Moderní domácí síť

A Modern Home Network

Milan Martinek

Bakalářská práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

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

Jméno a příjmení:	**Milan Martinek**
Osobní číslo:	**A12039**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Forma studia:	**prezenční**
Téma práce:	**Moderní domácí síť**
Téma anglicky:	**A Modern Home Network**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Navrhněte vhodné síťové prvky k realizaci domácí sítě.**
3. **Zrealizujte domácí sít s NAS připojenou do Internetu s VPN serverem pro vzdálený přístup.**
4. **Nakonfigurujte aktivní síťové prvky, včetně koncových zařízení.**
5. **Ověřte vzdálený přístup k jednotlivým domácím spotřebičům v síti.**

Rozsah bakalářské práce: -

Rozsah příloh: -

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

Seznam odborné literatury:

1. **KUROSE, James F. a Keith W. ROSS. Počítačové sítě. 1. vyd. Brno: Computer Press, 2014, 622 s. ISBN 978-80-251-3825-0.**
2. **KRČMÁŘ, Petr. Linux: postavte si počítačovou síť. 1. vyd. Praha: Grada, 2008, 182 s. ISBN 978-80-247-1290-1.**
3. **KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5. aktualizované vydání. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.**
4. **OpenVPN - The Open Source VPN. OpenVPN [online]. [cit. 2016-02-05]. Dostupné z: https://openvpn.net/**
5. **Síťové úložiště (NAS) Synology. Synology Inc. [online]. [cit. 2016-02-05]. Dostupné z: https://www.synology.com/cs-cz/**

Vedoucí bakalářské práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **19. února 2016**

Termín odevzdání bakalářské práce: **27. května 2016**

Ve Zlíně dne 19. února 2016

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Práce se zabývá návrhem a reálným vybudováním moderní vysokorychlostní zabezpečené domácí sítě s prvky, které lze rovněž využít i ve firemním sektoru. Nejprve byla navržena infrastruktura sítě a zapojeny síťové (částečně i televizní a rádiové) rozvody s důrazem na vysokorychlostní přenos dat (1 Gbps) v rámci lokální sítě a možností přechodu v budoucnu na 10 Gbps bez nutnosti zásahu do síťových rozvodů.

Dále byly vhodně navrženy a nakonfigurovány síťové prvky i koncová zařízení za účelem splnění nebo využívání šifrovaného vzdáleného připojení do lokální sítě pomocí OpenVPN nebo přímý přístup k vybraným síťovým prvkům pomocí směrování portů a HTTPS spojení. Vzdálená správa zařízení jako NAS server, router, počítač, chytrý telefon, chytrá žárovka, kamerový systém, chytrá televize, AV Receiver atd. Přístup k šifrovaným uživatelským datům a multimediálním souborům na centrálním síťovém úložišti NAS pomocí různých souborových protokolů a služeb. Pokročilá synchronizace dat mezi serverem a koncovými zařízeními uživatelů s podporou záloh několika verzí modifikovaných souborů. Zálohování důležitých dat z NAS serveru na externí cloudové úložiště pro případ jeho zničení nebo odcizení. Monitoring venkovního prostoru kolem domu včetně ukládání záznamu na NAS server.

Klíčová slova: moderní síť, vzdálený přístup, vzdálená správa, NAS server, DLNA, synchronizace, záloha, cloud, monitoring

ABSTRACT

This bachelor thesis deals with a design and real formation of a modern security of a high-speed home network with the features, which can be used also in the corporate sphere.

First of all, the infrastructure of the network was built and distribution networks (partially also television and radio) were connected, focused on high-speed data transmission (1 Gbps) in the local network. A possibility to switch from 1 Gbps to 10 Gbps was considered without any essential changes network distributions.

Furthermore, the network features and end devices were designed and configured with the objective to fulfil or utilize encrypted remote connection to the local network using Open-VPN or direct access to the selected network elements using port forwarding and HTTPS connection.The remote control as NAS server, router, computer, smart phone, smart bulb, the camera system and smart television, AV Receiver etc. The access to the encrypted end-user data and multimedia files on the central network storage NAS through different file protocols and services. An advanced data synchronization between the server and end-user devices with support for multiple backup versions of modified files. Backup of important data from NAS server to an external cloud storage for the occasion of his destruction or theft. An advanced data synchronization between the server and end-user devices with support for multiple backup versions of modified files. Backup of important data from NAS server to an external cloud storage for the occasion of his destruction or theft. Monitoring of house surrounding inclusive a storage of records in the NAS server.

Keywords: modern network, remote access, remote management, NAS, DLNA, synchronization, backup, cloud, monitoring

Rád bych poděkoval vedoucímu práce, Ing. Miroslavu Matýskovi, Ph.D. za pomoc, ochotný přístup a cenné rady, které mi poskytl během tvorby mé bakalářské 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

Situace, kdy není domácí síť zapotřebí a stačí jen jeden počítač, do kterého vede přímo kabel s Internetovým připojením, je již čím dál vzácnější. V dnešní moderní domácnosti má běžně každý technicky zdatný člen rodiny svůj chytrý telefon, počítač případně tablet a to není zdaleka vše. Jsou zde i další sdílená zařízení jako televize, tiskárna, domácí kino, ip kamery atd.

Moderní domácí síť by měla těmto zařízením poskytnout možnost vysokorychlostní pevné i bezdrátové konektivity pro bezproblémové připojení k Internetu, sdílení souborů mezi zařízeními, streamování videa ve vysokém rozlišení, bezdrátový tisk nebo i vzdálenou správu jednotlivých zařízení př. ovládání televize nebo žárovek pomocí telefonu.

Dále je dnes hlavně ve firmách, ale i moderních domácnostech stále více kladen důraz na dostupnost veškerých dat uložených na centrálním síťovém úložišti přístupném v rámci lokální sítě nebo i z Internetu pro všechna možná zařízení uživatelů. Data jsou pomocí této realizace neustále s námi za podmínky dostupnosti naší lokální sítě nebo Internetového připojení a je jedno, jestli jsme doma, v práci nebo na mezinárodní vesmírné stanici.

Tato úložiště se dají využít k synchronizaci a záloze veškerých potřebných dat, které si uživatel navolí. Tuto možnost ocení každý, kdo například stráví měsíce prací na projektu do práce a den před dokončením na pracovní cestě zjistí, že má neopravitelnou poruchu disku, nebo mu ukradli počítač. Pomocí zálohy v cloudovém úložišti stačí synchronizovat data s novým zařízením, nebo soubory editovat přímo prostřednictvím vzdáleného zabezpečeného napojení ke svému účtu ve webovém rozhraní operačního systému serveru pomocí jakéhokoliv internetového prohlížeče.

Za pomoci rozšiřované dostatečně rychlé internetové konektivity, dosahující běžně rychlosti desítek i stovek megabitů, lze bez problémů streamovat videosoubory z domácí sítě, jako například obraz z venkovní IP kamery v reálném čase. Nebo se lze na lokální síť rovnou zabezpečeně napojit pomocí VPN tunelu a pracovat bez omezení se všemi výhodami běžného lokálního připojení, jako například připojení k síťové tiskárně, vzdálená správa lokálního počítače, nebo ovládání žárovek atd.

I. TEORETICKÁ ČÁST

1 TEORIE K ZAPOJENÍ SÍŤOVÝCH ROZVODŮ

1.1 Kroucená dvojlinka

Kroucená dvojlinka je druh síťového kabelu. Je to nejrozšířenější vodič používaný u sítí LAN. Kabel se 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 [1].

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 [1].

Řazení podle rychlosti (pouze nejpoužívanější):

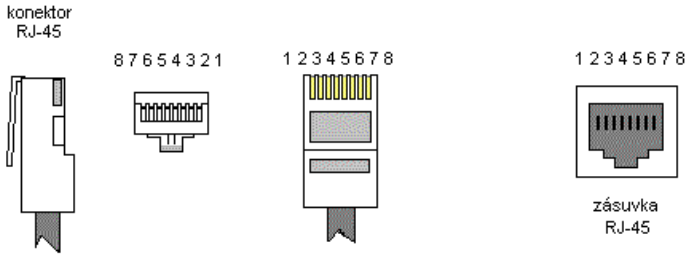
100BaseTX: lze zapojit přes kabel Cat 5 a vyšší, využívá 2 páry, 2 režimy komunikace polo duplex (jedním párem v jednom směru 100 Mbps) a plný duplex (oběma páry najednou, ale párem vždy jednosměrně 100 Mbps) (1 pár x 100Mbps v jednom směru a 2 pár ve směru opačném)

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].

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.

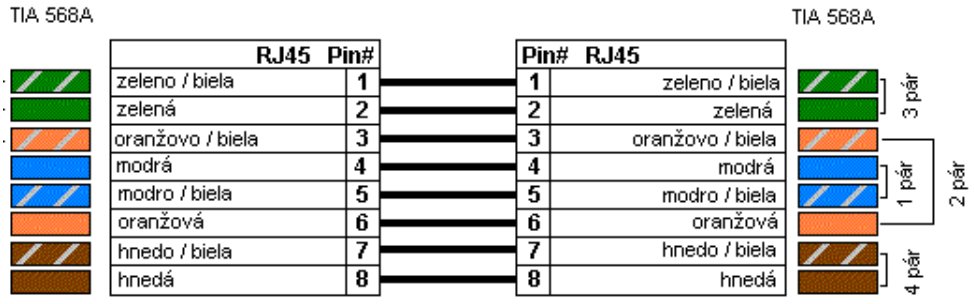


Obr. 1. Konektor RJ45 [3].

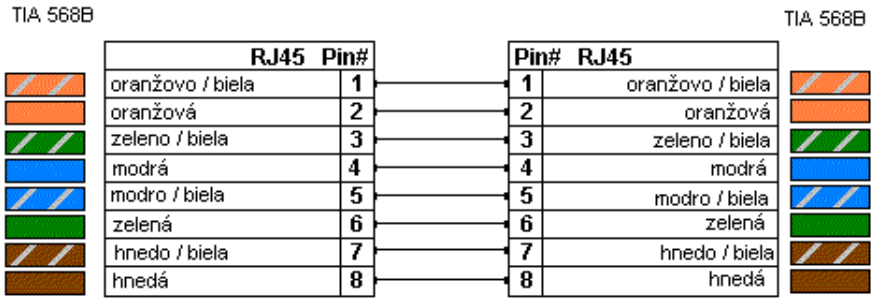
K zapojení lze využít 2 standardy s označením TIA/EIA (Telecommunications Industry Association/Electronic Industries Alliance) 568A a T568B v provedení kříženém nebo přímém [1].

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) [1].



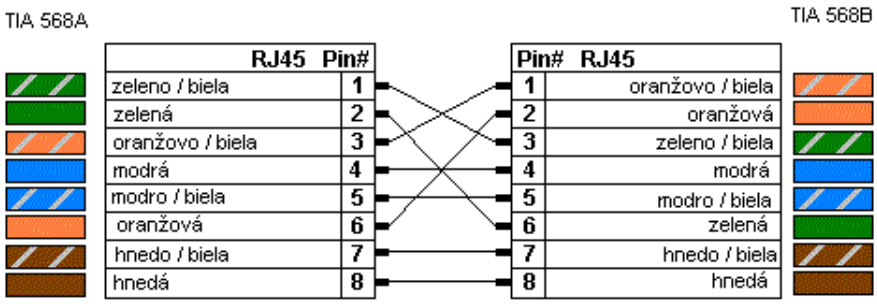
Obr. 2. Přímé zapojení RJ45 TIA 568A [3].



Obr. 3. Přímé zapojení RJ45 TIA 568B [3].

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 [1].



Obr. 4. Křížené zapojení RJ45 100 Mbps.

2 TEORIE KE KONFIGURACI SÍŤOVÝCH PRVKŮ

2.1 OpenVPN

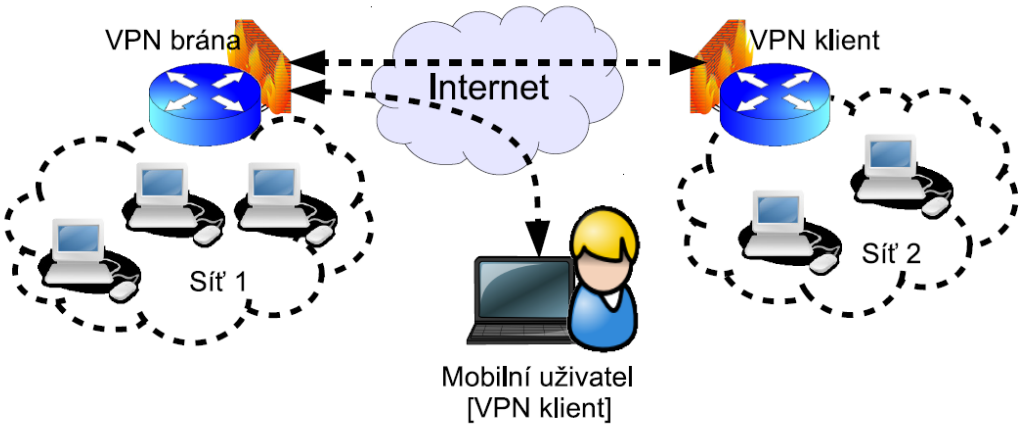
VPN (Virtual Private Network), neboli virtuální privátní síť, vytváří propojení (šifrovaný tunel) mezi jednotlivými sítěmi nebo koncovými zařízeními, které mohou být rozmístěny po celém Internetu do jedné virtuální sítě. Zařízení v této síti se poté chovají, jako by byly přímo fyzicky připojené do lokální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

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 z vnějšku vypadat, že pochází 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 [4] [5] .



Obr. 5. Princip virtuální privátní sitě [6].

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), je multiplatformní, možnost komprese dat, velké množství nastavení různých dodatečných zabezpečení a šifrovacích algoritmů (asymetrické šifrování).

2.2 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 přenášených 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 z pravidla 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) [4], [6].

2.3 TCP/UDP vrstva

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 [7].

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.

2.4 Předávání portů

Předávání portů (Port Forwarding) umožňuje vzdáleným zařízením s možností síťové komunikace přístup k síťovým zařízením nebo službám v lokální síti LAN.

Chceme-li se vzdáleně napojit na nějaké zařízení nebo službu v lokální síti, potřebujeme zvolit port, nebo rozsah portů, přes které se budeme připojovat z veřejné IP adresy, lokální IP (Internet Protocol) adresu zařízení na které se chceme napojit, místní port lokálního zařízení a druh přenosového protokolu (TCP/UDP). Takto vytvořené pravidlo zajistí, že všechny pakety, které přijdou na naši veřejnou IP adresu př. 234.234.234.234 a port př. 80, budou přesměrovány do vnitřní sítě na port př. 80 počítače př. 192.168.1.22.

2.5 ASUS AiRadar

Tato technologie, vyvinutá společností Asus, inteligentně přizpůsobuje charakteristiku antény místním podmínkám, čímž zaručuje kvalitnější směrovou emulaci signálu. Technologie AiRadar (Artificial Intelligence Radar) upravuje tvar signálu tak, aby nabízel co nejsilnější výstup, a převádí slabý, všesměrový signál na silnější směrovaný signál, u kterého zároveň zlepšuje propustnost [8].

2.6 AiProtection

AiProtection (Artificial Intelligence Protection) je služba starající se o zabezpečení routeru. Obsahuje bezpečností prvky Trend Micro Deep Packet Inspection engine, poskytuje vybraným domácím routerům zabezpečení na korporátní úrovni.

Kontroluje konfiguraci spjatou se zabezpečením a doporučí vhodné změny jako př. vypnout směrování portů, vypnutí UPnP (Universal Plug and Play) atd., dále detekuje a zároveň blokuje komunikaci u zařízení nakažených malwarem, škodlivé internetové stránky, nebezpečné datové pakety od útočníků poslané do síťě LAN (Local Area Network) přes některé zařízení se slabou ochranou jako IP kamery nebo televize s OS [9].

2.7 Adaptivní QOS

Adaptivní QOS (Quality Of Services) optimalizuje šířku pásma pro příchozí a odchozí komunikaci u kabelového i bezdrátového připojení, pomocí uživatelského nastavení priority určitým úlohám a aplikacím, př. VoIP (Voice over Internet Protocol) telefon, stream videa, her atd. [10].

2.8 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.

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 [11].

2.9 IFTTT

IFTTT (If This Then That) je známá automatizační služba, která se konfiguruje ve smyslu „pokud se něco stane, tak něco udělej“. Kdy se pracuje s určitými kanály (propojované služby př. zapnutí žárovky A, stisk tlačítka B). Pro příklad - pokud se stiskne určité tlačítko, tak vyšli povel žárovce, aby se zapnula, změnila barvu, intenzitu svitu atd. Komunikace probíhá pomocí šifrovaného Internetového spojení, kdy zařízení komunikují přes server služby, takže lze ovládat žárovku i vzdáleně mimo LAN bez nutnosti nějak nastavovat VPN nebo předávání portů atd. [12].

2.10 ONVIF

Tento protokol umožňuje standardizovanou univerzální komunikaci mezi síťovými kamerami navzájem nebo kamer se zařízeními určenými na jejich správu a zpracování obrazu, jako př. NAS server se speciálním administračním softwarem. Značnou výhodou tohoto standardu je jeho univerzálnost bez ohledu na výrobce určitého zařízení [13].

2.11 SMB/CIFS

SMB (Server Message Block) je síťový komunikační protokol pracující na aplikační vrstvě modelu OSI (Open Systems Interconnection). Varianta protokolu vyvíjená společností Microsoft se nazývá CIFS (Common Internet File Systém). Protokol je nejčastěji využíván ke sdílení souborů mezi uživateli v lokální síti [13].

2.12 FTP

FTP (File Transfer Protokol) je jeden z nejstarších protokolů vůbec. Jedná se o protokol typu klient-server. Server nabízí data (soubory) klientům, kteří se k němu připojují přes síť. Data proudí v textové podobě bez jakéhokoliv zabezpečení. Díky tomu má přenos nízké systémové nároky a dosahuje vysokých rychlostí. Nehodí se ovšem k přenosu citlivých dat po veřejných sítích (př. Internet).

Existují 2 různé režimy práce FTP serveru - aktivní a pasivní.

U aktivního se klient připojí k serveru skrze komunikační port 21 (ve výchozím nastavení) a pošle mu informaci o zvoleném portu na své straně pro přenos dat a začne na tomto portu poslouchat. Server se na port připojí a začne posílat data.

U pasivního se klient připojí skrze komunikační port 21 a požádá o přepnutí do pasivního režimu. Server pošle informaci o zvoleném portu na své straně, kde začne naslouchat. Klient se na port připojí a začne přenos dat. Nakonec strana odesílající data port zavře [14].

2.13 UTF-8

Kódování UTF-8 je nejčastějším zápisem znakové sady Unicode, která je určená pro všechny světové jazyky najednou. Jedná se o moderní kódování, které však ještě není podporované globálně [14].

2.14 WebDAV

WebDAV (Web-based Distributed Authoring and Versioning) je rozšířením HTTP (Hypertext Transfer Protocol) protokolu, který zajišťuje vzdálenou správu souborů na webovém serveru. Jedná se o komunikaci klientské aplikace se serverem pomocí upravených metod standartního HTTP protokolu, který je doplněn dalšími metodami pro práci se soubory (jejich vlastnostmi a kolekcemi). Při komunikaci lze využít zabezpečené komunikace pomocí HTTPS (Hypertext Transfer Protocol Secure) a SSL certifikátů.

2.15 RAID

Technologie RAID (Redundant Array of Inexpensive/Independent Disks) umožňuje vytvořit z více disků jeden úložný prostor.

U zapojení RAID 1 se data na pevných discích zrcadlí. Díky tomu je pole chráněno před závadou jednoho z disků. Zároveň dojde k cca dvojnásobnému zvýšení rychlosti při čtení. Velkou nevýhodou tohoto zapojení je zmenšení úložného prostoru na polovinu.

U zapojení RAID 5 jsou zapotřebí minimálně 3 disky. Typ RAID 5 unese závadu jednoho pevného disku. V případě závady se data z tohoto disku rekonstruují pomocí parity uložené na ostatních pevných discích. Proto je tento režim nejlepší volbou pro ochranu dat před závadou jednoho disku s ohledem na zachování co nejvyššího úložného prostoru [13].

2.16 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 [13].

2.17 UPnP/DLNA

UPnP je sada síťových protokolů vyhlašovaných UPnP Fórem. Umožňuje externím hostitelům zahajovat komunikační relace s hostiteli za NAT (Network Address Translation), překladačem IP adres, který většinou převádí více lokálních IP na veřejnou. Architektura tedy umožňuje P2P (Peer to Peer, Klient-Klient) spojení síťových zařízení. Umožňuje široké řadě drátových i bezdrátových zařízení vzájemné propojení a bezproblémovou spolupráci vytvořením síťových služeb, jako jsou například datové proudy médií. UPnP totiž může přenášet prakticky cokoliv. Je to přenosový protokol, který v mnoha ohledech vychází z prostého textového HTTP. UPnP podporuje využívání sítí bez nutnosti konfigurace, ke které dojde automaticky po připojení zařízení UPnP do sítě, která využívá technologii „plug-n-play“ [14],[13]. Úkolem UPnP je v našem případě dostat obsah z úložiště A skrze domácí síť do

zobrazovače B. Tím může být televizor, ale stejně tak třeba domácí Hi-Fi systém podporující připojení do LAN.

DLNA (Digital Living Network Alliance) je soubor pravidel založených organizací výrobců z různých průmyslových sektorů včetně spotřební elektroniky a výpočetní a mobilní techniky. Tato pravidla řídí a spravují multimediální protokol UPnP. DLNA zařízení jsou určena k tomu, aby přehrávala fotky, hudbu a videa.

Systém UPnP/DLNA se skládá ze serveru, ovladače a zobrazovače. Server se stará o samotné soubory, které poté umí přenášet po síti do zobrazovače obsahu jako televize, přehrávač v PC podporující DLNA atd. Ovladač je program, který dokáže kontrolovat přehrávání médií ze serveru na zobrazovač. Může to být také třetí zařízení jako mobilní aplikace, ve které se načte knihovna médií na DLNA serveru. Uživatel si pomocí ovladače vybere, na kterém spárovaném zařízení v síti (zobrazovači – televize, AV Receiver atd.) dané médium přehraje [15]. Některé DLNA/UPnP servery v systémech NAS podporují rovněž přehrávání titulků, překódování multimediálních souborů v reálném čase do formátů které dokáže zobrazovač zobrazit atd.

2.18 Multicast a IGMP Snooping

Multicast je metoda efektivní komunikace jednoho odesílatele více příjemcům. Příkladem může být internetové rádio proti běžnému rádiu, kdy je jeden zdroj a mnoho příjemců, kteří přijímají stejná data ve stejnou chvíli. V praxi se to často řeší tak, že se vytvoří jednotlivá spojení pro každého příjemce. Takže je značně zatěžován server a část síťové infrastruktury je zbytečně přetížena přenosem duplicitních dat.

Pomocí multicastu posíláme informaci současně skupině příjemců co nejefektivnějším způsobem, aby zpráva přes každý síťový uzel cestovala pouze jednou, kopie se vytváří, pouze pokud se cesty k příjemcům rozdělují [16].

IGMP snooping je optimalizační mechanizmus pro L2 switch. Standardně se multicast na switchi šíří jako broadcast, tedy na všechny porty mimo příchozího. IGMP (Internet Group Management Protocol) snooping zajišťuje zkoumání multicast provozu a detekci join (připojit) a leave (odejít) zpráv. Podle toho se určí, na kterém portu se nachází router a kde klienti, a sestavuje tabulku, podle které přeposílá multicast pouze na ty porty, kde klient tento provoz požaduje. Také odpovědi klientů odesílá pouze na router a ne ostatním klientům. Dynamicky tedy konfiguruje porty pro příjem multicastu [16].

2.19 Synology QuickConnect

Jedná se o službu společnosti Synology, která zajišťuje možnost vzdáleného připojení k NAS serveru v každém síťovém prostředí bez nutnosti vlastnit statickou veřejnou IP adresu, nebo nastavovat pravidla předávání portů na straně routeru (automatické přesměrování pomocí UPnP). Toho je docíleno propojením klienta se serverem prostřednictvím vzdáleného serveru společnosti. Toto spojení ovšem nedosahuje stejné odezvy a rychlosti jako v případě běžného zapojení. Dále lze využít k detekci a automatickému přepínání (přesměrování) mezi adresami WAN/LAN, když je klientské zařízení přemístěno. Tato funkce poskytuje výhodu při konfiguraci př. různých mobilních aplikací podporujících tuto funkci, kdy do pole, kde bychom zadávali IP adresu, vložíme QuickConnectID serveru. Připojení bude poté pro zařízení fungovat v LAN i mimo ni bez nutnosti měnit adresu [13].

2.20 Cloud

Cloud (také Cloud computing) je způsob poskytnutí výpočetního výkonu, úložiště, přístup k datům a jejich správa, případně i ukládání a zálohování dat v podobě služby pomocí sítě (většinou Internet). Uživatelé do cloudu přistupují pomocí softwarové aplikace (pomocí počítače, telefonu, atd.), nebo přes webové rozhraní cloudové služby v internetovém prohlížeči [13].

2.21 NAS

NAS server (Network Attached Storage) je centrální síťové úložiště. Ve své podstatě se jedná o malý úsporný počítač připojený k síti a optimalizovaný k provozu 24/7. Hlavní úlohou NAS serveru je centrální ukládání dat a jejich následné sdílení po lokální síti nebo přes internet do vzdálených zařízení. V souvislosti s prací s daty po síti poskytuje ovšem nepřeberné množství možností [13].

2.22 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 [13].

II. PRAKTICKÁ ČÁST

3 NÁVRH VHODNÝCH SÍŤOVÝCH PRVKŮ

3.1 Síťový kabel Solarix CAT6 UTP PVC

Pro rozvody strukturované kabeláže byl vybrán síťový kabel Solarix CAT6 UTP PVC. Tento kabel je vysoce kvalitní, jednotlivé páry vodičů jsou odděleny plastovým křížem (spacerem). Tento kříž odděluje jednotlivé páry po celé délce kabelu. Jeho smyslem je dodržení minimální vzdálenosti mezi jednotlivými páry uvnitř pláště kabelu a tím zmenšení rizika nežádoucího přeslechu mezi těmito páry. Samotné vodiče jsou vyrobeny z měděného drátu o velikosti AWG (American Wire Gauge) 23 a čistotou 99,97 % [17].

Kabel kategorie 6 byl zvolen z následujících důvodů:

- spolehlivý přenos Gigabit Ethernetu (1000BaseT), díky šířce pásma 250MHz je méně náchylný na ruchy okolí a případné degradace spojení na nižší rychlosti, jelikož aktivní prvky jako router nebo switch zareaguji tak, že přepnou na nejbližší nižší rychlost, tudíž 100 Mbps (Fast Ethernet).
- možnost 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).
- možnost do budoucna přejít na nový ethernetový protokol 10GBaseT, který podporuje poloviční duplex přenos 10 Gbps u kabelu kategorie 6 až do vzdálenosti 55 m [2].

Obr. 6. Kabel Solarix CAT6 UTP (PVCSXKD-6-UTP-PVC).

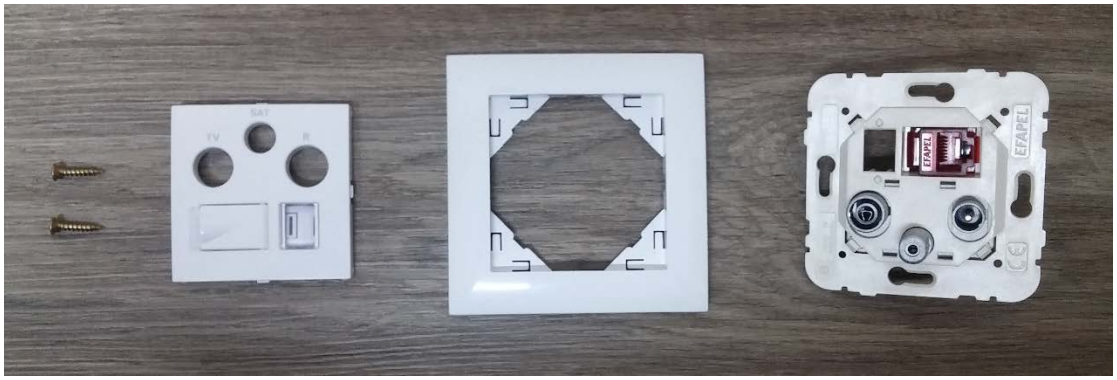
3.2 Multimediální zásuvky ELKO EP 21544 a EP 21546

Multimediální zásuvky byly vybrány pro svoje optimální členění potřebných konektorů potřebných v každém pokoji moderní domácnosti.

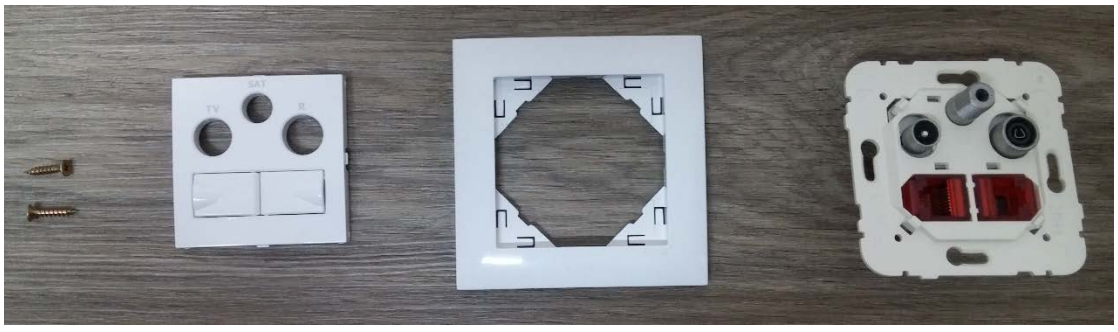
Každá zásuvka obsahuje:

- konektor IEC (International Electrotechnical Commission) Female pro připojení analogového rádia
- konektor IEC Male pro připojení digitálního pozemního vysílání (DVB-T)
- konektor F Male pro připojení satelitního vysílání (DVB-S)
- konektor RJ45 Female UTP CAT6 250 Mhz (2x u ELKO EP 21546)

K multimediálním zásuvkám je potřeba rovněž dokoupit krytku ELKO EP 90770 (s jedním konektorem RJ45 pro EP 21544), ELKO EP 90773 (se 2 konektory RJ45 pro EP 21546) a rámeček ELKO EP 90910 [18].



Obr. 7. Zprava zásuvka ELKO EP 21544, rámeček ELKO EP 90910 a krytka ELKO EP 90770.



Obr. 8. Zprava zásuvka ELKO EP 21546, rámeček ELKO EP 90910 a krytka ELKO EP 90770.

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

Konektory RJ45 byly značným úskalím zapojování domácí sítě. Se skládanými konektory pro kategorií 6 jsem do doby zapojování této sítě neměl žádné zkušenosti. V průběhu času byly vyzkoušeny 3 značky konektorů a po několika nekvalitních spojích způsobených netěsností mezi konektorem a vložkou, kdy vodiče při stlačení krimpovacími kleštěmi často sklouzly před piny konektoru na stranu, byly nakonec vybrány konektory od firmy Solarix 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 [19].

Obr. 9. 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.

Obr. 10. Krimpovací kleště Netrack RJ45 8p +6 p +4 p, tester Logilink.

3.4 Router Asus RT-AC68U

Při výběru routeru byl kladen důraz na podporu rychlého bezdrátového přenosu WiFi IEEE 802.11ac, přítomnost 2,4 a 5 GHz bezdrátového pásma s podporou MIMO, alespoň 4 gigabitové porty RJ45 (1000BaseT) a dostatečný výkon pro zprovoznění plnohodnotného VPN serveru. Z toho důvodu byl po přečtení mnoha recenzí a názorů z internetových diskuzních fór vybrán právě router Asus RT-AC68U.

Router Asus RT-AC68U byl ideální volbou pro navrhovanou síť z následujících důvodů:

- Podpora standardů WiFi IEEE (Institute of Electrical and Electronics Engineers) 802.11a/n/ac v síti 5 GHz a IEEE 802.11b/g/n v síti 2,4 GHz.
  Kdy maximální datový tok pro IEEE 802.11n s využitím technologie MIMO (Multi Input Multi Output) dosahuje při využití 3 streamů rychlosti 600 Mbps v pásmu 2,4 GHz a v případě IEEE 802.11ac u 5 GHz pásma 1300 Mbps.
  V tomto případě je rychlost bezdrátového přenosu srovnatelná s rychlostí kabelového přenosu. Ovšem tato udávaná rychlost je pouze teoretická a v reálných podmínkách se mi ji z důvodu různých rušení a překážek mezi přijímačem a vysílačem nepodařilo dosáhnout, ale i tak je rychlost dostatečná například pro plynulý stream videa ve 4K rozlišení.
- Podpora 2,4 a 5 GHz bezdrátového pásma.
- CPU (Central Processing Unit) Broadcom BCM4708A0, 2 jádra x 800 MHz.
- RAM (Random Access Memory) 256 MB.
- Flash paměť pro uložení firmware 125 MB.
- Porty: 4xRJ45 pro 10/100/1000 BaseT pro LAN, 1 x RJ45 pro 10/100/1000 BaseT pro WAN, 1xUSB 3.0, 1xUSB 2.0.
- Podpora WOL (Wake On Lan): funkce pro vzdálené probuzení klientských zařízení, jejichž síťová karta a Bios tuto funkci podporují.
- Šifrování: WEP (Wired Equivalent Privacy) 64bitové a 128bitové, WPA2-PSK (Wi-Fi Protected Access 2 Pre-Shared Key), WPA-PSK (Wi-Fi Protected Access Pre-Shared Key), WPA-Enterprise, WPA2-Enterprise, podpora WPS (Wireless Provisioning Services).
- VPN server: nativně PPTP (Point-to-Point Tunneling Protocol) a OpenVPN, s možností předávání (Pass-Through) IP Security, PPTP, L2TP.
- VPN klient: PPTP, L2TP (Layer 2 Tunneling Protocol), OpenVPN.

- Rozsáhlá podpora síťových protokolů a funkcí jako IPv4, IPv6, UPnP, IGMP/multicast v1/v2/v3, DNS Proxy, DHCP (Dynamic Host Configuration Protocol), NTP (Network Time Protocol) Client, DDNS, Adaptivní QoS, Tiskový server, DLNA mediální server, FTP server, Samba server, IPTV (Internet Protocol television), Dual WAN.
- ASUS AiRadar.
- AiProtection.
- Adaptivní QOS.
- 3G/4G sdílení spojení: v případě potřeby lze připojit 3G/4G přijímač do portu USB 3.0 a sdílet mobilní data. Tato funkce se může hodit při výpadku pevného internetového připojení od stálého poskytovatele internetu.
- Přehledné a intuitivní grafické webové rozhraní s možností podrobného nastavení všech integrovaných funkcí, síťové a provozní analýzy, čtení logů, podrobným firewalem, přehlednou správou připojených zařízení atd. s názvem AsusWRT.
- 220 x 83,3 x 160 mm.
- Maximální spotřeba: 33,25 W (19 V s max. proudem 1,75A) [8].

Obr. 11. Router Asus RT-AC68U [8].

3.5 Switch TP-LINK TL-SG108E

Při výběru switche byly kladeny požadavky rovněž jako u routeru na gigabitové ethernetové porty standardu 1000BaseT, podporu IGMP Snoopingu pro správnou funkci multicastových

aplikací jako př. DLNA server. Jelikož byl switch umístěn v podkroví rodinného domu, přístupného pouze po žebříku z venkovního vchodu, bylo důležité vybrat model se vzdálenou správou umožňující diagnostiku zapojení kabelů.

Kvůli častým výkyvům teplot bylo rovněž potřeba zvolit model s kvalitní kovovou konstrukcí, která poskytuje lepší odvod tepla a není tolik náchylná na vysoké teploty v letních měsících.

Poslední stěžejní parametr pro výběr byl počet portů. Tento parametr byl po návrhu síťové infrastruktury, kterou budu rozebírat v části zapojení sítě, stanoven na minimálně 8 portů.

Z toho důvodu byl zvolen L2 (Layer 2) switch TP-LINK TL-SG108E, který vyšel jako nejlepší volba v poměru cena/výkon. Switch disponuje následujícími parametry:

- Porty: 8xRJ45 pro 10BaseT, 100BaseTX, 1000BaseT UTP i STP.
- Zrcadlení portů, prevence smyček a diagnostika kabelů.
- Funkce Auto MDI/MDI-X (Medium Dependent Interface / Medium Dependent Interface Crossover) na všech portech eliminuje potřebu křížených kabelů nebo portů odchozího připojení.
- IGMP Snooping optimalizuje multicastové aplikace (př. DLNA)
- QOS umožní nastavit prioritu provozu pro jednotlivé porty a zařízení pomocí standardu IEEE 802.1p.
- Technologie úspory energie ušetří až 80% spotřeby, kdy automaticky upravuje spotřebu energie podle stavu připojení a délky kabelu, navíc detekuje nečinné porty, u kterých sníží spotřebu energie.
- Řízení toku dat pomocí standardu IEEE 802.3x zajišťujícímu spolehlivé přenosy.
- Podpora Jumbo frame pro zlepšení výkonnosti při přenosu objemných dat (16 KB).
- VLAN (Virtual Local Area Network) podle portů a tagů (podpora standardu IEEE 802.1q).
- TP-Link Easy Smart Configuration Utility (Aplikace umožňující vzdálené monitorování připojených portů, identifikaci problémů s připojením a konfiguraci).
- Zásobník paketů 1,5 Mb.
- Provozní teplota: 0°C – 40°C.
- Rozměry: 158 x 101 x 25 mm.
- Maximální spotřeba: 4,48 W [20].

Obr. 12. L2 switch TP-LINK TL-SG108E [20].

Obr. 13. L2 switch TP-LINK TL-SG108E.

3.6 NAS server Synology Diskstation DS716+

NAS server tvoří jádro celé moderní domácí sítě. Z toho důvodu bylo potřeba při výběru promyslet a pečlivě rozvrhnout značnou část potřebných parametrů.

3.6.1 Stěžejní body pro výběr

- Šachty pro 2 HDD 3,5" aby bylo možno v případě potřeby zapojit disky pole RAID I a ochránit tak data před poruchou jednoho z disků pomocí zrcadlení těchto dat na záložní disk.
- Možnost do budoucna rozšířit úložiště dokoupením expanzní jednotky a mít možnost zapojit disky do některých datově úspornějších diskových polí (př. RAID 5).
- Podpora WOL pro možnost vzdáleného spuštění serveru v případě jeho neočekávaného vypnutí, způsobeného př. výpadkem proudu.
- Dostatečně výkonný procesor s podporou hardwarového šifrování AES-NI (Advanced Encryption Standard New Instructions) pro možnost zabezpečit soukromá data v případě krádeže serveru nebo jakékoliv neoprávněné manipulace s daty.
- Podpora hardwarového převzorkování videa v reálném čase pro možnost snížit datový tok, rozlišení nebo změnit kodek (formát videa) z důvodu přizpůsobení video

streamu šířce pásma vzdáleného místa. Pomocí této úpravy nebude docházet k sekání u vzdálených zařízení, která se připojí v místě se slabou Internetovou konektivitou, a zároveň nedojde k nekompatibilitě u zařízení nepodporujících určitý kodek videa.

- Alespoň 2 GB paměti RAM.
- Alespoň 2 bezplatné licence zapojení IP kamer k vestavěnému monitoring systému.
- Optimalizovaný operační systém s častými aktualizacemi a možností rozšíření funkcí přidáním aplikačních balíčků.
- Nízká spotřeba.
- Kvalitní zpracování skříně s možností vysunutí pevných disků za provozu.
- Ostatní parametry specifické pro každý NAS jako centralizovaná správa a přístup k datům, synchronizace a zálohování souborů napříč platformami, uživatelské účty atd. jsou u obou hlavních výrobců (Synology a QNAP) podobné a nepatří ke stěžejním bodům pro výběr.

Po cca 14 dnech podrobného studia problematiky NAS serverů, pročítání recenzí a uživatelských zkušeností byl zvolen NAS server Synology Diskstation DS716+

NAS server Synology Diskstation DS716+ je vybaven následujícími parametry:

3.6.2 Vnitřní parametry

- CPU Intel Celeron N3150, čtyři jádra 1,6 GHz (při dočasném přetaktování až 2,08 GHz), systém hardwarového šifrování AES-NI.
- CPU obsahuje hardwarový převodní systém videosouborů ve formátu H. 264 (Advanced Video Coding), MPEG-2 a VC-1 při rozlišení až 4K (4096 x 2160) 30 snímků za sekundu pro jeden stream a při rozlišení FullHD (1920 x 1080) 30 snímků pro 3 streamy současně.

  Ostatní formáty videa, např. velmi rozšířený MPEG-4, lze dekódovat pouze softwarovou cestou a zde se uplatní výkon procesoru (jen pro zajímavost při osobním testování dokázal procesor softwarově převzorkovat videosoubor v reálném čase bez sekání až do rozlišení 1920 x 1080 při datovém toku max. 15 000 Mbps).
- RAM 2 GB DDR3 (Double Data Rate 3)
- Podpora souborových systémů (pro interní disky): EXT4 a nový Btrfs (B-tree file systém), kontroluje integritu dat, úsporu dat při vytváření několika verzí souboru atd.

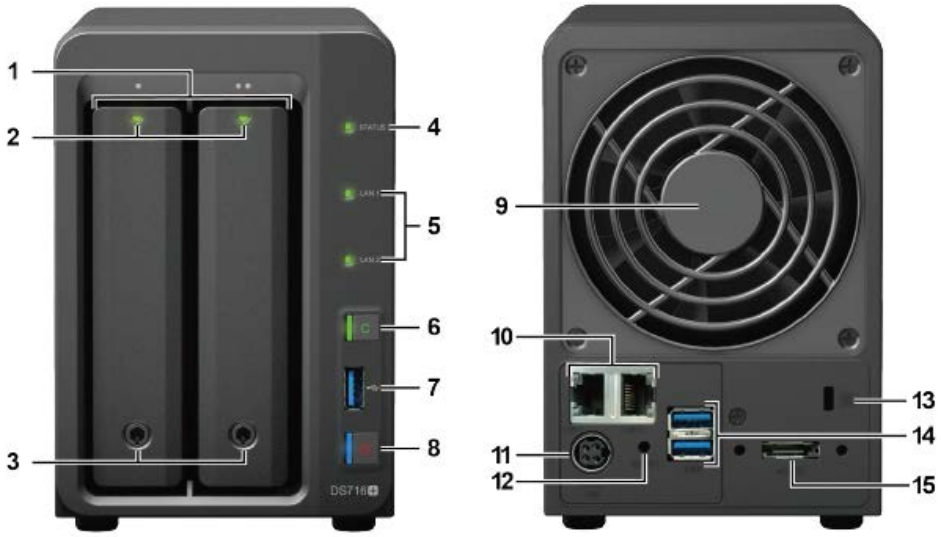
- Podpora souborových systému (externí disky):Btrfs, EXT4, EXT3 (third extended filesystem), FAT (File Allocation Table), NTFS (New Technology File Systém), HFS+ (Hierarchical File Systém +)
- Podporované typy svazků: Základní, JBOD (Just a Bunch Of Disks), Synology Hybrid RAID, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 (poslední 3 typy lze použít pouze v případě zapojení 3 a více disků zapojených v expanzní jednotce).
- Synology DiskStation Manager: operační systém, který je bezesporu hlavní výhodou a přidanou hodnotou oproti ostatním značkám a řešením. Měl jsem osobně možnost dlouhodobě vyzkoušet systémy od společností Qnap, Asustor i Synology a poslední z trojice je dle nejen mého názoru absolutní vítěz. Obzvláště poslední verze 6.0 je perfektně odladěná, stabilní, intuitivní, podrobně konfigurovatelná a hlavně pravidelně aktualizovaná. Tento pokročilý systém postavený na Linuxu poskytuje opravdu nepřeberné množství konfiguračních možností [21], [22].

3.6.3 Vnější parametry

1. Šachty pro 2 HDD 3,5" / 2,5" SATA II/III s podporou výměny pevných disků za provozu.
2. Led diody indikující status instalovaných disků.
3. Zámky šachet pro zabezpečení disků proti krádeži nebo neoprávněnému vysunutí.
4. Led dioda indikující přítomnost operačního systému DSM (DiskStation Manager) a přítomnost bloků s daty.
5. Led diody indikující 10/100/1000BaseT konektivitu případně problémy s připojením Ethernetových konektorů.
6. Tlačítko kopírování sloužící pro okamžité zkopírování obsahu USB úložiště do předem definovaného adresáře na interním disku za účelem možnosti okamžité zálohy a sdílení v osobním cloudu.
7. Port USB 3.0, sloužící primárně k funkci USB kopírování souborů viz bod 6, ovšem lze využít i k napojení ostatních zařízení jako tiskárny, disky atd.
8. Zapínací/Vypínací tlačítko, pro vypnutí je potřeba stisknout a držet dokud neuslyšíme varovný signál.
9. Větrák podporující pasivní chlazení procesoru a disků (hladina hluku 18 dB).
10. Duální LAN porty RJ45 10/100/1000BaseT s podporou režimů Failover (nepřetržité využití sítě i tehdy, pokud na jednom portu dojde k poruše LAN připojení) a Link Aggregation (vylepšuje rychlost připojení s využitím více síťových kabelů) [8].

11. Konektor napájecího adaptéru (65 W), spotřeba energie serveru při zatížení 18,96 W, spotřeba při hibernaci disků 8,84 W.
12. Tlačítko RESET, po dlouhém stisku a zaznění varovného signálu, obnoví základní IP adresu, DNS server a heslo správce do původního nastavení.
13. Kensington bezpečnostní slot pro možnost přimknutí serveru k zámku.
14. 2x USB 3.0 port k připojení zařízení USB jako externí HDD, tiskárny atd., lze využít k dalšímu rozšíření úložného prostoru.
15. eSATA (External Serial ATA) port k připojení expanzní jednotky až se 7 rozšiřujícími interními disky a možností jejich začlenění do pole RAID 5, 6 a 10 [21], [22].

Celkové rozměry: 157 mm x 103.5 mm x 232 mm



Obr. 14. NAS server Synology Diskstation DS716+ [21].

3.6.4 Výběr pevného disku

Životně důležitou součástí NAS serveru jsou interní pevné disky. Ovšem ne všechny typy disků jsou pro použití v serveru vhodné, jelikož disk v serveru, na rozdíl od počítače, je aktivní prakticky neustále. Z toho důvodu je potřeba zvolit disk uzpůsobený z výroby na neustálý provoz tzv. 24/7, neboli 24 hodin 7 dní v týdnu.

Po prostudování recenzí všech známých modelů na trhu byl nakonec vybrán 3,5" disk Western Digital RED 3 TB. Tento model byl vybrán, jelikož disponuje nejlepšími parametry v porovnání ceny za GB, statisticky nízké poruchovosti a dobrému poměru ceny a výkonu [23].

Model disponuje následujícími parametry:

- Navržen výrobcem pro práci s NAS serverem, kdy zajišťuje plnou kompatibilitu, optimalizaci výkonu a rozšířenou podporu zapojení do pole RAID díky firmwaru NASWare 3.0.
- Konstruován pro nepřetržitý provoz 24/7, o 35 % delší střední doba mezi poruchami oproti klasickým diskům (WD Green), 600 000 parkovacích cyklů hlav.
- Rychlost zápisu: max. 155 MBps.
- Rychlost čtení: 160 MBps.
- Rozhraní SATA 3.
- Vyrovnávací paměť: 64 MB.
- Otáčky: 5400 otáček za sekundu s technologií regulace pro úsporu energie [23].

Obr. 15. HDD Western Digital Red 3 TB.

3.7 Chytrá žárovka Lifx Color 1000 E27

Chytré žárovky jsou v této době (rok 2016) zatím pomalu zaváděná novinka začínajícího segmentu chytré domácnosti a z toho důvodu je výběr na našem domácím trhu naprosto žalostný. Dají se koupit pouze některé modely od čínských výrobců, ovšem tyto žárovky podporují pro komunikaci pouze technologii Bluetooth, takže se nedají zapojit jednoduše přímo do domácí sítě, mají nepoužitelný ovládací software a kvalitu zpracování.

Jediná použitelná žárovka, splňující požadavky jako komunikace pomocí WiFi, dostatečná svítivost a především použitelný software s dostatečnou možností konfigurace pro platformu Android a Windows, je žárovka od firmy Philips s názvem Hue a dále Lifx. Ovšem jen žárovka Lifx dovoluje komunikovat samostatně napřímo s routerem a nepotřebuje žádného

prostředníka v podobě centrálního hubu. Z toho důvodu byla nakonec vybrána žárovka Lifx Color 1000 ve verzi pro evropský (Edisonův) závit E27.

Bohužel z důvodů, které byly popsány výše, bylo nutné si žárovky objednat přímo od výrobce z USA. Tato zkušenost byla ovšem spjata s určitými riziky, jako nemožnost reklamace (doprava by stála více než samotná žárovka) a nakonec i zdlouhavá a nákladná komunikace s celním úřadem.

Žárovka Lifx Color 1000 E27 disponuje následujícími parametry:

- Svítivost: 1055 lm (ekvivalent 75 W).
- Životnost: 24984 hodin (22,8 roku při svícení 3 hodiny denně).
- Spotřeba: 11W při plném výkonu.
- Rozměry: 63 mm x 115 mm.
- Hmotnost: 240 g.
- Úhel paprsku: 130°.
- Teplota Barev: 2500 K – 9000 K.
- Možnost nastavení 16 miliónů barev včetně teplé i studené bílé barvy.
- Možnost nastavit u každé barvy jas a intenzitu.
- Parametry připojení k routeru: podpora standardu IEEE 802.11b/g na kanálu 2,4 GHz při nastavení bezpečnostního protokolu WPA2.
- Podpora platforem univerzální aplikace: iOS 8.0+, Android 4.0+, Windows 10 Univerzální aplikace.
- Podpora aplikací třetích stran: pomocí široké uživatelské základně se začíná implementovat podpora u různých aplikací pro automatizaci u mobilních zařízení se systémem Android i iOS (př. Tasker, Automateit).
- Oficiální podpora služby IFTTT [24].

Obr. 16. Chytrá žárovka Lifx Color 1000 E27.

3.8 Venkovní IP kamera Foscam FI9828P

Pro využití kamerového systému bylo rozhodnuto až v průběhu práce. Z toho důvodu je nemám zahrnuty ani ve svém oficiálním zadání. Ovšem při studiu problematiky a možností dnešních moderních sítí jsem si uvědomil, že by byla velká škoda nezačlenit kamerový systém do svého projektu.

Při výběru IP kamery byly kladeny následující požadavky:

- Nejdůležitějším parametrem, který byl požadován, je oficiální podpora kamery u monitorovací aplikace Surveillance Station společnosti Synology. Díky této podpoře je zaručena 100% spolupráce kamery s NAS serverem, které je docíleno přítomností ovladačů odladěných přímo pro určitý typ kamery.
- Druhým nejdůležitějším parametrem při výběru byla bezesporu kvalita přijímaného obrazu a velikost zorného úhlu. Proto bylo potřeba, aby měla čočka rozlišení minimálně 720p (tedy 1280x720) při 23 snímcích za sekundu a diagonální (úhlopříčný) zorný úhel alespoň 70°.
- Další důležitý parametr komunikace IP kamery a NAS serveru je podpora univerzálního standardu ONVIF. Díky tomuto parametru lze zaručit použitelnost kamer i v případě, že bude v budoucnu potřeba přejít na NAS jiné značky nebo komunikace s jiným zařízením podporujícím tento standard.
- Při návrhu vhodného umístění kamery bylo rozhodnuto, za účelem pokrýt co největší monitorovanou oblast co nejmenším počtem kamer, využít kameru typu PTZ (Pan Tilt Zoom) a umístit ji do rohové části domu, ve které bude mít možnost monitorovat všechny vchody do domu a zároveň většinu pozemku včetně příjezdových cest.
- Kvůli potřebě monitorovat oblast i v nočních hodinách (z důvodu bezpečnosti) bylo potřeba k výběru přidat možnost podsvícení zorné oblasti pomocí infračervených diod (takzvaný noční režim) alespoň do vzdálenosti 20 m.
- Z důvodu ušetření šířky síťového pásma a prostoru na pevném disku při záznamu bylo potřeba zajistit podporu moderního kompresního standardu videa H.264, který potřebuje méně než polovinu místa a propustnosti, kterou požaduje MPEG-4 a 80% méně v porovnání s MJPEG, což jsou formáty používané u starších kamer [25].

Při procházení nabídky byla po dodržení co nejlepšího poměru cena/kvalita a výše uvedených požadavků nakonec vybrána venkovní IP kamera Foscam FI9828P.

IP kamera Foscam FI9828P má následující parametry:

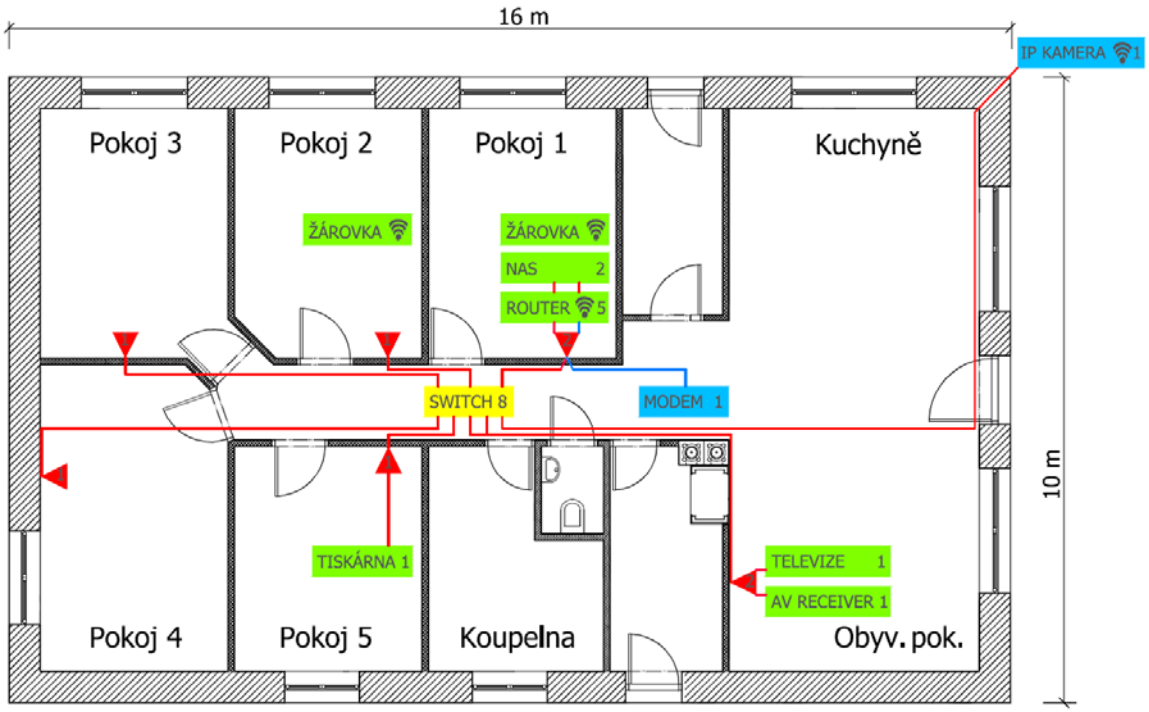
- Senzor: 1/3" CMOS
- Objektiv: světelnost 1.6 F, ohnisková vzdálenost: 2.8mm-12mm
- Kvalita zobrazení: max. rozlišení 1280x960 při 30 snímcích za sekundu, podpora úsporného kompresního standardu videa H.264 .
- Diagonální zorný úhel (úhlopříčný) max. 75° bez použití optického zoomu (schopnost objektivu měnit svou ohniskovou vzdálenost, zvýšením obraz přiblížíme).
- Horizontální zorný úhel (vodorovný) 30-70°, zvyšováním zoomu bude postupně docházet ke zvyšování ohniskové vzdálenosti a zmenšení zorného úhlu.
- PTZ: kameru lze horizontálně otočit o 355°, vertikálně naklonit o 78° a přiblížit 3x pomocí optického zoomu.
- Noční přisvětlení pomocí infračervených diod do vzdálenosti 20 m, s možností volby automatického nebo manuálního spuštění.
- Webové rozhraní sloužící ke konfiguraci a samotnému sledování kamer. Veškeré mé nastavení tohoto rozhraní budu popisovat v konfigurační části práce.
- WiFi standardu IEEE 802.11b/g/n se zabezpečením WEP,WPA,WPA2.
- Konektory: LAN port RJ-45 10/100BaseTX, externí mikrofon a reproduktor pomocí konektoru 3,5mm jack, External I/O sloužící ke spolupráci s alarmem.
- Podpora síťových protokolů, ONVIF, HTTP, HTTPS, TCP/IP, UDP, FTP, DHCP, DDNS, UPNP, P2P.
- Voděodolnost (certifikace IP66).
- Provozní teplota: od -20°C do 60°C.
- Rozměry: 153 x 92 x 86 mm.
- Maximální spotřeba: 4,2 W [25].

Obr. 17. Foscam FI9828P.

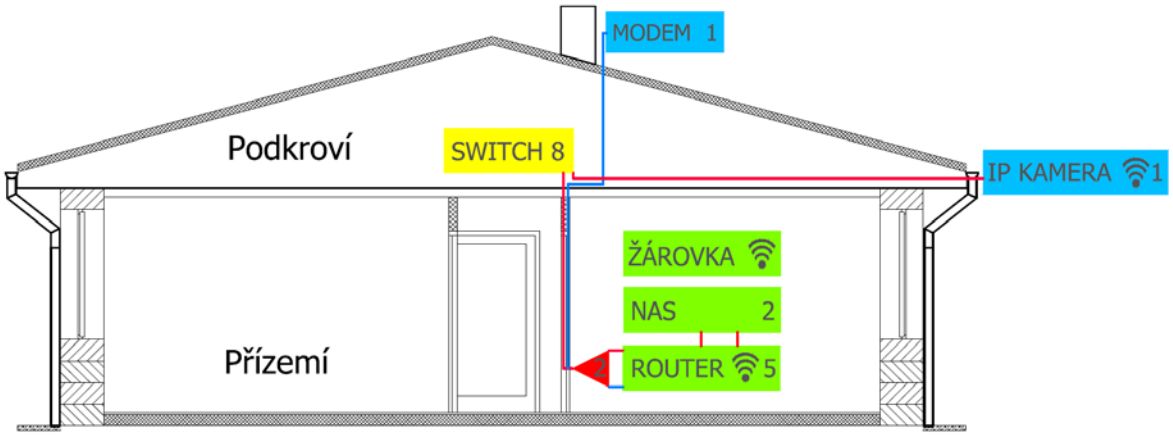
4 ZAPOJENÍ SÍTĚ

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

4.1 Návrh síťové infrastruktury



Obr. 18. Návrh síťové infrastruktury (pohled z vrchu).

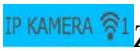


Obr. 19. Návrh síťové infrastruktury (řez pokoj č. 1).

1. WAN rozvody Gembird UTP CAT5E
2. LAN rozvody Solarix CAT6 UTP PVC
3. 

Značka pro multimediální zásuvku ELKO EP 21544 (1 Ethernet port)
4. 

Značka pro multimediální zásuvku ELKO EP 21546 (2 Ethernet porty)
5. 

Značka pro modem UBIQUITI PowerBeam M5 300 (1 Ethernet port)
6. 

Značka pro venkovní IP kameru Foscam FI9828P
7. 

Značka pro router Asus RT-AC68U (WiFi, 5 Ethernet portů)
8. 

Značka pro switch TP-LINK TL-SG108E (8 Ethernet portů)
9. 

Značka pro NAS server Synology DS716+ (2 Ethernet porty)
10. 

Značka pro chytrou žárovku Lifx Color 1000 (WiFi)
11. 

Značka pro chytrou televizi LG 47LB679V-ZF (1 Ethernet port)
12. 

Značka pro AV Receiver Yamaha Yamaha RX-V775 (1 Ethernet port)
13. 

Značka pro multifunkční tiskárnu Samsung M2070 (1 Ethernet port)

První pohled shora přehledně zobrazuje rozmístění a propojení jednotlivých síťových prvků včetně typu konektivity, kdy číslo u prvku definuje počet Ethernetových portů. Při podpoře bezdrátové komunikace je rovněž uveden znak.

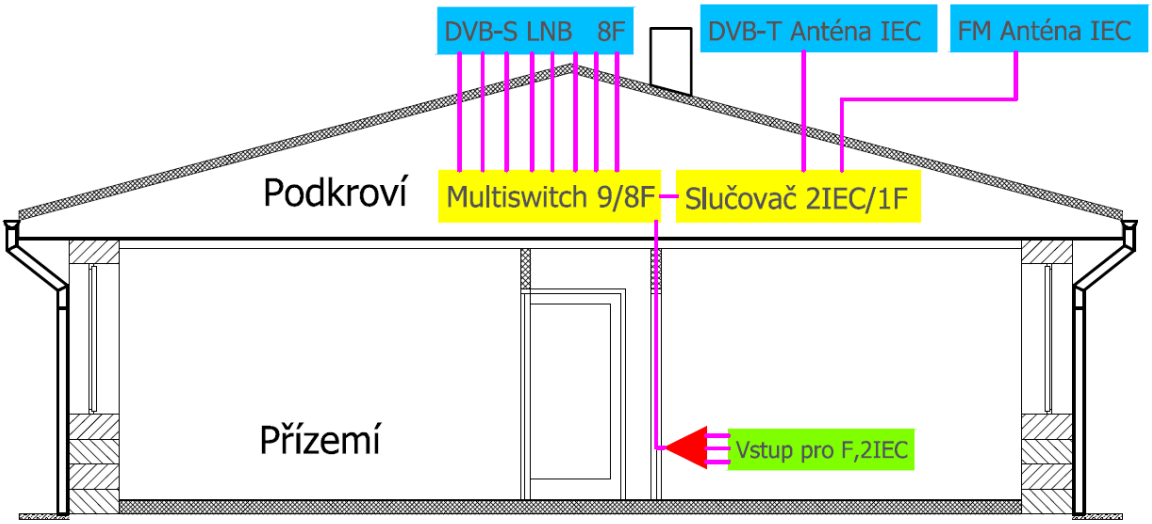
Dále lze podle barev určit polohu. Modrá značí umístění venku, zelená v přízemí a žlutá v podkroví.

Druhý pohled zobrazuje řez pokojem č. 1, kde ujasní vertikální rozmístění prvků a jejich propojení.

4.2 Instalace rozvodů

Síťové, DVB-T (Digital Video Broadcasting - Terrestrial), DVB-S (Digital Video Broadcasting - Satelite) a rádiové rozvody byly rozmístěny do všech 6-ti obytných pokojů rodinného domu. V práci budou podrobně popsány pouze rozvody síťové. Ostatní rozvody jsou nad rámec zadání práce. Ovšem jelikož jsem zvolil multimediální zásuvku, tak pro úplnost alespoň zkráceně nastíním jejich zapojení.

4.2.1 Nastínění zapojení televizních a rádiových rozvodů



Obr. 20. Návrh DVB-T,S a rádiové infrastruktury (řez pokoj č. 1).

U těchto rozvodů byl použit koaxiální kabel. Nejprve byly sloučeny signály z DVB-T a FM (Frequency Modulation) analogové antény pomocí slučovače se zabudovaným zesilovačem signálu se 2 vstupy konektoru IEC a výstupem na F konektor. Nakonec byl výstup slučovače připojen na vstup Multiswitche určený pro tyto účely.

Dále bylo svedeno 8 výstupů z LNB (Low-noise block) Konvertoru satelitní antény na vstupy Multiswitche rovněž pomocí F konektorů na obou stranách.

Nyní už stačilo natáhnout mezi Multiswitchem a zásuvkou pomocí ohebné trubice koaxiální kabel. Na libovolném výstupu Multiswitche připojit kabel F konektorem a poté druhou stranu napojit na zásuvku (viz 4.2.2).

4.2.2 Instalace síťových rozvodů

Pro instalaci síťových rozvodů bylo zakoupeno 100 m kabelu UTP CAT6 PVC Solarix. Ještě před instalací se bylo potřeba dostatečně zahalit a nasadit si kolem obličeje roušku. Na půdě je po celé podlaze rozložena skelná vata. Kabel byl veden z půdy zdmi až k otvorům pro zásuvky pomocí plastových ohebných trubic, kterým se také říká „husí krk“. Tyto hadice byly instalovány do zdí již při stavbě domu. Pomocí ohebných trubic lze kabely kdykoliv relativně jednoduše vyměnit, nebo přidat další.

Ovšem v mém případě jsem narazil na problém s nedostatečnou tloušťkou hadice, jejíž vnitřní průměr je 15mm, kdy hlavně v případě pokoje č. 1 a 6 (obývací pokoj) byly protáhnuty 3 kabely (2 síťové a koaxiální). Nakonec byl do hadice nejprve vsunut vázací drát o průměru cca 3 mm, jehož hrot byl zaoblen izolační páskou. Po dosažení drátu druhé strany byly konce kabelů přichyceny páskou k drátu, tak aby jej obklopovaly do trojúhelníku a zároveň byly zaobleny ostré hrany. Bylo nutné kabely tahat z přízemí pomocí drátu a zároveň je v podkroví pouze rovnat aby se v hadici nezpříčily. Doporučuji ještě alespoň po každých několika metrech kabely něčím namazat (v mém případě mazivo WD-40). Po protažení bylo v přízemí necháno vyčnívat cca půl metru kabelu od zdi. Stačilo by i méně cca 10 cm, ale pokud by se při osazování zásuvky něco nepodařilo a kabel by byl bez rezervy, prodražilo by se to daleko více než ztráta půl metru kabelu.

V podkroví bylo následně odvinuto potřebné množství kabelu, aby dosáhl do středu domu co nejefektivnější cestou mezi příčníky podél středu domu (viz. 4.1). Konec se bude později osazovat konektorem RJ45 a připojovat k switchi. Rovněž doporučuji před finálním odstřihnutím nejprve odvinout minimálně půl metru rezervu a 10 cm od konce kabel nějak označit, aby bylo později ve zněti kabelů jasné, ke kterému pokoji kabel patří. V mém případě byla rovněž použita černá izolační páska, kdy se číslo pokoje rovnalo počtu po sobě jdoucích proužků.

Tímto způsobem byly nataženy kabely i pro ostatní pokoje s tím rozdílem, že u pokojů č. 2-5 je potřeba natáhnout pouze jeden síťový kabel.

Obr. 21. Rozvod kabelů pomocí plastových hadic (podkroví).

V dalším kroku byly zapojeny zásuvky v jednotlivých pokojích. Pro lepší názornost podrobně popíši zapojení zásuvky ELKO EP 21544 s jedním síťovým portem. Varianta se 2 síťovými porty se zapojuje zcela identicky.

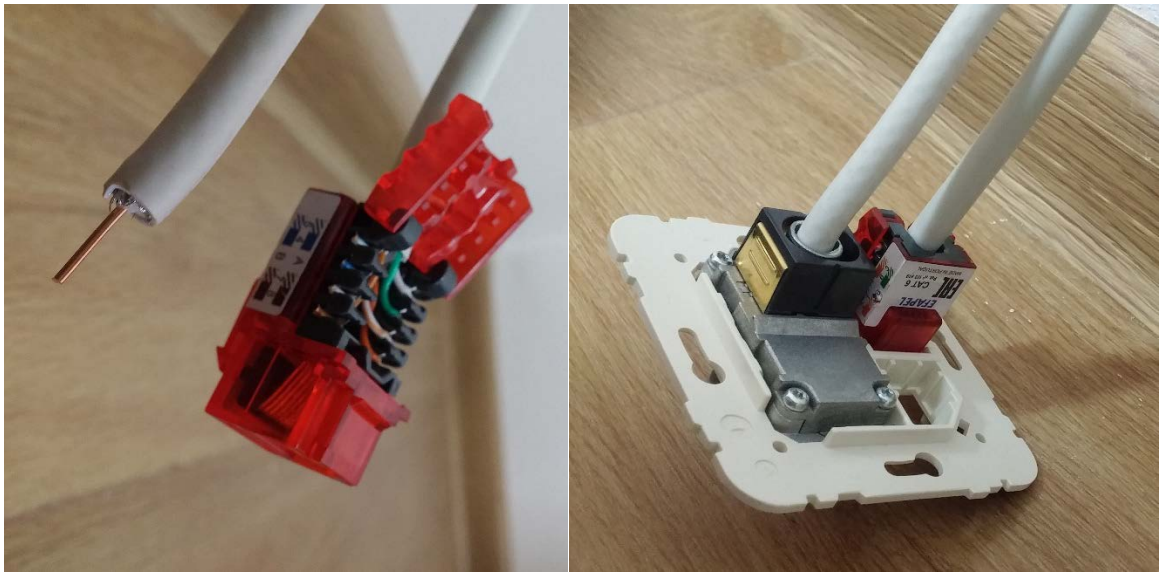
Nejprve bylo zapotřebí zastřihnout kabely na stejnou délku. U koaxiálního kabelu odřezat ostrým nožem cca 1,5 cm bužírky, opletení, stínící fólii až na střední vodič, který má na konci vyčnívat sám z kabelu. U síťového kabelu opatrně odřezat 3 cm bužírky. Jsou viditelné 4 páry kroucené dvojlinky oddělené plastovým křížem. Tyto páry je nutno jeden po druhém rozplést a narovnat. Plastový kříž v odhalené části u konce ustřihneme. Takto nachystaný kabel vsuneme do konektoru a zapojíme podle standardního nekříženého rozložení vodičů 1 až 8 v pořadí dle standardu TIA 568B:

Levá strana konektoru: 1 bílo oranžová, 2 oranžová, 3bílozelená, 4 modrá

Pravá strana konektoru: 5 bílo modrá, 6 zelená, 7 bílo hnědá, 8 hnědá

Po zapojení konce vodičů zastřihneme a konektor upevníme do zásuvky.

Při zasunování koaxiálního kabelu musíme dát pozor, abychom se dostali stínící tyčí, která vyčnívá na zásuvce v uchycovacím mechanizmu pro koaxiální kabel, mezi bužírku a stínící fólii. Poté kabel v mechanizmu zajistíme potlačením do boku, čímž se do kabelu zařežou po bocích 2 drážky.



Obr. 22. Zapojení zásuvky ELKO EP 21544.

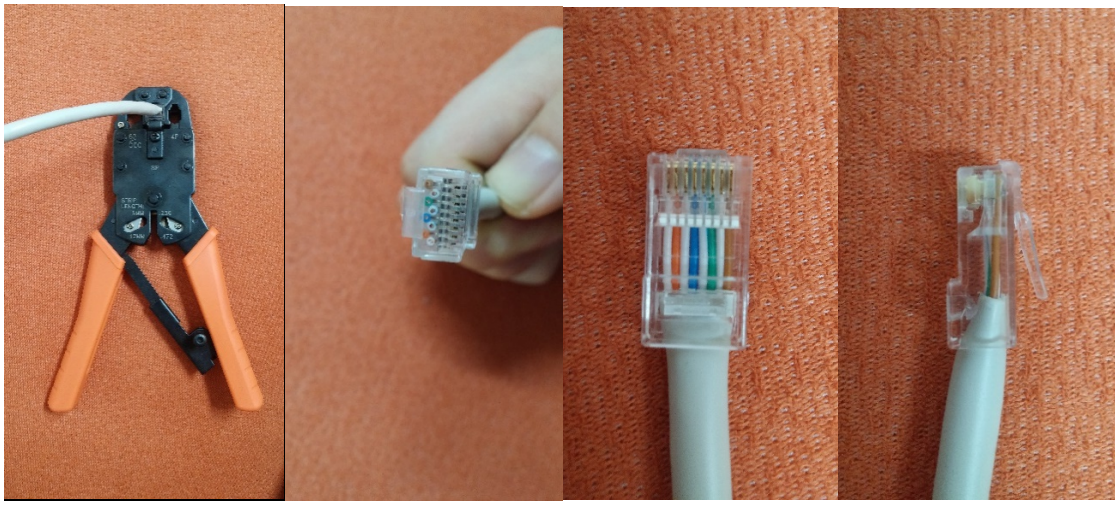
Zásuvka je nyní připravena na instalaci do zdi. Přebytečnou délku kabelu zatlačíme do gumové hadice, zásuvku přišroubujeme ke zdi, narazíme rámeček ELKO EP 90910 a krytku ELKO EP 90770.

Obr. 23. Instalace zásuvky ELKO EP 21544.

Nakonec byly osazeny konektory RJ45 na straně u switche. Příprava kabelu i pořadí vodičů jsou totožné jako u zásuvky. Seřazené vodiče podle standardu TIA 568B co nejdůkladněji narovnáme vedle sebe a následně je 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 zároveň s přední částí. Po dodržení těchto zásad můžeme přebytečnou délku vodičů na začátku kabelu až po začátek vložky ustřihnout.

Nyní nám nic nebrání uchopit konektor a zasunout jej tak, aby byl zobáček vložky na spodní části konektoru. Konektor důkladně dotlačíme. Vložka s vodiči se musí dotýkat okraje konektoru. 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.



Obr. 24. Instalace konektoru RJ45 CAT6.

Po zhotovení konektorů a zásuvek ve všech pokojích jsem přešel k testování. Pro tyto účely mi posloužil tester kabelů Logilink, kterým jsem proměřil správnou průchodnost elektrických signálů postupně všemi 8 vodiči v kabelu.

4.3 Instalace a zapojování síťových prvků

4.3.1 Radiomodem UBIQUITI PowerBeam M5 300

Modem, jako jediný síťový prvek, byl instalován s asistencí servisního technika poskytovatele Internetového připojení pro obec Jablůnka a Pržno firmy Anex s.r.o.

Modem byl umístěn tak, aby měl přímý výhled na věž místního kostela, kde je umístěn vysílač. Z toho důvodu byl pro umístění vybrán komín, jelikož je vůči vysílači v nejlepší pozici. Při instalaci byl nejprve přišroubován držák, do kterého byl modem usazen a správně nasměrován.

Následně byl vyvrtán otvor do střechy, jimž byl provlečen UTP kabel CAT5e a natažen až ke switchi. Na straně modemu byl na konci kabelu osazen konektor RJ45 a zasunut do samotného modemu. Následně byly zatmeleny okraje vrtaného otvoru.

V podkroví byl nejprve osazen konektor RJ45 a zapojen do napájeného portu POE (Power On Ethernet) pasivního injektoru. Pasivní injektor byl zapojen do zásuvky s přepěťovou ochranou. Z injektoru byl veden kabel UTP RJ45 CAT5e ohebnou trubicí do pokoje č. 1, kde byl jeho konec osazen do levého konektoru RJ45 zásuvky ELKO EP 21546 (viz 4.2.2). Ze zásuvky byl následně veden kabel RJ45 CAT5e do portu WAN (Wide Area Network) routeru Asus RT-AC68U.

Obr. 25. Instalace radiomodemu UBIQUITI PowerBeam M5 300, zapojení pasivního injektoru.

4.3.2 Router Asus RT-AC68U

Router byl strategicky umístěn do středu domu pro rovnoměrnou distribuci bezdrátového signálu. Byl položen na rohovou skříňku překrývající multimediální zásuvku v pokoji č.1. Všechny 3 antény pro bezdrátovou komunikaci byly zašroubovány do příslušných konektorů a postaveny kolmo k routeru. Následně byly 2 boční antény mírně nahnuty směrem od prostřední antény zhruba o 5-10°. Tím bylo zajištěno co nejvíce odrazů signálu u technologie MIMO čímž zajistíme optimální rychlost WiFI sítě odesíláním a přijímáním několika datových streamů současně [26].

Po připojení antén byly zapojeny konektory následovně:

- WAN: připojení modemu UBIQUITI PowerBeam M5 300 pomocí kabelu UTP CAT5e v režimu 100BaseT.
- LAN1: připojení NAS serveru pomocí UTP kabelu CAT6 v režimu IEEE 1000BaseT
- LAN2: záložní připojení NAS serveru pomocí UTP kabelu CAT6 v režimu IEEE 1000BaseT, využívá režimu Failover (nepřetržité využití sítě i tehdy, pokud na jednom portu dojde k poruše LAN připojení).
- LAN3: připojení Switche pomocí UTP kabelu CAT6 v režimu IEEE 1000BaseT.
- LAN4: port určený pro připojení zařízení majitele pokoje č. 1 dle potřeby, kabel UTP CAT6 vyveden k pracovnímu stolu.

Po zapojení konektoru byl připojen napájecí adaptér do přepěťové ochrany.

Obr. 26. Router Asus RT-AC68U umístění a zapojení.

4.3.3 NAS server Synology Diskstation DS716+

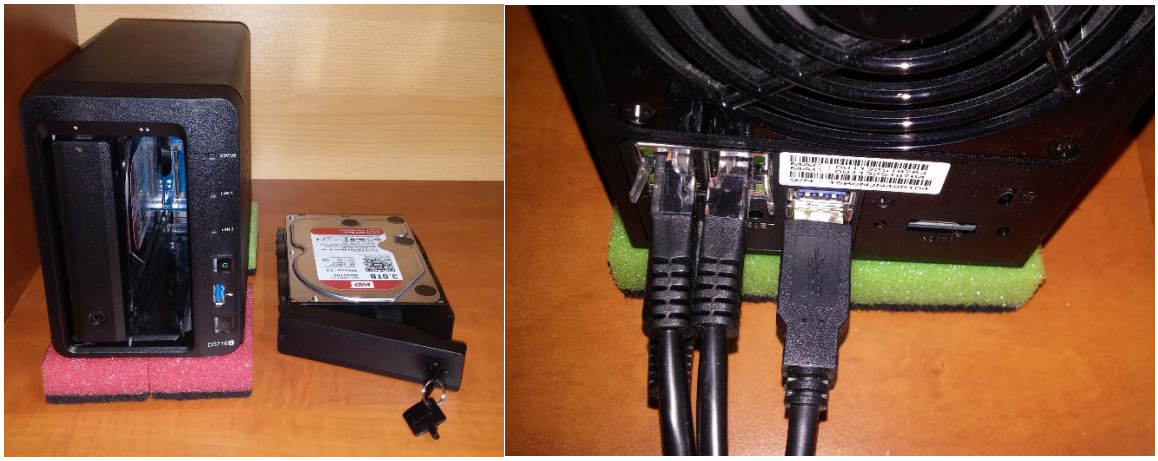
NAS byl strategicky umístěn do spodní police poblíž routeru a zásuvky kvůli dostatečnému odhlučnění několika vrstvami dřevotřísky, přehlednému umístění všech klíčových prvků na jedno místo pro pohodlnou správu a také vytvoření co nejkratších kabelových spojů. V poličce byl zajištěn dostatečný odvod tepla a cirkulace vzduchu vytvořením výřezů do zadní stěny. Tyto výřezy byly zároveň použity pro rozvody kabeláže.

Po dlouhodobém testování bylo zjištěno, že při maximálním zatížení disků server natolik vibruje, až rozkmitá desku pod sebou, což má za následek průnik hluku. Z toho důvodu byla vložena mezi server a desku tlumící vrstva. Po vyzkoušení několika materiálů se jevila jako nejúčinnější vrstva tvrdého polyuretanu zakončena vrstvou tvrdých drátěných vláken (houbička od firmy Spontex). Díky této mezivrstvě došlo ke značnému snížení hlučnosti a odstranění vibrací.

Obr. 27. NAS serveru Synology Diskstation DS716+ umístění.

V dalším kroku byly zapojeny do serveru disky. Nejprve odemkneme klíčem slot, který chceme vyjmout. Stiskneme spodní část slotu a vyskočí rukojeť. Tuto rukojeť uchopíme a vytáhneme slot ven.

Slot má podélně po stranách upevňovací panely. Tyto panely vyloupneme. Nyní můžeme do slotu vložit disk určený pro provoz 24 hodin 7 dní v týdnu (v mém případě Western Digital RED 3TB 3,5”). Disk vkládáme tak, aby byl shora viděn štítek disku a zároveň byl konektor v zadní části slotu (dál od úchytky). Dále disk ve slotu zajistíme přicvaknutím obou upevňovacích panelů. Takto připravený disk zasuneme na doraz do prázdného tunelu v serveru. Zajistíme rukojeť do slotu a nakonec slot zamkneme. Tento postup se opakuje i při zapojení druhého disku [22].



Obr. 28. NAS serveru Synology Diskstation DS716+ zapojení HDD a konektorů.

Konektory serveru byly zapojeny následovně:

- Port 1: připojení k routeru pomocí UTP kabelu CAT6 v režimu IEEE 1000BaseT
- Port 2: záložní připojení k routeru pomocí UTP kabelu CAT6 v režimu IEEE 1000BaseT, využívá režimu Failover (nepřetržité využití sítě i tehdy, pokud na jednom portu dojde k poruše LAN připojení)
- USB 3.0: port vyveden prodlužovacím kabelem na poličku pro snadné připojení externího disku

Po zapojení konektorů byl zapojen napájecí adaptér do přepěťové ochrany. V budoucnu bude dokoupen záložní zdroj UPS (Uninterruptible Power Source) který zajistí bezpečné vypnutí při výpadku elektrické sítě.

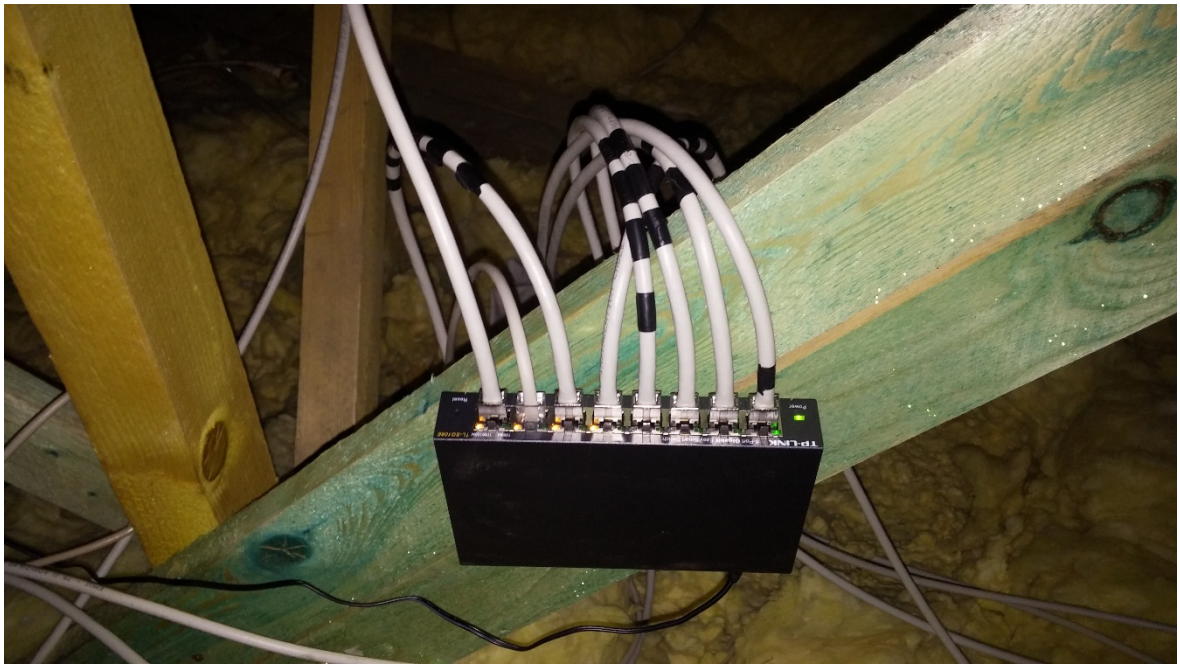
4.3.4 Switch TP-LINK TL-SG108E

Switch byl strategicky umístěn na půdu přibližně do středu domu. Volbou tohoto umístění bylo možné elegantně propojit všechny obytné pokoje v domě, aniž by kabeláž jakkoliv překážela. Zároveň výběrem switche se vzdálenou správou a diagnostikou připojených portů odpadá i nevýhoda špatného přístupu.

Samotný switch byl připevněn dvěma přiloženými šrouby do desky spojující 2 střešní trámy. Poté co jsem si již dříve nachystal kabeláž, stačilo pouze konektory vhodně připojit. Zapojení switche je přehledně vidět na Obr. 1. Návrh síťové infrastruktury (pohled shora).

Pro úplnost porty raději rozepíšu:

- Port 1: připojení k zásuvce pokoje č. 1 pomocí UTP kabelu CAT6 v režimu IEEE 1000BaseT (Router Asus RT-AC68U)
- Port 2-5: připojení postupně k zásuvce pokoje 2-5 pomocí UTP kabelu CAT6
- Port 6,7: připojení k zásuvce obývacího pokoje s 2 porty RJ45 pomocí UTP kabelu CAT6 v režimu IEEE 100BaseT (port 6 = TV, Port 7 = AV Receiver)
- Port 8: připojení k venkovní IP kameře pomocí UTP kabelu CAT6 v režimu IEEE 100BaseT



Obr. 29. L2 switch TP-LINK TL-SG108E – zapojení.

Po zapojení konektorů byla ke kameře zavedena zásuvka na střídavé napětí 230 V/50 Hz. Tato zásuvka byla z důvodu bezpečnosti doplněna o přepěťovou ochranu.

4.3.5 Venkovní IP kamera Foscam FI9828P

Kamera byla připevněna ke kovové konstrukci v rohové části domu za účelem pokrýt co největší monitorovanou oblast a využít tak plného potenciálu PTZ kamery. Díky tomuto umístění lze monitorovat všechny vchody do domu a zároveň většinu pozemku, včetně příjezdových cest. Kovová konstrukce byla vytvořena na míru a má délku 50 cm. Díky tomu je zajištěna viditelnost ze všech stran bez překážek (př odtokový systém). Kamera je ke kovové konstrukci připevněna čtyřmi šrouby. Na opačné straně konstrukci zajišťuje objímka uchycená ke stožáru pro reflektor.

Vznikla možnost později podle potřeby měnit polohu kamery natáčením nebo změnou výšky v rozsahu výšky stožáru. Kabeláž byla uchycena vázacími pásky a koncová část s konektory poté umístěna do dřevěné dutiny pod střechou kvůli ochraně před deštěm a dalším nepříznivým vlivům počasí.

Obr. 30. Venkovní IP kamera Foscam FI9828P – montáž.

Pro komunikaci byl natažen UTP kabel CAT6 od switche z portu 8 až do samotné střešní dutiny, kde byl propojen konektorem RJ45, kamera se switchem komunikuje v režimu IEEE 100BaseT. Kamera rovněž podporuje bezdrátovou komunikaci pomocí WiFi. Rozhodl jsem se využívat bezdrátovou komunikaci pouze jako zálohu v případě poruchy té kabelové, aby se zbytečně nezatěžovala šířka pásma bezdrátové sítě.

Obr. 31. Venkovní IP kamera Foscam FI9828P – zapojení.

Kamera bohužel nepodporuje napájení pomocí POE neboli přes síťový kabel jako třeba výše uvedený radiomodem. Z toho důvodu byla ke kameře zavedena zásuvka na střídavé napětí 230 V/50 Hz. Tato zásuvka byla z důvodu bezpečnosti doplněna o přepěťovou ochranu.

4.3.6 Ostatní trvale zapojená zařízení

Zapojení ostatních zařízení je již triviální:

Chytrou žárovku Lifx Color 1000 E27 je možno zašroubovat do evropského (Edisonova) závitu E27 v lampě, lustru nebo jakémkoliv jiném typu světla a zajistit dosah WiFi signálu a napájení.

Televizor LG 47LB679V-ZF, AV Receiver Yamaha Yamaha RX-V775 a tiskárnu Samsung M2070 připojíme pomocí UTP kabelu přes zásuvku na switch (viz 4.1)

Obr. 32. Žárovka Lifx Color 1000, Televizor, AV Receiver – zapojení.

5 KONFIGURACE SÍŤOVÝCH PRVKŮ

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

5.1 Radiomodem UBIQUITI PowerBeam M5 300

Radiomodem nebyl konfigurován autorem práce, ale technikem poskytovatele Internetového připojení firmy Anex s.r.o., Z toho důvodu mi nebyly poskytnuty přihlašovací údaje do administrace radiomodemu. Po konzultaci s poskytovatelem bylo zjištěno, že je zařízení konfigurováno jako wireless bridge (bezdrátový most) mezi centrálním routerem poskytovatele a mým klientským routerem.

5.2 Router Asus RT-AC68U

5.2.1 Instalace neoficiálního firmware

Ještě před konfigurací routeru byl z důvodu lepší optimalizace a podrobnější konfigurovatelnosti (hlavně v oblasti VPN) nahrazen oficiální firmware výrobce s názvem ASUSWRT za komunitně upravovaný a tudíž neoficiální ASUSWRT-Merlin [27].

Po stažení firmware ze stránek výrobce je nutno připojit se v lokální síti připojit do administrace routeru. Toho lze docílit otevřením internetového prohlížeče a přejít na základně předdefinovanou IP adresu routeru http://192.168.1.1, poté zadáme předdefinované přihlašovací jméno a heslo (udávané na zadním štítku routeru).

V administraci zvolíme Správa \ Aktualizace Firmwaru \ Nový soubor firmwaru \ Procházet a pomocí průzkumníka souborů najdeme stažený soubor RT-AC68U_380.58_0.trx případně novější verzi a zvolíme Nahrát. Počkáme několik minut, než se firmware nahraje a router se restartuje.

5.2.2 Nastavení přístupu k routeru

V administraci zvolíme Správa\Systém, zde nastavíme nové heslo pro přihlášení k administraci routeru. Heslo by mělo být z důvodu bezpečnosti dostatečně silné, obsahovat malá a velká písmena s diakritikou, číslice a speciální znaky, jako např. @ atd.

Nyní přejdeme k nastavení webového rozhraní a nastavíme Způsob přihlášení = BOTH, HTTPS Lan port = 8443, Povolit webovou správu přes WAN = Ano, Port pro webovou

správu přes WAN = HTTP 8080 HTTPS 8443. Vzdáleně přistupovat k administraci z internetu je bezpečnější použít VPN případně HTTPS spojení. Jelikož se jedná o šifrovanou komunikaci, kterou nelze jednoduše odposlouchávat nebo nějak zneužít, HTTP je použita pouze pro připojení v lokální síti.

Po aplikaci tohoto nastavení se lze k administraci routeru připojit:

- Lokálně nezabezpečeně nebo VPN: http://lokální_ip_adresa_routeru:80
- Vzdáleně zabezpečeně: https://veřejná_ip_adresa:8443
- Vzdáleně zabezpečeně přes DDNS: https://nazev.synology.me:8443

Další možností omezené konfigurace routeru je pomocí aplikace ASUS Router dostupné pro operační systém Android a iOS. Tuto aplikaci lze použít pouze za předpokladu, že se nacházíme v lokální síti, kdy po spuštění aplikace prohledá síť a najde dostupný Asus router. Po následném přihlášení lze sledovat aktivitu sítě, přihlášené klienty atd. [28].

Obr. 33. Prostředí firmware AsusWRT Merlin

5.2.3 Nastavení Internetového připojení

V administraci zvolíme WAN\Internetové připojení, zde nastavíme Typ připojení WAN = Statická IP a vyplníme neveřejnou IP adresu, masku podsítě, výchozí bránu a DNS server udaný poskytovatelem Internetu.

Po domluvě s poskytovatelem byla později přidělena veřejná IP adresa, ale bohužel k ní nelze přistupovat přímo z lokálního routeru. Poskytovatel na ni ve své administraci pouze přesměroval internetovou komunikaci z dříve přidělené neveřejné IP adresy pomocí překladu adres NAT. S tímto nastavením jsem měl později problémy při konfiguraci DDNS a VPN komunikace.

5.2.4 Nastavení bezdrátové komunikace

V administraci zvolíme Bezdrátové\Obecné, zde zvolíme Skupina = 2.4 Ghz. Nyní nakonfigurujeme bezdrátové připojení pro pásmo 2,4 Ghz. Zvolíme Síťový název (SSID) = Martnet_5G, Způsob přihlášení = WPA2-Personal, Kódování WPA = AES, Před sdílený WPA klíč = heslo pro přihlášení k bezdrátové síti. Ostatní parametry jako výběr kanálu nemusíme řešit a můžeme je nechat na automatickém výběru, jelikož je dům na vesnici v dostatečné vzdálenosti od ostatních bezdrátových WiFi sítí a tudíž nedojde k překrývání signálu žádnými sousedskými sítěmi, ale i tak byla pro jistotu provedena analýza případného překrývání síťových kanálů jak v pásmu 2,4 Ghz tak i 5 Ghz. K tomuto účelu doporučuji analyzační program inSSIDer, který je ve starších verzích bezplatný.

Poté bylo nakonfigurováno bezdrátové připojení pro pásmo 5 Ghz. Zde byly nastaveny totožné parametry zabezpečení, změněn byl pouze síťový název na Martnet_5G. Ostatní parametry byly rovněž ponechány ve výchozím stavu.

5.2.5 Nastavení zabezpečení pomocí služby AiProtection

Pro zvýšení zabezpečení byly zapnuty některé funkce integrované antivirové služby AiProtection od společnosti TrendMicro.

V administraci AiProtection\ Ochrana sítě zvolíme Blokování škodlivých stránek = ON. Tato možnost zapne filtrování nebezpečných Internetových stránek s možností infikace připojeného zařízení.

Provedením nastavení Ochrana před průnikem = ON, Rozpoznání a blokování napadených zařízení = ON, router detekuje a zároveň blokuje komunikaci u zařízení nakažených

malwarem, nebezpečné datové pakety od útočníků poslané do sítě LAN přes některé zařízení se slabou, jako IP kamery nebo televize s operačním systémem [10].

5.2.6 Nastavení LAN sítě a DHCP serveru

V administraci zvolíme LAN\LAN IP, zde nastavíme položku IP Adresa na 192.168.2.1. Díky tomuto nastavení nadefinujeme IP adresu routeru (výchozí bránu pro lokální zařízení) a zároveň přenastavíme lokální síť 192.168.1.0 na 192.168.2.0. Tímto nastavením se vyřešil možný konflikt IP adres za předpokladu připojení v budoucnu nějaký vzdálený router jako OpenVPN klient. Nedojde k situaci, kdy se router s adresou 192.168.1.1 připojí do VPN sítě, ve které se již nachází vzdálený router se stejnou adresou 192.168.1.1 a při pokusu o přihlášení do administrace dojde ke konfliktu IP adres.

V nastavení LAN\Server DHCP zvolíme Povolit manuální přiřazování = ANO. Tato možnost nám dovolí přiřazovat statické (neměnné) lokální adresy jednotlivým klientům pomocí jejich specifické MAC adresy zařízení.

Pro přehlednost byl vymyšlen systém přidělování statických IP adres. Statickým zařízením byl přiřazen rozsah od adresy 192.168.2.10 po 192.168.2.99.

Tab. 1. Přidělování statických IP adres statickým zařízením.

Adresa MAC	IP Adresa	Hostname
00:12:32:41:85:23	192.168.2.10	NAS_LAN1
00:15:36:21:87:64	192.168.2.11	NAS_LAN2
60:E3:24:D0:A9:E2	192.168.2.12	Switch
00:65:6E:64:69:C6	192.168.2.13	Kamera
E8:AB:FA:72:EC:B4	192.168.2.14	Kamera_2(budoucí)
30:CD:A1:1A:30:D4	192.168.2.15	Tiskarna_Samsung
00:A1:DE:A5:42:85	192.168.2.16	AVReceiver
D0:73:D5:12:29:B4	192.168.2.17	Lampa_1
D0:71:D5:11:C4:E0	192.168.2.18	Lampa_2
3C:CD:93:22:CB:51	192.168.2.19	Televize_LG

Koncovým zařízením byl přiřazen zbylý rozsah (do 192.168.2.254). Příklad nastavení:

Tab. 2. Přidělování statických IP adres koncovým zařízením.

Adresa MAC	IP Adresa	Hostname
AC:9B:A1:3E:72:AB	192.168.2.100	Admin-PC
MAC:10:A4:D0:DA:1C:D5	192.168.2.101	Admin-Telefon

Pokud nastavíme u klientů načítání údajů o síti z DHCP serveru, tak se později po připojení do sítě tato statická adresa společně s dalšími potřebnými konfiguračními údaji, jako veřejná brána, maska a DNS server, automaticky načtou.

Díky tomuto statickému přiřazení lokální IP adresy lze později s tímto zařízením komunikovat bez neustálého prohledávání sítě a zjišťování aktuální IP adresy. Obzvlášť u statických zařízení, jako tiskárna, IP kamera, NAS a dalších, na které se často připojujeme, je statická síťová cesta důležitá, protože je použita při konfiguraci přístupu k nim u dalších zařízení (př. v ovladačích při nastavení tiskárny atd.). Jen pro zajímavost, tuto nutnost nastavení statické cesty lze obejít např. nastavením DDNS adresy na příslušném síťovém zařízení.

5.2.7 Nastavení předávání portů

Tato komunikace není v základu bezpečná a hrozí u ní možnost odposlechu nebo samotného proniknutí do sítě. Z toho důvodu je lepší použít komunikaci pomocí VPN, která je šifrovaná a poskytuje robustní ochranu. Bohužel ne všechna zařízení podporují možnost VPN komunikace. Z toho důvodu byla nastavena na NAS serveru a dalších zařízeních, které to podporují, komunikace pomocí HTTPS společně s využitím SSL certifikátu.

V administraci zvolíme WAN\Předávání portů, zde nastavíme položku Povolit předávání portů = ANO. Do tabulky byly posléze přidány potřebné předávací parametry k jednotlivým zařízením nebo službám, ke kterým je potřeba zajistit přístup z internetu, a to ze zařízení, která nepodporují nebo nemají nastavenou VPN komunikaci:

Tab. 3. Předávání portů

Číslo	Název služby	Rozsah portu	Lokální IP	Místní port	Proto-kol
1	ROUTER-http	8080	192.168.2.1	80	TCP
2	ROUTER-https	8443	192.168.2.1	8443	TCP
3	NAS-http	5000	192.168.2.10	5000	TCP
4	NAS-https	5001	192.168.2.10	5001	TCP
5	NAS-WEBST	80	192.168.2.10	80	TCP
6	NAS-WEBSTSSL	443	192.168.2.10	443	TCP
7	NAS-WebDav	5006	192.168.2.10	5006	TCP
8	NAS-SurveillanceSt	19998	192.168.2.10	19998	UDP
9	NAS-SurveillanceSt	554	192.168.2.10	554	TCP
10	NAS-CloudStation	6690	192.168.2.10	6690	TCP
11	Kamera	88	192.168.2.13	443	TCP

5.2.8 Nastavení OpenVPN serveru

V administraci zvolíme VPN\OpenVPN Servers, zde nastavíme položku Server instance = Server 1, Podrobnosti VPN = Pokročilá nastavení.

V menu pokročilá nastavení nastavíme:

Typ rozhraní = TUN

- režim TUN: realizace tunelu na 3. síťové vrstvě (modelu OSI), lze jim tedy přenášet libovolnou IP komunikaci. Využívá směrování, případně překlad adres NAT (Network Address Translation) mezi vytvořenou podsítí s vlastním adresním rozsahem a zbylou částí sítě za VPN serverem. Tento režim bývá doporučován samotnými tvůrci. Poskytuje nižší zatížení sítě z důvodu nižší Broadcastové (všesměrové) komunikace mezi síťovými prvky v síti [5].
- režim TAP: realizace spojení na 2. linkové vrstvě, které simuluje přímé propojení konců VPN tunelu na úrovni Ethernetu a tudíž jde o přímé napojení na síť. Tato komunikace má vyšší provozní režii, ale připojený klient má veškeré výhody reálného připojení do lokální sítě, jako podporu aplikací a služeb využívající všesměrového vysílání (sdílení v síti Windows, DLNA komunikace, prohledávání zařízení v síti atd.) [5].

Protokol = UDP

- Použitím UDP protokolu dosáhneme nižších přenosových časů (než u TCP), jelikož UDP netrpí režií mechanismu kontroly chyb, kdy jsou pakety sekvenčně číslovány a příjemcem je potvrzováno jejich přijetí. OpenVPN pracuje na 2 (Linková vrstva) nebo 3 (Síťová IP vrstva) referenční vrstvě OSI, kde není předpokládáno zajištění spolehlivosti přenesení dat či uspořádání pořadí paketů, tyto záležitosti řeší až vyšší vrstvy (transportní). Použití UDP pro vytvoření nespolehlivé přenosové cesty je tedy z pohledu dat přenášených SSL tunelem v pořádku [6] [7].
- Pokud by byla data SSL kanálu přenášena protokolem TCP, může při přenosu dat skrz tento kanál dojít k podstatnému propadu rychlosti přenosu dat, protože jakmile dojde k opětovnému poslání paketů ve vnitřním TCP tunelu, k přepočítávání dojde v obou spojeních [6] [7].

Server Port = 1194

- Oficiální port služby 1194, případně port SSL 443, ovšem od verze OpenVPN 2.0 lze využít jakýkoliv jiný port [5].

Firewall = automaticky

- Při nastavení automatiky dojde k automatickému vytvoření pravidel pro povolení portu, na kterém běží server, a ip adres přidělených klientům.

Režim ověření = TLS

- Byl použit velmi bezpečný režim TLS, který provádí autentizaci pomocí asymetrického šifrování, dále šifruje přenášená data symetrickou šifrou a kontroluje jejich integritu pomocí HASH kontrolních součtů (viz 2.2).
- Potřebné klíče pro asymetrické šifrování jako privátní klíč, veřejný klíč, certifikát certifikační autority (CA) byly vygenerovány automaticky pomocí mechanizmů prostředí routeru. Lze je ale i přímo do serveru vložit, tzn. vygenerovat ručně pomocí příkazového řádku v PC prostřednictvím OpenSSL knihovny [29] [5]. Dále lze použít i certifikáty od důvěryhodné certifikační autority (nejbezpečnější varianta ale většinou paušálně placená).
- V našem případě nebyla použita zpoplatněná důvěryhodná autorita, certifikát byl podepsán samotným VPN serverem (self-signed) kvůli úspoře nákladů.

Username/Password Authentication = ANO

- Povolení autentizace pomocí jména a hesla. Při připojování k VPN jsou vyžadovány přihlašovací údaje. Tyto přihlašovací údaje je možno měnit v administraci routeru.

Pouze ověření uživatelským jménem / heslem = NE

- Kombinace více metod autentizace (použití autentizace certifikátem a zároveň uživatelským jménem/heslem) pro vyšší bezpečnost.

Auth digest = Default

- Algoritmy založené na hašovací funkci se používají k zajištění celistvosti a ochrany dat proti změnám. OpenVPN implicitně používá algoritmus HMAC-SHA1 (Hash Message Authentication Code- Secure Hash Algorithm 1) [6].

Podsíť / síťová maska VPN = 10.8.0.0 255.255.255.0

- Volba IP adres, které mají být použity uvnitř tunelu. Nastavení podsítě 10.8.0.0 s rozsahem adres pomocí síťové masky 255.255.255.0 pro klienty. Každý klient dostane po přihlášení dynamickou ip adresu jako u DHCP serveru [6].

Nabídnout LAN klientům = ANO

- Povolí klientům přístup do lokální sítě na straně VPN

Přikázat klientům, aby přesměrovali internetový provoz = NE

- VPN klient ve výchozím stavu přenáší veškerou síťovou komunikaci skrze VPN tunel včetně internetové komunikace, to má za následek značné zpomalení síťové komunikace závislé na schopnostech internetového připojení na straně VPN serveru nahrávat data do internetu (upload). Z toho důvodu byl nastaven režim, kdy má klient přístup do VPN, ale zároveň využívá domácí Internetovou konektivitu (výchozí brána je nastavena na domácí router a ne na VPN server)

Odpovědět na DNS = ANO

- Povolit aby server odpovídal klientům na DNS dotazy

Šifrovací šifra = AES-256-CBC

- OpenVPN šifruje přenášená data symetrickou šifrou, ve výchozím nastavení se jedná o blokovou šifru Blowfish s délkou klíče 128 bitů. V mém případě byla zvolena silnější šifra AES s delkou klíče 256 bitů.
- CBC (Cipher Block Chaining) zřetězený šifrovací blok je pracovní režim šifrovacího algoritmu, který šifruje bloky dat. CBC šifruje malé kousky dat namísto zpracovávání celého bloku najednou [6].

Komprimace = Adaptivní

- OpenVPN periodicky analyzuje vzorky přenášených dat a zapíná kompresi, pouze pokud se vyplatí (nejedná se již o zkomprimovaná data atd.) [5].

Global Log verbosity = 3

- Úroveň logování: konfiguruje se od 0 (minimální) do 15 (maximální), 0 -- tiché s výjimkou velmi závažných chyb (1 většinou tiché, zobrazuje i nezávažné síťové chyby, 3 střední úroveň, dobrá pro normální použití) [6].

Povolit Klient <-> Klient = ANO

- Povolení komunikace klientů mezi sebou přes VPN server.

Povolit pouze určené klienty = NE

- Povolení komunikace mezi sebou všem klientům. V případě potřeby lze povolit pouze určité klienty.

Další konfigurace je možno v případě potřeby zadávat pomocí konfiguračních příkazů do textového pole Vlastní konfigurace. Soupis možných konfigurací lze nalézt na oficiálních stránkách OpenVPN [5].Této možnosti nebylo potřeba využít, jelikož všechna potřebná nastavení byla přístupná v Pokročilých nastaveních administrace routeru.

Po dokončení pokročilých nastavení bylo možno přejít k vytvoření přihlašovacích údajů jednotlivých klientů. Tyto údaje byly zapsány do tabulky s názvem Uživatelské jméno a heslo v konfiguraci routeru na stránce VPN/OpenVPN Servers.

V posledním kroku byla uložena konfigurace zvolením tlačítka Použít a exportovat (kvůli možnosti odposlechu komunikace pouze v LAN síti) konfigurační soubor protokolu OpenVPN pomocí tlačítka Exportovat.

Obsah konfiguračního souboru client1.ovpn:

```
Client  //určení zda se jedná o konfiguraci klienta nebo serveru
dev tun //typ tunelu (TUN směrovaný IP tunel)
proto udp //využití nepotvrzovaného přenosového protokolu UDP
remote 188.244.61.91 1194 //veřejná IP adresa serveru a port na
                          kterém OpenVPN naslouchá
float  //povolení přijímání ověřených paketů z libovolné IP adresy
        a ne jen z pevně stanovené u parametru remote
cipher AES-256-CBC //typ symetrické šifry
comp-lzo adaptive  //využití adaptivní komprimace dat
keepalive 15 60 //udržení spojení, při nečinnosti spojení se pošle
                 po 15 sekundách na druhou stranu tunelu ping,
                 pokud neobdrží do 60 sekund odpověď tak spojení
                 restartuje
auth-user-pass //povolení ověřování pomocí uživatelského jména a
               hesla
ns-cert-type server //kontrola identity serveru pomocí
                    certifikátu, slouží k ochraně před možností
                    spojení k potencionálně nebezpečnému
                    nastrčenému serveru, který se vydává za náš.
<ca>
-----BEGIN CERTIFICATE-----
# //certifikát autority (veřejný klíč CA), sloužící k ověření pra-
vosti veřejných klíčů v našem případě se nejedná o zpoplatněnou
důvěryhodnou autoritu, certifikát byl podepsán samotným VPN serve-
rem (self-signed) pro ušetření nákladů
```

```
-----END CERTIFICATE-----
</ca>
<cert>
-----BEGIN CERTIFICATE-----
# //certifikát klienta (šiřitelný veřejný klíč klienta)
-----END CERTIFICATE-----
</cert>
<key>
-----BEGIN PRIVATE KEY-----
# //privátní klíč klienta (nutno držet v tajnosti)
-----END PRIVATE KEY-----
</key>
resolv-retry infinite //zajistí neomezenou dobu pokusů o opětovné
                        připojení v případě ztráty komunikace,
                        užitečné pokud se klient připojuje z
                        nespolehlivých sítí (př. mobilní internet)
nobind  //klient není vázán na lokální adresu a port a je mu při
          dělen dynamicky [5]
```

Konfigurační soubor obsahuje příkazy a certifikáty potřebné ke konfiguraci klientského přístupu k OpenVPN serveru. Před posláním konfiguračního souboru klientům bylo potřeba upravit hodnotu příkazu remote z vygenerované WAN IP routeru na veřejnou IP přidělenou poskytovatelem Internetu.

Vytvoření serveru 2

Po dokončení veškerého nastavení serveru 1 byl nastaven server 2 totožně jako server 1. Rozdíl je pouze v nastavení Typ rozhraní = TAP, Server port = 443 a namísto vytvoření podsítě pro připojení klientů byla zvolena možnost Přidělit z DHCP = ANO, kdy se klientovi přímo přiřadí IP adresa a další konfigurační údaje z DHCP serveru. Nakonec byl vyexportován konfigurační soubor client2.ovpn a nakonec byl server spuštěn. Tento druhý OpenVPN server byl nastaven pro případ potřeby přímého připojení na vzdálenou lokální síť s možností využívat vzdáleně aplikace a služby, které potřebují ke své činnosti možnost všesměrového vysílání (broadband).

Soubor client1.ovpn případně client2.ovpn byl použit společně s přihlašovacími údaji ke konfiguraci jednotlivých klientů (viz. 6.1.1 a 6.2.1).

Spuštění serverů a kontrola případných problémů

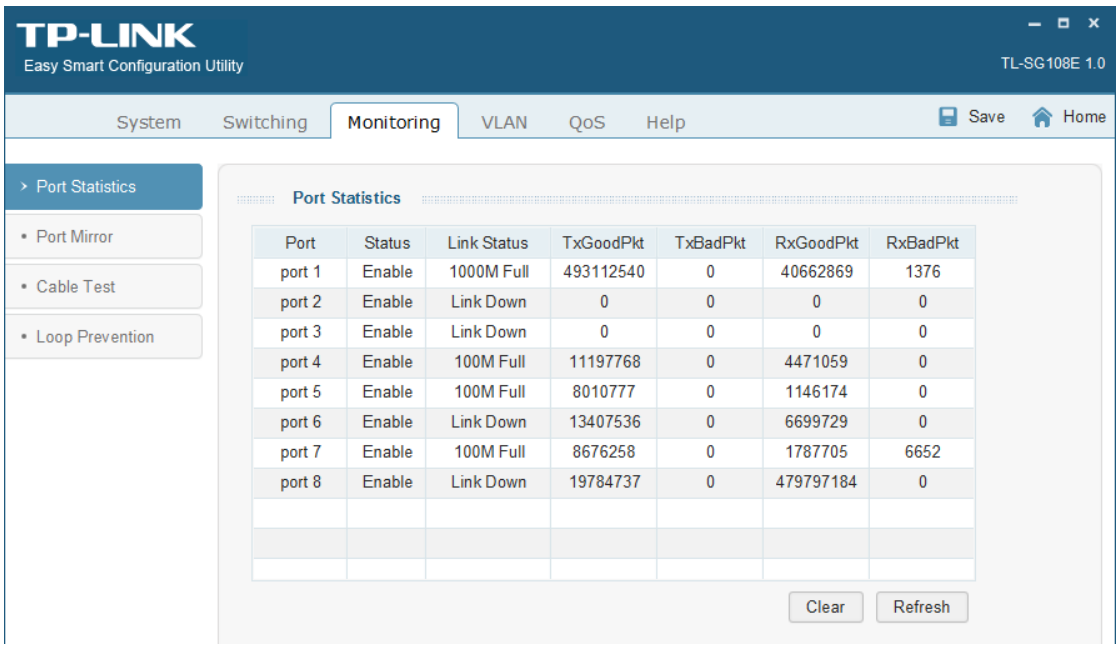
U obou serverů zvolíme Povolit server VPN = ON. Tím servery spustíme. Dále v administraci zvolíme Systémový záznam\Obecný záznam, a zkontrolujeme případné systémové záznamy (logy) jestli zde nejsou nějaké chybové hlášky.

5.3 Switch TP-LINK TL-SG108E

K administraci switche lze přistupovat skrze specializovanou aplikaci TP-Link Easy Smart Configuration Utility. Tato aplikace se stará o veškerou konfiguraci, jako je nastavení přístupu k routeru, nastavení jednotlivých portů (QOS, rychlosti, omezení datového toku..), testy kabeláže a statistiky [30].

Po nainstalování a spuštění aplikace prohledá lokální síť (sítě) a pokusí se najít switch. Nalezený switch byl označen a zvoleno IP settings. Zde bylo nastaveno DHCP settings = Enable. Následně došlo k napojení switche na rezervovanou statickou IP adresu přiřazenou včetně dalších parametrů pomocí DHCP serveru.

Dále byla zvolena položka Login, kdy po zadání jména a hesla admin došlo k přihlášení do administrace. Zde bylo nejprve v System\User Acount změněno výchozí heslo. Poté byl povolen IGMP Snooping, díky kterému zpřístupníme multicastovou komunikaci. Tato komunikace je potřebná k správné funkci DHCP serveru. Nakonec byly otestovány kabely a rychlost datového toku skrze jednotlivé porty switche.



Obr. 34 Prostředí aplikaci TP-Link Easy Smart Configuration Utility.

5.4 NAS server Synology Diskstation DS716+

5.4.1 Instalace DSM a konfigurace disků

Po spuštění serveru a zaznění zvukového signálu, že je zařízení připraveno, byl otevřen webový prohlížeč. Zde můžeme podle oficiálního postupu přejít na adresu find.synology.com, která spustí webovou službu Web Assistant. Tato služba prohledá LAN síť a zobrazí nalezený server s možností přesměrování na jeho přidělenou IP adresu. Mi již máme z dřívějška vyčleněnou statickou lokální IP na DHCP serveru routeru. Proto se můžeme přímo napojit na adresu 192.168.2.10:5000.

Po připojení se automaticky zahájí proces instalace systému DSM. Pokud není v síti LAN zpřístupněný Internet lze zvolit instalační soubor v zavaděči manuálně. Poté zvolíme Instalovat nyní a potvrdíme varovnou hlášku, že všechna data na discích budou přepsána. Po instalaci zvolíme Jméno serveru = MARTNET_NAS a zadáme přihlašovací údaje pro vytvoření administrátorského účtu. Nakonec se průvodce instalací dotáže, jestli chceme instalovat nové verze systému a aktualizace automaticky nebo manuálně. Bylo zvoleno Automaticky [13].

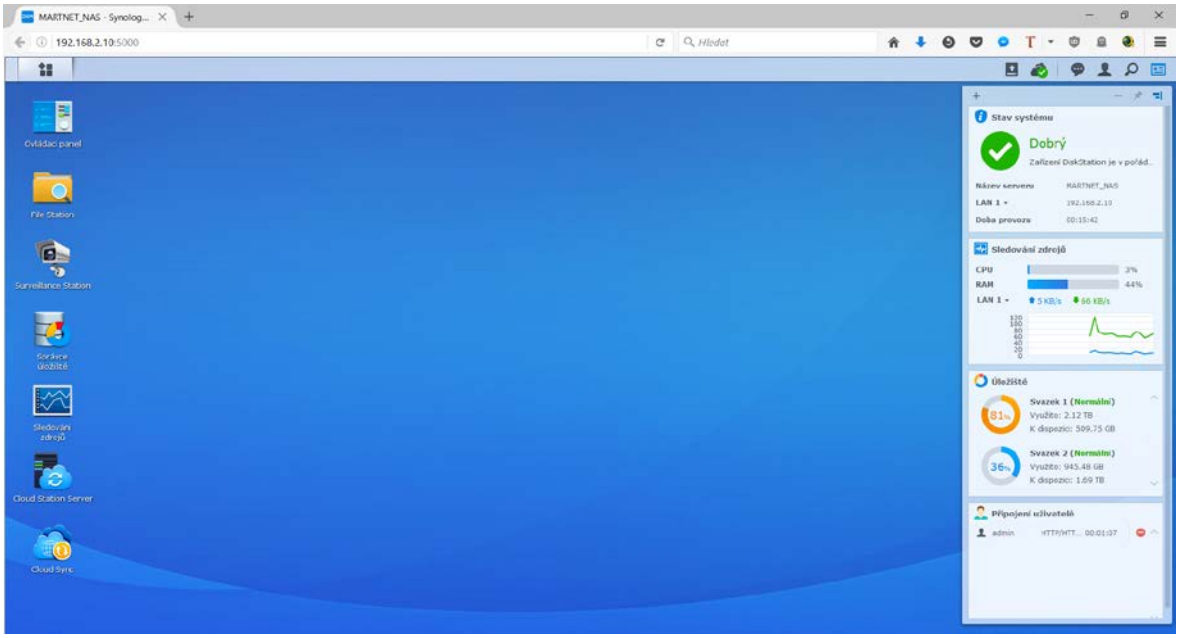
Po instalaci se načte prostředí DSM. Dalším krokem byla konfigurace disků.

Při použití 2 disků se stejnou velikosti (3 TB) bylo nutno rozhodnout, jak tyto disky nakonfigurovat. Byla možnost využití technologie RAID, která umožňuje vytvořit z více disků jeden úložný prostor, ovšem každá varianta by měla nevýhody.

V případě zapojení do pole RAID 0 by hrozila ztráta veškerých dat při poruše jednoho z disků. Zatímco při použití RAID 1 by se data zrcadlila na oba disky současně a tím by vznikla ochrana dat v případě poruchy jednoho z disků. Ovšem za cenu poloviční úložné kapacity.

Z toho důvodu s ohledem na co největší úložnou kapacitu bylo rozhodnuto zatím disky do pole RAID nezapojovat a nastavit je jako nezávislé jednotky. Kdy v budoucnu po získání dalších finančních prostředků na koupi expanzní jednotky a dalšího disku bude úložiště převedeno rovnou do pole RAID 5.

Pro konfiguraci disků bylo potřeba se přihlásit do DSM pomocí účtu administrátora. Poté zvolit Hlavní nabídka\Správce úložiště\Svazek\Vytvořit\Pokročilé nastavení, zde bylo zvoleno Typ RAID=Základní, Systém souborů=Btrfs, Velikost svazku=celá jednotka [13].



Obr. 35. Operační systém Synology Diskstation Manager (DSM).

5.4.2 Vytvoření datové struktury

Po úspěšném naformátování disků byla vytvořena datová struktura sdílených složek. Pro vytvoření nové sdílené složky bylo zvoleno Hlavní nabídka\Ovládací panel\Sdílená složka\Vytvořit, zde byl zadán název a dále podle potřeby nastaveny následující parametry:

1. Popis určité složky.
2. Umístění na určitý svazek (pevný disk).
3. Možnost skrýt sdílenou složku v části Místa v síti systému Windows v případě připojení přes protokol SMB/CIFS.
4. Možnost skrýt podsložky a soubory uživatelům bez oprávnění.
5. Možnost povolit koš (ze kterého může administrátor později obnovit nechtěně smazané soubory)
6. Možnost šifrovat tuto složku pomocí hardwarově akcelerovaného šifrování AES-NI s 256 bitovým klíčem, u tohoto nastavení bylo ještě nastaveno automatické připojení šifrované jednotky při spuštění.

V závislosti na těchto parametrech byla vytvořena následující struktura složek:

- **private(uživatel)** je uživatelská složka vytvořená pro jednotlivé uživatele. Použité parametry:1=Privátní složka, 2=Svazek 2, 3=NE,4=ANO, 5=ANO, 6=ANO

- **documents** je sdílená složka přístupná pro všechny uživatele ke sdílení společných dokumentů. Použité parametry:1=Sdílená složka, 2=Svazek 2, 3=NE, 4=NE, 5=ANO, 6=ANO
- **other** je sdílená složka přístupná pro všechny uživatele ke sdílení souborů které se nedají zařadit do žádné předdefinované sdílené složky. Použité parametry:1=Sdílená složka, 2=Svazek 2, 3=NE,4=NE, 5=ANO, 6=ANO
- **music** je sdílená složka přístupná pro všechny uživatele ke sdílení společné hudby, zároveň se jedná o multimediální indexovanou složku sdílenou v síti pomocí služby UPnP/DLNA. Použité parametry:1= Multimediální indexovaná složka, 2=Svazek 1, 3=NE,4=NE, 5=ANO, 6=NE
- **photo** je sdílená složka přístupná pro všechny uživatele ke sdílení společných fotek, zároveň se jedná o multimediální indexovanou složku sdílenou v síti pomocí služby UPnP/DLNA. Použité parametry:1= Multimediální indexovaná složka, 2=Svazek 2, 3=NE,4=NE, 5=ANO, 6=NE
- **video** je sdílená složka přístupná pro všechny uživatele ke sdílení společných videí, zároveň se jedná o multimediální indexovanou složku sdílenou v síti pomocí služby UPnP/DLNA. Použité parametry:1= Multimediální indexovaná složka, 2=Svazek 1, 3=NE,4=NE, 5=ANO, 6=NE
- **surveillance** je sdílená složka sloužící systému k ukládání kamerových záznamů. Použité parametry:1= Systémová složka (kamerový systém), 2=Svazek 2, 3=NE,4=NE, 5=NE, 6=NE
- **usbshare(číslo disku)** je sdílená složka prezentující připojené externí úložiště

Ze seznamu je patrné, že první disk byl určen k ukládání multimediálních souborů, zatímco druhý slouží k ukládání uživatelských dat společně s kamerovým systémem a dalšími systémovými záležitostmi [13].

5.4.3 Vytvoření uživatelských účtů a oprávnění

Po vytvoření datové struktury byly nastaveny uživatelské skupiny, kterým se přiřadila příslušná oprávnění. Poté při vytváření jednotlivých uživatelských účtů stačilo pouze tento účet přiřadit k příslušné skupině a v případě potřeby doladit oprávnění pro specifického uživatele. Tímto postupem administrátor zpřehlední práci při pozdějším vytváření účtů, než aby každému přiřazoval oprávnění zvlášť.

Pro vytvoření a nastavení nové skupiny bylo provedeno přihlášení pod administrátorským účtem a zvolit Hlavní nabídka\Ovládací panel\Skupina\Vytvořit, zde byl zadán Název skupiny=users, Popis skupiny = Skupina uživatelů. Podle potřeby byly nastaveny následující parametry:

Tab. 4. Skupina users – tabulka oprávnění.

Sdílená složka	Žádný přístup	Čtení/zápis	Jen pro čtení	Kvóta	Omez. rychlosti
private(uživatel)	Ostatní	Majitel		50GB	NE
documents		ANO		NE	NE
other		ANO		NE	NE
music			ANO	NE	NE
photo			ANO	NE	NE
video			ANO	NE	NE
surveilance			ANO	NE	NE

V systému se nachází skupina administrators, která byla vytvořena systémem společně s administrátorským účtem, takže ji nebylo potřeba vytvářet. Nicméně v ní není žádné omezení, vše je nastaveno na Čtení/zápis.

Po vytvoření skupin bylo možno přistoupit k samotnému vytváření jednotlivých uživatelských účtů. Uvedu zde příklad vytvoření běžného účtu. Nejprve bylo potřeba přejít do záložky uživatel v Ovládacích panelech. Po zvolení možnosti Vytvořit byly nastaveny následující parametry. Název=jméno příslušného uživatele (Milan), Popis=Uživatel, Email=na tento email se budou posílat upozornění související s účtem (př. výzva ke změně hesla, přesažení kvóty atd.), Heslo, Zakázat uživateli změnit heslo účtu=NE. Dále byla zvolená skupina, do které má uživatel spadat. V tomto případě se jedná o skupinu users. V nastavení přístupových práv pro sdílené složky bylo upraveno oprávnění pro privateMilan na Čtení/Zápis, složky ostatních uživatelů na Žádný přístup. Kvóta uživatelské složky byla ponechána na nastavení skupiny, tudíž 50 GB. Omezení rychlosti a přístupu k aplikacím DSM nebylo uživatelům omezeno.

5.4.4 Konfigurace vzdáleného přístupu

Pro bezpečný vzdálený přístup k webovému rozhraní operačního systému DSM a dalším přidruženým službám jako WebDAV server (přenos souborů), Cloud Station server (synchronizace a záloha souborů), Synology Surveillance station (kamery), atd. skrze internet bylo nakonfigurováno zabezpečené https spojení pomocí SSL certifikátu podepsaného důvěryhodnou certifikační autoritou Let’s Encrypt.

Nejprve bylo ověřeno správné nastavení přesměrování portů na routeru přes WAN:

- Port 5000 pro nezabezpečený přístup k DSM a mobilní aplikaci File Station sloužící k přenosu souborů ze serveru, skrze HTTP. Toto připojení je doporučeno jen jako záložní.
- Port 5001 pro zabezpečený přístup k DSM a mobilní aplikaci File Station sloužící k přenosu souborů ze serveru, skrze HTTPS.
- Porty 80, 443 pro ověření a správnou funkci SSL spojení, využívá pro komunikaci služba Let's Encrypt (důvěryhodná certifikační autorita bez poplatků)
- Port 5006 pro zabezpečený přístup k WebDAV serveru, skrze HTTPS.
- Port 6690 pro zabezpečenou komunikaci serveru CloudStation s klienty.
- Porty 19998, 554 pro komunikaci aplikace Surveillance Station (kamerový systém).

Pokud máme potřebné porty povoleny, dalším krokem je založení DDNS domény k naší veřejné IP adrese. SSL certifikát ověřený důvěryhodnou autoritou lze použít pouze v případě, že přistupujeme k NASu přes konkrétní URL, nikoliv přes IP adresu. DDNS byla použita, jelikož je zdarma oproti většině DNS domén a přizpůsobí se případné změně statické IP adresy.

DDNS přidáme v Hlavní nabídka\Ovládací panel\Externí přístup\DDNS\Přidat, zde zvolíme Poskytovatel služeb=synology.me, administrátorské přihlašovací údaje, Externí adresa (IPv4)=veřejná IP.

V Ovládací panel\Síť nastavíme Povolit HTTPS spojení, HTTPS=5001, HTTP=5000, Povolit zjišťování sítě Windows.

Nyní se lze vzdáleně připojit zadáním DDNS domény a portu 5001, ovšem po připojení pouze s vlastně podepsaným certifikátem se v prohlížeči zobrazí chyba, že komunikace není bezpečná. Proto musíme získat certifikát podepsaný důvěryhodnou autoritou, která se zaručí za identitu našeho serveru. Byla využita nová bezplatná služba Let's Encrypt.

Přejdeme do Ovládací panel\Zabezpečení\Certifikát\Přidat\Získat certifikát ze služby Let's Encrypt, zde zadáme Název domény=naše DDNS doména (nazev.synology.me), E-mail=emailová adresa administrátora pro ověření identity. Nakonec zvolíme Použít. Pokud se v přehledu certifikátů zobrazí nový certifikát s ikonou zeleného zámku, tak vše proběhlo úspěšně a můžeme spojení otestovat. Pokud prohlížeč po připojení k doméně signalizuje u adresy ikonu zeleného zámku, znamená to, že máme správně nastaveno bezpečné spojení v rámci celého serveru a přidružených služeb.

Možnosti napojení na operační systém Synology DSM (Diskstation Manager) 6:

- Lokálně nebo VPN: http://lokální_ip_adresa_nas_serveru:5000
- Vzdáleně zabezpečeně přes DDNS: https://nazev.synology.me:5001
- Vzdáleně zabezpečeně přes QuickConnect: http://QuickConnect.to/nazev

Ke konci bylo nastaveno připojení pomocí služby Synology Quick Connect. Služba byla využita k automatickému přesměrování WAN a LAN IP adresy u mobilních zařízení, která se často přesouvají i mimo LAN síť. Službu zapneme v Hlavní nabídka\ Ovládací panely\ QuickConnect\, zde nastavíme Povolit QuickConnect a zadáme QuickConnect ID=nazev.

Na závěr bylo nastaveno zabezpečení blokováním IP adres s příliš velkým počtem neúspěšných pokusů o přihlášení, aby nebylo možné přihlásit se k serveru útočníkem, který použije generátor hesel pro prolomení. Nastavení bylo provedeno v Ovládací panel\Zabezpečení\Automatický blok, zde bylo nastaveno Pokusy o přihlášení=10, Během (minuty)=5.

5.4.5 Konfigurace souborových služeb

K souborům na serveru se dá přistupovat skrze webové rozhraní OS DSM 6, nebo lze přistupovat přímo k souborům pomocí souborových protokolů. Byly konfigurovány 3 možnosti přístupu.

Konfigurace souborové služby Windows (SMB/CIFS):

Souborová služba Windows (Místa v síti) pracuje s protokolem SMB\CIFS. Služba byla zvolena jako univerzální přístup k datům všech zařízení v lokální síti bez nutnosti instalovat nebo konfigurovat jakéhokoliv souborového klienta, kdy uživateli stačí prohledat síť a přihlásit se k serveru pod svými přihlašovacími údaji. Poté má přístup ke všem sdíleným složkám, ke kterým má oprávnění. Jelikož protokol využívá broadcast (všesměrovou) komunikaci, nelze jej jednoduše využít ke vzdálenému připojení, s výjimkou OpenVPN tunelu v režimu TAP.

Při konfiguraci Souborové služby Windows (SMB/CIFS) bylo provedeno přihlášení do DSM pomocí účtu administrátora. Dále bylo zvoleno Ovládací panely\ Souborové služby\ Win/MAC/NFS\ Souborová služba Windows, zde bylo nastaveno Povolit souborovou službu Windows.

Konfigurace FTP

Tento protokol byl využit v LAN u zařízení, která nepodporují protokol SMB a pro přenos souborů skrze OpenVPN tunel, jelikož zajišťuje vyšší rychlost, než šifrované přenosové protokoly a zároveň má nižší nároky na systémové prostředky (šifrování souborového protokolu v šifrovaném OpenVPN tunelu je zbytečné).

Při konfiguraci FTP bylo provedeno přihlášení do DSM přes účet administrátora. Dále byly zvoleny Ovládací panely\ Souborové služby\FTP, zde bylo zvoleno Povolit službu FTP (bez šifrování), Nastavení čísla portu služby=21, Rozsah portů pasivního FTP=55536-55567, Kódování UTF-8=Automaticky (systém stanoví na základně možností klienta, jestli kódování povolí).

Konfigurace WebDAV

Tento protokol byl využit pro přímý vzdálený přístup k datům. Přenos souborů je zabezpečený pomocí certifikátu SSL.

Před konfigurací bylo ověřeno povolení přesměrování portu 5006 přes WAN v nastavení routeru pro IP adresu NAS serveru a dále nastaveno zabezpečené https spojení pomocí SSL certifikátu podepsaného důvěryhodnou certifikační autoritou.

Při konfiguraci WebDAV bylo provedeno přihlášení do DSM pomocí účtu administrátora. Dále zvolit Hlavní nabídka\WebDAV Server\Nastavení, zde bylo zvoleno Povolit HTTPS, Port HTTPS=5006, Povolit protokol WebDAV. Nakonec bylo nastavení uloženo.

Konfigurace UPnP/DLNA

Před samotnou konfigurací je potřeba ověřit, že byl na switchi povolen IGMP Snooping. Tato funkce je nezbytná pro správnou funkci multicastové (skupinové) komunikace, kterou UPnP/DLNA využívá.

Při konfiguraci UPnP/DLNA serveru byly nejprve vytvořeny indexované složky pro multimediální soubory v Hlavní nabídka\Ovládací panel\Služba indexování\Indexování médií\Indexovaná složka, zde byly vybrány 3 složky video, music a photo. Tyto složky musejí mít pevně daný anglický název, z důvodu kompatibility DLNA u některých přístrojů. Proto je doporučeno tyto názvy neměnit. Je samozřejmě možné složky podle potřeby přidávat. Po naplnění těchto složek obsahem je vhodné je poprvé přeindexovat pomocí tlačítka stejného názvu, poté už se budou indexovat automaticky.

V dalším kroku byla doinstalována a spuštěna aplikace Mediální server pomocí instalátoru balíčků v Hlavní panel\Centrum balíčků\Multimedia\Mediální server. V položce Obecná nastavení byly nakonfigurovány následující položky: Síťové rozhraní=LAN 1 (první síťový port na serveru), Jazyk nabídky=Česky, Styl nabídky= Rozšířený (zobrazí soubory v ovladači rozčleněné do složek a ne pouze jako seznam všech souborů).

5.4.6 Konfigurace zálohy souborů

Cloud Station Server

Jedná se o službu sdílení souborů, která umožňuje synchronizaci souborů mezi centralizovaným zařízením Synology NAS a několika klientskými počítači nebo mobilními zařízeními. Před synchronizací souborů s klientskými zařízeními je nutné na hostitelském serveru nainstalovat balíček Cloud Station Server. Na jednotlivých klientských zařízeních, která chceme použít pro synchronizaci, je nutné nainstalovat klientský nástroj [13].

Před zahájením synchronizace bylo zkontrolováno, zda je u routeru povoleno předávání portu TCP 6690.

Aplikace Cloud Station Server byla stažena v Centru balíčků. Přesněji Hlavní nabídka\Centrum balíčků\Zálohování\Cloud Station Server\Instalovat. Po dokončení instalace na svazek 2 byla aplikace spuštěna a zobrazeno Nastavení\Nastavení synchronizace. Zde se nachází seznam sdílených složek, kdy je zapotřebí každou složku zvlášť povolit pro synchronizaci a uvést maximální počet verzí souborů, které se budou postupně vytvářet při jeho editaci [13].

Tímto byla provedena nezbytná konfigurace serveru. Další nastavení se již provádí na straně klienta (viz 6.1.3)

Cloud Sync

Jedná se o službu určenou k synchronizaci a sdílení souborů mezi zařízením Synology NAS a veřejnými cloudovými službami. Tato byla využita pro zálohu těch nejdůležitějších souborů, jako např. dokumenty na vzdálený server (cloudové úložiště třetí strany). Tím jsou soubory chráněny před nečekanými událostmi (vyhoření domu a podobně).

Před samotnou instalací byla nalezena vhodná cloudová služba a vytvořen uživatelský účet. Nakonec byla vybrána služba hubiC, jelikož jako jediná nabízela zdarma až 50 GB úložného prostoru.

Aplikace Cloud Sync byla stažena v Centru balíčků. Přesněji Hlavní nabídka\Centrum balíčků\Zálohování\Cloud Sync\Instalovat. Po dokončení instalace na svazek 2 byla aplikace spuštěna a zobrazeno tlačítko +, pro přidání nového synchronizačního profilu. Vybereme ze seznamu službu hubiC a spárujeme ji s aplikaci Cloud Sync zadáním přihlašovacích údajů. Poté zvolíme Místní cesta=výběr složky na NAS serveru, Vzdálená cesta=výběr složky z úložiště hubiC kde se mají data zrcadlit, Směr synchronizace=Obousměrná (úpravy souborů na obou stranách se navzájem projeví). Nakonec lze nastavit šifrování dat předtím, než se na vzdálený server uloží. Tato možnost ovšem nebyla vybrána, jelikož v mém případě nejsou data natolik tajná a nebylo by už možné data prohlížet po připojení přímo na cloudovou službu.

5.5 Venkovní IP kamera Foscam FI9828P

5.5.1 Možnosti přístupu

Ke kamerám lze přistupovat přímo pomocí webového rozhraní. Toto rozhraní se stará o veškerou konfiguraci kamery jako síťové nastavení, uživatelské účty a oprávnění, základní možnosti nahrávání záznamu na vzdálený FTP server a samozřejmě živé sledování obrazu. Tyto možnosti ovšem nebyly využity, jelikož je výhodnější kameru využívat skrz rozhraní NAS serveru.

Přímé napojení na kameru bylo využito pouze za účelem možnosti propojení s aplikacemi třetích stran, jako například mobilní aplikace pro systém Android tinyCam Monitor [31].

Možnosti přímého napojení (lokální zabezpečené nejsou uvedeny):

- Lokálně nebo VPN: http://lokální_ip_adresa_kamery:88 (administrace…).
- Lokálně nebo VPN: http://lokální_ip_adresa_kamery:888 (ONVIF protokol).
- Vzdáleně zabezpečeně: https://veřejná_ip_adresa:88 (administrace…).
- Vzdáleně zabezpečeně přes DDNS: https://nazev.synology.me:88(administrace..).

Možnosti napojení na kamerový systém Synology Surveillance station:

- Lokálně nebo VPN: http://lokální_ip_adresa_nas_serveru:5000 (DSM 6).
- Vzdáleně zabezpečeně přes DDNS: https://nazev.synology.me:5001 (DSM 6).
- Vzdáleně zabezpečeně přes QuickConnect: http://QuickConnect.to/nazev (DSM6).

Po přihlášení do osobního účtu zvolit ikonu Surveillance station.

5.5.2 Konfigurace administrace kamery

Před připojením do administrace bylo nutno použít internetový prohlížeč s architekturou x86 a to nejlépe Internet Explorer nebo Mozilla Firefox. Prohlížeč Google Chrome a Mozilla Firefox x64 blokují potřebný doplněk (plugin) nezbytný k napojení do administrace.

Při prvním přístupu do administrace byly použity základní předvolené přihlašovací údaje (jméno i heslo = admin). Poté bylo zapotřebí nastavit správný čas, jelikož je to důležitý údaj pro záznam Basic Settings\Camera Time, Time zone = GTM (Greenwich Mean Time) +01:00, Sync with NTP server = YES. Poté byl nastaven uživatelský účet administrátora a operátora, který má oprávnění pouze k ovládání kamery v Basic Settings\ User Acounts. Operátorský účet bude využit z důvodu bezpečnosti pro přímé přihlašování na kamery nezkušenými uživateli nebo aplikacemi třetích stran např. na mobilních telefonech těchto uživatelů (tinyCam Monitor pro Android). Dále bylo potřeba nastavit Network\IP Configuration = DHCP, Wireless Settings nastaveno nebylo, jelikož je kamera napojena pomocí optimálnější varianty přes Ethernet port. Porty pro přístup jednotlivých protokolů byly ponechány ve výchozím nastavení, tudíž http = 88, HTTPS = 443, ONVIF = 888. Z důvodu bezpečnosti byly zakázány všechny ostatní možnosti napojení jako P2P a UPNP v Network\UPNP Enable=NO a Network\P2P Enable=NO. Ostatní nastavení byly provedeny již v aplikaci Synology Surveillance station.

5.5.3 Konfigurace Synology Surveillance station

Jak již bylo uvedeno výše, ke kameře je výhodné přistupovat přes monitorovací aplikaci Synology Surveillance station, která je součástí operačního systému NAS serveru. Jedná se o plnohodnotný profesionální balík prvků ke správě IP kamer, který obsahuje pokročilé funkce záznamu na NAS server, detekce pohybu, uživatelsky přívětivé plně konfigurovatelné prostředí, správa upozornění, zabezpečení připojení (viz citace) [32].

V operačním systému NAS serveru byla zvolena ikona Surveillance station. Na ploše prostředí kamerového systému přejdeme do IP kamera\Přidat\Nastavení zařízení, zde zvolíme Název=Dům, IP adresa=192.168.2.13, Port=88, Značka=Foscam, Model kamery=FI9828P V2, uživatelské jméno a heslo účtu z administrace IP kamery a potvrdíme tlačítkem Uložit.

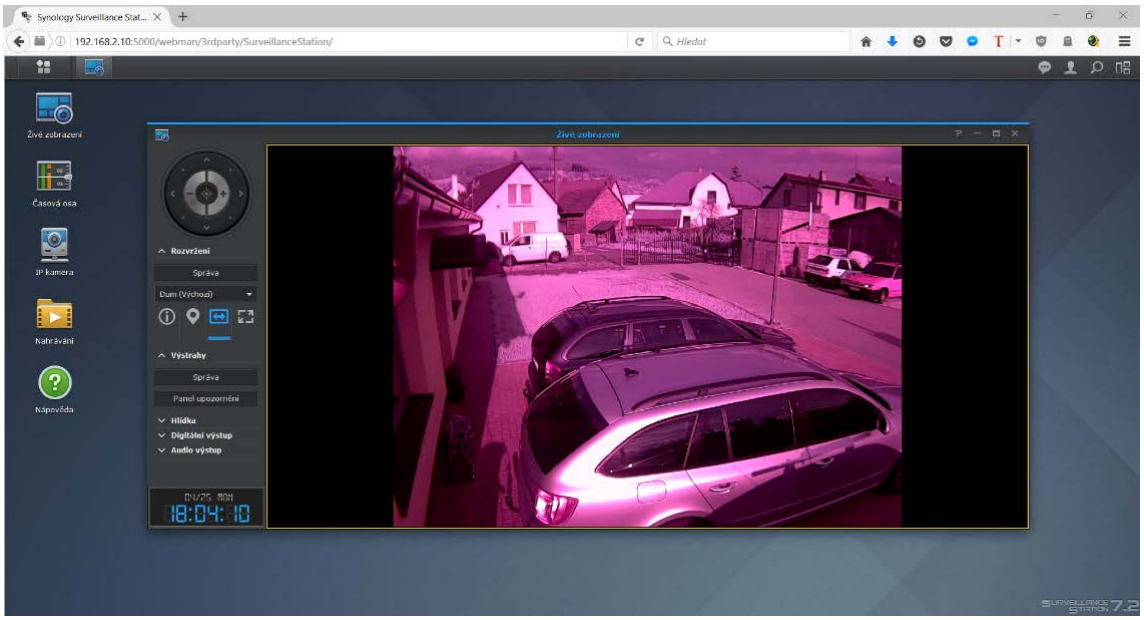
Následně přejdeme do položky Video, kde nastavíme Datový proud 1 pro živé vysílání a ukládání videa a Datový proud 2 pro mobilní přístup. V prvním případě nastavíme Rozli-

šení=1280x960, Rychlost snímků (fps)=25, Řízení přenosové rychlosti=Variabilní. V případě datového proudu 2, Rozlišení=640x480, Rychlost snímků (fps) = 15, Řízení přenosové rychlosti=Konstantní, Přenosová rychlost (Kbps)=256.

U nahrávání videa Nastavení nahrávání\Nahrávání bylo nastaveno Úložiště nahrávání=svazek2 (disk 2), Omezení archivní složky na (GB)=10. V Nastavení nahrávání\Plán byla nastavena nepřetržitá detekce pohybu. Díky tomu bude zapnut záznam, pouze pokud se bude v zorném poli něco pohybovat. Tím ušetříme značnou část místa na úložišti a zvýšíme čas počet dní záznamu bez nutnosti měnit kvótu úložiště.

Nakonec nastavíme Nastavení živého zobrazení, kde zvolíme Živé sledování=Z kamery, Mobilní přístup = Ze stanice Surveillance station. Tím zajistíme zobrazení živého záznamu v plné kvalitě bez žádné degradace způsobené překódováním.

Pro možnost vzdáleného přímého spojení z Internetu bylo potřeba aplikaci Synology Surveillance station povolit předávání portů na routeru (viz. 5.2.7) [13].



Obr. 36. Prostředí kamerového systému Synology Surveillance station.

6 KONFIGURACE KONCOVÝCH ZAŘÍZENÍ

Tato část práce se zabývá konfigurací koncových zařízení a to primárně jejich připojením do domácí sítě a následnými možnostmi využití těchto zařízení v síti.

6.1 Počítač

6.1.1 Připojení k OpenVPN serveru

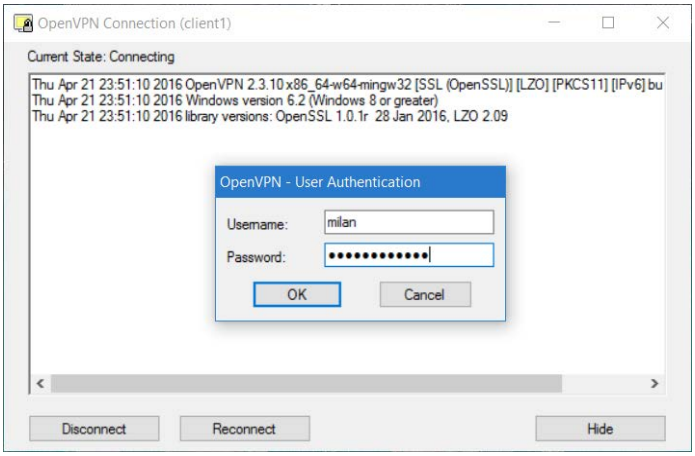
Pro spuštění OpenVPN komunikace byl stažen a nainstalován program OpenVPN z oficiálních Internetových stránek služby. Byl vybrán instalační soubor podle typu a verze systému včetně bitové varianty (x86, x64).

V dalším kroku bylo potřeba vložit konfigurační soubor client1.ovpn do příslušné složky config, která se nachází v místě, kde byl program nainstalován. Ve výchozím stavu se jedná o cestu: C:\Program Files\OpenVPN\config. Je důležité, aby při přesunu souboru nebyl použit nešifrovaný internetový přenos, jelikož je jeho součástí privátní klíč a další autorizační certifikáty.

Dále byl spuštěn program, ten se spustí na pozadí. Rozevřeme tedy roletu s těmito programy vedle systémového času. Na ikonu OpenVPN klikneme pravým tlačítkem myši a zvolíme Client1/Connect. Otevře se nám okno s log údaji o navazování komunikace, pokud vše proběhne úspěšně, zobrazí se okno s žádostí zadat uživatelské jméno a heslo. Po zadání a potvrzení se provede autorizace a následné připojení do VPN sítě, které poznáme na první pohled zelenou ikonou OpenVPN.

Po správném navázání spojení s druhou stranou dojde k vytvoření virtuální síťové karty. Cokoliv s pomocí této karty pošleme, bude automaticky zašifrováno a odesláno do virtuální sítě. Pokud bychom se chtěli připojit pomocí režimu TAP, je nutno nejprve vytvořit novou virtuální síťovou kartu k tomu určenou. Učiníme tak spuštěním souboru addtap.bat se správcovskými právy. Soubor je umístěn v adresáři C:\Program Files\TAP-Windows\bin [5].

Poté byl výše uvedený postup zopakován i pro připojení k serveru v režimu TAP.



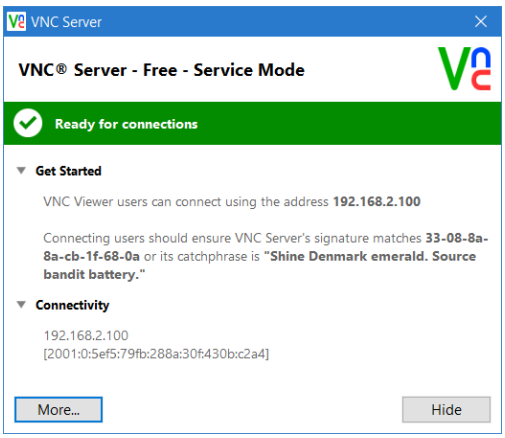
Obr. 37. OpenVPN - Přihlášení k OpenVPN serveru.

6.1.2 Vzdálená správa pomocí VNC serveru a klienta

Služba VNC byla použita pro vzdálenou správu počítačů a telefonů. Po testování a porovnávání byla pro počítače nakonec zvolena distribuce RealVNC a to hlavně proto, že je pravidelně aktualizována, poskytuje dostatečně podrobné přehledné nastavení a poskytuje VPN klienty a servery pro většinu platforem (kromě serveru pro Android).

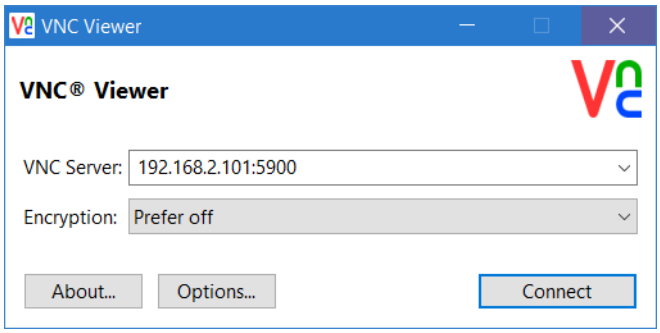
Nejprve byl stažen instalační soubor z oficiálních stránek RealVNC. [33] Při stahování byla provedena bezplatná registrace, kde byl udělen registrační kód. Dále v průběhu instalace je možno zvolit instalaci serveru (hostitel), klienta (ovládající) nebo obojí, heslo pro napojení na server (hostitele) 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 stavové okno zvolením ikony skryté v systémové liště u hodin. Zde byla potvrzena funkčnost.



Obr. 38. RealVNC server – stavové okno.

Dále byl nainstalován VNC klient na PC, který se bude k serveru připojovat. Byl zvolen klient, který je součástí instalátoru serveru z distribuce RealVNC.



Obr. 39. RealVNC klient – Windows.

Po stažení a instalaci RealVNC (Viewer) klienta byl v případě vzdálené komunikace spuštěn OpenVPN tunel, který byl dříve nakonfigurován a nyní slouží jako bezpečné spojení mezi zařízením kdekoliv v Internetu a zařízením v LAN síti. V případě lokální komunikace dvou zařízení v LAN síti ho není potřeba. Nakonec byl spuštěn RealVNC klient a nastaveno spojení:

VNC server = lokální_ip_zařízení:vncport

Encryption = Prefer off (šifrovaná komunikace není nutná díky OpenVPN tunelu)

Pokud by byla internetová konektivita nedostatečná a obraz by se sekal, lze v nastavení snížit kvalitu (barevná hloubka…).

6.1.3 Synchronizace dat pomocí NAS serveru

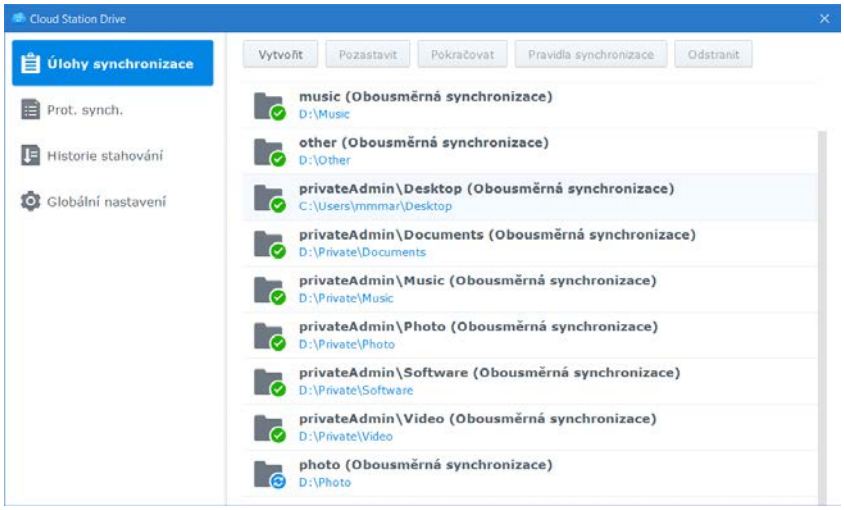
K synchronizaci dat byl využit pokročilý nástroj Synology Cloud Station Drive ve verzi pro systém Windows (viz citace) [34], [35]. Tato aplikace slouží jako klient, který komunikuje s hostitelským serverem skrze aplikaci Cloud Station Server.

Při instalaci programu byly zadány potřebné údaje pro napojení k serveru do určitého uživatelského účtu. Bylo tedy zadáno QuickConnectID, jméno a heslo příslušného uživatele.

Po instalaci bylo dále nastaveno v hlavní nabídce Globální nastavení\Řešení konfliktu verzí souborů = Zachovat nejnovější upravenou verzi.

Pro přidání nové složky počítače určené k synchronizaci bylo nejprve vstoupeno do hlavní nabídky programu. Zde zvolíme Úlohy synchronizace\Vytvořit, zde bylo do textového pole zadáno QuickConnectID našeho serveru Připojené zařízení Synology NAS = Martnet, případně lze vybrat nějaký jiný server k synchronizaci.

Poté zvolíme Další a přejdeme k samotné volbě cílové složky v PC uživatele a jejího protějšku na NAS serveru, kdy se zobrazí pouze složky, ke kterým má uživatel oprávnění. Dále zvolíme Rozšíření, zde lze odebrat případně podsložky z cílové složky, které se mají vyřadit ze synchronizace, to samé lze i u přípon souborů a dále směr synchronizace, který byl nastaven na volbu Ob**o**usměrná synchronizace. Nakonec byla zvolena možnost Povolit rozšířenou kontrolu konzistence, kdy se budou vytvářet verze souborů v případě změny jejich vnitřní struktury. Tyto verze jsou díky využití souborového systému BTRFS velmi úsporné, jelikož se ukládá jen změna v souboru a ne celý soubor.



Obr. 40. Synology Cloud Station Drive – Hlavní nabídka.

6.1.4 Připojení k serveru pomocí souborových protokolů

Připojení skrze souborové služby Windows (SMB/CIFS):

Doporučené využít v LAN nebo vzdáleně pomocí OpenVPN tunelu.

Otevřeme průzkumník Windows (zkratka WIN+E) a v bočním menu zvolíme Síť. Zde zvolíme MARTNET_NAS a přihlásíme se k serveru pod svými přihlašovacími údaji.

Připojení skrze FTP:

Doporučené využití v LAN u zařízení nepodporujících SMB/CIFS nebo vzdáleně skrze šifrované OpenVPN spojení.

K připojení byl využit program NetDrive. Tento program byl vybrán, jelikož dokáže namapovat připojená zařízení jako síťové disky v průzkumníku souborů Windows, nemá problém zobrazit znakovou sadu UTF-8 (na rozdíl od výchozího řešení ve Windows) a podporuje

streamování mediálních souborů (soubor lze okamžitě spustit a v průběhu přehrávání se dohrávají data do cache paměti) [36].

Po instalaci a spuštění programu bylo nataveno FTP spojení zvolením Add Drive, Type=FTP, Name=NAS FTP, URL= ftp://192.168.2.10, Port=21, Charset=UTF-8 a přihlašovací údaje příslušného uživatele. Nakonec stačí zvolit Save a Connect.

Připojení skrze WebDAV

Doporučené využití pro přímý přístup k datům mimo lokální síť a OpenVPN.

K připojení byla opět jako u FTP využita aplikace NetDrive. Byla vybrána, jelikož je značně rychlejší a stabilnější, než integrovaný klient v Průzkumníku Windows, který každou chvíli při přesunu souborů zamrzal. Byla zvolena možnost Add Drive, kde bylo nastaveno Type= WebDav, Name=NAS WebDav, URL= https://veřejná_ip nebo https://nazev.synology.me, SSL=Ano, Port=5006 a přihlašovací údaje příslušného uživatele. Nakonec stačí zvolit Save a Connect.

6.2 Mobilní telefon se systémem Android

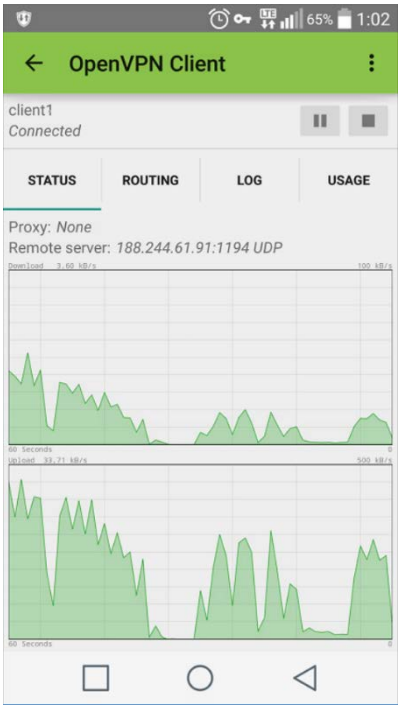
6.2.1 Připojení k OpenVPN serveru

Pro připojení pomocí telefonu s operačním systémem Android byla využita neoficiální placená aplikace OpenVPN Client a to z důvodu, jelikož jako jediná podporuje připojení v režimu TAP. Za aplikaci bylo zaplaceno (120 Kč), ale svou kvalitou, přehledností a pokročilými funkcemi předčila ve velké míře oficiální aplikaci, která navíc nepodporovala režim TAP [37].

Nejprve byla aplikace zakoupena a nainstalována v Internetovém katalogu aplikací Google Play. Následně se do telefonu vložily konfigurační soubory client1.ovpn a client2.ovpn.

Po spuštění aplikace byla zvolena možnost +\IMPORT VPN PROFILE, ve správci souborů byly nalezeny dříve vložené soubory a jeden po druhém importovány do aplikace.

Dále stačilo podle potřeby vybrat server, spustit jej a pro jistotu si zkontrolovat LOG údaje, zda proběhlo vše úspěšně.



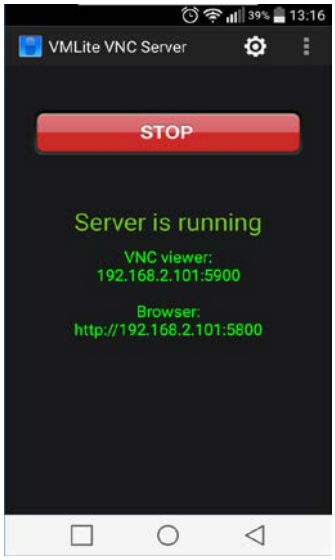
Obr. 41. OpenVPN Client – Status spojení.

Pokud bychom potřebovali zabezpečit komunikaci po internetu a skrýt svoji činnost, je možné přesměrovat veškerou Internetovou komunikaci do OpenVPN tunelu. Stačí změnit v aplikaci svoji výchozí bránu. To provedeme výběrem serveru, který chceme použít, zvolíme možnost úprav (ikona tužky)\Routing\Redirect gateway.

6.2.2 Vzdálená správa pomocí VNC serveru a klienta

V případě ovládání telefonu se systémem Android pomocí VNC je velmi málo možností výběru distribuce serveru (v době psaní této práce)). Nakonec byl nalezen jediný použitelný server s názvem VMLite VNC Server. Tato aplikace je bohužel placená, ale zato plně funkční, průběžně aktualizovaná a stabilní. [38] Tento VNC server lze spustit, pokud je na zařízení se systémem Android proveden tzv. ROOT zařízení, neboli jsou uživateli zpřístupněny práva super uživatele. ROOT se provádí u každého zařízení jiným způsobem, a proto doporučuji prostudovat postup pro svůj typ zařízení na stránce forum.xda-developers.com.

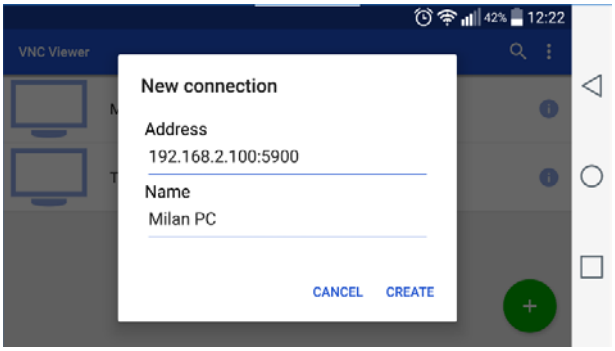
Po koupi, instalaci a spuštění aplikace bylo zvoleno nastavení (ikona matky), zde nastaveno VNC passport = heslo ke spojení, VNC port = 5900, případně další méně důležitá nastavení př. spuštění serveru společně se systémem, rotace obrazovky, počet přenesených snímků za sekundu atd.



Obr. 42. VMLite VNC Server – stavové okno.

V posledním kroku bylo zvoleno tlačítko Start server pro aktivaci serveru. Od tohoto okamžiku se můžeme k telefonu připojit a vzdáleně ho ovládat. Další postup napojení je totožný, jako v případě počítače, který byl již podrobně popsán.

VNC klient nainstalujeme na telefon s operačním systémem, který se bude k serveru připojovat. Byl zvolen klient ze stejné distribuce jako server, tudíž RealVNC klient, který byl stažen z internetového obchodu aplikací Google Play [39].



Obr. 43. RealVNC klient –Android.

Po stažení a instalaci RealVNC (Viewer) klienta byl v případě vzdálené komunikace spuštěn OpenVPN tunel, který byl dříve nakonfigurován a nyní slouží jako bezpečné spojení mezi zařízením kdekoliv v Internetu a zařízením v LAN síti. V případě lokální komunikace v LAN síti ho není potřeba. Nakonec byl spuštěn RealVNC klient, zvoleno +\New Connection a nastaveno:

Adress = lokální_ip_rařízení:vncport

Name = pojmenování zařízení do seznamu zařízení

6.2.3 Synchronizace dat pomocí NAS serveru

K synchronizaci dat mezi NAS serverem a telefonem byla využita oficiální mobilní aplikace Synology DS cloud [40]. Aplikace má identické možnosti nastavení i postupy konfigurace, jako v případě desktopové verze Synology Cloud Station Drive, která byla již výše podrobně popsána. Jediný rozdíl spočívá v možnosti automaticky zakázat synchronizaci na pozadí a synchronizovat pouze při spuštěné WiFi.

Aplikace byla nastavena pro synchronizaci fotek pořízených fotoaparátem telefonu. U systému Android se jedná v drtivé většině případů o složku /sdcard/DCIM.

6.2.4 Přístup k datům z NAS serveru

K připojení byla využita aplikace ES File Explorer. Jedná se o bezplatný a pokročilý správce souborů pro systém Android (viz. citace) [41].

Připojení skrze souborové služby Windows (SMB/CIFS)

Doporučeno využít v LAN nebo vzdáleně skrze OpenVPN tunel.

Po spuštění aplikace bylo vyvoláno hlavní menu (ikona v levém horním rohu, dále Síť\Síť\+\LAN. Zde nastavíme Server=192.168.2.10, přihlašovací údaje příslušného uživatele a Zobrazit jako=NAS SMB.

Připojení skrze FTP

Doporučené využití v LAN u zařízení nepodporujících SMB/CIFS nebo vzdáleně skrze šifrované OpenVPN spojení.

Po spuštění aplikace bylo vyvoláno hlavní menu (ikona v levém horním rohu, dále Síť\Síť\+\FTP. Zde nastavíme Server=192.168.2.10, Port=21, Způsob=Pasivní, Kódování=UTF-8, přihlašovací údaje příslušného uživatele a Zobrazit jako=NAS FTP.

Připojení skrze WebDAV

Doporučené využití pro přímý přístup k datům mimo lokální síť a OpenVPN.

Po spuštění aplikace bylo vyvoláno hlavní menu (ikona v levém horním rohu, dále Síť\Síť\+\webdav. Zde nastavíme Server=veřejná_ip nebo nazev.synology.me, Port=5006, Šifrování (https)=Ano, přihlašovací údaje příslušného uživatele a Zobrazit jako=NAS WEBDAV.

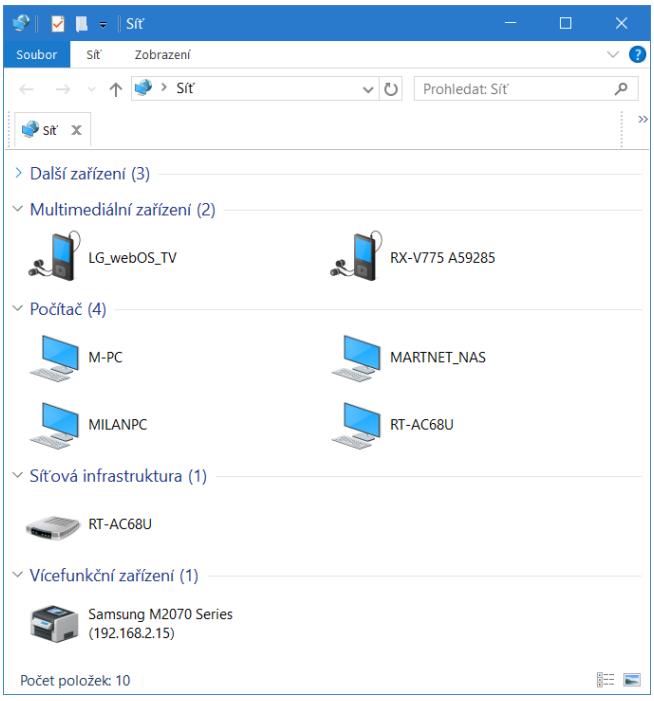
6.3 Televize

6.3.1 Reprodukce multimediálních dat z domácí sítě

Pro reprodukci multimediálních dat ze sítě byla využita technologie UPnP/DLNA. Kdy se pokládá televize za zobrazovač, případně i ovladač pro DLNA server, ze kterého se přesměrují multimediální data typu fotky, audio a video do zobrazovače (pro pochopení doporučuji přečíst si teorii v úvodu práce).

Pro příklad zde uvedu 2 základní příklady využití:

1. DLNA ovladač=počítač s Windows, DLNA Server=NAS, DLNA zobrazovač= TV
   Pokud je počítač, televizor i NAS ve stejné síti, případně je počítač k síti připojen skrze OpenVPN tunel v režimu TAP, už o sobě zařízení díky multicastové komunikaci vědí. Pro jistotu otevřeme průzkumník Windows (zkratka WIN+E) a v bočním menu zvolíme Síť. Zde nalezneme přehled všech zařízení v síti včetně DLNA serverů, které jsou řazeny jako multimediální zařízení.



Obr. 44. Windows 10 - Nalezená multimediální zařízení s podporou DLNA.

Nyní stačí vybrat soubor (zvuk, obraz, video) umístěný na jakémkoliv síťovém zařízení (v našem případě MARTNET_NAS) nebo přímo na lokálním disku PC. U souboru vyvoláme kontextovou nabídku a zvolíme Vysílat na zařízení.

Zde jsou zobrazeny automaticky všechny dostupné DLNA zobrazovače v síti. Vybereme tedy zařízení, na kterém se má soubor zobrazit a přehrát (v našem případě LG_WebOS_TV). Pokud bylo v nastavení televizoru zvoleno, že s ním může komunikovat jakékoliv DLNA zařízení, médium se začne během okamžiku přehrávat. Zároveň se zobrazí ovladač pro změnu hlasitosti, přetáčení atd.

2. DLNA ovladač=TV, DLNA Server=NAS, DLNA zobrazovač= TV
   Většina televizorů s podporou DLNA obsahuje aplikaci, díky které můžeme zvolit některý z DLNA serverů v LAN síti, prohlédnout si jeho knihovnu indexovaných souborů a vybrat soubor pro spuštění přímo na televizoru.
   Jak už bylo uvedeno výše v případě, že DLNA server SYNOLOGY_NAS po prvotní komunikaci se zobrazovačem zjistí, že určitý soubor nedokáže přehrát, začne v reálném čase soubor převádět do podporovaného formátu.

6.3.2 Vzdálená správa

Ke vzdálenému ovládání televize byla využita mobilní aplikace AnyMote [42]. Tato aplikace podporuje značné množství síťových zařízení jako TV, AV Receiver atd., kdy jim plně nahradí běžný ovladač.

Po instalaci aplikace byla zvolena hlavní nabídka\+\add remote\Wifi device\LG Smart TV\ Add device manualy, zde byla nastavena statická lokální IP adresa televize 192.168.2.19. Po uložení se v hlavní nabídce zobrazilo nové zařízení. Některé televize po prvním připojení zobrazí hlášku pro povolení spárovaného zařízení. Po potvrzení lze TV nadále přes síť vzdáleně ovládat.

Obr. 45. Vzdálená správa TV – aplikace AnyMote.

6.4 AV Receiver

6.4.1 Reprodukce multimediálních dat z domácí sítě

Pro reprodukci multimediálních dat ze sítě byla opět, jako v případě televize, využita technologie UPnP/DLNA. Principy i postupy jsou prakticky identické jako v případě televize až na skutečnost, že DLNA zobrazovač je tentokrát AV Receiver, na který budeme posílat převážně audio soubory.

6.4.2 Vzdálená správa

Ke vzdálenému ovládání AV receiveru byla rovněž jako u TV využita mobilní aplikace AnyMote [42]. Zde byla nastavena statická lokální IP adresa AV Receiveru 192.168.2.16.

Další z možností, jak zařízení vzdáleně ovládat, je pomocí Internetového prohlížeče připojeného do webového rozhraní. Pro připojení k rozhraní je potřeba zadat statickou lokální IP adresu AV Receiveru 192.168.2.16.

Obr. 46. AV Receiver Yamaha RX-V775 Webové rozhraní.

6.5 Žárovka

6.5.1 Konfigurace připojení

Po upevnění žárovky do objímky a zapnutí napájení byla stažena aplikace pro její správu [43]. Aplikace je dostupná v Internetových katalozích aplikací pro platformu Android, Apple iOS a Windows 10 Moderní aplikace.

Po prvním spuštění aplikace byl vytvořen účet, sloužící k synchronizaci nastavení v případě používání více klientských zařízení (jako PC, telefon, atd.) a také k možnosti vzdáleného přístupu k žárovkám pomocí cloudu. Kdy probíhá komunikace s žárovkou prostřednictvím vzdáleného serveru společnosti Lifx.

Párování žárovky bylo vyvoláno volbou +\Connect light, poté bylo potřeba odpojit se od lokální bezdrátové Wifi sítě a připojit se k žárovce, která nejprve běží v režimu bezdrátového přístupového bodu. Po připojení byla určena skrze aplikaci Lifx síť, na kterou se má žárovka napojit a přístupové údaje k této síti.. Jelikož žárovka nepodporuje WiFi pásmo 5 GHz byla vybrána 2,4 GHz sít. Poté se žárovka i mobil připojily do lokální bezdrátové sítě a od toho okamžiku spolu komunikují skrze ni. Po úspěšném připojení byla žárovka v aplikaci přiřazena do lokace Location = Domov, skupiny Group = Pokoj 1a jméno žárovky Name = Milan. Nyní bylo možné žárovku používat v lokální síti i vzdáleně z Internetu skrze cloud účet firmy Lifx [44].

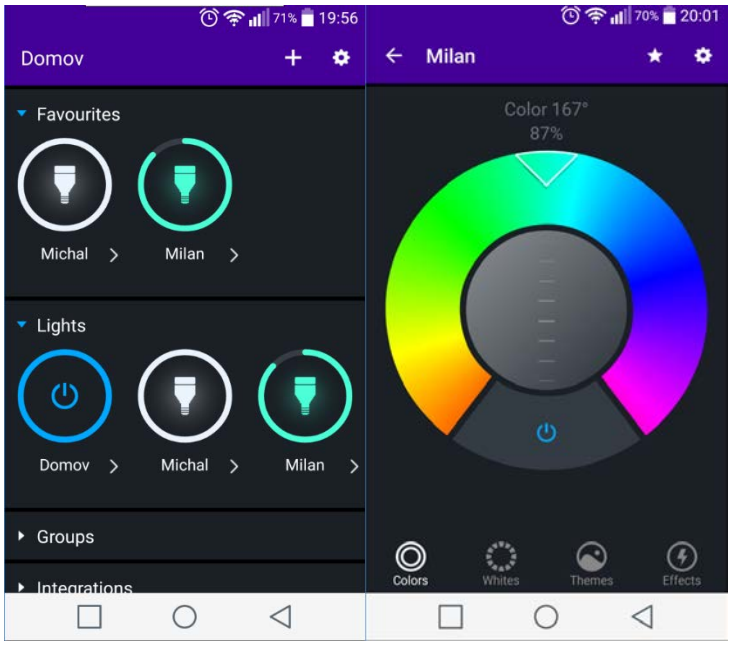
V případě špatného nastavení je potřeba žárovku uvést do továrního nastavení, které vyvoláme tak, že žárovku pětkrát po sobě rychle vypneme a zapneme. Správnost resetu poznáme sekvencí červeného, zeleného a bílého světla [44].

Dále byl povolen přístup k žárovce pomocí služby IFTTT. Nejprve byla stažena a nainstalována aplikace pro operační systém Android [45]. Po prvním spuštění byla provedena registrace z obdobných důvodů, jako v případě Lifx. Poté byl napojen účet IFTTT na účet Lifx pro zpřístupnění žárovky této službě. V aplikaci IFTTT bylo zvoleno Settings\Channels, zde byl vyhledán kanál Lifx\Connect. Po zadání přihlašovacích údajů a potvrzení Autorizace byl kanál přidán.

6.5.2 Vzdálená správa

Aplikace Lifx slouží k lokálnímu i nově přidanému vzdálenému ovládaní. Lze s ní provádět základní úkony jako zapínání, vypínání, změnu barvy a jasu světla, různé světelné efekty,

barevnou hudbu a časování automatického zapnutí a vypnutí a aktualizace firmware žárovky.



Obr. 47. Prostředí aplikace Lifx.

Pro pokročilé funkce slouží služba IFTTT, kterou se dá vytvořit libovolný algoritmus chování, a tudíž jsou možnosti konfigurace skoro neomezené. Služba pracuje na podobném principu, jako příkaz if v běžném programování, kdy lze do podmínky vložit jakýkoliv kanál v databázi služby (př. Gmail,..) a také samotné funkce telefonu.

Pro příklad uvedu nastavení, kdy pokud klesne baterie telefonu pod hranici 15 % tak 5x zablikej červenou barvou s intenzitou 80 %. V aplikaci zvolíme Create a new recipe, za podmínku if zvolíme Android Battery\Battery drops below 15 %, za podmínku then zvolíme Lifx\Blink lights, Which lights? = Domov –Pokoj 1, Turn on first? = Yes, Number of blinks = 5, Color = Red, Brightness = 80 % nakonec nastavení potvrdíme.

Pro případ dalších automatizačních aplikací třetích stran lze uvést Automateit a Tasker. Kromě automatizačních aplikací stojí za zmínku také známá aplikace AnyMote. Tato aplikace slouží k univerzálnímu ovládání většiny zařízení přes infraport nebo LAN.

6.6 Tiskárna

Při instalaci ovladačů tiskárny byla zvolena možnost síťové připojení skrze LAN. Tiskárna byla automaticky nalezena v sítí pod statickou IP adresou 192.168.2.15. Dále proběhla úspěšná instalace.

ZÁVĚR

Cílem práce bylo navrhnout a vybudovat moderní domácí síť s využitím NAS serveru a možností vzdáleného připojení pomocí VPN. Po důkladném studiu této problematiky, jako například využití NAS serveru, monitoringu, vzdálené správy, zabezpečení a dalších možností moderních počítačových sítí, byla práce rozšířena nad rámec zadání.

Všechny cíle, které byly stanoveny, se podařilo úspěšně splnit. Nejvíce času zabral návrh síťové infrastruktury. Především výběr vhodných komponentů a následné zapojení veškerých rozvodů. UTP kabel kategorie 6 v provedení drát je oproti běžně používanému 5E velmi netvarný a z počátku bylo velmi obtížné s ním pracovat, hlavně při osazování do skládaných konektorů RJ45.

Při studiu a následné realizaci šifrované OpenVPN komunikace bylo zapotřebí řešit několik úskalí, která se podařilo postupem času jedno po druhém vyřešit. Nejzdlouhavějším problémem bylo přizpůsobení konfigurace OpenVPN serveru domácímu druhu internetového připojení, kdy nebyla poskytovatelem Internetu přiřazena veřejná IP adresa přímo, ale pomocí několika překladů IP adres (NAT). Navíc byl zablokován potřebný komunikační port.

Další zapojování a konfigurace, jako je směrování portů, konfigurace NAS serveru, synchronizace dat, zálohování, kamerový systém, vzdálená správa, ovládání a přenosy dat pomocí různých souborových protokolů mezi zařízeními v síti a další, již probíhaly bez větších problémů.

Postupem času po nashromáždění potřebných finančních prostředků bude projekt rozšířen o UPS (Uninterruptible Power Supply/Source) záložní zdroj. Tento zdroj bude připojen na napájecí adaptér NAS serveru a v případě neočekávaného odpojení přívodu elektrické energie poskytne serveru napájení na dostatečně dlouhou dobu, aby se bezpečně vypnul a tak předešel ztrátě dat a dalším možným závadám.

Další rozšíření bude následovat zakoupením expanzní jednotky včetně 2 interních 3 TB disků, díky kterým bude možno NAS server zapojit do diskového pole RAID-5. Tím bude zajištěna ochrana dat před závadou jednoho disku s ohledem na zachování co nejvyššího úložného prostoru.

SEZNAM POUŽITÉ LITERATURY

[1] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.

[2] Proč kategorie 6?. *KOMPONENTY DATOVÝCH A TELEKOMUNIKAČNÍCH SÍTÍ | Intelek* [online]. [cit. 2016-04-14]. Dostupné z: http://www.intelek.cz/info.jsp?name=proc_cat6&highlight=305m

[3] Zapojenie -TP kábla. *Somr zdrojáky* [online]. [cit. 2016-05-05]. Dostupné z: http://www.somr.genezis.eu/elektro/ZapojenieSietoveho-TPkabla.html

[4] KRČMÁŘ, Petr. *Linux: postavte si počítačovou síť*. 1. vyd. Praha: Grada, 2008, 182 s. Průvodce (Grada). ISBN 9788024712901.

[5] OpenVPN - Open Source VPN. *OpenVPN* [online]. [cit. 2016-04-18]. Dostupné z: https://openvpn.net/

[6] Průvodce OpenVPN. *OpenManiak.com* [online]. [cit. 2016-04-18]. Dostupné z: http://openmaniak.com/cz/openvpn_tutorial.php

[7] KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 9788025122365.

[8] Dvoupásmový Wireless-AC1900 gigabitový router. *ASUS Česká republika* [online]. [cit. 2016-04-16]. Dostupné z: https://www.asus.com/cz/Networking/RTAC68U/

[9] Jak chrání AiProtection mou domácí síť?. *ASUS Česká republika* [online]. [cit. 2016-04-23]. Dostupné z: https://www.asus.com/cz/support/faq/1012070/

[10] ASUSWRT JEDNODUCHÉ UŽIVATELSKÉ ROZHRANÍ. *ASUS Česká republika* [online]. [cit. 2016-04-16]. Dostupné z: http://www.asus.com/cz/Networking/RTAC68U/ASUSWRT/

[11] VNC a Vzdálená plocha - kouzlo vzdáleného přístupu. *PCTuning* [online]. 2009 [cit. 2016-04-23]. Dostupné z: http://pctuning.tyden.cz/software/jak-zkrotit-internet/12639-vnc_a_vzdalena_plocha-kouzlo_vzdaleneho_pristupu?start=1

[12] Connect LIFX to hundreds of apps. *IFTTT* [online]. [cit. 2016-04-23]. Dostupné z: https://ifttt.com/lifx

[13] Znalostní databáze Synology. *Synology* [online]. [cit. 2016-04-29]. Dostupné z: https://www.synology.com/cs-cz/knowledgebase

[14] KUROSE, James a Keith ROSS. *Počítačové sítě*. 1. vyd. Brno: Computer Press, 2014, 622 s. ISBN 9788025138250.

[15] DLNA: snadné přehrávání filmů z PC v TV. *AVmania.cz* [online]. [cit. 2016-04-30]. Dostupné z: http://avmania.e15.cz/dlna-snadne-prehravani-filmu-z-pc-v-tv

[16] TCP/IP - skupinové vysílání IP Multicast a Cisco. *SAMURAJ-cz.com* [online]. [cit. 2016-05-01]. Dostupné z: http://www.samuraj-cz.com/clanek/tcpip-skupinove-vysilani-ip-multicast-a-cisco/

[17] Instalační kabel Solarix CAT6 UTP PVC 500m/cívka SXKD-6-UTP-PVC. *KOMPONENTY DATOVÝCH A TELEKOMUNIKAČNÍCH SÍTÍ | Intelek* [online]. [cit. 2016-04-14]. Dostupné z: http://www.intelek.cz/product.jsp?artno=26000001

[18] Domovní vypínače a zásuvky Logus 90: Technický katalog. *Elkoep.cz* [online]. 2013 [cit. 2016-04-23]. Dostupné z: http://eshop.elkoep.cz/documents/logus90/share_dokumentace/cs/logus90_technicky.pdf

[19] Konektor RJ45 CAT6 UTP 8p8c nestíněný skládaný na drát KRJ45/6SLD. *Intelek* [online]. [cit. 2016-04-23]. Dostupné z: http://www.intelek.cz/product.jsp?artno=11238905#

[20] 8portový gigabitový switch Easy Smart TL-SG108E. *TP-LINK* [online]. [cit. 2016-04-23]. Dostupné z: http://cz.tp-link.com/products/details/cat-41_TL-SG108E.html#overview

[21] DiskStation DS716+: Ideální NAS server pro rozvíjející se firmy. *Synology* [online]. [cit. 2016-04-23]. Dostupné z: https://www.synology.com/cs-cz/products/DS716+#

[22] Synology DiskStation DS716+ Stručná instalační příručka. *Synology* [online]. [cit. 2016-04-23]. Dostupné z: https://global.download.synology.com/download/Document/QIG/DiskStation/16-year/DS716+/Syno_QIG_DS716+_csy.pdf

[23] Velký test šesti pevných disků s kapacitou 3 TB: Western Digital Red. *PCTuning* [online]. 2015 [cit. 2016-04-14]. Dostupné z: http://pctuning.tyden.cz/hardware/disky-cd-dvd-br/34599-velky-test-sesti-pevnych-disku-s-kapacitou-3-tb?start=3

[24] Color 1000 Technical Info Sheet. *LIFX* [online]. [cit. 2016-04-23]. Dostupné z: http://www.lifx.com/pages/color-1000-info-sheet

[25] Foscam FI9828P Outdoor Waterproof: PTZ Wireless Dome IP Camera. *Foscam Official Website* [online]. [cit. 2016-04-24]. Dostupné z: http://foscam.com/fi9828p

[26] Wi-Fi: Jak si zajistit velké pokrytí, rychlost a silný signál. *Živě.cz* [online]. 2014 [cit. 2016-04-24]. Dostupné z: http://www.zive.cz/clanky/wi-fi-jak-si-zajistit-velke-pokryti-rychlost-a-silny-signal/anteny-a-jejich-nastaveni-deformace-a-ztrata-signalu-mereni/sc-3-a-172347-ch-90933/default.aspx#articleStart

[27] About. *Asuswrt-Merlin: A custom firmware for Asus routers* [online]. [cit. 2016-04-15]. Dostupné z: http://asuswrt.lostrealm.ca/about

[28] ASUS Router. *Google Play* [online]. [cit. 2016-04-17]. Dostupné z: https://play.google.com/store/apps/details?id=com.asus.aihome

[29] Quick & simple VPN setup guide: using OpenVPN on a ‘Tomato’ router. *Today, guess what ...* [online]. 2011 [cit. 2016-04-19]. Dostupné z: http://todayguesswhat.blogspot.cz/2011/03/quick-simple-vpn-setup-guide-using.html

[30] Download for TL-SG108E V1. *TP-LINK* [online]. [cit. 2016-04-25]. Dostupné z: http://www.tp-link.com/en/download/TL-SG108E_V1.html#Easy_Smart_Configuration_Utility

[31] TinyCam Monitor FREE. *Google Play* [online]. [cit. 2016-04-24]. Dostupné z: https://play.google.com/store/apps/details?id=com.alexvas.dvr

[32] Technické údaje - Surveillance 7.2. *Synology* [online]. [cit. 2016-04-25]. Dostupné z: https://www.synology.com/cs-cz/surveillance/7.2/spec

[33] VNC remote access software for desktop and mobile platforms.. *RealVNC remote access & control software for desktop and mobile* [online]. [cit. 2016-04-23]. Dostupné z: https://www.realvnc.com/download/vnc/

[34] Centrum pro stahování. *Synology* [online]. [cit. 2016-04-25]. Dostupné z: https://www.synology.com/cs-cz/support/download/DS716+

[35] Popis softwaru - DSM 6.0. *Synology* [online]. [cit. 2016-04-25]. Dostupné z: https://www.synology.com/cs-cz/dsm/6.0/software_spec/dsm

[36] NetDrive - The Network Drive for Windows (FTP, SFTP, WebDAV, Google Drive, Dropbox, Box.com, S3, OneDrive, OpenStack). *NetDrive* [online]. [cit. 2016-04-27]. Dostupné z: http://www.netdrive.net/

[37] OpenVPN Client. *Google Play* [online]. [cit. 2016-04-23]. Dostupné z: https://play.google.com/store/apps/details?id=it.colucciweb.openvpn&hl=cs

[38] VMLite VNC Server. *Google Play* [online]. [cit. 2016-04-23]. Dostupné z: https://play.google.com/store/apps/details?id=com.vmlite.vncserver

[39] VNC Viewer. *Google Play* [online]. [cit. 2016-04-23]. Dostupné z: https://play.google.com/store/apps/details?id=com.realvnc.viewer.android

[40] DS cloud. *Google Play* [online]. [cit. 2016-04-26]. Dostupné z: https://play.google.com/store/apps/details?id=com.synology.dscloud

[41] ES File Explorer File Manager. *Google Play* [online]. [cit. 2016-04-27]. Dostupné z: https://play.google.com/store/apps/details?id=com.estrongs.android.pop

[42] AnyMote Universal Remote. *Google Play* [online]. [cit. 2016-05-01]. Dostupné z: https://play.google.com/store/apps/details?id=com.remotefairy4&hl=cs

[43] LIFX. *Google Play* [online]. [cit. 2016-04-24]. Dostupné z: https://play.google.com/store/apps/details?id=com.lifx.lifx

[44] Setup your LIFX. *LIFX* [online]. [cit. 2016-04-24]. Dostupné z: https://support.lifx.com/hc/en-us/categories/200238164-Setup-your-LIFX

[45] IF by IFTTT. *Google Play* [online]. [cit. 2016-04-24]. Dostupné z: https://play.google.com/store/apps/details?id=com.ifttt.ifttt

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3G 3 Generation

4G 4 Generation

8P8C 8 position 8 contact

AES-NI Advanced Encryption Standard New Instructions

AiProtection Artificial Intelligence Protection

AiRadar Artificial Intelligence Radar

AWG American Wire Gauge

Btrfs B-tree file systém

CA Certification Authority

Cat 5 Category 5

Cat 6 Category 6

CBC Cipher Block Chaining

CIFS Common Internet File Systém

CPU Central Processing Unit

DDNS Dynamic Domain Name Service

DDR3 Double Data Rate 3

DHCP Dynamic Host Configuration Protocol

DLNA Digital Living Network Alliance

DNS Domain Name Service

DSM Synology DiskStation Manager

DVB-S Digital Video Broadcasting – Satelite

DVB-T Digital Video Broadcasting – Terrestrial

EIA Electronic Industries Alliance

eSATA External Serial ATA

EXT3 Third Extended Filesystem

EXT4 Fourth Extended Filesystem

FAT File Allocation Table

FM Frequency Modulation

FPS Frames Per Second

FTP File Transfer Protokol

GTM Greenwich Mean Time

HDD Hard Disk

HFS+ Hierarchical File Systém +

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

IFTTT If This Then That

IGMP Internet Group Management Protocol

IP Internet Protocol

IPTV Internet Protocol television

JBOD Just a Bunch Of Disks

L2 Layer 2

L2TP Layer 2 Tunneling Protocol

LAN Local Area Network

LNB Low-noise block

MAC Media Access Control

MDI Medium Dependent Interface

MDI-X Medium Dependent Interface Crossover

MIMO Multi Input Multi Output

NAS Network Attached Storage

NAT Network Address Translation

NAT Network Address Translation

NTFS New Technology File Systém

OpenVPN Open Virtual Private Network

OSI Open Systems Interconnection

P2P Peer to Peer

PoE Power on Ethernet

PPTP Point-to-Point Tunneling Protocol

PTZ Pan Tilt Zoom

PVC Polyvinylchlorid

QOS Quality Of Services

RAID Redundant Array of Inexpensive/Independent Disks

RAM Random Access Memory

RJ45 Registered Jack 45

SATA Serial ATA

SHA-1 Secure Hash Algorithm 1

SMB Server Message Block

SSL Secure Sockets Layer

STP Shielded Twisted Pair

TCP Transmission Control Protocol

TIA Telecommunications Industry Association

TLS Transport Layer Security

UDP User Datagram Protocol

UPnP Universal Plug and Play

UPS Uninterruptible Power Source

URL Uniform Resource Locator

UTF-8 UCS Transformation Format 8 bit

UTP Unshielded Twisted Pair

VLAN Virtual Local Area Network

VNC Virtual Network Computing

VoIP Voice over Internet Protocol

VPN Virtual Private Network

WD Western Digital

WebDAV Web-based Distributed Authoring and Versioning

WEP Wired Equivalent Privacy

WOL Wake On Lan

WPA-PSK Wi-Fi Protected Access Pre-Shared Key

WPA2-PSK Wi-Fi Protected Access 2 Pre-Shared Key

WPS Wireless Provisioning Services

SEZNAM OBRÁZKŮ

SEZNAM TABULEK