


VYPRACOVAL: <b>Václav Bradáč</b>	VED. PROJEKTANT: <b>Ing. Jaroslav Havlíček</b>	SCHVÁLIL:	 <b>AV MEDIA</b> <small>kommunikace obrazem</small> AV MEDIA a.s. 102 00 PRAHA 10, Pražská 63 tel.: +420 / 261 260 218, fax: +420 / 261 227 648	
MÚ - OÚ: <b>Ústí nad Labem</b>				
INVESTOR: <b>ZŠ Elišky Krásnohorské 3084/8, Ústí nad Labem</b>			A4	-
STAVBA - OBJEKT: <b>ZŠ Elišky Krásnohorské 3084/8, Ústí nad Labem</b>			DATUM	<b>12/2016</b>
			STUPEŇ	<b>DPS</b>
			MĚŘÍTKO	-
			ČÍS. ZAK.	-
OBSAH: <b>LAN + WIFI</b> <b>Technická zpráva</b>			ČÍSLO VÝKRESU: <b>1</b>	REV.

**SKTRUKTUROVANÁ KABELÁŽ + WIFI**

**ZŠ ELIŠKY KRÁSNOHORSKÉ 3084/8, ÚSTÍ NAD LABEM**

**TECHNICKÁ ZPRÁVA**

**IDENTIFIKAČNÍ ÚDAJE**

---

Stavba:	ZŠ Elišky Krásnohorské 3084/8, Ústí nad Labem
Místo stavby:	ZŠ Elišky Krásnohorské 3084/8, Ústí nad Labem
Dílčí část:	Strukturovaná kabeláž + WIFI
Stupeň dokumentace:	DPS
Investor:	ZŠ Elišky Krásnohorské 3084/8, Ústí nad Labem
Projektant profese:	Václav Bradáč
	<b>AV MEDIA a.s.</b> , Pražská 63, 102 00 Praha 10
Datum dokončení dokumentace:	12/2016

# OBSAH

<b>1</b>	<b>ÚVOD .....</b>	<b>3</b>
1.1	Výchozí podklady a jejich zohlednění v dokumentaci .....	3
1.2	Účel dokumentace .....	3
1.3	Charakteristika provozu a prostředí technologie .....	3
1.4	Začátek, konec a průběh provozních a distribučních tras rozvodů .....	3
<b>2</b>	<b>ZÁMĚR INVESTORA.....</b>	<b>3</b>
<b>3</b>	<b>AKTUÁLNÍ STAV .....</b>	<b>4</b>
<b>4</b>	<b>POPIS NOVÉHO TECHNICKÉHO ŘEŠENÍ .....</b>	<b>6</b>
<b>5</b>	<b>POŽADAVKY NA PROJEKTOVANOU INFRASTRUKTURU ŠKOLY.....</b>	<b>8</b>
<b>6</b>	<b>OFFLINE SIMULACE POKRYTÍ WIFI SIGNÁLEM .....</b>	<b>10</b>
<b>7</b>	<b>TECHNICKÉ INFORMACE K NAVRHOVANÉ WIFI TECHNOLOGII.....</b>	<b>12</b>
<b>8</b>	<b>POPIS STANDARDŮ INSTALACE .....</b>	<b>13</b>
8.1	Kontrola stavební připravenosti.....	13
8.2	Technologické postupy .....	13
8.3	Závěrečné ladění a testování funkčnosti zařízení .....	14
<b>9</b>	<b>POŽADAVKY A NÁROKY NA PROFESE.....</b>	<b>14</b>
9.1	Ochrana před úrazem elektrickým proudem .....	14
9.2	Určení prostředí .....	14
9.3	Protipožární opatření .....	14
9.4	Péče o životní prostředí .....	15
9.5	Požadavky na jiné technologie.....	15
9.5.1	Obecné zásady pro profesi silnoproud .....	15
9.6	Nároky na providera .....	15
<b>10</b>	<b>SERVIS.....</b>	<b>16</b>
10.1	Preventivní prohlídka (Profylaxe) .....	16
<b>11</b>	<b>ZÁVĚR.....</b>	<b>16</b>

TATO PROJEKTOVÁ DOKUMENTACE JE DUŠEVNÍM VLASTNICTVÍM FIRMY AV MEDIA, a.s., a VZTAHUJÍ SE NA NI VŠECHNA USTANOVENÍ AUTORSKÉHO ZÁKONA. DOKUMENTACI LZE UŽÍVAT POUZE VE SMYSLU PŘÍSLUŠNÉ SMLOUVY O DÍLO. KOPÍROVÁNÍ A JINÁ ROZŠÍŘOVÁNÍ DOKUMENTACE, NEBO JEJICH ČÁSTÍ MOHOU BYT PROVÁDĚNA JEN SE SOUHLASEM AV MEDIA, a.s.

# 1 ÚVOD

---

## 1.1 Výchozí podklady a jejich zohlednění v dokumentaci

- Stavební dokumentace podklady poskytnuté investorem
- Požadavky investora a uživatele

## 1.2 Účel dokumentace

Projekt je zpracován na úrovni projektové dokumentace pro výběr dodavatele s rozšířením na prováděcí dokumentaci. Tato technická zpráva popisuje navržené systémy a vysvětluje jejich funkcionalitu. Cílem je doplnění metalické počítačové sítě, instalace nových aktivních síťových prvků 1 Gbps s možností managementu, členění do virtuálních sítí (VLAN), podporou prioritizace provozu (QoS), s možností napájení určených zařízení skrze datový kabel (PoE), s rezervou cca 20% volných portů v síťových přepínačích. Vybudování robustní bezdrátové sítě 802.11ac ve frekvenčních pásmech 2,4 a 5 GHz pokrývající požadované části budovy.

**Součástí projektu není řešení a nacenění potřebných prací profese silnoproud, škola bude silnoproud realizovat sama prostřednictvím místních zdrojů.**

## 1.3 Charakteristika provozu a prostředí technologie

Zařízení může být umístěno pouze v prostorách a prostředích, které jsou stanoveny limity výrobce a jeho technickými podmínkami. Z hlediska životnosti se nedoporučuje zvýšená prašnost, vlhkost, extrémně zvýšená teplota a otřesy. Pro provoz se orientačně předpokládá teplota v rozmezí 0 až +25°C, relativní vlhkost max. 65%. Veškerý návrh technologie, kabelových a signálových tras je navržen dle dotčených bezpečnostních norem.

## 1.4 Začátek, konec a průběh provozních a distribučních tras rozvodů

Komponenty LAN a WIFI systému jsou mezi sebou propojeny kabelovými trasami pro přenos dat. Současně je celá technologie napojena na systém napájení. Napájení bude realizováno profesí silnoproud (není součástí tohoto projektu).

# 2 ZÁMĚR INVESTORA

---

- modernizace síťové infrastruktury pro potřeby uživatele
- instalace nových aktivních síťových prvků 1 Gbps s možností managementu, členění do virtuálních sítí (VLAN), podporou prioritizace provozu (QoS), s páteřním propojením optickými kabely 1 Gbps, s možností napájení určených zařízení skrze datový kabel (PoE), s rezervou cca 20% volných portů v síťových přepínačích
- Instalace nových aktivních síťových prvků 1 Gbps s možností managementu, členění do virtuálních sítí (VLAN), podporou prioritizace provozu (QoS), podporou dalších bezpečnostních funkcí a funkcí správy, s páteřním propojením UTP kabely rychlostí 1 Gbps, s rezervou cca 15% volných portů v síťových přepínačích.
- Zajištění kontroly nad webovým obsahem dostupným z lokální sítě pomocí webového filtru.
- Inovace serverové infrastruktury pro funkce autentifikace uživatelů a záznam aktivit v LAN a WAN.
- Zajištění krátkodobého napájení páteřních prvků síťové a serverové infrastruktury v případě výpadku proudu.

TATO PROJEKTOVÁ DOKUMENTACE JE DUŠEVNÍM VLASTNICTVÍM FIRMY AV MEDIA, a.s., a VZTAHUJÍ SE NA NI VŠECHNA USTANOVENÍ AUTORSKÉHO ZÁKONA. DOKUMENTACI LZE UŽÍVAT POUZE VE SMYSLU PŘÍSLUŠNÉ SMLOUVY O DÍLO. KOPÍROVÁNÍ A JINÁ ROZŠÍŘOVÁNÍ DOKUMENTACE, NEBO JEJICH ČÁSTÍ MOHOU BÝT PROVÁDĚNA JEN SE SOUHLASEM AV MEDIA, a.s.

### 3 AKTUÁLNÍ STAV

---

#### Pasivní síťové prvky (optická a metalická vedení):

- V budově existuje funkční LAN infrastruktura.
- Současná topologie a kapacita LAN infrastruktury umožňuje v omezené míře doplnění a rozšíření.
- Páteřní pasivní i aktivní prvky LAN jsou umístěny v dedikované místnosti s kontrolovaným přístupem bez řízeného provozního prostředí. Páteřní aktivní síťové prvky a servery jsou umístěny v oddělené části místnosti č. 2/211 ve 2. N.P. pavilonu CF.
- Některé pasivní a aktivní prvky LAN (např. páteřní infrastruktura v hlavní technologické místnosti) jsou přimontovány přímo na zeď nebo jsou instalovány do široké plastové lišty, další části infrastruktury jsou umístěny v několika malých a středních nástěnných rozvaděčích, jenž jsou obsazeny z cca 50% - 90%.
- UTP kabely jsou ukončeny v patchpanelech a jsou vedeny nejkratší cestou plastovými nástěnnými lištami bez další rezervy.
- Lišty jsou za hranicí své kapacity, některé lišty jsou z důvodu přeplnění ponechány otevřené, části lišt jsou poškozené.
- Vedení většiny UTP kabelů je přesně zmapováno a existuje aktualizovaný plán zapojení, LAN zásuvky i patchpanely jsou označeny číselným kódem.
- Všechny namátkou kontrolované UTP kabely jsou ve specifikaci CAT5e, jsou však neznámého stáří a neznámé kvality.
- LAN zásuvky nemají v místnostech unifikované umístění, nacházejí se převážně v blízkosti počítače, typicky jedna dvojjádrová zásuvka.
- Případný nežádoucí souběh LAN kabeláže s vedením 230 V nebyl prověřován.

#### Aktivní síťové prvky (LAN přepínače a routery):

- Připojení k síti Internet je realizováno optickým kabelem symetrickou neagregovanou rychlostí 100 Mbps, připojení je zakončeno v optické vaně v malém nástěnném rozvaděči v oddělené části místnosti č. 2/211 ve 2. N.P. pavilonu CF.
- Funkci hlavního směrovače (routeru) a brány v zabezpečuje zařízení *Linksys EA6500* ze segmentu pro domácnosti, nevhodné svým výkonem a funkcemi pro danou velikost sítě a počet uživatelů.
- Služby DNS a DHCP poskytuje server s operačním systémem *Windows Server 2008 R2*.
- Instalované LAN přepínače jsou produktovým mixem 1 Gbps (převážně *TP-Link*) a 100 Mbps (převážně *D-Link*) rackmount zařízení umístěných v rozvaděčích, v některých případech jsou tyto LAN přepínače doplněny desktopovými.
- S výjimkou gigabitového LAN přepínače *ZyXEL GS1910-24* v hlavní technologické místnosti, žádný z instalovaných síťových přepínačů nedisponuje možností správy, rozdělení sítě pomocí virtuálních sítí (VLAN), nebo dalšími funkcemi požadovanými v plánované síťové infrastruktuře.

## Bezdrátová síť (WiFi):

- potřeba bezdrátového připojení je řešena ad-hoc
- Většina pavilónů je pokryta WiFi signálem, bezdrátová síť je v malé míře využívána i pro výuku.
- Zadavatel nepředpokládá takové využití bezdrátové WiFi sítě, kdy by bylo vyžadováno souběžné připojení většího počtu vysoce aktivních uživatelů, nebo požadavek na určitou garantovanou šířku přenosového pásma na jednoho uživatele.
- Jako přístupové body jsou používána zařízení *Ubiquiti UniFi AC LR* ze segmentu SMB, resp. Entry-Enterprise.
- Přístupové body jsou řízeny softwarovým kontrolérem *UniFi Controller* nainstalovaným na jednom ze sekundárních školních serverů.
- Přístupové body jsou napájeny proprietárními „pasivními“ 24V PoE adaptéry (injektory) nekompatibilními se standardem 802.2af/at.
- Přístupové body jsou umístěny v pravidelných rozestupech vždy na jedné z delších svislých zdí chodeb, kvalita spojení v učebnách „za zády“ přístupového bodu, mimo jeho hlavní vyzařovací charakteristiku, je potom výrazně horší než v učebnách ve směru jeho hlavního vyzařování a příjmu.
- Současná bezdrátová WiFi infrastruktura umožňuje centrální řízení, správu a údržbu, podporuje rozdělení bezdrátových sítí dle účelu použití a případnou centralizovanou autentifikaci uživatelů.

## Serverová infrastruktura:

- Většina pavilónů je pokryta WiFi signálem, bezdrátová síť je v malé míře využívána i pro výuku.
- Zadavatel nepředpokládá takové využití bezdrátové WiFi sítě, kdy by bylo vyžadováno souběžné připojení většího počtu vysoce aktivních uživatelů, nebo požadavek na určitou garantovanou šířku přenosového pásma na jednoho uživatele.
- Jako přístupové body jsou používána zařízení *Ubiquiti UniFi AC LR* ze segmentu SMB, resp. Entry-Enterprise.
- Přístupové body jsou řízeny softwarovým kontrolérem *UniFi Controller* nainstalovaným na jednom ze sekundárních školních serverů.
- Přístupové body jsou napájeny proprietárními „pasivními“ 24V PoE adaptéry (injektory) nekompatibilními se standardem 802.2af/at.
- Přístupové body jsou umístěny v pravidelných rozestupech vždy na jedné z delších svislých zdí chodeb, kvalita spojení v učebnách „za zády“ přístupového bodu, mimo jeho hlavní vyzařovací charakteristiku, je potom výrazně horší než v učebnách ve směru jeho hlavního vyzařování a příjmu.
- Současná bezdrátová WiFi infrastruktura umožňuje centrální řízení, správu a údržbu, podporuje rozdělení bezdrátových sítí dle účelu použití a případnou centralizovanou autentifikaci uživatelů.

## 4 POPIS NOVÉHO TECHNICKÉHO ŘEŠENÍ

---

### *Strukturovaná kabeláž*

V celém komplexu školy zůstanou zachovány stávající metalické rozvody. Všechny stávající UTP kabely doporučuji proměřit a nevyhovující kabely vyměnit. Nové metalické rozvody budou realizovány jen v 1np pavilonu MVD3 a bude zakončeny ve stávajícím Racku RA6 ve 2np pavilonu MVD3. Horizontální kabeláž z racku ke koncovým prvkům (datové dvojbáseňky, access pointy) bude vedena metalickou kabeláží v provedení UTP CAT6. Datové dvojbáseňky v místnostech budou vždy umístovány do blízkosti stávajících 230V zásuvek. Nové rozvody budou splňovat parametry 1GB sítě. Kabely budou uloženy v lištách.

### *Datové rozvaděče – Racky*

V hlavním technologické místnosti navrhuji instalovat nový 19“ rozvaděč a veškerou techniku do něho přesunout. Ostatní rozvaděče budou vyměněny pro navýšení jejich kapacity.

### *Topologie zapojení aktivních prvků*

Hlavní přívod veřejného internetu od providera bude zapojen na HW firewall jednotku umístěnou v racku RA1. Za firewall jednotkou bude zapojen agregační switch a následně skrze stávající metalickou kabeláž budou zapojeny 24p nebo 48p metalické switche v podružných raccích. Z metalických switchů budou zapojeny datové dvojbáseňky a access pointy (access pointy budou napájeny pomocí PoE ze switchů).

Síť bude rozdělena do 3 logických částí tak, aby umožnila nastavit různé pravidla přístupu do místní sítě a Internetu pro zaměstnance, studenty a hosty.

- Učitelé a další personál, bude přistupovat pomocí VLAN a routování ke zdrojům v LAN a filtrovaný (s benevolentnějšími pravidly) či nefiltrovaný přístup na Internet.
- Žáci budou přistupovat pomocí VLAN a routování, studenti (zařízení, resp. drátové a bezdrátové sítě sloužící přímo pro výuku) budou mít filtrovaný přístup na Internet a budou mít přístup k výukovým zdrojům v LAN (fileservery a další aplikace).
- Hostovská (Guest) WiFi síť pro pouhý filtrovaný pomalý přístup na Internet, bez přístupu k zdrojům v lokální síti (fileservery apod.) = studenti, učitelé a návštěvníci se svými mobily apod..

Bezdrátové přístupové body jsou dle modelu uvažované 3 na patro a pavilon. Celkový počet bezdrátových bodů je 29. V tomto počtu je nezbytně nutné řídit kontrolérem bezdrátové sítě (WLAN Controller), jenž umožní inteligentní automatické přizpůsobování bezdrátové sítě aktuálním podmínkám, umožní jednoduché nasazení nových přístupových bodů, jejich jednoduchou správu a monitoring. Kontrolér bezdrátové sítě by měl umožňovat autentifikaci klientů oproti adresářové službě (např. Microsoft Active Directory. Pro velmi pravděpodobné daleko větší budoucí využívání výukového obsahu umístěného na síti Internet a pravděpodobný přesun řady výukových aplikací do prostředí cloudu je třeba navýšit rychlost připojení k síti Internet alespoň na symetrických 100 Mbps.

Instalované aktivní síťové prvky budou v provedení 1 Gbps s možností rozšířené administrace, členění sítě do virtuálních sítí (VLAN). Pro bezproblémové fungování rozšířené síťové infrastruktury bude osazen router schopný odbavovat požadavky sítě s internetovým připojením výhledově min. 100 Mbps a lokální síti s 300+ klienty, s podporou virtuálních sítí (VLAN).

### *Jištění proti výpadku proudu*

Kritické části systému budou jištěny pomocí UPS jednotek proti výpadku proudu. Při výpadku proudu by měly navržené UPS jednotky udržet systém v provozu po dobu min. 3-5 minut. V racku RA1 bude umístěna UPS jednotka o minimální velikosti 2200VA a v podružných rackech UPS jednotky o velikosti 750VA.

### *Webový filtr*

Přístup ze studentské sítě do internetu bude realizován prostřednictvím webového filtru. Jedná se o filtr, který kontroluje webový provoz, poskytuje detailní reporting, šetří datovou linku a snižuje zneužívání internetu pro nelegální aktivity. Přístup uživatelů na internet je efektivně řízen webovým filtrem, který filtruje s katalogem www stránek, které uživatelé skutečně navštěvují. Databáze je stále aktualizovaná o nově navštěvované stránky, které hodnotí a třídí profesionální tým kategorizátorů. Právě díky přesnému rozpoznání webového obsahu vyniká navržený filtr vysokou přesností a efektivitou filtrace, která dosahuje až 98 %.

### *Server*

Nedílnou součástí síťové infrastruktury je server s patřičným programovým vybavením, který slouží jako doménový řadič pro zajištění služby Active Directory (AD). AD nám poskytuje distribuovanou databázi síťových objektů (uživatelů, klientů, tiskáren ...) a možnost vytváření logických skupin (domén). Dále pak zajišťuje centralizovanou autentizaci a autorizaci uživatelů/klientů dostupných v síti, tedy hromadnou centralizovanou správu účtů a správu případných skupinových politik.



## 5 POŽADAVKY NA PROJEKTOVANOU INFRASTRUKTURU ŠKOLY

V posledních letech se setkáváme se stále aktivnějším využíváním interaktivních technologií ve výuce a s celkovou digitalizací výuky jako takové. Synonymem pro tento trend je aktivní využívání tabletů a mobilních výukových prostředků ve výuce. Tato nová výuková zařízení, jako jsou tablety, notebooky, e-čtečky a smartphony, potřebují pro své fungování odpovídající bezdrátovou infrastrukturu Wi-Fi. Nekvalitní Wi-Fi nebo její omezená implementace znamená, že celá generace technologií, které nabízejí digitalizaci výuky, není použitelná ve školních třídách. Mnohdy je to právě technologie, kterou již mladší studenti mají osvojenou a jejíž zapojení do výuky je často jednodušší než použití tradičních počítačů. Je velmi pravděpodobné, že současní žáci a studenti již budou naplno používat mobilní zařízení ve svém pracovním životě. Je proto účelné naučit je s těmito technologiemi pracovat adekvátně a produktivně už ve škole.

Musí být zaručena jednotnost a přehlednost systému pro správu Wi-Fi a bezpečnostních politik je klíčová z toho důvodu, aby byla síť efektivně nastavena, zabezpečena a zároveň vhodnou filtrací ochránila studenty před nevhodným obsahem. Zjednodušeně řečeno, pedagogický personál se má soustředit na své kompetence a na to, jak efektivně digitalizovat výuku, nikoli řešit proč v síti něco nefunguje.

Infrastruktura v moderní škole by proto měla být dostatečně kvalitní, aby mohli být všichni žáci současně připojeni a měli možnost spolupracovat. Mění se rovněž typ provozu, kdy vidáme zvyšování podílu multimediálních aplikací, streamování videa a sdílení digitalizovaného obsahu jako takového. V neposlední řadě pak dochází rovněž k nasazování mobilních kolaborativních technologií, které v rámci projektů inkluze například umožňují zapojení do výuky žáků dlouhodobě nemocných, ať už v nemocničním nebo domácím ošetřování.

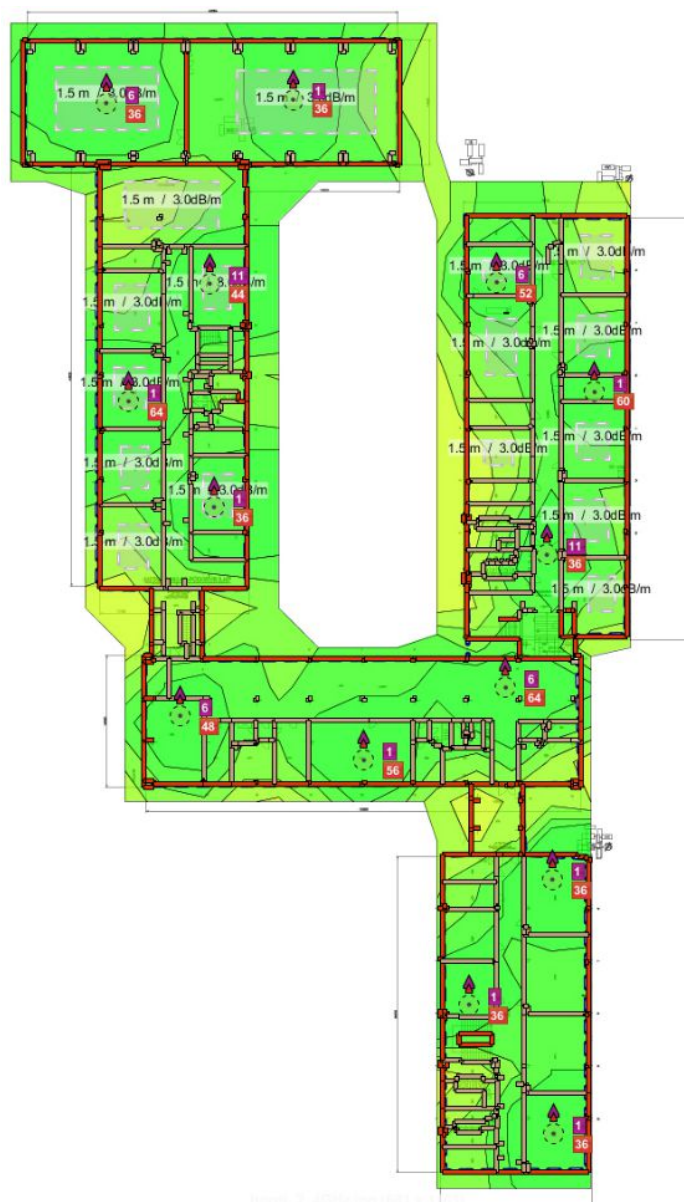
- Centrální systém řízení a monitorování sítě musí umožnit zabezpečenou vzdálenou správu, plnou konfiguraci a monitorování současně pro všechny poptávané komponenty sítě (bezpečnostní brány, přepínače, bezdrátové přístupové body a systém správy mobilních zařízení) a to prostřednictvím jednotného integrovaného webového rozhraní.
- Systém musí zajistit automatickou aktualizaci softwaru a instalaci bezpečnostních záplat do všech zařízení systému v rámci projektu a to v uživatelsky definovaném čase.
- Systém musí umožnit změny konfigurace více zařízení stejného typu současně a konfigurace nových zařízení pomocí šablon.
- Centrální systém řízení a monitorování sítě musí podporovat následující metody autentizace klientů LAN a WLAN infrastruktury: 802.1X ověření na základě údajů interní databáze systému, 802.1X ověření prostřednictvím RADIUS serveru, Webová autentizace na základě údajů interní databáze systému, Webová autentizace prostřednictvím RADIUS nebo LDAP serveru.
- Centrální systém řízení a monitorování sítě musí být schopen zobrazit všechny klientská zařízení připojená k síti školy během minimálně posledních 10 dnů. Výpis by měl obsahovat minimálně následující informace: Uživatelské jméno, IP a MAC adresa zařízení, Objem uživatelem / zařízením přenesených dat za dané období s rozpadem na jednotlivé rozpoznané aplikace
- Systém musí být schopen zobrazit seznam top žáků / studentů, kteří za dané období ve školní síti přenesli nejvíce dat.
- Systém musí být schopen zobrazit polohu a stav všech zařízení v systému v geografické mapě a také graficky zobrazit reálnou fyzickou topologii sítě školy.

- Systém musí být schopen zobrazit polohu všech klientských zařízení v závislosti na způsobu jejich připojení a to buď přímo v plánech jednotlivých podlaží, v geografické mapě nebo v kontextu portu příslušného LAN přepínače.
- Systém musí v případě bezpečnostní brány umožnit konfiguraci FW L3-L7 a IDS/IPS bezpečnostních pravidel, NATu, celkové šířky pásma na uplinku a propustnosti pro klienty a jednotlivé rozpoznané aplikace.
- Základní konektivita a přístup do Internetu musí být pro klienty zachován i v případě, že je Centrální systém řízení a monitorování sítě dočasně nedostupný.
- I v případě nedostupnosti Centrálního systému řízení a monitorování sítě musí být zajištěna možnost autentizace a autorizace nových klientů LAN i WLAN infrastruktury prostřednictvím 802.1x protokolu pomocí RADIUS.
- Systém musí umožnit rozdělení administrátorů do skupin s různými právy přístupu.
- Pro autentizaci administrátora přistupujícího přes webové rozhraní musí systém podporovat minimálně RADIUS protokol.
- Systém musí být schopen odesílat správcům emailové zprávy o důležitých systémových událostech.
- Systém musí být schopen odesílat zprávy na vzdálený SYSLOG server.
- Systém musí podporovat SNMP protokol pro vzdálenou správu a monitorování.
- Systém musí podporovat XML API pro integraci s navazujícími systémy školy poskytující informace o připojených komponentách sítě a také klientských zařízeních.
- Systém musí sledovat změny konfigurace systému a zahrnutých síťových komponent - Informace musí minimálně obsahovat: položku konfigurace, uživatelské jméno administrátora, který změnu provedl, novou hodnotu proměnné, v které ke změně došlo
- Systém musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 5-10 let.
- Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 5-10 let a to včetně všech aktualizací softwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Systém musí být v době prodeje výrobcem plně podporován a na žádnou jeho část nesmí být v době prodeje vyhlášeno ukončení prodeje.

## 6 OFFLINE SIMULACE POKRYTÍ WIFI SIGNÁLEM

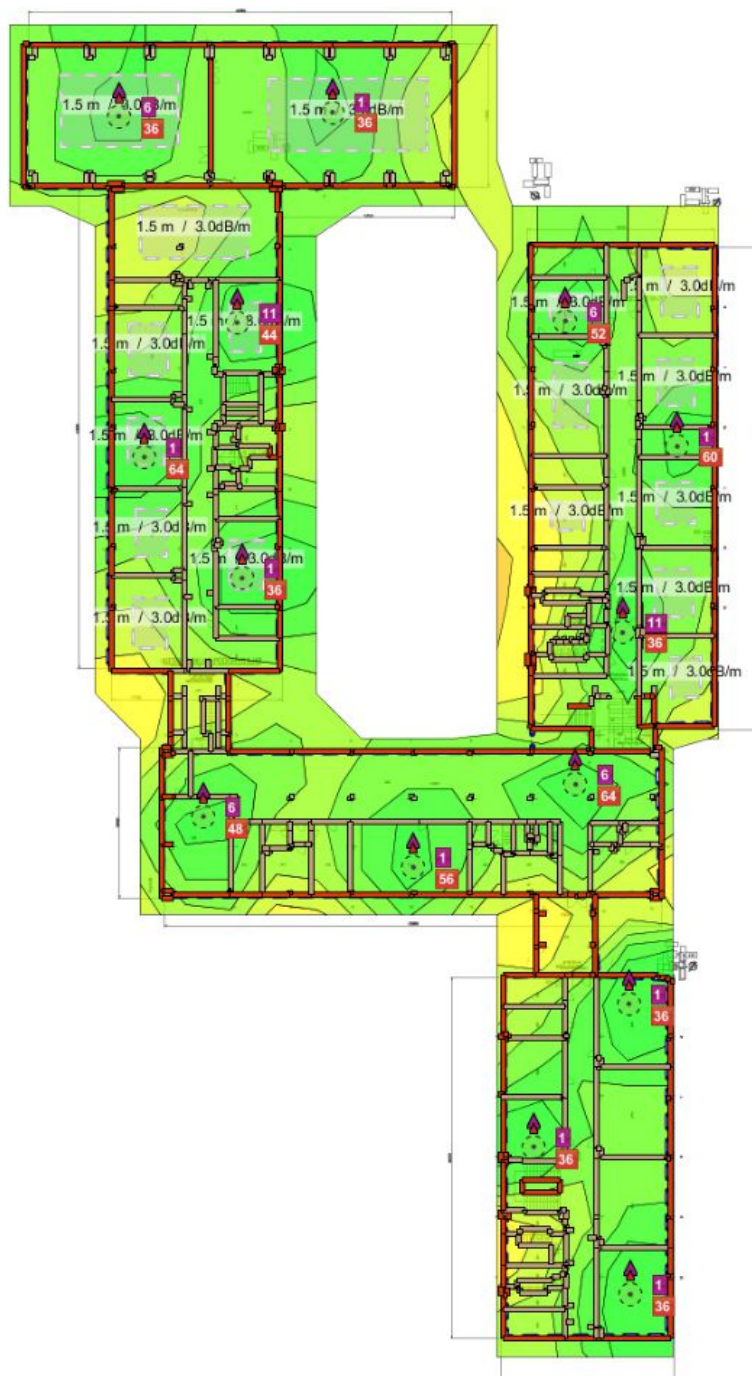
Simulace šíření signálu byla provedena v nástroji AirMagnet Planner. Simulace je připravena pro 2,4GHz a 5GHz pásmo. Všechny AP mají nastavený vysílací výkon na 15dBm, takže je zde rezerva, co se týče pokrytí (standard dovoluje až 20dBm na 2,4GHz a 23/30dBm na 5Ghz). Jako použitelnou sílu signálu je zvolena hranice -67dBm, vše horší než tato hranice je zobrazeno šedivou barvou. V rámci simulace byly definovány útlumy zdí, modré příčky 4dB, červené 8dB, červený plášť budovy 15dB. Také byli definovány útlumy prostředí, červené pro kancelářské prostory a modré pro chodby. Simulace nemůže nahradit reálné site survey měření na lokalitě, které by v tomto případě bylo třeba pro zpřesnění hodnot útlumu zdí apod.

Pokrytí WIFI 2,4GHz vzorové patro



TATO PROJEKTOVÁ DOKUMENTACE JE DUŠEVNÍM VLASTNICTVÍM FIRMY AV MEDIA, a.s., a VZTAHUJÍ SE NA NI VŠECHNA USTANOVENÍ AUTORSKÉHO ZÁKONA. DOKUMENTACI LZE UŽÍVAT POUZE VE SMYSLU PŘÍSLUŠNÉ SMLOUVY O DÍLO. KOPÍROVÁNÍ A JINÁ ROZŠÍŘOVÁNÍ DOKUMENTACE, NEBO JEJICH ČASTÍ MOHOU BYT PROVÁDĚNA JEN SE SOUHLASEM AV MEDIA, a.s.

## Pokrití WIFI 5GHz vzorové patro



TATO PROJEKTOVÁ DOKUMENTACE JE DUŠEVNÍM VLASTNICTVÍM FIRMY AV MEDIA, a.s., a VZTAHUJÍ SE NA NI VŠECHNA USTANOVENÍ AUTORSKÉHO ZÁKONA. DOKUMENTACI LZE UŽÍVAT POUZE VE SMYSLU PŘÍSLUŠNÉ SMLOUVY O DÍLO. KOPÍROVÁNÍ A JINÁ ROZŠÍŘOVÁNÍ DOKUMENTACE, NEBO JEJICH ČASTÍ MOHOU BYT PROVÁDĚNA JEN SE SOUHLASEM AV MEDIA, a.s.




## 7 TECHNICKÉ INFORMACE K NAVRHOVANÉ WIFI TECHNOLOGII

Dle doporučených postupů a výpočtů jsou běžně v praxi dosahované níže uvedené hodnoty pro 30 klientů na jenom AP (jedná se teoretické výpočty – reálná situace je vždy ovlivněná konkrétní situací radiofrekvenčního pásma, typem klientů a konfigurací bezdrátové sítě).

Klient 1-stream (anténa 1x1), 1 kanál: až 1,25Mbit/s na každého klienta na protokolu TCP/IP

Klient 2-stream (anténa 2x2), 1 kanál: až 2,5Mbit/s na každého klienta na protokolu TCP/IP

Maximální možnosti klientů jsou ukázány v následující tabulce (opět záleží na síle signálu, hodnotě SNR, atd....):

		Channel Width		
		20 MHz	40 MHz	80 MHz
Number of Streams	1 stream	87 Mbps	200 Mbps	433 Mbps 
	2 streams	173 Mbps	400 Mbps	866 Mbps 
	3 streams	289 Mbps	600 Mbps	1300 Mbps 

Typické datové toky pro různé aplikace:

Web	0,5 - 1 Mbps
Audio	0,1 Mbps
Video	1 - 4 Mbps
Printing	1 Mbps
Device Backups / File Sharing	up to 50 Mbps

Garance na zařízení:

- AP do vnitřních prostor – mají lifetime warranty
- AP do vnějších prostor – mají 1letou záruční lhůtu
- Bezpečnostní brány – mají lifetime warranty
- Switche – mají lifetime warranty
- Antény a další příslušenství – mají 1letou záruční lhůtu
- Výměna se děje po potvrzení HW závady formou Advanced replacement s odesláním do 1 dne

TATO PROJEKTOVÁ DOKUMENTACE JE DUŠEVNÍM VLASTNICTVÍM FIRMY AV MEDIA, a.s., a VZTAHUJÍ SE NA NI VŠECHNA USTANOVENÍ AUTORSKÉHO ZÁKONA. DOKUMENTACI LZE UŽÍVAT POUZE VE SMYSLU PŘÍSLUŠNÉ SMLOUVY O DÍLO. KOPÍROVÁNÍ A JINÁ ROZŠÍŘOVÁNÍ DOKUMENTACE, NEBO JEJICH ČÁSTÍ MOHOU BÝT PROVÁDĚNA JEN SE SOUHLASEM AV MEDIA, a.s.

## 8 POPIS STANDARDŮ INSTALACE

---

### 8.1 Kontrola stavební připravenosti

Odpovědný pracovník se účastní potřebných kontrolních dnů na stavbě a spolupracuje se stavebním dozorem. Zahájení a ukončení instalace, skluzy, stavební nepřipravenost a další důležité události na stavbě zapisuje do stavebního deníku.

### 8.2 Technologické postupy

Před instalací se odpovědný pracovník seznámí s projektovou dokumentací, návody k obsluze instalovaných zařízení a s instalačními postupy doporučenými výrobcí. Během instalace dodržuje tato pravidla a postupuje podle projektové dokumentace.

#### ***Napájení technologie (AP, switche.):***

- Rozvody napětí budou provedeny dle ČSN, třívodičově.

#### ***Provedení kabeláže:***

- Vedení kabelů bude provedeno v elektroinstalačních trubkách pod omítkou, kabelových kanálech a žlabech, ve stěnách ve standardních chráničkách, případně v sádkartonu i volně
- Volně vedené kabely jsou vhodně vyvázány v pravidelných intervalech.
- Při vedení kabelů je třeba dbát na prostorové odstupy signálových kabelů od kabelů silových
- Montážní lišty a kanály musí být namontovány pečlivě, rovně, v lomeních se používají originální spojky
- Kabely musí být přehledně označeny (vyvazovací páskou se štítkem a nestíratelným popisem pomocí lihového fixu, popř. přímo nestíratelným popisem na kabelu většího průměru) tak, aby při demontáži přístroje (např. z důvodu servisu) bylo při použití dokumentace jasné, který kabel patří do kterého konektoru.
- Umožní-li to situace, je vhodné při protahování kabelů (obtížnými a nepřístupnými trasami) nechat několik kabelů do rezervy (CAT6 aj.), případně nechat volnou chráničku s protahovacím drátem pro případné budoucí rozšíření systému.
- Konektory musí být napájeny kvalitně, bez studených spojů, kabely musí být zajištěny proti vytržení. Konektory, se kterými se často manipuluje, musí mít konektory napájeny buď od výrobce kabelu, nebo musí být použity kvalitní kovové krytky, které umožňují pevné uchycení kabelu.
- U všech kabelů je třeba dbát na správné zapojení konektorů a správnou polaritu signálů.
- Tam, kde je to možné, budou kabely ihned po montáži konektoru proměřeny a vyzkoušeny.
- Při montáži konektorů je třeba důsledně dodržovat barevné značení jednotlivých žil na kabelech

#### ***Montáž přístrojových stojanů (racků):***

- Přístroje je do přístrojových skříní třeba namontovat jednak z hlediska ergonomických (nejčastěji používané přístroje do přístupné výšky, jednak dle technických hledisek (tepelné vyzařování - přístroje vyzařující teplo do dolních částí a nechat větrací mezery, bezdrátové přístroje – antény v horní části aj.)

- Pro přístroje, které nemají standardní montážní úchyty do přístrojové skříně, je třeba použít vhodné police přístrojových skříní. Police musí být dimenzovány na hmotnost přístrojů a v případě potřeby musí mít úchyty v přední i zadní části racku. Přístroje musí být k policím vhodným způsobem přichyceny (šroub, kombinace oboustranné samolepící pásky s vyvazovací páskou okolo přístroje a police aj.)
- Při montáži kabelů je třeba kabely nainstalovat a vyvázat přehledně a kabely musí být označeny
- U přístrojů musí být nechána taková délková rezerva, aby bylo možno přístroj snadno vyjmout ze servisních důvodů. Pevně připojené kabely k přístrojům (např. napájecí) nesmí být vyvázány společně s ostatními, aby při vyjmutí přístroje nebylo nutno demontovat vyvázání
- Vedení kabeláže bude provedeno tak, aby na jedné straně byly silové a řídicí kabely a na straně druhé kabely signálové
- Pro napájení přístrojů v přístrojových skříních budou použity rozvodné panely s přepětovou ochranou, nejlépe s montážním uchycením do přístrojové skříně. Pokud je možno, tak bude napájení z jedné fáze
- V přístrojové skříně je třeba zajistit dostatečné odvětrání s ohledem na vyzařované teplo. Větrání může být buď pasivní (větrací mřížky) nebo aktivní (ventilátory).

### 8.3 Závěrečné ladění a testování funkčnosti zařízení

Na konci instalace musí odpovědný pracovník, důkladně vyzkoušet funkčnost celé nainstalované sestavy, která zahrnuje následující kroky:

- Přístroje, které používají uživatelská nastavení a vyladění musí být před předáním instalace nastaveny a vyladěny.
- Všechny signálové cesty a případně všechny používané kombinace musí být vyzkoušeny
- Obsahuje základní nastavení a nakonfigurování systému WIFI + LAN dodávaného v rámci projektu.

## 9 POŽADAVKY A NÁROKY NA PROFESI

---

### 9.1 Ochrana před úrazem elektrickým proudem

Ochrana před nebezpečným dotykovým napětím je řešena dle ČSN 33 2000-4-41 napětím SELV a samočinným odpojením vadné části od zdroje.

Část zařízení již ve svém principu pracuje pouze s napětím bezpečným.

### 9.2 Určení prostředí

V případě že určení není, požadujeme, aby dotčené prostory spadaly do kategorie - prostředí základní (resp. normální resp. obyčejné).

### 9.3 Protipožární opatření

Z hlediska požární bezpečnosti musí být dodrženo utěsnění prostupů. Prostupy kabelů a jiných elektrických rozvodů požárně dělicími konstrukcemi musí být utěsněny tak, aby se zamezilo šíření

požáru těmito rozvody. Konstrukce utěsnění prostupů kabelových a jiných elektrických rozvodů musí odpovídat požadavkům ČSN 730810 čl. 6.2.1., požární odolnost těsnění musí odpovídat požadavkům čl. 8.6 ČSN730802.

## 9.4 Péče o životní prostředí

Instalace zařízení a jeho používání nemá vliv na změnu stávajícího životního prostředí. Při provozu systému nevznikají žádné odpadové nebo zdraví škodlivé látky.

## 9.5 Požadavky na jiné technologie

### 9.5.1 Obecné zásady pro profesi silnoproud

Pro zajištění bezpečných a normou předepsaných technických podmínek provozu je nárokována oddělená el. technologická napájecí síť TN-S (bezproudové nulování), která by při správném provedení měla zabránit průnikům rušení a kolísání na síti do zařízení.

Při návrhu je nutno uvažovat s hodnotami příkonu zařízení v jednotlivých místnostech.

Zásady instalace rozvodů pro napájení techniky:

- Nulový a zemnicí vodič musí být oddělený.
- Oddělené vedení silnoproudé a strukturované kabeláže s rozestupem min 20cm.
- Poblíž míst, kde bude nainstalováno WIFI zařízení, nebudou silné zdroje elektromagnetického pole.
- Doporučujeme všechny napájecí zásuvky 230V pro AV techniku vybavit přepěťovou ochranou.

## 9.6 Nároky na providera

### Nároky na ISP (dodavatel internetového připojení)

- šíře pásma (bandwidth) odpovídající 128kbps/student nebo 512kbps/počítač nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů
- symetrické připojení bez agregace a omezení (FUP)
- vlastní nebo poskytovatelem přidělené veřejné IPv4 i IPv6 adresy
- plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)
- podpora DNSSEC a IPv6 protokolů
- zapojení poskytovatele připojení v bezpečnostním projektu FENIX resp. veřejné adresy využívané školou jsou zapojeny do infrastruktury FENIX[1] nebo ISP splňuje alespoň technické standardy definované projektem FENIX
- Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů
- Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.)
- Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, bloky wifi v určitém čase)

---

<sup>[1]</sup> V případě, kdy má ISP přidělené IP adresy od člena FENIX, musí být součástí projektu prohlášení ISP, ze kterého bude patrné, že příslušné adresy jsou v rámci FENIX propagovány. V případě, kdy má ISP vlastní ASn a není přímý člen FENIX, musí být součástí projektu prohlášení ISP, ze kterého bude patrné, že příslušné ASn propaguje do FENIX na základě smluvního vztahu některý ze členů FENIX.



- Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací a zpřístupnění jejich služeb)
- Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3954 nebo ekvivalent (NetFlow))
- Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie
- Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management)
- Systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios / Icinga)
- Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk)
- Nástroje pro centrální správu a audit ICT prostředků
- Systémy zálohování a obnovy dat serverové infrastruktury
- Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů
- Zabezpečení přístupových protokolů (SSL/TLS) služeb (např. emailové služby, webové servery, studijní a ekonomické agendy) atp.
- Podpora vzdáleného přístupu (VPN)

## 10 SERVIS

---

### 10.1 Preventivní prohlídka (Profylaxe)

K dosažení maximálních provozních výkonů systémů, funkčních celků a zařízení po celou dobu jejich životnosti, k udržení záruky a k podchycení možných rizik v provozu systému v budoucnosti je nutné pravidelně kontrolovat zařízení a udržovat ho ve funkčním stavu.

Doporučujeme minimálně 2x ročně provést preventivní prohlídku zařízení (profylaxi). Zákazník získá jistotu 100% funkčnosti zařízení a jistotu udržení záruky.

## 11 ZÁVĚR

---

Tato dokumentace navrhuje optimální řešení vybavení prostor a je koncipována jako dokumentace pro výběr dodavatele s rozšířením na provedení stavby. Tento projekt neřeší profese silnoproudu.

V Praze 12/2016

Zpracoval: Václav Bradáč