typ bezdrátového přístupového bodu: Meraki MR32
- Vysílací výkon: 25mW
- Útlum zdiva:
  - Červená – 10dB
  - Hnědá – 3dB
- Ořez síly signálu (znázorněn šedivou barvou): -75dBm



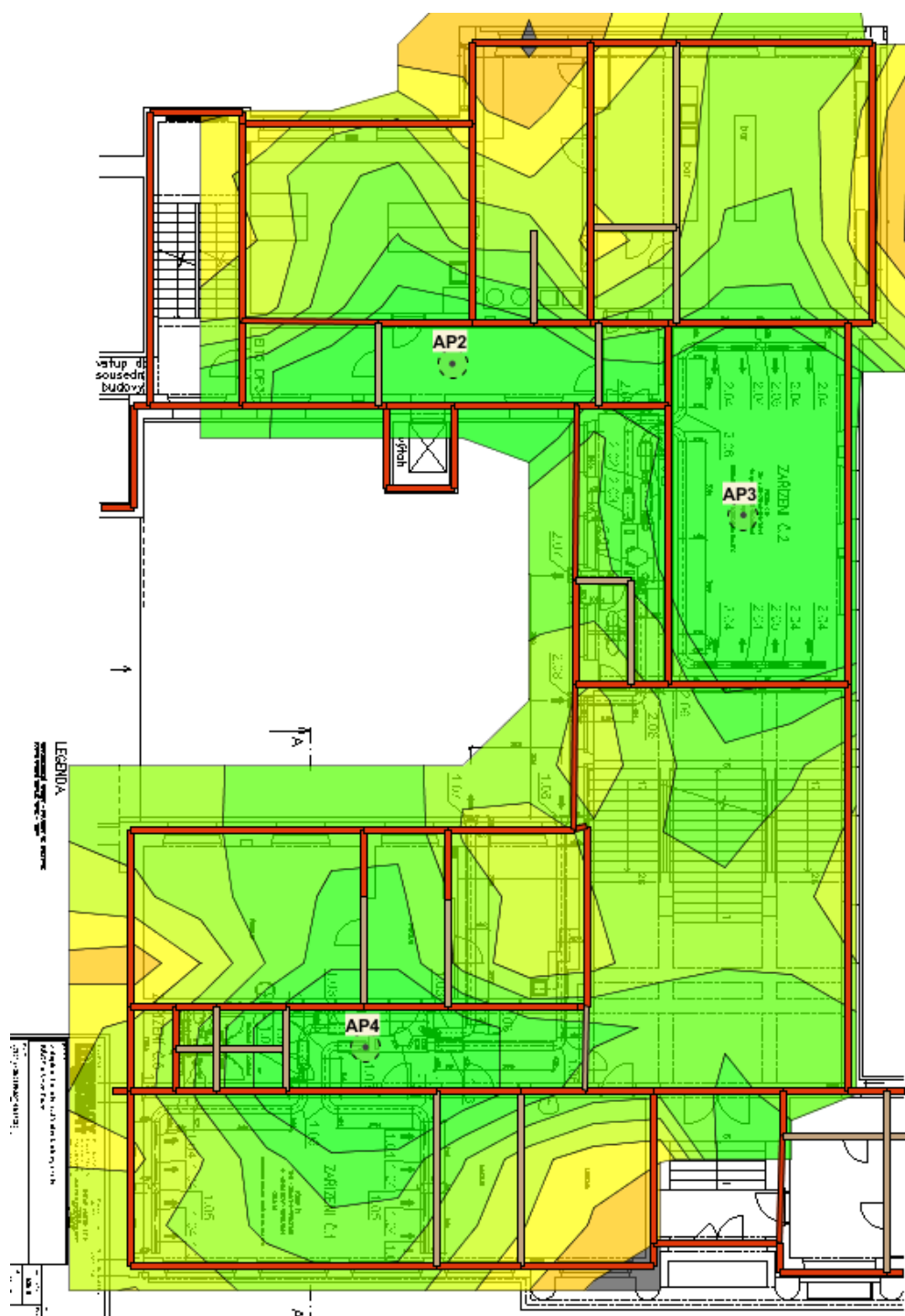
Obr. 6 Legenda síly signálu RSSI



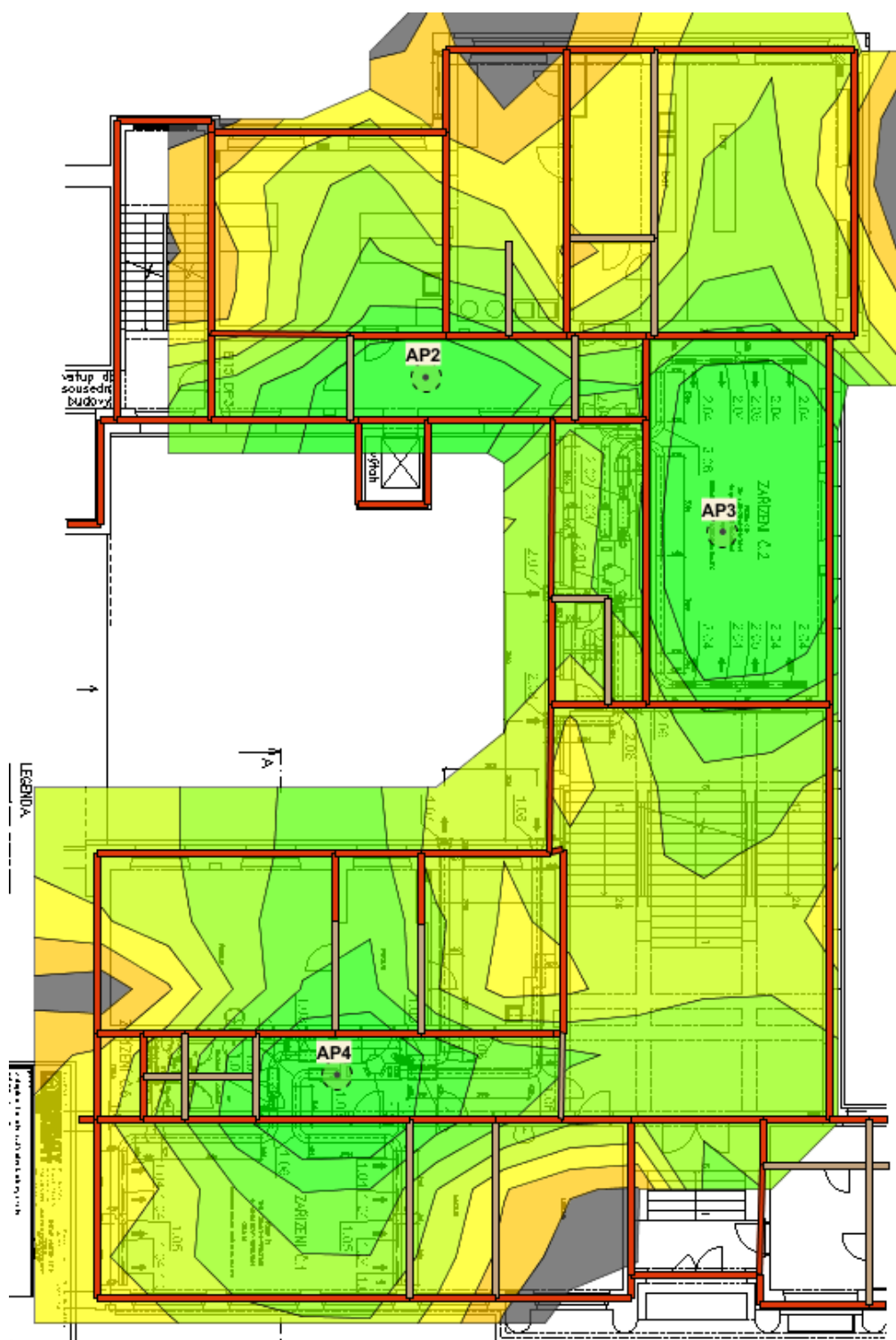
Obr. 7 Hlavní budova – 1.PP – síla signálu RSSI pro 2,4GHz



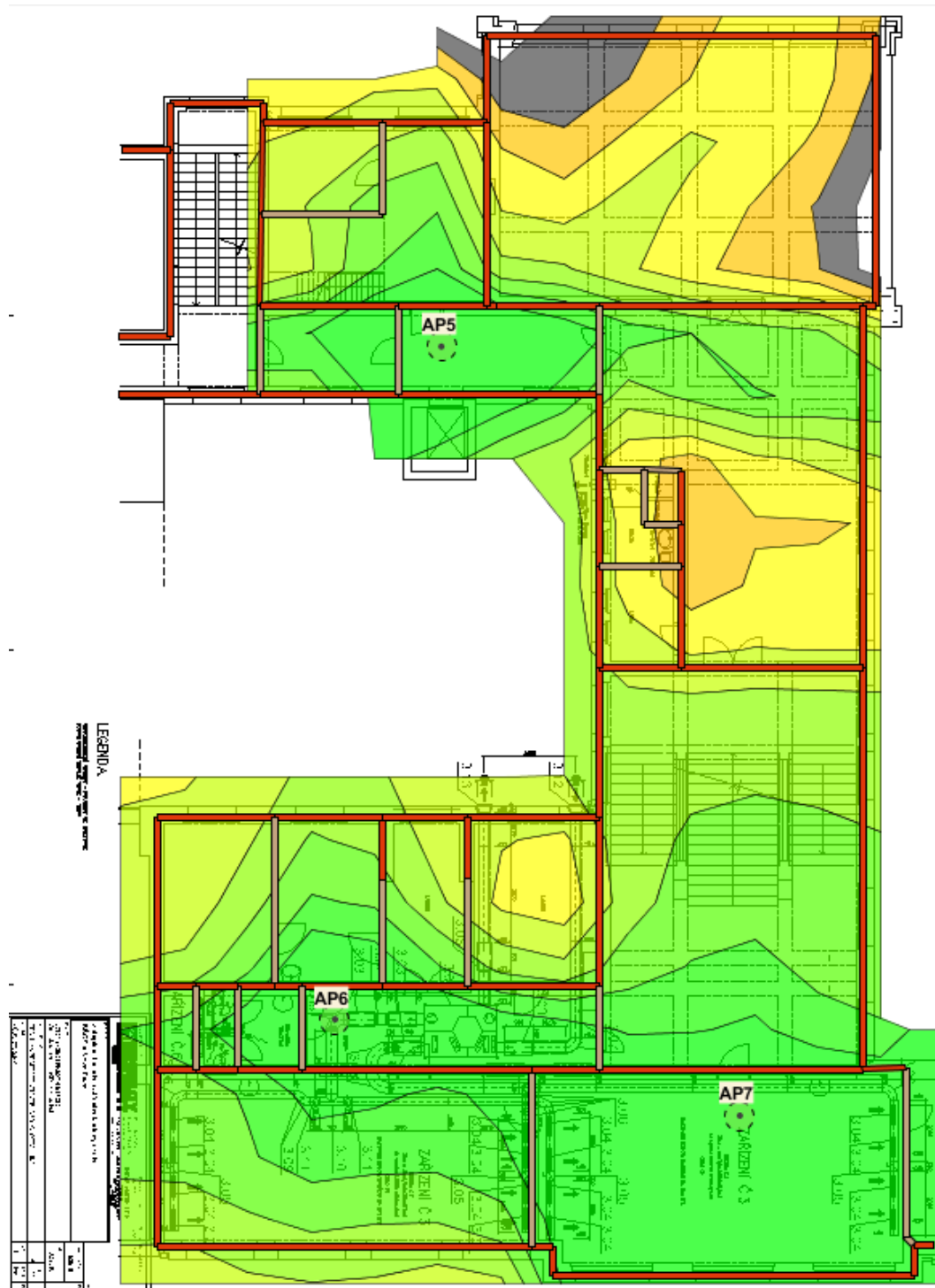
Obr. 8 Hlavní budova – 1.PP – síla signálu RSSI pro 5GHz



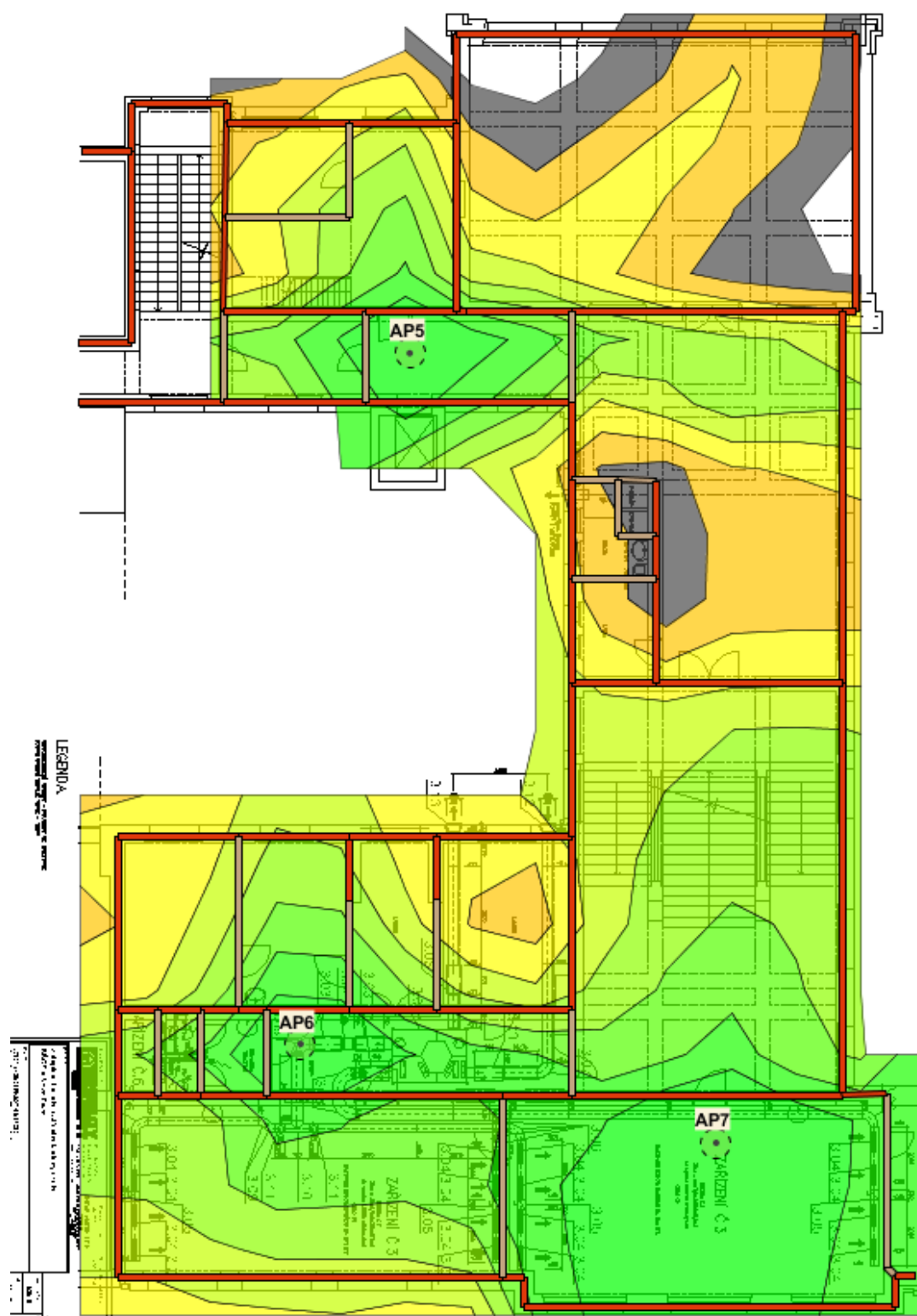
Obr. 9 Hlavní budova – 1.NP – síla signálu RSSI pro 2,4GHz



Obr. 10 Hlavní budova – 1.NP – síla signálu RSSI pro 5GHz



Obr. 11 Hlavní budova – 2.NP – síla signálu RSSI pro 2,4GHz

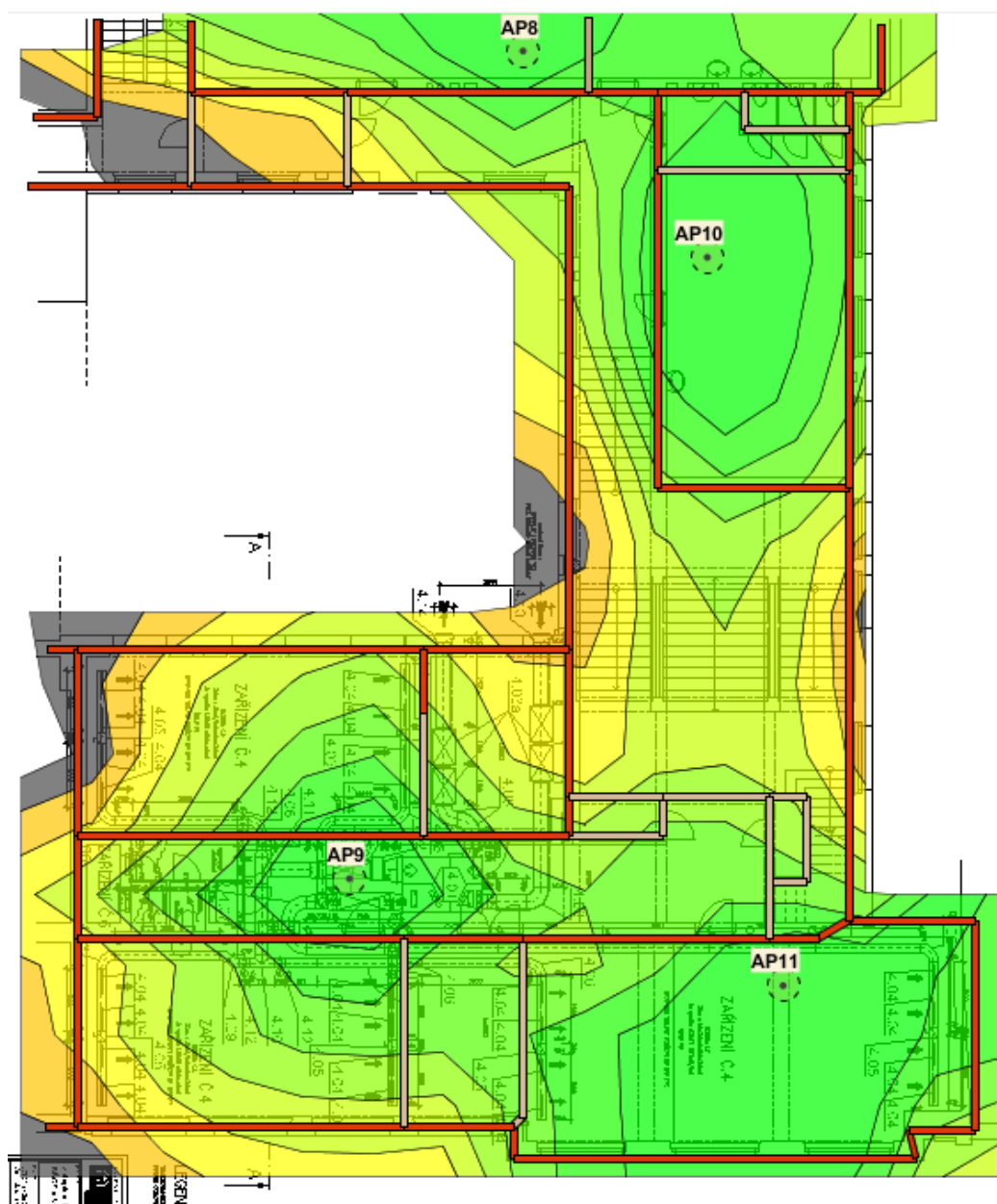


Obr. 12 Hlavní budova – 2.NP – síla signálu RSSI pro 5GHz

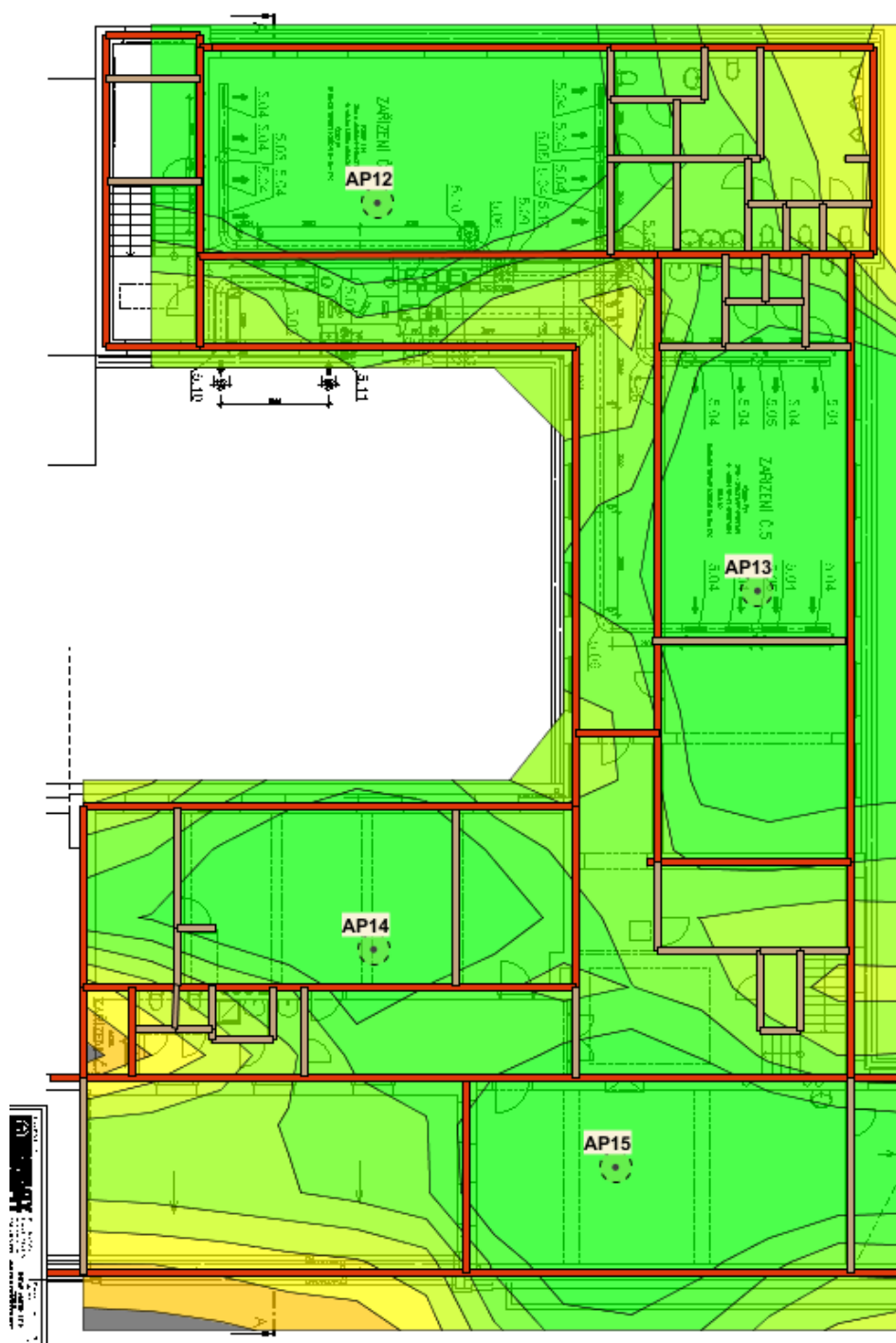


Obr. 13 Hlavní budova – 3.NP – síla signálu RSSI pro 2,4GHz

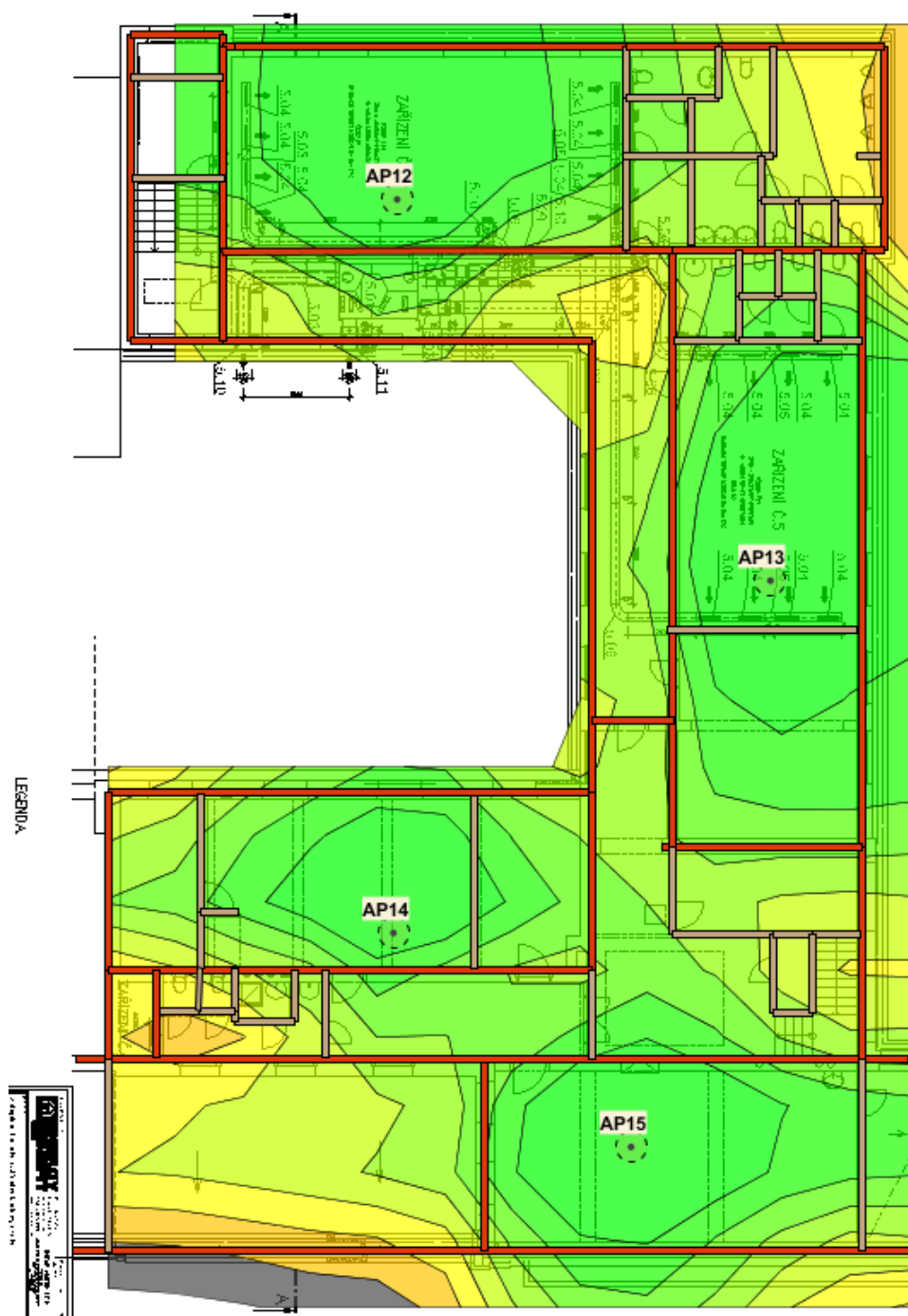




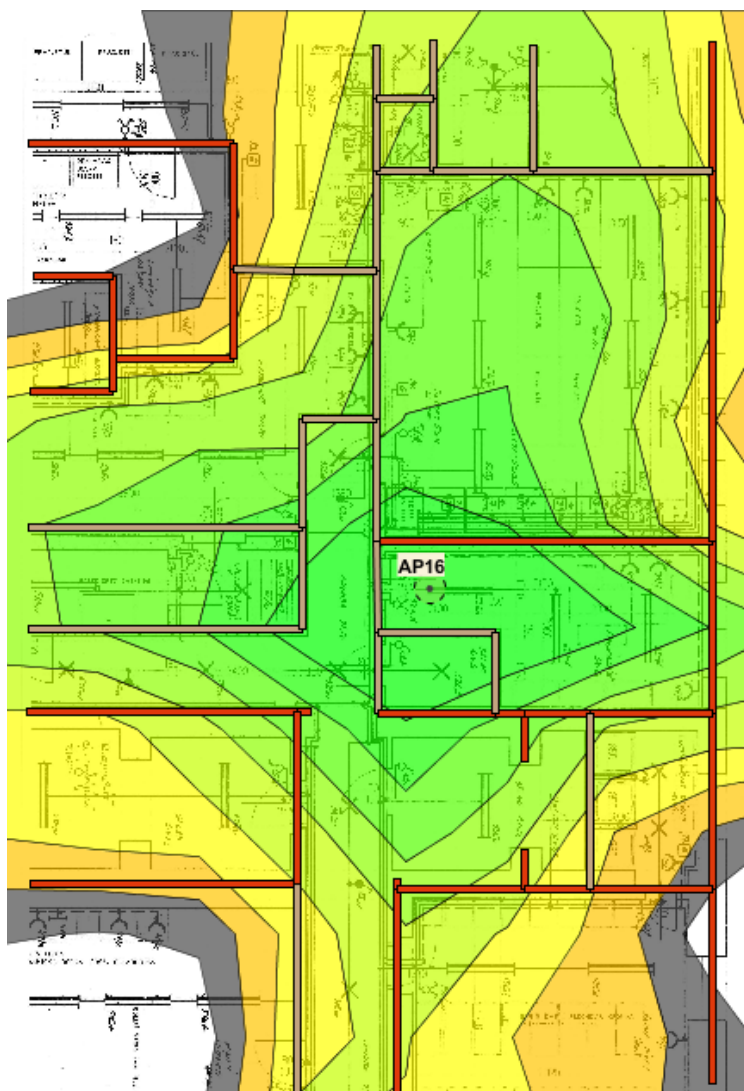
Obr. 14 Hlavní budova – 3.NP – síla signálu RSSI pro 5GHz



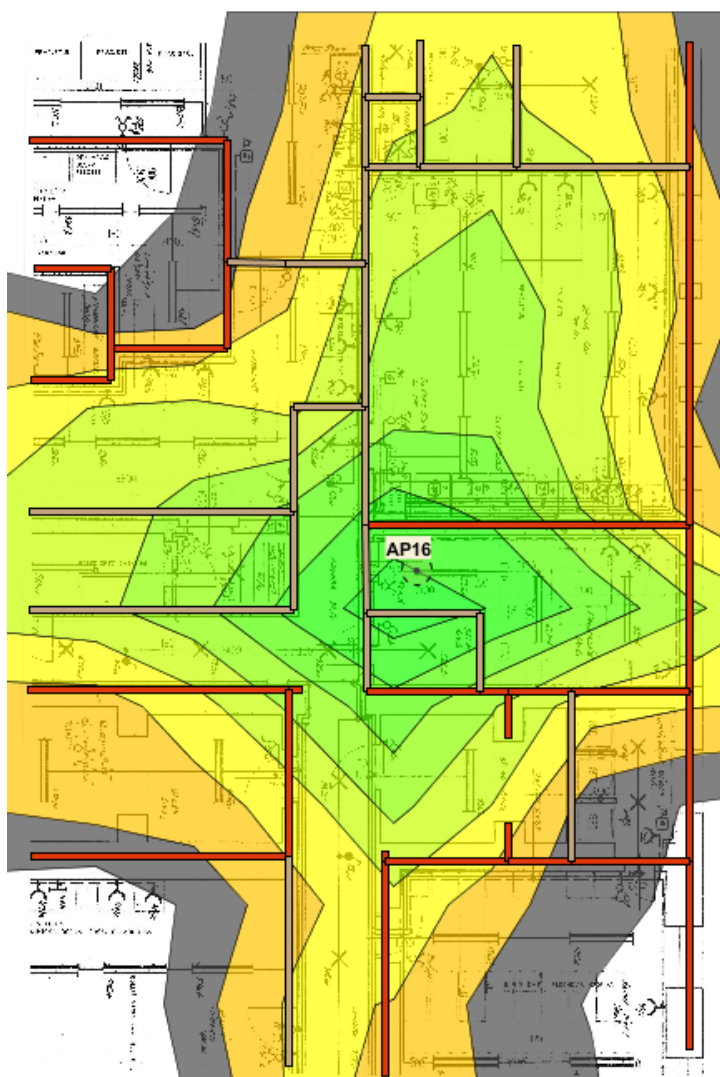
Obr. 15 Hlavní budova – 4.NP – síla signálu RSSI pro 2,4GHz



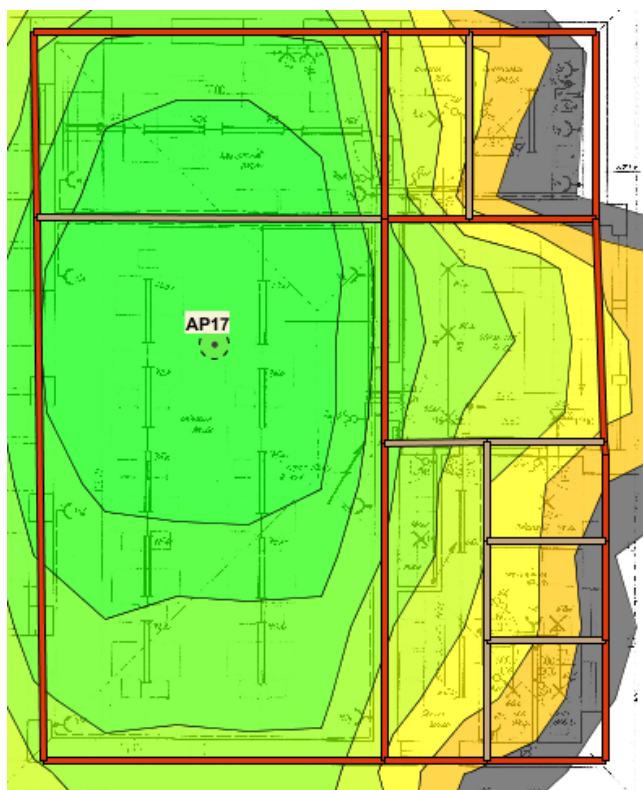
Obr. 16 Hlavní budova – 4.NP – síla signálu RSSI pro 5GHz



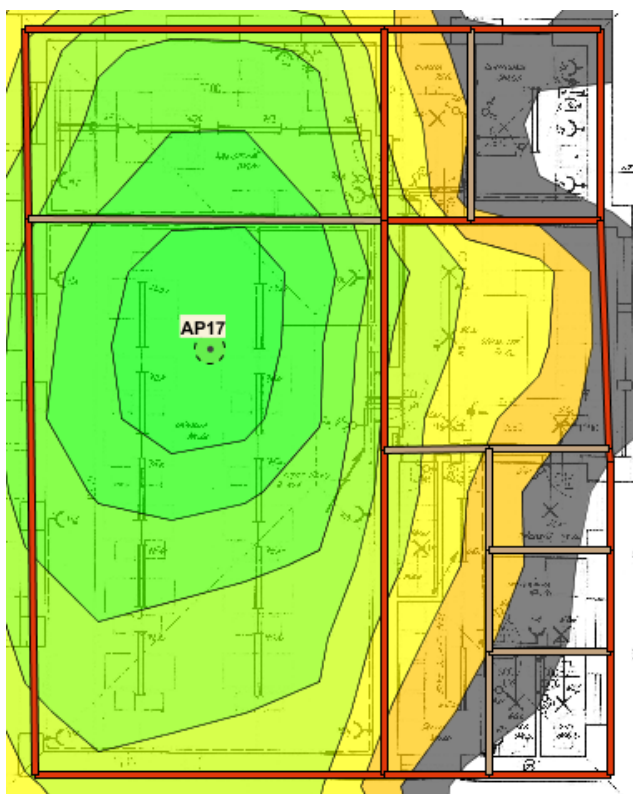
*Obr. 17 Cukrářská dílna – 0.NP – síla signálu RSSI pro 2,4GHz*



Obr. 18 Cukrářská dílna – 0.NP – síla signálu RSSI pro 5GHz



*Obr. 19 Cukrářská dílna – 1.NP – síla signálu RSSI pro 2,4GHz*



Obr. 20 Cukrářská dílna – 0.NP – síla signálu RSSI pro 5GHz