VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH A KONFIGURACE REDUNDANTNÍ ZABEZPEČENÉ WAN SÍTĚ PROSTŘEDNICTVÍM INTERNETU PRO ZDRAVOTNICKOU ZÁCHRANNOU SLUŽBU

DESIGN AND CONFIGURATION OF A REDUNDANT SECURE WAN NETWORK FOR MEDICAL EMERGENCY SERVICE

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Michal Pinčák**
AUTHOR

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

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Michal Pinčák**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2017/18

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 a konfigurace redundantní zabezpečené WAN sítě prostřednictvím internetu pro zdravotnickou záchrannou službu

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 2017/18

V Brně dne 28.2.2018

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Cieľom tejto diplomovej práce je vytvorenie návrhu redundantnej zabezpečenej VPN WAN siete pre Zdravotnícku záchrannú službu Pardubického kraja. Východiskom práce je analýza súčasného stavu firemnej počítačovej siete, ktorý bol vyhodnotený ako plne nevyhovujúci. Výsledkom je návrh WAN siete, ktorá splňuje požiadavky spoločnosti. Tento návrh je doplnený o projekt implementácie a finančné zhodnotenie daného projektu.

Abstract

The objective of this thesis is creating a design of a redundant secure VPN WAN network for Medical Emergency Service of Pardubice region. The starting point of this thesis is the analysis of the current state of the corporate computer network, which was evaluated as not satisfying. The result is a design of WAN network, which satisfies the requirements of the investor. The solution also includes the project of implementation and financial calculation of the project.

Kľúčové slová

Počítač, počítačová sieť, internet, topológia siete, redundancia, konfigurácia routrov

Keywords

Computer, computer network, internet, network topology, redundancy, router configuration

Bibliografická citácia

PINČÁK, M. *Návrh a konfigurace redundantní zabezpečené WAN sítě prostřednictvím internetu pro zdravotnickou záchrannou službu.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 100 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D.

Čestné prehlásenie

Prehlasujem, že predložená bakalárska práca je pôvodná a spracoval som ju samostatne. Prehlasujem, že citácie použitých prameňov sú úplné, že som vo svojej práci neporušil autorské práva (v zmysle Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brne, dňa

.....

Podpis

Poďakovanie

Na tomto mieste by som chcel poďakovať vedúcemu mojej diplomovej práce Ing. Viktorovi Ondrákovi, Ph.D. za jeho rady a ochotu. Poďakovanie patrí tiež Ing. Jiřímu Koutnému za sprístupnenie materiálov potrebných k vypracovaniu tejto práce a odborné rady.

OBSAH

ÚVOD 9
1 CIELE PRÁCE 10
2 ANALÝZA SÚČASNÉHO STAVU 11
2.1 Informácie o zvolenej firme 11
2.1.1 Základné informácie o firme 11
2.2 Organizačná štruktúra 12
2.2.1 Krajské zdravotnícke operačné stredisko (KZOS) 12
2.2.2 Výjazdové stanovištia 13
2.3 Topológia súčasnej siete 13
2.4 Využívanie počítačovej siete 15
2.5 Požiadavky investora 16
2.6 Prieskum trhu internetových poskytovateľov 16
2.6.1 Poskytovatelia pevného internetového pripojenia 17
2.6.2 Poskytovatelia LTE internetového pripojenia 18
3 TEORETICKÉ VÝCHODISKÁ PRÁCE 20
3.1 Počítačová sieť 20
3.2 Referenčný model ISO/OSI 20
3.2.1 Fyzická vrstva 20
3.2.2 Linková vrstva 21
3.2.3 Sieťová vrstva 21
3.2.4 Transportná vrstva 21
3.2.5 Relačná vrstva 21
3.2.6 Prezentačná vrstva 22
3.2.7 Aplikačná vrstva 22

3.2.8 Komunikácia medzi vrstvami referenčného modelu ISO/OSI 22
3.3 Architektúra TCP/IP 22
3.3.1 Vrstva sieťového rozhrania 23
3.3.2 Sieťová vrstva 23
3.3.3 Transportná vrstva 24
3.3.4 Aplikačná vrstva 24
3.4 Aktívne prvky 28
3.4.1 Switch (prepínač) 28
3.4.2 Router (smerovač) 29
3.4.3 Firewall 29
3.5 Routing (smerovanie) 30
3.5.1 Statické smerovanie 30
3.5.2 Dynamické smerovanie 31
3.5.3 Smerovacie protokoly 31
3.5.4 Smerovacie algoritmy 31
3.5.5 Smerovací protokol EIGRP 32
3.6 Virtuálne privátne siete (VPN) 33
3.6.1 Typy VPN 33
3.6.2 Základné prvky VPN sietí 35
3.6.3 Adresácia vo VPN sieťach 35
3.6.4 Tunely 35
3.6.5 Šifrovanie 36
3.7 IPSec 37
3.7.1 Bezpečnostné asociácie 38
3.7.2 Protokol AH (Authentication Header) 39
3.7.3 Protokol ESP (Encapsulating Security Paylaod) 39

3.7.4 Režimy IPSec 39
3.8 Dynamic Multipoint VPN (DMVPN) 40
3.8.1 Multipoint GRE (mGRE) 41
3.8.2 Protokol NHRP 43
3.9 Protokol HSRP 44
4 VLASTNÝ NÁVRH RIEŠENIA 46
4.1 Topológia siete 46
4.2 Výber internetových poskytovateľov 49
4.3 Výber konkrétneho typu routrov 50
4.3.1 Centrálna lokalita 50
4.3.2 Vzdialené lokality 51
4.4 Konfigurácia routrov v centrálnej lokalite 52
4.4.1 Základná konfigurácia 52
4.4.2 IPSec 54
4.4.3 Konfigurácia tunelu 55
4.4.4 EIGRP 56
4.4.5 Access Control lists (ACL) 57
4.4.6 HSRP 58
4.5 Konfigurácia routrov vo vzdialených lokalitách 58
4.5.1 Základná konfigurácia 59
4.5.2 DHCP 59
4.5.3 IPSec 59
4.5.5 IP inspect 60
4.5.6 Access Control Lists (ACL) 61
4.5.7 EIGRP 62
4.5.8 NAT 63

4.5.9 HSRP 63
4.6 Adresný plán 63
4.7 Monitoring 64
4.7.1 Monitoring funkčnosti zariadení a spojení 64
4.7.2 Monitorovanie záťaže a objemu prenášaných dát 64
4.7.3 Zber a archivácia logov 65
4.7.4 Zálohovanie a archivácia konfigurácií aktívnych prvkov 66
4.7.5 Činnosti spojené s monitoringom siete 66
4.8 Projekt nasadenia 67
4.8.1 Analýza proveditelnosti 67
4.8.2 Analýza rizík 67
4.8.3 Časová analýza 70
4.8.4 Prechod na nový systém 72
4.8.5 Finančné zhodnotenie 72
ZÁVER 75
ZOZNAM POUŽITÝCH ZDROJOV 76
ZOZNAM OBRÁZKOV 78
ZOZNAM TABULIEK 78
ZOZNAM SKRATIEK 79
ZOZNAM PRÍLOH 81

ÚVOD

V súčasnej dobe je využívanie prvkov počítačových sietí ku svojej každodennej činnosti pre veľkú väčšinu firiem nevyhnutnosťou. To platí aj pre mnou zvolenú firmu. V prípade Zdravotníckej záchrannej služby je významným faktorom aj spoľahlivosť počítačovej siete, nakoľko ZZS musí fungovať nepretržite. Nemenej podstatným je aj faktor bezpečnosti siete, pretože WAN sieťou tejto spoločnosti sú posielané citlivé a osobné údaje.

Predmetom mojej diplomovej práce je vytvorenie návrhu danej siete spôsobom, ktorý bude splňovať požiadavky definované vedením zvolenej spoločnosti. Konkrétne sa jedná o návrh topológie danej siete, výber vhodných poskytovateľov internetového pripojenia pre jednotlivé lokality, konfiguráciu aktívnych prvkov a návrh systému monitoringu tejto novo vytvorenej siete. Súčasťou práce je tiež projekt implementácie navrhnutého riešenia, ktorý obsahuje analýzu proveditelnosti, rizík, časovú analýzu a finančné zhodnotenie nákladov a prínosov daného riešenia WAN siete.

1 CIELE PRÁCE

Cieľom mojej práce je vytvorenie návrhu VPN WAN siete pre zdravotnícku záchrannú službu Pardubického kraja. Cieľom práce je, aby daná sieť splňovala požiadavky definované vedením spoločnosti a aby boli odstránené nedostatky týkajúce sa predovšetkým miery redundancie, ktoré má súčasná sieť.

2 ANALÝZA SÚČASNÉHO STAVU

Táto časť mojej diplomovej práce obsahuje základné a kontaktné informácie o zvolenej spoločnosti a jej organizačnej štruktúre. Následne je analyzovaný súčasný stav WAN siete, jej topológia a rýchlosť pripojenia jednotlivých lokalít. V ďalšej časti tejto kapitoly sú stručne popísané hardwarové aj softwarové prostriedky, ktoré daná firma ku svojej činnosti používa. V závere sú formulované požiadavky investora na návrh WAN siete a je realizovaný prieskum trhu internetových poskytovateľov.

2.1 Informácie o zvolenej firme

Pre vypracovanie mojej diplomovej práce som si zvolil firmu Zdravotnícka záchranná služba Pardubického kraja (ZZS PAK).

2.1.1 Základné informácie o firme

- **názov**: Zdravotnícka záchranná služba Pardubického kraja,
- **právna forma**: príspevková organizácia,
- **zriaďovateľ**: Pardubický kraj (5).

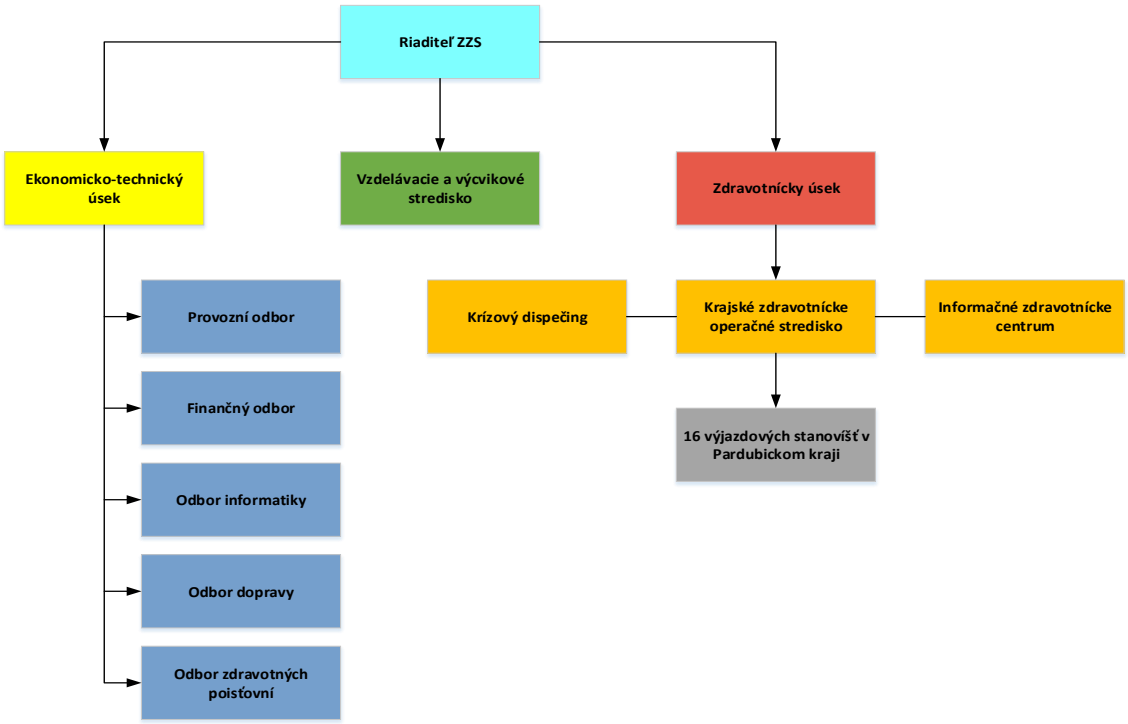
Hlavnou činnosťou ZZS PAK je prednemocničná neodkladná starostlivosť o postihnuté osoby na mieste úrazu alebo náhleho ochorenia a v priebehu ich transportu k ďalšiemu odbornému ošetreniu v zdravotníckom zariadení. Ďalšou činnosťou firmy je sústavné vzdelávanie lekárskych aj nelekárskych zamestnancov, pracovníkov ostatných zložiek integrovaného záchranného systému, odbornej aj laickej verejnosti v oblasti zdravotníctva a poskytovanie informácií verejnosti pri menej akútnych prípadoch prostredníctvom informačného zdravotníckeho centra (5).

Kontaktné údaje

- **Web:** www.zzspak.cz
- **Email:** zzspak@zzspak.cz
- **Telefón:** +420 466 034 107

2.2 Organizačná štruktúra

Najvyšším predstaviteľom ZZS PAK je riaditeľ ZZS. Táto firma sa ďalej delí na 3 časti (ekonomicko-technický úsek, zdravotnícky úsek a vzdelávacie a výcvikové stredisko). Pod zdravotnícky úsek patria jednotlivé výjazdové strediská, krajské zdravotnícke operačné stredisko (KZOS), informačné zdravotnícke centrum a záložný krízový dispečing. Ekonomicko- technický úsek sa delí na odbor dopravy, informatiky, zdravotných poisťovní, provozný a finančný odbor. Organizačná štruktúra ZZS PAK je znázornená na nasledujúcom obrázku (5).



Obr. 1: Organizačná štruktúra (vlastné spracovanie)

2.2.1 Krajské zdravotnícke operačné stredisko (KZOS)

Krajské operačné stredisko ZZS PAK sídli v Pardubiciach a jeho hlavnou činnosťou je riadenie a koordinácia jednotlivých výjazdových skupín v rámci celého Pardubického kraja. Súčasťou KZOS je aj krízový dispečing v meste Chrudim, ktorý slúži pre prípad nutnosti odstavenia KZOS, kedy preberá jeho funkciu. Doplnkovou časťou strediska je

tiež informačné zdravotnícke centrum, ktoré je určené na poskytovanie informácií v prípadoch, ktoré sú menej akútne (5).

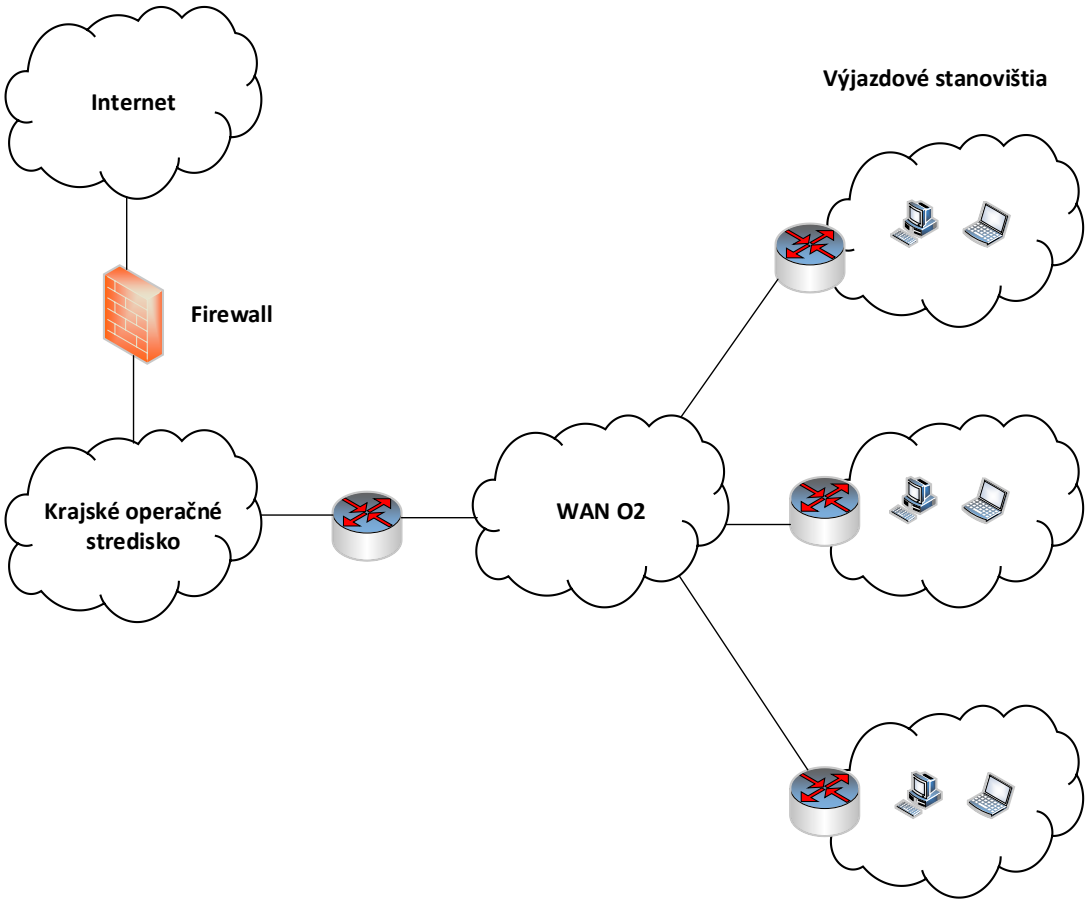
2.2.2 Výjazdové stanovištia

V rámci Pardubického kraja sa momentálne nachádza 16 výjazdových stanovíšť, z ktorých výjazdové skupiny vychádzajú k jednotlivým prípadom. Konkrétne sa jedná o nasledujúce lokality:

- Pardubice – Průmyslová,
- Pardubice – Teplého,
- Holice,
- Prelouč,
- Chrudim,
- Hlinsko,
- Skuteč,
- Svitavy,
- Litomyšl,
- Moravská Třebová,
- Polička,
- Ústí nad Orlicí,
- Červená Voda,
- Žamberk,
- Vysoké Mýto,
- Lanškroun (5).

2.3 Topológia súčasnej siete

Krajské operačné stredisko je s jednotlivými výjazdovými strediskami v Pardubickom kraji spojené WAN sieťou pod správou poskytovateľa - spoločnosti O2. Na KZOS, aj na výjazdových strediskách sú použité routre Cisco. KZOS je do siete internet pripojené cez firewall. Topológia WAN siete je znázornená na nasledujúcom obrázku. Znázornený spôsob pripojenia platí pre všetkých 16 výjazdových stanovíšť.



Obr. 2: Topológia súčasnej siete (vlastné spracovanie)

V rámci WAN siete od O2 je poskytovaná služba VPN Expres Lite, cez ktorú sú jednotlivé lokality pripojené pomocou asymetrického spoja. Na pripojenie je využitá ADSL prípojka, ktorá má pevnú IP adresu. Nad touto prípojkou je definovaný IP Sec tunel, ktorý prepája jednotlivé lokality s centrálou.

Vo väčšine lokalít je využívaná služba VPN Expres Lite 8M, ktorá poskytuje pripojenie do VPN s rýchlosťou 8 Mbit/s. Prvou výnimkou je lokalita Pardubice-Pardubičky, kde bola rýchlosť pripojenia zvýšená na 14 Mbit/s. Druhou z výnimiek je lokalita Chrudim, kde je rýchlosť pripojenia naopak nižšia - 2 Mbit/s. Prehľad lokalít spolu s poskytovanými službami znázorňuje nasledujúca tabuľka.

Tab. 1: Rýchlosť pripojenia do WAN (vlastné spracovanie)

Lokalita	Poskytovaná služba	Rýchlosť pripojenia do VPN
Moravská Třebová	VPN Express Lite	8 Mbit/s
Lanškroun	VPN Express Lite	8 Mbit/s
Holice	VPN Express Lite	8 Mbit/s
Červená voda	VPN Express Lite	8 Mbit/s
Přelouč	VPN Express Lite	8 Mbit/s
Žamberk	VPN Express Lite	8 Mbit/s
Litomyšl	VPN Express Lite	8 Mbit/s
Pardubice- Teplého	VPN Express Lite	8 Mbit/s
Svitavy	VPN Express Lite	8 Mbit/s
Vysoké Mýto	VPN Express Lite	8 Mbit/s
Ústí nad Orlicí	VPN Express Lite	8 Mbit/s
Skuteč	VPN Express Lite	8 Mbit/s
Hlinsko	VPN Express Lite	8 Mbit/s
Polička	VPN Express Lite	8 Mbit/s
Pardubice- Průmyslová	Internet Business 14M Pro	14 Mbit/s
Chrudim	Internet Business 2M Pro	2 Mbit/s

2.4 Využívanie počítačovej siete

Všetci zamestnanci ZZS PAK využívajú k svojej práci nejaké koncové uzly počítačovej siete. Operátori dispečingu využívajú hlavne telefóny a počítače, v prípade núdze tiež tablety. Posádky sanitiek využívajú tablety a tlačiarne umiestnené priamo v sanitkách. Management, oddelenie informatiky a ekonomickí pracovníci taktiež využívajú telefóny, počítače a tlačiarne.

ZZS PAK používa ku svojej činnosti predovšetkým informačný systém SOS. Medzi ďalšie aplikácie, ktoré sú zamestnancami využívané patrí dochádzkový systém , intranet, zdieľanie súborov a elektronické karty pacientov.

Pomocou informačného systému SOS môže ZZS vykonávať všetky činnosti, ktoré potrebuje ku svojej efektívnej práci. Medzi funkcie tohto systému patrí napríklad zaznamenávanie prichádzajúcich hovorov, určovanie polohy volajúceho podľa mobilnej siete, zvolávanie zamestnancov, sledovanie polohy a stavu jednotlivých vozidiel záchrannej služby alebo zasielanie správ s potrebnými údajmi o výjazdoch posádkam vozidiel. Informačný systém SOS zasiela dáta o výjazdoch do jednotlivých stanovíšť, k čomu je využívaná zabezpečená WAN sieť.

WAN sieťou sú taktiež posielané aj údaje o jednotlivých pacientoch pre elektronické karty pacientov.

2.5 Požiadavky investora

ZZS Pardubického kraja požaduje vybudovanie redundantnej WAN siete realizovanej prostredníctvom internetu s patričným stupňom zabezpečenia. Návrh tejto siete by mal spĺňať nasledujúce požiadavky:

- realizácia WAN siete prostredníctvom pripojenia do verejnej siete internet pomocou zabezpečených protokolov,
- realizácia WAN siete spôsobom, ktorý by nebol závislý na jednom poskytovateľovi – aby jednotlivé lokality mohli využívať služby rôznych operátorov a neboli viazané na O2,
- zavedenie dvoch vzájomne nezávislých vstupov internetu v centrálnej lokalite (v krajskom operačnom stredisku),
- konfigurácia dvoch nezávislých pripojení vo všetkých lokalitách (výjazdové stanovištia) s automatickým prepínaním provozu podľa dostupnosti jednotlivých pripojení.

2.6 Prieskum trhu internetových poskytovateľov

V tejto podkapitole sú popísané informácie získané z prieskumu poskytovateľov internetového pripojenia v jednotlivých lokalitách. Z údajov tohto prieskumu budú následne vo fáze návrhu zvolení najvhodnejší poskytovatelia pre jednotlivé lokality.

V rámci prieskumu trhu boli porovnávaní poskytovatelia, ktorých služby majú pokrytie v Pardubickom kraji. V prvej časti prieskumu trhu internetových poskytovateľov boli skúmané možnosti pripojenia prostredníctvom ADSL alebo VDSL technológie. V druhej

časti prieskumu boli analyzovaní poskytovatelia bezdrôtového pripojenia pomocou technológie LTE. Pre ADSL alebo VDSL pripojenie sa jedná o nasledujúce firmy:

- Avonet,
- Vodafone,
- Metronet,
- Wia,
- UPC.

V nasledujúcich podkapitolách sú uvedené možnosti internetového pripojenia, ktoré poskytujú jednotlivé firmy v lokalitách, kde má Zdravotnícka záchranná služba Pardubického kraja svoje výjazdové stanovištia. Výsledky prieskumu trhu poskytovateľov internetového pripojenia sú zhrnuté v tabuľke, ktorá je uvedená v prílohe 19. V tabuľke v prílohách je vždy uvedená varianta pripojenia s najvyššou prenosovou rýchlosťou, ktorá je v danej lokalite od daného poskytovateľa dostupná.

2.6.1 Poskytovatelia pevného internetového pripojenia

Avonet

Firma Avonet poskytuje internetové pripojenie DSL s 3 variantami prenosových rýchlostí:

- 20 Mbit/s download a 2 Mbit/s upload,
- 50 Mbit/s download a 5 Mbit/s upload,
- 100 Mbit/s download a 10 Mbit/s upload.

Vodafone

Spoločnosť Vodafone poskytuje nasledovné 3 varianty pripojenia k internetu (jedná sa o ADSL alebo VDSL pripojenie):

- 20 Mbit/s
- 50 Mbit/s
- 100 Mbit/s

Metronet

Metronet umožňuje internetové pripojenie v rámci celej ČR, teda aj v rámci celého Pardubického kraja. Jedná sa o ADSL alebo VDSL pripojenie. Na výber sú nasledujúce možnosti:

- 50 Mbit/s download, 5 Mbit/s upload,
- 100 Mbit/s download, 10 Mbit/s upload,
- 250 Mbit/s download, 25 Mbit/s upload.

UPC

Spoločnosť UPC ponúka internetové pripojenie s technológiou ADSL alebo VDSL s nasledujúcimi možnosťami:

- 50 Mbit/s download, 20 Mbit/s upload,
- 150 Mbit/s download, 20 Mbit/s upload,
- 300 Mbit/s download, 20 Mbit/s upload.

Mimo uvedených služieb firma ponúka aj optické pripojenie k internetu pre firmy – služba Fiber Bussiness. Táto služba však nemá pokrytie vo všetkých požadovaných lokalitách.

Wia

Wia poskytuje 4 možnosti internetového pripojenia s technológiou buď ADSL, alebo VDSL:

- 8 Mbit/s download, 8 Mbit/s upload,
- 20 Mbit/s downlaod, 2 Mbit/s upload,
- 50 Mbit/s download, 5 Mbit/s upload,
- 100 Mbit/s download, 10 Mbit/s upload.

2.6.2 Poskytovatelia LTE internetového pripojenia

Z firiem, ktoré poskytujú bezdrôtové LTE pripojenie k internetu, boli pre túto analýzu vybrané spoločnosti T-mobile, O2 a Vodafone.

T-mobile

Spoločnosť T-mobile poskytuje LTE pripojenie vo všetkých lokalitách, v ktorých má ZZS Pardubického kraja svoje výjazdové stanovištia. Poskytované sú 3 varianty pripojenia pomocou LTE, ktoré sa líšia prenosovou rýchlosťou:

- 20 Mbit/s,
- 50 Mbit/s,
- 100 Mbit/s.

Vodafone

Spoločnosť Vodafone tiež poskytuje pokrytie LTE internetom vo všetkých potrebných lokalitách. Vodafone udáva rýchlosť poskytovaného LTE pripojenia až do 335 Mbit/s.

O2

Aj spoločnosť O2 poskytuje pripojenie k LTE internetu vo všetkých lokalitách potrebných pre ZZS Pardubického kraja. LTE internetové pripojenie poskytuje s rýchlosťou 20 Mbit/s.

3 TEORETICKÉ VÝCHODISKÁ PRÁCE

Táto kapitola mojej diplomovej práce obsahuje teoretické východiská, ktoré budú použité pri realizácií návrhu WAN siete pre ZZS Pardubického kraja. V úvode tejto časti sú uvedené základné informácie o počítačových sieťach a ich delení podľa veľkosti. Následne je popísaný referenčný model ISO/OSI, architektúra TCP/IP a aktívne prvky používané v počítačových sieťach (konkrétne routre, switche a firewally).Teoretická časť obsahuje aj popis princípu adresácie v oblasti počítačových sietí a informácie o smerovacích protokoloch, pričom protokol EIGRP je popísaný detailnejšie. Nasledujúca časť kapitoly je venovaná problematike VPN sietí, šifrovania a koncepcii DMVPN. V závere teoretickej časti je popísaný protokol HSRP.

3.1 Počítačová sieť

Počítačová sieť je otvorený systém, ktorý ma deterministické správanie a zaisťuje komunikáciu medzi jednotlivými prvkami siete. Prvky počítačových sietí sa rozdeľujú na sieťovú infraštruktúru a koncové uzly. Sieťovú infraštruktúru je možné ďalej rozdeliť na aktívne a pasívne prvky (11).

3.2 Referenčný model ISO/OSI

Sieťový model ISO/OSI vznikol pre potreby zjednotenia sieťovej komunikácie. Tento model popisuje sieťovú komunikáciu pomocou siedmich vrstiev. Komunikáciu rozdeľuje na jednotlivé čiastkové kroky a popisuje každý z týchto krokov. Každá z vrstiev vykonáva konkrétne funkcie, ktoré zaisťujú komunikáciu v sieti. V tejto hierarchii sú služby nižšej vrstvy využívané vyššou vrstvou a nižšia vrstva svoje služby poskytuje vyššej vrstve. Mechanizmus predávania služieb prebieha vždy iba medzi susednými vrstvami sieťového modelu (10).

3.2.1 Fyzická vrstva

Úlohou prvej vrstvy modelu ISO/OSI je príjem a odosielanie dát. Prenos dát je zaisťovaný pomocou káblov, signálu vysielaného prostredím, alebo pomocou sieťovej karty. Prostredníctvom uvedených prostriedkov prúdia jednotlivé bity v podobe elektrických impulzov. Jednotlivé bity môžu nadobúdať hodnotu buď jedna, alebo nula.

Vo fyzickej vrstve nie je potrebná žiadna forma adresácie, pretože tá ja zaistená vyššími vrstvami (11).

3.2.2 Linková vrstva

V poradí druhou vrstvou sieťového modelu je linková vrstva. Základnou jednotkou prenosu na tejto vrstve je prenosový rámec a adresácia funguje na princípe lokálnych adries. Úloha linkovej vrstvy spočíva v príprave prenášaných dát (rámcov) na prenos. Linková vrstva teda prijíma a odosiela prenosové rámce. Okrem toho taktiež zabezpečuje synchronizáciu na úrovni rámcov, kontrolu cieľových adries jednotlivých rámcov a umožňuje tiež riadenie dátového toku (11).

3.2.3 Sieťová vrstva

Tretia vrstva modelu ISO/OSI umožňuje prenos dát aj medzi systémami, ktoré nie sú priamo susediace. Jednotkou prenosu na sieťovej vrstve je paket, adresácia je založená na globálnych adresách. Táto vrstva sa stará aj o zaistenie vhodnej trasy medzi jednotlivými lokálnymi sieťami (routing) a následné odosielanie paketov týmito trasami (forwarding) (10).

3.2.4 Transportná vrstva

Transportná vrstva zabezpečuje integritu dátových tokov a prenos dát medzi procesmi dvoch komunikujúcich zariadení. Jednotkou prenosu je datagram. Transportná vrstva je schopná detekovať stratu alebo poškodenie paketov a v tomto prípade si tiež dokáže vyžiadať opätovný prenos. V prípade, že pakety nedorazia v správnom poradí, je transportná vrstva schopná ich zoradiť a až následne odovzdať relačnej vrstve. Na úrovni tejto vrstvy modelu ISO/OSI je možné poskytovanie prenosu bez spojenia alebo so spojením. Spojovaný prenos je zaisťovaný protokolom TCP, na nespojovaný prenos je využívaný UDP protokol (10).

3.2.5 Relačná vrstva

Za jednotku prenosu je na tejto vrstve považované jedno spojenie. Úlohou relačnej vrstvy je riadenie interakcie komunikujúcich strán, obnova spojenia v prípade jeho výpadku a oznamovanie výskytu neštandardných stavov. Relačná vrstva umožňuje aj overovanie

užívateľov a zabezpečenie prístupov. Relačná vrstva nepotrebuje žiadnu adresáciu, pretože tá je už dostatočne zaistená nižšími vrstvami (1).

3.2.6 Prezentačná vrstva

Úlohou prezentačnej vrstvy je konverzia prenášaných dát do podoby, ktorá je vyžadovaná aplikačnou vrstvou. Konverzia dát je realizovaná napríklad prostredníctvom šifrovania alebo komprimovania. V prezentačnej vrstve už taktiež nie je potrebná žiadna adresácia a ani jednotka prenosu tu neexistuje (1).

3.2.7 Aplikačná vrstva

Aplikačnú vrstvu tvoria jednotlivé aplikácie, ktoré užívateľom sprístupňujú určité sieťové služby. K týmto službám patrí napríklad elektronická pošta, prenos súborov alebo preklad adries (DNS). Na tejto vrstve už tiež nie je potrebná adresácia a neexistuje ani jednotka prenosu (1).

3.2.8 Komunikácia medzi vrstvami referenčného modelu ISO/OSI

Medzi jednotlivými vrstvami referenčného modelu ISO/OSI prebiehajú dve formy komunikácie – **logická** a **fyzická** komunikácia (3).

Logická komunikácia znamená, že spolu komunikujú rovnocenné vrstvy z dvoch uzlov, pričom medzi nimi nedochádza k fyzickému spojeniu a komunikácia prebieha s využitím služieb nižších vrstiev (3).

Fyzická komunikácia prebieha v situácii, keď existuje aj fyzické spojenie. Tento druh komunikácie prebieha medzi dvoma susediacimi vrstvami jedného uzlu, alebo medzi fyzickými vrstvami dvoch rôznych komunikujúcich uzlov (3).

3.3 Architektúra TCP/IP

Architektúra TCP/IP vzniká použitím protokolu TCP nad protokolom IP. Prenos, ktorý poskytuje protokol IP je nespojovaný a nespoľahlivý. To znamená, že pri prenose dát nie je vytvorené spojenie medzi komunikujúcimi stranami a nie je garantované poradie paketov, ani ich samotné doručenie. Preto je nad IP protokolom použitý protokol TCP, ktorý mení charakter prenosu na spojovaný a spoľahlivý. TCP protokol vytvára spojenie medzi procesmi, v prípade jeho prerušenia zaisťuje obnovenie a tiež zabezpečuje

korektné ukončenie spojenia po dokončení prenosu dát. Spoľahlivosť prenosu je zaisťovaná pomocou riadenia toku dát a ich kontinuálneho potvrdzovania (1).

Model pre architektúru TCP/IP je do značnej miery podobný referenčnému modelu ISO/OSI. Na rozdiel od neho sa skladá len zo 4 vrstiev:

- **aplikačná vrstva** (Application Layer),
- **transportná vrstva** (Transport Layer),
- **sieťová vrstva** (Network Layer),
- **vrstva sieťového rozhrania** (Network Interface) (11).

3.3.1 Vrstva sieťového rozhrania

Najnižšia vrstva modelu architektúry TCP/IP svojimi komunikačnými funkciami odpovedá fyzickej a linkovej vrstve ISO/OSI modelu. Protokoly tejto vrstvy musia umožniť systému doručovanie dát iným systémom, ktoré sú na priamo pripojenej sieti. Medzi úlohy vrstvy sieťového rozhrania patrí aj zapuzdrovanie IP datagramov do prenosových rámcov odpovedajúcich formátov a dĺžok tak, aby tieto rámce ohli byť prenesené daným rozhraním. Táto vrstva je súčasne zodpovedná za mapovanie sieťových (IP) adries na fyzické (väčšinou MAC) adresy (11).

3.3.2 Sieťová vrstva

Sieťová vrstva v architektúre TCP/IP odpovedá sieťovej vrstve modelu ISO/OSI. Funkcie tejto vrstvy zahŕňajú:

- sieťovú adresáciu, smerovanie (routing) a predávanie (forwarding) datagramov (IP protokol a smerovacie protokoly napr. RIP,OSPF, IGRP, EIGRP),
- segmentáciu a zostavovanie datagramov do rámcov a z rámcov nižšej vrstvy (IP protokol),
- riadenie na úrovni sieťovej vrstvy (protokol ICMP),
- skupinové vysielanie (multicast), registráciu do skupín a špecifické smerovacie protokoly pre prenosy typu multicast (protokol IGMP) (1).

IP protokol poskytuje nespojovaný a nespoľahlivý prenos. Každý datagram teda musí niesť informácie o odosielateľovi a príjemcovi. Jednotlivé datagramy musia tiež obsahovať informáciu o poradí v správe, nakoľko sa posielajú nezávisle na sebe a poradie

ich doručenia nemusí odpovedať ich poradiu v správe. Označovanie poradia datagramov je nutné aj pre prípad, že by datagram musel byť fragmentovaný (1).

3.3.3 Transportná vrstva

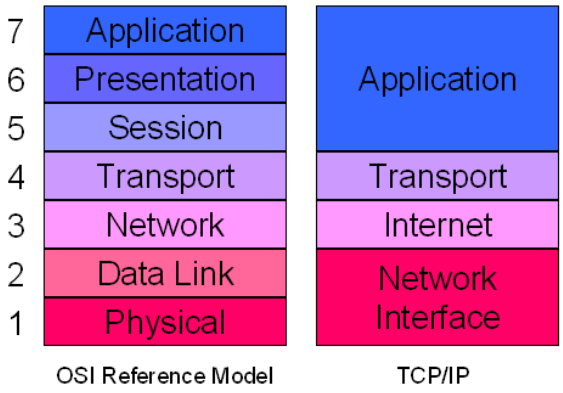
Transportná vrstva architektúry TCP/IP svojou činnosťou odpovedá transportnej vrstve z modelu ISO/OSI. Táto vrstva poskytuje transportnú službu so spojením alebo bez spojenia v závislosti na použitom transportnom protokole (11).

- **TCP protokol –** Poskytuje spojovanú a spoľahlivú transportnú službu. Tento protokol zaisťuje vytvorenie spojenia medzi dvomi protiľahlými procesmi a následne medzi nimi realizuje plne duplexný prenos dát po bytoch. V prípade straty spojenia zabezpečuje jeho obnovenie a tiež umožňuje korektné ukončenie spojenia po prenesení všetkých dát. Spoľahlivosť prenosu je zabezpečovaná pomocou riadenia toku dát a kontinuálneho potvrdzovania. Tým je taktiež zaistené, že poradie odosielaných dát odpovedá poradiu prijatých dát (1).
- **UDP protokol –** Poskytuje nespojovaný a nespoľahlivý prenos. Dáta, ktoré protokol UDP dostáva od sieťovej vrstvy nijakým spôsobom nemení. Výhodou tohto protokolu je, že môže byť použitý aj pre prenosy typu broadcast a multicast, nakoľko nie je naväzované spojenie medzi komunikujúcimi stranami. Protokol UDP je využívaný, keď je potrebná rýchla a efektívna komunikácia, pri ktorej nie je vyžadovaná spoľahlivosť (1).

3.3.4 Aplikačná vrstva

Aplikačná vrstva je najvyššou vrstvou architektúry TCP/IP a svojou funkciou odpovedá relačnej, prezentačnej a aplikačnej vrstve modelu ISO/OSI. Táto vrstva obsahuje protokoly, ktoré užívateľom poskytujú konkrétne aplikácie. Aplikácie podporované aplikačnými protokolmi je možné rozdeliť do dvoch skupín:

- **Užívateľské aplikácie –** Tieto aplikácie sú priamo využívané užívateľmi. Patria sem napríklad Telnet, HTTP, HTTPS, FTP, TFTP, SMTP.
- **Administratívne aplikácie –** Tieto aplikácie podporujú prácu užívateľov v sieti, ale pre užívateľa sú „neviditeľné“. Patria sem napríklad DNS, DHCP, SNMP, NTP, RADIUS (1).



Obr. 3: Porovnanie modelu ISO/OSI a architektúry TCP/IP (9)

3.3.5 IP adresy

Protokol IP verzie 4 využíva na adresáciu jednotlivých zariadení 32 bitové (4 Bytové) IP adresy. Pomocou IP adresy je jednoznačne definované určité sieťové rozhranie systému. Pokiaľ má zariadenie viac sieťových kariet, tým pádom viac sieťových rozhraní, bude mať teda aj niekoľko rôznych IP adries (1).

IP adresa je tvorená 4 Bytmi (32 bitmi) a je zapisovaná tak, že jednotlivé Byty sú oddelené bodkou. Hodnoty jednotlivých Bytov sú obvykle uvádzané v desiatkovej sústave (napr. 192.168.13.1). IP adresa sa delí na dve časti- na adresu siete a adresu uzlu v danej sieti. To, aká časť z IP adresy je adresou siete a adresou uzlu, môže byť uvedené dvomi rôznymi spôsobmi (3).

Prvým z nich je CIDR prefix. Jedná sa o číslo v desiatkovej sústave uvedené za IP adresou a za lomítkom, ktoré vyjadruje počet bitov z danej adresy, ktoré vyjadrujú adresu siete (napr. 147.225.123.66 / 24 znamená, že 24 bitov z uvedenej adresy je adresa siete). Druhým spôsobom je použitie masky siete. Jedná sa o 32 bitové číslo v dvojkovej sústave, kde bity, ktoré vyjadrujú adresu siete majú hodnotu 1 a na bity špecifikujúce adresu uzlu majú hodnotu 0. Maska siete býva uvádzaná v rovnakom formáte ako IP adresa – štyri čísla v desiatkovej sústave oddelené bodkou (napr. 147.225.123.66 255.255.255.0 – opäť vyjadruje, že adresu siete predstavuje 24 bitov z danej IP adresy) (3).

Triedy adries

V minulosti bolo používané delenie IP adries do niekoľkých tried:

- **siete triedy A** – adresa siete mala dĺžku 8 bitov, zvyšných 24 bitov predstavovalo adresu uzlu, to umožňovalo existenciu 256 sietí s veľkým množstvom uzlov v nich (vyše 16 miliónov),
- **siete triedy B** – adresa siete bola 16 bitov dlhá, ďalších 16 bitov bola adresa uzlu, tým pádom bola umožnená existencia 65 536 sietí s 65 536 uzlami v každej z nich,
- **siete triedy C** – adresu siete predstavovalo 24 bitov, adresa uzlu bola len 8 bitová, tým bola umožnená existencia vyše 16 miliónov sietí, z ktorých každá obsahovala 256 uzlov,
- **siete triedy D –** slúžili na skupinovú adresáciu (multicast),
- **siete triedy E** – boli špeciálne siete využívané pre experimentálne účely (2).

Rezervované IP adresy

Nie všetky adresy v rozsahu jednej siete (triedy A až C) označujú stanice, pretože niektoré IP adresy sú rezervované pre špeciálne účely. Jedná sa napríklad o adresy pre skupinové vysielanie (multicast), alebo ladenie komunikačných programov. Jednotlivé rezervované IP adresy spolu s ich významom sú uvedené v nasledujúcej tabuľke (10).

Tab. 2: Rezervované IP adresy (1)

Adresa	Význam
0.0.0.0	Tento počítač na tejto sieti (používané keď počítač ešte nepozná svoju adresu, ale musí komunikovať, môže byť použité len ako zdrojová adresa)
X.0.0.0.0	Adresa celej siete X (napr. 10.0.0.0)
0.0.0.X	Adresa stanice použitá, keď počítač nepozná adresu siete
255.255.255.255	Local broadcast – broadcast v danej sieti
X.255.255.255	Directed broadcast – broadcast, ktorý špecifikuje všetky zariadenia v sieti X
127.0.0.1	Loopback - toto zariadenie

Privátne adresy

Aj napriek vysokému počtu verejných IP adries, začalo postupne dochádzať k ich nedostatku. Z toho dôvodu boli určité rozsahy adresného priestoru vyčlenené. Tieto rozsahy sú označované ako privátne IP adresy. Privátne IP adresy musia splňovať podmienku, že neexistuje rovnaká verejná IP adresa a teda môžu byť použité pre adresovanie napr. interných podnikových alebo domácich sietí, ktoré sú k internetu pripojené prostredníctvom routra, alebo firewallu, ktorý vykonáva preklad adries (NAT). Konkrétne rozsahy privátnych adries uvádza nasledujúca tabuľka (2).

Tab. 3: Rozsahy privátnych IP adries (1)

Rozsah	Popis
10.x.x.x	1 sieť triedy C
172.16.x.x – 172.31.x.x	16 sietí triedy B
192.168.0.x – 192.168.254.x	254 sietí triedy C

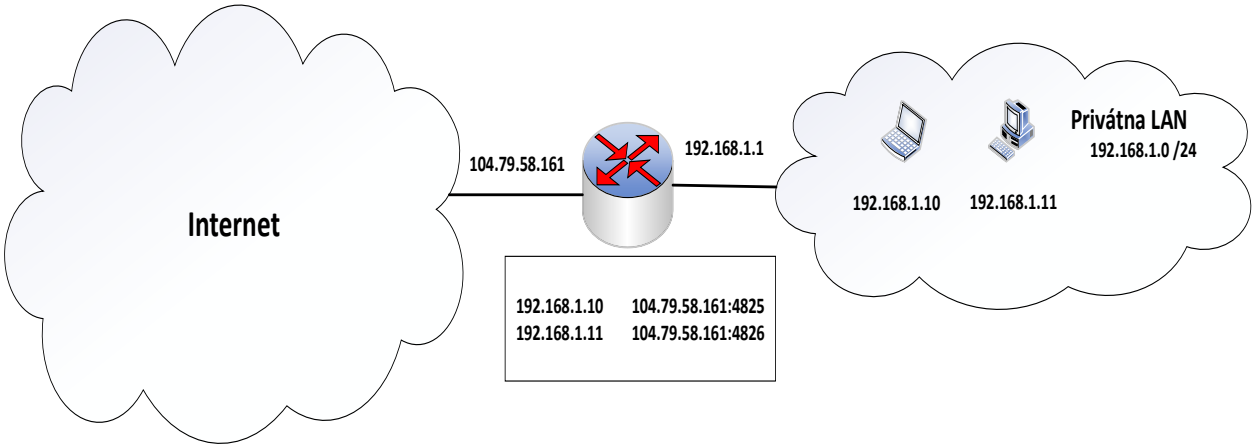
Preklad adries (NAT)

NAT (Network Address Translation) má za úlohu zaistenie komunikácie medzi privátnymi sieťami a internetom. Preklad adries znižuje množstvo unikátnych globálnych IP adries potrebných pre privátne siete (1).

Privátna sieť, ktorá sa pripojuje k internetu pomocou NAT musí mať minimálne jednu globálnu IP adresu. Táto adresa je pridelená na rozhranie routra, ktorý je pripojený do internetu. Tento router následne vykonáva preklad adries v prichádzajúcich aj odchádzajúcich datagramoch. U datagramov, ktoré odchádzajú z privátnej siete smerom do siete internet, nahrádza zdrojovú privátnu IP adresu uvedenú v hlavičke datagramu za svoju globálne platnú IP adresu. V datagramoch prichádzajúcich do privátnej siete zase prepisuje cieľovú adresu, ktorou pôvodne bola globálna adresa routra, na IP adresu konkrétneho zariadenia v privátnej sieti. Každé NAT zariadenie si musí udržovať tabuľku prekladov adries, ktorá obsahuje dvojice záznamov privátna IP adresa zariadenia – IP adresa zariadenia v sieti internet (3).

Keby NAT zariadenie malo len 1 globálne unikátnu IP adresu, mohlo by súčasne s internetom komunikovať len 1 zariadenie z privátnej siete. NAT preto môže k

prekladom využívať určitú množinu globálnych adries (tzv. NAT pool). Efektívnejšou metódou prekladu adries ale je tzv. PAT (Port Address Translation), pri ktorej sa okrem zdrojovej a cieľovej IP adresy využíva aj číslo cieľového portu a číslo portu použité na NAT zariadení. Pri použití PAT teda stačí 1 globálne unikátna IP adresa, prostredníctvom ktorej môže s internetom komunikovať množstvo zariadení z privátnej siete, nakoľko každé pripojenie je špecifikované pomocou čísla portu. Princíp funkcie mechanizmu PAT znázorňuje nasledujúci obrázok (10).



Obr. 4: Princíp prekladu adries mechanizmom PAT (vlastné spracovanie)

3.4 Aktívne prvky

Aktívne prvky sú zariadenia, ktoré umožňujú vzájomnú komunikáciu jednotlivých zariadení v počítačovej sieti. V tejto podkapitole bude popísaná činnosť switchov, routrov a firewallov.

3.4.1 Switch (prepínač)

Switch je aktívny prvok, ktorý pracuje na linkovej vrstve ISO/OSI modelu, aj keď existujú aj varianty switchov, ktoré pracujú na tretej (sieťovej vrstve) – bývajú označované ako L3 switche. Switche prepojujú lokálne siete a zabezpečujú prenos rámcov medzi svojimi portmi na základe MAC adries. Rámce pri prechode switchom nie sú nijakým spôsobom pozmenené, pretože switch nedokáže čítať informácie uvedené v dátovej časti prenosového rámca, ktoré prislúchajú vyšším vrstvám (3).

Switche sa postupne učia MAC adresy zariadení, ktoré sú pripojené k ich jednotlivým portom. Tieto adresy sú uchovávané vo vnútornej pamäti switcha a slúžia ako jednoznačný identifikačný prvok zariadenia. Keď switch dostane prenosový rámec, prehľadáva svoju tabuľku MAC adries a následne odosiela rámec na port, kde je podľa tabuľky pripojené zariadenie s danou adresou. Switche môžu byť rozdelené na manažovateľné a nemanažovateľné. Nemanažovateľné neposkytujú žiadnu možnosť správy alebo monitoringu. Manažovateľné switche je možné spravovať a konfigurovať prostredníctvom protokolov Telnet, SSH, HTTP, alebo HTTPS (1).

3.4.2 Router (smerovač)

Router je aktívny prvok pracujúci na sieťovej vrstve referenčného modelu ISO/OSI. Jeho hlavnými funkciami je smerovanie a odosielanie paketov do počítačových sietí podľa IP adries. Router si uchováva smerovaciu tabuľku (routing table), ktorá obsahuje informácie o dostupných sieťach. Medzi tieto informácie patrí IP adresa siete, maska siete, port routra, ktorý bude použitý pre odoslanie paketov do konkrétnej siete, metrika (určitá hodnota vyjadrujúca vhodnosť danej cesty) a prípadne adresa ďalšieho routra na ceste do danej siete. Práca routra pozostáva z 2 krokov. Prvým krokom je zvolenie optimálnej cesty v sieti (routing) a druhým je odoslanie paketov zvoleným smerom (forwarding) (11).

3.4.3 Firewall

IP protokol verzie 4 neobsahuje v podstate žiadny bezpečnostný mechanizmus, ktorý by chránil sieť pred útokmi z vonku. Z toho dôvodu býva bezpečnosť siete v tomto smere zaisťovaná najčastejšie pomocou firewallu. Firewall ochraňuje internú (napr. podnikovú) počítačovú sieť, pričom nijakým spôsobom negatívne neovplyvňuje fungovanie tejto siete. Úlohou firewallu teda je zabraňovať neoprávnenej komunikácií v preniknutí do internej siete. Taktiež je podstatné, aby všetka oprávnená komunikácia medzi internou sieťou a okolitým svetom cez firewall prechádzala (1).

Medzi funkcie, ktoré môže firewall vykonávať patrí:

- **Filtrovanie paketov** – pôvodne bolo možné pakety filtrovať len na základe zdrojovej a cieľovej IP adresy. V súčasnosti firewally umožňujú taktiež filtráciu na základe informácií protokolov vyšších vrstiev (napr. zdrojové a cieľové porty),

ktoré sú obsiahnuté v dátovej časti paketov. Pre dosiahnutie dostatočného stupňa zabezpečenia siete by malo filtrovanie paketov prebiehať v oboch smeroch (do siete aj von zo siete).

- **Aplikačná brána**- Všetky pakety pre špecifikované aplikácie sú zadržované. Firewall sa v tomto prípade správa ako zástupca aplikačného serveru. Aby bola vonkajšiemu užívateľovi povolená komunikácia so serverom, musí najskôr prebehnúť úspešná autentizácia.
- **Proxy server (zástupný server)**- Proxy server stojí medzi klientom a reálnym serverom v sieti a dokáže využívať filtráciu na základe IP adries, aj na základe aplikácií. Požiadavky, ktoré klient vysiela k serveru sa najskôr dostávajú k proxy serveru. Ten zvažuje, či sú jednotlivé požiadavky oprávnené a rozhoduje o tom, či budú poslané ďalej reálnemu serveru. Proxy server je pre komunikujúce strany transparentný, ale jeho použitie spôsobuje určité spomalenie komunikácie.
- **Riadenie prístupu**- V prvom kroku je využitý určitý autentizačný mechanizmus pre overenie totožnosti užívateľa na základe hesla. V ďalšom kroku je vykonaná autorizácia (overenie oprávnení užívateľa) pre používanie určitých služieb.
- **Šifrovanie komunikácie**- Prenášané dáta môžu byť šifrované, čo zvyšuje bezpečnosť komunikácie. Využívané sú hlavne 2 typy šifrovania – šifrovanie verejným kľúčom a šifrovanie súkromným kľúčom (1).

3.5 Routing (smerovanie)

Smerovanie v počítačových sieťach je možné rozdeliť do 2 skupín na **statické** a **dynamické**.

3.5.1 Statické smerovanie

Pri statickom smerovaní je používaná jediná cesta k cieľovému uzlu, ktorá je manuálne nakonfigurovaná na routri. Router v tomto prípade nemá žiadnu alternatívnu možnosť presmerovania komunikácie. Statické smerovanie býva používané najčastejšie z bezpečnostných dôvodov v situácii, keď je potrebné, aby pakety prechádzali po konkrétnej ceste v sieti. Tento spôsob smerovania býva tiež často využívaný v prípade, že do cieľovej siete existuje jediná cesta. V tomto prípade by použitie dynamického smerovania znamenalo zbytočné zaťaženie routra výpočtami smerovacích algoritmov.

Taktiež by bola výmenou smerovacích informácií zbytočne zaťažovaná sieť. Smerovanie pomocou manuálne zadaných trás môže byť použité v kombinácii s dynamickým smerovaním, pričom má statické smerovanie obvykle prednosť. Prioritu statického smerovania pred dynamickým je však možné zmeniť (3).

3.5.2 Dynamické smerovanie

Pri dynamickom smerovaní je na výber optimálnej trasy v sieti využívaný určitý smerovací algoritmus, ktorý je založený na informáciách, ktoré router získava od ostatných routrov v sieti. Aktuálne smerovacie informácie sa medzi jednotlivými routrami zasielajú buď v pravidelných intervaloch, alebo keď nastane zmena topológie. Dynamické smerovacie protokoly automaticky vyhľadávajú alternatívnu cestu v prípade výpadku spojenia na pôvodne zvolenej ceste (4).

3.5.3 Smerovacie protokoly

Dynamické smerovanie je zabezpečované prostredníctvom smerovacích protokolov. Pre protokol IP existuje viacero možností smerovacích protokolov, ktoré je možné rozdeliť do dvoch skupín:

- **Interné** – zaisťujú smerovanie v rámci administratívnej domény alebo v autonómnom systéme,
- **Externé** – zabezpečujú prenos smerovacích informácií medzi jednotlivými autonómnymi systémami a tiež smerovanie medzi rôznymi kombináciami interných smerovacích protokolov (4).

3.5.4 Smerovacie algoritmy

Dynamické smerovacie protokoly využívajú 2 rôzne typy smerovacích algoritmov:

- **algoritmus vektorov vzdialeností (distance vector),**
- **algoritmus stavu spojov (link state)** (6).

Algoritmus vektorov vzdialeností (distance vector)

Pri použití tohto algoritmu má router pri štarte vo svojej smerovacej tabuľke informácie len o priamo pripojených sieťach. Každý zo záznamov v smerovacej tabuľke obsahuje metriku, ktorá je v tomto prípade počítaná ako počet routrov na ceste do danej siete.

Router v periodických intervaloch posiela susedným routrom svoju routovaciu tabuľku a tiež od nich dostáva kópie ich tabuliek. Router následne porovnáva vzdialenosti do sietí v prijatých tabuľkách so svojou a v prípade, že nájde kratšiu cestu ako bola pôvodná, prepisuje si záznam vo svojej routovacej tabuľke. Tento algoritmus využívajú napríklad smerovacie protokoly RIP, RIP2,IGRP, EIGRP. Použitie algoritmu vektorov vzdialeností znamená nižšiu záťaž na router, ale vyššiu záťaž na sieť (6).

Algoritmus stavu spojov

Pri tomto algoritme je potrebné, aby každý router mal k dispozícií informáciu o topológie siete, prípadne o jej časti (protokol OSPF). Jednotlivé routre si udržujú graf znázorňujúci topológiu siete. Vzájomné prepojenia routrov sú ohodnotené metrikou na základe prenosových vlastností. Router v periodických intervaloch overuje dostupnosť svojich susedov pomocou zasielania krátkych správ. Informácie o stavoch spojov sú vysielané pomocou LSA (Link State Advertisment) všetkým routrom. Tento algoritmus využívajú smerovacie protokoly OSPF a IS-IS. Použitie algoritmu stavu spojov znamená vyššiu záťaž na pamäť a procesor routra, ale nižšiu mieru zaťaženia siete (1).

3.5.5 Smerovací protokol EIGRP

Smerovací protokol EIGRP (Enhanced Interior Gateway Routing Protocol) bol vyvinutý firmou Cisco Systems ako rozšírená verzia staršieho protokolu IGRP. Protokol EIGRP funguje na princípe algoritmu vektorov vzdialeností, ale obsahuje aj niektoré vlastnosti smerovacích protokolov využívajúcich algoritmus stavu spojov. Metrika pre tento protokol je počítaná na základe šírky pásma (bandwidth), oneskorenia (delay) a konštánt (K-values) (6).

Routre využívajúce tento smerovací protokol si vzájomne posielajú tzv. Hello pakety, ktoré sú zasielané v periodických intervaloch (5 sekúnd na rýchlych a 60 sekúnd na pomalých linkách). Tieto pakety sú typu multicast a slúžia na objavovanie susedov, s ktorými sú následne nadväzované vzťahy tzv. susedstvo (adjacency), a na detekovanie nefunkčných routrov. Aby jednotlivé routre mohli byť v adjacency vzťahu, musia byť členmi rovnakého autonómneho systému, musia používať zhodnú verziu protokolu EIGRP a musia mať rozhrania v rovnakej subsieti. Taktiež musia mať zhodné konštanty

pre výpočet metriky (K-values). Jednotlivé routre si udržujú routovacie tabuľky, tabuľky s údajmi o topológii siete a tabuľky svojich susedov (6).

3.6 Virtuálne privátne siete (VPN)

VPN je logická sieť vytvorená prostredníctvom verejnej infraštruktúry (internet alebo verejná IP sieť), ktorá si ale zachováva charakter privátnej siete. Táto sieť poskytuje zabezpečenie prebiehajúcej komunikácie, pričom jej kvalita ostáva nezmenená. Virtuálne privátne siete sú zásadné pre realizáciu zabezpečeného vzdialeného prístupu, keď je potrebné užívateľov pripojujúcich sa napr. z domova jednotne autentizovať a autorizovať ich k využívaniu siete a jej prostriedkov (1).

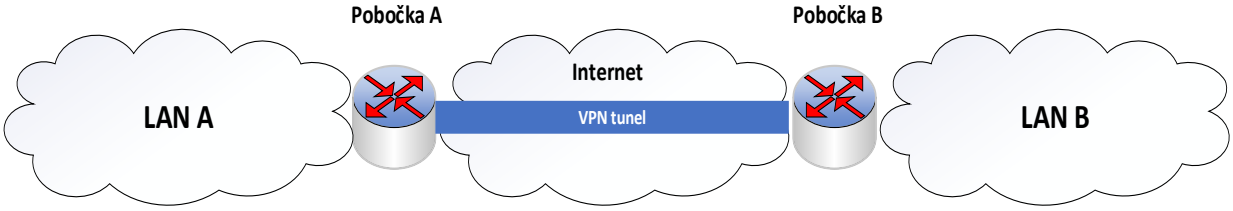
Princíp funkcie VPN sietí spočíva v umiestnení špeciálneho zariadenia (VPN gateway) na hranicu medzi privátnou a verejnou sieťou. Dáta odoslané užívateľom prechádzajú cez VPN gateway, sú následne prenesené verejnou sieťou až k VPN bráne na vzdialenej strane VPN siete, ktorá dáta spracúva pre použitie v cieľovej privátnej sieti. Siete VPN využívajú kombináciu šifrovania, tunelovania, autentizácie a riadenia prístupu pre zabezpečenie prístupu k privátnym sieťam prostredníctvom internetu (4).

3.6.1 Typy VPN

Siete VPN je možné rozdeliť do dvoch skupín: **Site-to-site VPN** a **Remote Access VPN**.

Site-to-site VPN

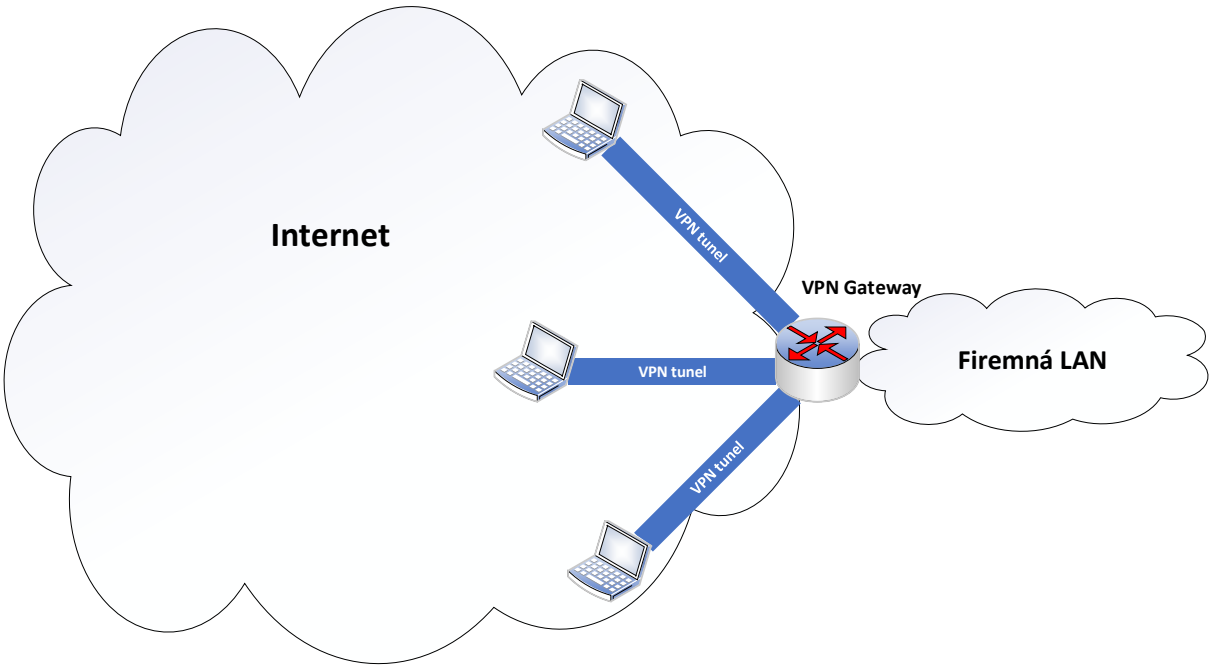
Pri tomto type VPN sú spojované 2 alebo viaceré LAN siete dohromady. Na realizáciu sa používajú špeciálne sieťové zariadenia (napr. firewall, router, server), ktoré slúžia ako VPN gateway a naviažu medzi sebou VPN spojenie. Odchádzajúca komunikácia je zabalená do VPN tunelu a následne odoslaná. Komunikácia, ktorá prichádza je rozbalená a do siete posielaná štandardným spôsobom. Tento spôsob realizácie VPN pripojenia býva využívaný napríklad pri prepojovaní jednotlivých pobočiek medzi sebou alebo s centrálou firmy (1).



Obr. 5: Princíp Site to Site VPN (vlastné spracovanie)

Remote Access VPN (vzdialený prístup)

Tento typ VPN slúži na pripojenie individuálnych vzdialených užívateľov do lokálnej siete. Vzdialený užívateľ musí využívať určitý špeciálny software (VPN klient). Na strane internej siete sa opäť používa VPN gateway, ktorá v tomto prípade musí poskytovať aj funkcie DNS a DHCP. Vyššie nároky bývajú kladené aj na autentizáciu klientov. Pri tomto type VPN spojenia sú často využívané protokoly IPSec alebo SSL (3).



Obr. 6: Princíp Remote Access VPN (vlastné spracovanie)

3.6.2 Základné prvky VPN sietí

Hlavným prvkom vo VPN sieťach sú VPN brány. Ich primárnou úlohou je poskytovanie zabezpečeného prístupu do siete oprávneným užívateľom a súčasne udržanie neoprávnených užívateľov mimo siete. K úlohám VPN brán tiež patrí šifrovanie komunikácie prebiehajúcej medzi sieťami a obvykle aj preklad adries (NAT). Brány VPN musia podporovať rôzne autentizačné mechanizmy (napr. digitálne podpisy, RADIUS) . Ako VPN brány sa obvykle používajú routre alebo firewally, ale môžu byť použité aj špeciálne zariadenia. Podstatné je, aby tieto zariadenia mali aspoň 1 rozhranie pripojené k dôveryhodnej privátnej sieti a aspoň 1 rozhranie pripojené k nedôveryhodnej vonkajšej sieti. Zariadenia použité ako VPN gateway obsahujú potrebný software aj hardware, zatiaľ čo komunikácia cez VPN na klientskych koncových zariadeniach je riešené len softwarom (1).

3.6.3 Adresácia vo VPN sieťach

Keďže VPN brány môžu ukončovať vysoké počty VPN tunelov, existujú rôzne možnosti pre prideľovanie adries jednotlivým klientom. Brány obvykle podporujú viac z uvedených možností (1) :

- **Statické prideľovanie IP adries –** pre každého klienta je rezervovaná 1 statická IP adresa,
- **Dynamické prideľovanie IP adries –** adresy sú klientom prideľované dynamicky (DHCP serverom), to znamená, že klient pri opätovnom pripojení môže dostať pridelenú vždy inú adresu,
- **Klientsky definované IP adresy –** IP adresa je špecifikovaná samotným klientom (3).

Výber metódy, ktorou bude prideľovanie adries v sieti prebiehať obvykle záleží predovšetkým na veľkosti adresného priestoru, ktorý ma konkrétna sieť k dispozícii (3).

3.6.4 Tunely

Virtuálne privátne siete využívajú mechanizmus tunelovania na vytvorenie dvojbodového logického spojenia medzi koncovými klientskymi sieťami, ktorý býva označovaný pojmom tunel. VPN sa realizuje pomocou tunelov vytváraných cez verejné

siete. Datagramy prenášané týmito tunelmi sú chránené proti útokom zvonku. Tunel je jednoznačne definovaný svojím vstupným a výstupným bodom a mechanizmom, pomocou ktorého sú pakety prenášané tunelom. Koncové body obvykle zabezpečujú autentizáciu, riadenie prístupu a dojednávanie ďalších bezpečnostných služieb (1).

Tunelovanie paketov znamená, že pôvodný paket je vložený do novo vytvoreného paketu. Tým pádom zostáva obsah pôvodného paketu nečitateľný pre transportnú sieť počas celého prenosu tunelom. Tunelovanie paketov môže prebiehať na vrstve L2 alebo L3 (4).

Tunelovanie na druhej vrstve

Tunelovanie na vrstve L2 využíva služby protokolu PPP, na ktorom sú založené protokoly tejto vrstvy. V oblasti VPN sietí sú využívané hlavne nasledujúce schopnosti protokolu PPP- dynamická adresácia klientov, autentizácia užívateľov, šifrovanie a kompresia dát a management šifrovacích kľúčov. Pri tunelovaní na druhej vrstve je najčastejšie využívaný protokol **L2TP** (Layer 2 Tunneling Protocol) alebo mechanizmus **GRE** (Generic Route Encapsulation) (4).

Tunelovanie na tretej vrstve

Pri tunelovaní na vrstve L3 je využívaný mechanizmus zapuzdrovania pôvodného IP datagramu do novo vytvoreného IP datagramu. Konfigurácia tunelov sa vykonáva vopred a obvykle manuálne. Autentizácia užívateľov prebieha buď v rámci L3VPN, alebo je požadovaná autentizácia komunikujúcich strán ešte pred zostavením tunelu. Ako bezpečnostný mechanizmus býva zvyčajne využívaný **IPSec**. Realizácia VPN na vrstve L3 predpokladá, že zákazník prenecháva dohľad nad vlastnou VPN sieťou poskytovateľovi VPN (1).

3.6.5 Šifrovanie

Pre zaistenie utajenia dát prenášaných prostredníctvom VPN sietí je používaný mechanizmus šifrovania. Šifrovanie býva realizované dvomi hlavnými spôsobmi: **verejným** alebo **súkromným** kľúčom (1).

Šifrovanie súkromným kľúčom (private key)

Šifrovanie súkromným kľúčom je symetrické, nakoľko sa pri ňom používa jediný súkromný kľuč, ktorý slúži pre zašifrovanie, aj dešifrovanie. Súkromný kľúč musí byť

známy len užívateľom, preto je utajený a je potrebné, aby bol dôsledne chránený. Kľúče sú známe obom komunikujúcim stranám a obvykle sú pomerne krátke, aby algoritmické výpočty, ktoré sú pomocou týchto kľúčov vykonávané, boli dostatočne rýchle a neboli zbytočne zložité. Z dôvodu nutnosti zaistenia bezpečnosti kľúčov pri ich prenose sieťou sa súkromné kľúče často menia. Tento typ kľúča je obvykle bezpečne uložený v počítači, prípadne na čipovej karte (1).

Pre šifrovanie pomocou súkromných kľúčov sú využívané napríklad nasledujúce štandardy: **DES** (Data Encryption Standard), **AES** (Advanced Encryption Standard) (3).

Šifrovanie verejným kľúčom (public key)

Šifrovanie verejným kľúčom je asymetrické, pretože pre zašifrovanie a dešifrovanie využíva dvojicu šifrovacích kľúčov. Jeden z kľúčov je verejný, druhý je súkromný. Obidva kľúče sú vygenerované koncovým systémom, pričom verejný kľúč je verejne dostupný a súkromný kľúč zostáva za všetkých okolností utajený. Tento typ šifrovania môže byť použitý pre ochranu prenášaných dát a tiež pre potreby autentizácie (1).

Výhodou asymetrického šifrovania je pomerne jednoduchá správa šifrovacích kľúčov, pretože sieťou je posielaný len verejný kľúč. Súkromný kľúč je uložený v lokálnom systéme a sieťou sa nedistribuuje (1).

Nevýhodou tohto typu šifrovania je zložitosť používaného šifrovacieho algoritmu, čo spôsobuje, že asymetrické šifrovanie je výrazne pomalšie ako šifrovanie symetrické. Z toho dôvodu je často využívaná ich kombinácia, kde sa pomalšie asymetrické šifrovanie používa na zašifrovanie a zabezpečenú distribúciu symetrických kľúčov a na ich základe sa následne šifrujú dáta pomocou rýchlejšieho symetrického šifrovania (1).

Pri asymetrickom šifrovaní sú využívané hlavne algoritmy **RSA** a **Diffie-Hellman**. Verejné kľúče sú tiež využívané v technológiách digitálnych podpisov a digitálnych certifikátov (4).

3.7 IPSec

IPSec je bezpečnostná architektúra, ktorá bola vytvorená pre protokol IP, nakoľko ten pôvodne neobsahoval žiadne bezpečnostné mechanizmy. IPSec podporuje autentizáciu, dôveryhodnosť a integritu na úrovni datagramov a obsahuje niekoľko protokolov pre

zasielanie autentizovaných a zašifrovaných dát v sieťach s architektúrou TCP/IP. Keďže IPSec funguje na úrovni sieťovej vrstvy, je plne transparentný pre aplikačné protokoly. Nevyžaduje teda žiadne softwarové zmeny v koncových systémoch. Táto bezpečnostná architektúra špecifikuje mechanizmy pre poskytovanie bezpečnostných služieb, ktoré sú realizované pomocou bezpečnostných protokolov (Authentication Header, Encapsulation Security Payload) a pomocou mechanizmov pre správu šifrovacích kľúčov (ISAKMP a IKE) (1).

3.7.1 Bezpečnostné asociácie

V rámci IPSec je definovaný koncept bezpečnostnej asociácie (SA- Security Association). SA definuje bezpečnostné opatrenia, ktoré sú uplatňované na jednotlivé datagramy podľa ich obsahu, odosielateľa a príjemcu. Bezpečnostná asociácia je jednoznačne definovaná pomocou 3 parametrov:

- **Cieľová IP adresa**,
- **Identifikátor bezpečnostného protokolu** – označenie čísla protokolu, pre AH je použité číslo 51, pre ESP 50,
- **Index bezpečnostného parametra (SPI – Security Parameter Index)** – 32 bitová hodnota, ktorá má lokálny vyznám pre cieľovú stanicu v rámci SA.

Každý uzol, ktorý pracuje s IPSec, si udržuje 2 databázy – **dátabázu bezpečnostnej politiky** (SPD – Security Policy Database) a **databázu bezpečnostných asociácií** (SPA – Security Policy Associations). SPA obsahuje parametre pre každú bezpečnostnú asociáciu (napr. SPI, MTU, bezpečnostný protokol, šifrovací algoritmus). V SPD sú uložené jednotlivé bezpečnostné politiky, ktoré sa v definovanom poradí uplatňujú na IP datagramy. Každý z týchto záznamov sa skladá zo selektoru a akcie (1).

Keď systém odosiela paket, ktorý vyžaduje určité bezpečnostné opatrenie, najskôr vyhľadá v databáze bezpečnostnú asociáciu. Následne je vykonané príslušné spracovanie a hodnota SPI je vložená do záhlavia datagramu. Tento datagram je v ďalšom kroku odoslaný smerom k príjemcovi. Príjemca po doručení datagramu na základe cieľovej adresy a hodnoty SPI vyhľadáva SA v databáze, a vykonáva odpovedajúcu operáciu. Dá sa teda povedať, že bezpečnostná asociácia je „dohodnutie“ bezpečnostných parametrov medzi dvomi komunikujúcimi stranami (4).

3.7.2 Protokol AH (Authentication Header)

Protokol AH je voliteľným doplnkom k IP datagramu vo forme autentizačného záhlavia, ktoré je vložené za pôvodné záhlavie datagramu a má za úlohu zaistenie autentizácie zdroja dát a integrity. Integrita znamená, že datagram nebol pri prenose sieťou nijakým spôsobom pozmenený. V autentizačnom záhlaví je využívané šifrovanie pomocou verejného kľúča, ktoré sa vykonáva už u zdroja dát pred fragmentáciou datagramu. Šifrovanie sa týka všetkých súčastí IP datagramu, v ktorých nedochádza k zmenám pri prenose k cieľovej stanici. Používa sa šifrovací algoritmus MD5 a tajný kľuč, pomocou ktorého prebieha šifrovanie v zdrojovom zariadení, je vložený do datagramu. Po doručení datagramu cieľovej stanici a jeho opätovnom zostavení je datagram dešifrovaný (10).

Metóda AH sa využíva v situácií, keď postačuje autentizácia každého jednotlivého datagramu, keďže samotné dáta v IP datagrame nie sú pri použití tohto protokolu šifrované (10).

3.7.3 Protokol ESP (Encapsulating Security Paylaod)

Protokol ESP zaisťuje utajenie správy tým, že sa zašifruje záhlavie, rovnako ako aj dátový obsah správy. Okrem toho poskytuje tiež podobné autentizačné služby ako protokol AH. Použitie protokolu ESP je vhodné v prípadoch, keď je potrebná autentizácia súčasne so šifrovaním prenášaných dát, aby bolo zabránené možnosti odposluchu a následného zneužitia dát (11).

ESP definuje možný obsah datagramu. Obsahuje záhlavie s informáciami o bezpečnostnom protokole (SPI), poradovým číslom a informáciami o použitom šifrovacom algoritme. Dátová časť je zašifrovaná pomocou určitého šifrovacieho algoritmu (napr. DES, AES) a v závere je kontrolný súčet, prostredníctvom ktorého je zisťovaná správnosť IP datagramu (11).

3.7.4 Režimy IPSec

IPSec môže pracovať v dvoch režimoch:

- **režim tunelu** (tunnel mode),
- **režim transportu** (transport mode).

V režime transportu je vkladané bezpečnostné záhlavie medzi pôvodné záhlavie datagramu a dáta. Režim transportu je teda určený na ochranu dát vyšších vrstiev. V prípade, keď je použitý tento režim, šifrovanie je vykonávané zdrojovou stanicou a šifrovaná je len transportná časť dát t.j. TCP/UDP segment alebo ICMP správa. ESP v transportnom režime šifruje a voliteľne tiež autentizuje len prenášané dáta (nie záhlavie datagramu), AH v tomto režime autentizuje prenášané dáta a tiež vybrané polia záhlavia IP datagramu. Režim transportu je používaný pre zabezpečenie koncovej komunikácie medzi stanicami cez externú sieť (11).

V režime tunelu sa celý pôvodný IP datagram vkladá do nového datagramu, ktorý má nezašifrované záhlavie. Pred vložením je možnosť tento pôvodný datagram zašifrovať. V režime tunelu teda nedochádza k žiadnej zmene v záhlaví datagramu. Záhlavie pôvodného datagramu obsahuje údaje o jeho cieli, záhlavie nového (vonkajšieho) datagramu špecifikuje koniec tunelu. Routre sa pri prenose daného datagramu sieťou riadia výhradne podľa informácií uvedených v záhlaví vonkajšieho datagramu. Režim tunelu býva obvykle využívaný pri budovaní VPN tunelov medzi niekoľkými podnikovými alebo inými internými sieťami (1).

Mechanizmy ESP a AH je možné používať medzi ľubovoľnými uzlami v sieti (koncové zariadenia, routre). Taktiež je možné ich využívať pre prenosy typu unicast, aj pre prenosy typu multicast (skupinové vysielanie). Mechanizmus AH poskytuje zaistenie integrity dát a autentizácie zdroja IP paketov, ale neposkytuje možnosť zašifrovania prenášaných dát. Mechanizmus ESP zase umožňuje šifrovanie, ale nechráni nové záhlavie IP paketu. Pre zabezpečenie silnej autentizácie spoločne s utajením prenášaných dát sa preto využíva kombinácia týchto dvoch mechanizmov, a to v režime transportu, ako aj v režime tunelu (1).

3.8 Dynamic Multipoint VPN (DMVPN)

DMVPN je technológia vyvinutá firmou Cisco Systems, ktorej hlavným cieľom je zjednodušenie správy rozsiahlejších VPN sietí. Koncept DMVPN umožňuje veľmi dobrú rozšíriteľnosť VPN sietí a tiež zjednodušenie ich konfigurácie a implementácie. Základom pri použití DMVPN je tzv. **hub-and-spoke** topológia tvorená jedným centrálnym zariadením (HUB), ku ktorému sú prostredníctvom VPN pripojené vzdialené zariadenia (SPOKE) (8).

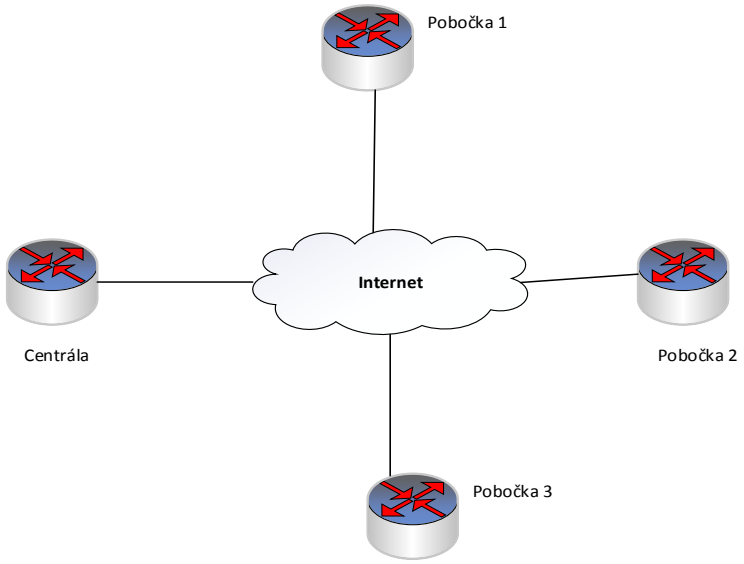
V rámci DMVPN sú vytvárané 2 druhy dynamických VPN spojení (**permanentné** a **dočasné**). Permanentné VPN tunely sú vytvorené medzi vzdialenými routrami a centrálnym routrom. Dočasné VPN tunely sú nadväzované medzi vzdialenými prvkami len v prípade, keď spolu tieto prvky potrebujú komunikovať. Centrálny prvok pri tom plní úlohu NHRP serveru. Dočasné tunely sú zrušené, keď je komunikácia medzi vzdialenými routrami ukončená. S využitím technológie DMVPN je tiež možné nadväzovanie VPN spojení medzi routrami, ktoré majú na svojich portoch dynamicky prideľované IP adresy, čo pri klasických site-to-site VPN možné nie je (8).

Koncept DMVPN využíva ku svojej činnosti 4 základné komponenty:

- **Multipoint GRE (mGRE)** – umožňuje podporu viacerých IPSec tunelov na jednom GRE interface,
- **Dynamické šifrovanie protokolom IPSec** – zabezpečenie dát prenášaných VPN tunelmi pomocou šifrovania,
- **Protokol NHRP** (Next Hop Resolution Protocol) – zabezpečenie prekladu IP adries koncových bodov tunelov na verejné IP adresy jednotlivých routrov,
- **Routovací protokol** – použitý môže byť napr. RIP, EIGRP, OSPF (8).

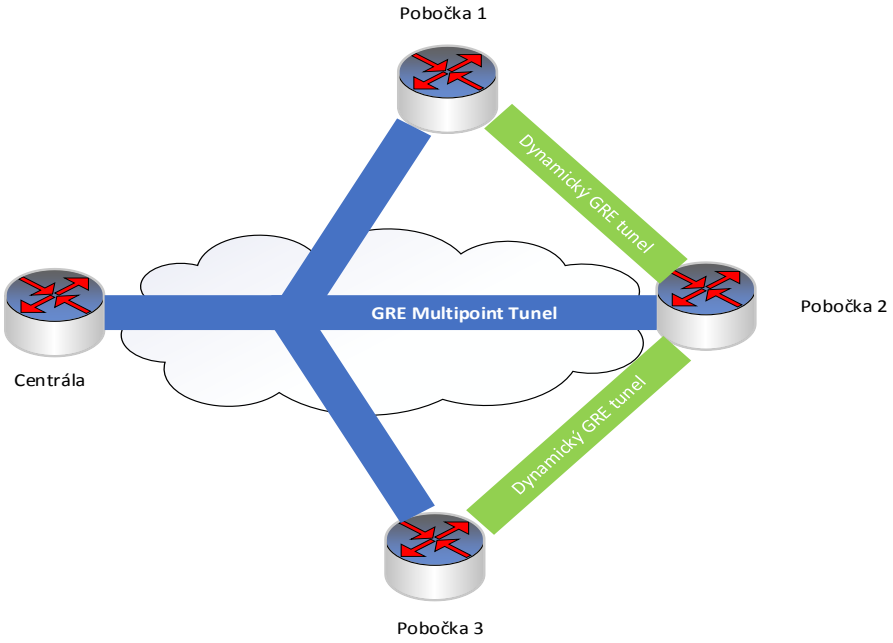
3.8.1 Multipoint GRE (mGRE)

Multipoint GRE je tunelovací protokol, ktorý vznikol rozšírením „klasického“ GRE protokolu a umožňuje vytvorenie GRE tunelu v viacerými cieľovými adresami. Protokol mGRE môže byť využitý napr. v situácií, keď je potrebné VPN spojenie centrály s viacerými pobočkami prostredníctvom internetu. Topológia takejto siete je znázornená na nasledujúcom obrázku (7).



Obr. 7: Topológia siete pre využitie tunelovacieho protokolu GRE (vlastné spracovanie)

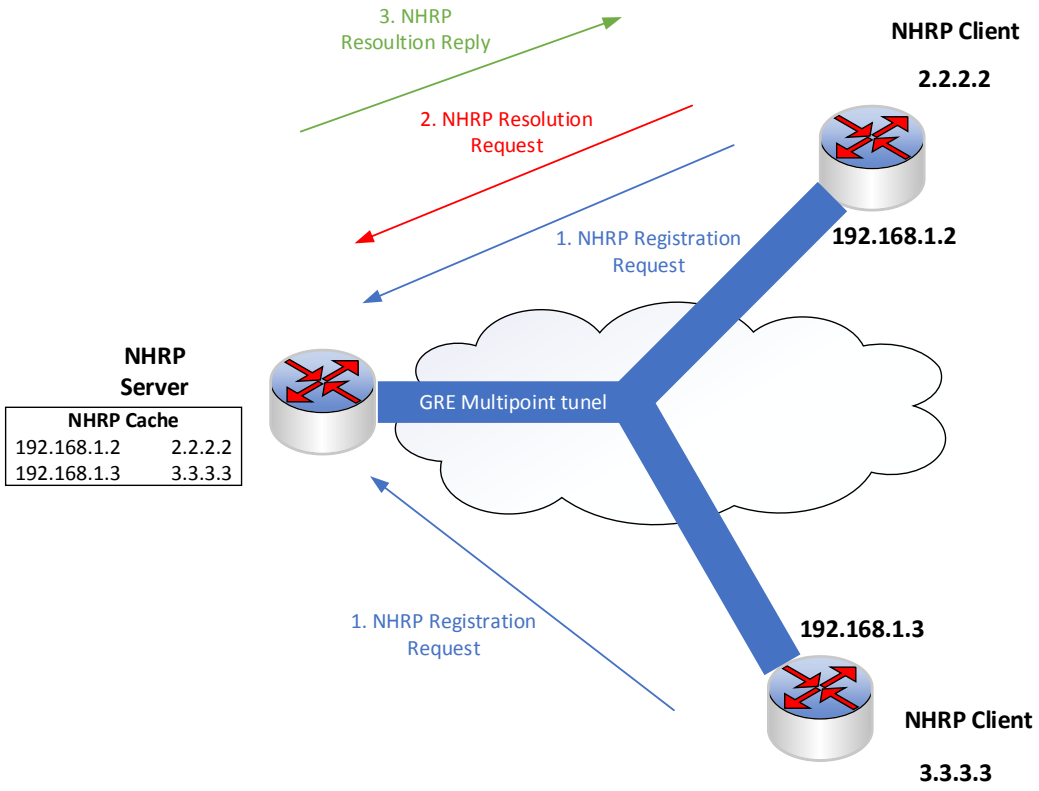
Pri použití „klasického“ GRE protokolu by bola nutná konfigurácia tunelov medzi centrálou a každou z pobočiek, taktiež ako medzi jednotlivými pobočkami. Využitím protokolu mGRE je možné vytvorenie jedného tunelu na routri v centrále, ktorý bude mať viacero cieľových adries (v jednotlivých pobočkách). Je teda možné vytvoriť tzv. „hub and spoke“ topológiu. Komunikácia medzi pobočkami a centrálou následne prebieha prostredníctvom tohto tunelu. V prípade vzájomnej komunikácie dvoch pobočiek sú medzi nimi vytvárané dynamické GRE tunely. To znamená zjednodušenie konfigurácie a zlepšenie možnosti rozšíriteľnosti danej siete. Situácia s využitím mGRE je znázornená na nasledujúcom obrázku (8).



Obr. 8: Vytvorené tunely pomocou protokolu mGRE (vlastné spracovanie)

3.8.2 Protokol NHRP

Next Hop Resolution Protocol pracuje v modeli klient – server. Jeden z routrov pôsobí ako NHRP server, ostatné routre majú rolu NHRP klientov. Jednotliví klienti sa na serveri registrujú odoslaním NHRP Registration Request, v ktorom odosielajú svoju verejnú IP adresu. Server si informácie získané od jednotlivých klientov ukladá do cache pamäte ako spojenia medzi verejnou IP adresou daného routra a adresou koncového bodu tunelu. V momente, keď je potrebné odosielanie dát z jednej pobočky do druhej prostredníctvom tunelu, odosielajúci router posiela NHRP Resolution Request, ktorým sa pýta na verejnú IP adresu cieľového routra. NHRP server odosiela NHRP Resolution Reply, pomocou ktorého odosielajúcemu routru oznamuje verejnú IP adresu cieľového routra. Princíp funkcie protokolu NHRP znázorňuje nasledujúci obrázok (7).



Obr. 9: Princíp fungovania protokolu NHRP (vlastné spracovanie)

3.9 Protokol HSRP

Táto podkapitola je venovaná popisu protokolu **HSRP** (Hot Standby Routing Protocol).

HSRP je proprietárny protokol, ktorý bol vyvinutý firmou Cisco Systems. Cieľom tohto protokolu je umožniť vytvorenie jedného virtuálneho routra z viacerých fyzických routrov, aby v prípade zlyhania jedného routra nebola ohrozená celá sieť, pre ktorú daný router slúžil ako východzia brána. Princíp funkcie protokolu spočíva vo vytvorení virtuálnej IP adresy a MAC adresy. Tieto adresy sú následne zdieľané nakonfigurovanou skupinou routrov, ktorých rozhrania majú vlastné MAC a IP adresy. Jeden zo skupiny routrov je zvolený ako aktívny. Tento router drží virtuálne adresy a normálnym spôsobom routuje provoz. Druhý z routrov je zvolený ako záložný (standby) a ostatné sú tzv. počúvajúce (listening). V prípade výpadku aktívneho routra je táto skutočnosť detekovaná protokolom HSRP a záložný (standby) router preberá funkciu aktívneho routra a virtuálnu IP a MAC adresu. Informácie o dostupnosti aktívneho routra sa medzi jednotlivými routrami šíria prostredníctvom zasielania Hello paketov, ktoré sú posielané

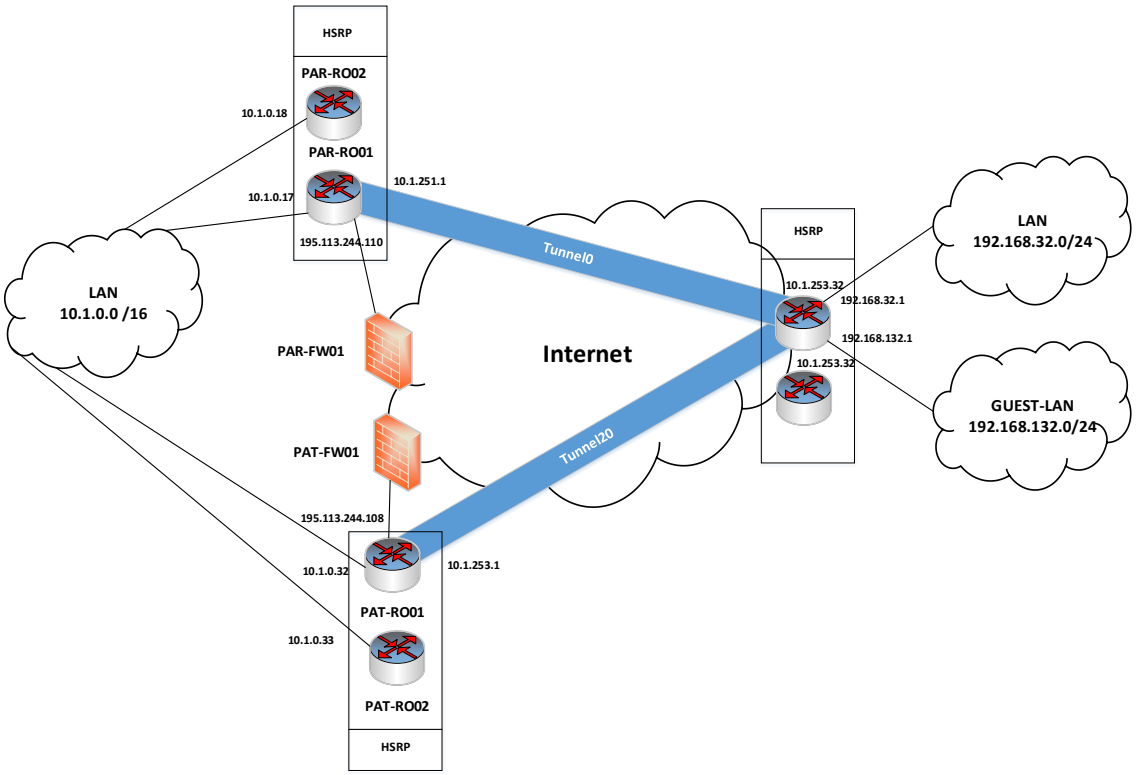
v intervale 3 sekúnd. Ak záložný router po definovanú dobu (holdtime, defaultne 10 sekúnd) neobdrží hello paket, prehlási aktívny router za nefunkčný a preberá jeho funkciu (6).

4 VLASTNÝ NÁVRH RIEŠENIA

Táto kapitola mojej diplomovej práce je venovaná vytvoreniu návrhu VPN WAN siete, ktorá bude spĺňať požiadavky definované vedením Zdravotníckej záchrannej služby Pardubického kraja. V úvode časti je navrhnutá topológia siete a je vytvorený adresný plán. Ďalším krokom je výber poskytovateľov internetového pripojenia pre jednotlivé lokality na základe údajov získaných v prieskume trhu týchto poskytovateľov. Nasledujúcim krokom je popis konfigurácie jednotlivých aktívnych prvkov a návrh spôsobu monitoringu vytvorenej siete. V závere tejto kapitoly je uvedené finančné zhodnotenie, časová analýza, štúdia proveditelnosti a analýza rizík celého projektu.

4.1 Topológia siete

Navrhovaná topológia siete využíva v centrálnej lokalite, rovnako ako vo vzdialených lokalitách pripojenie prostredníctvom 2 rôznych internetových poskytovateľov. V jednotlivých lokalitách budú zvolení poskytovatelia s rôznou technológiou prenosu (1. poskytovateľ – ADSL alebo VDSL, 2. poskytovateľ – LTE), aby bola zvýšená miera redundancie internetového pripojenia. Výsledná topológia siete je znázornená na nasledujúcom obrázku. Na obrázku je uvedená len 1 zo vzdialených lokalít, ostatné lokality sú pripojené k centrálnej lokalite rovnakým spôsobom.



Obr. 10: Topológia navrhovanej siete (vlastné spracovanie)

4.1.1 Centrálna lokalita

Centrálnu lokalitu v tomto prípade predstavuje lokalita, v ktorej je umiestnené Krajské operačné zdravotnícke stredisko (KZOS) ZZS Pardubického kraja. Konkrétne sa jedná o lokalitu Pardubice- Průmyslová. V tomto mieste bude umiestnený centrálny router (HUB), prostredníctvom ktorého budú vytvorené mGRE tunely do jednotlivých lokalít. Záložnou centrálnou lokalitou je lokalita Pardubice – Teplého, kde je umiestnený záložný centrálny router. Do týchto routrov je privedené internetové pripojenie od 2 zvolených poskytovateľov.

V lokalite Pardubice- Průmyslová sú umiestnené routre, ktoré sú nakonfigurované do jednej HSRP skupiny, aby bola zvýšená miera redundancie. V prípade výpadku primárneho routra (PAR-RO01) preberie záložný router (PAR-RO02) jeho funkciu. HSRP skupina má virtuálnu IP adresu 10.1.0.16, router PAR-RO01 má adresu 10.1.0.17 a router PAR-RO02 má adresu 10.1.0.18.

V lokalite Pardubice- Teplého sú tiež umiestené 2 routre, ktoré sú nakonfigurované ako jedna HSRP skupina. Tieto routre sú označené ako PAT-RO01 a PAT-RO02 a majú adresy 10.1.0.32 a 10.1.0.33. Virtuálna adresa HSRP skupiny je 10.1.0.31.

LAN sieť v centrálnej lokalite

LAN sieť v centrálnej lokalite využíva adresný rozsah 10.1.0.0 s maskou siete 255.255.0.0. Tento adresný rozsah je ďalej členený na subsiete hlavne podľa jednotlivých aplikácií (VoIP, kamery, PC, WiFi, servery).

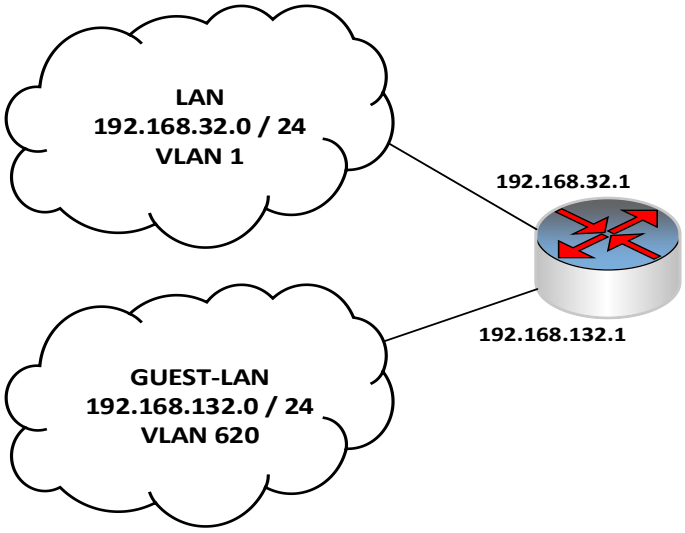
4.1.2 Vzdialené lokality

Vzdialenými lokalitami sú v prípade ZZS Pardubického kraja jednotlivé výjazdové stanovištia, ktoré sú rozmiestnené po celom kraji. V týchto lokalitách budú umiestnené vzdialené routre (SPOKE). V každej vzdialenej lokalite budú umiestnené 2 routre, do každého z nich bude privedené internetové pripojenie od jedného zvoleného poskytovateľa. Tieto 2 routre budú nakonfigurované ako HSRP skupina. Routre budú označené skratkou konkrétnej lokality a číslom (xxx-RO01,xxx-RO02).

LAN sieť vo vzdialených lokalitách

Počítačová sieť vo vzdialených lokalitách je rozdelená na 2 segmenty. Prvým z nich je LAN sieť, ktorá má adresný rozsah 192.168.x.0 s maskou siete 255.255.255.0. Druhým segmentom siete je GUEST-LAN, ktorý má vyhradený adresný rozsah 192.168.(x+100).0 s maskou siete 255.255.255.0. Číslo x sa líši v závislosti od konkrétnej lokality. Táto časť siete slúži pre hostí a má zakázaný prístup do internej siete. Zo segmentu siete GUEST-LAN je teda povolený len prístup smerom do siete internet.

Uvedené 2 segmenty siete sú oddelené na úrovni sieťovej aj linkovej vrstvy. Na sieťovej vrstve je oddelenie daných segmentov siete realizované použitím rozdielnych adresných rozsahov. Na linkovej vrstve sú segmenty oddelené použitím VLAN (virtuálnych lokálnych sietí). Časť LAN je zaradená vo VLAN 1, časť GUEST-LAN je zaradená do VLAN 620. V segmente siete označenom ako LAN sú umiestnené ďalšie aktívne prvky (switche, access pointy), počítače a telefóny zamestnancov konkrétneho výjazdového stanovišťa. Rozdelenie LAN siete jednej z lokalít je znázornené na nasledujúcom obrázku.



Obr. 11: Príklad adresácie LAN siete vo vzdialenej lokalite (vlastné spracovanie)

4.2 Výber internetových poskytovateľov

V tejto časti mojej diplomovej práce je realizovaný výber poskytovateľov internetového pripojenia pre jednotlivé lokality. V každej z lokalít je potrebné zvoliť dvoch poskytovateľov. Výber je realizovaný na základe informácií získaných v rámci prieskumu trhu poskytovateľov pripojenia k internetu. Výber bol realizovaný s ohľadom na požiadavky týkajúce sa rýchlosti pripojenia v jednotlivých lokalitách.

Na základe informácií získaných v prieskume trhu internetových poskytovateľov navrhujem využitie služieb spoločnosti UPC ako primárneho poskytovateľa. Táto firma poskytuje vo všetkých lokalitách VDSL pripojenie s prenosovou rýchlosťou 50 Mbit/s pre download a 20 Mbit/s pre upload. Rýchlosť internetového pripojenia bude teda vo všetkých lokalitách zvýšená oproti súčasnému stavu. Vyššia rýchlosť pripojenia k internetu bola zvolená s ohľadom na možný budúci rozvoj danej VPN siete, kde by pôvodné rýchlosti nemuseli dostačovať.

Ako poskytovateľ „záložného“ pripojenia bola zvolená firma O2, ktorá poskytuje LTE pripojenie s prenosovou rýchlosťou 20 Mbit/s. Služby tohto poskytovateľa budú využívané v dobe výpadku primárneho spojenia centrálnej lokality a jednotlivých vzdialených lokalít. Z toho dôvodu tu bla zvolená nižšia rýchlosť, ktorá by ale mala plne dostačovať pre potreby ZZS Pardubického kraja.

4.3 Výber konkrétneho typu routrov

Táto kapitola mojej diplomovej práce popisuje konkrétne modely routrov, ktoré boli zvolené pre použitie v projekte návrhu VPN WAN siete ZZS. Jeden z modelov bude použitý v centrálnej lokalite, druhý model bude umiestnený do všetkých vzdialených lokalít.

4.3.1 Centrálna lokalita

V krajskom zdravotníckom operačnom stredisku (centrálna lokalita) budú použité routre **Cisco C2921/K9**. Tento typ routra disponuje tromi gigabitovými portami RJ45, jedným konzolovým, jedným AUX portom a dvomi USB 2.0 portami. Jeden z RJ-45 portov je zdieľaný, miesto neho je teda možné použiť SFP modul. Router Cisco C2921 môže byť tiež napájaný prostredníctvom technológie Power over Ethernet (PoE). Router je v základe vybavený 512 MB RAM pamäťou a 256 MB Flash pamäťou. RAM pamäť môže byť rozšírená až na 2 GB, pre Flash pamäť je maximálnou veľkosťou 8 GB. Uvedený model routra Cisco je znázornený na nasledujúcom obrázku.

Obr. 12: Router Cisco C2921 - pohľad spredu (12)

Na nasledujúcom obrázku je znázornený pohľad na router Cisco C2921/K9 zo zadnej strany, kde je možné vidieť jednotlivé porty.

Obr. 13: Router Cisco C2921 - pohľad zozadu (12)

4.3.2 Vzdialené lokality

V jednotlivých výjazdových stanovištiach (vzdialené lokality) budú použité routre **Cisco C881GW+7-E-K9,** ktoré disponujú 1 WAN portom typu RJ45 s maximálnou prenosovou rýchlosťou 100 Mbit/s 8 LAN RJ-45 portmi s rovnakou rýchlosťou prenosu. Zvolený typ routra je tiež vybavený 1 konzolovým a 1 AUX portom. Cisco C881 obsahuje 128 MB flash pamäte a 256 MB pamäte RAM, ktorá môže byť rozšírená na 768 MB. Daný model routra je znázornený na nasledujúcom obrázku.

Obr. 14: Router Cisco C881 (13)

Routre vybraných typov poskytujú nasledujúce funkcie:

- aplikačný firewall,
- filtrovanie obsahu,
- realizácia VPN a WLAN sietí,
- možnosť centralizovaného managementu.

4.4 Konfigurácia routrov v centrálnej lokalite

Táto kapitola mojej práce popisuje postup konfigurácie routrov v centrálnej lokalite pre realizáciu VPN WAN siete ZZS Pardubického kraja. V úvodnej časti kapitoly je popísaná základná konfigurácia, následne je vysvetlený postup konfigurácie zložitejších parametrov a funkcií ako routovanie pomocou protokolu EIGRP, vytvorenie ACL, konfigurácia IPSec a IP inspectov a konfigurácia rozhraní tunelov.

4.4.1 Základná konfigurácia

Obidva routre umiestnené v centrálnej lokalite musia samozrejme obsahovať základnú konfiguráciu, ktorá pozostáva z príkazov uvedených v tejto podkapitole. Konkrétne príkazy použité v rámci základnej konfigurácie sú uvedené v prílohe 1.

- **Definícia názvu daného routra**

Routre umiestnené v centrálnej lokalite majú názvy PAR-RO01 a PAR-RO02.

- **Definícia časovej zóny, termínu zmeny času z letného na zimný a synchronizácie času na routri pomocou NTP serverov**

V konfigurácii je nastavený posun času na routri voči časovej zóne GMT (Greenwich Main Time) a je tiež nastavené automatické posunutie času na danom routri v termíne, kedy sa mení letný čas na zimný a opačne. Router má definované 2 NTP servery, pomocou ktorých si synchronizuje svoj čas. Jeden z nich je umiestnený v internej sieti, druhý zo serverov je v sieti internet. Preferovaný bude NTP server v privátnej podnikovej sieti.

- **Definícia užívateľov spolu s úrovňou oprávnení a heslami**

Príkaz privilege udáva úroveň oprávnení, ktoré daný užívateľ má (15 je maximum). Vytvorení užívatelia majú priradené najvyššie úroveň oprávnení, budú teda môcť vykonávať všetky druhy operácií v konfigurácii routrov. Jeden z účtov je určený pre IT oddelenie ZZS, druhý z nich je pre pracovníkov firmy, ktorá spravuje počítačovú sieť ZZS.

- **Nastavenie hesla pre prístup do privilegovaného režimu**

Parameter secret udáva, že heslo bude v konfigurácii zašifrované a teda nebude v konfigurácií viditeľné v nezašifrovanej podobe.

- **Nastavenie metód autentizácie a autorizácie**

Autentizácia aj autorizácia budú prebiehať lokálne (podľa užívateľských účtov vytvorených priamo na jednotlivých routroch). Tento typ autorizácie a autentizácie bude použitý aj pre vzdialený prístup na daný router.

- **Nastavenie vzdialeného prístupu pomocou protokolu SSH verzie 2 a vygenerovanie RSA kľúčov pre SSH prístup**

Protokol SSH umožňuje vzdialený prístup do príkazového riadku routra. Jeho výhodou je, že neprenáša dáta v nezašifrovanej podobe. RSA kľúče použité pre potreby protokolu SSH budú mať veľkosť 2048 bitov.

- **Povolenie prístupu na router protokolom HTTPS a zakázanie prístupu pomocou HTTP**

Nastavená bola tiež autentizácia do webového rozhrania prostredníctvom lokálnych užívateľských účtov a obmedzenie prístupu access listom označným číslom 23. Prístup protokolom HTTP bol zakázaný z dôvodu, že tento protokol prenáša nešifrované dáta, čo predstavuje určitú bezpečnostnú slabinu.

- **Určenie domény a IP adresy DNS servera**

Routre v centrálnej lokalite sú umiestnené do domény nazvanej zzs.local a DNS server je definovaný svojou IP adresou.

- **Logovanie úspešných a neúspešných pokusov o prihlásenie, zablokovanie po určitom počte neúspešných prihlásení v rámci definovaného časového intervalu**

Všetky pokusy o prihlásenie (úspešné aj neúspešné) budú zaznamenané do logu. Router sa zablokuje a 5 minút nebude umožňovať prihlásenie, ak sa vyskytnú 4 neúspešné pokusy o prihlásenie v priebehu 2 minút.

- **Nastavenie SNMP community**

Vytvorené SNMP community slúžia na to, aby bolo možné získavanie informácií o routri prostredníctvom protokolu SNMP, čo bude využívané pre potreby monitoringu a správy vytvorenej počítačovej siete.

- **Nastavenie logovania**

Logovanie, ktoré bude na daných routroch nakonfigurované, je možné rozdeliť do dvoch skupín. Prvou z nich je logovanie do tzv. interného bufferu, teda do vlastnej pamäte routra s nadefinovanou veľkosťou (51200 Bytov). Do tohto bufferu budú ukladané logy so závažnosťou na úrovni „warning“ alebo vyššou.
Druhým typom logovania bude odosielanie logov na server, ktorý je v konfigurácií určený svojou IP adresou. Na tomto serveri bude nainštalovaný Kiwi Syslog Server, v ktorom bude možné s logmi pracovať a uchovávať ich vo väčšom množstve. Pomocou príkazu logging source-interface je nastavené zdrojové rozhranie pre odosielanie logov na server.

4.4.2 IPSec

Konfiguráciu zabezpečenia tunelov pomocou bezpečnostnej architektúry IPSec je možné zhrnúť do dvoch krokov. Táto podkapitola mojej diplomovej práce obsahuje popis týchto krokov použitých pri konfigurácii routrov pre ZZS Pardubického kraja. IPSec musí byť nakonfigurovaný v centrálnej lokalite, tak isto ako aj v jednotlivých vzdialených lokalitách. Celá konfigurácia IPSec je uvedená v prílohe 2.

Prvým krokom konfigurácie je vytvorenie tzv. crypto isakmp policy. Pri vytváraní tejto politiky je potrebné nastaviť šifrovací algoritmus, ktorý bude použitý, metódu pomocou ktorej bude prebiehať autentizácia a veľkosť šifrovacích kľúčov, ktoré budú využité

v rámci metódy Diffie- Hellmann. Ďalšími nastavovanými parametrami je interval zasielania tzv. keepalive paketov a určenie, či sa jednotlivé zariadenia budú identifikovať svojím názvom (hostname) alebo IP adresou. V prípade konfigurácie, ktorou sa zaoberá moja diplomová práca, budú jednotlivé parametre nastavené nasledovne:

- **šifrovací algoritmus** – 3DES,
- **metóda autentizácie** – Pre-shared key,
- **veľkosť použitých šifrovacích kľúčov**- 1024 bitov,
- **interval posielanie keepalive paketov** – 30 sekúnd,
- **identifikácia zariadení** – pomocou názvu (hostname).

Keďže bola zvolená metóda autentizácie prostredníctvom pre-shared key, je potrebné tieto kľúče v konfigurácii definovať. Vytvorené kľúče je potrebné pomenovať, v tomto prípade boli nazvané ako ZZSPAK. Ďalším potrebným parametrom je adresa, ktorá vyjadruje koncový bod daného tunelu. Nakoľko v tomto prípade sa jedná o multibodový GRE tunel, použitá adresa bude 0.0.0.0 a maskou siete 0.0.0.0.

Nasledujúcim krokom v konfigurácií IPSec je vytvorenie IPSec transform-setu a IPSec profilu a nastavenie ich vybraných parametrov. Transform-set definuje režim, v ktorom bude IPSec fungovať (tunnel alebo transport), použitý algoritmus pre šifrovanie v rámci protokolu ESP (Encapsulating Security Payload) a hashovací algoritmus pre potreby autentizácie v rámci protokolu AH (Authentication Header) . IPSec profil je pomenovaný a následne prepojený s vopred vytvoreným transform setom.

Týmto je konfigurácia IPSec hotová a vytvorený profil môže byť použitý na zabezpečenie tunelu, prostredníctvom ktorého budú prenášané dáta.

4.4.3 Konfigurácia tunelu

Po korektnom nakonfigurovaní ISAKMP a IPSec je možné pristúpiť ku konfigurácií samotných tunelov, ktoré budú slúžiť na zabezpečený prenos dát sieťou internet. Konfigurácia týchto tunelov v centrálnej lokalite a v jednotlivých vzdialených lokalitách je do veľkej miery zhodná. Nasledujúca podkapitola mojej práce obsahuje podrobnejší popis konfigurácie v centrálnej lokalite. Konfigurácia tunelov vo vzdialených lokalitách bude popísaná menej detailne, pozornosť bude zameraná predovšetkým na významné

rozdiely oproti centrálnej lokalite. Kompletná konfigurácia tunelov v centrálnej lokalite je uvedená v prílohe 3.

Postup konfigurácie tunelu v centrálnej lokalite je možné zhrnúť do nasledujúcich bodov.

1. Vytvorenie rozhrania (interface) s názvom Tunnel a jeho číslom,
2. Priradenie IP adresy a masky siete vytvorenému rozhraniu,
3. Nastavenie tunelu do módu mGRE (multipoint GRE) - aby bolo možné danému tunelu priradiť niekoľko cieľových bodov,
4. Určenie zdroja tunelu – zdrojom môže byť určité rozhranie na danom routri. V tomto prípade bude zdrojom rozhranie GigabitEthernet 0/0, ktoré je vonkajším rozhraním routra v centrálnej lokalite a má verejnú IP adresu,
5. Povolenie protokolu NHRP na danom rozhraní a určenie ID (číslo) NHRP siete na tomto rozhraní – ID NHRP siete bolo zvolené ako 10000,
6. Nastavenie NHRP autentizácie – pre potreby autentizácie je definovaný autentizačný textový reťazec, ktorý musí byť rovnaký na všetkých zariadeniach v rámci jednej NHRP siete,
7. Nastavenie automatickej registrácie SPOKE routrov (routre vzdialených lokalít) u HUB routra (router v centrálnej lokalite),
8. Nastavenie ochrany tunelu pomocou vytvoreného IPSec profilu – IPSec profil, ktorý bol vytvorený v predchádzajúcich krokoch konfigurácie bude priradený na vytvorené rozhranie tunelu,
9. Zmenšenie MTU a TCP segmentu – kvôli encapsulácii je potrebné zmenšenie MTU (Maximum Transfer Unit) na hodnotu 1400 Bytov a tiež zníženie veľkosti TCP segmentu (TCP Maximum Segment Size) na 1360 Bytov. Uvedené zmeny sú realizované kvôli tomu, že IPSec v režime transportu pridáva k IP datagramom nové bezpečnostné záhlavie.

4.4.4 EIGRP

V mnou navrhovanej WAN VPN sieti bude použitý routovací protokol EIGRP. Konfigurácia tohto protokolu pozostáva z 2 čiastkových krokov. Prvým z nich je samotné „zapnutie“ routovania prostredníctvom EIGRP a definovanie sietí, ktoré budú zapojené do routovacieho procesu EIGRP protokolu. „Zapnutie“ routovania EIGRP protokolom je

nastavené vytvorením routovacieho procesu s určeným ID číslom (v tomto prípade sa jedná o „router eigrp 1“).

Konfigurácia routovacieho protokolu EIGRP pozostáva z určenia adresných rozsahov sietí, ktoré budú routrom v centrálnej lokalite propagované a definovania, ktorý typ záznamov v routovacej tabuľke bude redistribuovaný. Môže sa jednať o staticky definované záznamy, priamo pripojené siete, alebo routy získané pomocou iného routovacieho protokolu (napr. OSPF, RIP).

V centrálnej lokalite bude potrebné, aby routre propagovali 2 adresné rozsahy – 10.1.0.0 s maskou siete 255.255.255.0 10.1.251.0 s maskou 255.255.255.0. Rozsah 10.1.0.0 je určený pre LAN sieť v centrálnej lokalite a 10.1.251.0 je rozsah určený pre tunel z centrálnej lokality k jednotlivým vzdialeným lokalitám.

V lokalite Pardubice – Teplého bude namiesto adresného rozsahu 10.1.251.0 propagovaný rozsah 10.1.253.0. Jedná sa o adresný rozsah, ktorý je využitý druhým mGRE tunelom.

Redistribuované budú len staticky definované routy, keďže na routroch centrálnej lokality nefunguje žiadny iný routovací protokol. Konfigurácia routovania protokolom EIGRP je uvedená v prílohe 4.

4.4.5 Access Control lists (ACL)

ACL sú vo všeobecnosti súbory pravidiel, pomocou ktorých je obmedzovaný prístup k určitému objektu. V rámci aktívnych prvkov sa využívajú hlavne na filtrovanie paketov. Access control listy musia byť pomenované názvom alebo označené číslom. Následne môžu byť použité napr. na konkrétnom rozhraní, kde budú vhodným spôsobom obmedzovať komunikáciu. Pri vyhodnocovaní ACL sa používa tzv. pravidlo „first fit“. To znamená, že pri nájdení prvej zhody sa uplatní daná akcia a zoznam sa ďalej neprehľadáva. Z toho dôvodu záleží na poradí, v akom sú jednotlivé pravidlá definované.

ACL majú 2 rôzne typy:

- **Štandardné ACL (Standard)** – umožňujú filtrovanie len na základe zdrojových a cieľových IP adries,

- **Rozšírené ACL (Extended)** – poskytujú možnosti filtrovania paketov nielen na základe IP adries, ale aj podľa čísel portov, použitého protokolu a podobne.

V centrálnej lokalite sú použité dva access listy. Prvý z nich je štandardného typu a je označený číslom 23, druhý je rozšíreného typu a je označený číslom 102.

Access list s číslom 23 je použitý na obmedzenie vzdialeného prístupu na routre v centrálnej lokalite. V tomto ACL je prístup povolený len z vnútornej siete ZZS Pardubického kraja a zo siete firmy, ktorá spravuje počítačovú sieť ZZS. V konfigurácii je pri aplikácii tohto ACL použitý parameter in, ktorý určuje, že sa ACL sa uplatňuje na spojenia, ktoré na daný router prichádzajú.

Access list 102 je umiestnený na vonkajšom rozhraní routra v centrálnej lokalite. ACL číslo 102 je taktiež použitý s parametrom in, definuje teda pravidlá pre prístup do vnútornej podnikovej siete. V rámci tohto ACL sú povolené všetky správy protokolu ICMP, pakety protokolu NTP na synchronizáciu času a prístup firmy spravujúcej počítačovú sieť ZZS. Povolená je tiež komunikácia protokolom UDP po portoch 500 a 4500, ktoré sú využívané pre IKE a NAT-T a umožňujú fungovanie VPN na báze IPSec. Kompletné ACL centrálnej lokality sú uvedené v prílohe 5.

4.4.6 HSRP

Routre z centrálnej lokality (PAR-RO01 a PAR-RO02) sú nakonfigurované v jednej HSRP skupine. Majú teda „spoločnú“ virtuálnu IP adresu 10.1.0.16. Router PAR-RO01 je primárny, PAR-RO02 preberá jeho funkciu v prípade potreby. Rovnakým spôsobom sú nakonfigurované routre aj v lokalite Pardubice-Teplého, jediným rozdielom sú použité IP adresy a názvy zariadení. Routre v tejto lokalite sú pomenované ako PAT-RO01 a PAT-RO02. ich spoločnou virtuálnou adresou je 10.1.0.31, pričom RO01 má adresu 10.1.0.32 a RO02 10.1.0.33. Konfigurácia protokolu HSRP je uvedená v prílohe 6.

4.5 Konfigurácia routrov vo vzdialených lokalitách

V tejto kapitole je popísaná konfigurácia routrov, ktoré budú umiestnené do jednotlivých výjazdových stanovíšť. Nakoľko je ich konfigurácia v mnohých bodoch podobná až rovnaká, sú popisované predovšetkým rozdiely oproti konfigurácií centrálneho routra.

4.5.1 Základná konfigurácia

Základná konfigurácia routrov v jednotlivých vzdialených lokalitách sa z väčšej časti zhoduje s konfiguráciou použitou v centrálnej lokalite. Jediným rozdielom sú názvy jednotlivých zariadení, ktoré vždy vychádzajú z názvu konkrétnej lokality. Zvyšná časť základnej konfigurácie sa zhoduje s centrálnou lokalitou. Názvy routrov vo všetkých lokalitách sú uvedené v adresnom pláne.

4.5.2 DHCP

Na routroch umiestnených vo vzdialených lokalitách musia byť nakonfigurované 2 DHCP pooly, z ktorých sa pomocou protokolu DHCP prideľujú adresy niektorým zariadeniam. 1 z poolov slúži pre prideľovanie adries v rámci LAN siete, druhý je určený pre časť LAN siete, ktorá je určená pre hostí a má obmedzený prístup – GUEST-LAN.

V konfigurácií DHCP poolu je uvedený adresný rozsah, z ktorého sú prideľované adresy v danom segmente, názov domény, IP adresa DNS servera a IP adresa default gateway. Konfigurácia protokolu DHCP sa v jednotlivých vzdialených lokalitách líši v použitých adresných rozsahoch a IP adrese default gateway.

Z adresných rozsahov určených na prideľovanie adries zariadeniam sú vyňaté adresy, ktoré sú použité pre prvky v sieti, ktoré potrebujú mať pridelenú statickú IP adresu. Tieto adresy DHCP server nebude prideľovať zariadeniam, aby nevznikali duplicity IP adries v sieti. Príkazy použité v konfigurácii DHCP sú uvedené v prílohe 7.

4.5.3 IPSec

Konfigurácia IPSec je vo vzdialených lokalitách úplne identická s tou, ktorá bola použitá v lokalite centrálnej.

4.5.4 Konfigurácia tunelu (vzdialené lokality)

Postup konfigurácie tunelov a jednotlivé parametre sú na SPOKE routroch (vo vzdialených lokalitách) do veľkej miery podobné HUB routru (v centrálnej lokalite). Táto podkapitola mojej práce je zameraná na popis prvkov konfigurácie, ktoré sú vo vzdialených lokalitách rozdielne.

Prvým z rozdielov je samozrejme použitá IP adresa pre rozhranie tunelu. IP adresy sa v jednotlivých lokalitách líšia.. Routre vo vzdialených lokalitách na sebe majú 2 rozhrania tunelov (z routrov v centrálnej lokalite a z routra v lokalite Pardubice - Teplého). Sú označené ako Tunnel0 a Tunnel20. Konkrétne IP adresy rozhraní tunelov v jednotlivých lokalitách sú uvedené v adresnom pláne.

Ďalšou odlišnosťou je to, že routre v jednotlivých vzdialených lokalitách musia mať v konfigurácii rozhrania tunelu definovanú adresu tzv. **Next Hop Servera**, ktorým je centrálny router. Na Next Hop Server sú smerované dotazy od jednotlivých SPOKE routrov v situácii, keď potrebujú komunikovať so SPOKE routrom v inej vzdialenej lokalite. SPOKE router odosiela žiadosť Next Hop Serveru (HUB router), v ktorej sa pýta na verejnú IP adresu SPOKE routra, s ktorým potrebuje komunikovať. Definícia Next Hop Serveru je vykonaná použitím príkazu s uvedením IP adresy rozhrania tunelu na HUB routri

Konfigurácia vzdialených routrov má ďalší rozdiel v tom, že v konfigurácii potrebuje mať uvedené „spárovanie“ IP adresy rozhrania tunelu na HUB routri s verejnou IP adresou daného HUB routra.

Odlišnosťou môže byť tiež rozhranie použité ako zdroj tunelu. Rozdiel je však len v jeho označení. Vždy sa jedná o rozhranie na danom routri, ktoré je umiestnené v internej počítačovej sieti.

Mimo uvedených rozdielov sa konfigurácia NHRP protokolu a rozhraní tunelov vo vzdialených lokalitách zhoduje s centrálnou lokalitou. Musia byť teda použité rovnaký autentizačný reťazec, označenie NHRP siete (ID), mód tunelovacieho protokolu (GRE multipoint). Taktiež nutnosť zmenšenia IP datagramu a TCP segmentu platí aj pre všetky routre umiestnené vo vzdialených lokalitách. Príkazy v konfigurácii, ktoré boli rozdielne oproti centrálnej lokalite sú uvedené v prílohe 8.

4.5.5 IP inspect

IP inspect je nástroj, ktorý pomáha routru, aby sa správal sčasti ako firewall. Princíp funkcie tohto nástroja spočíva v hĺbkovej kontrole prechádzajúcich paketov a ukladaní spojení, ktoré sú iniciované z privátnej siete smerom do internetu do tzv. stavovej databázy. Pakety, ktoré sa vracajú z týchto spojení v smere z internetu do privátnej siete

sú následne prepúšťané vonkajším rozhraním a prichádzajú naspäť užívateľom. Bez použitia tejto technológie by buď nemohli byť použité žiadne ACL a sieť by teda nebola vôbec zabezpečená, alebo by sa pakety, ktoré by prichádzali späť z internetu, nedostávali k užívateľom, ktorí inicializovali spojenie, a teda TCP spojenie by ani nemohlo byť naviazané. IP inspecty môžu byť použité pre veľké množstvo rôznych protokolov.

V počítačovej sieti pre danú spoločnosť sú použité inspecty pre tieto protokoly – TCP, UDP, FTP, TFTP, ICMP, HTTP, HTTPS, DNS.

Vytvorený inspect musí byť následne použitý na určitom rozhraní routra, aby plnil funkciu, na ktorú je určený. V tomto prípade bude aplikovaný na rozhranie FastEthernet 4 (outside interface) s parametrom out, čo znamená, že hĺbková inšpekcia bude vykonávaná na paketoch smerujúcich z vnútornej siete do internetu. Kompletná konfigurácia IP inspectov je uvedená v prílohe 9.

4.5.6 Access Control Lists (ACL)

Prvý z nich definuje obmedzenia siete pre hostí (GUEST-LAN). Užívatelia tejto časti podnikovej siete majú zakázaný prístup do vnútornej siete, povolenú majú len komunikáciu smerom do internetu. Okrem toho majú povolené len odpovede echo-reply protokolu ICMP, dotazy a odpovede protokolu DNS a komunikáciu protokolom bootstrap na získavanie vlastnej IP adresy a masky siete. Užívatelia GUEST-LAN majú zakázané inicializovanie TCP spojení smerom do vnútornej siete, môžu však odpovedať na spojenia, ktoré boli inicializované z vnútornej siete.

Ďalším z použitých ACL je ACL s číslom 101, ktorý je umiestnený na vonkajšom rozhraní siete Zdravotníckej záchrannej služby. Tento ACL povoľuje komunikáciu prostredníctvom protokolu bootstrap na získanie IP adresy z DHCP serveru, DNS dotazy a odpovede, všetky príkazy protokolu ICMP mimo príkazu echo (ping) a prístup firme, ktorá spravuje počítačovú sieť ZZS. Povolená je tiež komunikácia protokolom UDP po portoch 500 a 4500, ktoré sú využívané pre IKE a NAT-T a umožňujú fungovanie VPN na báze IPSec. Tento ACL tiež povoľuje komunikáciu prichádzajúcu z verejných IP adries centrálnej lokality (adresy 195.113.244.108 a 195.113.244.110).
Pomocou ACL je tiež routovaná komunikácia z jednotlivých vzdialených lokalít smerom do internetu. Je nastavené, aby táto komunikácia prechádzala tunelom do centrálnej

lokality, kde následne prechádza cez firewall do siete internet. Na tento účel je vytvorený ACL s názvom INET, ktorý povoľuje len komunikáciu z LAN siete konkrétnej lokality mimo interných sietí. Tento ACL je následne využitý pri vytvorení route-mapy, ktorá nastavuje komunikácií, ktorá vyhovuje kritériám ACL INET, adresu next-hopu 10.1.251.1, čo je rozhranie tunelu v centrálnej lokalite.
Posledným z vytváraných ACL je ACL označený číslom 150, ktorý je následne použitý pre preklad adries pomocou mechanizmu NAT v jednotlivých lokalitách. Tento ACL vyhradzuje IP adresy z LAN siete konkrétnej lokality, pre ktoré je preklad adries použitý. ACL použité vo vzdialených lokalitách sú uvedené v prílohe 10.

4.5.7 EIGRP

Aj na routroch, ktoré sú umiestnené v jednotlivých výjazdových stanovištiach, je potrebné nakonfigurovať routovanie protokolom EIGRP. Konfigurácia je o niečo zložitejšia ako v centrálnej lokalite, nakoľko sú využívané aj tzv. distribute-listy, ktoré obmedzujú propagované routy.

Distribute-listy budú použité na obmedzovanie propagácie adresných rozsahov v dvoch smeroch (na rozhrania tunelov a z rozhraní tunelov). Pre ich konfiguráciu musí byť najskôr vytvorený ACL s daným názvom, a ten môže byť následne použitý v konfigurácii protokolu EIGRP. Konkrétna konfigurácia protokolu EIGRP a distribute-listov na Cisco routroch je uvedená v prílohách.

V oboch smeroch musia byť propagované adresné rozsahy dvoch tunelov t.j. 10.1.251.0 a 10.1.253.0 s maskou siete 255.255.255.0.

V smere z lokality do tunelov budú propagované siete LAN a GUEST-LAN z danej lokality, teda adresné rozsahy 192.168.x.0 a 192.168.(x+100).0, kde x predstavuje označenie konkrétnej lokality. Obidva z uvedených adresných rozsahov majú masku siete 255.255.255.0.

V smere z tunelov do lokality musí byť propagovaná sieť centrálnej lokality a adresné rozsahy vyjadrujúce ostatné vzdialené lokality. Jedná sa teda o siete 10.1.0.0 s maskou 255.255.0.0 a 192.168.0.0 s maskou 255.255.0.0.

4.5.8 NAT

Vo výjazdových stanovištiach musí byť nakonfigurovaný aj preklad adries NAT, nakoľko sú v nich využívané iné adresné rozsahy ako tunely a centrálna lokalita.

Konfigurácia mechanizmu NAT je realizovaná pomocou ACL s číslom 150, ktorý povoľuje adresné rozsahy 192.168.x.0 a 192.168.(x+100).0. Ten je následne využitý ako zdroj adries, ktoré môžu byť prekladané mechanizmom NAT. Na rozhraniach v LAN a GUEST-LAN sieti v jednotlivých lokalitách je použitý parameter in, nakoľko sa jedná o interné siete. Na rozhraniach tunelov je použitý parameter out, pretože tieto rozhrania sú v tomto prípade vonkajšími rozhraniami. V konfigurácii je tiež použitý parameter overload, ktorý vyjadruje, že pri preklade adries sa využívajú čísla portov, to znamená, že stačí 1 vonkajšia IP adresa pre všetky zariadenia komunikujúce z internej siete. Tento spôsob prekladu adries je niekedy označovaný ako PAT (Port Address Translation). Kompletná konfigurácia prekladu adries je uvedená v prílohách.

4.5.9 HSRP

Aj routre vo vzdialených lokalitách budú nakonfigurované do HSRP skupín. 2 routre v každej lokalite teda budú mať jednu spoločnú virtuálnu IP adresu, pričom ako primárny bude zvolený router, do ktorého je privedené internetové pripojenie od poskytovateľa UPC.

4.6 Adresný plán

Adresný plán bol vypracovaný po návrhu topológie danej siete. Centrálna lokalita využíva adresný rozsah 10.1.0.0 s maskou siete 255.255.0.0. Jednotlivé vzdialené lokality využívajú siete s rozsahmi 192.168.x.0 s maskou 255.255.255.0. Hodnota tretieho oktetu IP adresy sa líši v závislosti na lokalite. Tunely sú adresované pomocou rozsahov 10.1.251.0 a 10.1.253.0 v oboch prípadoch s maskou siete 255.255.255.0. Rozhrania tunelov v jednotlivých lokalitách sú adresované ako 10.1.251.x resp. 10.1.253.x, kde x opäť vyjadruje číslo konkrétnej lokality. Routre RO01 a RO02 v jednotlivých vzdialených lokalitách sú nadefinované ako HSRP skupina, majú teda všetky adresy zhodné, budú sa líšiť len vo verejných IP adresách, ktoré budú pridelené poskytovateľmi.

Podrobný adresný plán siete sa nachádza v prílohe 13.

4.7 Monitoring (MRTG + WHATSUP+logovanie)

Táto časť mojej diplomovej práce je venovaná problematike monitoringu navrhnutej VPN WAN siete. Sieť bude monitorovaná viacerými spôsobmi, konkrétne sa bude jednať o nasledujúce činnosti:

- monitoring funkčnosti zariadení a spojení,
- monitorovanie záťaže a objemu prenášaných dát,
- zber a archivácia logov,
- zálohovanie a archivácia konfigurácií aktívnych prvkov.

4.7.1 Monitoring funkčnosti zariadení a spojení

Monitoring funkčnosti zariadení a spojení bude realizovaný prostredníctvom programu **WhatsUp Gold**, pomocou ktorého je monitorovaná celá počítačová sieť Zdravotníckej záchrannej služby Pardubického kraja. Tento nástroj umožňuje sledovanie veľkého množstva rôznych parametrov na jednotlivých sieťových prvkoch. K zariadeniam a spojom, ktoré sú monitorované v súčasnosti, bude pridaná novo nainštalovaná časť siete. Nebude potrebné žiadne rozširovanie licencie programu WhatsUp Gold, nakoľko počet zariadení, ktoré môžu byť monitorované so súčasnou licenciou nebude prekročený.

V softwarovom nástroji WhatsUp Gold bude na routroch monitorované vyťaženie procesoru, vyťaženie RAM pamäte, dostupnosť daného zariadenia a stav všetkých spojení, ktoré na konkrétnom routri sú. Dostupnosť zariadenia je testovaná pravidelným odosielaním ICMP paketov, stav jednotlivých spojení a údaje o vyťažení RAM pamäte a procesoru sú získavané dotazmi protokolu SNMP.

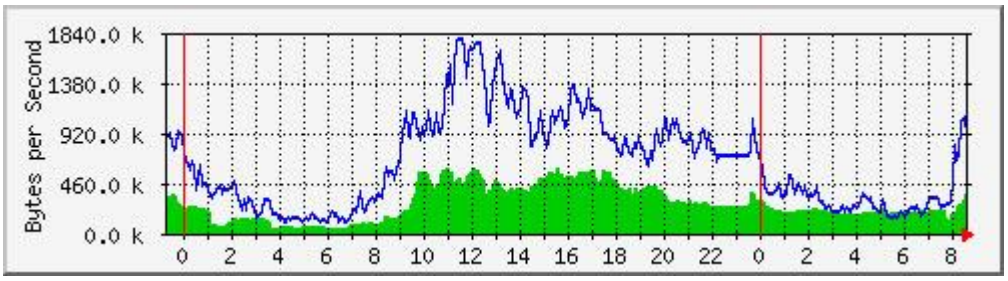
Tento program taktiež umožňuje zasielanie mailových správ o zmenách stavov jednotlivých sledovaných zariadení pracovníkom firmy spravujúcej sieť ZZS. Táto možnosť bude využitá, aby sa správcovia siete okamžite dozvedeli o výskyte problémov a mohli čo najrýchlejšie reagovať.

4.7.2 Monitorovanie záťaže a objemu prenášaných dát

Na monitoring záťaže a množstva dát, ktoré sú prenášané VPN WAN sieťou, bude využitý nástroj **MRTG** (Multi Router Traffic Grapher). Jedná sa o programový nástroj, ktorý umožňuje monitorovanie objemov dát prenášaných sieťovými zariadeniami, ktoré

podporujú SNMP protokol. MRTG dokáže automaticky zbierať údaje z MIB databáz jednotlivých prvkov a na ich základe vykresľuje grafy, pomocou ktorých je možné sledovanie objemov prenášaných dát a saturácie jednotlivých liniek.

Tento nástroj bude pre jednotlivé linky a rozhrania, na ktorých bude použitý, vytvárať podobné grafy, ako sú na nasledujúcom obrázku.



Obr. 15: Vzorový graf MRTG (14)

Grafy nástroja MRTG budú vytvárané pre spojenia medzi centrálnou lokalitou a jednotlivými vzdialenými lokalitami. Je možné vytvárať grafy provozu pre rôzne časové obdobia (deň, týždeň, mesiac, rok). Na serveri, na ktorom budú umiestnené všetky programy súvisiace s monitoringom siete, bude vytvorená úloha, ktorá bude program MRTG spúšťať každých 5 minút.

4.7.3 Zber a archivácia logov

Pre zber a archiváciu logov z jednotlivých aktívnych prvkov navrhujem využitie programu **Kiwi Syslog Server**, ktorý bude nainštalovaný na serveri , kde sa nachádzajú aj ostatné programy súvisiace s monitoringom siete. Zo zozbieraných logov budú následne vyfiltrované logy o významných udalostiach, ktoré budú následne prostredníctvom emailov posielané pracovníkom firmy, ktorá spravuje sieť ZZS Pardubického kraja. Významnými udalosťami sú napríklad úspešné aj neúspešné pokusy o prihlásenie na aktívne prvky, alebo udalosti, ktoré sú v logoch označené ako error (napr. strata konektivity na určitom rozhraní).

4.7.4 Zálohovanie a archivácia konfigurácií aktívnych prvkov

Zálohovanie konfigurácií slúži k tomu, aby bola možná obnova pôvodnej konfigurácie v prípade chyby obsluhy pri jej zmene, alebo strate pôvodnej konfigurácie z iných dôvodov. Zálohovanie konfigurácie bude prebiehať automaticky, pravidelne a v určenom čase. Využitý na to bude program **Kiwi Cat Tools**, ktorý túto funkcionalitu obsahuje. Ďalšou užitočnou funkciou, ktorá bude pri prevádzke navrhovanej siete využívaná, je možnosť realizácie hromadných zmien v konfiguráciách viacerých prvkov súčasne. Zálohované konfigurácie budú ukladané na tom istom serveri, kde budú umiestnené aj ostatné programy určené pre monitoring danej siete.

Navrhujem, aby zálohovanie konfigurácií prebiehalo raz denne, v nočnom čase, kedy je najmenšie vyťaženie prvkov a vo WAN sieti prebieha najmenšie množstvo komunikácie.

Novo zálohovaná konfigurácia sa vždy bude porovnávať s poslednou známou konfiguráciou daného prvku a prípadné zistené zmeny v konfigurácii budú prostredníctvom mailu oznámené pracovníkom firmy, ktorá spravuje počítačovú sieť ZZS Pardubického kraja.

4.7.5 Činnosti spojené s monitoringom siete

Raz mesačne bude zostavovaný report o vyťažení jednotlivých liniek v rámci WAN siete ZZS Pardubického kraja. Za túto činnosť bude zodpovedný jeden z pracovníkov firmy spravujúcej sieť ZZS.

Logy o udalostiach, ktoré sú vyhodnotené ako významné, budú prichádzať pracovníkom firmy spravujúcej sieť ZZS prostredníctvom mailov. Títo pracovníci sú zodpovední za reakciu, kontrolu a prípadnú nápravu konkrétnej udalosti.

Na základe údajov o dostupnosti jednotlivých zariadení bude raz mesačne vytváraný report, v ktorom budú uvedené percentuálne hodnoty dostupnosti jednotlivých zariadení. Monitorovanými zariadeniami budú routre vo všetkých lokalitách a tiež prvky v LAN sieťach jednotlivých lokalít (switche, access pointy, servery). Zodpovednosť za tvorbu týchto reportov bude mať tiež jeden určený pracovník z firmy, ktorá sa zaoberá správou siete pre ZZS.

4.8 Projekt nasadenia

V tejto kapitole bude popísaný projekt nasadzovania navrhnutej počítačovej siete do prevádzky. Projekt obsahuje analýzu rizík, časovú analýzu, analýzu proveditelnosti a v závere je zostavené finančné zhodnotenie.

4.8.1 Analýza proveditelnosti

Táto podkapitola mojej práce obsahuje zjednodušenú analýzu proveditelnosti pre projekt zavádzania navrhnutej počítačovej siete pre Zdravotnícku záchrannú službu Pardubického kraja.

Hlavným poslaním daného projektu je vytvorenie počítačovej siete pre prenos potrebných informácií medzi krajským zdravotníckym operačným strediskom a jednotlivými lokalitami, v ktorých sídlia výjazdové stanovištia záchrannej služby. Projekt sa zaoberá analýzou súčasného stavu, identifikáciou možných zlepšení v tejto počítačovej sieti, ich návrhom a následnou implementáciou. Súčasťou projektu je tiež analýza rizík, časová analýza a analýza nákladov a prínosov implementácie daného riešenia.

Z analýzy súčasného stavu bol vyvodený záver, že by bolo vhodné realizovať projekt, nakoľko súčasný stav siete nie je pre ZZS plne vyhovujúci tým, že neposkytuje dostatočnú úroveň redundancie. Práve miera spoľahlivosti a bezpečnosti WAN siete by mala byť hlavným prínosom implementácie tohto projektu. Z ekonomického pohľadu sa jedná o pomerne rozsiahlu investíciu, ktorá má ale dlhú životnosť, pretože sieť vytvorená navrhovaným riešením môže spoľahlivo fungovať po dlhé obdobie. V analýze rizík bolo zistené, že na realizáciu projektu pôsobí niekoľko významných rizík. Hodnoty týchto rizík je ale možné pomocou vhodných opatrení znížiť na prijateľnú úroveň.

Na základe výsledkov analýzy súčasného stavu, analýzy rizík, časovej analýzy a zhodnotenia nákladov a prínosov je možné usúdiť, že realizácia projektu je možná a vhodná.

4.8.2 Analýza rizík

V tejto podkapitole je prezentovaná analýza rizík pre daný projekt. V úvode sú identifikované hrozby a scenáre, následne sú ohodnotené jednotlivé riziká a sú pre ne

prijaté opatrenia. V závere časti je formulované ohodnotenie rizík po prijatí vhodných opatrení.

Identifikácia hrozieb a scenárov

Prvým krokom v rámci analýzy rizík projektu je identifikácia hrozieb, ktoré pôsobia na realizáciu projektu a scenárov, ktoré by tieto hrozby mohli spôsobiť.

Tab. 4: Identifikácia hrozieb a scenárov (vlastné spracovanie)

Por. číslo	Hrozba	Scenár
1	Prekročenie nákladov	Firma nebude mať dostatok voľných finančných zdrojov na dokončenie projektu.
2	Prekročenie časového termínu	Dlhšie trvajúca implementácia novej počítačovej siete.
3	Nedostatočné školenie užívateľov	Zamestnanci nevedia správne a plnohodnotne využívať možnosti novej počítačovej siete.
4	Nedostatočné bezpečnostné školenie užívateľov	Zamestnanci môžu svojím konaním poškodiť sieť alebo ohroziť jej bezpečnosť.
5	Nesprávne zvolený dodávateľ	Dodávateľ nesplňuje požiadavky na kvalitu prvkov siete, dodacie termíny a podobne.
6	Nedostupnosť zvolených aktívnych prvkov v momente potreby	Nie je možné pokračovať s inštaláciou siete.
7	Nedostatočné testovanie siete	Zistenie prípadných problémov až v rutinnej prevádzke.
8	Zmena v normách týkajúcich sa počítačových sietí	Navrhnutá sieť nevyhovuje požiadavkám normy.

Ohodnotenie rizík

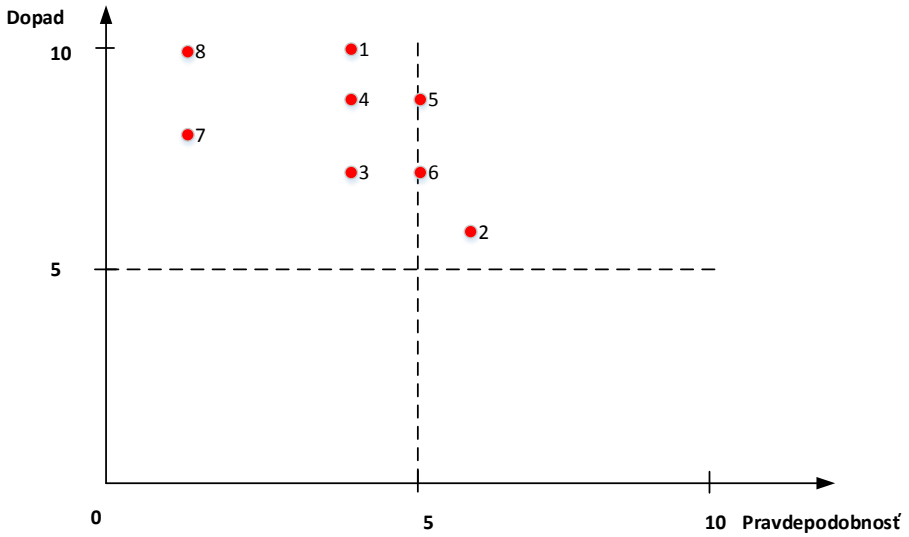
Pre ohodnotenie jednotlivých rizík bola využitá skórovacia metóda. Pre jednotlivé riziká bola stanovená miera pravdepodobnosti ich výskytu a veľkosť ich prípadného dopadu. Pravdepodobnosť aj dopad boli hodnotené číslami od 1 do 10. Hodnota rizika bola následne stanovená ako súčin hodnoty pravdepodobnosti a dopadu, nadobúdala teda hodnoty od 1 do 100.

Návrh opatrení

Po ohodnotení rizík projektu boli navrhované opatrenia, cieľom ktorých bolo znižovanie pravdepodobnosti alebo dopadu jednotlivých rizík. Prehľad navrhovaných opatrení je uvedený v tabuľke v prílohe 14.

Po vypracovaní návrhu opatrení boli stanovené nové hodnoty pravdepodobností a dopadov rizík. Navrhnuté opatrenia spolu s novými hodnotami jednotlivých rizík sú uvedené v prílohe 15.

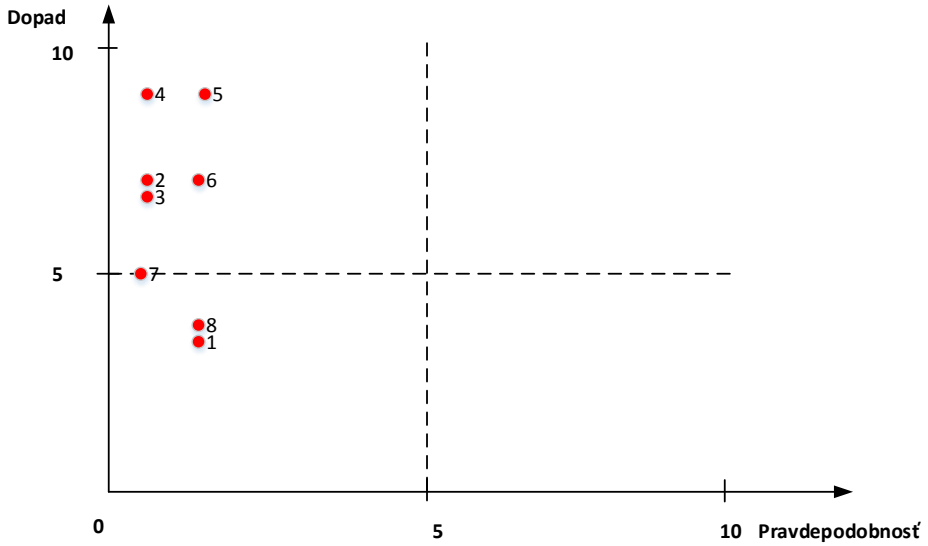
Pre riziká projektu počítačovej siete pre ZZS boli vypracované aj mapy rizík. Prvá mapa znázorňuje hodnoty rizík pred implementáciou opatrení, druhá z nich znázorňuje zníženie hodnôt rizík pôsobením vplyvu navrhnutých opatrení. V mapách rizík sú jednotlivé riziká označené číslami z tabuľky, v ktorej boli definované opatrenia k rizikám.



Obr. 16: Mapa rizík pred prijatím opatrení (vlastné spracovanie)

Z prvej mapy rizík je možné vidieť, že pred aplikáciou opatrení patrila väčšina rizík do časti významných rizík, 2 riziká boli na hranici medzi významnými a kritickými rizikami a jedno riziko patrilo do časti kritických rizík. Z toho vyplýva, že na všetky z rizík projektu musia byť použité určité opatrenia.

Druhá mapa rizík znázorňuje nové hodnoty rizík po ich znížení vhodnými opatreniami. Z grafu je možné vidieť, že 3 z rizík boli znížené tak, že ich nová hodnota odpovedá bezvýznamným rizikám. Ostatné riziká sú umiestnené v časti významných rizík ale u väčšiny bola znížená aspoň pravdepodobnosť na hodnotu 1 alebo 2.



Obr. 17: Mapa rizík po prijatí opatrení (vlastné spracovanie)

4.8.3 Časová analýza

Táto podkapitola mojej práce obsahuje časovú analýzu projektu zavádzania mnou navrhnutej počítačovej siete. V úvode podkapitoly je zostavený zoznam činností a sú pre ne odhadnuté doby trvania. Uvedené doby trvania jednotlivých činností sú v jednotkách Man Days (človekodni). Následne je zostavený sieťový graf.

Pre jednotlivé činnosti sú uvedené optimistické (a), pesimistické (b) a najpravdepodobnejšie (m) odhady trvania. V rámci výpočtov bude použitý odhad trvania činnosti t, ktorý bol vypočítaný nasledujúcim vzorcom:

$$t = \frac{a + 4m + b}{6}$$

Tab. 5: Zoznam činností projektu (vlastné spracovanie)

Činnosť	Popis	Predch. Činnosť	a	m	b	t
1	Prieskum trhu dodávateľov aktívnych prvkov	–	1	2	3	2
2	Výber dodávateľa	1	0,5	1	1,5	1
3	Nákup aktívnych prvkov	2	1	1,5	2	1,5
4	Konfigurácia aktívnych prvkov	3	2	3	4	3
5	Uzavretie zmlúv s internetovými poskytovateľmi	-	2	3	4	3
6	Umiestnenie aktívnych prvkov do jednotlivých lokalít	4	4	6	8	6
7	Označenie aktívnych prvkov	4	1	1,5	2	1,5
8	Prepojovanie aktívnych prvkov	6	4	6	8	6
9	Nastavenie monitoringu zariadení	8	3	5	7	5
10	Vypracovanie dokumentácie	9	4	7	10	7
11	Školenie užívateľov	10	2	3	4	3
12	Bezpečnostné školenie užívateľov	10	2	3	4	3
13	Testovacia prevádzka siete	10	10	12	15	12,2
14	Vyhodnotenie testovacej prevádzky siete	13	3	4	6	4,2
15	Odstránenie prvkov pôvodnej siete	14	4	6	8	6

Pre daný projekt bola pomocou programu MS Project stanovená doba trvania na 51 dní. Gantov diagram pre znázorňujúci postup realizácie je uvedený v prílohe 18. V programe MS Project bol zhotovený aj sieťový diagram, z ktorého je zrejmé, že 11 z celkových 15 činností projektu je súčasťou kritickej cesty. To znamená, že väčšina činností v projekte

sa nesmie oneskoriť, aby tým nebol ovplyvnený termín dokončenia projektu. Pri zavádzaní navrhnutej počítačovej siete bude teda nutné striktné dodržiavanie stanoveného časového plánu. Sieťový graf sa nachádza v prílohe 17.

4.8.4 Prechod na nový systém

V rámci implementácie návrhu danej počítačovej siete do prevádzky je nutné definovať postup, ktorým bude realizovaný prechod zo súčasnej siete na novú sieť. Pri realizácii tejto zmeny je nutné dbať na čo najkratšie výpadky komunikácie v sieti.

V jednotlivých vzdialených lokalitách bude problém riešený s využitím protokolu HSRP. K routrom od poskytovateľa, ktoré sú v lokalitách umiestnené v súčasnosti, budú pridané nové routre, ktoré sú súčasťou tohto projektu. Tieto 2 routre budú nakonfigurované do jednej HSRP skupiny s jednou spoločnou virtuálnou IP adresou. Primárnym bude novo umiestnený router, pôvodný router bude slúžiť ako záložný v prípade potreby. Pridávanie routrov a ich konfigurácia do HSRP skupín bude prebiehať postupne po jednotlivých lokalitách.

V centrálnej lokalite bude po umiestnení nových routrov do všetkých vzdialených lokalít realizovaná úprava routovania. V rámci tejto úpravy bude staticky definované, aby komunikácia prebiehala cez novo inštalované routre a teda novo navrhnutou VPN sieťou. V tomto režime bude prebiehať aj testovacia prevádzka siete, aby bolo možné v prípade potreby prepnúť routovanie komunikácie po pôvodnej WAN sieti od O2. Po ukončení a vyhodnotení testovacej prevádzky novej WAN siete budú pôvodné routre od poskytovateľa zo všetkých lokalít odstránené a v prevádzke bude len novo navrhnutá VPN WAN sieť.

Využitím tohto postupu je možné dosiahnuť výmenu routrov s minimálnymi výpadkami komunikácie v sieti. Tým pádom nebude činnosť Zdravotníckej záchrannej služby nijako výrazne obmedzená.

4.8.5 Finančné zhodnotenie

V tejto podkapitole je uvedené finančné zhodnotenie celého projektu implementácie navrhnutej počítačovej siete. V prvej časti podkapitoly sú analyzované a popísané náklady nutné na vytvorenie riešenia WAN siete navrhnutým spôsobom. Nasledujúca

časť je zameraná na zhodnotenie prínosov, ktoré budú implementáciou daného riešenia dosiahnuté.

Náklady

Náklady na dané riešenie je možné rozdeliť do nasledujúcich 4 skupín:

- hardwarové prostriedky,
- náklady na zriadenie internetového pripojenia prostredníctvom 2 poskytovateľov,
- inštalačné a konfiguračné práce,
- mesačné platby poskytovateľom internetového pripojenia.

Náklady je možné rozdeliť aj na jednorazovo vynaložené a mesačné náklady. Jednorazové náklady predstavujú náklady na hardwarové prvky, zriadenie internetového pripojenia v lokalitách a inštalačné a konfiguračné práce technikov. Mesačne hradené náklady predstavujú pravidelné platby poskytovateľom pripojenia k internetu.

Náklady na hardwarové prostriedky vyjadrujú sumu potrebnú na nákup routrov do centrálnej lokality, aj do všetkých vzdialených lokalít. V nákladoch na zriadenie internetového pripojenia sú zarátané poplatky na prácu technikov daného internetového poskytovateľa a náklady na nákup zariadení od poskytovateľov, pomocou ktorých bude realizované pripojenie k internetu. Náklady na inštalačné a konfiguračné práce zahŕňajú činnosti, ktoré budú realizované pracovníkmi firmy, ktorá spravuje sieť ZZS Pardubického kraja. Bol vyčíslený počet hodín, ktorý bude potrebný pri inštalácií, konfigurácií a prepojovaní aktívnych prvkov v jednotlivých lokalitách a pri zavádzaní systému monitoringu novo vytvorenej časti siete. Čiastka týchto nákladov bola vypočítaná pomocou sumy za hodinu práce technika a počtu hodín potrebných na uvedené činnosti na základe časovej analýzy projektu. V mesačných nákladoch nie sú zarátané platby za následnú správu počítačovej siete.

Nasledujúca tabuľka uvádza súhrnný rozpočet daného projektu. Podrobnejšia verzia rozpočtu sa nachádza v prílohe 16.

Tab. 6: Súhrnný rozpočet projektu (vlastné spracovanie)

Typ nákladov	Suma
Jednorazové náklady	1 413 882 Kč
Mesačné náklady	24 161 Kč

Na zavedenie navrhnutého riešenia VPN WAN siete by teda Zdravotnícka záchranná služba musela vynaložiť **1 413 882 Kč** jednorazovo a ďalších **24 161 Kč** mesačne.

Prínosy

Medzi najväčší prínos navrhnutého riešenia patrí zvýšenie spoľahlivosti WAN siete oproti riešeniu, kde bol využitý len 1 poskytovateľ internetového pripojenia. Pozitívom daného riešenia je tiež bezpečnosť v danej sieti, nakoľko komunikácia medzi jednotlivými lokalitami bude prebiehať prostredníctvom tunelov, v ktorých sa budú prenášať dáta v zašifrovanej podobe. To je nutné, nakoľko sa jedná o citlivé osobné údaje a údaje o zdravotnom stave, ktoré by mohli byť zneužité. Ďalším pozitívom, ktoré implementácia tejto siete prináša je nižší počet nutných zásahov do tejto počítačovej siete. S tým je spojená aj určitá úspora nákladov ZZS, keďže množstvo potrebných servisných zásahov a výjazdov pracovníkov firmy spravujúcej počítačovú sieť ZZS bude znížené.

ZÁVER

Implementácia mnou navrhnutej WAN siete je prínosným krokom, nakoľko Zdravotnícka záchranná služba túto sieť využíva ku svojej každodennej činnosti. Bezproblémová prevádzka siete je pre túto spoločnosť absolútnou nevyhnutnosťou, nakoľko poskytuje služby pri ktorých sa jedná o ľudské životy a zdravie. Výhodou mnou navrhnutej WAN siete je predovšetkým vysoká miera spoľahlivosti zaručená využitím dvoch HSRP skupín routrov umiestnených v centrálnej aj v záložnej lokalite. Vytvorený návrh počítačovej siete spĺňuje aj požiadavky na zabezpečenie komunikácie prechádzajúcej WAN sieťou, nakoľko všetky dáta vo WAN sieti sú prenášané tunelmi zabezpečenými pomocou mechanizmu IPSec. Dáta , ktoré prechádzajú WAN sieťou sú zašifrované, tým je znížené riziko ich úniku a následného zneužitia.

Mnou vytvorený návrh obsahuje výber konkrétnych typov routrov pre jednotlivé lokality a ich kompletnú konfiguráciu. Súčasťou práce je tiež návrh spôsobu monitoringu vytvorenej siete. V záverečnej časti je vypracovaný aj projekt implementácie danej WAN siete do prevádzky, ktorý obsahuje štúdiu proveditelnosti, časovú analýzu, analýzu rizík spolu s návrhom opatrení na zníženie hodnôt rizík a finančné zhodnotenie celého projektu.

Mnou vytvorený návrh redundantnej VPN WAN siete spĺňuje všetky požiadavky, ktoré boli definované vedením Zdravotníckej záchrannej služby Pardubického kraja.

ZOZNAM POUŽITÝCH ZDROJOV

(1) PUŽMANOVÁ, R. *TCP/IP v kostce*. 2. upr. a rozš. vyd. České Budějovice: Kopp, 2009. ISBN 978-80-7232-388-3.

(2) TRUELOVE, J. *Sítě LAN: hardware, instalace a zapojení*.1.vydání. Praha:Grada,2009.384 s. ISBN 978-80-247-2098-2.

(3) ONDRÁK, V. Prednášky – počítačové sítě. Brno: VUT Fakulta podnikatelská, 2014.

(4) BIGELOW, S. J. *Mistrovství v počítačových sítích.* 1.vydání. Brno: Computer Press, 2004. 992 s. ISBN 80-251-0178-9.

(5) ZZSPAK [online]. ©2009-2015.[cit 2018-02-08]. Dostupné z: http://www.zzspak.cz

(6) SAMURAJ-CZ [online]. ©2005-2018.[cit 2017-12-04]. Dostupné z: https://www.samuraj-cz.com

(7) CISCO [online]. ©2008-2018.[cit 2017-12-11]. Dostupné z: https://www.cisco.com/

(8) CISCO IOS DMVPN OVERVIEW [online]. ©2008-2018 .[cit 2017-12-16]. Dostupné z: https://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/DMVPN_Overview.pdf

(9) SYSTEMAK. *systemak.sk* [online]. © 2004-2016. [cit. 2017-11-09]. Dostupné z: http://www.systemak.sk/wp-content/uploads/2014/05/OSI_image3.gif

(10) HORÁK, J., KERŠLÁGER, M. Počítačové sítě: Pro začínající správce. 3.vyd. Brno: Computer Press, 2006. 212 s. ISBN 80-251-0829-9.

(11) KABELOVÁ, A., DOSTÁLEK, L. Velký průvodce TCP/IP a systémem DNS. 5. aktualizované vydání. Brno: Computer Press, 2008. 488 s. ISBN 978-80-251- 2236-5.

(12) CISCO [online]. ©2008-2018.[cit 2018-03-22]. Dostupné z: https://www.cisco.com/c/en/us/products/routers/2921-integrated-services-router-isr/index.html

(13) CISCO [online]. ©2008-2018.[cit 2018-03-22]. Dostupné z: https://www.cisco.com/c/en/us/products/collateral/routers/880g-integrated-services-router-isr/data_sheet_c78-682548.html

(14) MRTG [online]. ©2010-2017.[cit 2018-03-29]. Dostupné z: https://oss.oetiker.ch/mrtg/

ZOZNAM OBRÁZKOV

Obr. 1: Organizačná štruktúra (vlastné spracovanie) 12
Obr. 2: Topológia súčasnej siete (vlastné spracovanie) 14
Obr. 3: Porovnanie modelu ISO/OSI a architektúry TCP/IP (9) 25
Obr. 4: Princíp prekladu adries mechanizmom NAT (vlastné spracovanie) 28
Obr. 5: Princíp Site to Site VPN (vlastné spracovanie) 34
Obr. 6: Princíp Remote Access VPN (vlastné spracovanie) 34
Obr. 7: Topológia siete pre využitie tunelovacieho protokolu GRE (vlastné spracovanie) 42
Obr. 8: Vytvorené tunely pomocou protokolu mGRE (vlastné spracovanie) 43
Obr. 9: Princíp fungovania protokolu NHRP (vlastné spracovanie) 44
Obr. 10: Topológia navrhovanej siete (vlastné spracovanie) 47
Obr. 11: Príklad adresácie LAN siete vo vzdialenej lokalite (vlastné spracovanie) 49
Obr. 12: Router Cisco C2921 - pohľad spredu (12) 50
Obr. 13: Router Cisco C2921 - pohľad zozadu (12) 51
Obr. 14: Router Cisco C881 (13) 51
Obr. 15: Vzorový graf MRTG (14) 65
Obr. 16: Mapa rizík pred prijatím opatrení (vlastné spracovanie) 69
Obr. 17: Mapa rizík po prijatí opatrení (vlastné spracovanie) 70

ZOZNAM TABULIEK

Tab. 1: Rýchlosť pripojenia do WAN (vlastné spracovanie) 15
Tab. 2: Rezervované IP adresy (1) 26
Tab. 3: Rozsahy privátnych IP adries (1) 27
Tab. 4: Identifikácia hrozieb a scenárov (vlastné spracovanie) 68
Tab. 5: Zoznam činností projektu (vlastné spracovanie) 71
Tab. 6: Súhrnný rozpočet projektu (vlastné spracovanie) 74
Tab. 7: Adresný plán centrálnej lokality (vlastné spracovanie) IX
Tab. 8: Adresný plán vzdialených lokalít (vlastné spracovanie) IX
Tab. 9: Ohodnotenie rizík projektu (vlastné spracovanie) XI
Tab. 10: Ohodnotenie rizík projektu po prijatí opatrení (vlastné spracovanie) XII
Tab. 11: Rozpočet projektu (vlastné spracovanie) XIII

ZOZNAM SKRATIEK

ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GMT	Greenwich Main Time
GRE	Generic Routing Encapsulation
HSRP	Hot Standby Routing Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
LAN	Local Area Network
LTE	Long-Term Evolution
mGRE	Multipoint Generic Routing Encapsulation
MRTG	Multi Router Traffic Grapher

MTU	Maximum Transmission Unit
NAT	Network Address Translation
NHRP	Next Hop Resolution Protocol
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PAT	Port Address Translation
PoE	Power over Ethernet
RAM	Random Access Memory
SFP	Small Form-factor Pluggable Transciever
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TFTP	File Transfer Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VDSL	Very-high-bit-rate Digital Subscriber Line
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

ZOZNAM PRÍLOH

Príloha 1: Základná konfigurácia

Príloha 2: Konfigurácia IPSec

Príloha 3: Konfigurácia tunelov v centrálnej lokalite

Príloha 4: Konfigurácia EIGRP v centrálnej lokalite

Príloha 5: Konfigurácia ACL v centrálnej lokalite

Príloha 6: Konfigurácia HSRP v centrálnej lokalite

Príloha 7: Konfigurácia DHCP vo vzdialenej lokalite

Príloha 8: Konfigurácia tunelov vo vzdialenej lokalite

Príloha 9: Konfigurácia IP inspectov

Príloha 10: Konfigurácia ACL vo vzdialenej lokalite

Príloha 11: Konfigurácia EIGRP vo vzdialenej lokalite

Príloha 12: Konfigurácia NAT vo vzdialenej lokalite

Príloha 13: Adresné plány

Príloha 14: Ohodnotenie rizík projektu

Príloha 15: Ohodnotenie rizík po prijatí opatrení

Príloha 16: Rozpočet projektu

Príloha 17: Sieťový graf projektu

Príloha 18: Ganttov diagram projektu

Príloha 19: Zhrnutie prieskumu internetových poskytovateľov

PRÍLOHY

Príloha 1: Základná konfigurácia

```
hostname PAR-Ro01
clock timezone CZ 1 0
clock summer-time CZ recurring last Sun Mar 2:00 last Sun Oct 3:00
ntp server 10.1.16.1 prefer
ntp server 78.108.102.237
username zzsuser privilege 15 secret 5 xxxxxxx
username per4 privilege 15 secret 5 xxxxxxxx
enable secret 5 xxxxx
aaa new-model
aaa authentication login local_authen local
aaa authorization exec local_author local

line vty 0 4
 privilege level 15
 authorization exec local_author
authentication login local_authen
ip ssh version 2
line vty 0
 transport input ssh
crypto key generate rsa
no ip http server
ip http secure-server
ip http access class 23
ip http authentication local
ip domain name zzs.local
ip name-server 10.1.16.16
login block-for 300 attempts 4 within 120
login on-failure log
login on-success log
snmp-server community zzs_public RO
snmp-server community Pr1v@t3ZzS RO
logging buffered 51200 warnings
logging source-interface GigabitEthernet0/1
logging host 10.1.17.110
```

Príloha 2: Konfigurácia IPSec

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp identity hostname
crypto isakmp keepalive 30 periodic
crypto isakmp key ZZSPAK address 0.0.0.0 0.0.0.0
crypto ipsec transform-set 3DEC-MD5 esp-3des esp-md5-hmac
 mode transport
!
crypto ipsec profile Profile_Lokality
 set transform-set 3DEC-MD5
```

Príloha 3: Konfigurácia tunelov v centrálnej lokalite

```
interface Tunnel0

 ip address 10.1.251.1 255.255.255.0

 no ip redirects

 ip mtu 1400

 ip nhrp authentication VPN_ZZS

 ip nhrp map multicast dynamic

 ip nhrp network-id 100000

 ip nhrp holdtime 360

 ip tcp adjust-mss 1360

 tunnel source GigabitEthernet0/0

 tunnel mode gre multipoint

 tunnel key 100000

 tunnel protection ipsec profile Profile_Lokality
```

```
interface Tunnel20
 ip address 10.1.253.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication VPN_ZZS
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 360
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile Profile_Lokality
```

Príloha 4: Konfigurácia EIGRP v centrálnej lokalite

```
router eigrp 1
 network 10.1.0.0 0.0.0.255
 network 10.1.251.0 0.0.0.255
 redistribute static
router eigrp 1
 network 10.1.0.0 0.0.0.255
 network 10.1.253.0 0.0.0.255
 redistribute static
```

Príloha 5: Konfigurácia ACL v centrálnej lokalite

```
access-list 23 permit 10.1.0.0 0.0.255.255

access-list 23 permit 10.8.0.0 0.0.255.255

access-list 23 permit 192.168.0.0 0.0.255.255

access-list 23 permit 81.19.1.192 0.0.0.15


access-list 102 permit udp any any eq non500-isakmp

access-list 102 permit udp any any eq isakmp

access-list 102 permit udp any any eq 10000

access-list 102 permit esp any any

access-list 102 permit ahp any any

access-list 102 remark == PER4

access-list 102 permit ip 81.19.1.192 0.0.0.15 any

access-list 102 permit ip host 77.240.177.138 any

access-list 102 permit udp any eq ntp any eq ntp

access-list 102 remark == ICMP

access-list 102 permit icmp any any echo

access-list 102 permit icmp any any echo-reply

access-list 102 permit icmp any any time-exceeded

access-list 102 permit icmp any any unreachable

access-list 102 deny   ip 10.0.0.0 0.255.255.255 any

access-list 102 deny   ip 172.16.0.0 0.15.255.255 any

access-list 102 deny   ip 192.168.0.0 0.0.255.255 any log

access-list 102 deny   ip 127.0.0.0 0.255.255.255 any

access-list 102 deny   ip host 255.255.255.255 any

access-list 102 deny   ip any any log
```

Príloha 6: Konfigurácia HSRP v centrálnej lokalite

Router PAR-RO01

```
interface GigabitEthernet0/1
 ip address 10.1.0.17 255.255.255.0
 standby 1 ip 10.1.0.16
 standby 1 priority 110
 standby 1 preempt
```

Router PAR-RO02

```
interface GigabitEthernet0/1
 ip address 10.1.0.18 255.255.255.0
 standby 1 ip 10.1.0.16
 standby 1 preempt
```

Router PAT-RO01

```
interface GigabitEthernet0/1
 ip address 10.1.0.32 255.255.255.0
 standby 1 ip 10.1.0.31
 standby 1 preempt
 standby 1 priority 110
```

Router PAT-RO02

```
interface GigabitEthernet0/1
 ip address 10.1.0.33 255.255.255.0
 standby 1 ip 10.1.0.31
 standby 1 preempt
```

Príloha 7: Konfigurácia DHCP vo vzdialenej lokalite

```
ip dhcp pool GUEST-LAN
   network 192.168.132.0 255.255.255.0
   domain-name zzs.pak
   dns-server 8.8.8.8
   default-router 192.168.132.1
!
ip dhcp pool LAN
   network 192.168.32.0 255.255.255.0
   domain-name zzs.pak
   default-router 192.168.32.1
   dns-server 10.1.16.16 192.168.1.110
!
ip dhcp excluded-address 192.168.32.1 192.168.32.63
ip dhcp excluded-address 192.168.32.107
ip dhcp excluded-address 192.168.32.99
ip dhcp excluded-address 192.168.132.1 192.168.132.63
```

Príloha 8: Konfigurácia tunelov vo vzdialenej lokalite

```
interface Tunnel0
 ip nhrp nhs 10.1.251.1
 ip nhrp map 10.1.251.1 195.113.244.11
interface Tunnel20
 ip nhrp nhs 10.1.253.1
 ip nhrp map 10.1.253.1 195.113.244.108
```

Príloha 9: Konfigurácia IP inspectov

```
ip inspect name SDM_MEDIUM tftp
ip inspect name SDM_MEDIUM tcp
ip inspect name SDM_MEDIUM udp
ip inspect name SDM_MEDIUM ftp
ip inspect name SDM_MEDIUM tftp
ip inspect name SDM_MEDIUM icmp
ip inspect name SDM_MEDIUM http
```

```
ip inspect name SDM_MEDIUM https
ip inspect name SDM_MEDIUM dns


interface FastEthernet4
 description == Internet outside ==
 ip inspect SDM_MEDIUM out
```

Príloha 10: Konfigurácia ACL vo vzdialenej lokalite

```
ip access-list extended ACL-GUEST-LAN
 remark --- VLAN 620 Guest ---
 permit udp any any eq bootps
 permit udp any any eq bootpc
 permit udp any any eq domain
 permit icmp any host 192.168.132.1
 permit icmp any any echo-reply
 permit tcp any any established
 deny   ip any 10.0.0.0 0.255.255.255 log
 deny   ip any 192.168.0.0 0.0.255.255 log
 deny   ip any 172.16.0.0 0.15.255.255 log
 permit ip any any


access-list 101 remark -- IPSec --
access-list 101 permit udp any any eq isakmp
access-list 101 permit udp any any eq non500-isakmp
access-list 101 permit gre any any
access-list 101 remark -- Domain --
access-list 101 permit udp any eq domain any
access-list 101 remark -- PER4 --
access-list 101 permit ip 81.19.1.192 0.0.0.15 any
access-list 101 remark -- ZZS KHK --
access-list 101 permit ip host 195.113.244.108 any
access-list 101 permit ip host 195.113.244.110 any
access-list 101 remark -- DHCP --
access-list 101 permit udp any eq bootps any eq bootpc
access-list 101 remark -- ICMP --
access-list 101 permit icmp any any echo-reply
access-list 101 permit icmp any any time-exceeded
```

```
access-list 101 permit icmp any any unreachable
access-list 101 remark -- Deny --
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
access-list 101 deny   ip host 255.255.255.255 any
access-list 101 deny   ip any any log
```

Príloha 11: Konfigurácia EIGRP vo vzdialenej lokalite

```
ip access-list standard EIGRP-IN
 permit 10.1.0.0 0.0.255.255
 permit 192.168.0.0 0.0.255.255
ip access-list standard EIGRP-OUT
 permit 192.168.32.0 0.0.0.255
 permit 192.168.132.0 0.0.0.255


router eigrp 1
 distribute-list EIGRP-OUT out Tunnel0
 distribute-list EIGRP-IN in Tunnel0
 distribute-list EIGRP-OUT out Tunnel20
 distribute-list EIGRP-IN in Tunnel20
 network 10.1.251.0 0.0.0.255
 network 10.1.253.0 0.0.0.255
 network 192.168.32.0
 network 192.168.132.0
```

Príloha 12: Konfigurácia NAT vo vzdialenej lokalite

```
access-list 150 remark -- NAT --
access-list 150 permit ip 192.168.32.0 0.0.0.255 any
access-list 150 permit ip 192.168.132.0 0.0.0.255 any
ip nat inside source list 150 interface FastEthernet4 overload
```

```
interface Vlan620
 ip nat inside
interface Vlan1
 ip nat inside
interface Tunnel0
 ip nat outside
interface Tunnel20
 ip nat outside
```

Príloha 13: Adresné plány

Centrálne routre

Tab. 7: Adresný plán centrálnej lokality (vlastné spracovanie)

Zariadenie	Interface_OUTSIDE	Interface_INSIDE	Interface Tunnel0	Interface Tunnel20
PAR-RO01	195.113.244.110	10.1.0.17	10.1.251.1	-
PAR-RO02	195.113.244.110	10.1.0.18	10.1.251.1	-
PAT-R001	195.113.244.108	10.1.0.32	-	10.1.253.1
PAT-RO02	195.113.244.108	10.1.0.33	-	10.1.253.1

Routre vzdialených lokalít

Tab. 8: Adresný plán vzdialených lokalít (vlastné spracovanie)

Lokalita	Názov zariadenia	Interface Tunnel0	Interface Tunnel20	Interface LAN	Interface GUEST-LAN
Pardubice – Teplého	PAT-RO03	10.1.251.20	10.1.253.20	192.168.20.1	192.168.120.1
Pardubice – Teplého	PAT-RO04	10.1.251.20	10.1.253.20	192.168.20.1	192.168.120.1
Moravská Třebová	MTR-RO01	10.1.251.22	10.1.253.22	192.168.22.1	192.168.122.1
Moravská Třebová	MTR-RO02	10.1.251.22	10.1.253.22	192.168.22.1	192.168.122.1
Lanškroun	LNS-RO01	10.1.251.24	10.1.253.24	192.168.24.1	192.168.124.1
Lanškroun	LNS-RO02	10.1.251.24	10.1.253.24	192.168.24.1	192.168.124.1
Holice	HOL-RO01	10.1.251.26	10.1.253.26	192.168.26.1	192.168.126.1
Holice	HOL-RO02	10.1.251.26	10.1.253.26	192.168.26.1	192.168.126.1

Červená Voda	CV-RO01	10.1.251.28	10.1.253.28	192.168.28.1	192.168.128.1
Červená Voda	CV-RO02	10.1.251.28	10.1.253.28	192.168.28.1	192.168.128.1
Přelouč	PRE-RO01	10.1.251.30	10.1.253.30	192.168.30.1	192.168.130.1
Přelouč	PRE-RO02	10.1.251.30	10.1.253.30	192.168.30.1	192.168.130.1
Žamberk	ZAM-RO01	10.1.251.32	10.1.253.32	192.168.32.1	192.168.132.1
Žamberk	ZAM-RO02	10.1.251.32	10.1.253.32	192.168.32.1	192.168.132.1
Litomyšl	LIT-RO01	10.1.251.34	10.1.253.34	192.168.34.1	192.168.134.1
Litomyšl	LIT-RO02	10.1.251.34	10.1.253.34	192.168.34.1	192.168.134.1
Svitavy	SVI-RO01	10.1.251.36	10.1.253.36	192.168.36.1	192.168.136.1
Svitavy	SVI-RO02	10.1.251.36	10.1.253.36	192.168.36.1	192.168.136.1
Vysoké Mýto	VM-RO01	10.1.251.38	10.1.253.38	192.168.38.1	192.168.138.1
Vysoké Mýto	VM-RO02	10.1.251.38	10.1.253.38	192.168.38.1	192.168.138.1
Ústí nad Orlicí	UNO-RO01	10.1.251.40	10.1.253.40	192.168.40.1	192.168.140.1
Ústí nad Orlicí	UNO-RO02	10.1.251.40	10.1.253.40	192.168.40.1	192.168.140.1
Skuteč	SKU-RO01	10.1.251.42	10.1.253.42	192.168.42.1	192.168.142.1
Skuteč	SKU-RO02	10.1.251.42	10.1.253.42	192.168.42.1	192.168.142.1
Hlinsko	HLI-RO01	10.1.251.44	10.1.253.44	192.168.44.1	192.168.144.1
Hlinsko	HLI-RO02	10.1.251.44	10.1.253.44	192.168.44.1	192.168.144.1
Polička	POL-RO01	10.1.251.46	10.1.253.46	192.168.46.1	192.168.146.1
Polička	POL-RO02	10.1.251.46	10.1.253.46	192.168.46.1	192.168.146.1
Chrudim	CHR-RO01	10.1.251.48	10.1.253.48	192.168.48.1	192.168.148.1
Chrudim	CHR-RO02	10.1.251.48	10.1.253.48	192.168.48.1	192.168.148.1

Príloha 14: Ohodnotenie rizík projektu

Tab. 9: Ohodnotenie rizík projektu (vlastné spracovanie)

Por. číslo	Hrozba	Scenár	Pravdepodobnosť	Dopad	Hodnota rizika
1	Prekročenie nákladov	Firma nebude mať dostatok voľných finančných zdrojov na dokončenie projektu.	4	9	36
2	Prekročenie časového termínu	Dlhšia implementácia počítačovej siete.	7	6	42
3	Nedostatočné školenie užívateľov	Zamestnanci nevedia správne a plnohodnotne využívať možnosti novej počítačovej siete.	4	7	28
4	Nedostatočné bezpečnostné školenie užívateľov	Zamestnanci môžu svojím konaním poškodiť sieť alebo ohroziť jej bezpečnosť.	4	9	36
5	Nesprávne zvolený dodávateľ	Dodávateľ nesplňuje požiadavky firmy na kvalitu prvkov siete, dodacie termíny a podobne.	5	9	45
6	Nedostupnosť zvolených aktívnych prvkov v momente potreby	Nie je možné pokračovať s inštaláciou siete kým nebudú dodané potrebné aktívne prvky.	4	7	28

7	Nedostatočné testovanie siete	Zistenie prípadných problémov až v rutinnej prevádzke.	2	8	16
8	Zmena v normách týkajúcich sa počítačových sietí	Navrhnutá sieť nevyhovuje zmeneným požiadavkám normy.	2	10	20

Príloha 15: Ohodnotenie rizík po prijatí opatrení

Tab. 10: Ohodnotenie rizík projektu po prijatí opatrení (vlastné spracovanie)

Por. číslo	Opatrenie	Nová pravdepodobnosť	Nový dopad	Nová hodnota rizika
1	Dôkladná analýza nákladov a zavedenie rezerv na krytie neočakávaných výdavkov.	2	4	8
2	Dôkladné vytvorenie časového plánu projektu a jeho prísne dodržiavanie.	1	7	7
3	Školenie užívateľov so skúseným školiteľom a v dostatočnej intenzite.	1	7	7
4	Bezpečnostné školenie užívateľov so skúseným školiteľom a v dostatočnej intenzite.	1	9	9
5	Dôkladný prieskum dodávateľov a zakotvenie termínov dodávok jednotlivých prvkov do zmlúv s dodávateľom.	2	9	18
6	Objednanie prvkov s dostatočným časovým predstihom.	2	7	14

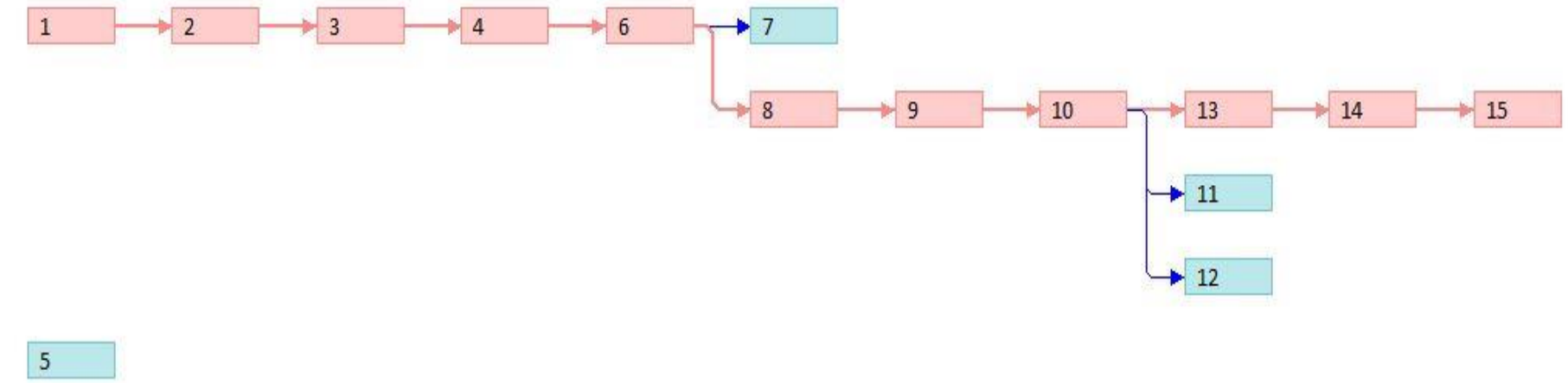
7	Dostatočne dlho trvajúce a prepracované testovanie siete skúseným odborníkom.	1	5	5
8	Vypracovanie návrhu počítačovej siete s ohľadom na možný budúci vývoj trendov v tejto oblasti.	2	4	8

Príloha 16: Rozpočet projektu

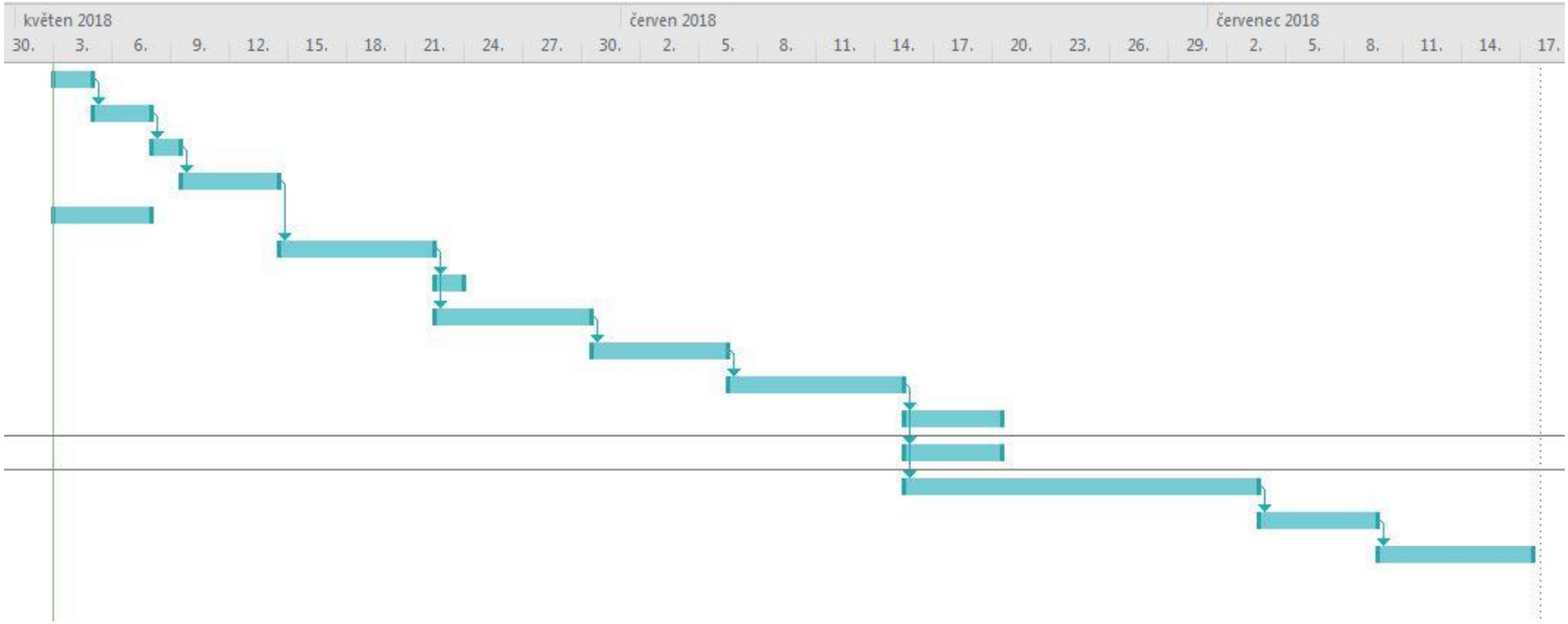
Tab. 11: Rozpočet projektu (vlastné spracovanie)

Skupina nákladov	Popis	Množstvo	Jedn. cena bez DPH	Celk. Cena bez DPH	DPH	Celk. cena s DPH	Typ nákladov
Hardware	Router Cisco C2921/K9	4	66 692	266 768	56 021	322 789	jednorazové
Hardware	Router Cisco C881GW+7-E-K9	30	18 487	554 610	116 468	671 078	jednorazové
Internet	O2- zriadenie pripojenia	16	3305	52880	11 105	63 985	jednorazové
Internet	Internet Optimal Air 20 Mbit/s	16	619	9904	2080	11 984	mesačné
Internet	UPC-zriadenia pripojenia	16	2 892	46 272	9 717	55 989	jednorazové
Internet	UPC Internet VDSL 50/20 Mbit/s	16	629	10 064	2 113	12 177	mesačné
Práca	Práce technikov pri inštalácií	228	1 000	228 000	47 880	275 880	jednorazové

Príloha 17: Sieťový graf projektu



Príloha 18: Ganttov diagram projektu



Príloha 19: Zhrnutie prieskumu internetových poskytovateľov

	Avonet	Vodafone	Metronet	Wia	UPC
Pardubice-Průmyslová	100/10 Mbit/s (DSL)	100 Mbit/s (ADSL/VDSL)	250/25 Mbit/s (ADSL/VDSL)	8/8 alebo100/10 Mbit/s (ADSL/VDSL)	300/20 Mbit/s
Pardubice-Teplého	100/10 Mbit/s (DSL)	50 Mbit/s (ADSL/VDSL)	250/25 Mbit/s (ADSL/VDSL)	50/5 Mbit/s (VDSL)	300/20 Mbit/s
Moravská Třebová	20/2 Mbit/s (DSL)	20 Mbit/s (ADSL/VDSL)	20/2 Mbit/s (ADSL/VDSL)	8/8 alebo 20/2 Mbit/s (ADSL/VDSL)	50/20 Mbit/s
Lanškroun	50/5 Mbit/s (DSL)	50 Mbit/s (ADSL/VDSL)	20/2 Mbit/s (ADSL/VDSL)	8/8 alebo 50/5 Mbit/s (ADSL/VDSL)	50/20 Mbit/s
Holice	50/5 Mbit/s (DSL)	50 Mbit/s (ADSL/VDSL)	50/5 Mbit/s (ADSL/VDSL)	50/5 Mbit/s (VDSL)	150/20 Mbit/s
Červená voda	20/2 Mbit/s (DSL)	20 Mbit/s (ADSL/VDSL)	20/2 Mbit/s (ADSL/VDSL)	8/8 alebo 20/2 Mbit/s (ADSL/VDSL)	50/20 Mbit/s
Přelouč	20/2 Mbit/s (DSL)	30 Mbit/s (ADSL/VDSL)	20/2 Mbit/s (ADSL/VDSL)	8/8 Mbit/s (ADSL)	150/20 Mbit/s
Litomyšl	20/2 Mbit/s (DSL)	20 Mbit/s (ADSL/VDSL)	20/2 Mbit/s (ADSL/VDSL)	8/8 alebo 20/2 Mbit/s (ADSL/VDSL)	50/20 Mbit/s
Žamberk	20/2 Mbit/s (DSL)	20 Mbit/s (ADSL/VDSL)	50/5 Mbit/s (ADSL/VDSL)	8/8 alebo 20/2 Mbit/s (ADSL/VDSL)	50/20 Mbit/s
Svitavy	20/2 Mbit/s (DSL)	20 Mbit/s (ADSL/VDSL)	20/2 Mbit/s (ADSL/VDSL)	x	50/20 Mbit/s

Vysoké Mýto	100/10 Mbit/s (DSL)	100 Mbit/s (ADSL/VDSL)	100/10 Mbit/s (ADSL/VDSL)	8/8 alebo 100/10 Mbit/s (ADSL/VDSL)	150/20 Mbit/s
Ústí nad Orlicí	20/2 Mbit/s (DSL)	30 Mbit/s (ADSL/VDSL)	x	8/8 Mbit/s (ADSL)	x
Skuteč	50/5 Mbit/s (DSL)	50 Mbit/s (ADSL/VDSL)	50/5 Mbit/s (ADSL/VDSL)	8/8 alebo 50/5 Mbit/s (ADSL/VDSL)	150/20 Mbit/s
Hlinsko	20/2 Mbit/s (DSL)	100 Mbit/s (ADSL/VDSL)	20/2 Mbit/s (ADSL/VDSL)	8/8 alebo 20/2 Mbit/s (ADSL/VDSL)	50/20 Mbit/s
Polička	50/5 Mbit/s (DSL)	50 Mbit/s (ADSL/VDSL)	50/5 Mbit/s (ADSL/VDSL)	8/8 alebo 50/5 Mbit/s (ADSL/VDSL	150/20 Mbit/s
Chrudim	100/10 Mbit/s	100 Mbit/s (ADSL/VDSL)	20/2 Mbit/s (ADSL/VDSL)	100/10 Mbit/s (VDSL)	150/20 Mbit/s