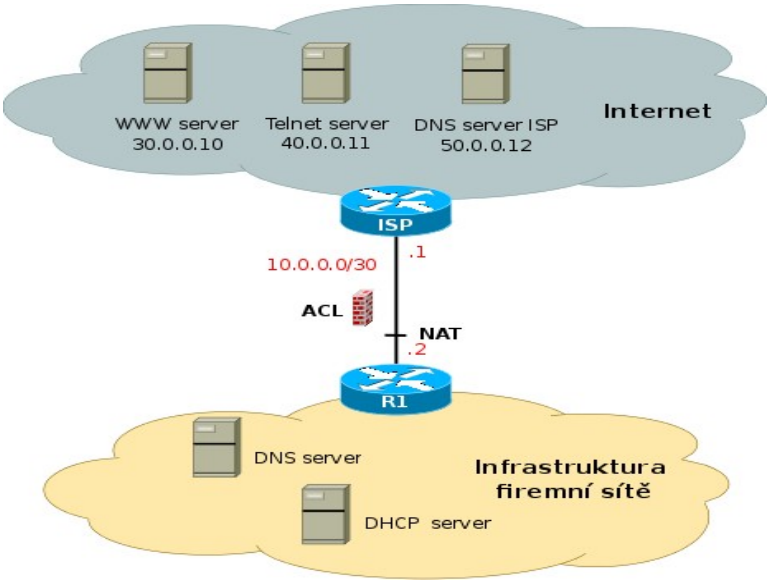
Počítačové sítě – ZS 2009/2010
Projekt návrhu sítě – zadání

Petr Grygárek, FEI VŠB-TU Ostrava

Zadání

Navrhněte konfiguraci podnikové sítě připojené do Internetu. Řešení po částech implementujre, ověřte a odevzdejte v Distribuované virtuální laboratoři počítačových sítí (Virtlab).

Popis sítě



Firemní síť je připojena ke směrovači ISP poskytovatele Internetu hraničním směrovačem zákazníka R1. Spojovací linka mezi směrovači ISP a R1 je adresována privátními adresami, které nejsou propagovány do Internetu. Na směrovači ISP je konfigurována statická cesta do sítí veřejného adresního rozsahu firmy, který je směrovačem ISP také propagován do Internetu.

Na hraničním směrovači firmy (R1) je realizována filtrace provozu mezi firmou a Internetem pomocí ACL (Access Control Lists). Počítače na Internetu jsou představovány servery na adresách 30.0.0.10, 40.0.0.11 a 50.0.0.12.

Aktivní prvky infrastruktury firemní sítě zahrnují směrovače Cisco, přepínače Cisco Catalyst řady 2900 a rozbočovače. Infrastruktura firemní sítě odpovídá jedné z topologií uvedených v příloze (pro skupinou studentů přidělí spolu s dalšími parametry cvičící). Směrovač ISP a servery v Internetu jsou předkonfigurovány a nejsou předmětem řešení projektu.

Požadavky pro návrh

Vypracujte konfiguraci sítě vaši firmy pro všechny síťové prvky (směrovače a přepínače), stanice a síťové služby (Linux) s ohledem na dále uvedené pokyny.

1. Adresní plán a konfigurace VLAN

Vypracujte a ve Virtlabu odevzdejte nákres ekvivalentní topologie sítě, jak se jeví protokolům 3.vrstvy OSI RM (tj. s odhlédnutím od použití VLAN).
Pro adresování firemní sítě bude cvičícím přidělen veřejný prefix sítě a požadované počty stanic na jednotlivých segmentech. Jeden ze segmentů sítě slouží pro obsluhu velkého počtu externích uživatelů a je na hranici firemní sítě skryt za NAT s omezeným počtem veřejných adres (v rámci návrhu adresování k tomu účelu vyhraďte jednu podsíť veřejného rozsahu). O který segment půjde, rozsah privátních adres a počet sdílených veřejných adres budou přiděleny cvičícím. Spojovací linka mezi směrovačem R1 a ISP je adresována podle obrázku.

Veřejný adresní rozsah firemní sítě adresujte podsíťováním s maskou podsítě proměnné délky (VLSM). Přidělte pouze nezbytný počet adres, případnou zbylou část adresního rozsahu ponechte pro další rozšiřování firmy. Při návrhu podsíťování nezapomeňte na rozsah veřejných adres vyhrazených pro NAT.
Rozhraním směrovačů přidělujte vždy nejnižší použitelné adresy na podsíti. PC na jednotlivých segmentech přiřaďte poslední použitelnou adresu z rozsahu příslušného segmentu. Navržené adresování zapište přehledně do původního plánku sítě i plánku ekvivalentní topologie a obojí odevzdejte jako soubor **ve formátu PDF** ve Virtlabu. V samostatném textovém dokumentu **ve formátu PDF** shrněte 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.

Z důvodu automatického testování je nutné IP adresy jednotlivých rozhraní síťových prvků zadat ještě do odevzdávacího formuláře ve Virtlabu (jednorázově, lze uložit pro pozdější použití).

U všech směrovačů i přepínačů nakonfigurujte jejich jména (příkaz **hostname**). Na všech přepínačích nakonfigurujte přiřazení portů do VLAN a trunk porty. Čísla VLAN použitých ve firemní sítí přidělí cvičící. Na všech směrovačích nakonfigurujte IP adresy rozhraní. Všechna rozhraní směrovačů i přepínačů budou mít nakonfigurován popis (příkaz **description**) informující, kam je dané rozhraní připojeno.

Na síťových rozhraních směrovačů a PC nastavte IP adresy a všechna rozhraní aktivujte, abyste dovolili vnitřní komunikaci zařízení zatím alespoň v rámci jednotlivých segmentů sítě.

2. Směrování a NAT

Uvnitř firmy 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. Hraniční směrovač R1 dosahuje sítí na Internetu pomocí statické implicitní (default) cesty. Ze směrovače R1 propagujte implicitní (default) cestu do použitého dynamického směrovacího protokolu.

Na rozhraní hraničního směrovače R1 vedoucím ke směrovači ISP realizujte dynamický NAT pro vnitřní segment firmy, který používá privátní adresy. Vnitřní privátní adresy se pomocí NAT dynamicky mapují na rozsah veřejně směrovatelných adres vyhrazený při návrhu podsíťování. Rozsahu veřejných adres pro NAT přidělte podle zadaného požadavku na jeho velikost odpovídající část rozsahu veřejných adres.

Na směrovači realizujícím NAT nakonfigurujte vzdálený přístup pomocí Telnetu (heslo na konzoli i pro vstup do privilegovaného režimu (enable password) nastavte na „cisco“)
Na všech PC nastavte výchozí bránu.

3. DHCP server (pro kombinovné studium volitelné)

Na cvičícím stanoveném směrovači nakonfigurujte DHCP server, který bude dynamicky přidělovat parametry síťového připojení stanicím na určeném segmentu (vč. adresy lokálního DNS serveru). Pokud na segmentu s DHCP konfigurujtete DNS server, nakonfigurujte na něm adresu staticky. Vyhněte se přidělování IP adres, které jsou na segmentu již pevně přiděleny.

4. DNS server (pro kombinovné studium volitelné)

Na cvičícím stanoveném PC s OS Linux nakonfigurujte DNS server.
V testovacím/odevzdávacím formuláři uveďte IP adresu zvoleného PC. DNS server bude poskytovat mapování jmen pro poddoménu domény **isp.cz.** odpovídající jménu vaší firmy (přidělí cvičící). Doménové jméno jmenného serveru samotného bude **ns.<JMENO_FIRMY>.isp.cz**. V DNS databázi vašeho serveru budou záznamy pro překlad jmen všech rozhraní vnitřních směrovačů firmy (R1-R3), mimo rozhraní do segmentu s privátními adresami). Jména rozhraní směrovačů budou mít tvar

I-<IP-ADRESA-ROZHRANI ODDELENA POMLCKAMI>.<JMENO_FIRMY>.isp.cz.
(např. I58-196-1-10.mojefirma.isp.cz)

DNS server napojte do globálního stromu pod doménu **.isp.cz.**, jejíž DNS server **dns.isp.cz** již běží na adrese **50.0.0.12** a je předkonfigurován.

Mimo překladu doménových jmen na IP adresy bude váš DNS server překládat i IP adresy z veřejného rozsahu vaši firmy na doménová jména. **Do konfigurace reverzního překladu vložte PTR záznamy pro všechna jména, pro něž jste vytvořili mapování jména na IP adresu**. Správce DNS ISP napojil váš DNS server s ohledem na vám přidělený adresní rozsah do podstromu domény **in_addr.arpa** (předkonfigurováno).

DNS server realizujte na Linuxu pomocí démona **bind** a konfigurujte jej jako **rekurzivní**. Jelikož nejsme připojeni k Internetu, jako jeho root name server nastavte DNS server na adrese **50.0.0.12.**

5. Zabezpečení sítě - ACL

Na rozhraní hraničního směrovače R1 vedoucím ke směrovači ISP implementujte filtraci provozu s použitím ACL (Access Control Lists). Požadavky jsou uvedeny dále. Cvičící stanoví, který ze segmentů přidělené topologie bude v roli segmentu níže symbolicky označeného T a který segmentu N.

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 firma k WWW serverům na Internetu přistupovat volně
3. DNS dotazy směrem ven a odpovědi zvnějšku jsou propouštěny volně, DNS dotazy dovnitř a příslušné odpovědi pouze na adresu vašeho firemního DNS serveru.

4. Stanicím a směrovačům ve firmě je dovolen ping (ICMP echo request) kamkoli do Internetu, stanice firmy však nemají být ohrožovány pokusy o ping zvnějšku (mimo DNS serveru, na který ping zvnějšku prochází). Na vnější rozhraní směrovače R1 je žádost o ping také povolena.
5. Realizujte anti-spoofing filtr, zahazující veškeré (podvržené) pakety přicházející z Internetu se zdrojovou adresou odpovídající adresám uvnitř firmy (jak privátnímu, tak veřejnému rozsahu). Nedovolte únik paketů s privátní zdrojovou adresou mimo vaší firmu (odpověď by byla v Internetu nesměrovatelná).

Veškerý výše neuvedený provoz je zakázán.
Nezapomeňte vždy na povolení obou směrů každého z dovolených typů provozů.

Organizace, odevzdávání a hodnocení projektu

Studenti budou rozděleni do skupin po dvou, v kombinovaném studiu může být na vyžádání skupina i jednočlenná. Každá skupina řeší společné zadání sítě v jedné firmě.
Projekt bude hodnocen za skupinu jako celek po částech odevzdávaných (nejpozději) v termínech uvedených pro každou část v rozvrhu cvičení, resp. tutoriálů. Maximální bodová hodnocení jednotlivých částí jsou uvedena tamtéž. V případě překročení termínu odevzdání se body nepřidělují. Pro udělení zápočtu je nutné dosáhnout minimální množství bodů specifikované na WWW stránkách předmětu v sekci *Podmínky zápočtu, způsob hodnocení* .

Části projektu budou odevzdány v systému Virtlab kterýmkoli členem řešitelské skupiny. Před odevzdáním je doporučeno nechat konfiguraci systémem Virtlab otestovat a opravit části řešení, které testům nevyhověly. Odevzdané řešení mohou všichni členové skupiny do termínu odevzdání pro danou část libovolně upravovat. Při odevzdávání je nutné vyplnit všechny položky odevzdávacího formuláře požadované pro danou část..

Orientace v odevzdaném řešení může být po odevzdání **přezkoušena** a **podmínit přiznání bodů** jednotlivým studentům řešitelské skupiny.

Poznámky k práci ve Distribuované virtuální laboratoři počítačových sítí

Použijte portál ***http://virtlab.cs.vsb.cz,*** Uživatelský manuál je umístěn v hlavním menu systému (sekce Nápověda).

Konta budou automaticky vytvořena všem zapsaným studentům POS na začátku semestru. Pro jednotlivé skupiny studentů budou v systému vytvořeny jim přidělené parametrizace zadání. Jako přihlašovací jméno použijte osobní číslo, heslo stejné jako u školní pošty a jiných systémů z VŠB-TU (z LDAP).

Uživatelská kvóta je standardně nastavena na 10 hodin, což určuje maximání souhrnnou délku rezervací, které může student realizovat v libovolném (plovoucím) 7-denním časovém okně. S ohledem na množství studentů v předmětu a opakující se přeplnění systému rezervacemi těsně před termíny odevzdání je nanejvýše doporučováno řešit a odevzdat projekty s dostatečným předstihem.

Volné síťové prvky se pro každou rezervaci vyhledávají dynamicky a automaticky se propojují do požadované topologie. Při každé rezervaci tak mohou být použity jiné prvky a propojení může být realizováno jinými rozhraními. Pro automatické přemapování názvů

rozhraní mezi rezervacemi lze použít pomocnou funkci Přemapování konfiguračních souborů v menu Podpůrné nástroje nebo Archivu konfigurací.

Rozbočovače ve Vaší topologii jsou nekonfigurovatelné a v rámci řešení se jimi není třeba zabývat.

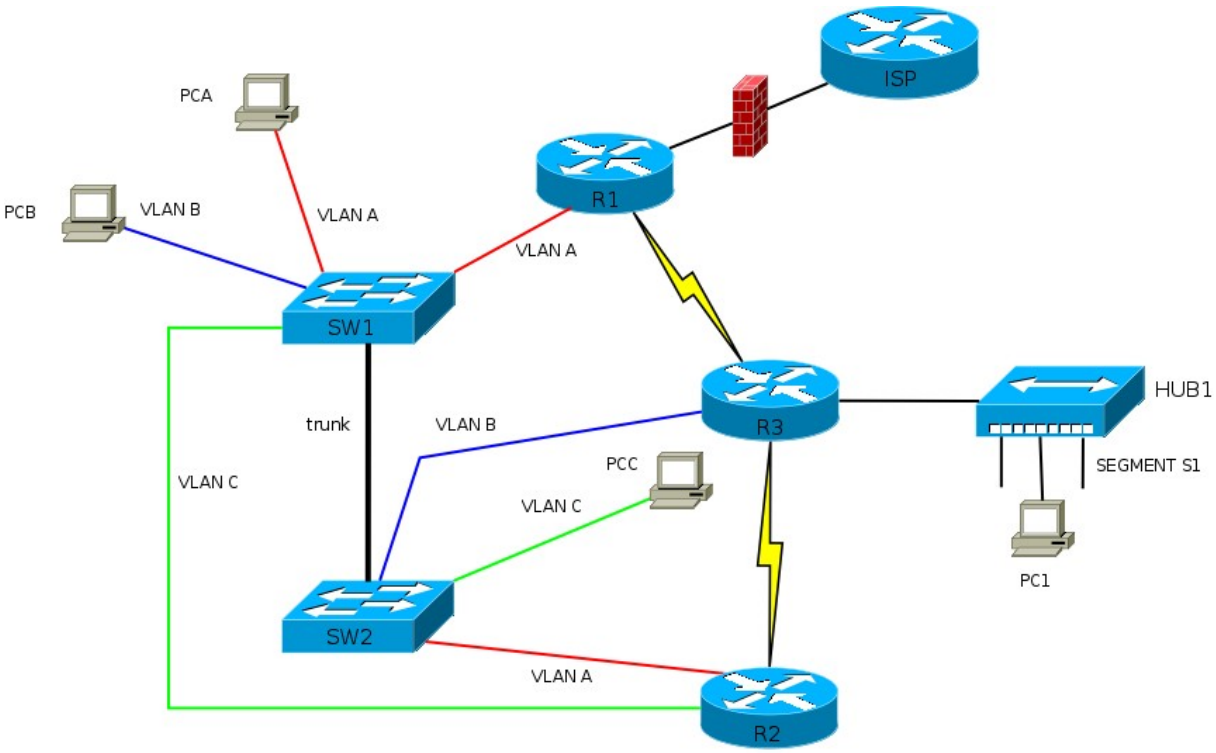
Po přihlášení do systému Virtlab si vždy přečtěte aktuální informace ve zprávě dne pro uživatele.

Důležité upozornění:

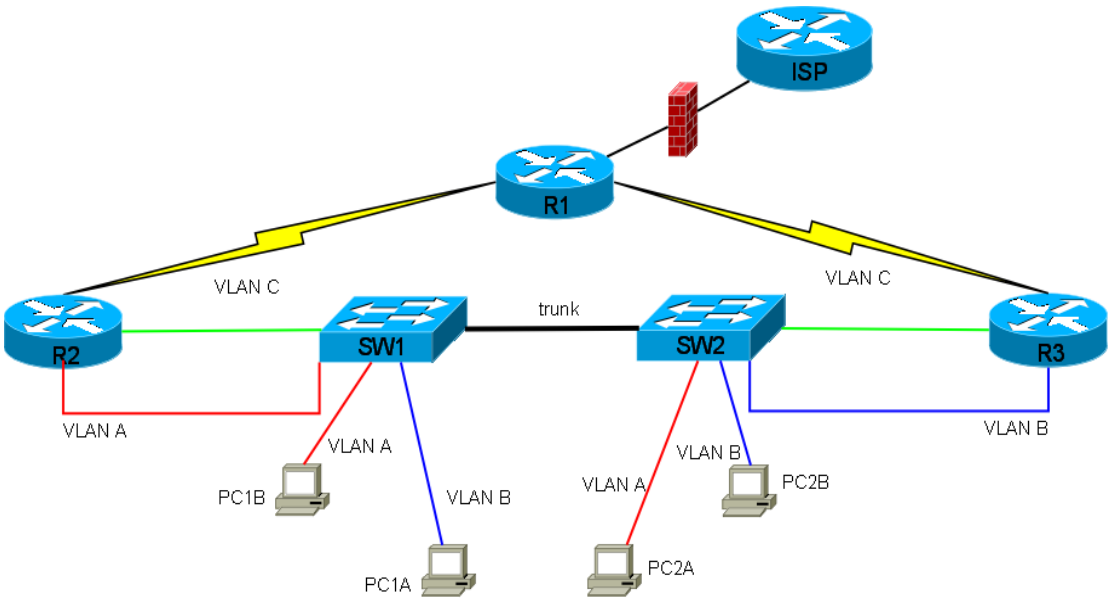
Při testování/odevzdávání úlohy nesmí být zaheslována konzola, heslo pro přístup do privilegovaného režimu musí být nastaveno na „cisco“. V opačném případě automatické otestování správnosti konfigurace selže a vaše řešení bude vyhodnoceno jako chybné.

Příloha – topologie firemních sítí

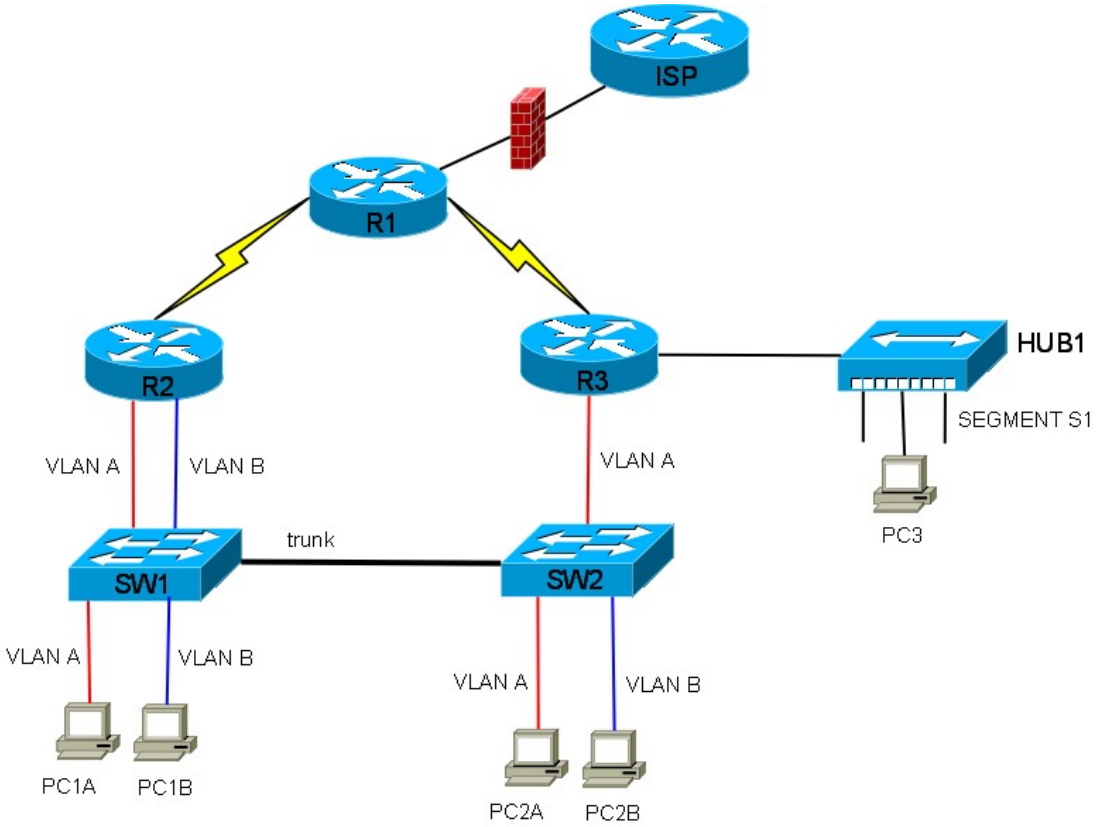
Topologie 1


ISP
PCA
R1
PCB
VLAN B
VLAN A
VLAN A
SW1
R3
HUB1
trunk
VLAN B
PCC
SEGMENT S1
VLAN C
VLAN C
PC1
SW2
VLAN A
R2

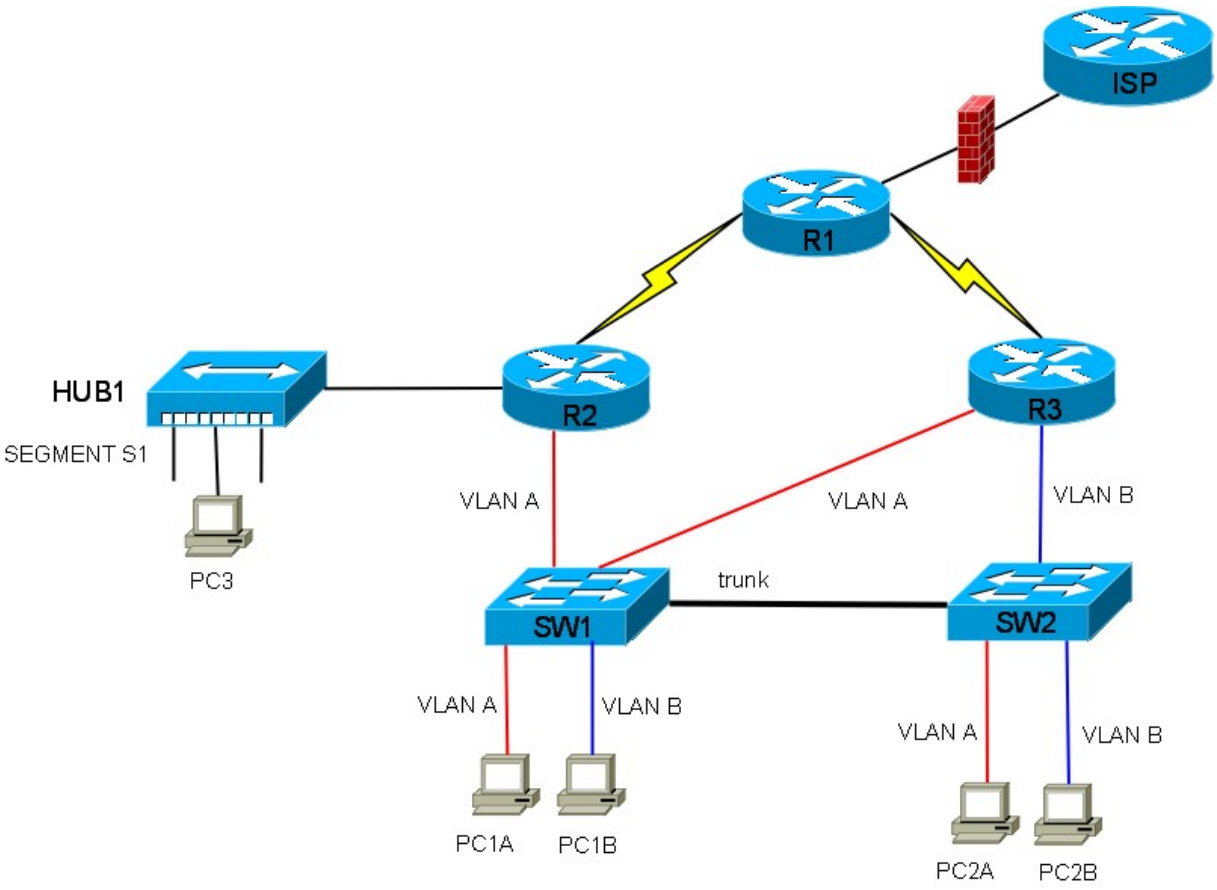
Topologie 2


ISP
R1
VLAN C
VLAN C
R2
SW1
trunk
SW2
R3
VLAN A
VLAN A
VLAN B
VLAN B
VLAN A
VLAN B
PC1B
PC2B
PC1A
PC2A

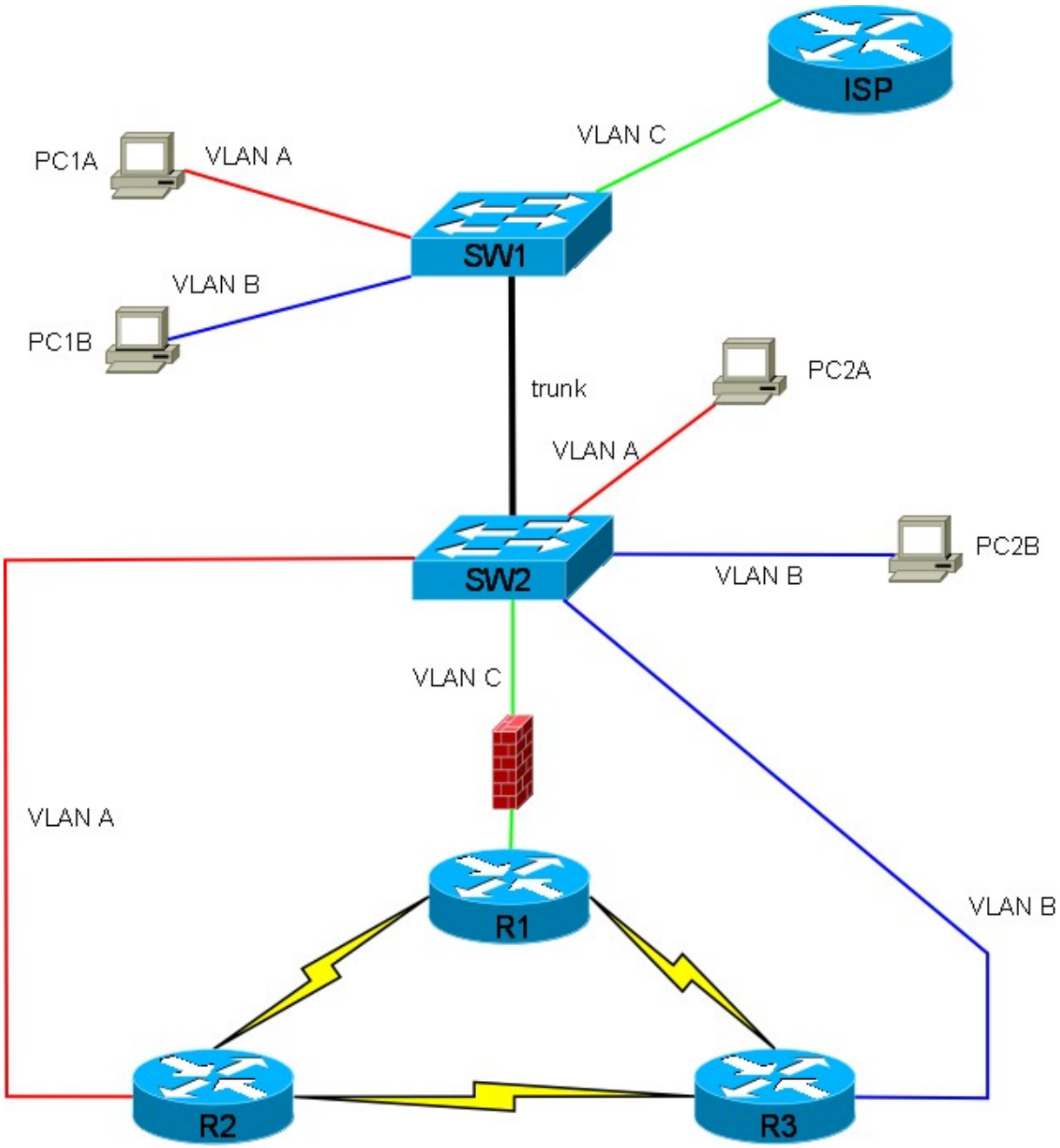
Topologie 3


ISP
R1
R2
R3
HUB1
SEGMENT S1
PC3
VLAN A
VLAN B
VLAN A
trunk
SW1
SW2
VLAN A
VLAN B
VLAN A
VLAN B
PC1A
PC1B
PC2A
PC2B

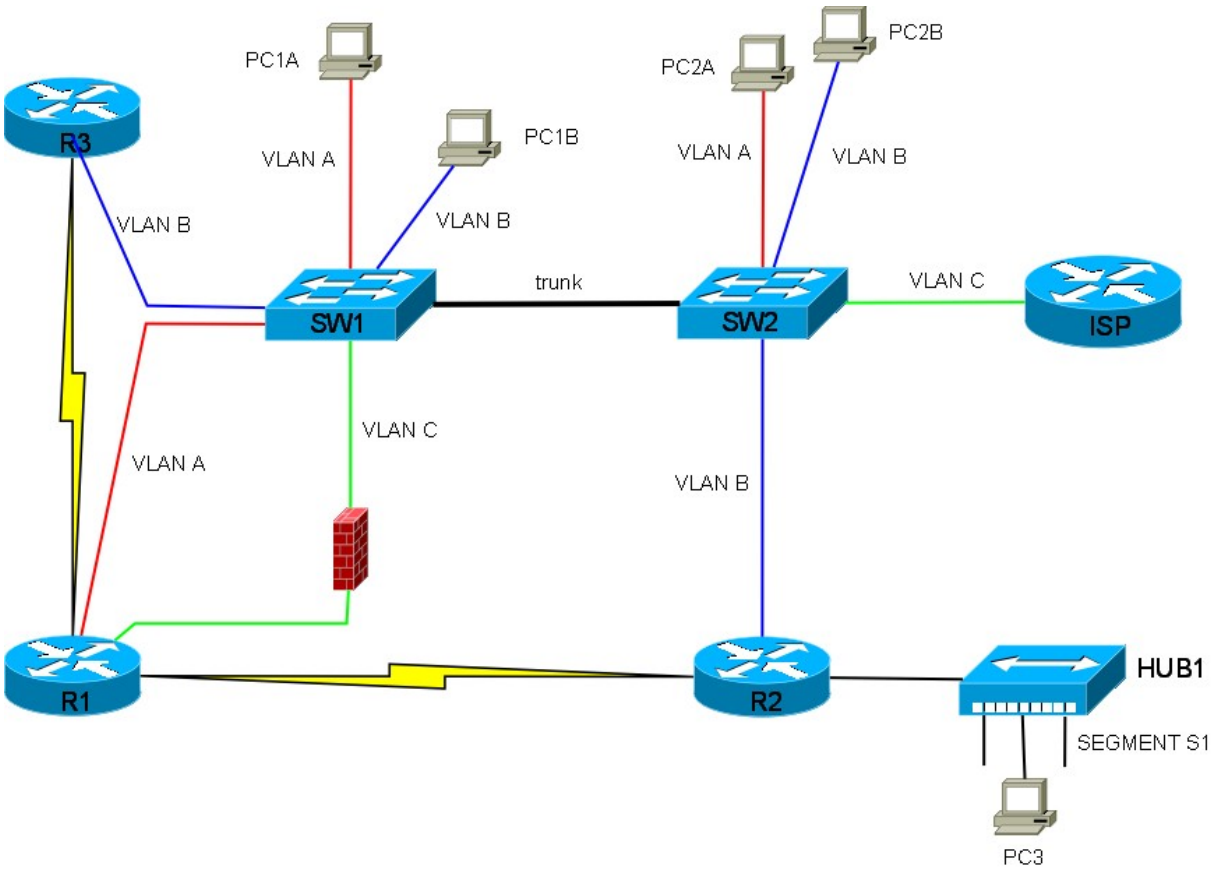
Topologie 4


ISP
R1
R2
R3
HUB1
SEGMENT S1
PC3
VLAN A
VLAN A
VLAN B
trunk
SW1
SW2
VLAN A
VLAN B
VLAN A
VLAN B
PC1A
PC1B
PC2A
PC2B

Topologie 5


ISP
VLAN C
PC1A
VLAN A
SW1
VLAN B
PC1B
trunk
PC2A
VLAN A
SW2
PC2B
VLAN B
VLAN C
VLAN A
R1
VLAN B
R2
R3

Topologie 6


PC1A
PC1B
PC2A
PC2B
R3
VLAN A
VLAN B
VLAN B
VLAN A
VLAN B
trunk
VLAN C
SW1
SW2
ISP
VLAN C
VLAN A
VLAN B
R1
R2
HUB1
SEGMENT S1
PC3