Počítačové sítě I – LS 2004/2005
Návrh a konstrukce sítě – zadání

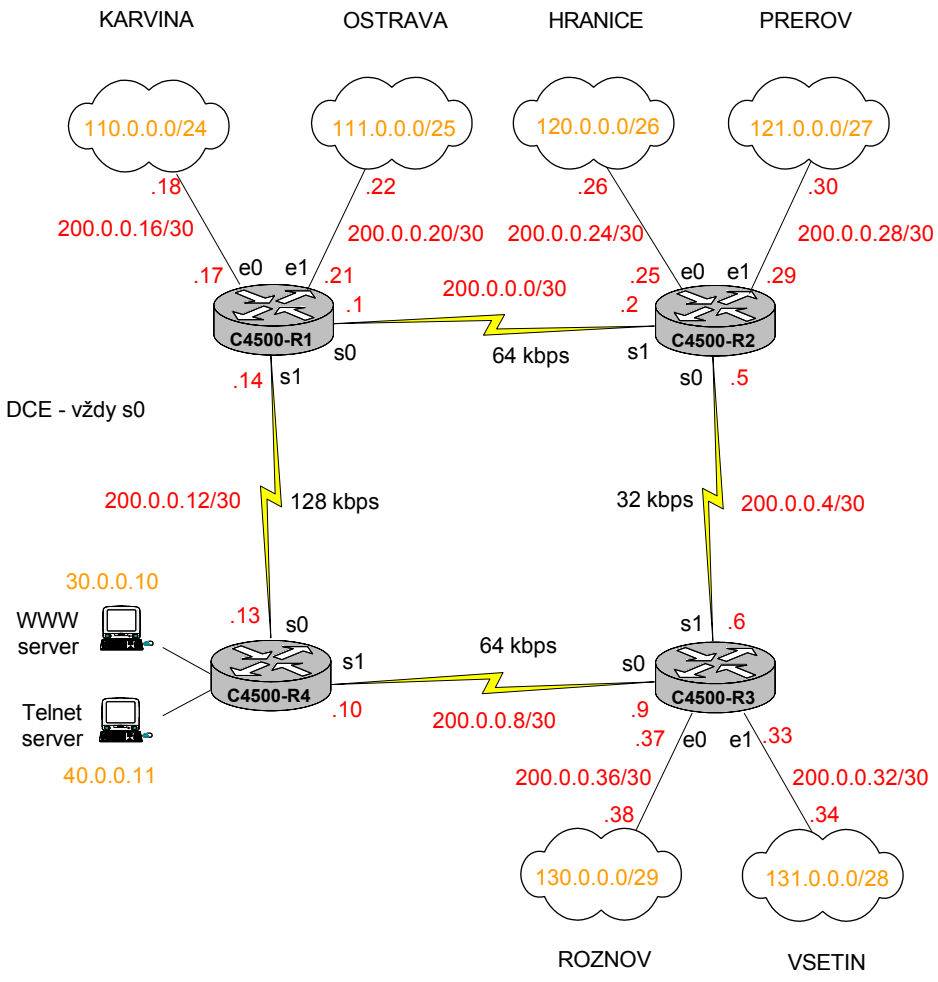
Petr Grygárek, FEI VŠB-TU Ostrava

Zadání

Navrhněte, prakticky zkonstruujte a zdokumentujte síť přidělené lokality připojené do sítě WAN.

Popis sítě

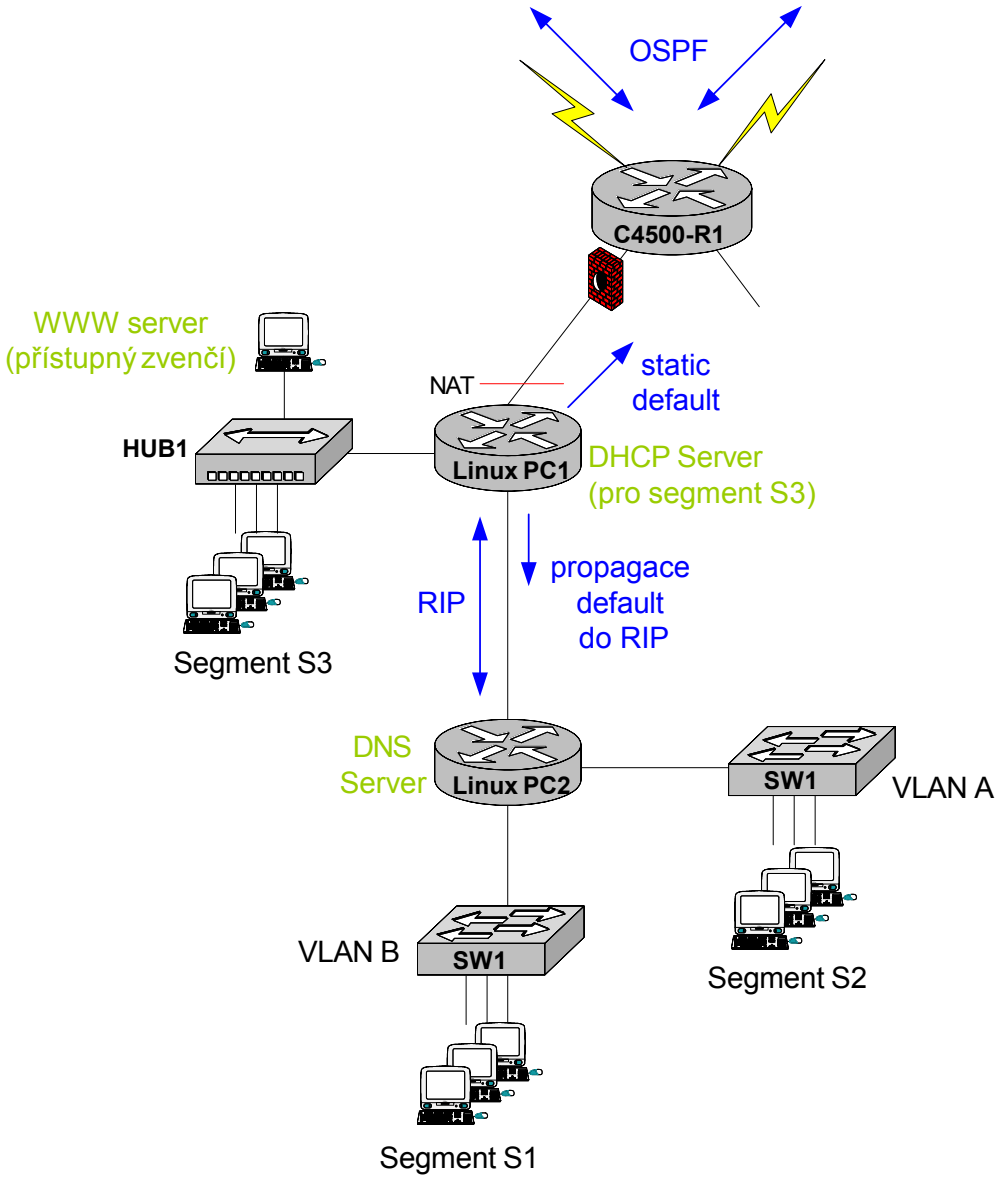
Síť (viz obrázek 1) sestává ze šesti topologicky shodných lokalit, připojených k páteřní síti založené na routerech Cisco 4500. Páteřní routery jsou vzájemně propojeny pronajatými synchronními sériovými linkami o různých přenosových rychlostech.
Každá lokalita je připojena k páteři přes jedno z rozhraní Ethernet některého routeru Cisco 4500. Na tomto rozhraní je realizována filtrace provozu do/z lokality pomocí ACL (Access Control Lists).



.

Obrázek 1

Jednotlivé lokality, konfigurované vždy jednou skupinou studentů, mají strukturu uvedenou na obrázku 2. V obrázku jsou označeny síťové prvky použité pro lokalitu KARVINA; prvky pro ostatní lokality jsou uvedeny v tabulce 1 pod obrázkem.



Obrázek 2

Pobočka	Páteřní směrač	Rozhraní	Přepínač	Hub
KARVINA	R1	e0	SW1	HUB1
OSTRAVA	R1	e1	SW2	HUB2
HRANICE	R2	e0	SW3	HUB3
PREROV	R2	e1	SW4	HUB4
ROZNOV	R3	e0	SW5	HUB5
VSETIN	R3	e1	SW6	HUB6

Tabulka 1 – Rozdělení síťových prvků pro jednotlivé lokality

Jednotlivé směrovače lokalit jsou tvořeny počítači PC s OS Linux („microDebian“) a se směrovacím démonem Zebra (resp. Quagga).

Poznámky k vypracování

Základní konfigurace

Všechna rozhraní směrovačů i přepínačů budou mít nakonfigurován popis (description) informující, kam je dané rozhraní připojeno.

Adresování

Navrhněte adresování sítě s maskou podsítě pevné délky.

Adresní rozsah páteřní sítě byl stanoven pevně. Tento rozsah zahrnuje spojovací linky mezi páteřními routery i linky napojující páteřní směrovače C4500 na Linux PC1 jednotlivých lokalit.
Pro vnitřní sítě každé lokality bude přidělen (jiný) prefix sítě z rozsahu privátních adres a požadované počty stanic na jednotlivých segmentech lokality. Použijte podsíťování s konstantní maskou podsítě. Přidělte pouze nezbytný počet adres, případné zbylé podsítě ponechte pro další rozšiřování lokality.
Rozhraním směrovačů přidělujte vždy nejnižší použitelné adresy na podsíti. Adresy podsítí a rozhraní jednotlivých směrovačů uveďte do plánku sítě v dokumentaci.

Překlad adres (NAT)

Na rozhraní Linux PC1 vedoucímu k páteřnímu směrovači C4500 je realizován NAT. Vaší oblasti je přidělen rozsah globálně směrovatelných adres, jak je uveden v příslušném „obláčku“ na obr. 1. Na tento rozsah jsou dynamicky mapovány privátní adresy ze segmentů S1 a S2. Adresy z ostatních segmentů lokality jsou přes NAT propouštěny bez modifikace (avšak v páteřní síti nejsou směrovatelné).

Doporučení:
Navrhněte si adresy podsítí pro segmenty S1 a S2 tak, abyste je byli schopni při určení zdrojových adres podléhajících NAT vyjádřit jedním společným prefixem, který zahrnuje právě jen adresy z těchto dvou segmentů.

Poslední adresa (privátního rozsahu) segmentu S3 je přidělená WWW serveru. Ten je dostupný zvnějšku oblasti pod poslední adresou přiděleného globálního adresového rozsahu, kterou vyhraďte pouze pro tento účel.

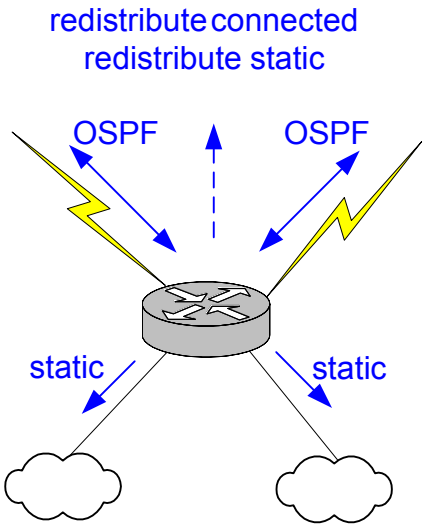
Směrování v lokalitách

Mezi směrovači Linux PC1 a Linux PC2 je provozován směrovací protokol RIP. Oba směrovače do RIP propagují všechny k nim připojené segmenty sítí (s výjimkou spojovací linky mezi Linux PC1 a C4500). Vnějších cílů dosahuje směrovač Linux PC1 pomocí statické default cesty. Linux PC2 se učí default cestu z RIP, do něhož jí propaguje Linux PC1.

Směrování v páteři

Páteřní síť včetně směrování je předkonfigurována. Směrování v páteřní síti je řešeno směrovacím protokolem OSPF s jedinou oblastí (area 0). Do protokolu OSPF jsou propagovány i spojovací linky do jednotlivých lokalit.

Jednotlivé směrovače páteře mají nakonfigurovány statické cesty do přilehlých oblastí (na jejich veřejně směrovatelné rozsahy adres). Tyto statické cesty jsou redistribuovány do OSPF. Situace je znázorněna na obrázku 3.



Obrázek 3

Poznámka:
Statické cesty do přilehlých lokalit, nakonfigurované na jednotlivých páteřních směrovačích, samozřejmě vedou do globálně směrovatelných rozsahů adres, nikoli na privátní adresy vnitřní strany NAT. Ty jsou totiž platné pouze v rámci každé lokality.

DHCP server

Na Linux PC1 zprovozněte DHCP server, který bude dynamicky přidělovat adresy stanicím připojeným k segmentu sítě S3. DHCP server realizujte pomocí démona dhcpd. Ověřte a zdokumentujte funkčnost.

DNS server

DNS server na Linux PC2 bude poskytovat záznamy pro doménu odpovídající jménu vám přidělené lokality. V DNS databázi budou jména všech rozhraní směrovačů vaší lokality a WWW server. Vhodný systém pojmenovávání zvolte sami (**zdokumentujte**!). Budou konfigurovány záznamy pro překlad doménových jmen na IP adresy i pro překlad IP adres na doménová jména. Předpokládá se využití DNS serveru pouze v lokality, proto použijte v záznamech privátní adresy (použitelné pouze uvnitř lokality).

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

DNS server realizujte na Linuxu pomocí démona bind.

Zabezpečení sítě - ACL

Na rozhraní směrovače C4500 připojujícím vaši lokalitu implementujte filtraci provozu s použitím ACL (Access Control Lists). Požadavky jsou následující:

1. Ze segmentu se S1 lze připojit na Telnet server 40.0.0.11
2. Stanice na segmentu S2 smějí na WWW server 30.0.0.10
3. Je dovolen přístup zvnějšku lokality na WWW server na segmentu S3 (dostupný pod veřejnou adresou přes NAT)
4. Ze segmentů S1 i S2 je možné přistupovat k libovolnému DNS serveru vně oblasti.
5. 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 lokality)
6. Nedovolte únik paketů s privátní zdrojovou adresou mimo vaší lokalitu (odpověď by byla v páteři nesměrovatelná).
7. Realizujte anti-spoofing filtr, tedy veškeré (podvržené) pakety přicházející z páteřní sítě se zdrojovou adresou odpovídající adresám uvnitř lokality (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 lokalitě

Organizace projektu

V každém cvičení jsou studenti rozděleni do skupin, každá skupina (max. 4 studentů) realizuje jednu z lokalit sítě.
Každá skupina navrhne konfiguraci všech síťových prvků a serverů pro svou lokalitu. Páteřní sítě je předkonfigurována. Praktickou realizaci a zdokumentování včetně dokumentace funkčnosti přidělené oblasti provedou všichni členové každé skupiny společně ve k tomu vyhrazených časech mimo řádná cvičení.

Požadavky na dokumentaci – ČTĚTE POZORNĚ

V plánku sítě zdokumentujte:

- Označení konkrétních rozhraní síťových prvků, které jste použili při vašem zapojení
- Přiřazení portů přepínačů do jednotlivých VLAN
- IP adresy jednotlivých rozhraní směrovačů

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

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

Popište vámi navržené schema pojmenovávání rozhraní směrovačů 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 (druhého) ACL, která řeší opačný směr provozu (je-li taková).

Uvedte výpisy konfigurací směrovačů Linux PC1, Linux PC2 a C4500 i přepínače.

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

Hodnocení projektu

Projekt bude hodnocen za skupinu jako celek v rozsahu 0-10 bodů.

Projekt musí být odevzdán (nejpozději) na cvičení v zápočtovém týdnu.
Body budou přiznány pouze při odevzdání v termínu a v uspokojivé kvalitě.

Odevzdání projektu je nutnou **podmínkou udělení zápočtu**.

Dokumentace k projektu bude odevzdána v písemné podobě, pouze po dohodě se cvičícím lze i v podobě elektronické.

Pokyny pro cvičící

Každé skupině přidělit:

- Rozhraní konkrétního směrovače, kde je lokalita připojena k páteři
- Rozsah použitelných privátních adres
- Počty požadovaných stanic na segmentech S1, S2 a S3 (různě pro různé oblasti sítě)
- Přístupový účet na směrovač C4500 pro vložení ACL
- Skutečná čísla VLAN použitá pro VLAN A a VLAN B