

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

ON-LINE DOKUMENTACE PRO KONFIGURACI AK- TIVNÍCH SÍŤOVÝCH PRVKŮ

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

MARTIN BAŠTI

BRNO 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

ON-LINE DOKUMENTACE PRO KONFIGURACI AK- TIVNÍCH SÍŤOVÝCH PRVKŮ

ON-LINE DOCUMENTATION FOR CONFIGURATION OF ACTIVE NETWORK DEVICES

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

MARTIN BAŠTI

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. TOMÁŠ PODERMAŇSKI

BRNO 2012

Abstrakt

Cílem této práce je vytvořit on-line dokumentaci pro konfiguraci síťových prvků, která usnadní práci síťovým administrátorům, odstráněním problémů s různou strukturou a kvalitou dokumentací od výrobců. Dokumentace bude využívat volně dostupný wiki systém, který umožní jednoduché úpravy obsahu a spolupráci více uživatelů, kterého výběr bude rozebrán v práci. Taktěž, se práce věnuje rozboru struktury dokumentace a popisu jednotlivých možností konfigurace, tak aby dokumentace umožňovala rychlé a jednoduché vyhledání požadované informace.

Abstract

The aim of this thesis is to create on-line documentation for network devices configuration, which will make network administrators' work easier by removing problems with various structure and quality of documentation from manufacturers. Documentation will use free wiki system, which allows simple editation of content and colaboration of more users. Process of choosing the best system will be described in thesis. Also we analyse structure of documentation and description of configuration possibilities, so that documentation allows quick and simple searching of required information.

Klíčová slova

on-line dokumentace, síťové prvky, směrovače, prepínače, wiki, konfigurace, síť

Keywords

on-line documentation, network devices, routers, switches, wiki, configuration, network

Citace

Martin Bašti: On-line dokumentace pro konfiguraci aktivních síťových prvků, bakalářská práce, Brno, FIT VUT v Brně, 2012

On-line dokumentace pro konfiguraci aktivních síťových prvků

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Ing. Tomáše Podermaňského.

.....
Martin Bašti
16. května 2012

Poděkování

Děkuji svému vedoucímu Ing. Tomášovi Podermaňskému, za odbornou pomoc při zpracování této bakalářské práce.

© Martin Bašti, 2012.

Tato práce vznikla jako školní dílo na Vysokém učení technickém v Brně, Fakultě informačních technologií. Práce je chráněna autorským zákonem a její užití bez udělení oprávnění autorem je nezákonné, s výjimkou zákonem definovaných případů.

Obsah

1 Úvod	4
2 Techniky konfigurácie aktívnych sieťových prvkov	5
2.1 Webové rozhranie	5
2.2 SNMP	5
2.3 Terminál(CLI)	5
3 Wiki systémy	9
3.1 Požiadavky na wiki systém	9
3.2 MediaWiki	9
3.3 DokuWiki	10
3.4 PmWiki	11
3.5 WikkaWiki	11
3.6 Ostatné wiki systémy	12
3.7 Výber wiki systému	12
4 Štruktúra dokumentácie	14
4.1 Popis formátu syntaxe v dokumentácii	15
4.2 Zápis konfigurácie	15
5 Analýza vybraných konfigurácií zariadení	17
5.1 Základné nastavenia	17
5.1.1 Základné príkazy	17
5.1.2 Konfiguračné módy	18
5.2 Konfigurácia data-linkovej vrstvy	19
5.2.1 VLAN siete	19
5.3 Konfigurácia sieťovej vrstvy	21
5.3.1 Konfigurácia IP a IPv6 adres	21
5.3.2 Unicast smerovanie	22
5.4 Ďalšie služby	24
5.4.1 DHCP server	24
6 Záver	26
A Screenshoty wiki systémov	29

B	Štruktúra dokumentácie	32
B.1	Základné nastavenia	32
B.2	Nastavenia data-linkovej vrstvy – prepínače	33
B.3	Nastavenia sieťovej vrstvy – smerovače	34
B.4	Ďalšie služby	34

Zoznam obrázkov

5.1	Tagovanie IEEE 802.1Q ¹	19
A.1	MediaWiki po inštalácií	29
A.2	DokuWiki po inštalácií	30
A.3	PmWiki po inštalácií	30
A.4	WikkaWiki po inštalácií	31

Zoznam tabuliek

2.1	Príklad konfigurácie IPv6 adresy na prvku Cisco 2960G	6
2.2	Príklad konfigurácie IPv6 adresy na prvku HP/H3C A5120-EI	6
2.3	Príklad konfigurácie IPv6 adresy na prvku EdgeCore 4626	6
2.4	Príklad konfigurácie IPv6 adresy na prvku Juniper EX4200	7
2.5	Príklad konfigurácie ACL na prvku Cisco 2960G	7
2.6	Príklad konfigurácie ACL na prvku HP/H3C A5120-EI	7
2.7	Príklad konfigurácie ACL na prvku EdgeCore 4626	8
3.1	Požadované vlastnosti jednotlivých wiki systémov	12
4.1	Formát syntaxe v dokumentácii.	15
4.2	Ukážka konfigurácie v manuáli výrobcu pre zariadenie EdgeCore	16
4.3	Ukážka konfigurácie pre zariadenie EdgeCore v našej dokumentácii	16
5.1	Základné príkazy pre Cisco, H3C a EdgeCore	17
5.2	Konfiguračné módy pre Cisco, H3C a EdgeCore	18
5.3	Vytvorenie a zobrazenie VLAN sietí	20
5.4	Priradenie VLAN k portom	21
5.5	Aktivácia podpory IPv6 protokolu na rôznych zariadeniach	22
5.6	Konfigurácia statických ciest	22
5.7	Konfigurácia RIP a RIPng	23
5.8	Konfigurácia DHCP servera	24

Kapitola 1

Úvod

Pri konfigurácii aktívnych sieťových prvkov vznikajú správcovi siete rôzne problémy spojené s dokumentáciou. Je potrebné ju zložito vyhľadávať na stránkach výrobcov daných zariadení, často je písaná neprehľadne a hľadanie konkrétnej časti, zaberá veľké množstvo času. Taktiež tento proces sťažuje aj fakt, že v sieti zvyčajne nevyužívame všetky vlastnosti zariadenia, ktoré sú popísané v dokumentácii. Pri používaní sa v niektorých zariadeniach môže objaviť nedokumentované správanie. Ide o drobnosti, ktoré by mohli mať fatálne následky. Aby sme sa im vyhli tak je potrebné udržiavať svoje vlastné poznatky o zariadeniach.

Tento problém rozširuje aj vyhľadávanie v dokumentácii od viacerých výrobcov, kde sa administrátori stretávajú s ďalšími ťažkosťami. Každý výrobca má vlastný štýl a štruktúru dokumentov, popis syntaxe príkazov a vlastné rozdelenie do kategórií. Taktiež výrobcovia poskytujú dokumentáciu v jednom niekoľkotisíc stranovom dokumente. Druhý extrém predstavuje vytvorenie novej podstránky pre každý konfiguračný príkaz zvlášť, ktorá vysvetľuje jeho syntax a použitie. Veľká väčšina výrobcov neposkytuje popis, čo zadanie konkrétneho príkazu vykoná. Popisujú len syntax, čo spôsobuje zdržanie, keď je potrebné v iných dokumentoch vyhľadávať funkcionality.

Takisto každý správca pozná spravidla dobre jednu platformu a občas potrebuje použiť, prípadne otestovať inú. V tom prípade by sa mu zišiel nejaký rýchly návod na jednotlivé konfigurácie, prípadne testy.

Riešenie predstavuje vytvorenie internej dokumentácie, v ktorej bude popis jednotlivých zariadení, použitých v sieti. V tomto dokumente budú popísané len vlastnosti, ktoré sa typicky využívajú v sieti, popis ich konfigurácie, činnosti, testovania funkčnosti a poznatky o neštandardnom správaní. Bude mať jednotnú štruktúru a štýl, čo značne uľahčí prácu s vyhľadaním informácie.

Najvhodnejšiu možnosť pre takúto dokumentáciu predstavuje webový systém, ktorý by umožňoval prístup odkiaľkoľvek, rýchle prehliadanie a vyhľadávanie, jednoduché pridávanie a editáciu informácií. Vytvorenie len textového dokumentu by nebolo dostatočne flexibilné.

V druhej kapitole sa zaoberáme popisom spôsobu konfigurácie jednotlivých zariadení, rozdielmi medzi výrobcami.

V ďalšej kapitole prechádzame popis jednotlivých Wiki systémov pričom si priblížime jednotlivé kritéria ich výberu.

V kapitole štyri riešime návrh vhodnej štruktúry pre dokumentáciu.

V piatej kapitole analyzujeme napoužívané príklady konfigurácií zariadení jednotlivých výrobcov.

V závere zhrnieme výhodnosť novej dokumentácie pre správcov siete.

Kapitola 2

Techniky konfigurácie aktívnych sieťových prvkov

2.1 Webové rozhranie

Webové rozhranie poskytuje väčšina výrobcov. V prípade lacnejších zariadení, určených pre domácnosti je to preferovaný spôsob konfigurácie, pretože sa nevyžadujú pokročilejšie znalosti o operačnom systéme. Niektorí výrobcovia neimplementujú do webového rozhrania možnosť na nastavenie všetkej funkčnosti, takmer vždy ponúka len obmedzené konfiguračné možnosti. Komplikovanejšie konfigurácie je často jednoduchšie nastaviť cez terminál, ako preklikávaním. Hlavnou výhodou webového rozhrania je možnosť poskytnutia grafického náhľadu na jednotlivé štatistiky o zariadení, o stave služieb a vyťažení. Avšak tieto informácie je možné získavať aj pomocou systému, ktorý bude centralizovane zbierať údaje o všetkých zariadeniach v sieti cez protokol SNMP. Často je potrebné v zariadeniach vykonať prvotnú konfiguráciu cez terminál, v ktorej je nutné aktivovať webové rozhranie, nastaviť užívateľov a heslá pre prístup. Pre pokročilejších užívateľov je to však menej výhodný spôsob, preto sa touto možnosťou nebudeme nezaoberať.

2.2 SNMP

SNMP(Simple Network Management Protocol) [3] je štandardizovaný protokol, vytvorený pre manažment zariadení na IP sieťach. Pôvodne vytvorený pre konfiguráciu, ale v praxi sa za týmto účelom používa skôr obmedzene. Jeho momentálne hlavné využitie predstavuje získavanie informácií o stave zariadení pre účely monitorovania siete. Konfigurovanie zariadenia je vhodnejšie robiť cez terminálový vstup. Taktiež je nutná prvotná konfigurácia cez terminál na aktiváciu a nastavenia SNMP agenta na zariadení. K SNMP sú dostupné rôzne grafické nástroje pre správu sietí. Tento variant ďalej nerozvíjame.

2.3 Terminál(CLI)

Aktívne prvky určené pre firemné siete a siete poskytovateľov internetu, poskytujú terminálové rozhranie(príkazový riadok) pre konfiguráciu. Ponúka všetky konfiguračné možnosti zariadenia. Avšak rôznorodá syntax zariadení spôsobuje problémy, pretože správcovia sú väčšinou zvyknutí pracovať s jednou až dvomi platformami zariadení. Správcovia sietí preferujú tento spôsob a budeme sa mu v práci ďalej venovať. Tak je možné zariadenie kon-

figurovať, buď cez fyzické pripojenie ku konzolovému portu na prvku, alebo cez vzdialené pripojenie pomocou Telnetu či SSH(secure shell). (Spravidla možnosť Telnetu a SSH je nutné najprv nastaviť cez konzolu.)

Väčšina výrobcov využíva pri konfigurácii rozdelenie do sekcií a podsekcií, resp. módov. Pri konfigurácii je potrebné sa dostať do privilegovaného módu, ktorý umožňuje zobrazovať stav zariadenia a jeho nastavenie, následne do konfiguračného módu kde je možné ich už nastavovať. Na jednotlivé módy sa môžu vzťahovať rôzne bezpečnostné mechanizmy ako prístup len pre určitých užívateľov či znalosť hesla. Konfiguračný mód má podsekcie, v ktorých sa nastavujú jednotlivé vlastnosti. Napríklad sekcia pre smerovanie, nastavenie rozhrania, vzdialeného prístupu, bezpečnosti a filtrovania atď. Platnosť zadávaných príkazov, sa vzťahuje len na danú sekciu, nezasahuje do ostaných. Je to výhodné riešenie, pretože nevypisujeme dlhé príkazy a nedochádza k veľkému počtu chýb.

Nasledujúce príklady konfigurácie boli vytvorené podľa oficiálnych dokumentácií výrobcov Cisco[4], H3C[13, 17], EdgeCore[12] a Juniper[8].

<code>enable</code>	Vstup do privilegovaného módu
<code>configure terminal</code>	Vstup do konfiguračného módu
<code>interface vlan 1</code>	Vstup do sekcie pre konfiguráciu rozhrania VLAN 1
<code>ipv6 address FD00::1/64</code>	Nastavenie IPv6 adresy na rozhranie VLAN 1

Tabuľka 2.1: Príklad konfigurácie IPv6 adresy na prvku Cisco 2960G

<code>system-view</code>	Vstup do konfiguračného módu
<code>interface vlan 1</code>	Vstup do sekcie pre konfiguráciu rozhrania VLAN 1
<code>ipv6 address FD00::1/64</code>	Nastavenie IPv6 adresy na rozhranie VLAN 1

Tabuľka 2.2: Príklad konfigurácie IPv6 adresy na prvku HP/H3C A5120-EI

<code>enable</code>	Vstup do privilegovaného módu
<code>config terminal</code>	Vstup do konfiguračného módu
<code>interface vlan 1</code>	Vstup do sekcie pre konfiguráciu rozhrania VLAN 1
<code>ipv6 address FD00::1/64</code>	Nastavenie IPv6 adresy na rozhranie VLAN 1

Tabuľka 2.3: Príklad konfigurácie IPv6 adresy na prvku EdgeCore 4626

Ako je vidieť na príkladoch v tabuľke 2.1, 2.2 a 2.3, výrobcovia majú minimálne rozdiely v delení konfigurácie do sekcií. Pomocou tohto rozdelenia je vhodné vytvoriť aj model štruktúry pre našu dokumentáciu, lebo pokryje takmer všetkých výrobcov.

Na druhej strane existujú aj výrobcovia, ktorí uprednostňujú dlhé príkazy. Napríklad JUNIPER, kde je možné priamo z globálneho konfiguračného módu zadať nastavenia detailov bez nutnosti vstupovať do podsekcií. Zápis je komplikovanejší a menej prehľadný, ako ukazuje príklad v tabuľke 2.4.

V prípade zložitejších konfigurácií je podobnosť syntaxe menšia. Príkladom môžu byť access listy pre filtráciu dátového toku na jednotlivých platformách. U každého výrobcu sú

<code>configure</code>	Vstup do konfiguračného módu
<code>set interfaces vlan unit 1 family inet6 address FD00::1</code>	Nastavenie IPv6 adresy na rozhranie VLAN 1

Tabuľka 2.4: Príklad konfigurácie IPv6 adresy na prvku Juniper EX4200

rozdiely v syntaxi, ale hlavným problémom je, že každý výrobca podporuje iné možnosti filtrácie. Pri lacnejších zariadeniach nie je možné využívať pokročilé filtrovacie funkcie.

<code>ipv6 access-list acl-ipv6</code>	Vytvorenie ACL s názvom <code>acl-ipv6</code>
<code>deny ipv6 FD00::/64 any</code>	Nastavenie blokovacieho pravidla
<code>permit icmp any any router-advertisement</code>	Povolovacie pravidlo pre špecifický typ ICMP správy
<code>exit</code>	Výstup z módu ACL
<code>interface vlan 1</code>	Výber rozhrania
<code>ipv6 traffic-filter acl-ipv6 in</code>	Umiestnenie pravidiel na rozhranie vo vstupnom smere

Tabuľka 2.5: Príklad konfigurácie ACL na prvku Cisco 2960G

V tabuľkách 2.5, 2.6 a 2.7 sú uvedené príklady konfigurovania filtrácie na sieťových rozhraniach pre jednotlivé platformy. Príklad zahŕňa vytvorenie filtra s pomenovaním, pridanie dvoch pravidiel, prvé ktoré bude blokovať IPv6 komunikáciu prichádzajúcu z adries začínajúcich na `FD00::` a druhé povolí všetky ICMPv6 správy prichádzajúce odšadiaľ, ktoré nesú informáciu o smerovači (RA – Router Advertisement). Na konci filtra je implicitne pridané pravidlo, ktoré blokuje všetky ostatné prichádzajúce pakety. Ďalšou časťou príkladu je umiestnenie filtra na požadované rozhranie v smere do zariadenia.

<code>acl ipv6 number 3000 name acl-ipv6</code>	Vytvorenie ACL s názvom <code>acl-ipv6</code>
<code>rule deny ipv6 source FD00::/64 destination any</code>	Nastavenie blokovacieho pravidla
<code>rule permit icmpv6 source any destination any icmp6-type router-advertisement</code>	Povolovacie pravidlo pre špecifický typ ICMP správy
<code>quit</code>	Výstup z módu ACL
<code>interface vlan 1</code>	Výber rozhrania
<code>packet-filter ipv6 name acl-ipv6 inbound</code>	Umiestnenie pravidiel na rozhranie vo vstupnom smere

Tabuľka 2.6: Príklad konfigurácie ACL na prvku HP/H3C A5120-EI

Ako vidieť v príkladoch, konfigurácie pre jednotlivé zariadenia obsahujú množstvo malých odlišností, kde napríklad je len jedno kľúčové slovo navyše, alebo je inak zapísané, prípadne je zmenené ich poradie. Tým pádom sú jednotlivé konfiguračné príkazy komplikované na zapamätanie pre viac zariadení naraz. Napríklad pri konfigurácii zariadenia H3C A5120-EI (tabuľka 2.6), sa vyžaduje aj číselné zadanie filtra, ale ostatné zariadenia si vyčia len so slovným zadaním názvu. Taktiež je nutné explicitne zadávať v jednotlivých

pravidlách či ide o zdroj alebo cieľ, kde ostatné zariadenia vyžadujú presné dodržanie postupnosti. Úplne rozdielne je už aplikovanie pravidiel na jednotlivé rozhrania, tam má každé zariadenie vlastný postup.

<code>ipv6 access-list extended acl-ipv6</code>	Vytvorenie ACL s názvom <code>acl-ipv6</code>
<code>deny FD00::/64 any-destination</code>	Nastavenie blokovacieho pravidla
<code>permit icmp any-source any-destination 134 0</code>	Povolovacie pravidlo pre špecifický typ ICMP správy
<code>exit</code>	Výstup z módu ACL
<code>interface vlan 1</code>	Výber rozhrania
<code>ipv6 access-group acl-ipv6 in</code>	Umiestnenie pravidiel na rozhranie vo vstupnom smere

Tabuľka 2.7: Príklad konfigurácie ACL na prvku EdgeCore 4626

Nanešťastie s každým novým hlavným vydaním operačného systému pre zariadenie, je možné, že dôjde k úprave syntaxy niektorých súčastí. V tom prípade bude potrebné vytvoriť dokumentáciu pre viac verzií. Avšak takáto zmena sa nedeje často a býva minoritná.

Výhodou terminálu je že prijíma klasický neformátovaný textový vstup. Teda vo wiki dokumentácií je možné si vytvoriť textovú šablónu pre zariadenie, v ktorej len nahradíme implicitné hodnoty vlastnými a tento výsledný text priamo nakopírujeme do terminálu. Výsledok je totožný, ako keby píšeme priamo, ale menej chybný a omnoho rýchlejší.

Kapitola 3

Wiki systémy

Vhodné riešenie pre vytvorenie online dokumentácie predstavuje wiki systém. Wiki [22], ako webová stránka, umožňuje prostredníctvom webového prehliadača pridávať, meniť a odstraňovať obsah, kooperáciu viacerých užívateľov. S týmto zameraním sú presne určené k tomu, čo potrebujeme. Wiki systémov je veľký počet a zároveň sú profesionálne spracované. Obsahujú množstvo rozšírení overených veľkým počtom používateľov. Mnoho profesionálnych wiki systémov je dostupných ako freeware [19].

Vhodný nástroj na porovnanie jednotlivých wiki aplikácií predstavuje webová aplikácia wikiwizard.org. Ponúka detailný rozpis vlastností wiki systémov a umožňuje porovnávanie medzi nimi [1].

V dodatku A sa nachádzajú screenshoty jednotlivých popisovaných wiki.

3.1 Požiadavky na wiki systém

Systém musí automaticky generovať obsah na stránkach, obsahovať správu užívateľov, umožňovať prístup viacerých používateľov s vyžadovaným prihlásením a poskytovať zamedzenie možnosti upravovať obsah anonymným alebo neprihláseným užívateľom. Vyžaduje sa udržiavanie histórie zmien v obsahu jednotlivých stránok, aby sa zamedzilo neželanému odstráneniu alebo znehodnoteniu informácií uvedených na stránkach. Mal by ďalej umožňovať fulltextové vyhľadávanie obsahu, jednoduchú navigáciu medzi podstránkami, vytváranie menu a pridanie navigačnej lišty. Splnenie týchto podmienok je dôležité, pretože cieľom aplikácie je rýchle vyhľadávanie požadovaných informácií.

Syntax pre vkladanie a formátovanie by mala byť jednoduchá, ľahko zapamätateľná, výhodou by bol vstavaný WYSIWYG editor. Systém by nemal užívateľa nútiť používať HTML, ale na druhej strane mal by znalým používateľom umožňovať jeho používanie spolu so základmi štýlovania.

3.2 MediaWiki

MediaWiki je voľne dostupné serverové riešenie pod GNU GPL licenciou, vytvorené v jazyku PHP[18]. Na tomto riešení je postavená aj Wikipedia, najväčšia slobodná encyklopédia.

- Pre svoju činnosť systém potrebuje databázu, podporuje MySQL, PostgreSQL, Oracle a SQLite databázové systémy,
- lokalizácia do 140 jazykov, vrátane češtiny a slovenčiny,

- široká používateľská základňa,
- možnosť pridať ako rozšírenie WYSIWYG editor,
- veľké množstvo dostupných doplnkov,
- uchovávanie a zobrazovanie histórie,
- nelimitovaný počet revízií stránok,
- index stránok a menné priestory,
- fulltextové vyhľadávanie,
- podpora vybraných HTML tagov,
- poznámky pod čiarou,
- stránky je možné editovať po sekciách,
- možnosť exportu stránok, po pridaní doplnku aj ako PDF formát,
- možnosť pridávania súborov, udržiava ich revízie,
- prehľadná syntax.

3.3 DokuWiki

System, vydaný pod GNU GPLv2 licenciou [11], je vytvorený v PHP a nepotrebuje k svojej činnosti databázu. Všetky dáta sú uložené v súborovom systéme.

- System je lokalizovaný do 55 jazykov, vrátane slovenčiny a češtiny,
- možnosť pridať ako rozšírenie WYSIWYG editor,
- viac ako 750 dostupných doplnkov,
- nelimitovaný počet revízií stránok,
- index stránok a menné priestory,
- fulltextové vyhľadávanie,
- predchádza konfliktom zamykaním stránok,
- nepodporuje priamo HTML tagy, ale umožňuje vložiť do stránky celý HTML a PHP kód, po aktivácii tejto funkčnosti v nastaveniach,
- podpora poznámok pod čiarou,
- podpora pomocou doplnku aj pre mobilnú verziu,
- stránky je možné editovať po sekciách,
- export stránok po nainštalovaní doplnku aj export PDF formátu,
- umožňuje pridávanie súborov, ale neudržiava ich revízie,
- syntax jednoduchá, avšak menej prehľadná, neumožňuje nastavenia odsadenia a zarovnania textu (až po nainštalovaní doplnku).

3.4 PmWiki

System je vydaný pod GNU GPLv2 licenciou. Vytvorený je v PHP, nepotrebuje pre svoju činnosť databázu, dáta jednotlivých stránok sú uložené v súboroch [20].

- Po nainštalovaní doplnkov možnosť ukladať dáta do MySQL alebo SQLite databázy,
- lokalizácia do 38 jazykov, vrátane slovenčiny a češtiny,
- dostupnosť širokej škály vzhľadov rozhrania a ich jednoduchá aplikácia,
- neposkytuje pohodlné nastavenia, veľká väčšina konfigurácií sa vykonáva manuálne v konfiguračnom súbore,
- možnosť pridať ako rozšírenie WYSIWYG editor,
- nelimitovaný počet revízií stránok,
- index stránok a menné priestory,
- fulltextové vyhľadávanie,
- nepodporuje HTML tagy (podpora niektorých tagov sa získa nainštalovaním doplnku),
- pre poznámky pod čiarou vyžaduje doplnok,
- stránky nie je možné natívne editovať po sekciách, je nutné nainštalovať doplnok,
- pre export stránok je potrebné nainštalovať doplnky,
- nahrávanie súborov musíme najprv nastaviť a aktivovať v konfigurácii, neumožňuje vyhľadávanie súborov,
- nevýrazná syntax, ktorá ľahko splynie s textom.

3.5 WikkaWiki

System vydaný pod GNU GPL licenciou. Vytvorený v PHP, potrebuje databázu pre svoju činnosť [23].

- Podporuje len MySQL databázový systém,
- lokalizácie neobsahujú slovenčinu ani češtinu, systém je lokalizovaný len do 4 jazykov,
- možnosť pridať ako rozšírenie WYSIWYG editor,
- nelimitovaný počet revízií stránok,
- index stránok a menné priestory,
- fulltextové vyhľadávanie,
- predchádza konfliktom zamykaním stránok,
- podpora niektorých HTML tagov,

- pre poznámky pod čiarou potrebuje doplnok,
- nepodporuje editáciu po sekciách,
- pre export HTML vyžaduje doplnok, nepodporuje export vo formáte PDF,
- umožňuje nahrávanie súborov, neudrzuje ich revízie,
- nepodporuje vyhľadávanie v súboroch,
- zložitá a neprehľadná syntax využívajúca prvky HTML tagov v kombinácií so špeciálnymi znakmi.

3.6 Ostatné wiki systémy

Nevenovali sme sa v práci prieskumu komerčným (plateným) wiki systémom. Mnohé z nich nájdeme aj vo verziách zadarmo. Avšak často sú odstránené základné komponenty pre funkčnosť, ktorú požadujeme, ako napríklad tímová kooperácia (Twiki systém [21]).

Popri systémoch, ktoré môžeme nainštalovať na vlastný server, sú dostupné aj on-line riešenia. Po registrácii môžeme založiť vlastnú wiki. Nevýhoda spočíva v tom, že wiki sídli na doméne, ktorá nepatrí nám a oproti systémom, určeným na inštaláciu na server, jej chýbajú rôzne nástroje. V prípade bezplatnej on-line wiki sa stanovuje limit na veľkosť a počet užívateľov. Čo sa týka platených online systémov, cena vyjde vyššie, ako keby si zakúpime vlastný webhosting a sami nainštalujeme voľne dostupnú wiki, založenú na PHP jazyku.

Ostatné wiki systémy neponúkajú dostatočné možnosti, majú slabú podporu, prípadne sú to len začínajúce projekty alebo málo rozvinuté a ukončené projekty.

3.7 Výber wiki systému

Vlastnosti[2]	Wikimedia	DokuWiki	PmWiki	WikkaWiki
správa užívateľov	áno	áno	áno	áno
len neanonymný prístup	áno	áno	áno	áno
história zmien	áno	áno	áno	áno
upload súborov	áno	áno	voliteľné	áno
fulltextové vyhľadávanie	áno	áno	áno	áno
konflikty na stránke	rozriešenie	zamykanie	rozriešenie	zamykanie
generovanie obsahu	áno	áno	áno	áno
syntax wiki	jednoduchá	jednoduchá	splýva s textom	zložitá
editácia po sekciách	áno	áno	doplnok	nie
vkladanie HTML tagov	niektoré	voliteľné	doplnok	niektoré
tabuľky	áno	len jednoduché	áno	áno
WYSIWYG editor	doplnok	doplnok	doplnok	doplnok
PDF export	doplnok	doplnok	doplnok	nie

Tabuľka 3.1: Požadované vlastnosti jednotlivých wiki systémov

Podľa tabuľky 3.1 všetky skúmané wiki systémy spĺňajú základné kritéria takmer na rovnakej úrovni.

Pre implementáciu sme vybrali systém MediaWiki. V sumári splnil zo všetkých systémov naše požiadavky najlepšie. Prednosťou je hlavne editovanie stránky po sekciách, ktoré implicitne dva systémy ani nemajú. Pri takých obsiahlych dokumentoch ako dokumentácia by bolo nereálne jednoducho upravovať obsah. Syntax systému je tiež najvhodnejšia zo všetkých skúmaných systémov. Je to najrozšírenejší, neustále vyvíjaný a podporovaný systém. Tým nám odpadajú problémy s neriešenými bezpečnostnými zraniteľnosťami. Má najširšiu ponuku doplnkov, čo je výhodné do budúcnosti, ak by sme chceli systém rozširovať o novú funkcionality. Ak by požadovaný doplnok nejestvoval pre MediaWiki systém, s veľkou pravdepodobnosťou by ho nemali ani ostatné systémy. Taktiež sú hlavné doplnky vytvorené na vynikajúcej úrovni. Má dobrý a prehľadne napísaný užívateľský aj technický manuál. Odporúčajú ho mnohí používatelia, ktorí s ním majú dobré skúsenosti.

Kapitola 4

Štruktúra dokumentácie

V štruktúre sme uvažovali nad dvomi možnosťami, ako spojiť jednotlivé zariadenia a konfigurácie. Prvou možnosťou bolo pre každú vlastnosť vytvoriť zoznam zariadení a k nim prislúchajúce konfigurácie. Druhou možnosťou bolo vytvoriť zoznam zariadení, pričom ku každému zariadeniu sa vytvorí stránka s kompletnou dokumentáciou. Pre implementáciu sme vybrali druhú možnosť, pretože je prehľadnejšie mať všetky konfigurácie pre jedno zariadenie, ktoré aktuálne konfigurujeme na jednom mieste, ako zložito vyhľadávať. Zriedkavo sa stáva, že by bolo potrebné nastaviť jednu vlastnosť na všetkých zariadeniach, no i tak sa jedna vlastnosť vyhľadá ľahšie, ako v prípade nového nenakonfigurovaného zariadenia, kde je potrebné nastavovať postupne všetky vlastnosti a neustále vyhľadávať konfigurácie. Z implementačného hľadiska vidíme ďalšiu výhodu pri exporte z wiki systému, kde bude možnosť exportovať pre konkrétne zariadenie všetky návody konfigurácie.

Dokumentácia je rozdelená do štyroch základných častí.

- Základné nastavenia,
- konfigurácia data-linkovej vrstvy – prepínače,
- konfigurácia sieťovej vrstvy – smerovače,
- ďalšie služby.

V kategórii základných nastavení sú uvedené konfigurácie pre nastavenie prístupu užívateľov, nastavenie zabezpečenia zariadenia, nastavenie vzdialeného prístupu a logovania. Ďalej je to údržba zariadenia a manažment súborového systému, aktualizácie firmvéru, základné príkazy špecifické pre zariadenie(**undo**, **do**, **exit**, **quit**, **set**). Táto časť je spoločná pre všetky typy zariadení.

Ďalšie kategórie sa nedajú jednoznačne rozdeliť podľa zariadení, pretože tie môžu byť kombináciou viacerých jednoduchších prvkov. Napríklad L3 prepínače, ktoré majú vlastnosti smerovačov alebo pokročilé smerovače, ktoré sa dajú nakonfigurovať na určitých portoch ako prepínače. Z toho dôvodu sa rozdeľujú do kategórií podľa vrstiev OSI modelu. Pre datalinkovú vrstvu(druhá vrstva) sú vybrané konfigurácie L2 protokolov (Ethernet, 802.1q, PPP, HDLC, Frame Relay), nastavenia na úrovni portov, zabezpečenie portov, vytváranie virtuálnych LAN sietí, filtrovanie na základe MAC adries. Väčšina nastavení pokrýva práve prepínač, ale samozrejme nastavenia na úrovni L2 je potrebné robiť aj na smerovačoch.

Pre sieťovú vrstvu(tretia vrstva) sú konfigurácie IP a IPv6 protokolu, nastavenia smerovania, filtrácia dátového toku. Konfigurácie sa týkajú hlavne smerovačov.

V poslednej kategórii sa nachádzajú konfigurácie pre služby vyšších vrstiev, hlavne aplikáčnej vrstvy a služby, ktoré poskytujú výrobcovia nad rámec požiadaviek štandardov. Taktiež sú v tejto sekcii príkazy na overenie nastavenia a debugovanie zariadenia, formát príkazov `ping`, `ping6`, `traceroute` a ďalších pre overenie funkčnosti zariadenia.

Úplný rozpis štruktúry je možné nájsť v dodatku B.

4.1 Popis formátu syntaxe v dokumentácii

Z dôvodu, že každý výrobca používa v dokumentácii vlastný formálny popis syntaxe, sme pre vlastné potreby zjednotili pravidlá popisu. Vychádzajú z najčastejšie používaných formátov u výrobcov, zobrazuje ich tabuľka 4.1. Tieto pravidlá budú použité v našej dokumentácii.

klúčové slovo	Musí sa povinne vyskytnúť v príkaze
[klúčové slovo]	Voliteľná možnosť výskytu
{ klúčové slovo 1 klúčové slovo 2 ... }	Povinný výber jedného
{ [klúčové slovo 1] [klúčové slovo 2] ... }	Povinný výber minimálne jedného
<hodnota>	Používateľom špecifikovaná hodnota
[<hodnota>]	Nepovinná hodnota špec. používateľom
{ hodnota 1 hodnota 2 ... }	Povinný výber jednej z hodnôt

Tabuľka 4.1: Formát syntaxe v dokumentácii.

Napríklad zápis pre konfiguráciu IPv6 adresy na rozhraní môže vyzeráť následne,

```
ipv6 address { <ipv6-address>/<prefix> | <ipv6-address> <prefix> } [eui-64]
```

znamená to, že môžeme adresu zadať dvomi spôsobmi a to buď ako `ipv6 address FD00::/64`, alebo `ipv6 address FD00:: 64`. Voľba `eui-64` je voliteľná, takže mohli by sme adresu zapísať v tvare aj ako `ipv6 address FD00::/64 eui-64`, respektíve v druhom formáte ako `ipv6 address FD00:: 64 eui-64`.

4.2 Zápis konfigurácie

V konfiguračných manuáloch jednotlivých zariadení, sú konfiguračné príklady zapísané v útržkoch, tj. popisujú aktuálny príkaz, kde je v popise uvedený mód, v ktorom sa daný príkaz konfiguruje, ale už tam nieje popísaný spôsob ako sa do tohto módu dostať. To spôsobuje ďalšie zdržanie, keď je nutné ďalej hľadať v dokumentácii, ako sa k danému módu dostať.

V našej dokumentácii je uvedená celá cesta ako nakonfigurovať danú vlastnosť. Je možné, že občasne bude takýto zápis zbytočne dlhý, ale vychádzame z toho že naša dokumentácia je určená pre správcov siete, ktorí nekonfigurujú pravidelne dané zariadenie, a tak je pre nich pohodlnejšie, keď nemusia hľadať cestu, ako sa dostať do daného konfiguračného podmódu. Správca, ktorý pravidelne konfiguruje jeden typ zariadení pravdepodobne nebude potrebovať túto našu dokumentáciu. Aby sa predišlo zbytočnému opakovaniu sledu príkazov zaisťujúcich vstup do konfiguračného podmódu, tak tento popis bude uvedený len na začiatku každej sekcie v dokumentácii, čo je možné rýchlejšie vyhľadať v prípade potreby, ako v oficiálnej referenčnej príručke príkazov od výrobcu, kde je takýto postup uvedený len v niektorej začiatkovej kapitole.

1. Enable DHCP Snooping

Command	Explanation
Globe mode	
ip dhcp snooping enable no ip dhcp snooping enable	Enable or disable the dhcp snooping function

2. Enable DHCP Snooping binding

Command	Explanation
Globe mode	
ip dhcp snooping binding enable no ip dhcp snooping binding enable	Enable or disable the dhcp snooping binding function

Tabuľka 4.2: Ukážka konfigurácie v manuáli výrobcu pre zariadenie EdgeCore

V tabuľke 4.2 je uvedený výsek príkladu konfigurácie pre zariadenie EdgeCore podľa popisu v manuáli od výrobcu[12]. Jasne vidíme, že je tam zadaný len názov konfiguračného módu, v ktorom je potrebné príkazy aplikovať, teda následne v prípade potreby musíme prísť do tohto módu nájsť v inej časti dokumentácie.

Enable DHCP Snooping Enable the dhcp snooping function enable config [terminal] ip dhcp snooping enable	Je zobrazená celá cesta, ako nakonfigurovať požadovanú vlastnosť
Enable DHCP Snooping binding Enable the dhcp snooping binding function ip dhcp snooping binding enable	Príkaz odsadením určuje, že patrí do daného konfiguračného podmódu

Tabuľka 4.3: Ukážka konfigurácie pre zariadenie EdgeCore v našej dokumentácii

Tento úsek konfigurácie bol prevedený do formy zápisu v našej dokumentácii a je zobrazený v tabuľke 4.3. Vynechali sme zápis `no ip dhcp snooping enable`, ktorý ruší dané nastavenie, pretože zápis rušenia je pre všetky konfigurácie rovnaký a jeho syntax bude popísaná na začiatku dokumentácie. V špeciálnych prípadoch môže byť príkaz zapísaný univerzálne ako `[no] ip dhcp snooping enable`, čo by ale nemalo nastávať často.

Príkaz konfigurácie druhej vlastnosti v poradí je odsadený na úroveň podmódu, ku ktorému prislúcha. Týmto je jednoznačne pochopiteľné, kam daný príkaz patrí a netreba vypisovať znovu sled príkazov, ktoré nás dostanú do potrebného módu. Stačí len pozrieť o pár riadkov vyššie, kde je uvedená celá cesta.

Kapitola 5

Analýza vybraných konfigurácií zariadení

V tejto kapitole sa budeme venovať niektorým vybraným príkladom konfigurácie zariadení od rôznych výrobcov. Zameriame sa hlavne na často používané konfigurácie a tiež tie, ktoré sú podstatne odlišné u rôznych výrobcov.

Jednotlivé konfigurácie boli odvodené z oficiálnych dokumentácií výrobcov Cisco[4, 5, 6, 7, 9, 10], H3C[14, 15, 16, 17] a EgdeCore[12].

5.1 Základné nastavenia

Táto časť konfiguračnej dokumentácie pokrýva všetky typy zariadení. Všetky typy zariadení, ktoré majú spoločné charakteristiky, ako je rozdelenie do konfiguračných módov, nastavovanie hesiel, autorizácie a zabezpečenia, nastavenie vzdialeného prístupu či spravovanie aktuálnej konfigurácie. S bezpečnosťou samozrejme súvisí aj nastavenie monitorovania zariadenia cez SNMP protokol a postup inštalácie bezpečnostných aktualizácií. Bez znalosti týchto základných nastavení je len ťažko zvládnuteľné nakonfigurovať správne a bezpečne sieťové zariadenie.

5.1.1 Základné príkazy

Nevyhnutnou súčasťou pri každej konfigurácii sa stávajú základné príkazy. Tieto príkazy zaisťujú pohyb medzi konfiguračnými módami, tj. vstup do vyššej úrovne a výstup z vyššej úrovne, umožňujú zrušenie niektorej časti konfigurácie alebo jej zobrazenie. Do tejto časti sme ďalej zaradili aj uloženie aktuálnej konfigurácie, čo je veľmi často používaný príkaz.

	Cisco	H3C	EdgeCore
Vstup do privilegovaného módu	enable		enable
Vstup do konfiguračného módu	configure	system-view	config
Zrušenie príkazu	no <stmt>	undo <stmt>	no <stmt>
Návrat do vyššej úrovne	exit	quit	exit
Návrat z konf. módu	end	return	end
Zobrazenie nastavení	show <stmt>	display <stmt>	show <stmt>

Tabuľka 5.1: Základné príkazy pre Cisco, H3C a EdgeCore

Ako vyplýva z tabuľky 5.1, tak príkazy zariadení Cisco a EdgeCore sú takmer totožné, na rozdiel od zariadení H3C, pri ktorých je základná syntax úplne odlišná. Táto priveľká odlišnosť spôsobuje dosť nepríjemností pri konfigurovaní dvoch rôznych zariadení s takto odlišnou základnou syntaxou.

5.1.2 Konfiguračné módy

Takmer všetci výrobcovia oddeľujú jednotlivé príkazy do rôznych úrovní, módov, ktoré umožňujú rozdeliť zobrazovanie konfigurácie od možnosti zadávať nejaké nové nastavenia. Vstup do módu s vyššími právomocami môže podliehať napríklad znalosti hesla, prípadne môže byť obmedzený na základe užívateľa.

Najbežnejším rozdelením u výrobcov sieťových zariadení je rozdelenie do troch základných módov. Sú to užívateľský, administratívny a globálny konfiguračný mód.

Užívateľský mód je základná úroveň dostupná užívateľovi po prihlásení do zariadenia, dovoľuje minimálny počet príkazov a to hlavne príkazy umožňujúce overovať konektivitu k ďalším zariadeniam, ako je napríklad `ping` a `traceroute`, získanie informácií o zariadení, jeho stav a verziu softvéru. Ďalej umožňuje užívateľovi použiť zariadenie, ako most k vzdialenému prihláseniu, k inému zariadeniu v sieti. Napríklad, ak máme záujem konfigurovať zariadenie vo vnútri siete, ku ktorému nie je možný prístup z internetu, tak sa prihlásime do zariadenia na hranici našej siete a z neho vytvoríme nové pripojenie na zariadenie vo vnútri siete a to môžeme konfigurovať, ako keby sme pripojení priamo. Tento mód neumožňuje vykonávať konfigurácie. Do vyššieho módu je najčastejšie možné sa dostať až po zadaní hesla. (Toto heslo je samozrejme odlišné od užívateľského hesla pre prihlásenie sa do zariadenia.)

Administratívny mód obsahuje všetky príkazy k zobrazeniu konkrétnych nastavení zariadenia, prácu so súborovým systémom, nástroje na odlaďovanie konfigurácie(debug), nastavovanie času a ďalšie možnosti, ktoré nezasahujú priamo do nastavení sieťových funkcií zariadenia. Taktiež obsahuje všetky dostupné príkazy z nižšej úrovne. Pri prechode do konfiguračnej úrovne zvyčajne už nie je vyžadované heslo.

Cisco	H3C	EdgeCore
User EXEC	—	User
Priviledged EXEC	User-view	Admin
Global configuration	System-view	Global

Tabuľka 5.2: Konfiguračné módy pre Cisco, H3C a EdgeCore

Globálny konfiguračný mód umožňuje zadávať konfiguráciu zariadenia, najmä konfiguráciu spojenú priamo s výkonom činnosti zariadenia na sieti. Najčastejšie globálny konfiguračný mód umožňuje vstupovať do podmódov konfigurácie, ako napríklad konfigurácia rozhrania, smerovania, filtrácie a virtuálnych LAN sietí. Tento spôsob sprehľadňuje syntax a zjednodušuje konfiguráciu.

Zásadným rozdielom je možnosť využívania príkazov z administratívneho módu. Niektorí výrobcovia striktne zakážu možnosť využívať príkazy administratívneho módu v konfiguračnom, tým pádom konfiguračný mód slúži čisto ku konfiguráciám a nieje v ňom ani možné overiť správne zadanie konfigurácie. Iní výrobcovia umožňujú použitím špeciálneho kľúčového slova sprístupniť príkazy administratívneho módu. (Napríklad Cisco umožňuje použiť príkaz `do <statement>`, kde za kľúčovým slovom nasleduje príkaz z administratívneho rozhrania.) Posledným typom sú zariadenia, ktoré môžu používať v globálnom konfiguračnom

móde všetky príkazy administračného módu (napríklad od výrobcu H3C).

Upozorňujeme, že toto rozdelenie je len generalizovanie z väčšiny nám dostupných zariadení a u niektorých výrobcov sa môže zásadne líšiť.

5.2 Konfigurácia data-linkovej vrstvy

Tieto konfigurácie sa aplikujú hlavne na zariadeniach typu prepínač, ktorého hlavná funkcia spočíva práve v zaistení spojenia na data-linkovej vrstve. (Druhá vrstva ISO OSI modelu.) Časť týchto konfigurácií zariadení je aplikovateľná aj na smerovače, ktoré sú zariadeniami nadradenej vrstvy.

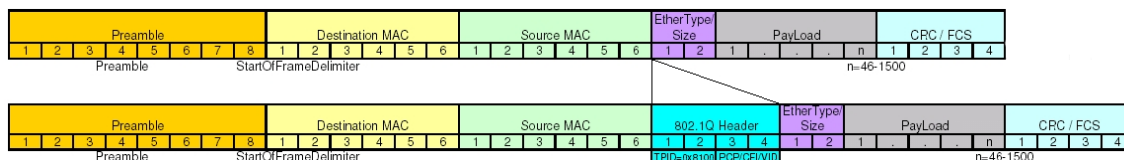
Medzi najdôležitejšie vlastnosti prepínačov patrí schopnosť vytvárať VLAN siete. Ďalšou špecifickou konfiguráciou tejto vrstvy je nastavenie fyzických portov zariadenia a k nim náležiacich protokolov. Pre rýchlu konvergenciu siete je potrebné ovládať niektoré špecifické nastavenia Spanning Tree Protokolu, ktorý zaisťuje bezslučkovosť siete na data-linkovej vrstve. Špeciálne na týchto zariadeniach je potrebné zaisťovať ochranu užívateľov pred bezpečnostnými hrozbami, ako sú falošné dhcp servery, neautorizovaný prístup do siete a pod. Túto ochranu zabezpečujú funkcie ako DHCP snooping, Router Advertisement/Neighbor Discovery guard a zabezpečenie portov pomocou filtrovania MAC adres.

5.2.1 VLAN siete

VLAN(Virtual Local Area Network) umožňuje vytvárať skupinu koncových zariadení s rovnakými požiadavkami, ktoré môžu komunikovať priamo na rovnakej broadcast doméne[10]. Zároveň táto technológia umožňuje, aby VLAN broadcast doména bola rozťahnutá na viac fyzických zariadení, tj. že koncové zariadenia pripojené k rozličným sieťovým prvkom môžu byť v rovnakej VLAN sieti. Keďže ide o dôležitú časť konfigurácie, tak budeme tejto časti venovať väčšiu pozornosť.

Tagovanie

Rozdelenie do VLAN sietí prebieha na základe tzv. tagovania rámcov. Najrozšírenejším protokolom pre tagovanie je v dnešnej dobe IEEE 802.1Q, ktorý vkladá do rámca svoju 4 bajtovú hlavičku, v ktorej je obsiahnuté 12 bitové pole určujúce identifikátor VLAN siete. Prvá a posledná hodnota sú rezervované pre špeciálne účely, z toho vyplýva, že dostupných je celkovo 4094 VLAN sietí. (Niektorí výrobcovia majú rezervovaných aj pár iných identifikátorov, napr. Cisco má špeciálny význam pre VLANy 1002 – 1005.)



Obr. 5.1: Tagovanie IEEE 802.1Q¹

¹Prevzaté z: http://upload.wikimedia.org/wikipedia/commons/2/23/TCPIP_802.1Q.jpg

V minulosti bolo možné na Cisco zariadeniach využívať aj privátny ISL(Inter-Switch Link) protokol k tagovaniu, ale momentálne samotný výrobca ho neodporúča nasadzovať do nových sietí a odporúča využiť štandard IEEE 802.1Q.

Vytvorenie VLAN siete

Pre vytvorenie novej VLAN siete je potrebné zadať jej identifikátor bez rozdielu, na akom zariadení ju konfigurujeme. Voliteľná možnosť je zadať aj popisné meno.

Tabuľka 5.3 zobrazuje postup pri vytvorení novej VLAN siete na jednotlivých zariadeniach a následné overenie vytvorenia tým, že sa zobrazí v zozname VLAN sietí. Ako je vidieť jednotlivé konfigurácie sú takmer totožné. Hlavný rozdiel je v zadaní názvu VLAN siete pri EdgeCore zariadeniach, kde v prípade záujmu musíme názov VLAN siete zadať už pri jej vytváraní a nie je ho možné neskôr zmeniť, zatiaľ čo Cisco a H3C zmenu názvu umožňujú. V prípade, že nezadáme názov VLAN siete, zariadenie automaticky vygeneruje názov obsahujúci jej identifikátor.

Cisco	H3C	EdgeCore
enable configure vlan 10 name test	system-view vlan 10 name test	enable config vlan 10 [name test]
enable show vlan	display vlan [all]	enable show vlan

Tabuľka 5.3: Vytvorenie a zobrazenie VLAN sietí

Nastavenie portov

Podstatným nastavením VLAN je priradenie fyzických portov zariadenia a nastavenie ich funkčnosti. Vzhľadom na VLAN môžeme rozdeliť funkčnosť portov do troch módov, a to access, trunk a hybrid, pričom nie všetky zariadenia podporujú všetky módy.

Access port sa využíva hlavne k pripojeniu koncových zariadení. Ethernetové rámce vychádzajúce z tohto portu sú netagované, tj. koncové zariadenie netuší v ktorej VLAN sa nachádza. Je to pre neho transparentné a nemusí riešiť príslušnosť k VLAN sieťam.

Trunk port zaisťuje prenos tagovaných rámcov, využíva sa pri prenose dát medzi dvomi aktívnymi prvkami, aby bola zachovaná príslušnosť rámcov k jednotlivým VLAN sieťam. Tieto trunk porty umožňujú nastaviť, ktoré VLAN rámce je možné prenášať daným portom. Špeciálnym prípadom je takzvaná natívna VLAN. Pre túto VLAN je možné určiť, že jej rámce budú cez trunk port ako jediné prenášané netagované.

Poslednou možnosťou je hybridný port, teda kombinácia oboch vyššie uvedených. Tento typ portu umožňuje nastaviť, pre ktoré VLAN siete sa majú rámce tagovať, tj. umožňuje narozdiel od trunk portu odosielať viac ako jednu netagovanú VLAN.

Tabuľka 5.4 znázorňuje príklad konfigurácie pridania portov do VLAN siete, a ich jednotlivé nastavenia do rôznych módov. Zámerne je z tabuľky vynechané zariadenie EdgeCore, ktorého syntax je totožná so syntaxou Cisco zariadení. Ako vidieť H3C ponúka viac možností ako nakonfigurovať access vlan, jednotlivé riadky sú označené hviezdíčkom (*). Pri trunk porte H3C neumožňuje nastavovať natívnu VLAN, ale poskytuje možnosť nakonfigurovať port ako hybridný a nastaviť požadovanú VLAN, aby sa netagovala. (Vid' príklad

Cisco	H3C
<pre>enable configure interface <ifname> switchport mode access switchport access vlan 10</pre>	<pre>system-view vlan 10 port <ifname> * quit interface <ifname> port link-type access port access vlan 10 *</pre>
<pre>switchport mode trunk switchport trunk allowed vl none switchport trunk allowed vl add 1, 10</pre>	<pre>port link-type trunk port trunk permit vlan 1 10</pre>
<pre>switchport trunk native vlan 1</pre>	
	<pre>port link-type hybrid port hybrid vlan 10 tagged port hybrid vlan 1 untagged</pre>

Tabuľka 5.4: Priradenie VLAN k portom

v tabuľke.) Zariadenia od Cisca ponúkajú viac možností ako nastaviť povolené VLAN na trunk porte, čím uľahčujú prácu a nie je potrebné zakaždým písať zoznam všetkých povolených VLAN sietí.

5.3 Konfigurácia sieťovej vrstvy

V tejto časti sa budeme zaoberať konfiguráciou IP a IPv6 adresácie, čo je podstatné pre každé sieťové zariadenie nezávisle od typu, ďalej špecializovanejšími konfiguráciami ako je smerovanie unicastu či multicastu, filtrácia dátového toku, ktoré sú hlavne výsadou smerovačov. Konfigurácie taktiež musia byť prispôbené k vzájomnej nekompatibilitate týchto protokolov.

5.3.1 Konfigurácia IP a IPv6 adres

Nevyhnutné nastavenie každého, či už koncového zariadenia, alebo aktívneho prvku v sieti, spočíva práve v konfigurácii IP adresy. V dnešnej dobe, keď je zásoba voľných blokov IP adres vyčerpaná, je potrebné ovládať aj konfiguráciu nastupujúceho IPv6 protokolu a jeho adresácie. Keďže sme vo fáze postupného prechodu na nové IPv6 služby využívaním hlavne Dual-stack mechanizmu (súbežné poskytovanie IP aj IPv6 služieb), tak je potrebné mať znalosti o oboch konfiguráciách.

Nanešťastie väčšina zariadení má implicitne vypnutú podporu IPv6 protokolu, a musíme ju povoliť vlastným zásahom do nastavení. Tabuľka 5.5 zobrazuje postup explicitného zapnutia podpory IPv6 na zariadeniach. Za poznámku stojí rozdielna konfigurácia pri Cisco zariadeniach, kde je rozdiel medzi konfiguráciou smerovača alebo L3 prepínača.

V niektorých prípadoch je potrebné, okrem globálneho zapnutia podpory IPv6, zapnúť podporu aj na jednotlivých fyzických rozhraniach zariadenia, inak neumožnia zadať IPv6 adresu. Najčastejšie to zaisťuje príkaz `ipv6 enable`, ale záleží na výrobcovi.

Samotné nastavenie IP a IPv6 adres je totožné u skúmaných výrobcov Cisco, H3C a EdgeCore. Nastavenie adres prebieha v konfiguračnom móde rozhrania, pomocou príkazu

Cisco	H3C	EdgeCore
<pre>enable configure ipv6 unicast-routing enable configure sdm prefer dual-ipv4-and-ipv6 -> { default vlan routing }</pre>	<pre>system-view ipv6</pre>	<pre>enable config ipv6 enable</pre>

Tabuľka 5.5: Aktivácia podpory IPv6 protokolu na rôznych zariadeniach

`ip address <ipaddr> <netmask>` pre IP protokol, resp. príkazu pre zadanie IPv6 adresy `ipv6 address <ipv6addr>/<prefix>`.

5.3.2 Unicast smerovanie

Hlavnou funkciou smerovačov, ako už názov napovedá, je smerovanie datagramov cez siete, tj. výber optimálnej cesty do cieľa pre datagram. Konfigurácia smerovania sa dá rozdeliť do dvoch hlavných okruhov, a to je manuálne nastavenie statických ciest, alebo nakonfigurovanie dynamických smerovacích protokolov.

Statické smerovanie

Spoliehať sa na statické smerovanie je možné len v malých sieťach, ale svoj význam má aj na hraničných smerovačoch sietí. Vo väčších sieťach jeho význam pozostáva z vytvárania záložných ciest, agregácie a nastavenia predvolenej cesty.

Cisco	H3C
<pre>enable configure ip route <address> -> <mask> <next-hop> -> [<administrative-distance>]</pre>	<pre>system-view ip route-static <address> -> <mask> <next-hop> -> [preference <value>]</pre>
<pre>ipv6 route -> <address>/<prefix-length> -> <next-hop> -> [<administrative-distance>]</pre>	<pre>ipv6 route-static -> <address>/<prefix-length> -> <next-hop> -> [preference <value>]</pre>

Tabuľka 5.6: Konfigurácia statických ciest

Tabuľka 5.6 zobrazuje spôsob zápisu nastavenia statickej cesty pre IP a IPv6 sietí. Zariadenia od výrobcu EdgeCore majú takmer rovnakú konfiguráciu ako Cisco, preto sme ich vynechali z tabuľky. Hodnoty `<address>` určujú adresu cieľovej siete, `<mask>` a `<prefix-length>` určujú masku siete, resp. dĺžku prefixu pre IPv6. Posledné povinné pole `next-hop` určuje adresu, na ktorú bude datagram preposlaný. Voliteľná možnosť je zadanie `<administrative-distance>`, resp. `preferencie <value>`, pomocou ktorých môžeme

určiť prioritu pre dané smerovacie pravidlo. Platí, čím nižšia hodnota, tým je dôležitejšia cesta. Na základe dostupnosti <next-hop> uzla a hodnoty preferencie sa bude zaraďovať cesta do smerovacej tabuľky.

Dynamické smerovanie

Pre veľké siete by statické cesty boli neudržateľné na konfiguráciu, vyžadovali by nemalé časové a ľudské zdroje. Z tohto dôvodu sa vo väčších sieťach využívajú smerovacie protokoly, ktorých konfigurácia je o niečo zložitejšia, poskytujú väčšie množstvo funkcií ako klasické statické cesty. Taktiež rozdiely medzi konfiguráciou smerovania pre IP a IPv6 smerovanie nie sú zanedbateľné.

Dnes využívanými smerovacími protokolmi sú hlavne RIP (Router Information Protocol), OSPF (Open Shortest Path First) a BGP (Border Gateway Protocol). Prvé dva sa používajú na smerovanie vo vnútri sietí jednotlivých organizácií.

Prvý spomenutý využíva ako metriku (výhodnosť cesty), počet skokov do cieľovej siete, ktorými musí datagram prejsť. Limit je pre neho 15 skokov a konverguje v ráde desiatok sekúnd, preto je vhodný do menších sietí a nekritických sietí.

OSPF využíva algoritmus hľadania najkratšej cesty na základe rýchlostí jednotlivých liniek do cieľovej siete. Vhodný je pre väčšie siete, dokáže rýchlo konvergovať a reagovať na zmeny. Avšak jeho konfigurácia vyžaduje hierarchický návrh siete a poskytuje veľké množstvo nastavení, ktoré môžu spôsobovať neznalým užívateľom veľké problémy.

BGP je smerovací protokol využívaný v smerovaní medzi jednotlivými poskytovateľmi služieb internetu. Jeho konfigurácia je podstatne náročnejšia a vyžaduje expertné znalosti sietí a správania jednotlivých implementácií. Z tohto dôvodu nebude BGP zahrnuté ani do dokumentácie, preto je potrebné prečítať originálnu dokumentáciu s podobným popisom.

Tieto protokoly sú definované v RFC štandardoch, nevyžadujú sa licenčné poplatky za ich používanie, preto sú vhodné hlavne v sieťach, kde sa vyskytujú zariadenia od rôznych výrobcov. Existujú aj privátne protokoly ako napríklad EIGRP (Enhanced Interior Gateway Routing Protocol) od spoločnosti Cisco, ale tým sa nebudeme venovať.

Cisco	H3C
<pre>enable configure router rip network <net> passive-interface <ifname></pre>	<pre>system-view rip network <net> silent-interface <ifname></pre>
<pre>ipv6 router rip <process-name> exit interface <ifname> ipv6 rip <process-name> enable</pre>	<pre>ripng <process-id> quit interface <ifname> ripng <process-id> enable</pre>

Tabuľka 5.7: Konfigurácia RIP a RIPng

Tabuľka 5.7 znázorňuje konfiguráciu RIP smerovania na Cisco a H3C zariadeniach. Pri oboch zariadeniach je rozdiel v syntaxi, ktorá zaisťuje vstup do konfiguračného módu smerovania.

Pri konfigurovaní RIP pre IP sieť nie je potrebné zadávať identifikátor procesu. Môže existovať len jedna inštancia na zariadení, v čom spočíva rozdiel oproti IPv6 RIPng (RIP

new generation – odvodené z pôvodného názvu IPv6 protokolu, protokol novej generácie), kde je umožnené vytvárať inštancii viac. Hlavným rozdielom je však pridávanie sietí do smerovacieho procesu. Kým v IP sieťach je potrebné nahradiť identifikátor <net> triednou sieťovou adresou, ktorá musí pokrývať rozsah rozhraní, ktoré chceme smerovať, tak pri IPv6 sa rozhranie pridáva do smerovacieho procesu priamo v konfiguračnom móde rozhrania. V oboch prípadoch, či už v IP alebo IPv6 konfigurácií RIP smerovania, sa príkazmi `passive-interface` pre Cisco a `silent-interface` pre H3C v konfiguračnom móde smerovania zakáže posielanie RIP paketov zadaným rozhraním.

5.4 Ďalšie služby

Služby pokrývajúce transportnú až aplikačnú vrstvu nad rámec základných požiadaviek kladených na zariadenie. Kvalitnejšie zariadenia bežne podporujú tieto služby, ako sú napr. preklad adres (NAT), DHCP server a rôzne nástroje na riešenie problémov a testovanie.

5.4.1 DHCP server

DHCP (Dynamic Host Configuration Protocol) umožňuje centralizovanému serveru určovať IP adresy, ktoré si koncové zariadenia v sieti nastavujú. Používať tento mechanizmus na aktívnych prvkoch sa oplatí hlavne v menších sieťach, kde nie sú potrebné pokročilé manažovacie funkcie. Vo veľkých sieťach stráca význam mať spustený DHCP server na aktívnom zariadení, pretože by to bola zbytočná záťaž.

Cisco	H3C
<pre>enable configure ip dhcp pool <name> network <ipaddr> <mask> default-router <ipaddr> dns-server <ipaddr> exit ip dhcp excluded-address -> <start-ipaddr> -> [<end-ipaddr>]</pre>	<pre>system-view dhcp server ip-pool <name> network ip range -> <min-ipaddr> <max-ipaddr> network mask <mask> gateway-list <ipaddr1> [... <ipaddr8>] dns-list <ipaddr1> [... <ipaddr8>] forbidden-ip <ipaddr1> [... <ipaddr8>] quit enable dhcp</pre>

Tabuľka 5.8: Konfigurácia DHCP servera

Tabuľka 5.8 znázorňuje základnú konfiguráciu DHCP servera na zariadeniach, zahŕňajúcu nastavenie adresného rozsahu z ktorého sa budú priradovať zariadeniam adresy. Ďalej obsahuje masku siete, zoznam DNS serverov a bránu. Na tomto príklade je jasne vidieť, že syntax oboch výrobcov je úplne rozdielna. Zmenené kľúčové slová, iné poradie, dokonca odlišná forma zadávania niektorých parametrov, ako znázorňujú príkazy `network` pre Cisco a príkazy `network ip range`, `network mask` pre H3C. Prvý menovaný príkaz vyžaduje zadanie sieťovej adresy a masky, podľa ktorej získa rozsah adres a následne ich priraduje. Ďalšie príkazy, patriace H3C zariadeniu, požadujú zadanie adresného rozsahu a masky oddelene.

Príkazy `ip dhcp excluded-address` a `forbidden-ip` zaistujú pre vybrané adresy zákaz ich použitia DHCP serverom pre priradenie ku koncovému zariadeniu. Konfigurácia prebieha v rozdielnych módoch, kým pri Cisco zariadení sa príkaz zadáva v globálnom konfiguračnom móde, tak pri H3C je ho nutné zadať pri konfigurácii DHCP pool-u. Rozdiel je aj v platnosti príkazov. Kým `ip dhcp excluded-address` platí pre všetky nakonfigurované DHCP rozsahy adries, tak `forbidden-ip` je platný len na aktuálny DHCP pool, v ktorom je nakonfigurovaný. To znamená, že daná adresa, môže byť priradená z niektorého ďalšieho pool-u.

Na tomto príklade DHCP konfigurácie je značne vidieť problémy odlišnosti pri jednotlivých zariadeniach a následne komplikácie vznikajúce užívateľom pri konfigurácii.

Kapitola 6

Záver

Pre problémy správcov, spojené s dokumentáciou k sieťovým prvkom, sme navrhli riešenie v podobe vlastnej dokumentácie, ktorá bude zjednocovať formát popisu konfigurácií a zároveň bude obsahovať len pre nás podstatné konfigurácie aktívnych prvkov. Dokumentácia bude bežať na wiki systéme, ktorým zabezpečíme jednoduché používanie a dosiahneme možnosť spolupráce na jej tvorení pre viacerých administrátorov. Zároveň použitím už existujúceho systému sa vyhneme komplikáciám, ktoré by vznikali pri vytváraní vlastného systému.

V práci sme ďalej rozoberali vhodnosť jednotlivých wiki systémov pre našu dokumentáciu. Podľa našich stanovených požiadaviek a recenzií užívateľov sme za najvhodnejší systém vybrali Wikimedia, ktorý splnil najlepšie naše požiadavky spolu s ďalšími benefitmi nad rámec požiadaviek.

Ďalej sme navrhli vhodnú jednotnú štruktúru pre dokumentáciu, ktorá bude použitá pre všetky sieťové prvky a správcom sietí uľahčí orientáciu v systéme.

Analýzou dokumentácií výrobcov sme zistili, že pri niektorých vlastnostiach je konfigurácia dostatočne podobná a nebolo by potrebné vytvárať zvlášť zjednodušenú dokumentáciu. Avšak existujú konfigurácie, ktorých rozdielnosť je voči iným výrobcom malá, o to však nepríjemnejšie, keď je pozmenené len jedno kľúčové slovo, prípadne je jeden indetifikátor navyše alebo chýba. V menšom množstve sa vyskytujú aj vlastnosti, ktorých konfigurácia je úplne odlišná. Používajú sa iné sledy príkazov, prípadne sa konfiguruje v inom móde. Potvrdili sa naše predpoklady o rozdielnosti konfigurácie, preto je v týchto prípadoch žiaduce mať vhodnú rýchlu náhradu manuálu.

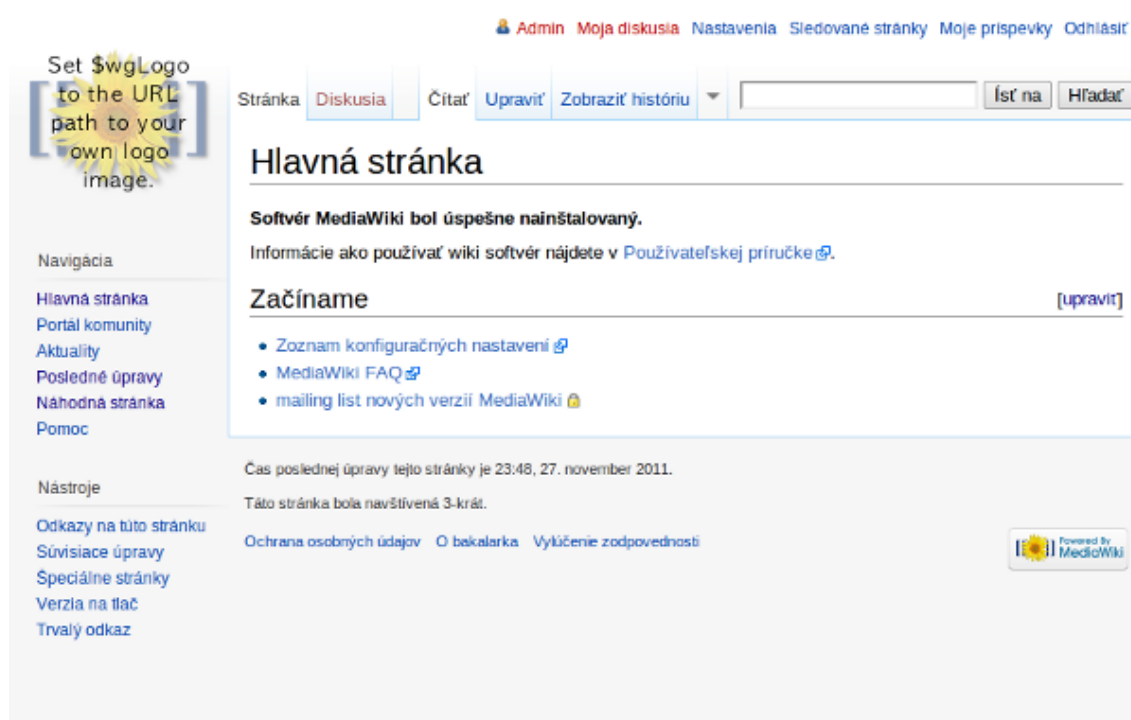
Literatúra

- [1] About WikiMatrix. [Online; cit. 2011-12-23].
URL <http://www.wikimatrix.org/about.php>
- [2] WikiMatrix — Compare them all. [Online; cit. 2011-12-23].
URL <http://www.wikimatrix.org/compare/MediaWiki+DokuWiki+PmWiki+WikkaWiki>
- [3] Case J., Fedor M., Schoffstall M. : RFC 1607 — A Simple Network Management Protocol. 1988, [Online; cit. 2011-12-22].
URL <http://tools.ietf.org/html/rfc1067>
- [4] Cisco Systems Inc. : Cisco IOS IPv6 Configuration Guide, Release 12.4. [Online; cit. 2012-04-22].
URL http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4/ipv6_12_4_book.html
- [5] Cisco Systems Inc. : Configuring DHCP. [Online; cit. 2012-04-22].
URL http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfdhcp.html
- [6] Cisco Systems Inc. : Configuring IP Routing Protocol–Independent Features. [Online; cit. 2012-04-22].
URL http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfindep.html#wp1000929
- [7] Cisco Systems Inc. : Configuring RIP. [Online; cit. 2012-04-22].
URL http://www.cisco.com/en/US/docs/ios/12_0/np1/configuration/guide/1crip.html
- [8] Cisco Systems Inc. : JUNOSˆ Internet Software Configuration Guide—IPv6. [Online; cit. 2012-02-16].
URL <http://www.juniper.net/techpubs/software/junos/junos53/swconfig53-ipv6/frameset.htm>
- [9] Cisco Systems Inc. : Using the Cisco IOS Command-Line Interface. [Online; cit. 2012-04-22].
URL http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics_ps6350_TSD_Products_Configuration_Guide_Chapter.html

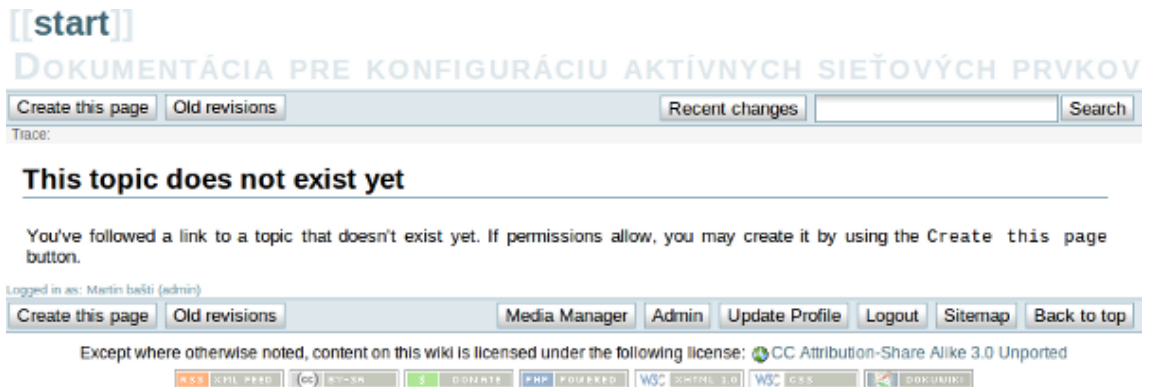
- [10] Cisco Systems Inc. : VLANs. [Online; cit. 2012-05-08].
URL <http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/vlans.html>
- [11] DokuWiki: What is DokuWiki? 2011, [Online; cit. 2011-12-23].
URL <http://www.dokuwiki.org/dokuwiki>
- [12] Edge-core : ES4626/ES4650 L3 Gigabit Ethernet Switch. [Online; cit. 2012-04-22].
URL http://www.edge-core.com/temp/ec_download/442/ES4626%20Management%20Guide.pdf
- [13] Hangzhou H3C Technologies Co., Ltd.: ACL and QoS Configuration Guide. [Online; cit. 2012-02-16].
URL <http://www.h3c.com/portal/download.do?id=1189768>
- [14] Hangzhou H3C Technologies Co., Ltd.: Fundamentals Configuration Guide. [Online; cit. 2012-05-08].
URL <http://www.h3c.com/portal/download.do?id=1189687>
- [15] Hangzhou H3C Technologies Co., Ltd.: Layer 2 — LAN Switching Command Reference. [Online; cit. 2012-05-08].
URL <http://www.h3c.com/portal/download.do?id=1034430>
- [16] Hangzhou H3C Technologies Co., Ltd.: Layer 3 — IP Routing Configuration Guide. [Online; cit. 2012-05-08].
URL <http://www.h3c.com/portal/download.do?id=1189732>
- [17] Hangzhou H3C Technologies Co., Ltd.: Layer 3 — IP Services Configuration Guide. [Online; cit. 2012-02-16].
URL <http://www.h3c.com/portal/download.do?id=1189723>
- [18] MediaWiki: How does MediaWiki work? — MediaWiki, The Free Wiki Engine. 2011, [Online; cit. 2011-12-23].
URL http://www.mediawiki.org/w/index.php?title=How_does_MediaWiki_work%3F&oldid=419815
- [19] Mishra, S.: 10 Free Wiki Software Platforms — Choose the Best One To Build You Wiki. [Online; cit. 2011-12-20].
URL <http://www.clickonf5.org/7599/10-free-opensource-wiki-software-engine/>
- [20] PmWiki: PmWiki. 2006, [Online; cit. 2011-12-23].
URL <http://www.pmwiki.org/wiki/PmWiki/PmWiki>
- [21] Twiki: Select the Product that is Right for You. 2011, [Online; cit. 2011-12-23].
URL http://www.twiki.net/select_product.html
- [22] Wikipedia: Wiki — Wikipedia, The Free Encyclopedia. 2011, [Online; cit. 2011-12-21].
URL <http://en.wikipedia.org/w/index.php?title=Wiki&oldid=466822560>
- [23] WikkaWiki: Wikka : HomePage. 2011, [Online; cit. 2011-12-23].
URL <http://wikkawiki.org/HomePage>

Dodatok A

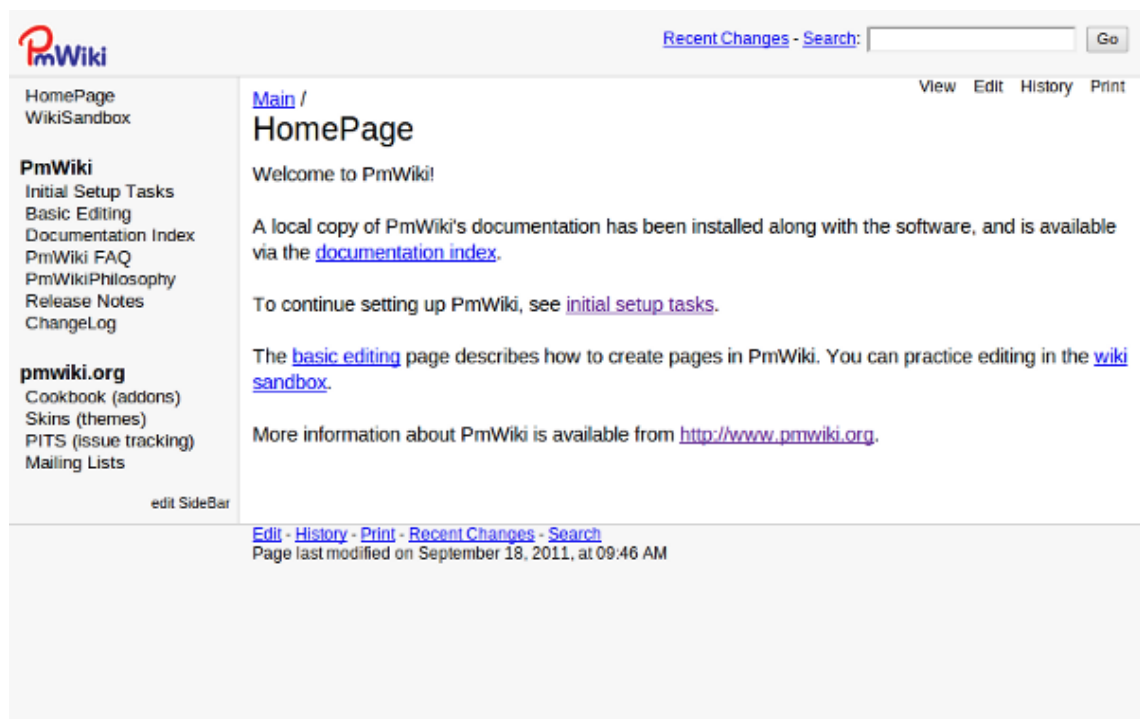
Screenshoty wiki systémov



Obr. A.1: MediaWiki po inštalácii



Obr. A.2: DokuWiki po inštalácii



Obr. A.3: PmWiki po inštalácii



Thanks for installing Wikka! This wiki runs on version [1.3.2](#), patch level [0](#). You may want to read the [release notes](#) to learn what's new in this release.

Getting started

Double-click on this page or click on the **Edit** link in the page footer to get started. If you are not sure how a wiki works, you can check out the [Wikka formatting guide](#) and play in the [SandBox](#).

KEEP UP-TO-DATE

To receive the latest news from the Wikka Development Team, you can sign up to one of our [mailing lists](#), subscribe to our [Blog](#) or join us for a chat on [IRC](#).

Some useful pages

- [Wikka formatting guide](#)
- [Documentation](#)
- [Recently modified pages](#)
- [System Information](#)

NEED MORE HELP?

Don't forget to visit the [WikkaWiki website](#)!

Obr. A.4: WikkaWiki po inštalácii

Dodatok B

Štruktúra dokumentácie

B.1 Základné nastavenia

- Základné príkazy
- Konfiguračné módy
- Správa súborového systému
- Uvedenie do factory default stavu
- Aktualizácia firmvéru
- Nastavenie hostname
- Nastavenie hesiel
- Nastavenie časovej zóny, času
- Časové servery
- Default gateway
- Vzdialené logovanie, SNMP
- AAA - Autentifikácia užívateľa
 - Lokálne
 - Radius server
 - TACACS+
- Nastavenie vzdialeného prístupu
 - SSH
 - Telnet
 - WEB management
- Nastavenie bezpečnosti(vypnutie nepotrebných nebezpečných služieb)

B.2 Nastavenia data-linkovej vrstvy – prepínače

- Tabuľka MAC adries
- ARP konfigurácia
- Konfigurácia fyzických portov
 - Loopback
 - Ethernet
 - * Link agregation, Etherchannel
 - * PoE
 - Sériové rozhrania
 - * HDLC
 - * PPP
 - CHAP, PAP
 - * FrameRelay
- VLAN
 - Správa VLAN
 - Trunking
 - GVRP, VTP
 - voice vlan
- LLDP, CDP
- L2 ACL
- Port-security
- Spanning Tree Protocol
- Multicast
 - IGMP snooping
 - MLD snooping
 - Multicast VLAN
- DHCP snooping
- RA,ND guard

B.3 Nastavenia sieťovej vrstvy – smerovače

- Konfigurácia rozhraní
 - IP
 - IPv6
 - Subinterfaces pre VLANy
 - Tunely
- Smerovanie
 - Default route
 - Statické cesty
 - RIP
 - RIPng
 - OSPFv2
 - OSPFv3
 - EIGRP
- Multicast smerovanie
 - IP
 - * PIM módy
 - IPv6
 - * PIM módy
- ACL
- DHCP Relay

B.4 Ďalšie služby

- NAT / PAT
- DHCP server
- NTP server
- Troubleshooting
 - Debug
 - Ping, ping6, traceroute
 - Zobrazenie konfigurácií