Počítačové sítě
Zadání semestrálních projektů

Petr Grygárek, FEI VŠB-TU Ostrava

Semestrální projekt I – strukturovaná kabeláž

Projekt realizují dvojice studentů. Každá dvojice studentů samostatně vytvoří projekt strukturované kabeláže s použitím jimi dodaného stavebního plánu zvolené budovy (vhodný je např. větší dvoupatrový objekt). Kabeláž bude realizována nestíněnou kroucenou dvoulinkou kategorie 5e. Se cvičícím zkonzultujte požadované počty zásuvek v jednotlivých místnostech (typicky 6), jako minimum však respektujte požadavek normy (min 2 zásuvky/10m^2 plochy).

Požadovaný rozsah práce :

- Navrhněte počet, umístění a systém pojmenování rozvaděčů (minimálně 2 rozvaděče). Nezapomeňte na dostatečný počet propojek mezi rozvaděči (i pro telefonní okruhy apod.)

- Do stavebního plánu zakreslete kabelové trasy a umístění zásuvek.

- Navrhněte vhodný systém pro označování zásuvek a portů na patch panelech a zaznamenejte označení do plánu.

- Proveďte sumarizaci potřebného materiálu (délka kabelů, počet zásuvek, patch panelů, rozvaděčových skříní, atd.).

- Proveďte cenovou kalkulaci potřebného materiálu (orientační ceníky materiálu najděte na Internetu).

Dále nad vytvořeným kabelážím systémem navrhněte osazení rozvaděčů aktivními prvky, aby 2/3 zásuvek bylo použitelných pro připojení stanic Ethernet 100BaseT. Omezte se na aktivní prvky pracující na spojové vrstvě.

Zdokumentujte vzájemné propojení aktivních prvků v rozvaděčích (konkrétní porty) a připojení jednotlivých zásuvek na konkrétní porty aktivních prvků. Vytvořte a zdokumentujte vhodný systém označování aktivních prvků. U každého aktivního prvku musí být z dokumentace zřejmé, ve kterém rozvaděči a na které jeho pozici se nachází.

Vhodné jsou schematické náčrtky umístění aktivních prvků a (pojmenovaných) patch panelů v rozvaděčích.

Cenová kalkulace se týká pouze kabelážního systému (nikoli aktivních prvků), samostatně je však uveden počet a délky potřebných patch kabelů včetně jejich ceny.

Semestrální projekt II - konstrukce sítě

Zadání

Navrhněte, prakticky zkonstruujte a zdokumentujte přidělenou oblast sítě WAN podle obrázku včetně uvedených síťových služeb.

Popis sítě

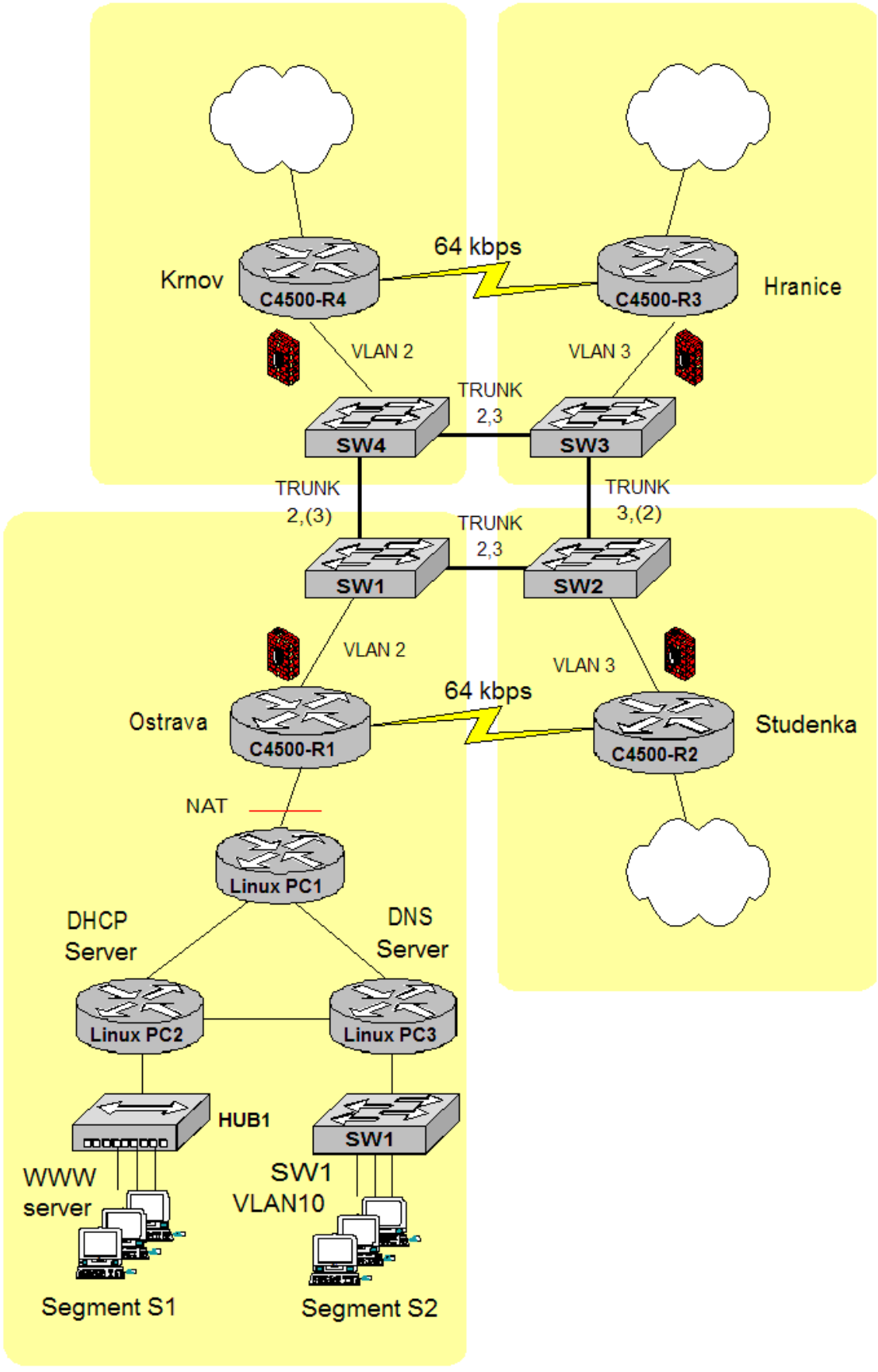
Síť (viz obrázek) sestává ze čtyřech topologicky shodných oblastí, vzájemně propojených jednak pronajatými synchronními sériovými linkami a jednak pomocí redundandní topologie z přepínačů C1900 využívající virtuálních sítí (VLAN).
Pronajaté sériové linky mají přenosovou rychlost 64kbps, na spojové vrstvě je použit protokol HDLC.

Struktura páteřních přepínačů je založena na přepínačích Cisco Catalyst 1900. Vzájemné propojení přepínačů je realizováno trunk linkami (z historických důvodů využívajících proprietární enkapsulaci ISL). Pro vyloučení smyček je provozován protokol Spanning Tree, který je parametrizován tak, aby v případě normální funkčnosti všech spojů provoz každé VLAN procházel pouze jedinou trunk linkou.

Každá oblast je připojena k páteři pomocí směrovače Cisco 4500, na němž je realizována také filtrace provozu pomocí ACL (Access Control Lists). Ostatní směrovače oblasti jsou tvořeny počítači PC s OS Linux a směrovacím démonem Zebra.

Poznámka:
Z důvodu nedostatku vybavení je přepínač segmentu S2 každé oblasti realizován jako samostatná oddělená viruální síť (VLAN10) přilehlého páteřního přepínače příslušné oblasti. Provoz této VLAN není propouštěn trunk linkami mimo přepínač.

Topologie sítě



Organizace projektu

V každém cvičení jsou studenti rozděleni do 4 skupin, každá skupina (max. 6 studentů) realizuje jednu z oblastí sítě. V každém cvičení jsou realizovány všechny 4 oblasti.

Každá skupina navrhne konfiguraci všech síťových prvků a serverů pro svou oblast. Všechny skupiny se společně dohodnou na adresaci v páteřní oblasti. Praktickou realizaci a demonstraci funkčnosti přidělené oblasti provedou všichni členové každé skupiny společně.

V závěrečné části semestru budou vyhrazena cvičení pro samostatnou práci na projektu a konzultace. Na prvních z nich bude všemi skupinami společně (avšak bez přímého vedení cvičícího) odzkoušena konfiguraci páteře (VLAN) a protokol OSPF mezi routery Cisco 4500).

Poznámky k vypracování

Adresování

Navrhněte adresování sítě s maskou podsítě pevné délky.

Adresní rozsah páteřní sítě (společný pro všechny 4 skupiny cvičení) je dán cvičícím. Do tohoto rozsahu patří i linky napojující páteřní směrovače C4500 na Linux PC1 jednotlivých oblastí sítě. Každé skupině je rovněž přidělená (jiná) privátní adresa sítě a požadované počty stanic na jednotlivých segmentech oblasti. Použijte podsíťování s konstantní maskou podsítě. Přidělte pouze nezbytný počet adres, případné zbylé podsítě ponechte pro další rozšiřování sítě.
Rozhraním směrovačů přidělujte vždy nejnižší použitelné adresy na podsíti. V dokumentaci uveďte adresování vaši oblasti i adresování páteře.

Směrování

Mezi směrovači Linux PC1, Linux PC2 a Linux PC3 je provozován směrovací protokol RIP. Vnějších cílů dosahují směrovače Linux PC1, Linux PC2 i Linux PC3 pomocí implicitní (default) cesty. Tu má směrovač Linux PC1 nakonfigurovánu staticky na vnitřní rozhraní Cisco 4500. Linux PC2 a Linux PC3 se učí default cestu z RIP, do něhož jí propaguje Linux PC1.

Na spojovací linkce mezi Linux PC1 a C4500 protokol RIP neprovozujte. Segmenty rozbočovače HUB1 a VLAN10 do RIP propagujte, avšak provoz RIP na těchto segmentech nedovolte (je zbytečný, žádné jiné zařízení na nich RIP neprovozuje).

Směrování v páteřní síti je řešeno směrovacím protokolem OSPF s redistribucí statických cest do sítí v jednotlivých oblastech konfigurovaných na přilehlých směrovačích do protokolu OSPF. Všechny páteřní směrovače jsou z pohledu oblastí (area) protokolu OSPF umístěny v páteřní oblasti (area 0).

Překlad adres (NAT)

Na rozhraní Linux PC1 vedoucímu k páteřnímu směrovači C4500 je realizován NAT. Vaší oblasti jsou přiděleny dva globálně směrovatelné rozsahy adres. Adresy stanic na segmentech S1 a S2 jsou na tyto globální rozsahy mapovány dynamicky. Adresy z ostatních segmentů oblasti sítě jsou přes NAT propouštěny bez modifikace (avšak v páteřní síti nejsou směrovatelné). Poslední adresa (privátního rozsahu) segmentu S1 je přidělená WWW serveru. Ten je dostupný zvnějšku oblasti pod poslední adresou (globálního) adresového rozsahu, pod nímž navenek (za NAT) vystupují stanice segmentu S1.
Statické cesty z jednotlivých páteřních směšovačů do přilehlé oblasti sítě samozřejmě vedou do globálně směrovatelných rozsahů, nikoli na privátní adresy platné pouze v rámci každé oblasti sítě.

DHCP server

Zprovozněte DHCP server, který bude dynamicky přidělovat adresy stanicím připojeným k segmentu sítě S1. DHCP server realizujte pomocí démona dhcpd. Ověřte a zdokumentujte funkčnost.

DNS server

DNS server bude poskytovat záznamy pro doménu odpovídající jménu vám přidělené oblasti sítě. V DNS databázi budou jména všech rozhraní směrovačů vaši oblasti a management adresy síťových prvků. Vhodný systém pojmenovávání zvolte sami (**zdokumentujte**!) Budou konfigurovány záznamy pro překlad doménových jmen na IP adresy i překlad IP adres na doménová jména. Předpokládá se využití DNS serveru pouze v rámci oblasti, proto použijte v záznamech privátní adresy (použitelné pouze uvnitř oblasti).

DNS Server bude sloužit pouze pro provoz lokálního provozu pobočky a nebude napojen na globální DNS strom. Každý DNS server proto bude autoritou nejen pro doménu jména vaši oblasti, ale i pro root doménu (".").

DNS server realizujte na Linuxu pomocí démona bind.

Přepínače páteřní sítě

Zkonfigurujte prioritu přepínačů tak, aby kořenem stromu Spanning Tree pro každou VLAN spojující dvě oblasti byl některý z dvojice přímo propojených přepínačů těchto oblastí. Nastavte ceny linek pro jednotlivé VLAN tak, aby algoritmus Spanning Tree nevyblokoval přímou linku mezi oblastmi propojenými pomocí VLAN, ale aby provoz tekl obchozí cestou přes ostatní přepínače jen v případě výpadku přímé trunk linky.

Při testování fukčnosti konfiguraci přepínačů páteřní sítě spolupracujte s ostatními skupinami.

Zabezpečení sítě - ACL

Na směrovačích C4500 implementujte filtraci provozu mezi vaší oblastí a zbytkem sítě s použitím ACL (Access Control Lists). Požadavky jsou následující:

1. Ze segmentu S1 lze pomocí Telnetu spravovat k oblasti přilehlý přepínač
2. Stanice na segmentu S1 mohou používat Secure Shell SSH na servery mimo oblast
3. Stanice na segmentu S2 smějí na WWW servery mimo oblast
4. Je dovolen přístup zvnějšku oblasti na WWW server na segmentu S1 (dostupný pod veřejnou adresou přes NAT)
5. Z S1 i S2 je možné přistupovat k libovolnému DNS serveru vně oblasti.
6. Stanicím na segmentech S1 i S2 je dovolen ping (ICMP echo request) kamkoli mimo oblast, neodpovídají však na žádost zvnějšku oblasti (směřovanou na adresy globálního rozsahu odpovídajícího S1, resp. S2)

7. Nedovolte únik paketů s privátní zdrojovou adresou mimo vaši oblast sítě (odpověď by byla v páteři nesměrovatelná).
8. Realizujte anti-spoofing filtr, tedy veškeré (podvržené) pakety přicházející z páteřní sítě se zdrojovou adresou odpovídající adresám uvnitř oblasti sítě (jak privátním, tak veřejnému rozsahu NAT), jsou zahazovány.

Veškerý výše neuvedený provoz je zakázán.

Stanovte, na kterém rozhraní a v kterém směru budou jednotlivé ACL aplikovány, vyznačte na plánku sítě.

Nezapomeňte vždy na povolení obou směrů každého z dovolených typů provozů.
Nezapomeňte na existenci NAT ve vaši oblasti sítě.

Management sítě

Směrovače C4500 a přepínače budou umožňovat vzdálený management pomocí služby Telnet. Přístupové heslo pro Telnet i heslo pro privilegovaný režim bude ‘cisco’.
Přepínače budou mít jako management adresu přiděleny poslední použitelné adresy ze segmentu VLAN, přes kterou zajišťují "přímé" spojení se sousední oblastí.

Dokumentace

V plánku sítě zdokumentujte:

- Označení konkrétních rozhraní síťových prvků, které jste použili pro propojení, u sériových linek vyznačte DCE.
- Přiřazení portů přepínačů do jednotlivých VLAN.
- IP adresy jednotlivých rozhraní směrovačů, management adresy přepínačů.

Uveďte souhrnně všechny použité podsítě, vždy s uvedením adresy sítě, masky podsítě, adresy výchozí brány (default gateway) pro podsíť, použitelných IP adres stanic a broadcast adresy pro podsíť.

Uveďte výpisy směrovacích tabulek všech směrovačů (po zkonvergování směrovacího protokolu).

Uvedte výpisy konfigurací směrovačů Linux PC1 – Linux PC3, C4500 i přepínačů.

Popište vámi navržené schema pojmenovávání rozhraní směrovačů a management adres v DNS.

Uveďte podstatné konfigurační soubory démona bind (DNS).

Uveďte konfiguraci ACL, vždy s uvedením rozhraní, na nějž je ACL aplikován a s vyznačením směru provozu, který filtruje. Smysl každé položky ACL stručně okomentujte. Položky ACL vhodně symbolicky označte a u každé položky uveďte označení položky (jiného) ACL, která řeší opačný směr provozu (je-li taková).

Uveďte část logu DHCP serveru dokumentujícího úspěšné přidělení adresy klientovi. Uveďte podstatné konfigurační soubory démona dhcpd.

Zdokumentujte ceny linek páteřní struktury přepínačů pro algoritmus Spanning Tree a vyznačte root bridge pro jednotlivé VLAN.

Hodnocení projektů

Projekty budou odevzdávány a hodnoceny takto:

Projekt I (10 bodů):

Odevzdání nejpozději do konce 7 týdne semestru cvičícímu. Skupina 2 studentů je hodnocena jako celek.

Projekt II (23 (30) bodů)

Odevzdání na cvičení v zápočtovém týdnu formou praktické demonstrace funkčnosti.

Projekt II bude ohodnocen za skupinu jako celek v rozsahu 0-23 bodů. Body získané skupinou budou jednotlivým studentům skupiny přiděleny po zodpovězení dvou stručných a konkrétních otázek, jejimž smyslem je ověřit, že se student orientuje v celé vytvořené konfiguraci. Podle počtu úspěšně zodpovězených otázek bude studentovi přiznány všechny nebo část z bodů přidělených skupině (2 správné odpovědi-100%, 1 správná odpověď 50%, žádná správná odpověď 0b). Při správném zodpovězení obou otázek bude navíc přiznána prémie 7 bodů a připočtena k hodnocení zkoušky.

Odevzdání **obou projektů** je nutnou **podmínkou udělení zápočtu**. Body budou přiznány pouze při odevzdání v termínu.

Po uvedených termínech nebudou projekty přijímány.

Podmínkou udělení zápočtu je dosažení alespoň **10 bodů** v součtu z obou projektů

Oba projekty budou odevzdány v písemné podobě. Písemná dokumentace k projektu sítě bude odevzdána před demonstrací funkčnosti (podmínka uznání odevzdání v termínu)

Pokyny pro cvičící (projekt II)

V každém cvičení přidělit:

- (Globální) adresu sítě pro adresování páteře, se studenty jako cvičení stanovit masku sítě, přidělit adresy na jednotlivá rozhraní C4500 vedoucí do páteřní sítě.

Každé skupině přidělit:

- Rozsah použitelných privátních adres
- Počty požadovaných stanic na segmentech S1 a S2 (různě pro různé oblasti sítě)
- Dva globálně směrovatelné rozsahy adres (typicky menší než počty stanic na S1, S2)

Upozorněte studenty na popis přiřazení management adresy pro Telnet (na Cisco routerechi C1900) a na potřebu a způsob přiřazení „description“ jednotlivým rozhraním.