
# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

## ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS


# NÁVRH SÍŤOVÉ INFRASTRUKTURY POBOČKOVÉ SÍTĚ
NETWORK INFRASTRUCTURE DESIGN OF A COMPANY BRANCHES

DIPLOMOVÁ PRÁCE
MASTER'S THESIS


AUTOR PRÁCE
AUTHOR
Bc. Marek Částek

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Viktor Ondrák, Ph.D.


BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

# Zadání diplomové práce

| | |
|---|---|
| Ústav: | Ústav informatiky |
| Student: | **Bc. Marek Částek** |
| Studijní program: | Systémové inženýrství a informatika |
| Studijní obor: | Informační management |
| Vedoucí práce: | **Ing. Viktor Ondrák, Ph.D.** |
| Akademický rok: | 2019/20 |

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

## Návrh síťové infrastruktury pobočkové sítě

**Charakteristika problematiky úkolu:**

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska práce
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

**Cíle, kterých má být dosaženo:**

Navrhnout počítačovou síť.

**Základní literární prameny:**

DONAHUE, G. A. Kompletní průvodce síťového experta. 1. vyd. Brno: Computer Press, 2009. 528 s. ISBN 978-80-251-2247-1.

HORÁK, J. a M. KERŠLÁGER. Počítačové sítě pro začínající správce. 5. aktualiz. vyd. Brno: Computer Press, 2011. 303 s. ISBN 978-80-251-3176-3.

JIROVSKÝ, V. Vademecum správce sítě. 1. vyd. Praha: Grada, 2001. 428 s. ISBN 80-7169-745-1.

SCHATT, S. Počítačové sítě LAN od A do Z. 1. vyd. Praha: Grada, 1994. 378 s. ISBN 80-85623-76-5.

TRULOVE, J. Sítě LAN: hardware, instalace a zapojení. 1. vyd. Praha: Grada, 2009. 384 s. ISBN 978-80-247-2098-2.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

| | |
|---|---|
| doc. RNDr. Bedřich Půža, CSc.<br>ředitel | doc. Ing. et Ing. Stanislav Škapa, Ph.D.<br>děkan |

Abstrakt

Diplomová práce se zaměřuje na návrh síťové infrastuktury pobočkové sítě společnosti Občanům, s.r.o. Návrh spočívá ve vytvoření kompletní dokumentace k implementaci počítačové sítě dle požadavků investora a obsahuje jak aktivní, tak pasivní prvky a konkrétní způsoby zabezpečení.

Abstract

This master's thesis focuses on computer network design of multiple Občanům, s.r.o. company branches. The design consists of creating complete implementation documentation according to investor demands, which also includes passive and active network components, and specific security technologies.

Klíčová slova

počítačová síť, komunikační infrastruktura, LAN, zabezpečení sítě, 802.1x

Key words

computer network, communication infrastructure, LAN, network security, 802.1x

Bibliografická citace

ČÁSTEK, Marek. Návrh síťové infrastruktury pobočkové sítě [online]. Brno, 2020 [cit. 2020-05-17]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/125653. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Viktor Ondrák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 1. března 2020

……..

podpis studenta

Poděkování

Rád bych poděkoval vedoucímu práce Ing. Viktorovi Ondrákovi, Ph.D. za cenné rady, věcné připomínky a vstřícnost při konzultacích v průběhu vypracování diplomové práce.

# OBSAH

# ÚVOD

Správně fungující počítačová síť je důležitou součástí každé společnosti, do jejich postupného rozvoje a zabezpečení směřují nezanedbatelné finanční prostředky. Přináší vyšší pracovní efektivitu, snazší přístup k informacím, umožňují sdílení softwarových i hardwarových prostředků a z toho plynoucí úspory. Efektivně a spolehlivě fungující počítačová síť je tedy základním stavebním kamenem podniku.

Ve svojí diplomové práci se zabývám návrhem síťového řešení pro vznikající síť malých firemních poboček, od kterých si společnost slibuje zejména stabilní zázemí pro obchodníky a usnadnění kontaktu se zákazníkem.

Počítačová síť bude vybudována profesionálně firmou, která se tímto zabývá, nicméně k tomu je třeba dobře vypracovaného návrhu a dokumentace nové sítě, který bude počítat i s jistou rozdílností těchto poboček, zejména v ohledu jejich rozlohy. V návrhu je třeba počítat nejen s výběrem aktivních a pasivních prvků, ale také s včleněním do stávající infrastruktury společnosti.

# 1 VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Cílem diplomové práce je návrh řešení počítačové sítě pro vznikající malé pobočky společnosti. Na základě analýzy současného stavu navrhnu a zadokumentuji takové síťové řešení, které bude odpovídat požadavkům investora a zároveň jej bude možné včlenit do stávající infrastruktury společnosti.

# 2 ANALÝZA SOUČASNÉHO STAVU

V této kapitole je provedena analýza společnosti, pro jejíž pobočky budu provádět návrh počítačové sítě.

Představím samotnou společnost, tedy investora, její požadavky a taktéž popíšu konkrétní vzorové pobočky, pro které budu návrh provádět. Na lokalitách se žádné stávající řešení počítačové sítě nevyskytuje. Poté popíšu aktuální síťovou infrastrukturu společnosti (holdingu), do které bude potřeba síťové řešení nových poboček začlenit.

## 2.1 Popis firmy

Společnost Občanům, s.r.o. se zabývá zejména poradenstvím v oblasti energetiky pro všechny typy klientů. Cestou k této činnosti byla liberalizace trhu v roce 2007, kdy bylo všem odběratelům elektřiny či plynu umožněno svobodně změnit dodavatele komodit zejména díky změnám dvou energetických směrnic Evropské unie, 2003/54/ES (společná pravidla pro trh s elektrickou energií) a 2003/55/ES (společná pravidla pro trh se zemním plynem).

Soustředí se na 3 nejběžnější komodity: elektřinu, plyn a vodu. Specializuje se na stlačení ceníkových cen za komodity na velkoobchodní úroveň pomocí tzv. energetických aukcí, kde soutěžícími jsou dodavatelé energií. Díky sdružování zákazníků pod větší celky mají dodavatelé výrazně lepší motivaci k nabídnutí nižších cen, než jakých by byl schopen dosáhnout jednotlivec.

Formou se jedná o společnost s ručením omezeným se zhruba 250 zaměstnanci. Občanům, s.r.o., je dceřinou společností holdingu TG Community Holding a.s. a zároveň investorem vytvoření síťové infrastruktury na svých pobočkách.

### 2.1.1 Marketingová strategie

Společnost oslovuje nové, potenciální zákazníky zejména pomocí sítě obchodních zástupců, tedy aktivním prodejem služeb a později také aktivním telemarketingem, jehož funkcí je domluvit schůzku klienta s obchodním zástupcem. Později přibyla i pasivní marketingová strategie v podobě e-přihlášky na webu a zapojení obcí jako celků do aukcí.

Firma jako zdroj nových zákazníků využívá také doporučení, díky své dobré pověsti, kterou si za dobu působení na trhu získala. Mezi takto získané zákazníky se řadí hlavně obce a firmy.

## 2.2 Základní údaje společnosti

Datum vzniku a zápisu: 28. srpen 2017

Obchodní firma: Občanům s.r.o.

Sídlo: Vídeňská 995/63, Štýřice, 639 00 Brno

Identifikační číslo: 06380964

Počet zaměstnanců: 250

## 2.3 Popis objektů

V plánu je pronájem až dvaceti takřka identických poboček, vždy půjde o kancelářské přízemní prostory o velikosti maximálně dvou místností, z nichž jedna bude sloužit pro setkávání s klienty. Prostory zpravidla obsahují sociální zázemí, tyto místnosti jsou ale z hlediska návrhu síťové infrastruktury nezajímavé, naopak z důvodu prostorových omezení není možné vytvořit dedikovanou telekomunikační místnost.

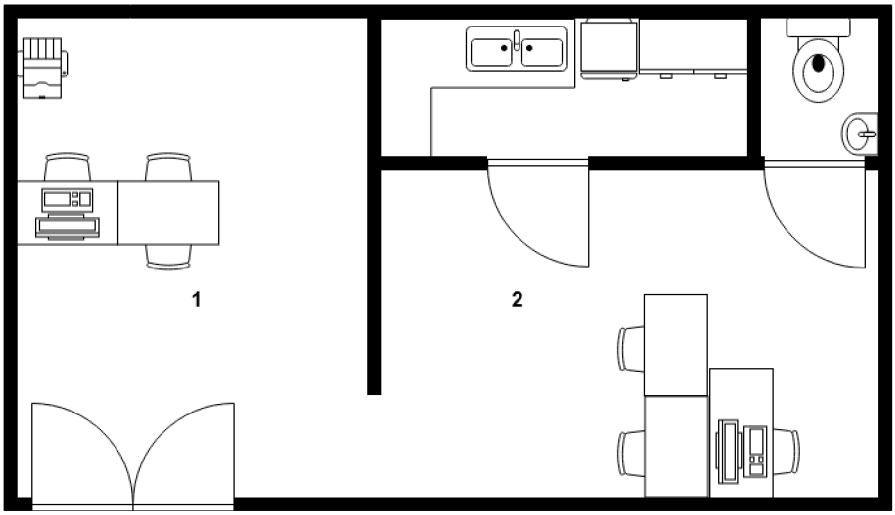
V první fázi dojde k pronájmu tří poboček, které se pouze nepatrně liší rozlohou:

- Jihlava, Masarykovo náměstí
- Brno, Mojmírovo náměstí
- Zlín, nám. T. G. Masaryka

Stěny mezi místnostmi i obvodové zdivo je ve všech třech případech zděné z plných cihel. Pouze na jedné z poboček (Jihlava) se nachází sádrokartonový podhled, na jeho přítomnost se při tvorbě návrhu tedy nelze spoléhat.

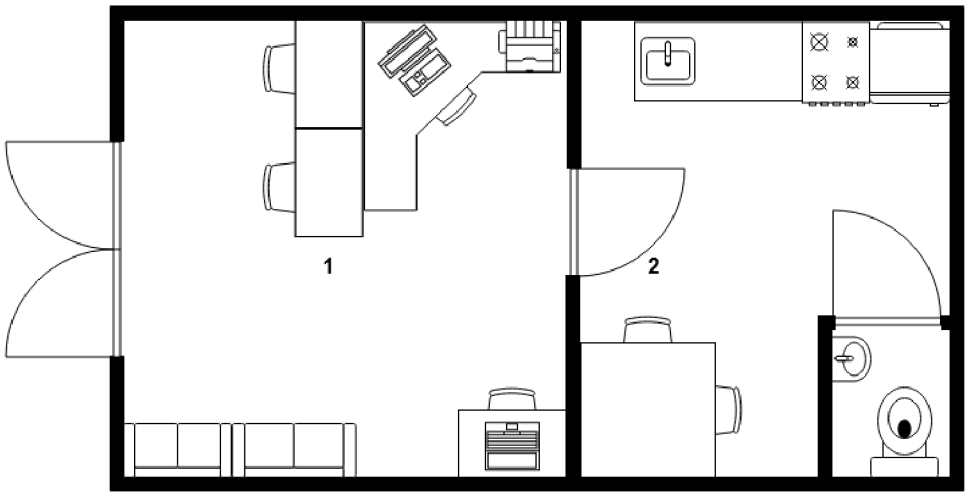
### 2.3.1 Popis místností

Z půdorysů je zřejmé, že pobočky mají dvě místnosti, přičemž vstup do prostor se nachází vždy v místnosti 1.



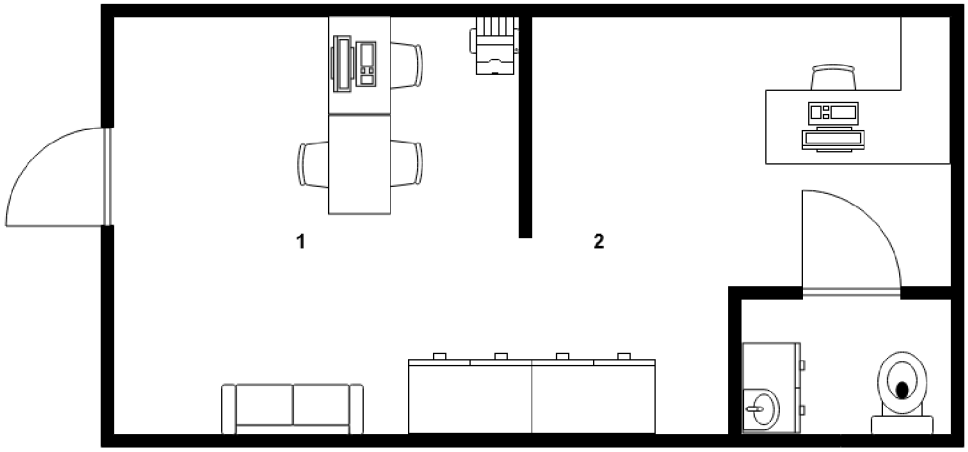

**Obrázek č. 1: Půdorys pobočky Jihlava**

(Zdroj: vlastní zpracování)




**Obrázek č. 2: Půdorys pobočky Zlín**

(Zdroj: vlastní zpracování)




**Obrázek č. 3: Půdorys pobočky Brno**

(Zdroj: vlastní zpracování)

Z půdorysů dále vyplývá, že místnost 1 je reprezentativním prostorem pro setkávání s klienty. Místnost 2 slouží jako zázemí, ve kterém je v případě poboček v Brně a Jihlavě umístěno druhé pracovní místo. V případě Zlínské pobočky toto prozatím plánováno není, protože druhé pracovní místo je taktéž v místnosti 1, dle domluvy s investorem zde ale přesto dojde k umístění dvou datových zásuvek.

**Tabulka č. 1: Popis místností** (Zdroj: vlastní zpracování)

| Pobočka | Číslo místnosti | Plocha | Počet přípojných míst | Připojená zařízení |
|---|---|---|---|---|
| **Jihlava** | 1 | 24 | 4 | PC, tiskárna, access point |
| **Jihlava** | 2 | 26 | 2 | PC |
| **Brno** | 1 | 25 | 4 | PC, tiskárna, access point |
| **Brno** | 2 | 17 | 2 | PC |
| **Zlín** | 1 | 36 | 4 | 2xPC, tiskárna, access point |
| **Zlín** | 2 | 30 | 2 | |

Kromě již zmíněného pokrytí všech místností bezdrátovým wifi signálem investor požaduje rozvržení dle přiložených půdorysů, tedy:

**Jihlava, místnost 1**

V této místnosti bude umístěno jedno PC, tiskárna a access point připevněný ke stropu, u příčky mezi místnostmi. U PC má být též umístěn stolní VOIP telefon.

**Jihlava, místnost 2**

V této místnosti je požadováno umístění PC se stolním telefonem, tedy kompletní druhé pracovní místo, nicméně taktéž se zde musí nacházet malý datový rozvaděč.

**Zlín, místnost 1**

Zde je požadováno umístění dvou pracovních míst, tedy 2x PC, 2x VOIP telefon a tiskárny. Taktéž zde bude třeba umístit access point, k příčce mezi místnostmi 1 a 2.

### Zlín, místnost 2

Zde bude umístěn pouze datový rozvaděč a dle domluvy s investorem budou též v rohu místnosti (u stolu) umístěny datové zásuvky.

### Brno, místnost 1

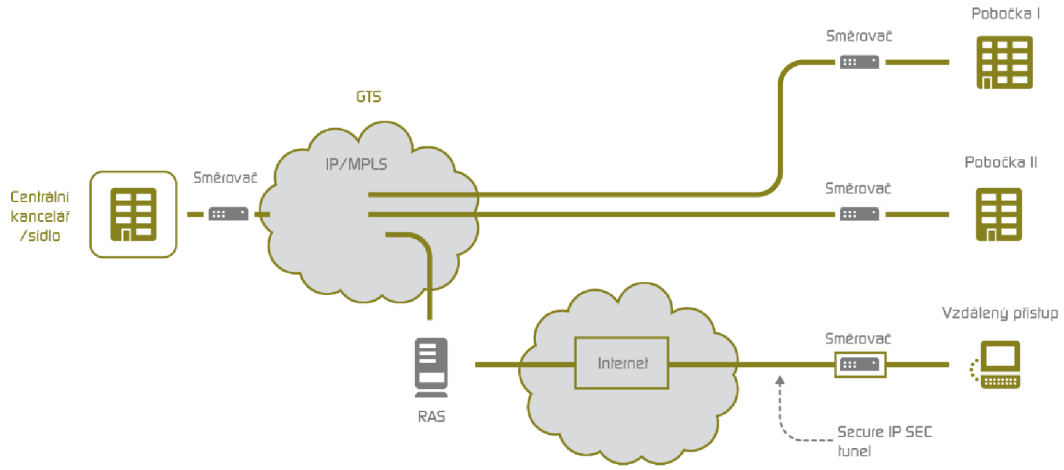
V místnosti 1 bude umístěno PC, stolní VOIP telefon a tiskárna. Na rozhraní místností 1 a 2 též dojde k montáži access pointu na strop.

### Brno, místnost 2

V této místnosti dojde k montáži datového rozvaděče, taktéž zde má být umístěno druhé plnohodnotné pracovní místo, tedy PC a VOIP telefon.

## 2.3.2 Internetové připojení

Holding využívá službu MPLS IP VPN od společnosti T-Mobile, tedy propojení všech firemních poboček do jedné privátní sítě, přičemž tato technologie zaručuje oddělení od ostatních VPN a od internetu. Na perimetru sítě, tedy na spoji mezi VPN a internetem, se nachází pokročilý hraniční firewall.




**Obrázek č. 4: Obecné schéma služby MPLS IP VPN T-Mobile, dříve GTS**

(Zdroj: 1)

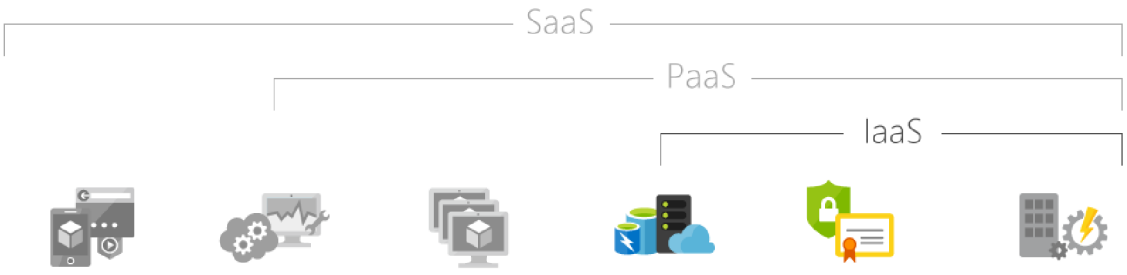
Pokud si zákazník objednal službu MPLS IP VPN a na dané lokalitě není možnost připojení přímo prostřednictvím T-Mobile, řeší to T-Mobile pronájmem linky nebo přímo fyzické vrstvy od dostupného poskytovatele připojení. Bez tohoto není možné koncovému zákazníkovi službu IP VPN nabídnout.

Na zmíněných pobočkách je možnost připojení pouze pomocí technologie ADSL, tedy klasickým pevným připojením přes telefonní kabely. Optická vlákna na dané lokality nejsou zavedena.

V případě, že nedojde k dohodě mezi T-Mobile a dostupným poskytovatelem připojení nebo je stávající přípojka svými parametry nevhodná k účelu profesionálního internetu, existuje varianta bezdrátového připojení pomocí technologie LTE.

## 2.4 Stávající síťová infrastruktura společnosti

Servery, na kterých běží veškeré síťové služby, jsou umístěny uvnitř VPN v datacentru T-Mobile v prostředí Infrastructure as a service (IaaS), tato služba je nabízena pod názvem "virtuální datové centrum". Platforma, na které je datacentrum provozováno, se nazývá VMware vCloud.

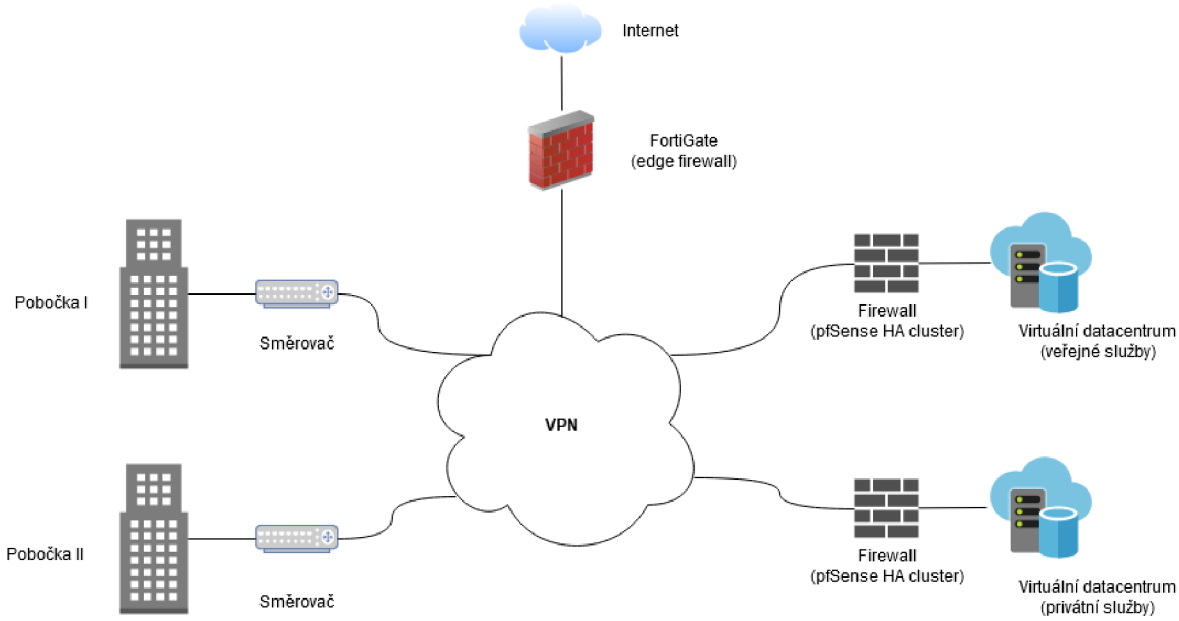



**Obrázek č. 5: Srovnání IaaS s ostatními cloudovými modely**

(Zdroj: 3)

V tomto datacentru jsou umístěny řadiče domény Windows, servery DNS, DHCP, NPS a NTP. Jde v podstatě o nahrazení fyzických serverů těmi virtuálními. Poskytovatel spravuje infrastrukturu, zatímco zákazník instaluje, konfiguruje a spravuje svůj vlastní software – operační systémy a aplikace (3).

Holding využívá dvě oddělená virtuální datacentra, přičemž jedno je vyhrazeno pro veřejné weby a aplikace.




**Obrázek č. 6: Architektura privátního segmentu sítě společnosti**

(Zdroj: vlastní zpracování)

### 2.4.1 Doménové řadiče

Holding využívá adresářovou služby Active Directory. V doméně jsou celkem dva doménové řadiče, oba jsou umístěny v datacentru T-Mobile uvnitř VPN na virtuálních strojích, přičemž tyto virtuální stroje jsou spuštěny na rozdílných hostitelích. Pokud tak dojde k náhodnému restartu hostitele (VMware node), nedojde k restartu obou DC.

Na obou těchto serverech je spuštěna služba DNS, klientské počítače v doméně však na tyto servery nejsou odkazovány.

Servery jsou aktuálně provozovány na operačním systému Windows Server 2012 R2.

### 2.4.2 Servery se síťovými službami

Na těchto serverech jsou provozovány role DNS, DHCP a NPS. Jsou provozovány v redundantní dvojici, stejně jako doménové řadiče a taktéž jsou provozovány na operačním systému Windows Server 2012 R2.

DHCP servery jsou synchronizovány v režimu DHCP failover, jako design tohoto řešení byla zvolena varianta load balance, každý ze serverů tedy obsluhuje přibližně 50% dostupných IP adres v každém DHCP scope. Klientské žádosti o přidělení IP adresy jsou rozděleny mezi servery na základě MAC adresy, kdy každý server provede hash MAC adresy příchozího DHCP požadavku, jehož výsledkem je číslo v intervalu 1-256. První DHCP Server odpovídá pouze na výsledky z intervalu 1-128, druhý na výsledky z intervalu 129-256.

NPS (radius) servery jsou též provozovány redundantně s duplicitní konfigurací, z principu protokolu radius zde není třeba žádná synchronizace. Pokud radius client neobdrží do stanoveného časového limitu odpověď od serveru, automaticky se pokusí komunikovat se serverem druhým.

### 2.4.3 Síť pro hosty

Síť pro hosty umožňuje návštěvníkům poboček používat internet bez nutnosti se připojovat na soukromou neboli interní síť. Zařízení připojená k síti pro hosty nemají přístup ke zdrojům sdíleným v interní síti, jako jsou například sdílené disky.

V praxi je toto řešeno pomocí VLAN, kdy je guest VLAN (síť pro hosty) oddělena od interní sítě pomocí striktního seznamu pravidel, která provoz řídí na základě zdrojové či cílové IP. Tato pravidla jsou definována na aktivních prvcích jednotlivých poboček. Z této sítě taktéž není přístup k serverové infrastruktuře, což znamenalo potřebu vytvořit dedikovaný DHCP server umístěný uvnitř této VLAN. Klienti využívají DNS servery poskytované společností T-Mobile.

V současné době je plánováno maskování provozu, který z této sítě směřuje do internetu, za odlišnou veřejnou IP adresu od interní sítě. Toto řešení výrazně zvýší míru separace sítí, například z důvodu odchozího spamu či jiného škodlivého provozu z některého zařízení připojeného k síti pro hosty.

### 2.4.4 Edge Firewall

Jako firewall na perimetru sítě, tedy firewall oddělující privátní segment sítě od veřejného internetu, je využíván FortiGate 1500D. Komunikace uvnitř sítě (mezi pobočkami a virtuálním datacentrem) přes tento firewall není směrována.

Jelikož pořízení této jednotky by bylo velice nákladné, byl zvolen pronájem tohoto zařízení od společnosti T-Mobile v rámci služby s názvem managed firewall. Firewall je plně ve správě zákazníka, s výjimkou následujícího:

- veškeré aktualizace firmware zařizuje výhradně T-Mobile
- FortiGate je zapojen v high availability (HA) clusteru, tzn. při jeho poruše dojde k přechodu na druhou jednotku s takřka nulovou dobou výpadku

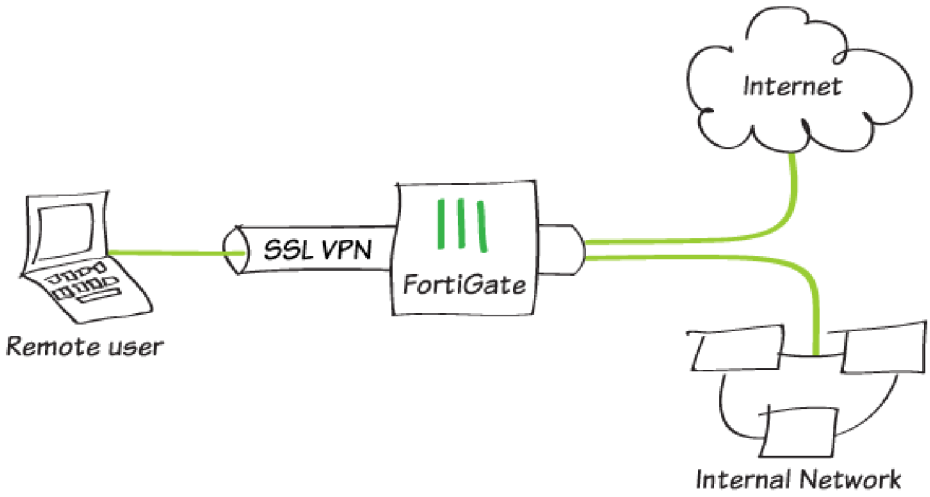
Kromě základní funkcionality stavového firewallu jsou zejména využívány funkce webfilteringu, SSL inspekce (kontroly šifrovaného SSL provozu), SSL VPN pro vzdálený přístup a centrálního managementu WiFi přístupových bodů.

Kvůli příznivé ceně řešení bylo zvoleno tzv. sdílené řešení, kdy je jediná jednotka FortiGate rozdělena virtuálně na více virtuálních domén pro několik zákazníků. Toto řešení má však také několik omezení, z nichž nejpodstatnějším je absence možnosti zasílat vygenerované logové zprávy na jakýkoliv syslog server.

Protože toto omezení bylo vyhodnoceno jako bezpečnostní hrozba, jedná se nyní o přechodu na dedikovaný FortiGate, který je vyhrazen pouze pro jednoho zákazníka a dovoluje odesílání logových zpráv na libovolný kolektorovací server.

### 2.4.5 SSL-VPN

Jako platforma pro bezpečný vzdálený přístup je využíváno SSL-VPN řešení od společnosti Fortinet. Uživatelé tak mají možnost se prostřednictvím zmíněné jednotky FortiGate, která plná úlohu VPN koncentrátoru, připojit do interní sítě takřka odkudkoliv z internetu. Připojení je možné pouze pomocí proprietárního software FortiClient, který musí být na pracovních stanicích nainstalován.




**Obrázek č. 7: Diagram SSL VPN**

(Zdroj: 2)

### 2.4.6 Pobočková infrastruktura

Společnost na svých dvou dosavadních pobočkách o 50 a 150 zaměstnancích využívá aktivních prvků Aruba a WiFi přístupových bodů FortiAP. Použité technologie zahrnují:

- Spanning tree (STP)
- ochranu přes síťovými smyčkami loop protection
- zabezpečení přístupu pomocí 802.1x + dynamic VLAN
- DHCP snooping, ARP protect
- WPA2 Enterprise zabezpečení WiFi

- 802.11q VLAN

Protože mezi pobočkami není provoz nijak řízen, jsou na pobočkových aktivních prvcích nastavena statická přístupová pravidla, tzv. ip access lists (IP ACL). Tyto ACL jsou statickými pravidly, která definují přístupová práva na základě zdrojové a cílové IP adresy v síti, typicky mezi jednotlivými VLAN, na které je síť rozdělena dle jednotlivých oddělení ve firmě.

## 2.5 Požadavky investora

- Funkční a spolehlivá síť z pohledu správce i uživatele
- Možnost připojení PoE IP kamer
- Pokrytí bezdrátovým signálem WiFi
- Dostatečný počet přípojných míst
- Důraz na nízkou cenu

Pronájem většího množství poboček je pro společnost novinkou, je tedy nejisté nakolik bude jejich vlastnictví rentabilní. Také z tohoto důvodu je v rámci síťového řešení poměrně velký tlak na cenu, který by ale neměl kompromitovat celkovou funkčnost řešení. Zároveň by řešení mělo být v souladu se zabezpečením sítě na ostatních pobočkách v holdingu.

Požadavkem jsou pouze 4 přípojná místa pro PC, což je vzhledem k velikosti pobočky dostatečné. Požadováno je zároveň připojení síťové tiskárny a VOIP brány pro ruční telefony.

## 2.6 Shrnutí analýzy současného stavu

Z analýzy vyplývá požadavek investora na vybudování počítačové sítě ve třech malých pobočkách v různých lokalitách, přičemž ani na jedné z lokalit se v tomto ohledu žádné stávající řešení nevyskytuje.

Požadavkem na tuto síť je zejména funkčnost a spolehlivost při připojení různých zařízení, a to jak z pohledu běžného uživatele, tak z pohledu správce této sítě. Není určena maximální výše rozpočtu, ale je kladen poměrně velký důraz na nízkou cenu celého řešení z důvodu nejisté rentability konceptu malých poboček.

Z pohledu stávající architektury interní sítě společnosti je důležité zachovat stávající úroveň zabezpečení. K tomuto je nezbytné připojit i tyto malé pobočky do VPN, využít existujících síťových služeb, jako je například radius, a zabezpečit aktivní prvky na těchto pobočkách z hlediska druhé i třetí síťové vrstvy.

# 3 TEORETICKÁ VÝCHODISKA PRÁCE

Pro porozumění principů komunikační infrastruktury a pochopení technologií, na kterých bude síťové řešení poboček vystavěno, v této kapitole rozeberu klíčové pojmy, které jsou důležité pro pochopení problematiky.

## 3.1 Počítačová síť

Definice počítačové sítě je podle většiny autorů jednoznačná. Lowe definuje počítačovou síť jako dva a více propojených počítačů takovým způsobem, že mezi sebou mohou vyměňovat informace (4, s. 7).

Podobně Horák a Keršláger popisují počítačovou síť jako souhrn nejen hardwarových, ale i softwarových prvků, které zprostředkovávají vzájemnou spolupráci více počítačů (5, s. 10).

Tanenbaum tvrdí, že počítačová síť je systém, který obsluhuje veškeré výpočetní potřeby společnosti a skládá se z množiny propojených, autonomních počítačů. Navíc doplňuje, že počítačová síť je takový systém, ve kterém nefiguruje jasná role master/slave (6, s. 2).

Účelem je zejména snadné sdílení informací, prostředků nebo aplikací a usnadnění práce uživatelům (4, s. 7).

## 3.2 Dělení počítačových sítí

Počítačové sítě je možné rozdělovat podle mnoha kritérií. Těmi nejdůležitějšími jsou ovšem rozsah sítě, topologie a vzájemný vztah mezi stanicemi.

### 3.2.1 Podle rozsahu

Sítě jsou běžně rozdělovány dle geografické velikosti, kterou pokrývají:

**LAN (local area networks)**

Jsou omezeny na jeden podnik, místnost či budovu. Počítače či zařízení v síti jsou tedy umístěny relativně blízko sebe. Svým rozsahem jsou nejmenší a slouží zejména ke sdílení lokálních prostředků (5, s. 9).

**WAN (wide area networks)**

Tyto sítě pokrývají velké geografické vzdálenosti, jako jsou například celá města nebo regiony. Jejich účelem je typicky propojení více LAN, například propojení dvou poboček v rozdílných městech (4, s. 13).

**MAN (metropolitan area networks)**

Tento typ sítě je rozsahem zařazen mezi WAN a LAN. MAN se využívá pro propojení dvou a více LAN v rámci jednoho města, které jsou ale vzdáleny natolik, že nelze k propojení využít kabelovou linku nebo bezdrátový propoj (4, s. 13).

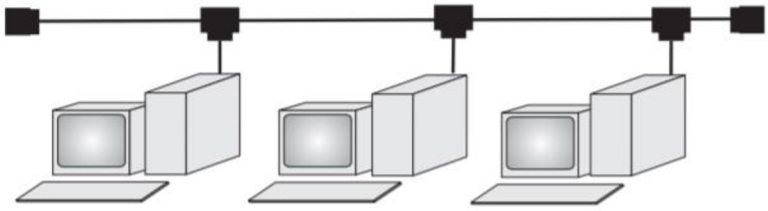
### 3.2.2 Podle topologie

Topologie je způsob, jakým jsou počítače v síti propojeny a z velké části určuje výsledné vlastnosti sítě.

**Sběrnicová topologie**

Ke spojení stanic je využito průběžné vedení, od stanice ke stanici. Přímo k vedení se pak stanice připojují odbočovacím prvkem, např. T-konektorem (5, s. 18).

Výhodou je poměrně malá spotřeba kabeláže. Nevýhodu představuje počet spojů, což přináší množství obtíží a poruch. Topologie je také ze svého principu nespolehlivá, jakékoliv přerušení sběrnice totiž znamená havárii celé sítě (5, s. 18).



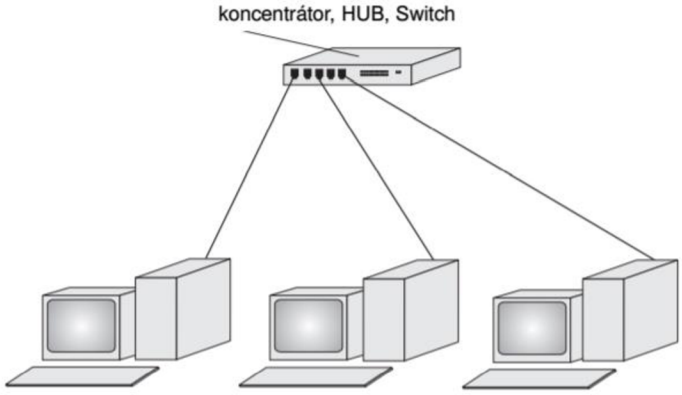
**Obrázek č. 8: Sběrnicová topologie**

(Zdroj: 5, s. 18)

### Hvězdicová topologie

Každá stanice je připojena vlastním kabelem. Všechny kabely jsou pak soustředěny do rozbočovače (dnes nejčastěji switche), který tak tvoří defacto střed sítě. Hvězda je ze všech topologií tou nejčastěji používanou (5, s. 19).

Výhodou je zejména nízká náchylnost k chybám a vysoká spolehlivost. Jednoduchá je zejména také lokalizace poruch, v porovnání se sběrnicovou topologií (5, s. 19).

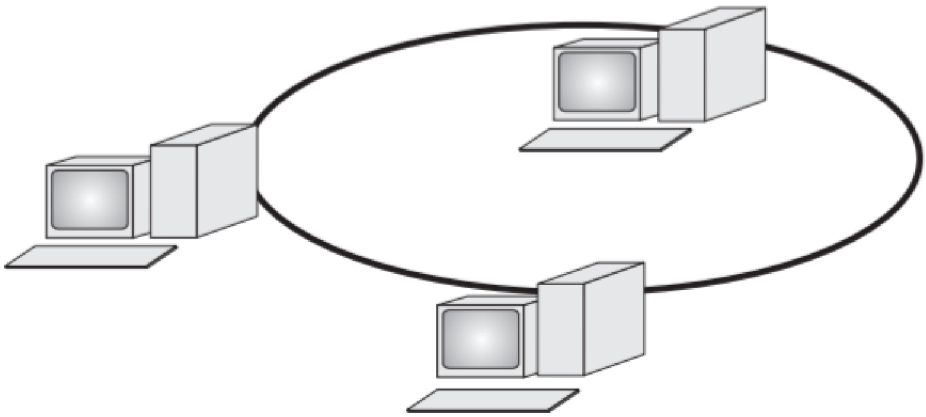



**Obrázek č. 9: Hvězdicová topologie**

(Zdroj: 5, s. 19)

### Kruhová topologie

Vedení mezi stanicemi tvoří souvislý kruh, což dovoluje použít mezi stanicemi metodu postupného předávání zpráv (token). Nevýhoda této sítě je ovšem velmi podobná jako u sběrnice, přerušení vodiče znamená poruchu celé sítě, což se v praxi zpravidla řeší zdvojením kabelu (např. u sítí IBM Token Ring) (5, s. 19).



**Obrázek č. 10: Kruhová topologie**

(Zdroj: 5, s. 19)

### 3.2.3 Podle vzájemného vztahu mezi stanicemi

Jde o rozdělení dle vzájemného vztahu stanic v síti na dva modely architektury počítačové sítě.

### Model Peer-to-Peer

V rámci tohoto modelu je ke všem stanicím na síti přistupováno tak, jako by byly sobě rovny. Znamená to, že mezi sebou mohou například sdílet data formou zpřístupnění určitých složek jinému počítači, nebo je možné povolit tisk na jedné tiskárně více

stanicím. Dnes, i přes dominanci modelu client/server, mají peer-to-peer sítě své místo zejména v prostředí s 10 klientskými stanicemi a méně (7, s. 35).

Výhodou je velká jednoduchost a nízké náklady na takovéto řešení sítě, není nutné kupovat servery a serverové operační systémy. Nevýhodou je ovšem obtížná správa přístupových práv, které se musí řešit na každém z počítačů, a také správa dat (7, s. 35).

**Model Client/Server**

Jde o architekturu, která soustředí data a veškeré služby na několik počítačů (serverů) v síti, od kterých je pak to služby možné nabízet klientům. Toto řešení je dnes nejpoužívanější a velkou měrou nevyhnutelné, což pramení z jeho výhod – bezpečnost dat, snazší a přehlednější správa a konfigurace. Nevýhodou jsou vysoké náklady na nákup serveru a serverového operačního systému (7, s. 32).

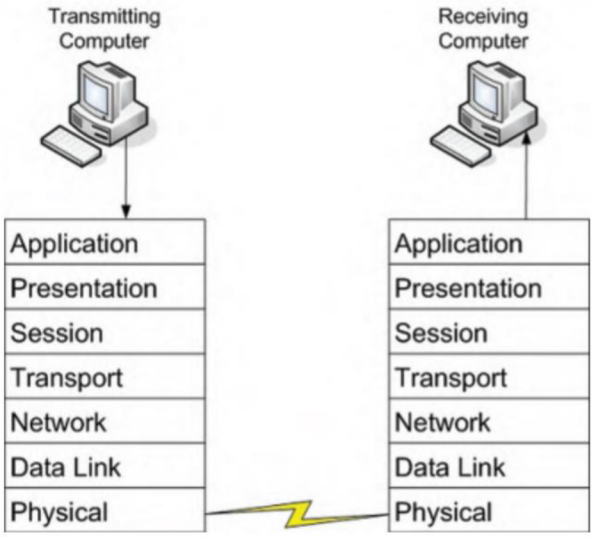
## 3.3 Modely síťové architektury

Počítačové sítě zprvu vyvíjelo více společností jako uzavřené a vzájemně nekompatibilní systémy. Hlavním účelem sítí je ale propojení počítačů, proto bylo nezbytné stanovit pro tyto sítě pravidla tak, aby mezi nimi bylo data možné přenášet. Referenčním síťovým modelem je tzv. model Open Systems Interconnection (OSI), který vytvořila mezinárodní organizace pro normalizaci ISO (5, s. 18).

### 3.3.1 Model OSI

OSI model byl vytvořen jako sedm vrstev nebo úrovní, přičemž na každé z nich pracují protokoly z několika různých sad protokolů. Nejznámější z nich je TCP/IP. Princip spočívá zejména v tom, že každá vrstva využívá služby vrstvy nižší a poskytuje své služby vrstvě vyšší (7, s. 46).

Model OSI specifikuje také horizontální komunikaci mezi sítěmi, přičemž dvě stejné vrstvy modelu mezi různými sítěmi musí umět spolupracovat (5, s. 18).




**Obrázek č. 11: OSI model sítě**

(Zdroj: 7, s. 48)

### Fyzická vrstva

Tato vrstva je fyzickým a elektrickým médiem pro přenos signálu. Zahrnuje kabeláž, konektory, zásuvky, patch panely a další fyzické vybavení nezbytné pro přenos signálu. Kromě mechanických vlastností ale popisuje také ty funkční, jako například bitovou synchronizaci, kódování a modulaci přenosu dat. Zjednodušeně lze říci, že úkolem této vrstvy je zajistit přenos jednotlivých bitů mezi příjemcem a odesílatelem. Měřitelnými jednotkami této vrstvy jsou bity (7, s. 46).

### Linková vrstva

Vrstva zajišťuje, udržuje a rozhoduje o přenosu dat pomocí vrstvy fyzické, k účelům adresace využívá fyzické adresy síťových rozhraní, tzv. MAC adresy (7, s. 46).

Jejím hlavním úkolem je transformace přenosového zařízení fyzické vrstvy na linku, kterou poté prezentuje vrstvě síťové. Tohoto je dosaženo rozdělením dat na tzv. rámce,

což jsou obvykle bloky dat o velikosti stovek nebo tisíců bitů, sekvenčním přenosem těchto rámců a zpracováním potvrzení o přijetí od adresáta. Měřitelnými jednotkami této vrstvy jsou rámce (6, s. 30).

#### Síťová vrstva

Účelem síťové vrstvy je přenos paketů mezi odesílatelem a příjemcem napříč sítěmi nebo celým internetem. Klíčovým prvkem této vrstvy je rozhodování o směrování paketů na základě směrovacích tabulek, které mohou být statické (ve formě statického seznamu pravidel) nebo dynamické, tak aby například reflektovaly zatížení sítě (6, s. 30).

Adresace probíhá na základě logických IP adres, které jednoznačně identifikují síťová rozhraní v počítačové síti. Měřitelnými jednotkami této vrstvy jsou pakety (7, s. 47).

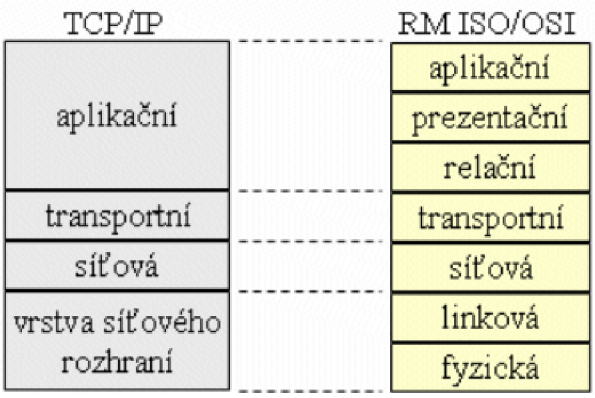
#### Transportní vrstva

Vrstva slouží zejména k rozdělení dat na menší segmenty, odeslání skrze síť a bezchybnému příjmu na straně adresáta. Spravuje tedy přenos těchto segmentů přes tři nižší vrstvy. Využívá také portů, identifikátorů v rámci zařízení, aby mohlo dojít k přenosu právě mezi konkrétními aplikacemi. Měřitelnými jednotkami této vrstvy jsou segmenty (6, s. 32).

### 3.3.2 Model TCP/IP

Síťový model TCP/IP je úzce spjat se sadou protokolů pro komunikaci v počítačové síti, vychází z modelu OSI. Ve srovnání se sedmivrstvým modelem OSI má však pouze 4 vrstvy, přičemž toto uspořádání je dnes nejrozšířenější a prosadilo se například v oblasti internetu (9).

U nejnižší vrstvy (vrstva síťového rozhraní) byly využity existující mechanizmy, které nejsou součástí přímo TCP/IP. Jde například o technologie Wi-Fi, DSL nebo Ethernet (8).




**Obrázek č. 12: Srovnání modelů OSI a TCP/IP**

(Zdroj: 9)

### Vrstva síťového rozhraní

Úkolem této vrstvy je vše, co souvisí s přímým vysíláním a příjmem datových paketů. V rámci TCP/IP je specifikována zejména použitou technologií. Vzhledem k velmi častému využití rodiny technologií Ethernet, která specifikuje architekturu pro fyzickou a linkovou vrstvu, se této vrstvě také říká vrstva ethernetová (10).

Ethernet se stal dominantní technologií pro drátové sítě a dnes je prakticky synonymem pro lokální síť, specifikuje např. využití kabelů s kroucenou dvojlinkou a optických kabelů (11, s. 141).

### Vrstva síťová

Vrstva síťová staví na schopnosti síťového rozhraní přenášet rámce mezi dvěma sousedními uzly, které mezi sebou mají přímé spojení, tím způsobem, že zajišťuje

přenos dat označených jako pakety napříč sítěmi. To zahrnuje hledání nejlepší cesty mezi odesílatelem a adresátem (směrování) (9).

Protokolem této vrstvy je v rámci TCP/IP zejména IP protokol, který zajišťuje adresaci pomocí IP adres, fragmentaci velkých datagramů a nespolehlivé (tzv. best-effort) doručení datagramů napříč sítěmi (11, s. 666).

### Vrstva transportní

Služby transportní vrstvy jsou nejčastěji realizovány pomocí protokolu Transmission Control Protocol (TCP). Úkolem této vrstvy je zajistit přenos mezi odesílatelem a adresátem, což jsou v případě TCP/IP přímo entity vrstvy vyšší (programy). Podle jejich nároků může regulovat tok dat, zajistit spolehlivost přenosu (v případě protokolu TCP) a změnit nespolehlivý charakter přenosu vrstvy síťové na spolehlivý (10).

Druhým protokolem, který na této vrstvě může zajistit přenos, je User Datagram Protocol (UDP). Ten slouží zejména pro takové aplikace, kde by spolehlivost přenosu byla nežádoucí (10).

### Vrstva aplikační

Na úrovni této vrstvy jsou provozovány jednotlivé aplikace nebo jejich součásti, které musí být navzájem kompatibilní. Nalezneme zde protokoly nejvyšší úrovně, jako je např. FTP (protokol pro přenos souborů) nebo SMTP (poštovní protokol) (6, s. 37).

## 3.4 Aktivní síťové prvky

Část úkolů prvních třech vrstev síťových modelů je integrována do elektroniky síťové karty, kterou jsou uzly připojeny k síti, a data jsou přenášeny po kabeláži. Výběr trasy, přístupová oprávnění pro jednotlivé pakety nebo kontrola jejich správnosti jsou však

úkony, které musejí provádět další prvky vložené do sítě. Tyto prvky aktivně ovlivňují dění v síti, proto jsou nazývány aktivními prvky (5, s. 21).

### 3.4.1 Switch

Základní funkcí switche je větvení signálu, nebo také rozbočování sítě. Eliminuje základní nevýhodu rozbočovače (hubu) a defacto převzal jeho roli. Switch dokáže vytvořit virtuální okruh mezi komunikujícími stanicemi, dokáže odeslat data na port, kterému jsou určena (5, s. 21).

Switch je zařízením druhé, linkové vrstvy referenčního modelu OSI. Adresace tedy probíhá na základě MAC adres jednotlivých zařízení, které si switch v průběhu procesu zvaného Address Resolution Protocol (ARP) ukládá do své vnitřní tabulky. Dokáže tak rámce odeslat pouze na ten port, za kterým je umístěno cílové zařízení (12).

### 3.4.2 Router

Router (směrovač) pracuje na úrovni třetí vrstvy OSI modelu. Jeho úkolem je shromáždění informací o připojených sítích a výběr nejvhodnější cesty pro posílaný paket, nezřídka také obsahuje funkcionality filtrace paketů (5, s. 22).

Pomocí těchto informací zajišťuje IP routing, tedy směrování paketů napříč sítěmi na základě IP adresy a pravidel ve směrovací tabulce. Běžné je jeho využití v roli výchozí brány (default gateway). Té využívají uzly v případě, že potřebují odeslat paket do vzdálené sítě a zároveň neznají konkrétní cestu, kterou k ní paket mohou odeslat. Odešlou jej tedy výchozí bráně, která síťovou cestu k této vzdálené síti má zapsanou ve své směrovací tabulce (13).

### 3.4.3 Access Point

Access Point (AP) je zařízení definované v rámci standardu 802.11 pro bezdrátové sítě. Slouží jako most mezi drátovou a bezdrátovou sítí, skládá se z rádia a drátového

síťového rozhraní. Jeho účelem je poskytování bezdrátového přístupového bodu k síti pro několik klientských stanic (11, s. 383).

## 3.5 Komunikační infrastruktura

Komunikační infrastruktura je pojem zastřešující množinu technických prostředků, které zajišťují komunikaci v rámci jednotlivých systémů a subsystémů. Defacto se jedná o kabelážní systémy a další fyzické prostředky pro přenos komunikace (14, s. 8).

Infrastrukturu tvoří kabely, konektory, rozvaděče, kabelové trasy nebo například prostor u bezdrátových sítí. Všechny tyto součásti pak tvoří tzv. kabelážní systém. Krom toho také do infrastruktury patří aktivní prvky jako switche, routery a firewally (14, s. 8).

### 3.5.1 Kabelážní systémy

Kabelážní systémy se obecně dělí do dvou skupin – jednoúčelové a univerzální. Univerzální se vyznačují zejména vyšší aplikační množinou, než je jeden typ přenosu. Technické řešení takovéto kabeláže se nazývá strukturovaná kabeláž nebo multimediální strukturovaná kabeláž, přičemž druhá varianta podporuje svými přenosovými parametry rozsáhlý okruh analogových i digitálních aplikací. Toto řešení je z velké míry univerzální a dokáže propojit cokoliv s čímkoliv. V současné době je toto často jediná kabeláž, která se v objektech vyskytuje mimo silového rozvodu (14, s. 9).

### 3.5.2 Základní pojmy

Základním prvkem kabelu je kroucený pár. Ten tvoří dva zkroucené izolované vodiče, z nichž každý může být samostatně stíněn. Stíněn může být i kabel jako celek. Mezi

páry může být vložen prvek pro prostorové oddělení párů. Variabilní je též plášť kabelu, může být např. armovaný nebo vícenásobný (14, s. 16).

**Tabulka č. 2: třídy použití sítě a kategorie kabeláže** (Zdroj: 14, s. 15)

| třída | kategorie | frekvenční rozsah | obvyklé použití |
|---|---|---|---|
| A | 1 | do 100kHz | analogový telefon |
| B | 2 | do 1MHz | ISDN |
| C | 3 | do 16MHz | Ethernet 10 Mbit/s |
| - | 4 | do 20MHz | Token ring 16 Mbit/s |
| D | 5 | do 100MHz | FE, GE |
| E | 6 | do 250MHz | ATM1200 |
| EA | 6A | do 500MHz | 10GE |
| F | 7 | do 600MHz | 10GE |
| FA | 7A | do 1000MHz | 10GE |

**Kategorie** – klasifikace linky a kanálu, rozlišovacím kritériem je frekvenční rozsah v MHz (14, s. 15)

**Třída** – klasifikace aplikací sítí, hodnotí parametry nainstalovaného celku včetně způsobu a preciznosti instalace (14, s. 15)

**Datový rozvaděč** – skříň (rack), ve které jsou umístěny přepojovací kabely, prvky organizace kabeláže, aktivní prvky a další zařízení (14, s. 19)

**Horizontální vedení** – propojuje datový rozvaděč se zásuvkou na pracovišti (14, s. 19)

**Páteřní vedení** – propojuje datové rozvaděče (14, s. 19)

**Pracovní oblast** – připojovací kabely na pracovištích a v datovém rozvaděči (14, s. 19)

### 3.5.3 Sekce kabelážního systému

Sekcemi rozumíme logické členění infrastruktury komunikačního systému. Základním rozdělením jde o horizontální, pracovní a páteřní sekci. Přenosovým prostředím v tomto případě může být metalická kabeláž, optické vlákno nebo prostor v případě bezdrátových sítí, které využívají rádiový signál (14, s. 19).

### Horizontální sekce s metalickými párovými kabely

Tvoří ji linka o maximální délce 90m, přičemž vždy musí být použit vodič typu drát. Jedna strana této linky je zakončena v zásuvce v jacku RJ45, druhá strana je zakončena v zásuvce v datovém rozvaděči, což je obvykle taktéž jack RJ45 přepojovacího panelu. V případě použití stínených kabelů je třeba stínění linky uzemnit pouze v datovém rozvaděči. Od rozvaděče je veden k datové zásuvce takový počet kabelů, jaký je počet portů datové zásuvky (14, s. 21).

Na linku navazuje pracovní vedení, které tvoří připojovací kabel v datovém rozvaděči a připojovací kabel na pracovišti, kterým do datové zásuvky připojujeme zařízení. Horizontální linka včetně pracovního vedení na obou koncích tvoří horizontální kanál, maximální povolená délka tohoto kanálu je 100m. Fyzická topologie je vždy hvězda (14, s. 21).

### Páteřní sekce

Normou ČSN EN 50173 je definována topologie páteřní sekce jako hierarchická hvězda, s možností doplnění dalších redundantních vedení a uzlů. Páteřní sekce typicky propojuje jednotlivé komunikační uzly, které jsou tvořeny datovými rozvaděči s potřebným vybavením (14, s. 24).

Základní páteřní rozvod budovy či areálu je vždy zásadně realizován na optických kabelech. Důvodem je především galvanické oddělení jednotlivých uzlů sítě a ochrana před přepětím, ale i možnost rychlejších systému přenosu než na UTP kabelech (14, s. 25).

## 3.5.4 Prvky konektivity IKS

Prvkem konektivity rozumíme vybavení, které ukončuje linku horizontální trasy. Řadíme mezi ně zejména přepojovací panely a datové zásuvky (telecommunication

outlets). Dle zvoleného řešení kabeláže jsou buď optické, nebo metalické. Provedením mohou být integrované (pevně osazené) nebo modulární, které dovolují vyměnit dílčí prvky panelů a zásuvek (14, s. 67).

### 3.5.5 Datové rozvaděče IKS

Datové rozvaděče jsou umístěny v jednotlivých uzlech IKS, slouží k ochraně umístěných zařízení před poškozením, ale i ochraně prostředí vně rozvaděče. Slouží k uložení prvků konektivity IKS, aktivních prvků, prvků organizace kabeláže, záložních zdrojů elektrické energie nebo třeba serverů (14, s. 197).

Vnitřní montážní výška (prostor pro prvky IKS) je udávána v jednotkách zvaných UNIT (1U=44,45mm). Montážní šířka je udávána v palcích (14, s. 197).

### 3.5.6 Trasy kabeláže IKS

Z pohledů jednotlivých sekcí kabeláže IKS je můžeme rozdělit na páteřní trasy areálu, páteřní trasy budovy a horizontální trasy. Protože se každý typ trasy nachází v různém prostředí, vyžaduje odlišné instalační i technické postupy (14, s. 270).

Pro trasy horizontální sekce se nejčastěji využívají drátěné žlaby či rošty uložení ve zdvojené podlaze či podhledech, přičemž je třeba dodržovat zásady ohybu kabelů. Pro trasy vedené po povrchu omítky se většinou využívají plastové lišty, u nich je ovšem třeba vybrat takový systém, který umožní dodržet zmíněné zásady ohybu kabelů (14, s. 279).

Řešení páteřních tras pak úzce souvisí s konstrukcí budovy. Většina řešení je shodná s řešením horizontální trasy, je ovšem vhodné uložit páteřní vedení do samostatných žlabů a chrániček tak, aby nebyly uloženy v jednom svazku s vedením horizontální sekce (14, s. 269).

### 3.5.7 Značení prvků IKS

Požadavky značení IKS vycházejí z evropských norem EN 50174. IKS je rozsáhlý systém a zejména z provozních důvodů je důležité mít jej přehledně a řádně označen. Značení se zaznamenává již v projektu, instalační technik pouze zaznamenává případné změny. Při vybírání způsobu značení je dobré myslet na skutečnost, že IKS je v provozu často mnoho let, z toho důvodu je dobré aby značení bylo odolné otěru i vnějším vlivům a dobře čitelné (14, s. 285).

Norma neurčuje způsob značení, určuje pouze co všechno musí být označeno (14, s. 285):

- Všechny kabely minimálně na obou koncích,
- kabelové svazky na koncích a v místě křížení tras,
- patch panely a jejich porty,
- zásuvky a jejich porty,
- datové rozvaděče
- technologické místnosti,
- aktivní prvky (14, s. 285).

Identifikační kód, využívaný ke značení, může mít dvě podoby: reverzní a přímý (14, s. 285).

**Přímý identifikační kód**

Vychází z filozofie přiřazení portu datové zásuvky k určitému portu datového rozvaděče. Příkladem je kód O.PP.MMM.ZZ.X, kde O je číslo objeku, PP je číslo podlaží, MMM je číslo místnosti, ZZ je číslo zásuvky v místnosti a X je číslo portu v zásuvce. Tento typ kódu má zpravidla 8 až 12 znaků a lze jej tedy použít pouze u malých instalací, protože díky své délce je nevhodný ke značení většího množství portů (14, s. 286).

**Reverzní identifikační kód**

Filozofie tvorby tohoto kódu je zcela opačná, protože přiřazuje portu příslušné zásuvky port určitého patch panelu v určitém datovém rozvaděči. Příkladem může být kód RPXX, kde R je označení datového rozvaděče, P je označení patch panelu a XX je číslo portu patch panelu. Díky své délce kolem 5 znaků splňuje podmínku čitelnosti a je možné jej používat i v instalacích, kde se nachází větší množství zásuvek (14, s. 287).

# 4 VLASTNÍ NÁVRH

Z provedené analýzy současného stavu je zřejmé, že společnost disponuje potřebnou infrastrukturou, která umožňuje připojení dalších poboček do firemní VPN. V tomto návrhu se tak budu zabývat několika oblastmi, které dohromady vytvoří nejlepší možné řešení komunikační infrastruktury v souladu s firemními standardy, přičemž budu respektovat přání a požadavky investora. Na jednotlivých plánovaných pobočkách určím trasy vedení kabeláže, rozmístění síťových zásuvek, datových rozvaděčů a dalších prvků fyzické vrstvy. Budu se také věnovat aktivním prvkům a jejich konkrétnímu nastavení včetně návrhu ACL i začlenění nových poboček do stávající síťové infrastruktury. Na závěr provedu ekonomické zhodnocení tohoto řešení.

## 4.1 Výběr aktivních prvků

Vzhledem k cílovému počtu poboček (výhledově až dvacet) a vzhledem k poměrně malému týmu pracovníků, který se stará o technický provoz společnosti, bude nejlepší využít pronájmu některých zařízení od společnosti T-Mobile. Tuto službu je možné zřídit spolu s managementem těchto zařízení, nevýhodou je ztráta kontroly nad výběrem konkrétních modelů. Jelikož jedinými dvěma aktivními prvky na každé pobočce bude switch a přístupový bod wifi, budu se dále věnovat právě jim.

### 4.1.1 Switch

V případě pronájmu je nezbytné stanovit požadované funkcionality, které budou na zařízení vyžadovány. Jde zejména o:

- IP routing
- VLAN support
- DHCP relay
- RADIUS authentication (802.1x), MAC-based authentication

- Loop protection, ARP protection, DHCP snooping, user number limit per interface
- VLAN assignment based on NPS policies and MAC addresses
- Source/destination IP based packet filtering (IP ACL)
- Bridge ACL or port isolation
- Dynamic ACL assigment based on NPC policies
- PoE+

Z předchozích zkušeností s tímto typem služby od stejného dodavatele odhaduji, že bude zvolen switch řady Huawei S5300 bez možnosti vyjednání alternativy. Dostačující počet portů na switchi je 8, vzhledem k počtu přípojných míst.

### 4.1.2 WiFi Access Point

Vzhledem k požadavku investora na pokrytí poboček bezdrátovým WiFi signálem se musí na každé z poboček nacházet přístupový bod.

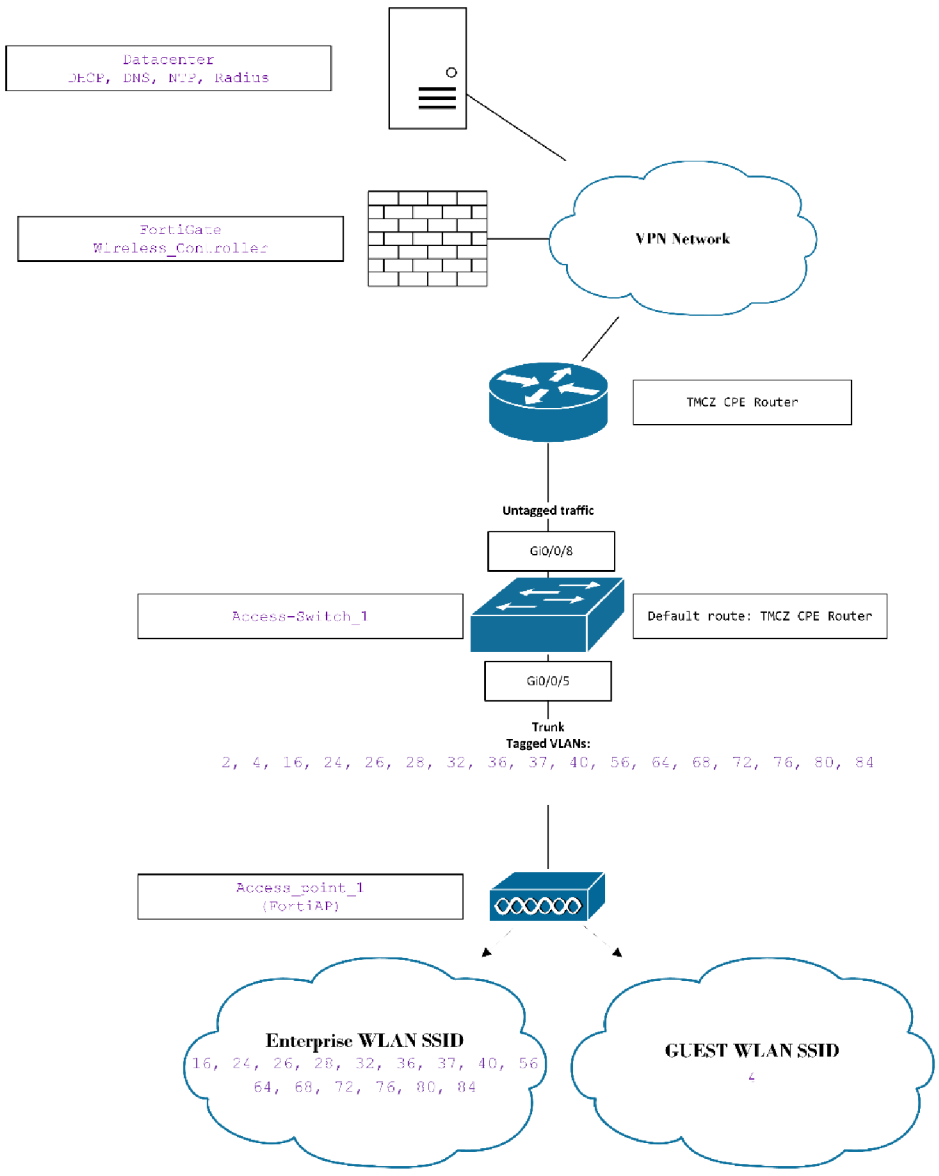
Aktuálně je na všech ostatních pobočkách využívané řešení od společnosti Fortinet, jako kontrolér přístupových bodů slouží jednotka FortiGate, která je zároveň firewallem na perimetru sítě. Jelikož nově zřizované pobočky budou též součástí VPN a budou tedy schopny komunikovat s kontrolérem, je možné toto řešení využít i zde.

V tomto případě jsou požadované klíčové funkcionality následující:

- Dual radio 2,4 + 5 GHz 802.11a/b/g/n/ac
- WPA2-PSK + WPA2-Enterprise (802.1x support)
- 802.1x dynamic VLAN support
- Multiple SSID support
- 1000baseT PoE port
- Local-bridge standalone SSID mode
- Per-client rate limiting

Jelikož se access point (AP) bude nacházet vždy zhruba uprostřed kanceláří, je zbytečné aby měl externí antény, protože nebude třeba nijak upravovat vyzařovací charakteristiku.

Důležitou funkcionalitou je zde local-bridge režim, ve kterém veškerý provoz klientů není směrován přes kontrolér. Toto dovoluje AP fungovat ve volitelně omezené míře i při výpadku kontroléru (FortiGate), což dovolí klientům v této situaci alespoň komunikovat uvnitř VPN.




**Obrázek č. 13: Obecné schéma pobočkové sítě**

(Zdroj: vlastní zpracování)

Zvolil jsem model Fortinet FortiAP 221E s předpokládanou montáží na strop a dobrým poměrem cena/výkon. Jelikož opětovná využitelnost FortiAP je velká, není nezbytné tento hardware pronajímat.

## 4.2 Adresní plán poboček

Vnitřní síť využívá privátního adresního rozsahu 10.0.0.0/8, přičemž síťové adresy třídy B jsou rezervovány pro jednotlivé pobočky, zatímco adresy třídy C jsou vyhrazeny pro jednotlivé VLAN, na které je síť segregována.

Toto rozdělení dovoluje vytvoření teoreticky až 255 VLAN s prefixem /24 na každé pobočce, což by v každé síti dovolilo přiřazení až 254 adres klientským stanicím.

Pro dosavadní (velké) firemní pobočky byl rezervován rozsah 10.240.0.0/12. Vzhledem k zcela jiné povaze nově zřizovaných poboček, nejisté prognóze budoucího vývoje a pravděpodobně menšího počtu potřebných VLAN je nejlepší volbou alokovat tomuto projektu samostatný adresní rozsah 10.208.0.0/12. Toto je znázorněno tabulkou v příloze č.1.

## 4.3 Adresní plán jednotlivých VLAN

Podniková síť je segregována na 27 virtuálních sítí (VLAN), přičemž zařízení nebo uživatelé jsou rozřazeni do těchto sítí dle oprávnění, která pro svoji práci potřebují, protože síťové prostupy jsou povolovány nebo blokovány právě na základě klientských IP adres.

Na těchto menších pobočkách se, narozdíl od kmenových poboček společnosti, budou vyskytovat z 99% klienti zařazení do jediné z těchto sítí, bylo by tedy zbytečné plánovat na těchto pobočkách se všemi 27 virtuálními sítěmi. Stejně tak by bylo zbytečné alokovat na každou z těchto malých lokalit celou síťovou adresu třídy B.

Rozdělil jsem tak z přiděleného rozsahu 10.208.0.0/12 menší skupiny adres s prefixem /19. Toto dovoluje vytvoření až 32 VLAN, každou s prefixem /24, pro každou pobočku, což je více než dostatečné. Zároveň dojde i k efektivnějšímu využití adresního prostoru. Přesné rozdělení je znázorněno tabulkou v příloze č.1.

Konkrétní sítě, které budou muset být nastaveny na aktivních prvcích jednotlivých poboček, popisuji v tabulce níže.

**Tabulka č. 3: popis jednotlivých VLAN** (Zdroj: vlastní zpracování)

| Označení VLAN | VLAN ID | Popis |
|---|---|---|
| int-mgmt | 2 | Management síť, určená ke správě zařízení (aktivních prvků) |
| int-guest | 4 | Síť pro návštěvníky a neautorizovaná zařízení |
| int-prnt | 8 | Síť pro tiskárny |
| int-voip | 9 | Síť pro VOIP brány a další zařízení určená k telefonii |
| int-security | 10 | Síť pro IP kamery |
| zs-user | 16 | |
| zs-dev | 24 | |
| zs-devops | 26 | |
| zs-ops | 28 | |
| tgi-user | 32 | |
| tgi-dir | 36 | |
| tgi-acc | 37 | |
| tgi-ext | 40 | Uživatelské VLAN |
| ke-user | 56 | |
| ob-user | 64 | |
| ob-dir | 68 | |
| or-user | 72 | |
| or-dir | 76 | |
| zo-user | 80 | |
| zo-dir | 84 | |

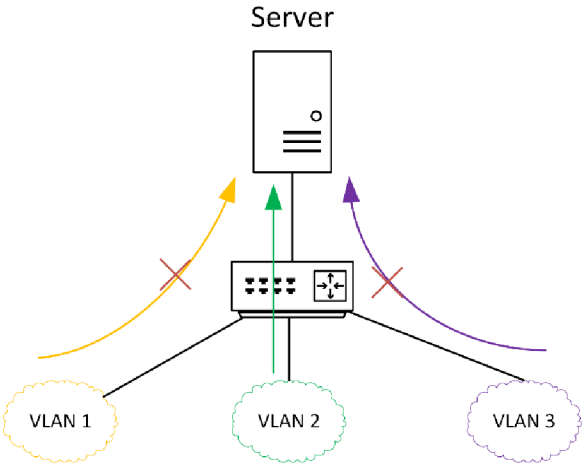
## 4.4 ACL – Access Control Lists

Seznam pravidel, na základě kterého switch filtruje síťový provoz, je úzce spjat s existencí VLAN. Bohužel není možné ACL přiřazovat jednotlivým klientům dynamicky z radius serveru, ačkoliv switch je na toto připraven – dynamické ACL se konfigurují pro jednotlivé porty při procesu autentizace, což by znamenalo, že

uživatelům připojeným přes AP (které je samostatným radius clientem a řeší si autentizaci klientů po své ose) by tyto ACL nebyly nastaveny.

Vybrané AP žádnou podobnou funkcionalitou neoplývá, k tomu by bylo třeba vybrat zcela nové řešení a koupit nový kontrolér. Cena by ale v tomto případě nebyla vyvážena přínosy.

Je tedy třeba konfigurovat ACL na úrovni switche přímo pro jednotlivé VLAN. Toto řešení zajistí filtraci veškerého provozu konkrétní VLAN dle konkrétních pravidel, provoz uživatelů připojených přes WiFi AP je v tomto tedy obsažen. Nevýhodou je nutnost udržovat seznamy pravidel na potenciálně až dvaceti zařízeních (dle počtu poboček), což se ale dá vyřešit distribucí pravidel z TFTP serveru.

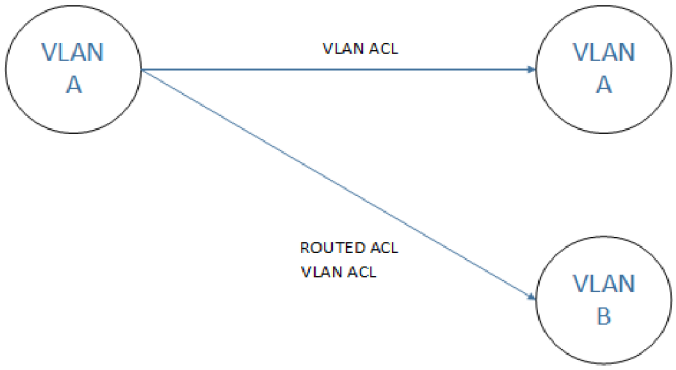



**Obrázek č. 14: Základní koncept IP ACL**

(Zdroj: vlastní zpracování)

V návrhu je využito pouze jedné ze dvou koncepcí ACL – extended (filtrace na základě zdrojové a cílové IP adresy). Switche Huawei mají obecně možnost nastavení ACL ve směrech inbound (vstup) nebo outbound (výstup). Toto je vždy posuzováno z pohledu switche. Při nastavení "inbound" tedy srovnává provoz, který do dané VLAN vstupuje (ať už z uživatelského zařízení, nebo z jiné VLAN), se seznamem pravidel na úrovni L3, při směrování. Tuto skutečnost je třeba vždy zohlednit při návrhu, v mém případě jsou všechny ACL nastaveny právě na směr "inbound" a v ACL filtruji provoz dle cílové IP adresy.

Některé switche umí nastavit ACL takovým způsobem, aby byla filtrována přímá komunikace na úrovni L2, tedy komunikace mezi zařízeními ve stejné VLAN. V případě, že dodavatelem vybrané zařízení tuto funkcionalitu nepodporuje, musí dle požadavků podporovat alespoň funkcionalitu "port isolation", tedy izolaci portů, což docílí (v tomto konkrétním případě) stejného výsledku - jednotlivá zařízení v lokální síti v rámci jedné VLAN spolu nebudou moci komunikovat.




**Obrázek č. 15: Srovnání schopností filtrace provozu VLAN ACL a Routed ACL**

(Zdroj: vlastní zpracování)

Tabulka níže obsahuje přiřazení jednotlivých ACL na konkrétní VLAN. Konkrétní návrh ACL včetně komentářů jednotlivých pravidel je obsahem přílohy č. 2. Port isolation je třeba nastavit tak, aby byla znemožněna komunikace mezi zařízeními uvnitř jednotlivých VLAN, ale aby komunikace napříč VLAN byla stále umožněna, jelikož ta je v mnoha případech žádoucí a je řízena na úrovni ACL.

**Tabulka č. 4: Asociace ACL a VLAN** (Zdroj: vlastní zpracování)

**ACL to VLAN association**

| VLAN Name | ID | ACL | Port isolation |
|---|---|---|---|
| int-mgmt | 2 | int-mgmt-acl | no |
| int-guest | 4 | int-guest-acl | yes |
| int-prnt | 8 | int-prnt-acl | yes |
| int-voip | 9 | int-voip-acl | yes |
| int-security | 10 | int-security-acl | yes |
| zs-user | 16 | user-acl | yes |

| | | | |
|---|---|---|---|
| zs-dev | 24 | zs-dev-acl | yes |
| zs-devops | 26 | zs-dev-acl | yes |
| zs-ops | 28 | zs-ops-acl | yes |
| tgi-user | 32 | user-acl | yes |
| tgi-dir | 36 | tgi-dir-acl | yes |
| tgi-acc | 37 | tgi-acc-acl | yes |
| tgi-ext | 40 | user-acl | yes |
| ke-user | 56 | user-acl | yes |
| ob-user | 64 | user-acl | yes |
| ob-dir | 68 | user-acl | yes |
| or-user | 72 | user-acl | yes |
| or-dir | 76 | user-acl | yes |
| zo-user | 80 | user-acl | yes |
| zo-dir | 84 | user-acl | yes |

K návrhu ACL jsem přistoupil konzervativním způsobem, kdy jsem nejdříve zakázal přístup do vnitřní sítě, povolil přístup do internetu a poté jsem dle potřeb jednotlivým VLAN přiděloval oprávnění k přístupu do vnitřní sítě nebo datacentra. VLAN pro tiskárny, IP kamery nebo VOIP zařízení nemají povolen ani přístup k internetu, protože pro jejich funkčnost není nezbytný.

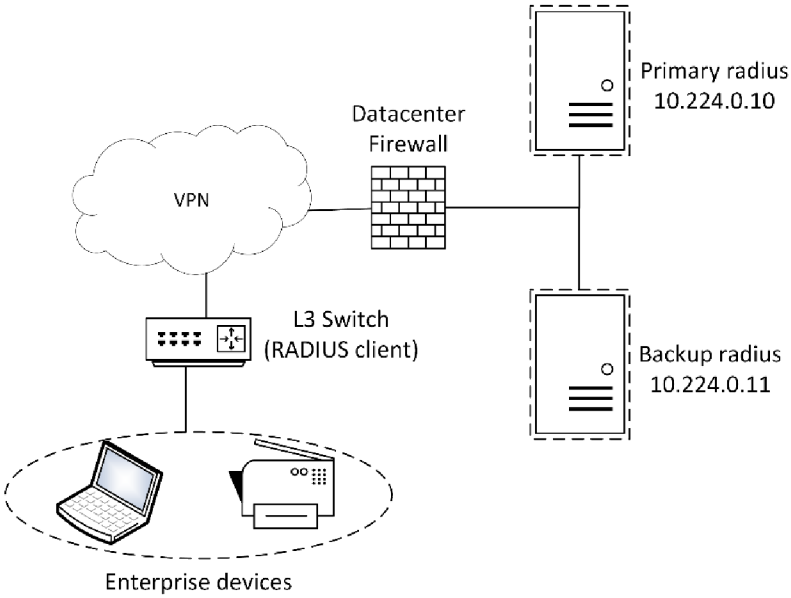
Zvláštním případem je VLAN int-mgmt, ve které se nacházejí management rozhraní síťových zařízení a zároveň se do ní připojují administrátoři, kteří je potřebují spravovat.

## 4.5 Autentizace klientů v síti

Protože všechna zařízení připojená k síti nebudou pod fyzickou kontrolou, je nezbytné nastavit řízení přístupu k počítačové síti. Zabrání se tak přístupu neautorizovaných osob do interní sítě bez toho, aby byla udržována fyzická bezpečnost všech přípojek, což je v tomto případě nemožné. Při návrhu využiji standardu 802.1x, který se vztahuje nejen na pevné (drátové), ale i na bezdrátové sítě WiFi.

Společnost disponuje dvěma Microsoft NPS servery, což je implementace RADIUS serveru od Microsoftu. Databáze uživatelů a přístupových údajů je v tomto případě

čerpána z Active Directory, takže přihlašovací údaje pro přístup k interní síti jsou stejné jako údaje pro přihlášení k doménovému PC.




**Obrázek č. 16: Umístění RADIUS serverů v síti**

(Zdroj: vlastní zpracování)

Autentizace pomocí protokolu 802.1x bude zapnuta na všech portech pro koncová zařízení, přičemž neautorizovaná VLAN pro klienty, kteří neposkytnou žádné přihlašovací údaje nebo poskytnou chybné údaje, je síť s označením int-guest (VLAN ID 4).

Protože v síti se nachází NPS servery dva, je možné tohoto využít pro případ selhání jednoho z nich. Radius klient (switch) využívá primární server do chvíle, kdy od něj přestanou přicházet odpovědi. V tom případě se začne dotazovat sekundárního. Toto chování lze ovlivnit následujícími parametry:

**Dead-time**

Specifikuje čas v minutách, po který se switch nebude snažit komunikovat se serverem od kterého nepřichází odpovědi. Typicky je možné nastavit takřka libovolnou dobu, v mém případě bude nastaveno 60 minut.

**Radius-server timeout**

Specifikuje maximální dobu, po kterou switch čeká na odpověď od serveru, než pokud zaznamená jako selhání. Defaultní doba je 5 vteřin.

**Radius-server retransmit**

Pokud nepřijde od radius serveru odpověď, tento parametr určuje počet opakování před uzavřením spojení. Defaultní počet je 3.

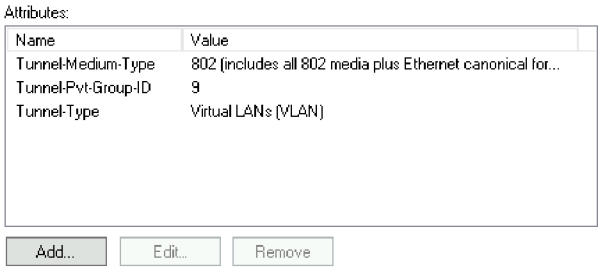
### 4.5.1 Dynamické přiřazení VLAN koncovým stanicím

V případě úspěšné autentizace nabízí radius klienti zpravidla dva režimy. Prvním je přiřazení klientů do jedné konkrétní VLAN, která je určena pro autentizované klienty, a druhým je režim dynamických VLAN, kdy je v odpovědi od NPS serveru zároveň klientovi (switch) předáno VLAN ID sítě, do které má síťové zařízení umístit.

Kvůli velkému množství VLAN, které zároveň určují pro uživatele nebo zařízení jejich oprávnění v rámci síťových přístupů, je v mém návrhu nezbytné využít režimu dynamických VLAN.

V rámci switche zpravidla pro tento režim není třeba provádět žádnou konfiguraci, režim dynamických VLAN je defaultním režimem. Ze strany radius serveru je VLAN ID předáno v rámci atributu Tunnel-Pvt-Group-ID, jak ukazuje obrázek níže. Členství

ve VLAN je ekvivalentní členství v konkrétních radius skupinách v rámci AD – přiřazením uživatele do radius skupiny jej zároveň přiřadíme do VLAN.



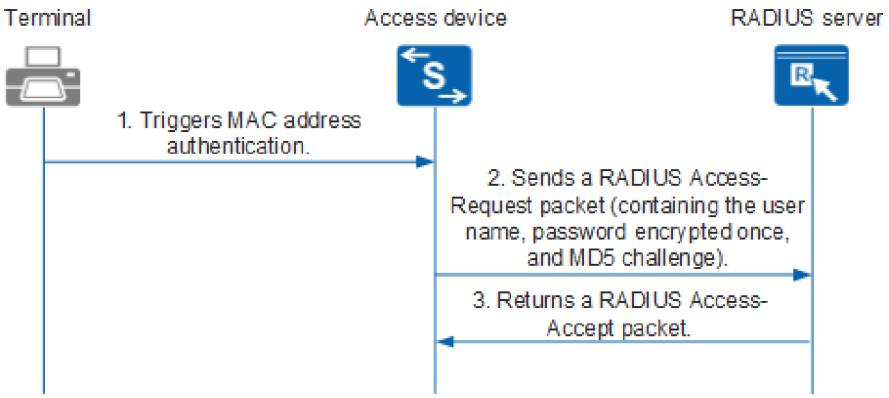

**Obrázek č. 17: Ukázka nastavení RADIUS atributů pro VLAN 9, int-voip**

(Zdroj: vlastní zpracování)

### 4.5.2 Autentizace tiskáren a VOIP telefonů pomocí MAC adresy

Ne všechna zařízení jsou kompatibilní se standardem 802.1x. Zejména tiskárny, VOIP telefony a další podobná zařízení tento typ přihlašování neovládají, a tak jedinou možností, jak je přiřadit do správné VLAN dynamicky, je autentizace pomocí MAC adresy.

Tento způsob přihlašování přináší bezpečností riziko, jelikož je MAC adresu velmi snadné změnit, nicméně v případě mého návrhu bude použit pouze pro VLAN int-prnt a int-voip, tedy právě pro tiskárny a VOIP telefony. Tyto VLAN jsou velmi restriktivní svými síťovými přístupy, a tak riziko z toho plynoucí je přijatelné.



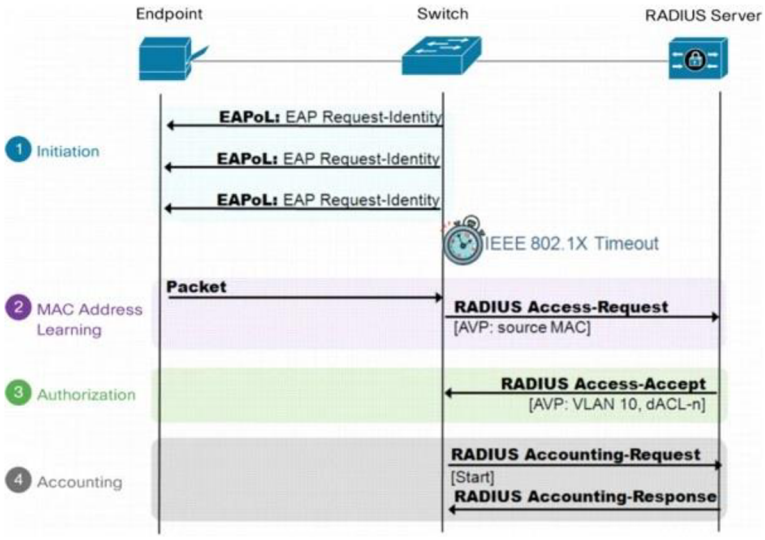

**Obrázek č. 18: Diagram MAC autentizace**

(Zdroj: 15)

V případě switchů Huawei odešle switch na radius server MAC adresu nově připojeného zařízení jako jméno a heslo standardně pomocí protokolu 802.1x. Pokud v databázi uživatelů toto zařízení existuje, je přístup k síti povolen a zařízení je přiřazené do správné VLAN, podle ID obsaženého v odpovědi od serveru.

Switch tedy celou autentizaci provede za koncovou stanici. Protože ta neumí poskytnout své jméno a heslo, použije místo toho jeho MAC adresu jako jednoznačný identifikátor.

Tento typ autentizace bude nastaven na všech portech a bude využíván pouze v případě, že standardní autentizace pomocí 802.1x selže (tzv. mac authentication bypass). Defaultní timeout (parametr mac-bypass-delay) pro selhání 802.1x je 30 vteřin, což je velmi dlouhá doba, po které už většina zařízení neodesílá DHCP discover pakety a nikdy jim tedy není přiřazena IP adresa. Z tohoto důvodu bude timeout snížen na 10 vteřin.




**Obrázek č. 19: Diagram MAC authentication bypass**

(Zdroj: 16)

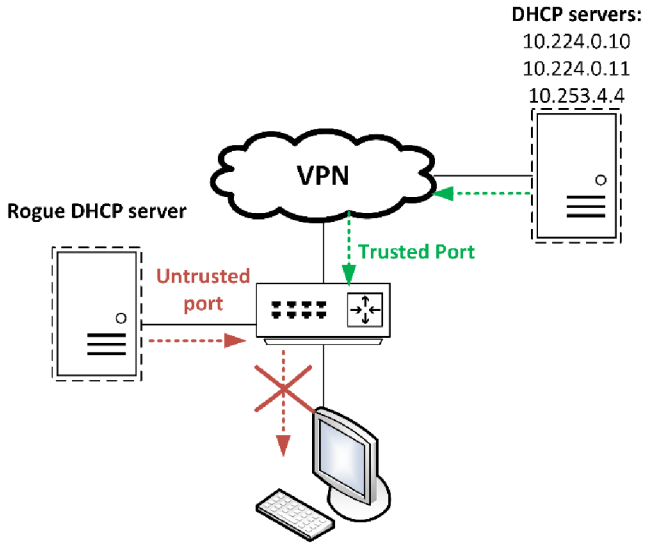
## 4.6 Zabezpečení linkové vrstvy

Zabezpečení na nižších vrstvách zahrnuje zejména opatření pro protokoly DHCP a ARP, ale také do něj můžeme zahrnout ochranu proti síťovým smyčkám a limit počtu MAC adres na všech portech pro koncová zařízení.

### 4.6.1 DHCP Snooping

Jako ochranu před útokem pomocí připojení dalšího DHCP serveru do sítě je nezbytné tuto funkcionalitu nastavit na přístupovém switchi. Důvěryhodný pro příchod odpovědí od DHCP serveru bude pouze port, kterým je switch připojen do VPN - všechny ostatní porty budou označeny jako nedůvěryhodné. V konfiguraci se též specifikují povolené IP adresy serverů, které mohou na DHCP požadavky od klientů odpovědět.

Switch taktéž buduje DHCP Snooping tabulku, kde zaznamenává MAC adresu zařízení a jemu přiřazenou IP adresu. Pokud se zařízení pokouší komunikovat z jiné IP adresy, než jakou má přiřazenou v binding tabulce, je tato komunikace blokována.



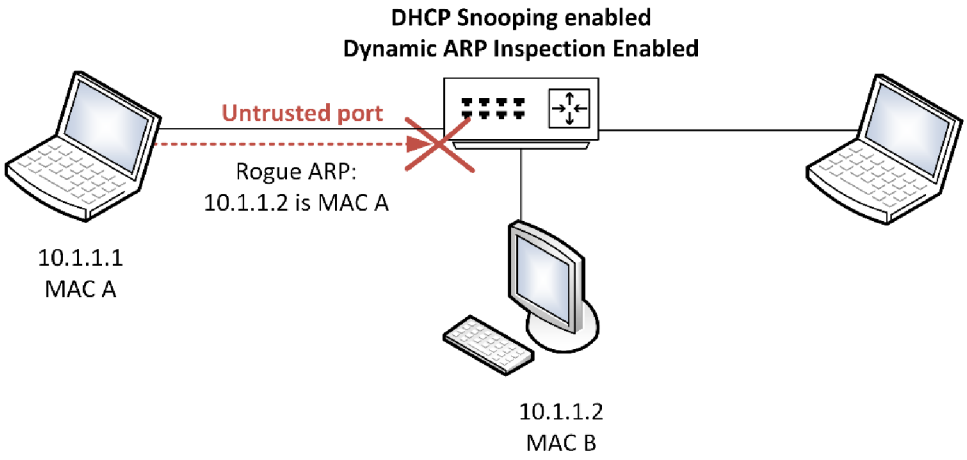

**Obrázek č. 20: Princip funkce DHCP Snoopingu**

(Zdroj: 20)

### 4.6.2 Dynamic ARP Inspection

Jakožto opatření proti ARP útokům je nezbytné na switchi nastavit tuto funkcionalitu na všech portech, kromě portu kterým je switch připojen do VPN. Switch kontroluje veškeré ARP požadavky a odpovědi tím způsobem, že je porovnává s tabulkou MAC

adres a přiřazených IP adres, kterou udržuje DHCP snooping. Pokud některý z ARP paketů není validní, nedojde k aktualizaci lokální ARP cache a přeposlání paketu.




**Obrázek č. 21: Princip funkce dynamic ARP inspection**

(Zdroj: 21)

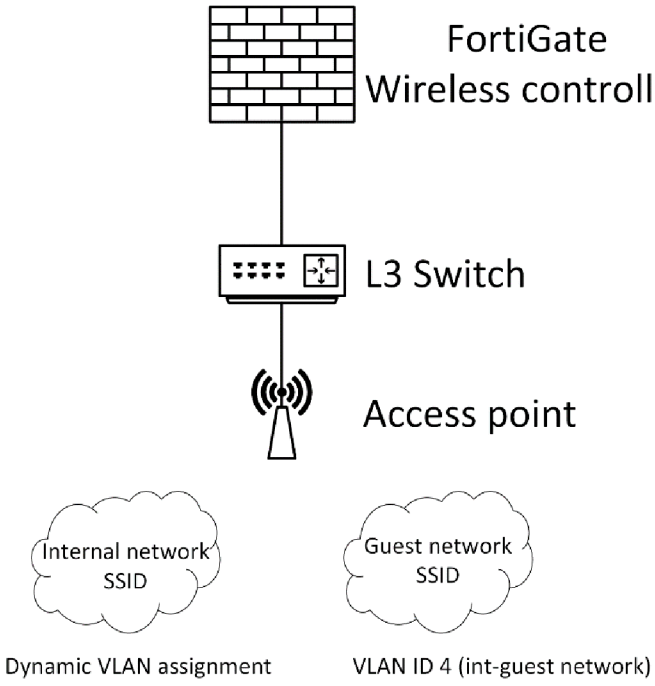
### 4.6.3 Loop protection

V případě switchů Huawei tato funkcionalita odesílá v pravidelném intervalu na všech portech speciální "loop detection" pakety. Pokud tyto pakety poté detekuje jako příchozí na jiném portu, automaticky předpokládá že je na switchi síťová smyčka a vypíná příslušný port. Tato funkcionalita bude zapnuta na všech portech.

S tím úzce souvisí i nutnost zapnutí spanning tree protokolu, označení portů pro koncová zařízení jako "edge" portů a konfigurace automatického vypnutí těchto portů při obdržení BPDU (spanning tree information) paketů.

## 4.7 Konfigurace WiFi AP

Na každém AP budou nastaveny 2 SSID, jedno pro interní síť a jedno pro hosty. Koncept popisuje obrázek níže.

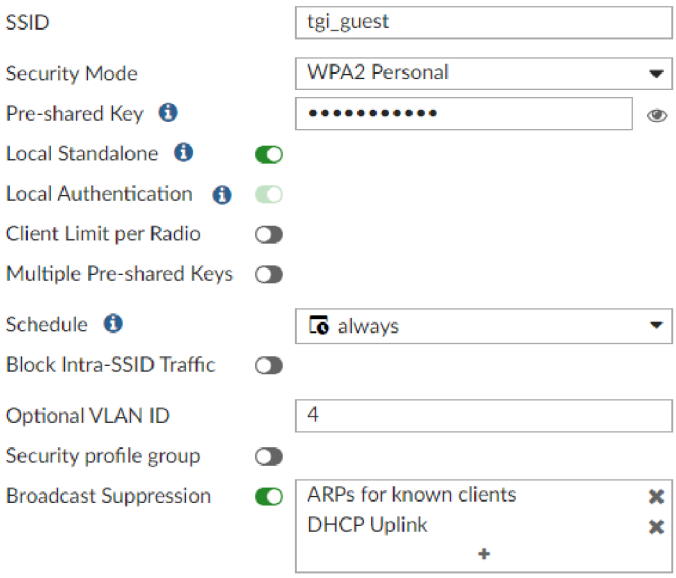



**Obrázek č. 22: Nastavení WiFi AP**

(Zdroj: vlastní zpracování)

### 4.7.1 Síť pro hosty

Konfigurací bude tato síť standardně zabezpečena pomocí WPA2-PSK, tedy pomocí předsdíleného hesla. Uživatelé budou staticky zařazeni do VLAN 4, tedy do int-guest sítě. SSID bude nakonfigurováno v "local bridge" módu, kdy je po výpadku spojení s kontrolérem schopno fungovat samostatně.

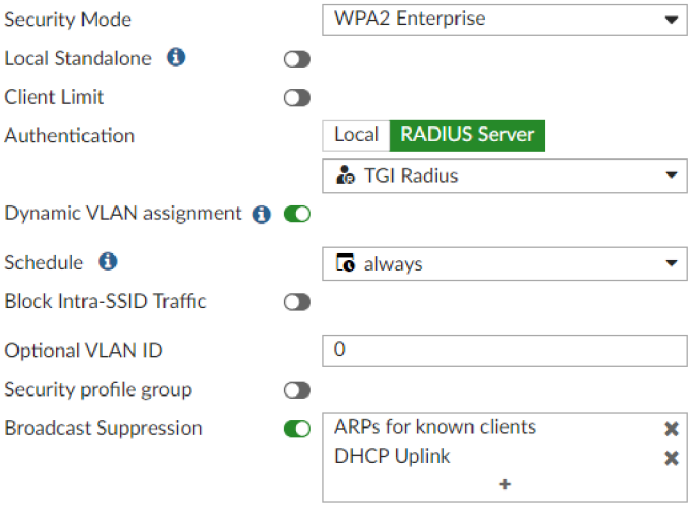



**Obrázek č. 23: Nastavení guest SSID**

(Zdroj: vlastní zpracování)

### 4.7.2 Interní wifi síť

Tato síť bude zabezpečena v režimu WPA2-Enteprise, tedy pomocí uživatelského jména a hesla, ověřovaného RADIUS serverem. Podobně jako na drátové síti bude i na tomto SSID nastaven režim dynamických VLAN, kdy VLAN ID je pro zařízení získáváno z RADIUS serveru v parametru odpovědi. Stejně jako síť pro hosty, i toto SSID bude nakonfigurováno v módu "local bridge".




**Obrázek č. 24: Nastavení internal SSID**

(Zdroj: vlastní zpracování)

## 4.8 Technologie přenosu a topologie fyzické vrstvy

Vzhledem k malému rozsahu bude infrastruktura každé pobočky tvořena jednou horizontální sekcí, která bude mít topologii typu hvězda, jak stanovuje norma ČSN EN 50173. Vzhledem k topologii a požadavkům investora navrhuji pro přenos využít metalické kabely a technologii WiFi.

Počítačová síť bude využívána k běžnému kancelářskému provozu, zcela dostačující tedy bude Gigabit Ethernet. K provozu této technologie je nezbytné využít materiály kategorie 5 k dosažení třídy D. Pro pokrytí poboček WiFi signálem doporučuji využít standard 802.11ac/n/a na obou frekvenčních pásmech, tedy 2,4 GHz a 5 GHz.

## 4.9 Počet přípojných míst

Návrh v tomto ohledu vychází z požadavků investora pro jednotlivé pobočky, kdy na každé z (prozatím budovaných) poboček budou pomocí kabelu připojeny nanejvýše dva počítače a tiskárna. Zbytek uživatelských zařízení (notebooky konzultantů nebo mobilní telefony) bude připojen bezdrátově. Se zásuvkami pro VOIP stolní telefony není počítáno, protože je využíváno systému, kdy k síti je připojena pouze VOIP základna, se kterou telefony komunikují bezdrátově v kmitočtovém pásmu 1880-1900 MHz.

**Tabulka č. 5: Popis místností** (Zdroj: vlastní zpracování)

| Pobočka | Číslo místnosti | Plocha | Počet přípojných míst | Připojená zařízení |
|---|---|---|---|---|
| **Jihlava** | 1 | 24 | 4 | PC, tiskárna, access point |
| **Jihlava** | 2 | 26 | 2 | PC |
| **Brno** | 1 | 25 | 4 | PC, tiskárna, access point |
| **Brno** | 2 | 17 | 2 | PC |

| | | | | |
|---|---|---|---|---|
| **Zlín** | 1 | 36 | 4 | 2xPC, tiskárna, access point |
| **Zlín** | 2 | 30 | 2 | |

## 4.10 Rozmístění přípojných míst

Schéma rozmístění se nachází v příloze č. 3, příloze č. 4 a příloze č. 5. Vzhledem k požadavku investora na nízkou cenu řešení a celkové nejistotě rentability poboček do budoucna budou přípojná místa umístěna na všech pobočkách v plastových instalačních lištách, vedených po zdech podél země. Jedinou výjimkou jsou porty pro WiFi AP, které budou umístěny na stropě, vždy jako zakončení příslušné instalační lišty.

**Obrázek č. 25: Ukázka řešení přípojného místa**

(Zdroj: 17)

### 4.10.1 Kabelové trasy

Kabeláž je rozmístěna na každé z poboček do několika tras vedení kabeláže. Ty byly navrhnuty tak, aby bylo vyhověno požadavkům investora v ohledu předpokládaného rozmístění techniky a zároveň bylo přihlédnuto k faktu, že místnost 1 bude vždy sloužit ke kontaktu se zákazníkem. Z toho důvodu je v návrhu patrná snaha o minimalizaci

viditelných instalačních lišt v této místnosti. Pro jednotlivé pobočky trasy detailně popisuji níže. Délky tras včetně značení jsou pak zaneseny v příloze č. 6.

**Brno**

Kabelová trasa A je svedena z datového rozvaděče k zemi, v místnosti 2 pak pokračuje podél obvodové stěny až k plánovanému pracovnímu místu. Na jejím konci jsou umístěny dvě zásuvky, 3.01 a 3.02. Do místnosti 1 je vedena průrazem stěny (32x20 mm), která rozděluje obě místnosti, bezprostředně pod datovým rozvaděčem. Za tímto průrazem je umístěna zásuvka 2.01. Dále pokračuje podél obvodové stěny u země až do poloviny místnosti, kde se nachází zásuvky 1.01 a 1.02. Kabelová trasa B je vedena od datového rozvaděče u stropu, podél stěny oddělující místnosti 1 a 2, na jejím konci se nachází datová zásuvka pro AP. Detailní rozkreslení se nachází v příloze č. 3.

**Jihlava**

Kabelová trasa A je vedena od datového rozvaděče průrazem u stropu do místnosti 1, pokračuje 30 cm a na jejím konci je umístěna datová zásuvky pro AP. Trasa B pak vede z datového rozvaděče u stropu do kuchyně a z ní pak do místnosti 1. Ihned za průrazem do této místnosti je rohem vedena k zemi a dále pokračuje podél obvodové stěny, aby mohlo dojít k instalaci zásuvek 2.01, 1.01 a 1.02. Trasa C je pak od rozvaděče vedena u stropu v rámci místnosti 2, v druhém ohybu je však svedena k zemi a pokračuje dále k předpokládanému pracovnímu místu, kde jsou umístěny zásuvky 3.01 a 3.02. Veškeré otvory ve zdech musí být v rozměru 32x20 mm. Detailní nákres je umístěn v příloze č. 4.

**Zlín**

Kabelová trasa A vede z rozvaděče k zemi, kde je vedena průrazem přímo do místnosti 1, pokračuje cca 50 cm za stěnu a je zakončena zásuvkou 2.01. Trasa B je vedena z

datového rozvaděče u stropu ke stěně, která rozděluje místnosti 1 a 2, a podél této stěny pokračuje. Zhruba 10-20 cm za průchodem mezi oběma místnosti uhýbá průrazem do místnosti 1, kde je po 20 cm zakončena zásuvkou 4.01 pro AP. V místnosti 2 pak pokračuje až k protější obvodové stěně, kde je svedena rohem k zemi a průrazem vedena do místnosti 1, kde je po 80-100 cm zakončena zásuvkami 1.01 a 1.02. Veškeré otvory ve zdech musí opět být v rozměru 32x20 mm.

## 4.11 Značení kabeláže a tras

Vzhledem k velmi malému rozsahu každé sítě jsem zvolil nejjednodušší možné, ale stále velice přehledné značení ve formátu Z.X, kde Z je číslo přípojného místa a X je číslo portu. Takto značen bude port v přepojovacím panelu i zásuvce, stejné značení ponese na obou koncích i samotný kabel.

Přepojovací panely budou značeny ve formátu PPx, kde x je číslo panelu. Podobně značeny budou i datové rozvaděče ve formátu DRx.

## 4.12 Kabeláž

Pro realizaci kabelových rozvodů se budu věnovat sekci horizontální a pracovní. Každá z poboček bude mít pouze jeden datový rozvaděč, páteřní sekcí tedy nemá smysl se zabývat. Vzhledem k běžnému kancelářskému provozu postačí kabeláž kategorie 5, síť bude tvořena fyzickou topologií typu hvězda.

### 4.12.1 Horizontální sekce

Horizontální sekce je realizována pomocí nestíněného párového krouceného kabelu kategorie 5 typu drát. Vybral jsem kabel Belden 1583E, který má plášť z PVC a jako takový je vhodný pro vnitřní rozvody, neboť nevede oheň a je samozhášivý. Zároveň podporuje Gigabit Ethernet.

**Obrázek č. 26: Kabel Belden 1583E**

(Zdroj: 18)

### 4.12.2 Pracovní sekce

Pro pracovní sekci bude nezbytné zakoupit hotové kabely různé délky, tzv. patch cordy typu lanko, které jsou pro tuto sekci nejvhodnější. K propojení koncových zařízení a zásuvek budou použity různé délky šedých patch cordů. K propojení v datovém rozvaděči budou převážně využity šedé patch cordy délky 20-50 cm. Jedinými výjimkami bude propojení switche s koncovým zařízením T-Mobile, které bude realizováno patch cordem červené barvy, a propojení switche s WiFi AP, které bude realizováno patch cordem žluté barvy. Navrhuji využít nestíněné kabely kategorie 5 od společnosti Panduit. Katalogové číslo se v tomto případě liší dle barvy a délky.

**Obrázek č. 27: Patch Cord Panduit**

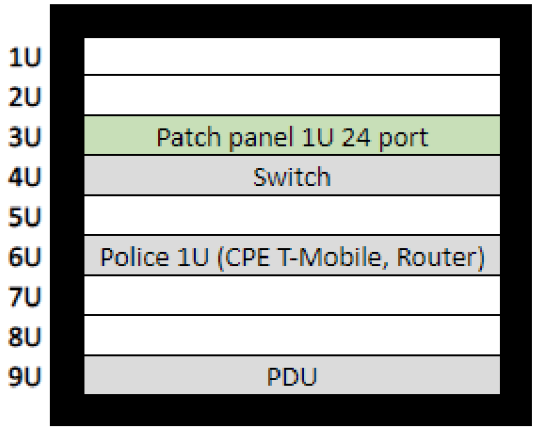
(Zdroj: 26)

## 4.13 Datový rozvaděč

Z důvodu omezeného prostoru jsem ve svém návrhu vybral rozvaděč nástěnný s označením RUA-09-AS5 od výrobce Triton, který bude umístěn cca 30 cm od stropu. Jde o 19" rozvaděč o výšce 9U a hloubce 500 cm, což vzhledem k malému počtu prvků, které bude obsahovat, dostačuje. Vyznačuje se odnímatelnými bočnicemi pro snazší instalaci jednotlivých prvků, přičemž je kompletně uzamykatelný. Důležitá pro realizaci návrhu je příprava na vývod kabelů v horní i spodní části rozvaděče, jelikož obou variant je na pobočkách využíváno.

Rozmístění jednotlivých prvků v rámci rozvaděče detailně popisuje obrázek níže, přičemž toto rozmístění bude pro všechny pobočky identické. V horní části je ponecháno 2U volného místa, následuje patch panel, switch, 1U volného místa a police pro koncové zařízení (CPE) T-Mobile. Dle mých zkušeností je dodávané zařízení pro takto malé instalace ne vždy montovatelné na vertikální lišty rozvaděče, je tedy bezpečnější počítat s umístěním na polici. V nejspodnější části bude rozvaděč obsahovat zásuvkovou lištu (PDU) k napájení jednotlivých zařízení. VOIP základna pro ruční telefony bude umístěna vně rozvaděče (na jeho stropnici), protože její umístění uvnitř

by mělo negativní dopad na signál mezi základnou a telefony. Jde o relativně malé zařízení, a tak je toto řešení akceptovatelné.




**Obrázek č. 28: Rozmístění prvků uvnitř datového rozvaděče**

(Zdroj: vlastní zpracování)

Součástí rozvaděče bude i zásuvková lišta (PDU), pomocí které bude řešeno napájení aktivních prvků a případně daléích zařízení. Zásuvková lišta bude též od společnosti Triton s označením RAB-PD-X11-A1. Jde o lištu se 7 zásuvkami, vypínačem a přepěťovou ochranou.

**Obrázek č. 29: Zásuvková lišta Triton**

(Zdroj: 25)

## 4.14 Prvky vedení kabeláže

Vzhledem k požadavkům investora bylo k vedení tras vybráno nejlevnější možné řešení, kterým jsou plastové instalační lišty na stěny. Na vybraných lokalitách zpravidla nelze počítat s využitím zdvojených stropů nebo podlah a instalace sítě "pod omítku" by byla v tomto druhu projektu příliš nákladná.

### 4.14.1 Trasy kabeláže

K vedení tras od datového rozvaděče až po přípojná místa jsem vybral systém instalačních minilišt DLPlus od společnosti Legrand v rozměru 32x20mm, které se vyznačují snadnou instalací a velkým množstvím příslušenství.

**Obrázek č. 30: Systém instalačních lišt DLPlus**

(Zdroj: 17)

Protože přípojná místa budou instalována přímo na instalačních lištách, je zároveň nezbytné zakoupit adaptéry systému DLPlus s katalogovými čísly 31611 (zásuvky u země) a 31646 (stropní zásuvky pro AP), pomocí kterých budou na lišty zásuvky namontovány.

**Obrázek č. 31: Zásuvkový adaptér DLPlus**

(Zdroj: 19)

## 4.15 Spojovací prvky

Spojovací prvky slouží obecně k ukončení linky, v případě mého návrhu se tedy bude jednat o konektory, zásuvky a přepojovací panel. Datové zásuvky a přepojovací panely budou modulární, ale protože společnost Legrand vyrábí rámečky pouze pro svůj proprietární systém modulů Mosaic, budou typy modulů rozdílné.

### 4.15.1 Datové zásuvky

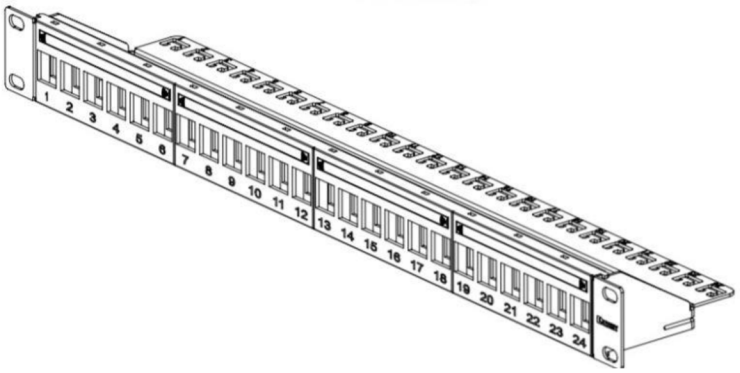
Datové zásuvky byly vybrány kvůli kompatibilitě se systémem instalačních lišt taktéž od společnosti Legrand. Jde o řešení určené k montáži na povrch stěny, kdy se datová zásuvka skládá z plastového rámečku pro modulární systém zásuvek Mosaic. Pro realizaci návrhu bude potřeba zakoupit rámečky pro 2 moduly. Tam, kde bude osazena pouze jedna pozice, bude prázdné místo zaslepeno (17).

**Obrázek č. 32: Rámeček pro systém Mosaic**

(Zdroj: 22)

### 4.15.2 Přepojovací panel

Do datového rozvaděče jsem zvolil modulární patch panel pro konektory typu keystone od výrobce Panduit s označením KP24WSBL, který obsahuje vyvazovací hrazdu. V datovém rozvaděči se vždy bude nacházet jeden patch panel o výšce 1U s 24 pozicemi pro konektory. Nevyužité pozice budou zaslepeny. Rozvržení patch panelu je detailně popsáno v příloze č. 7, přičemž pro všechny pobočky je stejné.



**Obrázek č. 33: Modulární patch panel Panduit KP24WSBL**

(Zdroj: 23)

### 4.15.3 Konektory

Pro instalaci budou potřeba dva typy konektorů, jelikož datové zásuvky a přepojovací panely jsou navrženy pro rozdílné typy modulů.

Pro terminaci linky na straně patch panelu jsem vybral keystone moduly od výrobce Panduit s označením NK5E88MBLY. Jde o modul kategorie 5 se zlacenými kontakty v černé barvě.

**Obrázek č. 34: Keystone modul Panduit NK5E88MBLY**

(Zdroj: 24)

V datových zásuvkách bude využito modulů systému Mosaic od společnosti Legrand, které jsou kompatibilní s vybranými rámečky. Moduly jsou kategorie 5 a je garantována výdrž 2 500 odpojení/zapojení patch cordů.


**Obrázek č. 35: RJ45 modul systému Mosaic**

(Zdroj: 17)

## 4.16 Ekonomické zhodnocení

Tato sekce pojednává o veškerých materiálních nákladech, které by vznikly při realizaci návrhu řešení. Do rozpočtu není započítána cena za samotný návrh a fyzickou instalaci. Naopak je v nákladech zahrnut veškerý materiál, cena aktivních prvků i měsíční náklad na provoz sítě. Návrh aktivních prvků počítá s využitím již existující infrastruktury, jako je například RADIUS server, v tomto ohledu ale nevzniknou žádné dodatečné náklady.

Podrobné rozepsání všech položek rozpočtu se nachází v příloze č. 8 pro pobočku Brno, v příloze č. 9 pro pobočku Jihlava a v příloze č. 10 pro pobočku Zlín.

Investor požaduje řešení s co nejnižšími náklady, což by ale zároveň nemělo kompromitovat celkovou funkčnost sítě. V návrhu jsou vybrány kvalitní produkty renomovaných výrobců, přesto je cena za realizaci funkční, spolehlivé a bezpečné sítě velmi přijatelná, jak ukazuje tabulka níže.

**Tabulka č. 6: Předpokládané náklady** (Zdroj: vlastní zpracování)

| | | |
|---|---|---|
| **Brno** | Jednorázová platba při zavedení pobočky bez DPH | 34,158.00 Kč |
| | Měsíční platba se závazkem na dva roky bez DPH | 4,000.00 Kč |
| | Celková cena za dva roky provozu bez DPH | 130,158.00 Kč |
| **Jihlava** | Jednorázová platba při zavedení pobočky bez DPH | 36,027.00 Kč |
| | Měsíční platba se závazkem na dva roky bez DPH | 4,000.00 Kč |
| | Celková cena za dva roky provozu bez DPH | 132,027.00 Kč |
| **Zlín** | Jednorázová platba při zavedení pobočky bez DPH | 34,937.00 Kč |
| | Měsíční platba se závazkem na dva roky bez DPH | 4,000.00 Kč |
| | Celková cena za dva roky provozu bez DPH | 130,937.00 Kč |

Jednorázovou platbou se rozumí cena za materiál a aktivní prvky. Měsíční platba se skládá z platby za připojení k IP VPN a ceny za službu Managed LAN, což je pronájem, konfigurace a správa switche.

Cena za IP VPN je vždy stanovena dle podmínek na konkrétní lokalitě a dle požadované rychlosti, obvykle se pohybuje kolem 500-1000 Kč měsíčně.

Cena za konfiguraci a správu switche je stanovena pro zákazníka individuálně dle konkrétních požadavků a dalších kritérií, dle mých zkušeností se pohybuje kolem hranice 3000 Kč měsíčně. Zákazník neplatí žádný jednorázový poplatek při zřízení, vysoké vstupní náklady poskytovatele (nákup switche a jeho konfigurace) jsou rozpočítány do měsíčních plateb.

# ZÁVĚR

Cílem mé diplomové práce byl návrh řešení počítačové sítě pro vznikající síť malých poboček společnosti.

V teoretické části práce jsem se zaměřil zejména na podrobný popis principů komunikační infrastruktury a popis technologií, jejichž pochopení je pro komplexní návrh počítačové sítě nezbytné. Praktická část práce se pak zabývala analýzou stávající síťové infrastruktury společnosti a taktéž popisem objektů, jejichž novou síťovou infrastrukturu je dle požadavků investora potřeba navrhnout. Analýza současného stavu odhaluje rozmístění a rozsah poboček, pro které je návrh třeba vypracovat a taktéž technické prostředí, do kterého je nezbytné nové lokality po stránce komunikační infrastruktury začlenit. Společně s konzultacemi s investorem představuje analýza základní opěrný bod pro samotné řešení.

Návrh řešení pak představuje komplexní řešení pobočkové komunikační infrastuktury, které splňuje veškeré požadavky investora na funkčnost, spolehlivost a snadnou správu, přičemž představuje vyvážený kompromis mezi náklady a přínosy. Koncept je též jednoduše využitelný pro větší množství dalších lokalit, které jsou v budoucnosti v rámci rozšíření společnosti plánovány.

# 5 SEZNAM POUŽITÉ LITERATURY


1. IP VPN | T-Mobile Czech Republic. *T-Mobile Czech Republic* [online]. Copyright © 2020 T [cit. 26.01.2020]. Dostupné z: http://www.gts.cz/sluzby/data/ip-vpn

2. Cookbook | FortiGate / FortiOS 5.4.0 | Fortinet Documentation Library. *Fortinet Documentation Library* [online]. Dostupné z: https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/912474

3. Co je IaaS? Infrastruktura jako služba | Microsoft Azure. *Object moved* [online]. Copyright © 2020 Microsoft [cit. 26.01.2020]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-iaas/

4. LOWE, Doug. *Networking all-in-one for dummies*. 6th edition. Hoboken, New Jersey: John Wiley & Sons, Incorporated, [2016]. --For dummies. ISBN 978-1-119-15472-3.

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

6. TANENBAUM, Andrew S. *Computer networks*. 3rd ed. Upper Saddle River, N.J.: Prentice Hall PTR, c1996. ISBN 0-13-349945-6.

7. PANEK, Crystal. *Networking fundamentals*. Indianapolis: John Wiley & Sons, 2019. ISBN 978-1-119-65074-4.

8. Síťový model TCP/IP.*University information system MENDELU* [online]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=10011

9. Rodina protokolů TCP/IP.Archiv článků a přednášek Jiřího Peterky [online]. Dostupné z: https://www.earchiv.cz/b05/b0600001.php3

10. Síťový model TCP/IP.Archiv článků a přednášek Jiřího Peterky [online]. Dostupné z: https://www.earchiv.cz/a92/a231c110.php3

11. *Internetworking technologies handbook*. 4th ed. Indianapolis, IN: Cisco Press, c2004. Cisco Press networking technology series. ISBN 1-58705-119-2.

12. Layer 2 switching. *Free CCNA Tutorials. Study CCNA for free!* [online]. Dostupné z: https://study-ccna.com/layer-2-switching/

13. What is IP routing?. *Free CCNA Tutorials. Study CCNA for free!* [online]. Dostupné z: https://study-ccna.com/what-is-ip-routing/

14. JORDÁN, Vilém a Viktor ONDRÁK. *Infrastruktura komunikačních systémů I: univerzální kabelážní systémy*. Druhé, rozšířené vydání. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5115-5.

15. Understanding MAC Address Authentication - S2720, S5700, and S6720 V200R013C00 Configuration Guide - User Access and Authentication - Huawei. [online]. Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. [cit. 09.04.2020]. Dostupné z: https://support.huawei.com/enterprise/en/doc/EDOC1100065684/71e2c72/understanding-mac-address-authentication

16. MAC Authentication Bypass Deployment Guide - Cisco. *Cisco - Global Home Page* [online]. Dostupné z: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html

17. Plastové instalační lišty a minilišty DLPlus | Legrand | *Elektrické instalace a datové rozvody* [online]. Dostupné z: https://www.legrand.cz/plastove-instalacni-listy-a-minilisty-dlplus

18. Online Catalog | Belden[online]. Copyright © [cit. 28.04.2020]. Dostupné z: https://catalog.belden.com/index.cfm?event=browse&c=Category_172687&n=10&sr=1&sby=relevancy

19. 31707 DLPLUS ADAPTÉR LIŠT. PRO 31611. *Emas.cz - elektromateriál pro vás* [online]. Copyright © [cit. 02.05.2020]. Dostupné z: https://www.emas.cz/31707-dlplus-adapter-list-pro-31611

20. Application Scenarios for DHCP Snooping - Fat AP and Cloud AP V200R010C00 CLI-based Configuration Guide - Huawei. [online]. Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. [cit. 02.05.2020]. Dostupné z: https://support.huawei.com/enterprise/en/doc/EDOC1100064366/f44535b2/application-scenarios-for-dhcp-snooping

21. Dynamic ARP Inspection - Cisco Meraki. *Home - Cisco Meraki* [online]. Copyright © Copyright 2020 Cisco Meraki [cit. 02.05.2020]. Dostupné z: https://documentation.meraki.com/MS/Other_Topics/Dynamic_ARP_Inspection

22. 31611 DLPLUS RÁMEČEK MOSAIC 2M. *Emas.cz - elektromateriál pro vás* [online]. Copyright © [cit. 03.05.2020]. Dostupné z: https://www.emas.cz/31611-dlplus-ramecek-mosaic-2m

23. Panduit | KP24WSBL. *Panduit | Network Infrastructure and Industrial Electrical Wiring* [online]. Dostupné z: https://www.panduit.com/en/products/copper-systems/patch-panels-accessories/modular-patch-panels/kp24wsbl.html

24. Panduit | NK5E88MBLY. *Panduit | Network Infrastructure and Industrial Electrical Wiring* [online]. Dostupné z: https://www.panduit.com/en/products/copper-systems/connectors/jack-modules/nk5e88mbly.html

25. Rozvody 230 V | www.triton.cz. [online]. Copyright © Copyright TRITON Pardubice s.r.o. [cit. 03.05.2020]. Dostupné z: https://www.triton.cz/cs/datove-rozvadece/prislusenstvi/rozvody-230-v

26. Panduit | Patch Cords. Panduit | Network Infrastructure and Industrial Electrical Wiring [online]. Dostupné z: https://www.panduit.com/en/products/copper-systems/patch-cords-accessories/patch-cords.html

# 6 SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

PC – personal computer

VOIP - voice over internet protocol

MPLS IP VPN - multiprotocol label switching internet protocol virtual private network

ADSL - asymmetric digital subscriber line

LTE - 3GPP Long Term Evolution

IaaS - 3GPP Long Term Evolution

DNS - domain name system

DHCP - dynamic host configuration protocol

NPS – network policy server

NTP – network time protocol

AD – active directory

DC – domain controller

VLAN - virtual local area network

SSL – secure sockets layer

STP – spanning tree protocol

ARP – address resolution protocol

PoE – power over ethernet

LAN – local area network

WAN – wide area network

MAN – metropolitan area network

MAC – media access control

TCP – transmission control protocol

UDP – user datagram protocol

FTP – file transfer protocol

SMTP – simple mail transfer protocol

AP – access point

UTP – unshielded twisted pair

IKS – integrovaná komunikační infrastruktura

ACL – access control list

SSID – service set identifier

# 7 SEZNAM OBRÁZKŮ

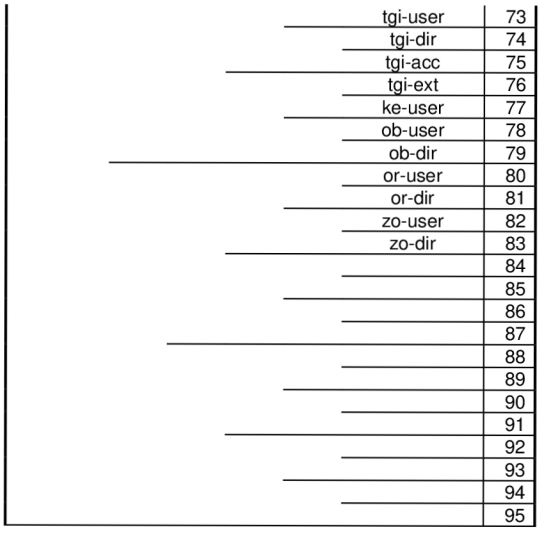
# 8 SEZNAM TABULEK

# 9 SEZNAM PŘÍLOH

# Příloha č. 1: Adresní plán nově zřizovaných poboček

| Branches, 10.192.0.0-10.255.0.0 | | | | | |
|---|---|---|---|---|---|
| /12 | /13 | /14 | /15 | /16 | |
| | | | | | 192 |
| | | | | | 193 |
| | | | | | 194 |
| | | | | | 195 |
| | | | | | 196 |
| | | | | | 197 |
| | | | | | 198 |
| | | | | | 199 |
| | | | | | 200 |
| | | | | | 201 |
| | | | | | 202 |
| | | | | | 203 |
| | | | | | 204 |
| | | | | | 205 |
| | | | | | 206 |
| | | | | | 207 |
| | | | | | 208 |
| | | | | | 209 |
| | | | | | 210 |
| | | | | | 211 |
| | | | | | 212 |
| | | | | | 213 |
| | | | | | 214 |
| branches | | | | *see "JIH/BRN/ZLN" table* | 215 |
| | | | | | 216 |
| | | | | | 217 |
| | | | | | 218 |
| | | | | | 219 |
| | | | | | 220 |
| | | | | | 221 |
| | | | | | 222 |
| | | | | | 223 |
| | | | | PRIVATE | 224 |
| | | VHE | | DMZ | 225 |
| | | | | PUBLIC | 226 |
| | | | | *not used* | 227 |
| | | | | | 228 |
| | | | | | 229 |
| | | | | | 230 |
| | | | | | 231 |
| Datacenter | | | | MANAGED SERVICES | 232 |
| | | | | | 233 |
| | | | | | 234 |
| | | | | | 235 |
| | | | | | 236 |
| | | | | | 237 |
| | | | | INTERCONNECTIONS | 238 |
| | | | | Fortigate | 239 |
| | | | | | 240 |
| | | | | | 241 |
| | | | | | 242 |
| | | | | | 243 |
| | | | | | 244 |
| | | | | | 245 |
| | | | | | 246 |
| | | | | | 247 |
| LOCALITY | | | | | 248 |
| | | | | | 249 |
| | | | | | 250 |
| | | | | | 251 |
| | | | | | 252 |
| | | | | BRN02 | 253 |
| | | | | BRN01 | 254 |
| | | | | REMOTE VPN | 255 |

| JIH/BRN/ZLN – 10.208.0.0/16 | | | | | | |
|---|---|---|---|---|---|---|
| /19 | /20 | /21 | /22 | /23 | /24 | |
| | | | | | int-mgmt | 0 |
| | | | | | int-guest | 1 |
| | | | | | int-prnt | 2 |
| | | | | | int-voip | 3 |
| | | | | | int-security | 4 |
| | | | | | zs-user | 5 |
| | | | | | zs-dev | 6 |
| | | | | | zs-devops | 7 |
| | | | | | zs-ops | 8 |
| | | | | | tgi-user | 9 |
| | | | | | tgi-dir | 10 |
| | | | | | tgi-acc | 11 |
| | | | | | tgi-ext | 12 |
| | | | | | ke-user | 13 |
| | | | | | ob-user | 14 |
| | | | | | ob-dir | 15 |
| JIH01 | | | | | or-user | 16 |
| | | | | | or-dir | 17 |
| | | | | | zo-user | 18 |
| | | | | | zo-dir | 19 |
| | | | | | | 20 |
| | | | | | | 21 |
| | | | | | | 22 |
| | | | | | | 23 |
| | | | | | | 24 |
| | | | | | | 25 |
| | | | | | | 26 |
| | | | | | | 27 |
| | | | | | | 28 |
| | | | | | | 29 |
| | | | | | | 30 |
| | | | | | | 31 |
| | | | | | int-mgmt | 32 |
| | | | | | int-guest | 33 |
| | | | | | int-prnt | 34 |
| | | | | | int-voip | 35 |
| | | | | | int-security | 36 |
| | | | | | zs-user | 37 |
| | | | | | zs-dev | 38 |
| | | | | | zs-devops | 39 |
| | | | | | zs-ops | 40 |
| | | | | | tgi-user | 41 |
| | | | | | tgi-dir | 42 |
| | | | | | tgi-acc | 43 |
| | | | | | tgi-ext | 44 |
| | | | | | ke-user | 45 |
| | | | | | ob-user | 46 |
| | | | | | ob-dir | 47 |
| BRN04 | | | | | or-user | 48 |
| | | | | | or-dir | 49 |
| | | | | | zo-user | 50 |
| | | | | | zo-dir | 51 |
| | | | | | | 52 |
| | | | | | | 53 |
| | | | | | | 54 |
| | | | | | | 55 |
| | | | | | | 56 |
| | | | | | | 57 |
| | | | | | | 58 |
| | | | | | | 59 |
| | | | | | | 60 |
| | | | | | | 61 |
| | | | | | | 62 |
| | | | | | | 63 |
| | | | | | int-mgmt | 64 |
| | | | | | int-guest | 65 |
| | | | | | int-prnt | 66 |
| | | | | | int-voip | 67 |
| ZLN01 | | | | | int-security | 68 |
| | | | | | zs-user | 69 |
| | | | | | zs-dev | 70 |
| | | | | | zs-devops | 71 |
| | | | | | zs-ops | 72 |


tgi-user 73
tgi-dir 74
tgi-acc 75
tgi-ext 76
ke-user 77
ob-user 78
ob-dir 79
or-user 80
or-dir 81
zo-user 82
zo-dir 83
84
85
86
87
88
89
90
91
92
93
94
95

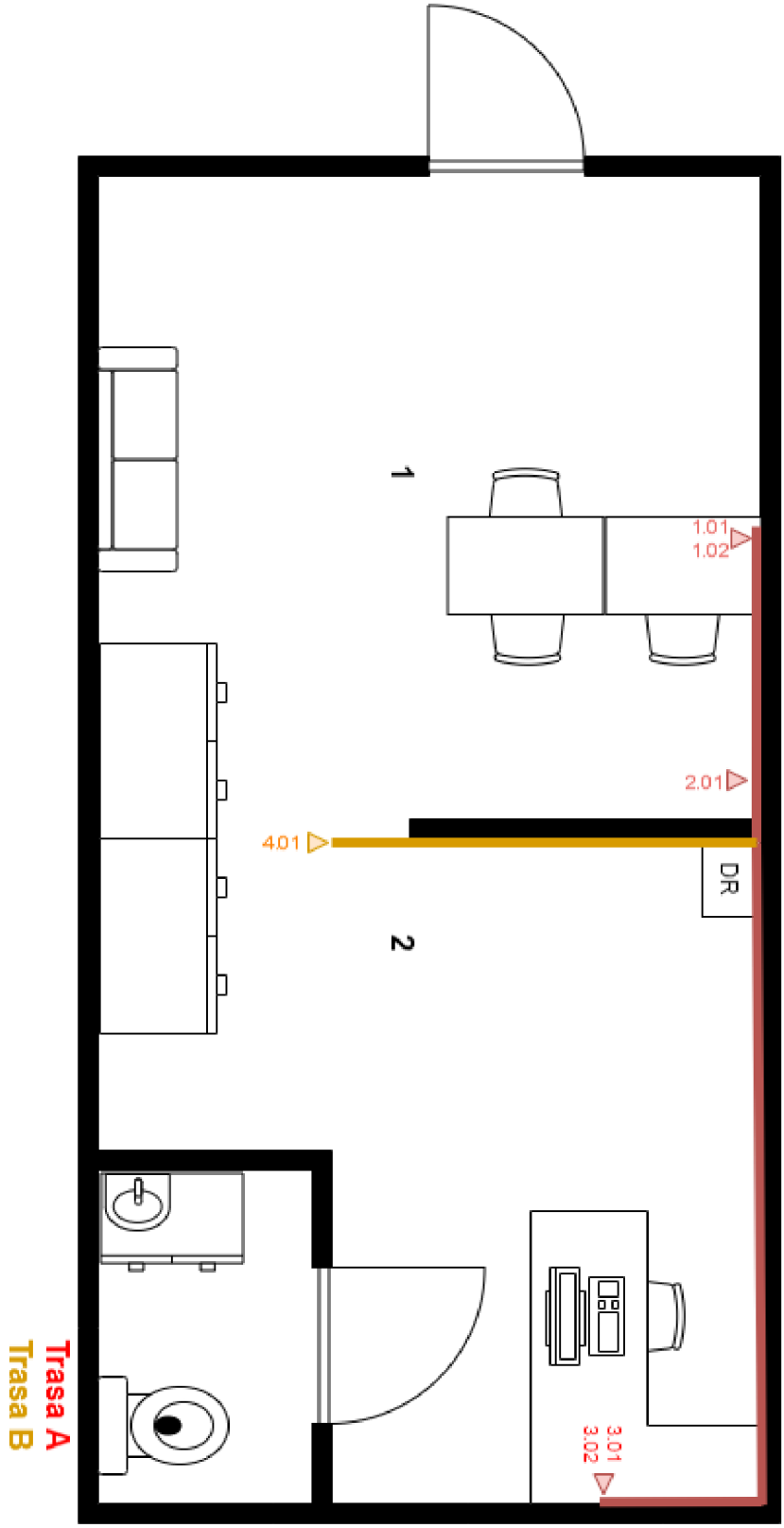
# Příloha č. 2: Návrh ACL

| Název ACL | ID pravidla | Akce | Zdrojový rozsah | Prefix zdroje | Cílový rozsah | Prefix cíle | Poznámka |
|---|---|---|---|---|---|---|---|
| int-guest-acl | 12 | permit | | | 10.253.4.4 | 30 | DHCP |
| | 20 | permit | | | 10.225.0.4 | 32 | přístup k proxy serverům v datacentru |
| | 30 | permit | | | 10.226.0.4 | 32 | |
| | 40 | permit | | | 10.226.1.4 | 32 | |
| | 50 | deny | | | 10.0.0.0 | 8 | odepření přístupu do privátních sítí |
| | 51 | deny | | | 172.16.0.0 | 12 | |
| | 52 | deny | | | 192.168.0.0 | 16 | |
| | 60 | permit | | | 0.0.0.0 | 0 | implicitní povolení (přístup k internetu) |
| int-prnt-acl | 10 | permit | | | 10.224.0.10 | 31 | DHCP, DNS, Radius |
| | 11 | permit | | | 10.224.0.4 | 30 | NTP servers |
| | 20 | permit | | | 10.224.0.12 | 31 | přístup k file serveru a print serveru |
| | 70 | permit | | | 10.255.28.0 | 24 | přístup pro management tiskáren z VPN |
| | 80 | permit | | | 10.255.240.4 | 30 | přístup pro dodavatele tiskových řešení z VPN |
| | 100 | permit | 10.208.2.0 | 24 | 10.208.14.0 | 23 | přístup pro uživatele tiskáren (Jihlava) |
| | 101 | permit | 10.208.34.0 | 24 | 10.208.46.0 | 23 | přístup pro uživatele tiskáren (Brno) |
| | 102 | permit | 10.208.66.0 | 24 | 10.208.78.0 | 23 | přístup pro uživatele tiskáren (Zlín) |
| | 260 | deny | | | 0.0.0.0 | 0 | implicitní zamítnutí |
| zs-dev-acl | 10 | permit | | | 10.224.0.0 | 14 | přístup k serverům v datacentru (doménové řadiče, file servery, síťové služby a jiné) |
| | 130 | permit | | | 10.232.0.2 | 31 | |
| | 140 | permit | | | 192.168.1.0 | 24 | |
| | 30 | permit | | | 10.253.3.0 | 24 | přístup k serverům na jiných lokalitách |
| | 40 | permit | | | 10.254.3.0 | 24 | |
| | 110 | permit | | | 10.253.30.0 | 24 | přístup k vývojovým serverům na jiných lokalitách |
| | 120 | permit | | | 10.254.30.0 | 24 | |
| | 150 | deny | | | 10.0.0.0 | 8 | odepření přístupu do privátních sítí |
| | 151 | deny | | | 172.16.0.0 | 12 | |
| | 152 | deny | | | 192.168.0.0 | 16 | |
| | 160 | permit | | | 0.0.0.0 | 0 | implicitní povolení (přístup k internetu) |
| zs-ops-acl | 10 | permit | | | 10.224.0.0 | 14 | přístup k serverům v datacentru (doménové řadiče, file servery, síťové služby a jiné) |
| | 160 | permit | | | 192.168.1.0 | 24 | |
| | 161 | permit | | | 192.168.0.2 | 32 | |
| | 162 | permit | | | 192.168.7.0 | 24 | |
| | 30 | permit | | | 10.253.3.0 | 24 | přístup k serverům na jiných lokalitách |
| | 40 | permit | | | 10.254.3.0 | 24 | |
| | 120 | permit | | | 10.253.30.0 | 24 | přístup k vývojovým serverům na jiných lokalitách |
| | 130 | permit | | | 10.254.30.0 | 24 | |
| | 51 | permit | | | 10.253.28.0 | 23 | přístup do stejné VLAN na jiných lokalitách |
| | 52 | permit | | | 10.254.28.0 | 23 | |
| | 53 | permit | | | 10.255.28.0 | 23 | |
| | 54 | permit | | | 10.208.8.0 | 24 | |
| | 55 | permit | | | 10.208.40.0 | 24 | |
| | 56 | permit | | | 10.208.72.0 | 24 | |
| | 150 | permit | | | 10.224.16.16 | 30 | management přístup k VOIP ústředně |
| | 170 | permit | | | 172.25.34.52 | 32 | management přístup k edge firewallu |
| | 200 | deny | | | 10.0.0.0 | 8 | odepření přístupu do privátních sítí |
| | 201 | deny | | | 172.16.0.0 | 12 | |
| | 202 | deny | | | 192.168.0.0 | 16 | |
| | 250 | permit | | | 0.0.0.0 | 0 | implicitní povolení (přístup k internetu) |
| user-acl | 10 | permit | | | 10.224.0.4 | 30 | přístup k vybraným serverům v datacentru (doménové řadiče, file servery a síťové služby) |
| | 20 | permit | | | 10.224.0.8 | 29 | |
| | 310 | permit | | | 192.168.7.0 | 24 | |
| | 60 | permit | | | 10.224.0.64 | 32 | přístup k proxy serverům v datacentru |
| | 70 | permit | | | 10.225.0.4 | 32 | |
| | 80 | permit | | | 10.226.0.4 | 32 | |
| | 90 | permit | | | 10.226.1.4 | 32 | |

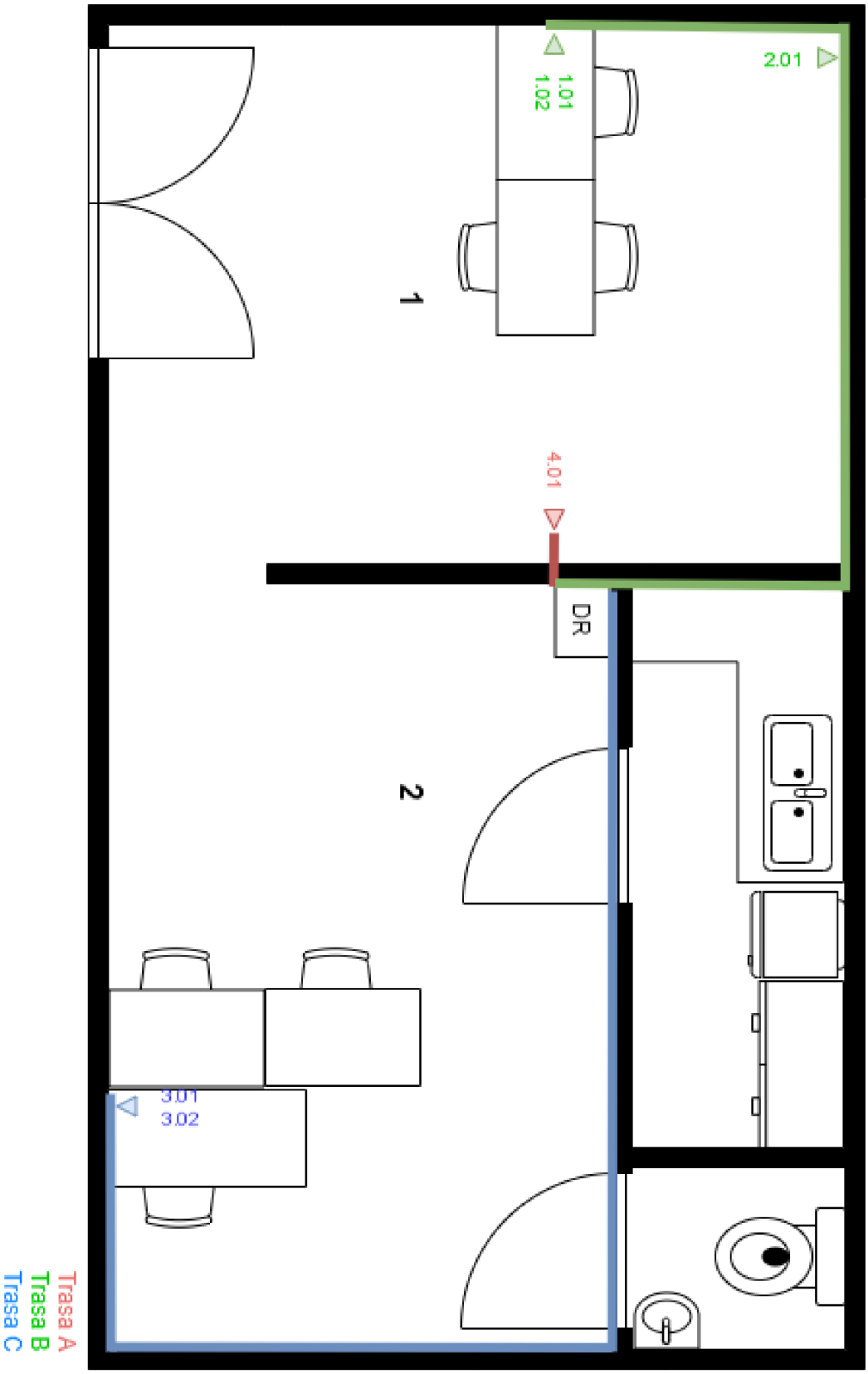
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 40 | permit | | | 10.253.3.0 | 24 | přístup k serverům na jiných lokalitách |
| | 50 | permit | | | 10.254.3.0 | 24 | |
| | 290 | permit | | | 10.224.1.0 | 24 | přístup k VOIP ústřednám |
| | 300 | permit | | | 10.224.16.16 | 30 | |
| | 400 | permit | 10.208.14.0 | 23 | 10.208.2.0 | 24 | přístup k tiskárnám (Jihlava) |
| | 401 | permit | 10.208.46.0 | 23 | 10.208.34.0 | 24 | přístup k tiskárnám (Brno) |
| | 402 | permit | 10.208.78.0 | 23 | 10.208.66.0 | 24 | přístup k tiskárnám (Zlín) |
| | 550 | deny | | | 10.0.0.0 | 8 | odepření přístupu do privátních sítí |
| | 551 | deny | | | 172.16.0.0 | 12 | |
| | 552 | deny | | | 192.168.0.0 | 16 | |
| | 600 | permit | | | 0.0.0.0 | 0 | implicitní povolení (přístup k internetu) |
| tgi-dir-acl | 10 | permit | | | 10.224.0.4 | 30 | přístup k vybraným serverům v datacentru (doménové řadiče, file servery, síťové služby a další) |
| | 20 | permit | | | 10.224.0.8 | 29 | |
| | 30 | permit | | | 10.224.0.18 | 31 | |
| | 190 | permit | | | 10.224.0.64 | 32 | přístup k proxy serverům v datacentru |
| | 200 | permit | | | 10.225.0.4 | 32 | |
| | 210 | permit | | | 10.226.0.4 | 32 | |
| | 220 | permit | | | 10.226.1.4 | 32 | |
| | 50 | permit | | | 10.253.3.0 | 24 | přístup k serverům na jiných lokalitách |
| | 60 | permit | | | 10.254.3.0 | 24 | |
| | 71 | permit | | | 10.253.10.0 | 24 | přístup k IP kamerám |
| | 72 | permit | | | 10.254.10.0 | 24 | |
| | 73 | permit | | | 10.208.4.0 | 24 | |
| | 74 | permit | | | 10.208.36.0 | 24 | |
| | 75 | permit | | | 10.208.68.0 | 24 | |
| | 131 | permit | | | 10.253.36.0 | 24 | přístup do stejné VLAN na jiných lokalitách |
| | 132 | permit | | | 10.254.36.0 | 24 | |
| | 133 | permit | | | 10.255.36.0 | 24 | |
| | 134 | permit | | | 10.208.10.0 | 24 | |
| | 135 | permit | | | 10.208.42.0 | 24 | |
| | 136 | permit | | | 10.208.74.0 | 24 | |
| | 240 | permit | | | 10.224.1.0 | 24 | přístup k VOIP ústřednám |
| | 250 | permit | | | 10.224.16.16 | 30 | |
| | 260 | deny | | | 10.0.0.0 | 8 | odepření přístupu do privátních sítí |
| | 261 | deny | | | 172.16.0.0 | 12 | |
| | 262 | deny | | | 192.168.0.0 | 16 | |
| | 270 | permit | | | 0.0.0.0 | 0 | implicitní povolení (přístup k internetu) |
| tgi-acc-acl | 10 | permit | | | 10.224.0.4 | 30 | přístup k vybraným serverům v datacentru (doménové řadiče, file servery, síťové služby a další) |
| | 20 | permit | | | 10.224.0.8 | 29 | |
| | 30 | permit | | | 10.224.0.18 | 31 | |
| | 100 | permit | | | 10.224.0.64 | 32 | přístup k proxy serverům v datacentru |
| | 110 | permit | | | 10.225.0.4 | 32 | |
| | 120 | permit | | | 10.226.0.4 | 32 | |
| | 130 | permit | | | 10.226.1.4 | 32 | |
| | 50 | permit | | | 10.253.3.0 | 24 | přístup k serverům na jiných lokalitách |
| | 60 | permit | | | 10.254.3.0 | 24 | |
| | 150 | permit | | | 10.224.1.0 | 24 | přístup k VOIP ústřednám |
| | 160 | permit | | | 10.232.0.2 | 31 | |
| | 180 | deny | | | 10.0.0.0 | 8 | odepření přístupu do privátních sítí |
| | 181 | deny | | | 172.16.0.0 | 12 | |
| | 182 | deny | | | 192.168.0.0 | 16 | |
| | 200 | permit | | | 0.0.0.0 | 0 | implicitní povolení (přístup k internetu) |
| int-voip-acl | 10 | permit | | | 10.224.0.10 | 31 | DHCP, DNS, Radius |
| | 11 | permit | | | 10.224.0.4 | 30 | NTP servers |
| | 60 | permit | | | 10.255.28.0 | 23 | přístup pro management VOIP z VPN |
| | 80 | permit | | | 10.224.1.0 | 24 | přístup k VOIP ústřednám |
| | 90 | permit | | | 10.224.16.16 | 30 | |
| | 100 | deny | | | 0.0.0.0 | 0 | implicitní zamítnutí |
| int-security- | 10 | permit | | | 10.224.0.10 | 31 | DHCP, DNS, Radius |

| | | | | | |
|---|---|---|---|---|---|
| **acl** | 11 | permit | 10.224.0.4 | 30 | NTP servers |
| | 21 | permit | 10.253.10.0 | 24 | přístup do stejné VLAN na jiných lokalitách |
| | 22 | permit | 10.254.10.0 | 24 | |
| | 23 | permit | 10.208.4.0 | 24 | |
| | 24 | permit | 10.208.36.0 | 24 | |
| | 25 | permit | 10.208.68.0 | 24 | |
| | 81 | permit | 10.253.36.0 | 24 | přístup k IP kamerám z vybraných uživatelských VLAN |
| | 82 | permit | 10.254.36.0 | 24 | |
| | 83 | permit | 10.255.36.0 | 24 | |
| | 84 | permit | 10.208.10.0 | 24 | |
| | 85 | permit | 10.208.42.0 | 24 | |
| | 86 | permit | 10.208.74.0 | 24 | |
| | 140 | permit | 10.255.28.0 | 23 | přístup pro management IP kamer z VPN |
| | 150 | deny | 0.0.0.0 | 0 | implicitní zamítnutí |
| **int-mgmt-acl** | 10 | permit | 10.224.0.10 | 31 | DHCP, DNS, Radius |
| | 20 | permit | 10.224.0.4 | 30 | NTP servers |
| | 30 | permit | 10.225.1.12 | 32 | zálohy konfigurací, ACL a DHCP binding tabulek |
| | 40 | permit | 10.253.2.0 | 24 | přístup do stejné VLAN na jiných lokalitách |
| | 50 | permit | 10.254.2.0 | 24 | |
| | 70 | permit | 10.208.0.0 | 24 | |
| | 80 | permit | 10.208.32.0 | 24 | |
| | 90 | permit | 10.208.64.0 | 24 | |
| | 120 | permit | 10.254.1.2 | 32 | přístup k síťovým zařízením na jiných lokalitách |
| | 130 | permit | 10.253.1.2 | 32 | |
| | 140 | permit | 10.253.1.3 | 32 | |
| | 150 | permit | 10.253.1.4 | 32 | |
| | 100 | permit | 10.255.2.0 | 24 | přístup pro management síťových zařízení z VPN |
| | 110 | permit | 172.25.34.52 | 32 | management přístup k edge firewallu |
| | 160 | permit | 195.144.99.128 | 29 | přístup k firewallům na perimetru datacentra |
| | 170 | permit | 10.238.0.8 | 29 | |
| | 180 | deny | 0.0.0.0 | 0 | implicitní zamítnutí |

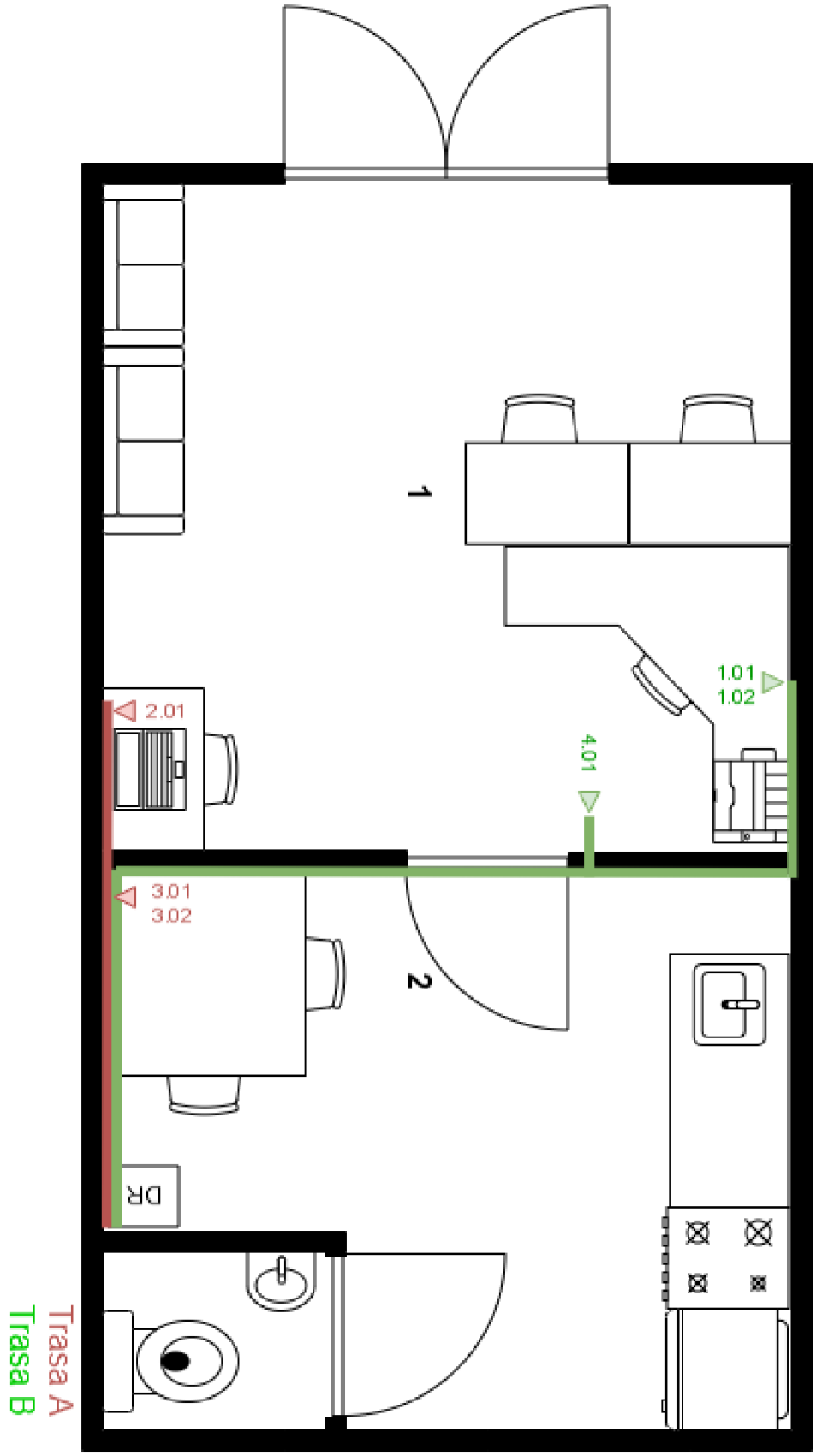
**Příloha č. 3: Schéma tras a přípojných míst, pobočka Brno**



**Příloha č. 4: Schéma tras a přípojných míst, pobočka Jihlava**



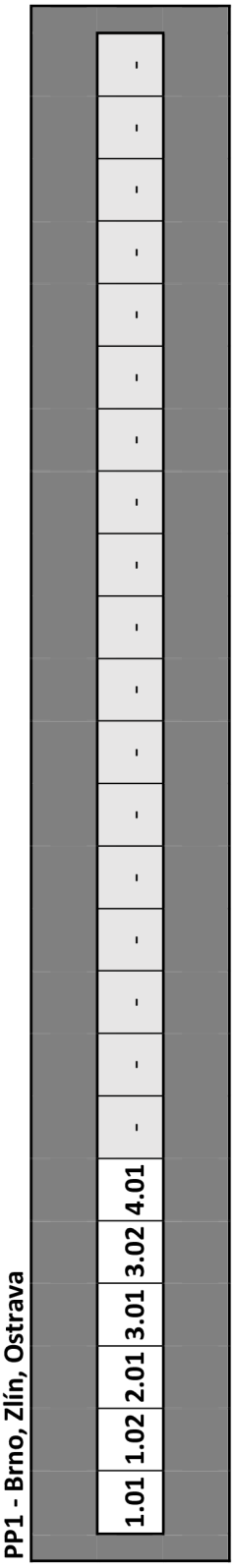
**Příloha č. 5: Schéma tras a přípojných míst, pobočka Zlín**



# Příloha č. 6: Kabelová tabulka

| Lokalita | Místnost | Patch panel | Port patch panelu | Zásuvka | Port | Značení portu | Určení portu | Značení kabelu | Délka kabelu v metrech |
|---|---|---|---|---|---|---|---|---|---|
| Brno | 1 | 1 | 1 | 1 | 1 | 1.01 | PC | 1.01 | 4.6 |
| | | 1 | 2 | 1 | 2 | 1.02 | Volný port | 1.02 | 4.6 |
| | | 1 | 3 | 2 | 1 | 2.01 | Tiskárna | 2.01 | 2.4 |
| | | 1 | 4 | 4 | 1 | 4.01 | AP | 4.01 | 3.7 |
| | 2 | 1 | 5 | 3 | 1 | 3.01 | PC | 3.01 | 7.3 |
| | | 1 | 6 | 3 | 2 | 3.02 | Volný port | 3.02 | 7.3 |
| Jihlava | 1 | 1 | 1 | 1 | 1 | 1.01 | PC | 1.01 | 8.2 |
| | | 1 | 2 | 1 | 2 | 1.02 | Volný port | 1.02 | 8.2 |
| | | 1 | 3 | 2 | 1 | 2.01 | Tiskárna | 2.01 | 6.2 |
| | | 1 | 4 | 4 | 1 | 4.01 | AP | 4.01 | 0.8 |
| | 2 | 1 | 5 | 3 | 1 | 3.01 | PC | 3.01 | 13.2 |
| | | 1 | 6 | 3 | 2 | 3.02 | Volný port | 3.02 | 13.2 |
| Zlín | 1 | 1 | 1 | 1 | 1 | 1.01 | PC | 1.01 | 12.2 |
| | | 1 | 2 | 1 | 2 | 1.02 | Tiskárna | 1.02 | 12.2 |
| | | 1 | 3 | 2 | 1 | 2.01 | PC | 2.01 | 6.2 |
| | | 1 | 4 | 4 | 1 | 4.01 | AP | 4.01 | 7.4 |
| | 2 | 1 | 5 | 3 | 1 | 3.01 | Volný port | 3.01 | 5.2 |
| | | 1 | 6 | 3 | 2 | 3.02 | Volný port | 3.02 | 5.2 |
| | | | | | | | **Celková délka** | | **128.1** |
| | | | | | | | **+ 20% rezerva** | | **153.72** |

## Příloha č. 7: Rozvržení patch panelů



# Příloha č. 8: Náklady projektu – pobočka Brno

| | Název položky | Počet | M.j. | Cena za m.j bez DPH | Celková cena za uvedený počet bez DPH |
|---|---|---|---|---|---|
| **Měsíční platba** | Managed LAN (Pronájem switche a jeho správa, závazek 2 roky) | 1 | ks | 3,000.00 Kč | 3,000.00 Kč |
| | Profesionální internet (MPLS IP VPN, závazek 2 roky) | 1 | ks | 1,000.00 Kč | 1,000.00 Kč |
| **Jednorázová platba** | Fortinet FortiAP 221E | 1 | ks | 13,000.00 Kč | 13,000.00 Kč |
| | Datový rozvaděč Triton RUA-09-AS5 | 1 | ks | 3,600.00 Kč | 3,600.00 Kč |
| | 19" Rack police Triton RAX-UP-350-A1, h. 350mm | 1 | ks | 500.00 Kč | 500.00 Kč |
| | Patch panel 1U 24 port, Panduit KP24WSBL | 1 | ks | 2,500.00 Kč | 2,500.00 Kč |
| | Keystone záslepka Panduit, NKBMBL-X | 18 | ks | 15.00 Kč | 270.00 Kč |
| | Keystone modul Panduit NK5E88MBLY | 6 | ks | 150.00 Kč | 900.00 Kč |
| | PDU Triton RAB-PD-X11-A1, 7x230V | 1 | ks | 1,700.00 Kč | 1,700.00 Kč |
| | Patch cord Panduit UTPCH1Y (šedý, 0.3m) | 6 | ks | 150.00 Kč | 900.00 Kč |
| | Patch cord Panduit UTPCH1YLY (žlutý, 0.3m) | 1 | ks | 150.00 Kč | 150.00 Kč |
| | Patch cord Panduit UTPCH2RDY (červený, 0.6m) | 1 | ks | 180.00 Kč | 180.00 Kč |
| | Legrand DLPlus instalační lišta 30017, 32x20mm | 20 | m | 80.00 Kč | 1,600.00 Kč |
| | Legrand DLPlus, spojka krytu přímá 33604 | 22 | ks | 25.00 Kč | 550.00 Kč |
| | Legrand DLPlus vnitřní/vnější variabilní roh 30271 | 2 | ks | 45.00 Kč | 90.00 Kč |
| | Legrand DLPlus odbočka T 30274 | 1 | ks | 80.00 Kč | 80.00 Kč |
| | Legrand DLPlus koncový díl (záslepka) 31209 | 2 | ks | 50.00 Kč | 100.00 Kč |
| | Legrand DLPlus zásuvkový adaptér na konec lišty 31646 | 1 | ks | 60.00 Kč | 60.00 Kč |
| | Legrand DLPlus zásuvkový adaptér 31707 | 3 | ks | 70.00 Kč | 210.00 Kč |
| | Legrand DLPlus zásuvkový rámeček pro 2 moduly 31611 | 4 | ks | 140.00 Kč | 560.00 Kč |
| | Legrand záslepka Mosaic, 1 modul 77070 | 2 | ks | 30.00 Kč | 60.00 Kč |
| | Legrand RJ45 modul Mosaic 76561 | 6 | ks | 270.00 Kč | 1,620.00 Kč |
| | Patch cord Panduit UTPCH4Y (šedý, 1.2m) | 6 | ks | 150.00 Kč | 900.00 Kč |
| | Patch cord Panduit UTPCH8Y (šedý, 2.4m) | 6 | ks | 200.00 Kč | 1,200.00 Kč |
| | Patch cord Panduit UTPCH12Y (šedý, 3.6m) | 6 | ks | 240.00 Kč | 1,440.00 Kč |
| | Patch cord Panduit UTPCH15Y (šedý, 4.6m) | 6 | ks | 300.00 Kč | 1,800.00 Kč |
| | UTP kabel Belden 1583E | 40 | m | 4.70 Kč | 188.00 Kč |

| | |
|---|---|
| **Jednorázová platba při zavedení pobočky bez DPH** | 34,158.00 Kč |
| **Měsíční platba se závazkem na dva roky bez DPH** | 4,000.00 Kč |
| **Celková cena za dva roky provozu bez DPH** | 130,158.00 Kč |

# Příloha č. 9: Náklady projektu – pobočka Jihlava

| | Název položky | Počet | M.j. | Cena za m.j bez DPH | Celková cena za uvedený počet bez DPH |
|---|---|---|---|---|---|
| **Měsíční platba** | Managed LAN (Pronájem switche a jeho správa, závazek 2 roky) | 1 | ks | 3,000.00 Kč | 3,000.00 Kč |
| | Profesionální internet (MPLS IP VPN, závazek 2 roky) | 1 | ks | 1,000.00 Kč | 1,000.00 Kč |
| **Jednorázová platba** | Fortinet FortiAP 221E | 1 | ks | 13,000.00 Kč | 13,000.00 Kč |
| | Datový rozvaděč Triton RUA-09-AS5 | 1 | ks | 3,600.00 Kč | 3,600.00 Kč |
| | 19" Rack police Triton RAX-UP-350-A1, h. 350mm | 1 | ks | 500.00 Kč | 500.00 Kč |
| | Patch panel 1U 24 port, Panduit KP24WSBL | 1 | ks | 2,500.00 Kč | 2,500.00 Kč |
| | Keystone záslepka Panduit, NKBMBL-X | 18 | ks | 15.00 Kč | 270.00 Kč |
| | Keystone modul Panduit NK5E88MBLY | 6 | ks | 150.00 Kč | 900.00 Kč |
| | PDU Triton RAB-PD-X11-A1, 7x230V | 1 | ks | 1,700.00 Kč | 1,700.00 Kč |
| | Patch cord Panduit UTPCH1Y (šedý, 0.3m) | 6 | ks | 150.00 Kč | 900.00 Kč |
| | Patch cord Panduit UTPCH1YLY (žlutý, 0.3m) | 1 | ks | 150.00 Kč | 150.00 Kč |
| | Patch cord Panduit UTPCH2RDY (červený, 0.6m) | 1 | ks | 180.00 Kč | 180.00 Kč |
| | Legrand DLPlus instalační lišta 30017, 32x20mm | 30 | m | 80.00 Kč | 2,400.00 Kč |
| | Legrand DLPlus, spojka krytu přímá 33604 | 40 | ks | 25.00 Kč | 1,000.00 Kč |
| | Legrand DLPlus vnitřní/vnější variabilní roh 30271 | 5 | ks | 45.00 Kč | 225.00 Kč |
| | Legrand DLPlus plochý roh 30273 | 6 | ks | 70.00 Kč | 420.00 Kč |
| | Legrand DLPlus koncový díl (záslepka) 31209 | 3 | ks | 50.00 Kč | 150.00 Kč |
| | Legrand DLPlus zásuvkový adaptér na konec lišty 31646 | 1 | ks | 60.00 Kč | 60.00 Kč |
| | Legrand DLPlus zásuvkový adaptér 31707 | 3 | ks | 70.00 Kč | 210.00 Kč |
| | Legrand DLPlus zásuvkový rámeček pro 2 moduly 31611 | 4 | ks | 140.00 Kč | 560.00 Kč |
| | Legrand záslepka Mosaic, 1 modul 77070 | 2 | ks | 30.00 Kč | 60.00 Kč |
| | Legrand RJ45 modul Mosaic 76561 | 6 | ks | 270.00 Kč | 1,620.00 Kč |
| | Patch cord Panduit UTPCH4Y (šedý, 1.2m) | 6 | ks | 150.00 Kč | 900.00 Kč |
| | Patch cord Panduit UTPCH8Y (šedý, 2.4m) | 6 | ks | 200.00 Kč | 1,200.00 Kč |
| | Patch cord Panduit UTPCH12Y (šedý, 3.6m) | 6 | ks | 240.00 Kč | 1,440.00 Kč |
| | Patch cord Panduit UTPCH15Y (šedý, 4.6m) | 6 | ks | 300.00 Kč | 1,800.00 Kč |
| | UTP kabel Belden 1583E | 60 | m | 4.70 Kč | 282.00 Kč |

| | |
|---|---|
| **Jednorázová platba při zavedení pobočky bez DPH** | 36,027.00 Kč |
| **Měsíční platba se závazkem na dva roky bez DPH** | 4,000.00 Kč |
| **Celková cena za dva roky provozu bez DPH** | 132,027.00 Kč |

# Příloha č. 10: Náklady projektu – pobočka Zlín

| | Název položky | Počet | M.j. | Cena za m.j bez DPH | Celková cena za uvedený počet bez DPH |
|---|---|---|---|---|---|
| **Měsíční platba** | Managed LAN (Pronájem switche a jeho správa, závazek 2 roky) | 1 | ks | 3,000.00 Kč | 3,000.00 Kč |
| | Profesionální internet (MPLS IP VPN, závazek 2 roky) | 1 | ks | 1,000.00 Kč | 1,000.00 Kč |
| **Jednorázová platba** | Fortinet FortiAP 221E | 1 | ks | 13,000.00 Kč | 13,000.00 Kč |
| | Datový rozvaděč Triton RUA-09-AS5 | 1 | ks | 3,600.00 Kč | 3,600.00 Kč |
| | 19" Rack police Triton RAX-UP-350-A1, h. 350mm | 1 | ks | 500.00 Kč | 500.00 Kč |
| | Patch panel 1U 24 port, Panduit KP24WSBL | 1 | ks | 2,500.00 Kč | 2,500.00 Kč |
| | Keystone záslepka Panduit, NKBMBL-X | 18 | ks | 15.00 Kč | 270.00 Kč |
| | Keystone modul Panduit NK5E88MBLY | 6 | ks | 150.00 Kč | 900.00 Kč |
| | PDU Triton RAB-PD-X11-A1, 7x230V | 1 | ks | 1,700.00 Kč | 1,700.00 Kč |
| | Patch cord Panduit UTPCH1Y (šedý, 0.3m) | 6 | ks | 150.00 Kč | 900.00 Kč |
| | Patch cord Panduit UTPCH1YLY (žlutý, 0.3m) | 1 | ks | 150.00 Kč | 150.00 Kč |
| | Patch cord Panduit UTPCH2RDY (červený, 0.6m) | 1 | ks | 180.00 Kč | 180.00 Kč |
| | Legrand DLPlus instalační lišta 30017, 32x20mm | 25 | m | 80.00 Kč | 2,000.00 Kč |
| | Legrand DLPlus, spojka krytu přímá 33604 | 25 | ks | 25.00 Kč | 625.00 Kč |
| | Legrand DLPlus vnitřní/vnější variabilní roh 30271 | 2 | ks | 45.00 Kč | 90.00 Kč |
| | Legrand DLPlus plochý roh 30273 | 3 | ks | 70.00 Kč | 210.00 Kč |
| | Legrand DLPlus odbočka T 30274 | 1 | ks | 80.00 Kč | 80.00 Kč |
| | Legrand DLPlus koncový díl (záslepka) 31209 | 2 | ks | 50.00 Kč | 100.00 Kč |
| | Legrand DLPlus zásuvkový adaptér na konec lišty 31646 | 1 | ks | 60.00 Kč | 60.00 Kč |
| | Legrand DLPlus zásuvkový adaptér 31707 | 3 | ks | 70.00 Kč | 210.00 Kč |
| | Legrand DLPlus zásuvkový rámeček pro 2 moduly 31611 | 4 | ks | 140.00 Kč | 560.00 Kč |
| | Legrand záslepka Mosaic, 1 modul 77070 | 2 | ks | 30.00 Kč | 60.00 Kč |
| | Legrand RJ45 modul Mosaic 76561 | 6 | ks | 270.00 Kč | 1,620.00 Kč |
| | Patch cord Panduit UTPCH4Y (šedý, 1.2m) | 6 | ks | 150.00 Kč | 900.00 Kč |
| | Patch cord Panduit UTPCH8Y (šedý, 2.4m) | 6 | ks | 200.00 Kč | 1,200.00 Kč |
| | Patch cord Panduit UTPCH12Y (šedý, 3.6m) | 6 | ks | 240.00 Kč | 1,440.00 Kč |
| | Patch cord Panduit UTPCH15Y (šedý, 4.6m) | 6 | ks | 300.00 Kč | 1,800.00 Kč |
| | UTP kabel Belden 1583E | 60 | m | 4.70 Kč | 282.00 Kč |
| | **Jednorázová platba při zavedení pobočky bez DPH** | 34,937.00 Kč | | | |
| | **Měsíční platba se závazkem na dva roky bez DPH** | 4,000.00 Kč | | | |
| | **Celková cena za dva roky provozu bez DPH** | 130,937.00 Kč | | | |