Aplikace formální konceptuální analýzy pro speciální síťové prvky

Bc. Pavel Měsíček

Diplomová práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Pavel Měsíček**
Osobní číslo:	**A19802**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Aplikace formální konceptuální analýzy pro speciální síťové prvky**
Téma práce anglicky:	**Applying Formal Concept Analysis for Special Network Elements**

Zásady pro vypracování

1. Formou literární rešerše zpracujte teoretickou část práce pro praktické využití formální konceptuální analýzy se softwarovým zpracováním a verifikací získaných hodnot.
2. Stanovte supremum a infimum pro speciální síťové prvky.
3. Aplikujte formální konceptuální analýzu do oblasti speciálních síťových prvků a vyhodnoťte softwarové zobrazení výpočtů svazů kontextů.
4. Popište svazy kontextů a atributových implikací včetně navigace pro Galoisovy konexe množin speciálních síťových prvků
5. Získané výsledky data mining uveďte ve 3D prostředí s využitím diagramů.

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

Seznam doporučené literatury:

1. NAVARA, Mirko a Petr OLŠÁK. Základy Fuzzy množin. Vyd. 1. Praha: Vydavatelství ČVUT, 2002, 136 s. ISBN 80-01-02585-3.
2. NOVÁK, Vilém. Fuzzy množiny a jejich aplikace. Praha: Nakladatelství technické literatury, 1990. ISBN 80-03-00325-3.
3. BĚLOHLÁVEK, Radim. Konceptuální svazy a formální konceptuální analýza [on-line]. 2004 [cit. 2019-10-06]. Dostupné z WWW: http://belohlavek.inf.upol.cz/publications.pdf.
4. ELZINGA, P. G. Formalizing the concepts of crimes and criminals [online]. Amsterdam, 2011 [cit. 2019-10Ş06]. Dostupné z: http://dare.uva.nl/document/2/96595. PhD thesis. Amsterdam Business School Research Institute.
5. ZADEH, L. A. Fuzzy Sets [online]. California, 1965 [cit. 2019-10-06]. Dostupné z: http://www.cs.berkeley.edu/.zadeh/papers/Fuzzy 20Sets-InformationControl-1965.pdf. University of California, Berkeley. Concept Explorer.

Vedoucí diplomové práce: **Ing. Ján Ivanka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **9. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

Jméno, příjmení: Pavel Měsíček

Název bakalářské/diplomové práce: Aplikace formální konceptuální analýzy pro speciální síťové prvky

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 28. 7. 2020

PAVEL MĚSÍČEK v.r.
.....
podpis diplomanta

ABSTRAKT

Diplomová práce je zaměřena na formální konceptuální analýzu do oblasti speciálních síťových prvků. Analýza je zpracována pro switche, firewally a routery, které tvoří základ síťové infrastruktury. V teoretické části je popsána formální konceptuální analýza a rozšíření o fuzzy logiku spolu s popisem suprema a infima. Teoretickou část uzavírá popis switchů, firewallů a routerů. Praktická část práce popisuje program Concept Explorer. Dále je zde vytvořena formální konceptuální analýza pro vybrané síťové prvky. Z každé kategorie bylo vybráno šest produktů. Výstupem každé dílčí práce je konceptuální svaz spolu s atributovými implikacemi. V závěru praktické části je vybráno supremum a infimum pro switche, firewally a routery.

Klíčová slova: formální konceptuální analýza, atributové implikace, supremum, infimum, konceptuální svaz, koncept, kontext, síťové prvky.

ABSTRACT

This diploma thesis deals with the formal concept analysis in the sphere of peculiar network elements. The analysis is utilized for switches, firewalls and routers since all of the these are a fundamental base of the network infrastructure. The theoretical part focuses on the description of the formal concept analysis and an extension of the fuzzy logic along with a description of supremum and infimum. The end of this part is devoted to the description of switches, firewalls and routers. The practical part of this diploma thesis describes the Concept Explorer programme and the formal concept analysis for the peculiar network elements is created. Six products were chosen from each category. The outcome of each part is a concept association together with attribute implications. In the conclusion of the practical part, supremum and infimum is chosen for switches, firewalls and routers.

Keywords: formal concept analysis, attribute implications, supremum, infimum, concept association, concept, context, network elements.

Děkuji svému vedoucímu práce panu Ing. Jánu Ivankovi za pomoc s výběrem tématu a cenné rady při jeho zpracování. Rád bych také poděkoval svým rodičům a přítelkyni za podporu po dobu mého studia.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

„Když nejde o život, nejde o nic.“

Jan Werich

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **10**
1 FORMÁLNÍ KONCEPTUÁLNÍ ANALÝZA **11**
1.1 VYMEZENÍ ZÁKLADNÍCH POJMŮ FKA 11
1.1.1 Formální kontext, koncept a konceptuální svaz 11
1.1.2 Atributové implikace 13
1.2 VÍCEHODNOTOVÉ KONCEPTY A KONCEPTUÁLNÍ ŠKÁLOVÁNÍ 14
2 FUZZY ROZŠÍŘENÍ **16**
2.1 FUZZY LOGIKA 17
2.2 FUZZY KONCEPT, KONTEXT A KONCEPTUÁLNÍ SVAZ 19
2.3 SUPREMUM 20
2.4 INFIMUM 20
3 SPECIÁLNÍ SÍŤOVÉ PRVKY **21**
3.1.1 MAC adresa 21
3.1.2 IP adresa 21
3.1.3 Paket a rámec 21
3.1.4 TCP/IP a OSI 22
3.2 SWITCH 23
3.3 FIREWALL 24
3.3.1 Typy firewallu 25
3.4 ROUTER 27
II PRAKTICKÁ ČÁST **28**
4 APLIKACE FORMÁLNÍ KONCEPTÁLNÍ ANALÝZY **29**
4.1 PROGRAM CONCEPT EXPLORER 29
4.1.1 Ovládání programu 29
4.1.2 Orientace v konceptuálním svazu programu Concept Explorer 31
5 VYBRANÉ SÍŤOVÉ PRVKY **32**
5.1 ANALÝZA PRO VYBRANÉ SWITCHE 32
5.1.1 Zvolené atributy 32
5.1.2 Zvolená zařízení 34
5.1.3 Výstup programu ConExp pro switche 39
5.2 ANALÝZA PRO VYBRANÉ FIREWALLY 41
5.2.1 Zvolené atributy 41
5.2.2 Zvolené programy 44
5.2.3 Výstup programu ConExp pro Firewally 48
5.3 ANALÝZA PRO VYBRANÉ ROUTERY 50

5.3.1 Zvolené atributy 50
5.3.2 Zvolená zařízení 53
5.3.3 Výstup programu ConExp pro routery 60
6 3D ZOBRAZENÍ VÝSLEDKŮ 63
ZÁVĚR 66
SEZNAM POUŽITÉ LITERATURY 67
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 72
SEZNAM OBRÁZKŮ 74
SEZNAM TABULEK 76

ÚVOD

Internet od své prvotní myšlenky, která je zde již více než půl století, ušel velký kus cesty. Pro většinu uživatelů je dnes internet poměrně běžným standardem, který přináší spoustu užitku, ale může přinést i velké strasti. S jeho nástupem přišel také nový typ zločinů, který se vyskytuje v kyberprostoru. Aby bylo možné stále uchovávat data v bezpečí, je nutné dodržovat zásady kyberbezpečnosti. Je podstatné stále udržovat softwarové a hardwarové komponenty aktuální, aby byly schopny odolávat útokům kyberzločinců.

Běžný uživatel internetu by měl dbát zásad pohybu v síti. Neměl by navštěvovat nedůvěryhodné webové stránky, používat stejná hesla pro všechny účty či otevírat pochybné e-maily. Jsou zde však i jiné potřeby, o které je nutné dbát. Patří sem především údržba domácí infrastruktury. Je nutné mít správně nastavené a aktualizované switche, firewally a routery. Zmíněné komponenty se starají o bezpečnou komunikaci interní sítě s internetem. Existuje řada útoků na uvedené komponenty a prakticky není možné zajistit naprostou bezpečnost komunikace, nicméně pořízení a nastavení kvalitních komponent snižuje riziko na minimum.

Diplomová práce se zaměřuje na zvolení správných produktů z široké řady dostupných síťových komponent. Pro tuto činnost byla zvolena formální konceptuální analýza, která je schopna zobrazit souvislosti, jež není možné vidět běžným způsobem.

Teoretická práce je zaměřena na specifikaci formální konceptuální analýzy. Jsou popsány definice jako konceptuální škálování, atributové implikace a konceptuální svaz, jenž jsou podstatné při náležité tvorbě formální konceptuální analýzy. Dále je zde popsáno rozšíření o Fuzzy logiku, která upřesňuje výsledky zvolené analýzy. V neposlední řadě jsou zmíněny speciální síťové prvky včetně protokolů a vrstev, pomocí kterých bezpečná komunikace probíhá.

V praktické části byl specifikován zvolený program Concept Explorer, který s prostřednictvím správných hodnot dokáže vytvořit konceptuální svaz a atributové implikace. Pro každou analýzu u switchů, firewallů a routerů bylo fixně vybráno šest objektů. Z hlediska atributů pro jednotlivé prvky bylo nutné zvolit takové, které zajišťují rychlý a bezpečný přenos dat. Poslední část práce je zobrazení výstupu 3D grafů, za pomoci kterých je možné určit supremum a infimum.

I. TEORETICKÁ ČÁST

1 FORMÁLNÍ KONCEPTUÁLNÍ ANALÝZA

Dnešní svět je velmi přesycen množstvím informací. Z tohoto důvodu byl vytvořen obor, jenž nese název informatika a který se zabývá zpracováním dat. Při manipulaci s daty je velmi důležité využít nástroje, popř. metody, které usnadní vyhledávání v databázích nebo zobrazí netriviální informace ze vstupních dat, tím pádem dá uživateli nový pohled na danou problematiku. Mezi takovou metodu patří formální konceptuální analýza.

Formal Concept Analysis, do češtiny přeloženo jako formální konceptuální analýza (dále jen FKA), byla vynalezena v roce 1982 německým matematikem Rudolfem Willem. Metoda je explorativní, resp. průzkumová a zabývá se vizualizací tabulkových dat. Pro tuto metodu je nezbytné převést vstupní data na binární [1].

Při využití FKA získáme konceptuální svaz a atributové implikace. U konceptuálního svazu platí, že je to sjednocení množin jistých shluků, které jsou uspořádány hierarchicky, což znamená, že jdou vidět v podobě nadřazených a podřazených prvků. Tyto specifické množiny se dále nazývají formální koncepty a je možné je nalézt ve vstupní tabulce dat. Jak již bylo zmíněno, druhý výstup se nazývá atributové implikace a popisuje vazby mezi atributy v tabulce dat [1].

1.1 Vymezení základních pojmů FKA

1.1.1 Formální kontext, koncept a konceptuální svaz

Definice 1. *(Formální) kontext je trojice ⟨X, Y, I⟩, kde I je binární relace mezi množinami X a Y [1].*

Definice se dá zapsat jako $\langle x, y \rangle \in I$. Prvky množiny X jsou objekty a prvky Y jsou atributy. Předchozí zápis značí, zda daný objekt má konkrétní atribut. Jelikož FKA pracuje pouze s bivalentními hodnotami, je nutný převod na jedničky a nuly. V následující tabulce (Tab. 1), lze vidět ukázku formálního kontextu [1].

Tab. 1 Formální kontext [Vlastní zdroj].

x_i / y_i	y_1	y_2	y_3	y_4	y_5
x_1	1	1	0	1	0
x_2	0	1	0	0	0
x_3	0	1	1	0	0
x_4	1	1	0	1	1

Jakýkoli kontext $\langle X, Y, I \rangle$ naznačuje zobrazení $\uparrow: 2X \rightarrow 2Y$ a $\downarrow: 2Y \rightarrow 2X$ předpisem

$$A\uparrow = \{y \in Y; \forall x \in A: \langle x, y \rangle \in I\} \quad (1)$$

pro $A \subseteq X$ a

$$B\downarrow = \{x \in X; \forall y \in B: \langle x, y \rangle \in I\} \quad (2)$$

pro $B \subseteq Y$.

Množina atributů $A\uparrow$ je společná všem objektům z A. Množina celkových objektů $B\downarrow$ sdílí atributy z B [1].

Definice 2. *Zobrazení $f: 2X \rightarrow 2Y$ a $g: 2Y \rightarrow 2X$ tvoří tzv. Galoisovu konexi mezi množinami X a Y, pokud pro $A, A1, A2 \subseteq X$ a $B, B1, B2 \subseteq Y$ platí $A1 \subseteq A2 \Rightarrow f(A2) \subseteq f(A1)$; $B1 \subseteq B2 \Rightarrow g(B2) \subseteq g(B1)$; $A \subseteq g(f(A))$; $B \subseteq f(g(B))$* [1].

Věta 1. *Pro binární relaci $I \subseteq X \times Y$ tvoří indukovaná zobrazení $\uparrow I$ a $\downarrow I$ Galoisovu konexi mezi X a Y. Naopak, tvoří-li f a g Galoisovu konexi mezi X a Y, existuje binární relace $\subseteq X \times Y$ tak, že $f = \uparrow I$ a $g = \downarrow I$. Tím je dán vzájemně jednoznačný vztah mezi Galoisovými konexemi mezi X a Y a binárními relacemi mezi X a Y* [1].

Pro jednodušší pochopení Galoisových konexí a výše zmíněné podmínky $A1 \subseteq A2 \Rightarrow f(A2) \subseteq f(A1)$ je nutné zajít dále do historie, kde byla vymyšlena Port-Royalská škola, ze které vychází FKA [1].

Port-Royalská škola pracovala s rozsahy a obsahy. Jako rozsah je bráno sjednocení všech objektů a obsahem se uvádí koalice všech atributů. Pro pojem *kapr* se rozsahem považuje uskupení všech ryb a obsahem se považuje sjednocení všech vlastností jako jsou žábry, šupiny atd. [1].

Nyní lze vysvětlit předchozí podmínka, která popisuje obrácený poměr rozsahů a obsahů. Čím více objektů bude, tím méně budou mít společného [1].

Definice 3. *(Formální) koncept v kontextu $\langle X, Y, I \rangle$ je dvojice (A, B), kde $A \subseteq X$ a $B \subseteq Y$ jsou takové, že $A\uparrow = B$ a $B\downarrow = A$ [1].*

Dle definice se ve formálním konceptu vyskytuje dvojice (A, B), kde množina A představuje objekty, které následně sdílí atributy z množiny B. Dále množina B obsahuje atributy společné objektům z množiny A. V matematice se toto tvrzení označuje jako fixní bod Galoisovy konexe dané $\uparrow$ a $\downarrow$ [1].

Množinu všech formálních konceptů v $\langle X, Y, I \rangle$ se značí B (X, Y, I), tj.

$$B(X, Y, I) = \{(A, B) \mid A \subseteq X, B \subseteq Y, A\uparrow = B, B\downarrow = A\} \quad (3)$$

Definice 4. *Konceptuální svaz je množina B (X, Y, I) spolu s relací ≤ definovanou na B (X, Y, I) předpisem (A1, B1) ≤ (A2, B2) právě když A1 ⊆ A2 (nebo, ekvivalentně, B2 ⊆ B1) [1].*

Poměr ≤ je tedy souvislostí mezi podpojmem-nadpojmem [1].

Věta 2 (hlavní věta o konceptuálních svazech). *Mějme formální kontext ⟨X, Y, I⟩. (1) B (X, Y, I) je vzhledem k ≤ úplný svaz, ve kterém jsou infima a suprema dána předpisy:*

$$\bigwedge_{j\in J}\langle A_j, B_j\rangle = \left\langle \bigcap_{j\in J} A_j, \left(\bigcap_{j\in J} A_j\right)^{\uparrow}\right\rangle = \left\langle \bigcap_{j\in J} A_j, \left(\bigcup_{j\in J} B_j\right)^{\downarrow\uparrow}\right\rangle \quad (4)$$

$$\bigvee_{j\in J}\langle A_j, B_j\rangle = \left\langle \left(\bigcap_{j\in J} B_j\right)^{\downarrow}, \bigcap_{j\in J} B_j\right\rangle = \left\langle \left(\bigcup_{j\in J} A_j\right)^{\uparrow\downarrow}, \bigcap_{j\in J} B_j\right\rangle \quad (5)$$

*(2) Daný úplný svaz **V** = ⟨V, ⊑⟩ je izomorfní s B (X, Y, I), právě když existují zobrazení γ: X →V, μ: Y →V, pro která je γ(X) supremálně hustá v **V**, μ (Y) infimálně hustá v **V** a ⟨x, y⟩ ∈ I platí právě, když γ(x) ≤ μ(y) (pro každé x ∈ X, y ∈ Y)* [1].

1.1.2 Atributové implikace

Atributová implikace neboli atributová souvislost, která je nad množinou Y atributů, je výraz ve tvaru A ⇒ B, kde A, B ⊆ Y. [1]

Definice 5. *Pro implikaci A ⇒ B a množinu C ⊆ Y říkáme, že A ⇒ B platí v C, popř. že C je modelem A ⇒ B, jestliže platí, že pokud A ⊆ C, pak i B ⊆ C. Obecněji, pro množinu M ⊆ 2^Y množin atributů a množinu T = {A_j ⇒ B_j | j ∈ J} implikací říkáme, že T platí v M, popř. že M je modelem T, jestliže A_j ⇒ B_j platí v C pro každé C ∈ M a A_j ⇒ B_j ∈ T.* [1]

Implikace se považuje za platnou v kontextu ⟨X, Y, I⟩, zdali je platná v systému M = {{x}↑ | x ∈ X} obsahů všech objekt-konceptů. Následně se považuje za platnou implikace v konceptuálním svazu B (X, Y, I), jestliže je platná v systému Int (I) všech obsahů [1].

Věta 3. *Atributová implikace platí v ⟨X, Y, I⟩, právě když platí v B (X, Y, I)* [1].

Definice 6. *Implikace A ⇒ B (sémanticky) plyne z množiny T implikací (zapisujeme T | = A⇒B), jestliže A⇒B platí v každé C ⊆ Y, ve které platí T. Množina T implikací se nazývá*

- *uzavřená, zdali obsahuje každou implikaci, která z ní plyne;*
- *neredundantní, zdali žádná implikace z T neplyne z ostatních (tj. nikdy není* $T - \{A \Rightarrow B\} \models A \Rightarrow B$*)* [1].

Jestliže z množiny T implikací kontextu ⟨X, Y, I⟩ plyne každá implikace kontextu ⟨X, Y, I⟩, dá se považovat za úplnou. Tím je báze kompletní a neredundantní množina implikací daného kontextu. [51]

Zde je podstatné se zajímat pouze o netriviální implikace a vynechávat takové, které vyplývají z ostatních. Například s banální implikací A ⇒ B, kde B ⊆ A není nutné dále pracovat. Nicméně je nezbytné být na pozoru, aby byla množina neustále úplná, resp. z ní implikace plynou a zároveň není redundantní [1].

Věta 4. *Množina T implikací je uzavřena, právě když pro každé* $A, B, C, D \subseteq Y$ *platí:*

1. $A \Rightarrow A \in T$;
2. *pokud* $A \Rightarrow B \in T$, *pak* $A \cup C \Rightarrow B \in T$;
3. *pokud* $A \Rightarrow B \in T$ *a* $B \cup C \Rightarrow D \in T$, *pak* $A \cup C \Rightarrow D \in T$ [1].

Definice 7. *Pseudointent kontextu* $\langle X, Y, I\rangle$ *je množina* $A \subseteq Y$, *pro kterou platí, že* $A \neq A{\downarrow\uparrow}$ *a že* $B{\downarrow\uparrow} \subseteq A$ *pro každý Pseudointent* $B \subset A$ [1].

Věta 5. *Množina*
$\{A \Rightarrow A{\downarrow\uparrow} \mid A$ *je pseudointent* $\langle X, Y, I\rangle\}$, *implikace je úplná a neredundantní, tj. báze* [1].

1.2 Vícehodnotové koncepty a konceptuální škálování

Jak již bylo řečeno FKA pracuje pouze s bivalentními logickými atributy. Pokud se však bude analýza aplikovat na položky jako je cena, úroveň, materiál atd., nebude prakticky možné si vystačit pouze s „1“ a „0“. Z tohoto důvodu bylo vynalezeny vícehodnotové koncepty a především konceptuální škálování [1].

Definice 8. *Vícehodnotový kontext je čtveřice* $\langle X, Y, W, I\rangle$, *kde* $I \subseteq X \times Y \times W$ *je ternární relace taková, že pokud* $\langle x, y, v\rangle \in I$ *a* $\langle x, y, w\rangle \in I$, *pak* $v = w$ [1].

K objektům, které se značí písmenem X a k vícehodnotovým atributům, které se označují písmenem Y, přibylo do definice písmeno W, jenž je množinou zobrazující hodnoty atributů. Vysvětlení zápisu ⟨x, y, v⟩ ∈ I je takové, že objekt x má atribut y s hodnotou w. Lze zapsat také jako y(x) = w. Aby mohly být vícehodnotové kontexty analyzovány pomocí FKA, je

nutné je převést na základní kontext pomocí škálování na tzv. rozšíření základních kontextů [1].

Definice 9. *Škála (scale) pro atribut y vícehodnotového kontextu je kontext* $S_y = (X_y, Y_y, I_y)$, *pro který* $y(X) \subseteq X_y$ *(kde* $y(X) = \{y(x) \mid x \in X\}$*). Prvky množin* X_y *a* Y_y *se nazývají škálové hodnoty a škálové atributy [1].*

V následující tabulce (Tab. 2) lze vidět, že atribut již neobsahuje pouze bivalentní logické atributy. Nyní je nutné uplatit jednu ze standardních škál jako jsou interordinální, ordinální, nominální, dichotomické či biordinální atd.

Tab. 2 Názorná ukázka – vícehodnotový kontext [1].

x_i / y_i	y_1	y_2	y_3
x_1	3	1	17
x_2	5	0	44
x_3	14	1	73

V předchozí tabulce (Tab. 2) jsou vyobrazeny atributy, se kterými není možné pracovat, proto je nutné vytvořit novou tabulku (Tab. 3) a pomocí škálování se znovu dopracovat k hodnotám, se kterými je již možné pracovat [1].

Jak lze vidět, pouze atribut y_2 je připraven pro práci s FKA. Pro y_1 a y_3 bylo nutné vytvořit škálování o třech kategoriích [1].

Tab. 3 Názorná ukázka – konceptuální škálování [51].

x_i / y_i	$y_{1(0\text{-}4)}$	$y_{1(5\text{-}10)}$	$y_{1(11\text{-}15)}$	y_2	$y_{3(0\text{-}25)}$	$y_{3(26\text{-}45)}$	$y_{3(46\text{-}75)}$
x_1	1	0	0	1	1	0	0
x_2	0	1	0	0	0	1	0
x_3	0	0	1	1	0	0	1

Definice 10. *Je-li* (X, Y, W, I) *vícehodnotový kontext a jsou-li* S_y $(y \in Y)$ *škály, pak kontext odvozený jednoduchým škálováním je kontext* (X, Z, J), *kde*

- $N = \cup_{y \in Y} Y_y$ $(Y_y = \{y\} \times Y_y)$;
- $(x, (y, z)) \in J \Leftrightarrow y(x) = w$ *a* $(w, z) \in I_y$ [1].

2 FUZZY ROZŠÍŘENÍ

V předchozích dvou kapitolách byla provedena analýza formou literární rešerše základní problematika FKA, resp. práce s formálním konceptem a formálním kontextem, tzn. že dokáže pracovat pouze s 1 a 0. Proto přichází na řadu rozšíření o Fuzzy logiku, jedná se o nejdůležitější rozšíření, díky které může objekt nabývat jiných hodnot. Ve Fuzzy logice se rozebírá, zda je pojem vágní, tzn. že daný objekt patří do extendu určitého pojmu a nemusí to nutně znamenat 1 nebo 0 [1].

Jako důležitý předpoklad, který očekává využití Fuzzy logiky je fakt, že zdánlivě spousta naturálních situacích přispívá k objekt-atributovým datům s Fuzzy atributy. Díky tomuto výroku lze usnadnit pojem kontext [1].

Definice 11. ***(Formální) Fuzzy kontext*** *je trojice ⟨X, Y, I⟩, kde X a Y jsou množiny (objektů a atributů) a I je Fuzzy relace mezi X a Y* [1].

Objekt x, který má atribut y je označován jako stupeň *I* (x, y). Na počátku se zvolí struktura pravdivostních hodnot, resp. je nutné vybrat množinu pravdivostních hodnot a logických operací. Jakmile je vybrána, je možné s ní pracovat dále. Úplný reziduovaný svaz L = ⟨L, ⊗, →, ∧, ∨, 0, 1⟩ se považuje za běžnou strukturu a rovněž patří mezi hlavní struktury Fuzzy logiky. Písmeno L uchovává pravdivostní hodnoty hodnot (např. Lukasiewiczova implikace a → b = min (1, 1–a + b), Gödelova implikace a → b = 1 pro a ≤ b; = b pro a> b) [1].

Pro zmíněný Fuzzy kontext ⟨X, Y, I⟩, Fuzzy množinu A v X a Fuzzy množinu B v Y formulujeme Fuzzy množinu $A^{\uparrow}$ v Y a $B^{\downarrow}$ v X předpisy:

$$A^{\uparrow}(y) = \bigwedge_{x \in X} A(x) \rightarrow I(x, y)$$

a

$$B^{\downarrow}(y) = \bigwedge_{y \in Y} B(y) \rightarrow I(x, y)$$

Jako názorný příklad lze uvést, pokud za L dosadíme dvouprvkový reziduovaný svaz a ten je následně jednoduchou Booleovou algebrou klasické logiky: $A^{\uparrow}(y)$ je pravdivostní hodnota tvrzení "y má je sdílen všemi objekty z A", podobně pro $B^{\downarrow}(x)$ [1].

Definice 12. ***(Formální) Fuzzy koncept*** *ve Fuzzy kontextu ⟨X, Y, I⟩ je dvojice (A, B), kde A je Fuzzy množina objektů, B je Fuzzy množina atributů takových, že $A^{\uparrow} = B$ a $B^{\downarrow} = A$* [7].

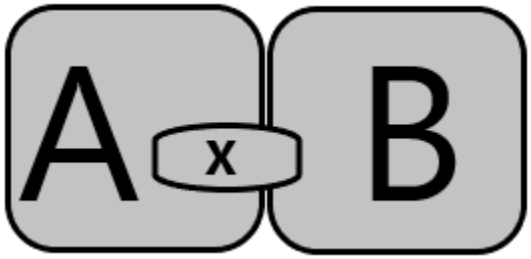
Rozsah A i obsah B Fuzzy konceptu je možné považovat za Fuzzy množinu, tedy je ve shodě s intuicí. Označíme-li B (X, Y, I) množinu všech Fuzzy konceptů v ⟨X, Y, I⟩ a vybavíme-li ji relací ≤ (podpojem-nadpojem) definovanou jako v běžném případě, tj.

(A1, B1) ≤ (A2, B2) právě když A1 ⊆ A2 (nebo, ekvivalentně, B2 ⊆ B1), (zde ovšem A1 ⊆ A2 znamená, že A1(x) ≤ A2(x) pro každý x ∈ X) dostaneme tzv. Fuzzy konceptuální svaz. Strukturu Fuzzy konceptuálních svazů popisuje následující věta, která zobecňuje hlavní větu o konceptuálních svazech z Fuzzy pohledu [51].

Věta 6. *Mějme formální Fuzzy kontext ⟨X, Y, I⟩. (1) B (X, Y, I) je vzhledem k ≤ úplný svaz, ve kterém jsou infima a suprema dána jako v (3) a (4). (2) Daný úplný svaz V = ⟨V, ⊑⟩ je izomorfní s B (X, Y, I), právě když existují zobrazení γ: X × L → V, μ: Y × L → V, pro která je γ(X×L) supremálně hustá v V, μ (Y ×L) infimálně hustá v V a a ⊗ b ≤ I (x, y) platí právě když γ (x, a) ≤ μ (y, b) (pro každé x ∈ X, y ∈ Y, a, b ∈ L)* [7].

2.1 Fuzzy logika

Název „Fuzzy“ je v překladu nejasnost, mlhavost atd. proto nelze jednoznačně určit u následujícího obrázku (Obr. 1), zda prvek X patří do množiny A, jelikož obsahuje stopové prvky množiny B.



Obr. 1 Prvek spadající do množiny A i B
[Vlastní zdroj].

Zde se začíná mluvit o tzv. částečné příslušnosti. Již nejedná o dvouprvkovou množinu {0, 1}, u které lze vidět ostré hranice, ale nastávají situace pro vytvoření množiny <0, 1>. Pro množinu <0, 1> se objevuje odchýlení od reality a přichází částečná příslušnost [2].

Fuzzy množiny se ve společnosti vyskytují stále, jelikož částečná příslušnost jde slovně vyjádřit velmi snadno - čeština či jiné světové jazyky obsahují slova jako málo, docela, téměř atd. [2].

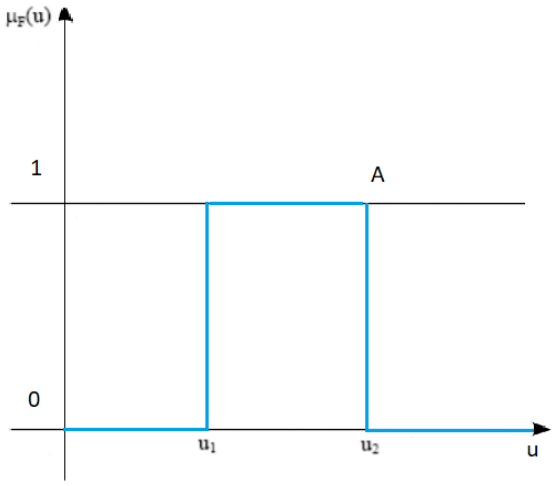
Definice 13. *Fuzzy množina je objekt A popsaný zobecněnou charakteristickou funkcí nazývanou funkcí příslušnosti* $\mu A: X \rightarrow \langle 0,1 \rangle$ *přiřazující* $\forall x \in X$ *hodnotu* $\mu A(x) \in \langle 0,1 \rangle$ *vyjadřující míru jakou prvek* $x \in A$. *[3]*

Všechny fuzzy podmnožiny univerza X tvoří množinu označovanou F(X) [3].

Stupeň příslušnosti, která je zapsán jako $\mu A: X \rightarrow \langle 0,1 \rangle$ *popisuje*, zda prvek X spadá do běžné množiny A. Zde může velikost nabývat dvou hodnot:

- Prvek příslušnosti 0 – prvek do množiny A (zcela) nenáleží,
- stupeň příslušnosti 1 – prvek do množiny A (zcela) náleží [4].

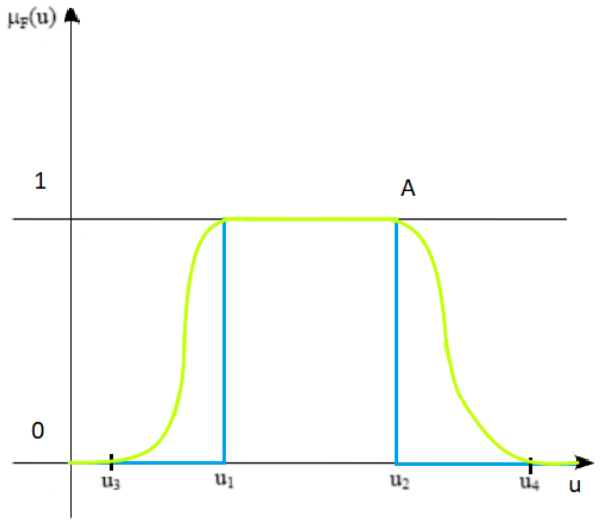
Jak již bylo řečeno, prvek může z většiny spadat do množiny A, ale určitou menšinovou částí taky do množiny B. Na následujícím obrázku (Obr. 2) lze vidět průběh běžné funkce příslušnosti [14].



Obr. 2 Průběh funkce - μA(u) pro běžnou množinu A [14].

Na následujícím obrázku (Obr.3) lze vidět odlišnost oproti předchozímu (Obr. 2). Zde se rovněž jedná o průběh funkce, ale s příslušností Fuzzy množiny A. Jak je možné vidět, všechny prvky z intervalu (-∞,u3) a (u4, + ∞) do množin A nespadají. Naopak zde spadají

prvky (u3, u4) a (u2, u3), a to z hlediska částečné příslušnosti, která je zde přidělena díky funkci μA(u) [14].



Obr. 3 Průběh funkce – μA(u) pro fuzzy množinu A [14].

2.2 Fuzzy koncept, kontext a konceptuální svaz

Znovu se zde opakují pojmy jako koncept, kontext a konceptuální svaz. Jelikož základní pojmy FKA nestačí, bylo nutné tyto pojmy a definice převést do Fuzzy množin, aby bylo možné pracovat se stupnicí pravdivosti mezi hodnotami 1 a 0 [1].

Definice 14. *(Formální) Fuzzy kontext je trojice ⟨X, Y, I⟩, kde X a Y jsou množiny (objektů a atributů) a I je Fuzzy relace mezi X a Y [1].*

Definice 15. *(Formální) Fuzzy koncept ve Fuzzy kontextu ⟨X, Y, I⟩ je dvojice (A, B), kde A je Fuzzy množina objektů, B je Fuzzy množina atributů takových, že* $A\uparrow = B$ *a* $B\downarrow = A$ *[1].*

Definice 16. *(Formální) Fuzzy konceptuální svaz je množinou všech Fuzzy konceptů B(X, Y,I) v ⟨X,Y,I⟩, obohacenou relací podpojmu-nadpojmu* $\leq$*, kde* $(A1,B1) \leq (A2,B2) \Leftrightarrow A1 \subseteq A2 \vee B2 \subseteq B1$ *[1].*

2.3 Supremum

Pojem supremum nahrazuje pojem „největší prvek“ z důvodu, že je možné jej nalézt u více množin. Supremum mají například omezené otevřené intervaly reálných čísel - zde supremum nahrazuje názvosloví „nejvyšší prvek“ [3].

V případě, kdy je možné očekávat, že množina X je uspořádána relací R, o prvku a∈X se dá říci, že je supremem podmnožiny Y ⊆ X, pokud je to nejmenší prvek množiny všech horních závor množiny Y. Tato skutečnost se zapisuje jako $a = sup_R(Y)$ [51].

2.4 Infimum

Pojem supremum nahrazuje pojem „nejmenší prvek“ z důvodu, že je možné jej nalézt u více množin. Infimum mají například omezené otevřené intervaly reálných čísel, zde infimum nahrazuje názvosloví „nejvyšší prvek“ [3]

V případě, kdy je možné očekávat, že množina X je uspořádána relací R, o prvku a∈X se dá říci, že je infimem podmnožiny Y ⊆ X, pokud je to největší prvek množiny všech dolních závor množiny Y. Tato skutečnost se zapisuje jako $a = inf_R(Y)$ [51].

3 SPECIÁLNÍ SÍŤOVÉ PRVKY

Doba se stále posunuje dále a bezpečnost na internetu se stala velmi klíčovým aspektem bezpečnosti jako takové. Útoky hackerů jsou stále propracovanější a dokáží způsobit velké škody jak společnostem, tak i jednotlivcům. Aby se minimalizovalo riziko těchto útoků, je důležité se bránit a mít správně nastavené tři základní zařízení, mezi které patří router (česky směrovač), switch (do češtiny se dá přeložit jako přepínač) a firewall neboli bezpečnostní brána. Některé domácí sítě stále využívají tyto prvky integrované do jednoho zařízení, což však již není možné u větších sítí. Pro pochopení, jak tyto prvky spolu souvisí a jak pracují, je nutné si vysvětlit pojmy jako je paket, rámec. Následovně anglické názvy Media Access Control (dále jen MAC adresa), Internet Protocol (dále jen IP adresa), síťové modely Transmission Control Protokol / Internet Protokol (dále jen TCP/IP) a Open Systems Interconnection (dále jen OSI).

3.1.1 MAC adresa

MAC adresa může být zapsána ve tvaru 12 znaků nebo šesti dvojic, které jsou rozděleny dvojtečkou či pomlčkou. Obsahuje čísla 0-9 a písmena A-F, slouží pro identifikaci síťové karty a měla by být jedinečná. MAC adresu lze změnit a tuto funkci především využívají hackeři pro útok zvaný MAC Spoofing. Jedná se o adresu složenou ze 48 bitů, která se následně rozdělí po 24 bitech. První polovina označuje výrobce a je přidělena za finanční poplatek. Druhou polovinu výrobce rozdělí na své výrobky. Problém by nastal, pokud by se setkaly dvě stejné MAC adresy ve stejné síti [5].

3.1.2 IP adresa

IP adresy se používají pro rozpoznání uzlu v síti. Jako první verze byla IPv4 a zapisovala se v decimální soustavě, problém je zde však, že mají pouze 32 bitů. Dále byla vyvinuta verze IPv6, která má 64 bitů a je zapisována v hexadecimální soustavě. Tato technologie by nemusela svůj rozsah vyčerpat příliš rychle, jelikož obsahuje 2^{64} adres [5].

3.1.3 Paket a rámec

Paket pracuje v síťové vrstvě a jedná se o datovou jednotku protokolu. V paketu se ukrývá především zdrojová a cílová IP adresa, zato rámec obsahuje zdrojovou a cílovou MAC adresu. Paket obsahuje blok dat, který se využívá u přenášení souboru od odesílatele k příjemci. Dále se zapouzdří do rámců, které již pracují o vrstvu níž, resp. ve fyzické vrstvě.

Rámec si zde přidá hlavičku a zakončení a následně se využije fragmentace čili rozdělení rámců na menší oddíly. U příjemce se z rámců opět vytvoří odesílaný soubor [4].

3.1.4 TCP/IP a OSI

OSI a TCP/IP patří mezi nejpoužívanější síťové modely. Z hlediska praxe se často využívá popisování podle modelu TCP/IP, jelikož se využívá pro navazování spojení a komunikace. Zato model OSI lze uplatnit především v literatuře, jelikož se téměř pro navazování komunikace nevyužívá [6].

Ministerstvo obrany Spojených států amerických vyvinulo model TCP/IP, který se skládá ze 4 vrstev:

1. **vrstva síťového rozhraní** – je to nejnižší vrstva síťového rozhraní a závisí na implementaci sítě, může se jednat o Ethernet, Token ring, x.25, SMDS a FDDI. Je vhodná především pro přenos datagramů. Používá SSL, http, DNS,
2. **síťová vrstva** – tato vrstva zajišťuje adresaci, směrování a předávání paketů. Používá IP, ICMP a OSPF,
3. **transportní vrstva** – jedná se o End-to-End spojení a doručení. Zajišťuje kompletní přenos dat. Využívá spojovaný protokol TCP a nespojovaný UDP,
4. **aplikační vrstva** – všechny aplikace, které fungují v síti mají svůj vlastní port, přes který funguje komunikace. Zde se využívají protokoly, jako je FTP, DHCP, Telnet atd., které se využívají pro přenos konkrétních dat [6].

Model OSI vyvinula Mezinárodní organizace pro normalizaci. Využívá se především vývoj zařízení pro digitální komunikaci. Na rozdíl od modelu TCP/IP 7 vrstev:

1. **fyzická vrstva** – na této vrstvě se neřeší, co konkrétního se přenáší v bitech, ale zabývá se fyzickým zasíláním dat. Do této vrstvy patří kabely, binární přenos a signály. Využívá 802.11g a 100BaseT,
2. **linková vrstva** – hlásí neopravitelné chyby, navazuje spojení mezi zařízeními v daném subnetu, zaznamenává datový tok a stará se o synchronizaci rámců. Využívá Ethernet, PPP, ARP,
3. **síťová vrstva** – jak již z názvu vypovídá, stará se o adresování a směrování v síti. Jedná se i o propojení několika sítí. Využívá IP, ICMP a OSPF,

4. **transportní vrstva** – jako jediná má stejné vlastnosti jako v modelu TCP/IP. Rovněž se stará o End-to-End spojení a poskytnutí kvalitního přenosu. Také využívá protokoly TCP a UDP,
5. **relační vrstva** – na této vrstvě probíhá komunikace dvou aplikací a udržuje se tzv. session. Využívá NetBIOS,
6. **prezenční vrstva** – zde se provádí šifrování přeposílaných dat. Zabývá se strukturou dat. Využívá se Samba,
7. **aplikační vrstva** – jedna se o poskytování přístupu aplikacím do komunikačního systému a povolování portů pro jejich spolupráci. Využívá http, DNS, POP3, SSH a Telnet [6].

TCP/IP byl vynalezen dříve než model OSI, z tohoto důvodu je skladba vrstev jiná. Při porovnání je sloučena fyzická a linková vrstva. Dále je v aplikační vrstvě sloučena aplikační, prezenční a relační vrstva, což lze názorně vidět v následující tabulce (Tab. 4) [6].

Tab. 4 Porovnání TCP/IP a ISO modelu [6].

<table>
<tr><th>TCP/IP</th><th>ISO</th></tr>
<tr><td rowspan="3">Aplikační vrstva</td><td>Aplikační vrstva</td></tr>
<tr><td>Prezenční vrstva</td></tr>
<tr><td>Relační vrstva</td></tr>
<tr><td>Transportní vrstva</td><td>Transportní vrstva</td></tr>
<tr><td>Síťová vrstva</td><td>Síťová vrstva</td></tr>
<tr><td rowspan="2">Vrstva síťového rozhraní</td><td>Linková vrstva</td></tr>
<tr><td>Fyzická vrstva</td></tr>
</table>

3.2 Switch

Switch je tzv. nástupce zařízení hub (česky rozbočovač) a také zařízení most. Hub fungoval na linkové vrstvě modelu TCP/IP a rozesílal všechny rámce na ostatní porty kromě příchozího. Switch je již „inteligentnější“ a odešle rámec ve většině případů pouze příjemci. Oproti hubu pracuje na internetové vrstvě modelu TCP/IP a pracuje s MAC adresami, díky kterým dokáže rozesílat rámce na správný port [9].

Aby switch dokázal vyhodnotit správný port, využívá CAM tabulku. Do této tabulky switch přidává porty a MAC adresy. Tím pádem při přijetí rámce si nejdříve zjistí jeho MAC adresu a odešle rámec na určitý port. Pokud nastane situace, že nemá záznam pro danou adresu,

odešle rámec na všechny porty, stejně jako to dělal hub. Zde je však odezva rychlá a přichází odpověď okamžitě [9].

Switche můžou mít různé rychlosti pro přeposílání rámců. Nejvíce se využívá cut-through, kdy odešle rámec hned, jakmile zjistí cílovou MAC adresu, resp. port. U tohoto typu se však nekontrolují chyby. Zato typ store-and-forward kontroluje celé rámce a uloží do vyrovnávací paměti a kontroluje jeho součet. Pokud je všechno v pořádku, tak rámec odešle a pokud se zjistí chyba, daný rámec zahodí [9].

Existuje spousta útoků na tento prvek, mezi hlavní patří zahlcení switche různými MAC adresami. Tento útok se nazývá MAC flooding a v podstatě udělá ze switche hub, který rozesílá rámce na všechny porty [9].

Obr. 4 Názorný obrázek Switch TP-Link T2600G-28TS [7].

3.3 Firewall

Úloha firewallu je oddělování trafiku mezi sítí LAN a internetem. Jedná se o tzv. bezpečnostní bránu zkoumající data oběma směry podle jasně daných pravidel, které si uživatel nastaví, popř. jsou již nastaveny výrobcem. Snaha firewallu je zamezit či alespoň snížit riziko prolomení sítě, blokování nevyžádaných dotazů a škodlivých kódů. V domácích sítích či malých firmách je často využit pouze desktopový firewall spolu s antivirovým programem. Zde je však nutné mít správně nastavený jak antivirus, tak firewall [11].

Pro větší prostředí je velmi dobrá kombinace desktopového firewallu a směrovače DSL neboli hardwarového firewallu. Oba typy se doplňují a zkvalitňují služby. Pro desktopový firewall je podstatné zvolit takový software, který je vyladěn a neobsahuje chyby. Dále musí být dobře nakonfigurován, musí zvládnout kontrolu sama sebe a aktualizovat se pravidelně na poslední verzi daného softwaru. Pro směrovač platí, aby se ihned po zapojení změnilo defaultní heslo, proběhlo zakázání Plug and Play a rovněž aktualizace na poslední verzi

firmwaru ihned, jak to bude možné. Výhoda směrovače spočívá v tom, že se jedná o samostatnou jednotku a útoků na něj je podstatně méně než u desktopové verze [11].

V zásadě každý firewall funguje jako filtr pro pakety a zkoumá tok dat u určitých IP adres. Zde si systémový administrátor určí, která data přes firewall projdou a která nikoli. Stačí zde malá chyba při nastavení, či objevení díry v systému a celá práce je svým způsobem ztracena, jelikož útočníkům stačí málo k tomu, aby se dostali do lokální sítě. Firewall se stále trénuje a učí, při instalaci nových programů bude vždy nutné rozhodnout, zda budou mít přístup do sítě [11].

3.3.1 Typy firewallu

Zde se jedná o čtyři základní typy:

1. **paketové filtry** – jedná se o první způsob, kdy se kontrola paketů provádí na síťové a transportní vrstvě modelu OSI. Zde se kontroluje, zda může být přeposlán paket mezi dvěma danými adresami a porty. Využívá se Access Control List, JunOS či ipchains, který byl implementován v linuxovém jádře,
    - **výhody –** vysoká rychlost, tento typ se stále využívá v místech, kde není nutná velká kontrola paketů a přeposílá se velké množství dat,
    - **nevýhody –** u modernějších protokolů je nutné otevírat i další porty pro spojení, která následně mohou být využita jinými protokoly, které nebyly prvotně plánované čili slabá úroveň kontroly spojení [13].
2. **Aplikační brány** – Proxy firewally nebo také aplikační brány oddělují sítě. Název aplikační brána je odvozena ze způsobu kontroly. Ta totiž probíhá na sedmé vrstvě modelu OSI. Zde se navazují dvě spojení, nejdříve se klient připojí na Proxy firewall, který zpracuje a vytvoří nové spojení k serveru, kde klientem je Proxy firewall. Data se zase v předchozím spojení předají klientovi. Využíval se The firewall Toolkit (zkráceně fwtk) a TIS:
    - **výhody** – benefitem oproti paketovým filtrům je především ochrana známých protokolů,
    - **nevýhody –** mezi nevýhody patří vysoké požadavky na hardware a zpracování kontroly je mnohem pomalejší. Dále je zde omezen počet spojení pro zpracování [13].

3. **Stavové paketové filtry** – zde se jedná o modernější způsob paketových filtrů, kdy se do paměti ukládají informace o již dříve povolených spojeních. Díky této funkci dokáží dříve rozhodnout, jestli pakety mohou být povoleny nebo se musí opakovat proces kontroly. Do této skupiny firewallů patří Cisco IOS Firewall, Check Point, ale pouze do verze 4.0, a také starší forma Cisco PIX:
    - **výhody** – jak již z předchozího textu vyplývá, díky ukládání povolených spojení se zrychluje zpracování paketů. Vyšší úroveň zabezpečení než u původních paketových filtrů a lehká konfigurace, která minimalizuje riziko špatného nastavení,
    - **nevýhody** – neposkytuje takovou úroveň zabezpečení jako Proxy firewall [13].
4. **Stavové paketové filtry s kontrolou protokolů a IDS** – oproti předchozí verzi zvládnou kontrolovat spojení až na úroveň aplikací a známých protokolů. Například pokud se nejedná o požadavek www serveru, ale tunelování druhého protokolu, dokáže zamezit tok http spojení. Dále se využívá systém pro detekci útoků, anglická zkratka zní IDS. Velmi výrazně se podobá antiviru. Heuristické analýzy dokáží odhalit vzorce útoků. Do této skupiny spadá ISG, SSG a Check Point FireWall-1, ale již od novější verze 4.1:
    - **výhody** – poskytuje vyšší úroveň bezpečnosti. Oproti proxy firewallu poskytuje vyšší rychlost kontrol,
    - **nevýhody** – jedná se o zpomalení oproti běžným stavovým paketovým filtrům. Jelikož obsahuje velké množství funkcí, zvyšuje šance na zneužití chyb v kódu [13].

Obr. 5 Názorný obrázek Firewallu Zyxel NSG200 [12].

3.4 Router

Router pracuje zejména na síťové vrstvě modelu OSI, ale využívá také linkovou a fyzickou vrstvu. Koncový router, který odděluje lokální síť LAN od internetu WAN se nazývá brána. Tento router slouží ke komunikaci s jinou IP adresou mimo lokální síť. Ke komunikaci router využívá směrování neboli routování. Zde si router vytvoří routovací tabulku, ve které jsou zaznamenány cesty. U jednoduchých sítí postačí statické routování, tzn., že jsou data do tabulky zadávány ručně. Dále je defaultní routování, kdy není známa cesta do patřičné sítě [8].

U složitějších sítí by tento způsob byl velmi pracný, proto byl vynalezen způsob zvaný dynamické routování. Zmíněná funkce dokáže reagovat na změnu topologie v síti, ale je zde nutné využít routovací protokoly. Mezi nejvyužívanější protokoly patří RIP anglicky Routing Information Protocol nebo OSPF anglicky Open Shortest Path First [8].

Obr. 6 Názorný obrázek TP-LINK TL-R480T+ [10].

II. PRAKTICKÁ ČÁST

4 APLIKACE FORMÁLNÍ KONCEPTÁLNÍ ANALÝZY

Pro aplikaci formální konceptuální analýzy lze využít řadu programů. Mezi nejznámější patří Anaconda, Diagram, Toscana, ConImp a Concept Explorer (dále ConExp), který již byl aplikován v bakalářské práci. Tento program byl vybrán z důvodu intuitivního ovládání.

4.1 Program Concept Explorer

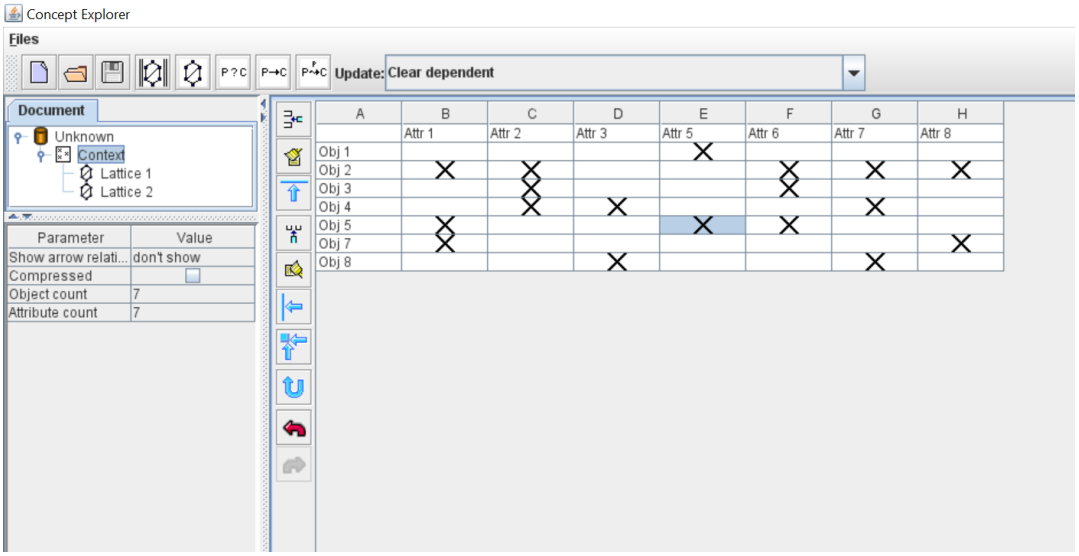
Jako hlavní vývojář a autor programu je Dr. rer. nat. Serhiy Yevtushenko, který s pomocí vedoucího prof. Dr. Tatyana Taran vyvinuli tento program jako součást diplomové práce. Nyní je program open source a je dostupný na Sourceforge, kde je možnost jeho stáhnutí zcela zdarma.

Mezi jeho hlavní nástroje patří:

- kontextové úpravy,
- vykonání atributního vyšetření,
- vytvoření konceptuálního svazu,
- objevení asociačních pravidel platných v kontextu.

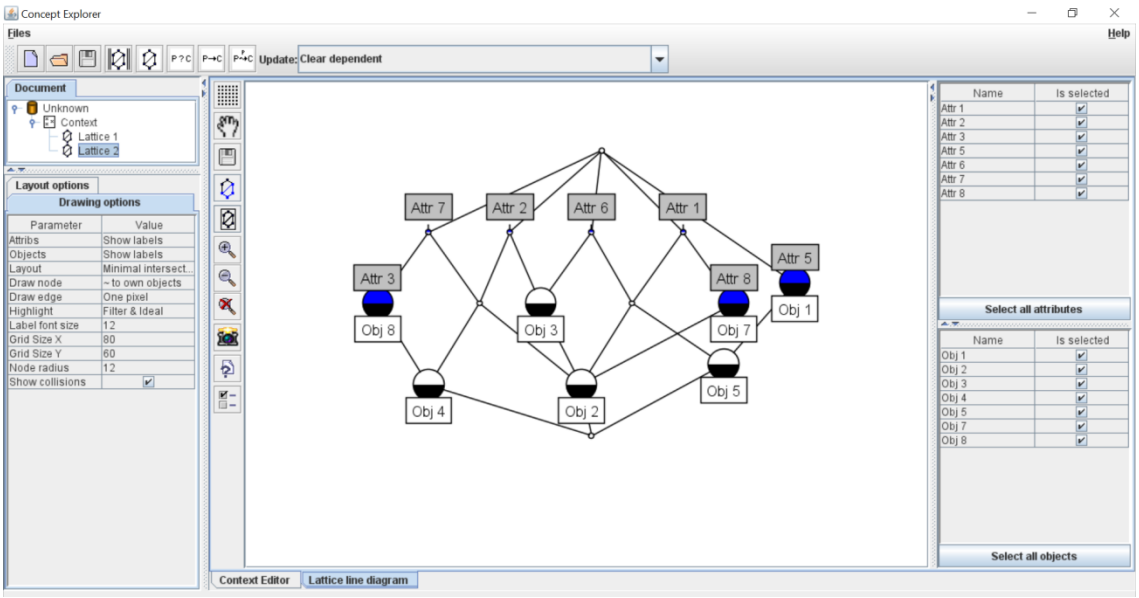
4.1.1 Ovládání programu

Po otevření programu lze vidět následující obrázek (Obr. 7). V horní liště programu figurují podstatná tlačítka jako vytvoření nového dokumentu, načtení, uložení, spočítání konceptů, vytvoření konceptuálního svazu, provedení atributního průzkumu, vypočítání důsledků a vypočítání asociačních pravidel. V levé části lze vidět řetězení objektu, parametry a hodnotu. Zde lze vyčíst například, kolik je objektů a atributů v dokumentu. V hlavní pracovní části programu je tabulka, ve které se dvojím kliknutím vytvoří křížek, což značí, že označený objekt má daný atribut. Křížky a prázdná políčka nahrazují binární hodnoty jedna a nula. Názvy objektů a atributů lze dvojím kliknutím přejmenovat na odpovídající název. Je zde několik dalších tlačítek, která přidávají a ubírají pole pro objekt, rovněž tak platí stejný prostup u atributů. Dále lze využít tlačítko zpět, popř. vrátit předchozí akci.



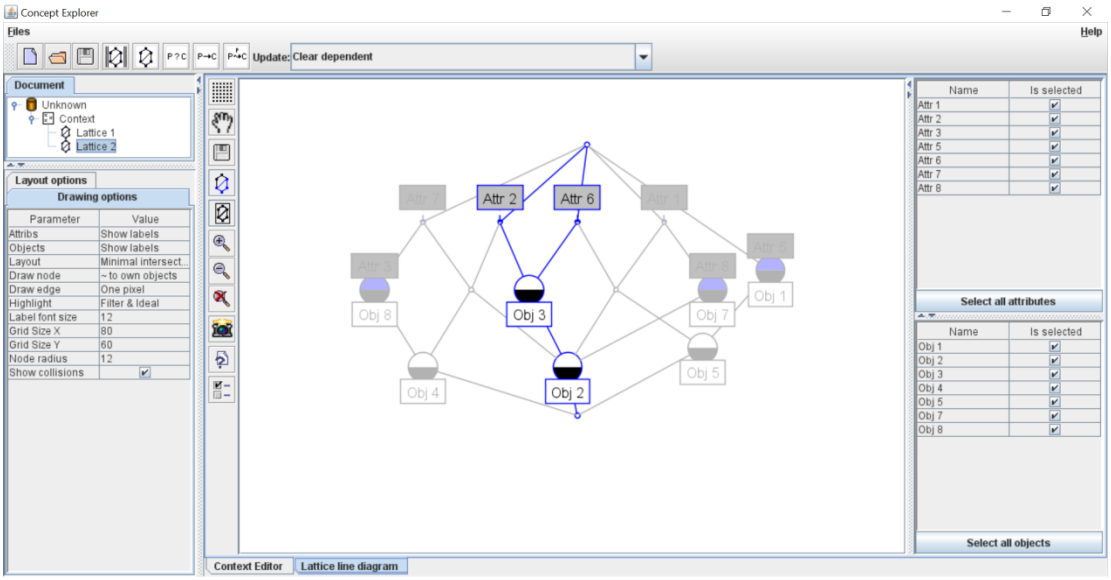
Obr. 7 Ukázka programu ConExp – kontextová tabulka [Vlastní zdroj].

Na základě vytvořené tabulky (Obr. 7) v programu ConExp lze vygenerovat konceptuální svaz, mezi tabulkou a vytvořeným konceptuálním svazem lze snadno přecházet pomocí záložek ve spodní části programu, což lze vidět na následujícím obrázku (Obr. 8).



Obr. 8 Ukázka programu ConExp – konceptuální svaz [Vlastní zdroj].

Konceptuální svaz v programu ConExp lze dále tvarovat a upravovat. V levé části programu může být nastavena viditelnost názvů atributů a objektů. Dále je možné konceptuální svaz tvarovat a popř. si vyjmout pouze část pro lepší orientaci, což lze vidět na dalším obrázku (Obr. 9).



Obr. 9 Ukázka programu ConExp – vyznačení pro lepší orientaci [Vlastní zdroj].

4.1.2 Orientace v konceptuálním svazu programu Concept Explorer

V předchozím obrázku (Obr. 9) lze vidět dva typy obdélníků a dva typy půlkruhů. Pro orientaci je nutné jejich objasnění:

1. Obdélníky
    - šedý obdélník – zobrazuje názvy atributů,
    - bílý obdélník – zobrazuje názvy objektů.
2. Půlkruhy
    - tmavě modrý půlkruh – vyobrazuje spojení s atributem,
    - černý půlkruh – vyobrazuje spojení s objektem.

5 VYBRANÉ SÍŤOVÉ PRVKY

Existuje velká škála síťových prvků, a aby daná analýza byla relevantní, bude nezbytné se zaměřit na určitou třídu. Praktická část diplomové práce bude zaměřena na síťové prvky pro domácí sítě, malé a středně velké podniky. Pokud by se analýza zaměřila na produkty směřované pro velké organizace, neměla by příliš velkou vypovídající hodnotu.

5.1 Analýza pro vybrané Switche

Jak již bylo řečeno, práce bude zaměřena na IT strukturu pro domácí sítě, malé a středně velké podniky. Z toho důvodu nebudou v analýze zohledněny switche do racku, ale pouze stolní.

5.1.1 Zvolené atributy

Mezi atributy bylo vybráno devět nejpodstatnějších funkcí, které mohou switche obsahovat:

- podporované rychlosti,
- počet portů,
- přepínací kapacita,
- materiál konstrukce,
- management,
- Power of Ethernet,
- Quality of Service,
- VLAN,
- Buffer,
- cena [21, 22].

5.1.1.1 Podporované rychlosti

V komunikaci hraje rychlost klíčovou roli. Pro výběr je nutno zvážit, jakou síť domácnost či firma využívá. Pokud by se jednalo o moderní vysokorychlostní síť s rychlostí až 1 Gb/s, mohly by některé typy switchů rychlost snižovat. Je možné vybrat mezi dvěma podporovanými rychlostmi:

- 10/100 Mbit/s u starších switchů,

- 10/100/1000 Mbit/s u modernějších switchů [21, 22].

5.1.1.2 Počet portů

Hlavním atributem byl zvolen počet portů, který se ale dále dělí na porty pro kabely RJ-45, jenž je v domácnosti nejběžnější, jsou jím propojovány notebooky, počítače, tiskárny atd. Jako další port je možné nalézt Small Form-factor pluggable (dále jen SFP), který slouží pro propojování sítí pomocí optických kabelů. V neposlední řadě je nutné zmínit Dual Personality, do češtiny je možné jej přeložit jako dvojitý konektor. Zde je možné zvolit, zda chce uživatel využít optický kabel, resp. RJ-45 [21, 22].

Uživatel si musí vybrat, pro jaký účel bude dané zařízení využívat, jelikož velké množství portů přináší další možnosti, ale také vyšší náklady na spotřebu elektrické energie. Počet portů u switche začíná u čísla pět [21, 22].

5.1.1.3 Přepínací kapacita

Atribut, který rovněž souvisí s rychlostí komunikace. Jedná se o množství Gb přenesených za jednu vteřinu na všech portech v obou směrech. Díky této technologii je možné přenést velká data bez delší prodlevy. Přepínací kapacita závisí na počtu portů a přenosové rychlosti. Pokud má být schopna zajistit plné využití všech portů např. u switche, který jich vlastní osm, je nutné, aby zde byla přepínací kapacita minimálně 16 Gbps [21, 22].

5.1.1.4 Materiál konstrukce

Pro většinu zařízení, u kterých je šance, že se budou přehřívat, je nutné dbát na materiál konstrukce. V zapojení do racku je prakticky nemožné najít switch z plastového materiálu. Domácí sítě nemají takové nároky, ale rovněž se mohou přehřívat. Proto je dobré volit zařízení z odolných kovů, který se stará o tzv. pasivní chlazení. Naopak plast, který se využívá pro většinu levnějších provedení, hůře odvádí teplo [22].

5.1.1.5 Management

Následující atributy počínaje Managementem jsou funkce, které dokáží vytvořit zařízení se širokou škálou možností. Jedná se o manažerování neboli řízení switche pomocí uživatelského rozhraní, které se používá například pro prvopočáteční nastavení, síťové předpisy a řízení síťového provozu [21].

5.1.1.6 Power of Ethernet

Power of Ethernet (dále jen PoE) je speciální řešení. Tato funkce dokáže pomocí kabelu, jenž vede data, také napájet připojené zařízení. Jeho využití je především pro IP kamery, přídavné switche, VoIP telefony a přístupové stanice [21].

5.1.1.7 Quality of Service

Pomocí funkce Quality of Service (dále jen QoS) je možné nastavovat šířku pásma pro jednotlivá připojená zařízení. Nejvíce se tato funkce využívá proto, aby nedocházelo k přehlcení switche. Dále je možné měnit přenosové rychlosti pro určitá zařízení a v neposlední řadě jim určovat priority [21].

5.1.1.8 VLAN

Virtuální logicky nezávislá síť dále jen VLAN, je služba, která povoluje vytvářet oddělené sítě, díky nimž je možné zlepšit správu sítě, zesílit výkon a zdokonalit bezpečnost. Některá zařízení povolují i vytvoření několika VLAN zároveň [21].

5.1.1.9 Buffer

Switche pracují jako zařízení Cut-Through, což znamená, že přijatý rámec přeposílá, jakmile se dozví cílovou MAC adresu. Hodí se pro sítě, kde rozhoduje rychlost. Zařízení, které využívají buffer, se nazývají Store-and-Stare. Zde se přijme rámec a uloží do své paměti, resp. do bufferu. Provede kontrolní součet a pokud je vše v pořádku, přeposílá rámec dále [9].

5.1.1.10 Cena

Jelikož jsou vybrány produkty pro malé podniky a domácnosti, bude maximální cena do 5 000 Kč.

5.1.2 Zvolená zařízení

FCA bude provedena na šest switchů od společností TP-Link, D-Link, Edimax a ZyXEL.

5.1.2.1 D-Link DGS -1100-05

Jako první switch byl vybrán D-Link DGS-1100-05, který svou cenou patří do střední třídy.

Tab. 5. Atributy pro D-Link DGS-1100-05 [15].

Podporované rychlosti	10/100/1000 Mbps
Počet portů	5
Přepínací kapacita	10 Gb/s
Materiál konstrukce	Kov
Management	Ano
PoE	Ne
QoS	Ano
VLAN	Ano
Buffer	Ne
Cena	755 Kč

Obr 10. D-Link DGS-1100-05 [15].

5.1.2.2 Edimax ES-5808P

Edimax ES-5808P patří mezi nejdražší zařízení, které pro analýzu bylo vybráno.

Tab. 6 Atributy pro Edimax ES-5808P [16].

Podporované rychlosti	10/100 Mbps
Počet portů	8
Přepínací kapacita	16 Gb/s
Materiál konstrukce	Kov
Management	Ano
PoE	Ano
QoS	Ano
VLAN	Ano
Buffer	Ano
Cena	4 139 Kč

Obr. 11 Edimax ES-5808P [16].

5.1.2.3 TP-LINK TL-SG108E

Třetí zařízení vyvíjí firma TP-Link a jedná se o model TL-SG108E.

Tab. 7 Atributy pro TP-LINK TL-SG108E [17].

Podporované rychlosti	10/100/1000 Mbps
Počet portů	8
Přepínací kapacita	8 Gb/s
Materiál konstrukce	Kov
Management	Ano
PoE	Ne
QoS	Ano
VLAN	Ano
Buffer	Ne
Cena	879 Kč

Obr. 12 TP-LINK TL-SG108E [17].

5.1.2.4 D-Link DES-108/E

Dále je zde znovu model od společnosti D-Link s modelem DES-108/E, který spadá do nejlevnější cenové kategorie.

Tab. 8 Atributy pro D-Link DES-108/E [18].

Podporované rychlosti	10/100 Mbps
Počet portů	8
Přepínací kapacita	1,6 Gb/s
Materiál konstrukce	Kov
Management	Ne
PoE	Ne
QoS	Ano
VLAN	Ne
Buffer	Ne
Cena	429 Kč

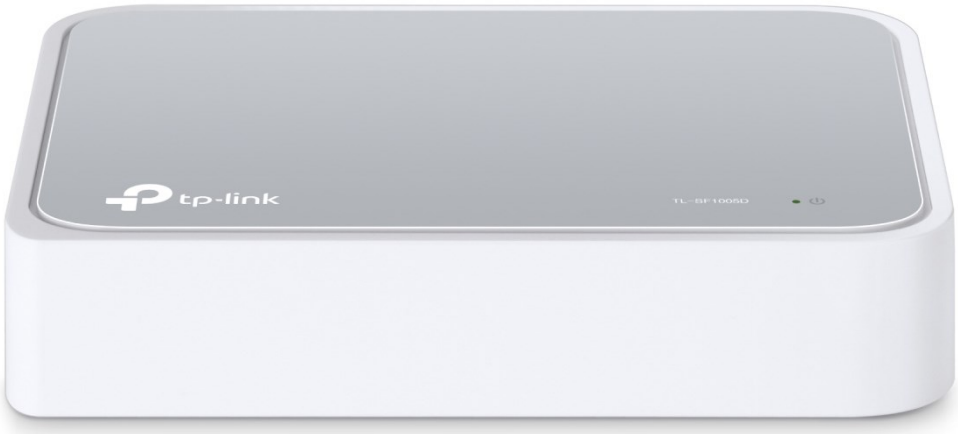
Obr. 13 D-Link DES-108/E [18].

5.1.2.5 TP-Link TL-SF1005D

Opět se zde nachází zařízení od společnosti TP-Link s modelem TL-SF10005D.

Tab. 9 Atributy pro TP-Link TL-SF1005D [19].

Podporované rychlosti	10/100 Mbps
Počet portů	5
Přepínací kapacita	1 Gb/s
Materiál konstrukce	Plast
Management	Ne
PoE	Ne
QoS	Ne
VLAN	Ne
Buffer	Ne
Cena	229 Kč



Obr. 14 TP-Link TL-SF1005D [19].

5.1.2.6 ZyXEL ES-108A v3

Jako poslední bylo vybráno zařízení od společnosti ZyXEL s modelem ES-108A v3.

Tab. 10 Atributy pro ZyXEL ES-106A v3 [20].

Podporované rychlosti	10/100 Mbps
Počet portů	8
Přepínací kapacita	1,6 Gb/s
Materiál konstrukce	Kov
Management	Ne
PoE	Ne
QoS	Ano
VLAN	Ne
Buffer	Ne
Cena	419 Kč

Obr. 15 ZyXEL ES-106A v3 [20].

5.1.3 Výstup programu ConExp pro switche

V následující tabulce (Tab. 11) je sjednocení všech vybraných modelů.

Tab. 11 Sjednocení vybraných modelů [Vlastní zdroj].

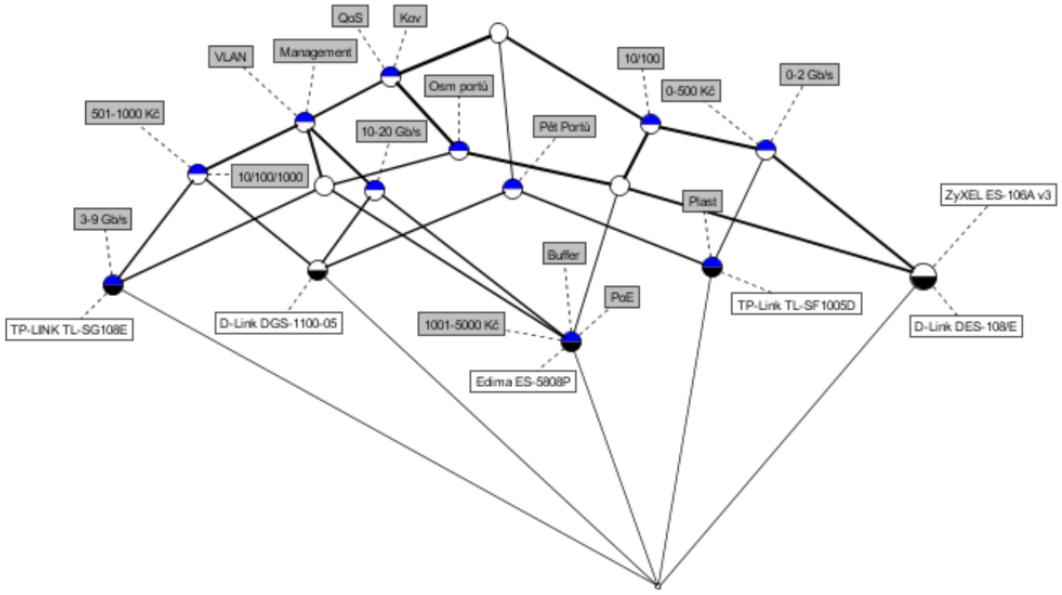
Vybrané switche	Podporované rychlosti	Počet portů	Přepínací kapacita	Materiál konstrukce	Management	Power of Ethernet	Quality of service	VLAN	Buffer	Cena
D-Link DGS-1100-05	10/100/1000	5	10	Kov	Ano	Ne	Ano	Ano	Ne	755
Edimax ES-5808P	10/100	8	16	Kov	Ano	Ano	Ano	Ano	Ano	4 139
TP-LINK TL-SG108E	10/100/1000	8	8	Kov	Ano	Ne	Ano	Ano	Ne	879
D-Link DES-108/E	10/100	8	1,6	Kov	Ne	Ne	Ano	Ne	Ne	429
TP-Link TL-SF1005D	10/100	5	1	Plast	Ne	Ne	Ne	Ne	Ne	229
ZyXEL ES-106A v3	10/100	8	1,6	Kov	Ne	Ne	Ano	Ne	Ne	419

S předchozí tabulkou (Tab. 11) není možné momentálně pracovat, proto bude nutné provést konceptuální škálování, které převede hodnoty na 1 a 0.

Tab. 12 Konceptuální škálování – switche [Vlastní zdroj].

Vybrané switche	Rychlost 10/100/1000	Rychlost 10/100	Pět portů	Osm portů	Kapacita 0-2 Gb/s	Kapacita 3-9 Gb/s	Kapacita 10-20 Gb/s	Plast	Kov	Management	Power of Ethernet	Quality of service	VLAN	Buffer	Cena 0-500 Kč	Cena 501-1000 Kč	Cena 1001-5000 Kč
D-Link DGS-1100-05	1	0	1	0	0	0	1	0	1	1	0	1	1	0	0	1	0
Edimax ES-5808P	0	1	0	1	0	0	1	0	1	1	1	1	1	1	0	0	1
TP-LINK TL-SG108E	1	0	0	1	0	1	0	0	1	1	0	1	1	0	0	1	0
D-Link DES-108/E	0	1	0	1	1	0	0	0	1	0	0	1	0	0	1	0	0
TP-Link TL-SF1005D	0	1	1	0	1	0	0	1	0	0	0	0	0	0	1	0	0
ZyXEL ES-106A v3	0	1	0	1	1	0	0	0	1	0	0	1	0	0	1	0	0

S výslednou tabulkou po konceptuálním škálováním nic nebrání tomu ji přepsat do programu ConExp.



Obr. 16 Konceptuální svaz – switche [Vlastní zdroj].

Pro atributové implikace je možné využít výpočet důsledků v programu ConExp, dále je možné vidět propracovanější souvislosti.

```
1 < 2 > 10/100/1000 ==> Kov Management QoS VLAN 501-1000 Kč;
2 < 1 > 10/100 Pět Portů ==> 0-2 Gb/s Plast 0-500 Kč;
3 < 4 > Osm portů ==> Kov QoS;
4 < 3 > 0-2 Gb/s ==> 10/100 0-500 Kč;
5 < 1 > 3-9 Gb/s ==> 10/100/1000 Osm portů Kov Management QoS VLAN 501-1000 Kč;
6 < 2 > 10-20 Gb/s ==> Kov Management QoS VLAN;
7 < 1 > Plast ==> 10/100 Pět Portů 0-2 Gb/s 0-500 Kč;
8 < 5 > Kov ==> QoS;
9 < 3 > Management ==> Kov QoS VLAN;
10 < 5 > QoS ==> Kov;
11 < 1 > Pět Portů Kov QoS ==> 10/100/1000 10-20 Gb/s Management VLAN 501-1000 Kč;
12 < 3 > 10/100 Kov QoS ==> Osm portů;
13 < 3 > VLAN ==> Kov Management QoS;
14 < 3 > 0-500 Kč ==> 10/100 0-2 Gb/s;
15 < 2 > 501-1000 Kč ==> 10/100/1000 Kov Management QoS VLAN;
16 < 1 > 10/100/1000 10-20 Gb/s Kov Management QoS VLAN 501-1000 Kč ==> Pět Portů;
17 < 1 > 10/100/1000 Osm portů Kov Management QoS VLAN 501-1000 Kč ==> 3-9 Gb/s;
18 < 1 > 1001-5000 Kč ==> 10/100 Osm portů 10-20 Gb/s Kov Management PoE QoS VLAN Buffer;
19 < 1 > PoE ==> 10/100 Osm portů 10-20 Gb/s Kov Management QoS VLAN Buffer 1001-5000 Kč;
20 < 1 > Osm portů 10-20 Gb/s Kov Management QoS VLAN ==> 10/100 PoE Buffer 1001-5000 Kč;
21 < 1 > 10/100 Osm portů Kov Management QoS VLAN ==> 10-20 Gb/s PoE Buffer 1001-5000 Kč;
22 < 1 > Buffer ==> 10/100 Osm portů 10-20 Gb/s Kov Management PoE QoS VLAN 1001-5000 Kč;
23 < 0 > 10/100 Osm portů 0-2 Gb/s 10-20 Gb/s Kov Management PoE QoS VLAN Buffer 0-500 Kč 1001-5000 Kč ==> 10/100/1000 Pět Portů 3-9 Gb/s Plast 501-1000 Kč;
```

Obr. 17 Atributové implikace – switche [Vlastní zdroj].

5.2 Analýza pro vybrané firewally

V teoretické části byly popsány typy firewallu. Pro analýzu však byly vybrány pouze Next-generation firewalls (anglická zkratka NGFW). Zmíněný termín lze přeložit jako firewally nové generace.

5.2.1 Zvolené atributy

Atributy pro daný prvek byly vybrány ty nejpodstatnější, které by firewally nové generace měly obsahovat:

- antivirus a antispyware funkce,
- IDPS,
- Sandboxing,
- prevence úniku dat,
- ochrana proti botům,
- DDoS ochrana,
- dvoufaktorové ověření,
- cena.

5.2.1.1 Antivirus a antispyware funkce

Antivirus slouží pro detekování a odstraňování škodlivých softwarů, které mají za úkol poškodit či narušit dané zařízení. Antispyware se rovněž snaží hledat a odstraňovat infikované soubory, nicméně význam spywaru je odposlouchávání, sbírání a poskytování informací třetí straně [23].

5.2.1.2 IDPS

Jedná se o jedny z nejdůležitějších funkcí u firewallů. Zkratka IDS vychází z anglického sousloví Intrusion Detection Systems neboli systém pro detekci narušení. Jak již z názvu vyplývá, jedná se o pasivní systém, který detekuje napadení a posílá upozornění uživateli [24].

Na druhé straně zkratka IPS je odvozením od Intrusion Prevention Systems, v překladu systém prevence narušení. Zde se jedná o aktivní prvek, který má za úkol při detekci narušení zablokovat či resetovat spojení s podezřelým škodlivým zdrojem [24].

Novější normy již uvádí spojení zmíněných funkcí jako systém detekce a prevence narušení. Anglický název vyplynul ze spojení Intrusion Detection Prevention Systems a zkratkou je IDSP [24].

5.2.1.3 Sandboxing

Zmíněná anglická technika vychází ze slova Sandbox neboli pískoviště. Pomocí Sandboxingu se vytvoří testovací prostředí, které je absolutně oddělené od produkce a provádí se zde testování nedůvěryhodných e-mailů, souborů či webových odkazů. Pokud by se v testovacím prostředí zjistilo, že daný e-mail, soubor nebo odkaz obsahoval vir či spyware, testovací prostředí by se smazalo a obsah přijatého škodlivého softwaru by nezpůsobil žádné škody. Někdy je zmíněná technika označována jako detonace neboli odpálení škodlivého souboru [25].

5.2.1.4 Prevence úniku dat

Jedná se o neoprávněný přenos dat z podniku k externímu příjemci. Stejný termín se využívá pro přenos jak fyzický, tak elektronický. U firewallu se jedná o elektronický přenos zejména prostřednictvím webu a e-mailu. Při úniku dat může dojít k poklesu příjmů či ztrátě důvěry u zákazníků [26].

Pomocí zmíněné funkce dokáží administrátoři nastavit interní pravidla, díky kterým nemohou koncoví uživatelé neoprávněně zveřejňovat citlivé informace [26].

5.2.1.5 Ochrana proti botům

Pojem bot je odvozením od slova robot. Jedná se o počítačový program, který má za úkol opakovaně dělat běžné činnosti na internetu, především ve webových aplikacích. Na počátku této technologie hackeři využívali pouze jednoduché skripty, které se vyvinuly na složitější programy, jenž využívají například strojové učení [27].

Pro ochranu se využívá detekce spamu a blokování spamu, díky kterým je možné uchovávat čisté prostředí v komentářích či analytických datech. Dále sleduje příchozí požadavky, zda se nejedná o podezřelou aktivitu a tím detekuje potencionální útoky [27].

5.2.1.6 DDoS ochrana

Útoky Denial of Service, které jsou více známé jen pod zkratkou DoS, česky odepření služby, se využívají pro její zahlcení. Útočníkův cíl není získat kontrolu nad danou službou, ale úmysl je její poškození. Do této kategorie spadá útok DDoS neboli Distributed of Service (do češtiny přeloženo jako distribuované odmítnutí služby). Zde se jedná o využití několika nakažených počítačů, které zasílají požadavky na konkrétní službu [28].

Při vyřazení služby z provozu ztrácí firmy velké množství výdělku, pokud se jedná například o elektronický obchod či odchod potencionálních zákazníků ke konkurenci. Odhaduje se, že i menší firmy může útok stát téměř 3 miliony Kč. Objednání útoku na Dark webu stojí kolem 2000 Kč, proto o tomto řešení může uvažovat největší konkurent dané společnosti a tyto útoky rozhodně není moudré podceňovat [28].

5.2.1.7 Dvoufaktorové ověření

Dvoufaktorové ověření, někdy se také označuje jako dvoufaktorová autentizace, slouží ke zvýšení úrovně zabezpečení. Na první úrovni lze vidět pouze uživatelské jméno a heslo. Pokud se bude jednat o slabé heslo, popř. nebude splňovat všechny doporučené kombinace, je velká šance, že útočníci tuto úroveň prolomí například slovníkovou metodou. Druhá úroveň již nabízí k uživatelskému jménu a heslu také ověření pomocí tokenu či mobilního zařízení. Pokud během pověření proběhne všechno v pořádku, firewall změní politiku a povolí přístup uživateli k dané službě [29].

5.2.1.8 Cena

Zvolené programy mají rozdílné fakturování. Některé se platí ročně a jiné zase měsíčně. Z tohoto byly ceny převedeny na roční zúčtování a vždy se jedná pouze o jedno zařízení.

5.2.2 Zvolené programy

FCA bude provedena pro následující firewally nové generace.

5.2.2.1 Cato Networks

Prvním vybraným objektem se stal produkt Cato Network.

Tab. 13 Atributy pro Cato Network [30].

Antivirus a antispyware funkce	Ano
IDPS	Ano
Sandboxing	Ne
Prevence úniku dat	Ne
Ochrana proti botům	Ne
DDoS ochrana	Ne
Dvoufaktorové ověření	Ano
Cena	26 Kč

Obr. 18 Logo společnosti Cato Networks [30].

5.2.2.2 Barracuda NextGen Firewall

Nejdražším zvoleným objektem se stal Barracuda NextGen Firewall.

Tab. 14 Atributy pro Barracuda NextGen Firewall [31].

Antivirus a antispyware funkce	Ano
IDPS	Ano
Sandboxing	Ano
Prevence úniku dat	Ne
Ochrana proti botům	Ano
DDoS ochrana	Ano
Dvoufaktorové ověření	Ne
Cena	806 Kč

Obr. 19 Logo společnosti Barracuda [31].

5.2.2.3 Zscaler Firewall

V podobné cenové relaci se pohybuje také Zscaler Firewall.

Tab. 15 Atributy pro Zscaler Firewall [32]

Antivirus a antispyware funkce	Ano
IDPS	Ne
Sandboxing	Ano
Prevence úniku dat	Ano
Ochrana proti botům	Ne
DDoS ochrana	Ne
Dvoufaktorové ověření	Ne
Cena	728 Kč

Obr. 20 Logo společnosti Zscaler [32].

5.2.2.4 Forcepoint NGFW

Čtvrtým objektem byl zvolen Forcepoint NGFW.

Tab. 16 Atributy pro Forcepoint NGFW [33].

Antivirus a antispyware funkce	Ano
IDPS	Ano
Sandboxing	Ano
Prevence úniku dat	Ano
Ochrana proti botům	Ano
DDoS ochrana	Ano
Dvoufaktorové ověření	Ano
Cena	624 Kč

Obr. 21 Logo společnosti Forcepoint [33].

5.2.2.5 Cyberoam Next Generation Firewall

Mezi nejlevnější vybrané objekty patří následující Cyberoam Next Generation Firewall.

Tab. 17 Atributy pro Cyberoam Next Generation Firewall [34].

Antivirus a antispyware funkce	Ano
IDPS	Ano
Sandboxing	Ne
Prevence úniku dat	Ano
Ochrana proti botům	Ne
DDoS ochrana	Ano
Dvoufaktorové ověření	Ano
Cena	37 Kč

Obr. 22 Logo společnosti Cyberoam [34].

5.2.2.6 Sophos Next-Generation Firewall

Posledním vybraným objektem se stal Sophos Next-Generation Firewall.

Tab. 18 Atributy pro Sophos Next-Generation Firewall [35].

Antivirus a antispyware funkce	Ano
IDPS	Ano
Sandboxing	Ano
Prevence úniku dat	Ano
Ochrana proti botům	Ano
DDoS ochrana	Ne
Dvoufaktorové ověření	Ano
Cena	182 Kč

Obr. 23 Logo společnosti Sophos [35].

5.2.3 Výstup programu ConExp pro Firewally

V následující tabulce (Tab. 19) je sjednocení všech vybraných modelů.

Tab. 19 Sjednocení vybraných modelů [Vlastní zdroj].

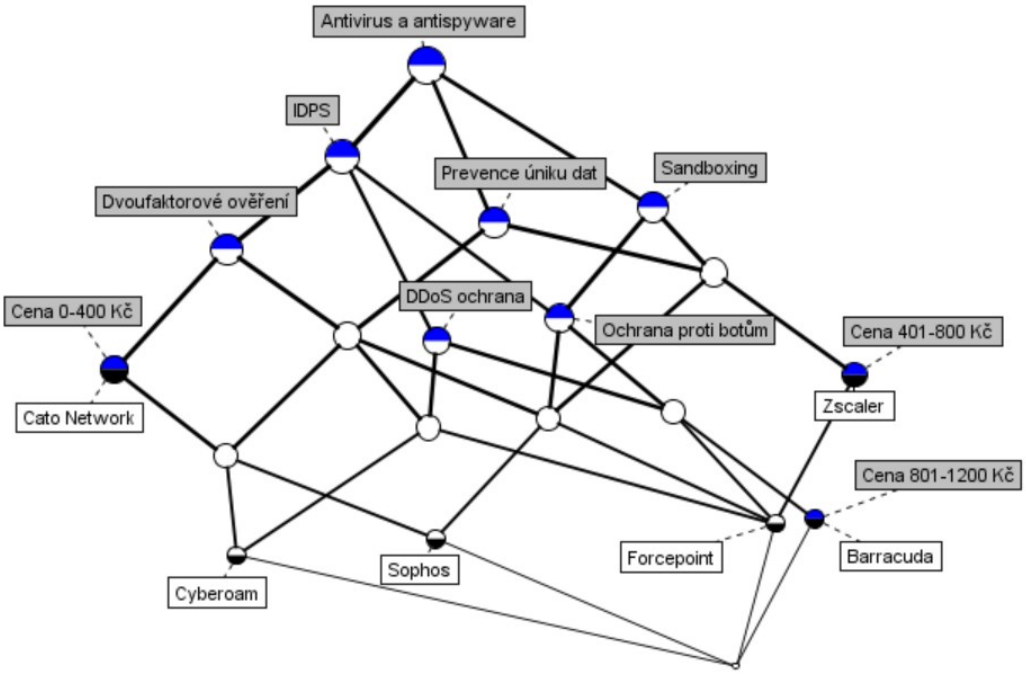
Vybrané Firewally	Antivirus a antispyware	IDPS	Sandboxing	Prevence úniku dat	Ochrana proti botům	DDoS ochrana	Dvoufaktorové ověření	Cena
Cato Network	Ano	Ano	Ne	Ne	Ne	Ne	Ano	26 Kč
Barracuda	Ano	Ano	Ano	Ne	Ano	Ano	Ne	806 Kč
Zscaler	Ano	Ne	Ano	Ano	Ne	Ne	Ne	728 Kč
Forcepoint	Ano	Ano	Ano	Ano	Ano	Ano	Ano	624 Kč
Cyberoam	Ano	Ano	Ne	Ano	Ne	Ano	Ano	37 Kč
Sophos	Ano	Ano	Ano	Ano	Ano	Ne	Ano	182 Kč

S předchozí tabulkou (Tab. 19) není možné momentálně pracovat, proto bude nutné provést konceptuální škálování, které převede hodnoty na 1 a 0.

Tab. 20 Konceptuální škálování – firewally [Vlastní zdroj].

Vybrané Firewally	Antivirus a antispyware	IDPS	Sandboxing	Prevence úniku dat	Ochrana proti botům	DDoS ochrana	Dvoufaktorové ověření	Cena 0-400 Kč	Cena 401-800 Kč	Cena 0-1200 Kč
Cato Network	1	1	0	0	0	0	1	1	0	0
Barracuda	1	1	1	0	1	1	0	0	0	1
Zscaler	1	0	1	1	0	0	0	0	1	0
Forcepoint	1	1	1	1	1	1	1	0	1	0
Cyberoam	1	1	0	1	0	1	1	1	0	0
Sophos	1	1	1	1	1	0	1	1	0	0

S výslednou tabulkou po konceptuálním škálováním nic nebrání tomu ji přepsat do programu ConExp.



Obr. 24 Konceptuální svaz – firewally [Vlastní zdroj].

Pro atributové implikace je možné využít výpočet důsledků v programu ConExp, dále je možné vidět propracovanější souvislosti.

```
1 < 6 > { } ==> Antivirus a antispyware;
2 < 3 > Antivirus a antispyware IDPS Sandboxing ==> Ochrana proti botům;
3 < 3 > Antivirus a antispyware IDPS Prevence úniku dat ==> Dvoufaktorové ověření;
4 < 3 > Antivirus a antispyware Ochrana proti botům ==> IDPS Sandboxing;
5 < 3 > Antivirus a antispyware DDoS ochrana ==> IDPS;
6 < 4 > Antivirus a antispyware Dvoufaktorové ověření ==> IDPS;
7 < 2 > Antivirus a antispyware IDPS Sandboxing Ochrana proti botům Dvoufaktorové ověření ==> Prevence úniku dat;
8 < 2 > Antivirus a antispyware IDPS DDoS ochrana Dvoufaktorové ověření ==> Prevence úniku dat;
9 < 1 > Antivirus a antispyware IDPS Sandboxing Prevence úniku dat Ochrana proti botům DDoS ochrana Dvoufaktorové ověření ==> Cena 401-800 Kč;
10 < 3 > Antivirus a antispyware Cena 0-400 Kč ==> IDPS Dvoufaktorové ověření;
11 < 2 > Antivirus a antispyware Cena 401-800 Kč ==> Sandboxing Prevence úniku dat;
12 < 1 > Antivirus a antispyware IDPS Sandboxing Prevence úniku dat Ochrana proti botům Dvoufaktorové ověření Cena 401-800 Kč ==> DDoS ochrana;
13 < 1 > Antivirus a antispyware Cena 801-1200 Kč ==> IDPS Sandboxing Ochrana proti botům DDoS ochrana;
14 < 0 > Antivirus a antispyware IDPS Sandboxing Prevence úniku dat Ochrana proti botům DDoS ochrana Dvoufaktorové ověření Cena 401-800 Kč Cena 801-1200 Kč ==> Cena 0-
400 Kč;
15 < 0 > Antivirus a antispyware IDPS Sandboxing Prevence úniku dat Ochrana proti botům DDoS ochrana Dvoufaktorové ověření Cena 0-400 Kč Cena 401-800 Kč ==> Cena 801-
1200 Kč;
```

Obr. 25 Atributové implikace – firewally [Vlastní zdroj].

5.3 Analýza pro vybrané routery

Routery obsahují velkou škálu vlastností, které je nutné zohlednit při koupi do podniku či domácnosti.

5.3.1 Zvolené atributy

Mezi atributy bylo vybráno 14 podstatných vlastností, které mohou routery obsahovat:

- Wi-Fi standardy,
- pracovní frekvence,
- USB,
- LTE,
- rychlost přenosu (RJ45 port),
- rychlost přenosu,
- Firewall
- Print server,
- File server,
- VPN,
- QoS,
- Podpora IPv6,
- Multimediální server,
- Cloud.

5.3.1.1 Wi-Fi standardy

Wi-Fi standardy slouží především pro zrychlení, propustnost a dosah Wi-Fi sítí. Společnost Wi-Fi Alliance, která vlastní tuto obchodní značku, se zabývá certifikací IEEE 802.11. Následující tabulka (Tab. 21) poukazuje na detailnější rozdíly mezi standardy [36].

Tab. 21 IEEE Standardy [36].

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Datum vydání	1999	1999	2003	2009	2014
Frekvence	5 Ghz	2.4 Ghz	2.4 Ghz	2.4 Ghz & 5 Ghz	2.4 Ghz & 5 Ghz
Maximální rychlost	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1.3 Gbps

Ve výše zmíněné tabulce (Tab. 21) nefiguruje nejnovější IEEE standard 802.11ax, který byl vydán v roce 2019 s pásmem 2.4 Ghz & 5 Ghz a s maximální rychlostí až 12 Gbps. Standard 802.11ax nefiguruje v žádném vybraném routeru pro FKA [37].

5.3.1.2 Pracovní frekvence

Pro standardy 802.11n a 802.11ac platí, že dokáže využít obě pásma zároveň. Frekvence 2.4 Ghz je specifická tím, že zvládne snadněji proniknout zábranami, ale je o poznání pomalejší. Naopak 5 Ghz pracuje na menší vzdálenost, zato maximální rychlost je řádově vyšší [37].

5.3.1.3 USB

USB port může připadat spoustě uživatelů zbytečný u zařízení jako je router, jelikož lze dosáhnout stejné funkcionality jiným způsobem. Nicméně využití USB portu je vhodné pro sdílení tiskárny či zapojení externího uložiště, které mohou využít všichni uživatelé v síti [38].

5.3.1.4 LTE

Slot pro LTE modem je vhodný pro uživatele, kteří mají levný tarif u operátora, popř. zcela neomezená data. Do routeru stačí zapojit pouze kartu SIM a přístup k internetu je zaručen téměř na celém území České republiky, jelikož pokrytí rychlé LTE sítě je jedna z priorit u operátorů [39].

5.3.1.5 Rychlost přenosu (RJ45 port)

Zde je nutno zvážit, jaké zařízení bude uživatel používat připojené do nabízených portů. V nynější době dosahují internetová připojení vysokých rychlostí a pomalejší porty by mohly redukovat rychlost pro připojená zařízení pomocí kabelu [40].

5.3.1.6 Rychlost přenosu

Jak již bylo řečeno výše, na rychlost internetu má vliv zvolená frekvence a překážky, které sílu signálu mohou ovlivňovat. Nicméně často si uživatelé neuvědomují fakt, že zastaralý router rovněž negativně ovlivňuje rychlost připojení. Z tohoto důvodu je nutné kontrolovat datovou propustnost a využívané standardy. Bylo by velmi zbytečné, aby rychlé připojení, které poskytovatel nabízí, nebylo využito kvůli zastaralé infastruktuře [40].

5.3.1.7 Firewall

Pokud se uživatel rozhodne neinvestovat do kvalitního firewallu z přesvědčení, že ztráta dat neovlivní jeho činnost, může využít pouze takové routery, které poskytují základní Firewall zabezpečení.

5.3.1.8 Print server

Funkce Print serveru slouží pro připojení Wi-Fi tiskárny do každého zařízení a nezáleží zde na operačním systému. Uživatel nemusí budovat vlastní Print server, který by byl mnohem nákladnější. Podobná funkcionalita již byla zmíněna výše za pomocí USB portu. Nicméně zabudovaný Print server již pomalu upadá a řada výrobců jej přestává využívat z důvodu nahrazení USB. [41].

5.3.1.9 File server

Jak již z názvu vypovídá, jedná se o sdílení souborů a složek v síti. Rovněž je nyní možné nalézt podobnost s funkcionalitou u USB portu, ale i zde se jedná o propracovanější a jednodušší nasazení [41].

5.3.1.10 VPN

Řada IT odborníků považuje VPN za velmi kvalitní ochranu sítě proti napadení, ale špatné nastavení může způsobit také častější úniky DNS a IP adres [42].

Použití VPN se různí. Drtivá část uživatelů vyhledává VPN v oblastech, kde není možné používat aplikace jako například Facebook nebo získat větší výběr obsahu filmů a seriálů u

streamovací společnosti Netflix. Nicméně hlavním cílem VPN by mělo zůstat silné a bezpečné šifrování [42].

VPN služby je možné zakoupit, popř. vyhledat volně dostupné verze. Zde je však velký problém s limity. VPN routery řeší tento problém. Poskytují neomezený počet připojení a také VPN připojení je neustále dostupné [42].

5.3.1.11 QoS

Funkce QoS neboli Quality of Service již byla zmíněna u switchů a je využívána pro prioritizování u přijímání signálu, aby nedocházelo ke zpomalování zbylých zařízení v síti [21].

5.3.1.12 Podpora IPv6

Použitelné adresy v IPv4 jsou již nějaký čas vyčerpány, proto se zavádí přechod na IPv6. Výhoda IPv6 spočívá v tom, že není nutné dále překládat adresy, ale každé zařízení získá svoji veřejnou adresu. V některých případech dokáže zrychlit přenos tím, že nebude využívat u routerů překlad. Především bude jednodušší připojení vzdáleně k ostatním zařízením v síti [43].

5.3.1.13 Multimediální server

Multimediální server by se dal popsat jako File server, který se zaměřuje především na video, audio a obrázky [41].

5.3.1.14 Cloud

Vytvoření Cloudu umožňuje přístup k datům z různých zařízení. Přihlášení je pomocí dvoufaktorového ověření. Výhoda vzhledem k multimediálnímu serveru a File serveru je, že zde zařízení nemusí být připojeno k domácí síti [44].

5.3.1.15 Cena

Jak již bylo zmíněno, jedná se o produkty pro domácnosti a menší podniky, proto cena nebude vyšší než 3 000 korun.

5.3.2 Zvolená zařízení

Pro FCA byly zvoleny routery od společností ASUS, Tenda Technology, TP-LINK a Netis.

5.3.2.1 Tenda Technology F3

Jako první router byl vybrán typ F3 od společnosti Tenda Technology, který je ze všech produktů nejlevnější.

Tab. 22 Atributy pro Tenda Technology F3 [45].

Wi-Fi standard	802.11n
Pracovní frekvence	2.4Ghz
USB	Ne
LTE	Ne
Rychlost přenosu (RJ45 port)	100 [Mb/s]
Rychlost přenosu [Mb/s]:	300
Firewall	Ne
Print Server	Ne
File Server	Ne
VPN	Ne
QoS	Ano
Podpora IPv6	Ne
Multimediální server	Ne
Cloud	Ne
Cena	333 Kč

Obr. 26 Tenda Technology F3 [45].

5.3.2.2 ASUS RT-N12 D1

Jako druhý v pořadí byl vybrán produkt od společnosti ASUS s názvem RT-N12 D1.

Tab. 23 Atributy pro ASUS RT-N12 D1 [46].

Wi-Fi standard	802.11n
Pracovní frekvence	2.4Ghz
USB	Ne
LTE	Ne
Rychlost přenosu (RJ45 port)	100 [Mb/s]
Rychlost přenosu [Mb/s]:	300
Firewall	Ne
Print Server	Ne
File Server	Ne
VPN	Ano
QoS	Ne
Podpora IPv6	Ne
Multimediální server	Ne
Cloud	Ne
Cena	650 Kč

Obr. 27 ASUS RT-N12 D1 [46].

5.3.2.3 TP-LINK Archer C6

Následuje společnost TP-LINK s produktem Archer C6.

Tab. 24 Atributy pro TP-LINK Archer C6 [47].

Wi-Fi standard	802.11ac
Pracovní frekvence	2.4Ghz &5Ghz
USB	Ne
LTE	Ne
Rychlost přenosu (RJ45 port)	1000 [Mb/s]
Rychlost přenosu [Mb/s]:	1200
Firewall	Ano
Print Server	Ne
File Server	Ne
VPN	Ano
QoS	Ne
Podpora IPv6	Ano
Multimediální server	Ne
Cloud	Ne
Cena	999 Kč

Obr. 28 TP-LINK Archer C6 [47].

5.3.2.4 Netis WF-2880

Do kategorie, které již překračují částku 1 000 Kč, se řadí Netis WF-2880.

Tab. 25 Atributy pro Netis WF-2880 [48].

Wi-Fi standard	802.11ac
Pracovní frekvence	2.4Ghz &5Ghz
USB	Ano
LTE	Ne
Rychlost přenosu (RJ45 port)	1000 [Mb/s]
Rychlost přenosu [Mb/s]:	1200
Firewall	Ne
Print Server	Ne
File Server	Ne
VPN	Ne
QoS	Ano
Podpora IPv6	Ne
Multimediální server	Ne
Cloud	Ne
Cena	1 289 Kč

Obr. 29 Netis WF-2880 [48].

5.3.2.5 ASUS RT-AC1200G+

Nejdražším produktem ve výběru disponuje ASUS s RT-AC1200G+.

Tab. 26 Atributy pro ASUS RT-AC1200G+ [49].

Wi-Fi standard	802.11ac
Pracovní frekvence	2.4Ghz &5Ghz
USB	Ano
LTE	Ano
Rychlost přenosu (RJ45 port)	1000 [Mb/s]
Rychlost přenosu [Mb/s]:	1200
Firewall	Ano
Print Server	Ano
File Server	Ano
VPN	Ano
QoS	Ano
Podpora IPv6	Ano
Multimediální server	Ano
Cloud	Ano
Cena	1 990 Kč

Obr. 30 ASUS RT-AC1200G+ [49].

5.3.2.6 TP-LINK Archer C7

Poslední v pořadí je produkt od společnosti TP-LINK Archer C7.

Tab. 27 Atributy pro TP-LINK Archer C7 [50].

Wi-Fi standard	802.11ac
Pracovní frekvence	2.4Ghz &5Ghz
USB	Ano
LTE	Ne
Rychlost přenosu (RJ45 port)	1000 [Mb/s]
Rychlost přenosu [Mb/s]:	1750
Firewall	Ano
Print Server	Ano
File Server	Ano
VPN	Ano
QoS	Ano
Podpora IPv6	Ano
Multimediální server	Ano
Cloud	Ne
Cena	1 790 Kč

Obr. 31 TP-LINK Archer C7 [50].

5.3.3 Výstup programu ConExp pro routery

V následující tabulce (Tab. 28) je sjednocení všech vybraných modelů.

Tab. 28 Sjednocení vybraných modelů [Vlastní zdroj].

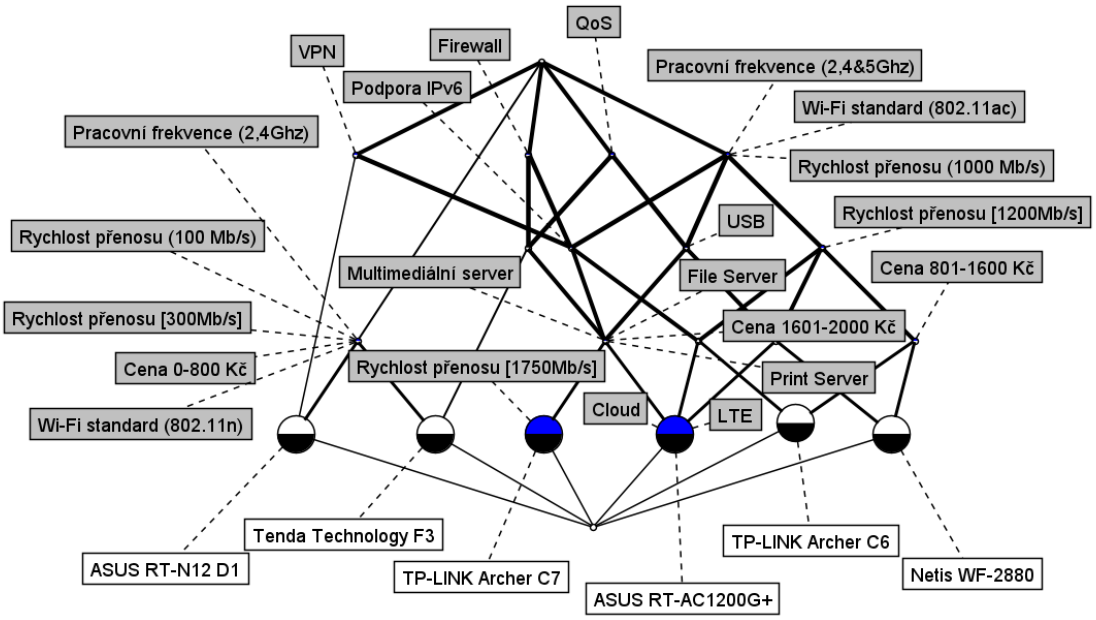
Vybrané routery	Wi-Fi standard (802.11)	Pracovní frekvence (Ghz)	USB	LTE	Rychlost přenosu (RJ45 port)	Rychlost přenosu [Mb/s]:	Firewall	Print Server	File Server	VPN	QoS	Podpora IPv6	Multimediální server	Cloud	Cena (Kč)
Tenda F3	n	2,4	Ne	Ne	100	300	Ano	Ne	Ne	Ne	Ano	Ne	Ne	Ne	333
RT-N12 D1	n	2,4	Ne	Ne	100	300	Ne	Ne	Ne	Ano	Ne	Ne	Ne	Ne	650
Archer C6	ac	2,4&5	Ne	Ne	1000	1200	Ano	Ne	Ne	Ano	Ne	Ano	Ne	Ne	999
WF-2880	ac	2,4&5	Ano	Ne	1000	1200	Ne	Ne	Ne	Ne	Ano	Ne	Ne	Ne	1289
RT-AC1200G+	ac	2,4&5	Ano	Ano	1000	1200	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano	1990
Archer C7	ac	2,4&5	Ano	Ne	1000	1750	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ne	1790

S předchozí tabulkou (Tab. 28) není možné momentálně pracovat, proto bude nutné provést konceptuální škálování, které převede hodnoty na 1 a 0.

Tab. 29 Konceptuální škálování – routery [Vlastní zdroj].

Vybrané routery	Wi-Fi standard (802.11n)	Wi-Fi standard (802.11ac)	Pracovní frekvence (2,4Ghz)	Pracovní frekvence (2,4&5Ghz)	USB	LTE	Rychlost přenosu (100 Mb/s)	Rychlost přenosu (1000 Mb/s)	Rychlost přenosu [300Mb/s]:	Rychlost přenosu [1200Mb/s]:	Rychlost přenosu [1750Mb/s]:	Firewall	Print Server	File Server	VPN	QoS	Podpora IPv6	Multimediální server	Cloud	Cena 0-800 Kč	Cena 801-1600 Kč	Cena 1601-2000 Kč
Tenda F3	1	0	1	0	0	0	1	0	1	0	0	1	0	0	0	1	0	0	0	1	0	0
RT-N12 D1	1	0	1	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0
Archer C6	0	1	0	1	0	0	0	1	0	1	0	1	0	0	1	0	1	0	0	0	1	0
WF-2880	0	1	0	1	1	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	1	0
RT-AC1200G+	0	1	0	1	1	1	0	1	0	1	0	1	1	1	1	1	1	1	1	0	0	1
Archer C7	0	1	0	1	1	0	0	1	0	0	1	1	1	1	1	1	1	1	0	0	0	1

S výslednou tabulkou po konceptuálním škálováním nic nebrání tomu ji přepsat do programu ConExp.



Obr. 32 Konceptuální svaz – routery [Vlastní zdroj].

Pro atributové implikace je možné využít výpočet důsledků v programu ConExp, dále je možné vidět propracovanější souvislosti.

1 < 4 > Rychlost přenosu (1000 Mb/s) ==> Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz);
2 < 4 > Pracovní frekvence (2,4&5Ghz) ==> Wi-Fi standard (802.11ac) Rychlost přenosu (1000 Mb/s);
3 < 4 > Wi-Fi standard (802.11ac) ==> Pracovní frekvence (2,4&5Ghz) Rychlost přenosu (1000 Mb/s);
4 < 3 > Podpora IPv6 ==> Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) Rychlost přenosu (1000 Mb/s) Firewall VPN;
5 < 3 > Firewall VPN ==> Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) Rychlost přenosu (1000 Mb/s) Podpora IPv6;
6 < 3 > Rychlost přenosu [1200Mb/s] ==> Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) Rychlost přenosu (1000 Mb/s);
7 < 3 > USB ==> Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) Rychlost přenosu (1000 Mb/s) QoS;
8 < 3 > Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) Rychlost přenosu (1000 Mb/s) QoS ==> USB;
9 < 3 > Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) Rychlost přenosu (1000 Mb/s) VPN ==> Firewall Podpora IPv6;
10 < 3 > Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) Rychlost přenosu (1000 Mb/s) Firewall ==> VPN Podpora IPv6;
11 < 2 > Cena 1601-2000 Kč ==> Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) USB Rychlost přenosu (1000 Mb/s) Firewall Print Server File Server VPN QoS Podpora IPv6 Multimediální server;
12 < 2 > Cena 801-1600 Kč ==> Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) Rychlost přenosu (1000 Mb/s) Rychlost přenosu [1200Mb/s];
13 < 2 > Cena 0-800 Kč ==> Wi-Fi standard (802.11n) Pracovní frekvence (2,4Ghz) Rychlost přenosu (100 Mb/s) Rychlost přenosu [300Mb/s];
14 < 2 > Multimediální server ==> Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) USB Rychlost přenosu (1000 Mb/s) Firewall Print Server File Server VPN QoS Podpora IPv6 Cena 1601-2000 Kč;
15 < 2 > VPN QoS ==> Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) USB Rychlost přenosu (1000 Mb/s) Firewall Print Server File Server Podpora IPv6 Multimediální server Cena 1601-2000 Kč;
16 < 2 > File Server ==> Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) USB Rychlost přenosu (1000 Mb/s) Firewall Print Server VPN QoS Podpora IPv6 Multimediální server Cena 1601-2000 Kč;
17 < 2 > Print Server ==> Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) USB Rychlost přenosu (1000 Mb/s) Firewall File Server VPN QoS Podpora IPv6 Multimediální server Cena 1601-2000 Kč;
18 < 2 > Rychlost přenosu [300Mb/s] ==> Wi-Fi standard (802.11n) Pracovní frekvence (2,4Ghz) Rychlost přenosu (100 Mb/s) Cena 0-800 Kč;
19 < 2 > Rychlost přenosu (100 Mb/s) ==> Wi-Fi standard (802.11n) Pracovní frekvence (2,4Ghz) Rychlost přenosu [300Mb/s] Cena 0-800 Kč;
20 < 2 > Pracovní frekvence (2,4Ghz) ==> Wi-Fi standard (802.11n) Rychlost přenosu (100 Mb/s) Rychlost přenosu [300Mb/s] Cena 0-800 Kč;
21 < 2 > Wi-Fi standard (802.11n) ==> Pracovní frekvence (2,4Ghz) Rychlost přenosu (100 Mb/s) Rychlost přenosu [300Mb/s] Cena 0-800 Kč;
22 < 1 > Cloud ==> Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) USB LTE Rychlost přenosu (1000 Mb/s) Rychlost přenosu [1200Mb/s] Firewall Print Server File Server VPN QoS Podpora IPv6 Multimediální server Cena 1601-2000 Kč;
23 < 1 > Rychlost přenosu [1750Mb/s] ==> Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) USB Rychlost přenosu (1000 Mb/s) Firewall Print Server File Server VPN QoS Podpora IPv6 Multimediální server Cena 1601-2000 Kč;
24 < 1 > LTE ==> Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) USB Rychlost přenosu (1000 Mb/s) Rychlost přenosu [1200Mb/s] Firewall Print Server File Server VPN QoS Podpora IPv6 Multimediální server Cloud Cena 1601-2000 Kč;
25 < 1 > Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) USB Rychlost přenosu (1000 Mb/s) Rychlost přenosu [1200Mb/s] Firewall Print Server File Server VPN QoS Podpora IPv6 Multimediální server Cena 1601-2000 Kč ==> LTE Cloud;
26 < 1 > Wi-Fi standard (802.11n) Pracovní frekvence (2,4Ghz) Rychlost přenosu (100 Mb/s) Rychlost přenosu [300Mb/s] QoS Cena 0-800 Kč ==> Firewall;
27 < 1 > Wi-Fi standard (802.11n) Pracovní frekvence (2,4Ghz) Rychlost přenosu (100 Mb/s) Rychlost přenosu [300Mb/s] Firewall Cena 0-800 Kč ==> QoS;
28 < 0 > Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) USB LTE Rychlost přenosu (1000 Mb/s) Rychlost přenosu [1200Mb/s] Firewall Print Server File Server VPN QoS Podpora IPv6 Multimediální server Cloud Cena 801-1600 Kč Cena 1601-2000 Kč ==> Wi-Fi standard (802.11n) Pracovní frekvence (2,4Ghz) Rychlost přenosu (100 Mb/s) Rychlost přenosu [300Mb/s] Rychlost přenosu [1750Mb/s] Cena 0-800 Kč;
29 < 0 > Wi-Fi standard (802.11ac) Pracovní frekvence (2,4&5Ghz) USB LTE Rychlost přenosu (1000 Mb/s) Rychlost přenosu [1200Mb/s] Rychlost přenosu [1750Mb/s] Firewall Print Server File Server VPN QoS Podpora IPv6 Multimediální server Cloud Cena 1601-2000 Kč ==> Wi-Fi standard (802.11n) Pracovní frekvence (2,4Ghz) Rychlost přenosu (100 Mb/s) Rychlost přenosu [300Mb/s] Cena 0-800 Kč Cena 801-1600 Kč;
30 < 0 > Wi-Fi standard (802.11n) Wi-Fi standard (802.11ac) Pracovní frekvence (2,4Ghz) Pracovní frekvence (2,4&5Ghz) Rychlost přenosu (100 Mb/s) Rychlost přenosu (1000 Mb/s) Rychlost přenosu [300Mb/s] Cena 0-800 Kč ==> USB LTE Rychlost přenosu [1200Mb/s] Rychlost přenosu [1750Mb/s] Firewall Print Server File Server VPN QoS Podpora IPv6 Multimediální server Cloud Cena 801-1600 Kč Cena 1601-2000 Kč;

Obr. 33 Konceptuální implikace – routery [Vlastní zdroj].

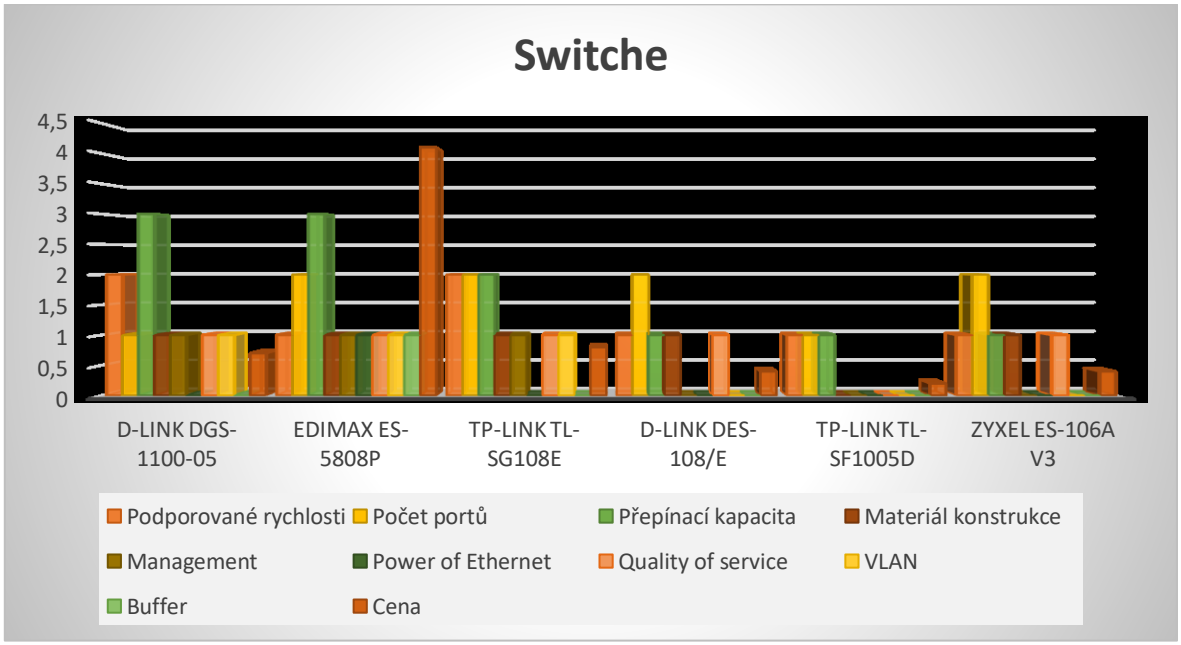
6 3D ZOBRAZENÍ VÝSLEDKŮ

Aby bylo možné získat supremum a infimum pro switche, routery a firewally, bude nezbytné vytvořit 3D model zobrazení výsledků. Na níže uvedených grafech (Obr. 34, 35, 36) lze vidět vyobrazené 3D modely výsledků. Pro každý prvek je nutné vyzdvihnout primární atributy. Díky prioritě atributů lze dále určit supremum a infimum.

Pro switche je nejpodstatnější rychlost, do které spadá i přepínací kapacita, která musí být úměrná počtu portů. Důležitou funkcí je management, aby bylo možné dále upravovat switch. V neposlední řadě rozhoduje také cena.

Supremem se stal TP-LINK TL-SG108E, jelikož dokáže zvládnout gigabitovou rychlost a počet portů je úměrný přepínací rychlosti. Nadále vlastní všechny podstatné funkce a přes nízkou cenu se vyrovná dražším modelům.

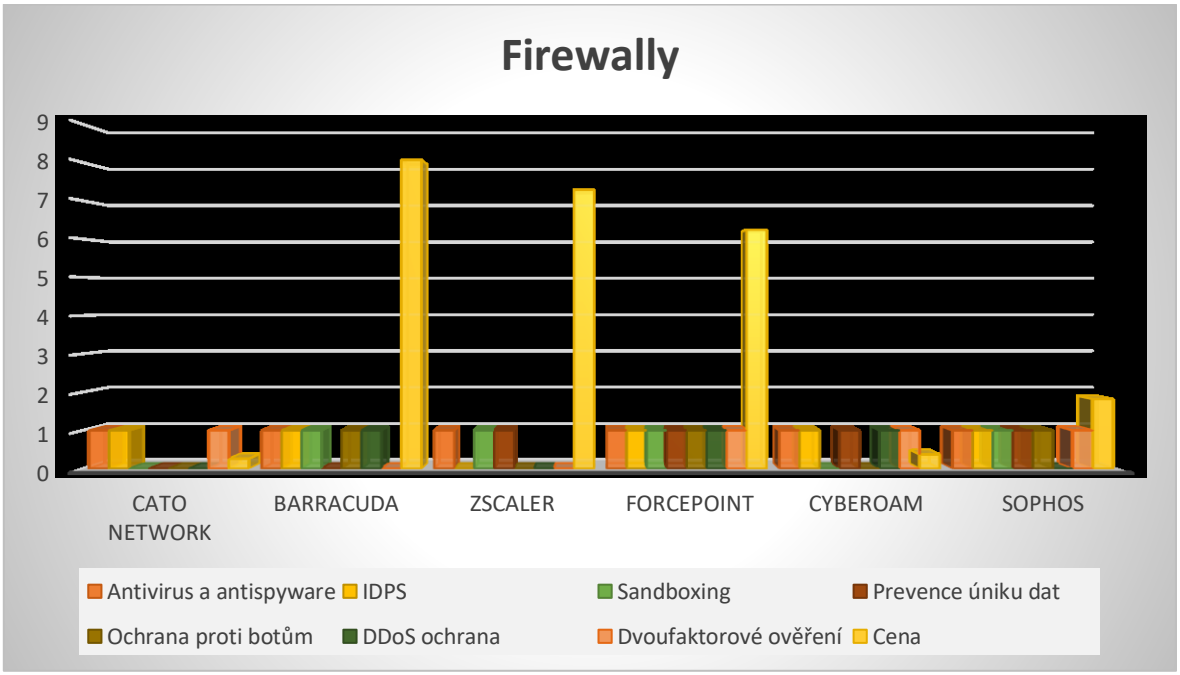
Infimem se zde stal rovněž produkt od výrobce TP-LINK model TL-SF1005D. Zde je možné vidět nejnižší rychlost a přepínací kapacita rozhodně nebude stačit na počet portů. Není zde žádná funkce, a proto i cena je velmi nízká. Jedná se o produkt pro nejméně náročné uživatele, nicméně v dnešní době pro stabilní funkci internetu rozhodně nestačí.



Obr. 34 Graf výsledných hodnot – switche [Vlastní zdroj].

U firewallů patří mezi prioritní atributy především IDPS, DDoS ochrana a cena. Z tohoto důvodu se supremem stal Forcepoint NGFV, jelikož obsahuje všechny vybrané atributy a cena z hlediska funkcí patří k nejnižším na trhu.

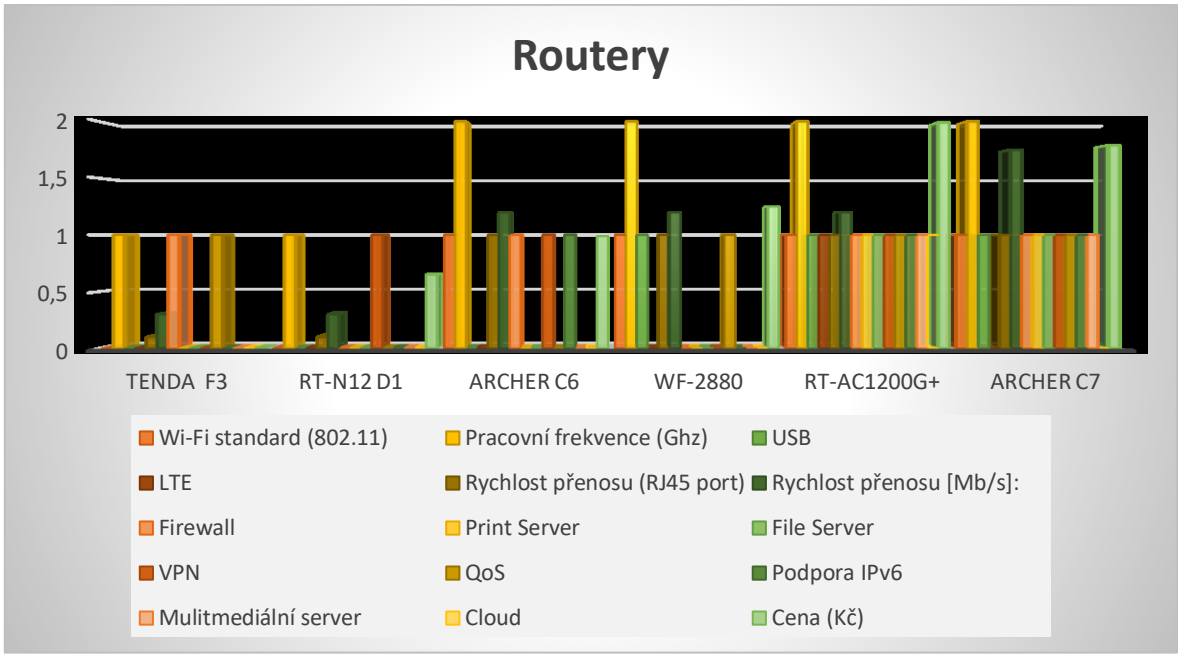
Infimem se stal Cato Network, který vyniká pouze svojí cenou. Nicméně z hlediska funkcí je nejméně schopný firewall a jeho využití je především u takové IT struktury, kde dostupnost a bezpečnost nehraje příliš velkou roli.



Obr. 35 Graf výsledných hodnot – firewally [Vlastní zdroj].

Prioritní atributy pro routery jsou Wi-Fi standard 802.11ac, rychlost přenosu a USB port, který dokáže nahradit Print server i File server. Především díky rychlosti, která by měla být nejpodstatnější, se stal supremem TP-LINK Archer C7. Zmíněný router podporuje rychlost 1750 Mb/s, čímž překonává všechny své konkurenty. V těsném závěsu se nachází ASUS RT-AC1200G+, jelikož navíc obsahuje také LTE a Cloud, nicméně jsou to technologie, které nejsou tak podstatné při pořízení routeru.

Infimem se stal produkt ASUS RT-N12 D1, jelikož je dražší než produkt Tenda Technology F3. Dále poskytuje standard 802.11n s rychlostí 300 Mb/s a nabízí pouze podporu VPN, která je v dnešním progresivním trhu nedostatečná.



Obr. 36 Graf výsledných hodnot – routery [Vlastní zdroj].

ZÁVĚR

Cílem diplomové práce bylo zakomponovat formální konceptuální analýzu do oblasti speciálních síťových prvků. Zmíněná analýza byla provedena pro switche, firewally a routery. Formou literární rešerše je zde definována formální konceptuální analýza, která pracuje s tabulkovými daty. Dále jsou rozebrány podstatné úpravy dat, aby bylo možné zkonstruovat konceptuální svaz a vytvořit atributové implikace. Cílem každé formální konceptuální analýzy je vytvořit výstup, jenž zobrazí informace, které nelze vidět na první pohled. V teoretické části následuje rozšíření o Fuzzy logiku, která již nepracuje pouze s Booleovskými výrazy, ale používá se pro složitější případy, kde je nutné zpřesnit jednotlivé informace.

Druhá polovina teoretické části se zabývá popisem switchů, firewallů a routerů. Aby bylo možné popsat funkcionalitu jednotlivých síťových prvků, bylo nezbytné definovat zkratky a pojmy jako jsou IP a MAC adresy, paket, rámec, referenční model OSI a TCP/IP protokol. Pomocí definování zmíněných pojmů bylo možné vysvětlit, jak jednotlivé síťové prvky pracují.

V praktické části je popsán program pro tvorbu formální konceptuální analýzy Concept Explorer. Jsou zde definovány funkce pro vstup konceptuálního škálování a vytvoření konceptuálního svazu spolu s atributovými implikacemi. Dále bylo fixně zvoleno pro každý síťový prvek šest objektů, které doplňují podstatné atributy, jež jsou nezbytné pro funkci zvolených produktů. Pro switche se supremem, a tudíž nejlepším produktem, stal TP-LINK TL-SG108E, jelikož zvládá gigabitovou rychlost a cena je více než přívětivá. Infimem byl zvolen produkt značky TP-LINK model TL-SF1005D. U firewallů byly již výraznější rozdíly z důvodu širokého rozpětí cenové relace. Supremem se stal Forcepoint NGFV, který disponuje nízkou cenou a řadou důležitých funkcí. Infimem byl zvolen produkt Cato Network, jelikož z hlediska funkcí zaštiťuje pouze Antivirus a IDPS. Poslední v pořadí následovala analýza routerů. Zde se Supremem stal TP-LINK Archer C7 z důvodu podpory rychlosti až 1750 Mb/s, dále ze zmíněných atributů neobsahuje pouze technologii Cloud. ASUS model RT-N12 D1 byl zvolen infimem, jelikož jeho rychlost je již velmi nízká a z hlediska funkcí podporuje pouze VPN.

V závěru práce je zobrazena verifikace získaných dat formální konceptuální analýzy ve 3D prostředí. Patřičné objekty mají přehledně zobrazené atributy, kterými disponují.

SEZNAM POUŽITÉ LITERATURY

[1] BĚLOHLÁVEK, Radim. Konceptuální svazy a formální konceptuální analýza [online]. 2004 [cit. 2020-02-13]. Dostupné z WWW: http://belohlavek.inf.upol.cz/publications/Bel_Ksfka.pdf.

[2] NOVÁK, Vilém. Fuzzy množiny a jejich aplikace. Praha: Nakladatelství technické literatury, 1990. ISBN 80-03-00325-3.

[3] NAVARA, Mirko a Petr OLŠÁK. Základy Fuzzy množin. Vyd. 1. Praha: Vydavatelství ČVUT, 2002, 136 s. ISBN 80-01-02585-3.

[4] *Difference Between Frame and Packet* [online]. 18 august 2017 [cit. 2020-02-07]. Dostupné z: https://techdifferences.com/difference-between-frame-and-packet.html

[5] VODA, Zbyšek. *JAK JE TO S IP, MAC ADRESAMI A SÍTĚMI* [online]. 18.12.2019 [cit. 2020-02-07]. Dostupné z: https://arduino.cz/jak-je-to-s-ip-a-mac-adresami/

[6] *Difference Between TCP/IP and OSI Model* [online]. 25 March, 2016 [cit. 2020-02-07]. Dostupné z: https://techdifferences.com/difference-between-tcp-ip-and-osi-model.html

[7] *Switch TP-Link T2600G-28TS(TL-SG3424) JetStream 24-Port Gigabit L2 Managed/4xSFP Combo* [online]. 25 March, 2016 [cit. 2020-02-07]. Dostupné z: https://www.abctech.cz/switch-tp-link-t2600g-28ts-tl-sg3424-jetstream-24-port-gigabit-l2-managed-4xsfp-combo_d13984.html#

[8] BOUŠKA, Petr. *Víte, jak pracuje router?* [online]. [cit. 2020-02-07]. Dostupné z: https://www.samuraj-cz.com/clanek/vite-jak-pracuje-router/

[9] BOUŠKA, Petr. *Víte, jak pracuje switch?* [online]. [cit. 2020-02-07]. Dostupné z: https://www.samuraj-cz.com/clanek/vite-jak-pracuje-switch/

[10] *TP-LINK TL-R480T+* [online]. [cit. 2020-02-07]. Dostupné z: https://www.alza.cz/tp-link-tl-r480t-d324486.htm?kampan=adw1_sitove-prvky-a-nas_pla_all_sitove-prvky-a-nas-css_wifi_c_20219_1o4_TP645l2&gclid=Cj0KCQiAsvTxBRDkARIsAH4W_j9My6aXp2WNgIOeBerNXNuiMPF6ijsotpyzv30y2CXzGQVpSThOsAsaAutSEALw_wcB

[11] ARNOLD, Arne. *Vše, co potřebujete vědět o firewallech* [online]. [cit. 2020-02-11]. Dostupné z: https://pcworld.cz/archiv/vse-co-potrebujete-vedet-o-firewallech-17497

[12] *Zyxel NSG200* [online]. In: [cit. 2020-02-13]. Dostupné z: https://www.alza.cz/zyxel-nsg200-d5502450.htm

[13] *Softwarové Firewally* [online]. [cit. 2020-02-13]. Dostupné z: https://www.antivirovecentrum.cz/firewally.aspx

[14] VOLNÁ, Eva. Základy softcomputingu [online]. Ostrava, 2012 [cit. 2020-03-06]. Dostupné z: http://www1.osu.cz/~volna/Zaklady_softcomputingu_skripta.pdf. Ostravská univerzita v Ostravě.

[15] *Gigabit Smart Managed Switches DGS-1100 série* [online]. [cit. 2020-03-28]. Dostupné z: https://eu.dlink.com/cz/cs/products/dgs-1100-series-gigabit-smart-switches

[16] *8 Ports Desktop Power over Ethernet Web Smart Fast Ethernet Switch ES-5808P* [online]. [cit. 2020-03-28]. Dostupné z: https://www.edimax.com/edimax/merchandise/merchandise_detail/data/edimax/au/smb_switches_poe/es-5808p/

[17] *8portový gigabitový switch Easy Smart TL-SG108E* [online]. [cit. 2020-03-28]. Dostupné z: https://www.tp-link.com/cz/business-networking/easy-smart-switch/tl-sg108e/

[18] *8-Port Fast Ethernet Unmanaged Desktop Switch DES-108* [online]. [cit. 2020-03-28]. Dostupné z: https://eu.dlink.com/cz/cs/products/des-108-8-port-fast-ethernet-switch

[19] *5portový stolní switch 10/100 Mbit/s TL-SF1005D* [online]. [cit. 2020-03-28]. Dostupné z: https://www.tp-link.com/cz/service-provider/unmanaged-switch/tl-sf1005d/

[20] *8-Port Desktop Fast Ethernet Switch* [online]. [cit. 2020-03-28]. Dostupné z: https://www.zyxel.com/cz/cs/products_services/8-Port-Desktop-Fast-Ethernet-Switch-ES-108A-v3/overview

[21] ČERNÁ, Michaela. *Srovnávací test a recenze nejlepších switchů* [online]. Leden 2020 [cit. 2020-03-28]. Dostupné z: https://www.arecenze.cz/switche/#jak-vybrat-switch

[22] BRÁZDIL, Radek. *Jak vybrat switch – na jaké parametry se zaměřit* [online]. 23.08.2019 [cit. 2020-03-28]. Dostupné z: https://rychlost.cz/clanek/2019-08-jak-vybrat-switch-na-jake-parametry-se-zamerit/

[23] *Antivirus vs Firewall* [online]. AUKTA, Shikha. 3 November 2017 [cit. 2020-04-02]. Dostupné z: https://www.malwarefox.com/antivirus-vs-firewall/

[24] *What is an Intrusion Prevention System – IPS* [online]. [cit. 2020-04-02]. Dostupné z: https://www.checkpoint.com/definitions/what-is-ips/

[25] *What is Sandboxing?* [online]. [cit. 2020-04-02]. Dostupné z: https://www.barracuda.com/glossary/sandboxing

[26] *What is Data Leakage?: Data Leakage Defined, Explained, and Explored* [online]. [cit. 2020-04-02]. Dostupné z: https://www.forcepoint.com/cyber-edu/data-leakage

[27] GOLDGOF, Mike. *Advanced bot protection What is Advanced Bot Protection?* [online]. August 8, 2019 [cit. 2020-04-04]. Dostupné z: https://blog.barracuda.com/2019/08/08/what-is-advanced-bot-protection/

[28] GRYGAŘÍKOVÁ, Michaela. *Anti-DDoS ochrana aneb Proč jen firewall nestačí* [online]. 09.09. 2019 [cit. 2020-04-04]. Dostupné z: https://www.master.cz/blog/anti-ddos-ochrana-proc-firewall-nestaci/

[29] *Multi-Factor Authentication from Duo* [online]. [cit. 2020-04-04]. Dostupné z: https://duo.com/product/multi-factor-authentication-mfa

[30] *Cato Networks Cloud-based Next Generation Firewall* [online]. [cit. 2020-04-05]. Dostupné z: https://roi4cio.com/en/products/product/cato-networks-cloud-based-next-generation-firewall-1/

[31] *Barracuda NextGen Firewall (NGFW)* [online]. [cit. 2020-04-05]. Dostupné z: https://roi4cio.com/en/products/product/barracuda-nextgen-firewall-ngfw/

[32] *Zscaler Cloud Firewall* [online]. [cit. 2020-04-05]. Dostupné z: https://roi4cio.com/en/products/product/zscaler-cloud-firewall-1/

[33] *Forcepoint NGFW* [online]. [cit. 2020-04-05]. Dostupné z: https://roi4cio.com/en/products/product/forcepoint-ngfw/

[34] *Cyberoam Next Generation Firewall* [online]. [cit. 2020-04-05]. Dostupné z: https://roi4cio.com/en/products/product/cyberoam-next-generation-firewall-1/

[35] *Sophos Next-Generation Firewall* [online]. [cit. 2020-04-05]. Dostupné z: https://roi4cio.com/en/products/product/sophos-next-generation-firewall-1/

[36] SHAW, Keith. *802.11: Wi-Fi standards and speeds explained* [online]. [cit. 2020-07-06]. Dostupné z: https://www.networkworld.com/article/3238664/80211-wi-fi-standards-and-speeds-explained.html

[37] PHILLIPS, Gavin. *The Most Common Wi-Fi Standards and Types Explained* [online]. [cit. 2020-07-06]. Dostupné z: https://www.makeuseof.com/tag/understanding-common-wifi-standards-technology-explained/

[38] SHAREEF, Umar. *What is the use of USB in router?* [online]. [cit. 2020-07-06]. Dostupné z: http://www.zelect.in/router/what-is-the-use-of-usb-in-router

[39] *The simplest difference between 3G/4G LTE and WiFi-only routers* [online]. [cit. 2020-07-06]. Dostupné z: https://www.dignited.com/14656/the-simplest-difference-between-3g4g-lte-and-wifi-only-routers/

[40] BENZL, Lukáš. *Kdy váš Wi-Fi router zpomaluje rychlost připojení?* [online]. 01.11.2017 [cit. 2020-07-06]. Dostupné z: https://rychlost.cz/clanek/2017-08-kdy-vas-wi-fi-router-zpomaluje-rychlost-pripojeni/

[41] ORTH, Mindi. *How to Use a Router to Make a Printer a Wireless Printer* [online]. January 11, 2019 [cit. 2020-07-06]. Dostupné z: https://smallbusiness.chron.com/use-router-make-printer-wireless-printer-56526.html

[42] WELEKWE, Amakiri. *VPN routery: O co přesně se jedná a jak jeden nainstalovat (v rekordním čase)* [online]. [cit. 2020-07-06]. Dostupné z: https://cs.vpnmentor.com/blog/jak-nainstalovat-vpn-smerovace/

[43] *Srovnání protokolů IPv4 a IPv6* [online]. 11.8.2015 [cit. 2020-07-06]. Dostupné z: https://www.dostupnyinternet.cz/blog/protokol-ipv4-ipv6/

[44] *Dvoupásmový router Wireless-AC1200* [online]. [cit. 2020-07-06]. Dostupné z: https://www.asus.com/cz/Networking/RT-AC1200G-Plus/

[45] TENDA F3 (F303). *TSBOHEMIA.CZ* [online]. [cit. 2020-07-09]. Dostupné z: https://www.tsbohemia.cz/tenda-f3-f303-_d228084.html

[46] ASUS RT-N12 D1. *TSBOHEMIA.CZ* [online]. [cit. 2020-07-09]. Dostupné z: https://www.tsbohemia.cz/asus-rt-n12-d_d158963.html

[47] TP-LINK Archer C6. *TSBOHEMIA.CZ* [online]. [cit. 2020-07-09]. Dostupné z: https://www.tsbohemia.cz/tp-link-archer-c6_d308325.html

[48] Netis WF-2880. *TSBOHEMIA.CZ* [online]. [cit. 2020-07-09]. Dostupné z: https://www.tsbohemia.cz/netis-wf-2880_d228851.html

[49] ASUS RT-AC1200G+. *TSBOHEMIA.CZ* [online]. [cit. 2020-07-09]. Dostupné z: https://www.tsbohemia.cz/asus-rt-ac1200g-_d235295.html

[50] TP-LINK Archer C7 (AC1750). *TSBOHEMIA.CZ* [online]. [cit. 2020-07-09]. Dostupné z: https://www.tsbohemia.cz/tp-link-archer-c7-ac1750-_d173401.html

[51] MĚSÍČEK, Pavel. *Aplikace Port-Royalské logiky pro speciální ochranu*. Zlín, 2017. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce Ivanka, Ján.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

FKA	Formální konceptuální analýza
IP	Internet Protocol
MAC	Media Access Control
TCP/IP	Transmission Control Protocol/Internet Protocol
OSI	Open System Interconnection
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
SMDS	Switched Multi-megabit Data Service
FDDI	Fiber Distributed Data Interface
SSL	Secure Sockets Layer
DNS	Domain Name Service
ICMP	Internet Control Message Protocol
OSPF	Open Shortest Path First
TCP	Transmission Control Protocol
UTP	User Datagram Protocol
FTP	File Transfer Protocol
DHCP	Dynamic Host Configuration Protocol
PPP	Point-to-Point Protocol
ARP	Address Resolution Protocol
POP3	Post Office Protocol version 3
SSH	Secure Shell
CAM	Content Addressable Memory
LAN	Local Network Area
DSL	Digital Subscriber Line
WAN	Wide Area Network

RIP	Routing Information Protocol
ConExp	Concept Explorer
SFP	Small Form-factor Pluggable
PoE	Power of Ethernet
QoS	Quality of Service
VoIP	Voice over Internet Protocol
VLAN	Virtual Local Area Network
GB	Gigabyte
Mb	Megabit
MB	Megabyte
IDPS	Intrusion Detection and Prevention System
DoS	Denial of Service
DDoS	Distributed Denial of Service
IEEE	Institute of Electrical and Electronics Engineers
Ghz	Gigahertz
USB	Universal Seriál Bus
LTE	Long Term Evolution
SIM	Subscriber Identity Module
RJ45	Registered Jack – 45
Wi-Fi	Wireless Fidelity
VPN	Virtual Private Network

SEZNAM OBRÁZKŮ

Obr. 1 Prvek spadající do množiny A i B [Vlastní zdroj]. 17
Obr. 2 Průběh funkce - μA(u) pro běžnou množinu A [14]. 18
Obr. 3 Průběh funkce – μA(u) pro fuzzy množinu A [14]. 19
Obr. 4 Názorný obrázek Switch TP-Link T2600G-28TS [7]. 24
Obr. 5 Názorný obrázek Firewallu Zyxel NSG200 [12]. 26
Obr. 6 Názorný obrázek TP-LINK TL-R480T+ [10]..... 27
Obr. 7 Ukázka programu ConExp – kontextová tabulka [Vlastní zdroj]. 30
Obr. 8 Ukázka programu ConExp – konceptuální svaz [Vlastní zdroj]..... 30
Obr. 9 Ukázka programu ConExp – vyznačení pro lepší orientaci [Vlastní zdroj]. 31
Obr 10. D-Link DGS-1100-05 [15]..... 35
Obr. 11 Edimax ES-5808P [16]. 36
Obr. 12 TP-LINK TL-SG108E [17]..... 36
Obr. 13 D-Link DES-108/E [18]..... 37
Obr. 14 TP-Link TL-SF1005D [19]..... 38
Obr. 15 ZyXEL ES-106A v3 [20]..... 38
Obr. 16 Konceptuální svaz – switche [Vlastní zdroj]. 40
Obr. 17 Atributové implikace – switche [Vlastní zdroj]. 41
Obr. 18 Logo společnosti Cato Networks [30]. 44
Obr. 19 Logo společnosti Barracuda [31]..... 45
Obr. 20 Logo společnosti Zscaler [32]. 46
Obr. 21 Logo společnosti Forcepoint [33]..... 46
Obr. 22 Logo společnosti Cyberoam [34]. 47
Obr. 23 Logo společnosti Sophos [35]. 48
Obr. 24 Konceptuální svaz – firewally [Vlastní zdroj]. 49
Obr. 25 Atributové implikace – firewally [Vlastní zdroj]. 50
Obr. 26 Tenda Technology F3 [45]..... 54
Obr. 27 ASUS RT-N12 D1 [46]. 55
Obr. 28 TP-LINK Archer C6 [47]..... 56
Obr. 29 Netis WF-2880 [48]..... 57
Obr. 30 ASUS RT-AC1200G+ [49]..... 58
Obr. 31 TP-LINK Archer C7 [50]..... 59
Obr. 32 Konceptuální svaz – routery [Vlastní zdroj]. 61
Obr. 33 Konceptuální implikace – routery [Vlastní zdroj]..... 62
Obr. 34 Graf výsledných hodnot – switche [Vlastní zdroj]..... 63

Obr. 35 Graf výsledných hodnot – firewally [Vlastní zdroj]. 64
Obr. 36 Graf výsledných hodnot – routery [Vlastní zdroj]. 65

SEZNAM TABULEK

Tab. 1 Formální kontext [Vlastní zdroj]. 11
Tab. 2 Názorná ukázka – vícehodnotový kontext [1]. 15
Tab. 3 Názorná ukázka – konceptuální škálování [51]. 15
Tab. 4 Porovnání TCP/IP a ISO modelu [6]. 23
Tab. 5. Atributy pro D-Link DGS-1100-05 [15]. 35
Tab. 6 Atributy pro Edimax ES-5808P [16]. 35
Tab. 7 Atributy pro TP-LINK TL-SG108E [17]. 36
Tab. 8 Atributy pro D-Link DES-108/E [18]. 37
Tab. 9 Atributy pro TP-Link TL-SF1005D [19]. 37
Tab. 10 Atributy pro ZyXEL ES-106A v3 [20]. 38
Tab. 11 Sjednocení vybraných modelů [Vlastní zdroj]. 39
Tab. 12 Konceptuální škálování – switche [Vlastní zdroj]. 40
Tab. 13 Atributy pro Cato Network [30]. 44
Tab. 14 Atributy pro Barracuda NextGen Firewall [31]. 45
Tab. 15 Atributy pro Zscaler Firewall [32] 45
Tab. 16 Atributy pro Forcepoint NGFW [33]. 46
Tab. 17 Atributy pro Cyberoam Next Generation Firewall [34]. 47
Tab. 18 Atributy pro Sophos Next-Generation Firewall [35]. 47
Tab. 19 Sjednocení vybraných modelů [Vlastní zdroj]. 48
Tab. 20 Konceptuální škálování – firewally [Vlastní zdroj]. 49
Tab. 21 IEEE Standardy [36]. 51
Tab. 22 Atributy pro Tenda Technology F3 [45]. 54
Tab. 23 Atributy pro ASUS RT-N12 D1 [46]. 55
Tab. 24 Atributy pro TP-LINK Archer C6 [47]. 56
Tab. 25 Atributy pro Netis WF-2880 [48]. 57
Tab. 26 Atributy pro ASUS RT-AC1200G+ [49]. 58
Tab. 27 Atributy pro TP-LINK Archer C7 [50]. 59
Tab. 28 Sjednocení vybraných modelů [Vlastní zdroj]. 60
Tab. 29 Konceptuální škálování – routery [Vlastní zdroj]. 60