Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Analýza internetové komunikace v prostředí vzdělávacích zařízení

Adam Žingor

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Adam Žingor

Informatika

Název práce

Analýza internetové komunikace v prostředí vzdělávacích zařízení

Název anglicky

Analysis of Internet communication in the educational facilities

---

Cíle práce

Cílem práce je návrh počítačové sítě s bezdrátovým připojením a možností monitorování aktivity uživatelů ve vzdělávacím prostředí.
Dílčími cíli jsou:
• Návrh kompletního řešení a jeho konfigurace,
• Analýza dat z provozu,
• Návrh doporučení (síťové prvky, zabezpečení a možnosti pro monitorování komunikace).

Metodika

Použité metody pro získávání podkladů k bakalářské práci budou založeny na zkušenostech autora, využití odborné literatury, publikace odborných článků a sběru informací z praktické části práce. Na podkladě získaných a zpracovaných poznatků budou formulovány závěry bakalářské práce.

Praktická část práce zahrnuje:

• Analýzu současného stavu,

• Návrh počítačové sítě,

• Ověření naplnění hypotézy,

• Formulace dosažených výsledků a závěr.

Doporučený rozsah práce

30–40

Klíčová slova

Wi-Fi, Počítačová síť, LAN, WLAN, síťové prvky

Doporučené zdroje informací

HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 3., aktualiz. vyd. Brno: Computer Press, 2006. Bestseller (Computer Press). ISBN 80-251-0892-9

MEYERS, Mike. CompTIA Network+ Certification: All-in-One Exam Guide. Seventh Edition (Exam N10-007). New York City: McGraw Hill, 2018. ISBN 1260122387

SCOTT, Russell. Networking for Beginners: An Easy Guide to Learning Computer Network Basics. Take Your First Step, Master Wireless Technology, the OSI Model, IP Subnetting, Routing Protocols and Internet Essentials: Stefano Cardinale, 2021. ISBN 1801693714

Technická dokumentace a materiály společnosti Ubiquiti [online]. Dostupné z: https://help.ui.com/

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Vojtěch Novák, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 7. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 11. 03. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Analýza internetové komunikace v prostředí vzdělávacích zařízení" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2024 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Vojtěchu Novákovi, Ph.D. za vstřícnost, metodickou podporu a dobrou náladu při konzultacích. Rád bych také poděkoval všem, kteří mě v průběhu mého vzdělávání podporovali v dobrých i špatných chvílích.

Analýza internetové komunikace v prostředí vzdělávacích zařízení

Abstrakt

Bakalářská práce se zabývá problematikou počítačových sítí v prostředí vzdělávacích zařízení. Teoretická část se neomezuje pouze na základy počítačových sítí, ale detailně rozebírá i otázky zabezpečení a fungování bezdrátových technologií v této specifické oblasti. Zvláštní pozornost je věnována možnostem monitoringu internetové komunikace, poskytující komplexní pohled na bezpečnost a efektivitu sítě.

V praktické části je analyzován současný stav sítě jednoho ze vzdělávacích zařízení v České republice. Na základě této analýzy jsou navrženy konkrétní úpravy, zahrnující výměnu komponent a jejich konfiguraci, s cílem dosáhnout spolehlivého a bezpečného provozu a tím pádem i efektivnějšího integrování digitálních technologií do výuky, včetně přípravy sítě pro chytrá zařízení IoT nebo telefonování pomocí VOIP. Samozřejmostí je i vytvoření oddělené bezdrátové sítě pro hosty.

Závěr práce vychází z praktických poznatků a přináší ověření naplnění předpokladů, doplněné o konkrétní doporučení pro optimalizaci školní počítačové sítě. Tímto způsobem zasahuje nejen do technických aspektů sítě, ale také nabízí cenné podněty pro efektivnější výuku.

Klíčová slova: Wi-Fi, počítačová síť, LAN, WLAN, VLAN, síťové prvky, bezpečnost, monitoring, firewall, vzdělávání, digitální technologie

Analysis of Internet communication in the educational facilities

Abstract

This bachelor's thesis deals with the issues of computer networks in the environment of educational institutions. The theoretical part does not limit itself only to the basics of computer networks, but also analyzes in detail the security and functionality of wireless technologies in this specific area. Particular attention is paid to the possibilities of monitoring internet communication, providing a comprehensive view of the security and efficiency of the network.

The practical part analyzes the current state of the network of one of the educational institutions in the Czech Republic. Based on this analysis, specific modifications are proposed, including the replacement of components and their configuration, with the aim of achieving reliable and secure operation and thus more efficient integration of digital technologies into teaching, including the preparation of the network for smart IoT devices or VOIP telephony. Of course, a separate wireless network for guests is also created.

The conclusion of the thesis is based on practical knowledge and brings verification of the fulfillment of the assumptions, supplemented by specific recommendations for the optimization of the school computer network. In this way, it intervenes not only in the technical aspects of the network, but also offers valuable suggestions for more effective teaching.

Keywords: Wi-Fi, computer network, LAN, WLAN, VLAN, network devices, security, monitoring, firewall, education, digital techologies

Obsah

1 Úvod

S rostoucím počtem koncových zařízení připojených, ať už drátově nebo bezdrátově, do školní sítě je potřeba zajistit bezpečnou a spolehlivou komunikaci napříč všemi těmito zařízeními. Tento růst je také podpořen aktuálním rozvojem v oblasti digitalizace napříč školami zapojenými do digitalizace vzdělávání z Národního plánu obnovy, který je zaměřen především na nákup digitálních pomůcek, jako jsou například tablety nebo notebooky, tudíž se jedná o další klienty v počítačové síti, kteří budou připojeni pomocí bezdrátové technologie. (1) (2)

Jelikož se práce věnuje prostředí vzdělávacích zařízení, bude potřeba zmínit i přizpůsobení sítě konkrétním potřebám daného zařízení a dostatečně ji zabezpečit proti možným kybernetickým útokům.

V určitém okamžiku mohou některé z těchto zařízení přestat fungovat, proto bude monitoring sítě sloužit i pro odhalování závad na infrastruktuře nebo pro vyhodnocení dostatečného pokrytí bezdrátovou technologií pro spolehlivý přenos dat.

V dnešní digitální éře hraje vzdělávání pomocí digitálních učebních pomůcek klíčovou roli ve formování budoucnosti společnosti. Práce tak implementuje technologické inovace, které mohou přinést významné přínosy pro vzdělávací proces.

Součástí závěru práce je také doporučení pro další optimalizaci. Výstupní data mohou také sloužit jako zpětná vazba pro vyhodnocení kvality výuky s digitálními pomůckami, jelikož bude možné monitorovat aktivitu žáků během vyučování, případně může dojít k dodatečným úpravám zabezpečení školní sítě, například k optimalizaci filtrů pro blokaci nevhodného obsahu.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je navrhnout počítačovou síť s bezdrátovým připojením a možností monitorování aktivity uživatelů ve vzdělávacím prostředí.

Součástí návrhu je kompletní řešení a jeho konfigurace, společně s návrhem doporučení po analýze dat z jejího provozu.

2.2 Metodika

Metodika použitá v této bakalářské práci je založena na kombinaci různých přístupů, které umožňují systematicky získávat a analyzovat relevantní informace, a nakonec formulovat závěry.

Díky relevantní odborné literatuře je možno zpracovat začátek práce, který se věnuje rešerši a vysvětlení teoretických východisek potřebných pro pochopení problematiky. Následně jsou uvedeny i jednotlivé komponenty, které jsou nezbytné pro úspěšné dosažení cíle práce. Závěr teoretické části práce vysvětluje metody pro analýzu provozu v počítačové síti.

Druhá polovina práce je věnována praktické části, kdy je na základě analýzy současného stavu počítačové sítě navržena její úprava, tak aby byla schopna připojit její uživatele pomocí bezdrátové technologie a analyzovat jejich aktivitu. Autor využije své osobní zkušenosti a znalosti v oblasti problematiky zkoumaného tématu.

Po pečlivé analýze aktuálního stavu jsou formulovány předpoklady hypotéz, které slouží jako základ pro další kroky v rámci této práce.

Dílčím cílem práce je návrh kompletního řešení spolu s jeho konfigurací. Praktická část práce se mimo jiné věnuje také konfiguraci síťových prvků s cílem zajistit bezpečnost a spolehlivost celé sítě. V samostatné podkapitole je práce detailně zaměřena na konkrétní nastavení technologie pro zabezpečení počítačové sítě. Zahrnuje podrobné vysvětlení a popis všech pravidel, která jsou součástí tohoto nastavení, a dále objasňuje přínos každého pravidla. Cílem této části je poskytnout uživatelům hlubší porozumění technickým aspektům zabezpečení sítě a ukázat, jakým způsobem jednotlivá pravidla přispívají k ochraně síťového prostředí.

Pro splnění dílčího cíle analýzy dat z provozu je nezbytné implementovat efektivní řešení pro sběr dat ze síťového monitoringu. Při výběru vhodného řešení je klíčové

zabezpečit jeho spolehlivé fungování a zároveň zajistit jednoduchou možnost extrakce relevantních informací.

Na základě analýzy síťového provozu a vyhodnocení sesbíraných dat je možné ověřit naplnění hypotézy. Na podkladě získaných a zpracovaných poznatků budou formulovány závěry bakalářské práce. Tyto závěry budou reflektovat dosažené výsledky, zhodnotí jejich přínos v kontextu zkoumané problematiky a nabídnou možná doporučení pro budoucí využití nebo úpravy. To může zahrnovat opatření jako je optimalizace webových filtrů nebo úpravy rozmístění přístupových bodů pro bezdrátové připojení.

Tato opatření jsou rovněž spojena s perspektivou zkvalitnění výuky prostřednictvím digitálních pomůcek, které jsou k síti připojeny.

Celkově tato metodika umožňuje systematický a komplexní přístup k řešení zkoumaného problému, který kombinuje teoretické poznatky s praktickými zkušenostmi a výsledky. Tímto způsobem lze lépe porozumět problému a navrhnout účinná řešení, která jsou dobře promyšlená a realistická. Integrace teorie s praxí přináší hlubší pochopení dané problematiky a zvyšuje pravděpodobnost úspěchu implementace navržených opatření.

3 Teoretická východiska

Tato část práce bude věnována především obecným informacím a představením komponent a součástí, které budou později využity k návrhu sítě a analýze provozu v praktické části práce. Dále budou představeny také komunikační standardy a typy zabezpečení.

3.1 Obecné informace o počítačových sítích

Základním stavebním kamenem pro stavbu počítačové sítě jsou síťové prvky. Jedná se o komponenty, které zajišťují přenos dat pro uživatele počítačové sítě. Jejich hlavním úkolem je zasílání obdržených dat na správné koncové místo. O to, aby se data dostala tam kam mají, se starají takzvané aktivní síťové prvky, které určitým způsobem zpracovávají přenášený signál, především tedy datové pakety, což jsou bloky dat přenášené v počítačových sítích. Neméně důležitou součástí jsou i pasivní síťové prvky, jejichž úkolem není data nějakým způsobem zpracovávat, ale spolehlivě je přenášet. Jedná se například o strukturovanou kabeláž.

Samotné počítačové sítě lze dělit i dle velikosti. V domácnostech, firmách nebo jiných organizacích používáme síť lokální (LAN – Local Area Network) a pro globální počítačovou síť, jednoduše řečeno pro internet, využíváme takzvaně síť rozsáhlou (WAN – Wide Area Network). Některé lokální sítě jsou také spojovány do sítě metropolitní (MAN – Metropolitan Area Network), takovou síť využívá například hlavní město Praha pro komunikaci mezi jednotlivými úřady. (3)

3.2 Komunikační protokoly

V základu je samozřejmě důležité mít počítače fyzicky propojené do sítě tak, aby byly navzájem dostupné. Důležité je, aby oba počítače znaly a používaly stejný komunikační protokol, díky kterému dokážou vzájemně komunikovat. Přestože bude počítač, se kterým bude chtít uživatel komunikovat, využívat stejný komunikační protokol, budu ho muset mezi ostatními nějak identifikovat a vyhledat. Každý konkrétní počítač, ale dnes i například chytrý mobilní telefon, tablet a jiná „chytrá“ zařízení musejí být nastavena tak, aby byla v rámci svého komunikačního protokolu jedinečná a tím pádem byla umožněna jejich identifikace pro ostatní zařízení. (4)

Z počátku počítačové sítě vyvíjelo více firem, díky tomu to byly uzavřené a nekompatibilní systémy. Jelikož je hlavním účelem sítí vzájemné propojování, nastala potřeba pro stanovení pravidel pro přenos dat. Díky tomu v roce 1977 založila organizace ISO vlastní výbor pod názvem OSI (Open System Interconnection) a o dva roky později byl vytvořen standard s názvem „Reference Model of Open Systems Interconnection" (Referenční model propojování otevřených systémů), v praxi obvykle označovaný jako RM OSI nebo ISO/OSI. Tento model je tvořen sedmi vrstvami, které jsou rozděleny na fyzickou, linkovou, síťovou, transportní, relační, prezentační a aplikační. (5) (6)

3.2.1 TCP/IP

V současnosti nejpoužívanější sadou protokolů je TCP/IP (Transmission Control Protocol/Internet Protocol), která je zcela univerzální v tom smyslu, že ji lze využívat pro komunikaci mezi počítači s různými operačními systémy. Díky této vlastnosti se TCP/IP stalo standardem pro komunikaci v celosvětové síti Internet. Jeho historie je spjata s americkou vládní agenturou ARPA, která stála za vývojem jedné z prvních počítačových sítí. Hlavní rozvoj těchto protokolů nastal s vývojem internetu, který v podstatě vychází z tehdejší vojenské sítě ARPANET. Na rozdíl od ISO/OSI se TCP/IP model skládá ze čtyř vrstev, jejichž pořadí je znázorněno na obrázku níže. (7)

Tabulka 1 Přehled architektury TCP/IP

<table>
<tr><th>OSI</th><th>TCP/IP</th><th colspan="7">Aplikace a protokoly</th></tr>
<tr><td>7. aplikační
6. presentační
5. relační</td><td>Aplikační vrstva</td><td>telnet</td><td>FTP</td><td>TFTP</td><td>SMTP</td><td>RIP</td><td>DNS</td><td>Ostatní</td></tr>
<tr><td>4. transportní</td><td>Transportní vrstva</td><td colspan="4">TCP</td><td colspan="3">UDP</td></tr>
<tr><td rowspan="2">3. síťová</td><td rowspan="2">Síťová vrstva</td><td colspan="3" rowspan="2">IP</td><td>ICMP</td><td colspan="3" rowspan="2"></td></tr>
<tr><td colspan="2">ARP</td><td>RARP</td></tr>
<tr><td>2. linková
1. fyzická</td><td>Vrstva síťového rozhraní</td><td colspan="3">token ring</td><td colspan="2">ethernet</td><td colspan="2">jiné typy protokolů</td></tr>
</table>

Zdroj: Kutý, Michael. *ISO – OSI TCP/IP*

TCP/IP se až na pár výjimek příliš nezabývá fyzickou a linkovou vrstvou neboli vrstvou síťového rozhraní. V praxi je třeba pro přenos IP-paketů využívat zařízení vyhovující ISO/OSI a stejně tak realizovat i internetové služby. (8)

Síťovou vrstvu prakticky obsluhuje IP-protokol (Internet Protocol), který se stará o přenos takzvaných IP datagramů neboli datových paketů, které v sobě nesou směrovací

informace pro dopravu datagramu k adresátovi. Díky tomu je možno, aby je síť přenášela samostatně a může se tak stát, že k adresátovi dorazí i v jiném pořadí, než byly odeslány. (8)

Transportní vrstva zajišťuje přenos dat. Tato vrstva je narušena komunikací mezi hostiteli. Samotné řízení přenosu poskytuje spolehlivý, na spoj orientovaný přenos dat mezi dvěma počítači, které používají internetový protokol pro sdílení dat. Transportní vrstva předává data internetové vrstvě při vysílání a předává data aplikační vrstvě při příjmu. (9)

Aplikační vrstva popisuje aplikační protokoly TCP/IP a definuje, jak aplikační vrstva spolupracuje s vrstvou transportní. Aplikační vrstva poskytuje uživatelské rozhraní pro sdílení dat. Aplikační vrstva může být webový prohlížeč, e-mailový klient nebo klient pro přenos souborů. Aplikační vrstvě se tato práce bude věnovat i nadále, jelikož zahrnuje všechny protokoly vyšší úrovně, jako jsou DNS, HTTP, DHCP, FTP a další. (9)

3.2.2 IP adresa

Dalším předpokladem fungování celé sítě je také správné nastavení a zadání masky podsítě společně s IP adresou. IP adresa se zapisuje ve 32bitovém číselném tvaru, který je tečkami rozdělen na 4 menší části, takový tvar je přezdíván IPv4. Každá z těchto částí se pohybuje v rozmezí hodnot 0-255. V praxi jsme však výběrem IP adresy pro zařízení v místní síti výrazně omezeni, jelikož na principu TCP/IP fungují i všechny ostatní velké sítě a mezi ně patří i internet. Pro zachování celosvětového pořádku v používání IP adres se tak používá rozdělení do tříd, které je znázorněno v tabulce 2. (4)

Tabulka 2 Třídy IP adres

Třída	Rozsah IP adres
Třída A	1.x.x.x – 126.x.x.x
Třída B	128.0.x.x – 191.254.x.x
Třída C	192.0.0.x – 223.254.254.x
Třída D	224.0.0.x – 239.254.254.254

Zdroj: Kostrhoun, Aleš. *Stavíme si malou síť* (2001)

Třída D je určena pro multicast (způsob posílání jedné zprávy více počítačům současně). Někdy se ještě v tabulce tříd uvádí třída E, která je určena pro experimentální účely.

IP adresu musí mít každý počítač jinou, jinak by nebylo možné jej od sebe navzájem rozlišit. Jeden počítač může mít i více IP adres, pokud má více síťových adaptérů.

IP adresu si nelze samostatně určit, přiděluje je mezinárodní autorita pověřená správou veřejných IP adres. V současné době používaná verze IPv4 umožňuje adresovat okolo 4.2 miliardy IP adres, což se v počátku zavádění této verze zdálo jako dostatečné množství, později ovšem začaly IPv4 adresy docházet a začala pomalu nastupovat verze IPv6. Problém zde nastává v nekompatibilitě verzí IPv4 a IPv6.

Řešením je takzvané dvojí adresování, kdy zařízení dostane jak IPv4, tak i IPv6 adresu. Přechod na IPv6 je tak dlouhodobý proces, který stále probíhá. V roce 2024 již většina velkých poskytovatelů nabízí IPv6 připojení, ale stále existují miliony zařízení, která IPv6 nepodporují. Jedna z technik pro využití úspory adres je NAT (Network Address Translation), která umožňuje více zařízením sdílet jednu veřejnou IP adresu. (10)

3.2.3 Neveřejné síťové rozsahy

Výše uvedená tabulka IP adres znázorňovala rozdělení IP adres do tříd z celosvětového hlediska. Pro tvorbu LAN sítě, bude spíše zajímavé rozdělení takzvaných soukromých IP adres (private subnets). Soukromé síťové adresy nejsou přiděleny žádné konkrétní organizaci a může je využívat kdokoli bez nutnosti souhlasu internetových registrů. IP adresy takového rozsahu jsou určené pro využití při výstavbě lokálních sítí jako jsou domácí, školní nebo firemní sítě. Adresy z privátního rozsahu jsou k nalezení i v MAN sítích. Rozsah adres definuje dokument RFC1918 mezinárodní organizace IETF (Internet Engineering Task Force), která se zabývá vývojem a standardizací protokolů pro internet. Tyto adresy jsou uvedeny v tabulce 3.

Tabulka 3 Privátní IP adresy

Třída	**Rozsah IP adres**
Třída A	10.0.0.0 – 10.255.255.255
Třída B	172.16.0.0 – 172.31.255.255
Třída C	192.168.0.0 – 192.168.255.255

Zdroj: Moskowitz, Robert; Karrenberg, Daniel; Yakov, Rekhter; Lear, Eliot; Jan Geert, de Groot. *Address Allocation for Private Internets* (1996)

Rozsahy ze sítě 10.0.0.0 bývají obvykle využívány ve firmách, školách nebo jiných institucích, kde se nachází velké množství zařízení připojených k síti. Rozsah třídy B je pak určený pro středně velké sítě, zatímco rozsah 192.168.0.0 bývá obvykle využívaný v domácích sítích. (10)

Takové adresy jsou pro ostatní zařízení v internetu neviditelné a o jejich oddělení od sítě Internet se stará router, který je pomocí NAT technologie a pravidel ve firewallu oddělí, zároveň však umožní zařízením s takovou adresou do internetu komunikovat. Routeru a firewallu se bude tato práce věnovat později.

3.2.4 Maska podsítě

Pro IP adresu je neodmyslitelnou součástí také síťová maska, též nazývána jako maska podsítě. Jedná se o 32bitové číslo, které nám umožňuje poznat, která část adresy je síťová a která je hostitelská pomocí jedniček a nul. Hostitelské bity jsou nastaveny na nulu a síťové bity na jedničky. Jak je vidět v tabulce 1, adresy mají kromě třídy A vždy stejné počáteční dvě části, oddělené tečkami. Následně dochází většinou ke změně pouze posledních dvou, nebo dokonce jen jedné části adresy. Dle formátu masky je možné poznat, pro kolik zařízení je síť určena. Adresa "255" je vždy přiřazena vysílací adrese a adresa "0" je vždy přiřazena síťové adrese. Ani jednu z nich nelze přiřadit hostitelům, protože jsou vyhrazeny pro tyto speciální účely. Cílem masek podsítí je jednoduše umožnit proces vytváření podsítí. Výraz "maska" se používá proto, že maska podsítě v podstatě používá vlastní 32bitové číslo k maskování IP adresy. (11)

Počet a typ IP adres, které daná místní síť vyžaduje, je možno určit na základě její výchozí masky podsítě, které jsou uvedeny v tabulce 4.

Tabulka 4 Výchozí masky podsítí

Třída	**Maska podsítě**
Třída A	255.0.0.0
Třída B	255.255.0.0
Třída C	255.255.255.0

Zdroj: Empson, Scott. *CCNA Kompletní přehled příkazů* (2009)

Standardní moderní síťový prefix používaný pro IPv6 i IPv4 je zápis CIDR (Classless Inter-Domain Routing). Adresy IPv4 reprezentované v notaci CIDR se nazývají síťové masky a určují počet bitů v prefixu adresy za oddělovačem lomítka vpřed (/). CIDR prefix je zapisován ve tvaru IP adresa/prefix. Prefixová délka určuje, kolik bitů adresy tvoří síťovou část. Například, pokud máme CIDR prefix "192.168.1.0/24", znamená to, že prvních 24 bitů (3 oktety) tvoří síťovou část, a zbývajících 8 bitů tvoří část určující konkrétní zařízení v této síti. Prefixová délka může být různá a určuje, jak velká síť je definována tímto prefixem.

Čím vyšší je prefixová délka, tím menší je počet dostupných IP adres v síti, protože více bitů je využito pro identifikaci sítě. K výpočtu potřebného prefixu (masky) je nejvhodnější využít některou z volně dostupných kalkulaček na internetu nebo si ho dohledat v tabulce s hodnotami prefixů pro IPv4 CIDR bloky s dostupnými adresami a maskami podsítí. (11)

3.2.5 DHCP

Protokol DHCP (Dynamic Host Resolution Protocol) slouží k dynamickému přiřazování IP adres jednotlivým počítačům a v dnešní době i všem jiným zařízením, která se budou chtít připojit do počítačové sítě. V sítích TCP/IP totiž musí mít každé takové zařízení přiřazenou tak zvanou IP adresu. Pokud není v síti nainstalovaný DHCP server, je nutno veškeré IP adresy přiřazovat ručně, tomuto způsobu se říká statické přidělování IP adres. Díky DHCP serveru tuto problematiku není třeba řešit a DHCP server bude IP adresy jednotlivým zařízením přidělovat automaticky, pokud si o ni zažádají. (4)

3.2.6 DNS

Jelikož by pro člověka, jakožto uživatele, bylo složité si zapamatovat všechny potřebné IP adresy k využívání jeho oblíbených aplikací na internetu, existuje pro každou IP adresu takzvané doménové jméno. DNS (Domain Name Service) slouží jako jakýsi telefonní seznam právě pro vazbu mezi jménem počítače a IP adresou. DNS obsahuje jednotlivé záznamy (též nazývané jako DNS věty) a odpovídá tak za správné nalezení IP adresy webových stránek, respektive příslušné domény. Například pokud uživatel zadá do počítače „google.cz“, DNS musí pro uživatele nalézt správnou IP adresu a díky tomu dojde k navázání spojení na příslušný web i bez znalosti jeho IP adresy. (8)

Kromě těchto protokolů jsou součástí sady TCP/IP například i protokoly ICMP (Internet Control Messaging Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol), SNMP (Simple Network Protocol) a další. (4)

3.3 Aktivní prvky

Jak již bylo zmíněno v obecných informacích, aktivní prvky jsou zařízení, která se aktivně podílejí na komunikaci v síti a jsou napájena z elektrické sítě. Mají vlastní procesor a paměť a jsou schopna samostatného fungování. Na rozdíl od pasivních prvků, jako jsou

kabely a konektory, aktivní prvky zpracovávají data a zajišťují jejich přenos mezi zařízeními v síti.

3.3.1 MAC adresa

Ještě předtím, než budou zmíněny samotné aktivní prvky, je důležité vysvětlit co je to MAC adresa (z anglického „Media Access Control“). Jedná se o jedinečný identifikační prostředek síťového zařízení. Někdy se také označuje jako „fyzická adresa“. Tuto adresu získávají síťová zařízení (nejčastěji síťové karty) již při výrobě. MAC adresa se dělí na dvě poloviny. První polovina označuje výrobce, druhou polovinu si výrobce určuje sám a může ji například použít, jako výrobní číslo daného zařízení. Důležité je, aby se v jedné síti nenacházely dvě zařízení se stejnou MAC adresou, jelikož jak bylo již zmíněno, slouží k jednoznačné identifikaci. Pokud by se v síti objevila dvě zařízení se stejnou MAC adresou, mohly by nastat problémy s komunikací. MAC adresa se zapisuje ve tvaru 01-23-45-67-89-ab nebo 01:23:45:67:89:ab. (12)

3.3.2 Router a gateway

Směrovač (router) je zařízení, které se specializuje na směrování datových paketů mezi různými sítěmi nebo podsítěmi. Jeho hlavním účelem je rozhodování o tom, kam mají být data směrována na základě jejich IP adresy. Ve většině případů router přenáší data mezi LAN a WAN sítěmi a je označován jako nejinteligentnější aktivní prvek, s nímž se dá při výstavbě běžné domácí nebo firemní sítě potkat. Router pracuje na síťové vrstvě a rozhoduje o optimální cestě pro přenos dat z jednoho místa na druhé. Je schopen pracovat s více různými protokoly a směrovat data mezi nimi. Propojuje tedy mezi sebou počítače, aniž by musel poskytovat přístup k internetu, nicméně právě to je jeho hlavní úkol. Neméně důležité je také provádění NAT, což v praxi umožní více zařízením v LAN, sdílet jednu veřejnou IP adresu pro přístup na internet. (13) (14)

Obrázek 1 Ubiquiti UniFi Dream Router

Zdroj: Ubiquiti, Inc.

Pro efektivní směrování paketů používá směrovač interní směrovací tabulku (routing table). Směrovač přečte hlavičku paketu, aby zjistil, kam směřuje, a poté se poradí se směrovací tabulkou, aby zjistil nejefektivnější cestu k danému cíli. (13)

Jako router je často označována i výchozí brána (gateway), což je obecně zařízení nebo software, který spojuje dvě různé sítě a umožňuje jim komunikovat. Na rozdíl od routeru však může pracovat na různých vrstvách. Může to být fyzický hardware, jako router, nebo software, který funguje jako rozhraní mezi různými sítěmi. I když se funkčnost směrovače a výchozí brány liší, v dnešní době je právě router, společně s výchozí bránou a firewallem, fyzicky jedno zařízení, kterému se tato práce bude věnovat později. Dnes je téměř samozřejmost, že je součástí i směrovač (switch). Proto, když dnes někdo vysloví slovo router, vybaví se nám jakési zařízení typu „vše v jednom“, kdy takové zařízení obsahuje výchozí bránu, směrovač, firewall a switch. V domácím prostředí se pak stále častěji nacházejí Wi-Fi routery, což znamená, že má toto zařízení v sobě navíc i bezdrátový přístupový bod. Příklad Wi-Fi routeru je znázorněn na obrázku 1.

3.3.3 Switch

Přepínače (switche) jsou dalším aktivním prvkem pro počítačovou síť. Hlavní funkcí switche je vyřešení nedostatku portů pro fyzické připojení dalších počítačů nebo jiných zařízení do počítačové sítě. Dnes již plně nahradily dříve používané huby (rozbočovače), které přijatý paket zaslaly na všechny ostatní porty. Switch je na rozdíl od hubu mnohem chytřejší zařízení, které pakety nasměruje přímo na příslušný port. (15)

U portů je důležitý jejich rychlostní standard a jejich typ. Standardem je dnes gigabitový port RJ-45, případně 10 gigabitový port SFP+.

Při výběru je velmi důležité, jestli je programovatelný (spravovatelný) nebo neprogramovatelný a dále také to, jestli umí pracovat s VLAN. Pomocí virtuálních LAN je možné oddělit určitý síťový provoz od ostatního, a kromě přehlednosti nám umožňují síť lépe zabezpečit.

Dalším parametrem při výběru switche je i to, zdali a na kolika portech umí POE (Power over Ethernet). Díky PoE je možno napájet další aktivní prvky bez potřeby je napájet externím napájecím zdrojem. V praxi tak není nutné, například u přístupových bodů, řešit zda je v blízkosti elektrická zásuvka. U PoE je důležité si dát pozor na jeho standard a u switche pak na to, kolik wattů je schopen zařízením napájeným pomocí PoE dodat. Například switch na obrázku 2 má maximální výkon PoE+ na jeden port je 32 W a maximální PoE výkon tohoto modelu je 95 W. (16)

Obrázek 2 Ubiquiti USW-24-POE Gen2

Zdroj: Ubiquiti, Inc.

3.3.4 Přístupový bod

Přístupový bod, zkráceně AP (z anglického názvu ,,Access Point) zprostředkovává bezdrátové spojení mezi jednotlivými zařízeními. Takové spojení většinou probíhá mezi bezdrátovým hostem a nějakým zařízením v LAN nebo je za jeho pomoci umožněno koncovým zařízením přistupovat do internetu.

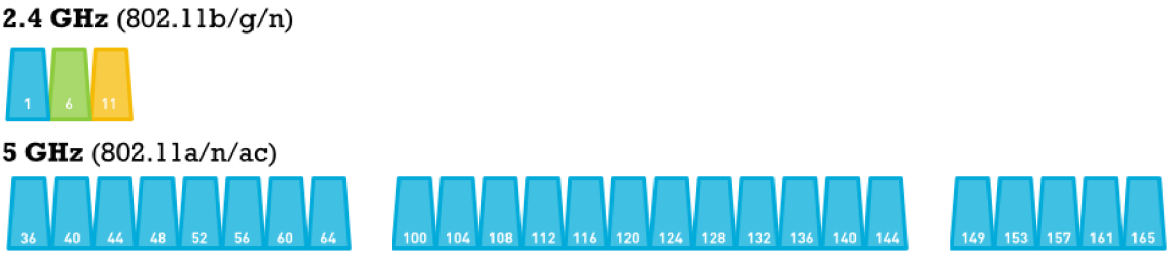
Samotný přístupový bod se v praxi bere jako základ bezdrátové sítě. Jedná se o hardware obsahující radiový vysílač/přijímač a zdířku RJ-45 pro připojení ke zbytku počítačové sítě. Nejčastěji jsou přístupové body zapojeny do switche, ze kterého se i pomocí PoE napájí. (14)

Kromě vysílacího výkonu je při výběru přístupového bodu důležité, jaký bezdrátový standard podporuje. Dnešní nejrozšířenější standard je Wi-Fi 6, též označovaný jako IEEE 802.11ax, který je provozován ve frekvenčním pásmu 5 GHz. Nicméně na trhu jsou dnes již k dispozici přístupové body s podporou Wi-Fi 6E. (17)

Běžné Wi-Fi sítě dnes používají frekvenční pásma 2,4 GHz a 5 GHz, nově je možné provozovat Wi-Fi i v pásmu 6 GHz. Pásma se od sebe odlišují svými vlastnostmi a nejsou zpětně kompatibilní. Mezi hlavní výhodu pásma 2,4 GHz náleží obecně lepší dosah a lepší průchodnost přes překážky, jako jsou například zdi nebo nábytek. Dnes se toto pásmo už dá považovat za zastaralé, a to především z důvodu jeho zahlcenosti a pomalejší propustnosti. Jeho hlavním problémem je malý počet dostupných kanálů a také to, že toto pásmo využívá mnoho jiných zařízení a může docházet k rušení. Přesto se i dnes toto pásmo stále nechává zapnuté, a to především z důvodu zpětné kompatibility se staršími zařízeními. (18)

Oproti tomu lze v pásmu 5 GHz dosáhnout mnohem vyšších přenosových rychlostí, pokud ho koncové zařízení podporuje. Jeho nevýhodou je oproti pásmu 2,4 GHz kratší dosah. Obecně platí, že čím vyšší je frekvence, tím kratší je vlnová délka, a proto je pro pásmo 5 GHz mnohem složitější prostupovat překážkami. Díky širokému spektru dostupných kanálů, které se vzájemně nepřekrývají, což znázorňuje i obrázek 3, lze například osadit do prostoru více přístupových bodů a tím zajistit dostatečné pokrytí, bez vzájemného rušení. K větší propustnosti lze využít i možnosti zvětšení šířky kanálu, tato možnost je u pásma 2,4 GHz značně omezená, jelikož může snadno dojít k vzájemnému překrývání kanálů mezi sebou. Aby k překrývání nedošlo, používají se výhradně kanály 1, 6 a 11, proto může snadno dojít ke vzájemnému rušení právě těchto kanálů, a to především v budovách s větším množstvím přístupových bodů, které se nachází blízko sebe. (18)

Obrázek 3 Rozdíl šířky frekvenčního pásma 2,4 GHz a 5 GHz



Zdroj: Metageek

Pokud je potřeba Wi-Fi připojením pokrýt větší prostor, je vhodné instalovat přístupové body do sítě Mesh. Jednotlivé AP pak tvoří jednu síť a koncové zařízení (např. mobilní telefon) si je mezi sebou automaticky přepojuje a nedochází tak k výpadkům při fyzickém přemístění. Zároveň je schopna taková síť mít jen jedno SSID, což je označení pro identifikátor (název) Wi-Fi sítě. (19)

3.4 Zabezpečení

Kromě pravidelných aktualizací aktivních prvků, je především potřeba myslet na zabezpečení celé sítě už při jejím návrhu a rozumět všem podstatným pojmům v této oblasti. Níže jsou proto jednotlivě vysvětleny.

3.4.1 WPA

Zabezpečení standardem WPA (Wi-Fi Protected Access) se u bezdrátových sítí Wi-Fi používá již od roku 2003. Bezpečnostní standardy WPA se postupně vyvíjely v závislosti na aktuálních bezpečnostních hrozbách. Aktuální verzí WPA je WPA3, které kromě nových funkcí umožňuje i robustnější ověřování a udržuje tak i dnes bezdrátové sítě dostatečně bezpečné. WPA3 obsahuje další funkce speciálně pro osobní a podnikové sítě. Technologie WPA3 je odolná i proti offline slovníkovým útokům, kdy se protivník pokouší určit síťové heslo vyzkoušením možných hesel bez další interakce se sítí. (20)

Nutno konstatovat, že WPA3 dnes ještě není tolik rozšířené a většina sítí funguje na standardu WPA2, kdy zachovávají zpětnou kompatibilitu pro zařízení, které podporují pouze WPA. Sítě s WPA2 již nejsou považovány za ty nejlépe zabezpečené, avšak ve většině případech je nutné kompatibilitu sítě s WPA2 zachovat, jelikož spousta zařízení standard

WPA3 nepodporuje. Se sítěmi s velmi zastaralým standardem WEP, se dá dnes setkat už jen velmi zřídka, jelikož tento standard je již dlouhou dobu prolomen. (21)

3.4.2 VLAN

VLAN (Virtual Local Area Network) má za úkol oddělit fyzickou síť (LAN) na několik oddělených virtuálních sítí. Jedná se o formu logické segmentace, která může být učiněna nezávisle na fyzické poloze uživatelů sítě. V praxi se pak VLAN chová jako fyzická LAN, pakety mířící mimo danou VLAN musí být směrovány přes router, aby je bylo možné doručit na cílové místo. (22)

Separátní VLAN jsou vhodné například pro řízení provozu na síti, dnes jsou však považovány, pokud je vše správně nastaveno ve firewallu, jako základní stavební kámen bezpečnosti lokální sítě.

Ve většině případů se VLAN směrují na routeru, avšak aby bylo možné zvolit porty, na kterých VLAN bude, je zapotřebí použít spravovatelný (řízený) switch, na kterém se vše nastaví.

VLAN pak mohou být na portech switche ve dvou režimech, a to buď jako tagovaná (tagged), kdy každé zařízení, musí své pakety označit značkou, do které VLAN maji být pakety zařazeny. V opačném případě je switch v závislosti na nastavení portu zařadí do netagované VLAN, nebo paket zahodí. V případě netagovaného (untagged) portu platí, že taková VLAN může být na daném portu pouze jedna. Funguje totiž jako výchozí, takže po připojení zařízení do takového portu jej není již potřeba dále nastavovat.

3.4.3 Firewall

Po vytvoření virtuálních lokálních sítí (VLAN) je potřeba také jejich provoz oddělit. Samotné vytvoření virtuální sítě, totiž jejich provoz navzájem neizoluje.

Firewall neslouží jen pro bezpečnost mezi vnitřními sítěmi, ale jedná se o zařízení nebo software, který funguje jako filtr a chrání tak interní síť. Síťový firewall je nejčastěji implementován přímo v routeru. Typická práce firewallu je blokovat nebo povolit trasu daného paketu v síti. Firewall v dnešní podobě má možnost určit, zda je daný paket součástí již existujícího spojení. Takzvaný Next-Generation Firewall (NGFW) umí pracovat na několika vrstvách OSI modelu, díky čemuž může filtrovat provoz mnohem efektivněji než klasický firewall. Moderní firewall kombinuje velké množství různých funkcí a jeho správná konfigurace je tak nesmírně důležitá pro celou bezpečnost počítačové sítě. Samotná

konfigurace moderního firewallu ve většině případů funguje na principu seznamu řízení přístupu (ACL), kdy se aplikuje pravidlo na určité rozhraní, které řídí buď přicházející nebo odcházející provoz. (23)

UTM (Unified Threat Management) je označení pro sloučení tradičního firewallu společně s dalšími bezpečnostními systémy jako je IPS, load balancing a další. (23)

3.5 Možnosti sledování provozu

Pokud existuje požadavek na sledování provozu na síti, je zapotřebí nasadit nějaký způsob jejího monitoringu. Řada technik označujících termín monitorování sítě se používá k sledování a kvantifikaci toho, co přesně se v síti děje. Mechanismy používané ke sběru dat ze sítě se klasifikují jako pasivní nebo aktivní, ačkoli oba mohou být použity společně. (24)

3.5.1 Pasivní monitoring

K pasivnímu sběru dat dochází z určitého síťového prvku. Data mohou být sbírána za účelem pozorování aktuálního provozu. Data mohou být sbírána v surové podobě (tj. nemodifikovaná) nebo jsou nějakým dalším způsobem, rovnou při jejich sběru, upravována, aby z nich bylo později možné snadněji získat důležité informace. Data sbíraná metodou pasivního monitoringu jsou většinou určena k pozdější analýze, to ale nemění nic na tom, že mohou být použita jako předmět analýzy v reálném čase. Hlavním znakem pasivního monitoringu zůstává fakt, že nijak aktivně nezasahuje do provozu, který je sledován. (24)

3.5.2 Aktivní monitoring

Aktivní monitoring se naopak zabývá zkoumáním problémů v síti nebo měření jejího výkonu. Takový přístup spočívá v odesílání dat do sítě a následném měření, například odezvy HTTP požadavků, a sběru informací. Data z aktivního monitoringu mohou být nápomocna za účelem úpravy sítě pro vylepšení stability nebo kvality přenosu dat v ní. (24)

3.5.3 Deep Packet Inspection

DPI (Deep Packet Inspection) neboli hloubková kontrola paketů je pokročilým nástrojem pro zkoumání přenášených dat v počítačové síti. Zatímco běžné filtrování paketů dokáže přečíst pouze základní informace o paketu, jako je odesílatel, příjemce a čas odeslání, DPI umí získávat informace nad rámec hlaviček paketů, což umožňuje pokročilejší a

proaktivnější monitorování, a především lze využitím této funkce posílit zabezpečení sítě, jelikož DPI může pracovat ve spojení s firewallem a blokovat škodlivý obsah. (25)

Pokud je funkce DPI zapnuta, proniká až k jádru paketu a shromažďuje a hlásí informace na aplikační vrstvě, například objem provozu konkrétní aplikace používané jednotlivými uživateli. Nutno však poznamenat, že funkce DPI je výpočetně náročná a může tak ovlivnit výkon sítě, pokud není zařízení, na kterém je DPI prováděno, dostatečně výkonné. (26)

3.5.4 Vlastní DNS server

Jednodušší možností pro sledování provozu může být vytvoření vlastního DNS serveru. V síti se nastaví jako výchozí a uživatelé přes něj směrují své požadavky. Vlastní DNS server pak figuruje jako prostředník mezi tím reálným a samotným uživatelem. Díky tomu lze provádět monitoring navštěvovaných webů.

Uživatelé ale mohou takový server jednoduše obejít, a to tím, že se rozhodnou použít jakýkoliv jiný. Proto metoda monitoringu pomocí vlastního DNS serveru není příliš efektivní.

4 Vlastní práce

Tato část práce je věnována podrobné konfiguraci síťových prvků pro správné fungování počítačové sítě v prostředí vzdělávacího zařízení s možností bezdrátového připojení pomocí Wi-Fi a možností sledování provozu pro následnou analýzu komunikace na počítačové síti.

Pro účely vypracování byla vybrána základní škola, která již svoji infrastrukturu má. Bylo tudíž potřeba analyzovat současný stav a navrhnout ideální řešení pro konkrétní případ, včetně výběru nových aktivních prvků.

Závěr této kapitoly je věnován ověření naplnění hypotéz.

4.1 Analýza současného stavu

Nejprve bylo potřeba zjistit, v jakém stavu se aktuální infrastruktura nachází, a to nejen co se týče výchozí brány, zabezpečení a přístupových bodů. Důležité je též zjistit, jaká zařízení se budou k síti připojovat a navrhnout tak ideální řešení pro zajištění jejich spolehlivé konektivity.

4.1.1 Fyzické rozložení stávajících prvků

Hlavní budova školy je rozdělena na několik částí. V suterénu školy se nachází šatny a jídelna. V přízemí je ředitelna, kancelář hospodářky školy, hlavní vchod a učebny. V patře se nachází další učebny a na půdě se včetně dalších učeben nachází ještě počítačová učebna.

Na každém patře, kde jsou učebny, se kromě několika kabinetů nachází i dvě rackové skříně, což jsou montážní plechové skříně, kam se umisťují aktivní i pasivní síťové prvky, též jsou označovány jako rozvaděče. Každá z nich je umístěna na jednom z konců chodby. Další rack se nachází v PC učebně a suterénu. Rack, ve kterém se nachází přívodní konektivita a router, se nachází v přízemí, ve třídě 209.

V každé učebně se nachází přístupový bod pro bezdrátové připojení, další jsou rozmístěny v kabinetech a kancelářích.

4.1.2 Diagnostika současného stavu

Nejdůležitějším místem zůstává třída 209, kde je umístěn „hlavní“ rack s přívodem konektivity od poskytovatele, routerem, switchem, UPS a NAS.

Od tohoto „centrálního“ místa je dále po celé škole vedena strukturovaná kabeláž do ostatních, níže uvedených, racků. Z těch je pak vedena strukturovaná kabeláž do přístupových bodů ve třídách, případně do dalších zařízení, která jsou součástí školní infrastruktury. Přístupové body jsou očíslovány dle čísla učebny nebo místnosti, ve které se nacházejí.

Racky v budově školy jsou očíslovány jako:

- R0 – Suterén, chodba;
- R1 – Třída 209, přízemí;
- R2 – Přízemí, chodba;
- R3 – Přízemí, chodba;
- R4 – Patro, chodba;
- R5 – Patro, chodba;
- R6 – PC učebna.

4.1.3 Současné aktivní prvky

Před samotným výběrem a následnou implementací vhodných komponent je zapotřebí si udělat představu o aktuálním fungování sítě, a také vědět, jaká zařízení se k ní budou připojovat. Neméně důležité je znát i jejich počet.

Současně se v síti nachází:

- router: Ubiquiti EdgeRouter X;
- 7x switch (přepínač): TP-Link TL-SG1024;
- přístupové body (AP): 26x Ubiquiti UAP AC LR;
- controller (kontrolér) pro správu přístupových bodů: Ubiquiti Cloud Key Gen2 Plus (centrální bod pro správu).

V každé učebně, kabinetu a kanceláři se nachází alespoň jeden stolní počítač. Dále je nutné zajistit bezdrátovou konektivitu v každé místnosti pro práci na zařízení, která se k síti budou připojovat bezdrátově. Z tohoto důvodu má již škola v provozu větší počet přístupových bodů. Neméně důležitá je informace o využívání většího množství žákovských tabletů a učitelských notebooků. Dále je nutné počítat i s dalšími zařízeními, které se budou ke školní síti připojovat, jako jsou různá IoT čidla, například pro zavlažování, nebo VOIP telefony. Aktuální rychlost přístupu k internetu je 80/80 Mbps. Vzhledem k počtu připojených zařízení do sítě, se tato rychlost aktuálně jeví jako nedostatečná. Proto bude

nutné vyjednat s poskytovatelem internetového připojení větší rychlost přípojky a s tím související výměnu antény na střeše budovy. Každopádně tato úprava je již záležitostí poskytovatele a přímo nesouvisí s nastavením a optimalizací vnitřní sítě školy.

4.1.4 Současná konfigurace

Síť aktuálně využívá pouze jeden rozsah IP adres, tudíž zde nejsou žádné VLAN. Zabezpečení je aktuálně řešeno jen zaheslovaným přístupem k Wi-Fi. Po připojení do sítě je možné se dostat do všech zařízení, která nejsou dále chráněna heslem.

Přístupové body jsou označeny a je jim přiřazena statická IP adresa. Jako výchozí brána slouží Ubiquiti EdgeRouter X s IP 10.0.1.1, maska sítě je 255.255.252.0. Firewall je prakticky ve výchozím nastavení a žádná pokročilejší detekce nežádoucích jevů zde není aktivní.

4.2 Očekávání hypotéz

Tato podkapitola se věnuje formulaci hypotéz, u kterých dojde na konci práce k verifikaci nebo falzifikaci na základě jejich předpokladů. Je tedy potřeba jasně specifikovat, co se bude zkoumat a stanovit očekávání po implementaci nového řešení pro místní počítačovou síť.

4.2.1 Zabezpečení

Jedním z předpokladů je implementace nového řešení pro vylepšení zabezpečení počítačové sítě. Očekáváno je takové řešení, které bude umět detekovat anomálie v reálném čase a případně i blokovat nepovolený obsah.

Očekává se také rozdělení místní sítě na několik podsítí, především oddělení části pro žáky od části pro vyučující.

4.2.2 Monitoring síťových prvků

Dalším předpokladem je zajištění síťového monitoringu, který bude umět detekovat výpadky jednotlivých aktivních prvků.

Součástí je i přehledné rozhraní, kde bude jasně uvedeno, v jakém stavu je daný síťový prvek – například zda v pořádku pracuje, dochází k jeho aktualizaci, je odpojený, případně zda došlo k nějaké chybě.

4.2.3 Monitoring aktivity uživatelů

Síťový monitoring bude umožňovat monitorovat aktivitu uživatelů na základě navštěvovaných webových stránek a používaných aplikací. Data z monitoringu bude možné filtrovat dle uživatelů, kde bude přehledně vidět, v jaký čas uživatel danou aplikaci používal a kolik přenesených dat během této aktivity využil.

Co se týče samotného ověření naplnění této hypotézy, tak na základě sesbíraných dat bude umožněno ověřit, zda je monitoring skutečně přínosný a dále bude možné vydat doporučení dle chování uživatelů, a to ať už pro samotné uživatele počítačové sítě nebo pro pozdější vylepšení síťového zabezpečení, případně pro optimalizaci výkonu sítě.

4.3 Návrh řešení

Tato část práce je věnována výběru samotných komponent pro rekonstrukci. V závěru se věnuje jejich instalaci a odstranění nalezených problémů.

4.3.1 Výběr komponent

Jelikož škola využívá přístupové body od výrobce Ubiquiti, které jsou naprosto dostatečné pro zdejší provoz a jsou spravovatelné v systému UniFi, dává zde smysl výměna routeru za router kompatibilní právě s Ubiquiti UniFi. Dále dojde k výměně přepínače (switche) v každém rozvaděči (racku), jelikož aktuální switche nejsou spravovatelné a není tak možné na nich nastavovat porty pro VLAN. Dále bude zapotřebí zajistit lepší konektivitu do sítě Internet od místního poskytovatele.

Jako router byl vybrán Ubiquiti UniFi Dream Machine Special Edition (UDM-SE), který zajistí potřebný výkon i pro nasazení DPI a zároveň bude sloužit jako centrální bod pro správu přístupových bodů a směrovačů.

Důvodem výběru tohoto zařízení je jeho status jako nejnovější model v řadě UniFi, což zaručuje dlouhodobou softwarovou podporu. Dalším důvodem výběru právě toho modelu byl fakt, že na něm bude možné hostovat aplikaci UniFi, ze které bude možné spravovat přístupové body, které už škola má nainstalované. Zároveň tento router nabízí i přehledný a pokročilý firewall, který bude potřebný pro naplnění hypotézy v oblasti zabezpečení.

V neposlední řadě ho lze použít i jako centrální bod kamerového systému, což může být benefitem, pokud by se pro něj škola v budoucnu rozhodla, například z důvodu zabezpečení majetku.

Při výběru přepínačů bylo třeba uvažovat nad využitím jejich funkcí jako je PoE nebo možnost jejich vzájemného propojení optickými kabely do budoucna. Switche s funkcí PoE bude vhodné instalovat do rozvaděčů na chodbách u učeben za účelem napájení přístupových bodů. Naopak není potřeba tuto funkci mít například v PC učebně.

Po zvážení všech možných scénářů došlo k výběru různých typů přepínačů od Ubiquiti, kdy všechny jsou z řady UniFi, aby bylo možné je centrálně spravovat. Zohlednit bylo potřeba také jejich výkon pro PoE. Vybrané prvky jsou uvedeny v tabulce 5. (27)

Tabulka 5 Komponenty pro realizaci rekonstrukce

Rack	Zařízení	Typ
R0	Ubiquiti USW 24 PoE	PoE Switch
R1	Ubiquiti UDM-SE	Router
R1	Ubiquiti USW Pro 24	Switch
R2	Ubiquiti USW 24 PoE	PoE Switch
R3	Ubiquiti USW 24 PoE	PoE Switch
R4	Ubiquiti USW 24 PoE	PoE Switch
R5	Ubiquiti USW 24 PoE	PoE Switch
R6	Ubiquiti USW 24 G2	Switch

Zdroj: vlastní zpracování

4.3.2 Instalace komponent

Než došlo k samotné instalaci nových prvků, bylo vhodné ještě předtím zajistit zvýšení rychlosti připojení internetu. Po instalaci nové antény místním poskytovatelem došlo ke zvýšení konektivity až na 300/300 Mbps.

Fyzická montáž samotných síťových prvků pak probíhala poměrně jednoduše a standardně, jelikož se všechny prvky instalovaly do rackových skříní namísto starých prvků.

Jediné, na co bylo potřeba dát pozor bylo zapojení switchů. Konkrétně bylo rozhodnuto, že přívod do switche bude pro přehlednost vždy na poslední pozici. Dále bylo potřeba všechna zařízení, která vyžadují PoE, připojit do příslušných portů, jelikož USW 24 PoE nemá PoE na všech 24 dostupných portech. Díky tomu bylo možné značně zredukovat množství PoE adaptérů v rozvaděčích a rozvaděče začaly na první pohled působit

„uklizenějším“ dojmem. Vzhledem k umístění rozvaděčů na chodbách školy bylo vhodné provést i estetické úpravy v této oblasti.

4.3.3 Nález problému ve strukturované kabeláži

Po prvním zapnutí a oživení celé sítě byla zjištěna jedna nepříjemná záležitost. Fyzické propojení strukturovanou kabeláží mezi R1 a R3 fungoval pouze rychlostí 100 Mbps, což z prvopočátku značilo problém v samotné kabeláži. Po otestování spoje pomocí testeru UTP kabelů bylo zjištěno, že je kabel na více žílách poškozený. Oprava však nebyla nutná, jelikož tato místa byla propojena dalšími záložními kabely, které bylo možné využít.

Protože kabelů zde bylo více a vybrané switche umožňují agregaci (což znamená, že lze využít 2 kabely jako jednu linku), bylo zde možné rychlost navýšit až na 2000 Mbps. V ostatních rozvaděčích už toto možné nebylo, protože je do nich zaveden pouze jeden CAT5e kabel z centrálního racku R1. Všechny ostatní racky byly propojeny rychlostí 1000 Mbps a takovou rychlost lze považovat za zcela dostatečnou. Switch v racku R1 má, pro větší škálovatelnost do budoucna, porty umožňující až 10 Gbps. Jeden z těchto portů byl využit pro propojení právě daného switche s routerem, který je taktéž v racku R1 umístěn.

4.4 Konfigurace

Poté, co bylo vše usazeno na své místo, bylo třeba zahájit samotnou konfiguraci. Tato fáze zahrnovala nastavení všech aktivních síťových prvků, především routeru, který bude sloužit i jako centrální bod pro správu celé sítě. Právě na něm bude hostována aplikace systému UniFi.

4.4.1 Základní nastavení aktivních prvků

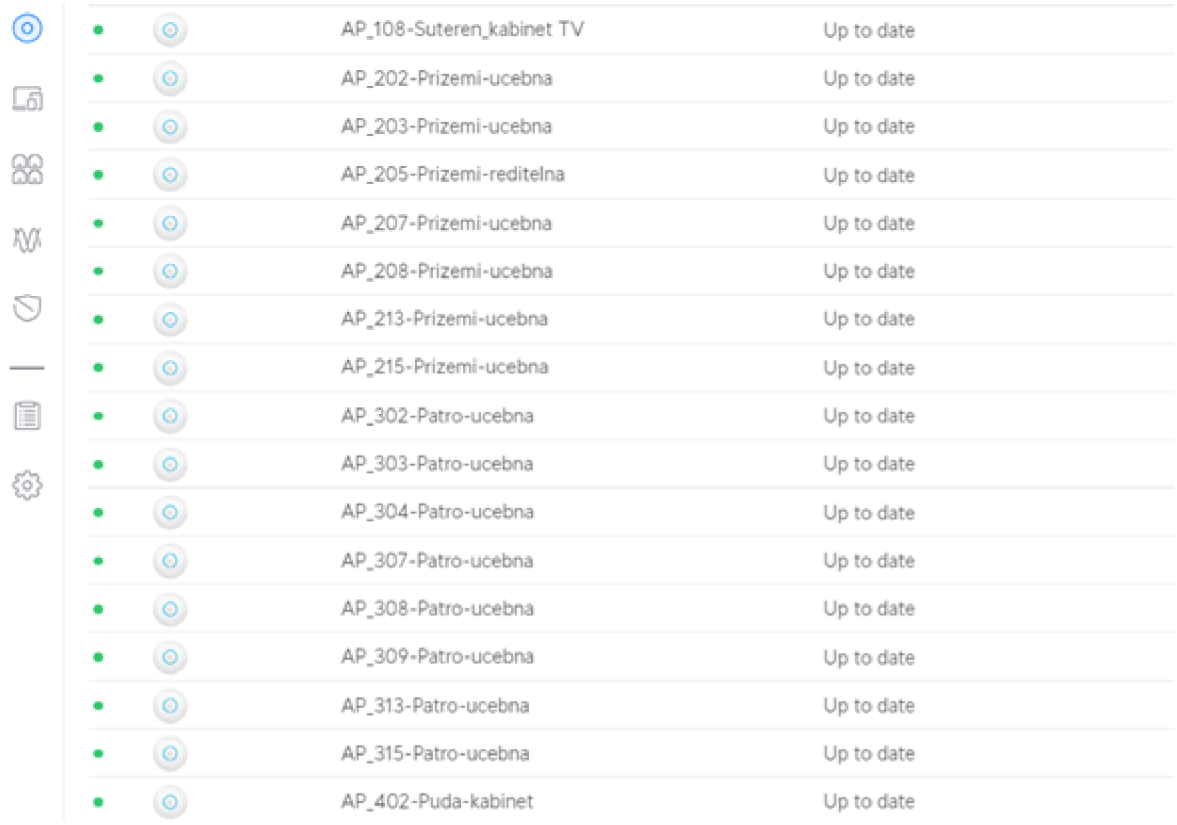
V první řadě bylo potřeba zálohovat současnou konfiguraci systému UniFi, protože budou využity současné přístupové body. Pokud by záloha nebyla obnovena a systém by se nastavoval celý znovu, bylo by potřeba všechny přístupové body resetovat, a to by při aktuálním počtu bylo časově velmi náročné.

Zálohu tak bylo nutné stáhnout z aktuálního kontroléru na pevný disk počítače, ze kterého se bude později nastavovat router, právě na něm bude v tomto případě aplikace systému UniFi hostována. Současný kontrolér (CloudKey), tak již nebude potřeba. Po prvním zapnutí routeru se obnovila současná záloha a rázem byly v systému UniFi vidět všechny aktuálně umístěné přístupové body, včetně jejich názvu. Z názvu bylo možné vyčíst

jejich umístění, jelikož při jejich instalaci byly pojmenovány dle čísla místnosti nebo učebny, ve které se nachází.

Takový stav je velmi výhodný nejen pro přehlednost, ale především pro fyzickou identifikaci v případě poruchy přístupového bodu. Díky správnému označení je přesné umístění ihned známo z rozhraní kontroléru, jak je vidět na obrázku 4.

Obrázek 4 Označení přístupových bodů



Zdroj: vlastní zpracování

Následovalo osvojení přepínačů (přidání do kontroléru UniFi). Po tomto kroku bylo možné spravovat již všechna zařízení, která zde budou využita jako aktivní prvek.

Spolu s tím následovalo i nastavení agregace mezi zmiňovanými switchi R1 a R3 pro zvýšení propustnosti mezi nimi. Tento krok je nejdříve nutné nastavit na v topologii vzdálenějším prvku a následně na tom, který je blíže – v tomto případě R1, jelikož tímto nastavením dojde k výpadku připojení právě mezi těmito prvky, dokud se tato změna nenastaví i na switchi R1. Tato funkce se nastavuje v takzvaném manažeru portů (Port manager), jak je vidět na obrázku 5.

Obrázek 5 Port manager

Zdroj: vlastní zpracování

Díky manažeru a vzájemnému propojení všech UniFi prvků je možno vidět, do jakého portu jsou zařízení a prvky připojeny. S ohledem na to, že je switch R1 ve verzi „Pro“, jej bylo možné propojit s routerem pomocí SFP+ konektoru rychlostí 10 Gbit, znázorněné modrou barvou na portu 26. K tomu bylo potřeba využít speciálního kabelu s konektory SFP+ (tento typ konektoru je určený především pro optické moduly). Byl tak navíc zakoupen kabel „Ubiquiti UniFi 10 Gbps SFP+ Direct Attach Cable“.

4.4.2 IP rozsahy vnitřních sítí a nastavení DHCP

Po vzájemném propojení všech prvků nastal čas na konfiguraci sítí. V první řadě bylo potřeba si rozvrhnout, v jakém rozsahu a s jakými maskami budou sítě nastaveny. Zde bylo nutno zohlednit také množství koncových zařízení, které se k síti budou připojovat.

Základní (Default) síť bude využita k tomu, aby se k ní připojovali aktivní prvky sítě, nikoliv koncová zařízení. Tím lze docílit oddělení vnitřních prvků sítě od samotných uživatelů, to udělá síť bezpečnější, za předpokladu že uživatelé budou na oddělené VLAN.

V tabulce 6 je uvedeno, jak budou sítě rozděleny a zároveň to, pro jakou skupinu koncových zařízení je daná síť uvedena.

Tabulka 6 Rozdělení VLAN

VLAN ID	Název (určení)	Výchozí brána	Rozsah	DHCP	Maska
1	Default	10.0.0.1	10.0.0.1–10.0.3.254	10.0.3.1–10.0.3.250	22
10	Učitelé	10.0.10.1	10.0.10.1–10.0.13.254	10.0.11.1–10.0.13.250	22
20	Žáci	10.0.20.1	10.0.20.1–10.0.23.254	10.0.21.1–10.0.23.250	22
30	IoT	10.0.30.1	10.0.30.1–10.0.33.254	10.0.31.1–10.0.33.250	22
40	VOIP	10.0.40.1	10.0.40.1–10.0.43.254	10.0.41.1–10.0.43.250	22
50	Hosté	10.0.50.1	10.0.50.1–10.0.53.254	10.0.51.1–10.0.53.250	22

Zdroj: vlastní zpracování

Důležité bylo zvolit dostatečně velký DHCP rozsah serveru, který bude dostatečný pro zdejší podmínky. U sítě Default, která je určená pro aktivní prvky a jejich management, není potřeba, aby byl DHCP server tak rozsáhlý. Menší DHCP rozsah je vhodný i u sítě určené pro VOIP, jelikož se zde očekává větší množství zařízení připojených pomocí statické IP adresy. VLAN ID 1 znační, že se jedná o „výchozí“ síť routeru.

4.4.3 Nastavení bezdrátového připojení

Po samotném rozdělení podsítí bylo potřeba stanovit, které z nich se budou vysílat na přístupových bodech. Díky řešení UniFi stačí nastavit SSID a heslo, případně ostatní parametry jen jednou v kontroléru a nastavení se poté duplikuje na všechny ostatní přístupové body – společně se pak tváří jako jedna velká Wi-Fi síť. Od uživatele pak není vyžadována žádná další akce při přechodu mezi přístupovými body. Systém sám vyhodnotí, ke kterému bodu je klient nejblíže a jeho zařízení je tak automaticky připojeno na nejbližší přístupový bod, případně na takový, který mu bude zajišťovat nejlepší možnou konektivitu.

Aktuálně instalované přístupové body umožňují vysílat pouze čtyři různá SSID, proto je nutné stanovit, které z nich je potřeba vysílat, a které z nich budou omezeny pouze na drátovou možnost připojení.

Určitě se bude jednat o síť pro učitele a pro žáky, naopak není nutné vysílat síť pro VOIP, jelikož se tato zařízení připojují drátově. Ke každému SSID je tak přiřazena příslušná VLAN, jak je uvedeno v tabulce 7.

Tabulka 7 SSID Wi-Fi sítí

VLAN ID	SSID
1	-
10	Skola-Ucitele
20	Skola-Zaci
30	Skola-IoT
40	-
50	Skola-Host

Zdroj: vlastní zpracování

Bezpečnostní protokol pro ověřování byl nastaven na WPA3 se zpětnou kompatibilitou pro WPA2, PMF (Protected Management Frames) tak byly nastaveny jako volitelné. Díky tomu je síť připravena do budoucna pro využívání WPA3, zároveň je umožněno i starším zařízením se k síti připojit.

Šířka kanálu v pásmu 2,4 GHz byla nastavena na 20 MHz a v pásmu 5 GHz na 40 MHz, jelikož jsou zde některé přístupové body poměrně blízko u sebe, kdy v případě využití větší šířky pásma může docházet k vzájemnému rušení.

Nastavení kanálu bylo ponecháno v automatickém režimu, jelikož systém UniFi si díky funkci „Noční optimalizace“ umí nastavit kanály sám na základě vzájemného rušení přístupových bodů i rušení sousedních Wi-Fi sítí.

4.4.4 Firewall

V záložce „Firewall & Security“ je po prvním spuštění jen pár základních pravidel, kdy samotné oddělení VLAN mezi sebou je potřeba nastavit ručně, spolu s dalšími pravidly. Dále je nutné zabránit přístupu do rozhraní kontroléru ze všech sítí mimo „Default“, jelikož tato síť bude sloužit jako jediná, která bude umožňovat lokální přístup do rozhraní kontroléru. Pro přehlednost jsou pravidla firewallu uvedena v tabulce 8.

Tabulka 8 Pravidla firewallu

Název pravidla	Zdroj	Destinace	Akce	Status	Typ
Povolit navázaná a související spojení	Odkudkoliv	Kamkoliv	Povolit	Navázané, Související	LAN In
Zahodit neplatná spojení	Odkudkoliv	Kamkoliv	Zahodit	Neplatný	LAN In

Povolit síť „Default“ na všechny VLAN	Default	RFC1918	Povolit	-	LAN In
Zablokovat komunikaci mezi VLAN	RFC1918	RFC1918	Zahodit	-	LAN In
Zablokovat učitele na ostatní výchozí brány	Učitelé	10.0.0.1, 10.0.20.1, 10.0.30.1, 10.0.40.1, 10.0.50.1	Zahodit	-	LAN Local
Zablokovat žáky na ostatní výchozí brány	Žáci	10.0.0.1, 10.0.10.1, 10.0.30.1, 10.0.40.1, 10.0.50.1	Zahodit	-	LAN Local
Zablokovat IoT na ostatní výchozí brány	IoT	10.0.0.1, 10.0.10.1, 10.0.20.1, 10.0.40.1, 10.0.50.1	Zahodit	-	LAN Local
Zablokovat VOIP na ostatní výchozí brány	VOIP	10.0.0.1, 10.0.10.1, 10.0.20.1, 10.0.30.1, 10.0.50.1	Zahodit	-	LAN Local
Zablokovat hosty na ostatní výchozí brány	Hosté	10.0.0.1, 10.0.10.1, 10.0.20.1, 10.0.30.1, 10.0.40.1	Zahodit	-	LAN Local
Zablokovat učitele na rozhraní	Učitelé	10.0.10.1:80, 10.0.10.1:443, 10.0.10.1:22	Zahodit	-	LAN Local
Zablokovat žáky na rozhraní	Žáci	10.0.20.1:80, 10.0.20.1:443, 10.0.20.1:22	Zahodit	-	LAN Local
Zablokovat IoT na rozhraní	IoT	10.0.30.1:80, 10.0.30.1:443, 10.0.30.1:22	Zahodit	-	LAN Local
Zablokovat VOIP na rozhraní	VOIP	10.0.40.1:80, 10.0.40.1:443, 10.0.40.1:22	Zahodit	-	LAN Local
Zablokovat hosty na rozhraní	Hosté	10.0.50.1:80, 10.0.50.1:443, 10.0.50.1:22	Zahodit	-	LAN Local

Zdroj: vlastní zpracování

Výše uvedená nastavení zajišťují primárně zamezení komunikace mezi VLAN. Každá podsíť tak funguje jako samostatná LAN a vzájemné komunikaci mezi VLAN je tak zamezeno. Pouze ze sítě „Default“, neboli sítě určené pro řízení a správu aktivních prvků, je možné komunikovat do ostatních sítí. Komunikovat z jakékoliv VLAN se sítí „Default“ je zakázáno a VLAN jí může pouze odpovídat. To zajišťují první dvě pravidla v tabulce.

Pokud by tedy někdo chtěl síť takzvaně „skenovat“, což znamená, že by chtěl zobrazit všechna připojená zařízení na síti, uvidí pouze ostatní klienty, nikoliv aktivní prvky sítě. Jak bylo již zmíněno, ty jsou přístupné pouze ze sítě „Default“.

V síti určené pro hosty je navíc nastaveno, že ji není možné skenovat. To znamená, že klientská zařízení nemohou komunikovat mezi sebou a její uživatelé tak mají pouze přístup k internetu. Takové nastavení se může zdát na první pohled jako přínosné pro zabezpečení sítě, ovšem v praxi s sebou přináší i několik negativních jevů, jako je například nemožnost odesílání souborů k tisku nebo zamezení distribuce aktualizací po koncová zařízení mezi sebou v rámci sítě, které může vést k vytížení linky pro přístup k internetu. Toto nastavení se nenastavuje ve firewallu, ale v nastavení Wi-Fi sítě.

I přes výše uvedené, je stále možné na síti vidět výchozí bránu, v tomto případě router. Po zadání jeho IP adresy do adresního řádku v prohlížeči je tak možné zobrazit přihlašovací stránku do jeho rozhraní a v tomto případě tak i do celého kontroléru sítě.

Aby se zamezilo možnému útoku na router, kdy by se útočník mohl snažit heslo prolomit, bylo zamezeno přístupu do jeho rozhraní pomocí blokace portů určených pro komunikaci s routerem. Na zvolených portech 80 a 443 je blokováno webového rozhraní, na portu 22 pak přístup pomocí SSH (Secure Shell).

4.4.5 IDS/IPS

Za účelem naplnění předpokladu hypotézy bude nutné využít funkci pro identifikaci podezřelých aktivit. Tato funkce je k nalezení v nastavení firewallu, a kromě blokace IP adres na základě polohy je možné ji využít společně s DPI za účelem blokace podezřelé aktivity a jiných anomálií. V nastavení firewallu na vybraném routeru (UDM-SE) je možné nastavit blokování určitých zemí a detekci podezřelých aktivit například i na základě síťového protokolu, kdy v případě použití funkce „Oznámit a Blokovat“ toto probíhá zcela automaticky.

Všechny detekované anomálie jsou pak zaznamenávány a je možné je zpětně analyzovat a učinit případná opatření. Tento systém je též označován jako „Systém pro

detekci a prevenci průniku“ z anglického označení IDPS (Intrusion Detection and Prevention Systems). Tento systém je možné různě konfigurovat, například je možné:

- Detekovat provoz, případně zobrazit oznámení;
- Detekovat provoz, případě jej blokovat a zobrazit oznámení;
- Použít různé úrovně detekce (nízká, střední, vysoká) nebo vlastní citlivost na určité anomálie;
- Vybrat jednu nebo více sítí, ve kterých je funkce povolena;
- Konfigurovat IP adresy nebo podsítě, které mají být vyloučeny.

V tomto případě byla funkce nakonfigurována v režimu s automatickou blokací, kdy tato konfigurace byla aplikována na všechny podsítě. Co se týče úrovně detekce, byla zde aktivována detekce všech nežádoucích aktivit, které by mohly na síti vzniknout.

4.4.6 Nastavení VLAN na směrovačích

V neposlední řadě je pak třeba zajistit, že jsou správně nastavené porty na samotných přepínačích. Je potřeba zajistit, aby přístupové body měly k dispozici všechny VLAN, které mají vysílat, zároveň i přístup k síti „Default“, aby bylo možné je konfigurovat. Zároveň je potřeba všechny ostatní porty od sítě „Default“ oddělit, aby se zamezilo neoprávněnému přístupu do konfigurace síťových prvků.

Ve výše zmíněném manažeru portů tak bylo potřeba nastavit u každého směrovače, aby na portu, do kterého je připojený přístupový bod byly dostupné sítě: Default, Učitelé, Žáci, IoT a Hosté. Ostatní porty se nastavily dle toho, co je do nich zapojeno. Například port vedoucí do stolního PC v učebně má k dispozici pouze síť pro učitele (tedy žádnou jinou). Pokud bude potřeba, aby měl učitel přístup do jiné sítě, je vhodné toto nastavovat v pravidlech firewallu.

Na závěr byly všechny nevyužité porty nastaveny jako učitelské, to znamená, že pokud se do nich kdokoliv připojí, bude mít přístup pouze do učitelské sítě. V závěru byly pro účel údržby ponechány volné porty na routeru i s přístupem do sítě „Default“. K routeru není možné fyzicky volně přistupovat – je totiž uzamčený v rozvaděči.

4.5 Analýza

V závěru vlastního zpracování a implementace daného řešení je nezbytná pečlivá selekce optimálního nástroje pro sledování aktivity uživatelů.

4.5.1 Cisco Umbrella

Během počáteční fáze průzkumu možných řešení pro analýzu provozu bylo rozebráno a zkoumáno několik variant, mezi nimiž vynikalo relativně rozšířené Cisco Umbrella. Tato platforma, známá pro svou schopnost analyzovat síťový provoz, však během následné implementace odhalila své omezení. Kritickým faktorem se stal požadavek na veřejnou IP adresu. I když by mohl být tento problém relativně jednoduše překonán, je nutno avizovat, že důležitým aspektem je také fakt, že tato platforma vyžaduje finanční investici, neboť se jedná o placený nástroj.

Tyto faktory vedly k závěru, že pro efektivní monitorování a sledování aktivity uživatelů je vhodné hledat alternativní řešení, které lépe vyhovuje specifickým potřebám dané organizace či prostředí.

4.5.2 Pi-Hole

Jako další možnost, tentokrát neplacenou, byla nasazena Pi-Hole. V základu je tento software určený především pro blokaci internetové reklamy, avšak nabízí i historii DNS požadavků od jednotlivých klientů. Pi-Hole plní roli interního DNS serveru, který se aktivně podílí na filtrování obsahu. Nicméně, vzhledem k tomu, že sledování aktivity uživatelů není jeho hlavním účelem, nýbrž spíše vedlejším benefitem, vzniká zde výzva v oblasti přehlednosti, kdy je poměrně složité v něm hledat konkrétní použité aplikace či jinak smysluplně procházet nasbíraná data.

Z tohoto důvodu bylo usouzeno, že bude smysluplnější vyhledání dalšího řešení, které by lépe vyhovovalo potřebám komplexního monitorování aktivity.

4.5.3 UniFi Traffic Indentification

Nakonec k vyhodnocení analýzy provozu a ověření hypotézy postačila data z identifikace síťového provozu v systému UniFi. Díky tomu, že je zde implementován UniFi router jako výchozí brána, je možné procházet nasbíraná data přímo dle konkrétního připojeného zařízení, a kromě navštívených webů a použitých aplikací, je zde viditelný i přenesený objem dat.

Přehlednosti dat pak pomáhá i graf s časovou osou, na kterém je možno vidět, jak bylo zařízení používáno v čase i včetně objemu přenesených dat. Informace získané z „Traffic Identification“ jsou tak naprosto dostatečné a v prostředí je možné se snadno orientovat.

Níže, na snímku obrazovky (obrázek 6), je vidět identifikace síťového provozu za jeden pracovní týden jednoho z náhodně vybraných zařízení v síti.

Obrázek 6 Identifikace provozu v prostředí UniFi Traffic Identification

Application	Total Data (Traffic %)
All Traffic	32.1 GB
SSL/TLS	14.4 GB (44.9%)
Outlook.com	4.71 GB (14.7%)
iCloud	4.05 GB (12.7%)
Facebook	3.38 GB (10.5%)
Youtube	2.01 GB (6.3%)
Twitter	679 MB (2.1%)
Apple.com	617 MB (1.9%)
Microsoft.com	486 MB (1.5%)
Google APIs(SSL)	401 MB (1.3%)
Sharepoint	381 MB (1.2%)
Microsoft Office	193 MB (0.6%)

Zdroj: vlastní zpracování

I takový systém má svá omezení. Jedním z nich je nemožnost exportu dat mimo uzavřené prostředí UniFi. Tato restrikce může být pociťována jako nevýhodná, zejména v situacích, kdy vzniká potřeba provádět dlouhodobou analýzu těchto dat nezávisle na původním systému. Tím pádem může být ztíženo sdílení informací s externími entitami nebo vykonávání pokročilých analýz a vizualizací, které by přesahovaly rámec interního prostředí UniFi.

Faktem také zůstává nemožnost sledování šifrovaného provozu, zde na obrázku označeného jako SSL/TLS. Sledování šifrovaného provozu není účelem tohoto řešení a ve

vzdělávacím prostředí se považuje za nežádoucí, ba dokonce spíše za nemorální, věnovat pozornost sledování takového provozu. Tato stanoviska zdůrazňují, že sledování zašifrované komunikace nesouvisí s hlavním záměrem řešení a je vnímáno jako odporující zásadám etiky a ochrany soukromí. Tímto přístupem se reflektuje důležitost respektování soukromí uživatelů v rámci vzdělávacího prostředí a vyhýbání se potenciálním etickým dilematům, která by mohla vzniknout v souvislosti se sledováním šifrovaného provozu. Takové řešení vytváří prostředí, které klade důraz na bezpečnost a etické normy v souladu s hodnotami vzdělávací instituce.

4.6 Ověření hypotéz

Hypotézu se podařilo naplnit v oblasti zabezpečení počítačové sítě, kdy se díky nově dodaným a správně nakonfigurovaným síťovým prvkům podařilo oddělit části sítě navzájem od sebe pomocí VLAN a firewallových pravidel. Ochrana je dále podpořena pomocí funkcí pro detekci a blokaci podezřelých aktivit.

Hypotézu se podařilo naplnit také v oblasti monitoringu sítě. Bylo verifikováno správné rozmístění přístupových bodů pro bezdrátové připojení do sítě pomocí Wi-Fi, kdy dle nasbíraných dat systémem UniFi byla potvrzena správná hustota v jejich rozmístění, konkrétně lze tuto informaci nalézt v záložce „Radios“. Díky jednotnému prostředí UniFi existuje přehledné rozhraní pro správu a zobrazení aktuálního stavu aktivních prvků.

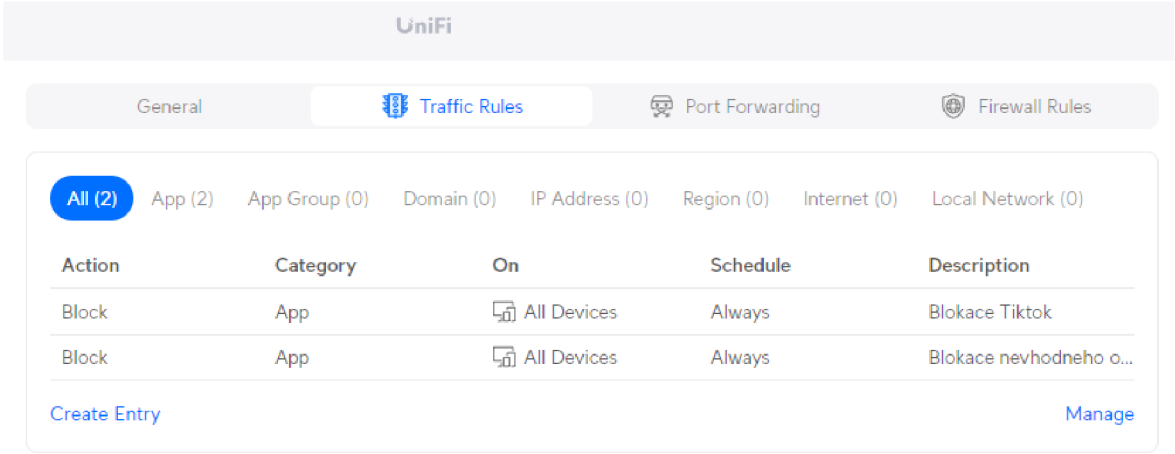
Hypotézu se podařilo naplnit i na základě získaných informací z monitoringu uživatelů. Dle nejčastěji využívaných aplikací bylo možné zjistit, které aplikace žáci nejčastěji využívají v době výuky. Na základě těchto dat je pak možné vydat doporučení pro blokaci určitých aktivit, či předat tato data přímo danému vyučujícímu.

5 Zhodnocení a doporučení

Po analýze nashromážděných dat systémem UniFi, bylo zjištěno, že žáci velmi často přistupují k aplikaci TikTok. Dle Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) se jedná o bezpečností hrozbu, konkrétně obava z možných bezpečnostních hrozeb vyplývá především z množství shromažďovaných dat o uživatelích a způsobu, jakým jsou sbírána. Dalším poznatkem bylo využívání této aplikace během vyučovacích hodin, což znázorňovala křivka na grafu využití této aplikace v systému UniFi. (28)

Doporučením tak může být například blokace aplikace TikTok pomocí „UniFi Traffic Rules“, což je součást firewallu UniFi, kde je možné vybrané aplikace blokovat. Dále bylo vydáno doporučení pro využití webového filtru pro blokaci nevhodných webů nebo jiného závadného obsahu. Tuto možnost taktéž nabízí firewall v systému UniFi.

Obrázek 7 Nastavení blokace aplikací pomocí „Traffic Rules“



Zdroj: vlastní zpracování

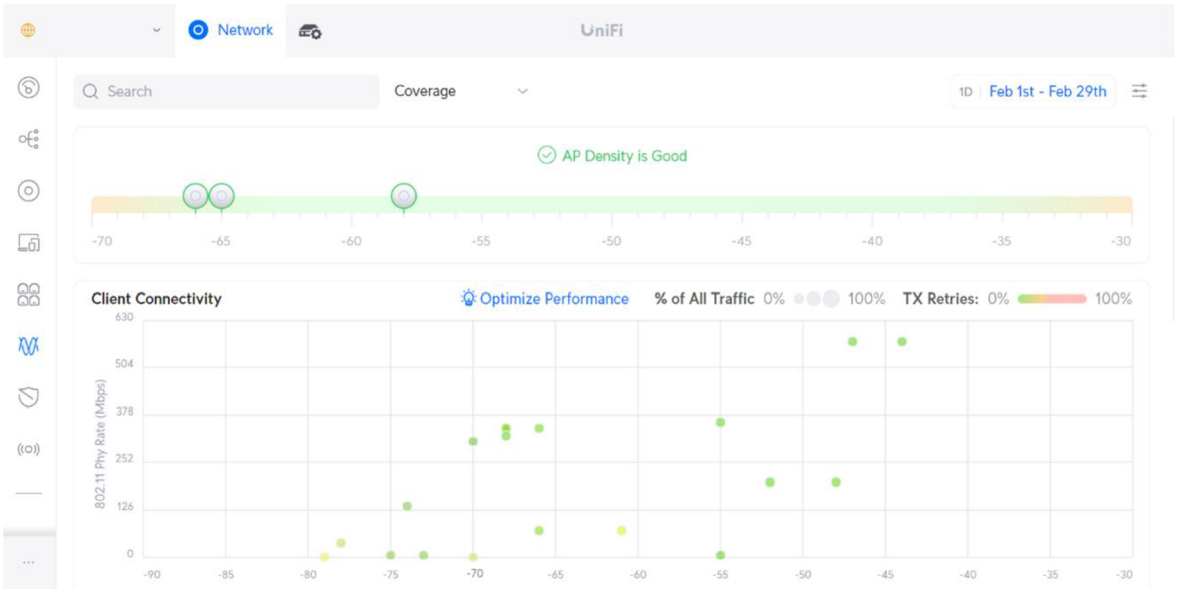
Co se týče práce na samotné infrastruktuře školní sítě, zde bylo docíleno větší bezpečnosti díky oddělení jednotlivých částí sítě od sebe. Taktéž zde byla posílena bezpečnost o firewall s funkcí pro odhalování a blokaci anomálií v reálném čase.

Do budoucna pak monitoring školní sítě může přinést výhodu při řešení různých závad, jelikož v případě výpadku nějakého zařízení je automaticky zaslána notifikace administrátorovi sítě o daném problému.

Monitoring sítě také přispěl k odhalení zmíněného problému se strukturovanou kabeláží mezi rozvaděči, kdy tato oprava přispěla k propustnosti mezi těmito body. Především se tato oprava projevila po zvýšení rychlosti internetu od místního poskytovatele, kdy následně bylo možné dosahovat v celé síti rychlostí až 300 Mbps do sítě internet. Pokud by oprava nebyla realizována nebo by závada nebyla nalezena, měla by celá tato část budovy dostupnou pouze 100 Mbps linku nejen do internetu, ale i do celého zbytku místní sítě, což znamená například i ke sdíleným diskům, či jiným prvkům sítě, které škola využívá.

Na aktivních prvcích určených pro bezdrátové připojení došlo pouze ke konfiguračním úpravám, jelikož vybraná škola měla dané prvky dobře rozložené v prostoru a nejednalo se o zastaralá zařízení. Fakt o správném rozložení a fungování celého bezdrátového systému byl podpořen diagnostikou ze systému UniFi, která na základě spolehlivosti připojení bezdrátových klientů vyhodnotila stav jako „skvělý“, což je vidět i na obrázku 8.

Obrázek 8 Ověření správnosti rozmístění přístupových bodů



Zdroj: vlastní zpracování

Předem stanovené předpoklady hypotéz tak byly verifikovány a doporučení mohlo být vydáno.

6 Závěr

Cílem této bakalářské práce bylo navrhnout počítačovou síť s bezdrátovým připojením a možností monitorování aktivity uživatelů ve vzdělávacím prostředí. Základem práce bylo nejprve vysvětlit problematiku počítačových sítí a poté se detailněji zabývat fungováním aktivních prvků, včetně jejich součástí, jako je například firewall.

S tím dále souvisela i praktická část práce, kde bylo nutné v první řadě analyzovat současný stav a navrhnout úpravu počítačové sítě, tak aby do ní mohl být začleněn monitoring, pomocí kterého bude možné ověřit naplnění hypotézy.

Za účelem naplnění předpokladů byl vybrán vhodný hardware, který byl následně instalován na své místo, včetně odstranění přebytečných napájecích adaptérů pro přístupové body v rámci podpory PoE u nových přepínačů.

Díky velmi zachovalé a kvalitně provedené instalaci přístupových bodů nebyla nutná jejich výměna, což značně ušetřilo práci i finanční prostředky. Nicméně došlo ke změně jejich konfigurace vlivem vytvoření nových podsítí a s tím související úpravou bezdrátových sítí.

Po prvním spuštění a vyřešení počátečních problémů, které souvisely se současnou infrastrukturou, bylo možné přejít k samotné konfiguraci aktivních prvků, tak aby síť byla bezpečná a spolehlivá. Bylo tak potřeba nastavit veškerá pravidla firewallu pro provoz více podsítí v rámci školní sítě včetně zamezení přístupu k přihlášení do administrace kontroléru.

Dalším krokem byla aktivace funkce pro detekci anomálií v reálném čase, společně s možností pro blokování nepovoleného obsahu. Díky správnému nastavení a oddělení jednotlivých částí sítě bylo možné naplnit předpoklad v oblasti zabezpečení sítě.

Díky jednotnému rozhraní pro správu aktivních prvků byl naplněn i předpoklad pro zajištění monitoringu síťových prvků, který umožňuje informovat příslušné osoby o výpadcích pomocí zasílání notifikací o aktuálním stavu.

V poslední řadě bylo zapotřebí implementovat řešení pro analýzu internetové komunikace. Základem bylo porovnat dostupné možnosti a následně vybrat takové řešení, které bude vhodné pro dosažení stanoveného cíle. Během provozu sítě došlo k sběru dat, která byla následně vyhodnocena za účelem vydání doporučení společně s ověřením naplnění hypotézy, kdy se monitoring ukázal jako vhodná pomůcka i v prostředí vzdělávacího zařízení. Tato práce může posloužit jako inspirace pro další školní instituce, které hledají způsoby, jak zlepšit své prostředí.

7 Seznam použitých zdrojů

1. Moderní vzdělávání je předpokladem pro uplatnění v digitální době. *Národní plán obnovy.* [Online] 2022. [Citace: 1. Srpen 2023.] https://www.planobnovycr.cz/vzdelavani-a-trh-prace-2.

2. Digitální učební pomůcky - inspiromat pro školy. *edu.cz.* [Online] Ministerstvo školství, mládeže a tělovýchovy, 2022. [Citace: 1. Srpen 2023.] https://www.edu.cz/digitalizujeme/digitalni-ucebni-pomucky/.

3. Redakce PCT. Jak se plete počítačová síť - základy sítí. *PCTuning.cz.* [Online] PCTuning.cz & Grunex, 4. Květen 2004. [Citace: 1. Srpen 2023.] https://pctuning.cz/article/jak-se-plete-pocitacova-sit-zaklady-siti. ISSN 1214-0201.

4. Kostrhoun, Aleš. *Stavíme si malou síť.* Praha : Computer Press, 2001. ISBN 80-7226-510-5.

5. Kvapil, Jan. Co je čím ... v počítačových sítích. *Computerworld.* 1992, 1992, Sv. 12, 12.

6. ISO. *Open Systems Interconnection (OSI) Reference Model (August 1981) ISO Second Draft Proposal (DP) 7498.* [Technický informační bulletin] Washington, D.C. : National Communications System, 1981. ISO 7498.

7. Novák, Jan. Model TCP/IP. *Internet a Jeho Služby.* [Online] 2012. [Citace: 1. Září 2023.] https://ijs.8u.cz/index.php/standardizace-v-pocitacovych-sitich/model-tcp-ip.

8. Kabelová, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS.* Praha : Computer Press, 2002. ISBN 80-7226-675-6.

9. Kaur, Kirandeep, a další. *A Comparative Study of OSI and TCP/ IP Models.* místo neznámé : Vandana Publications, 24. Duben 2023. 1380687973.

10. CoreApp Technologies s.r.o. Co je to IP adresa? *CoreApp.* [Online] 4. Duben 2023. [Citace: 15. Září 2023.] https://www.coreapp.cz/blog/co-je-to-ip-adresa.

11. Avi Networks. Subnet Mask Definition. *Subnet Mask.* [Online] [Citace: 15. Září 2023.] https://avinetworks.com/glossary/subnet-mask/.

12. Novák, Jan. Fyzická adresa (MAC). *Internet a jeho služby.* [Online] 2012. [Citace: 20. Září 2023.] https://ijs.8u.cz/index.php/adresovani-v-internetu/fyzicka-adresa-mac.

13. What is a router? *Cloudflare Learning Center.* [Online] Cloudflare, Inc. [Citace: 20. Září 2023.] https://www.cloudflare.com/learning/network-layer/what-is-a-router/.

14. Horák, Jaroslav. *Počítačové sítě pro začínající správce.* Praha : Computer Press, 2001. ISBN 80-7226-566-0.

15. Williams, Lawrence. Hub vs Switch – Difference Between Them. *Guru99.* [Online] Guru99 Tech Pvt Ltd, 19. Září 2023. [Citace: 1. Říjen 2023.] https://www.guru99.com/hub-vs-switch.html.

16. Ubiquiti UniFi Switch 24 PoE. *i4wifi.* [Online] 100MEGA Distribution s.r.o. [Citace: 1. Říjen 2023.] https://www.i4wifi.cz/cs/227960-ubnt-unifi-switch-24-poe.

17. Co je WiFi 6? *Alza.cz.* [Online] Alza.cz a.s., 31. Březen 2021. [Citace: 7. Říjen 2023.] https://www.alza.cz/wifi-6#zrychlujeme.

18. Problémy s Wi-Fi a uspořádání vaší domácnosti. *Podpora Microsoft.* [Online] Microsoft. [Citace: 20. Říjen 2023.] https://support.microsoft.com/cs-cz/windows/probl%C3%A9my-s-wi-fi-a-uspo%C5%99%C3%A1d%C3%A1n%C3%AD-va%C5%A1%C3%AD-dom%C3%A1cnosti-e1ed42e7-a3c5-d1be-2abb-e8fad00ad32a.

19. MESH WiFi síť – co to je a proč se vyplatí ji mít. *Alza.cz.* [Online] Alza.cz a.s., 5. Říjen 2021. [Citace: 7. Říjen 2023.] https://www.alza.cz/mesh-sit.

20. Discover Wi-Fi. *Wi-Fi.org.* [Online] Wi-Fi Alliance, 2018. [Citace: 20. Říjen 2023.] https://www.wi-fi.org/discover-wi-fi/security.

21. Jaspreet, Kaur. *WiFi Security: WEP, WPA, and WPA2.* 2017.

22. Scott, Russell. *Networking for Beginners.* Columbia : autor neznámý, 2019. 9781704314105.

23. Meyers, Mike. *CompTIA Network+ Certification: All-in-One Exam Guide. Seventh Edition (Exam N10-007).* New York City : McGraw Hill, 2018. 1260122387.

24. Hall, James. *Multi-layer network monitoring and.* [Technical Report] Number 571, Cambridge : University of Cambridge, Computer Laboratory, Červenec 2003. 1476-2986.

25. Awati, Rahul. deep packet inspection (DPI). *TechTarget.* [Online] Říjen 2021. [Citace: 15. Prosinec 2023.] https://www.techtarget.com/searchnetworking/definition/deep-packet-inspection-DPI.

26. Ubiquiti, Inc. EdgeRouter - Deep Packet Inspection Engine. *Ubiquiti Help Center.* [Online] [Citace: 15. Prosinec 2023.] https://help.ui.com/hc/en-us/articles/204951104-EdgeRouter-Deep-Packet-Inspection-Engine.

27. —. UniFi - PoE Availability and Modes. *UniFi Help Center.* [Online] [Citace: 28. Leden 2024.] https://help.ui.com/hc/en-us/articles/115000263008-UniFi-PoE-Availability-and-Modes.

28. Národní úřad pro kybernetickou a informační bezpečnost. Aplikace TikTok představuje bezpečnostní hrozbu. *NÚKIB.* [Online] 8. Březen 2023. [Citace: 2. Únor 2024.] https://nukib.gov.cz/cs/infoservis/hrozby/1941-aplikace-tiktok-predstavuje-bezpecnostni-hrozbu/.

29. Moskowitz, Robert, a další. Address Allocation for Private Internets. [Online] Únor 1996. [Citace: 11. Listopad 2023.] https://datatracker.ietf.org/doc/html/rfc1918.

30. Kutý, Michael. [Online] [Citace: 5. Září 2023.] https://michaelkuty.github.io/ssz-ai-hk-3/_images/protokoly.png.

31. Empson, Scott. *CCNA Kompletní přehled příkazů.* místo neznámé : Albatros, 2009. str. 336. 978-80-251-2286-0.

32. Designing a Dual-Band Wireless Network. *Metageek.* [Online] [Citace: 10. Říjen 2023.] https://www.metageek.com/inc/images/landingpages/dual/dualbandwifi.png.

33. Ubiquiti, Inc. Dream Router. *UniFi Starts Here.* [Online] [Citace: 10. Říjen 2023.] https://ui.com/eu/en/cloud-gateways/wifi-integrated/dream-router.

34. —. Standard 24 PoE. *Tech Specs.* [Online] [Citace: 15. Říjen 2023.] https://techspecs.ui.com/unifi/switching/usw-24-poe.

8 Seznam obrázků

9 Seznam tabulek

10 Seznam použitých zkratek

LAN – Local Area Network

WAN – Wide Area Network

MAN – Metropolitan Area Network

ARPA – Advanced Research Projects Agency

OSI – Open system interconnection)

RM OSI – Reference Model of Open Systems Interconnection

TCP – Transmission Control Protocol

IP – Internet Protocol

DNS – Domain Name Service

URL – Uniform Resource Locator

HTTP – Hypertext Transfer Protocol

DHCP – Dynamic Host Resolution Protocol

FTP – File Transfer Protocol

NAT – Network Address Translation

IETF – Internet Engineering Task Force

CIDR – Classless Inter-Domain Routing

ICMP – Internet Control Messaging Protocol

ARP – Address Resolution Protocol

RARP – Reverse Address Resolution Protocol

SNMP – Simple Network Protocol

MAC – Media Access Control

SFP – Small Form-factor Pluggable

VLAN – Virtual Local Area Network

PoE – Power over ethernet

AP – Access point

IEEE – Institute of Electrical and Electronics Engineers

Wi-Fi – Wireless Fidelity

SSID – Service Set Identifier

DPI – Deep packet inspection

NGFW – Next-generation Firewall

UTM – Unified Thread Management

ACL– Access control list

UPS – Uninterruptible power supply

NAS – Network Attached Storage

IoT – Internet of Things

VOIP – Voice over IP

Mbps – Megabit za sekundu

UTP – Unshielded Twisted Pair

CAT5e – Kategorie 5e

PMF – Protected Management Frames

SSH – Secure Shell

IDPS – Intrusion Detection and Prevention Systems

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

SSL – Secure Sockets Layer

TLS – Transport Layer Security