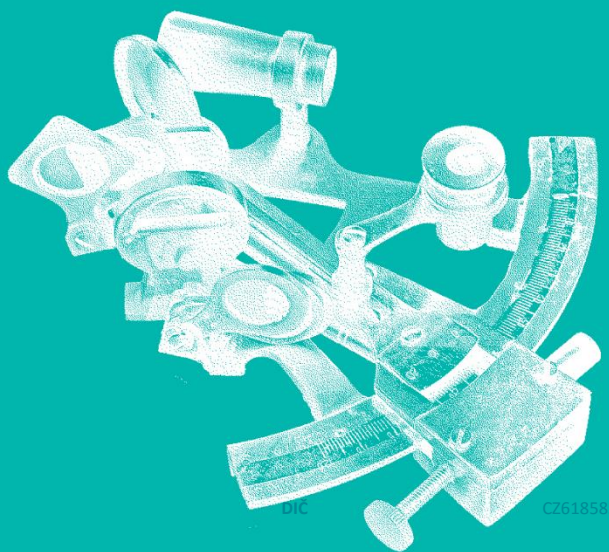
ZAJIŠTĚNÍ KONEKTIVITY DO ŠKOL - PROJEKTOVÁ DOKUMENTACE – AKTIVNÍ PRVKY

Střední škola technická a řemeslná Nový Bydžov



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

WWW.ALEF.COM PRAGUE — BRATISLAVA — BUDAPEST

Obsah

Úvod

Projektová dokumentace je zpracována pro SŠTŘ Nový Bydžov, sídlící na adrese Dr. M. Tyrše 112, Nový Bydžov. Jedná se o modernizaci dílenského areálu školy sídlící na adrese Na Švarcavě, Nový Bydžov. Cílem je ověřit a vydefinovat, jak je splněno zadávání výzvy č. 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

IDENTIFIKAČNÍ ÚDAJE

ÚDAJE O STAVBĚ

Název objektu: **Střední škola technická a řemeslná Nový Bydžov**
Dotčené objekty:

- objekt dílenský areál – Na Švarcavě, Nový Bydžov, katastrální území Nový Bydžov, parcelní čísla 1365/1, 1365/2, 1365/3 a 1268/1

ÚDAJE O STAVEBNÍKOVI

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

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

SEZNAM VSTUPNÍCH PODKLADŮ

Projektová dokumentace vznikla na základě těchto podkladů:

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

ÚDAJE O ÚZEMÍ

Objekt	Katastrální území
Objekt dílenský areál - Na Švarcavě, Nový Bydžov	katastrální území Nový Bydžov, parcelní čísla 1365/1, 1365/2, 1365/3 a 1268/1

B. SOUHRNNÁ TECHNICKÁ ZPRÁVA

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

VÝCHOZÍ STAV

V dílenském areálu je aktuálně 110 žáků. Konektivita pro dílenský areál je 5 Mbit/s pro příchozí i odchozí směr internetového provozu, agregace 1:1, bez FUP. Poskytovatelem internetového připojení je p. Ing. David Bendák. V současné době jsou poskytovatelem internetu přidělovány pouze IPv4 adresy.

Dílenský areál je aktuálně celý vyklizen, probíhá zde rekonstrukce, proto bude celá lokální síť budována od nuly.

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 110 je potřeba zajistit internetové připojení alespoň 15 Mbit/s pro oba směry provozu.

Jelikož se celá lokální síť buduje na zelené louce, tak je třeba zajistit implementaci RADIUS serveru, který bude sloužit pro bezpečný přístup žáků do lokální sítě. Zároveň provést konfiguraci a integraci do systému Eduroam pro mobilitu žáku a učitelů. Dále je třeba nasadit centrální databáze identit, jako je například Active Directory.

Aktuální poskytovatel internetového připojení neposkytuje IPv6 adresy a nesplňuje podmínky bezpečnostního projektu FENIX.

Technické řešení projektu

Níže je v jednotlivých částech popsán technický návrh řešení projektu.

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 110 je potřeba zajistit internetové připojení alespoň 15 Mbit/s pro oba směry provozu. Konektivita dílenského areálu bude realizována samostatně, bude oddělená od zbytku sítě školy.

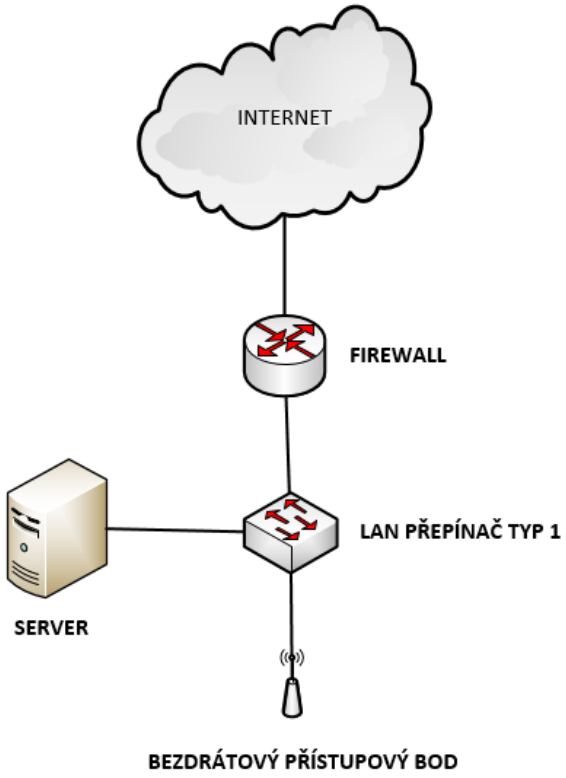
Dle výzvy musí být poskytovatel internetu součástí bezpečnostního projektu FÉNIX nebo alespoň splňovat jeho technické požadavky. Hlavní výhody pro školu jsou takové, že poskytovatel internetu provozuje redundantní a nepřetížené linky do nejméně dvou uzlů NIX.CZ. Má dohledové středisko fungující v režimu 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.

Interní LAN

Navržená infrastruktura se skládá z následujících částí:

- Firewall
- LAN přepínače
- Bezdrátové přístupové body
- Sonda
- Server
- UPS

Na perimetru sítě je zamýšlen firewall, do kterého je připojen distribuční LAN přepínač typ 1, který se bude starat o směrování VLAN a připojení serveru. Bezdrátové přístupové body budou napájeny přes PoE.



OBR. 1 BLOKOVÉ SCHÉMA SÍTĚ

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.

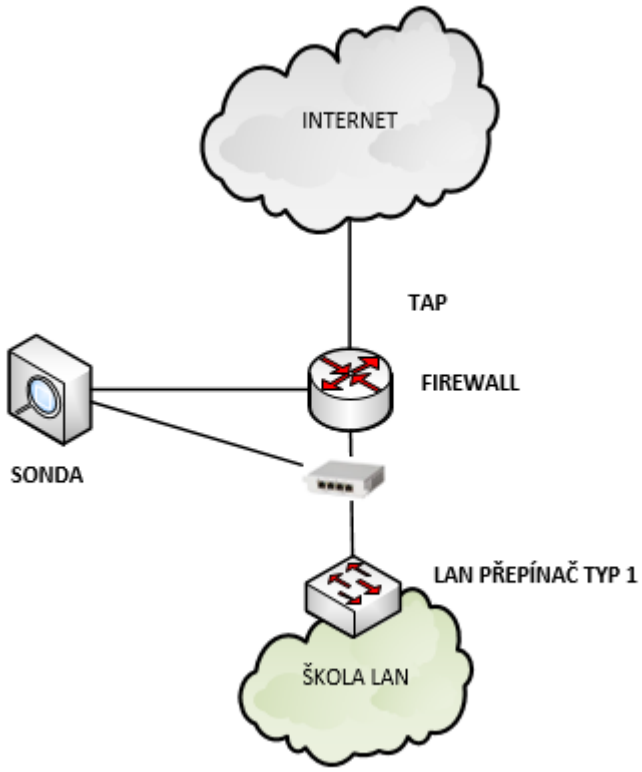
Řešení zahrnuje následující komponenty:

- 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 k distribučnímu LAN přepínači typu 1. Pro analýzu toků je doporučené monitorovat obě tyto linky. Avšak lze řešení zjednodušit a monitorovat pouze jednu linku na LAN síti. V takovém designu je třeba počítat s tím, že

veškerý uživatelský provoz by měl být NATován (překládán) na jednu veřejnou IP adresu, tak aby byla splněna podmínka o logování NAT. Potom není třeba monitorovat provoz vně firewallu.

Monitoring linky bude prováděn pomocí jednoho metalického TAPu, který bude sbírat data z obou směrů a zrcadlit agregovaný provoz do sondy, která bude zároveň provádět sběr dat. Tato sonda bude nasbíraná data uchovávat a na vyžádání generovat reporty o uživatelské aktivitě v čase.

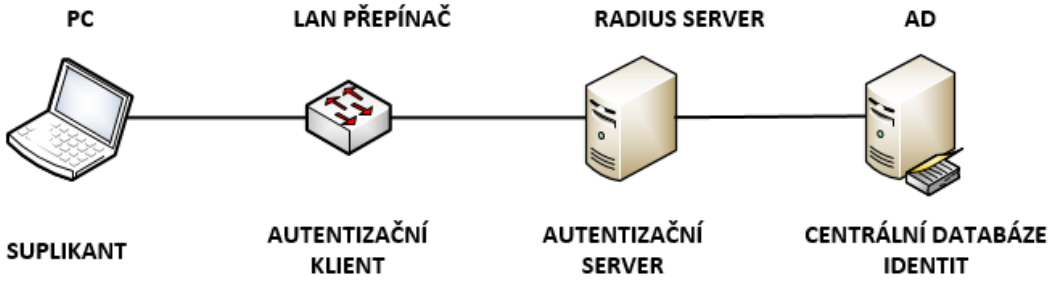


OBR. 2 BLOKOVÉ SCHÉMA PRO ANALÝZU SÍŤOVÉHO PROVOZU

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. 3 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.

Jako centrální databázi identit doporučujeme použít systém Microsoft Active Directory.

Autentizační server navrhujeme řešit na službě NPS (Network Policy Server), která bude nainstalována na serveru se systémem MS Windows Server a která 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.

Zapojení do systému Eduroam

Dle znění výzvy č. 33 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).

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.

Počty zařízení v jednotlivých objektech

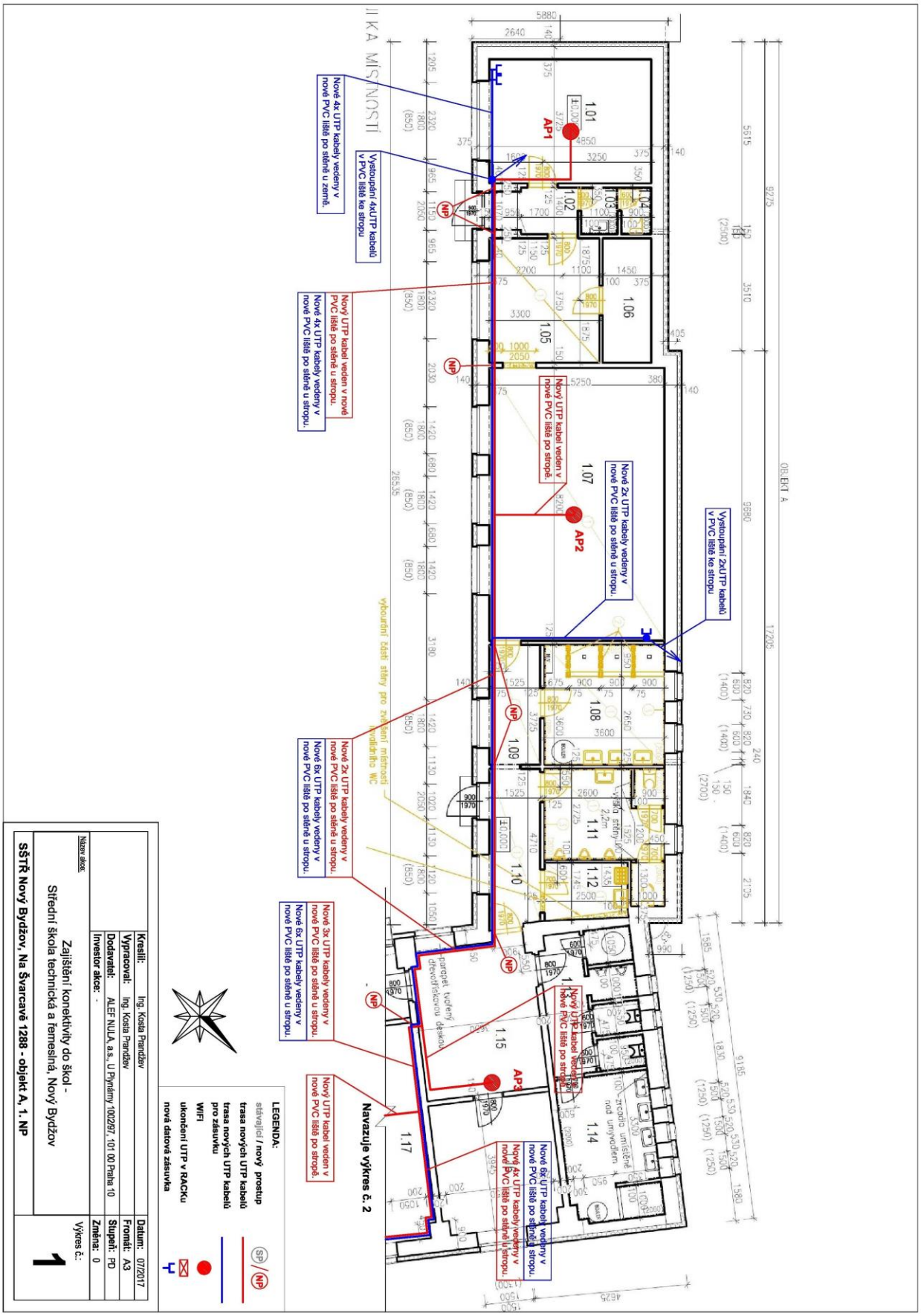
Počet zařízení, které budou umístěny v dílenském areálu, je uveden v tab. 1.

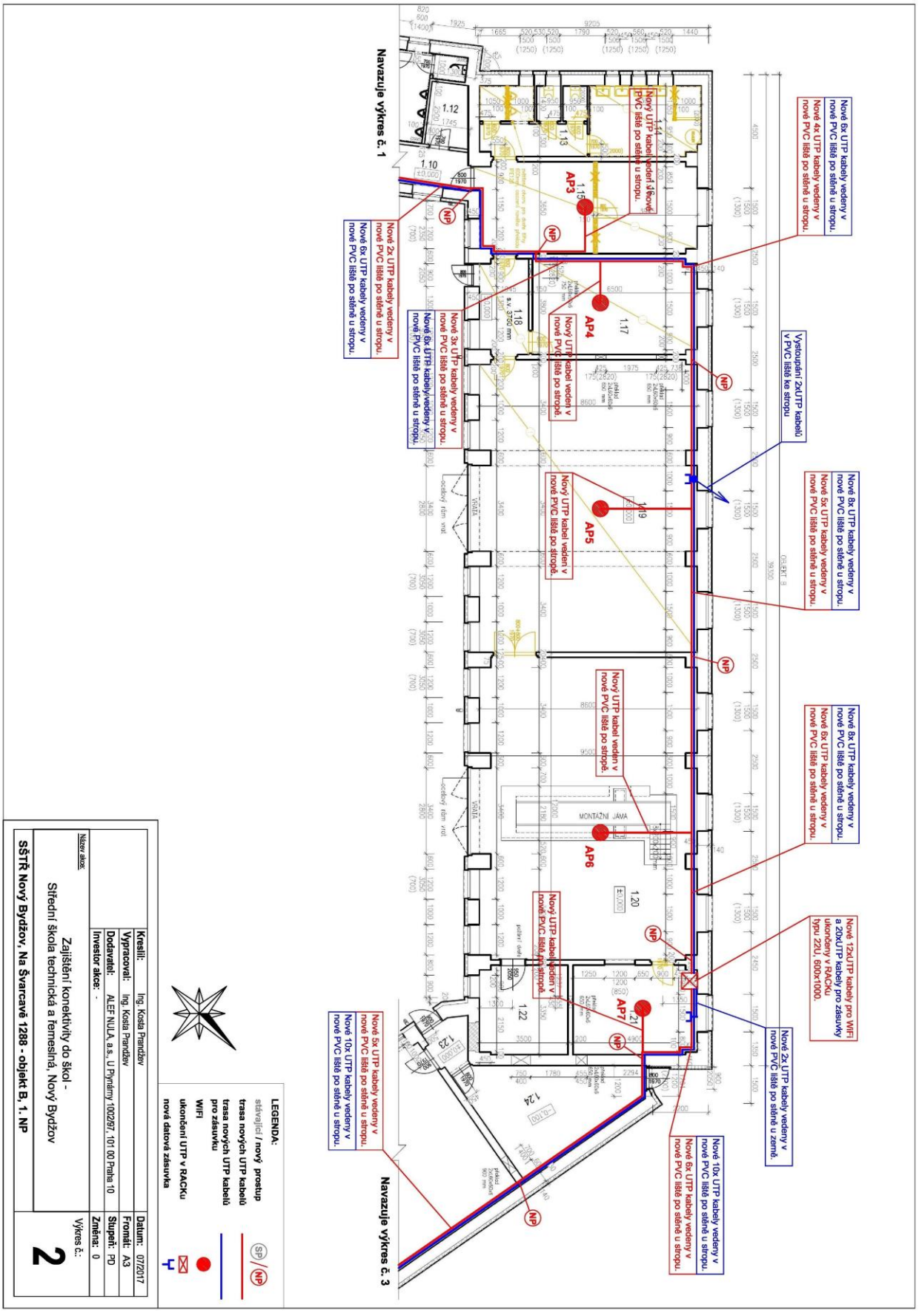
Název	Počet
Firewall	1
LAN přepínač typ 1	2
Bezdrátový přístupový bod	12
Server	1
Sonda	1
Metalický TAP	1
UPS	1

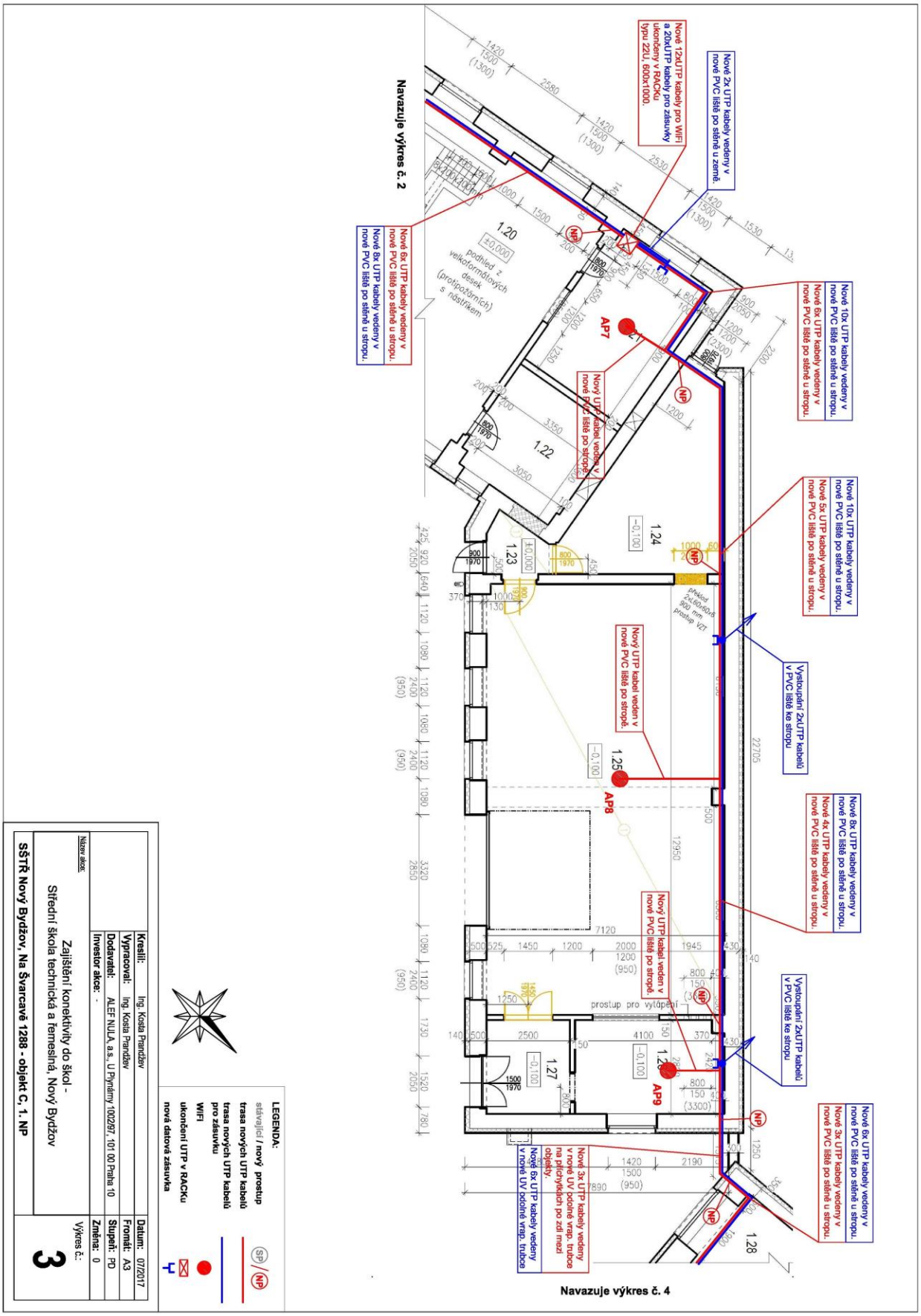
TAB. 1 POČET ZAŘÍZENÍ

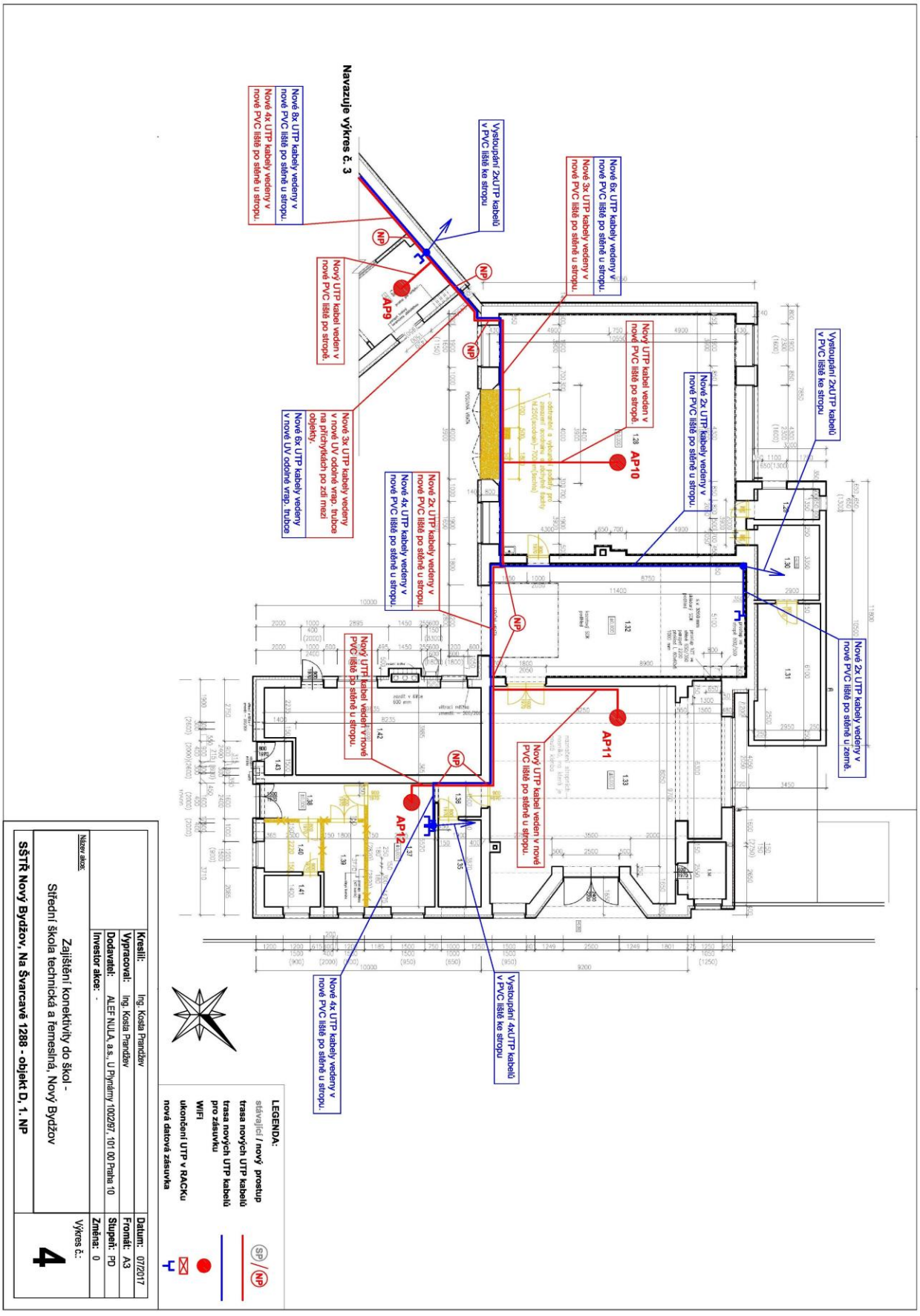
C. SITUAČNÍ VÝKRESY

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.


AP1
AP2
AP3
1.01
1.02
1.03
1.04
1.05
1.06
1.07
1.08
1.09
1.10
1.11
1.12
1.14
1.15
1.17
OBJEKT A
Nové 4x UTP kabely vedeny v nové PVC liště po stěně u země.
Vystoupání 4xUTP kabelů v PVC liště ke stropu
Nový UTP kabel veden v nové PVC liště po stěně u stropu.
Nové 4x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nový UTP kabel veden v nové PVC liště po stropě.
Nové 2x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Vystoupání 2xUTP kabelů v PVC liště ke stropu
Nové 2x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 6x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 3x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 6x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nový UTP kabel veden v nové PVC liště po stropě.
Nové 6x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 4x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Navazuje výkres č. 2
LEGENDA:
stávající / nový prostup
trasa nových UTP kabelů
trasa nových UTP kabelů pro zásuvku
WiFi
ukončení UTP v RACKu
nová datová zásuvka
Kreslil: Ing. Kosta Prandžav
Vypracoval: Ing. Kosta Prandžav
Dodavatel: ALEF NULA, a.s., U Plynárny 1002/97, 101 00 Praha 10
Investor akce: -
Název akce:
Zajištění konektivity do škol -
Střední škola technická a řemeslná, Nový Bydžov
SŠTŘ Nový Bydžov, Na Švarcavě 1288 - objekt A, 1. NP
Datum: 07/2017
Formát: A3
Stupeň: PD
Změna: 0
Výkres č.:
1


Navazuje výkres č. 1
Navazuje výkres č. 3
Nové 6x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 4x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nový UTP kabel veden v nové PVC liště po stěně u stropu.
Nové 2x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 6x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 3x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 6x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nový UTP kabel veden v nové PVC liště po stropě.
Vystoupání 2xUTP kabelů v PVC liště ke stropu
Nové 8x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 5x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nový UTP kabel veden v nové PVC liště po stropě.
Nové 8x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 6x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nový UTP kabel veden v nové PVC liště po stropě.
Nové 12xUTP kabely pro WiFi a 20xUTP kabely pro zásuvky ukončeny v RACKu typu 22U, 600x1000.
Nový UTP kabel veden v nové PVC liště po stropě.
Nové 2x UTP kabely vedeny v nové PVC liště po stěně u země.
Nové 5x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 10x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 6x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 10x UTP kabely vedeny v nové PVC liště po stěně u stropu.
AP3
AP4
AP5
AP6
AP7
MONTÁŽNÍ JÁMA
LEGENDA:
stávající / nový prostup
trasa nových UTP kabelů
trasa nových UTP kabelů pro zásuvku
WiFi
ukončení UTP v RACKu
nová datová zásuvka
Kreslil: Ing. Kosta Prandžav
Vypracoval: Ing. Kosta Prandžav
Dodavatel: ALEF NULA, a.s., U Plynárny 1002/97, 101 00 Praha 10
Investor akce: -
Název akce:
Zajištění konektivity do škol -
Střední škola technická a řemeslná, Nový Bydžov
SŠTŘ Nový Bydžov, Na Švarcavě 1288 - objekt B, 1. NP
Datum: 07/2017
Formát: A3
Stupeň: PD
Změna: 0
Výkres č.:
2


Navazuje výkres č. 2
Nové 12xUTP kabely pro WiFi a 20xUTP kabely pro zásuvky ukončeny v RACKu typu 22U 600x1000.
Nové 2x UTP kabely vedeny v nové PVC liště po stěně u země.
Nové 6x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 8x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 10x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 5x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 4x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 3x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nový UTP kabel veden v nové PVC liště po stropě.
Vystoupání 2xUTP kabelů v PVC liště ke stropu.
Nové 3x UTP kabely vedeny v nové UV pódiové vrap. trubce na přípichytkách po zdi mezi objekty.
Nové 6x UTP kabely vedeny v nové UV pódiové vrap. trubce
1.20
podhled z velkoformátových desek (protipožárních) s nástřikem
1.22
1.23
1.24
1.25
1.26
1.27
1.28
AP7
AP8
AP9
prostup pro vytápění
Navazuje výkres č. 4
LEGENDA:
stávající / nový prostup
trasa nových UTP kabelů
trasa nových UTP kabelů pro zásuvku
WiFi
ukončení UTP v RACKu
nová datová zásuvka
Kreslil: Ing. Kosta Prandžav
Vypracoval: Ing. Kosta Prandžav
Dodavatel: ALEF NULA, a.s., U Plynárny 1002/97, 101 00 Praha 10
Investor akce: -
Název akce:
Zajištění konektivity do škol - Střední škola technická a řemeslná, Nový Bydžov
SŠTŘ Nový Bydžov, Na Švarcavě 1288 - objekt C, 1. NP
Datum: 07/2017
Formát: A3
Stupeň: PD
Změna: 0
Výkres č.:
3


Navazuje výkres č. 3
Nové 8x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 4x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Vystoupání 2xUTP kabelů v PVC liště ke stropu
Nové 6x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 3x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nový UTP kabel veden v nové PVC liště po stropě.
Nové 2x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 3x UTP kabely vedeny v nové UV odolné vrap. trubce na přichytávačích po zdi mezi objekty.
Nové 6x UTP kabely vedeny v nové UV odolné vrap. trubce
Nové 2x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nové 4x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Nový UTP kabel veden v nové PVC liště po stěně u stropu.
Nové 2x UTP kabely vedeny v nové PVC liště po stěně u země.
Nové 4x UTP kabely vedeny v nové PVC liště po stěně u stropu.
Vystoupání 4xUTP kabelů v PVC liště ke stropu
AP9
AP10
AP11
AP12
LEGENDA:
stávající / nový prostup
trasa nových UTP kabelů
trasa nových UTP kabelů pro zásuvku
WiFi
ukončení UTP v RACKu
nová datová zásuvka
Kreslil: Ing. Kosta Prandžav
Vypracoval: Ing. Kosta Prandžav
Dodavatel: ALEF NULA, a.s., U Plynárny 1002/97, 101 00 Praha 10
Investor akce: -
Název akce:
Zajištění konektivity do škol -
Střední škola technická a řemeslná, Nový Bydžov
SŠTŘ Nový Bydžov, Na Švarcavě 1288 - objekt D, 1. NP
Datum: 07/2017
Formát: A3
Stupeň: PD
Změna: 0
Výkres č.:
4

D. DOKUMENTACE OBJEKTŮ A TECHNICKÝCH A TECHNOLOGICKÝCH ZAŘÍZENÍ

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.

FIREWALL (POVINNÉ MINIMÁLNÍ PARAMETRY)

- 4 x Gb RJ45 port
- propustnost FW min. 500 Mbps
- propustnost IPSec VPN (UDP 512B, AES256) min. 150 Mbps
- lokální disková kapacita min. 16 GB, možnost logování na lokální disk nebo na logovací server
- možnost vysoce dostupného zapojení dvou firewallů Active-Active nebo Active-Passive
- statefull firewall
- podpora IPV6 – NAT46, 66, 64
- dynamické směrování pro IPv4 and IPv6 (RIP, OSPF, BGP a Multicast IPv4)
- policy based routing a source based routing
- funkce Load Balancing, WAN optimalizace
- monitoring a logování NAT (RFC 2663)
- logování přístupu uživatelů do Internetu min. IP adresa – čas – uživatel v stávající Microsoft Active Directory
- podpora pro rate limiting
- podpora pro antispoofing
- podpora pro ACL/xACL
- aplikační kontrola (na L7 vrstvě) s propustností min. 200 Mbps
- funkcionalita Antivir (Proxy nebo Flow), Antispyware a Antimalware
- funkcionalita Web filter - kontrola http a https provozu, kategorizace a selekce obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirová kontrola stahovaného obsahu
- integrace s Active Directory pro SSO
- funkcionalita IPS s propustností min. 200 Mbps
- SSL inspekce
- min. 5 virtuálních firewallů s oddělenou konfigurací a správou
- integrovaná 2faktorová autentizace klientů VPN či administrátorů firewallu bez nutnosti využívat další software
- správa přes min. HTTPS, SSH
- snadná konfigurace ACL/FW na základě identifikovaných útoků přes webové rozhraní
- licencování na neomezený počet uživatelů
- pravidelné automatické aktualizace signatur od výrobce
- dostupnost bezpečnostních aktualizací po celou dobu udržitelnosti projektu (5 let)
- Požadujeme novou konfiguraci, (cca 10 NAT pravidel, Antivir, WebFilter) na nově dodaný firewall.
- Součástí konfigurace bude vazba na ActiveDirectory (cca 90 uživatelů), konfigurace SSL offloading, IPS/Aplikační kontrola a vzdáleného přístupu.

SERVER (POVINNÉ MINIMÁLNÍ PARAMETRY)

CPU	min. na úrovni Xeon E5-2620v4 8C
CPU patic	2
RAM obsazeno	16 GB
RAM slotů	12 na CPU
Cache battery backup	ANO
Cache na řadiči	ANO 2GB

Ethernet	4x 1GE
HDD formát	2,5"
HDD hot plug	Ano
HDD technologie	SAS/SATA
počet HDD	8
Osazeno HDD	4 ks 1TB Hotplug 2.5in
Optická mechanika	ANO
PCI-e sloty	Ano
PCI-X sloty	ANO
PCI sloty	Ne
Pozice pro další zdroj	Ano
Provedení	RACK
RAID řadič	RAID 0,1,5,6,10
Vzdálená správa	Ano
Zdroj hot plug	Ano
Počet zdrojů	2
Osazeno zdrojů	2 ks

SONDA PRO MONITOROVÁNÍ SÍŤOVÉHO PROVOZU (POVINNÉ MINIMÁLNÍ PARAMETRY)

- Počet monitorovacích portů: min. 1 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)

LOGOVÁNÍ PŘÍSTUPU UŽIVATELŮ DO SÍTĚ UMOŽŇUJÍCÍ DOHLEDÁNÍ VAZEB IP ADRESA – ČAS – UŽIVATEL

- Na novém řadiči Microsoft ActiveDirectory bude nastaveno logování přístupu do sítě umožňující dohledání vazeb IP adresa – čas – uživatel

LAN PŘEPÍNAČ TYP 1 (POVINNÉ MINIMÁLNÍ PARAMETRY)

- Do nového rozvaděče budou dodány 2ks L3 přepínačů s podporou PoE s neblokující architekturou přepínacího subsystému (wire speed) a s min. parametry uvedenými níže.
- Na přepínači bude vytvořena L2/L3 konfigurace
- Na přepínači budou nastaveny základní bezpečnostní protokoly min. NTP, SSH, HHTPS. SNMP apod.
- 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. 24 RJ-45 100/1000 Mb/s PoE+
- Počet SFP portů min. 4
- Kapacita přepínání min. 56 Gb/s
- Datový tok min. 41,7 milionů paketů/s
- Velikost tabulky MAC adres min. 32 000 záznamů
- Vlastnosti přepínače:
    - Podpora plnohodnotné správy přes IPv4 a IPv6 rozhraní.
    - Podpora stohování
    - 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
- Bezpečnost:
    - 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).
    - IPv6 ND snooping.
    - Private VLAN.

BEZDRÁTOVÝ PŘÍSTUPOVÝ BOD (POVINNÉ MINIMÁLNÍ PARAMETRY)

- 12ks bezdrátových přístupových bodů (AP)

- Bezdrátová síť bude provozována jako centralizovaná architektura s využitím funkcionality kontroleru na jednom libovolném AP. Tento řídí distribuci konfigurací, rozkládání zátěže, roaming, ladění kanálů, detekci rušení a jeho funkcionalitu může v případě HW poruch převzít jiné AP.
- Podporou automatického rozložení zátěže klientů
- AP musí splňovat specifikaci 802.11a/b/g/n/ac, ac Wave 2
- 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 protokolů 802.11v, 802.11k, 802.11r, OKC
- 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
- Podpora WPA2
- Podpora multi SSID
- Podpora ACL pro filtrování provozu
- Až 16 možných vysílaných BSSID na jednu radiovou část
- Možnost přenastavit režim činnosti AP do režimů: uživatelský přístup, monitor nebo spektrální analýza
- AP obsahuje HW pro spektrální analýzu (detekce zdroje rušivého signálu – interference)
- Jednotlivá AP musí mít plnohodnotnou WIFI-Alliance certifikaci
- Součástí dodávky AP musí být instalační sada pro pevnou instalaci na zeď
- Minimálně pasivní zapojení do federovaného systému eduroam (www.eduroam.cz).
- Součástí dodávky bude návrh topologie wifi 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, fyzická montáž AP a konfigurace WiFi systému pro cca 90 uživatelů
- Bude konfigurován min. oddělený provoz pro pedagogický sbor, studenty a návštěvy.

UPS

- 3000VA (2700W) LCD 230V
- Montáž do datového rozvaděče, velikost 2U
- Alfanumerický LCD displej - intuitivní rozhraní poskytuje podrobné a přesné údaje a možnost lokální konfigurace.
- Zelený režim s vysokou účinností - optimální účinnost, která šetří náklady na dodávku energie a chlazení.
- Napájení v síťové kvalitě - rozšířený rozsah automatické regulace napětí (AVR), filtrace šumu a přepěťová ochrana.
- Komunikační porty - sériový, USB a Smart-slot pro karty s příslušenstvím
- Skupina spínaných zásuvek - umožňuje opětovný start zařízení, odpojení méně důležitých zátěží pro úsporu kapacity, časové plánování zapínání a vypínání.
- Odpojení baterie - pohodlná možnost odpojit baterii při přepravě.
- Vyspělá správa baterií - nabíjení s kompenzací teploty prodlužuje životnost a vyspělé algoritmy doporučují datum výměny.

Požadujeme kompletní montáž HW, aktualizaci firmware, zapojení do sítě LAN a konfiguraci UPS. Na serveru bude nainstalován OS Windows Server (min. ver. 2012 R2) včetně posledních aktualizací. Dále bude nakonfigurována služba DNS, DHCP a Active Directory pro cca 90 uživatelů. Každý uživatel bude mít vytvořen jedinečný účet. Služba Active Directory bude mít vazbu na UTM FireWall (logování dle uživatelů v AD).

DNSSEC RESOLVER NA STRANĚ ŠKOLY

- Požadujeme konfiguraci DNSSEC na novém řadiči Microsoft ActiveDirectory 2012 R2 (2016) na kterém bude spuštěna služba DNS. Tento DNS server je primárním DNS serverem pro všechna zařízení v síti LAN.

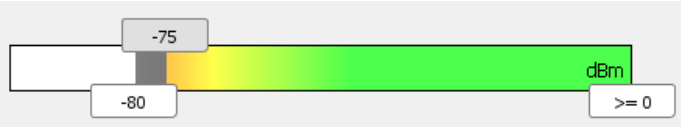
PŘÍLOHA

SIMULACE ŠÍŘENÍ WI-FI SIGNÁLU

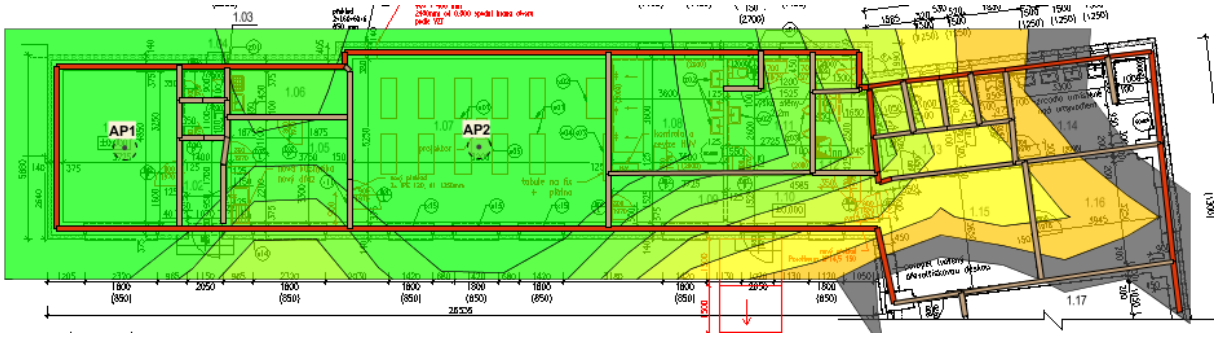
Na obrázcích níže je výstup ze simulace šíření Wi-Fi signálu pro pásmo 2,4 i 5GHz. Je zobrazena síla signálu v jednotkách dBm.

Pro účely simulace byly zvoleny následující hodnoty:

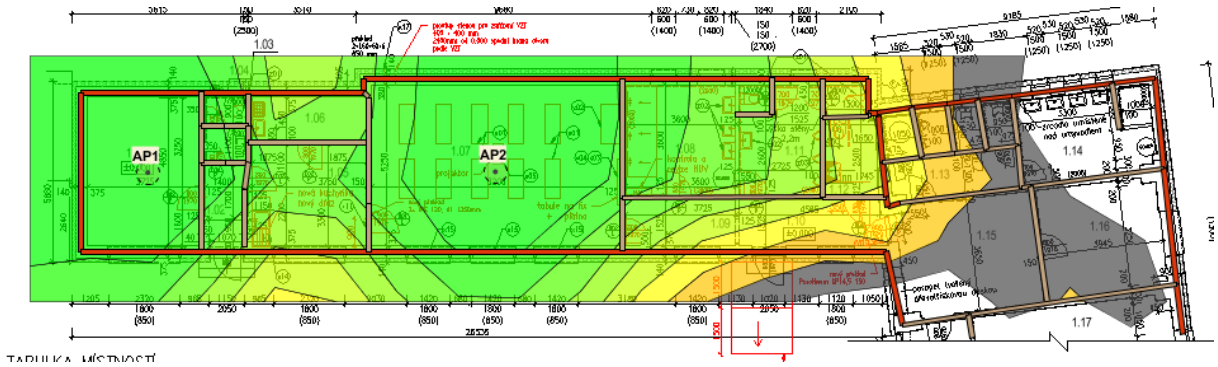
- Typ bezdrátového přístupového bodu: Meraki MR32
- Vysílací výkon: 25mW
- Útlum zdiva:
  - Červená – 10dB
  - Hnědá – 3dB
- Ořez síly signálu (znázorněn šedivou barvou): -75dBm



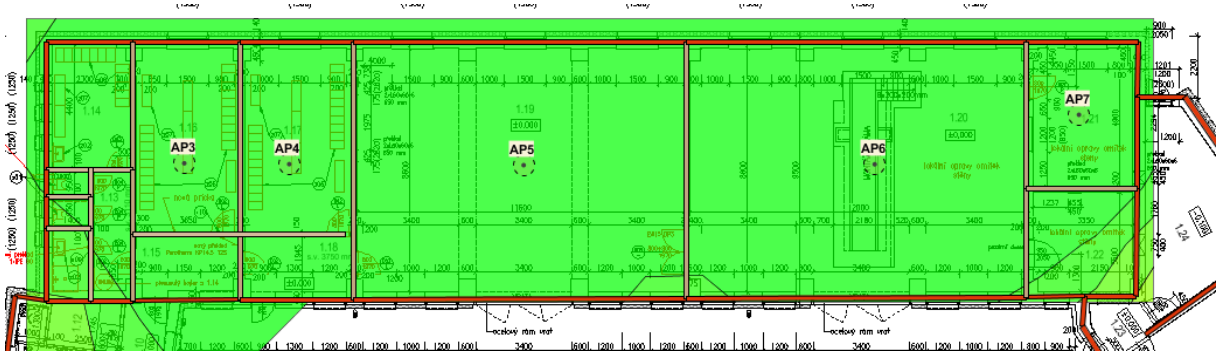
OBR. 4 LEGENDA SÍLY SIGNÁLU RSSI



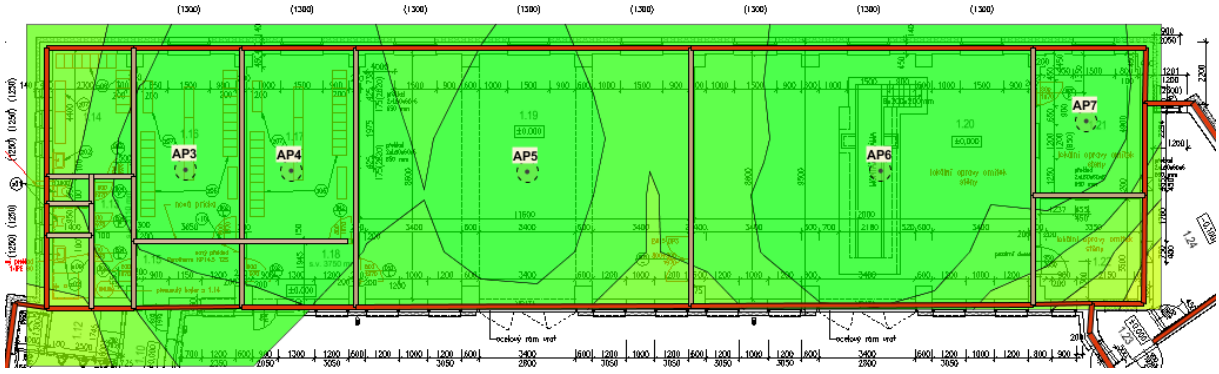
OBR. 5 DÍLENSKÝ AREÁL 1.NP - OBJEKT A – SÍLA SIGNÁLU RSSI PRO 2,4GHZ



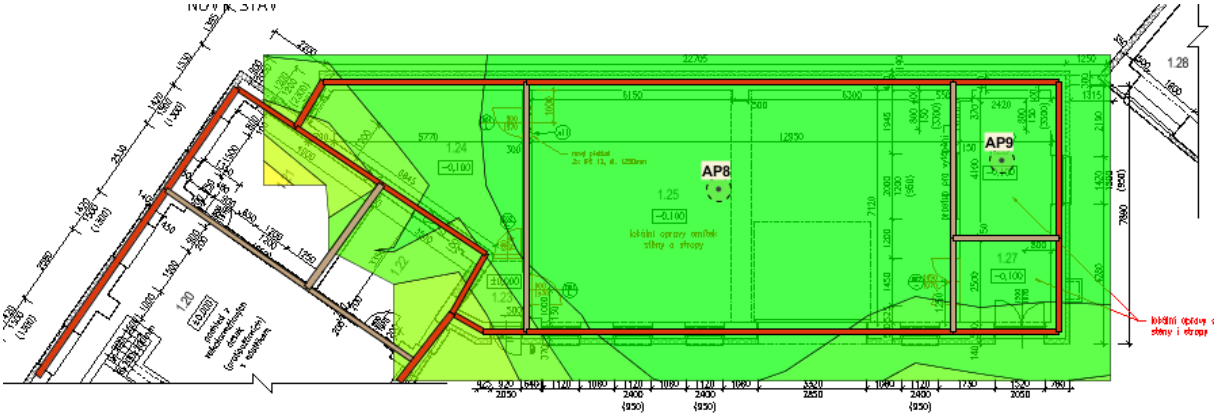
OBR. 6 DÍLENSKÝ AREÁL 1.NP - OBJEKT A – SÍLA SIGNÁLU RSSI PRO 5GHZ



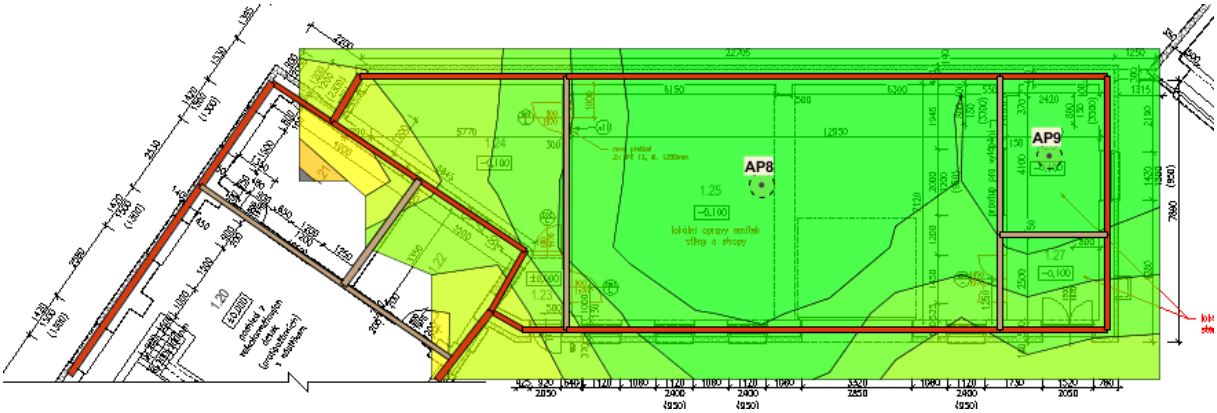
OBR. 7 DÍLENSKÝ AREÁL 1.NP - OBJEKT B – SÍLA SIGNÁLU RSSI PRO 2,4GHZ



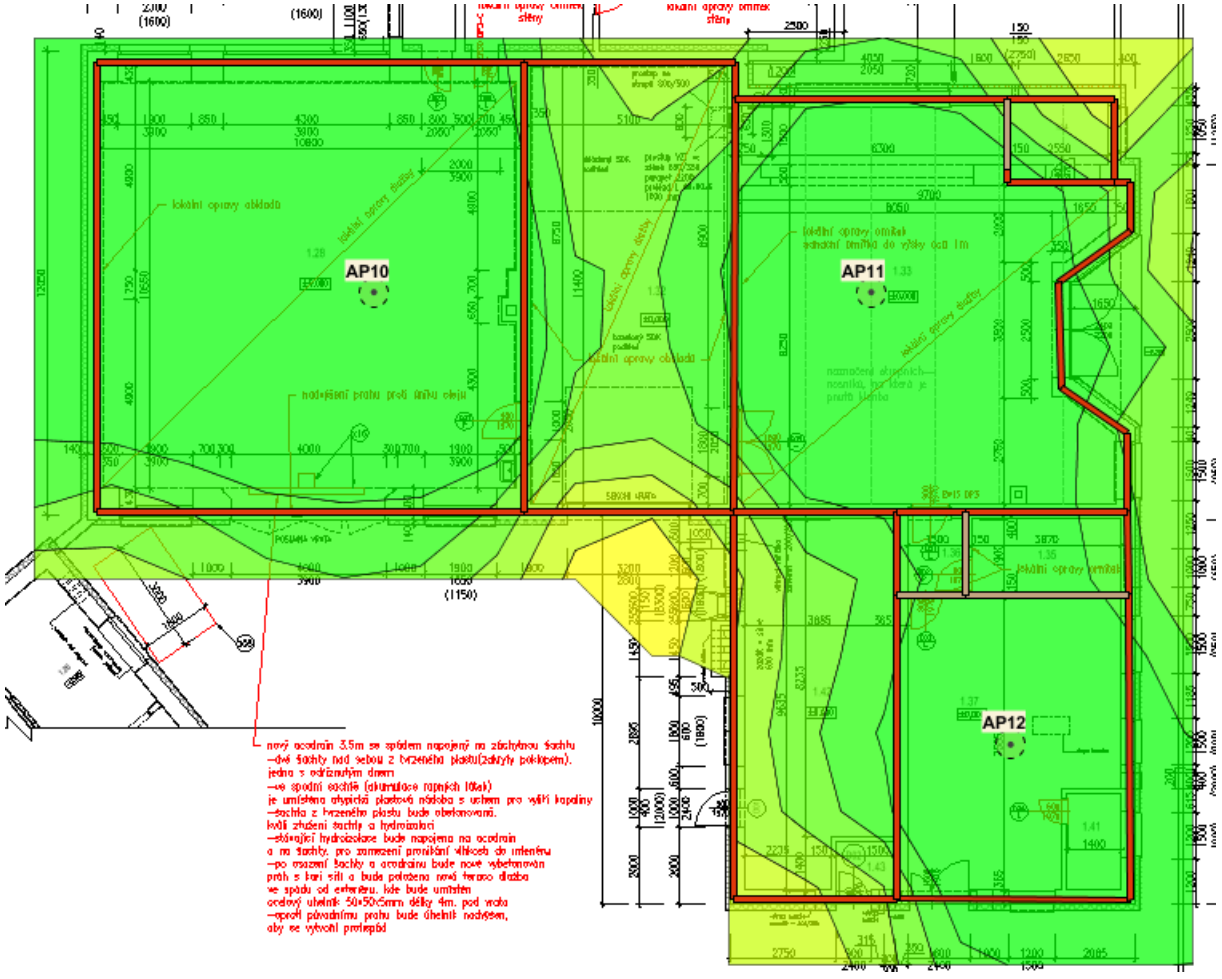
OBR. 8 DÍLENSKÝ AREÁL 1.NP - OBJEKT B – SÍLA SIGNÁLU RSSI PRO 5GHZ



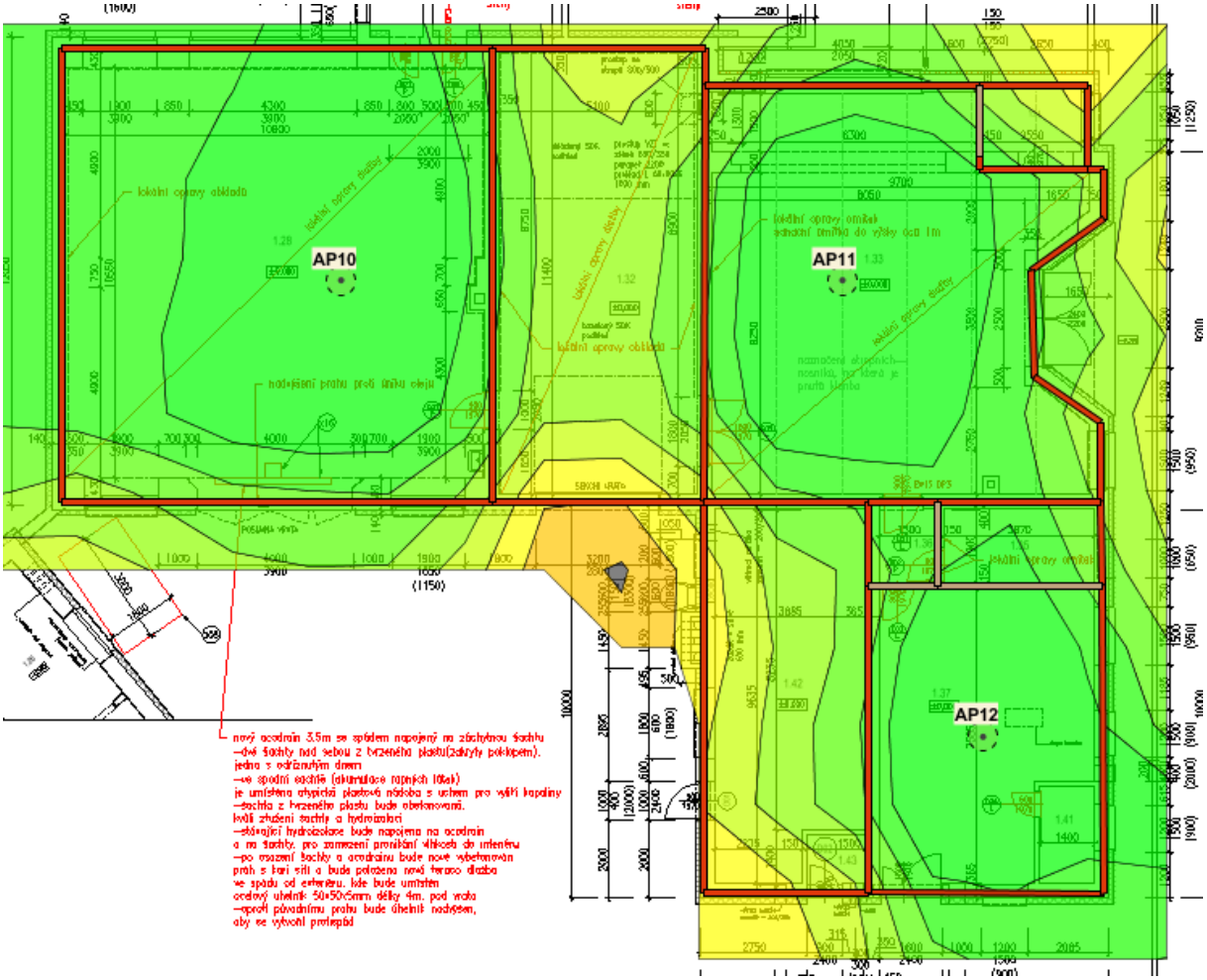
OBR. 9 DÍLENSKÝ AREÁL 1.NP - OBJEKT C – SÍLA SIGNÁLU RSSI PRO 2,4GHZ



OBR. 10 DÍLENSKÝ AREÁL 1.NP - OBJEKT C – SÍLA SIGNÁLU RSSI PRO 5GHZ



OBR. 11 DÍLENSKÝ AREÁL 1.NP - OBJEKT D – SÍLA SIGNÁLU RSSI PRO 2,4GHZ



OBR. 12 DÍLENSKÝ AREÁL 1.NP - OBJEKT D – SÍLA SIGNÁLU RSSI PRO 5GHZ