Využití informačních technologií v gastronomii

Usage of Information Technologies in Gastronomy

Bc. Milan Martinek

Diplomová práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Milan Martinek**
Osobní číslo:	**A16119**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Forma studia:	**prezenční**
Téma práce:	**Využití informačních technologií v gastronomii**
Téma anglicky:	**The Exploitation of Information Technologies in Gastronomy**

Zásady pro vypracování:

1. **Zpracujte teoretické podklady k danému tématu.**
2. **Navrhněte a zrealizujte firemní síť.**
3. **Zaveďte pokladní systém se skladovým hospodářstvím, platebním terminálem a propojením s EET.**
4. **Navrhněte dohledový kamerový systém.**
5. **Nakonfigurujte vzdálenou správu pokladního systému a kamer.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **KRÁL, Mojmír. Bezpečný internet: chraňte sebe i svůj počítač. Praha: Grada Publishing, 2015. ISBN 978-80-247-5453-6.**
2. **SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.**
3. **KRČMÁŘ, Petr. Linux: postavte si počítačovou síť. Praha: Grada, 2008. Průvodce (Grada). ISBN 978-80-247-1290-1.**
4. **KABELOVÁ a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press. ISBN 978-80-251-2236-5.**
5. **SHINDER, Debra Littlejohn. Počítačové sítě: nepostradatelná příručka k pochopení síťové teorie, implementace a vnitřních funkcí. Praha: SoftPress, c2003. Cisco systems. ISBN 80-864-9755-0.**

Vedoucí diplomové práce: **Ing. Jiří Korbel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **8. prosince 2017**

Termín odevzdání diplomové práce: **28. května 2018**

Ve Zlíně dne 8. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

Ing. Miroslav Matýsek, Ph.D.
ředitel ústavu

ABSTRAKT

Práce se zabývá návrhem, reálným vybudováním a konfigurací moderní zabezpečené firemní sítě, pokladního systému se skladovým hospodářstvím, platebním terminálem a napojením na EET, dohledovým kamerovým systémem a vzdálenou správou těchto systémů.

Nejprve byla navržena infrastruktura jednotlivých systémů a zavedeny potřebné datové a napájecí rozvody s důrazem na ochranu proti výpadku nebo výkyvům elektrické rozvodné sítě.

Dále byly vhodně navrženy a nakonfigurovány prvky systémů včetně koncových zařízení.

Síťové prvky byly navrženy a nakonfigurovány za účelem vytvoření zabezpečené privátní firemní sítě s možností vzdáleného připojení skrze OpenVPN případně L2TP IPsec VPN šifrovaný tunel. Následně byla vytvořena separovaná síť pro zákazníky s omezenými právy komunikace a autentizací pomocí webového portálu na základě odsouhlasení podmínek užití.

Prvky pokladního systému byly vhodně navrženy a nakonfigurovány za účelem vytvoření podrobné databáze surovin, polotovarů a z nich vycházejících složených výrobků s napojením na skladové hospodářství a vytvoření grafického prostředí pokladního terminálu včetně konfigurace jeho funkcí jako mapa stolů, EET, vzdálená správa, tiskárna do kuchyně a další.

Nakonec byl vytvořen kamerový systém, za účelem monitoringu prostorů restaurace s využitím CCTV kamer a spravovaný DVR rekordérem s možností lokálního a vzdáleného zabezpečeného připojení.

Klíčová slova: firemní síť, VPN, VLAN, WiFi, HTTPS, Firewall, DVR rekordér, CCTV kamera, vzdálená správa, pokladní systém, EET

ABSTRACT

This work deals with the design, real development and configuration of a modern secured corporate network, including cash register system with warehouse management, payment terminal with connection to EET, surveillance camera system and remote management of these systems.

First, the infrastructure of the individual systems was designed and the necessary data and power cabling was installed, with an emphasis on protection against power outages or fluctuations.

In addition, individual system elements, including terminal devices, were appropriately designed and configured.

Network elements have been designed and configured to create a secure, privately-owned enterprise network with remote connectivity through OpenVPN or an L2TP IPsec VPN encrypted tunnel. Subsequently, a separate network for customers with limited rights of communication and authentication was created through the web portal based on the agreement of the terms of use.

The elements of the cash system have been appropriately designed and configured to create a detailed database of raw materials, semi-finished products and resulting products with a link to warehouse management. Further, a graphical environment was created for the cash terminal including configuration of its functions such as table maps, EET, remote management, printer in the kitchen, etc.

Finally, a camera system was created to monitor the premises of the restaurant using CCTV cameras, managed by a DVR recorder with local and remote secure connection.

Keywords: company network, VPN, VLAN, WiFi, HTTPS, firewall, DVR recorder, CCTV camera, remote administration, cash register system, EET

Rád bych poděkoval vedoucímu práce, Ing. Jiřímu Korbelovi, Ph.D. za pomoc, ochotný přístup a cenné rady, které mi poskytl během tvorby mé diplomové práce. Dále pak v neposlední řadě mojí rodině, bez jejíž pomoci a podpory bych to nedokázal.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne

Marčinek.....
podpis diplomanta

OBSAH

ÚVOD

Gastronomická zařízení, ve kterých hosté nevyžadují připojení k internetu, platbu pomocí bezdotykové platební karty nebo případně chytrého telefonu jsou čím dál vzácnější. Dříve bylo běžné, že si hospodští vedli evidenci skladu, výpisů tržeb a dalších výkazů na papír. Také personál musel sčítat veškerou útratu jednotlivých hostů na kusy papíru, neustále obcházet všechny prostory, všímat si nových nebo odcházejících zákazníků a pamatovat si, kde přesně si někdo něco objednal.

V dnešní moderní společnosti jsou lidé zvyklí neustále využívat připojení k internetu, a to i v restauracích, kdy se při jídle nebo pití večer s přáteli podívají na zpravodajství, hledají informace, případně sdílejí pořízené fotografie nebo komunikují skrze chatovací aplikaci a zároveň při odchodu domů zaplatí pomocí platební karty. Pro tyto účely je potřeba poskytnout pokrytí bezdrátové sítě po celém objektu s možností autentizace, která by nezatěžovala personál a zároveň zajistit ochranu firemní sítě ale i ostatních zákazníků před možným útočníkem, který by měl různé nekalé úmysly.

Na druhou stranu i personálu je potřeba ulehčit práci a počet nachozených kilometrů. Při zavedení moderního pokladního systému včetně skladového hospodářství a možností vzdálené správy bude většina potřebné administrativní práce, výkazů zboží a zdlouhavého počítání delegována na samotný pokladní systém. Systém zároveň může díky přehledné mapě stolů ujasnit obsluze jednotlivé objednávky zákazníků a sám nahlásí kuchaří, které pokrmy připravit a na který stůl patří. Zároveň obstará i ze zákona povinnou komunikaci se servery ministerstva financí kvůli elektronické evidenci tržeb (EET).

Další důležitou částí všech rozsáhlých restauračních zařízení, kde personál nemůže mít přehled o všech prostorách je kamerový systém. Tento systém je možné využít k získání přehledu o nově příchozích hostech nebo těch co již dojedli a přejí si zaplatit, a to aniž by bylo nutné neustále obcházet kolem stolů. Zároveň lze tento systém využít k ochraně majetku restaurace.

Velmi důležitá je také možnost zabezpečené vzdálené správy a monitoringu všech těchto systémů. Nejlepší způsob, jak toho docílit je napojení vzdáleného zařízení do lokální firemní sítě skrze VPN tunel a pracovat tak bez omezení se všemi výhodami běžného lokálního připojení. Tato práce se zabývá řešením výše uvedených problémů.

I. TEORETICKÁ ČÁST

1 TEORIE K SÍŤOVÝM PRVKŮM

1.1 Kroucená dvojlinka

Kroucená dvojlinka je druh síťového kabelu. Je to nejrozšířenější vodič používaný u sítí LAN. Kabel se nejčastěji skládá z 8 vodičů tvořících 4 páry. U kroucené dvojlinky spočívá ochrana proti vzájemnému rušení v kroucení. Oba vodiče tvoří jeden pár a jsou navzájem zkrouceny, pravidelně střídají svou vzájemnou polohu. V praxi se nejčastěji využívá kabel kategorie 5e, který je určen pro rychlosti max. do 1 Gbps. Dále jsou využívány kabely kategorie 6 a 7 s širším přenosovým pásmem, určené pro nejrychlejší 1 Gbps a 10 Gbps přenosy. Kabely jsou zakončeny koncovkou RJ-45, která se zapojuje do aktivního zařízení či do PC [2].

Řazení podle druhu provedení:

Nestíněná kroucená dvojlinka: UTP (Unshielded Twisted Pair), jednotlivé páry jsou vloženy do vnější plastické izolace, kategorie 6 má navíc plastový kříž, který odděluje jednotlivé páry.

Stíněná kroucená dvojlinka: STP (Shielded Twisted Pair), od nestíněného kabelu se liší kovovým opletením. Toto stínění zvyšuje ochranu proti vnějšímu rušení. Stíněn může být každý pár uvnitř kabelu, nebo se stíní pouze plášť kabelu. Tyto kabely se využívají v místech s velkým rušením [2] [1].

Řazení podle rychlosti (pouze nejpoužívanější):

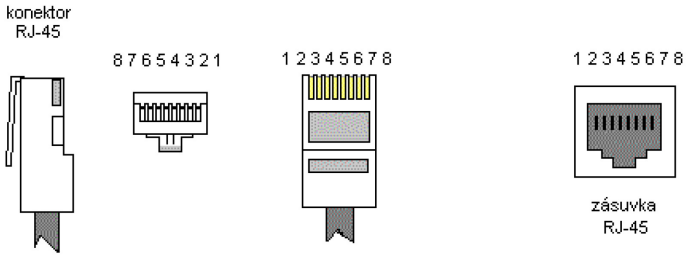
100BaseTX: lze zapojit přes kabel Cat 5 a vyšší, využívá 2 páry, 2 režimy komunikace polo duplex (jedním párem v jednom směru 100 Mbps) a plný duplex (oběma páry najednou, ale párem vždy jednosměrně 100 Mbps) (1 pár x 100Mbps v jednom směru a 2 pár ve směru opačném)

1GBaseT: lze zapojit přes kabel Cat 5E a vyšší, využívá 4 páry, maximální délka kabelu 100 m, v případě kabelu Cat 5E lze využít pouze polo duplex (využívá střídavě 4 páry v jednom směru), v případě kabelu Cat 6 a vyšší lze využít i plný duplex (2 páry x 500Mbps v jednom směru a 2 páry ve směru opačném).

10GBaseT: lze zapojit přes kabel Cat 6 a vyšší, 4 páry, v případě kabelu Cat 6 lze využít pouze polo duplex až do vzdálenosti 55 m [2].

1.2 Konektor RJ45

Používá se k zapojení síťových kabelů UTP a STP. Jedná se o koncovku 8P8C (8 pozic, 8 vodičů). Vyrábí se v podobě zásuvky nebo zástrčky. Zástrčku přichytíme pomocí nožů, které se zasunou do jednotlivých vodičů většinou krimpovacími kleštěmi. U zásuvky naopak většinou jednotlivé vodiče zatlačíme mezi 2 nože.

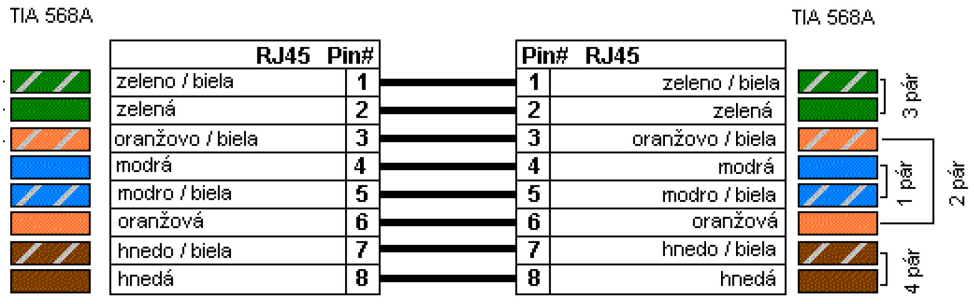


Obrázek 1: Konektor RJ45 [2].

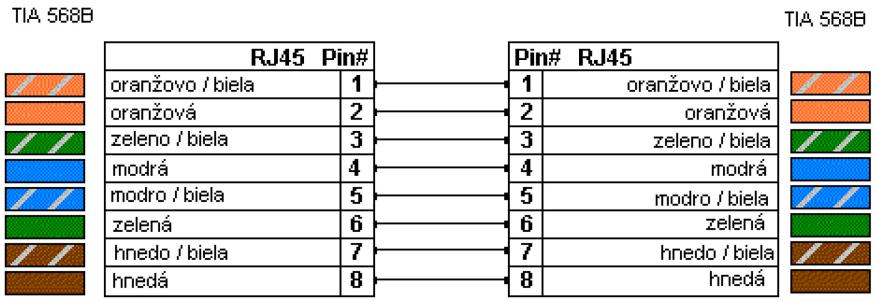
K zapojení lze využít 2 standardy s označením TIA/EIA (Telecommunications Industry Association/Electronic Industries Alliance) 568A a T568B v provedení kříženém nebo přímém [2].

Přímé zapojení

U přímého kabelu jsou oba konce zapojeny identicky. Pro dosažení maximální propustnosti dat je nutné dodržet příslušné barevné pořadí jednoho ze standardů, aby nedocházelo k vysokofrekvenčnímu rušení. Přímé zapojení se aktuálně využívá ve většině případů, jelikož většina zařízení podporuje autodetekci křížení. U starších zařízení bude ovšem fungovat pouze u odlišných zařízení typu PC-switch (v případě PC-PC fungovat nebude) [2].



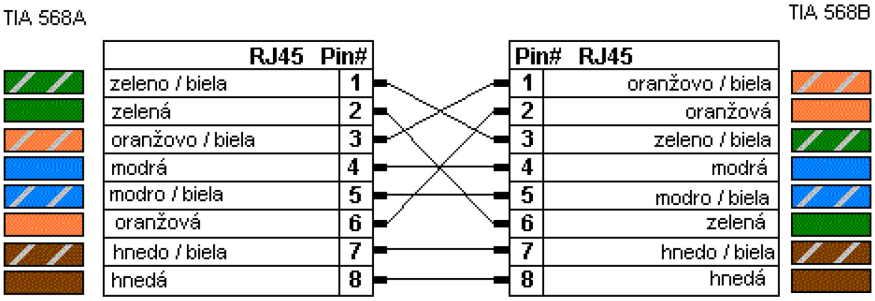
Obrázek 2: Přímé zapojení RJ45 TIA 568A [2].



Obrázek 3: Přímé zapojení RJ45 TIA 568B [2].

Křížené zapojení

Kabel má na kocích u 100 Mbps Ethernetu prohozený oranžový pár se zeleným (piny 1+2 a 3+6), jeden konec odpovídá zapojení TIA 568A a druhý konec TIA T568B. U gigabitového Ethernetu navíc modrý pár s hnědým (piny 4+5 a 7+8). Toto zapojení je využíváno u starších zařízení, které nepodporují autodetekci křížení a jsou stejného typu př. PC-PC [2].

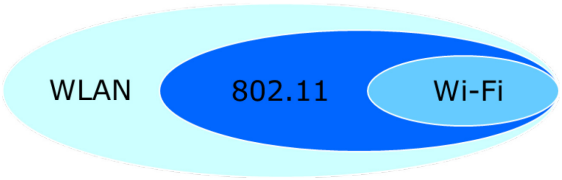


Obrázek 4: Křížené zapojení RJ45 100 Mbps [2].

1.3 Standard IEEE 802.11

Bezdrátové sítě pro lokální účely se souhrnně označují jako WLAN (Wireless LAN). Do této skupiny se řadí techlologie 802.11, Bluetooth, HiperLAN, HomeRF atd.

Aby mezi sebou mohla komunikovat zařízení různých výrobců i různých platforem, existují mezinárodní standardy. Jejich specifikací se zabývá institut **IEEE (z angl. Institute of Electrical and Electronic Engineers)** - specifikace standardů bezdrátových lokálních sítí jsou publikovány pod číslem 802.11. Tento dokument dále obsahuje užší specifikace rozlišené revizními písmeny: např. 802.11n a 802.11ac [3] [4].



Obrázek 5: Hierarchie standardu IEEE 802.11 [3].

Wi-Fi (Wireless Fidelity) neboli bezdrátová věrnost je pouze certifikace která se uděluje produktům, které vyhovují standardům (IEEE 802.11) a splňují požadavky na vzájemnou kompatibilitu. Certifikaci uděluje je organizace Wi-Fi Alliance - dříve WECA (Wireless Ethernet Compatibility Alliance) [3].

1.3.1 Přehled standardů:

Standard	MIMO	Max. rychlost (20 MHz kanál)	Max. rychlost (40 MHz kanál)	Podporované pásmo
802.11	ne	2 Mb/s	nepodporuje	2,4 GHz
802.11b	ne	11 Mb/s	nepodporuje	2,4 GHz
802.11g	ne	54 Mb/s	nepodporuje	2,4 GHz
802.11a	ne	54 Mb/s	nepodporuje	5 GHz
802.11n	1T1R	75 Mb/s	150 Mb/s	2,4 GHz a 5 GHz
802.11n	2T2R	150 Mb/s	300 Mb/s	2,4 GHz a 5 GHz
802.11n	3T3R	225 Mb/s	450 Mb/s	2,4 GHz a 5 GHz
802.11n	4T4R	300 Mb/s	600 Mb/s	2,4 GHz a 5 GHz
Standard	MIMO	Max. rychlost (80 MHz kanál)	Max. rychlost (160 MHz kanál)	Podporované pásmo
802.11ac	1T1R	433 Mb/s	866 Mb/s	5 GHz
802.11ac	2T2R	866 Mb/s	1 732 Mb/s	5 GHz
802.11ac	4T4R	1 732 Mb/s	3 464 Mb/s	5 GHz
802.11ac	8T8R	3 464 Mb/s	6 928 Mb/s	5 GHz

Tabulka 1: Rychlosti nejpoužívanějších standrardů 802.11.

1.3.2 802.11n

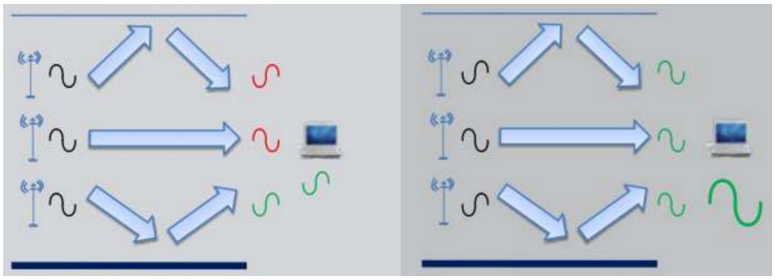
Zcela nejrozšířenějším je dnes standard 802.11n, který může komunikovat v obou pásmech (2,4 i 5 GHz). Úpravou fyzické a linkové vrstvy a zavedením technologie MIMO (vícecestné šíření signálu) přináší reálnou rychlost i více než 100 Mb/s. Existují však routery a i mnohé notebooky pouze s jedinou anténou (1T1R – jedna anténa u vysílače, jedna u přijímače), takže nemohou využít technologii MIMO, čímž teoretická rychlost klesá na 150 Mb/s (reálně 5–6 MB/s). Tento odlehčený standard se nazývá 802.11n-lite [3] [5].

- Standard využívá modulaci maximálně 64-QAM.
- Maximální rychlost 600 Mb/s při využití 4 kanálů MIMO.

1.3.3 802.11ac

Standard 802.11ac komunikuje výhradně v pásmu 5 GHz, nebude žádná 2,4GHz verze. Je však zaručená zpětná kompatibilita, takže čip pro 802.11ac bude umět komunikovat i na 2,4 GHz, ale pouze na starších standardech a s upřednostněním 5GHz pásma, pokud to bude druhá strana umět. 802.11ac využívá šířku kanálu od 20 až do 160 MHz, nejběžnější by měl být 80MHz kanál.

Další novinkou je Technologie **Beamforming**, která zajišťuje co nejlepší „formování“ signálu tak, aby se i přes různé překážky a odrazy dostal v co nejlepší kvalitě tam, kam má a proto lze očekávat mnohem lepší pokrytí signálem. Beamforming funguje tak, že několik antén dokáže načasovat fáze signálu způsobem, aby se k cíli dostal co nejsilnější (třeba poskládaný z odrazů) [3] [5].



Obrázek 6: Funkce Beamformingu [5].

- Standard využívá modulaci až 256-QAM .
- Maximální rychlost 6928 Mb/s při využití 8 kanálů MIMO.
- Podpora MU-MIMO (Multi User - Multi Input Multi Output) – viz. níže Technologie MIMO.

1.3.4 Pásma a kanály

Ve 2,4GHz pásmu je v Evropě k dispozici celkem třináct kanálů, a to od frekvence 2,401 do 2,483 GHz, což znamená, že je k dispozici celková šířka pásma pouze 82 MHz. Kanály se navzájem překrývají, takže je výsledkem, že existují ve skutečnosti pouze tři nepřekrývající se kanály (pro šířku pásma 20 MHz) – 1, 6 a 11 (2,401 až 2,423 GHz; 2,426 až 2,448 GHz a 2,451 až 2,473 GHz). Ve 2,4GHz pásmu tak mohou fungovat maximálně tři Wi-Fi routery, aniž by se navzájem rušily, všechny ovšem pouze s 20MHz šířkou pásma Pokud potřebujeme šířku pásma 40 MHz, můžete použít jen kanály 1 a 9 v případě použití dvou routerů vedle sebe, a i přesto se budou pásma mírně překrývat [3] [6] [7].

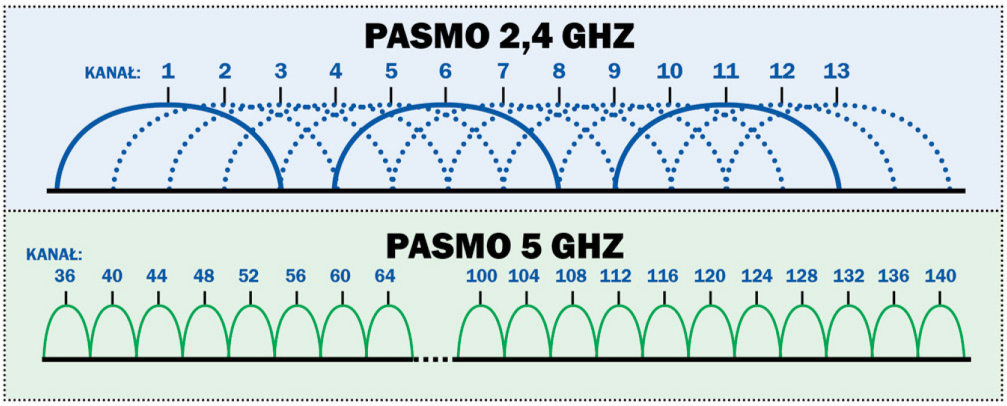
- **Pouze tři nepřesahující se 20MHz kanály (1, 6 a 11), celková šířka pásma jen 82 MHz.** Pokud to prostředí neumožňuje, lze střídat kanály 1, 5, 9 a 13, jsou s minimálními přesahy.
- **V Evropě je povoleno použít antény s maximálním vyzářeným výkonem 100 mW (20 dBm).**

1.3.5 Pásmo 5GHz

Zatímco u pásma 2,4 GHz je frekvenční rozsah pouhých 82 MHz, u 5GHz činí vysokých 520 MHz (od 5,18 do 5,70 GHz). **K dispozici je zde celkem devatenáct kanálů s šířkou 20 MHz, které se již navzájem nepřekrývají.**

U 5GHz sítě však nastává problém s menším dosahem signálu, kterému dělají překážky větší problém než u 2,4GHz sítě. **Při šířce kanálu 40 MHz může v 5GHz pásmu komunikovat souběžně devět zařízení, aniž by se navzájem rušily.** Výsledkem jsou celkem čtyři při MIMO 2T2R nebo tři při MIMO 3T3R. U nového standardu 802.11ac je však již šířka kanálu 80 MHz (fyzická rychlost 433 Mb/s pro jeden stream), takže u třech streamů (3T3R) obsadíte téměř polovinu 5GHz pásma. Vzájemně se nerušící Wi-Fi 802.11ac routery s fyzickou rychlostí 1 300 Mb/s tak mohou být vedle sebe jen dva. V budoucnu lze tedy očekávat, že i 5GHz pásmo bude hodně obsazené. Zvyšují se totiž nejen požadavky na rychlost, ale také počet uživatelů, kteří Wi-Fi používají [3] [6] [7].

- **Devatenáct nepřesahujících 20MHz kanálů, celková šířka pásma 520 MHz.**



Obrázek 7: Zobrazení vzájemného rušení kanálů v pásmu 2,4GHz a 5GHz [8].

Z těchto 19 kanálů je prvních osm (kanály 48–64, 5,180–5,240 GHz) určeno pouze pro použití uvnitř budov (maximální vysílací výkon omezen do 200 mW). Zbylých jedenáct (kanály 100–140, 5,500–5,700 GHz) už lze použít i mimo budovy (vysílací výkon do 1 W),

vysílací zařízení ale musí být vybavena dynamickým výběrem frekvencí a regulací výstupního výkonu [3] [6] [7].

1.3.6 Technologie MIMO

Technologie MIMO přináší výrazné zvýšení rychlosti díky tomu, že je vysíláno více signálů (streamů) vícero anténami a na straně přijímače také více anténami přijímáno. Antény musí být natočeny různě, aby šly signály jinými cestami a navzájem se nerušily. V cíli se poskládají dohromady a data jsou přenášena s výslednou až 2× (2T2R), 3× (3T3R) či 4× (4T4R) vyšší rychlostí oproti n-lite. Problémem ale samozřejmě je obsazení dalších kanálů.

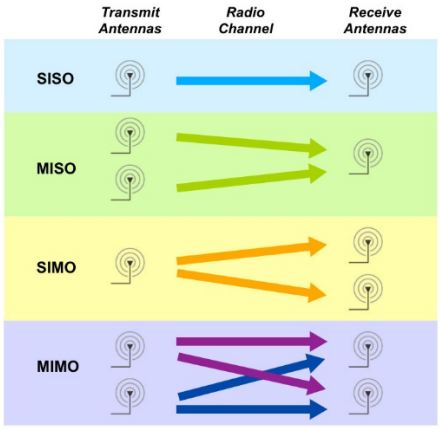
Vícenásobné antény pracují na principu vysílání několika signálů různými, na sobě nezávislými cestami, každá anténa má svůj přijímač/vysílač bezdrátového signálu. Pro správný provoz těchto prvků je nutné použití vyhodnocovacích algoritmů v čipových sadách, které řídí vysílání informace jednotlivými anténami (přijímači) v závislosti na jejich momentálním vytížení. Navíc se signály bezdrátové sítě od překážky v prostoru odrážejí a může dojít k rušení signálu, jeho útlumům, což mají tyto algoritmy také odstranit, nebo alespoň výrazně zmírnit [3] [9].

-SISO: single input, single output

-MISO: multi input, single output

-SIMO: single input, multi output

-MIMO: multi input, multi output, u MIMO může základna komunikovat jen s jedním zařízením současně bez ohledu na počet použitých signálů (streamů), takže při komunikací více zařízení se musejí střídat.



Obrázek 8: Přehled vysílání [9].

1.4 OpenVPN

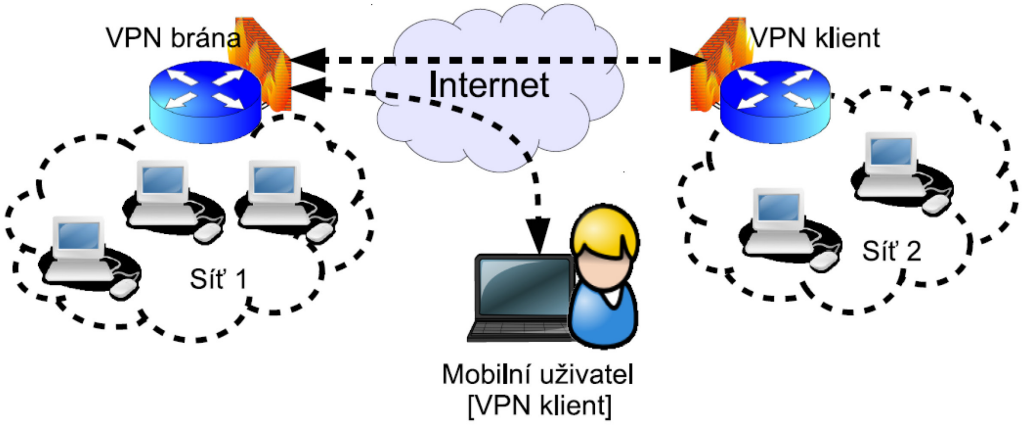
VPN (Virtual Private Network), neboli virtuální privátní síť, vytváří propojení (šifrovaný tunel) mezi jednotlivými sítěmi nebo koncovými zařízeními, které mohou být rozmístěny po celém Internetu do jedné virtuální sítě. Zařízení v této síti se poté chovají, jako by byly přímo fyzicky připojené do lokální sítě za serverem (bránou), včetně všech výhod, které z toho plynou.

K tomuto úkonu je potřeba klient a server. Server musí mít veřejnou IP adresu, na té pak naslouchá a čeká na příchozí připojení od klientů. Klienty tvoří jednotlivé síťové prvky, které mají zájem stát se součástí sítě, jako počítač, telefon s operačním systémem, nebo dokonce router s integrovaným klientským softwarem. S pomocí napojení dalšího routeru jako klienta je možno připojit i zařízení, které se samy o sobě k VPN nedokáží připojit (televize s přístupem k síti, atd.) [10].

Princip připojení je následovný:

1. Klient se připojí k určenému serveru.
2. Obě strany vytvoří šifrovaný kanál pro následnou komunikaci.
3. Proběhne autentizace klienta, jestli má právo se připojit. Obecně může autentizace být realizována např. uživatelským jménem a heslem, sdíleným klíčem, certifikátem či jinými prostředky.
4. Klientovi se přiřadí IP adresa a stane se součástí sítě.

Veškerá další síťová komunikace klienta nyní může být směrována do VPN serveru a klientské připojení k Internetu pak může sloužit jen pro udržování a využívání šifrovaného kanálu. Díky tomu bude veškerá Internetová aktivita klienta zvnějšku vypadat, jako by pocházela ze sítě, do které se klient virtuálně napojil. Všechny požadavky do Internetu nebudou směrovány z klientského PC, ale poputují kanálem do VPN a tam posléze přes router odejdou do Internetu. Klient má na výběr, zda přistupovat do internetu přímo nebo skrytě skrz VPN tunel [2] .



Obrázek 9: Princip virtuální privátní sitě [2].

OpenVPN je plnohodnotnou implementací VPN šířená pod svobodnou licencí. K hlavním výhodám patří silné zabezpečení s použitím TLS/SSL (Transport Layer Security/ Secure Sockets Layer) včetně Open SSL, je multiplatformní, možnost komprese dat, velké množství nastavení různých dodatečných zabezpečení a šifrovacích algoritmů (asymetrické šifrování). Běží nejlépe na UDP protokolu, může být nakonfigurován tak, aby se spustil na portu 443 (port HTTPS) z toho důvodu nelze komunikace zablokovat pomocí firewalu. V opačném případě by byla zablokována i běžná HTTPS komunikace [11].

Výhody:

- Schopnost obejít většinu firewallů.
- Vysoce konfigurovatelný.
- Open source projekt, jeho zadní vrátka mohou být snadno prověřena.
- Kompatibilní s různými šifrovacími algoritmy.
- Vysoce bezpečný.

Nevýhody:

- Složitější nastavení.
- U klientských zařízení vyžaduje software třetích stran.

1.5 SSL/TLS zabezpečená komunikace

Protokol SSL (Secure Socket Layer) a TLS (Transport Layer Security), který ze SSL vychází, slouží k zajištění bezpečné komunikace přes Internet. K tomuto účelu využívají asymetrickou kryptografii (pro výměnu klíčů), symetrickou kryptografii (pro šifrování přenáše-

ných dat) a otisky zpráv MAC (Media Access Control), nebo MAC funkce (Message Authentication Code) pro zajištění integrity přenášených dat. SSL umožňuje jednostrannou nebo oboustrannou autentizaci pomocí certifikátů.

Tři základní fáze:

- dohoda účastníků na podporovaných algoritmech
- výměna klíčů založena na šifrování s veřejným klíčem a autentizaci vycházející z certifikátů
- šifrování provozu symetrickou šifrou (rychlejší a méně náročné na výkon CPU)

Asymetrické ověření identity a symetrické šifrování datového toku:

Soukromý klíč držíme v tajnosti, zatímco veřejný klíč ověřený (podepsaný) certifikační autoritou a zpravidla uložený na serveru autority dáme volně k dispozici v podobě certifikátů protější straně, se kterou chceme komunikovat. Cílem certifikátu je potvrdit, že veřejný klíč patří osobě, která tvrdí, že je jeho majitel. Bez certifikátů bychom si nemohli být jisti, že veřejný klíč skutečně patří lidem, kteří vlastní odpovídající soukromý klíč. Protější strana má nyní jistotu, že dostala náš klíč a není nastrčený někým cizím.

Pokud zašifruje protější strana zprávu naším ověřeným veřejným klíčem a pošle nám ji, dešifrujeme ji pouze svým soukromým klíčem. Toto pravidlo platí samozřejmě i v případě opačné komunikace.

K autentizaci bývá použit opačný postup, pokud zašifrujeme data soukromým klíčem, lze je dešifrovat klíčem veřejným. Za předpokladu, že k soukromému klíči nemá nikdo cizí přístup, lze ověřit, že jsme původci odeslané zprávy, jelikož ji může druhá strana dešifrovat naším ověřeným veřejným klíčem (certifikátem).

Asymetrická kryptografie je však oproti symetrické, ve které jak odesilatel, tak příjemce používá k šifrování i dešifrování stejný klíč, mnohem náročnější na výpočetní výkon, a proto se používá pouze ve fázi navazování spojení k ověření identity.

Jakmile jsou si obě strany jisté svojí vzájemnou identitou, je zvolen sdílený tajný klíč (statický nebo Diffie-Hellmann), který je použit pro hašovací funkci (zajištění celistvosti a ochrany dat proti změnám) a symetrický šifrovací algoritmus (šifrování dat procházejících tunelem) [2].

1.6 L2TP/IPsec VPN

L2TP (Layer 2 Tunnel Protocol) je protokol vytvářející virtuální privátní tunel na 2 vrstvě ISO/OSI, ale zároveň neposkytuje žádné šifrování komunikace, která přes něj prochází. Vzhledem k tomu, je implementován společně se sadou protokolů pro šifrování dat před přenosem IPsec, které poskytují zabezpečení komunikace tunelem.

Nastavení je relativně rychlé a snadné. Při nastavování lze narazit na problémy, protože protokol využívá UDP port 500, který je snadným cílem pro blokování NAT firewally.

Výhody:

- Považováno za bezpečné řešení.
- Nativně implementováno na všech moderních přístrojích a operačních systémech.
- Snadná konfigurace.

Nevýhody:

- Pomalejší než OpenVPN (pokud není využita hardware akcelerace IPSec).
- Může být ohrožen ze strany NSA (National Security Agency).
- Komunikaci mohou snadno blokovat firewally.

1.7 Protokoly TCP a UDP

Vrstva TCP/UDP (Transmission Control Protocol/ User Datagram Protocol) předpokládá, že spojení mezi počítači je zajištěno, proto se bez zbytečných starostí může věnovat předávání dat mezi aplikacemi na vzdálených počítačích. Pro adresaci aplikací zavádí tato vrstva porty. Datový tok na sousední PC je určen nejenom IP adresou, ale i číslem portu. Základní přenosovou jednotkou na této vrstvě je TCP segment nebo UDP datagram. TCP segment nebo UTP datagram se poté zapouzdří do IP datagramu [2].

Protokol TCP je spojovaná služba, příjemce potvrzuje přijímaná data, v případě ztráty dat si příjemce vyžádá zopakování přenosu.

Protokol UDP přenáší data pomocí datagramů, odesílatel odešle datagram a už ho nezajímá, jestli byl doručen [12].

1.8 VNC

VNC (Virtual Network Computing) je aplikace, která zachytává události klávesnice a myši z klientského systému a dále je odesílá přes síťové spojení na server, kde jsou předány hostitelskému systému. V praxi na něco klikneme, VNC server si přebere souřadnice a na tom stejném místě v hostitelském systému se klik provede. Provedené změny se pak zpětně promítnou do VNC klienta (server odesílá obraz plochy zpět klientovi).

U VNC se bere plocha jako jeden obrázek (bitmapa), na který se malují jednotlivá okna a objekty, výsledný obraz se poté pošle klientovi. Pokud se na tomto obrázku něco změní (př. pohneme ikonou), tak se přenese pouze změna oproti předchozímu stavu a ne znovu celý snímek. Tím dojde k značnému snížení přenesených dat. Datový tok lze samozřejmě snižovat i změnou rozlišení, barevné hloubky atd.

VNC je nezávislý na platformě. To znamená, že můžeme mít VNC server nainstalován na operačním systému Android a připojíme se k němu klientem systému Windows.

Další velkou výhodou je možnost souběžné interakce více uživatelů současně. Ve stejnou dobu může ovládat tu samou pracovní plochu uživatel sedící u PC i vzdáleně připojený technik. Na rozdíl od RDP (Remote Desktop Protokol), kdy nejprve dojde k odhlášení lokální plochy (uživatelského účtu), a až poté se připojí k účtu vzdálený uživatel.

VNC distribucí je více, jednotlivé řešení se liší přidanými funkcemi, jako je přenos souborů, šifrování přenosu, možnosti nastavení atd. K nejznámějším patří RealVNC, UltraVNC a TightVNC [2].

1.9 RDP

RDP (Remote Desktop Protocol) je protokol vzdálené plochy společnosti Microsoft, který umožňuje uživateli ovládat vzdálený počítač prostřednictvím síťové komunikace. Uživatel na svém počítači využívá klientský software pro zobrazení grafického uživatelského rozhraní (GUI).

Na serveru (ovládaném zařízení) využívá RDP vlastní ovladač videa k vykreslení výstupu displeje sestavováním informací o vykreslení do síťových paketů pomocí protokolu RDP. Tyto informace následně odesílá pomocí síťové komunikace klientovi.

Na straně klienta služba RDP obdrží data o vykreslování, převede pakety do vhodné podoby pro volání API GDI (Graphics Device Interface) starající se o grafické rozhraní systému Microsoft Windows.

Vstupní události klientské myši a klávesnice jsou rovněž přesměrovány z klienta na server. Na serveru používá RDP vlastní ovladač klávesnice a myši k přijímání těchto událostí [13].

Další funkce protokolu RDP:

- Možné zabezpečení komunikace šifrováním RC4 až 128bit, podpora TLS.
- Možnost redukovat datový tok pomocí mechanismů komprese dat.
- Sdílení schránky systému Windows mezi klientským a vzdáleným zařízením.
- Přesměrování tiskových úloh na klientské zařízení
- Přesměrování zvuku ze serveru ke klientovi
- Přesměrování místních klientských disků, které budou viditelné pro relaci vzdálené plochy [13].

1.10 HTTPS

HTTPS (Hypertext Transfer Protocol Secure) poskytuje ochranu proti sledování komunikace či útokům man-in-the-middle. Protokol HTTPS šifruje data při přenosu mezi serverem a počítačem uživatele, aby je nemohly zachytit a sledovat třetí strany se špatnými úmysly. Certifikáty (SSL/TLS) ověří entitu serveru a umožní tak počítači uživatele zjistit, jestli server skutečně patří danému majiteli (př organizaci). Jestliže je webová stránka zabezpečená pomocí protokolu HTTPS a vlastní ověřený certifikát, zobrazí se ve většině prohlížečů obrázek zeleného zámku [2] [4].

1.11 DDNS

Služba DDNS (Dynamic Domain Name Service) nabízí jednodušší připojení k síťovému zařízení přes Internet, a to prostřednictvím mapování názvu hostitele k IP adrese. Zároveň umožňuje v reálném čase aktualizovat záznamy uložené o internetové doméně na DNS serveru. Aktualizace umožňují používat pro spojení se zařízením DDNS jméno místo neustále se měnící IP adresy [2] [12].

2 PRŮZKUM VHODNÉHO ZABEZPEČENÍ LAN SÍTĚ

2.1 Zablokování vysílání SSID

Nejjednodušším zabezpečením bezdrátové sítě pomocí jejího zdánlivého skrytí je blokace SSID identifikátoru sítě. Klienti síť nezobrazí v seznamu dostupných bezdrátových sítí, protože nepřijímají broadcasty se SSID. Kdo nezná jméno sítě, nemůže se do ní připojit a bez použití speciálního software je pro něj „neviditelná“ [14].

2.2 Kontrola MAC adres

V případě, že se podaří útočníkovi připojit do sítě zevnitř objektu, již se na něj nevztahuje šifrované zabezpečení bezdrátové sítě. Z toho důvodu je zapotřebí alespoň částečně zamezit přístup vytvořením filtru povolených MAC adres.

Access point bezdrátové sítě má k dispozici seznam MAC adres klientů, kterým je dovoleno se připojit (tzv. whitelist). Zrovna tak je možné nastavit blokování určitých MAC adres (blacklist). Ovšem zkušený útočník se může vydávat za stanici, která je již do bezdrátové sítě připojena pomocí klonování stejné MAC adresy. Tuto kontrolu je vhodné využít v sítích, kde se připojují neustále stejná klientská zařízení [14] [15] [16].

Pokud se v LAN případně VLAN síti nachází důležitá komunikace, je nutno tuto komunikaci šifrovat i uvnitř sítě některým ze zabezpečených protokolů jako HTTPS, WebDAV s použitím SSL/TLS šifrování.

2.3 Změna přihlašovacích údajů do administrace Access pointu

Pro přístup do administrace Access pointu je velmi vhodné ihned po přihlášení změnit autentizační údaje. Pokud se útočník již nějakým způsobem dostane do sítě, není pro něj problém přihlásit se do administrace pod základními přednastavenými údaji od výrobce. V základu je většinou nastaveno jméno i heslo admin, případně nějaké další přednastavené heslo. Útočníkovi stačí podle MAC adresy, přihlašovací obrazovky nebo přednastavené hodnoty SSID zjistit výrobce zařízení a posléze si příslušné přihlašovací údaje vyhledat [14] [15].

2.4 WEP (Wired Equivalent Privacy)

Uvedení: 1999

Druh šifrování: RC4

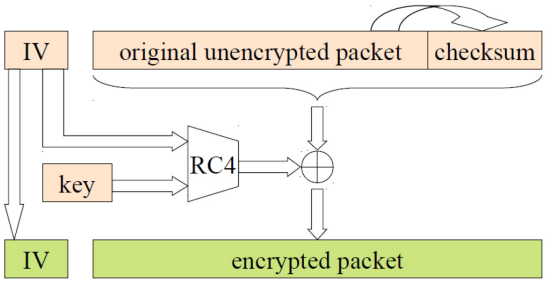
-Funguje na symetrickém principu, kdy se pro šifrování a dešifrování používá stejný algoritmus i totožný statický klíč.

-Jsou 2 nejrozšířenější velikosti klíče pro šifrování rámce:

64-bitový klíč je složen ze 40 bitového uživatelského klíče a 24 bitového dynamicky se měnícího vektoru IV (Initialization Vector)

128-bitový klíč je složen ze 104 bitového uživatelského klíče a 24 bitového dynamicky se měnícího vektoru IV

Inicializační vektor IV se mění s každým rámcem a je generován náhodně, takže výsledná šifra je jedinečná pro každý jednotlivý rámec.



Obrázek 10: Šifrování paketu pomocí WEP [17].

-Integritu dat zajišťuje kontrola integrity ICV (Integrity check value) 32bitový kontrolní součet CRC připojený ke každému odchozímu rámci.

Operace XOR označena jako ⊕.

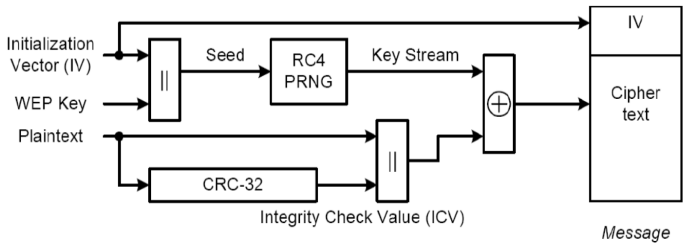
Platí že:

text ⊕ keystream = šifrový text

šifrový text ⊕ keystream = text

text ⊕ šifrovaný text = keystream

PRNG (Pseudo random Generation Algorithm)



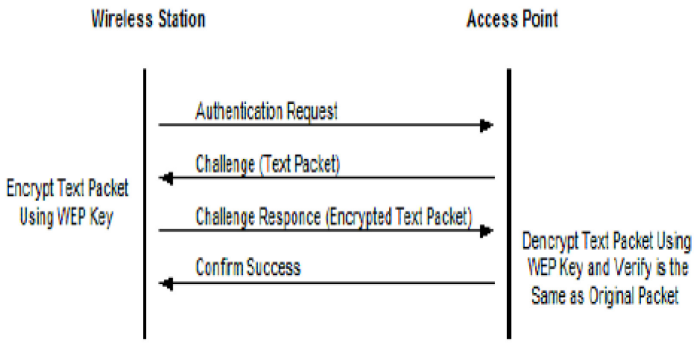
Obrázek 11: Šifrování pomocí WEP [17].

Rotace klíče: NE

Distribuce klíče: ručně zapsané do každého zařízení

Autentizace:

1. Klient pošle žádost o ověření Access Pointu
2. Access Point Odesílá Klientovi výzvu.
3. Klient použije nakonfigurovaný 64bitový nebo 128bitový výchozí klíč k zašifrování textu výzvy a pošle ho Access Pointu.
4. Access Pointu dešifruje šifrovaný text pomocí svého nakonfigurovaného klíče WEP, který odpovídá výchozímu klíči Klienta.
5. AP porovnává dešifrovaný text s původním textem.
6. Pokud se dešifrovaný text shoduje s původním výzvovým textem, pak Access point a Klient sdílejí stejný klíč WEP a Access point ověřil Klient.
7. Klient se připojí k síti.



Obrázek 12: WEP Autentizace [17].

Zranitelnosti šifrování:

- **stejný klíč** na všech klientech v téže WiFi (jelikož je na všech zařízeních stejný klíč, je třeba klíče překonfigurovat na všech zbylých zařízeních).
- **statický a krátký klíč**: inicializační vektor IV s velikostí 24 bitů se sice mění s každým paketem, ale v reálném čase se opakuje (slabá šifra RC4).
- problém se **změnou klíčů** v rozsáhlých sítích (WEP nepodporuje automatickou změnu klíčů).
- **ICV** (Integrity Check Value) nechrání data před útokem man-in-the-middle nedostatečný kontrolní součet CRC-32.

Zranitelnosti autentizace:

- **jednostranná autentizace**: uživatel nemůže vědět, že se připojuje k autorizovanému Access Pointu
- **autentizace zařízení** (ne uživatele): krádeží některého již připojeného zařízení získá potencionální útočník sdílený klíč
- **autentizace sdíleným klíčem**: možnost odchycení a prolomení klíče (výzva a odpověď mezi klientem a Access pointem se posílají v nezabezpečené formě) [18] [19].

Tento šifrovací protokol byl již v roce 2001 úspěšně prolomen, nyní jej lze se závislosti na vytíženosti sítě a počtu bitů šifrování prolomit do několika minut některým ze specializovaných programů jako je například AirCrack [18] [19] [17].

2.5 802.1× a metody EAP

Jedná se o bezpečnostní mechanismus pro všechny typy LAN, který se stará o rozšíření možností autentizace uživatelů, integrity zpráv a distribuci klíčů. Tento mechanismus spadá do podvýboru IEEE 802.1: Higher Layer LAN Protocols Working Group.

Řízení přístupu je vhodné využít zejména u velkých firem a korporací, a to v případě, kdy nemáme pod fyzickou kontrolou všechna připojení k datové firemní síti.

Zabezpečí přístup pouze oprávněným klientům na základě jejich specifických přístupových údajů a neumožní přístup těm, kteří nemají povoleno se do této firemní sítě přihlašovat.

Autentizační mechanismus je tvořen ze 3 částí:

- Supplicant: aplikace na klientovi, který se snaží připojit do sítě
- Autentizátor: aplikace na síťové straně, jejímž cílem je ověřit klienta
- autentizační server - entita poskytující autentizační informace autentizátoru

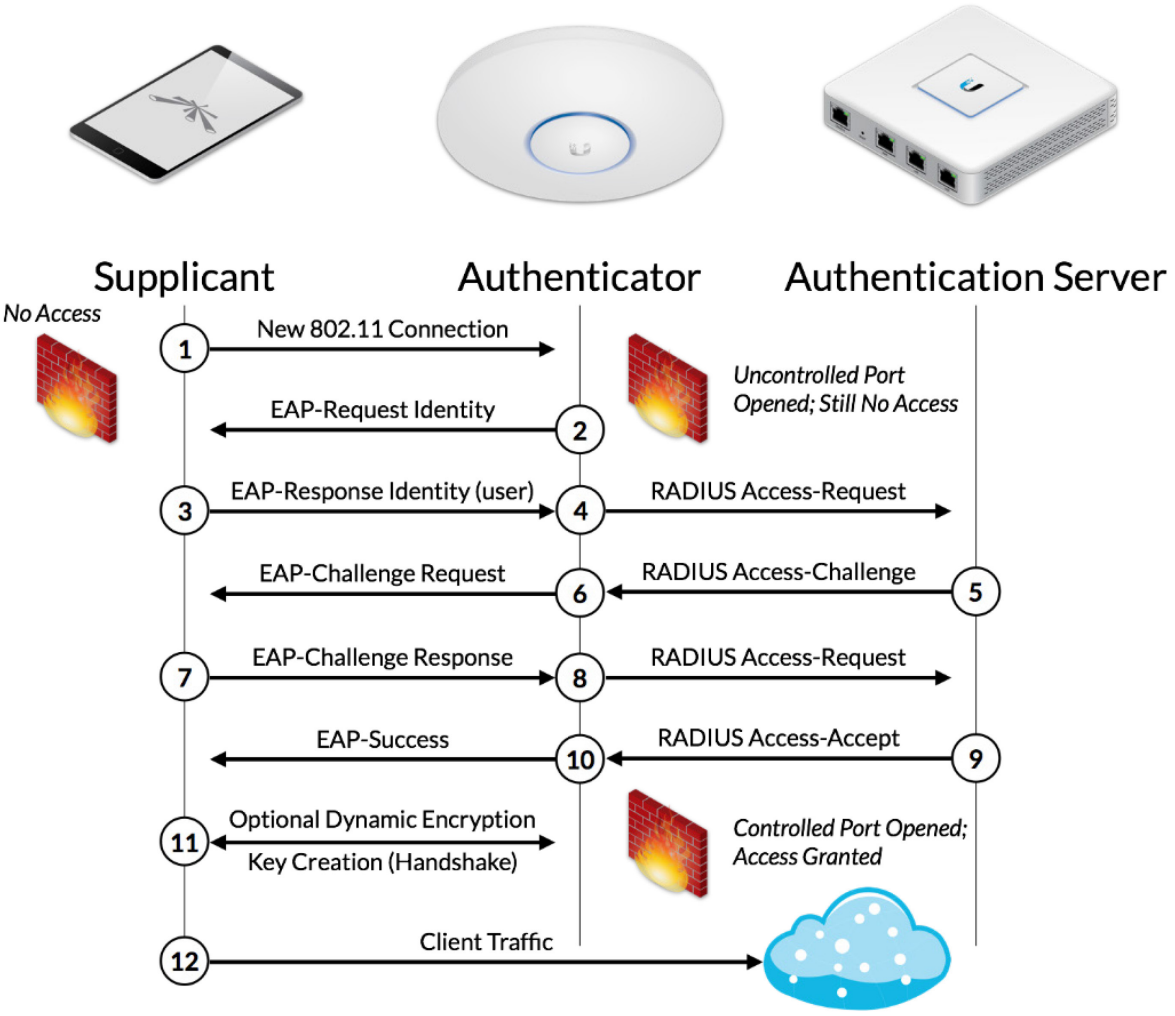
Pro komunikaci mezi jednotlivými částmi je využit protokol EAP (Extensible Authentication Protocol), který slouží jako rozšiřitelný autentizační mechanismus a umožňuje využít implementaci několika druhů autentizačních protokolů.

Nejčastěji EAP-TTLS (Tunneled Transport Level Security) nebo PEAP (Protected EAP), s různou úrovní bezpečnosti (prostřednictvím hesel nebo digitálních certifikátů).

EAP se mezi Suplicantem (klient) a Authentizátorem (AP) zapouzdřuje do ethernetových rámců EAPOL (EAP Over LAN) nebo případně EAPOW (EAP Over WLAN).

Proces ověřování:

1. Supplicant (klientovo zařízení) se připojí k portu v blokovaném stavu a jediné, co portem prochází, jsou autentizační rámce.
2. Access point (autentizátor) vyšle na základě detekce jeho přítomnosti žádost o autentizaci (**EAP-Request Identity)** zabalenou do rámců EAPOL/EAPOW.
3. Supplicant (klientovo zařízení) žádost vyhodnotí a odpoví zprávou **EAP-Response/Identity (ID uživatele)**
4. Access point (autentizátor) zprávu přijme, vybalí ji z rámce EAPOL/EAPOW, zabalí do rámce protokolu RADIUS (**RADIUS Access-Request**) a odešle ji pro ověření Autentizačnímu serveru RADIUS.
5. Autentizační server RADIUS zprávou **RADIUS Access Challenge** vyzve k zaslání autentizačních informací prostřednictvím autentizátoru (Access pointu) od supplicanta (klientovo zařízení)
6. Autentizátor (Access point) výzvu Radius Access Challenge opět přebalí do EAPOL/EAPOW a tento upravený požadavek jako EAP-Challenge Request
7. Supplicant (klientovo zařízení) odpoví autentizační zprávou **EAP- Challenge Response**, ve které budou všechny potřebné údaje jako přihlašovací jméno, heslo, certifikát atd. podle zvolené úrovně zabezpečení.
8. Autentizátor (Access point) odpověď EAP- Challenge Response opět přebalí do rámce RADIUS a přepošle autentizačnímu serveru RADIUS jako RADIUS Access Request
9. V případě, že autentizační informace umožňují přístup, autentizační server RADIUS odpoví zprávou RADIUS Access-Accept.
10. Tuto zprávu Autentizátor (Access point) vyhodnotí, odblokuje port pro komunikaci, nastaví parametry portu (např. přiřazení do VLAN) a přepošle **zprávu EAP-Success** Supplicantovi (klientovo zařízení).
11. V této chvíli je celý autentizační proces ukončen a Supplicant (klientovo zařízení) může bez problému přistupovat k síti.
    Dále se v tomto bodě komunikuje s DHCP serverem o přidělení adresy a nadále už se komunikuje prostřednictvím běžných bezpečnostních algoritmů jako WEP, WPA, WPA2.



Obrázek 13: Autentizace pomocí 802.11× [20].

Po úspěšné autentizaci se dále protokol 802.11× stará o dynamickou výměnu klíčů pomocí zabudovaného managementu klíčů, kdy Access point distribuuje šifrovací klíče autentizovaným Supplicantům (klientovo zařízení). Dynamické klíče jsou známy pouze danému Supplicantovi (klientovo zařízení), mají omezenou životnost a používají se k šifrování rámců na daném portu, dokud se stanice neodhlásí nebo neodpojí. [18] [19] [21]

2.6 WPA (WiFi Protected Access)

Uvedení: v roce 2002, dočasné řešení WiFi Alliance jako odezva na zpožďující se přípravu normy 802.11i a prolomení WEP

Je zpětně slučitelné s WEP což znamená, že lze použít i na zařízeních, která podporují pouze WEP po aktualizaci ovladačů a přitom je dopředně slučitelné s 802.11i WPA2 u novějších zařízení.

Druh šifrování: RC4

- Novinkou oproti WEP je prodloužená délka vektoru IV na 48 bitů a 128 bitový klíč.
- **TKIP** (Temporal Key Integrity Protocol): nový protokol používající pro silnější zabezpečení dynamicky se měnící klíč **pro každý paket**
- **MIC** (Message-Integrity Check): nový mechanismus pro kontrolu integrity zpráv

Rotace klíče: Dynamická rotace klíče

Distribuce klíče: Automatická distribuce

Autentizace: 802.1x (RADIUS server) nebo PSK (Pre-shared key)

- 802.1x: Pro autentizaci a management klíčů používá 802.1× využívající dynamické klíče, které jsou výhodné pro podnikové sítě, ale vyžadují složitější síťovou infrastrukturu se serverem RADIUS.
- PSK (Pre-shared key): používání předem nastavených sdílených klíčů pro běžné uživatele a střední firmy (jednodušší implementace).
- Již nemohou být připojeny 2 klientská zařízení s totožnou MAC adresou současně.

Tento protokol byl již také prolomen prohlášen za nebezpečný a není doporučeno jej používat [18] [19] [1].

2.7 802.11i (WPA2)

Uvedení: v roce 2004 schválen jako standard 802.11i, ale hardware je certifikován WiFi Aliancí pod označením WPA2

Druh šifrování: 128 bitový AES (Advanced Encryption Standard) volitelně také RC4 s TKIP pro zpětnou slučitelnost s WPA.

- CCMP (Counter-mode CBC (Cipher Block Chaining) MAC (Message Authentication Code) Protocol): robustní šifrovací protokol na bázi AES
- MAC (Message Authentication Code): dynamicky mění 128 bitový klíč
- Ruší se použití inicializačního vektoru a zavádí se číslování paketů (PN packet number)
- Každý rámec obsahující Packet Numter (PN) stejné nebo nižší než předchozí rámec je zahozen.

Rotace klíče: Dynamická rotace klíče

Distribuce klíče: Automatická distribuce

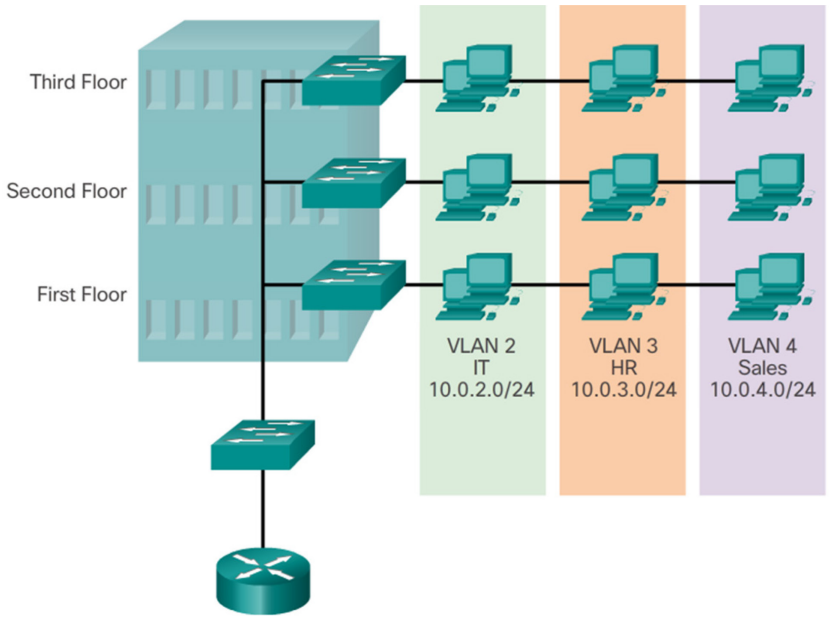
Autentizace: 802.1x nebo PSK

- WPA2 Enterprise: využívá 802.1x pro autentizaci a management klíčů s dynamickou rotací. Metoda je výhodná pro podnikové sítě. Vyžaduje složitější síťovou infrastrukturu se serverem RADIUS.
- WPA2 Personal: používání předem nastavených sdílených klíčů PSK (Pre-shared key) pro běžné uživatele a střední firmy. Klíč byl na obou stranách zapsán pomocí bezpečného kanálu ještě před tím, než ho bylo potřeba použít.

WPA2 (802.11i) se obtížně nasazuje celoplošně, jelikož starší zařízení bez možnosti aktualizace na WPA2 zabezpečení se nadále v sítích používají (typicky s WEP). V situaci, kdy se WEP nelze vyhnout, je jedinou možností umístit zařízení s WEP na VLAN (subnet) a povolit výhradně provoz ze známých stanic. Další z možností je využití VPN šifrovaného tunelu z nezabezpečené sítě do naší domácí sítě například pomocí bezplatného rozšířeného řešení OpenVPN [15] [17] [18] [19].

2.8 VLAN (Virtual Local Area Network)

VLAN (Virtual LAN): logické rozdělení sítě nezávisle na fyzickém uspořádání. Můžeme tedy síť segmentovat na menší subsítě uvnitř fyzické struktury původní sítě. S VLAN můžeme následně pracovat stejně jako s normálními sítěmi. Tedy použít mezi nimi jakýkoliv způsob směrováni. Často se dnes využívá L3 switch (switch, který funguje na třetí vrstvě OSI) pro směrování mezi VLAN [3].



Obrázek 14: Využití VLAN [22].

-Trunk port: port zařazen do více VLAN, které rozlišíme tagem v MAC rámci podle protokolu IEEE 802.1q,

-Důvody využití: seskupování uživatelů podle služeb nebo organizace, snížení broadcastu v síti

-Výhody: přesun zařízení mezi sítěmi pouze přenastavením portu do jiné VLAN, zabezpečení, škálování (IT, VoIP, hosti), snížení HW a ceny, menší broadcast (cílená komunikace pouze na potřebné porty)

-Zařazování: podle portů na switchi, MAC adres, protokolu 3 vrstvy OSI (TCP/IP adresy pevně nastavené v zařízení), autentizace přes RADIUS server pomocí protokolu IEEE 802.1x [22]

2.9 Firewall

Bránu Firewall lze chápat jako zařízení (kombinace hardwaru a softwaru) nebo aplikaci (software) určenou k řízení toku přenosu internetového protokolu (IP) dovnitř nebo ven ze sítě. Brány firewall se používají ke zkoumání síťového provozu a prosazování zásad (firewall policies), založených na pokynech obsažených v sadě pravidel firewallu. Brány firewall jsou obvykle zařazeny do kategorie Síťové nebo Hostitelské:

Síťový firewall je nejčastěji zařízení připojené k síti pro účely kontroly přístupu k jednomu nebo více hostitelům nebo podsítím.

Hostitelský Firewall je nejčastěji aplikace, která kontroluje síťovou komunikaci jednotlivému hostiteli (např. PC) samostatně.

Paketová filtrace: kontrola otevřených spojení pomocí IP adres a portů, kde probíhá komunikace, pravidla uvádí, z jaké adresy a portu a na jakou adresu a port se smí poslat paket, **NEkontroluje obsah.**

Stavová paketová filtrace: paketová + si ukládají informace o povolených spojeních, rychlejší detekce, jestli paket patří do již povoleného spojení. Nazývá se také Stateful Inspection, **NEkontroluje obsah.**

Aplikační brány: komunikace formou 2 spojení, klient se připojí na aplikační bránu (proxy), ta otevře na základě požadavku nové spojení k serveru a stává se pro něj klientem (klient->proxy->server), **kontroluje obsah** [15]**.**

3 TEORIE KE KAMEROVÉMU SYSTÉMU

3.1 HD-TVI (HD Transport Video Interface)

Technologie přenosu videa využívaná pro přenos videa, zvuku a dat po koaxiálním kabelu do vzdálenosti 500m. Videa lze přenášet ve vysokém rozlišení, aktuálně až 8MPx (4K). Je navržena pro využití se stávajícími CCTV koaxiálními rozvody. Podpora UTC protokolu pro vzdálené nastavení moderních CCTV kamer umožňuje kontrolu OSD menu a PTZ (Pan Til Zoom) po koaxiálním kabelu. Toto znamená, že není nutné chodit ke kameře kvůli úpravě jejího nastavení [23].

3.2 H.265 HEVC (High Efficiency Video Coding)

Aktuálně rychle se rozšiřující formát komprese videa. Má za úkol postupně nahradit nejrozšířenější video formát současně využívaný u všech mobilních platforem, Blu-Ray, digitální satelitní a pozemní vysílání, videí streamovaných na internetu (YouTube) a dalších. Pro příklad kodek H.265 HEVC byl vybrán pro kódování nové verze digitálního pozemního vysílání DVB-T2 (Digital Video Broadcasting – Terrestrial 2) televize v České republice.

Velkou výhodou tohoto nového formátu je snížení datového toku, a tudíž i potřebné úložné kapacity videa průměrně o 50 % v závislosti na druhu videa.

Nevýhodou formátu H.265 jsou výpočetní nároky kompresních a dekompresních algoritmů, které přesahují většinu hardware optimalizovaného pro práci s H.264. Z toho důvodu je při přechodu na tento formát většinou nutné zakoupit nový výkonnější hardware, ovšem většina nových mobilních i desktopových procesorů podporují hardwarovou akceleraci tohoto kodeku.

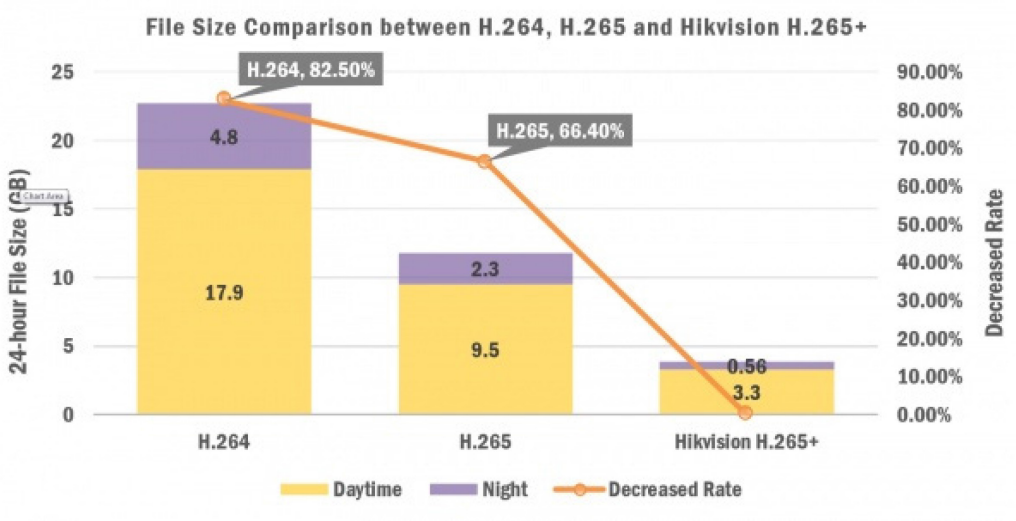
3.3 H.265+

Největší světový výrobce kamerových systémů vyvinul kompresi H.265+. Tato komprese je patentovaná technologie založená na standardu H.265 HEVC, optimalizovaná pro aplikace bezpečnostních kamerových systémů.

Výhodou je, že dokáže ještě více snížit datový tok streamu videa tak, aby se snížily nároky na rychlost připojení a velikost úložiště DVR rekordéru a zároveň nesnižuje kvalitu detailů a ostrost obrazu při zachování velmi ostrého obrazu.

Nejvyšší optimalizace se dosáhne u stabilního pozadí, kde se informace mění velice zřídka. Algoritmus se poté primárně zaměří na objekty, které se pohybují po této stagnující scéně.

Test monitoringu kavárny provedený společností Hikvision prokázal, že průměrný datový tok mezi kompresí H.264 a kompresí H.265+ se snížil o 83 %. Rozdíl mezi kompresí H.265 a H265+ je snížení datového toku o 66,4 % [24].



Obrázek 15: Porovnání velikosti souboru videa po 24 hodinách mezi H.264, H.265 a H.265+ [24].

3.4 WDR (Wide Dynamic Range)

Kompenzace protisvětla. Používá se při velkém kontrastu snímaného prostoru, kde jsou najednou v obraze světlé i tmavé plochy. Jde o speciální algoritmus výpočtu, který vychází ze dvou snímků. Jeden snímek je pořízen při rychlé uzávěrce a druhý při pomalé uzávěrce. Následně dochází ke zpracování obou obrazů a vyhodnocení tmavých a světlých ploch [23] [25].

Obrázek 16: WDR (Wide Dynamic Range) OFF/ON [25].

3.5 DNR (Digital Noise Reduction)

Jedná se o technologii redukce šumu obrazu. Při špatných světelných podmínkách se vyskytuje v obraze šum, který je možné snížit pomocí speciálního algoritmu, zejména při zachycení pohyblivých snímků při slabém osvětlení a poskytuje přesnější a ostřejší kvalitu obrazu [23] [25].

Obrázek 17: DNR (Digital Noise Reduction) OFF/ON [25].

3.6 Smart IR

Jedná se o technologii inteligentního ovládání přísvitu infračervených diod na kameře, která zabezpečí dobrou rozlišitelnost objektů nebo osob pohybujících se směrem ke kameře za slabých světelných podmínek při zapnutém nočním režimu. Kamery bez této technologie mají přísvit vždy na plný výkon a objekty pohybující se směrem ke kameře jsou přeexponované. Kamery se Smart IR analyzují obraz a úpravou výkonu přísvitu zajistí rozlišitelnost objektu [23] [25].

Obrázek 18: Smart IR OFF/ON [25].

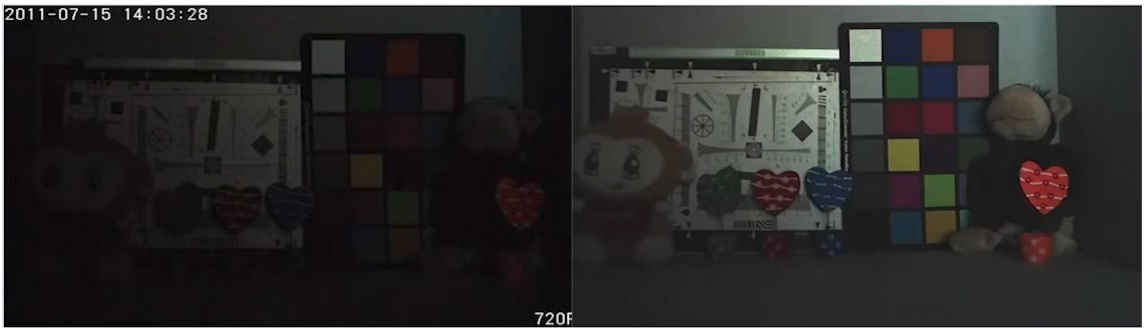
3.7 EXIR

Technologie infračerveného přísvitu od firmy Hikvision, Většinou se jedná o LED diodu, před kterou je umístěna čočka pro rovnoměrný rozptyl infračerveného světla. Výhodou je vyšší světelný výkon cca o 30 %, větší dosvit a rovnoměrné osvětlení monitorované scény, kdy nedochází k přesvětlení středu obrazu a tmavých okrajích [23] [25].

Obrázek 19: EXIR OFF/ON [25].

3.8 Citlivost kamery

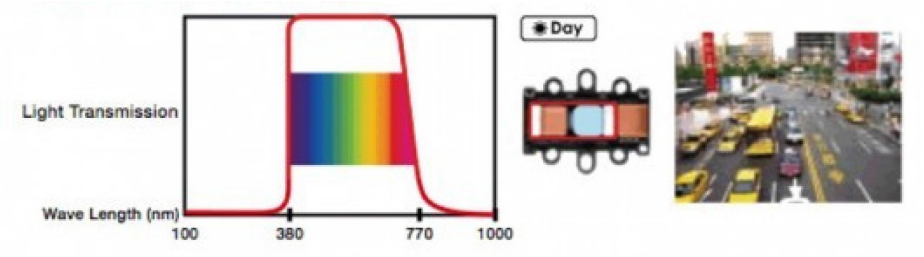
Vyjadřuje schopnost snímat obraz při nízkém osvětlení. Měří se podle intenzity osvětlení v jednotkách lux (lx). Čím nižší citlivost je, tím později je nutné při stmívání přepnout kameru do černobílého režimu s přísvitem infračervených diod. U každé kamery se udává hranice citlivosti v barevném a černobílém režimu [23] [25].



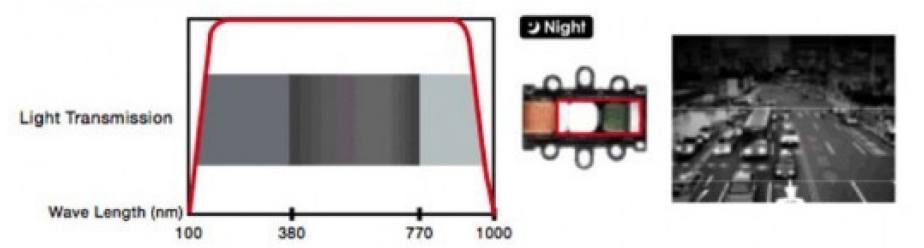
Obrázek 20: Citlivost kamery 0,27lx běžná/ Hikvision Low-light kamera [25].

3.9 IR cut filtr

Filtr IR záření zasunutý v průběhu dne mezi snímací senzor a objektiv. Při nízkém osvětlení je naopak vysunut a kamera se přepne do černobílého módu, který je naopak mnohem citlivější na infračervené spektrum světla než v barevném režimu. Infračervené světlo je v barevném režimu nepotřebné, proto se filtruje pomocí IR cut filtru [23].



Obrázek 21: Aktivace IR cut filtru



Obrázek 22: Deaktivace IR cut filtru [23].

3.10 Provozování kamerového systému z hlediska zákona o ochraně osobních údajů

Na kamerové sledování i pořizování záběrů osob se v každém případě primárně vztahují ustanovení občanského zákoníku upravujícího podmínky ochrany soukromí, osobnosti a podoby člověka. V případě pořizování záznamu obydlí člověka jde o zásah do soukromí upravený v § 86 občanského zákoníku.

Provozování kamerového systému je považováno za zpracování osobních údajů, pokud je automatizovaně prováděn záznam monitorovaného veřejného prostoru a zároveň je účelem pořizovaných informací a záznamů využití k identifikaci fyzických osob v souvislosti s určitým jednáním.

1. Kamerové sledování nesmí nadměrně zasahovat do soukromí a je možno jej použít v případě kdy sledovaného účelu nelze účinně dosáhnout jinou cestou (např. lepším zabezpečením majetku).

2. Je vyloučeno užití kamerového systému v prostorách určených k ryze soukromým úkonům (např. toalety, sprchy).

3. Je třeba předem jednoznačně stanovit účel pořizování záznamů, který musí korespondovat s důležitými, právem chráněnými zájmy správce (např. ochranou majetku před krádeží). Záznamy tak mohou být využity pouze v souvislosti se zjištěním události, která poškozuje tyto důležité, právem chráněné zájmy správce.

4. Musí být stanovena lhůta pro uchovávání záznamů. Doba uchovávání dat by neměla přesáhnout časový limit maximálně přípustný pro naplnění účelu provozování kamerového systému. Data by měla být uchovávána v rámci časové smyčky např. 24 hodin, pokud jde o trvale střežený objekt, nebo případně i dobu delší, v zásadě však nepřesahující několik dnů.

5. Nutností je řádně zajistit ochranu snímacích zařízení, přenosových cest a datových nosičů, na nichž jsou uloženy záznamy, před neoprávněným nebo nahodilým přístupem, změnou, zničením či ztrátou nebo jiným neoprávněným zpracováním.

6. Subjekt údajů musí být o užití kamerového systému a o tom, kdo jej provozuje vhodným způsobem informován (např. nápisem umístěným u vchodu do objektu).

Při dodržení výše uvedených ustanovení § 86 občanského zákoníku nebrání právní předpisy chránit si nemovitost (včetně pozemku) kamerou. Ta však musí být nastavena na sledování chráněné nemovitosti a **nesmí nepřiměřeně zasahovat do soukromí druhých, zejména tím, že by byla nastavena do prostoru nemovitosti (včetně pozemku) souseda**. **Záběr kamery nesmí nepřiměřeně monitorovat ani veřejné prostranství v okolí nemovitosti (ulice, náměstí)** nad rámec nezbytný pro identifikaci případného útočníka proti plášti budovy nebo oplocení soukromého pozemku.

V souvislosti s provozováním kamerového systému má správce povinnost vést záznamy o činnostech zpracování. Nově po nabytí účinnosti obecného nařízení GDPR (General Data Protection Regulation) dne 25. května 2018 záznamy již správce pouze uchovává, tj. nezasílá ÚOOÚ (Úřad pro ochranu osobních údajů). Kamerový systém není třeba nově ani registrovat [26].

Záznam o činnostech zpracování pro kamerový systém musí obsahovat tyto údaje:

Označení správce	Milan Martinek (majitel firmy)
Účel zpracování	ochrana majetku správce, života a zdraví osob prostřednictvím stálého kamerového systému.
Popis kategorií subjektů údajů	Zaměstnanci a příležitostně vstupující osoby do monitorovaného prostoru (dodavatelé, návštěvy apod.)
Popis kategorií osobních údajů	Podoba a obrazové informace o chování a jednání zaznamenaných osob.
Příjemci osobních údajů a informace o případném předání osobních údajů do třetích zemí	V odůvodněných případech orgány činné v trestním řízení, případně jiné zainteresované subjekty pro naplnění účelu zpracování (např. pojišťovna).
Lhůta pro výmaz	Doba uchování záznamu je 7 dní. Záznam zachyceného incidentu je uchován po dobu nezbytnou pro projednání případu.
Technická a organizační bezpečnostní opatření	Bezpečnostní kryt, řízený přístup k datům, školení oprávněných osob, vedení záznamů o předání nahrávek oprávněným orgánům a osobám.

Tabulka 2: Záznam o činnostech zpracování pro kamerový systém [26].

4 TEORIE K POKLADNÍMU SYSTÉMU

4.1 Elektronická evidence tržeb

4.1.1 Legislativa

Elektronická evidence tržeb (EET) je popsána zákonem č. 112/2016 Sb. a byla zavedena jako odpověď na dlouhodobé a systematické krácení daňové povinnosti, jelikož finanční správa neměla potřebné kapacity na daňovou kontrolu všech podnikatelů v republice.

Dále byly odstraněny nerovné podmínky v konkurenčním boji mezi poctivými a nepoctivými podnikateli, kteří šetřili na odvodech daní státu a mohli tak poskytovat výhodnější výrobky nebo služby.

Zákonu podléhají všechny subjekty, které platí nebo mají platit daně z příjmů v České republice, a to podnikající fyzické osoby a právnické osoby s podnikatelskou činností.

Tyto subjekty musí evidovat tržby pocházející z podnikatelské činnosti uhrazené v hotovosti, šekem, směnkou a jinými obdobnými způsoby např. stravenkou. Výjimku mají pouze nově od 1. 3. 2018 transakce platby kartou tedy přímý převod z účtu na účet [27].

Povinnost přechodu na tento nový způsob evidence mají podnikatelé postupně podle odvětví podnikatelské činnosti ve fázích:

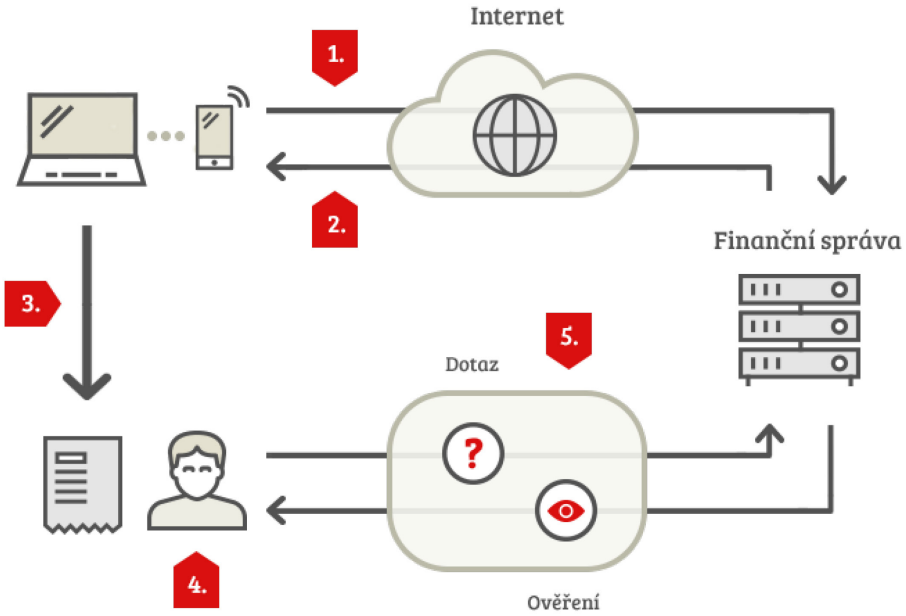
- 1. fáze (od 1. prosince 2016) ubytovací a stravovací služby.
- 2. fáze (od 1. března 2017) maloobchod a velkoobchod.
- 3. fáze ostatní činnosti, například svobodná povolání, doprava, zemědělství.
- 4. fáze vybraná řemesla a výrobní činnosti.

Poslední 2 fáze byly v době psaní diplomové práce pozastaveny rozhodnutím Ústavního soudu ze dne 12. prosince 2017 sp. zn. Pl. ÚS 26/16 a připravuje se opravná novela zákona.

Údaje o tržbách lze evidovat v běžném režimu on-line nebo ve zjednodušeném režimu off-line po schválení výjimky finančním úřadem a jedná se především o provozovny bez možnosti přístupu k internetu nebo případy, kdy by evidování běžným způsobem znemožnilo nebo zásadně ztížilo plynulý a hospodárný výkon podnikání [27].

4.1.2 Princip Evidence tržeb v běžném režimu

Komunikace probíhá pomocí protokolu HTTPS v zabezpečené formě pomocí SSL asymetrického šifrování. Nutností je obstarat si certifikát a heslo k jeho autentizaci na daňovém portálu ministerstva financí a následně importovat tyto prvky do pokladního systému společně s číslem provozovny a dalších údajích o provozovně a podnikateli (postup je popsán podrobněji v praktické části práce). Od té doby probíhá online nepřetržitá komunikace mezi servery Finanční správy a pokladním systémem. Dále je popsán podrobněji princip komunikace při vystavení digitální nebo papírové účtenky zákazníkovi:



Obrázek 23: Evidence tržeb v běžném režimu [28].

1. Před tiskem účtenky zašle pokladní systém datovou zprávu o transakci ve formátu XML na server Finanční správy. **Zpráva obsahuje:**

- **PKP** (Popisný kód poplatníka) je kód o velikosti 344 znaků generovaný pokladním systémem a jednoznačně identifikuje příslušnou tržbu. Uvádí se na účtenku pouze v případě poruchy komunikace (mezní doba odezvy vyšší než 2s) nebo při účtování ve zjednodušeném režimu.
- **BPK** (Bezpečnostní kód poplatníka) je otisk kódu PKP o velikosti 44 znaků a uvádí se na účtenku vždy.
- DIČ (Daňové identifikační číslo) poplatníka
- označení provozovny, ve které je tržba uskutečněna (pro první provozovnu č. 11)

- označení pokladního zařízení, na kterém je tržba evidována
- pořadové číslo účtenky
- datum a čas přijetí tržby nebo vystavení účtenky (pokud je vystavena dříve)
- celkovou částku tržby
- údaj, zda je tržba evidována v běžném nebo zjednodušeném režimu

2. Server Finanční správy příjme XMS data, zkontroluje podpis certifikátu a uloží data účtenky do databáze. Zpět pokladnímu systému vygeneruje a pošle podepsané potvrzení o přijetí evidované tržby společně s kódem FIK (Fiskální identifikační kód).

   FIK je unikátní kód potvrzující zaevidování tržby pro každou potvrzovanou datovou zprávu o délce 39 znaků generovaný serverem Finanční správy. Na účtenku se uvádí vždy s výjimkou neúspěšné komunikace nebo při účtování ve zjednodušeném režimu, v těchto případech ho nahradí kód PKP.

3. Podnikatel vystaví účtenku (vytiskne nebo pošle elektronicky), kterou předá zákazníkovi. Účtenka musí obsahovat stejné povinné údaje jako v případě datové zprávy, až na jeden údaj. Tím je nahrazení popisného kódu poplatníka (PKP) fiskálním identifikačním kódem (FIK) v případě že nedojde k poruše komunikace (mezní doba odezvy vyšší než 2s) nebo při účtování ve zjednodušeném režimu.

4. Zákazník obdrží účtenku

5. Zákazník si může ověřit svoji účtenku prostřednictvím webového rozhraní Ověření účtenky na daňovém portálu Ministerstva financí.
   Podnikatel si ověří tržby evidované pod jeho jménem ve webovém rozhraní Správa údajů o evidenci tržeb na daňovém portálu Ministerstva financí [28].

II. PRAKTICKÁ ČÁST

5 NÁVRH VHODNÝCH SÍŤOVÝCH PRVKŮ

5.1 Záložní zdroj Eaton 5E 1500i USB

Při výběru záložního zdroje byl kladen důraz na dostatečný výstupní výkon a kapacitu baterie pro napájení všech důležitých zařízení, které je zapotřebí udržet v aktivním stavu i po náhodném výpadku elektrické sítě do doby, než odpovědný personál obnoví tok elektřiny v objektu (nahodí jistič) nebo se přepojí na elektrocentrálu (v případě dlouhodobého problému) je napojeno na záložní zdroj UPS.

Tento zdroj zároveň musí sloužit i jako přepěťová ochrana a stabilizovat výstupní napětí tzn. posilovat nižší napětí (boost) a potlačovat vyšší napětí (trim), **aniž by přecházel na akumulátorové napájení**. Tyto zdroje se označují jako Line-Interactive. Z toho důvodu byl po přečtení mnoha recenzí a názorů z internetových diskuzních fór vybrán model Eaton 5E 1500i USB.

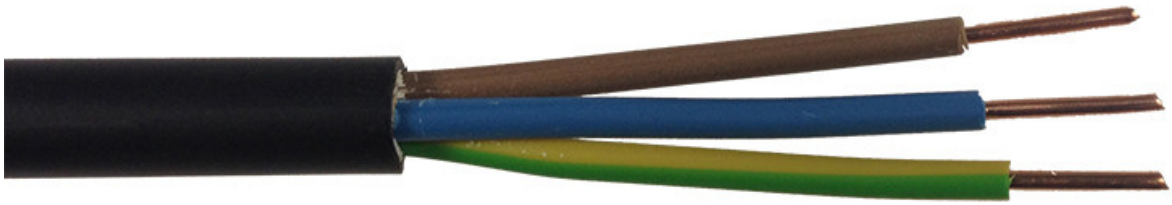
Záložní zdroj Eaton 5E 1500i USB byl vybrán z následujících důvodů:

- Maximální vstupní zatížení: 1500 VA / 900 W
- Line-interactive (stabilizace výstupního napětí, aniž by přecházel na akumulátor)
- Možnost integrace do systémů správy napájení klientského zařízení s OS Windows a monitoring stavu UPS pomocí USB spojení.
- Stabilní výstup 230V/50Hz.
- Přibližní záložní čas: 50 minut (1 PC) [29].

Obrázek 24: Záložní zdroj Eaton 5E 1500i USB [29].

Pro rozvod AC 230V/50Hz byla využita následující kabeláž:

Obrázek 25: Kabel CEE 7/5 (E) zásuvka IEC C14 vidlice



Obrázek 26: Kabel CYKY 3 x 1,5 J

Obrázek 27: Vícenásobná zásuvka na kabel IP44 gumová, 3 x 230V/16A, Vidlice 50252 230V černá gumová IP44

5.2 Konvertor Optika/Ethernet Tp-link MC220L + SFP modul

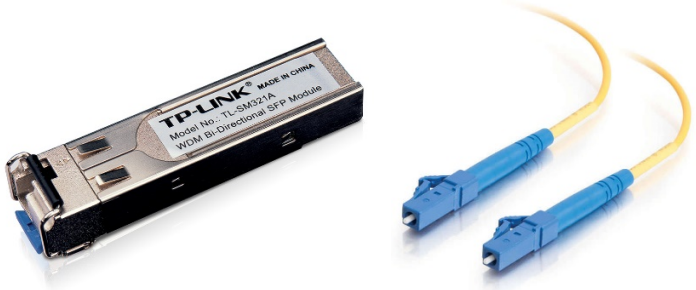
Následující konvertor Tp-link MC220L byl poskytnut poskytovatelem internetového připojení, firmou Anext s.r.o. Je určen k převodu médií z optického vedení 1000BASE-SX (2x mnoho vidové vlákno s vlnovou délkou 850 nm), 1000BASE-LX (2x mnoho vidové nebo jedno vidové vlákno, 1330nm) případně 1000BASE-BX (jednovidové optické vlákno, 1490 nm downstream a 1310 nm upstream) na metalické vedení 1000Base-T a naopak. Konvertor byl vybrán z následujících důvodů:

- 1x Gigabit slot pro SFP modul (Small Form-factor Pluggable) neboli vložný modul optického převodníku osazený zpravidla duplexním LC (Lucent Connector) konektorem. SFP moduly se vyrábí a dodávají v mnoha variantách podle použitého typu vlákna, přenosového protokolu, překlenované vzdálenosti a vlnové délky.
- 1x Gigabit RJ45 port s funkcí Auto MDI/MDIX (Medium Dependent Interface / Medium Dependent Interface Crossover) na všech portech eliminuje potřebu křížených kabelů nebo portů odchozího připojení.
- Dosah vedení až 0,55 km u mnoho vidového a 10 km u jedno vidového optického kabelu.
- Maximální spotřeba energie : 3,95W [30].

Obrázek 28: Konvertor Optika/Ethernet Tp-link MC220L [30].

Osazený SFP modul TP-Link TL-SM321A podporuje:

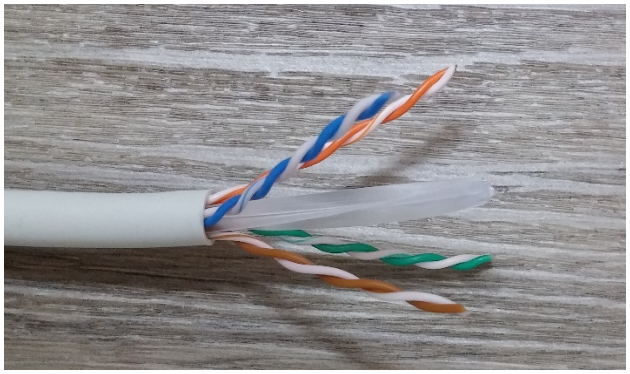
- 1 optický 1000Base-BX port pro Single-mode vlákno 9/125um s 1 konektorem LC



Obrázek 29: Obousměrný SPF modul TP-Link TL-SM321A, Single-mode vlákno 9/125um s 1 konektorem LC [31].

5.3 Síťový kabel CAT6 UTP

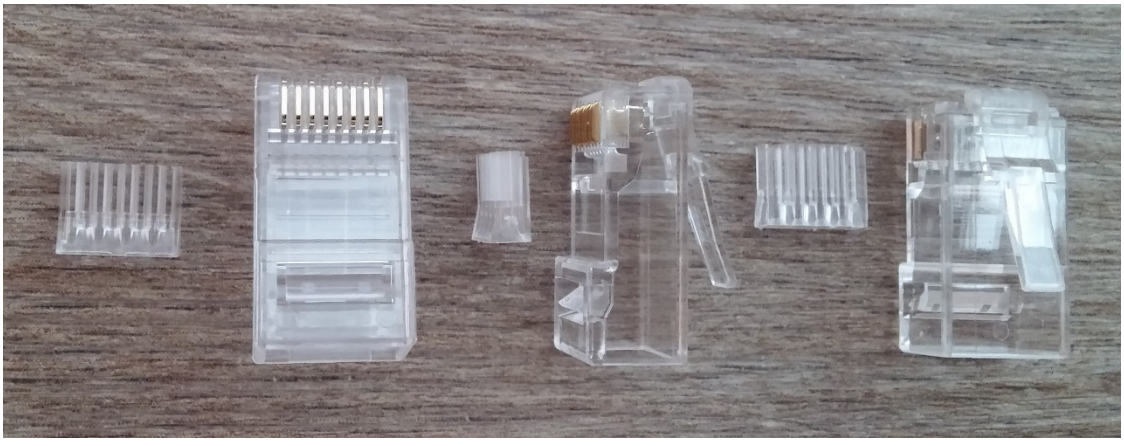
Kabel kategorie 6 byl zvolen pro spolehlivý přenos Gigabit Ethernetu (1000BaseT), díky šířce pásma 250MHz je méně náchylný na ruchy okolí a případné degradace spojení na nižší rychlosti. Také lze v případě potřeby přejít na plný duplex Gigabit Ethernet (1000BaseTX), který podporuje přenos 1 Gbps ve stejnou chvíli v obou směrech (tj. 2 páry x 500Mbps v jednom směru a 2 páry ve směru opačném).



Obrázek 30: Kabel CAT6 UTP

5.4 Konektor RJ45 CAT6 UTP 8p8c na drát KRJ45/6SLD

Tyto konektory jsou určeny pro UTP kabel kategorie 6 s pozlacenými piny uzpůsobenými pro průřez vodiče typu drát. Skládají se ze dvou částí, samotného konektoru a vložky. Vložka slouží k lepší manipulaci s vodiči [2].



Obrázek 31: Konektor KRJ45/6SLD.

K samotné práci byly při zapojování dále použity krimpovací kleště Netrack RJ45 8p +6 p +4 p a tester kabelů Logilink pro konektory RJ11, RJ12 a RJ45.

Obrázek 32: Krimpovací kleště Netrack RJ45 8p, tester Logilink, kabel, konektor, krytka.

5.5 POE Injektor Ubiquiti POE-24-12W-G

POE (Power Over Ethernet) injektor Ubiquiti POE-24-12W-G byl dodán v balení společně s Access Pointem Ubiquiti UniFi AP AC Long Range. Z důvodu jeho dostatečných parametrů byl využit k napájení výše uvedeného Access Pointu společně s Routerem Ubiquiti EdgeRouter X. Mezi tyto parametry patři:

- **Vstupní port napájení:** IEC 320 C6, 100-240AC, 50/60Hz, 0,2-0,3A.
- **Vstupní datový port LAN:** RJ45 stíněný, Gigabit.
- **Výstupní datový port POE:** RJ45 stíněný, Gigabit, 24V DC, 0,5 A, 12W.
- **Zabezpečení zařízení připojeného k výstupnímu datovému portu POE:** Ochrana proti přepětí (1500A (8/20 µs)), špičkovým pulzním proudům (36A (10/1000 µs)), elektrostatickému výboji (při využití stíněného kabelu a konektorů do portu LAN), AC kabel s uzemněním [32].

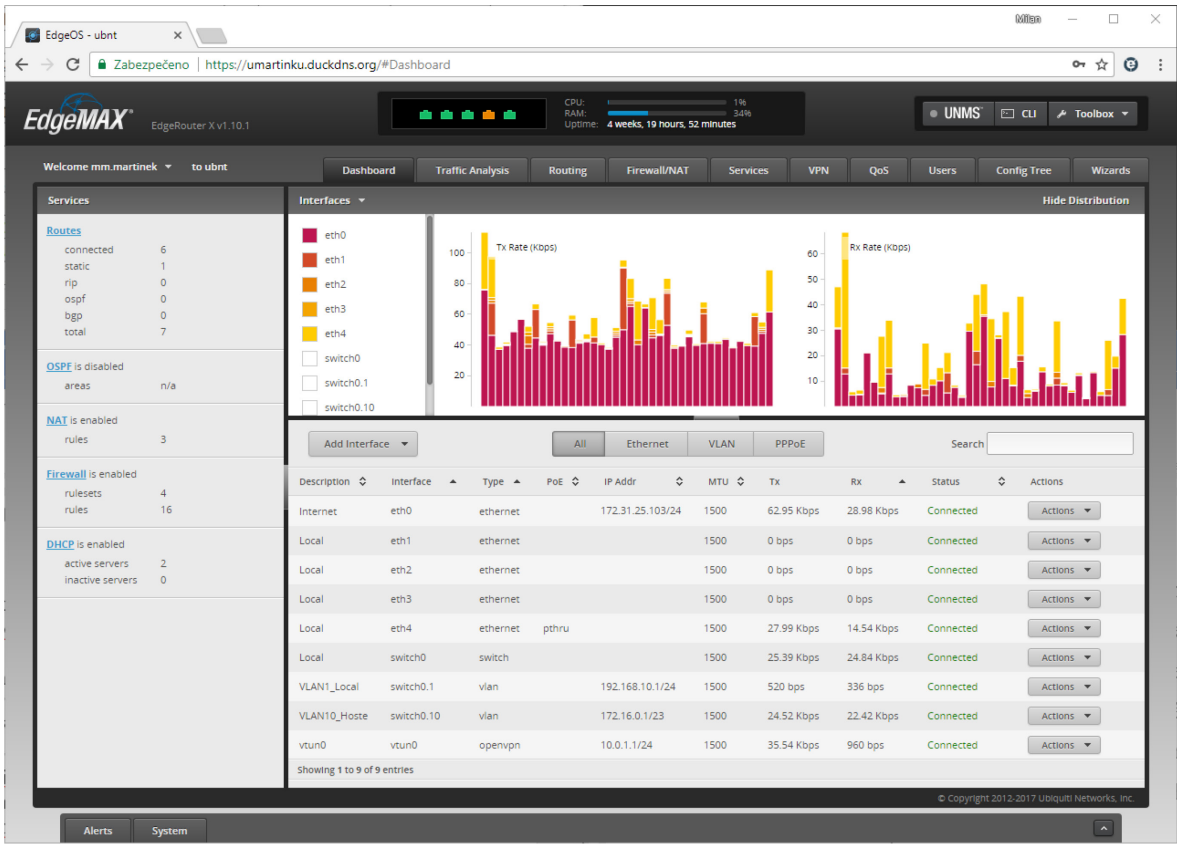
Obrázek 33: POE Injektor Ubiquiti POE-24-12W-G [32].

5.6 Router Ubiquiti EdgeRouter X

Při výběru routeru byl kladen důraz získat za přijatelnou cenu všechny potřebné technologie pro konfiguraci navržené sítě. Bylo nutno zvolit router korporátní třídy určený pro profesionální využití a zajistit podporu OpenVPN serveru, VLAN, Firewall s možností konfigurace podrobné bezpečnostní politiky, dostatečným výkonem pro využití SSL šifrování s využitím šifry AES 256bit, možností pokročilé konfigurace, diagnostiky a správy sítě, minimálně 5 gigabitových portů RJ45 (aby nebylo nutno dokupovat switch) a minimálně jeden s podporou POE výstupu pro napájení Access Pointu.

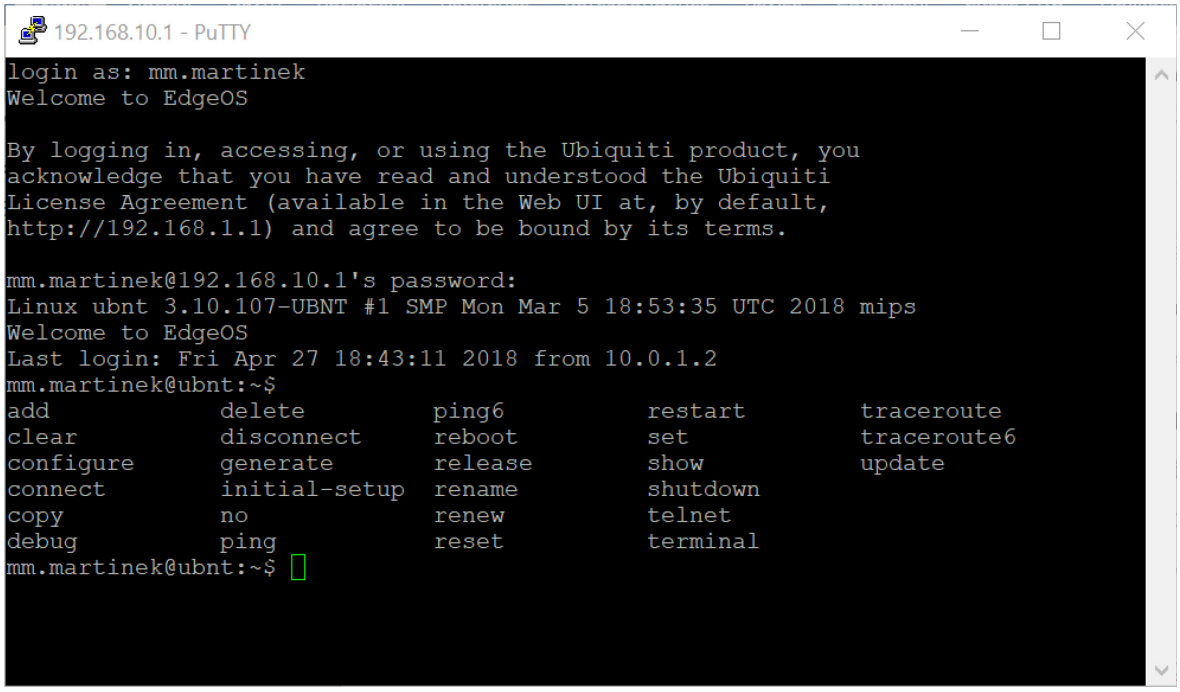
Z toho důvodu byl po přečtení mnoha recenzí a názorů z internetových diskuzních fór vybrán právě router Ubiquiti EdgeRouter X a to z následujících důvodů:

- Konfigurace pomocí GUI (Graphical User Interface) webového operačního systému EdgeOS 1.10 s možností detailního nastavení většiny podporovaných služeb s využitím struktury okenních nabídek, případně konfiguračního stromu veškerých nastavených parametrů. Součástí GUI rozhraní je rovněž podrobná diagnostika sítě a správa připojených klientů.



Obrázek 34: Router Ubiquiti EdgeRouter X GUI.

- Pokročilá konfigurace pomocí CLI (Command Line Interface) s využitím zabezpečené komunikace skrze SSH (Secure Shell) prostřednictvím software klienta Putty atd. nebo online klienta ve webovém GUI rozhraní.



Obrázek 35: Router Ubiquiti EdgeRouter X CLI SSH SW Putty

- **Porty**: 5x Gigabit RJ45 (1x POE IN 24V, 1x POE OUT) plně konfigurovatelné
- **Napájení**: 24V (12-50W) POE RJ45 portu nebo napájecího adaptéru pro zpřístupnění portu POE OUT
- **Maximální spotřeba energie:** 5W
- **Podpora protokolů:** DHCP, VLAN, DDNS, DNS, SSH
- **Firewall:** NAT, Směrování portů, ACL (Access Control List) druh stavového firewalu, který filtruje provoz na základě zdrojové a cílové IP adresy nebo rozsahů a použitého protokolu. Navíc udržuje již navázané relace.
  Řízení přístupu podle oblastí: Umožňuje zvolit různé politiky kontroly pro různé hostitelské skupiny připojené na stejné rozhraní routeru. Není závislé na ACL. Vše je zablokované, pokud není výslovně povoleno.
- **VPN**: OpenVPN (typu síť-síť nebo vzdálený přístup), L2TP IPSec (typu síť-síť nebo vzdálený přístup)
- **Procesor:** Dual-Core 880 MHz, MIPS1004Kc
- **Operační paměť RAM (Random Access Memory):** 256MB DDR3
- **Úložiště:** 256 MB [33].

Obrázek 36: Router Ubiquiti EdgeRouter X [33].

Zvažováno bylo také o bratrské zařízení z rodiny Ubiquiti EdgeRouter s názvem EdgeRouter X SFP, který obsahuje navíc slot pro Gigabit SFP modul (Small Form-factor Pluggable) pro připojení optického kabelu přímo do routeru a nebylo by nutno využívat externí převodník TP-Link MC220L a celá síť by se zjednodušila. Ovšem nakonec bylo od tohoto řešení upuštěno, jelikož převodník byl již dříve dodán poskytovatelem Internetového připojení a router s tímto slotem byl cca o 40% dražší, navíc nebylo jasné, jestli bude možno optickou přípojku dotáhnout až k pozici umístění routeru, jelikož majitel restaurace plánuje v budoucnu restauraci rekonstruovat a rozšiřovat. Z těchto důvodů byla nakonec vybrána varianta bez slotu pro SFP modul.

Obrázek 37: Router Ubiquiti EdgeRouter X SFP [33].

5.7 Access Point Ubiquiti UniFi AP AC Long Range

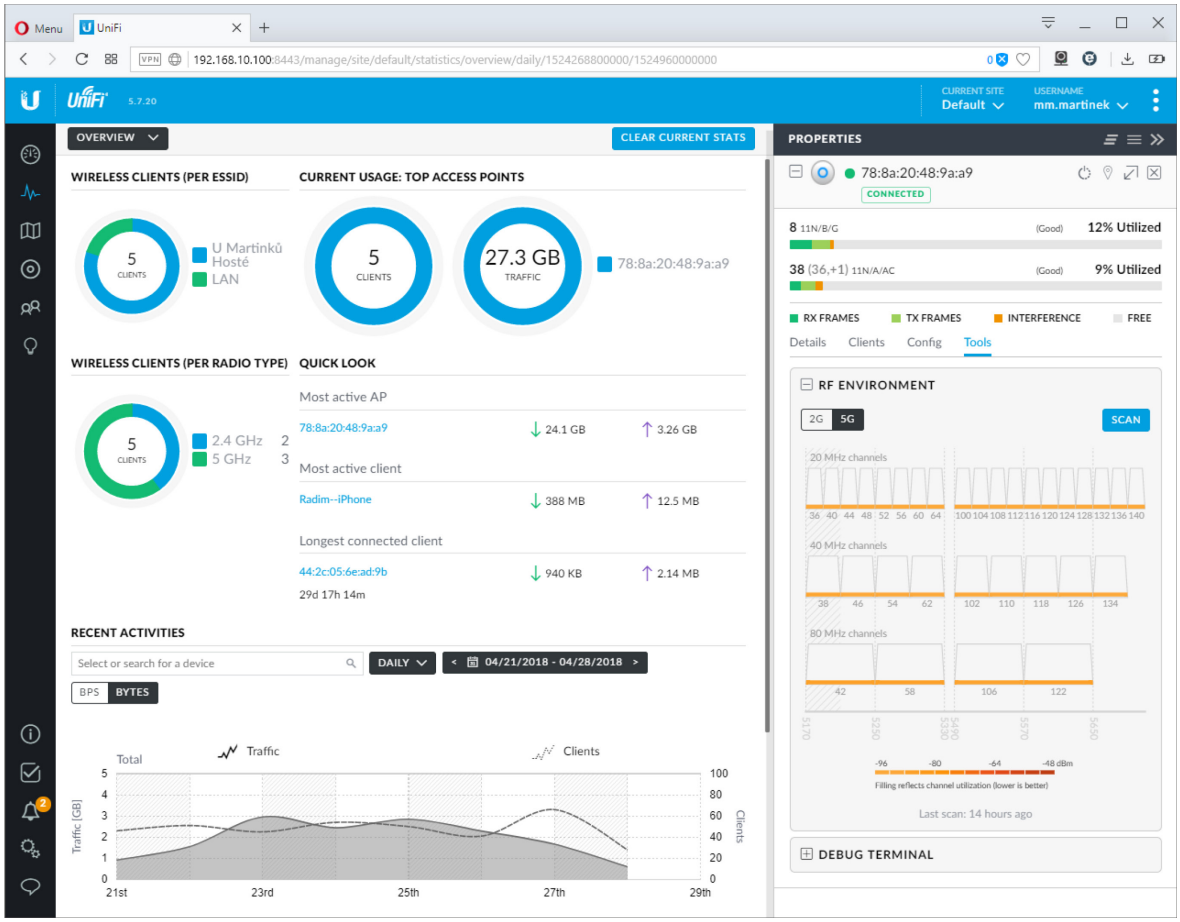
Topologie sítě tvořená centrálním routerem a jedním nebo v případě potřeby více oddělenými Access pointy byla zvolena za účelem vytvořit vysoce **modulární síť** s kvalitním pokrytím WiFi WLAN a podporou efektivního moderního standardu IEEE 802.11ac na pásmu 2,4GHz, zároveň méně rušeném pásmu 5GHz a vysíláním více streamů pomocí technologie MIMO. Dále byl kladen důraz na podporu POE napájení pomocí UTP kabelu, aby bylo možné sloučit napájení s POE výstupem routeru, případně v případě budoucího rozšíření POE výstupy switche. Bylo nutno zvolit Access point korporátní třídy, určený pro profesionální využití a nejlépe totožné značky s routerem, aby byla zajištěna maximální kompatibilita a podpora funkcí potřebných pro realizaci autorova návrhu. Mezi tyto funkce patří především VLAN, možnost konfigurace inicializačního portálu pro hosty, podrobné možnosti zabezpečení firemní WLAN a přehledné dohledové centrum pro správu přihlášených klientů.

Z toho důvodu byl po podrobném průzkumu trhu vybrán Access point Ubiquiti UniFi AP AC Long Range a to z následujících důvodů:

- **Porty**: 1x Gigabit RJ45 POE IN.
- **Napájení**: 24V DC, pasivní POE RJ45 port.
- **Maximální spotřeba energie:** 6,5W, režimy úspory energie.
- **Anténa**: Dual-Band, Tri-Polarity (Horizontální, Vertikální, Šikmá), Výstupní výkon: 2,4 GHz: 24 dBm, 5 GHz: 22 dBm, úprava pro lepší příjem signálu klientů se slabými vysílači (telefony) [34].

Obrázek 38:Ubiquiti UniFi AP AC Long Range [34].

- **WiFi:** 802.11 a/b/g/n/ac, 2,4GHz: MIMO 3x3, 450 Mbps, 5GHz: MIMO 2x2, 867 Mbps.
- **Podpora zabezpečení:** WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES).
- **Podpora protokolů a funkcí:** VLAN, QOS (Omezení uživatelské rychlosti), Inicializační portál pro hosty, 250+ současně připojených klientů .
- Pokročilá konfigurace pomocí CLI (Command Line Interface) s využitím zabezpečené komunikace skrze SSH (Secure Shell) prostřednictvím software klienta Putty.
- Konfiguraci a dohledové centrum zajišťuje specializovaný software Unifi Controler, který je nutno nahrát na síťový server. Prostřednictvím přehledného GUI rozhraní poskytuje centralizovanou správu a diagnostiku všech podporovaných sítových zařízení v síti včetně připojených klientů [34].



Obrázek 39: Unifi Controler.

6 NÁVRH POKLADNÍHO SYSTÉMU

Při výběru vhodného pokladního systému byl proveden rozsáhlý průzkum možných systémů, které se na trhu aktuálně vyskytují. Následně byl stanoven užší výběr 2 pokladních systémů na základě:

- Vhodných parametrů potřebných pro provoz gastronomického zařízení.
- Osobních praktických zkušeností autora z pohledu technika a administrátora původního systému O2 Ekasa.
- Požadavků a námětů obslužného personálu gastronomického zařízení.

V konečné fázi byly oba pokladní systémy důkladně otestovány autorem práce za přítomnosti vedení firmy a po následné diskusi bylo učiněno rozhodnutí.

6.1 O2 Ekasa

Původní řešení pokladního systému, které bylo před plánovanou změnou využíváno, se nazývá Ekasa od společnosti O2 Česká republika. Bylo vytvořeno jako odpověď na nový zákon č. 112/2016 Sb. pojednávající o elektronické evidenci tržeb. Aktuálně se stal řešením pro nejvíce uživatelů na trhu. Zákazníky nalákaly nejspíše na první pohled výhodné pořizovací náklady a cenová politika, kdy veškerý potřebný hardware lze pořídit za 4 995 Kč. Na tuto cenu lze rovněž uplatnit slevu na dani ve výši 5000 Kč dle novely zákona o daních z příjmů § 35bc. Po těchto počátečních nákladech platí klient měsíčně paušální poplatek 499 Kč. Tuto částku si lze ponížit v případě, že zákazníci platí u klienta kartou pomocí platebního terminálu dodávaného společně s Ekasou. Přesněji při platbách kartou nad 50 tisíc se částka poníží na 250 Kč / měsíc a při platbách kartou nad 100 000 Kč je služba zcela zdarma [35].

Obrázek 40: O2 Ekasa (terminál) [35].

K hlavním výhodám patří:

- Cloudová záloha na servery 02 Czech republic.
- Možnost prohlížení a úpravy dat skrze webovou službu O2 eKancelář.
- EET komunikace a aktualizace software Ekasy pomocí LTE sítě O2.
- Telefonická podpora zdarma.

K hlavním nevýhodám patří:

- Nestabilita a časté pády aplikace
- Časté chyby v rozhraní aplikace (nejvíce při konfiguraci skladových zásob).
- Při vyšším počtu položek a složených výrobků propojených se skladem dochází k značnému zpomalení uživatelského prostředí a celkové odezvy aplikace.
- Velmi slabé možnosti nastavení aplikace a přizpůsobení uživatelského prostředí.
- Nestabilita a časté samovolné odpojování bluetooth platebního terminálu.
- Nelze se připojit pomocí ethernetového rozhraní, k dispozici pouze WiFi.
- Nestabilita a časté samovolné odpojování síťové tiskárny do kuchyně.
- Nemožnost připojit více než jednu tiskárnu skrze rozhraní USB.
- Nekvalitní hardware náchylný na časté závady.
- Špatně vyřešená synchronizace mezi Ekasou a Cloudovým úložištěm (často se stávalo, že se některé položky nesynchronizovaly z Cloudu do Ekasy, nebo se tvořily duplicity té samé položky s upravenými parametry i s parametry před úpravou, následně se stala databáze položek velmi matoucí a nepoužitelná).
- Neschopnost pracovníků telefonické podpory poradit s problémem, který nelze vyhledat ve stručné verzi uživatelské příručky.

6.2 Dotykačka

Dále bylo uvažováno nad aktuálně velmi oblíbeným pokladním systémem Dotykačka. Systém nabízí 3 druhy licencí ve formě měsíčního předplatného, které se liší zejména počtem odemknutých dodatečných funkcí, jako například evidence skladů, dodavatelů a podobně. V porovnání s O2 Ekasou nabízí více možností konfigurace a propracovanějších funkcí. Po předvedení systému obchodním zástupcem firmy a následným podrobným testováním bylo

zjištěno, že je značně propracovanější, a hlavně více odladěný než původní systém od O2 [36].

Obrázek 41: Dotykačka Univerzální (terminál) [36].

K hlavním výhodám patří:

- Pravidelné aktualizace zdarma.
- Přehledné a plynulé uživatelské prostředí.
- Cloudová záloha a správa dat z pokladen skrze webový prohlížeč.
- Telefonická podpora a vzdálený servis technika zdarma.

K hlavním nevýhodám patří:

- Měsíční předplatné bez možnosti zakoupit trvalou licenci.
- Nemožnost připojit více než jednu tiskárnu skrze rozhraní USB.
- Nemožnost volby vlastního hardware pokladny nebo příslušenství jako tiskárny atd.
- Nemožnost detailní konfigurace celého systému.
- Nemožnost tvorby vlastních návrhů uživatelského rozhraní včetně programování funkcí jednotlivých ikon.
- Nemožnost vytvořit vlastní datový server bez nutnosti odesílat firemní data do cloudu.
- Nemožnost založení uživatelských účtů stálých zákazníků s automatickým přiřazením slevy.

6.3 Zvolené řešení Consulta Conto MAX

Vítěz volby. Jedná se o moderní vysoce modulární a konfigurovatelný pokladní systém, vhodný do náročných gastronomických provozů nebo hotelů. Je postaven na databázi SQL (Structured Query Language) a využívá platformu Microsoft Windows. Jedná se o placený software prodávaný formou jednorázové platby s možností přikoupení dalších modulů a aktualizací [37].

Obrázek 42: Consulta Conto MAX [37].

Po konzultaci s majiteli restaurace byla vybrána verze Consulta Conto MAX, která obsahuje v ceně následující moduly:

- modul restaurační funkce (operace se stoly, zákazníci, pokoje)
- modul rozšířené obchodní funkce (neomezená PLU, neomezené skupiny)
- modul síťové verze (napojení na externí sklad, síťový provoz)
- modul kalkulací a skladu (evidence skladu, inventury, kalkulace)
- modul statistik prodejů (rozšířené statistiky, vyhledávání)
- modul zákaznických slev a plánování (akční slevy, plánování, zákaznické karty)
- + přikoupen modul Podpora připojení platebního terminálu

K hlavním výhodám patří:

- Běh na nejrozšířenější platformě Microsoft Windows (podpora velkého množství přídavných zařízení jako jsou tiskárny, čtečky čárových kódů, zákaznický displej, čtečku zákaznických karet, obchodní váhy, skener atd.).

- Možnost podrobné konfigurace celého systému i přídavných modulů.
- Možnost tvorby vlastních návrhů uživatelského rozhraní včetně programování funkcí jednotlivých ikon.
- Vlastní datový server bez nutnosti odesílat firemní data do cloudu.
- Modularita systému zajišťuje v případě potřeby rozšíření o další pokročilé funkce.
- Možnost připojení více tiskáren přes rozhraní USB.
- Možnost provádět jakékoliv rozšíření hardware jako například v případě potřeby zvýšit velikost interního úložiště nebo úhlopříčky dotykového displeje.
- Minimální nároky na Hardware.
- Okamžité reakce uživatelského prostředí.

K hlavním nevýhodám patří:

- Kvůli komplexnosti systému a potřebě značných technických znalostí z oblasti sítí, konfiguraci platebního terminálu, sestavování serveru (kasy), vytváření databáze, uživatelského rozhraní atd., je nezbytná přítomnost školeného technika nebo člověka s IT zaměřením.
- Placené aktualizace pokladního systému.
- Žádná telefonická podpora, pouze technický manuál. Pro běžné uživatele nutnost objednat placeného servisního technika.

Pokladní systém byl nahrán na počítač od firmy LYNX. Tato sestava je oficiálně doporučena firmou Consulta (výrobce pokladního systému Conto Max). Počítač je zároveň využíván jako server pro různé síťové služby, například Unifi Controler a podobně.

PC sestava Lynx byla vybrána z následujících důvodů:

- **Operační systém:** Windows 10
- **Procesor:** Intel Celeron J1800, 2.41 GHz, 2 jádra, TDP (Thermal Design Power) 10W, dedikovaná grafika Intel HD Graphics Z3700 792 MHz
- **Operační paměť RAM:** 2GB DDR3 (Double Data Rate 3)
- **Úložiště:** SSD (Solid State Drive) Transcend SSD370S 32GB, rychlost čtení: 230 MB/s, rychlost zápisu: 40 MB/s
- **Pasivní chlazení**
- **Využívané porty:** HDMI (High Definition Multimedia Interface), 3x USB (Universal Seriál Bus) 3.0, RJ45 (Gigabit Ethernet)

- **Monitor:** AsusVT168, 10 bodové dotykové ovládání kompatibilní s Windows 10, rozlišení 1366×768 px, úhlopříčka 15,6"

Obrázek 43: Počítačová sestava LYNX Conto Max 15" [37].

6.3.1 Tiskárna Epson TM-T20II

K počítači bylo nutno zajistit 2 tiskárny. První k tisku účtenek pro zákazníky, výpisů tržby a dalších výkazů, které generuje software pokladního terminálu. Druhá do kuchyně k tisku bonů neboli výpisu produktů, které si zákazník objednal a je zapotřebí zhotovit je v kuchyni. Při výběru byl kladen důraz na spolehlivost a rychlost tisku. Tiskárny se v době obědů a večerních hodin používají prakticky neustále, navíc zákon č. 112/2016 Sb o elektronické evidenci tržeb přikazuje, aby každému zákazníkovi byla nabídnuta účtenka (i když nemá povinnost ji přijmout).

Tiskárna Epson TM-T20II byla vybrána z následujících důvodů:

- **Druh tiskárny:** termální pro tisk na 80mm kotoučky.
- **Rychlost tisku:** 200 mm/s.
- **Konektivita:** Ethernet 100 Base-TX RJ45, USB 2.0.
- **MTBF (Mean Time Between Failure):** 360 000 hodin (cca 41 let).
- **Střední počet cyklů mezi poruchami**: 60 000 000 řádků.
- **Životnost řezačky**: 1 500 000 řezů.
- **Spotřeba energie:** 43,2W při tisku, 2,4W pohotovostní režim [38].

Obrázek 44: Tiskárna Epson TM-T20II [38].

K připojení tiskárny do kuchyně byl zvolen aktivní USB kabel o délce 20m (běžná max. délka běžného kabelu se udává do 5m). Kabel obsahuje 2 aktivní zesilovače signálu napájené interně pouze z konektoru serveru.

Obrázek 45: USB 2.0 aktivní repeater 20m prodlužovací.

6.3.2 Platební terminál Verifone VX675

Při výběru platebního terminálu byl kladen důraz na podporu bezdrátové WLAN konektivity pomocí technologie WiFi pro zajištění mobility. Díky podpoře WiFi a vestavěné baterii lze obsloužit zákazníka přímo u kteréhokoliv stolu a nemusí chodit k pultu číšníka.

Jediný platební terminál kompatibilní s modulem pro obsluhu platebních terminálů pokladního systému Consulta Conto Max a podporou WiFi se nazývá Verifone VX675:

- Podpora všech běžných typů platebních karet (VISA, MasterCard, Maestro) a elektronických stravenek (Sodexo, Edenred, Callio).
- Podpora bezkontaktních platebních karet.
- Automatický přenos údajů o platbě z pokladního systému po volbě platby kartou.
- **Displej**: 2.8“, rozlišení 320x240 pixelů, barevný TFT.

- **Konektivita**: 2,4GHz WiFi IEEE 802.11b/g/n, Bluetooth.
- **Baterie**: Li-Ion 3,6 V, 2450 mAh.
- **Tiskárna**: termotisk 30 řádků za sekundu, šířka a průměr kotoučku 57x38 mm.
- **Napájení**: Stojánek s výstupem 5V DC, 1A (5W) [39].

Obrázek 46:Platební terminál Verifone VX675 [39].

7 NÁVRH VHODNÉHO KAMEROVÉHO SYSTÉMU

7.1 DVR Rekordér Hikvision DS-7216HQHI-K2/A

Při výběru kamerového systému byl kladen velký důraz na pořizovací cenu. Z doby před inovací kamerového systému zbyly původní CCTV (Closed Circuit Television) kamery a koaxiální/napájecí rozvody. Z toho důvodu bylo rozhodnuto zvolit moderní DVR (Digital Video Recorder) kamerový rekordér kompatibilní i se starými CVBS (Composite Video Baseband Signal) signály standardu NTSC (National Television Systém Committee) a PAL (Phase Alternating Line), ale zároveň i moderní přenos HD-TVI (HD Transport Video Interface) a IP. Díky tomuto řešení lze nějaký čas využít původní kamery a postupně přecházet na kvalitní kamery s využitím původních rozvodů.

Dále bylo nutno zajistit dostatečný počet kamerových vstupů pro možnost budoucího rozšíření po plánované nadstavbě budovy.

Z toho důvodu byl po prostudování mnoha možných variant a odborných recenzí produktů zvolen právě DVR Rekordér Hikvision DS-7216HQHI-K2/A kvůli následujícím parametrům:

Video vstupy:

- **Komprese videa:** H.265+/H.265
- **Počet vstupů pro CCTV kamery:** 16x BNC (Bayonet Neill Concelman connector)
- **Maximální rozlišení záznamu CCTV kamer:** 4x3MPx 15 FPS (Frames Per Second), 12x 1080p 15 FPS (720p 25FPS)
- **Podporované standardy CCTV kamer:** HD-TVI, CVBS (PAL: 704x 576, NTSC: 704x480)
- **Počet vstupů pro IP kamery:** 2x bez fyzických konektorů, je tedy potřeba kamery vyhledat v LAN síti skrze hlavní Ethernet port RJ45
- **Maximální rozlišení záznamu IP kamer:** 4MPx 25FPS

Video výstupy:

- **Video výstupy:** HDMI s maximálním rozlišením 4K (3840x2160), VGA (Video Graphics Array) s maximálním rozlišením 1080p (1920 x 1080)
- **Synchronní přehrávání:** 16 kanálů synchronně do jednoho video výstupu

- Podpora hlavního a vedlejšího video streamu (s nižším datovým tokem) v případě potřeby snížení datového toku při přenosu na vzdálené zařízení pomocí pomalé přenosové cesty, jako například telefon přes mobilní data operátora.

Datové úložiště:

- **Počet slotu pro HDD:** 2x SATA s kapacitou maximálně 6TB
- Ukládání do cloudového úložiště (Dropbox/Google Drive/Microsoft OneDrive)

Síťový management:

- **Maximální počet vzdálených přístupů:** 128
- **Podporované síťové protokoly:** TCP/IP, DHCP, DNS, DDNS, HTTPS, ONVIF
- Webové rozhraní sloužící k zobrazení kamer v reálném čase, přehrávání video záznamů a kompletní konfiguraci celého kamerového systému.

Externí rozhraní:

- 2x USB (1x USB 2.0; 1x USB 3.0)
- 1x RJ45 Gigabit Ethernet konektor (LAN/WEB server)

Vlastnosti zařízení:

- **Rozměry:** 315 x 242 x 45mm
- **Maximální spotřeba energie**: 25W bez HDD [40].

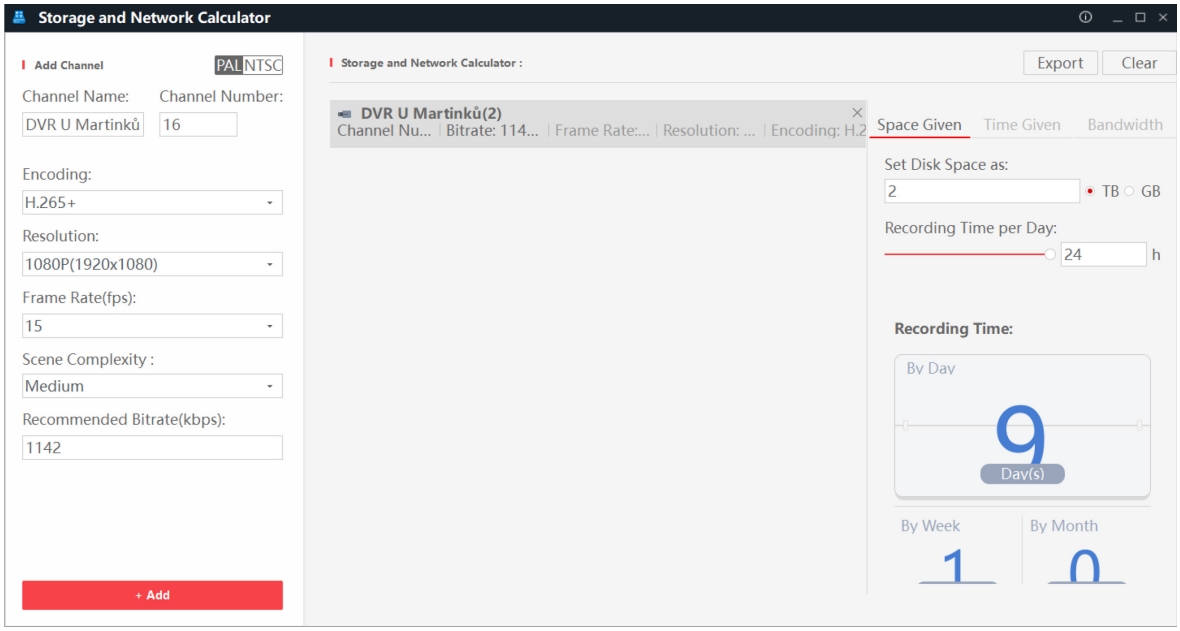
Obrázek 47: DVR Rekordér Hikvision DS-7216HQHI-K2/A (zadní strana) [40].

Obrázek 48: DVR Rekordér Hikvision DS-7216HQHI-K2/A (přední strana) [40].

7.1.1 Výběr vhodné kapacity a druhu pevného disku

Životně důležitou součástí DVR rekordéru je interní pevný disk. Ovšem ne všechny typy disků jsou pro použití v dohledovém systému vhodné, protože na rozdíl od počítače je aktivní prakticky neustále. Z toho důvodu je nutno zvolit disk uzpůsobený z výroby na neustálý provoz tzv. 24/7, neboli 24 hodin 7 dní v týdnu a optimalizovaný na ukládání videa ve vysokém rozlišení.

Vhodná kapacita byla vypočítána pomocí oficiální utility společnosti Hikvision s názvem Storage and Network Calculator [41]. Při výpočtu bylo počítáno již s 1080p kamerami Hikvision DS-2CE16D8T-IT/28 a také s moderním úsporným kodekem ukládání videa H.265+, dále bylo nastaveno snímkování 15FPS, standard PAL a obsazenost všech 16 kanálů rekordéru:



Obrázek 49: Výpočet vhodné velikosti HDD pro DVR rekordér.

Cílem bylo dosáhnout alespoň týdenního záznamu. Z toho důvodu bylo zjištěno, že optimální volbou bude kapacita **2TB** , která dostačuje pro 9 dní celodenního záznamu.

Po prostudování recenzí všech známých modelů na trhu byl nakonec vybrán 3,5" disk **Western Digital Purple WD20PURZ 2TB.** Tento model byl vybrán, jelikož disponuje nejlepšími parametry statisticky nízké poruchovosti a dobrému poměru ceny a výkonu.

Model disponuje následujícími parametry:

- Navržen výrobcem pro práci s bezpečnostními systémy DVR i NVR a je kompatibilní se systémy mnoha předních výrobců dohledových systémů včetně Hikvision.

- Konstruován pro nepřetržitý provoz 24/7 a optimalizaci ukládání videa.
- **Spolehlivost**: Podpora pracovního zatížení až 180 TB za rok a až 64 kamer s rozlišením HD, počet neobnovitelných chyb při bitovém čtení: <1 z 10^{14}
- **Rychlost čtení/zápisu**: max. 145 MBps.
- **Rozhraní:** SATA 6Gbps.
- **Vyrovnávací paměť**: 64 MB.
- **Otáčky**: 5400 otáček za minutu.
- **Maximální spotřeba**: 4,4W (čtení/zápis) [42].

Obrázek 50: HDD Western Digital Purple WD20PURZ 2TB.

7.2 CCTV Kamera AVTech KPC 139 ZEP (původní)

CCTV Kamera AVTech KPC 139 ZEP byla zachována z doby před inovací kamerového systému. Bylo tak rozhodnuto vedením restaurace z důvodu úspory finančních prostředků kvůli plánovanému rozšiřování a rekonstrukci objektu restaurace v blízké budoucnosti. Tyto kamery budou tedy v budoucnu v případě potřeby nahrazovány a při zvyšování počtu kamer budou již pořízeny moderní CCTV kamery Hikvision DS-2CE16D8T-IT/28.

Kamera AVTech KPC 139 ZEP má následující parametry:

- **Senzor**: CCD (Charged Coupled Device)
- **Standard přenosu videa**: CVBS (PAL, NTSC)
- **Rozlišení**: PAL: 752x 582, NTSC: 768x494
- **Citlivost**: 0,3 lux denní, 0lux noční (IR ON)
- **Přísvit**: 35 IR LED diod, dosah 25m
- **Objektiv**: 3,6mm, úhel záběru 92,6°

- **Odolnost**: IP67 (prachotěsnost, odolnost proti ponoření do vody na 30 minut do hloubky 1 metr)
- **Napájení**: 12V DC, 90mA, 340mA (při zapnutém přísvitu) [43]
- **Maximální spotřeba energie**: 4W

Obrázek 51: CCTV Kamera AVTech KPC 139 ZEP [43].

7.3 CCTV Kamera Hikvision DS-2CE16D8T-IT/28 (nová)

Nejdůležitějším kritériem při výběru vhodné CCTV kamery byla kvalita obrazu dostatečná k rozpoznání případného pachatele protiprávního jednání a možnosti jeho následného usvědčení pomocí záznamu této kamery, ale zároveň i k detekci především nově příchozích hostů na místech, kde obsluha nevidí a má tudíž možnost rychleji získat přehled a zákazníka bez zdržení obsloužit.

Z toho důvodu bylo vyžadováno rozlišení minimálně FullHD (1920x1080px) a proveden průzkum aktuálních technologií a potřebných optimálních parametrů CCTV kamer o kterých se podrobněji rozepisuji v teoretické části práce. Tyto technologie napomáhají ke kvalitě a použitelnosti záznamu především za zhoršených světelných podmínek. Po prostudování těchto záležitostí a recenzí několika modelů byla nakonec vybrána kamera Hikvision DS-2CE16D8T-IT/28, která se jevila jako ideální volba v poměru cena/výkon.

Kamera Hikvision DS-2CE16D8T-IT/28 disponuje následujícími parametry:

- **Senzor**: CMOS (Complementary Metal–Oxide–Semiconductor)
- **Standard přenosu videa**: HD-TVI (PAL, NTSC) s podporou vzdálené konfigurace OSD (On Screen Display) menu přes koax
- **Rozlišení**: 2Mpix (1920 x 1080), rychlost videa max. 25FPS
- **Citlivost**: 0,005 lux denní režim, 0lux noční režim (EXIR IR ON)
- **Přísvit**: EXIR, dosah 20m
- **Objektiv**: 2,8mm, úhel záběru 103,5°

- **Odolnost**: IP67 (prachutěsnost, odolnost proti ponoření do vody na 30 minut do hloubky 1 metr), provozní teplota -40°C až 60°C
- **Napájení**: 12V DC, 90mA, 340mA (při zapnutém přísvitu)
- **Maximální spotřeba energie**: 4W
- **Technologie zdokonalení obrazu (viz teoretická část)**: WDR 120dB, DNR, Smart IR, IR cut filtr
- **Nastavení úhlů:** Pan:0°-360°; Tilt:0°-90°; Rotate:0°-360°
- **Rozměry:** 58mm x 61mm x 163mm [44].

Obrázek 52: CCTV Kamera Hikvision DS-2CE16D8T-IT/28 (nová) [44].

7.4 CCTV Adaptér Zmodo PA-1059

Napájecí adaptér CCTV kamer byl vybrán pro napájení všech aktuálně zapojených 6 kamer včetně možnosti rozšíření o další 3. Poskytuje následující parametry:

- **Vstup:** 100V - 240V AC
- **Výstup:** 12V DC, maximální proud 5A
- **Konektory:** 9x Napájecí DC konektor jack (zdířka) pro kamery.
- **Obsahuje**: 1x napájecí adaptér, 1x rozdělovací kabel pro 9 kamer, 1x napájecí AC kabel [45].

Obrázek 53: CCTV Adaptér Zmodo PA-1059 [45].

7.5 Konektory

Obrázek 54: Napájecí DC konektor jack (kolík) do kamery, Napájecí DC konektor jack (zdířka) pro kamery [45].

Obrázek 55: Redukce F – BNC, konektor F 6,5mm [45].

8 CELKOVÉ ZAPOJENÍ (KALKULACE A NÁKLADY)

V části kalkulace byla provedena celková kalkulace nákladů na zhotovení a realizaci projektu. Zároveň byl zhotoven přehled technických prostředků potřebných pro sestavení projektu včetně schématu celkového zapojení.

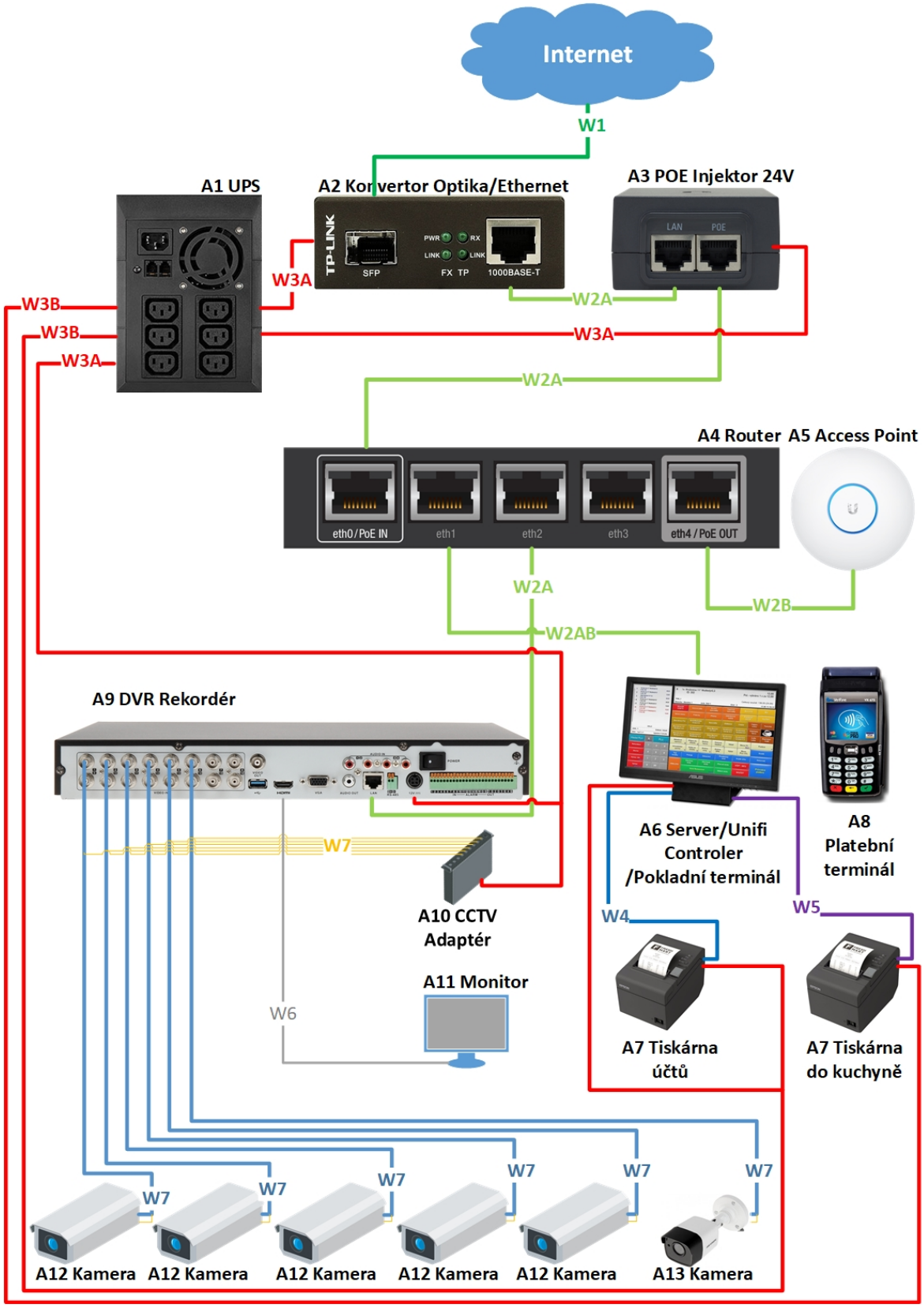
Položky	Počet hodin	Cena bez DPH (Kč)	DPH (%)	Cena s DPH (Kč)
Technické prostředky		43 592	21	52 746
Projektové práce	58	11 600	21	14 036
Tvorba konfigurací	215	43 000	15	49 450
Montážní práce	32	6 400	15	7 360
Školení uživatele	16	3 200	21	3 872
Náklady na dopravu		2 350	21	2 844
Celkem		**110 142**		130 306

Tabulka 3: Celkové náklady na zhotovení a realizaci projektu.

Níže uvedená tabulka a celkové schéma zapojení názorně zobrazuje všechny využité prvky projektu a jejich pořizovací cenu.

Zn.	Název	Dodavatel	Specifikace	KS	KČ (kus bez DPH)	KČ (bez DPH)
A1	UPS	Eaton	5E1500IUSB	1	2949,6	2949,6
A2	Konvertor Optika/Ethernet	Tp-link	MC220L + SFP modul	1	STÁVAJÍCÍ	
A3	POE Injektor 24V	Ubiquiti	POE-24-12W-G	1	PŘÍSLUŠENSTVÍ K A5	
A4	Router	Ubiquiti	EdgeRouter X	1	1090,1	1090,1
A5	Access Point	Ubiquiti	UniFi AP AC Long Range	1	1898,3	1898,3
A6	Server/Pokladní terminál	LYNX	Conto MAX 15"	1	16520,7	16520,7
	Server/Pokladní terminál	Consulta	Conto modul platební terminál	1	2950,0	2950,0
A7	Tiskárna	Epson	POS TM-T20II Ethernet + USB	2	3476,0	6952,1
A8	Platební terminál	Verifone	VX675	1	ZAPŮJČENO OD BANKY	
A9	DVR rekordér	Hikvision	DS-7216HQHI-K2/A	1	6325,6	6325,6
	HDD pro záznam	Western Digital	PURPLE WD20PURZ 2TB SATA/600 64MB cache	1	1500,0	1500,0
A10	CCTV Adaptér	Zmodo	PA-1059 9 Port 12V 5A	1	285,1	285,1
A11	Monitor	Asus	VB199TL	1	STÁVAJÍCÍ	
A12	CCTV Kamera	Avtech	KPC 139 ZEP	5	STÁVAJÍCÍ	
A13	CCTV Kamera	Hikvision	DS-2CE16D8T-IT/28	1	757,0	757,0
W1	Vedení Internet optické	Fiber Arsenal	LC-LC vlákno 9/125, single mode, simplex, 20 m	1	STÁVAJÍCÍ	
W2A	Vedení LAN	Datacom	Cat6, UTP, 1m s konektory	3	24,0	71,9
W2B	Vedení LAN	Solarix	SXKD-6-UTP-PVC	30	9,5	285,1
	Vedení LAN	PremiumCord	konektor RJ45, UTP Cat6, na drát/lanko	4	4,1	16,5
W3A	Vedení 230V AC	Jonex	Kabel CEE 7/5 (E) zásuvka IEC C14 vidlice 0,3m	3	72,7	218,2
W3B	Vedení 230V AC	Jonex	Kabel CEE 7/5 (E) zásuvka IEC C14 vidlice 0,3m	2	72,7	145,5
	Vedení 230V AC		Vícenásobná zásuvka IP44 3 x 230V/16A	2	198,3	396,7
	Vedení 230V AC	Legrand	Vidlice 50252 230V černá gumová IP44	2	51,2	102,5
	Vedení 230V AC		CYKY 3 x 1,5 J	30	9,9	297,5
W4	Vedení tiskárna	PremiumCord	USB 2.0, A-B - 2m	1	28,9	28,9
W5	Vedení tiskárna	PremiumCord	USB 2.0 aktivní repeater 20m prodlužovací	1	495,0	495,0
	Vedení tiskárna	PremiumCord	USB 2.0, A-B - 2m	1	28,9	28,9
W6	Vedení monitor	PremiumCord	HDMI 1.4 propojovací 3m	1	99,2	99,2
	Vedení monitor	Akasa	DVI Male - HDMI Female redukce	1	86,8	86,8
W7	Vedení CCTV kamery	Konig	CCTV Kabel BNC / DC (různé délky v m)	75	STÁVAJÍCÍ	
	Vedení CCTV kamery		Napájecí DC konektor jack (kolík) do kamery	1	14,0	14,0
	Vedení CCTV kamery		Napájecí DC konektor jack (zdířka) pro kamery	1	14,0	14,0
	Vedení CCTV kamery		Redukce F – BNC	2	26,4	52,9
	Vedení CCTV kamery		konektor F 6,5mm průměr	2	5,0	9,9
Celkem KČ (bez DPH)						43592,1
Celkem KČ (s DPH)						52746,5

Tabulka 4: Náklady pro zajištění technických prostředků

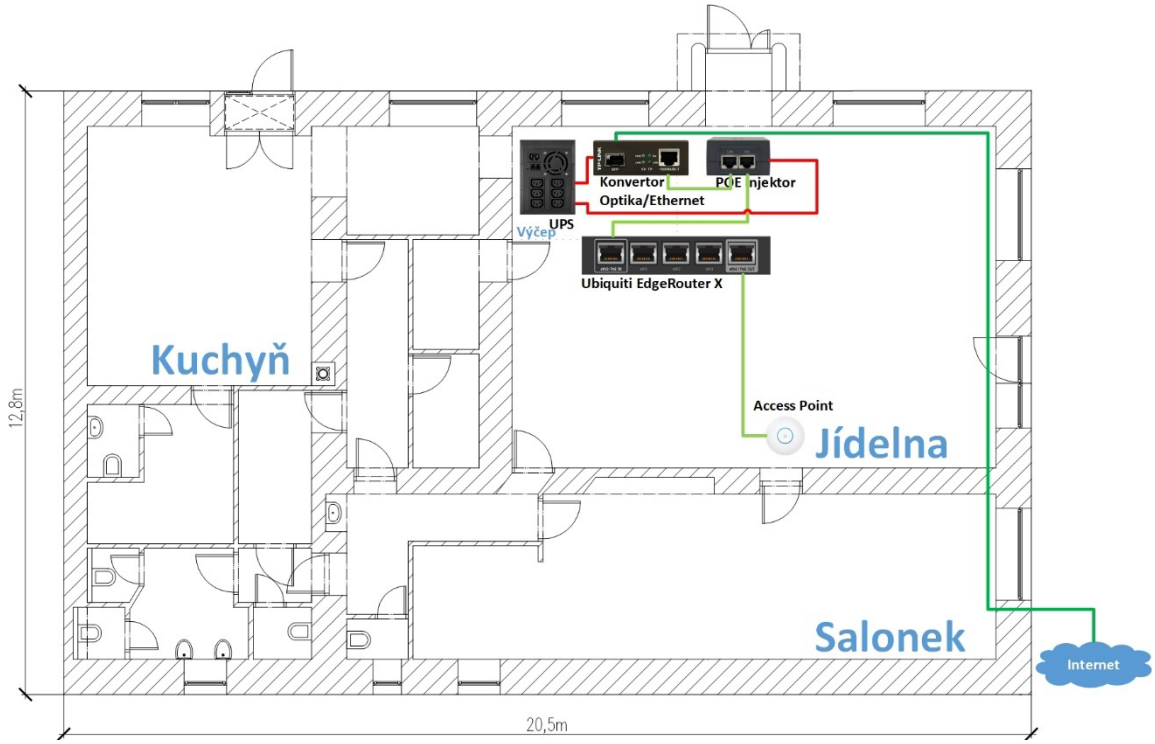


Obrázek 56: Schéma celkového zapojení.

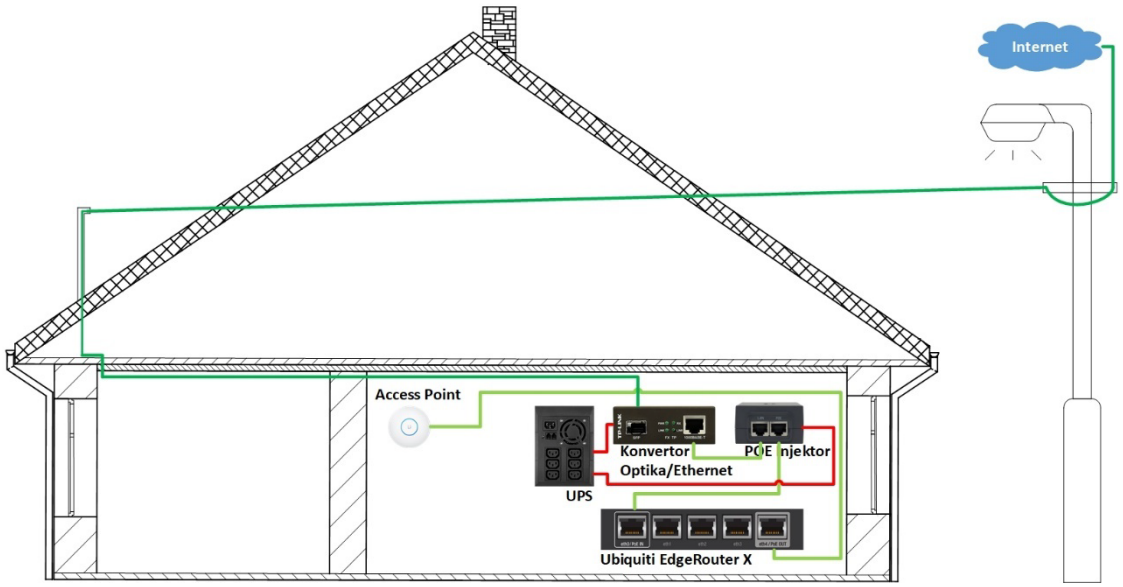
9 ZAPOJENÍ SÍŤOVÝCH PRVKŮ

V části zapojení sítě byla popsána veškerá manuální práce při budování síťové infrastruktury od kabeláže až po instalaci a zapojování prvků sítě. Nejprve bylo však nutno navrhnout samotnou síťovou infrastrukturu.

9.1 Návrh síťové infrastruktury



Obrázek 57: *Návrh síťové infrastruktury (pohled z vrchu).*



Obrázek 58: *Návrh síťové infrastruktury (bokorys, řez jídelna).*

Název	Dodavatel	Specifikace
UPS	Eaton	5E1500IUSB
Konvertor Optika/Ethernet	Tp-link	MC220L + SFP modul
POE Injektor 24V	Ubiquiti	POE-24-12W-G
Router	Ubiquiti	EdgeRouter X
Access Point	Ubiquiti	UniFi AP AC Long Range
Vedení 230V AC	Jonex	Kabel CEE 7/5 (E) zásuvka IEC C14 vidlice 0,3m
Vedení Internet optické	Fiber Arsenal	LC-LC vlákno 9/125, single mode, simplex, 20 m
Vedení LAN	Datacom	Cat6, UTP, 1m s konektory
Vedení LAN	Solarix	Kabel SXKD-6-UTP-PVC, 15m
Vedení LAN	Premium-Cord	konektor RJ45, UTP Cat6, na drát/lanko

Tabulka 5: Prvky síťové infrastruktury.

První pohled shora zobrazuje přibližné rozmístění a propojení jednotlivých síťových prvků včetně typu propojení.

Druhý pohled zobrazuje řez jídelnou a ujasní vertikální rozmístění prvků a jejich propojení.

Poznámka: udávaný optický kabel o délce 20m je pouze propojení mezi konvertorem optika/Ethernet a přípojkou od poskytovatele internetového připojení. Nejedná se o celkovou délku optického kabelu. Ve schématu je pro názorné účely optické vedení bráno jako celek.

9.2 Instalace síťových rozvodů

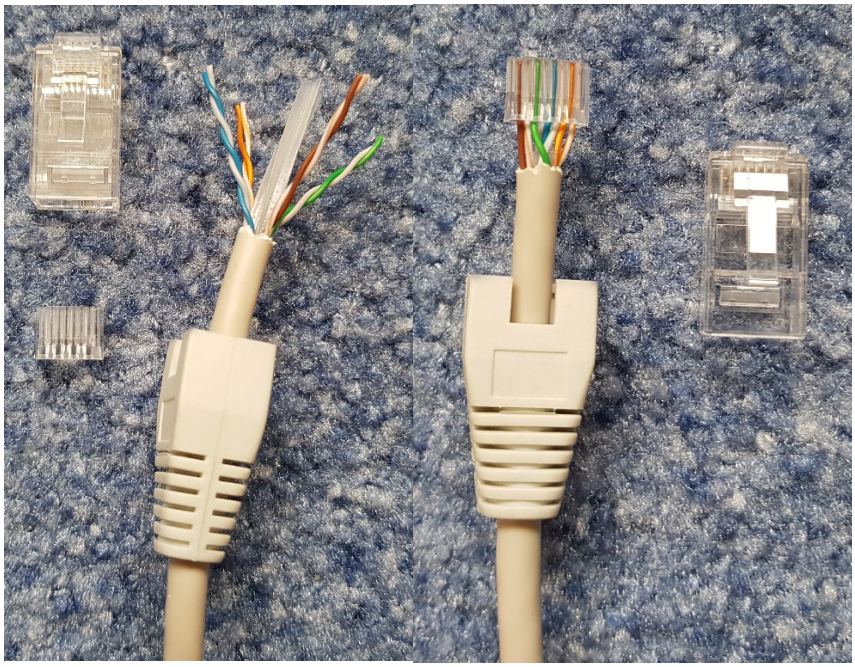
Síťové rozvody byly zhotoveny pro propojení access pointu a serveru (pokladního terminálu) k routeru. Ostatní prvky sítě byly umístěny v blízkosti routeru a tudíž propojeny běžným UTP Cat6 kabelem včetně konektorů RJ45 o velikosti 1m.

Při instalaci rozvodů byl použit kvalitní kabel Solarix SXKD-6-UTP-PVCU. Nejprve byl natažen od routeru směrem k access pointu a serveru v předem zhotovených ochranných lištách. Dále byly na obou koncích zhotoveny konektory.

Při osazování konektoru RJ45 na konci síťového kabelu je nutno opatrně odřezat cca 3 cm bužírky. Jsou viditelné 4 páry kroucené dvojlinky oddělené plastovým křížem. Tyto páry jeden po druhém rozpleteme a narovnáme. Plastový kříž v odhalené části u konce ustřihneme. Vodiče v takto připraveném kabelu seřadíme podle standardního nekříženého rozložení vodičů 1 až 8 v pořadí dle standardu TIA 568B:

1 bílo oranžová, 2 oranžová, 3bílozelená, 4 modrá, 5 bílo modrá, 6 zelená, 7 bílo hnědá, 8 hnědá

Co nejdůkladněji narovnané a seřazené vodiče následně nasuneme do vložky konektoru tak, abychom měli zobáček vložky nahoře. Vložku následně posuneme tak, aby při zkušebním přiložení konektoru vedle kabelu zasahovala bužírka do cca 1/3 vnitřku zadní části konektoru a vložka byla doražená až do konce přední části. Po dodržení těchto zásad můžeme přebytečnou délku vodičů na začátku kabelu až po začátek vložky ustřihnout.



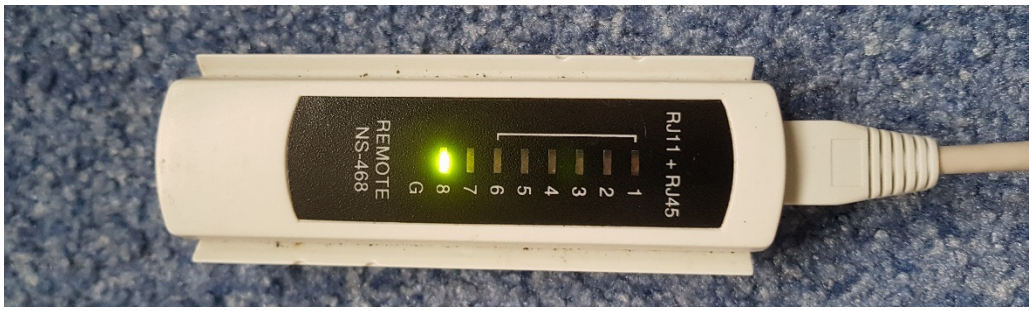
Obrázek 59: Osazení konektoru RJ45 (část 1)

Nyní nám nic nebrání uchopit konektor a zasunout jej tak, aby zobáček vložky doléhal ke spodní části konektoru. Konektor proto důkladně dotlačíme. Bužírka by měla být dostatečně zanořena vně konektoru zhruba do 1/3.

Takto připravený konektor vložíme při současném dotláčení do krimpovacích kleští. Pro jistotu doporučuji kleště 3x zmáčknout. Tímto dojde k proniknutí nožů na pinech konektoru do jednotlivých vodičů a zároveň se na konci přichytí bužírka.

Obrázek 60: Osazení konektoru RJ45 (část 2)

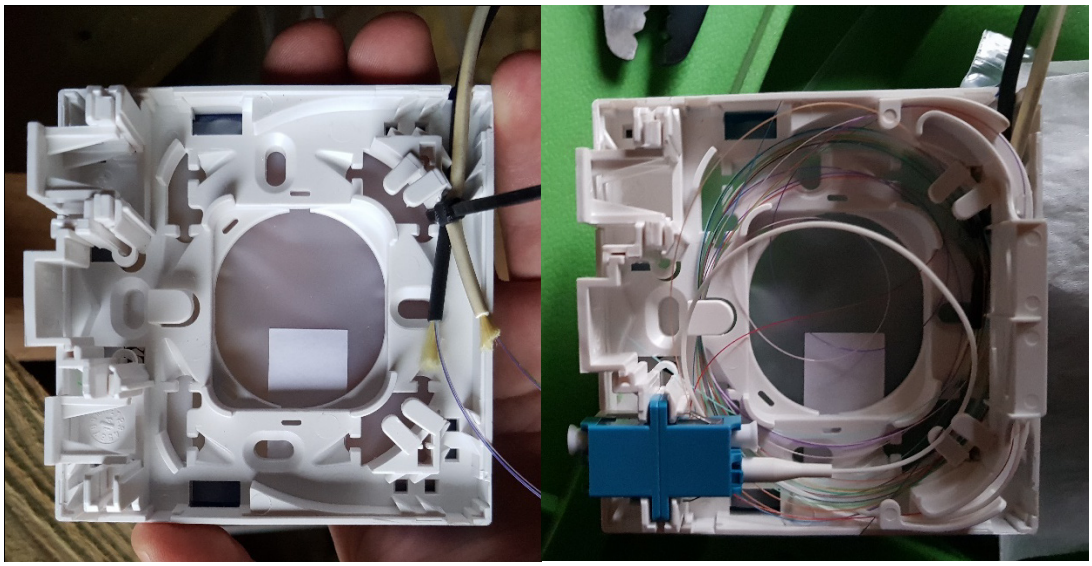
Po zhotovení konektorů v obou rozvodech byla otestována jejich funkčnost. Pro tyto účely byl využit tester síťové kabeláže Logilink, kterým byla proměřena správná průchodnost elektrických signálů postupně všemi 8 vodiči kabelu.



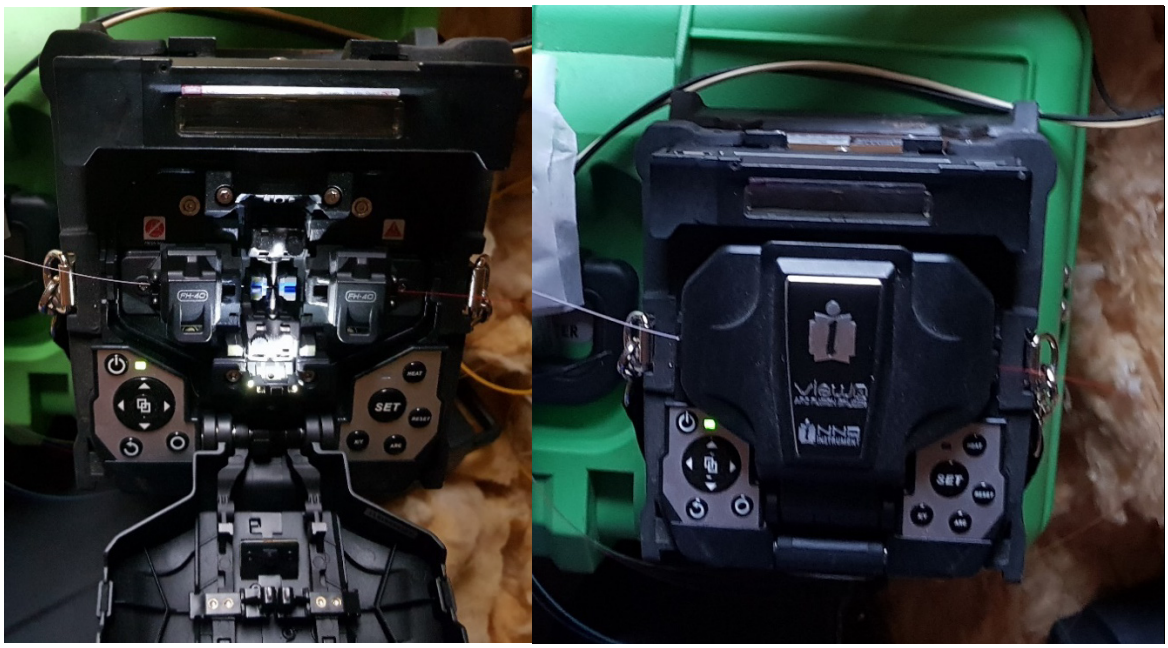
Obrázek 61: Testování síťového kabelu.

9.3 Zavedení optické přípojky z MAN do LAN

Pro zavedení optické přípojky k internetu do budovy z MAN sítě (Metropolitan Area Network) poskytovatele internetu je zapotřebí odklonit minimálně jedno vlákno z obvykle více vláknového venkovního vedení. Fotodokumentace níže znázorňuje zapojení optické přípojky restaurace poskytovatelem internetového připojení, firmou Anex s.r.o.



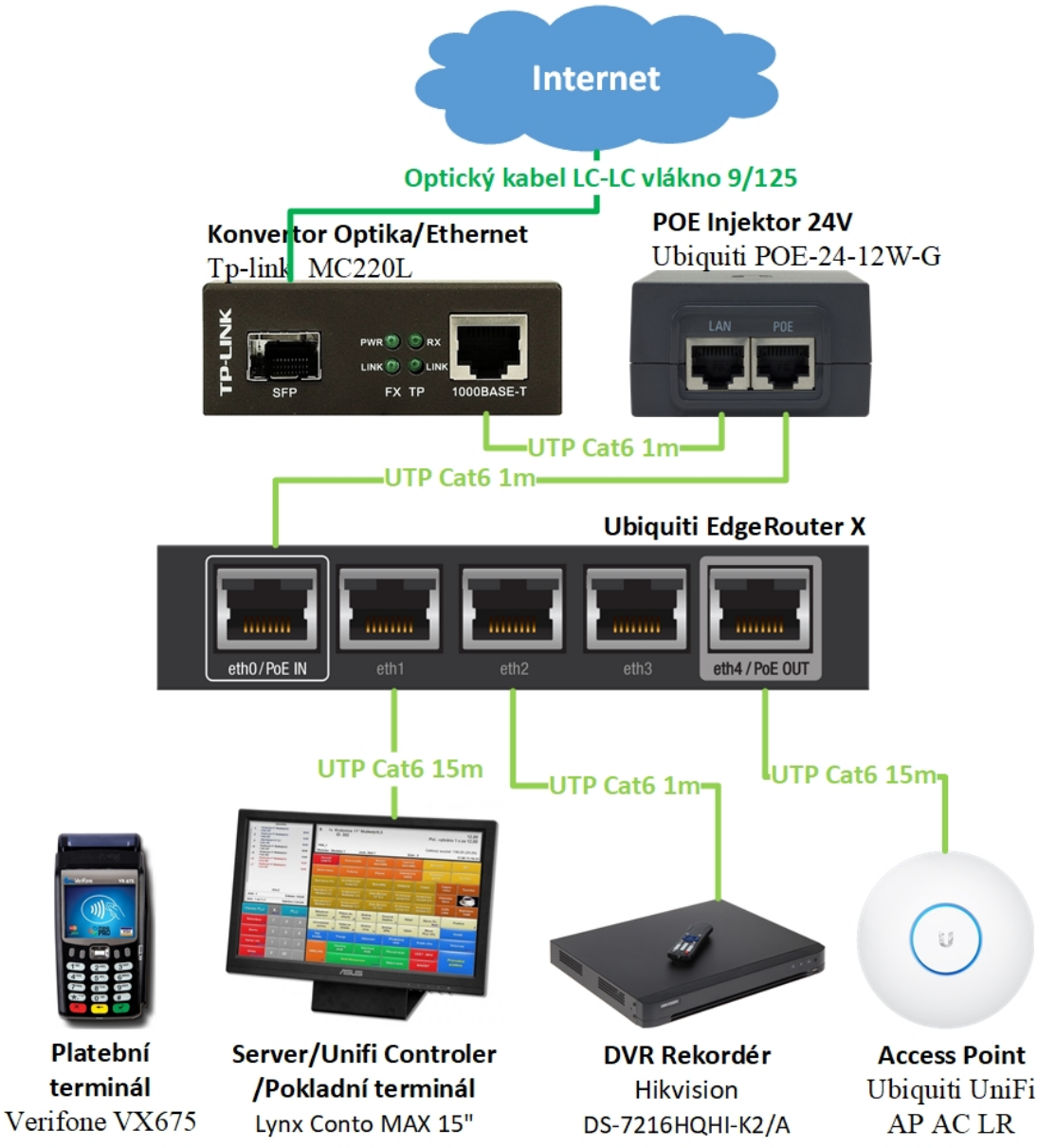
Obrázek 62: Zapojení optické přípojky.



Obrázek 63: Svařování optického single mode vlákna.

9.4 Instalace a zapojování síťových prvků

V případě DVR Rekordéru a tudíž i prvků umístěných v jeho blízkosti (konvertor Optika/Ethernet, router a UPS záložní zdroj) bohužel nemohla být provedena fotodokumentace ani přesný popis umístění z důvodu nutného utajení přesné polohy citlivých dat uložených na HDD DVR Rekordéru jako jsou kamerové záznamy na veřejnost nepovolaným osobám. Z toho důvodu zde bude pro ilustraci poskytnuta fotodokumentace těchto prvků z doby testování a konfigurace prováděná v jiném prostředí. Jménem majitele gastronomického zařízení se za tuto nepřesnost omlouvám.



Obrázek 64: Kompletní schéma síťového zapojení (nezobrazeno UPS napájení)

Gastronomické zařízení je připojeno k síti internet optickým vedením lokálního poskytovatele Internetového připojení o propustnosti 1Gbps.

Toto optické vedení je nejprve převedeno na metalické pomocí konvertoru Optika/Ethernet Tp-link MC220L.

Pomocí UTP kabelu Cat6 je přivedena internetová konektivita do routeru Ubiquiti Edgerouter X skrze pasivní POE injektor Ubiquiti POE-24-12W-G, který přidává do UTP Cat6 vedení 24V 0,5A a napájí router na portu eth0/POE IN s dostatečným výkonem 12W. Bezdrátovou konektivitu v LAN poskytuje Access Point Ubiquiti UniFi AP AC Long Range.

Obrázek 65: Názorné testovací zapojení POE injektoru, routeru a access pointu bez konvertoru Optika/Ethernet, klientských zařízení a napájení pomocí UPS

Pomocí Access pointu je do zabezpečené sítě WLAN bezdrátově připojen platební terminál Verifone VX675 (více informací v konfigurační části).

Access point byl strategicky umístěn do optimální pozice přibližně ve středu objektu (viz. Návrh síťové infrastruktury). Tato pozice se po provedení měření ukázala jako nejoptimálnější umístění pro rovnoměrnou distribuci bezdrátového signálu ve vnitřních prostorách i zahrádce v oblasti, kde se vyskytují hosté.

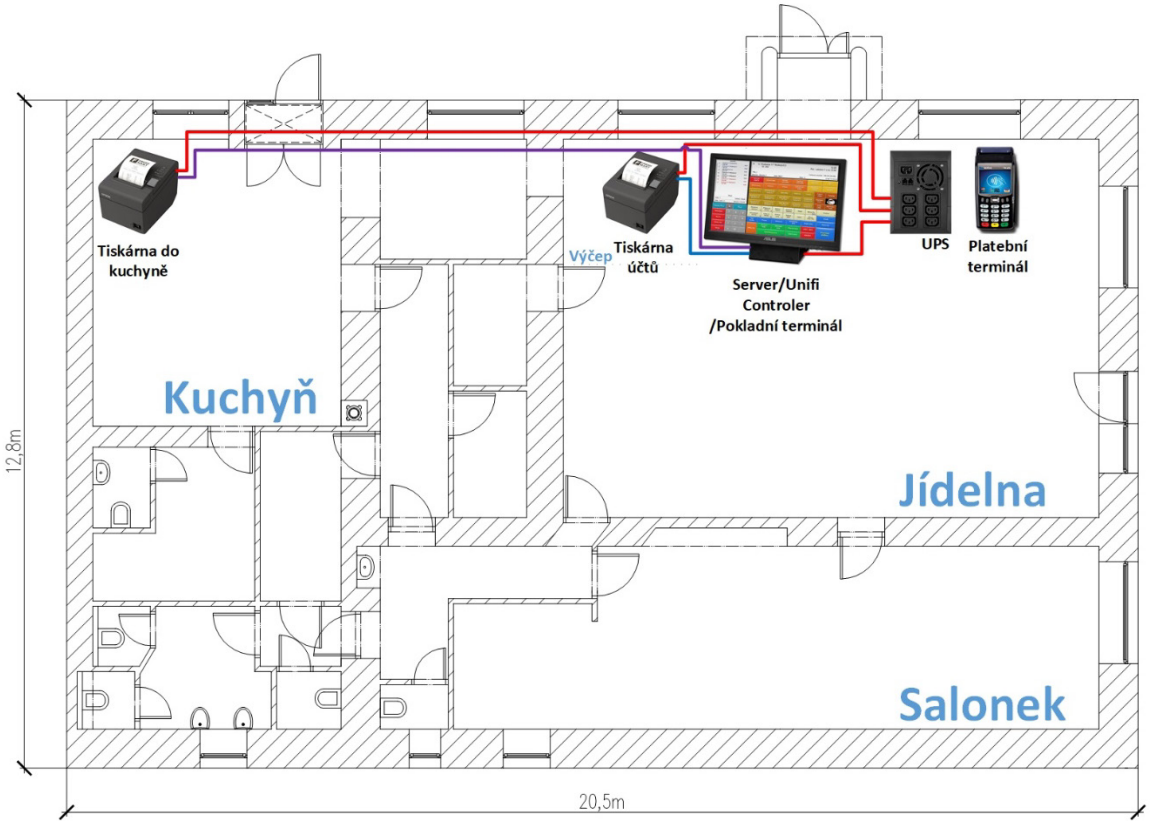
Obrázek 66: Zapojení Access Pointu Ubiquiti UniFi AP AC LR

Obrázek 67: Zapojení Access Pointu Ubiquiti UniFi AP AC LR (detail).

10 ZAPOJENÍ POKLADNÍHO SYSTÉMU

V části zapojení pokladního systému bylo popsáno zapojení serveru, tiskáren, platebního terminálu včetně potřebného vedení.

10.1 Návrh infrastruktury pokladního systému



Obrázek 68: Návrh infrastruktury pokladního systému (pohled z vrchu).

Název	Dodavatel	Specifikace
UPS	Eaton	5E1500IUSB
Server/Pokladní terminál	LYNX	Conto MAX 15"
Tiskárna účtů	Epson	POS TM-T20II
Tiskárna do kuchyně	Epson	POS TM-T20II
Platební terminál	Verifone	VX675
Vedení 230V AC	Jonex	Kabel CEE 7/5 (E) zásuvka IEC C14 vidlice 0,3m
Vedení 230V AC		Vícenásobná zásuvka IP44 3 x 230V/16A
Vedení 230V AC	Legrand	Vidlice 50252 230V černá gumová IP44
Vedení 230V AC		CYKY 3 x 1,5 J
Vedení tiskárna	PremiumCord	USB 2.0, A-B - 2m
Vedení tiskárna	PremiumCord	USB 2.0 aktivní repeater 20m prodlužovací
Vedení tiskárna	PremiumCord	USB 2.0, A-B - 2m

Tabulka 6: Prvky infrastruktury pokladního systému.

10.2 Instalace a zapojování prvků pokladního systému

Při montážních pracích na pokladním systému byly nejprve nachystány veškeré kabelové rozvody. Síťový UTP rozvod Cat6 s konektorem RJ45 byl zhotoven již dříve společně s instalací síťových prvků. Bylo tedy nutno zavést elektrické připojení od UPS záložního zdroje k rohové části barového pultu, kde bylo plánováno umístit server společně s tiskárnou účtů a nabíjecí stanicí pro platební terminál. V tomto místě byla na konci vedení umístěna vícenásobná zásuvka s krytím IP44 3 x 230V/16A. Se samotným platebním terminálem se lze volně pohybovat neomezeně po celém objektu a přilehlých prostorech. Je limitován pouze dosahem WLAN sítě. Další elektrický rozvod byl zhotoven mezi tiskárnou do kuchyně a rovněž UPS záložním zdrojem.

Po dokončení elektrických rozvodů následoval rozvod komunikace vzdálené tiskárny do kuchyně se serverem. Bylo uvažováno o 2 možných druzích spojení. Prvním z nich je propojení se serverem pomocí LAN sítě. Ovšem po minulých negativních zkušenostech s tímto druhem propojení u O2 Ekasy, kdy byla komunikace často nestabilní, a to i při nastavení priority spojení na routeru pomocí QoS (Quality of Service), bylo od záměru upuštěno. Tiskárna byla nově připojena napřímo se serverem pomocí USB vedení. Na vzdálenost 15m bylo nutno zapojit speciální kabeláž s USB 2.0 aktivním repeaterem (opakovačem) zesíleného signálu (jelikož běžný USB kabel po 5 metrech délky již nemusí správně fungovat).

UPS záložní zdroj Eaton 5E1500IUSB slouží k napájení všech důležitých zařízení, které je zapotřebí udržet v aktivním stavu i po náhodném výpadku elektrické sítě do doby než odpovědný personál obnoví tok elektřiny v objektu (nahodí jistič) nebo se přepojí na záložní generátor (v případě dlouhodobého problému). Tento zdroj zároveň slouží i jako přepěťová ochrana a dokáže na výstupu poskytovat stabilní napájení připojených zařízení i během kolísání napětí

K záložnímu zdroji UPS je připojen konvertor Optika/Ethernet a POE injektor pomocí vedení 230V AC CEE 7/5 zásuvka IEC C14 vidlice, tento krátký kabel 0,3m poskytuje možnost připojení napájecích adaptérů napájených zařízení. Tím je zajištěna funkce celé LAN sítě včetně připojení do internetu.

Dále je připojen server (A6) a obě tiskárny. Tato zařízení jsou od UPS vzdáleny cca 15m a proto bylo nutno zajistit navíc rozvod CEE 7/4 na CEE 7/5 (E) prostřednictvím kabelu CYKY 3 x 1,5 J zapojený podle normy TN-S. Platebním terminálem není potřeba zdroj UPS zatěžovat, jelikož má integrovanou baterii s dostatečnou výdrží.

Po zhotovení veškerých rozvodů byly rozmístěny a zapojeny jednotlivé periferní zařízení:

První zařízení – tiskárna do kuchyně Epson TM-T20II připojena k serveru pomocí konektoru USB 2.0 je využita k tisku bonů neboli výpisu produktů, které si zákazník objednal a je zapotřebí zhotovit je v kuchyni.

Obrázek 69: Zapojení tiskárny do kuchyně Epson TM-T20II.

Druhé zařízení – platební terminál Verifone VX675 připojen k serveru a zároveň k internetu pomocí zabezpečeného okruhu LAN sítě (více v části konfigurace síťových prvků). Je využit k bezhotovostním kontaktním i bezkontaktním platebním transakcím mezi bankovním účtem zákazníka a majitele.

Obrázek 70: Zapojení platebního terminálu Verifone VX675

Třetí zařízení – tiskárna účtů Epson TM-T20II připojena k serveru pomocí konektoru USB 2.0 je využita k tisku účtenek pro zákazníky, denních případně měsíčních výpisů tržby a dalších výkazů, které generuje software pokladního terminálu.

Obrázek 71: Zapojení tiskárny účtů Epson Epson TM-T20II, příprava kabeláže k propojení se serverem.

Čtvrté a poslední zařízení - server (pokladní terminál) LYNX Conto MAX 15" byl sestaven ze 3 částí, a to dotykového monitoru Asus VT168 připojeného k pasivně chlazené PC skříni HDMI a USB kabelem (pro ovládání dotykové vrstvy monitoru), tyto 2 části jsou následně osazeny do upínací kovové konstrukce.

Server plní z důvodu úspory nákladů několik funkcí. Je využit jako pokladní terminál, server pokladního systému, controler access pointu Ubiquiti Unifi, autentizační server WiFi pro zákazníky atd.

Obrázek 72: Sestavení serveru LYNX Conto MAX 15".

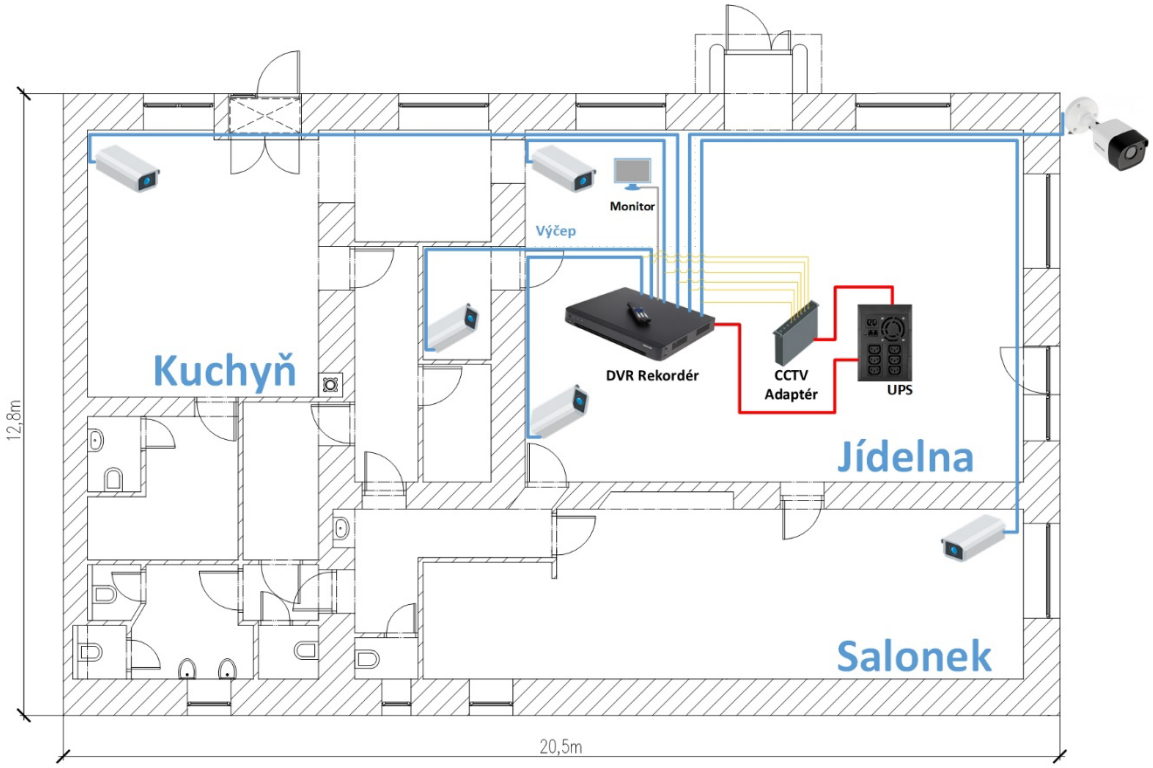
Obrázek 73: Zapojení serveru LYNX Conto MAX 15".

Obrázek 74: Výsledná konfigurace pokladního terminálu (SW i HW).

11 ZAPOJENÍ KAMEROVÉHO SYSTÉMU

V části zapojení kamerového systému bylo popsáno zapojení DVR rekordéru, CCTV kamer a dohledového monitoru včetně potřebného vedení.

11.1 Návrh infrastruktury kamerového systému



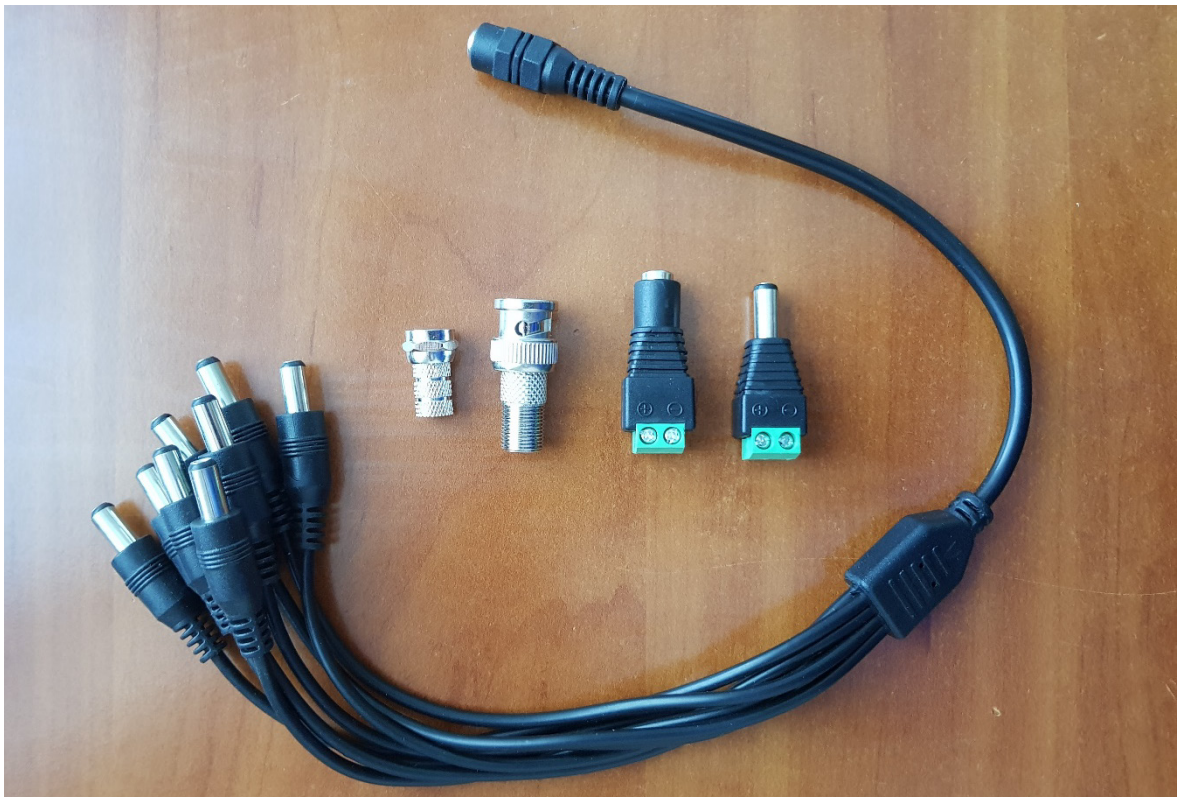
Obrázek 75: Návrh infrastruktury pokladního systému (pohled shora).

Název	Dodavatel	Specifikace
UPS	Eaton	5E1500IUSB
DVR rekordér	Hikvision	DS-7216HQHI-K2/A
HDD pro záznam	Western Digital	PURPLE WD20PURZ 2TB SATA/600 64MB cache
CCTV Adaptér	Zmodo	PA-1059 9 Port 12V 5A
Monitor	Asus	VB199TL
CCTV Kamera	Avtech	KPC 139 ZEP (5 kusů)
CCTV Kamera	Hikvision	DS-2CE16D8T-IT/28 (1 kus)
Vedení 230V AC	Jonex	Kabel CEE 7/5 (E) zásuvka IEC C14 vidlice 0,3m
Vedení CCTV kamery	Konig	CCTV Kabel BNC / DC (různé délky v m)
Vedení CCTV kamery		Napájecí DC konektor jack (kolík) do kamery
Vedení CCTV kamery		Napájecí DC konektor jack (zdířka) pro kamery
Vedení CCTV kamery		Redukce F – BNC
Vedení CCTV kamery		konektor F 6,5mm průměr

Tabulka 7: Prvky infrastruktury kamerového systému.

11.2 Instalace kamerových rozvodů

Jak již bylo dříve vysvětleno v části výběru vhodných prvků kamerového systému, 5 CCTV kamer včetně koaxiálního vedení s napájením BNC/DC bylo z důvodu finančních úspor ponecháno a budou postupně nahrazeny až po plánované rekonstrukci a rozšíření druhého patra objektu. Aktuálně byla nahrazena venkovní kamera na zahrádce velmi pokročilou FullHD kamerou Hikvision DS-2CE16D8T-IT/28 a také byl nahrazen vadný rozvod kamery ve výčepu.



Obrázek 76: Konektory kamerových rozvodů včetně rozvaděče CCTV adaptéru.

Instalace BNC konektoru

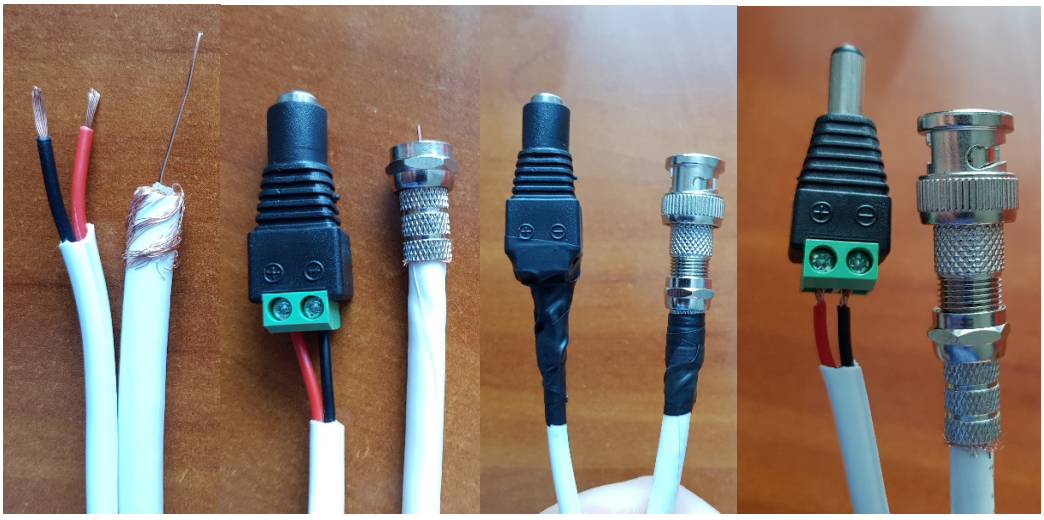
Při instalaci kamerových rozvodů je nutno nejprve podélně rozdělit multi kabel na část koaxiálu a část DC napájení cca 10 cm. Na koaxiální části se musí odstranit cca 1,5 cm bužírky. Pozor, aby se neporušilo opletení a případně u některých kabelů stínící fólie. Dále je nutno zahnout opletení, případně i fólii přes okraj bužírky, a odříznout izolaci středního vodiče (viz. první pohled). V dalším kroku se našroubuje (směrem doprava) F konektor do té míry, než se horní část kabelu dotkne kovového dorazu konektoru (viz. druhý pohled). Střední vodič zastřihneme mírně nad okrajem konektoru. Nakonec na F konektor našroubujeme BNC konektor. Nakonec spoj zaizolujeme izolační páskou kvůli ochraně před oxidací.

Instalace napájecího DC jack konektoru (zdířka směrem do napájecího zdroje)

Na DC části kabelu s 2 vodiči nejprve odizolujeme cca 1,5 cm vrchní bužírky a posléze cca 5mm bužírek jednotlivých kabelů. (viz. první pohled). Dále vložíme červený kabel do zelené zdířky s nápisem + a **černý do zdířky s nápisem –** (viz druhý pohled). Nakonec spoj zaizolujeme izolační páskou kvůli ochraně před zkratem a oxidací.

Instalace napájecího DC jack konektoru (kolík směrem do kamery)

Postupujeme stejně jako v případě DC jack konektoru zdířky.



Obrázek 77: Osazování konektorů BNC/DC.

Obrázek 78: Osazování konektorů BNC/DC dokončení.

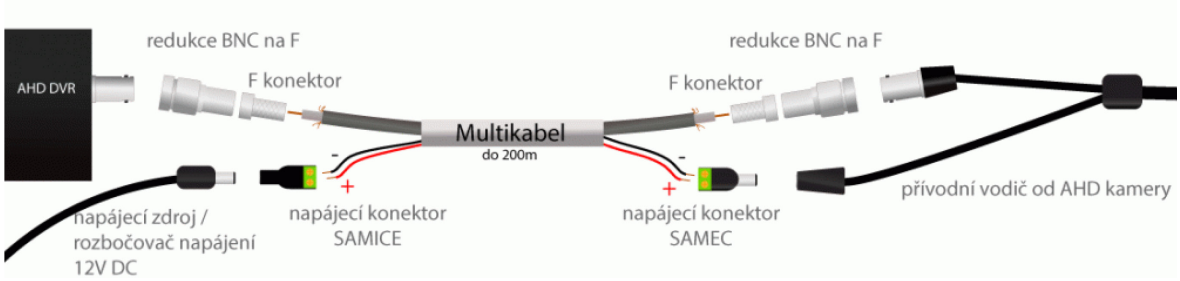
11.3 Instalace a zapojování prvků kamerového systému

11.3.1 Instalace CCTV kamery DS-2CE16D8T-IT/28

Před samotnou instalací kamery je nejprve důležité důkladně si promyslet vhodnou pozici, ze které bude kamera sledovat oblast určenou k monitorování a jestli potřebný úhel záběru koresponduje se zorným úhlem čočky kamery, aby nedocházelo ke slepým místům.

Zvolen byl dřevěný trám střešní konstrukce v rohu venkovního altánu pro hosty (zahrádky), který se jevil jako ideální místo, jelikož z něj lze pokrýt celou oblast a zorný úhel čočky kamery 103,5° je více než dostatečný. Zároveň byla kamera nasměrována směrem k parkovišti restaurace aby nesnímala žádný cizí majetek nebo prostor, kvůli kterému by bylo nutno žádat o povolení majitele majetku nebo se registrovat na webových stránkách Úřadu na ochranu osobních údajů.

Při samotné instalaci je nejprve potřeba přiložit šablonu (pokud je k dispozici), případně samotnou kameru na zvolené místo a obkreslit na trám otvory pro vruty. U dřevěných materiálů, jako v tomto případě, lze přímo přišroubovat vruty bez předvrtání. Záleží na fyzické zručnosti jedince. Po našroubování kamery zapojíme BNC a DC jack kolík konektor přivedeného vedení multi kabelu na BNC zdířku a DC jack zdířku přívodního vedení CCTV kamery (viz. schéma).



Obrázek 79: Názorné zobrazení zapojení kamerových rozvodů [46].

Obrázek 80: Zapojení kamery Hikvision DS-2CE16D8T-IT/28 (zahrádka v1).

Obrázek 81: Zapojení kamery Hikvision DS-2CE16D8T-IT/28 (zahrádka v2).

Obrázek 82: Kamera AVTech KPC 139 ZEP (Jídelna).

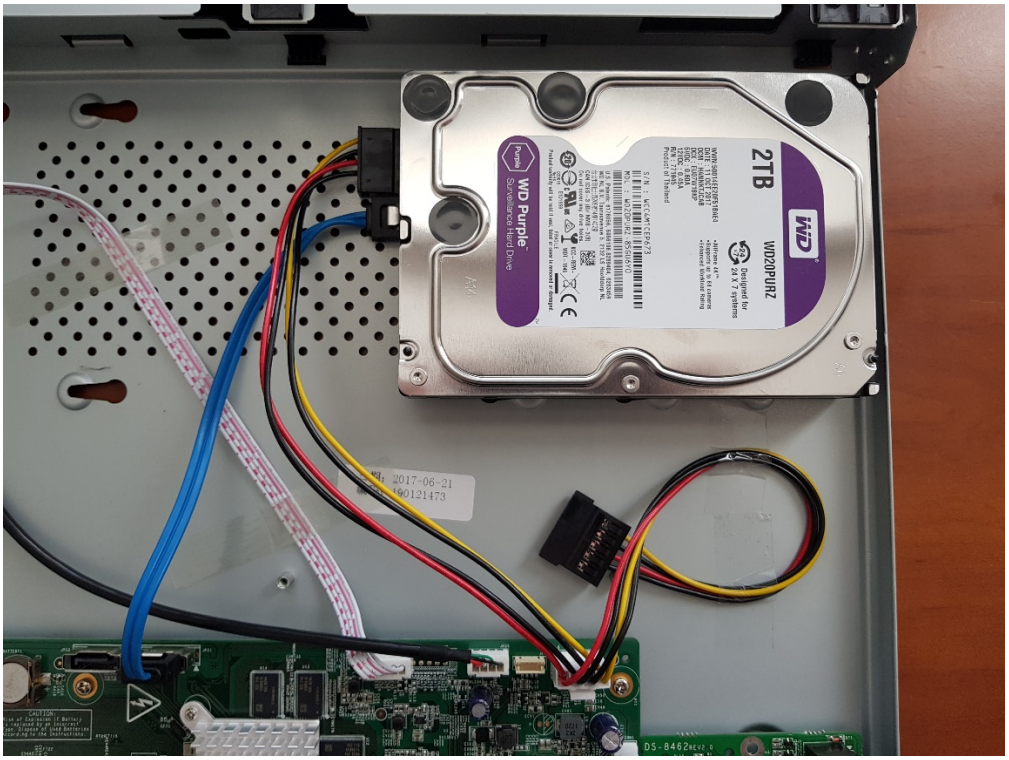
11.3.2 Instalace DVR rekordéru Hikvision DS-7216HQHI-K2/A

Dříve, než bylo možno přejít k propojení DVR Rekordéru Hikvision DS-7216HQHI-K2/A (viz schéma zapojení), konfiguraci a nahrávání záznamů z kamer, musel být instalován zakoupený HDD Western Digital PURPLE WD20PURZ 2TB. Nejprve byl sejmut přední kryt.

Obrázek 83: Příprava instalace HDD do DVR rekordéru.

Ze spodní strany disku byly do půlky závitu našroubovány 4 vruty a následně byl osazen do prvního ze dvou slotů určených pro osazení disku. Hlavičky z poloviny utažených vrutů na spodní straně disku byly zasunuty do fixních otvorů slotu a po posunutí disku do strany a následným dotažením vrutů byl disk upevněn.

Po upevnění disku byl propojen se základní deskou DVR rekordéru pomocí SATA (Serial ATA) datového kabelu. Posléze bylo zapojeno i napájení. Vývod napájení druhého disku byl zajištěn proti pohybu páskou.



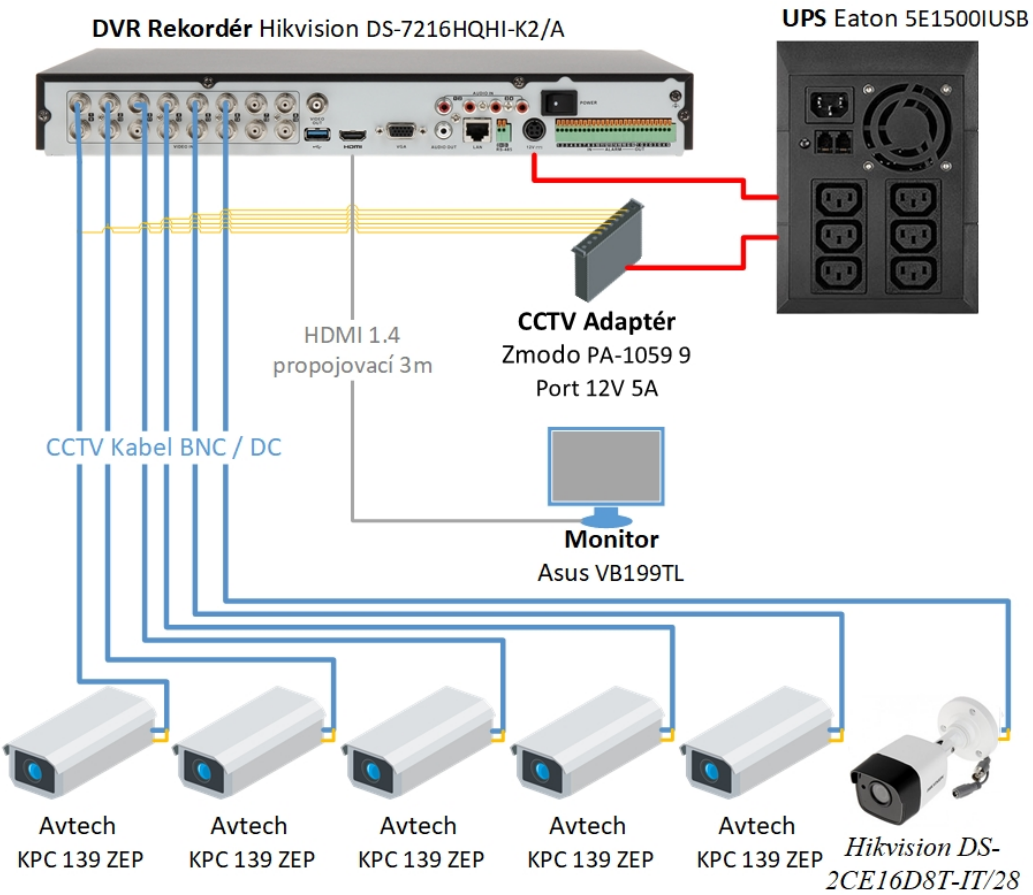
Obrázek 84: Instalace HDD do DVR rekordéru.

Po překontrolování byl osazen zpět přední kryt a provedeno testovací zapojení do sítě.

Obrázek 85: Testovací zapojení sítě a DVR rekordéru.

Záznamové zařízení je nutno uchovat v čisté a suché místnosti, kde teploty nepřekročí stanovenou mez dle manuálu k zařízení. Rekordér může být umístěn jak horizontálně, tak vertikálně, ale nesmí dojít k ucpání otvorů, které přivádí studený vzduch pro chlazení pevného disku a elektroniky. Vhodným místem může být uzamykatelná skříňka, kde může cirkulovat vzduch.

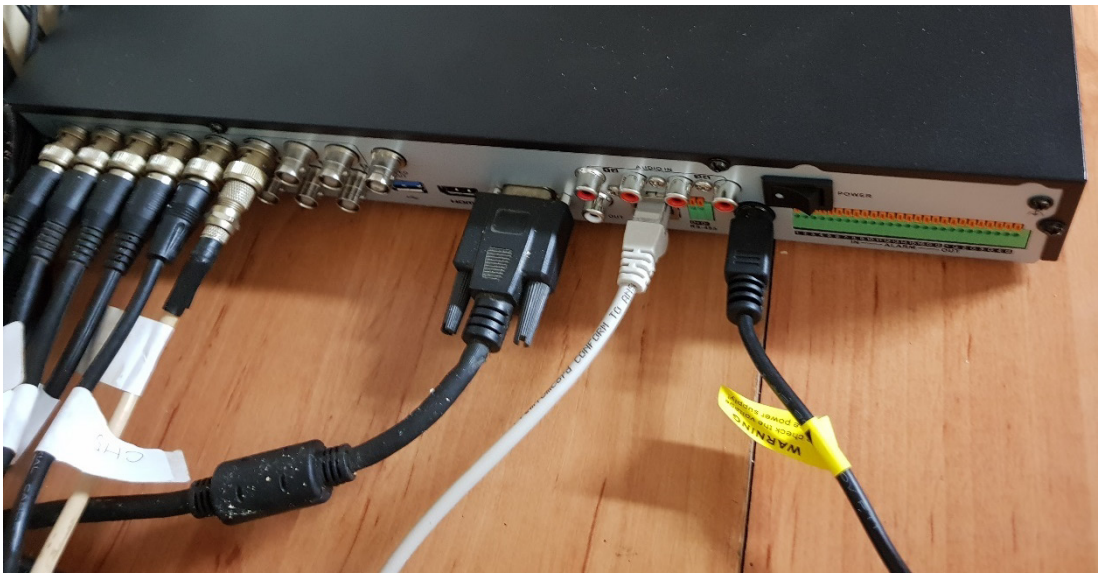
Zároveň podle nařízení úřadu na ochranu osobních údajů a nově i zákon na ochranu osobních údajů (GDPR) platného od května 2018 musí být záznamové zařízení dostatečně chráněno proti zneužití osobních údajů na něm uložených (obličejů a dalších parametrů, které mohou identifikovat příslušnou osobu) a zároveň má mít k němu přístup pouze určený správce, případně správcem povolaná osoba. Z toho důvodu také není pořízená fotodokumentace přímo z místa uložení v objektu restaurace, ale pouze z doby testování. Veškeré zapojení je znázorněno na následujícím schématu:



Obrázek 86: Schéma zapojení kamerového systému.

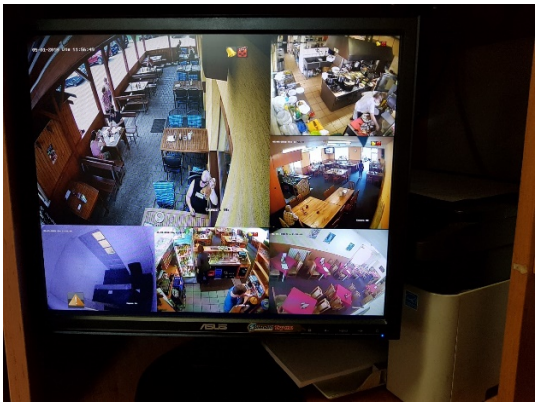
Po nalezení vhodného umístění, které vyhovuje požadavkům Úřadu pro ochranu osobních údajů a GDPR bylo zde přivedeno a zapojeno:

- Veškeré vedení jednotlivých kamer (zapojeno 6 BNC konektorů)
- Rozvod UTP Cat6 pro připojení do sítě LAN.
- Rozvod napájení CEE 7/5 (E) zásuvka IEC C14 vidlice z UTP záložního zdroje.
- VGA pro připojení dohledového monitoru Asus VB199TL (později nahrazeno vedením HDMI)
- USB přijímač pro připojení bezdrátové myši sloužící jako ovládací prvek DVR rekordéru při využití dohledového monitoru.



Obrázek 87: Zapojení DVR rekordéru v prostředí restaurace.

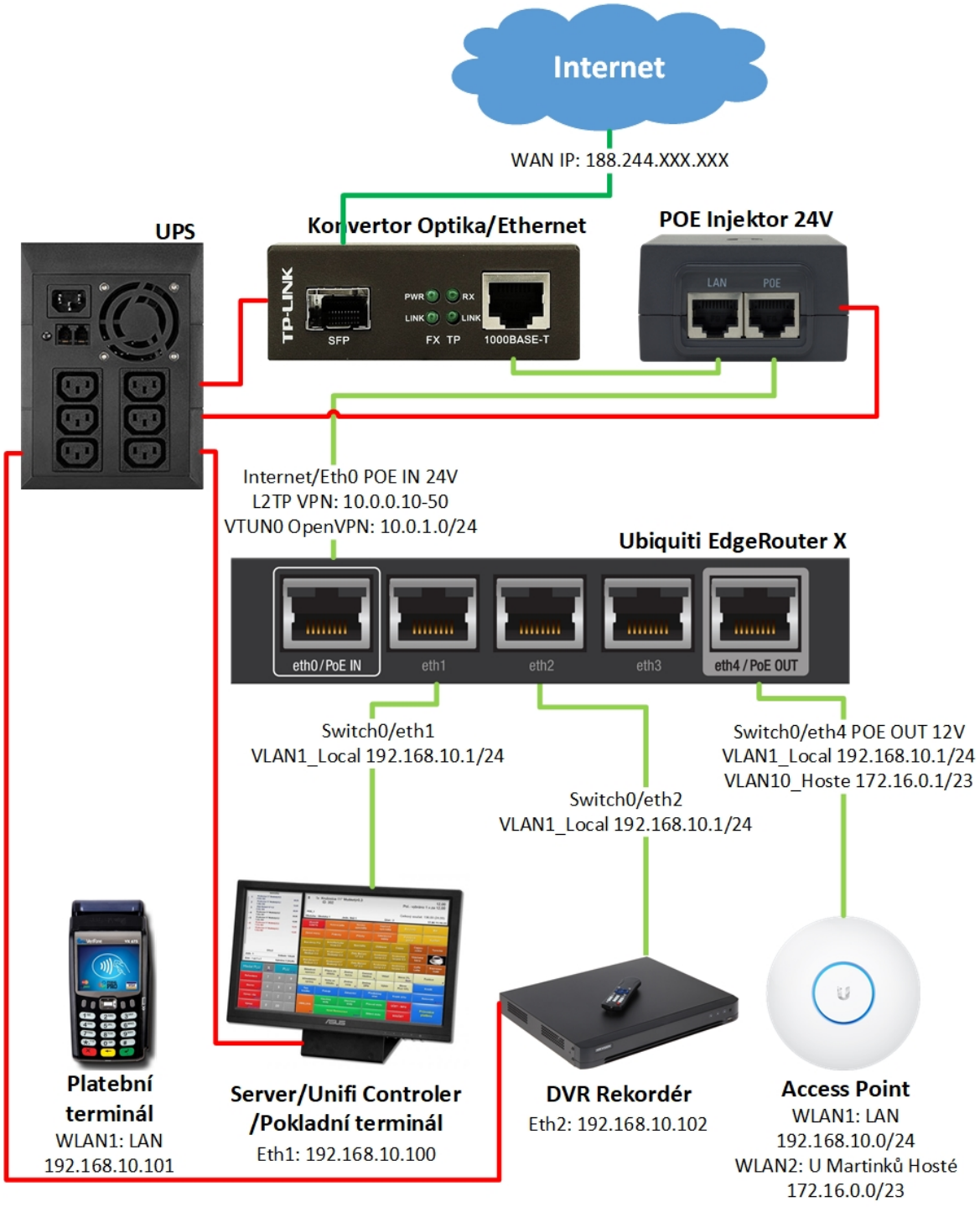
V posledním kroku instalace kamerového systému bylo přivedeno vedení video výstupu DVR rekordéru do police ve výčepu. Zde byl instalován dohledový monitor Asus VB199TL určený pro personál.



Obrázek 88: Dohledový monitor Asus VB199TL.

12 KONFIGURACE SÍŤOVÝCH PRVKŮ

V části konfigurace síťových prvků je popsáno veškeré nastavení síťových prvků včetně popisu, jak k těmto prvkům přistupovat.



Obrázek 89: Schéma konečného síťového zapojení.

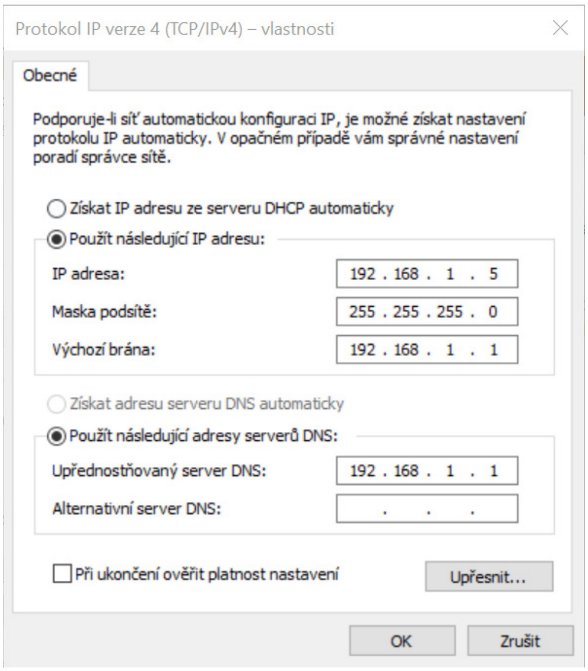
12.1 Router Ubiquiti EdgeRouter X

12.1.1 Úvodní přihlášení do webového operačního systému EdgeOS, aktualizace firmware, základní nastavení

Nejprve byl připojen notebook administrátora s operačním systémem Windows 10 k routeru pomocí UTP kabelu do portu RJ45 eth0. Následně byla manuálně nakonfigurována síťová karta pro připojení do přednastavené sítě routeru.

Cesta k nastavení (Windows 10):

Win+X > Síťová připojení > Změnit možnosti adaptéru > Ethernet > Vlastnosti> Protokol IP verze 4 (TCP/IPv4) > Vlastnosti >



Obrázek 90: Konfigurace PC pro připojení do výchozí sítě routeru.

Po tomto nastavení již lze spustit prohlížeč internetu a zadat adresu výchozí brány 192.168.1.1. Zobrazí se přihlašovací obrazovka. Zadáme předdefinované přihlašovací jméno a heslo (udávané většinou na zadním štítku routeru).

Po prvotním přihlášením byl aktualizován firmware na aktuální verzi ze stránek výrobce [47].

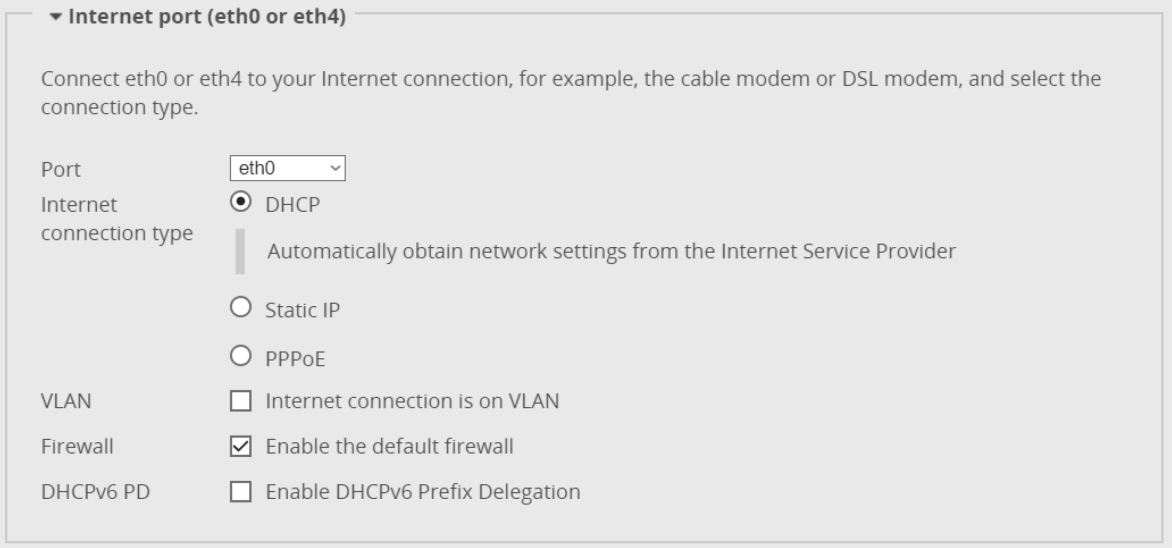
Cesta k nastavení (router EdgeOS):

System > Upgrade System Image > Upload a file > V dialogovém okně byl zvolen stažený firmware. Po dokončení procesu se router automaticky restartuje.

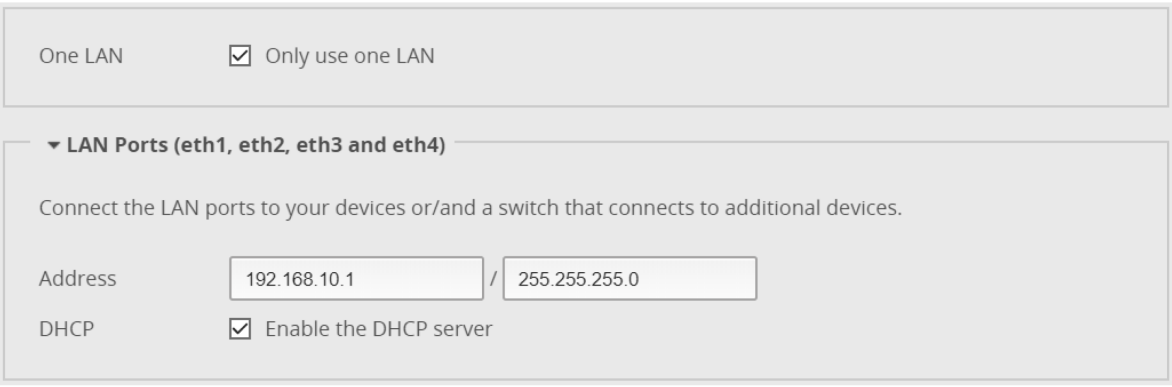
Následně byla provedena základní konfigurace připojení k WAN, LAN, nových přihlašovacích údajů k administraci routeru.

Cesta k nastavení (router EdgeOS):

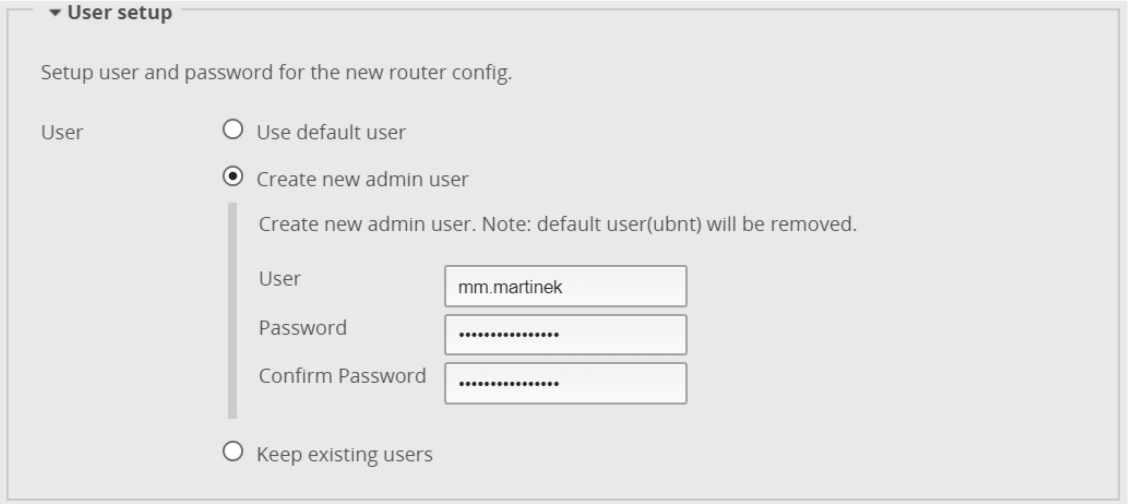
Wizards > Basic Setup >



Obrázek 91: Konfigurace WAN.



Obrázek 92: Konfigurace LAN.

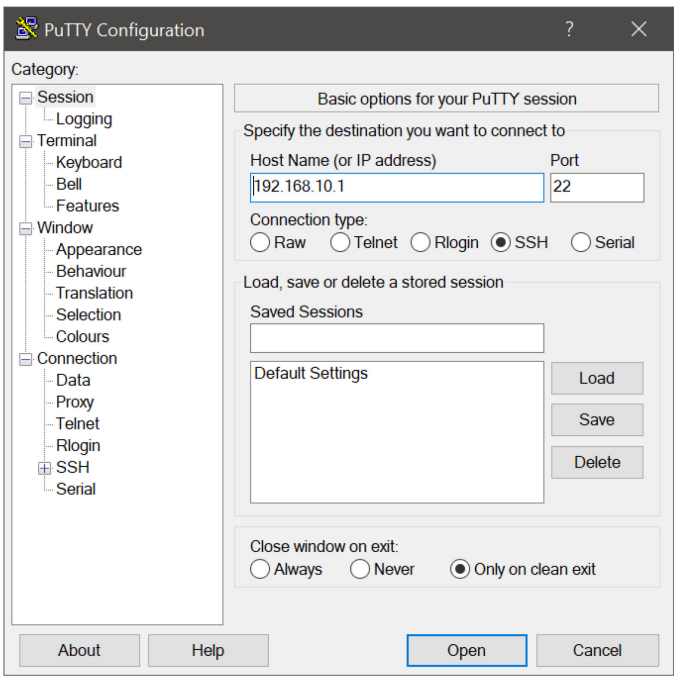


Obrázek 93: Konfigurace nových přihlašovacích údajů k administraci routeru.

Po dokončení konfigurace a uložení byl proveden restart routeru a v připojeném PC byla manuálně nakonfigurována síťová karta zpět do předešlého nastavení pro získání IP adresy a DNS serverů z DHCP serveru routeru.

12.1.2 Konfigurace SSH klienta pro připojení k CLI routeru

Pro další pokročilé nastavení bylo nutno připojit se k CLI konfiguračnímu rozhraní routeru. První možnost připojení je přímo přes terminál EdgeOS GUI. Druhá bezpečnější varianta, která byla využita je skrze SSH server. K tomu účelu byl nainstalován do PC program PuTTY, který zpřístupní CLI komunikaci přes SSH šifrovaný protokol [48].



Obrázek 94: Konfigurace SSH klienta PuTTY.

12.1.3 Konfigurace klonování MAC adresy routeru, HW akcelerace, napájení Access pointu pomocí POE

Po dokončení úvodní konfigurace bylo nutno přepojit notebook z portu eth0, který je již nastaven jako WAN port, na některý z portů právě nakonfigurovaného virtuálního switche (přepínače) eth1-eth3, eth 4 bude později nastaven jako trunk port POE OUT pro připojení access pointu. Do portu eth0 již může být zapojen přívod internetu z POE injektoru a do eth4 acces point (viz. Instalace a zapojování síťových prvků).

Konfigurace klonování MAC adresy routeru

Dalším krokem pro zprovoznění internetové konektivity bylo klonování MAC adresy starého routeru na router aktuální. Lokální poskytovatel internetového připojení využívá MAC adresu routeru k identifikaci zákazníka a přes ni mu povolí připojení a nastaví parametry jako veřejnou IP adresu, rychlost uploadu, downloadu, atd.

```
configure
set interfaces ethernet eth0 mac 04:8d:38:72:xx:xx
commit ; save
exit
```

HW akcelerace

HW akcelerace urychluje některé procesy jako kontrolu paketů, NAT, VLAN, IPsec (AES-128 / AES-256 / MD5 / SHA-1 / SHA-256) jelikož jsou obstarávány na HW úrovni a ne jako běžný SW proces [49].

```
configure
set system offload hwnat enable
set system offload ipsec enable
commit ; save
exit
reboot
```

Napájení Access pointu pomocí POE

```
configure
set interfaces ethernet eth4 poe output pthru
commit ; save
```

12.1.4 Vytvoření DNS domény a SSL certifikátu podepsaného certifikační autoritou

Jelikož přístup k administraci routeru znamená plnou kontrolu nad celou firemní sítí, byl přístup k EdgeOS zabezpečen jako HTTPS stránka s SSL zabezpečením ověřeným certifikační autoritou. Přístup k administraci byl prozatím nastaven pouze pro LAN síť se vzdáleným přístupem pomocí VPN. SSL šifrování tudíž plní přídavnou ochrannou funkci proti útočníkovi který pronikl již dovnitř LAN.

Registrace DNS domény

DNS doména byla založena u poskytovatele DuckDNS z důvodu bezplatného užívání.

Po registraci přes Google Účet majitele firmy byla v administraci vytvořena následující doména + byl vygenerován ověřovací token (neuvedeno):

Obrázek 95: Registrace DNS domény u DuckDNS.org [50].

Nastavení DuckDNS domény v routeru

Níže uvedená konfigurace přiřazuje registrovanou doménu k rozhraní eth0 (WAN) [51].

```
configure
set service dns dynamic interface eth0 service custom-duckdns
set service dns dynamic interface eth0 service custom-duckdns host-name umartinku
set service dns dynamic interface eth0 service custom-duckdns login nouser
set service dns dynamic interface eth0 service custom-duckdns password [token]
set service dns dynamic interface eth0 service custom-duckdns protocol dyndns2
set service dns dynamic interface eth0 service custom-duckdns server www.duc-
kdns.org
commit ; save
exit
```

Instalování ACME API

Důležitým krokem je vytvoření složky a stažení souborů API (Application Programming Interface) protokolu ACME (Automatic Certificate Management Environment) a úprava pravidel přístupu pro tyto soubory, kdy majitel může číst, zapisovat i spouštět, skupina a ostatní mají povolení číst a spouštět uvedené soubory.

Protokol ACME (Automatic Certificate Management Environment) je komunikační protokol pro automatizaci interakcí mezi certifikační autoritou (jako je Lets Encrypt) a webovým serverem (routeru), což umožňuje automatizované nasazení infrastruktury veřejných klíčů.

```
mkdir -p /config/scripts/acme/dnsapi

curl -o /config/scripts/acme/acme.sh https://raw.githubusercon-
tent.com/Neilpang/acme.sh/master/acme.sh

curl -o /config/scripts/renew.acme.sh https://raw.githubusercon-
tent.com/hungnguyenm/edgemax-acme/master/renew.acme.sh

curl -o /config/scripts/reload.acme.sh https://raw.githubusercon-
tent.com/hungnguyenm/edgemax-acme/master/reload.acme.sh

curl -o /config/scripts/acme/dnsapi/dns_duckdns.sh https://raw.githu-
busercontent.com/Neilpang/acme.sh/master/dnsapi/dns_duckdns.sh

chmod 755 /config/scripts/acme/acme.sh /config/scripts/renew.acme.sh
/config/scripts/reload.acme.sh /config/scripts/acme/dnsapi/dns_duc-
kdns.sh
```

První žádost o certifikát

- -d je doména, která má vydávat certifikát.
- -n je ID poskytovatele DNS pro identifikaci komunikačního skriptu u ACME API.
- -t je značka rozhraní API.
- -k je odpovídající hodnota značky API.

```
sudo /config/scripts/renew.acme.sh -d umartinku.duckdns.org -n dns_duc-
kdns -i -v -t "DuckDNS_Token" -k "[uživatelův token]"
```

Konfigurace routeru

Nastavení domény směrem k interní IP adrese routeru pomocí statického mapování hostitele:

```
set system static-host-mapping host-name umartinku.duckdns.org inet
192.168.10.1
```

Nastavení umístění souboru s certifikátem serveru a privátním klíčem pro webové rozhraní EdgeOS.

```
configure
set service gui cert-file /config/ssl/server.pem
commit ; save
```

12.1.5 Konfigurace VLAN1_Local a VLAN10_Hoste

V lokální síti byly nakonfigurovány 2 VLAN sítě:

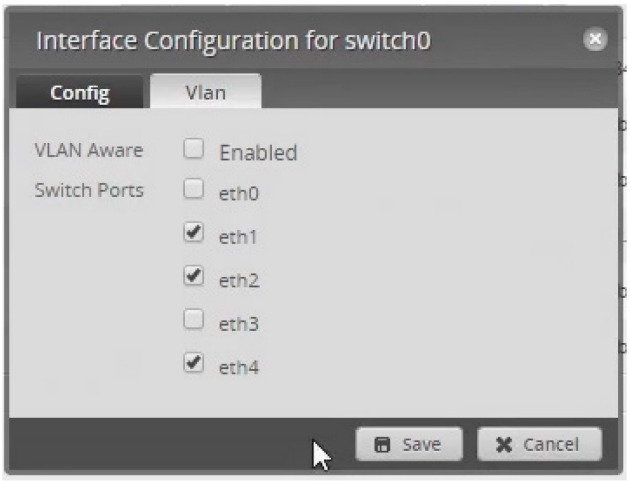
První VLAN síť s názvem VLAN1_Local slouží k bezpečné komunikaci důvěryhodných pracovníků firmy a jednotlivých síťových zařízení.

Druhá VLAN síť s názvem VLAN10_Hoste slouží pro připojení zákazníků k síti Internet.

Při konfiguraci ve webovém GUI rozhraní EdgeOS byl nejprve vyřazen z důvodu bezpečnosti port eth3 z rozhraní virtuálního switche switch0 a byla mu následně přiřazena IP adresa z odlišné třídy neveřejných IP adres skupiny A 10.0.0.1. Tento krok byl proveden z důvodu zajištění záložního připojení, aby nedošlo k nechtěnému uzamčení konfiguračního rozhraní při nastavování VLAN a jednotlivých portů virtuálního switche switch0.

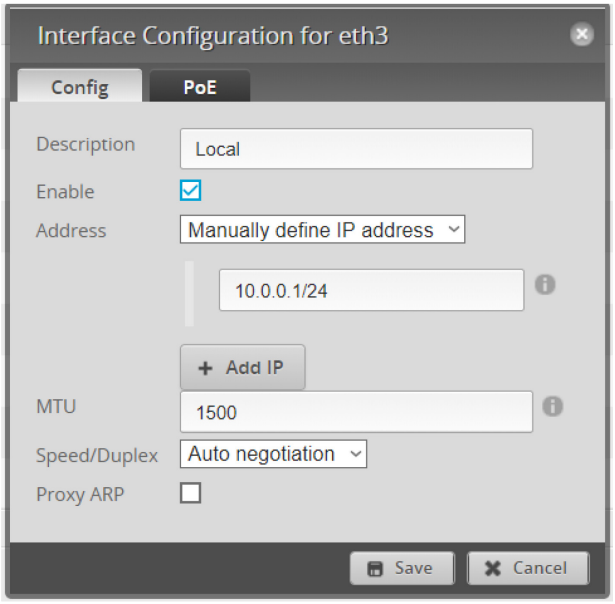
Cesta k nastavení (router EdgeOS):

Dashboard > switch0 > Actions > Config > Vlan >



Obrázek 96: Odebrání portu eth3 z rozhraní switch0.

Dashboard > eth3 > Actions > Config >



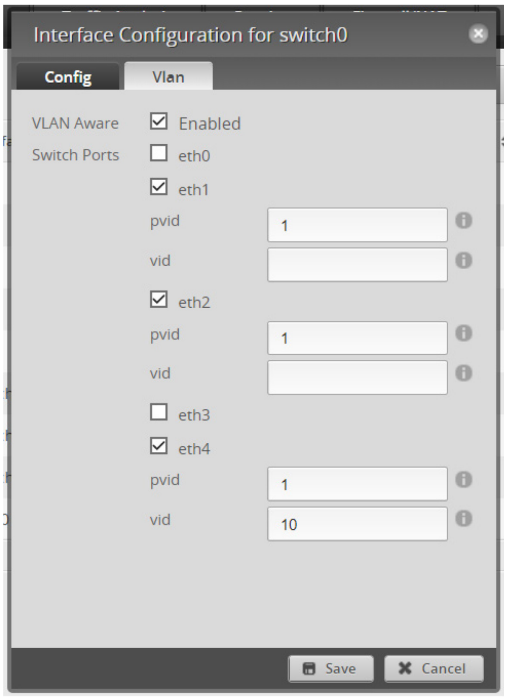
Obrázek 97: Konfigurace záchranného portu eth3.

Dále byly nakonfigurovány jednotlivé porty virtuálního switch0 pro hlavní VLAN1_Local definovanou na všech portech pomocí identifikátoru **PVID (Port Virtual Local Area Network) = 1**, tato VLAN identifikována pomocí portů. Přijímá všechny pakety, které přicházejí nebo odcházejí přes libovolný port. Jediným kritériem filtrování pro tento druh VLAN je samotný fyzický port, ke kterému je zařízení připojeno. Pokud tedy VLAN1_Local síť obsahuje členy portů eth1 až eth4. Zařízení připojeno k portu eth1, může komunikovat s porty eth2 až eth4. Jestliže jiné zařízení je připojeno př k portu eth5, komunikace s libovolným z portů VLAN1_Local není možná.

Zároveň byla na trunk portu eth4 definována VLAN10_Hoste založená na značkách, která určuje své členy pomocí identifikátoru **VID (Virtual local area network ID)=10.** Tento princip se značně liší od sítí VLAN založených na portech. Pokud se v seznamu vstupního či výstupního filtrování nacházejí další pravidla, proběhne kontrola paketu pomocí dalších kritérií filtrování, která rozhodnou o tom, zda jej lze předat dál. Značkované VLAN se mohou šířit i mimo jeden aktivní prvek, jak je tomu u portových VLAN.

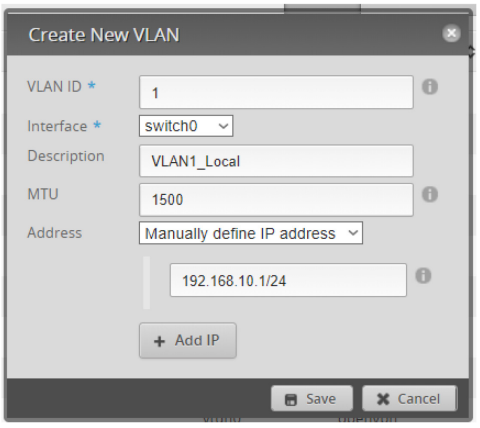
Cesta k nastavení (router EdgeOS):

Dashboard > switch0 > Actions > Config > Vlan >

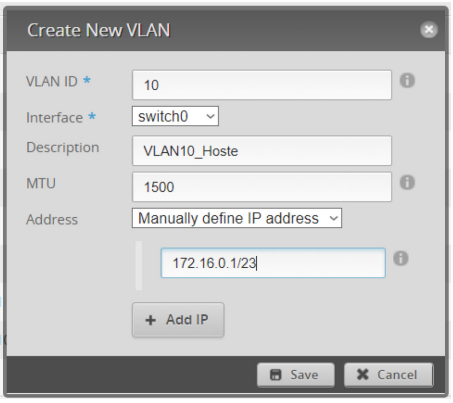


Obrázek 98: Konfigurace VLAN identifikátorů portů switch0.

Dále byly přidány rozhraní VLAN1_Local a VLAN10-Hoste.



Obrázek 99: Konfigurace rozhraní VLAN1_Local.



Obrázek 100: Konfigurace rozhraní VLAN10_Hoste.

Po úspěšné konfiguraci VLAN byl router resetován a záchranný port eth3, (který byl na začátku vyčleněn) byl přidán zpět do switch0 s VID 1 a byla mu odebrána manuálně definovaná IP adresa.

Dále bylo provedeno testování, při kterém byla zjištěna nefunkčnost komunikace s DNS servery. Při přihlášení na VLAN pomocí PC byl v příkazovém řádku proveden test:

```
netsh interface ipv4 show config
ping 8.8.8.8
ping www.youtube.com
```

Ping test youtube.com vyšel bez odezvy.Z toho důvodu bylo zjištěno, že je nutno nastavit na routeru DNS forwarding (přesměrováni) pro obě VLAN rozhraní:

```
configure
edit service dns
 set forwarding listen-on switch0.1
 set forwarding listen-on switch0.10
 set forwarding cache-size 150
 commit ; save
exit
```

12.1.6 Konfigurace DHCP serveru a mapování statických klientů

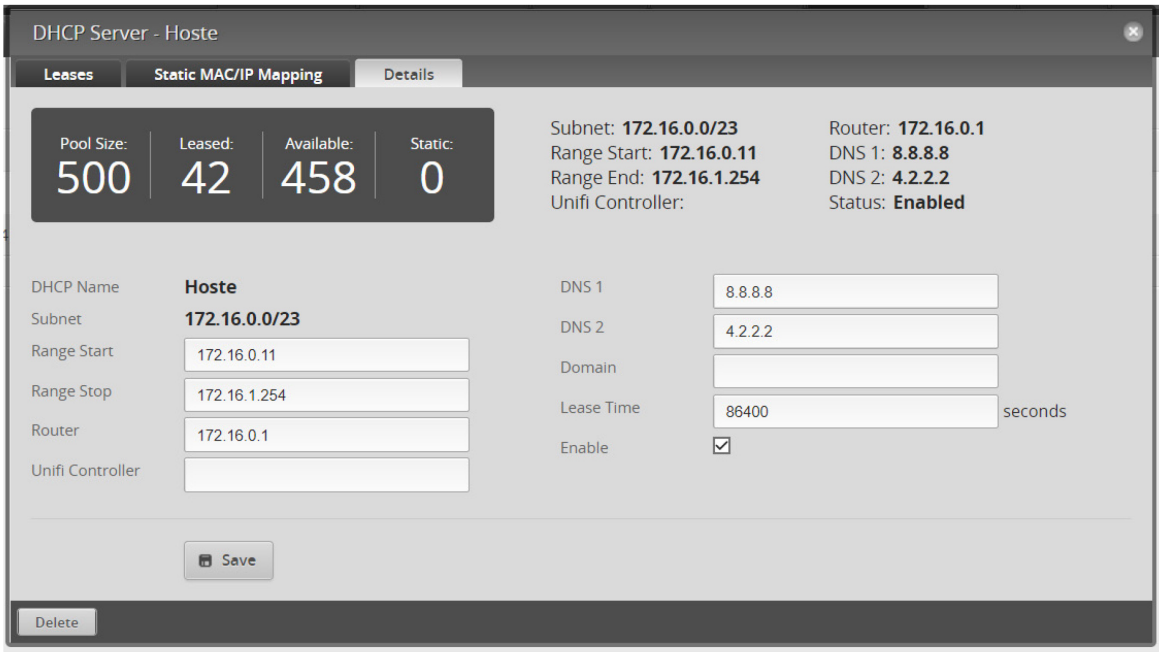
V dalším kroku byla provedena konfigurace DHCP serveru pro obě VLAN.

U DHCP serveru pro VLAN10_Hoste byla provedena změna rozsahu na subnet 172.16.0.0/23 pro zvýšení rozsahu IP adres na 511 respektive 500 po úpravě spodního rozsahu na .11 abychom získali rezervu mimo DHCP rozsah pro servisní účely.

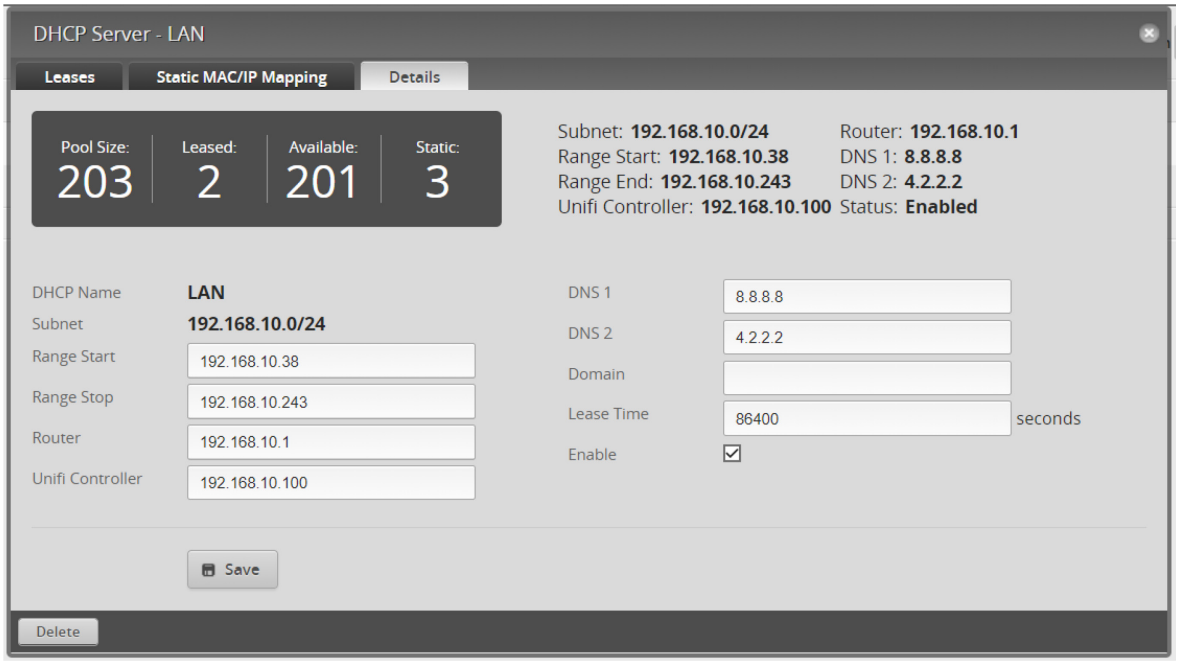
U DHCP serveru pro VLAN1_Local byl nastaven subnet 192.168.10.0/24 a staticky namapována IP adresa Unifi Controlleru 192.168.10.100. Dále byly nastaveny statické IP adresy klientských zařízení podle MAC adres. Jednalo se o DVR rekordér, platební terminál a server (Unifi Controller). Ostatní nastavení je viditelné níže.

Cesta k nastavení (router EdgeOS):

Services > DHCP Server > Add DHCP Server >



Obrázek 101: Konfigurace DHCP pro VLAN10_Hoste.



Obrázek 102: Konfigurace DHCP pro VLAN1_Local.

Name ▲	MAC Address ⇕	IP Address ⇕
DVR_recorder	18:68:cb:a2:3e:5d	192.168.10.102
Platebni_terminal	44:2C:05:6E:AD:9B	192.168.10.101
Server_Controler	34:97:F6:39:19:8C	192.168.10.100

Showing **1** to **3** of **3** entries

Obrázek 103: Konfigurace statických IP adres HW klientů.

12.1.7 Konfigurace pravidel firewallu definující práva hostů

V části konfigurace firewallu jsou popsány kroky potřebné k tomu, aby hostitelská síť neměla přístup k jiným sítím v LAN (jako je VLAN1_Local, VPN atd.) zatímco poskytuje přístup k internetu, serveru DNS a DHCP.

1.Vytvoření síťové skupiny

Nejprve byla definována síťová skupina se všemi adresami LAN sítě pro pozdější odkázání na tuto skupinu při vytváření pravidla brány firewall. Ta blokuje přístup na všechny adresy místní sítě ve skupině pro klienty ze sítě pro hosty VLAN10_Hoste.

```
Configure
edit firewall group network-group LAN
 set network 192.168.0.0/16
 set network 172.16.0.0/12
 set network 10.0.0.0/8
top
commit ; save
```

2. Pravidla sítě hostů VLAN10_Hoste pro přístup směrem do LAN

Skupina ve výchozím nastavení přijímá veškerou komunikaci a postupně je pravidly usměrňována.

Pravidlo 1 umožňuje hostům reagovat na provoz iniciovaný z jedné z důvěryhodných sítí LAN. Propouští tedy pakety, které jsou součástí již navázaného spojení zvnějšku (př FTP...).

```
edit firewall name Host_do_LAN
 set default-action accept
 set rule 1 action accept
 set rule 1 description Povoleni_jiz_navazaneho_spojeni
 set rule 1 log disable
 set rule 1 protocol all
 set rule 1 state established enable  //Kontrola paketů v obou směrech
(které jsou součástí obousměrné komunikace)
 set rule 1 state related enable  //propouští pakety které jsou součástí
již navázaného spojení
top
commit ; save
```

Pravidlo 2 povoluje hostům přístup k určitému zařízení nebo službě v důvěryhodné síti LAN. V našem případě se jedná o portál pro autentizaci hostů umístěném na serveru, který je nutno sdílet. Číslo pravidla musí být nižší, než pravidla drop vytvořeného ve stejné skupině pravidel Host_do_LAN !

```
Configure
edit firewall name Host_do_LAN
 set rule 2 action accept
 set rule 2 description Povoleni_Guest_portal
 set rule 2 destination address 192.168.1.10
 set rule 2 destination port 8880
top
commit ; save
```

Pravidlo 3 brání hostům v dosažení sítě LAN definované v síťové skupině z prvního kroku až na výjimky s nižším číslem pravidla (viz výše).

```
edit firewall name Host_do_LAN
 set rule 3 action drop
 set rule 3 description Blokace_Host>IP(10,172,192)
 set rule 3 log disable
 set rule 3 protocol all
 set rule 3 destination group network-group LAN
top
commit ; save
```

Nakonec aplikujeme tento set pravidel na rozhraní, kde jsou hosté připojeni v příchozím (in) směru.

```
edit interfaces switch switch0
 set vif 10 firewall in name Host_do_LAN
commit ; save
```

2. Pravidla sítě hostů VLAN10_Hoste pro lokální komunikaci

Skupina pravidel ve výchozím stavu blokuje veškerou komunikaci (například pokusy o přihlášení k routeru). Dodatečnými pravidly povoluje hostům získat informace o DNS a DHCP z routeru + nechá projít již navázané spojení.

Vytvoření skupiny pravidel Host_do_LOCAL, která ve výchozím nastavení ruší veškerou komunikaci (hostů mezi sebou).

```
edit firewall name Host_do_LOCAL
 set default-action drop
top
commit ; save
```

Pravidla umožňují hostům používat router pro vyhledání DNS (TCP / UDP port 53), přijímat adresu DHCP (port UDP 67) a nechá projít již navázané spojení.

```
edit firewall name Host_do_LOCAL
 set rule 1 action accept
 set rule 1 description Povoleni_DNS
 set rule 1 log disable
 set rule 1 protocol tcp_udp
 set rule 1 destination port 53

 set rule 2 action accept
 set rule 2 description Povoleni_DHCP
 set rule 2 log disable
 set rule 2 protocol udp
 set rule 2 destination port 67

 set rule 3 action accept
 set rule 3 description Povoleni_jiz_navazaneho_spojeni
 set rule 3 log disable
 set rule 3 protocol all
 set rule 3 state established enable
 set rule 3 state related enable
top
commit ; save
```

Nakonec aplikujeme tento set pravidel na rozhraní, kde jsou hosté připojeni v místním (local) směru (uvnitř vlastní sítě) [52].

```
edit interfaces switch switch0
 set vif 10 firewall local name Host_do_LOCAL
commit ; save
```

12.1.8 Konfigurace L2TP IPsec VPN komunikace

Prvním krokem konfigurace L2TP VPN je povolení potřebných komunikačních portů, kterými jsou UDP 1701 (L2TP), UDP 500 (IKE), UDP 4500 (NAT-T), protokol 50 (ESP).

```
configure
edit firewall name WAN_LOCAL
 set rule 30 action accept
 set rule 30 description IKE pro L2TP server
 set rule 30 destination port 500
 set rule 30 log disable
 set rule 30 protocol udp

 set rule 40 action accept
 set rule 40 description ESP pro L2TP server
 set rule 40 log disable
 set rule 40 protocol esp

 set rule 50 action accept
 set rule 50 description NAT-T pro L2TP server
 set rule 50 destination port 4500
 set rule 50 log disable
 set rule 50 protocol udp

 set rule 60 action accept
 set rule 60 description L2TP server
 set rule 60 destination port 1701
 set rule 60 ipsec match-ipsec
 set rule 60 log disable
 set rule 60 protocol udptop
top
commit ; save
```

Dále byla nakonfigurována autentizace serveru pomocí předsdíleného klíče.

```
set vpn l2tp remote-access ipsec-settings authentication mode pre-shared-secret
set vpn l2tp remote-access ipsec-settings authentication pre-shared-secret [heslo]
set vpn l2tp remote-access authentication mode local
set vpn l2tp remote-access authentication local-users username [jméno] password [heslo]
```

V dalším kroku byl definován rozsah IP adres, který budou využívat klienti L2TP VPN. Pro účely VPN komunikace byl definován nový rozsah neveřejných IP adres ze skupiny A. Lze ale využít i rozsah adres z místní podsítě (192.168.10.0/24), za předpokladu, že budou mimo rozsah přidělovaný DHCP serverem a nenastane tedy situace, že se budou překrývat s adresami IP vydanými serverem DHCP nebo používanými jinými zařízeními v síti.

```
set vpn l2tp remote-access client-ip-pool start 10.0.0.10
set vpn l2tp remote-access client-ip-pool stop 10.0.0.50
```

Dále byly definovány DNS servery, které bude L2TP VPN server využívat.

```
set vpn l2tp remote-access dns-servers server-1 8.8.8.8
set vpn l2tp remote-access dns-servers server-2 4.2.2.2
```

Bylo definováno rozhraní WAN, které bude přijímat požadavky L2TP klientů.

```
set vpn l2tp remote-access dhcp-interface eth0
```

Nakonec bylo definováno rozhraní IPsec, které bude přijímat požadavky L2TP klientů.

```
set vpn ipsec ipsec-interfaces interface eth0
commit ; save
```

Při diagnostice byly využity dva příkazy. První zobrazí připojené klienty k L2TP VPN serveru a druhý zobrazí tok dat skrze povolené WAN_LOCAL porty [53].

```
show vpn remote-access
show firewall name WAN_LOCAL statistics
```

12.1.9 Konfigurace OpenVPN komunikace

Vytvoření klíče Diffie-Hellman

V prvním kroku konfigurace OpenVPN bylo provedeno přihlášení do CLI rozhraní routeru. Bylo provedeno přihlášení jako uživatel root a následně vygenerován soubor klíče Diffie-Hellman (DH) v adresáři / config / auth o velikosti 2048 bitů.

Jedná se vygenerování velmi dlouhého prvočísla, které umožňuje klientovi a serveru vytvářet jedinečné klíče relace, aniž by klíč vysílali. Klíč slouží k šifrování veškeré další komunikace mezi klientem a serverem (pro symetrické šifrování po provedení asymetrické autentizace).

```
sudo su
openssl dhparam -out /config/auth/dh.pem -2 2048
```

Vytvoření CA certifikátu

Bylo zahájeno generování kořenového certifikátu certifikační autority CA (do položky Common Name musí být zadán unikátní název pro všechny certifikáty).

```
cd /usr/lib/ssl/misc/
./CA.sh -newca

PEM Passphrase: [heslo]
Country Name: CZ
State Or Province Name: [lokalita]
Locality Name: [lokalita]
Organization Name: [organizace]
Organizational Unit Name: Support
Common Name: ROOT
Email Address: xx.xx@xx.com
```

Po zhotovení bude vytvořen nový adresář nazvaný demoCA se dvěma důležitými soubory:

private / cakey.pem - soukromý klíč certifikační autority (nutno držet v bezpečí). Kdokoliv s tímto klíčem bude moci vydat nové certifikáty pro připojení k naší VPN.

cacert.pem - veřejný klíč certifikační autority (bude poskytován klientům)

Vytvoření certifikátu serveru

Dále vytvoříme veřejný a soukromý klíč pro server. Do položky Common Name musí být zadán unikátní název pro všechny certifikáty.

```
./CA.sh -newreq

PEM Passphrase: [heslo]
Country Name: CZ
State Or Province Name: [lokalita]
Locality Name: [lokalita]
Organization Name: [organizace]
Organizational Unit Name: Support
Common Name: SERVER
Email Address: xx.xx@xx.com
```

Po dokončení této akce budete mít dva nové soubory:

newkey.pem - soukromý klíč pro server (nutno držet v bezpečí)

newreq.pem - nepodepsaný veřejný klíč serveru (musí být podepsáno vytvořenou CA)

Podpis certifikátu

Dojde k vytvoření podepsaného certifikátu certifikační autoritou. Veřejný klíč serveru podepíše certifikační autorita vydávající veřejný certifikát. Nyní klienti vědí, že mohou důvěřovat serveru nesoucímu tento certifikát. Během tohoto příkazu bylo nutno zadat heslo, které se použijte při vytváření vytváření CA.

```
./CA.sh -sign
```

Získáme další soubor, který je uveden níže:

newcert.pem - Toto je veřejný klíč pro server

Přesunutí souborů certifikátů

Je doporučeno přesunout důležité soubory do adresáře, kde nebudou během upgradu firmwaru vymazány. Kromě přesouvání souborů je také přejmenujeme.

```
cp /usr/lib/ssl/misc/demoCA/cacert.pem /config/auth/
cp /usr/lib/ssl/misc/demoCA/private/cakey.pem /config/auth/
mv /usr/lib/ssl/misc/newcert.pem /config/auth/SERVER.pem
mv /usr/lib/ssl/misc/newkey.pem /config/auth/SERVER.key
```

demoCA / cacert.pem - Veřejný klíč CA, který byl vytvořen během procesu vytváření CA.

demoCA / private / cakey.pem Soukromý klíč CA, který slouží dále k podpisu nových certifikátů pro uživatele VPN.

newcert.pem - podepsaný veřejný klíč serveru OpenVPN.

newkey.pem - soukromý klíč serveru slouží k šifrování komunikace.

Všechny tyto soubory se přesunou do adresáře / config / auth / routeru, což je oblast v systému souborů, která není ovlivněna upgrady firmwaru.

Generování klientských klíčů

Stejný postup, jako u generování klíčů serveru, ale nyní úkon provádíme pro každého klienta, který potřebuje mít přístup k vytvářené VPN. Vyplňované heslo je potřeba si uložit a

Common name musí obsahovat opět jedinečný název (př. jméno nebo id klienta). Na konci je nutno soubory opět přesunout do zabezpečené složky.

```
./CA.sh -newreq
./CA.sh -sign
mv /usr/lib/ssl/misc/newcert.pem /config/auth/ADMIN.pem
mv /usr/lib/ssl/misc/newkey.pem /config/auth/ADMIN.key
```

Odstranění hesla z klíčů klientů a serveru

Tento krok umožňuje klientům připojit se pouze pomocí poskytnutého certifikátu bez nutnosti pokaždé zadávat heslo.

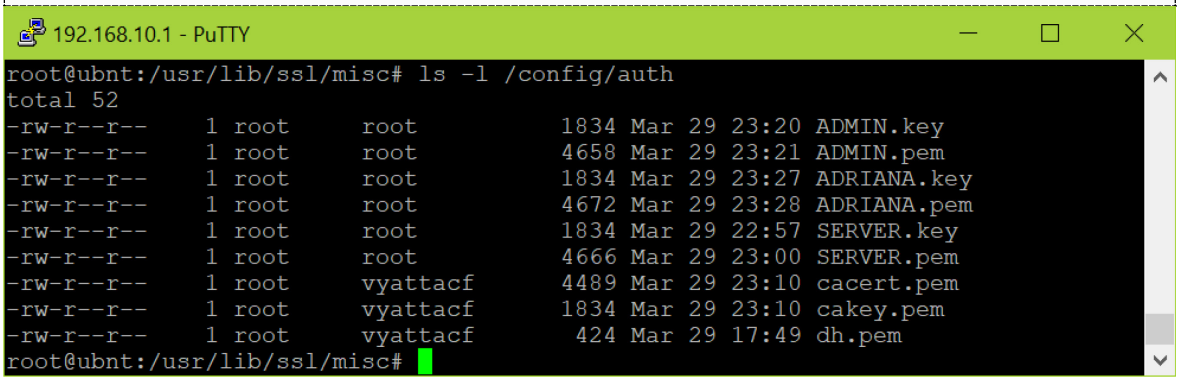
```
openssl rsa -in /config/auth/SERVER.key -out /config/auth/SERVER-no-pass.key
openssl rsa -in /config/auth/ADMIN.key -out /config/auth/ADMIN-no-pass.key
openssl rsa -in /config/auth/ADRIANA.key -out /config/auth/ADRIANA-no-pass.key
```

Přepíšete existující klíče s verzemi no-pass.

```
mv /config/auth/SERVER-no-pass.key /config/auth/SERVER.key
mv /config/auth/ADMIN-no-pass.key /config/auth/ADMIN.key
mv /config/auth/ADRIANA-no-pass.key /config/auth/ADRIANA.key
```

Ověření dostupnosti všech souborů v zabezpečeném adresáři

```
ls -l /config/auth
exit
```



Obrázek 104: Ověření dostupnosti certifikačních souborů OpenVPN.

Nastavení firewallu pro naslouchání Open VPN komunikace na portu 1194.

```
configure
set firewall name WAN_LOCAL rule 80 action accept
set firewall name WAN_LOCAL rule 80 description "OpenVPN"
set firewall name WAN_LOCAL rule 80 destination port 1194
set firewall name WAN_LOCAL rule 80 log enable
set firewall name WAN_LOCAL rule 80 protocol udp
commit ; save
```

Nastavení DNS předávání

Pro naslouchání žádosti na novém rozhraní vtun0.

```
configure
set service dns forwarding listen-on vtun0
commit ; save
```

Konfigurace rozhraní virtuálního tunelu OpenVPN

Klientům připojeným přes OpenVPN bude přidělena adresa ze subnetu 10.0.1.0/24 a budou mít přístup ke klientům uvnitř subnetu firemní LAN 192.168.10.0/24.

```
configure
set interfaces openvpn vtun0 mode server
set interfaces openvpn vtun0 server subnet 10.0.1.0/24
set interfaces openvpn vtun0 server push-route 192.168.10.0/24
set interfaces openvpn vtun0 server name-server 192.168.10.1
commit ; save
```

Dále bylo nastaveno šifrování AES 256bit a hashovací algoritmus SHA256.

```
configure
set interfaces openvpn vtun0 encryption aes256
set interfaces openvpn vtun0 hash sha256
commit ; save
```

Propojení certifikátu a klíče serveru, klíče DH s rozhraním virtuálního tunelu.

```
configure
set interfaces openvpn vtun0 tls ca-cert-file /config/auth/cacert.pem
set interfaces openvpn vtun0 tls cert-file /config/auth/SERVER.pem
set interfaces openvpn vtun0 tls key-file /config/auth/SERVER.key
```

```
set interfaces openvpn vtun0 tls dh-file /config/auth/dh.pem
commit ; save
```

Dodatečná nastavení upřesňující využití komunikačního portu 1194, TLS (SSL) a zapnutí komprimace dat v tunelu pro ušetření datového toku.

```
configure
set interfaces openvpn vtun0 openvpn-option "--port 1194"
set interfaces openvpn vtun0 openvpn-option --tls-server
set interfaces openvpn vtun0 openvpn-option "--comp-lzo yes"
commit ; save
```

Při diagnostice byly využity dva příkazy. První zobrazí připojené klienty k L2TP VPN serveru a druhý zobrazí tok dat přes povolené WAN_LOCAL porty [54] [55].

```
show openvpn status server
show firewall name WAN_LOCAL statistics
```

12.1.10 Návrh realizace

Nová síťová infrastruktura byla budována a laděna souběžně se zachováním funkčnosti starého řešení. Po dokončení propojení a provedení finální konfigurace autor síť důkladně otestoval a zahájil 2denní testovací období. V tomto období došlo (po domluvě s vedoucím) k přenastavení autentizačních údajů, připojení a zaškolení zaměstnanců firmy. Jelikož nenastaly po uplynutí testovacího období žádné problémy proběhlo kompletní přepojení všech zařízení na novou infrastrukturu a vypojení infrastruktury staré.

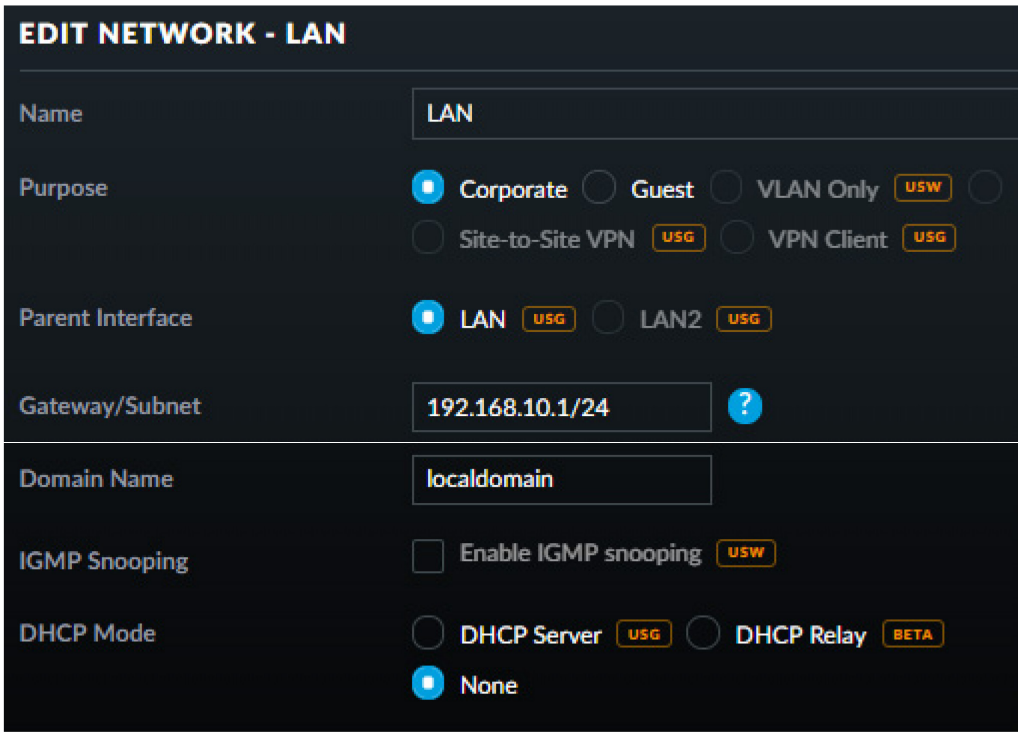
12.2 Access Point Ubiquiti Unifi AP AC LR

12.2.1 Napojení na síť routeru Ubiquiti EdgeRouter X

V první fázi konfigurace Access pointu Ubiquiti Unifi AP AC LR bylo nutno napojit jej na již dříve nakonfigurovanou síť routeru Ubiquiti EdgeRouter X. V editaci sítě byla proto nastavena brána 192.168.10.1 a dále pak byl vypnut interní DHCP server. O přidělování IP adres i bezpečnostní pravidla firewallu se bude starat centrálně router.

Cesta k nastavení (Access point Unifi Controller):

Settings > Networks > LAN > Edit >



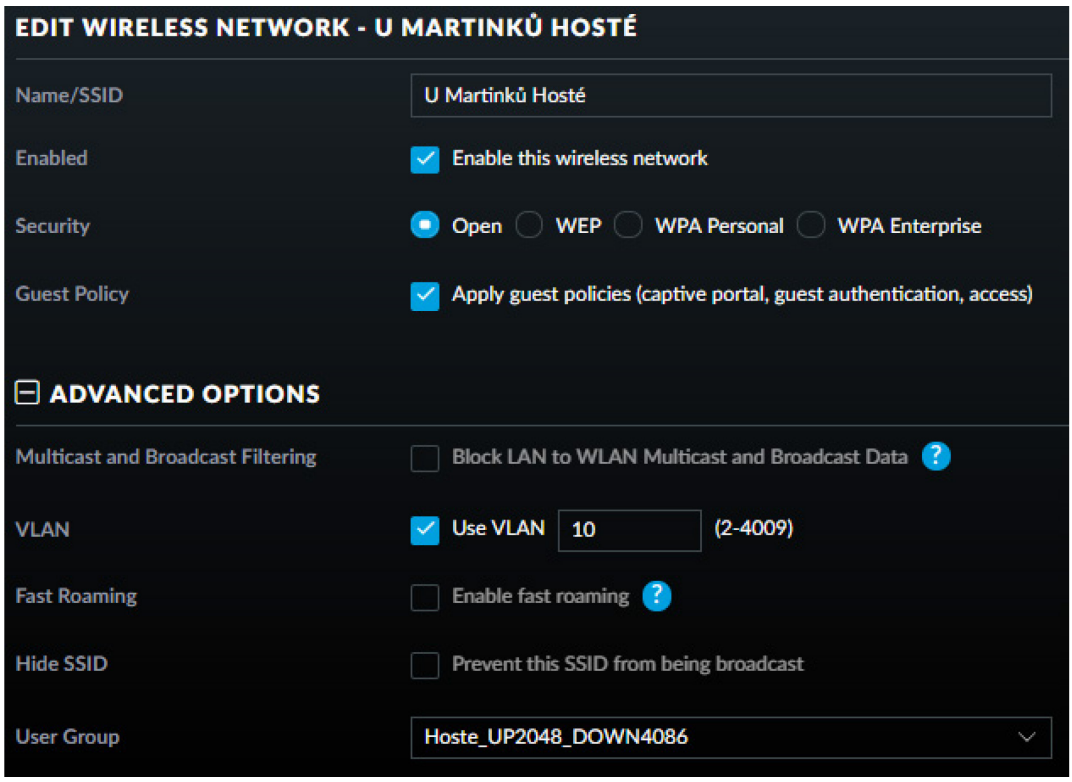
Obrázek 105: Konfigurace napojení AP na síť routeru.

12.2.2 Konfigurace WLAN pro hosty

U sítě pro hosty byla využita autentizace pomocí webového portálu na základě odsouhlasení podmínek užití. Tato metoda byla využita jako kompromis mezi bezpečností a efektivitou poskytování připojení k internetu větší skupině neustále se obměňujících lidí. Dále byla tato WLAN síť (SSID: U Martinků Hosté) napojena na VLAN10_Hoste pomocí VID 10. Nakonec bylo nastaveno přiřazení této sítě do uživatelské skupiny Hoste_UP2048_DOWN4086, díky čemuž dojde podle nastavení skupiny k omezení rychlosti připojení jednotlivce na stahovací rychlost 4086 Kbps a odesílací rychlost 2048 Kbps.

Cesta k nastavení (Access point Unifi Controller):

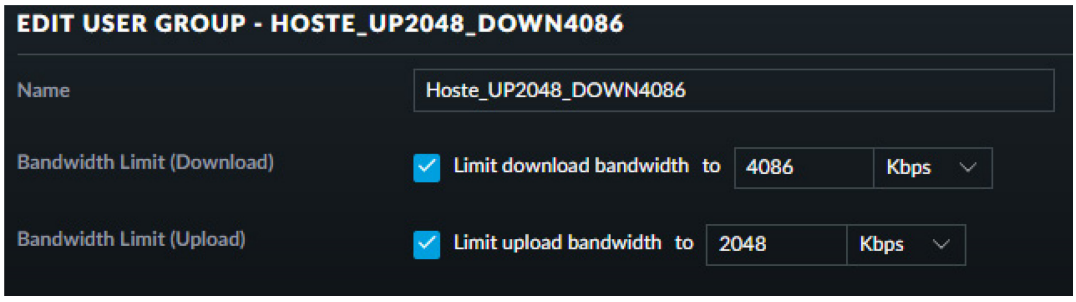
Settings > Wireless Networks > Create new wireless network >



Obrázek 106: Konfigurace WLAN pro hosty.

Cesta k nastavení (Access point Unifi Controller):

Settings > User Groups > Edit user group >



Obrázek 107: Konfigurace omezení rychlosti WLAN pro hosty.

12.2.3 Autentizace hostů pomocí webového portálu

Jak již bylo napsáno výše u konfigurace WLAN pro hosty, u sítě určené hostům restaurace byla využita autentizace pomocí webového portálu na základě odsouhlasení podmínek užití. Tento portál je přizpůsoben na velikost zobrazení pro displeje mobilních telefonů a běžných desktopových zařízení. Obsahuje logo restaurace, které bylo vytvořeno z bezplatné předlohy

a následně upraveno v bezplatném editoru vektorových fotografií Inscape. Dále obsahuje přepínač na 2 jazykové mutace (Čeština a Angličtina), zaškrtávací políčko pro odsouhlasení podmínek užití, které jsou následující:

Podmínky použití

Přístupem k bezdrátové síti potvrzujete, že jste plnoletí, přečetli jste si a souhlasíte s tím, že budete touto dohodu vázáni.

Bezdrátové síťové služby poskytují majitelé nemovitosti Restaurace U Martinků adresa Jablůnka 140 a jsou zcela na jejich uvážení. Váš přístup k síti může být z jakéhokoli důvodu zablokován, pozastaven nebo ukončen.

Souhlasíte s tím, že nebudete používat bezdrátovou síť pro jakýkoli účel, který je nezákonný, a přejímáte plnou zodpovědnost za vaše jednání.

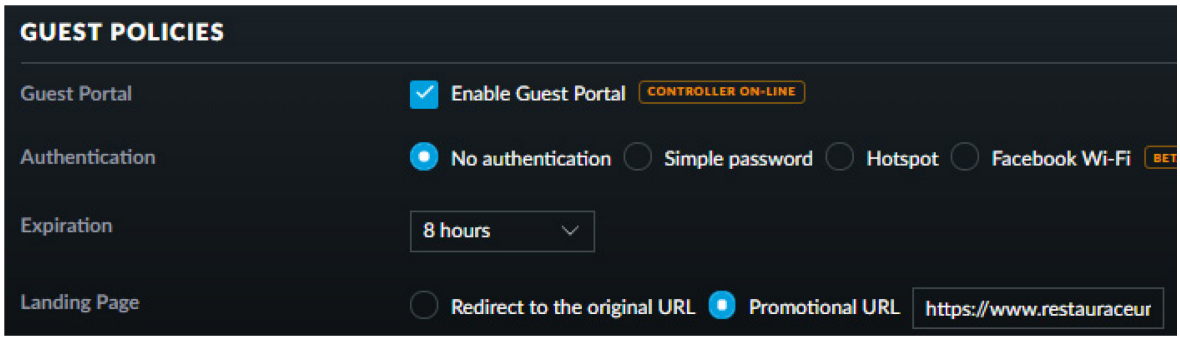
Bezdrátová síť je poskytována "tak jak je" bez jakýchkoli záruk, ať již vyjádřených nebo implicitních.

Po přečtení podmínek užití a jejich odsouhlasení je možné zvolit tlačítko Připojit, které na základě stisku zákazníka autentizuje, umožní mu přístup k internetu a zároveň jej přesměruje na oficiální stránky restaurace do sekce denní menu (restauraceumartinku.cz/denni-menu/).

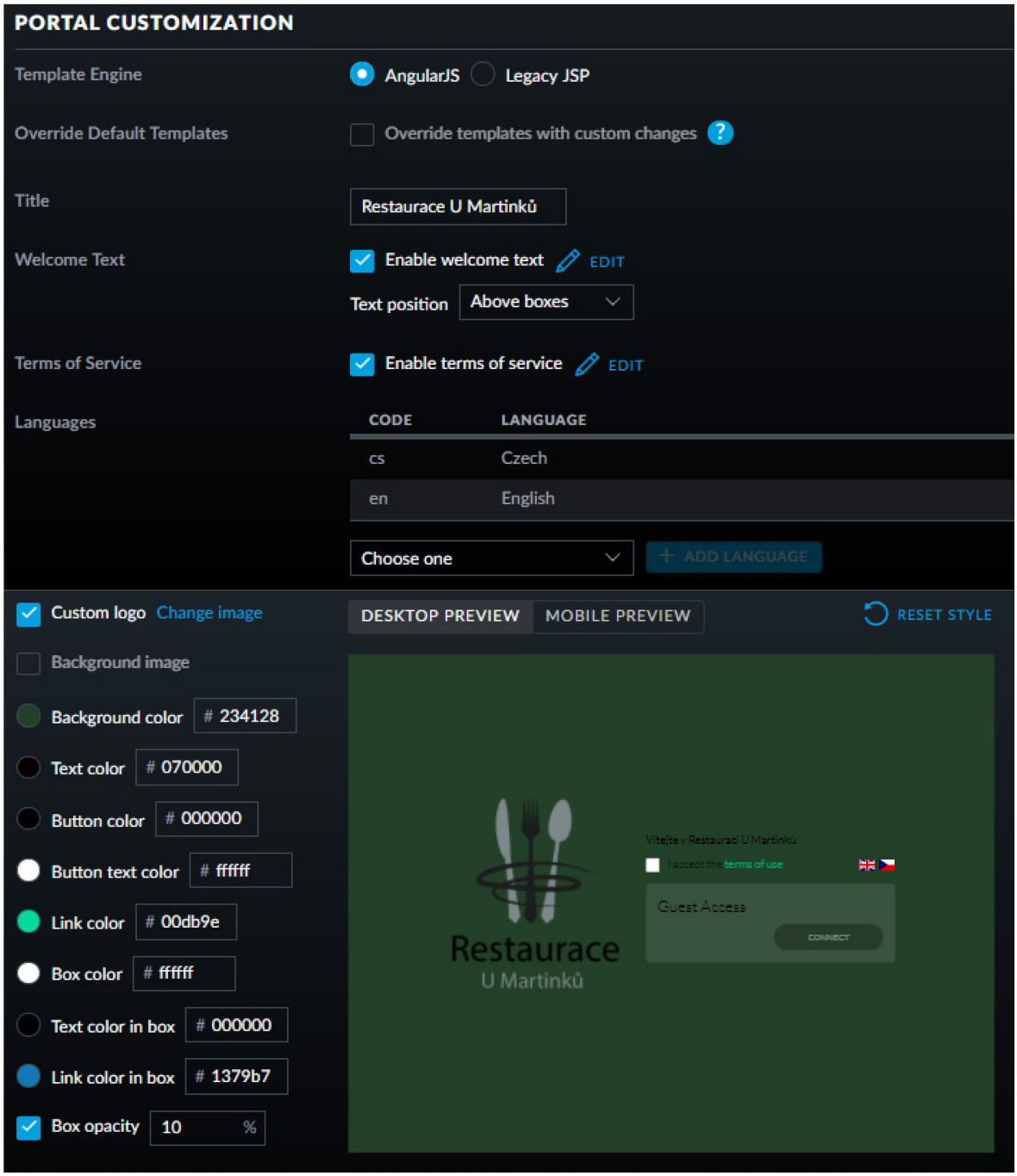
Konfigurace webového portálu je uvedena níže:

Cesta k nastavení (Access point Unifi Controller):

Settings > Guest Control >



Obrázek 108: Úvodní konfigurace webového portálu pro hosty.

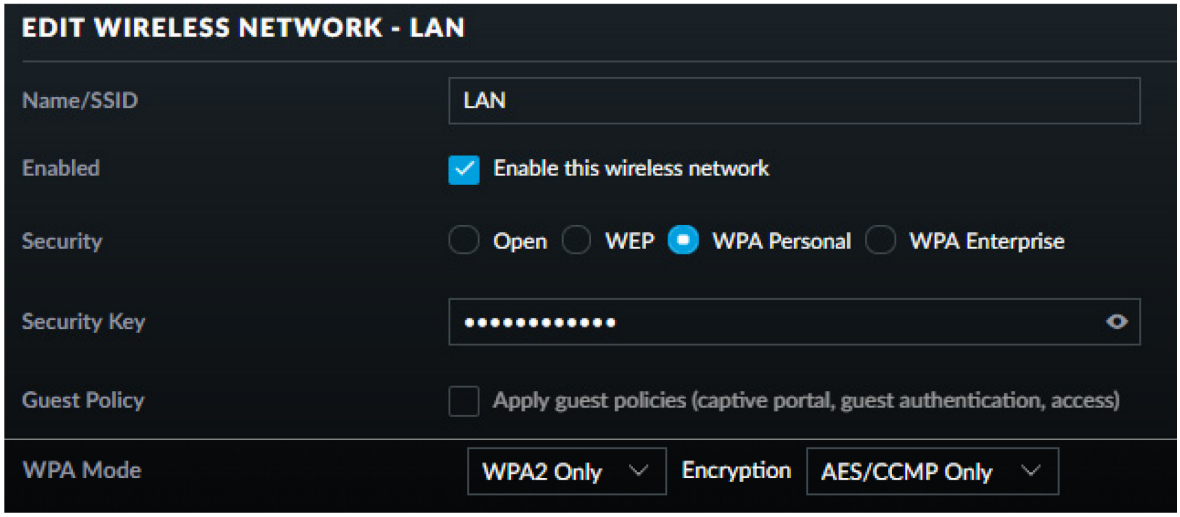


Obrázek 109: Konfigurace Webového portálu pro hosty.

12.2.4 Konfigurace firemní WLAN

Firemní WLAN (SSID: LAN) je napojena na základní firemní VLAN1_Local PVID=1. Dále je nakonfigurováno zabezpečení bezdrátového přenosu dle přihlédnutí ke studii zabezpečení sítě v teoretické části na WPA2-PSK s využitím šifry AES. Toto nastavení bylo vybráno jako nejbezpečnější řešení kompatibilní se všemi zařízeními, a to včetně platebního terminálu. Bylo uvažováno také o Radius serveru, ale nakonec bylo od tohoto záměru upuštěno,

jelikož jej nepodporují všechna připojená zařízení, jako je právě zmiňovaný platební terminál, některé síťové tiskárny a podobně. Jedinou možnosti by bylo pro tato zařízení vytvořit další VLAN, ale vzhledem k nízkému počtu zaměstnanců firmy by se Radius server na úkor znepřehlednění a zbytečné fragmentaci sítě nevyplatil.



Obrázek 110: Konfigurace firemní WLAN.

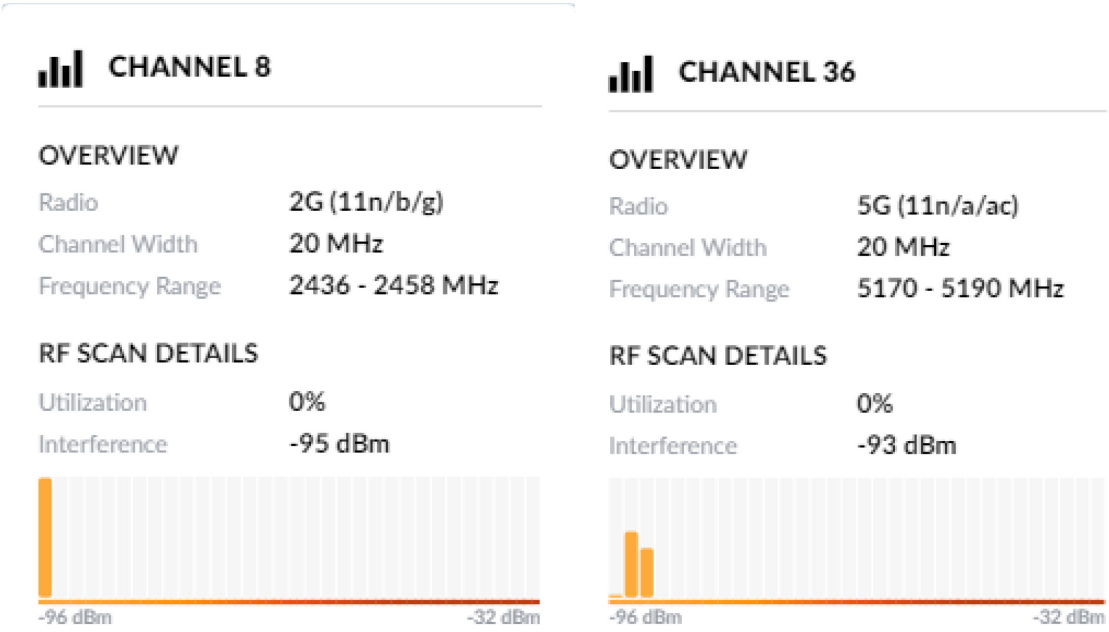
12.2.5 Konfigurace parametrů WiFi

Při konfiguraci parametrů WiFi byl využit diagnostický nástroj Unifi Controlleru, který zmapuje okolní WiFi sítě a zjistí jejich nastavení jako frekvenci pásma kanálu, číslo kanálu a sílu signálu antény. Z těchto údajů vytvoří mapu zarušení sítě a následně automaticky zvolí optimální kanál s nejnižším procentuálním využitím okolních sítí. Po provedení této diagnostiky byl zvolen kanál 8 pro pásmo 2,4GHz a 36 pro pásmo 5GHz.

Cesta k nastavení (Access point Unifi Controller):

Devices > Unifi AP-AC-LR > Tools > RF Environment > Scan

Obrázek 111: Automatická volba kanálů pro 2,4GHz a 5GHz.



Obrázek 112: Diagnostika zarušení WiFi sítě a automatická volba kanálů.

12.3 Platební terminál Verifone VX675

Platební terminál byl nakonfigurován pro komunikaci s WLAN SSID: LAN.

Cesta k nastavení (Platební terminál Konfigurační menu):

ADM > M+ Manager > Technik > [heslo k servisnímu menu] > Network > WiFi/SSL > WiFi >

SSID > Manual > LAN

Security > WPA2-AES > [Heslo WLAN SSID:LAN]

IP > IP adress > 192.168.10.101

IP > Netmask > 255.255.255.0

IP > Gateway > 192.168.10.1

Dále byl nakonfigurován režim platby pomocí pokladního systému a následný restart:

Cesta k nastavení (Platební terminál Konfigurační menu):

ADM > M+ Manager > Technik > [heslo k servisnímu menu] > Cash register > Network

ADM > M+ Manager > Restart

Konfiguraci komunikace s bankou prováděl servisní technik příslušné banky.

13 KONFIGURACE SERVERU

13.1 Konfigurace pokladního systému Consulta Conto Max

V sekci konfigurace pokladního systému byly popsány hlavní části konfigurace potřebné k zprovoznění pokladního systému. Dodatečné konfigurace zákaznických účtů, slev, týdenních rozpisů denního menu a podobně byly provedeny, ale z důvodu ochrany osobních údajů a již značného rozsahu práce nebyly popsány.

13.1.1 Instalace a aktivace pokladního systému

Před konfigurací pokladního systému byla provedena nejprve instalace a následná aktivace. Instalační soubor byl stažen ze stránek firmy Consulta. V průvodci instalací byla vybrána instalace všech modulů pokladního systému na jeden server z důvodu úspory nákladů:

Conto Server: Vrstva, která zpracovává požadavky od všech klientů a obsahuje základní logiku celé aplikace Conto. Tato vrstva je multithreadová (více vláknová), zpracovává požadavky klientů souběžně.

Jeho součástí je databázové jádro, které uchovává všechny informace pro chod systému, nastavení aplikace Conto a prodejní data. O správu dat se stará FirebirdSQL. Je to multiplatformní relační databáze, kterou vyvíjí a spravuje Firebird Foundation.

Conto Klient: klient určen pro samotné pokladny, určen pro personál.

Konfigurátor: klient, který umožňuje nastavení aplikace Conto včetně editace prodejních dat a správy i samotné databáze Conto.

Tiskový server: speciální druh klienta, který úzce spolupracuje s aplikačním serverem Conto. Tiskový server obsluhuje dle nastavení konkrétní periferní zařízení typu tiskárna.

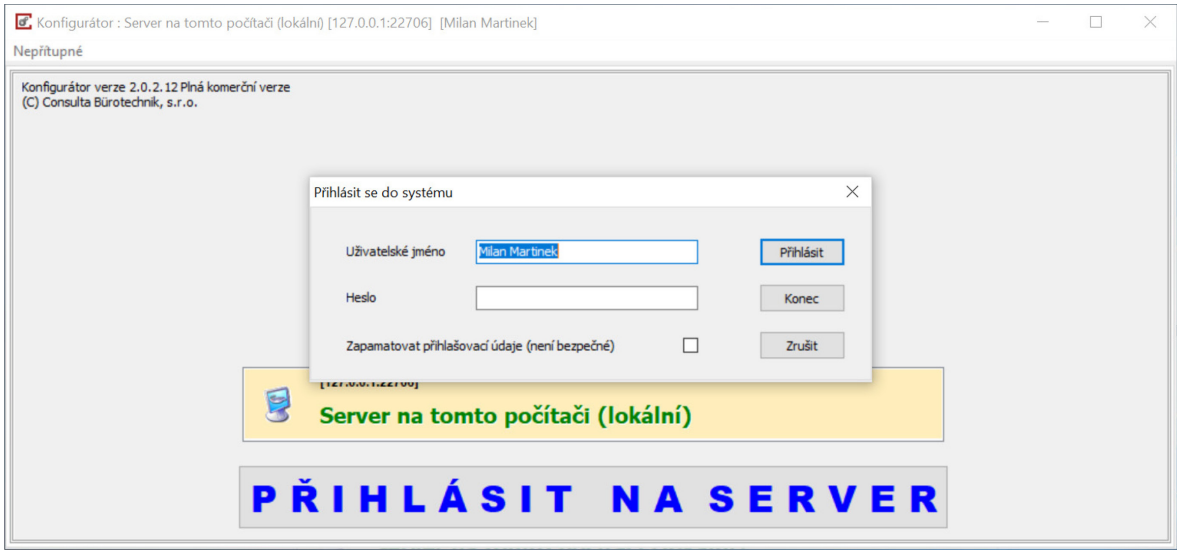
Dále byly nainstalovány všechny moduly, které budou po aktivaci odemčeny podle zakoupené licence Conto Max a zvolen přednastavený vzhled a nastavení pro restaurace. Tato nastavení budou následně přetvořena pro účely aktuální restaurace.

Po úspěšné instalaci následuje aktivace klienta a konfigurátoru. Každý program bylo nutno instalovat zvlášť. Po prvním spuštění bylo zobrazeno aktivační okno s jedinečným aktivačním kódem pokladny. Tento kód byl odeslán na mail výrobce společně s kupní smlouvou a následně výrobce zaslal aktivační kód, který byl použit.

13.1.2 Import EET certifikátu, nastavení firemních údajů

K zavedení EET komunikace na pokladním terminálu bylo podstatné DIČ majitele, ID provozovny a certifikát majitele včetně hesla k certifikátu. Certifikát včetně hesla a ID provozovny byl získán z daňového portálu ministerstva financí na základě registrace majitele restaurace na tomto portálu.

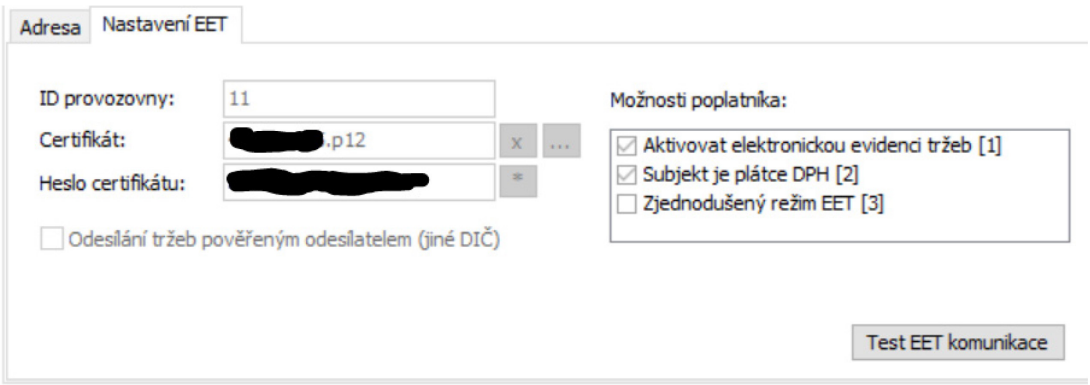
Pro editaci nastavení EET bylo nutné být přihlášený jako uživatel s oprávněním Admin v programu Conto Konfigurátor.



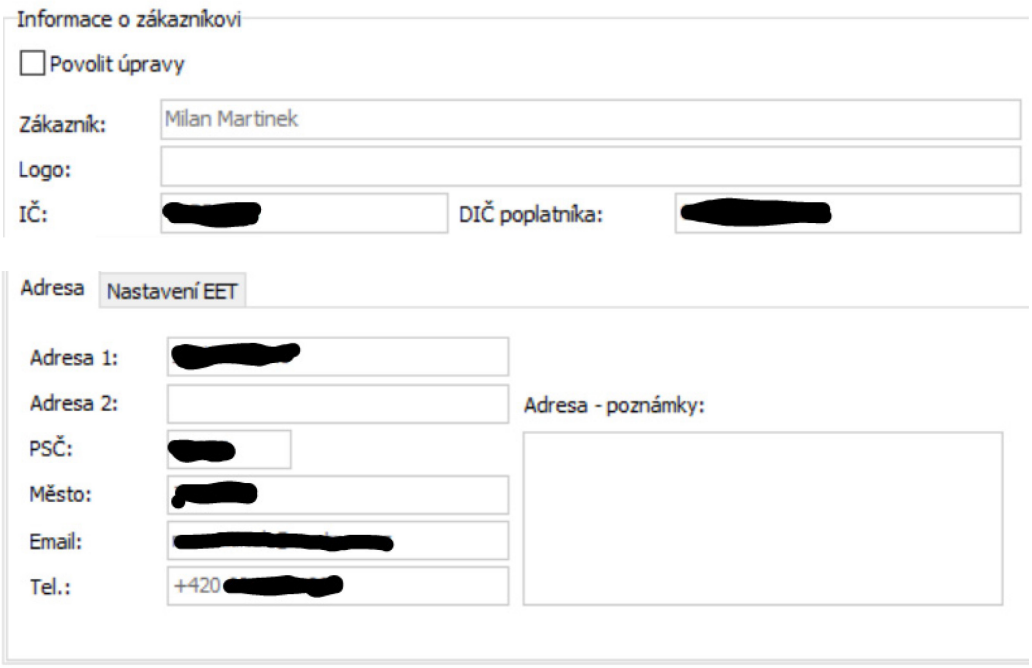
Obrázek 113: Přihlášení Conto Konfigurátor.

Cesta k nastavení (Server Conto Konfigurátor):

Základní nastavení > Zákazník > Povolit úpravy >



Obrázek 114: Konfigurace EET – Conto Konfigurátor.



Obrázek 115: Konfigurace údajů o majiteli - Conto Konfigurátor.

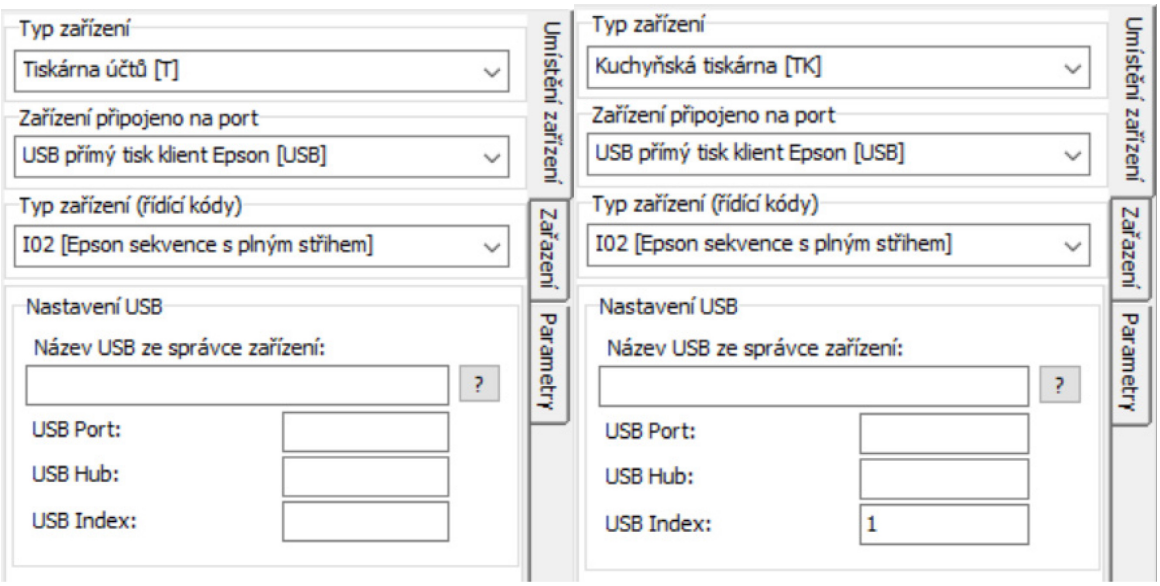
13.1.3 Konfigurace periferií (tiskárny, platební terminál)

Po úspěšném nainstalování ovladačů a inicializaci tiskárny účtů a tiskárny do kuchyně byly tyto tiskárny nakonfigurovány pro použití s pokladním systémem.

Cesta k nastavení (Server Conto Konfigurátor):

Periferie > Seznam všech zařízení > Tiskárna účtů >

Periferie > Seznam všech zařízení > Kuchyňská tiskárna >



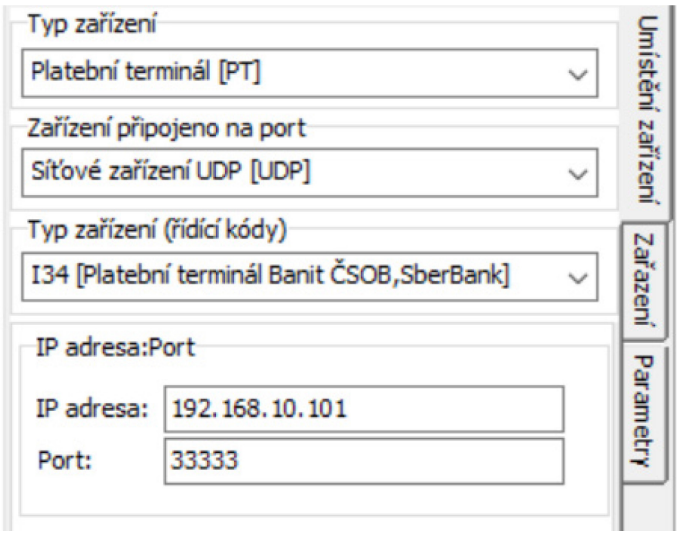
Obrázek 116: Konfigurace tiskáren – Conto Konfigurátor.

Obě totožné tiskárny byly odlišeny pomocí parametru USB Index. Parametry tisku a údajů na účtence byly ponechány podle výchozích hodnot programu. Nakonec byl proveden úspěšný test tisku.

Jako poslední zařízení byl nakonfigurován platební terminál.

Cesta k nastavení (Server Conto Konfigurátor):

Periferie > Seznam všech zařízení > Platební terminál >



Obrázek 117: Konfigurace platebního terminálu - Conto Konfigurátor.

Po inicializaci terminálu bylo nutno nastavit platební funkci.

Cesta k nastavení (Server Conto Konfigurátor):

Prodejní data > Platby > Karta > Parametry > Platební terminál 1 [g]

Nakonec byly všechny změny uloženy na server.

Cesta k nastavení (Server Conto Konfigurátor):

Komunikace > Odeslat data na server (F5)

13.1.4 Vytváření databáze veškerého zboží, polotovarů a surovin

V druhé fázi byly sestaveny za přítomnosti provozního pracovníka restaurace konfigurační databázové tabulky zboží, polotovarů a surovin členěných do různých skupin. U každé položky byly uvedeny parametry, jako měrná jednotka, cena, skupina, typ výrobku atd.

Všechny tabulky byly nejprve exportovány z konfigurátoru ve formě .sfv souborů a byly využity jako šablona, která se následně editovala v tabulkovém editoru.

Nejprve byly editovány jednotlivé oddělení, každé oddělení má vlastní ID, které bude dále využito pro napojení skupiny zboží, dále byl u některých položek nastaven parametr 4 (nezobrazovat v náhledech) a 6 (nezobrazovat do jídelníčku):

ID	Název	Výtěžnost	Par.
G001	Bar		
G002	Kuchyň		
G009	Polotovary		4,6
G010	Suroviny		4,6

Obrázek 118: Seznam oddělení – Conto Konfigurátor.

Následně byly editovány jednotlivé skupiny zboží. Opět má každá položka vlastní ID, které bude dále využito na napojení položek zboží na skupinu. Každá skupina byla zařazena do příslušného oddělení. U skupin zboží, které se bude připravovat v kuchyni, byl přiřazen tisk bonu pomocí tiskárny do kuchyně (parametr 4). Posledním parametrem je přiřazení sazby DPH 15 % (parametr 2) nebo 21 % (parametr 1).

ID	Název	Zař.	Tisk	DPH
D001	Teplé nápoje	G001		2
D002	Nealko	G001		2
D003	Pivo	G001		1
D004	Cukrovinky	G001		2
D005	Lihoviny	G001		1
D006	Whiskey	G001		1
D007	Likéry	G001		1
D008	Minutky	G002	4	2
D009	Přílohy	G002	4	2
D010	Pizza	G002	4	2
D011	Víno	G001		1
D012	Cigarety	G001		1
D013	Dezerty	G002	4	2
D014	Saláty	G002	4	2
D015	Denní menu	G002	4	2
D021	Sklad l	G010		2
D022	Sklad kg	G010		2

Obrázek 119: Seznam skupin zboží – Conto Konfigurátor.

Dále byly editovány suroviny. Každá položka má vlastní ID, název, ve kterém je pro přehlednost uvedeno, jestli se jedná o skladovou položku a v jakých jednotkách se uvádí, dále zařazení do určité skupiny zboží, cena, která se ovšem u surovin neuvádí, typ zboží (parametr

S označuje surovinu), aktuální skladové množství, údaj určující minimální skladové množství, než dojde k upozornění na doskladnění a index dodavatele (parametr 5 určuje obchodní řetězec Makro).

ID	Název	Zař.	Cena	Typ	Sklad	MinZas	Dodav.
2103	Bramborové tolárky (sklad kg)	D022	0,00	S	0	1	5
2104	Dušená šunka (sklad kg)	D022	0,00	S	0	1	5
2105	Eidam (sklad kg)	D022	0,00	S	0	1	5
2107	Hermelín (sklad kg)	D022	0,00	S	0	1	5
2108	Hovězí maso (sklad kg)	D022	0,00	S	0	1	5
2109	Hranolky (sklad kg)	D022	0,00	S	0	1	5

Obrázek 120: *Seznam surovin (neúplný) - Conto Konfigurátor.*

Následně byly editovány výrobky. Každá položka zde tvoří ID, název, zařazení do určité skupiny zboží, cena a typ výrobku (parametr W značí složený výrobek s odpisem surovin ze skladu).

ID	Název	Zař.	Cena	Typ
807	Hranolky	D009	25,00	W
811	Krokety	D009	32,00	W
816	Tatarka	D009	15,00	W
901	Pizza Hawai	D010	104,00	W
902	Pizza Hawai (1/2)	D010	57,00	W
903	Pizza Kuřecí	D010	117,00	W
904	Pizza Kuřecí (1/2)	D010	64,00	W

Obrázek 121: Seznam výrobků (neúplný) - Conto Konfigurátor.

Po dokončení tabulek byly exportovány pomocí Conto konfigurátoru do příslušné sekce na server pokladního systému.

Cesta k nastavení (Server Conto Konfigurátor):

Prodejní data > Položky > Oddělení [G] > Tabulka - nástroje > Import

Nakonec byly všechny změny uloženy na server.

Cesta k nastavení (Server Conto Konfigurátor):

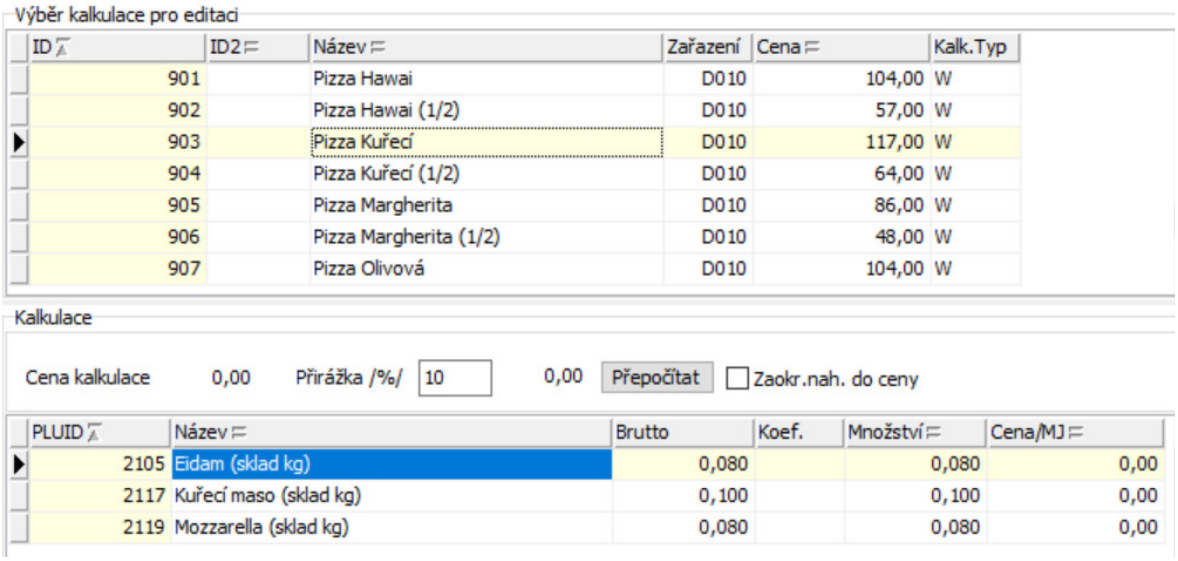
Komunikace > Odeslat data na server (F5)

13.1.5 Vytváření složených výrobků

V třetí fázi byly sestavovány složené výrobky. Ke každému výrobku s parametrem W, jenž značí složený výrobek s odpisem surovin ze skladu, byly dále definovány suroviny v přesném množství, které se ve výrobku vyskytuje. Díky této definici lze analyzovat přibližný stav surovin na skladě.

Cesta k nastavení (Server Conto Konfigurátor):

Sklad > Kalkulace >



Obrázek 122: Vytváření složených výrobků – Conto Konfigurátor.

13.1.6 Konfigurace uživatelských účtů a oprávnění pro jednotlivé zaměstnance

Dle přání majitele restaurace byly sestaveny 2 skupiny uživatelů s různou úrovní oprávnění přístupu k jednotlivým funkcím.

První skupina „Administrátoři“ má plný přístup ke všem funkcím.

Druhá skupina „Obsluha“ má zamezený přístup k systémovým funkcím a příkazům, refundaci položek, obnově již zaplaceného účtu, výmazu zaplaceného účtu, otevírání cizích stolů a všem funkcím konfigurátoru.

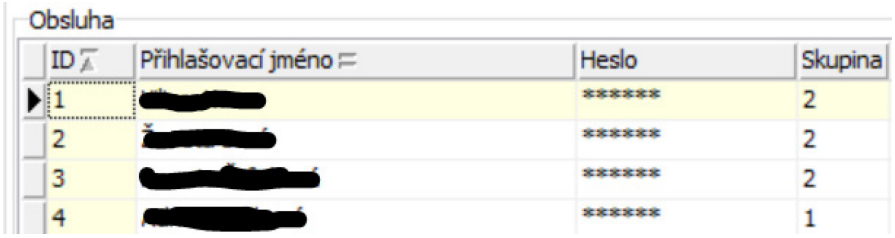
Cesta k nastavení (Server Conto Konfigurátor):

Základní nastavení > Oprávnění > Obsluha > Povolené funkce

Po sestavení skupin byly k těmto skupinám přiřazeni jednotliví uživatelé.

Cesta k nastavení (Server Conto Konfigurátor):

Základní nastavení > Obsluhy > Obsluha > Povolené funkce

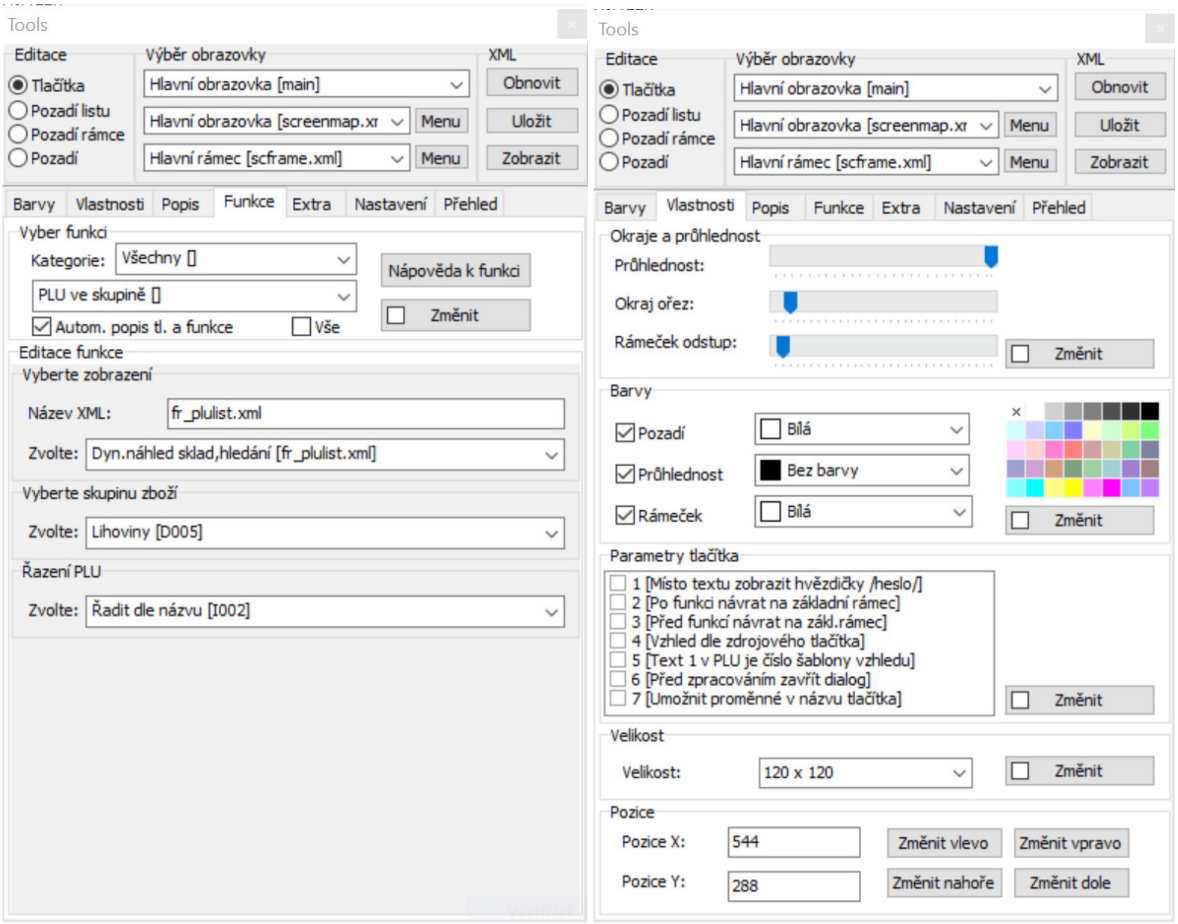


Obrázek 123: Konfigurace uživatelských skupin – Conto Konfigurátor.

13.1.7 Návrh uživatelského prostředí pokladního terminálu

Ve čtvrté fázi bylo sestavováno uživatelské prostředí terminálu, programovány funkce tlačítek, nabídek, mapy stolů v restauraci.

K editaci grafického rozhraní pokladního terminálu slouží okno pro editaci obsahující sadu nástrojů, které je možné použít při editaci obrazovky. Horní část obsahuje funkce pro práci s celým oknem anebo dílčími rámci okna, spodní část obrazovky obsahuje nástroje pro konkrétní nastavení tlačítka nebo rámce obrazovky.



Obrázek 124: Editor prvků grafického rozhraní – Conto Konfigurátor.

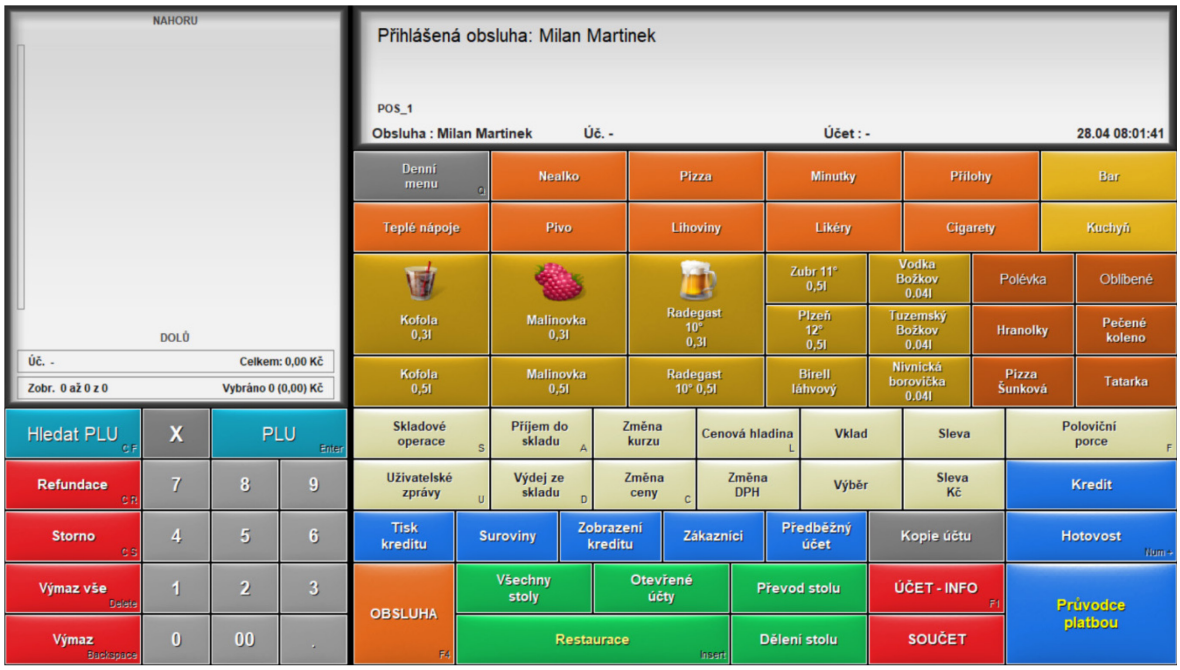
Dále je k dispozici okno se vhledem. V tomto okně je možné upravovat vzhled obrazovky, kterou jste vybrali v okně "Tools" a ty části, které jste zvolili v části "Editace" okna "Tools".

Cesta k nastavení (Server Conto Konfigurátor):

Základní nastavení > Editace klientů > POS_1 > Editace vzhledu > Tools

Pomocí těchto nástrojů společně s nápovědou programu a oficiálním programovacím návodem byly nakonfigurovány funkce i vzhled uživatelského prostředí terminálu, programovány funkce tlačítek, nabídek a mapy stolů v restauraci [56].

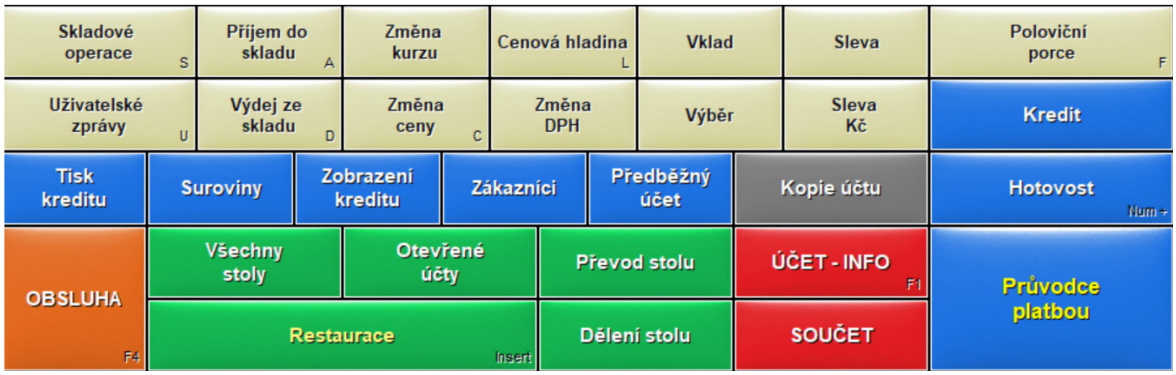
Editace hlavní nabídky:



Obrázek 125: Editovaná část hlavní nabídky – Conto Klient

Obrázek 126: Editovaná část hlavní nabídky (skupiny a oddělení) – Conto Klient

Obrázek 127: Editovaná část hlavní nabídky (zboží přímo) – Conto Klient



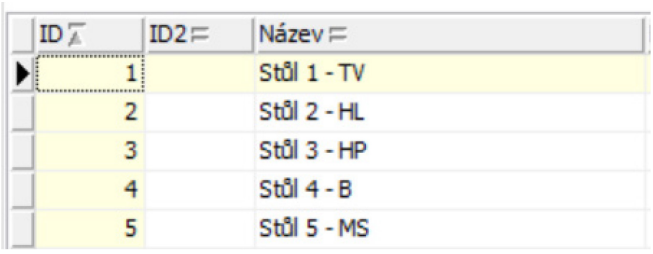
Obrázek 128: Editovaná část hlavní nabídky (funkční tlačítka) – Conto Klient.

Editace nabídky PIZZA

Obrázek 129: Editovaná část skupina položek (Pizza) – Conto Klient

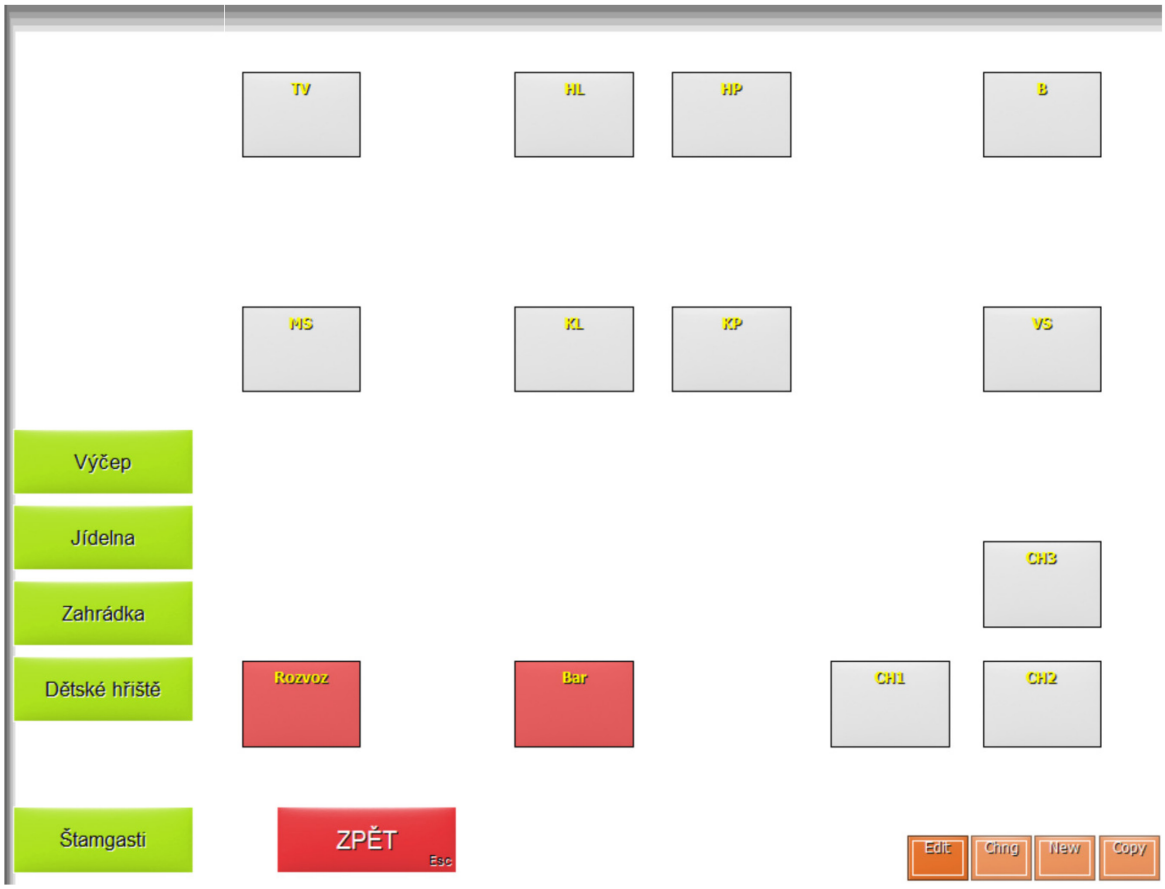
Editace mapy stolů v restauraci: vytvoření seznamu stolů v konfigurátoru, poté v GUI

Cesta k nastavení (Server Conto Konfigurátor): Prodejní data > Stoly >



ID	ID2	Název
1		Stůl 1 - TV
2		Stůl 2 - HL
3		Stůl 3 - HP
4		Stůl 4 - B
5		Stůl 5 - MS

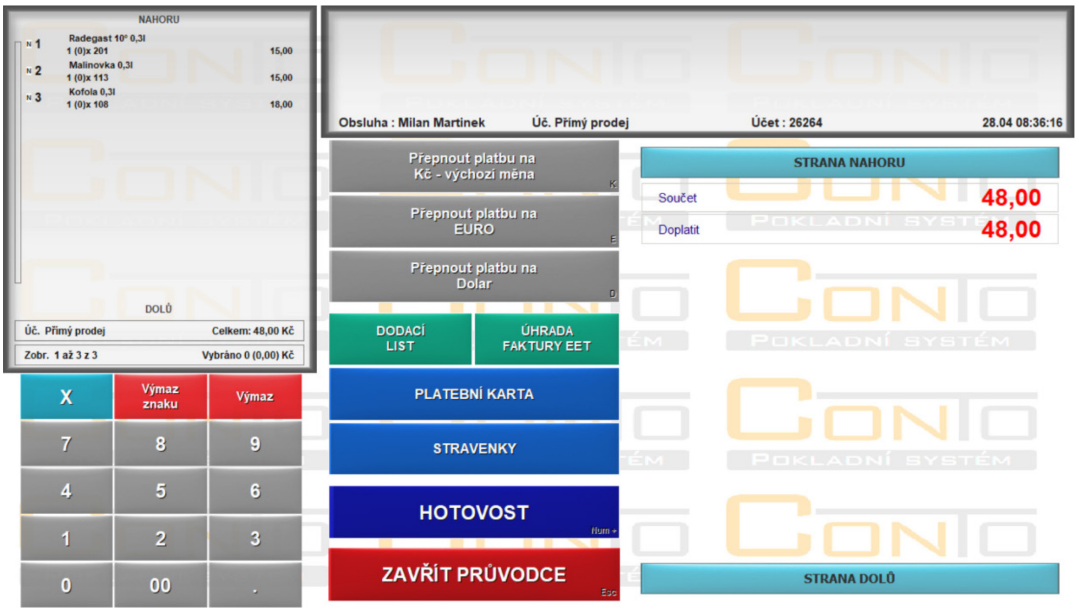
Obrázek 130: Seznam stolů (neúplný) - Conto Konfigurátor.



Obrázek 131: Editace mapy stolů (výčep) – Conto Klient.

Zelená tlačítka přepínají jednotlivé místnosti mapy, tlačítka stolů přesměrují na účet stolu, zároveň zobrazují finanční součet aktuální objednávky a informují o neuzavřeném účtu.

Editace průvodce platbou



Obrázek 132: Editovaná část průvodce platbou – Conto Klient.

13.1.8 Přechod na nový pokladní systém

V páté fázi byl instalován všechen hardware do prostředí restaurace, došlo k zaškolení zaměstnanců a přiřazení jejich osobního pinu k účtu uživatele.

V šesté fázi bylo zahájeno zkušební období, kdy se zaměstnanci seznamovali s novým prostředím a funkcemi pokladního systému.

V sedmé fázi byl na konci měsíce (fakturačního období) po pracovní době provedena konečná migrace z O2 Ekasy na nový pokladní systém Consulta Conto Max.

Nejprve byla smazána veškerá data prodejů, nákupů, počítadla atd. navedená v průběhu testovacího období.

Mazání dat lze vyvolat speciálním kódem v prostředí Conto Klient. Po přihlášení pomocí účtu s administrátorským oprávněním a zadání sekvence X0004 na numerické klávesnici, dojde k vyvolání mazací funkce.

Následně byla provedena kompletní inventura skladových zásob a navedení aktuálního stavu zásob do pokladního systému.

V posledním kroku byla zapnuta komunikace s elektronickou evidencí tržeb Ministerstva financí. Zároveň byl ze starého pokladního systému Ekasa odstraněn EET certifikát. Ekasa samotná byla odpojena, vypnuta a u firmy O2 vypovězena smlouva na předplatné platebního terminálu a pokladního systému.

13.2 Instalace a konfigurace Unifi Controlleru na server jako služba Windows

Unifi Controller byl nainstalován na server LYNX Conto MAX 15". Instalace se skládá z těchto kroků:

1.Stažení a instalace Java verze 8 Update 169 x64.

2.Stažení a instalace Unifi Controlleru 5.7.20 [47].

3.Povolení komunikačních portů ve firewallu (Windows Defender) [57] [16].

Cesta k nastavení (Windows 10):

Win+X > Nastavení > Aktualizace a zabezpečení > Windows Defender > Centrum zabezpečení Windows Defender > Firewall a ochrana sítě > Upřesnit nastavení > Příchozí pravidla > Nové pravidlo:

Popis	Protokol	Port	
Unifi (port TCP pro přesměrování portálu HTTPS)	TCP	8843	Povolit
Unifi (# UDP port použitý pro STUN)	UDP	3478	Povolit
Unifi (místní server TCP port pro DB server)	TCP	27117	Povolit
Unifi (port TCP používaný pro mobilní testování UniFi)	TCP	6789	Povolit
Unifi (port TCP pro GUI / API řadiče, jak je vidět ve webovém prohlížeči)	TCP	8443	Povolit
Unifi (port TCP pro přesměrování HTTP portálu)	TCP	8880	Povolit
Unifi (pro vysílání AP-EDU)	UDP	5656-5699	Povolit
Unifi (TCP port pro komunikaci mezi zařízením a řadičem)	TCP	8080	Povolit
Unifi (port 10001 pro zjišťování AP)	UDP	10001	Povolit

4.Konfigurace softwaru UniFi Controller jako službu systému Windows s cílem vytvořit bezobslužnou, samospustitelnou jednotku.

Nejprve bylo nutno poprvé program otevřít pomocí ikony na ploše nebo v nabídce Start. Jakmile se objeví "UniFi Controller (abc)", můžeme zavřít. Tímto krokem byly vytvořeny potřebné soubory.

Dále byl otevřen příkazový řádek s právy administrátora (Win+X > Windows PowerShell (správce)), zde nejprve pomocí prvního příkazu přejdeme do složky se soubory UniFi v počítači, dále nainstalujeme službu UniFi Controller a nakonec ji spustíme.

```
cd "%UserProfile%\Ubiquiti UniFi\"
java -jar lib\ace.jar installsvc
java -jar lib\ace.jar startsvc
```

Dále je možné provést zkušební spuštění Unifi Controlleru pomocí webového prohlížeče přímo v serveru zadáním adresy **https: //localhost: 8443,** případně z jiného zařízení zadáním přidělené pevné IP adresy serveru z DHCP tudíž **https: //192.168.10.100: 8443** [58].

5.Při prvním spuštění byla zvolena země, časové pásmo, detekováno zařízení Access point Ubiquiti UniFi AP AC LR který byl přidán do seznamu spravovaných zařízení a byla provedena registrace administrátorského účtu Unifi Controlleru.

13.3 Konfigurace RDP s možností více současných relací

Součástí systému Windows 10 je zabudovaná služba RDP pro vzdálené ovládání počítače. Tuto službu lze rozšířit pomocí programu RDP Wrapper. Toto rozšíření umožňuje ponechat

aktivní jeden uživatelský účet systému Windows, zatím co se na další lze vzdáleně napojit pomocí služby RDP.

Součástí instalačního balíku RDPWrap jsou soubory:

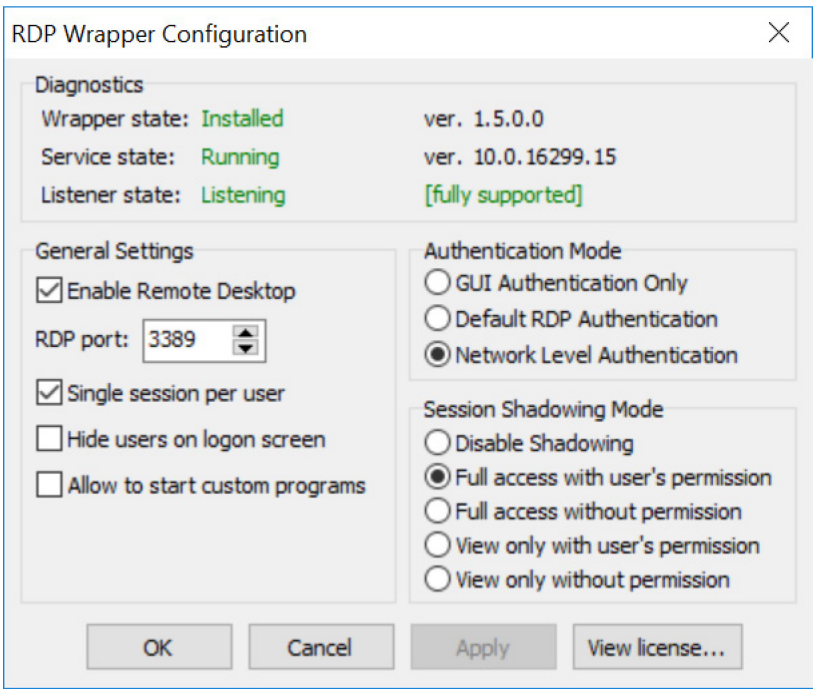
RDPWinst.exe - program pro instalaci / odinstalaci knihovny RDP Wrapper.

RDPConf.exe - nástroj pro konfiguraci RDP wrapper.

RDPCheck.exe - místní kontrola RDP - nástroj pro kontrolu RDP.

install.bat, uninstall.bat, update.bat - dávkové soubory pro instalaci, odinstalování a aktualizaci RDP Wrapper.

Pro instalaci je nutno spustit dávkový soubor install.bat a následně spustit nástroj pro konfiguraci RDPConf.exe, kde by mělo být následující nastavení [59]:



Obrázek 133: Konfigurace RDP Wrapper.

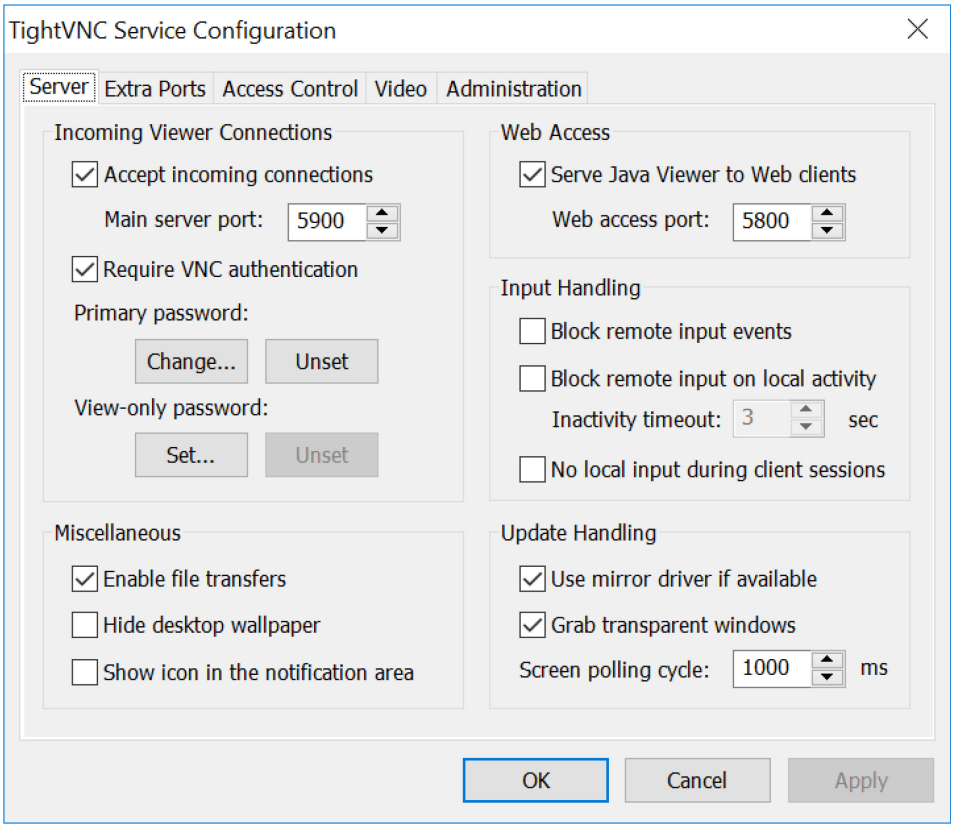
13.4 Konfigurace VNC

Služba VNC byla použita pro vzdálenou podporu zaměstnanců restaurace v případě výskytu problému u aktuálně přihlášeného účtu (zobrazené ploše) s možností vzájemné interakce mezi zaměstnancem a vzdáleným poskytovatelem podpory. Po testování a porovnávání byla pro počítač nakonec zvolena distribuce TightVNC a to hlavně proto, že je multiplatformní,

zdarma, má dobré uživatelské ohlasy, lze spustit jako služba Windows, má dostatečně podrobné nastavení a lze se na něj bez problému napojit všemi VPN klienty jiných výrobců.

Nejprve byl stažen instalační soubor z oficiálních stránek TightVNC [60]. V průběhu instalace je možno zavést VNC server jako službu systému Windows, zvolit instalaci serveru (hostitel), klienta (ovládající) nebo obojí, heslo pro napojení na server (hostitele) a port, na kterém bude server naslouchat. Zabezpečení spojení nebylo nutno řešit, jelikož byl ke vzdálené komunikaci přes internet použit dříve popisovaný OpenVPN tunel a v rámci lokální sítě není potřeba spojení zabezpečovat.

Po instalaci a spuštění serveru bylo zkontrolováno jeho konfigurační okno a provedeno následující nastavení.



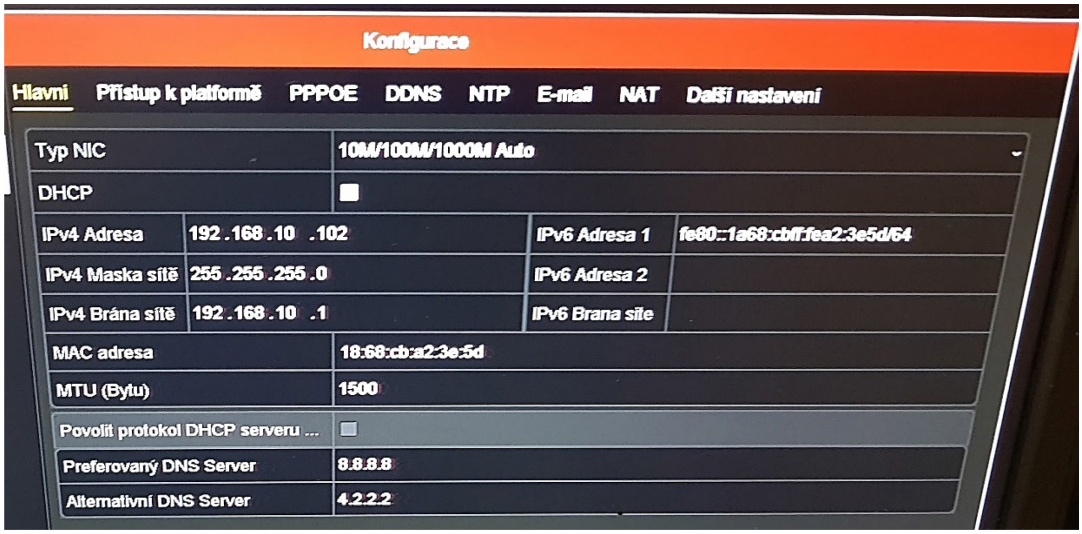
Obrázek 134: TightVNC server – konfigurační okno.

14 KONFIGURACE KAMEROVÉHO SYSTÉMU

14.1 Úvodní nastavení, připojení k síti, inicializace HDD

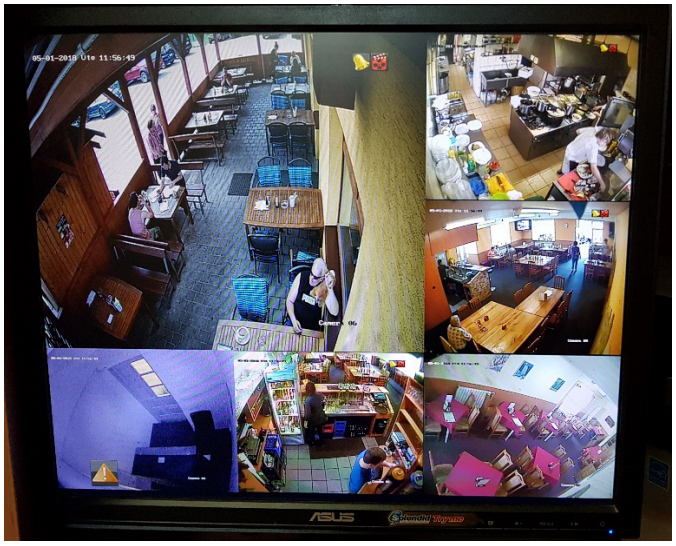
Prvotní nastavení bylo nutno provést pomocí dohledového monitoru a myši. Připojení pomocí sítě přes webové rozhraní bylo zablokováno do doby, než dojde k aktivaci DVR rekordéru. V grafickém prostředí dohledového monitoru byl automaticky po prvním spuštění rekordéru aktivován průvodce nastavením, kde byl založen účet administrátora, grafické gesto pro odemknutí systémového nastavení, byl nastaven čas, vybrán jazyk a došlo k nastavení síťového rozhraní, komunikačních portů a správy HDD.

Při nastavení síťového rozhraní bylo nastaveno načítání síťových údajů z DHCP serveru, dále byly nakonfigurovány komunikační porty serveru 8000, HTTP 88, RTSP 554.



Obrázek 135: Konfigurace DVR – úvodní nastavení sítě.

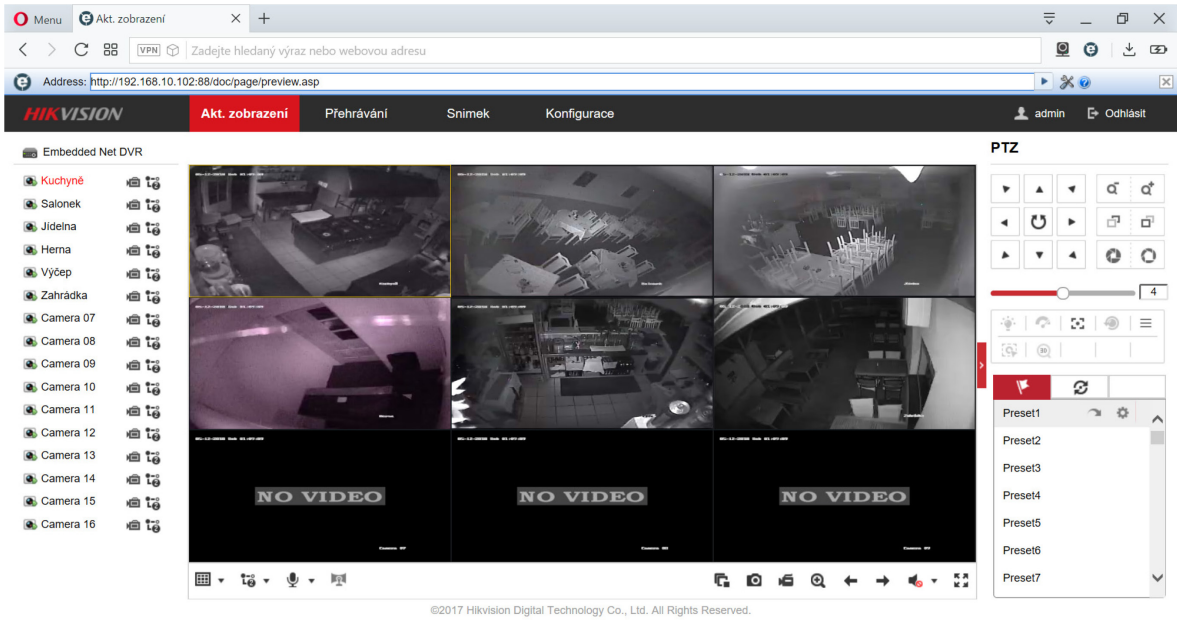
Ve správci HDD byla provedena inicializace, při které byl disk kompletně naformátován. Po dokončení konfigurace skrze průvodce nastavením bylo navoleno rozložení kamer na obrazovce dohledového monitoru.



Obrázek 136: Konfigurace rozložení kamer na dohledovém monitoru.

14.2 Konfigurace připojení k webovému rozhraní DVR rekordéru

Pro zobrazení video streamu pomocí posledních verzí oblíbených internetových prohlížečů Google Chrome, Mozilla Firefox a Opera bylo nutné nainstalovat doplněk IE Tab. Tento doplněk zobrazí v prostředí prohlížeče novou záložku s oknem vykreslovaným pomocí jádra prohlížeče Internet Explorer. Internet Explorer již jako jediný zachovává podporu NPAPI (Netscape Plugin Application Programming Interface). Tento plugin staršího data potřebný pro přenos videa byl vyhodnocen jako bezpečnostní riziko a z toho důvodu jej většina prohlížečů začala blokovat. Přesto ho většina kamerových systémů stále používá.



Obrázek 137: Webové rozhraní DVR Rekordéru – Aktuální zobrazení.

Doplněk IE Tab byl nalezen a nainstalován pomocí Chrome Web Store [61]. Po dokončení instalace se v prohlížeči vedle panelu zadávání adres zobrazí nová ikona aplikace. Po stisku ikony se zobrazí nová karta prohlížeče, na této kartě se v horní části zobrazí vedlejší panel pro zadání adresy. Do panelu byla zadána IP DVR rekordéru: **http://192.168.10.102:88/**.

Do přihlašovacího okna webového rozhraní byly zadány přihlašovací údaje již dříve založeného administrátorského účtu.

14.3 Aktualizace firmware, přidání uživatelských účtů

Po prvním přihlášení do webového rozhraní byl aktualizován firmware stažený ze stránek výrobce [41].

Cesta k nastavení (DVR rekordér Webové rozhraní):

Konfigurace > Systém > Údržba > Aktualizace > Procházet

Dále byly vytvořeny uživatelské účty pro personál. Byly odlišeny 3 skupiny. První z nich je administrátor s veškerým oprávněním. Druhá skupina byli Operátoři, kterým byla zamezena konfigurace systému, nahrávání i kamer. Třetí skupina Uživatelé, kterým byla zamezena konfigurace a ukládání nebo přehrávání záznamu kamer.

Cesta k nastavení (DVR rekordér Webové rozhraní):

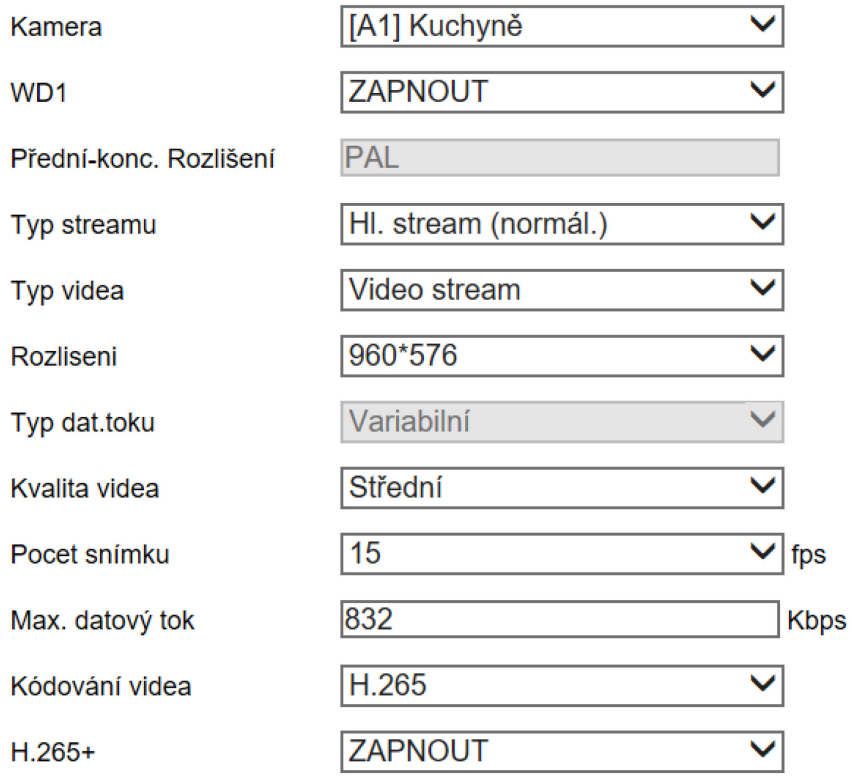
Konfigurace > Systém > Údržba > Management účtů > Přidat

14.4 Konfigurace kamer

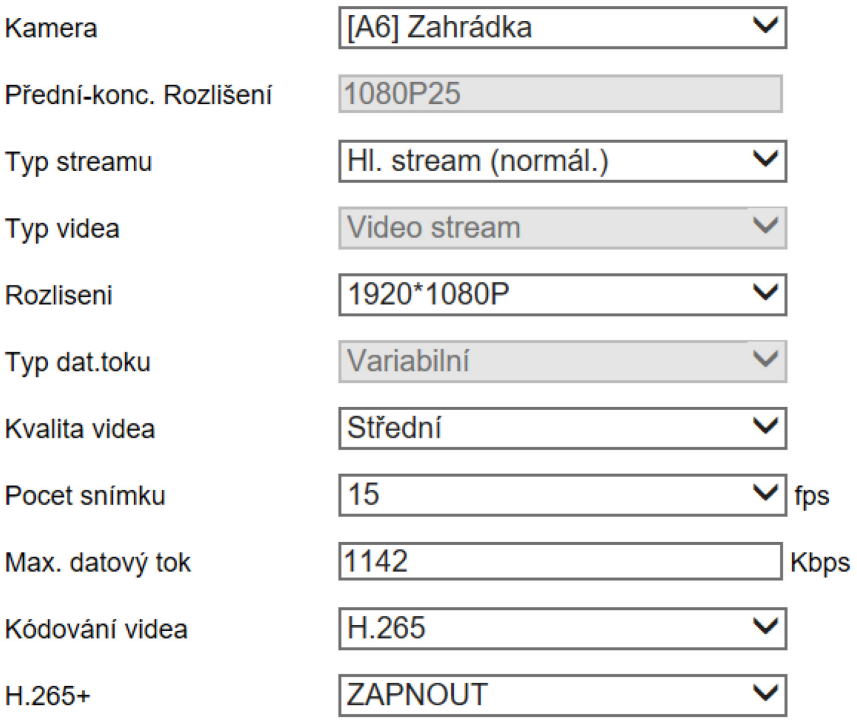
Při konfiguraci byly nastavovány 2 druhy kamer. Prvních 5 kamer je původních (Avtech KPC 139 ZEP) a následně šestá moderní kamera Hikvision DS-2CE16D8T-IT/28, která se bude postupně rozšiřovat do všech 16 kamerových vstupů.

Cesta k nastavení (DVR rekordér Webové rozhraní):

Konfigurace > Video a audio > Video > Kamera



Obrázek 138: Konfigurace kamery Avtech KPC 139 ZEP.



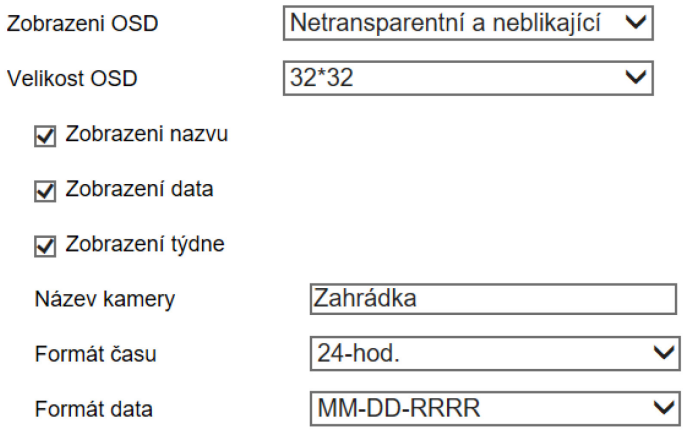
Obrázek 139: Konfigurace kamery Hikvision DS-2CE16D8T-IT/28.

Dále byly kamery pojmenovány a nastaveno zobrazení údajů v obrazu kamery.

Cesta k nastavení (DVR rekordér Webové rozhraní):

Konfigurace > Snímek > Nastavení OSD > Kamera

Obrázek 140: Konfigurace rozmístění údajů v obrazu kamery.



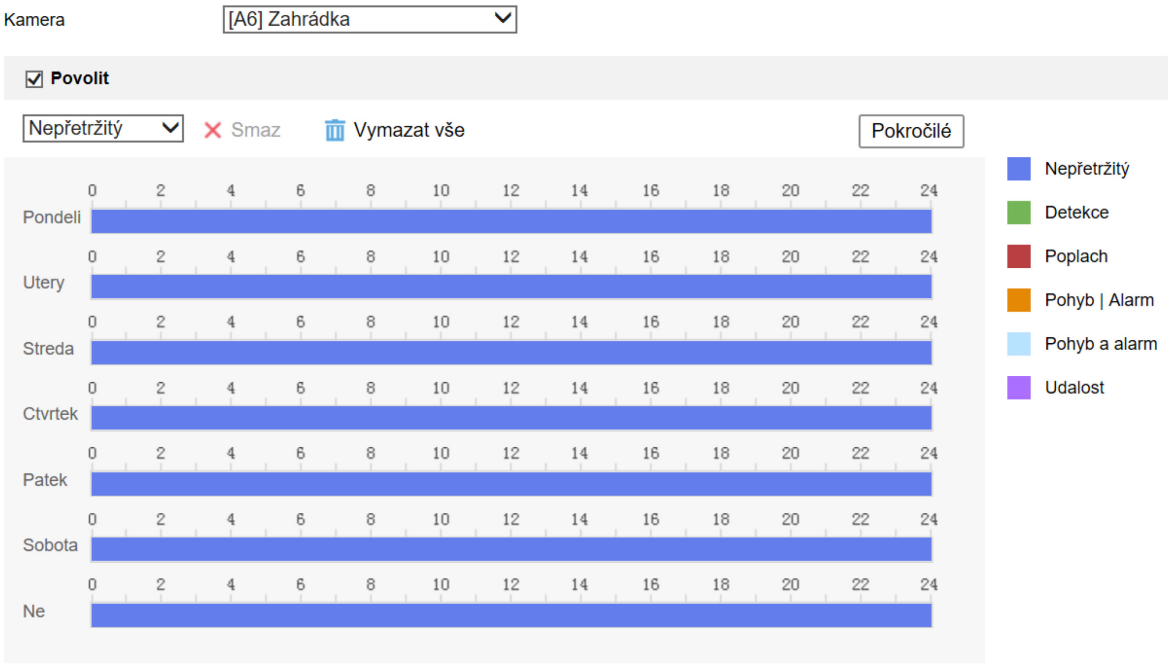
Obrázek 141: Konfigurace údajů v obrazu kamery.

14.5 Konfigurace záznamu a detekce pohybu

Při konfiguraci záznamu kamer byl nastaven na všech šesti kamerách nepřetržitý nonstop záznam. Bylo tak rozhodnuto kvůli využití kodeku h.265+. Tento kodek byl popsán v teoretické části. Jeho hlavní výhodou oproti i tak velmi úspornému h.265 je, že při natáčení statického a neměnného obrazu se sníží datový tok na úplné minimum.

Cesta k nastavení (DVR rekordér Webové rozhraní):

Konfigurace > Úložiště > Nastavení rozvrhu > Kamera >



Obrázek 142: Konfigurace záznamu kamer DVR rekordéru.

Nakonec byla nakonfigurována detekce pohybu pro lepší orientaci podle událostí při sledování záznamu kamer.

Cesta k nastavení (DVR rekordér Webové rozhraní):

Konfigurace > Události > Události > Detekce > Kamera > Zapnout detekci pohybu

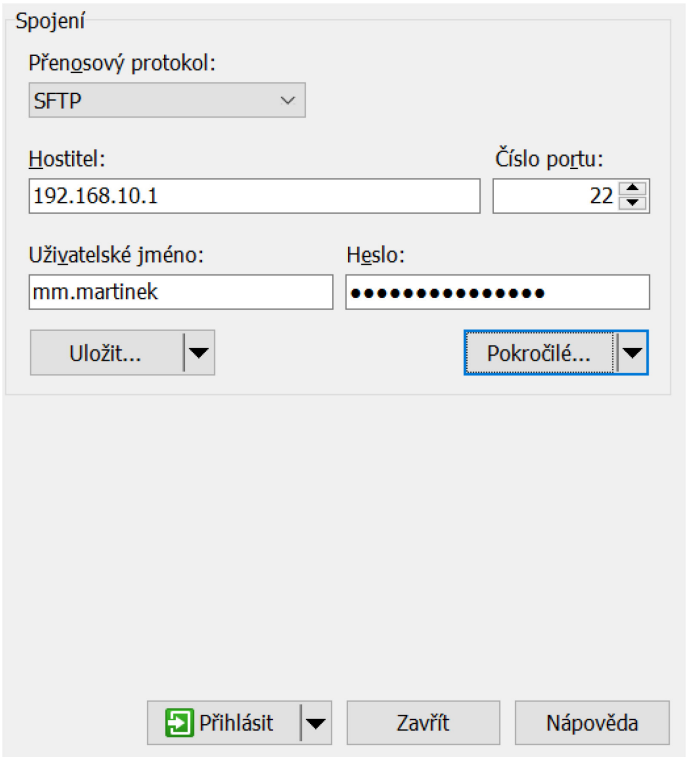
15 KONFIGURACE KONCOVÝCH ZAŘÍZENÍ

Tato část práce se zabývá konfigurací koncových zařízení a to primárně jejich připojením do firemní sítě, včetně využití služeb této sítě (kamerový systém, vzdálená správa serveru, pokladního systému atd.).

15.1 Připojení k OpenVPN serveru

15.1.1 Stažení certifikátů z adresáře routeru

Pro stažení certifikátů vytvořených v části konfigurace OpenVPN serveru lze využít jakýkoliv SFTP (SSH File Transfer Protocol) klient. Proto byl využit program WinSCP , který je zcela zdarma a určen pro platformu Windows [62]. Po instalaci bylo nutno zajistit dosah připojení do VLAN, ve které je router umístěn. Dále bylo nakonfigurováno nové spojení, kdy po spuštění programu bylo vyvoláno dialogové okno:



Obrázek 143: Navázání SFTP spojení s routerem pomocí WinSCP.

Po navázání spojení byl zobrazen adresář /config /auth a přenesen soubor cacert.pem společně s veřejným a soukromým klíčem příslušného uživatele, který se potřebuje připojit k OpenVPN serveru.

15.1.2 Vytvoření konfiguračního souboru klienta

Do textového souboru byla vložena následující konfigurace:

```
client        // konfigurace klienta
dev tun       // realizace tunelu na 3. síťové vrstvě (modelu OSI)
proto udp     //využití nepotvrzovaného přenosového protokolu UDP
remote 188.244.XX.XXX 1194 //veřejná IP serveru a port OpenVPN


float         //povolení přijímání ověřených paketů z libovolné IP
resolv-retry infinite //zajistí neomezenou dobu pokusů o opětovné
                      připojení v případě ztráty komunikace, užitečné
                      pokud se klient připojuje z nespolehlivých sítí
nobind        // klient není vázán na lokální adresu a port a je mu při
                dělen dynamicky
persist-key   //Neumožní znovu přečíst soubory klíčů při restartu.
persist-tun   //Nezavře a znovu otevře zařízení TUN / TAP při restartu.
verb 3        // Nastavení počtu detailů v logu konzole OpenVPN


auth SHA256    //kontrola integrity dat pomocí hashovací funkce SHA256
cipher AES-256-CBC // šifrování přenášených dat symetrickou šifrou AES
comp-lzo yes   //komprimace přenášených dat pro úsporu datového toku


//odkaz na názvy souborů certifikátů ve složce s konfiguračním souborem
ca cacert.pem //certifikát certifikační autority (veřejný klíč CA),
                sloužící k ověření pravosti veřejných klíčů,
                aktuálně podepsán pomocí OpenSSL (self-signed)
cert ADMIN.pem //certifikát klienta (šiřitelný veřejný klíč)
key ADMIN.key  //privátní klíč klienta (nutno držet v tajnosti) [55]
```

Tento soubor byl následně uložen a přejmenován na config.ovpn.

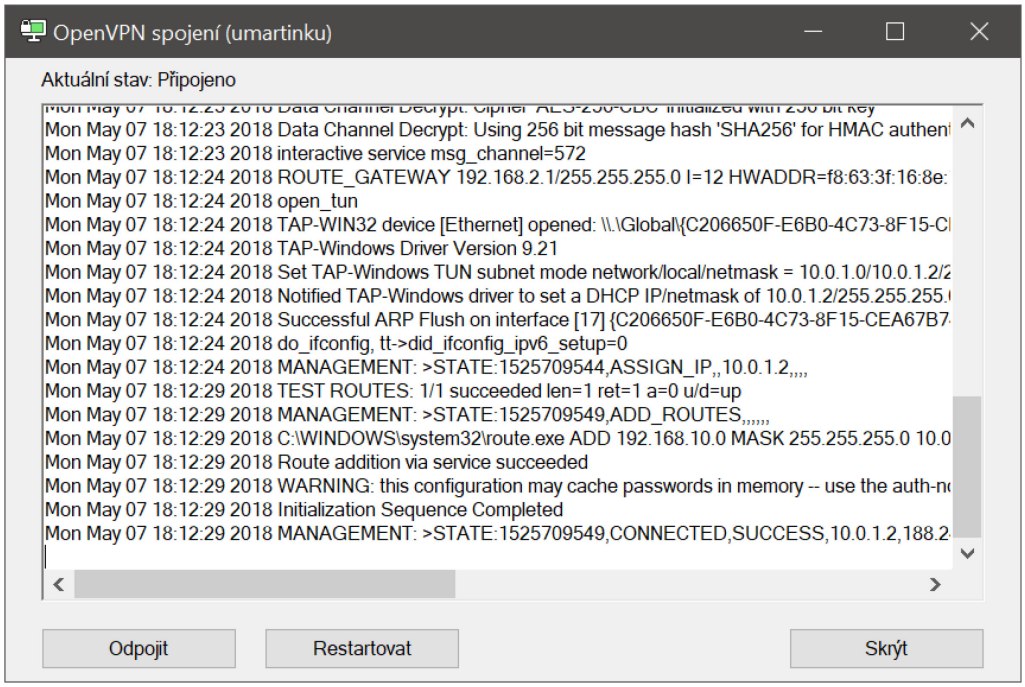
15.1.3 Konfigurace OpenVPN klienta

Nejprve byl stažen a nainstalován program OpenVPN z oficiálních Internetových stránek služby. Byl vybrán instalační soubor podle typu a verze systému včetně bitové varianty (x86, x64).

V adresáři C:\Program Files\OpenVPN\config byla vytvořena složka s názvem firmy a do ni byl vložen konfigurační soubor config.ovpn, veřejný klíč certifikační autority cacert.pem, společně s veřejným a soukromým klíčem příslušného uživatele. Je důležité, aby při přesunu souborů nebyl použit nešifrovaný internetový přenos z důvodu možného narušení bezpečnosti spojení v případě odcizení certifikátů.

Dále byl spuštěn program. Pomocí ikony v oznamovací oblasti vedle ukazatele času vyvoláme kontextové menu a zvolíme umartinku/Připojit.

Otevře se nám okno s log údaji o navazování komunikace, pokud vše proběhne úspěšně, poznáme na první pohled zelenou ikonu OpenVPN.



Obrázek 144: OpenVPN - Přihlášení k OpenVPN serveru.

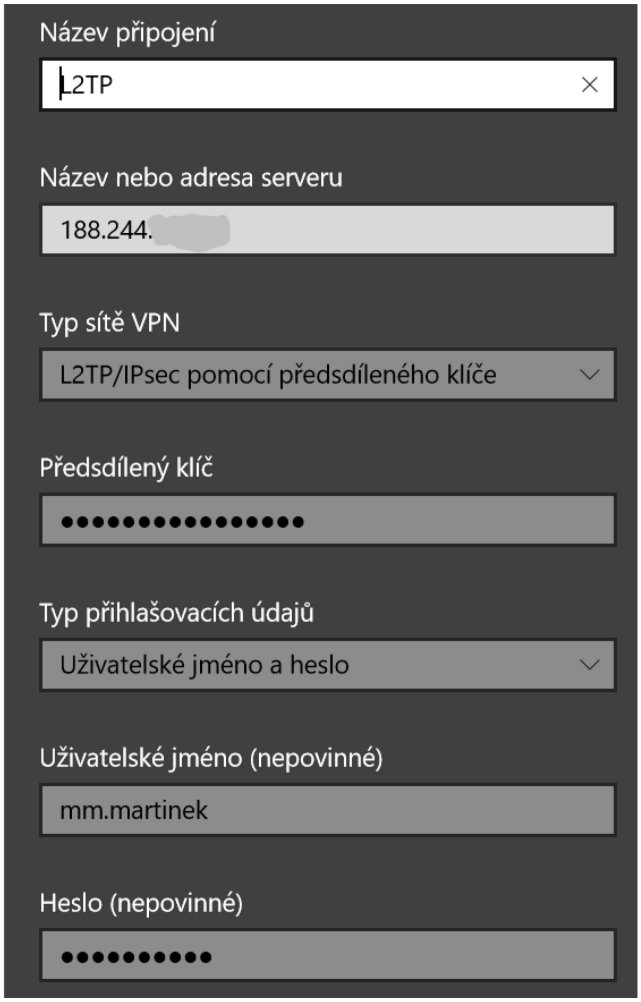
15.2 Připojení k L2TP IPsec VPN serveru

Pro připojení k L2TP IPsec VPN serveru byl využit nativní klient systému Windows 10.

15.2.1 Konfigurace L2TP IPsec VPN

Cesta k nastavení (Windows 10):

Win+X > Síťová připojení > VPN > Přidat připojení VPN >



Obrázek 145: Konfigurace L2TP IPsec VPN spojení ve Windows 10.

Win+X > Síťová připojení > Změnit možnosti adaptéru > L2TP > Vlastnosti >Zabezpečení > Povolit tyto protokoly > Protokol MS-CHAP v2 (Microsoft CHAP verze 2) > OK

15.2.2 Připojení k L2TP IPsec VPN

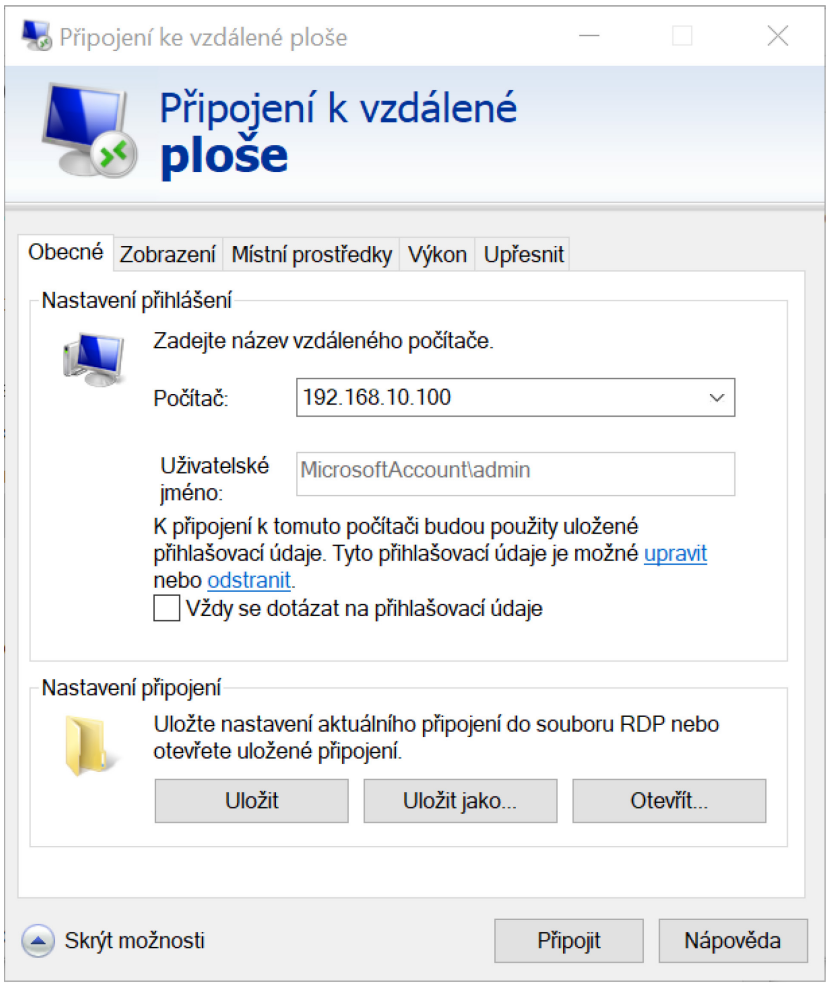
Všechny VPN sítě nakonfigurované pomoci nativního klienta ve Windows 10 jsou zobrazeny v kontextovém menu s přehledem okolních WiFi sítí. Stačí tedy zvolit síť L2TP a dát připojit.

15.3 Připojení k RDP serveru

Na počítač, který se bude k RDP serveru připojovat, není nutno instalovat žádný dodatečný software klienta. Klient Připojení ke vzdálené ploše je součástí všech aktuálních edic systému Microsoft Windows.

Cesta k programu (Windows 10):

Start > Příslušenství Windows > Připojení ke vzdálené ploše >



Obrázek 146: Konfigurace Připojení ke vzdálené ploše.

Zde je nutno zadat IP adresu serveru a přihlašovací údaje uživatelského účtu systému Windows, na který je potřeba se připojit.

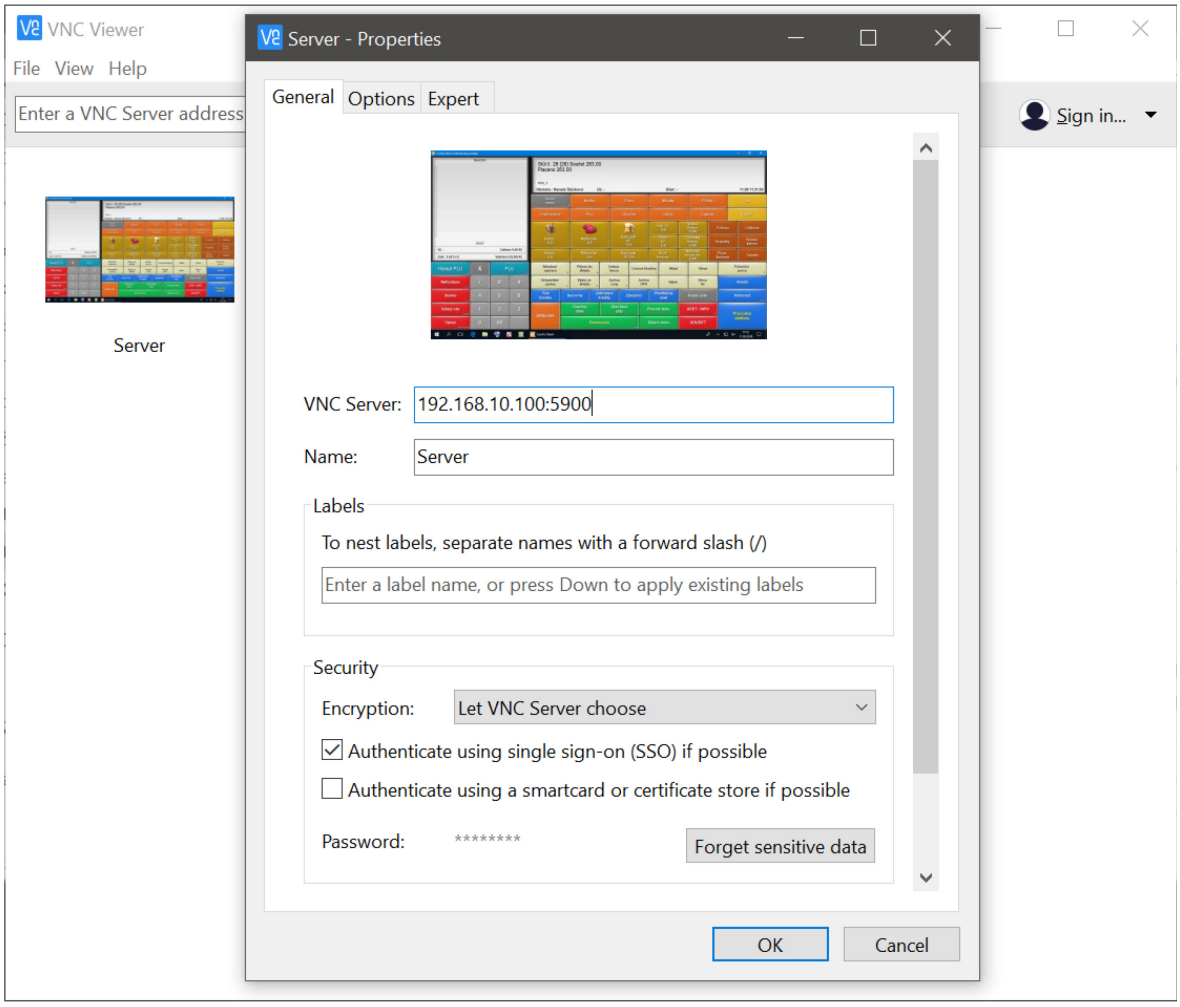
15.4 Připojení k VNC serveru

Na počítač, který se bude k VNC serveru připojovat, byl nainstalován VNC klient od společnosti RealVNC [63]. Po otestování několika VNC klientů byl tento vyhodnocen jako nejlepší. Podporuje TightVNC server, lze si vytvořit seznam spravovaných zařízení a má v případě potřeby podrobné možnosti konfigurace. Pokud by byla internetová konektivita nedostatečná a obraz by se sekal, lze v nastavení snížit kvalitu (rozlišení, barevná hloubka…).

Po úspěšné instalaci RealVNC klienta byl v případě potřeby vzdálené komunikace spuštěn OpenVPN (nebo L2TP IPsec) tunel, který byl dříve nakonfigurován a nyní slouží jako bezpečné spojení mezi zařízením ve WAN a lokálním serverem v LAN síti restaurace. Nakonec byl spuštěn RealVNC klient a bylo nakonfigurováno spojení:

VNC server = lokální_ip_serveru:vncport

Password = heslo



Obrázek 147: RealVNC klient – přihlašovací okno.

ZÁVĚR

Cílem práce bylo navrhnout, vybudovat a nakonfigurovat moderní zabezpečenou firemní síť, pokladní systém se skladovým hospodářstvím, platebním terminálem napojeným na EET, dohledovým kamerovým systémem a vzdálenou správou těchto systémů.

Všechny cíle, které byly stanoveny, se podařilo úspěšně dokončit. Zároveň byl při návrhu i vytváření kladen důraz na co nejoptimálnější funkcionalitu a využitelnost všech systémů v reálném provozu restauračního zařízení. Z toho důvodu je výsledný popis obsáhlejší, než bylo původně zamýšleno.

Jediným větším úskalím z průběhu vytváření práce byla časová náročnost celkové tvorby. Ostatní drobné problémy byly vyřešeny dostudováním dané problematiky, případně konzultací s vedoucím diplomové práce panem Ing. Jiřím Korbelem, Ph.D.

V blízké budoucnosti je plánováno rozšíření projektu. Po dokončení probíhající rekonstrukce a rozšíření objektu restaurace bude zvýšen počet moderních CCTV kamer Hikvision DS-2CE16D8T-IT/28 a zároveň bude nahrazeno všech 5 zbývajících původních kamer na tento nový model. V konečném stavu bude využito všech 16 kamerových vstupů DVR rekordéru s možností záznamu na plánovaných 9 dní.

Zároveň bude dokoupen další Access point Ubiquiti UniFi AP AC LR pro zajištění optimálního pokrytí firemní WLAN sítě i v nově přistaveném druhém patře objektu.

BIBLIOGRAFIE

[1] SOSINSKY, Barrie. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: Computer Press, 2010. Mistrovství (Computer Press). ISBN 978-80-251-3363-7.

[2] MARTINEK, Milan. *Moderní domácí síť*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2016, 98 s. (142 877 znaků). Dostupné také z: http://hdl.handle.net/10563/38807. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav automatizace a řídicí techniky. Vedoucí práce Matýsek, Miroslav.

[3] MATÝSEK, Miroslav. *Počítačové sítě: UČEBNÍ PREZENTACE UTB FAI ÚPKS* [online]. 04.05.2016. 2016 [cit. 2017-12-01]. Dostupné z: http://vyuka.fai.utb.cz/course/view.php?id=71

[4] SHINDER, Debra. *Počítačové sítě: nepostradatelná prírucka k pochopení sítové teorie, implementace a vnitrních funkcí [sic]*. Praha: SoftPress, 2003. Cisco systems. ISBN 80-86497-55-0.

[5] Nový standard Wi-Fi: Gigabit vzduchem. *Zive.cz* [online]. b.r. [cit. 2018-04-21]. Dostupné z: https://www.zive.cz/clanky/novy-standard-wi-fi-gigabit-vzduchem/sc-3-a-165687/

[6] Wi-Fi sítě - vše co jste kdy chtěli vědět 1/2. *Pctuning.tyden.cz* [online]. b.r. [cit. 2018-04-21]. Dostupné z: https://pctuning.tyden.cz/hardware/site-a-internet/11138?start=2

[7] Wi-Fi: Jak si zajistit velké pokrytí, rychlost a silný signál. *Zive.cz* [online]. b.r. [cit. 2018-04-21]. Dostupné z: http://www.zive.cz/clanky/wi-fi-jak-si-zajistit-velke-pokryti-rychlost-a-silny-signal/wi-fi-standardy-nastaveni-kanalu-rozsireni-rozsahu/sc-3-a-172347-ch-90932/default.aspx#articleStart

[8] Wszystko co musisz wiedzieć o dwupasmowym Wi-Fi. *Komputerswiat.pl* [online]. b.r. [cit. 2018-04-21]. Dostupné z: http://www.komputerswiat.pl/poradniki/sprzet/siec-domowa/2013/05/wi-fi-na-dwoch-pasmach.aspx

[9] Optimising mobile networks with MIMO and DAS. *Analog-eetimes.com* [online]. b.r. [cit. 2018-04-21]. Dostupné z: http://www.analog-eetimes.com/content/optimising-mobile-networks-mimo-and-das

[10] KRČMÁŘ, Petr. *Linux: postavte si počítačovou síť*. 1. vyd. Praha: Grada, 2008. Průvodce (Grada). ISBN 978-80-247-1290-1.

[11] Srovnání VPN Protokolů: PPTP vs. L2TP vs. OpenVPN vs. SSTP vs. IKEv2. *Vpnmentor.com* [online]. b.r. [cit. 2018-04-21]. Dostupné z: https://cs.vpnmentor.com/blog/srovnani-vpn-protokolu-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

[12] KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

[13] Remote Desktop Protocol (Windows). *Msdn.microsoft.com* [online]. b.r. [cit. 2018-04-22]. Dostupné z: https://msdn.microsoft.com/cs-cz/library/windows/desktop/aa383015(v=vs.85).aspx

[14] Základy WiFi: jak zabezpečit bezdrátovou síť?. *Pctuning.tyden.cz* [online]. b.r. [cit. 2017-12-01]. Dostupné z: https://pctuning.tyden.cz/hardware/site-a-internet/7660-zaklady_wifi-jak_zabezpecit_bezdratovou_sit?start=2

[15] MALANÍK, David. *Bezpečnost bezdrátových sítí. Možnosti bezdrátového spojení. Typy zabezpečení. Odolnost vůči průniku. Autorizační metody.* [online]. b.r. [cit. 2017-12-01]. Dostupné z: http://vyuka.fai.utb.cz/mod/resource/view.php?id=6222

[16] KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. První vydání. Praha: Grada Publishing, a.s., 2015. Průvodce (Grada). ISBN 978-80-247-5453-6.

[17] *Wireless Network Security: Wireless Networks and Mobile Computing* [online]. b.r. [cit. 2017-12-03]. Dostupné z: www.uottawa.ca

[18] Bezpečnost WiFi záleží jen na vás. *Lupa.cz* [online]. b.r. [cit. 2017-12-01]. Dostupné z: https://www.lupa.cz/clanky/bezpecnost-wifi-zalezi-jen-na-vas/

[19] Bezpečnost WLAN podle IEEE. *Lupa.cz* [online]. b.r. [cit. 2017-12-01]. Dostupné z: https://www.lupa.cz/clanky/bezpecnost-wlan-podle-ieee/

[20] *Intro to Networking - AAA, 802.1X, EAP & RADIUS: 802.1X Authentication End-to-End* [online]. b.r. [cit. 2017-12-03]. Dostupné z: https://help.ubnt.com/hc/en-us/articles/115007253447-Intro-to-Networking-AAA-802-1X-EAP-RADIUS

[21] 802.1X - autentizace v počítačových sítích. *Webserver.ics.muni.cz* [online]. b.r. [cit. 2017-12-03]. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/590.html

[22] MATÝSEK, Miroslav. *PROVOZ POČÍTAČOVÝCH SÍTÍ: UČEBNÍ PREZENTACE UTB FAI ÚPKS* [online]. 2016 [cit. 2017-12-03].

[23] Technické pojmy používané v oblasti kamerových systémov. *Alertech.sk* [online]. b.r. [cit. 2018-04-30]. Dostupné z: https://www.alertech.sk/technicke-pojmy

[24] H.265+: Komprese H.265+ zahajuje éru Technologie 4K. *Express-alarm.cz* [online]. b.r. [cit. 2018-04-30]. Dostupné z: https://www.express-alarm.cz/?p=205/h265

[25] Hikvision Advanced Imaging Technology -- WDR, 3DDNR & Low-light. *Youtube.com* [online]. 2013 [cit. 2018-04-30]. Dostupné z: https://www.youtube.com/watch?v=iIs-vpbpI3k

[26] Stanovisko č. 1/2016 - Umístění kamerových systémů v bytových domech (nové): Úřad pro ochranu osobních údajů. *Uoou.cz* [online]. 2018 [cit. 2018-04-29]. Dostupné z: https://www.uoou.cz/stanovisko-c-1-2016-umisteni-kamerovych-systemu-v-bytovych-domech-nove/d-29507

[27] Elektronická evidence tržeb. *Etrzby.cz* [online]. b.r. [cit. 2018-04-29]. Dostupné z: http://www.etrzby.cz/cs/index

[28] Způsoby evidence a účtenka. *Etrzby.cz* [online]. b.r. [cit. 2018-04-29]. Dostupné z: http://www.etrzby.cz/cs/zpusoby-evidence-a-uctenka

[29] *Eaton 5E UPS: Essential line interactive UPS* [online]. 2013 [cit. 2018-04-23]. Dostupné z: http://pqlit.eaton.com/ll_download_bylitcode.asp?doc_id=26070

[30] Gigabitový média konvertor sítě Ethernet MC220L. *Tp-link.com* [online]. b.r. [cit. 2018-04-24]. Dostupné z: https://www.tp-link.com/cz/products/details/cat-43_MC220L.html#overview

[31] Obousměrný SPF modul WDM TL-SM321A. *Tp-link.com* [online]. b.r. [cit. 2018-04-24]. Dostupné z: https://www.tp-link.com/cz/products/details/cat-43_TL-SM321A.html

[32] *Ubiquiti PoE Adapters Datasheet* [online]. 2018 [cit. 2018-04-26]. Dostupné z: https://dl.ubnt.com/datasheets/poe/PoE_Adapters_DS.pdf

[33] *EdgeRouter X Datasheet* [online]. 2017 [cit. 2018-04-27]. Dostupné z: https://dl.ubnt.com/datasheets/edgemax/EdgeRouter_X_DS.pdf

[34] *UniFi AC AP Datasheet* [online]. 2018 [cit. 2018-04-28]. Dostupné z: https://dl.ubnt.com/datasheets/unifi/UniFi_AC_APs_DS.pdf

[35] Pořiďte si O2 eKasu, nejpoužívanější EET pokladnu. *O2.cz* [online]. b.r. [cit. 2018-04-08]. Dostupné z: https://www.o2.cz/podnikatel/elektronicka-evidence-trzeb

[36] Dotykačka - pokladní systémy a registrační pokladny pro EET. *Dotykacka.cz* [online]. b.r. [cit. 2018-04-09]. Dostupné z: https://www.dotykacka.cz

[37] Pokladní software Conto Max. *Consulta.cz* [online]. b.r. [cit. 2018-04-08]. Dostupné z: http://www.consulta.cz/pokladni-software-conto-max

[38] Epson TM-T20II: Ethernet, PS, EDG, EU - Epson. *Epson.cz* [online]. b.r. [cit. 2018-04-29]. Dostupné z: https://www.epson.cz/viewcon/corporatesite/products/mainunits/overview/20641

[39] *Verifone VX675 datasheet* [online]. 2017 [cit. 2018-04-29]. Dostupné z: https://www.verifone.com/sites/default/files/2017-12/vx675_datasheet_a4_042617.pdf

[40] *DVR specifications K series Datasheet of DS7200HQHIK2* [online]. 2017 [cit. 2018-05-01]. Dostupné z: https://www.hikvision.com/uploadfile/image/10885_DDVRspecKseriesDatasheetofDS7200HQHIK2.pdf

[41] Hikvision Europe Download Tools: Storage and Network Calculator. *Hikvision.com* [online]. b.r. [cit. 2018-05-02]. Dostupné z: http://overseas.hikvision.com/Europe/tools_82.html

[42] *WD Purple Series Spec Sheet* [online]. 2017 [cit. 2018-05-02]. Dostupné z: https://www.wdc.com/content/dam/wdc/website/downloadable_assets/eng/spec_data_sheet/2879-800012.pdf

[43] *CCTV AVTech KPC 139 ZEP Datasheet* [online]. b.r. [cit. 2018-05-01]. Dostupné z: http://multiperkasa.com/pdf/KPC-139-Zep.pdf?file_id=2

[44] *DS-2CE16D8T-IT 2 MP Ultra Low-Light EXIR Bullet Camera Datasheet* [online]. 2017 [cit. 2018-05-02]. Dostupné z: https://www.hikvision.com/uploadfile/image/10815_DAnalogspecD8TDatasheetofDS2CE16D8TIT.pdf

[45] 9 Port Power Supply CCTV Camera Power | Security Camera Power Adapter. *Zmodo.com* [online]. b.r. [cit. 2018-05-02]. Dostupné z: http://surveillance.zmodo.com/security-camera-power-adapter-pa-1059.html

[46] Jak instalovat kamerový systém (AHD, TVI, CVI, Analog) I Nejkam.cz I Specialisté na kamerové systémy. *Nejkam.cz* [online]. b.r. [cit. 2018-05-03]. Dostupné z: https://www.nejkam.cz/a/jak-instalovat-kamerovy-system

[47] Ubiquiti Networks - Downloads. *Ubnt.com* [online]. b.r. [cit. 2018-05-05]. Dostupné z: https://www.ubnt.com/download/

[48] Download PuTTY - a free SSH and telnet client for Windows. *Putty.org* [online]. b.r. [cit. 2018-05-05]. Dostupné z: https://www.putty.org

[49] EdgeRouter - Hardware Offloading Explained – Ubiquiti Networks Support and Help Center. *Ubnt.com* [online]. b.r. [cit. 2018-05-05]. Dostupné z: https://help.ubnt.com/hc/en-us/articles/115006567467

[50] Duck DNS. *Duckdns.org* [online]. b.r. [cit. 2018-05-05]. Dostupné z: https://www.duckdns.org/index.jsp

[51] DuckDNS on EdgeRouter. *Loganmarchione.com* [online]. b.r. [cit. 2018-05-05]. Dostupné z: https://loganmarchione.com/2017/04/duckdns-on-edgerouter/

[52] EdgeRouter - How to Protect a Guest Network – Ubiquiti Networks Support and Help Center. *Ubnt.com* [online]. b.r. [cit. 2018-05-07]. Dostupné z: https://help.ubnt.com/hc/en-us/articles/218889067-EdgeRouter-How-to-Protect-a-Guest-Network

[53] EdgeRouter - L2TP IPsec VPN Server – Ubiquiti Networks Support and Help Center. *Ubnt.com* [online]. b.r. [cit. 2018-05-07]. Dostupné z: https://help.ubnt.com/hc/en-us/articles/204950294

[54] EdgeRouter - OpenVPN Server – Ubiquiti Networks Support and Help Center. *Ubnt.com* [online]. b.r. [cit. 2018-05-07]. Dostupné z: https://help.ubnt.com/hc/en-us/articles/115015971688-EdgeRouter-OpenVPN-Server

[55] OpenVPN on Ubiquiti EdgeRouter – Dev Notes. *Daywiss.wordpress.com* [online]. b.r. [cit. 2018-05-07]. Dostupné z: https://daywiss.wordpress.com/2015/07/23/openvpn-on-ubiquiti-edgerouter/

[56] *Uživatelský manuál Conto POS systém: Programovací manuál*. 2.0.2.12. Consulta Bürotechnik s.r.o. Cukrovarská 519/20 68201 Vyškov, 2017.

[57] UniFi - Ports Used – Ubiquiti Networks Support and Help Center. *Ubnt.com* [online]. b.r. [cit. 2018-05-06]. Dostupné z: https://help.ubnt.com/hc/en-us/articles/218506997-UniFi-Ports-Used

[58] UniFi - Run the Controller as a Windows service – Ubiquiti Networks Support and Help Center. *Ubnt.com* [online]. b.r. [cit. 2018-05-06]. Dostupné z: https://help.ubnt.com/hc/en-us/articles/205144550-UniFi-Run-the-Controller-as-a-Windows-service

[59] RDP Wrapper Library. *Github.com* [online]. b.r. [cit. 2018-05-11]. Dostupné z: https://github.com/stascorp/rdpwrap/releases

[60] TightVNC: VNC-Compatible Free Remote Control / Remote Desktop Software. *Tightvnc.com* [online]. b.r. [cit. 2018-05-11]. Dostupné z: https://www.tightvnc.com

[61] IE Tab - Chrome Web Store. *Chrome.google.com* [online]. b.r. [cit. 2018-05-12]. Dostupné z: https://chrome.google.com/webstore/detail/ie-tab/hehijbfgiekmjfkfjpbkbammjbdenadd?hl=en

[62] Co je WinSCP. *Winscp.net* [online]. b.r. [cit. 2018-05-07]. Dostupné z: https://winscp.net/eng/docs/lang:cs

[63] Download VNC Viewer | VNC Connect. *Realvnc.com* [online]. b.r. [cit. 2018-05-11]. Dostupné z: https://www.realvnc.com/en/connect/download/viewer/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACL	Access Control List
ACME	Automatic Certificate Management Environment
AES-NI	Advanced Encryption Standard New Instructions
API	Application Programming Interface
BNC	Bayonet Neill Concelman connector
BPK	Bezpečnostní kód poplatníka
CA	Certification Authority
CBC	Cipher Block Chaining
CCD	Charged Coupled Device
CCTV	Closed Circuit Television
CLI	Command Line Interface
CMOS	Complementary Metal–Oxide–Semiconductor
CPU	Central Processing Unit
CVBS	Composite Video Baseband Signal
DDNS	Dynamic Domain Name Service
DDR3	Double Data Rate 3
DDR3	Double Data Rate 3
DHCP	Dynamic Host Configuration Protocol
DIČ	Daňové identifikační číslo
DNR	Digital Noise Reduction
DNS	Domain Name Service
DVB-T2	Digital Video Broadcasting – Terrestrial 2
DVR	Digital Video Recorder
FIK	Fiskální identifikační kód
FPS	Frames Per Second

GDI	Graphics Device Interface
GUI	Graphical User Interface
HDMI	High Definition Multimedia Interface
HD-TVI	HD Transport Video Interface
HEVC	High Efficiency Video Coding
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
L2	Layer 2
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LC	Lucent Connector
LNB	Low-noise block
MAC	Media Access Control
MDI/MDIX	Medium Dependent Interface / Medium Dependent Interface Crossover
MTBF	Mean Time Between Failure
NAT	Network Address Translation
NPAPI	Netscape Plugin Application Programming Interface
NTSC	National Television Systém Committee
OpenVPN	Open Virtual Private Network
OSD	On Screen Display
OSI	Open Systems Interconnection
PAL	Phase Alternating Line

PKP	Popisný kód poplatníka
PoE	Power over Ethernet
PTZ	Pan Til Zoom
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RJ45	Registered Jack 45
SFTP	SSH File Transfer Protocol
SHA-1	Secure Hash Algorithm 1
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TDP	Thermal Design Power
TDP	Thermal Design Power
TLS	Transport Layer Security
UDP	User Datagram Protocol
ÚOOÚ	Úřad pro ochranu osobních údajů
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WDM	Wavelength-Division Multiplexing
WDR	Wide Dynamic Range
WEP	Wired Equivalent Privacy
WPA2-PSK	Wi-Fi Protected Access 2 Pre-Shared Key
WPA-PSK	Wi-Fi Protected Access Pre-Shared Key
WPS	Wireless Provisioning Services

SEZNAM OBRÁZKŮ

SEZNAM TABULEK