Využití access listů pro vymezení přístupu uživatelů ve firemní počítačové síti

Adrián Košťál

Bakalářská práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

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

Jméno a příjmení:	**Adrián Košťál**
Osobní číslo:	**A12102**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Využití access listů pro vymezení přístupu uživatelů ve firemní počítačové síti**
Téma anglicky:	**The Use of Access Lists for Defining User Access in a Corporate Computer Network**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Vyřešte IP adresaci v síti pro diferencovaný přístup skupin a jednotlivců.**
3. **Navrněte funkční model sítě.**
4. **Konfigurujte access listy na Cisco aktivních prvcích.**
5. **Vyhodnoťte vliv access listů na diferencovaný přístup skupin a jednotlivců ve firemní síti.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LAMMLE, Todd. Inc. Cisco Certified Network Associate. Alameda: SYBEX Inc., 1999. ISBN 0-7821-2647-2.**
2. **M. THOMAS, Thomas. OSPF Network Design Solutions: Second Edition. Indianapolis: Cisco Press, 2003. ISBN 1-58705-032-3.**
3. **SOSINSKY, Barrie A. Mistrovství počítačové sítě. Vyd. 1. Brno: Computer Press, 2010, 840 s. ISBN 978-80-251-3363-7.**
4. **COLE, Eric a James W CONLEY. Network security bible: autorizovaný výukový průvodce. Indianapolis: Wiley Publishing, 2009, 891 s. ISBN 978-0-470-50249-5.**
5. **Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S. In: Cisco Systems, Inc. [online]. San Jose, 2014 [cit. 2015-02-03]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/sec-data-acl-xe-3s-book.pdf.**

Vedoucí bakalářské práce:	**Ing. Miroslav Matýsek, Ph.D.** Ústav počítačových a komunikačních systémů
Datum zadání bakalářské práce:	**6. února 2015**
Termín odevzdání bakalářské práce:	**3. června 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně 3. 6. 2015

.....
podpis diplomanta

ABSTRAKT

Cieľom práce bolo vytvoriť model reálne fungujúcej firemnej siete s aplikovaním prístupových zoznamov pre diferencovaný prístup jednotlivých užívateľov, alebo skupín k sieťovým prostriedkom a internetu. Po overení funkčnosti komunikácie v modelovej sieti bolo úlohou nakonfigurovať Cisco aktívne zariadenie. Výsledkom riešenia danej problematiky je sieť v simulačnom prostredí a zoznam použitých príkazov z programovania skutočných zariadení.

Kľúčové slová: Počítačová sieť, Bezpečnosť, Ochrana, Prístupové Zoznamy, IP adresa

ABSTRACT

The goal of this work, was creating a real model of function company network with aplicating an access lists, in different levels of access for all users or groups to network components and internet. After verification the functionality of communication in model network, my quest was configurating a Cisco active device. The result of address the issue is network in simulation interface and list of used commands from programing the real devices.

Keywords: Computer network, Security, Firewall, Access List, IP address

POĎAKOVANIE

Týmto by som rád poďakoval predovšetkým svojmu vedúcemu za ochotu pracovať so mnou na tejto práci. Ďakujem patrí taktiež aj pánovi Ing. Jiřímu Korbelovi za umožnenie prístupu do odbornému laboratóriu s aktívnymi prvkami, kde som mohol vykonať odskúšanie konfigurácie.

OBSAH

ÚVOD

V dnešnej dobe sú počítačové siete súčasťou väčšiny firiem alebo spoločností. Tvoria základ komunikácie a prenosu dát medzi jednotlivými zariadeniami, či už sa jedná o malú lokálnu alebo veľkú svetovú sieť. Veľkým rozšírením a vysokou dostupnosťou bežnému užívateľovi vzrastá aj možnosť ohrozenia. Ide o útoky pôsobiace na sieť a ich úlohou je spôsobiť škody, napríklad odcudzenie osobných údajov, stratu dát alebo znefunkčnenie siete. Dôvodom zníženia počtu napadnutí vo firemnej sieti bolo rozhodnutie zaoberať sa práve touto témou.

V prvej časti sa práca zameriava na komplexný návrh vytvorenia firemnej siete. Obsahuje celkovú IP adresáciu každého zariadenia s použitím privátnej adresy a podsieťovania. Ďalším krokom bolo vytvorenie modelu siete podľa skutočných parametrov a požiadaviek na správnu funkčnosť. Realizácia modelu siete prebehla v simulačnom prostredí programu Cisco packet tracer a umožňuje nakonfigurovať virtuálne zariadenie s funkciami reálneho routru.

V ďalšej časti bolo cieľom vytvoriť diferencovaný prístup jednotlivcom a skupinám vo firemnej sieti k službám pomocou prístupových zoznamov. Pridelením práv jednotlivcom má za následok obmedzenie prístupu do siete neoprávneným osobám a zníženie možnosti napadnutia siete, či už z vonku alebo z vnútra siete.

Možné riziká a útoky treba eliminovať a je potrebné dbať na bezpečnosť v aktívnej sieti. Konfigurácia prístupových zoznamov je hlavným prínosom pre každého správcu siete, ktorý ich zavedie do priameho použitia v praxi. Pri ich aplikovaní sa výrazne zvýši plynulosť prevádzky a znížia sa hrozby pre dáta a funkčnosť systému.

Posledná časť obsahuje prepojenie jednotlivých aktívnych zariadení a celkovú konfiguráciu podľa vopred vytvoreného modelu. Po nej nasledovalo vyskúšanie prenosu dát a zistenie, či všetky časti a nastavenia siete fungovali správne.

I. TEORETICKÁ ČÁST

1 IP ADRESY

Počítačová sieť, ako je všeobecne známe, obsahuje koncové zariadenie, ktorým možno chápať počítač alebo tlačiareň. Komunikácia medzi nimi prebieha za pomoci IP adresy danej buď administrátorom siete alebo je pridelená automaticky. Najčastejšie je v sieti prideľovaná konkrétna adresa pre jedno zariadenie, nakoľko toto číslo musí byť jedinečné a len jedno v sieti, inak by sieť nemohla fungovať a nastávali by komplikácie pri prenose dát. Na začiatku konfigurácie siete musí administrátor vypočítať približný počet zariadení, ktorým bude potrebné prideliť IP adresu a vhodným riešením je zvoliť väčší rozsah pre možné rozrastanie siete [1].

1.1 IPv4

Jedná sa o prvú verziu prenosového protokolu IP verzia 4 s označením IPv4 (Internet Protokol version 4). V súčasnosti je IPv4 považovaný za štandard, avšak na základe malého množstva možných pridelených IP adries sa už voľné adresy minuli. Vyčerpanie bolo predpokladané už pred mnohými rokmi, keďže pri zavedení tohto štandardu nepočítali s tak rozsiahlym využitím pre mnoho druhov zariadení. Z tohto dôvodu vznikla technológia NAT (Network Address Translation). Jej funkciou je schovanie celého rozsahu privátnych adries za jednu verejnú. Pomocou nej sa podarilo oddialiť vyčerpanie, avšak nebolo možné predísť tejto situácii. Novým štandardom pre IP adresáciu sa stal protokol IPv6 (Internet Protokol version 6) [2].

Za IP adresu považujeme 32 bitové číslo, a teda matematicky 2^{32}, ktoré je rozdelené na štyri časti po 8 bitov, to znamená že najvyššie možné použiteľné číslo v jednom oktete môže byť 255. Ako príklad IP adresa 192.168.125.113. Pri vnútorných (súkromných) sieťach sa za týmto číslom ďalej definuje, do akej triedy adresa patrí. Tak isto z neho vyplýva, koľko voľných IP adries možno prideliť zariadeniam v sieti. Pri adrese 192.168.0.0/24 je využitých posledných 8 bitov (číslo na konci) k zadefinovaniu zariadení. 8 bitov = rozsah od 0 do 255 čo znamená 254 voľných IP adries nakoľko adresa 192.168.0.0 je označovaná ako názov siete a 192.168.0.255 znamená obežník. Celkový počet použiteľných adries vo svete je 4 294 967 296, ale nie každú adresu je možné použiť. Na každú novú podsieť sa strácajú 2 adresy a existujú ďalšie rozsahy IP adries vyhradené na osobitné účely a nemožno ich použiť v bežnej sieti (triedy adries D a E) [3].

IP adresy rozdeľujeme na:

- verejné,
- ilegálne,
- súkromné → A: 10.0.0.1 - 10.255.255.254,
  → B: 127.16.0.1 - 172.31.255.254,
  → C: 192.168.0.1 - 192.168.255.254.

Podľa prvého oktetu (čísla) sa verejné IP adresy delia na:

Tab. 1. Delenie IP adries

	1. OKTET	**IP ADRESA**			
A	0-126	S	H	H	H
B	128-191	S	S	H	H
C	192-223	S	S	S	H
D	224-239	MULTICAST			
E	240-255	Špeciálne výskumné účely			

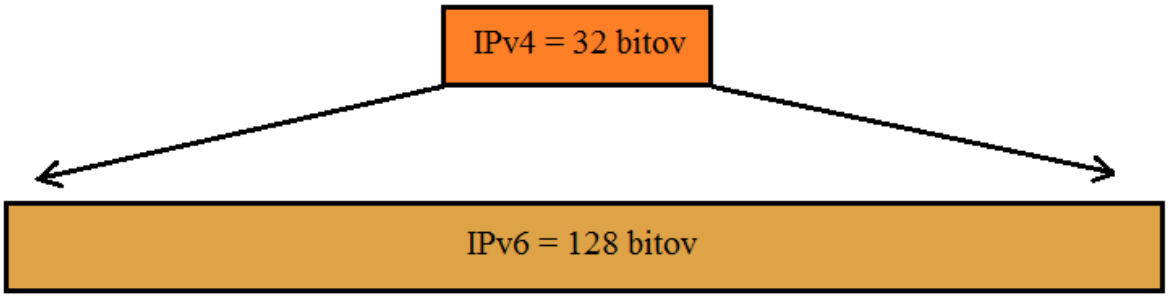
S - adresa sieťe,

H - adresa hostiteľa.

1.2 IPv6

IPv6 je nový štandard nahradzujúci dodnes používaný protokol IPv4. Dôvodom prechodu je vyčerpanie všetkých adries, bezpečnosť a zaistenie čo najmenšieho fragmentovaného adresného priestoru. Najviditeľnejšou zmenou medzi v4 a v6 je dĺžka adresy. Zväčšila sa z 32 bitov na 128 bitov, čo umožňuje rozsah adries na $2^{128} = 3.4 \times 10^{38}$.

Porovnanie adresného priestoru:



Obr. 1. Porovnanie veľkosti adries

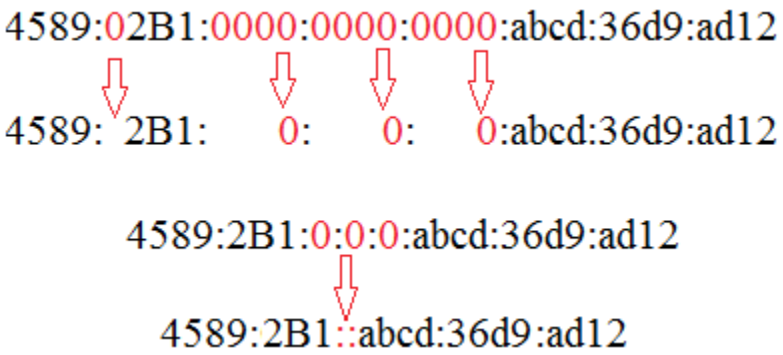
Počet možných kombinácií je teda veľmi veľký, na jedného človeka pripadá $5*10^{28}$ adries. IPv6 bol prijatý ako nasledovník už pred mnohými rokmi, avšak celosvetové používanie je zatiaľ niekoľko percent v porovnaní s veľkosťou celosvetovej IPv4 siete [4].

Najčastejším a najprehľadnejším zápisom je hexadecimálny tvar 16^{32}, kedy každý znak môže vyjadrovať 16 možností. Tvar adresy IPv6 vyzerá napríklad takto: 4589:5:2b1:df:369:b687:abcd:36d9. V situáciach, kedy adresa obsahuje postupnosť aspoň dvoch po sebe idúcich bajtov s hodnotou 0, ide zápis adresy upraviť do tvaru dvojitej dvojbodky [4].

Príklad: adresa má hodnotu **4589:02b1:0000:0000:0000:abcd:36d9**

zjednodušený zápis **4589:2b1::abcd:36d9**

Postup:



Obr. 2. Zjednodušenie zápisu IPv6

Toto zjednotenie možno použiť len jedenkrát v adrese.

Adresový model IPv6:

- Priraďuje sa rozhraniam.
- Rozhranie v IPv6 má spravidla niekoľko adries.
- Má svoj rozsah.
- Určený čas platnosti.
- Vlastný typ.

Kategórie IPv6 adries:

- Adresy z rozsahu **FE80::/10**, napríklad **FE8**, **FE9**, **FEA** a **FEB** umožňujú komunikáciu dvom uzlom v rovnakej sieti. Nevyžaduje explicitné nastavenie akejkoľvek adresy, vygenerovanie a pridelenie je úlohou operačného systému. Komunikácia medzi uzlami z rôznych sietí nie je možná. Tento spôsob umožňuje ušetriť adresy, nakoľko môžu byť použité v smerovacích tabuľkách smerovačov a nemusíme adresovať spojenie medzi nimi.
- Adresy začínajúce **FF**, t.j. z rozsahu **FF00::/8** vyznačujeme ako adresy pre multicasting (podobne ako trieda D pri IPv4).
- **0:0:0:0:0:0:0:0/128, (**skrátene **::/128)** nešpecifikovaná adresa používaná pre komunikáciu samého seba, tzv. loopback.
- Ostatné verejné adresy bežne používané, začínajú prvými bajtmi v rozsahu od **2000** až **3FFF** s prefixom **/ 3**.

Vlastnosti IPv6:

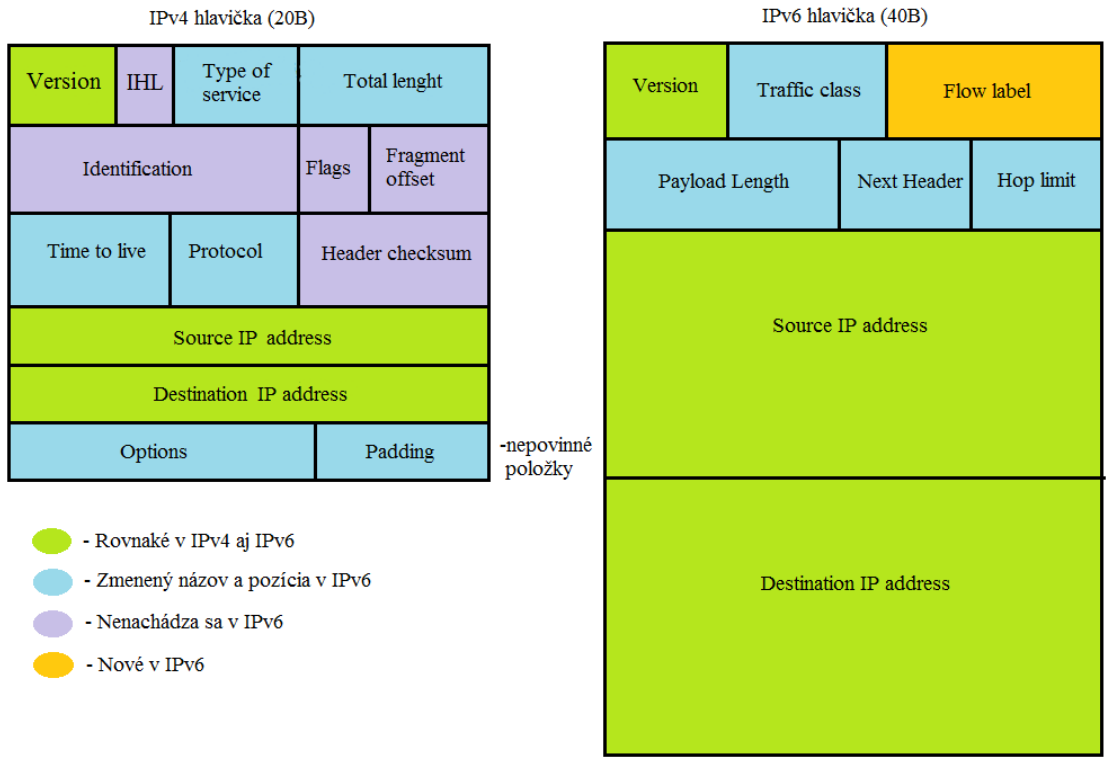
- Rozšírený adresný priestor.
- Globálna dosiahnuteľnosť.
- Agregácia.
- Multihoming.
- Autokonfigurácia.
- Plug-and-Play.
- Komunikácia bez NAT.
- Efektívne smerovanie.

- Bez broadcastov.
- Mobilita a bezpečnosť.

Po pripojení počítača do siete fungujúcej na protokole IPv6 operačný systém automaticky pridelí tomuto rozhraniu link-local adresu. Vytvorí ju spojením predčíslia FE80:: a hodnoty MAC (Media Access Control) adresy pripojeného zariadenia. Týmto spôsobom generácie číslo získa záruku unikátnosti, keďže samotná MAC adresa je jedinečná. Následne operačný systém očakáva periodické správy zo smerovača, ktoré sú povinne odosielané. Obsahujú informácie o adrese IPv6 a sieti, v ktorej sa nachádza. Stanica si uloží na svoje sieťové rozhranie adresu získanú od smerovača. Vďaka tomuto postupu nie je potrebné používať službu DHCP (Dynamic Host Configuration Protocol) na automatické pridelenie adresy. Platí to pri jednoduchších IPv6 sieťach [5], [20].

Zmenou oproti protokolu IPv4 je štruktúra hlavičky paketu, ktorá už neobsahuje málo používané polia, alebo boli zmenené na nepovinné. Spracovanie je jednoduchšie a hoci hlavička paketu protokolu IPv6 má veľkosť 40B, čo je dvojnásobná veľkosť oproti hlavičke IPv4, zatiaľ neboli zistené žiadne negatívne vlastnosti [5].

Porovnanie hlavičiek IPv4 a IPv6



Obr. 3. Porovnanie hlavičiek protokolov

- **Version** - IPv4 / IPv6.
- **IHL** - informácia o veľkosti hlavičky.
- **Type of service** - QOS (quality of services) typ služby určuje spôsob spracovania datagramu.
- **Total lenght** - dĺžka paketu vrátane hlavičky a dát.
- **Identification** - jednoznačná identifikácia datagramu.
- **Flags** - indikuje fragentáciu IP paketu pri prenose.
- **Fragment of set** - pri fragmentácii udáva, kam fragment patrí.
- **Time to live** - ochrana proti zacykleniu.
- **Protocol** - informácia o zapuzdrenom protokole z vyššej vrstvy.
- **Header checksum** - kontrolný súčet veľkosti dát hlavičky.
- **Source address** - adresa odosielateľa.
- **Destination IP address** - adresa komu sú dáta smerované.
- **Traffic class** - trieda dát.
- **Flow label** - identifikácia toku dát.

- **Payload length** - dĺžka dát.
- **Next header** - ďalšia hlavička.
- **Hop limit** - funkcia time to live (ochrana proti zacykleniu).

1.2.1 Typy IPv6 adries

- Unicast
  - Adresa je pridelená jedinému sieťovému rozhraniu a pakety sú poslané len tomuto konkrétnemu zariadeniu.
- Multicast
  - Pre one-to-many adresovanie (jedna adresa viacerým zariadeniam).
  - Efektívnejšie využíva prostriedky siete.
  - Používa širší adresový rozsah.
- Anycast
  - One-to-nearest (alokované z unicastového priestoru).
  - Všetky takéto zariadenia by mali poskytovať rovnaké služby.
  - Zdrojové zariadenia odosielajú pakety na anycast adresu.
  - Smerovače rozhodnú o najbližšom uzle s danou adresou.

1.3 Maska podsiete

Maska podsiete je číslo priradené k IP adrese a určuje jednotlivého hostiteľa, sieť alebo konkrétny rozsah siete. Umožňuje vytvoriť z jednej sieťovej adresy viac adries podsietí, a tým získať väčší priestor pre adresovanie. Maska siete je 32 bitové číslo rozdelené na 4 časti, v každom z bajtov určuje bit s hodnotou 1 adresu siete a v ostatných bitoch budú nuly, ktoré vyjadrujú voľné adresy pre podsieťovanie. Masky sa rozdeľujú do troch skupín:

Trieda A: 255.0.0.0,

Trieda B: 255.255.0.0,

Trieda C: 255.255.255.0.

Tieto masky nemožno zameniť v zmysle, že nie je možné nastaviť masku podsiete triedy B na 255.0.0.0. V tomto prípade bude hostiteľ považovať adresu za neplatnú, a obvykle ju nemožno zadať. V prípade triedy A nie je možné zmeniť prvý bajt v maske, v zásade musí byť jej hodnota minimálne 255.0.0.0. Podobne nie je možné nastaviť hodnotu 255.255.255.255, pretože obsahuje samé jednotky a jedná sa o obežník [6], [9].

1.4 Čísla Portov

Protokoly TCP (Transmition Control Protocol) a UDP (User Datagram Protocol) musia pri komunikácii s vyššími vrstvami používať čísla portov. Tieto čísla totiž dovoľujú rozlišovať rôzne komunikácie, ktoré sú v sieti aktívne v jeden časový okamžik. Zdrojový hostiteľ dynamicky na zdrojovej strane prideľuje čísla portov s hodnotou 1024 a viac. Čísla portov do hodnoty 1023 sú definované v štandarde RFC 3232, ktorý sa zaoberá známymi portami. Virtuálne okruhy, ktoré nepoužívajú aplikácie s dobre známym číslom portu, majú miesto toho pridelené náhodné čísla portov z určitého rozsahu. Tieto čísla portov identifikujú v segmente TCP zdrojovú a cieľovú aplikáciu alebo proces. Zdroj pri každom novom spojení volí iné čísla portov, vďaka čomu môže rozlišovať relácie s rôznymi hostiteľmi. Ak by server nemal od odosielajúceho hostiteľa jedinečné číslo, nevedel by odkiaľ informácie prichádzajú. Protokol TCP a protokoly vyšších vrstiev nerozlišujú odosielajúceho hostiteľa podľa hardwarovej a logickej adresy ako protokoly linkovej a sieťovej vrstvy. Miesto toho používajú čísla portov. Je možné ľahko si predstaviť, aký zmätok by nastal na strane prijímajúceho hostiteľa, keby všetci hostitelia požadovali pripojenie napríklad k FTP (File Transfer Protocol) pomocou rovnakého čísla zdrojového portu [6], [10], [15].

Kľúčové porty založené na protokoloch TCP a UDP:

Tab. 2. Najpoužívanejšie porty

TCP	**UDP**
FTP 21	DNS 53
Telnet 23	TFTP 69
SMTP 25	SNMP 161
DNS 53	
HTTP 80	
HTTPS 443	

2 BEZPEČNOSŤ SIETE

Každá sieť sa môže stať terčom útoku. V každom okamžiku hrozí napadnutie stále prepracovanejšími a neustále sa vyvíjajúcimi vírmi, škodlivým softwarom alebo priame ohrozenie siete útokom narušiteľa. Napadnutie škodlivým softwarom alebo priamou infiltráciou do siete bežný užívateľ nepozná. Najčastejším príznakom je spomalenie počítača, zahltenie siete a v najhorších prípadoch prázdny účet alebo znefunkčnenie prevádzky siete. Ak sa chod siete spomalí alebo niektoré zariadenie nepracuje ideálne, skontrolujte svoj stav antivírusovej ochrany. Na zabezpečenie existuje veľa návodov, no najskôr treba analyzovať možné hrozby. Každý systém pre ochranu je prelomiteľný, či už z vonku alebo jednoduchšie, z vnútra siete. Odporúčanou metódou je využitie viacerých vrstiev zabezpečenia, kedy útočník musí postupne prelomiť dve alebo viac bariér. Dôležitou súčasťou bezpečnej siete je pravidelná zmena hesla a bezpečné oddelenie dvoch častí siete.

2.1 Hrozby od užívateľa v sieti

Veľké percento ohrozenia tvoria práve užívatelia (najčastejšie zamestnanci) vo firemnej LAN (Local Area Network). Toto nebezpečenstvo nemá väčšinou pravý pôvod na lokálnom počítači, taktiež ale existujú výnimky. Infiltrácia obvykle dorazí na zariadenie nakazeným pamäťovým zariadením. Ďalší prípad nastáva pri nedostatočnej kontrole nad právami používateľov, kedy ich konanie na internete môže spôsobiť závažné problémy. Užívateľ stiahne súbor, či už z mailu alebo omylom klikne na skrytý link a stiahne infikovanú aplikáciu. Jej činnosť môže mať rôzne dopady na sieť [4].

2.1.1 Vírusy

Vírus je kód alebo kľúč vytvorený k napadnutiu hostiteľského programu a rozšíreniu sa, keď je infikovaný program spustený. Vkladá svoje kópie do iných súborov a tak získava prostriedky na ďalšie rozmnožovanie. Jeho súbory sa stávajú prostriedkom na správne fungovanie. To znamená, že vírus je sám reprodukovateľný, teda obnoviteľný a okamžite sám účinkuje. Niektoré sa spúšťajú s oneskorením, teda v určitý deň a čas sa vírus spustí na všetkých infikovaných zariadeniach pre cielený hromadný útok za účelom zahltenia serveru alebo siete. Prenášané sú mnohými cestami, kedy nevedomky užívateľ spustí

disketu, CD (Compact Disk), výmenný pevný disk, vrátane súborov stiahnutých z internetu alebo emailové prílohy. Vplyv vírusu na systém závisí od druhu, keďže každý vírus je vytvorený za iným účelom. Najčastejšími príznakmi činnosti vírusu je spomalenie zariadenia, nestabilita systému, zmeny kapacity disku atď. [2], [12].

Podľa umiestnenia v pamäti delíme vírusy na:

- **Rezidentné** - spustenie napadnutého programu spôsobí trvalé uloženie vírusu do pamäte počítača (najčastejšie do konvenčnej pamäte) a za určitých podmienok môže napadnúť ďalšie programy, jeho činnosť sa zvyčajne končí po resetovaní alebo vypnutí počítača. Po usadení vírus sleduje užívateľa a jeho činnosť.
- **Nerezidentné** - nákazu spôsobuje len spustenie napadnutého vírusu, nevyužíva operačnú pamäť [2], [12].

Počítačové vírusy sa prenášajú medzi systémovými mechanizmami zabudovanými do operačných systémov alebo aplikácií, ktoré napádajú. Existuje mnoho neškodných vírusov a autori ich vyvíjajú skôr ako cvičenie v programovaní, avšak mnohé ďalšie nesú so sebou mnoho nebezpečenstva a snažia sa zmeniť, alebo poškodiť dáta či systém [2].

2.2 Útoky ohrozujúce LAN

- **Denial of service (DoS)** útočník vysiela množstvo žiadostí na server, ktorý všetky ukladá do zásobníka v poradí podľa prijatia. Úlohou je zahltenie systémových zdrojov tak, že nemôže reagovať na žiadosti o pripojenie. DoS útok môže byť efektívne vykonaný zaplavením toľkých súčasných žiadostí, až dôjde k pádu systému a jeho reštartu. Iný spôsob je prenos obrovských položiek na systémový pevný disk, využitie celého priestoru pamäte [11].
  - **Buffer overfow** - Preplnenie vyrovnávacej pamäte - proces získava omnoho viac dát ako predpokladá. Ak proces nemá naprogramované rutinné riešenie nadmerného toku údajov, koná neočakávaným spôsobom, čo môže útočník využiť. Napríklad ping-of-death útok využije Internet Control Message Protocol (ICMP) na zasielanie nepovolených ECHO balíkov s viac ako 65K oktetmi dát, ktoré môžu byť príčinou preplnenia systému premennými a vedú k zrúteniu systému. Preplnením vyrovnávacej pamäte sa zvyčajne snaží tlačiť zneužitý kód na zásobník, a potom modifikovať adresu návratu k pracovaniu škodlivého kódu [3], [12].

- **SYN attack** - Útočník využíva vyrovnávaciu pamäť TCP protokolom. Úlohou je zaplnenie cieľového systému malými žiadosťami v stave spracovania podľa poradia nadviazaného spojenia. Na žiadosti napadnutej siete nikto neodpovedá a nereaguje. Tieto príčiny zadržujú systém, ktorý čaká na riadnu odpoveď. Systém sa v tejto chvíli stáva nepoužiteľným a častým následkom býva jeho zrútenie [3].
  - **TCP SYN attack** - Tento typ prívalového útoku zneužíva serverové tri cesty nadviazania spojenia. Počas klasického trojcestového nadviazania spojenia, klient pošle serveru SYN správu a server pošle späť SYN-ACK, keď klient pošle nakoniec ACK späť, skompletizuje nadviazanie spojenia. TCP SYN prívalový útok zneužíva tento proces nastavovaním klienta neposielať späť záverečnú ACK správu, čo spôsobuje situáciu známu ako "polootvorené" spojenie. Toto polootvorené spojenie môže byť jednoducho vytvorené cez IP pascu (spoofing). Útok klient bude posielať napálenému SYN paketu do cieľového serveru, ale keď server skúsi poslať SYN-ACK späť, cieľová IP nie je schopná uzavrieť nadviazanie spojenia s ACK. Ako výsledok, server naplní svoju pamäť dátami opisujúcimi všetky tieto nevyriešené pripojenia. Ihneď ako je pamäť plná, zariadenie nebude prijímať nové spojenia dokedy nevyčistí svoju pamäť. Servery budú napokon zadržovať infikované požiadavky, ktoré môže útočník stále posielať. V niektorých prípadoch sa systém môže zrútiť z konštantných žiadostí. Je tu niekoľko prostriedkov obrany pred TCP SYN prívalom, v závislosti na type služby siete pri poskytovaní. Umiestnenie serverov za firewall založený na zastavení prichádzajúcich SYN paketov je prevenciou tohto typu útoku [3], [8].
- **Teardrop attack** - Modifikuje dĺžku a fragmentáciu vyrovnávacieho poľa v sekvenčnom IP protokole paketov. Cieľový systém sa potom stane zmäteným a zrúti sa po obdržaní protichodných inštrukcií na to, v akom nepomere sú tieto fragmenty paketov [12].
- **Smurf** - Útok zahŕňa hackerské metódy (IP spoofing, ICMP) za potrebou vniknutia do prevádzky cieľovej siete, následne spustí DoS útok. Pozostáva z troch elementov: vstupná stránka, odrazová stránka, cieľová stránka. Útočník (vstupná stránka) posiela falošné ping pakety vysielacej adrese širšej siete (odrazová stránka). Tento modifikovaný paket obsahuje adresy cieľovej siete. Toto spôsobí, že paket dostanú všetky zariadenia v odrazovej sieti. Každé z nich reaguje

opätovným vyslaním odpovede na adresu cieľovej stránky. Následne môže prísť k zahlteniu siete s nutným reštartom zariadení [3], [12].

- **Back door** - Útok prebieha pomocou dial-up modulu, alebo asynchrónnym externým pripojením. Stratégia spočíva v prístupe cez premostenie kontrolných mechanizmov tým, že zariadenie sa tvári ako modem [8].
- **Spoofing** - IP spoofing je používaný votrelcom na presvedčenie systému, že komunikuje so známym, overeným objektom k poskytnutiu prístupu do systému. IP spooofing zahŕňa zmeny paketu na TCP leveli, ktorý sa používa k útoku na systémy poskytujúce rôzne služby. V skutku útočník posiela pakety, v ktorých je ako zdrojová adresa uvedená IP známeho, dôveryhodného hostiteľa namiesto vlastnej. Cieľový hostiteľ akceptuje paket a akcia sa môže začať [8].
  - **DHCP spoofing** - V LAN sa nachádza neznáme zariadenie, ktoré sa správa ako DHCP server. Odpovedá klientom na požiadavky DHCP a priradí im nesprávne IP adresy. Celá komunikácia následne prebieha cez pridanú bránu a útočník môže skúmať celý obsah paketu [3].
- **Man in the middle** - Útočníci napichujú samých seba v centre komunikácie - napríklad, útočník A dosahujúci jeho, alebo jej verejný kľúč pre inú osobu P. Potom, ktokoľvek chce poslať zakódovanú správu osobe P použitím verejného kľúča osoby P, je nevedome použitý verejný kľúč útočníka A. Z toho dôvodu, A môže čítať správy určené pre P. A potom môže správy poslať P, zakódované v reálnom verejnom kľúči osoby P. Samozrejme, A môže modifikovať správu pred preposlaním osobe P [3], [8].
- **Port scanning** - Tento spôsob napadnutia využíva skenovací softvér na určenie stavu, či je zariadenie aktívne alebo nie. Táto technika pomáha vyhnúť sa márneniu času neaktívnymi hostiteľmi. Port skenuje zhromažďovanie dát o jednotlivých hostiteľoch v rámci podsiete. Skenovanie môže byť uskutočnené použitím PING pomocným programom. Po určení, ktorí hostitelia a pridružené porty sú aktívne, útočník bude iniciovať rôzne typy skúmania na aktiváciu portov. Príklady skúmania sú nasledujúce:
  - zhromaždenie informácii z Domain Name System (DNS),
  - určenie sieťových služieb, ktoré sú prístupné, ako e-mail, FTP, a vzdialené zahájenie činnosti,
  - určenie typu a zverejnenie / prepustenie operačného systému [3].

Ping of death - Tento typ útoku je využívaný zámerne vytvorením IP paketu na overenie cieľového systému s IP veľkosťou väčšou ako maximum 65,535 bytov. IP pakety tejto

veľkosti nie sú normálne povolené, ale fragmentáciou IP paketu za účelom zhromaždenia čo možno najväčšej veľkosti akú môže dosiahnuť. Keď sa snaží o znovu zhromaždenie paketu, cieľový systém skúsi preplniť zásobník a ten spadne. Prevencia tohto typu útoku je vykonaná umiestnením kontrolného prvku pre maximálnu veľkosť IP paketu na firewall. Tie, ktoré sú väčšie ako maximálna veľkosť budú vymazané [3], [7].

2.3 Heslo

Heslo môžeme považovať za bezpečný prostriedok pri autorizácii vstupu do systému, alebo siete. Jeho sila je založená na počte a druhu znakov. To znamená, čím viac rôznych znakov v hesle použijeme, tým je jeho sila väčšia. Silu hesla môžeme definovať ako prekážku, cez ktorú musí neoprávnená osoba prejsť, ak sa chce dostať do systému. Pri použití veľmi silného hesla sa čas potrebný na jeho prelomenie zvyšuje, čo často odrádza útočníkov. Slabé heslo nie je zložité prelomiť za krátky čas s použitím techniky „hrubá sila„ alebo „slovníkovým útokom„. Okrem prelomenia slabého hesla ho možno uhádnuť, ak heslo tvorí dátum narodenia, postupnosť čísel, poprípade meno blízkej osoby alebo svoje. Za základy bezpečnosti sa považuje heslo si nikde nepísať, obzvlášť nie v blízkosti počítača, nepoužívať jedno heslo na viacerých dôležitých účtoch. Heslo pre prihlásenie do siete je potrebné meniť každý jeden až dva mesiace, toto nariadenie môže zaviesť administrátor.

3 FIREWALL

V súčasnosti, kedy počítačové siete nadobúdajú stále väčšie rozmery ako aj možnosť útoku tretej strany za účelom získania dôležitých informácií, alebo úmyselného poškodenia, riziko hrozieb narastá. S vyvíjajúcimi technológiami sa aj počet útočníkov a rôznych nežiaducich softwarov vyšší. Za účelom chránenia nášho počítača proti útočníkom zo siete, alebo internetu a niektorým druhom malvéru bez autorizovaného prístupu, bol vyvinutý firewall. Je to špeciálne bezpečnostné zariadenie umiestnené medzi „internetom„ a privátnou sieťou ktoré funguje ako brána, cez ktorú musia prejsť všetky dáta. Neustále sleduje komunikáciu, ktorá vstupuje a vystupuje cez toto pripojenie. Popri tom si dáva pozor na prevádzku, kedy môže podľa zavedených pravidiel zamietnuť alebo povoliť prístup do siete. Firewall je teda bezpečnostný prostriedok v globálnej sieti, kde inak neplatia žiadne pravidlá. Jeho úlohou je neustále strážiť bezpečnosť zapojených prostriedkov v sieti [7], [13].

Firewall je kombinácia hardwaru a softwaru, ktorá izoluje vnútornú sieť organizácie od veľkého internetu a umožňuje nechať prejsť niektoré pakety a zablokovať iné. Brána firewall umožňuje správcovi siete vykonávať kontrolu prístupu medzi vonkajším svetom a prostriedkami spravovanej siete riadením prenosových tokov smerom k týmto prostriedkom a od nich [3].

Firewall kontroluje sieťovú komunikáciu, ktorá vstupuje do niektorého z jeho rozhraní a aplikuje na ňu bezpečnostné opatrenia. Na základe týchto pravidiel prenos povolí, alebo zamietne. Základom tohto druhy ochrany je oddelenie siete od internetu. Využíva sa hardwarové zariadenie v jednom počítači, a ide teda o takzvanú fyzickú izoláciu siete. Firewall môže komunikovať do externej siete jedným protokolom a do privátnej iným. Tento druh komunikácie nazývame protokolovou izoláciou. Taktiež filtrujú prevádzku siete podľa zdrojovej a cieľovej IP adresy, podľa protokolu a stavu pripojenia, a môžu zabrániť infekčným červom, ale aj ďalším útokom pomocou niekoľkých ciest. Typickým a súčasne najúčinnejším prostriedkom ochrany je klasické použitie firewallu pre blokovanie portu, ktoré v systéme za zariadením nepotrebujeme používať. Rovnako môže ovládať tok smeru von zo siete. Spoločnosti často umožňujú webovým serverom prístup na port TCP/80, avšak z niekoľkých dôvodov to nie je príliš dobré riešenie. Následkom môže byť, že cez tento port vnikne červ do siete a rovnakým portom ho môže aj opustiť [8], [14].

Existuje veľa typov firewallu, ktoré môžu byť veľmi jednoduché, ale aj veľmi zložité. Najčastejšie sú aplikované ako software, alebo software nainštalovaný na hardwarové zariadenie, poprípade ide rovno o hardwarové zariadenie. S firewallom v softwarovej podobe sa najčastejšie stretávame v prostredí operačného systému, kedy je jeho súčasťou (Windows, Linux). Iné majú podobu malého zariadenia, ktoré má vlastný operačný systém a slúži ako nepreniknuteľná brána [21].

3.1.1 Delenie

Firewally delíme do niekoľkých skupín:

- Personálne firewally.
- Firewally v smerovačoch.
- Hardwarové (nižšie aj vyššie kategórie).
- Serverové firewally.
- Proxy firewally.

Dnešné firewally často pokrývajú viac ako jednu z týchto kategórií. Pri porovnávaní musíme dbať na niekoľko faktorov: vlastnosti, výkonnosť (meriame priepustnosť) a cena. Pre porovnanie alebo otestovanie firewallov neexistuje žiadny bežný výkonnostný test, preto každý výrobca používa svoje metódy ktoré nechce zverejniť [21].

3.1.2 Personálny firewall

Softwarový firewall určený pre osobnú ochranu jedného počítača sa v malých domácich sieťach vyskytuje menej často. Aplikácia do operačného systému spôsobila veľký prevrat. Prvá verzia OS s firewallom je Microsoft XP SP1. Jeho pridanie do systému pomohlo lepšiemu zabezpečeniu a ochrane pred vonkajšími útokmi. Tento typ ochrany môže mať negatívny vplyv na starší počítač, kedy firewall spomaľuje počítač. Nepríjemným sa môžu stať vyskakovacie okná a dialógy, ktoré prerušujú prácu a pýtajú si rôzne potvrdenia k vykonaniu akcie. Systém by mal pracovať samostatne, avšak nie je dobré používať dva alebo viac programov súčasne. Pôsobením viacerých softwarov môžu nastať neočakávané situácie, kedy je ich funkčnosť a spoľahlivosť obmedzená. Zvyčajne sa jedná o lacnú alebo voľne šíriteľnú aplikáciu [3].

3.1.3 Firewally v smerovačoch

Firewally v smerovačoch sú veľmi rozšírená funkcia takmer v každom smerovači od nižšej triedy až po vysokú triedu. V lacnejších variantoch firewally podporujú obmedzené funkcie, prekladajú NAT adresy, blokujú adresy a porty. Patria sem smerovače pre domáce použitie. Majú priateľské konfiguračné prostredie v grafickom móde, ktoré by mal zvládnuť aj menej skúsený človek. Možnosti nastavenia firewallu sú väčšinou dané výrobcom, kedy zmeny povolené užívateľom nemajú zásadný vplyv na funkčnosť. Prístup do konfiguračného módu je realizovaný pomocou webového prehliadača. Vo vyššej kategórii smerovačov môže byť v zabezpečení aj antivírusová kontrola, rôzne aplikačné filtre s hĺbkovou kontrolou paketov. Funkcia smerovača a firewallu v jednom zariadení má pre správcu výhodu, môže konfigurovať všetky prvky z jedného miesta [3].

3.1.4 Hardwarové firewally

Zariadenie s funkciou firewallu má obmedzené schopnosti pri smerovaní komunikácie a sústredí sa na bezpečnosť. Nižšie rady sú jednoduché prvky fungujúce ihneď po zapojení, určené pre domácnosti a malé siete do 50 užívateľov. Často majú rovnaký software ako nákladnejšie rady u rovnakého výrobcu, lenže ich funkcie sú obmedzené a spoplatnené. Možnosti pre upgrady sú veľmi obmedzené. Základné modely obsahujú statické filtrovanie paketov, preklad NAT adries, filtrovanie adries a portov.

Vyššia rada firewallov je úplne rozdielna. Ich primárnou úlohou je nepreniknuteľnosť, vysoká miera dostupnosti a dostatočný výkon. Väčšina zariadení obsahuje odolnosť proti výpadku siete s možnosťou pripojenia záložného zdroja energie. Primárnym využitím týchto zariadení sú veľké siete obsahujúce množstvo cenných dát, ktoré sú dôvodom ochrany. Najvyššie rady majú najpokročilejšie funkcie pre zvýšenie výkonnosti. Pri vyberaní sú dôležité tieto vlastnosti:

- Počet optických rozhraní.
- Ukladací priestor (cache).
- Služby webovej a reverznej proxy.
- Odľahčenie SSL.
- Modularita a škálovateľnosť.

Rozdiel medzi zariadeniami vyššej triedy od ostatných nájdeme v schopnosti blokovať ICMP správy, filtrovanie na aplikačnej vrstve, schopnosť rozsiahleho upgradu, silná podpora od výrobcu a vysoká cena. Najvyššie rady hardwarových firewallov podporujú 5000 až 500 000 pripojených užívateľov [21].

3.1.5 Serverové firewally

Ide o softwarový firewall vložený na server. V tomto prípade musí server spájať aspoň dve siete, aby mohol plniť funkciu firewallu. Na tomto zariadení však bežia ďalšie služby pre niektorú zo sietí. Po aplikovaní softwaru bude teda plniť funkcie brány, firewallu a serveru súčasne. Toto riešenie je lacné, pretože nepotrebuje samostatné hardwarové zariadenie na ktorom by fungoval. Nevýhodou je zníženie bezpečnosti v prípade, že útočník za určitých okolností zneužije bežiace služby pre získanie práva administrátora. V tom prípade môže zmeniť nastavenia alebo ich úplne vymazať [21].

3.1.6 Proxy firewally

Aplikačné proxy firewally sa obvykle usilujú o najvyššiu vrstvu pre ich nastavenia. Proxy je náhradou za koncové spojenie v spojovo - orientovaných službách. Napríklad, proxy môžu byť rozmiestnené medzi vzdialenými užívateľmi, ktorí môžu byť na verejnej sieti ako je Internet, a určitým serverom na internete. Všetko, čo vzdialení používatelia vidia je proxy, takže nepozná identitu serveru, s ktorým aktuálne komunikuje. Rovnako, server vidí iba proxy a nepozná pravého používateľa. Proxy môže byť efektívne chránený filtrovaným mechanizmom medzi verejnou sieťou a chránenou domácou sieťou. Pretože aplikácie sú kompletne chránené proxy, a taktiež akcie zaberajú miesto v úrovni aplikácie, tieto firewally sú veľmi efektívne pre citlivé aplikácie. Autentické schémy, ako sú heslá a biometria, môžu byť nastavené na sprístupnenie proxy opevňujúce bezpečnostné implementácie. Vo veľa prípadoch, určením dodatočných proxy nastavení môžu byť na pomoc pri práci hlavného firewallu a proxy servera. Proxy agents sú aplikácie a protokoly špecifickej realizácie, ktoré konajú pre úžitok ich určených aplikačných protokolov. Protokoly, pre ktoré aplikácie proxy agents môže byť nastavené zahŕňajú nasledovné:

- HTTP (Hypertext Transfer Protocol)
- FTP

- RTP (The Real-time Transport Protocol)
- SMTP (Simple Mail Transfer Protocol)

Hlavná nevýhoda používania aplikačných proxy firewallov je rýchlosť. Pretože tieto firewallové aktivity zaberajú miesto na aplikačnej vrstve a zahrňujú veľké množstvo spracovaných údajov, aplikačný proxy je viazaný rýchlosťou a hodnotou. Ponúkajú najlepšiu ochranu zo všetkých firewallových technológií. Určité proxy môžu byť používané ako asistenčná technológia hlavných firewallov na zlepšenie rýchlosti spracovania [3], [21].

3.2 Prístupové zoznamy

Riadenie prístupu do siete je základným prvkom bezpečnosti siete. Prístupový zoznam ACL je kľúčový komponent pre ochranu informácií a minimalizovanie škôd hroziacich od útočníka. V dnešnom počítačovom prostredí, kde veľké množstvo výpočtového výkonu a citlivé informácie každého človeka sú uložené na jeho vlastnom počítači, riadenie prístupu je kľúčové pre akúkoľvek organizáciu. Dôležitými vlastnosťami je dôvernosť, integrita a zachovanie dostupnosti k informáciám [16].

V preklade znamená skratka ACL Zoznam Kontroly Prístupu. Pomocou tohto zoznamu pravidiel kontrolujeme komunikáciu na sieti za pomoci niekoľkých parametrov, ktoré vyznačujú obmedzenie prijatých paketov v závislosti od údajov odosielateľa. Medzi kontrolné požiadavky patria:

- Typ sieťového protokolu.
- Číslo portu.
- Zdrojovú a cieľovú IP.

Hlavné úlohy ACL sú:

- Obmedzenie nechcenej prevádzky.
- Riadenie prevádzky.
- Riedenie IP toku.
- Poskytnutie základnej bezpečnosti.

ACL je navrhnutý na kontrolu prístupu k informáciám a zmiernenie zraniteľnosťi pred hrozbami zo siete. Hrozba je udalosť alebo aktivita, ktorá má potenciál spôsobiť škodu na

sieti. V tomto prípade, hrozba bude mať snahu obísť alebo získať mechanizmy kontroly prístupu a povoliť útočníkovi získanie neautorizovaného prístupu do siete. Neautorizovaný prístup môže zahŕňať zverejňovanie, pozmeňovanie alebo odmietnutie prístupu k citlivým informáciám. Zraniteľnosť je slabosť, ktorá môže byť využitá hrozbou spôsobujúcou škodu v sieti. Pravdepodobnosť, že sa hrozba naplnila a jej výsledok je poškodenie siete, definujeme ako riziko [18].

3.2.1 Nasadenie ACL

Rozdelenie, kam všade je nutné vytvoriť vlastné zoznamy:

- Každý podporovaný protokol má definovaný ACL zvlášť (IP, IPX).
- Jeden ACL riadi tok dát iba v jednom smere, nie v oboch (komplikovanejšie riešenia ACL vyžadujú implementáciu ACL na viacerých rozhraniach).
- Jeden ACL na sieťové rozhranie (Serial port, Ethernet, ...) [22].

Priradenie ACL na rozhranie:

Router(config) #interface TYPE SPEC
Router(cinfig-if) #ip access-group [ACCESS-LIST-# / ACCESS-LIST-NAME] [in / out]

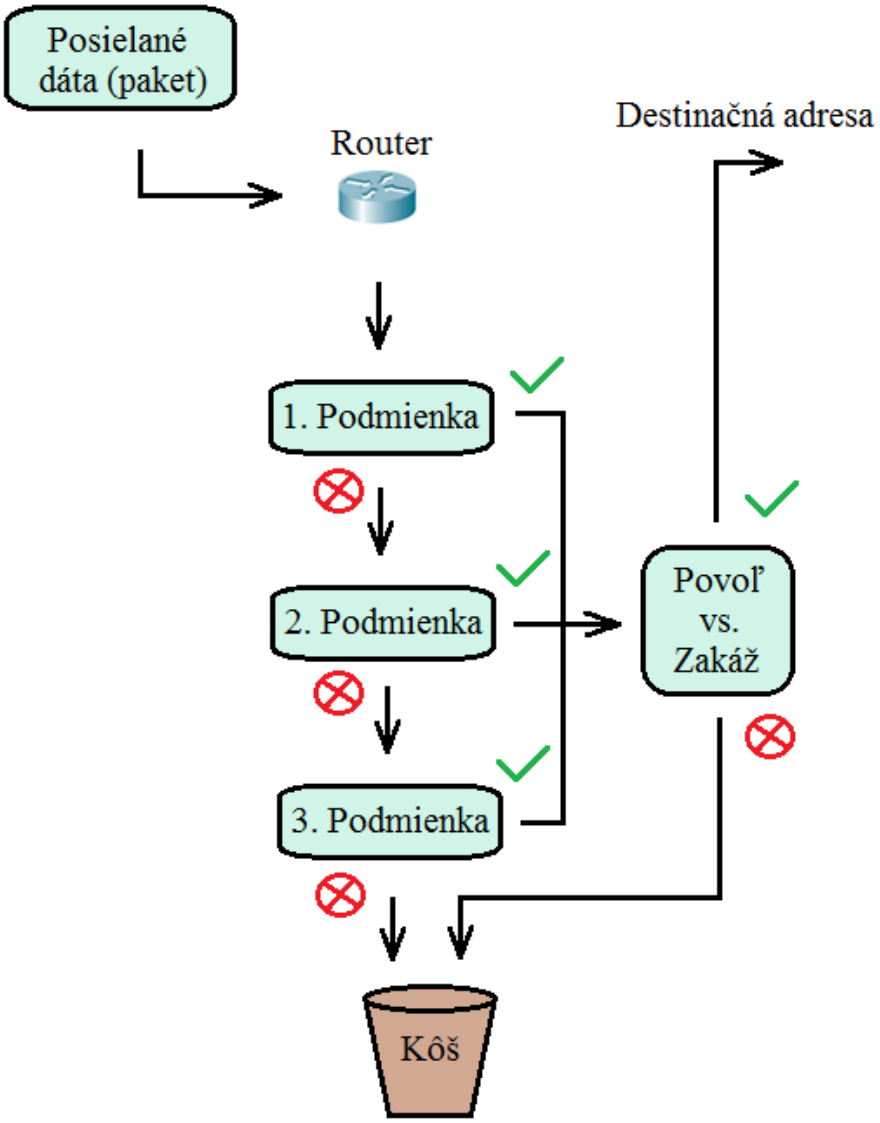
- ACCESS-LIST-# : číslo ACL priraďované na rozhranie.
- ACCESS-LIST-NAME : alebo názov priraďovaného ACL.
- IN / OUT : v akom smere aplikujem ACL [22].

3.2.2 Princíp ACL

ACL je zoznam sekvenčne prehľadávaných podmienok. Pravidlá môžu komunikáciu zablokovať alebo povoliť. Podmienky určujú dva stavy, ktoré je možné nadstaviť:

- **Permit** - Povoľ danú prevádzku, ak spĺňa podmienku.
- **Deny** - Zakáž prevádzku, ak nespĺňa podmienku.

V prípade dát dorazených na sieťové rozhranie, ktoré má v smere posielania priradený ACL pre daný typ protokolu, začína proces kontroly. Obsahuje zoznam testovacích podmienok, ktoré sa aplikujú na IP prevádzku prechádzajúcu rozhraniami smerovača [22].



Obr. 4. Proces kontroly dát ACL

- Kontrolujú sa všetky definované pravidlá ACL.
- Ak parametre paketu spĺňajú podmienku, sieťová komunikácia zakáže alebo povolí komunikáciu.
- V prípade nezhody postupne vykoná porovnanie so všetkými podmienkami.
- Pri nezodpovedaní žiadnej z podmienok, zariadenie automaticky dáta nepustí a sú odstránené.

3.2.3 Vytvorenie ACL

Prvým procesom pri vytváraní zoznamu je definícia, čo chce správca danému zariadeniu povoliť alebo zakázať. Pri jednoduchej požiadavke, napríklad zablokovanie prístupu určitej skupine IP adries postačí použitie jednoduchého ACL.

Tvar jednoduchého ACL:

Router(config)#access-list (1-99) [deny / permit / remark] TEST_Podmienka [WILDCARD] [Log]

- Remark: poznámka o ACL.
- TEST_Podmienka: IP adresa, na ktorú sa vzťahujú podmienky.
- WILDCARD: špecifikuje rozsah IP adries, na ktoré sa uplatňuje podmienka.
- Log: loguje pakety odpovedajúce kritériu.

Pri zložitejších právach, ako napríklad povolenie určitých portov pre konkrétnu IP adresu je nutné použiť zložitý ACL.

Konfigurácia zložitého ACL:

Router(config)#access-list (100-199 alebo 2000-2699) [deny / permit / remark] Protocol [source address / wildcard] [zdrojový port] [destination address / wildcard] [equals] [cieľový port] estamblished

- Protocol: TCP, UDP, ICMP (Internet Control Message Protocol), IP.
- Source address: Zdrojová IP adresa plus maska pri väčšom rozsahu.
- Zdrojový port: 21, 22, 25, 80, 443.
- Destination address: Adresa príjemcu plus maska.
- Equals: znak rovnosti eq- špecifický port, gt- všetky väčšie ako špecifické, lt- všetky menšie ako špecifické, neq- všetky okrem špecifického, range- všetky porty.
- Estamblished: Len pre TCP protokol, povolí komunikáciu, ak už bolo naviazané spojenie.

3.2.4 Pomenovanie alebo očíslovanie ACL

Všetky ACL musia byť identifikované menom alebo číslom. Názov prístupového zoznamu je výhodnejší ako číslo pretože môže znamenať označenie pre ľahšie zapamätanie alebo spojitosť s jeho funkciou. Možno zmeniť poradie príkazov alebo pridať príkazy pomenované prístupovým zoznamom [19].

Pomenované ACL podporujú nasledujúce funkcie, ktoré nie sú podporované číslovanými ACL:

- Nastavenie filtrácie IP.
- Nespojiteľnosť portov.
- Vymazanie záznamov s „no permit" alebo „no deny" príkazom.

Nie všetky príkazy, ktoré akceptujú číslované ACL budú akceptovať pomenované ACL.

Napríklad funkcia vty používa iba číslované prístupové zoznamy [19].

3.3 Ľubovoľné riadenie vstupu

„*Pri použití DAC (Discretionary Access Control) majiteľ objektu rozhoduje v rámci vlastného uváženia, k akým objektom má daný užívateľ prístup. Autorizovaná entita alebo subjekt majúci právomoc v rámci určitých obmedzení, ktoré špecifikujú objekty ku ktorým je možné pristupovať. Jedným zo spôsobov ako špecifikovať DAC je tabuľka*“ [3].

Tab. 3. Špecifikácia DAC

Access Control List			
Subjekt	**1. Objekt**	**2. Objekt**	**3. Objekt**
	Plat (súbor)	**Odmeny (súbor)**	**Hodnotenie (proces)**
Program Sun Explore	Čítať	Čítať	Žiadne
Riaditeľ	Žiadne	Čítať	Povolené
Sekretárka	Čítať/Písať	Čítať/Písať	Žiadne
Proces Clean	Čítať/Písať	Čítať	Žiadne

„Zvyčajne je vlastníkom objektu osoba, ktorá ma právo na všetky zmeny. Vo väčšine systémov sa stane tvorca objektu aj jeho vlastníkom. Z toho dôvodu vlastník musí opatrne riadiť a kontrolovať sieť aby sa ubezpečil, že vždy prideľuje najmenšie práva aké subjekt potrebuje k vykonávaniu jeho práce. Vlastník môže v podstate vykonávať akúkoľvek zmenu prístupových práv k dátam, preto je dôležité aby bol protokol správne napísaný, nakoľko je zavedený pre bezpečnosť a správne fungovanie siete. Výhodou DAC je jednoduchosť implementácie, keďže táto funkcia je zabudovaná v takmer každom dnes dostupnom operačnom systéme a aplikácií. Nevýhodou môže byť neúmyselne vykonaná zmena a potrebným bude bod obnovy. Pre robustnejší systém je potrebná systematická ochrana a povinné kontrolovanie prístupu“ [3].

3.4 Povinné riadenie vstupu

„V mandatory access control (MAC) musia byť zistené formálne zhody, že subjektu sú pridelené dostatočné povolenia, ktoré potrebuje pre prístup k citlivým informáciám. Subjekt môže použiť autorizáciu vo forme povolenia, ktoré je porovnané s klasifikáciou objektu. Zvyčajne sa pre objekty klasifikujú ako vyhradené, dôverné, tajné a prísne tajné. Rovnako tak, ak jednotlivec získa prístup k vyhradeným a dôverným informáciám, bude mať taktiež prístup aj k dokumentom vyhradeným. S MAC má subjekt práva pre prístup iba k objektom s rovnakou alebo nižšou klasifikáciou. Takže ak chce subjekt s povolením k tajným informáciám otvoriť dokument prísne tajný, tento prístup bude zamietnutý. Ďalšou úrovňou ochrany je vedieť, aké povolenia potrebuje subjekt na plnenie svojich pridelených povinností“ [3].

II. PRAKTICKÁ ČÁST

4 IP ADRESÁCIA

IP adresa nemôže byť ku konkrétnemu rozhraniu pridelená ľubovoľne, ale musí spĺňať presné podmienky. Štandardná konfigurácia pozostáva z:

- Nadstavenia IP adresy rozhrania - musí patriť do rozsahu siete, v ktorom sa nachádza.
- Správnej masky.
- Správnej brány siete (default getway).

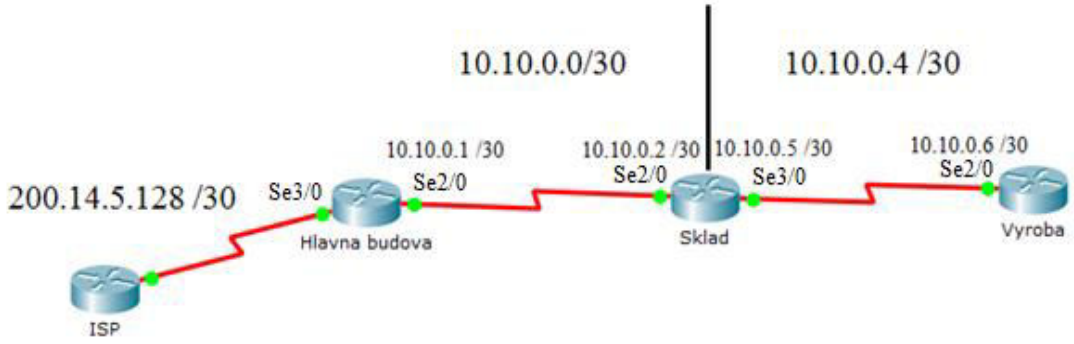
V rámci firemnej siete je pre IP adresáciu použitý rozsah triedy A, ktorá umožňuje veľký voľný priestor pre pridelenie zariadeniam. Pri použití tohto rozsahu nemusíme dbať na šetrenie miestom, a teda je možné prehľadné rozdelenie, poprípade pridanie ďalších sieťových zariadení pri rozšírení siete. Správca si taktiež ľahko zapamätá skupiny alebo zistí, z akej časti je vzniknutý problém.

Podľa tretieho oktetu IP adresy je sieť rozdelená do kategórií:

- 10.10.0.x – WAN prepojenie medzi routrami.
- 10.10.1.x – Kancelárske priestory hlavnej budovy.
- 10.10.2.x – Sklad.
- 10.10.3.x – Výroba.
- 10.10.4.x – Wifi v hlavnej budove.
- 10.10.5.x – Servery.

4.1 WAN

WAN (Wide Area Network) je prepojenie medzi routrami v sieti, každý z nich sa nachádza v jednej budove. Typ portu použitý pre túto cestu je Serial. Prenos dát je zaistený protokolom OSPF (Open Shortest Path First).



Obr. 5. WAN prepojenie

Tab. 4. IP adresácia medzi budovami

Router	**Port**	**IP adresa**	**Názov**
Hlavná budova	Se3/0	200.14.5.129 /30	Pripojenie ISP
Hlavná budova	Se2/0	10.10.0.1 /30	WAN 1
Sklad	Se2/0	10.10.0.2 /30	WAN 1
Sklad	Se3/0	10.10.0.5 /30	WAN 2
Výroba	Se2/0	10.10.0.6 /30	WAN 2

4.2 Rozsahy adries v budovách

V hlavnej budove sa nachádzajú kancelárske priestory spolu so serverovňou. Každá skupina užívateľov má pridelený rozsah zariadení, ten je väčší ako skutočný potrebný priestor z dôvodu možného pridania ďalších prvkov do siete.

Tab. 5. IP adresácia Hlavnej budovy

Skupina	**IP adresa**
Vedenie	10.10.1.10 - 10.10.1.29 /24
Sekretariát	10.10.1.30 - 10.10.1.49 /24
Prevádzkové účtovníctvo	10.10.1.50 - 10.10.1.69 /24
Mzdové účtovníctvo	10.10.1.70 - 10.10.1.89 /24
Predaj	10.10.1.90 - 10.10.1.100 /24
Wifi	10.10.4.2 - 10.10.4.30 /24
WWW server	10.10.5.10 /24
Databáza	10.10.5.30 /24
Správca	10.11.1.2

Budova skladu sa nenachádza v priamej blízkosti k hlavnej budove, teda je nutné vytvorenie prepojenia medzi nimi. Do siete je v nej pripojených niekoľko zariadení, jedná sa o vedúceho skladu a ostatnú skupinu tvoria skladníci.

Tab. 6. IP adresácia Skladu

	IP adresa
Vedenie skladu	10.10.2.5 - 10.10.2.9/24
Skladníci	10.10.2.10 - 10.10.2.10/24

Tab. 7. IP adresácia Výroby

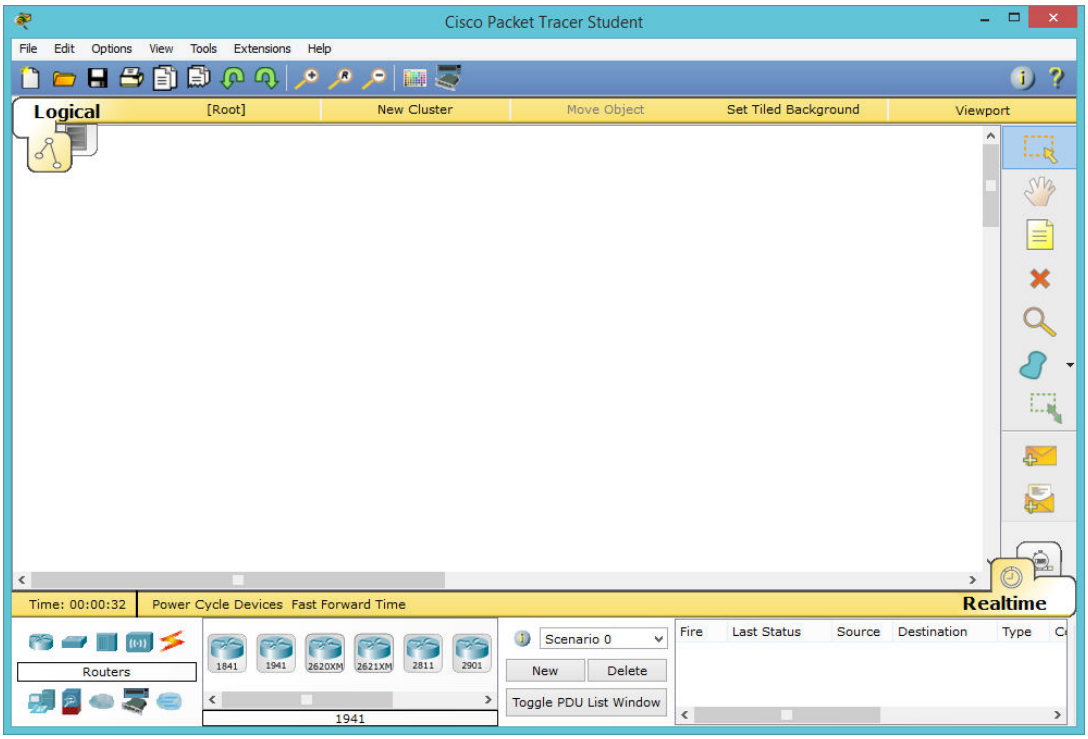
	IP adresa
Vedúci výroby	10.10.3.5 - 10.10.3.9 /24
Výroba	10.10.3.10 - 10.10.3.30 /24

5 NÁVRH SIETE

Pri navrhovaní a následnom vytváraní firemnej počítačovej siete je nutné sa ako prvým bodom zaoberať definovaním a požiadavkami na sieť. Tieto vlastnosti sú pre každú firmu špecifické a jedinečné, udáva ich prostredie, v ktorom bude prebiehať prevádzka siete, požadovaný výpočtový výkon a možné rozšírenie adresného priestoru. V neposlednom rade ide o samotného užívateľa. Plánovanie siete podľa kritérií je najdôležitejší proces pri návrhu celkového riešenia. Má obsahovať celú infraštruktúru z pohľadu hardwarových zariadení, ale aj softwarového riešenia. Hlavným bodom je zhotovenie funkčného modelu siete v simulačnom prostredí programu Cisco Packet Tracer. Jeho databáza obsahuje všetky zariadenia použité pri zhotovení zmenšeného modelu firemnej siete.

5.1 Cisco Packet Tracer

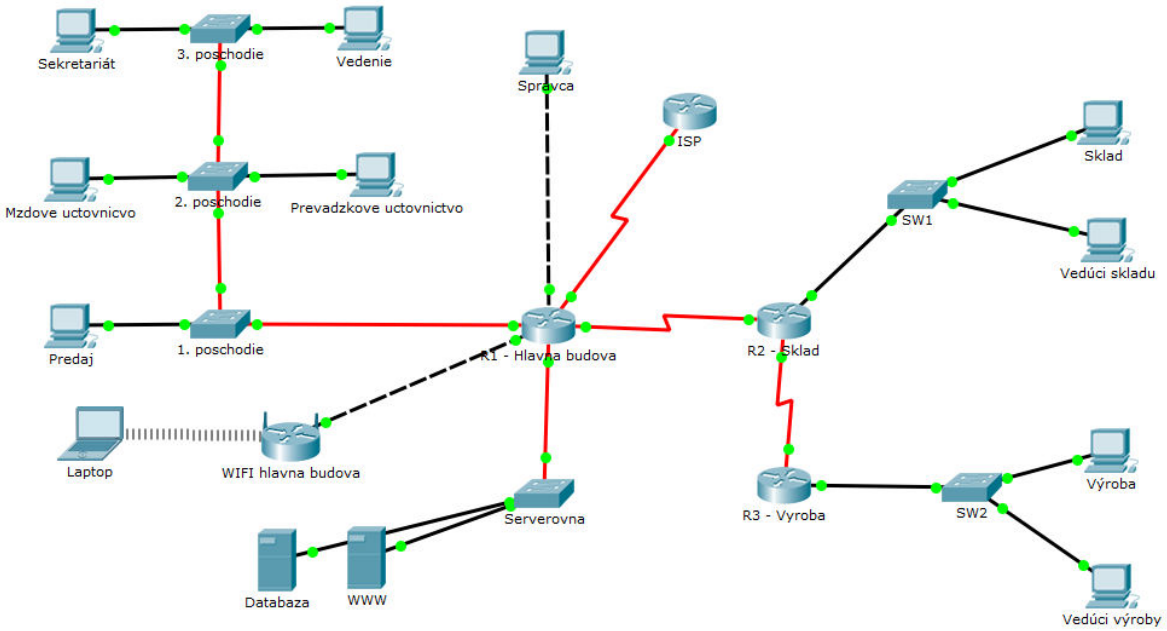
Simulačný program vyvinutý spoločnosťou Cisco, ktorá vyrába sieťové zariadenia. Umožňuje vytvorenie reálnej siete s možnosťou jej konfigurácie. Obsahuje skutočné prostriedky a zariadenia, s ktorými bežne pracuje správca siete. Dovoľuje študentom stiahnutie bezplatnej verzie.



Obr. 6. Simulačné prostredie Cisco Paket Tracer

5.2 Model siete

Model siete vytvorený v simulačnom prostredí, technické riešenie na základe skutočných požiadavkám reálnej sieti. V rámci konfigurácie je na zariadeniach nadstavená IP adresácia, teda komunikácia zabezpečená routovacím protokolom OSPF.



Obr. 7. Model siete

Pri pohľade na sieť zo strany aktívnych prvkov, sa často hovorí o hierarchickom vzhľade, ktorý má tri vrstvy. Centrálna najvýkonnejšia časť sa označuje ako jadro (core layer), druhá menej výkonná časť sa nazýva distribučná (distribution layer), a najnižšie je prístupová (access layer) vrstva. Takáto štruktúra má veľa výhod, hlavne sa jedná o jednoduchú prehľadnosť a rozšíriteľnosť. V prípade tejto sieti do core vrstvy patria routre v budovách (hlavná budova, sklad, výroba). Ostatné zariadenia sú zaradené do prístupovej vrstve. Distribučnú vrstvu táto sieť z dôvodu nízkeho počtu zariadení nepotrebuje.

Tab. 8. Rozpis a počet zariadení

Zariadenie	Počet kusov
Router	3
Wifi Router	1
Switch	6
Server	2
Koncové zariadenia	11

Počet zariadení v sieti zodpovedá aktuálnym požiadavkám. V prípade potreby je možné kedykoľvek pridať ďalšie, v závislosti na potrebách pripojenia ďalších zariadení alebo rozšíriteľnosti siete do nových priestorov.

5.3 Protokol

Open Shortest Path First (OSPF) použitý v konfigurácii je smerovací dynamický protokol, vytvorený pre rýchlu reakciu na zmenu topológie siete, ktorá využíva IP a na jej základe smeruje pakety. Jeho požiadavky na funkčnosť sú nízke a sieť takmer nie je zaťažená smerovacími informáciami. Rozsah konfigurácie OSPF na aktívnych zariadeniach zahŕňa všetky priamo pripojené podsiete, teda je nutné udať názov všetkých priamo pripojených sietí a wildcard mask (tvar je opačný ako pri maske podsiete, teda 255.255.255.0 má tvar 0.0.0.255). Dôležitým údajom v zápise je uvedenie oblasti, najčastejšie sa používa označenie area 0 [17].

6 KONFIGURÁCIA ACCESS LISTOV

Sieť sa riadi bezpečnostnou politikou, ktorej myšlienka je pridelenie čo najmenších práv pre užívateľov. Zvolené konfigurácie ACL poskytujú dostatočné možnosti zamestnancov pre prácu vo firme. Najnižší počet povolení nám zaistí vysokú bezpečnosť proti útokom z vnútorných aj vonkajších priestorov siete.

6.1 Hlavná budova

V hlavnej budove sa nachádza najdôležitejší sieťový prvok. Ide o router spájajúci celú LAN sieť (kancelárske priestory, serverovňu, wifi pripojenie) s prístupom na internet. Zohráva kľúčovú úlohu pri toku všetkých dát. Cez tento bod sa musí útočník z vonkajšej siete dostať do vnútra. To je dôvod pre najlepšie zabezpečenie s najvyšším počtom access listov. Tie nám definujú všetky práva paketov, teda ide o podmienky, ktoré musí spĺňať každý paket smerujúci von alebo do vnútra siete. Najdôležitejším je teda port na routri, ku ktorému je sieť pripojená k svojmu poskytovateľovi internetového pripojenia. Poskytovateľ je pripojený cez sériový port s číslom 3/0 a na ňom je umiestnený rozšírený access list s číslom 103 a 104. Ďalším dôležitým prvkom zabezpečenia je odopretie prístupu každému zariadeniu okrem správcu siete na port telnet. Pre tento typ ochrany bol použitý jednoduchý ACL, ktorý je dostatočný a spĺňa všetky podmienky.

access list 1

```
vedenie(config)#access-list 1 permit 10.11.1.2
vedenie(config)#line vty 0 4
vedenie(config-line)#access-class 1 in
```

access list 101

```
vedenie(config)#access-list 101 permit tcp any any eq 80
vedenie(config)#access-list 101 permit tcp any any eq 443
vedenie(config)#access-list 101 permit tcp any any eq 53
vedenie(config)#access-list 101 permit udp any any eq 53
vedenie(config)#access-list 101 permit tcp any host 10.10.5.10
vedenie(config)#interface fastEthernet 0/0
vedenie(config-if)#ip access-group 101 in
```

- Rozšírený ACL rieši prístup skupiny užívateľov z Wifi pripojenia.

- V rámci bezpečnosti má každý prístup len k WWW serveru LAN siete a pripojenie do vonkajšej siete cez port 80 a 443, čo je HTTP a HTTPS.
- Umiestnený je na porte v smere toku dát do routra.

access list 102

```
vedenie(config)#access-list 102 deny tcp any any eq 23
vedenie(config)#access-list 102 permit tcp 10.10.1.10 0.0.0.1 eq 80 any
vedenie(config)#access-list 102 permit tcp 10.10.1.10 0.0.0.1 eq 443 any
vedenie(config)#access-list 102 permit tcp 10.10.1.10 0.0.0.1 eq 53 any
vedenie(config)#access-list 102 permit udp 10.10.1.10 0.0.0.1 eq 53 any
vedenie(config)#access-list 102 permit ip any 10.10.5.0 0.0.0.255
vedenie(config)#access-list 102 permit tcp any any eq 25
vedenie(config)#interface fastEthernet 4/0
vedenie(config-if)#ip access-group 102 in
```

- Kontroluje prevádzku z kancelárskych priestorov do LAN siete.
- Každému zo zariadení zakazuje telnet.
- Vedenie firmy má prístup na internet.
- Všetci majú povolený mail a komunikáciu so servermi.
- ACL je umiestnený zo siete smerom do routra.

access list 103

```
vedenie(config)#access-list 103 deny ip 10.10.0.0 0.0.255.255 any
vedenie(config)#access-list 103 deny ip 10.11.0.0 0.0.255.255 any
vedenie(config)#access-list 103 permit tcp any host 10.10.5.10 eq 25
vedenie(config)#access-list 103 permit tcp any host 10.10.5.10 eq 80
vedenie(config)#access-list 103 permit tcp any host 10.10.5.10 eq 443
vedenie(config)#access-list 103 permit udp host 200.14.5.130 eq 53 10.0.0.0
0.255.255.255
vedenie(config)#access-list 103 permit icmp any 10.0.0.0 0.255.255.255 echo-reply
vedenie(config)#access-list 103 permit tcp any eq 80 host 10.10.5.10 established
vedenie(config)#access-list 103 permit tcp any eq 443 host 10.10.5.10 established
hlavna-budova(config)#interface serial 3/0
hlavna-budova(config-if)#ip access-group 101 in
```

- Kontroluje prevádzku z Internetu do LAN siete.

- Zakazuje prístup IP adresám použitých pre adresáciu v sieti (anti-spoofing filter proti falošným zdrojovým IP).
- Povoľuje prístup všetkým zariadeniam z Internetu k WWW serveru cez port 25 (mail) a port 80, 443 (HTTP, HTTPS).
- DNS server umiestnený u ISP má povolenie odpovedať zariadeniam v LAN.
- Povoľuje odpovede ICMP (ping) vyslané so siete, ostatné zakazuje.
- Nezakazuje spojenie k Internetu vytvorené užívateľom zo siete.
- Umiestnený v smere do siete.

access list 104

```
hlavna-budova(config)#access-list 104 permit udp 10.0.0.0 0.255.255.255 host 200.14.5.130 eq 53
hlavna-budova(config)#access-list 104 permit icmp 10.0.0.0 0.255.255.255 any echo
hlavna-budova(config)#interface serial 3/0
hlavna-budova(config-if)#ip access-group 104 in
```

- Povoľuje DNS pre všetky IP adresy v sieti.
- Umožňuje poslať ping z LAN každému zariadeniu.
- Umiestnený na porte von zo siete.

access list 105

```
hlavna-budova(config)#access-list 105 permit tcp host 10.10.5.10 eq 25 any established
hlavna-budova(config)#access-list 105 permit tcp host 10.10.5.10 eq 80 any established
hlavna-budova(config)#access-list 105 permit tcp host 10.10.5.10 eq 443 any established
hlavna-budova(config)#access-list 105 permit tcp host 10.10.5.30 eq 21 any established
hlavna-budova (config)#interface fastEthernet 5/0
hlavna-budova (config-if)#ip access-group 105 in
```

- Povoľuje odpovede serveru WWW na komunikáciu cez porty 25 (ICMP), 80 (HTTP) a 443 (HTTPS).
- Serveru Databáza umožňuje komunikáciu cez FTP.
- Umiestnený smerom do routra zo Serverovne.

6.2 Sklad

Sklad je časť siete nachádzajúca sa medzi hlavnou budovou a výrobou. V sieti stačilo použiť dva štandardné a jeden zložitý ACL, čo zaisťuje dostatočnú ochranu a spoľahlivý prístup do siete pre užívateľov.

access list 1

sklad(config)#access-list 1 permit host 10.11.1.2
sklad(config)#access-list 1 permit 10.10.5.0 0.0.0.255
sklad(config)#access-list 1 deny any sklad(config)#interface fastEthernet 0/0
sklad(config-if)#ip access-group 1 out

- Do siete má prístup len správca.
- Užívatelia môžu komunikovať so servermi.
- Všetka komunikácia smerom do tejto siete zamietnutá.

access list 2

sklad(config)#access-list 2 permit 10.11.1.2
sklad(config)#line vty 0 4
sklad(config-line)#access-class 2 in

- Jednoduchý ACL dovoľuje telnet na router iba správcovi siete.

access list 101

sklad(config)#access-list 101 permit tcp host 10.10.2.5 any eq 25
sklad(config)#access-list 101 permit tcp any host 10.10.5.30 eq 21
sklad(config)#access-list 101 permit tcp any host 10.10.5.10 eq 80
sklad(config)#access-list 101 permit tcp any host 10.10.5.10 eq 443
sklad(config)#interface fastEthernet 0/0
sklad(config-if)#ip access-group 101 in

- Správca má povolenú komunikáciu cez mail.
- Každý sa môže pripojiť cez FTP port na server Databáza a cez port 80, 443 na server WWW.
- Všetko ostatné zamietnuté.

- ACL umiestnený zo siete Sklad do LAN.

6.3 Výroba

Výroba je posledné zariadenie nachádzajúce sa na konci siete. Pre zaistenie bezpečnosti z tejto oblasti postačí využiť 3 ACL. Štandardný je využitý pre obmedzenie prístupu do routru, ďalšie dva zložité definujú rôzne práva užívateľov pre komunikáciu so zvyškom firemnej siete.

access list 1

```
vyroba(config)#access-list 1 permit 10.11.1.2 /telnet len pre správcu
vyroba(config)#line vty 0 4
vyroba(config-line)#access-class 1 in
```

- Jednoduchý ACL dovoľuje telnet na router iba správcovi siete.

access list 101

```
vyroba(config)#access-list 101 permit tcp host 10.10.3.5 any eq 80
vyroba(config)#access-list 101 permit tcp host 10.10.3.5 any eq 443
vyroba(config)#access-list 101 permit tcp host 10.10.3.5 any eq 53
vyroba(config)#access-list 101 permit udp host 10.10.3.5 any eq 53
vyroba(config)#access-list 101 permit tcp 10.10.3.0 0.0.0.255 any eq 25
vyroba(config)#access-list 101 permit tcp any host 10.10.5.30
vyroba(config)#interface fastEthernet 0/0
vyroba(config-if)#ip access-group 101 in
```

- Vedúcemu výroby povoľuje komunikáciu cez porty 80, 443 a priradenie IP adresy DNS serverom u ISP.
- Každý v sieti má prístup k mailu a serveru databáza.
- Ostatná komunikácia zakázaná.
- Kontroluje dáta z Výroby do LAN.

access list 102

```
vyroba(config)#access-list 102 permit tcp host 10.11.1.2 any
vyroba(config)#access-list 102 permit tcp any any established
vyroba(config)#interface fastEthernet 0/0
vyroba(config-if)#ip access-group 102 out
```

- Správca má prístup do siete.

- Povolí komunikáciu založeného TCP spojenia.
- Smer ACL z routru do siete Výroba.

7 IMPLEMENTÁCIA ACL NA CISCO AKTÍVNE ZARIADENIA

Po vytvorení modelu siete s kompletnou konfiguráciou bolo pokračovaním zrealizovanie a odskúšanie na aktívnych zariadeniach. Proces prebiehal v školskej učebni na testovacích prístrojoch. Prvý krok bol výber routrov a typ prepojenia medzi nimi. V učebni bol prístupný len starší typ zariadenia a databáza simulačného prostredia Cisco Packet Tracer neobsahuje tento model.

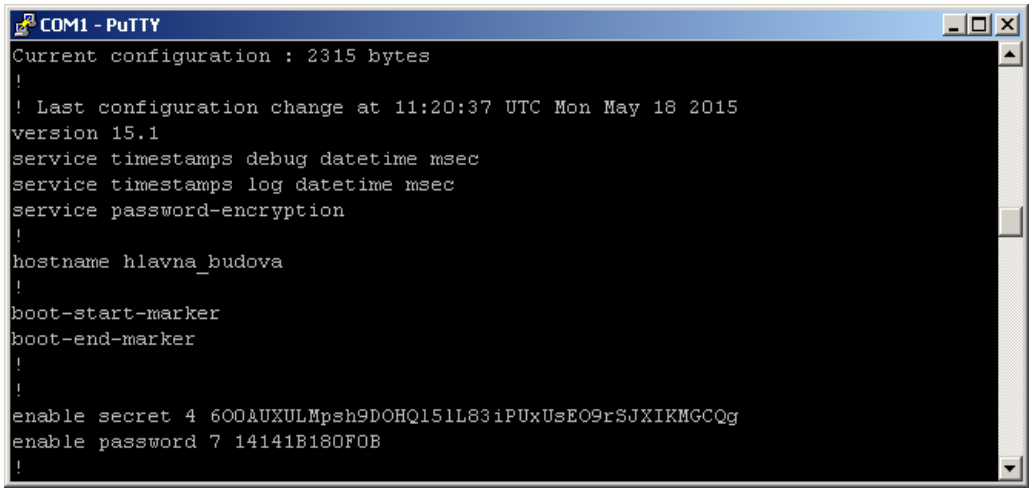
7.1 Použité porty

V simulačnom prostredí bola využitá možnosť pridania akéhokoľvek portu, a to je dôvod, prečo konečná konfigurácia neobsahuje rovnaký počet použitých portov. Pri reálnom zariadení je taktiež možnosť pridania ďalšieho portu, no z dôvodu vysokej ceny sa tento proces nedal uskutočniť.

Tab. 9. Označenie portov

	Cisco packet tracer	**Reálny**
R1 Hlavná Budova	Se 2/0	Se 0/1/0
	Se 3/0	Se 0/1/1
	Fa 5/0	Fa 0/1
	Fa 4/0	Fa 0/0
	Fa 0/0	Nepoužité
	Fa 1/0	Nepoužité
R2 Sklad	Se2/0	Se 0/1/0
	Se 3/0	Se 0/1/1
	Fa 0/0	Fa 0/0
R3 Výroba	Se 2/0	Se 0/1/0
	Fa 0/0	Fa 0/0

7.2 Hlavná budova



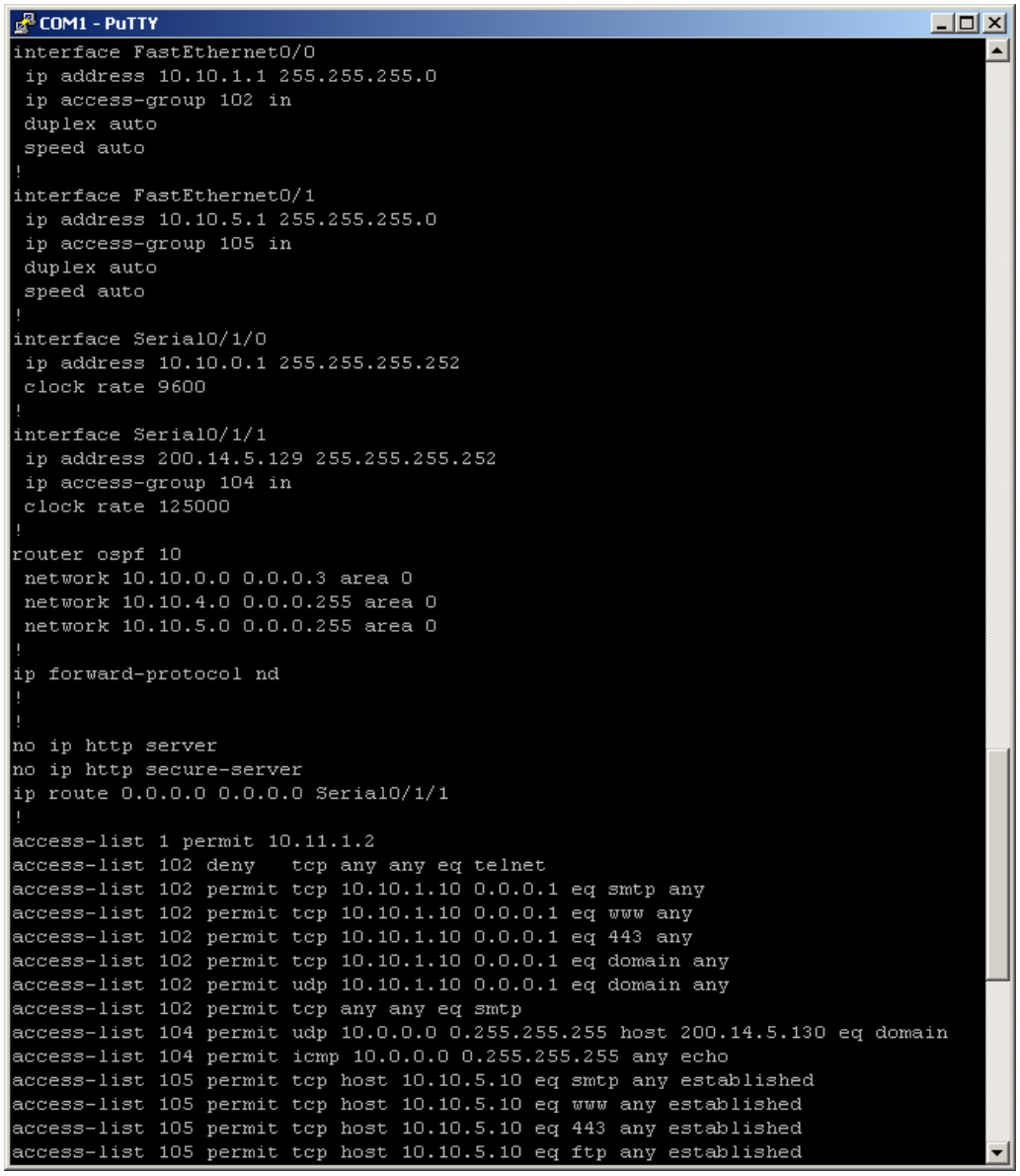
Obr. 8. Základná konfigurácia R1

Na obrázku 8 je vidno základnú konfiguráciu routra R1 s názvom hlavna_budova. Výpis obsahuje informácie o názve zariadenia a zaheslovaní módov. Na ochranu týchto hesiel pri výpise bolo použité šifrovanie, toto nastavenie potvrdzuje výpis service password-encryption.

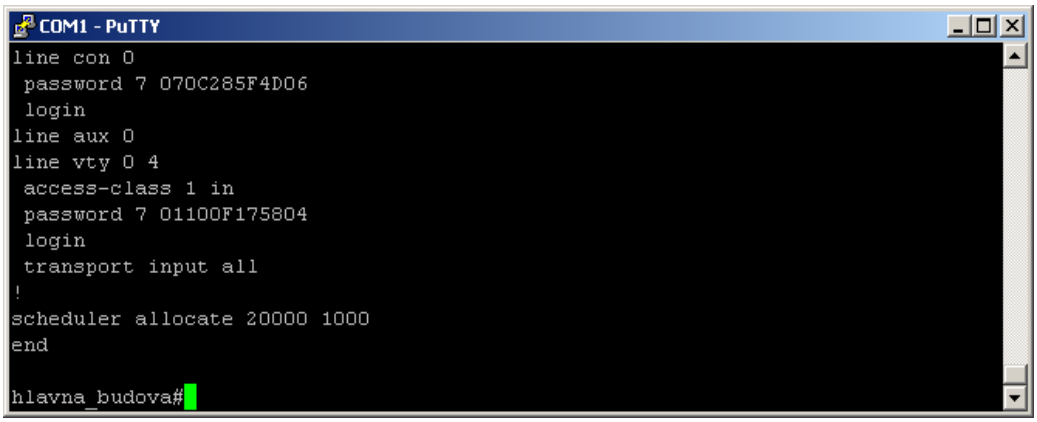
Na obrázku 9 je výpis o konfigurácii portov, každému z nich bola priradená IP adresa a ACL. Zmenu medzi číslami portov simulačného a reálneho modelu je možno vidieť v tabuľke 9. Ďalším dôležitým výpisom je informácia o routovacom protokole OSPF. Obsahuje zoznam sietí, s ktorými má zariadenie možnosť komunikovať a vymieňať si dáta.

ip route 0.0.0.0 0.0.0.0 Serial 0/1/1 - označuje port v sieti pripojený k ISP. Ostatné príkazy vyjadrujú konfiguráciu všetkých ACL na tomto zariadení.

Obrázok 9 znázorňuje zaheslovanie prístupových portov, kedy skratka con, aux znamená fyzický port a vty je virtuálny port. Pre lepšie zabezpečenie zariadenia proti útoku z vonku siete je na virtuálny port pridelený ACL. Ten umožňuje prístup do routru len správcovi siete.



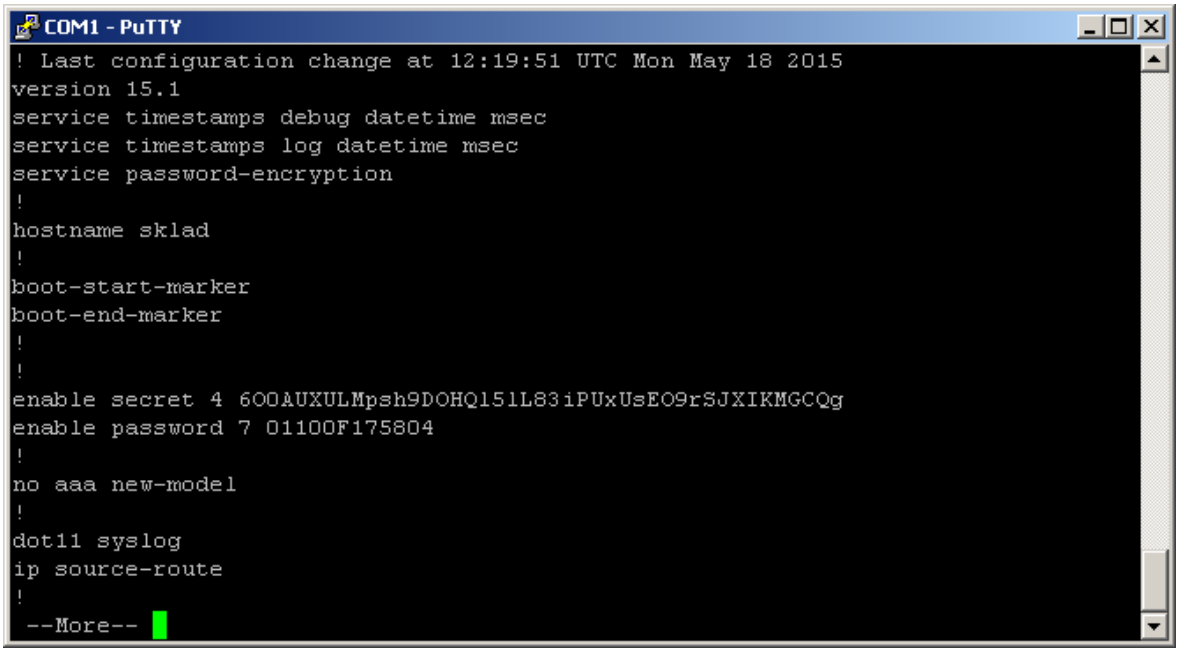
Obr. 9. Porty, protokol, ACL



Obr. 10. Porty

7.3 Sklad

Časť siete medzi hlavnou budovou a výrobou. Nachádzajú sa v nej dve skupiny užívateľov s rôznymi prístupovými povoleniami. Základná konfigurácia prebehla rovnako ako pri ostatných routroch, rozdiel vidieť len v zvolenom názve zariadenia.

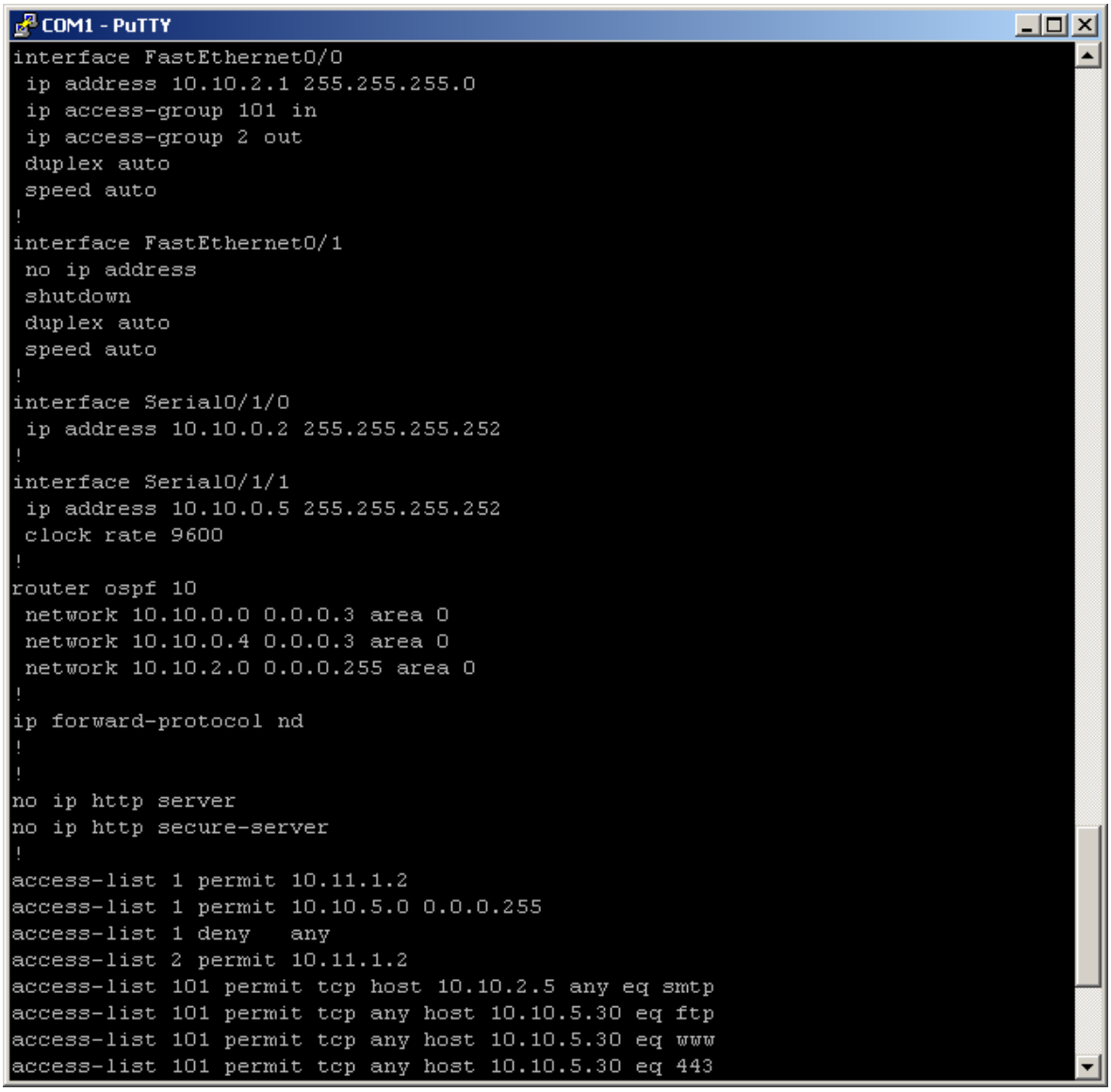


Obr. 11. Základná konfigurácia R2

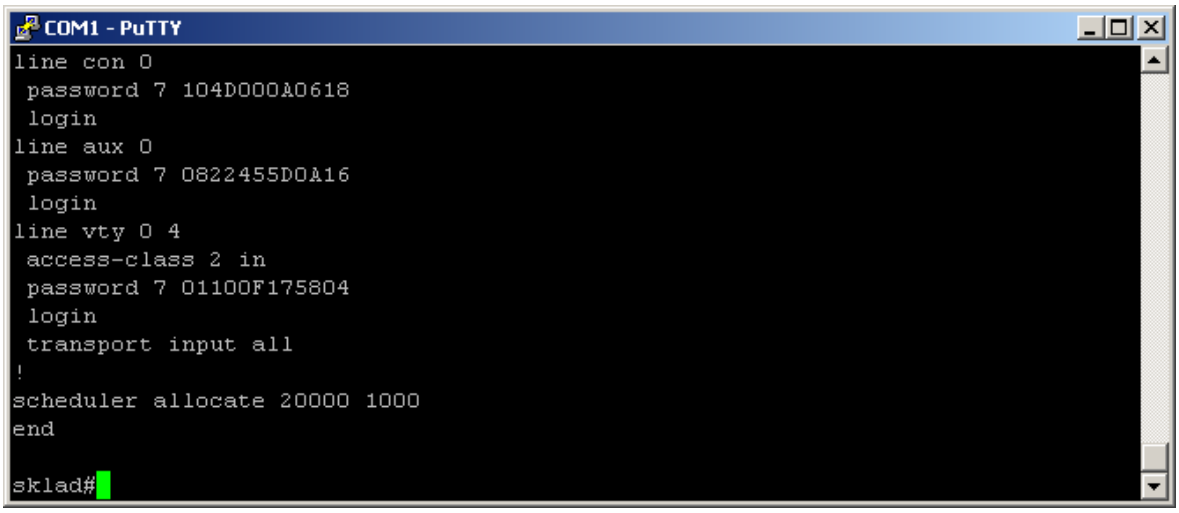
Z výpisu konfigurácie aktívneho zariadenia na obrázku 11 je vidieť zvolený názov ako sklad, zaheslovanie módov a následné šifrovanie týchto hesiel.

V ďalšom výpise na obrázku 12 sú konfigurované porty, a k nim pridelené prístupové zoznamy. Pod zobrazením štyroch portov je informácia o routovacom protokole OSPF. Zo zápisu je možné vyčítať, že zariadenie má použité tri porty, dva pre spojenie s ostatnými routrami a jeden port, na ktorý je pripojená podsieť sklad. Pod výpisom z protokolu sa nachádza informácia o prístupových zoznamoch a zahŕňa celkový tvar ako pri ich nadstavovaní.

Posledný výpis z programovania routeru sklad je na obrázku 13 a znázorňuje výpis o prístupových portov. K nim by mal mať prístup len správca alebo technik. Na virtuálny port vty 0 4 je z dôvodu telnetu pridaný prístupový zoznam pre pripojenie správcu k tomuto zariadeniu.



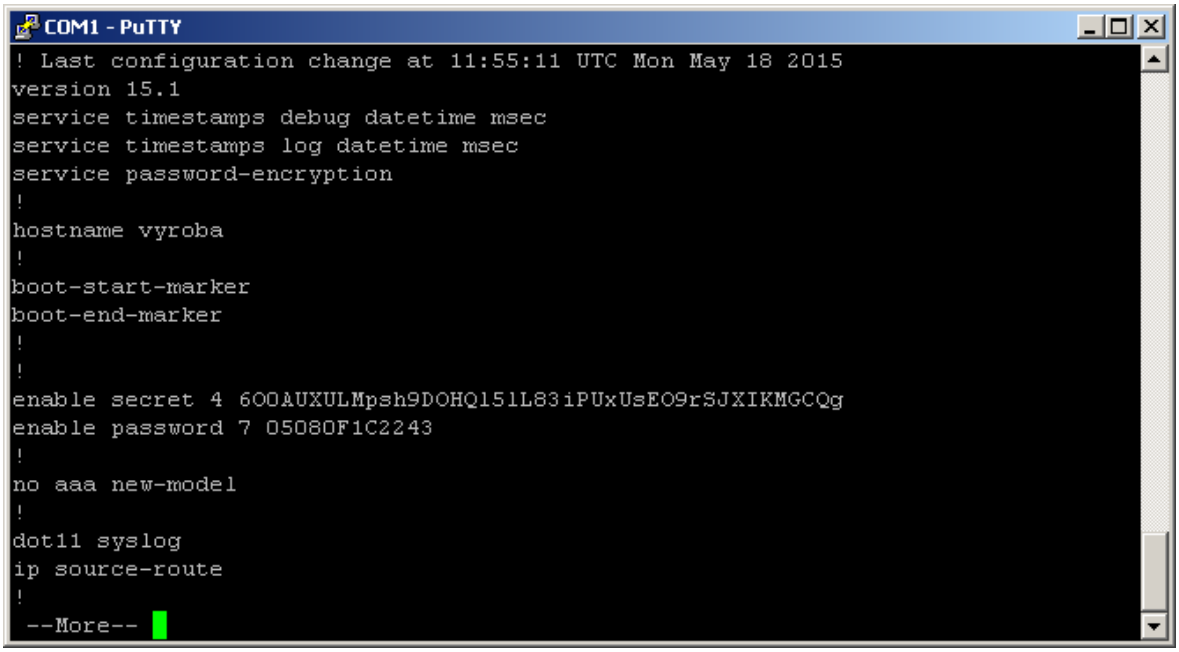
Obr. 12. Porty, protokol a ACL na R2



Obr. 13. Virtuálne a prístupové porty na R2

7.4 Výroba

Zariadenie na konci siete s najmenšími právami komunikácie a prístupu k zariadeniam. Užívatelia v tejto časti nepotrebujú pre svoju činnosť takmer žiadne povolenia.

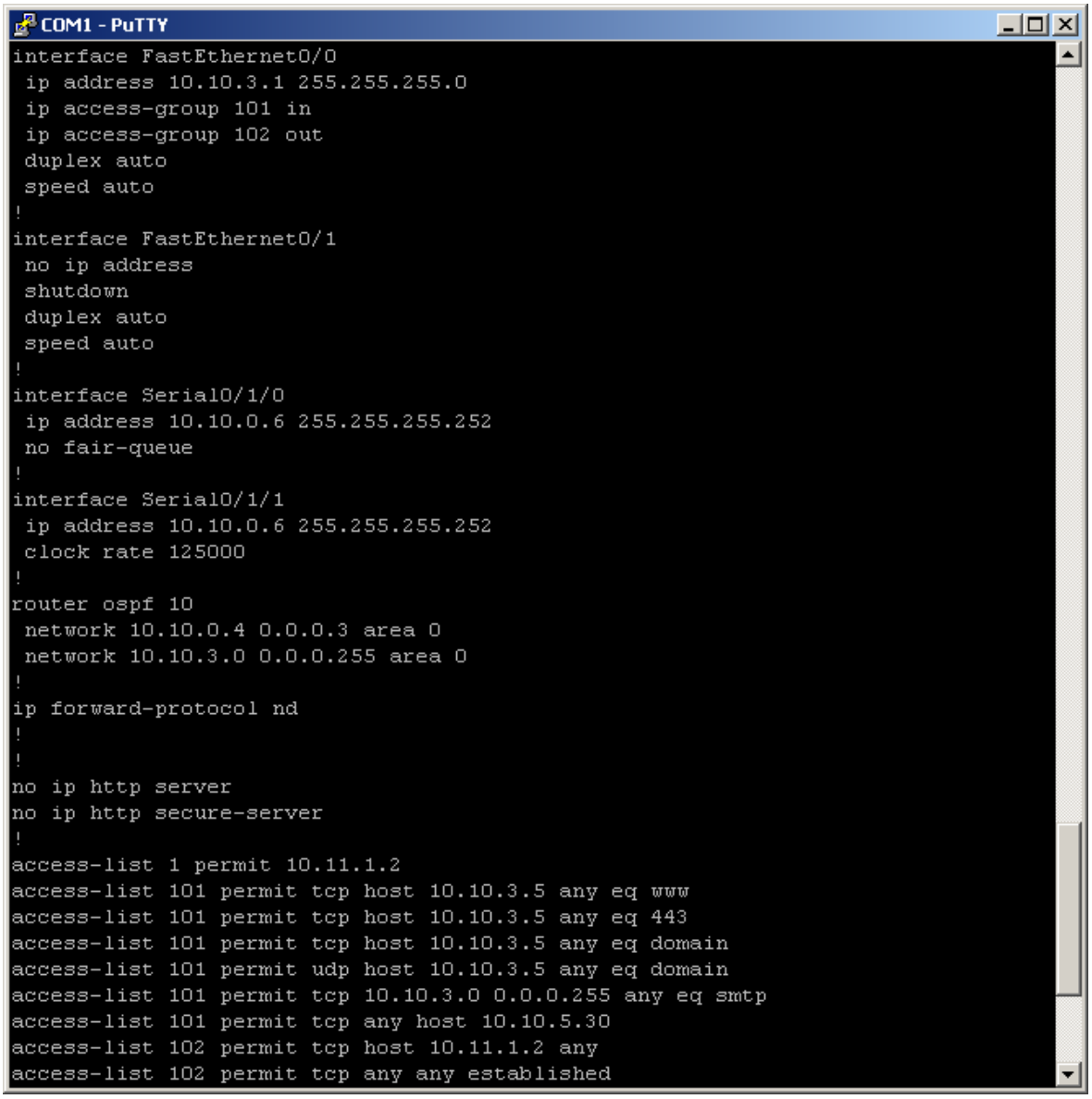


Obr. 14. Základná konfigurácia R3

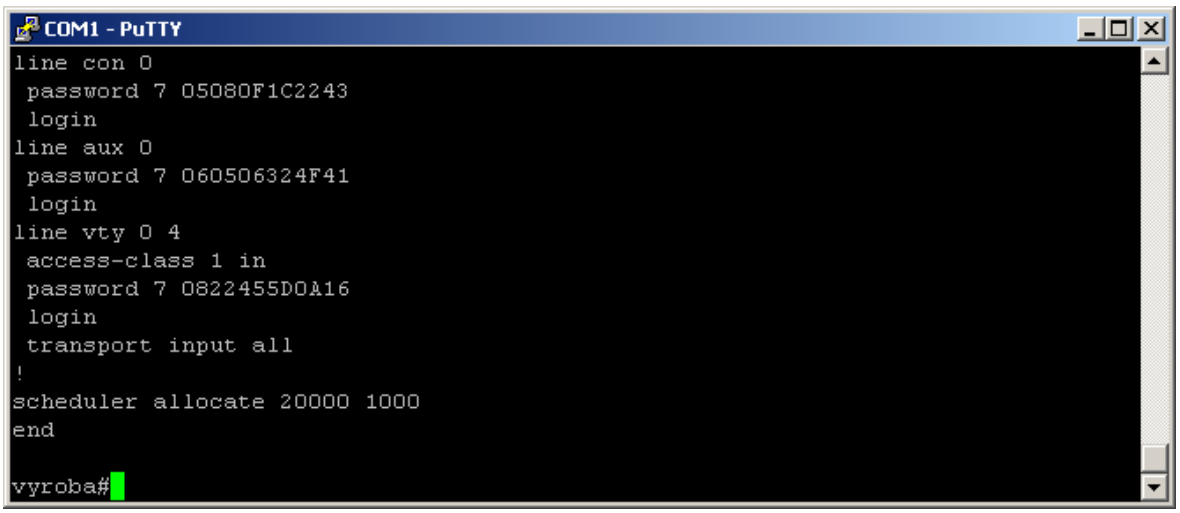
Obrázok 14, 15 a 16 je výpis konfigurácie posledného zariadenia, obsahuje rovnaké časti ako zariadenia opísané pred ním. Na obrázku 14 vidno pomenovanie routru, nadstavenie hesla prístupových módov a ich následné zašifrovanie.

V ďalšom výpise na obrázku 15 sú konfigurované porty, a k nim pridelené prístupové zoznamy. Pod výpisom portov je informácia o routovacom protokole OSPF a jeho sieťach, ku ktorým je zariadenie pripojené. Po výpise protokolu sa nachádza informácia o prístupových zoznamoch a zahŕňa celkový tvar ako pri ich nadstavovaní.

Posledný výpis zo zariadenia výroba je na obrázku 16 a znázorňuje výpis o prístupových portoch.



Obr. 15. Porty, protokol a ACL na R3



Obr. 16. Zabezpečené porty R3

8 VPLYV ACL NA SIEŤ

Hlavnou prioritou správcu siete by mala byť ochrana kritických, citlivých a dôležitých dát spolu so sieťovými prostriedkami pred všetkými druhmi zneužitia. Prístupové zoznamy sú integrovanou súčasťou bezpečnostných riešení v aktívnych zariadeniach Cisco. Správa konfigurácia a použitie ACL predstavuje dôležitú súčasť základných nastavení z dôvodu vlastnosti veľmi pružného sieťového nástroja. Ich prínos pre zvýšenie efektivity a funkčnosti siete má obľubu pri ich častom použití. Správca ma po aplikovaní mimoriadnu úroveň kontroly celkovej prevádzky v rámci podniku. V niektorých situáciách môže správca zhromažďovať štatistiky prenesených dát, a po ich vyhodnotení implementovať potrebné zásady zabezpečenia.

Medzi hlavné dôvody použitia ACL v sieti sú limity, ktoré znížia nežiadanú prevádzku pre zvýšenie výkonu siete. To umožní riadenie toku medzi jednotlivými zariadeniami, ktoré správca obmedzí. V rámci jednoduchých ACL má správca len obmedzené možnosti z hľadiska pridelenia práv. Jednoducho zakáže, alebo povolí komunikáciu z jednej strany podľa umiestnenia na porte. Použitím rozšíreného ACL sa rozširujú jeho možnosti pre detailnejšie zadanie podmienky. Tieto funkcie sú veľmi užitočné, ak chce povoliť časti alebo konkrétnemu zariadeniu minimálne práva v rámci siete.

ZÁVER

Počítačová sieť a jej ochrana predstavuje v súčasnosti najviac preferovaný problém v rôznych oblastiach informačných technológií. Cieľom práce bolo vytvoriť firemnú sieť s access listami pre vymedzenie vstupu užívateľom.

Pred samotnou realizáciou boli v práci rozobrané dôležité aspekty týkajúce sa počítačových sietí a možné druhy útokov ohrozujúce bezpečnú funkčnosť prevádzky. Súčasne obsahuje popis zabezpečenia formou firewallu, ktorého funkciou sú access listy.

V rámci prideľovania IP adries je v sieti použitý súkromný rozsah triedy A, ktorý poskytuje veľký priestor pre pripojenie mnohých zariadení. Firma tejto veľkosti nikdy nevyužije všetky dostupné IP adresy. Toto riešenie je použité z dôvodu dobrej prehľadnosti v sieti a zároveň umožňuje ľahké orientovanie pre správcu.

Zhotovenie modelu prebehlo v simulačnom prostredí Cisco Packet Tracer a poskytuje reálnu predstavu o dizajne firemnej siete. Konfigurácia obsahuje kompletné nastavenie pre spoľahlivé fungovanie celej siete, komunikácia medzi zariadeniami je sprostredkovaná protokolom OSPF.

Návrh pre prístup užívateľov do siete spočíval v minimalizácii ich práv. Na toto riešenie boli použité štandardné a zložité access listy. Tie vymedzujú jednotlivý prístup k funkciám siete. V modeli nebolo možné použiť časový prístupový zoznam, ktorý je podporovaný len novšími typmi zaradení.

Pri konfigurácii na aktívnych prvkoch vznikol problém s počtom portov. V návrhu siete boli použité prídavné moduly s portami pre zväčšený počet rozhraní k hlavnému routru. Aktívne zariadenia obsahujú menší počet rozhraní a ich pridanie vyžaduje veľké náklady. Kúpa rozširovacích modulov by bola pre tento prípad zbytočná, preto vhodným riešením pri konfigurácii bolo vynechanie dvoch skupín užívateľov, teda išlo o správcu siete a wifi pripojenie v budove. Prednosť k pripojeniu dostali kancelárske priestory a serverovňa, nakoľko zohrávajú dôležitejšiu úlohu vo funkčnosti siete. Následkom tohto rozhodnutia nebolo možné odskúšať prístupové zoznamy určené pre vynechané rozhrania. Ostatné funkcie pracovali správne.

ZOZNAM POUŽITEJ LITERATÚRY

[1] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005, 338 s. ISBN 80-251-0417-6.

[2] SOSINSKY, Barrie A. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. Vyd. 1. Brno: Computer Press, 2010, 840 s. ISBN 978-80-251-3363-7.

[3] COLE, Eric, Ronald L KRUTZ a James W CONLEY. *Network security bible*. 2nd ed. Indianapolis, IN: Wiley, c2009, xliv, 891 p. ISBN 0470502495.

[4] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.

[5] SIMMONS, Curt a James F CAUSEY. *Mistrovství v sítích Microsoft Windows XP*. Vyd. 1. Brno: CP Books, 2005, 620 s. Microsoft Office (CP Books). ISBN 80-251-0583-0.

[6] LAMMLE, Todd. *CCNA: výukový průvodce přípravou na zkoušku 640-802*. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-80-251-2359-1.

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

[8] SZOR, Peter. *Počítačové viry: analýza útoku a obrana*. Vyd. 1. Brno: Zoner Press, 2006, 608 s. Encyklopedie Zoner Press. ISBN 80-86815-04-8.

[9] MAREK, Vlastimil. *Něco v síti: fejetony, které vycházely od roku 1997 na internetu na adrese http://svet.namodro.cz* [online]. In: . [cit. 2015-05-01]. DOI: http://www.samuraj-cz.com/clanek/tcpip-adresy-masky-subnety-a-vypocty/

[10] MATOUŠEK, Petr. *Síťové aplikace a jejich architektura*. 1. vyd. Brno: VUTIUM, 2014, 396 s. ISBN 978-80-214-3766-1.

[11] TIMM, Carl, Richard PEREZ a Adam ELY. *Seven deadliest social network attacks*. Burlington, MA: Syngress/Elsevier, 2010, xxi, 133 p. Syngress seven deadliest attacks series. ISBN 15-974-9545-X.

[12] MERHAUT, Filip a Ivan ZELINKA. *Počítačové viry a bezpečnost*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2008 [i.e. 2009], 142 s. ISBN 978-80-7318-763-7.

[13] MANZUIK, Steve, Chris GATFORD a Andre GOLD. *Network security assessment: from vulnerability to patch*. Rockland, MA: Syngress Pub., 2007, xxii, 372 p. ISBN 9781597491013..

[14] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí (praktické rady a návody)*. 1. vyd. Praha: Grada, 2003, 200 s. ISBN 80-247-0663-6.

[15] KÁLLAY, Fedor. *Počítačové sítě a jejich aplikace*. 1. vyd. Praha: Grada, 1999, 311 s. ISBN 80-716-9407-X.

[16] LAMMLE, Todd. *CCNA Cisco certified network associate study guide*. 2nd ed. San Francisco: Sybex, 2000, lx, 766 p. ISBN 07-821-2647-2.

[17] THOMAS, Thomas M. *OSPF network design solutions*. 2nd ed. Indianapolis, IN: Cisco Press, 2003, xx, 747 p. Cisco Press networking technology series. ISBN 15-870-5032-3.

[18] ODOM, Wendell, Rus HEALY a Naren MEHTA. *Směrování a přepínání sítí: autorizovaný výukový průvodce*. Vyd. 1. Brno: Computer Press, 2009, 879 s. ISBN 978-80-251-2520-5.

[19] BALCHUNAS, Aaron. *Access Control Lists* [online]. 2007, (1.11) [cit. 2015-05-13]. Dostupné z: http://www.routeralley.com/guides/access_lists.pdf.

[20] BOHÁČ, Leoš a Pavel BEZPALEC. *Datové sítě: přednášky*. 1. vyd. V Praze: České vysoké učení technické, 2011, 204 s. ISBN 978-80-01-04694-4.

[21] STREBE, Matthew a Charles PERKINS. *Firewally a proxy-servery*. Vyd. 1. Brno: Computer Press, 2003, xxi, 450 s. ISBN 80-722-6983-6.

[22] Security Configuration Guide: *Access Control Lists, Cisco IOS XE Release 3S*. In: Cisco Systems, Inc. [online]. San Jose, 2014 [cit. 2015-05-25]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/sec-data-acl-xe-3s-book.pdf

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

ACL	Access Control List.
CD	Compact Disk
DAC	Discretionary Access Control
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IHL	Internet Header Length
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
NAT	Network Address Translation
OS	Operačný systém
OSPF	Open Shortest Path First
PING	Packet InterNet Groper
QOS	Quality Of Services
RTP	The Real-time Transport Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer

TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VLSM	Variable Length Subnet Mask
WAN	Wide Area Network

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK