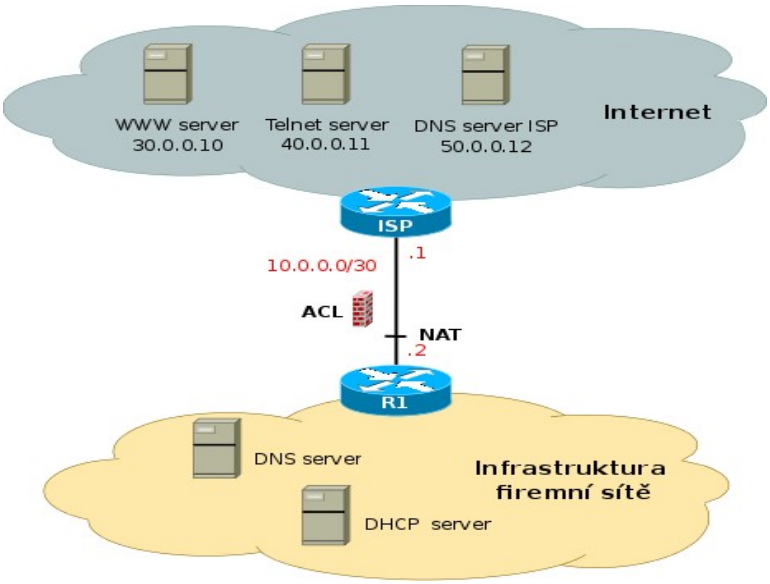
Počítačové sítě – ZS 2008/2009
Projekt návrhu sítě – zadání

Petr Grygárek, FEI VŠB-TU Ostrava

Zadání

Navrhněte a zdokumentujte konfiguraci podnikové sítě připojené do Internetu. Řešení po částech vyzkoušejte v Distribuované virtuální laboratoři počítačových sítí (Virtlab) a poskytněte konfigurační soubory a požadované výpisy pro dokumentaci funkčnosti.

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, pro usnadnění diagnostiky chyb jsou však vnitřním směrovacím protokolem propagovány do firemní sítě. 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 dokumentaci sítě vaši firmy včetně konfiguračních souborů pro všechny síťové prvky (směrovače a přepínače) a síťové služby (Linux) s ohledem na dále uvedené pokyny. Konfiguraci ověřte ve Virtlabu.

1. Adresní plán a konfigurace VLAN

Vypracujte 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 nebo více podsítí veřejného rozsahu). O který segment půjde, rozsah privátních adres a počet sdílených veřejných adres budou přiděleny cvičícím.

Veřejný adresní rozsah firemní sítě adresujte podsíťováním s maskou podsítě pevné délky. Přidělte pouze nezbytný počet adres, případné zbylé podsítě 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. Ve zvláštní tabulce 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.

Na cvičícím přiděleném segmentu vyhraďte a do dokumentace uveďte adresu vašeho firemního DNS serveru.

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

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. Symbolické označení VLAN a odpovídající přidělená čísla uveďte ve zvláštní tabulce. Na všech směrovačích nakonfigurujte IP adresy rozhraní. Všechna rozhraní směrovačů i přepínačů budou mít nakonfigurován popis (příkaz **description**) informující, kam je dané rozhraní připojeno.

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 jednu nebo více podsítí rozsahu veřejných adres.

3. DHCP server (pro kombinovné studium volitelné)

Na vhodném směrovači nakonfigurujte DHCP server, který bude dynamicky přidělovat parametry síťového připojení stanicím na cvičícím určeném segmentu (vč. adresy lokálního DNS serveru). Vyhněte se IP adresám, které jsou na segmentu již pevně přiděleny.
Uveďte konfigurační příkazy nutné pro realizaci požadované funkcionality. Na směrovači s DHCP serverem zadejte příkaz **debug ip dhcp packet**, který zajistí vypisování komunikace klientů s DHCP serverem. Na PC v přiděleném segmentu si pomocí příkazu **dhclient** vyžádejte IP adresu. Uveďte a popište vygenerovaná debug hlášení související s protokolem DHCP a výpis z příkazu **sh ip dhcp bindings**.

4. DNS server (pro kombinovné studium volitelné)

Na cvičícím určeném segmentu vaší firmy s veřejnými adresami vyhraďte PC s OS Linux, na kterém nakonfigurujte DNS server. **V dokumentaci uveďte 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 (mimo rozhraní do segmentu s privátními adresami) a vnitřního DNS serveru. Jména rozhraní směrovačů budou mít tvar

<JMENO_ROZHRANI>-<JMENO_SMEROVACE>.<JMENO_FIRMY>.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.

5. Zabezpečení sítě - ACL

Na rozhraní hraničního směrovače R1 vedoucím ke směrovači ISP implementujte filtraci provozu s použitím ACL (Access Control Lists). Požadavky jsou následující (určení segmentů symbolicky označených T a N ve vaší topologie stanoví cvičící):

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 servery.
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. Každá skupina (max. 4 studentů) 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, odevzdání všech částí ve cvičícím akceptované kvalitě je však povinné.

Části projektu budou odevzdány v písemné podobě. Zadní strana každé odevzdané části projektu musí obsahovat **vlastnoruční podpisy** všech řešitelů. Svým podpisem student **stvrzuje podíl na návrhu všech částí odevzdaného řešení**. Orientace v odevzdaném řešení může být po odevzdání **přezkoušena** a **podmínit přiznání bodů** jednotlivým studentům řešitelské skupiny.

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

Jednotlivé postupně odevzdávané části projektu budou obsahovat níže uvedené náležitosti. Precizní splnění všech požadavků a odevzání všech požadovaných bodů dokumentace funkčnosti bude zásadně ovlivňovat bodové hodnocení. Je rovněž nezbytné respektovat termíny odevzdání projektu.

1. Adresní plán a konfigurace VLAN

- Přidělený veřejný i privátní rozsah adres, přidělené určení segmentu s privátními adresami a segmentu s DNS serverem
- Tabulka mapující symbolické označení VLAN použitých v zadání topologie na přidělená čísla VLAN.
- Nákres ekvivalentní topologie 3. vrstvy OSI RM
- Návrh IP adresování, jeho dokumentace do plánků sítě (**původního i do nákresu ekvivalentní topologie**)
- Určení masky podsítě a tabulka adresování podsítí s těmito sloupci: *Adresy sítě, adresa výchozí brány (resp. i alternativních bran), rozsah použitelných IP adres stanic, broadcast adresa pro podsíť.*
- Stanovená IP adresa DNS serveru firmy.
- Popis namapování (propojení) síťových prvků pro vaši rezervaci ve Virtlabu (cut&paste z GUI Virtlabu)
- Výstup příkazu **show cdp neighbor** ze všech přepínačů i směrovačů
- Konfigurační příkazy pro konfiguraci VLAN na přepínačích

- Konfigurační příkazy pro konfiguraci IP adres na rozhraních směrovačů
- výsledky úspěšného **ping** mezi přilehlými rozhraními směrovačů
- výsledky úspěšného **ping** ze všech PC na jednotlivých segmentech sítě na výchozí bránu příslušného segmentu, resp. VLAN
-

Jelikož správné vypracování adresního plánu ovlivní všechny další části projektu, doporučujeme jej před odevzdáním konzultovat se cvičícím.

2. Směrování a NAT

- Popis namapování (propojení) síťových prvků pro vaši rezervaci ve Virtlabu (cut&paste z GUI Virtlabu)
- Konfigurační příkazy směrovačů pro konfiguraci směrování (vč. přiřazení adres na rozhraní)
- Výpisy směrovacích tabulek všech směrovačů.
- U protokolu OSPF výpis z příkazu **show ip ospf neighbor**.
- Příkazy potřebné pro konfiguraci NAT
- Překladová tabulka vzniklá přistoupením na hlavní stránku WWW serveru v Internetu z počítače na segmentu s privátními adresami použitím prohlížeče **lynx** (**show ip nat translation**).

3. Zabezpečení sítě – ACL

- Konfiguraci IP adres na rozhraní směrovačů (z předchozí části projektu)
- Popis namapování (propojení) síťových prvků pro vaši rezervaci ve Virtlabu (cut&paste z GUI Virtlabu)
- Tabulky pravidel pro směry provozu do a z firemní sítě s těmito sloupci:
  Pořadí, povolení/zákaz, L3/L4 protokol, zdrojová adresa/maska, zdrojový port, cílová adresa/maska, cílový port, další případná omezení
- Příkazy pro konfiguraci ACL pro oba směry provozu, včetně příkazů pro přiřazení ACL na patřičné rozhraní a určení směru filtrace

4. DNS server (pro kombinovné studium volitelné)

- Popis namapování (propojení) síťových prvků pro vaši rezervaci ve Virtlabu (cut&paste z GUI Virtlabu).
- Konfiguraci IP adres na rozhraní směrovačů (z předchozí části projektu)
- Adresa firemního DNS serveru

- Podstatné konfigurační soubory démona **bind** běžícího na firemním DNS serveru
  (**jen změny proti implicitním hodnotám**).
- ověření funkčnosti přímého i reverzního překladu pro všechny vložené záznamy pomocí programu **dig** z některé stanice

5. DHCP server (pro kombinovné studium volitelné)

- Popis namapování (propojení) síťových prvků pro vaši rezervaci ve Virtlabu (cut&paste z GUI Virtlabu).
- Konfigurační příkazy nutné pro realizaci DHCP serveru s uvedením směrovače, na kterém byly vloženy
- Výstupy příkazů **debug ip dhcp packet** a **sh ip dhcp bindings** generované po vyžádání IP adresy z klientského PC pomocí příkazu **dhclient.**

Poznámky k práci ve Distribuované virtuální laboratoři počítačových sítí

Použijte portál http://virtlab.cs.vsb.cz

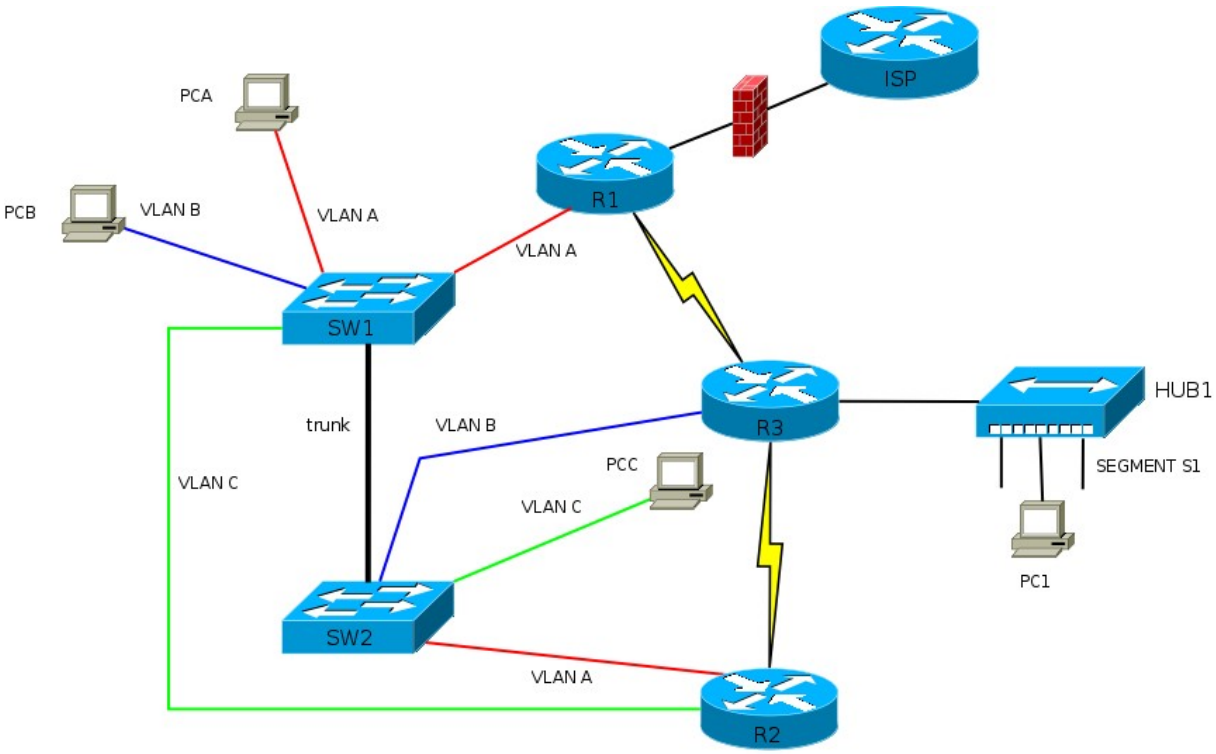
Konta budou automaticky vytvořena všem zapsaným studentům POS na začátku semestru. Jako přihlašovací jméno použijte osobní číslo, heslo stejné jako u školní pošty a jiných systémů z VŠB-TU (z LDAP).

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. Proto ke každé vyřešené části projektu uvádějte i aktuální mapování, které se zobrazí při přístupu k úloze.

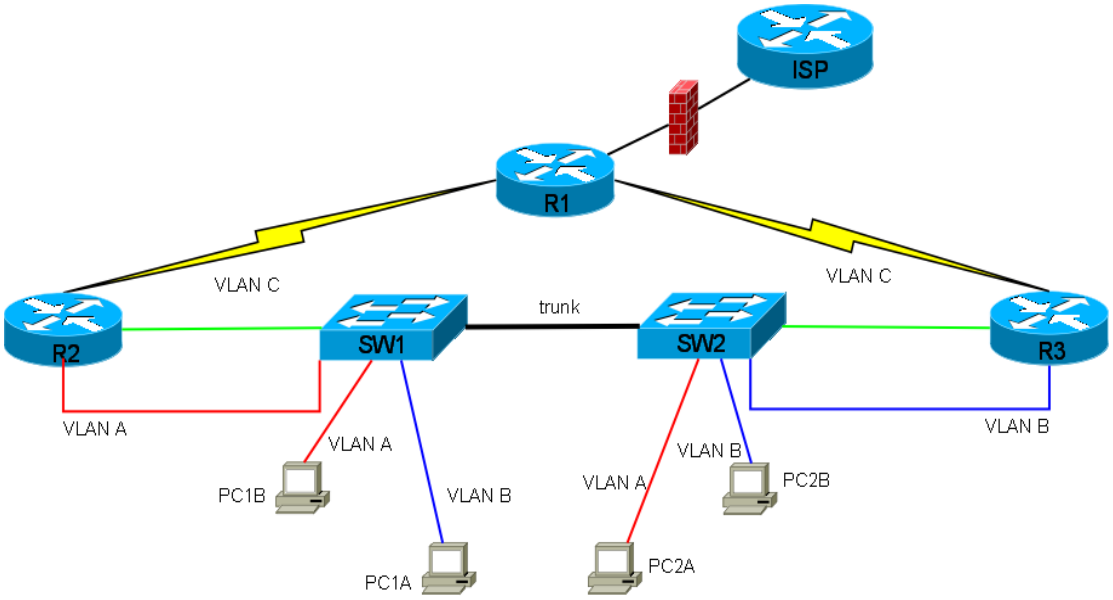
Rozbočovače ve Vaší topologii jsou nekonfigurovatelné a v rámci řešení se jimi není třeba zabývat.

Příloha – topologie firemních sítí

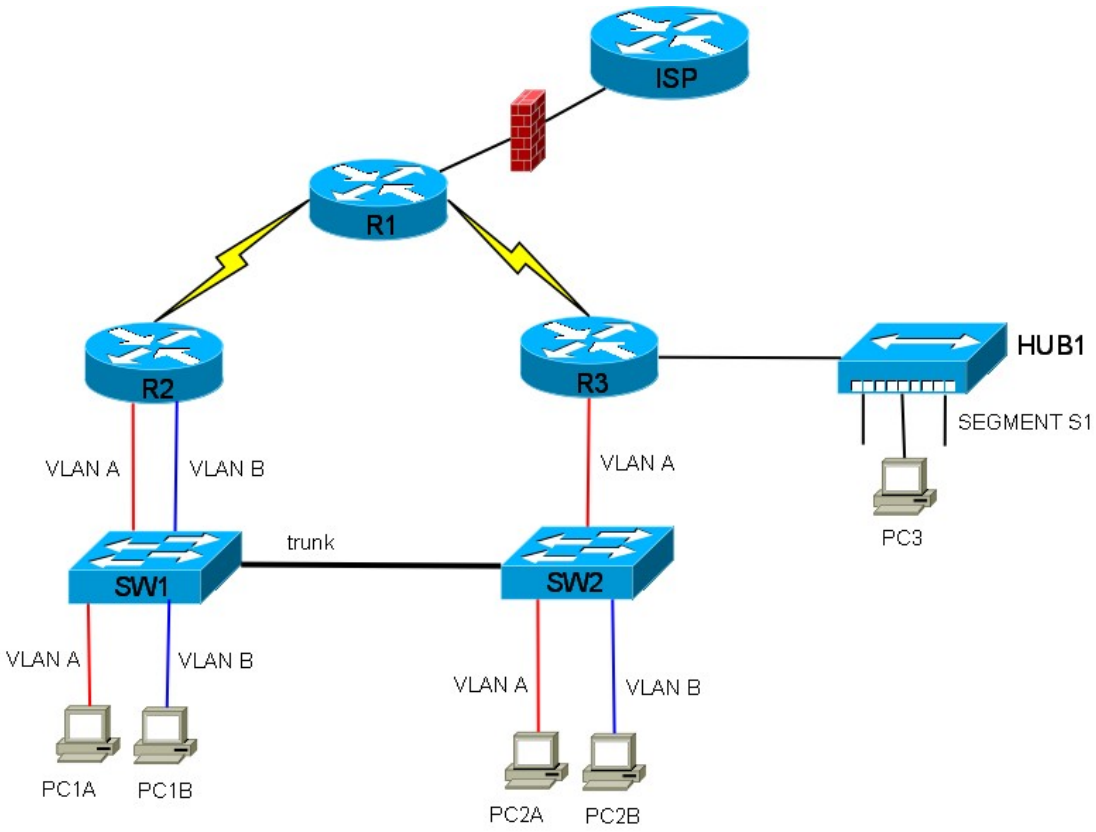
Topologie 1


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

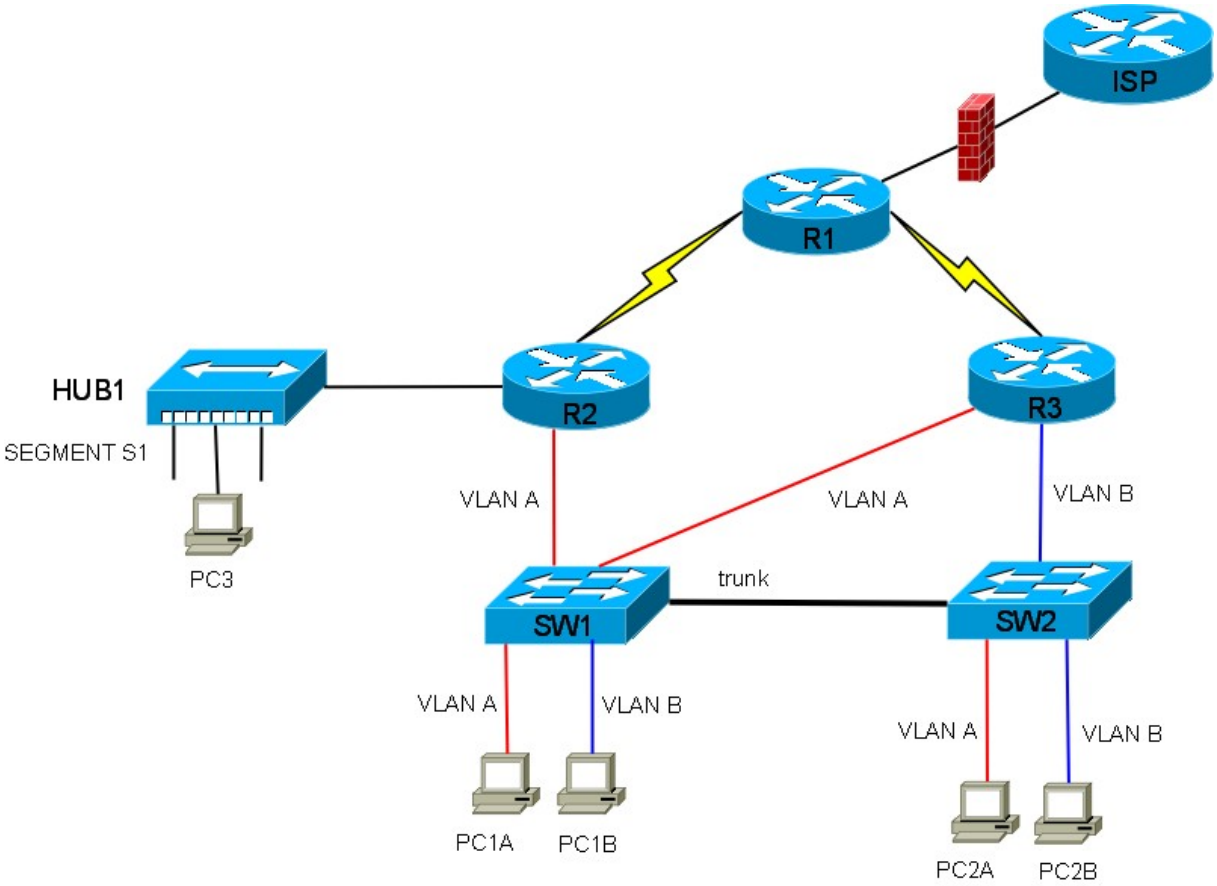
Topologie 2


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

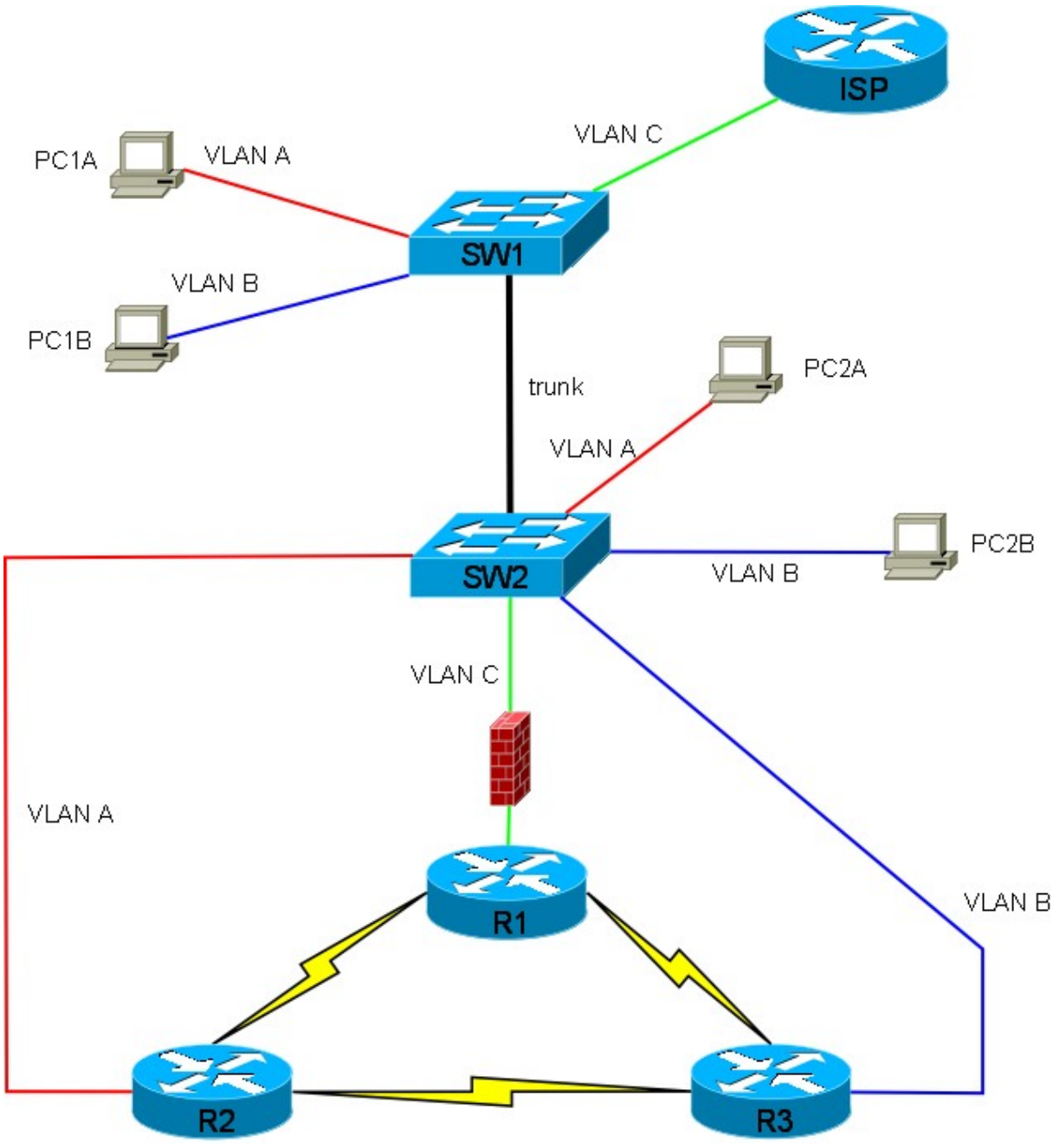
Topologie 3


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

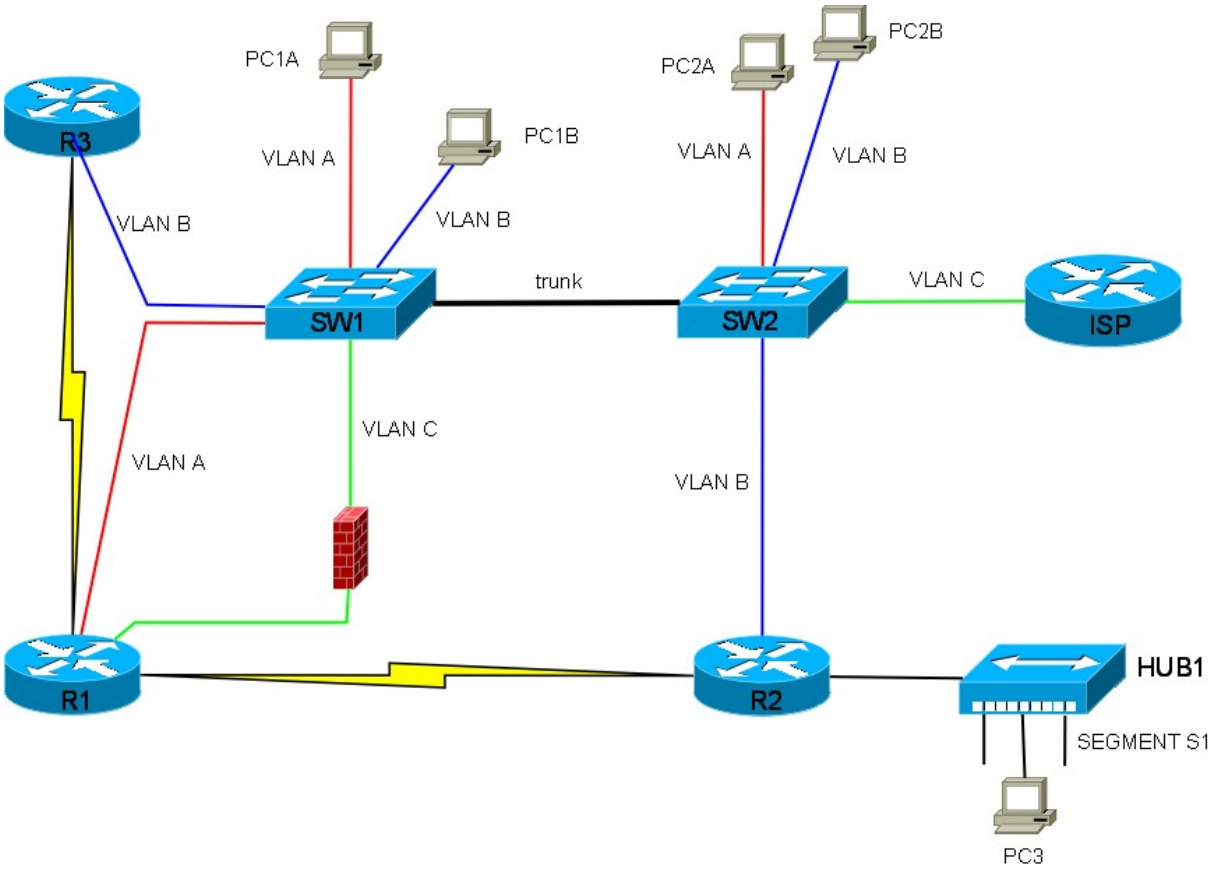
Topologie 4


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