Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Ivo Špičák** **Oponent:** **ing. Josef Kaderka, Ph.D.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Akademický rok: **2014/2015**

Téma diplomové práce: **Návrh a konfigurace aktivních prvků ve středně velké nadnárodní společnosti**

Diplomovou práci Bc. Iva Špičáka (dále diplomanta) považuji za úplnou. Řešené úkoly pokládám za jednoduché, jednalo se o standardní návrh spíše malé sítě, tvořené deseti aktivními prvky (směrovačem, L3 přepínačem a osmi L2 přepínači). Přitom byly použity obvyklé postupy a technologie, v dané síti se nevyskytly žádné atypické požadavky. Základní linie byla poplatná podmínkám mateřské zahraniční firmy.
Text práce včetně závěru a seznamu použité literatury, seznamu použitých symbolů a zkratek a dalších zabírá 84 stran. Je doplněn výpisy konfiguračních souborů směrovače, L3 přepínače a jednoho L2 přepínače. Text je rozdělen na část teoretickou a část praktickou.
Část teoretická o rozsahu 22 stran představuje kompilát základních údajů o různých oblastech počítačových sítí (modely síťové architektury, protokoly aj.). Tento kompilát se jeví dosti jednoduchým a často nepřesným. Působí dojmem, že autor upřednostňuje vlastní pohled před realitou, vyplývající například ze standardů. V řadě případů situaci podává zjednodušeně, zřejmě na základě omezení daných praktickými zkušenostmi s konkrétními zařízeními. Ne vždy se seznámil s aktuálním stavem popisované problematiky.
Část praktickou o rozsahu 35 stran považuji za zbytečně obsáhlou. Její úvod obsahuje popis původní situace, analýzu a doporučení pro nové řešení. Zbytek této části je tvořen detailními popisy elementárních konfiguračních úkonů prováděných na jednotlivých zařízeních, často např. jednotlivých příkazů včetně komentářů. Domnívám se, že takový přístup by byl vhodný pro výuku na střední škole či popularizační článek, ale je diskutabilní pro úroveň diplomové práce.
V textu práce se vyskytuje dosti značné množství nedostatků a to jazykových, typografických a také věcných. Jejich výběr uvádím níže.

Připomínky k textu práce		
Str.	**Připomínka**	**Komentář**
9	Úvod – šroubované formulace	Není možné použít žádné multifunkční řešení, které by vyhovovalo všem možným podmínkám, nicméně existují standardy v rámci síťové problematiky, jako jsou přenosová média, síťové prvky či síťové protokoly.
11	Dělení sítí	Uvedené dělení je poněkud umělé – v literatuře se upřednostňují jiné pohledy.
11	Datové neboli počítačové sítě	Ne vždy se oba pojmy považují za synonymní.
11	„homogenní sítě“	Toto by se v praxi dalo realizovat jen obtížně a rozhodně ne dlouhodobě udržovat.
12	Popisy protokolů a	Popis vztahu protokolů a referenčních modelů síťové architektury je poněkud zmatečný. Především poslání modelů je vždy stejné, tudíž

	modelů	omezující věta „Ve vrstvě modelu OSI je přiřazena řada protokolů, jež plní funkce dané vrstvy“, není korektní; navíc je gramaticky nesprávná.
12	Horizontální komunikace	Pojmem „horizontální“ se týká komunikace stejných vrstev různých uzlů, kdy lze od jejich nižších či vyšších vrstev abstrahovat. Komunikace mezi protokoly sousedních vrstev pak implikuje to, že dané vrstvy se nalézají v tomtéž uzlu, tj. vertikální komunikaci.
12	hlavička - zápatí	Preferoval bych buď použít dvojici záhlaví – zápatí nebo hlavička – patička (tuto druhou raději ne).
13	V uspořádání kapitol nevidím logiku (která se nabízí – např. po vrstvách referenčního modelu ISO/ISI).	1.2 Síťové protokoly 1.2.1 Vrstvy referenčního modelu OSI a dané síťové protokoly 1.2.2 Protokol NTP 1.2.3 Protokol TCP 1.2.4 Protokol DHCP (zde je v posledních dvou větách zaměněna příčina a důsledek 1.2.5 Protokol OSPF 1.2.6 Protokol VTP
13	SMTP	Ke zprávě může adresát přistupovat i jinak, např. přímo lokálním programem (má-li na daném severu účet) či prostřednictvím webového rozhraní (a serverů v pozadí atd.).
13	Modely síťové architektury	Bylo by dobré zmínit detailněji uspořádání modelu síťové architektury TCP/IP. Tento je tvořen pouze čtyřmi vrstvami, které jsou označeny jinak nežli je tomu u modelu ISO/OSI. Například nezná vrstvu síťovou, té funkčně odpovídá vrstva internetová; která ale není třetí, nýbrž druhou – je ovšem pravda, že síťoví specialisté si i tak rozumí.
14	Protokoly	Rozhodně by bylo dobré zmínit protokol IPv6.
15	Ethernet	Ethernet svými funkce pokrývá linkovou a fyzickou vrstvu (hovoří se podvrstvách MAC a LLC). Autorem uváděné údaje o linkové vrstvě ovšem patří do vrstvy fyzické.
15	Protokol NTP	Protokol NTP sice vznikl již v roce 1985, ovšem je průběžně vyvíjen a jeho poslední verze pochází z roku 2010. Jeho činnost daleko komplikovanější nežli autor uvádí, primárně jde o synchronizaci času mezi skupinou serverů, role klientů je přitom pasivní.
16	Protokol TCP	Není jasné, proč autor zničehonic použil pojem „zásobník“. Jedná se o implementaci protokolu TCP na jedné či druhé straně spojení.
17	Protokol DHCP	Autor zbytečně používá jak pojem broadcast, tak všesměrové vysílání. Činnost DHCP by zasloužila věcně správnější popis, alespoň takový, jako je v odkazovaném zdroji. Třetí vrstva modelu TCP/IP je transportní. Všesměrové vysílání na transportní vrstvě nedává smysl.
17	Odkazy	Autor se mnohokráte odkazuje na tentýž (dosti obsáhlý) zdroj vždy jen číslem [1], ovšem pokaždé v jiné souvislosti. V takovém případě by bylo vždy vhodné uvést i stranu.
18	Popis protokolu OSPF	Je vypracován nepříliš přesně, snad až laicky – protokol OSPF se rozhodně neskládá z oblastí a jeho vztah k autonomním systémům není prakticky žádný – jedná se o interní protokol. Obrázek č. 3 a doprovodný text jsou až naivně jednoduché – při dané topologii by se při vzniku popisovaného problému všechny interní

		směrovací protokoly chovaly stejně. Podobně obrázek č. 4 – není jasné, proč by uvedená tabulka měla souviset právě s OSPF. Gramaticky správný tvar je "standard", nikoliv „standart". Cisco nepoužívá rovnici 108/šířka pásma, nýbrž 10^8/ šířka pásma. ID směrovače není IPv4 adresou, i když má formálně stejný tvar a může být od ní někdy odvozen. „Soused označuje dva nebo více směrovačů" – věta je gramaticky nesprávná. Vysvětlení významu OSPF oblasti je velmi neprůhledné až matoucí.
20	Protokol VTP	Občasné gramatické chyby, např. „… informace pak šeří všem ostatním …", „Mohou vyvářet, upravovat, …". Bylo by vhodné zmínit, že VTP doména nemá nic společného s doménou v pojetí DNS nebo systémů Microsoft. Výchozí režim přepínačů Cisco sice je server, avšak tento se neuplatní, neboť není nastavena žádná doména. Nejsou zmíněny bezpečnostní aspekty VTP!
22	VLAN	Výrok „… trunk, což znamená, že tento port je zařazen do více VLAN", je zavádějící. Trunkový port není zařazen do žádné VLAN, nýbrž umožňuje přenášet tagované rámce, tj. rámce nesoucí informaci o jejich příslušnosti do některé VLAN. Výrok „Síť VLAN je považována za vlastní podsíť nebo všesměrovou doménu" je nejasný až nesprávný.
24	1.3.2 Statické sítě VLAN	Gramatická chyba: „toto přiřazení portu zachová trvale, dokud nejsou ručně změněny".
25	1.3.4 Identifikace sítí VLAN	Věta „Porty přepínače jsou výhradní rozhraní vrstvy 2, která jsou přidružena k fyzickému portu" není srozumitelná. „… všem sítím VLAN, pokud se jedná o trunkový port" – pro trunk lze specifikovat seznam povolených VLAN.
25	1.4 Přepínání	Autor ne zcela jasně odlišuje přepínání na druhé vrstvě od přepínání na třetí vrstvě.
26	1.4 Přepínání	Ve větě „Protokol (CDP) pracuje na druhé vrstvě TCP/IP modelu a je závislý na protokolech vyšší vrstvy" jsou dvě chyby – CDP pracuje na druhé vrstvě modelu ISO/OSI a dále není závislý na protokolech vyšší vrstvy.
26	1.5 Směrování	Gramatické chyby: „Směrovače pro svou páci vyžívají směrovací protokoly".
27	1.5 Směrování	Autorova představa o autonomním systému je velmi, velmi zjednodušená. Číslo AS má od roku 2007 rozsah 32 bitů (viz RFC 4893), nikoliv 16 bitů.
28	1.5 Směrování	Z obrázku č. 8 a přidruženého textu se naprosto nedá odvodit, jak redistribuce směrovacích informací probíhá nebo jak se projevuje.
28	1.6.1 Kroucená dvojlinka	Zkratka EMI zpravidla znamená „Electromagnetic Interference", nikoliv indukce.
		„Pro Ethernet 10 Mb/s-100 Mb/s se používají dva páry" – to neplatí absolutně, např. 100BASE-T4 (802.3u) používá 4 páry, ale vystačí s kabelem kategorie 3.
29	1.6.2 Optický kabel	Popis je velmi neodborný.
32		Vidová disperse - optický kabel neobsahuje vodiče (vyjma

		speciálních, např. podmořských). Degradaci signálu způsobuje časový rozdíl příchodu nejrychlejšího a nejpomalejšího světelného paprsku.

Připomínky ke konfiguraci zařízení	
Zařízení	**Připomínka**
Konfigurace směrovače 2801 (dkczr-ddc1)	Protokol OSPF není nijak zabezpečen. Vzdálený přístup je možný odkudkoliv; není použit protokol SSH; heslo pro přístup na konsolu včetně virtuální je nedostatečně zabezpečeno, navíc je velmi slabé („hesao“ - je-li výpis reálný). Komunikace s NTP serverem není zabezpečena. Je povolen protokol CDP.
Konfigurace přepínače 2960 (dkczsw-ddc2)	Vzdálený přístup je možný odkudkoliv; není použit protokol SSH; heslo pro přístup na konsolu včetně virtuální je nedostatečně zabezpečeno, navíc je velmi slabé („hesao“ - je-li výpis reálný); heslo pro přechod do privilegovaného režimu je nedostatečně zabezpečeno („decisr“). Komunikace s NTP serverem není zabezpečena. Trunkem mohou procházet rámce z libovolné virtuální LAN. Na přístupových portech jsou definovány virtuální LAN 57 a 61, přičemž jsou vytvořena rozhraní pro VLAN 57 a 63. Není ošetřena nativní VLAN.
Konfigurace přepínače 2960 (dkczsw-ddc1)	Vzdálený přístup je možný odkudkoliv; není použit protokol SSH; heslo pro přístup na konsolu včetně virtuální je nedostatečně zabezpečeno, navíc je velmi slabé („hesao“ - je-li výpis reálný); heslo pro přechod do privilegovaného režimu je nedostatečně zabezpečeno („decisr“). Komunikace s NTP serverem není zabezpečena. Trunkem mohou procházet rámce z libovolné virtuální LAN. Na přístupových portech jsou definovány virtuální LAN 57 a 61, přičemž jsou vytvořena rozhraní pro VLAN 57 a 63. Není ošetřena nativní VLAN.

K práci mám tyto připomínky, jež by měly být při obhajobě zodpovězeny:

a) Kde autor vidí svůj vlastní, nový přínos?
b) Zvážil perspektivní přechod na protokol IPv6?
c) Z jakého důvodu prakticky ignoroval možnosti zabezpečení síťových zařízení a protokolů?

Celkové hodnocení práce:

Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

E - dostatečně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 2.6.2015 Podpis oponenta diplomové práce