Počítačové sítě, ZS 2007/2008, kombinované studium
Návrh sítě – zadání

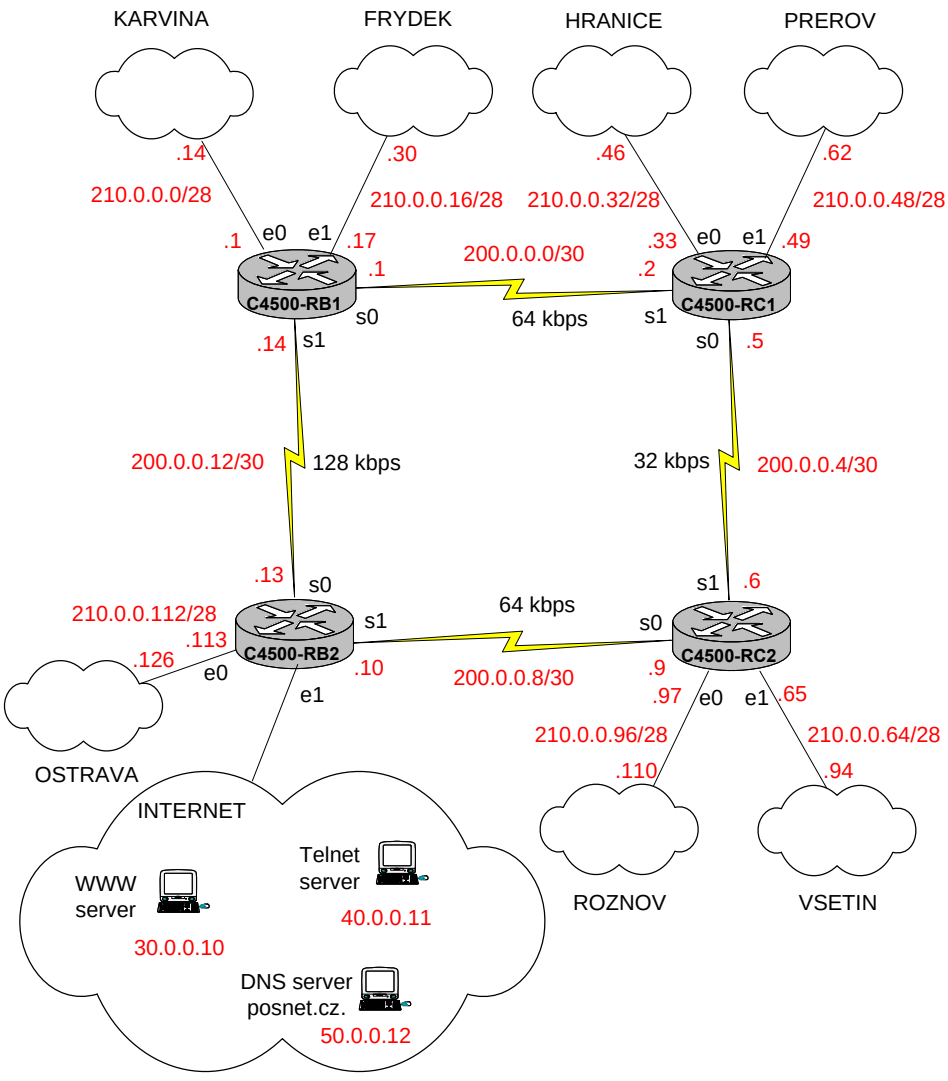
Petr Grygárek, FEI VŠB-TU Ostrava

Zadání

Navrhněte a zdokumentujte konfiguraci sítě přidělené lokality korporátní sítě WAN připojené do Internetu.

Popis sítě

Síť (viz obrázek 1) sestává z lokalit, připojených k páteřní síti založené na směrovačích Cisco (v obrázcích je pro příklad vyznačen model C4500). 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. Na tomto rozhraní je také realizována filtrace provozu do/z lokality pomocí ACL (Access Control Lists). Topologie lokalit jsou uvedeny v Příloze (přidělí tutor).



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 tutor. Konfigurace páteřní sítě (mimo ACL vaší lokality) již není ve vaši kompetenci.

Požadavky pro návrh

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

Základní zapojení a konfigurace VLAN

Stanovte a v plánku 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 tutor. Symbolické označení VLAN a odpovídající čísla shrněte ve zvláštní tabulce.

Uveďte konfigurační příkazy pro konfiguraci všech přepínačů (**pouze příkazy pro realizaci požadované funkcionality, ne úplné výpisy s implicitním nastavením** (show running-config)). Všechna rozhraní směrovačů i přepínačů budou mít nakonfigurován popis (description) informující, kam je dané rozhraní připojeno.

Uveďte nákres ekvivalentní topologie sítě, jak se jeví protokolům 3. vrstvy OSI RM (s odhlédnutím od použití VLAN). Přepínač reprezentující VLAN **b** na přepínači **SWa** označte **SWa/b**. V nákresu také označte fyzická rozhraní síťových prvků.

Adresní plán

Páteřní síť používá pevně stanovený veřejný rozsah IP adres (obr.1). Tento rozsah zahrnuje spojovací linky mezi páteřními směrovači i linky napojující páteřní směrovače Cisco na směrovač(e) jednotlivých lokalit.

Pro vnitřní sítě každé lokality bude tutorem 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) plánku sítě (k jednotlivým síťovým rozhraním), vč. adres rozhraní aktivních prvků. Toto schéma přikládejte vždy znovu při odevzdávání dalších částí projektu.**

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

Překlad adres (NAT)

Na směrovači připojujícím lokalitu k páteřnímu směrovači Cisco je realizován NAT. Adresy z privátního rozsahu se dynamicky mapují na rozsah veřejně směrovatelných adres alokovaný z rozsahu vaši lokality. Rozsahu veřejných adres, na který se privátní adresy z části sítě za NAT překládají, rezervujte podle potřeby jednu nebo více podsítí veřejného rozsahu lokality.

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

Jedna z adres privátního rozsahu za NAT je pevně přidělena WWW serveru. Ten je dostupný zvnějšku pod jednou pevně stanovenou adresou veřejného rozsahu pro NAT, kterou vyhraďte pouze pro tento účel. **Obě adresy jasně uveďte v textové části dokumentace.**

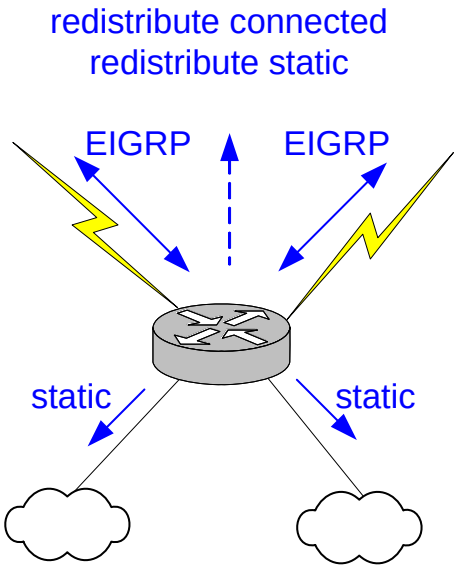
Doporučení:
Z důvodu snadnější konfigurace dynamického NAT kombinovaného se statickým záznamem může být výhodné pro WWW server vyhradit první nebo poslední adresu z rozsahu adres pro NAT.

Do dokumentace uveďte příkazy potřebné pro konfiguraci iptables.

Směrování

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. Nespojitost IP 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 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 páteřním směšovačům Cisco). Směrovače připojené k páteřním směšovačům Cisco dosahují vnějších cílů pomocí statické implicitní (default) cesty. Z těchto směrovačů propagujte implicitní cestu do dynamického směrovacího protokolu použitého v lokalitě.

Směrování v lokalitě je realizováno pomocí démonů **zebrad a ripd nebo ospfd.**
V dokumentaci textově stručně okomentujte směrování – použitý směrovací protokol, které směrovače dosahují vnějších cílů pomocí statického směrování a které směrovače propagují do směrovacího protokolu implicitní cestu. **Uveďte přehledně výpisy konfiguračních souborů těchto démonů ze všech směrovačů lokality s OS Linux** (jen potřebný nastavení, ne implicitně přítomné příkazy).

Zabezpečení sítě - ACL

Na rozhraní páteřního směrovače Cisco 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, stanice lokality však nemají být ohrožovány pokusy o ping zvnějšku (mimo serverů). Na vnější rozhraní směrovačů přímo připojených k C4500 je žádost o ping povolena.
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 vaší lokalitu (odpověď by byla v páteři nesměrovatelná).

Veškerý výše neuvedený provoz je zakázán.

Přiřazení segmentů T a N určí tutor.

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 vaši lokalitě

Volitelná část: 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 vaši 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 vaši 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 vaši lokalitě tutorem 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 poskytne tutor.

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.

Volitelná část: DHCP server

Nakonfigurujte na vhodném směrovači (Linux) DHCP server, který bude dynamicky přidělovat adresy stanicím na tutorem 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.

Organizace, odevzdávání a hodnocení projektu

Studenti budou 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 Harmonogramu

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

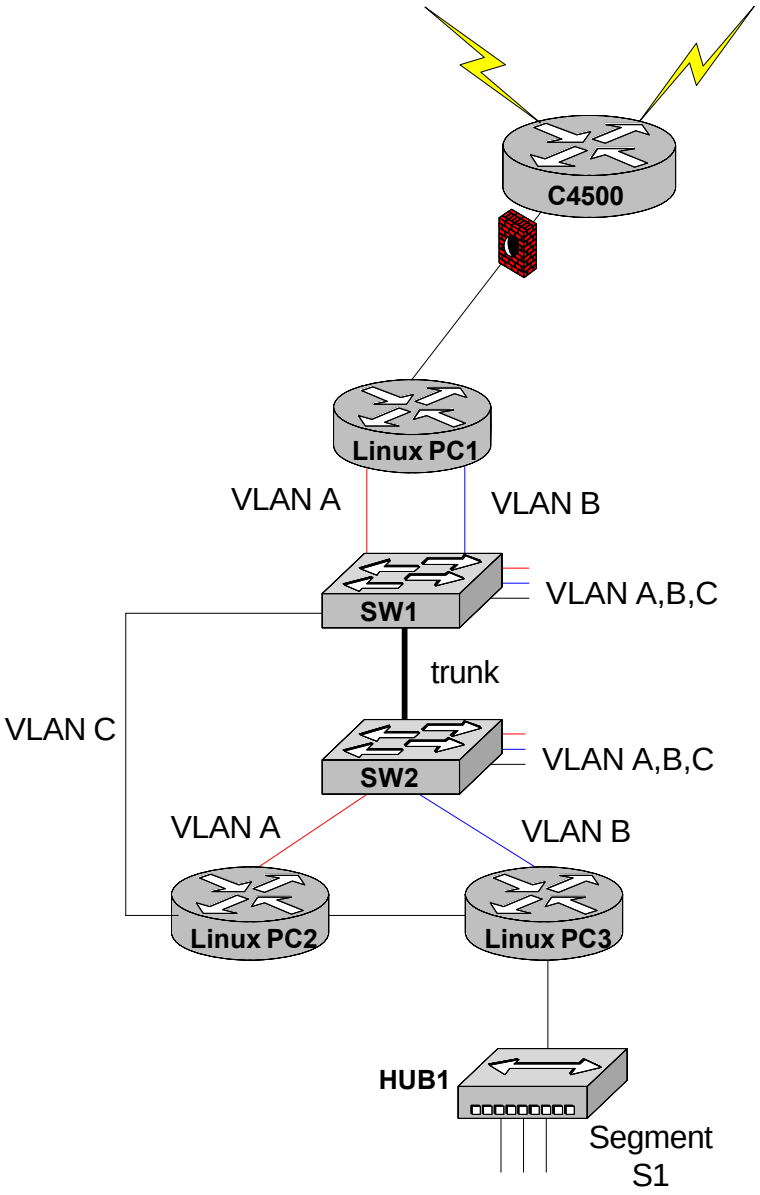
Pokyny pro tutory

Každé skupině přidělit:

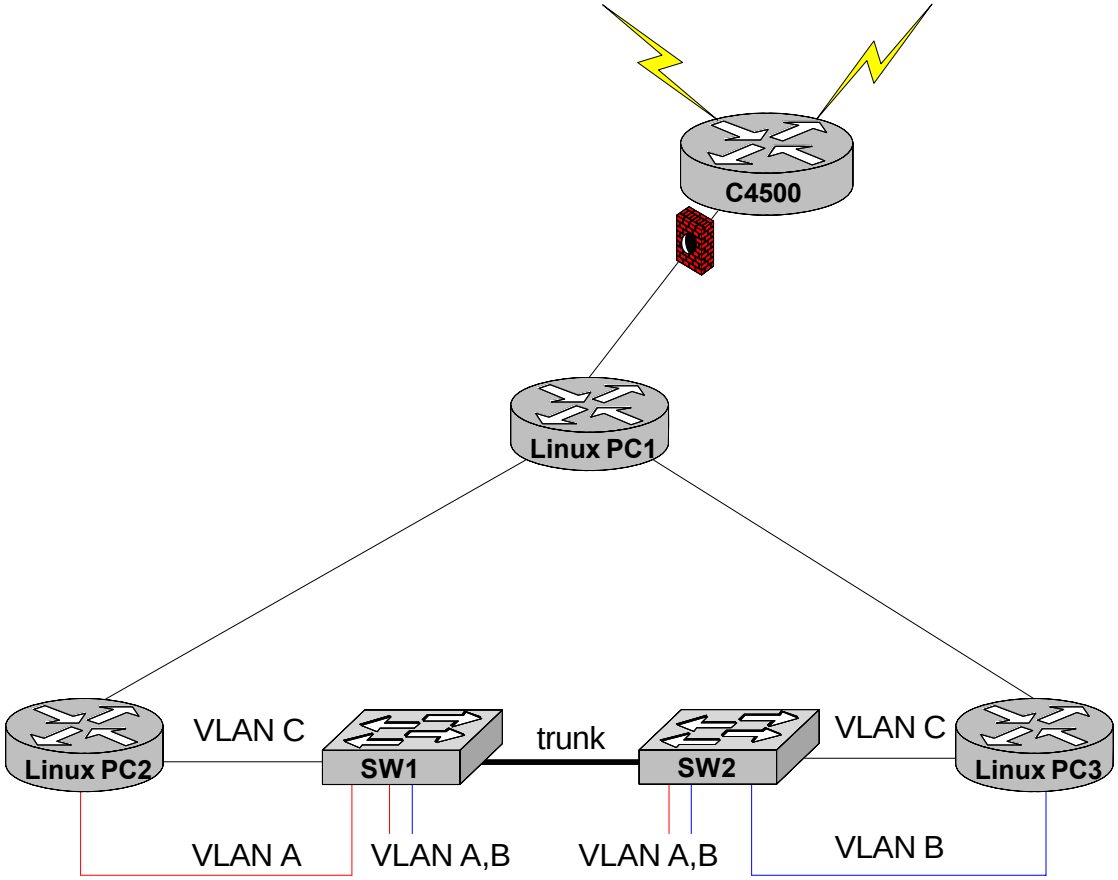
- Umístění lokality vzhledem k páteři (rozhraní Cisco routeru, resp. jméno lokality)
- Topologii lokality
- Skutečná čísla VLAN (>=2) a počty portů v jednotlivých VLAN
- Rozsah veřejných a privátních adres lokality
- Počty požadovaných stanic na jednotlivých segmentech lokality, počet adres NAT poolu
- Směrovací protokol lokality (RIP nebo OSPF)
- Skutečné segmenty pro zástupné symboly T a N pro ACL
- Na vyžádání
  - Segment, pro který pracuje DHCP server (ne segment za NAT)
  - Záznamy DNS serveru poskytovatele delegující část poddomény in_addr.arpa na DNS server lokality.

Příloha – topologie lokalit

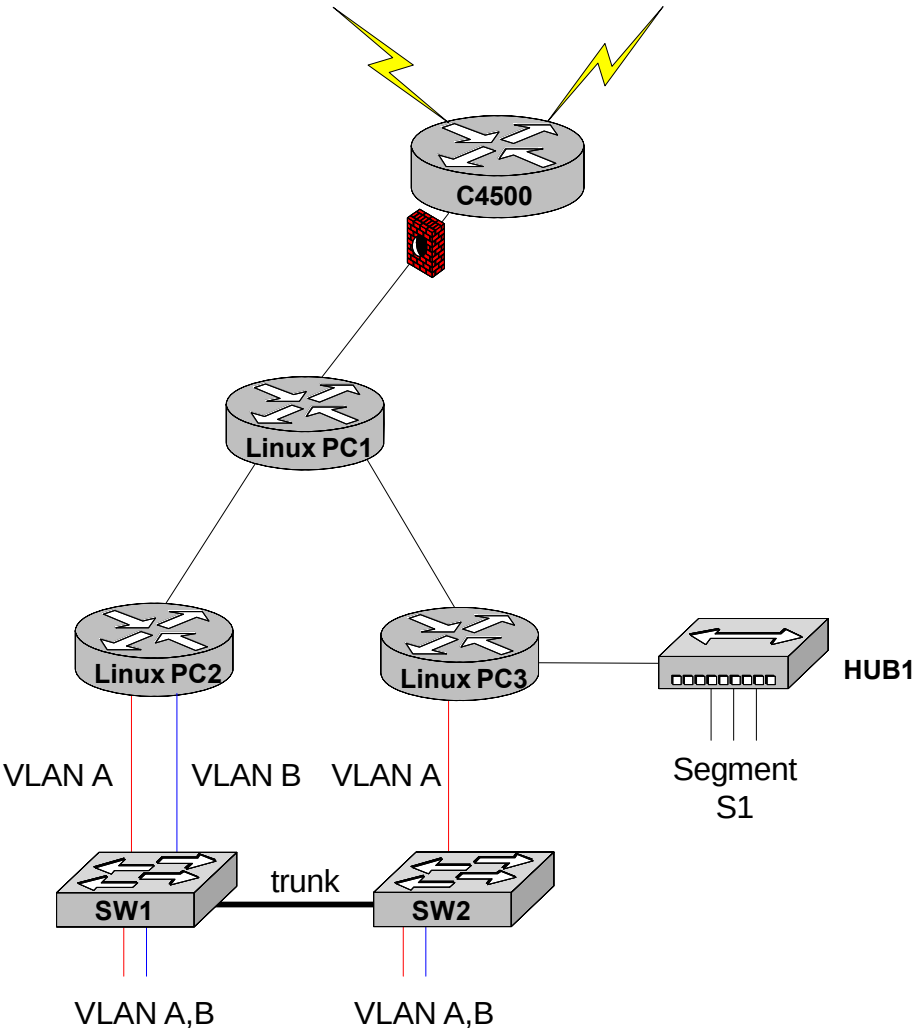
Topologie 1


C4500
Linux PC1
VLAN A
VLAN B
SW1
VLAN A,B,C
trunk
VLAN C
SW2
VLAN A,B,C
VLAN A
VLAN B
Linux PC2
Linux PC3
HUB1
Segment
S1

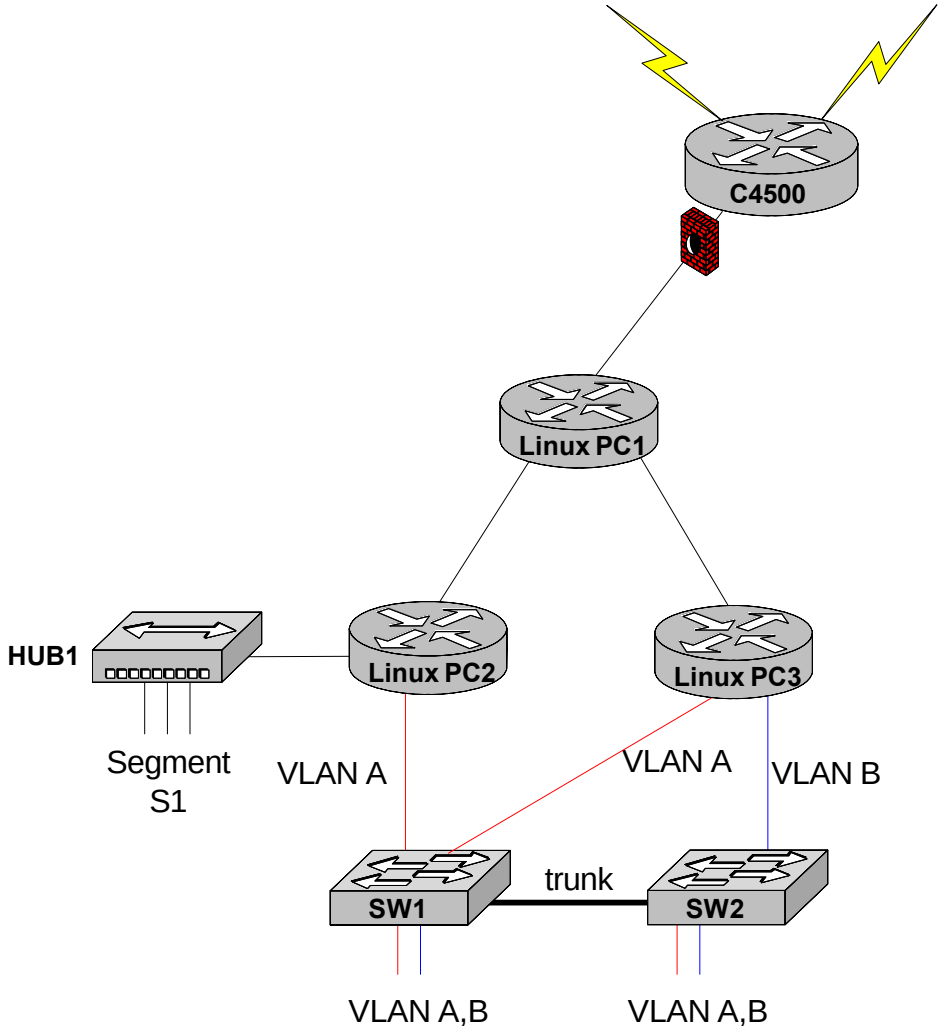
Topologie 2


C4500
Linux PC1
Linux PC2
VLAN C
SW1
trunk
SW2
VLAN C
Linux PC3
VLAN A
VLAN A,B
VLAN A,B
VLAN B

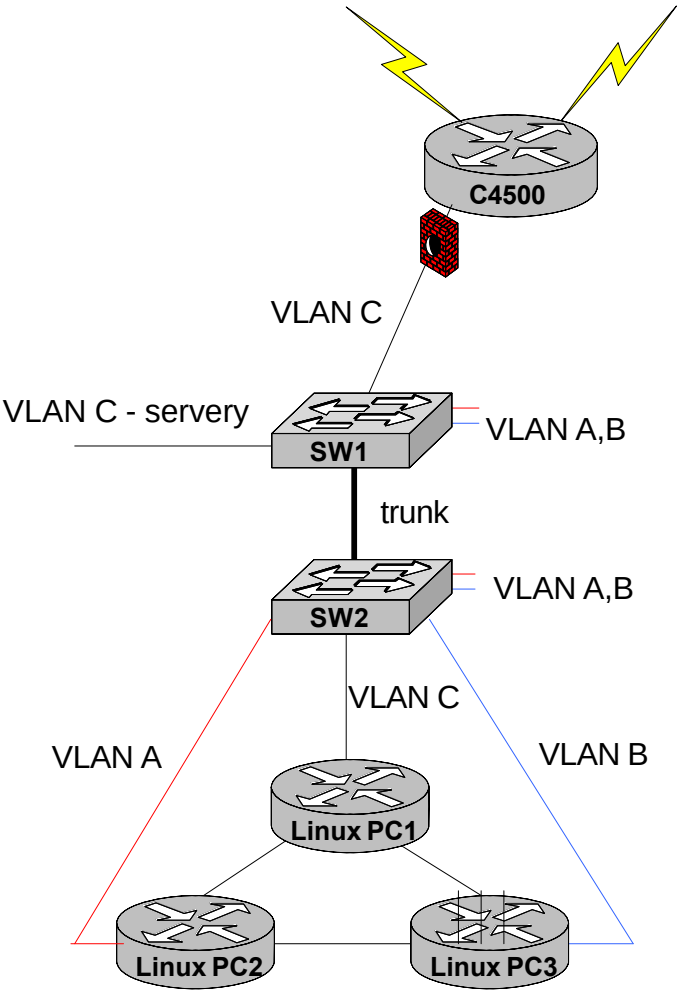
Topologie 3


C4500
Linux PC1
Linux PC2
Linux PC3
HUB1
VLAN A
VLAN B
VLAN A
Segment
S1
SW1
trunk
SW2
VLAN A,B
VLAN A,B

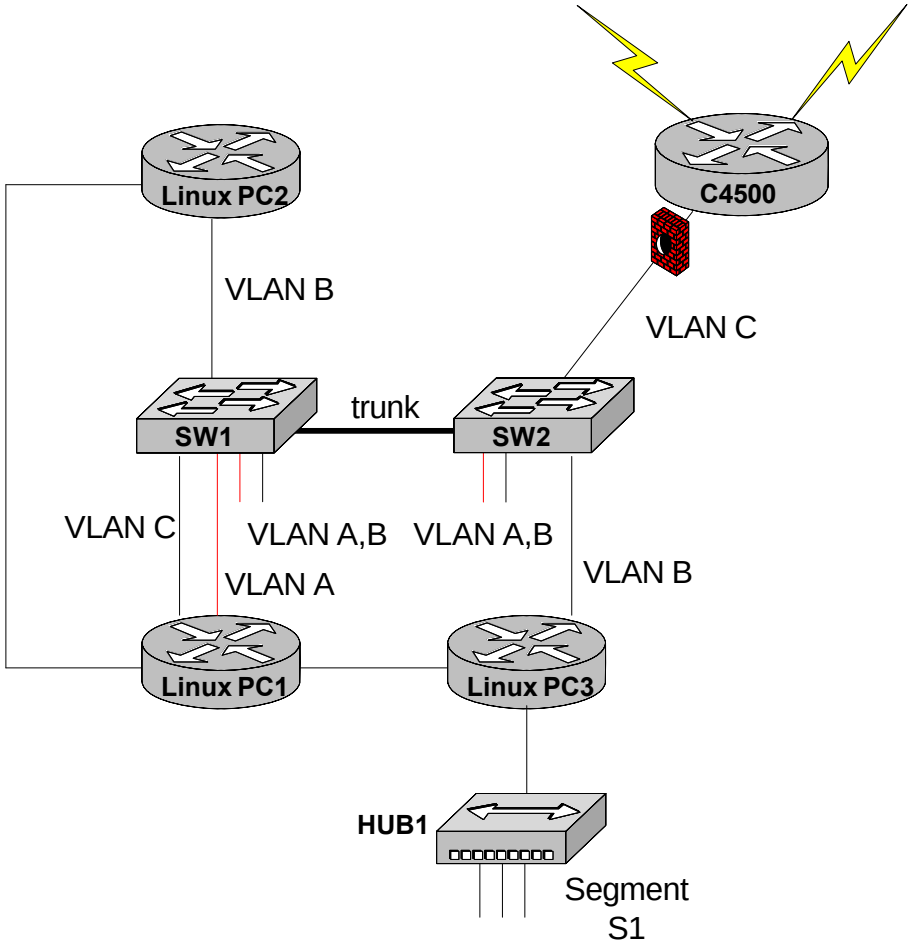
Topologie 4


C4500
Linux PC1
HUB1
Linux PC2
Linux PC3
Segment
S1
VLAN A
VLAN A
VLAN B
trunk
SW1
SW2
VLAN A,B
VLAN A,B

Topologie 5


C4500
VLAN C
VLAN C - servery
SW1
VLAN A,B
trunk
SW2
VLAN A,B
VLAN C
VLAN A
VLAN B
Linux PC1
Linux PC2
Linux PC3

Topologie 6


Linux PC2
C4500
VLAN B
VLAN C
SW1
trunk
SW2
VLAN C
VLAN A,B
VLAN A,B
VLAN A
VLAN B
Linux PC1
Linux PC3
HUB1
Segment
S1