

Počítačové sítě – ZS 2006/2007

Návrh sítě – zadání

Petr Grygárek, FEI VŠB-TU Ostrava

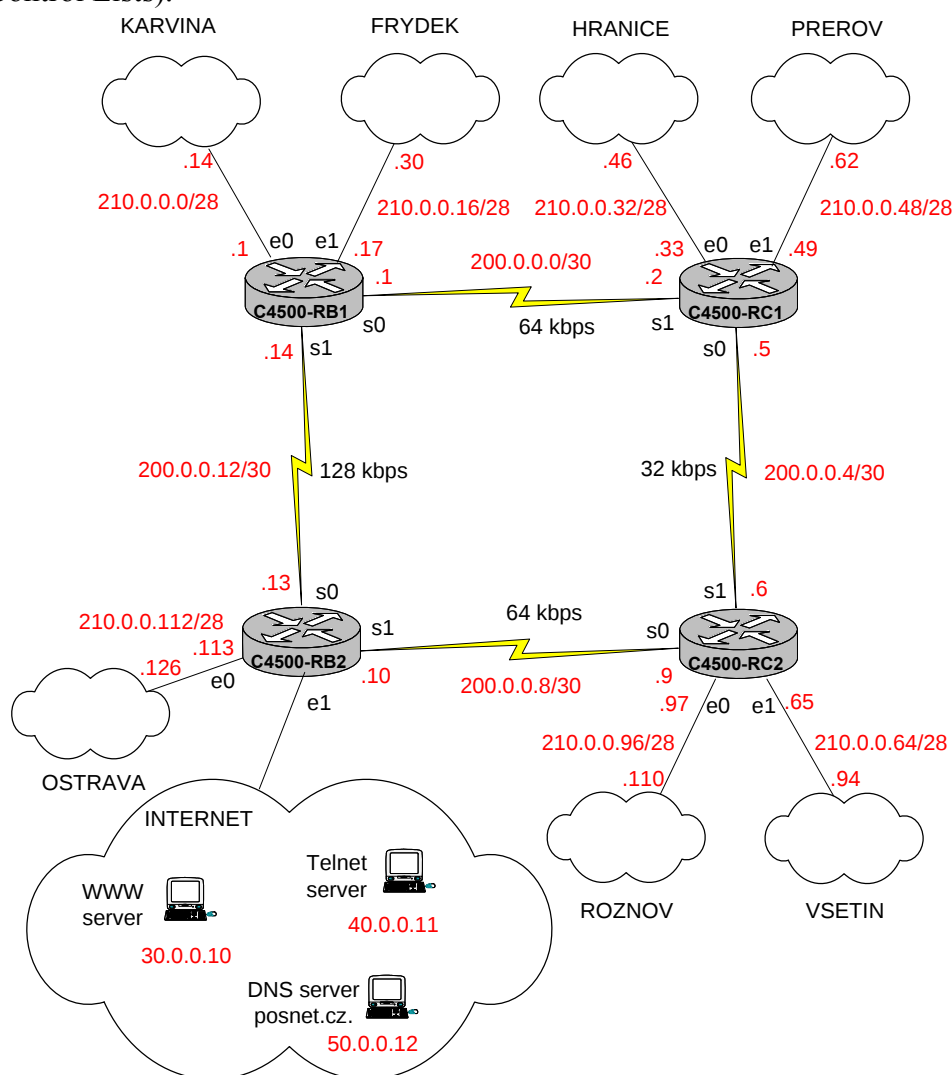
Zadání

Navrhnete a zdokumentujete konfiguraci sítě přidělené lokality korporátní sítě WAN připojené do Internetu.

Popis sítě

Síť (viz obrázek 1) sestává ze lokalit, připojených k páteřní síti založené na směrovačích Cisco 4500. Páteřní směrovače jsou vzájemně propojeny pronajatými synchronními sériovými linkami o různých přenosových rychlostech. Prostřednictvím směrovače RB2 je páteřní síť připojena do Internetu.

Každá lokalita je připojena k páteři přes jedno z rozhraní Ethernet některého směrovače Cisco 4500. Na tomto rozhraní je také realizována filtrace provozu do/z lokality pomocí ACL (Access Control Lists).



Obrázek 1

Aktivní prvky lokalit zahrnují směrovače s OS Linux (microDebian) se směrovacím démonem Zebra (resp. Quagga), přepínače Cisco Catalyst 1900 a rozbočovače. Topologie jednotlivých lokalit, navrhovaných vždy jednou skupinou studentů, jsou uvedeny v příloze. Konkrétní topologii a požadované parametry pro jednotlivé lokality přidělí skupinám studentů cvičící. Páteří síť je předkonfigurována.

Požadavky pro návrh

Vypracujte dokumentaci vaší lokality včetně konfiguračních souborů pro všechny síťové prvky (směrovače Linux i Cisco, přepínače Cisco) a síťové služby (Linux) s ohledem na dále uvedené pokyny.

1. Základní zapojení a konfigurace VLAN

Stanovte a v plánu sítě zdokumentujte konkrétní rozhraní (resp. porty), kterými jsou jednotlivé síťové prvky propojeny. U přepínačů zdokumentujte trunk porty a čísla VLAN přiřazená portům napojeným na jiné aktivní prvky nebo stanice. Čísla VLAN použitých v lokalitě přidělí cvičící. Symbolické označení VLAN a odpovídající čísla shrňte ve zvláštní tabulce.

Uveďte úplné výpisy konfigurací všech přepínačů. Všechna rozhraní směrovačů i přepínačů budou mít nakonfigurován popis (description) informující, kam je dané rozhraní připojeno.

Uveďte náčrt topologie sítě, jak se jeví protokolům 3. vrstvy OSI RM (s odhlédnutím od použití VLAN).

2. Adresování a NAT

Adresní plán

Páteří síť používá pevně stanovený veřejný rozsah IP adres (obr.1). Tento rozsah zahrnuje spojovací linky mezi páteřími směrovači i linky napojující páteří směrovače C4500 na směrovač(e) jednotlivých lokalit.

Pro vnitřní síť každé lokality bude cvičícím přidělen (jiný) veřejný prefix sítě a požadované počty stanic na jednotlivých segmentech lokality. Pro jeden segment sítě bude přidělen privátní rozsah adres a stanice na tomto segmentu budou dosahovat vnějších cílů s použitím překladu adres (NAT).

Navrhněte adresování sítě s maskou podsítě pevné délky. Přidělte pouze nezbytný počet adres, případné zbylé podsítě ponechte pro další rozšiřování lokality. Rozhraním směrovačů přidělujte vždy nejnižší použitelné adresy na podsíti. Zapište navržené adresování přehledně do (původního) plánu sítě, vč. adres rozhraní aktivních prvků.

Uveďte souhrnně v tabulce všechny použité podsítě, vždy s uvedením adresy sítě, masky podsítě, adresy výchozí brány (resp. i alternativních bran) pro podsít', rozsahu použitelných IP adres stanic a broadcast adresy pro podsít'.

Překlad adres (NAT)

Na směrovači připojícím lokalitu k páteřnímu směrovači C4500 je realizován NAT. Adresy z privátního rozsahu se dynamicky mapují na pool veřejně směrovatelných adres z rozsahu vaší lokality. Poolu veřejných adres, na který se privátní adresy z části sítě za NAT překládají, přiřadíte podle požadavku na velikost poolu jednu nebo více podsítí veřejného rozsahu lokality.

Doporučení:

Navrhněte si adresy podsítí v lokalitě tak, aby v případě potřeby použití více podsítí pro pool adres NAT tyto podsítě tvořily souvislý rozsah adres.

Jedna z adres privátního rozsahu za NAT je pevně přidělena WWW serveru. Ten je dostupný zvenjšku pod jednou pevně stanovenou adresou NAT poolu, kterou vyhradíte pouze pro tento účel. Obě adresy jasně uveďte v dokumentaci.

Doporučení:

Z důvodu snadnější konfigurace dynamického NAT kombinovaného se statickým záznamem může být výhodné pro WWW server vyhradit první nebo poslední adresu v NAT poolu.

Do dokumentace uveďte příkazy potřebné pro konfiguraci iptables.

3. Směrování

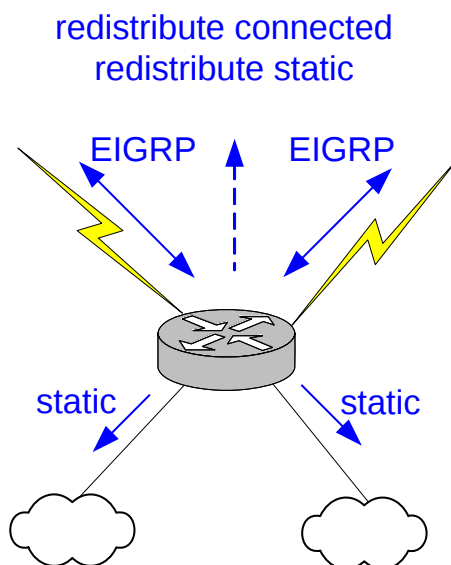
Směrování v lokalitách

Mezi směrovači Linux v jednotlivých lokalitách je podle požadavků pro jednotlivé skupiny studentů provozován směrovací protokol RIP nebo OSPF. U OSPF je použita jediná oblast (area 0).

Všechny směrovače propagují veškeré k nim připojené segmenty sítí (s výjimkou spojovací linky k C4500). Směrovače připojené k C4500 dosahují vnějších cílů pomocí statické implicitní (default) cesty. Z těchto směrovačů propagujte implicitní cestu do použitého dynamického směrovacího protokolu.

Směrování v páteři

Páteřní síť včetně směrování je již realizována a mimo oblast vašeho řešení. Směrování v páteřní síti je z historických důvodů řešeno proprietárním směrovacím protokolem EIGRP firmy Cisco. Do protokolu EIGRP jsou propagovány i spojovací linky do jednotlivých lokalit. Jednotlivé směrovače páteře mají nakonfigurovány statické cesty do veřejných adresních rozsahů přilehlých lokalit. Tyto statické cesty jsou redistribuovány do EIGRP. Nespojnost podsítí v páteři v případě EIGRP není na závadu, protože EIGRP šíří s adresami sítí i masky podsítí. Situace je znázorněna na obrázku 2.



Obrázek 2

Směrování v lokalitě je realizováno pomocí démonů zebra a ripd nebo ospfd. V dokumentaci stručně okomentujte směrování – použitý směrovací protokol, které směrovače dosahují vnějších cílů pomocí statického směrování a které směrovače propagují do směrovacího protokolu implicitní cestu. Uvedte přehledně výpisy konfiguračních souborů těchto démonů ze všech směrovačů lokality s OS Linux.

4. DNS server

Na některém směrovači s OS Linux nakonfigurujte DNS server, který bude poskytovat mapování jmen pro poddoménu domény **posnet.cz**. odpovídající jménu vám přidělené lokality. V DNS databázi budou záznamy pro překlad jmen všech rozhraní směrovačů vaší lokality (mimo rozhraní za NAT), WWW serveru a vždy alespoň jedné stanice na každém segmentu, k němuž lze stanice připojovat. Vhodný systém pojmenovávání zvolte sami a zdokumentujte. DNS server napojte do globálního stromu pod doménu **.posnet.cz**, jejíž DNS server **dns.posnet.cz** již centrální IT oddělení vaší firmy spravuje na adrese **50.0.0.12**. Specifikujte, jaké záznamy je třeba do databáze serveru **dns.posnet.cz** přidat pro zajištění propojení vašeho DNS serveru do stromu.

Mimo překladu doménových jmen na IP adresy bude váš DNS server překládat i IP adresy z veřejného rozsahu vaší lokality na doménová jména. Do konfigurace reverzního překladu vložte PTR záznamy pro všechna jména, pro něž jste vytvořili mapování jména na IP adresu. Předpokládejte, že poskytovatel Internetu pro vaši firmu napojil váš DNS server s ohledem na vám přidělený adresní rozsah do podstromu domény **in_addr.arpa**. Pokud byl vaší lokalitě cvičicím přidělen rozsah adres neodpovídající žádné třídě adres, byla delegace domény pro reverzní překlad u poskytovatele nakonfigurována v souladu s RFC 2317. Spojovací záznamy nakonfigurované v DNS poskytovatele pro delegování reverzního překladu adres vám poskytnete cvičící.

DNS server realizujte na Linuxu pomocí démona bind. V dokumentaci uveďte, na kterém směrovači DNS server běží a všechny podstatné konfigurační soubory démona bind (DNS). Popište vámi navržené schema pojmenovávání rozhraní směrovačů a počítačů v DNS.

5. DHCP server

Nakonfigurujte na vhodném směrovači DHCP server, který bude dynamicky přidělovat adresy stanicím na cvičicím určeném segmentu. Vyhněte se IP adresám, které jsou na segmentu již pevně přiděleny. DHCP server realizujte pomocí démona dhcpd.

Uveďte podstatné konfigurační soubory démona dhcpd.

6. 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 T se lze připojit na Telnet server 40.0.0.11
2. Stanice na segmentu N nesmějí na WWW server 30.0.0.10, jinak smí celá lokalita k WWW serverům vně oblasti přistupovat volně
3. Je dovolen přístup zvnějšku lokality na WWW server lokality umístěný za NAT (pod jeho veřejnou adresou)
4. DNS dotazy směrem ven a odpovědi zvnějšku jsou propouštěny volně, DNS dotazy dovnitř a příslušné odpovědi pouze na adresu vašeho DNS serveru lokality.
5. Stanicím a směrovačům v lokalitě je dovolen ping (ICMP echo request) kamkoli mimo oblast, s výjimkou směrovačů přímo připojených k C4500 však nemají být ohrožovány pokusy o ping zvnějšku
6. Realizujte anti-spoofing filtr, zahazující veškeré (podvržené) pakety přicházející z páteřní sítě se zdrojovou adresou odpovídající adresám uvnitř lokality (jak privátním, tak veřejnému rozsahu). Nedovolte únik paketů s privátní zdrojovou adresou mimo vaši lokalitu (odpověď by byla v páteři nesměrovatelná).

Veškerý výše neuvedený provoz je zakázán.

Přiřazení segmentů T a N určí cvičící.

Uveďte konfiguraci ACL pro oba směry provozu formou tabulky ve tvaru podle Příkladu konfigurace ACL z http://www.cs.vsb.cz/grygarek/POS/projekt0304/acl_priklad.pdf. Položky ACL v dokumentaci symbolicky označte číslem požadavku (viz číslování výše), k jehož realizaci pravidlo slouží.

Uveďte na které rozhraní a který směr budete jednotlivé ACL aplikovat..

**Nezapomeňte vždy na povolení obou směrů každého z dovolených typů provozů.
Nezapomeňte na existenci NAT ve vaší lokalitě**

Organizace, odevzdávání a hodnocení projektu

V každém cvičení jsou studenti rozděleni do skupin, každá skupina (max. 4 studentů) navrhne a zdokumentuje jednu z lokalit sítě.

Projekt bude hodnocen za skupinu jako celek po částech odevzdávaných (nejpozději) v termínech uvedených pro každou část v rozvrhu cvičení. Maximální bodová hodnocení jednotlivých částí jsou uvedena níže. V případě překročení termínu odevzdání se body nepřidělují, odevzdání všech částí ve cvičícím akceptované kvalitě je však povinné.

Části projektu budou odevzdány v písemné podobě, v elektronické podobě pouze při předchozím odsouhlasení ze strany cvičícího.

Při hodnocení odevzdané dokumentace bude zohledněna o celková kultura zpracování, zejména přehlednost.

Skupina odevzdává postupně tyto části projektu:

1. Náskres topologie s konkretizací rozhraní směrovačů a přiřazení portů přepínačů do VLAN, náskres ekvivalentní topologie 3. vrstvy OSI RM, konfigurace přepínačů a VLAN (cv. 7) – 2 b
2. Adresování, NAT (cv. 8) -3b
3. Směrování – konfigurace Zebra (cv. 10) – 2 b
4. DNS (cv. 11) – 4 b
5. Dhcpd (cv. 12) – 2b
6. ACL (cv. 13). – 3 b

Podrobné požadavky na náležitosti jednotlivých odevzdávaných částí jsou uvedeny v Požadavcích pro návrh.

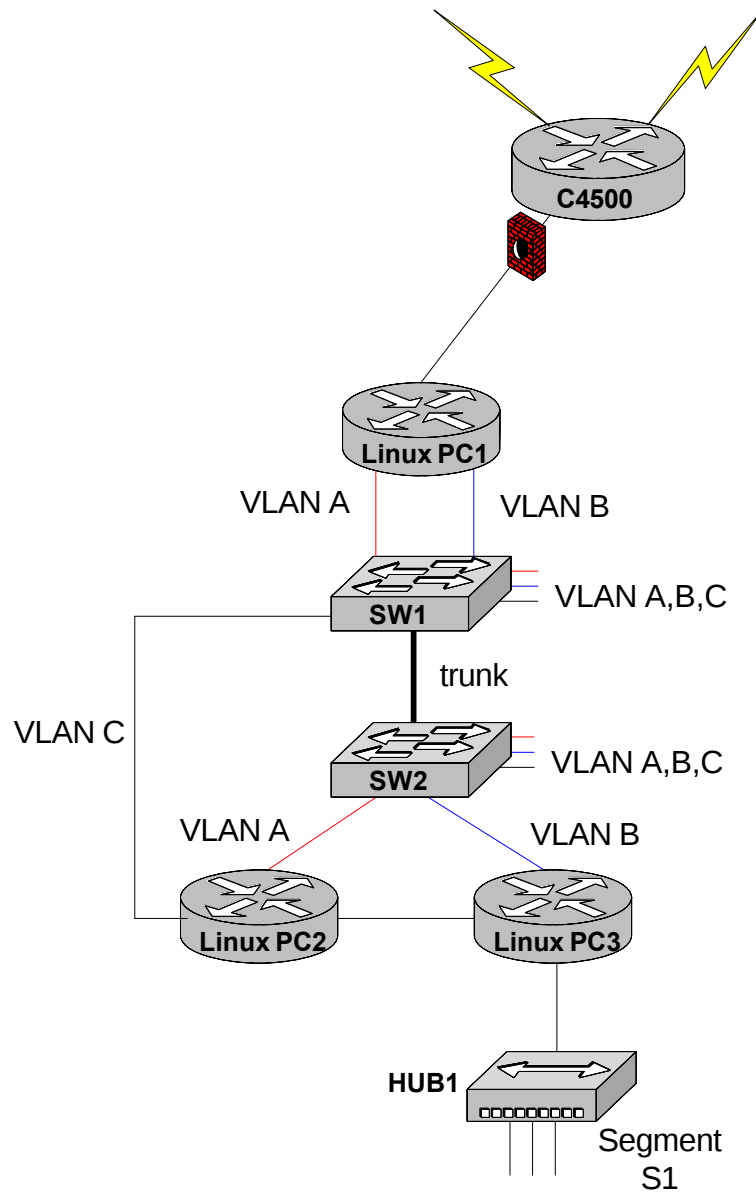
Pokyny pro cvičící

Každé skupině přidělit:

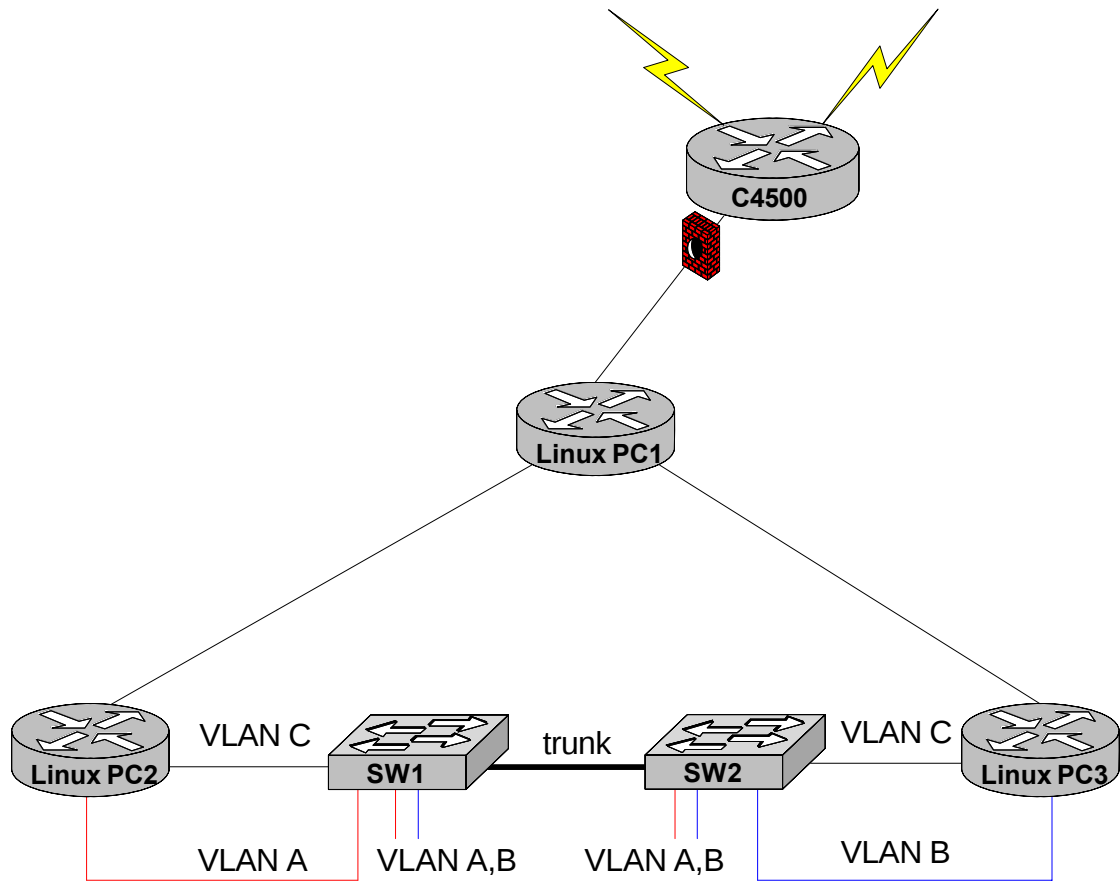
- Umístění lokality vzhledem k páteři (rozhraní C4500, resp. jméno lokality)
- Topologii lokality
- Rozsah veřejných a privátních adres lokality
- Počty požadovaných stanic na jednotlivých segmentech lokality
- Směrovací protokol lokality (RIP nebo OSPF)
- Skutečná čísla VLAN (≥ 2) a počty portů v jednotlivých VLAN
- Segment, pro který pracuje DHCP server (ne segment za NAT)
- Segment sítě podléhající NAT
- Počet adres NAT poolu.
- Segmenty T a N pro ACL
- Záznamy DNS serveru poskytovatele delegující část poddomény in_addr.arpa na DNS server lokality.

Příloha – topologie lokalit

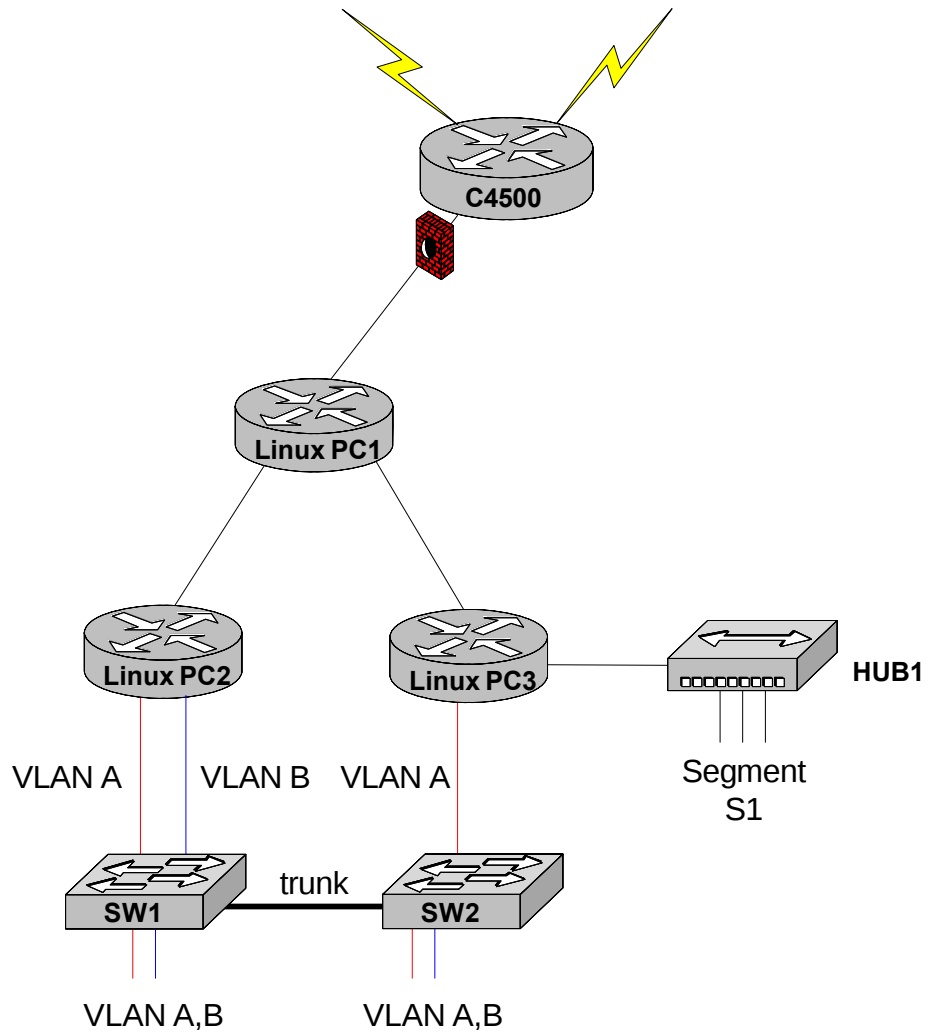
Topologie 1



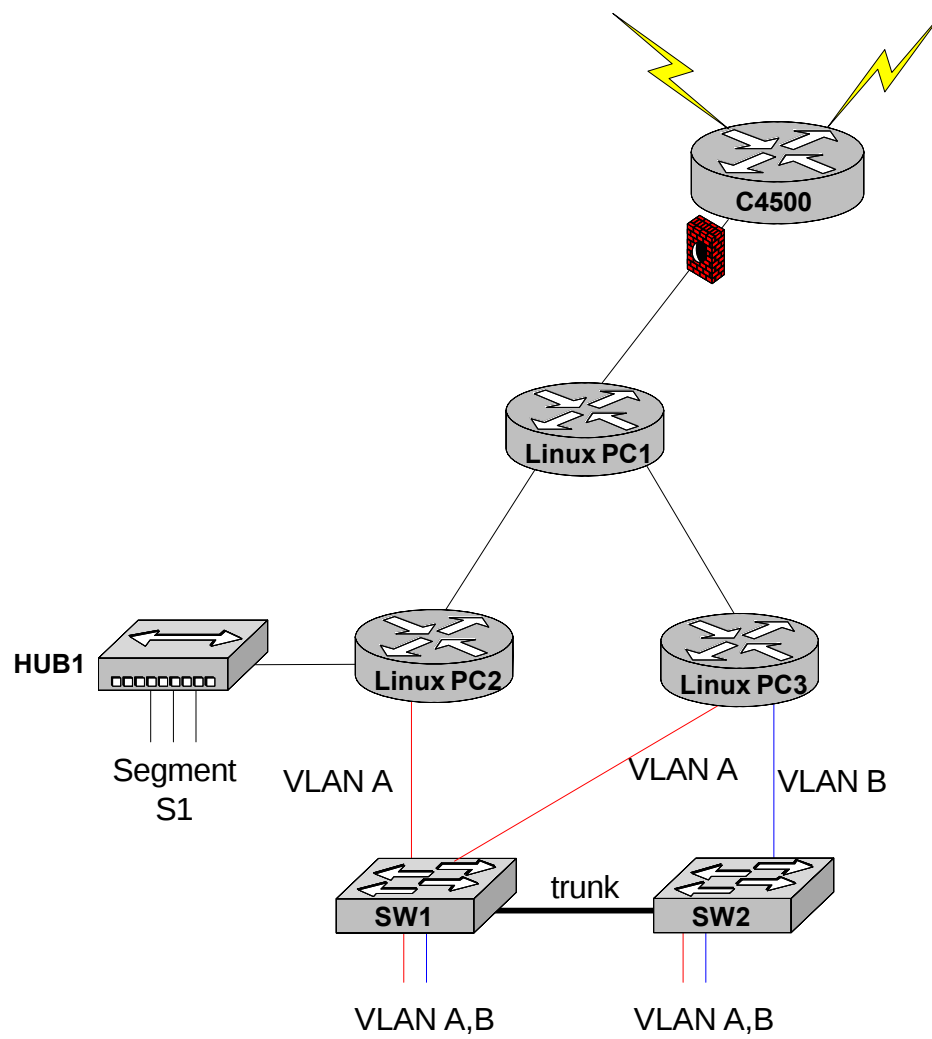
Topologie 2



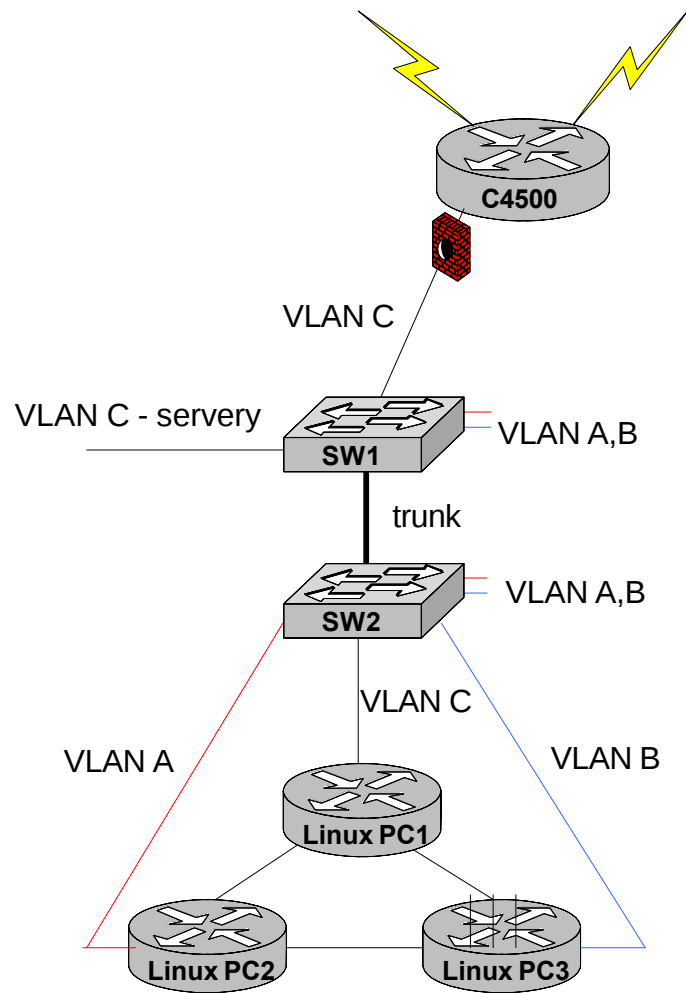
Topologie 3



Topologie 4



Topologie 5



Topologie 6

