Упражнение 8. Конфигуриране на виртуални локални мрежи (VLAN)

1. Цел на упражнението.

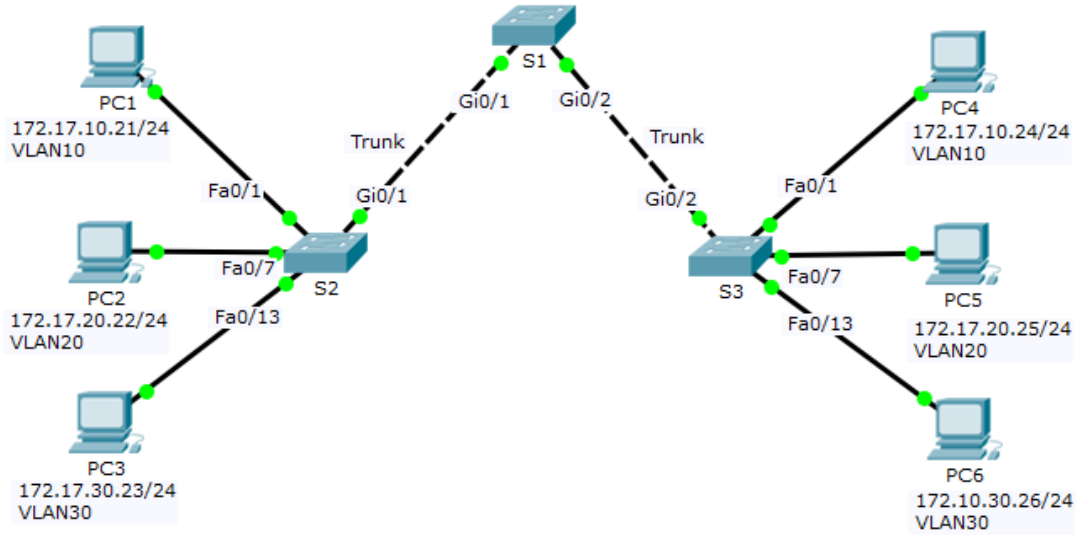
Целта на упражнението е да се получат практически знания и умения за конфигуриране и администриране на виртуални локални мрежи (VLAN).

2. Теоретични сведения

2.1 Същност на виртуални локални мрежи

С нарастването на една компютърна мрежа се увеличава излишният трафик в нея, както и broadcast трафика. Разделянето на мрежата на по-малки подмрежи помага за ограничаване на излишния трафик, както и повишава сигурността на достъпа между отделните подмрежи. За разделянето на мрежа на подмрежи е необходимо отделните подмрежи да се свържат с устройство на трето ниво – маршрутизатор (router). Традиционното разделяне на мрежите с маршрутизатор става на географски принцип, разделяйки отделните етажи на сградата или отделните сгради. Понякога географското разпределение не съответства точно на целите на разделянето и не е най-удобния механизъм.

Виртуалните локални мрежи предоставят механизъм за разделяне на мрежата на подмрежи, без необходимост да се следва географското разположение на компютрите в мрежата. Механизмът предполага създаване на VLAN с различни номера в паметта на отделните комутатори (switch) и назначаването на портовете им в съответни VLAN. Така всички портове, назначени в една виртуална локална мрежа могат да комуникират помежду си, независимо от факта, че се намират на различни комутатори, в различни сгради или етажи. Примерна схема на мрежа, разделена на VLAN може да се види на фигура 8.1.



Фиг. 8.1. Примерна мрежа, разделена на VLAN

В този пример компютри PC1 и PC4, намиращи се във VLAN 10 ще могат да комуникират помежду си, но между отделните VLAN няма да има комуникация. Това означава, че broadcast пакетите от отделните VLAN ще достигат само до компютрите от същия VLAN.

Различните VLAN имат номер и име. Номерът трябва да съвпада на различните комутатори, тъй като той идентифицира принадлежността на пакета към даден VLAN. Името на VLAN има локално значение и е само за описание. Съществуват комутатори за организации (Enterprise), които поддържат VLAN с номера от 1 до 1024, като обикновено номера 1001 – 1024 са служебни. Другият вид комутатори са предназначени за доставчици на услуги (Service Provider) и поддържат разширен набор номера на VLAN до 4096.

2.2 Портове за достъп (Access) и гръбначни портове (Trunk)

Портовете, на които са свързани клиентските компютри, принтери и сървъри обикновено са зазначени да предават информация за един единствен VLAN. Те се наричат портове за достъп (Access port) и предават стандартни Ethernet кадри, които се разпространяват само в съответния VLAN. Портовете, които свързват отделните комутатори, намиращи се в различните сгради или етажи трябва да носят информацията от всички VLAN, които са конфигурирани на комутатора. Те се наричат гръбначни (Trunk) портове и информацията, която се предава по тях е модифицирана. Най-често използвания протокол за гръбнак на виртуални локални мрежи в момента е IEEE802.1q. Той определя формата на 4-байтовия маркер (tag), който се вмъква в заглавната част на Ethernet кадъра след MAC адресите и определя принадлежността на кадъра към определен VLAN.

По даден гръбначен сегмент обикновено има една VLAN, чиито данни се предават без маркер. Тя се нарича „родна“ (native) VLAN.

В примера от фигура 8.1 ако предположим, че компютър PC3 предава информация на PC6, то в заглавната част на Ethernet кадъра се поставят MAC адреса на PC3 за източник и MAC адреса на PC6 за получател. Кадърът стига до комутатор S2, той търси MAC адреса на получателя в таблицата си и вижда, че той се намира на порт Gigabit0/1, който е настроен в режим „гръбнак“ (trunk). Затова комутаторът вмъква маркер за принадлежност към VLAN 30 и получения IEEE802.1q кадър се изпраща по двата гръбначни сегмента до комутатор S1 и S3. Комутатор S3 получавайки кадъра намира, че MAC адресът на получателя е на порт за достъп Fast0/6, затова премахва маркера и получения Ethernet кадър се предава до получателя – PC6.

В примерите в това упражнение се използва следната схема:

На всеки от трите комутатора са създадени три VLAN с номера 10, 20 и 30.

На всеки комутатор портовете са назначени така:

- Интерфейси Gi0/1 и Gi0/2 – Trunk;
- Интерфейси Fa0/1 – 0/6 – access във VLAN 10;

- Интерфейси Fa 0/7 – 0/12 – access във VLAN 20;
- Интерфейси Fa 0/13 – 0/18 – access във VLAN 30.

IP адресите са:

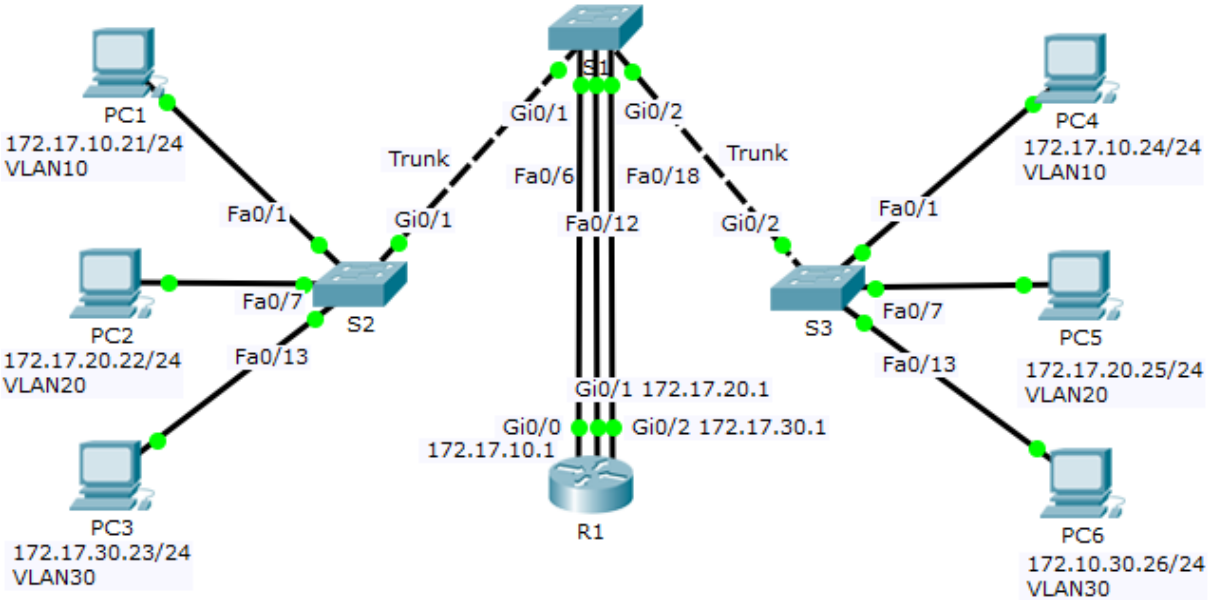
VLAN	мрежа	маска	шлюз
10	172.17.10.0	255.255.255.0	172.17.10.1
20	172.17.20.0	255.255.255.0	172.17.20.1
30	172.17.30.0	255.255.255.0	172.17.30.1

2.3 Маршрутизация между виртуални локални мрежи

За да има комуникация между отделните VLAN е необходимо в мрежата да се включи устройство от трето ниво – маршрутизатор или комутатор на ниво 3, който да прави маршрутизация между отделните подмрежи. За да се прави това е необходимо IP адресите във всеки VLAN да бъдат различна IP мрежа. Съществуват главно три начина за маршрутизация между VLAN.

2.3.1 Отделен интерфейс за всеки VLAN

При този начин маршрутизаторът трябва да има отделен физически интерфейс за връзка към всеки VLAN, към и от която ще маршрутизира. На всеки от интерфейсите се задава IP адрес от адресното пространство на съответния VLAN и всеки интерфейс се включва в порт за достъп (access) на комутатор, назначен в съответния VLAN. IP адресът, назначен на интерфейса на маршрутизатора се назначава за шлюз по подразбиране (Default Gateway) на компютрите от неговия VLAN. Принципна схема на работата е показана на фигура 8.2.



Фиг. 8.2. Маршрутизация между VLAN с отделни интерфейси

В примера маршрутизаторът R1 има три физически интерфейса:

- Gi0/0, с IP адрес 172.17.10.1/24, свързан към access порта на комутатор S1 – Fa0/6 във VLAN 10;
- Gi0/1, с IP адрес 172.17.20.1/24, свързан към access порта на комутатор S1 – Fa0/12 във VLAN 20;
- Gi0/2, с IP адрес 172.17.30.1/24, свързан към access порта на комутатор S1 – Fa0/18 във VLAN 30.

Когато компютър PC1 иска да предаде данни на компютър PC2, той умножава своя IP адрес и IP адреса на кореспондента си по мрежовата маска и разбира, че получателят е в мрежа 172.17.20.0, различна от тази на PC1 – 172.17.10.0. Затова той изпраща пакета до получател с IP адрес 172.17.20.22, но в заглавната част на Ethernet кадъра за получател се оставя MAC адреса на интерфейс Gi0/0 на R1, тъй като неговият IP адрес е назначен за шлюз по подразбиране на PC1. Кадърът се приема от комутатор S2, той търси MAC адреса на Gi0/0 на R1 в таблицата си и виждайки, че той се намира на порт Gi0/1 на S2 го маркира с IEEE802.1q маркер за принадлежност към VLAN 10. Така кадърът стига до комутатор S1, който премахва маркера, тъй като MAC адресът на получателя е свързан на access порт във VLAN 10.

Маршрутизаторът получава пакета на интерфейс Gi0/0, умножава IP адреса по мрежовата маска, търси мрежата на получателя в маршрутизиращата си таблица и вижда, че тя е свързана на неговия интерфейс Gi0/1, затова го изпраща там до MAC адреса на PC2. По познатия начин комутатор S1 вмъква маркер за принадлежност към VLAN 20, предава го по гръбначния порт към S2, който премахва маркера и така Ethernet кадъра стига до крайния получател.

Този начин не налага маршрутизаторът да може да интерпретира протокола IEEE802.11q, но изисква отделен физически интерфейс за всеки VLAN, затова не е подходящ за мрежа с голям брой VLAN мрежи.

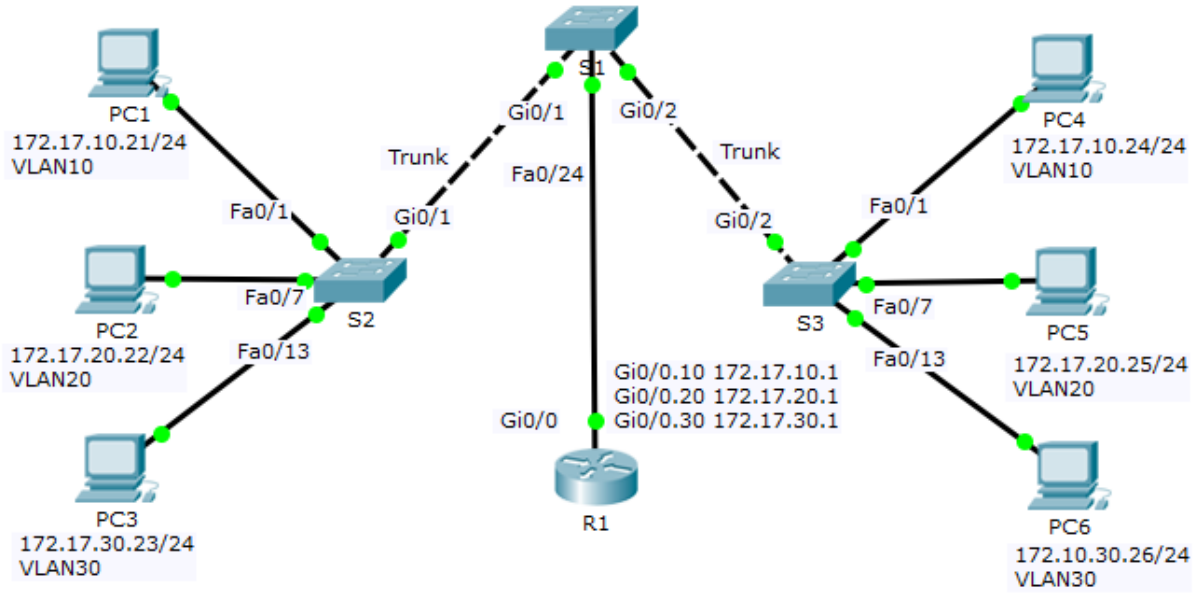
2.3.2 Един интерфейс за всички VLAN

При този механизъм маршрутизаторът се свързва чрез един единствен физически интерфейс към гръбначен (trunk) порт на комутатор, където трябва да са позволени всички VLAN, които ще се маршрутизират. За това в литературата понякога се среща именуван като „router-on-a-stick” (маршрутизатор на пръчка). В този случай маршрутизаторът трябва да разбира протокола IEEE 802.1q, тъй като му се налага да приема маркирани кадри, да премахва маркери, да изработва и вмъква нови маркери.

За всеки VLAN се създава логически подинтерфейс, който се назначава в съответния VLAN, указвайки му номера на VLAN и му се назначава IP адрес от съответния VLAN, който е назначен за шлюз по подразбиране на компютрите в този VLAN. В примера са създадени следните подинтерфейси:

- Gi0/0.10 – за VLAN 10 с IP адрес 172.17.10.1/24;
- Gi0/0.20 – за VLAN 20 с IP адрес 172.17.20.1/24;
- Gi0/0.30 – за VLAN 30 с IP адрес 172.17.30.1/24;

Физическият интерфейс Gi0/0 на маршрутизатора няма назначен IP адрес и е свързан към интерфейс Fa0/24 на комутатор S1, който е в режим trunk. Тази мрежова топология е показана на фигура 8.3.



Фиг. 8.3. Маршрутизация с един интерфейс за всички VLAN

Ако разгледаме горния пример, при който PC1 предава за PC 2, комуникацията става по същия начин, с тази разлика, че R1 получава кадъра маркиран за VLAN 10, по което разбира, че е предназначен за логически подинтерфейс Gi0/0.10, където се премахва маркера и се търси получателя. След като открие получателя PC2 във VLAN 20, маршрутизаторът вмъква нов маркер за принадлежност към VLAN 20 и така изпраща маркирания кадър по гръбначния интерфейс към комутатора S1.

Този начин използва един физически интерфейс за маршрутизация между всички VLAN, но изисква маршрутизатор, който може да интерпретира протокол IEEE802.1q. Друга характеристика на метода е, че единственият физически интерфейс, който се използва за предаване на информация между всички VLAN може да се окаже тясно място и да предизвика забавяния и изхвърляне на пакети в мрежата.

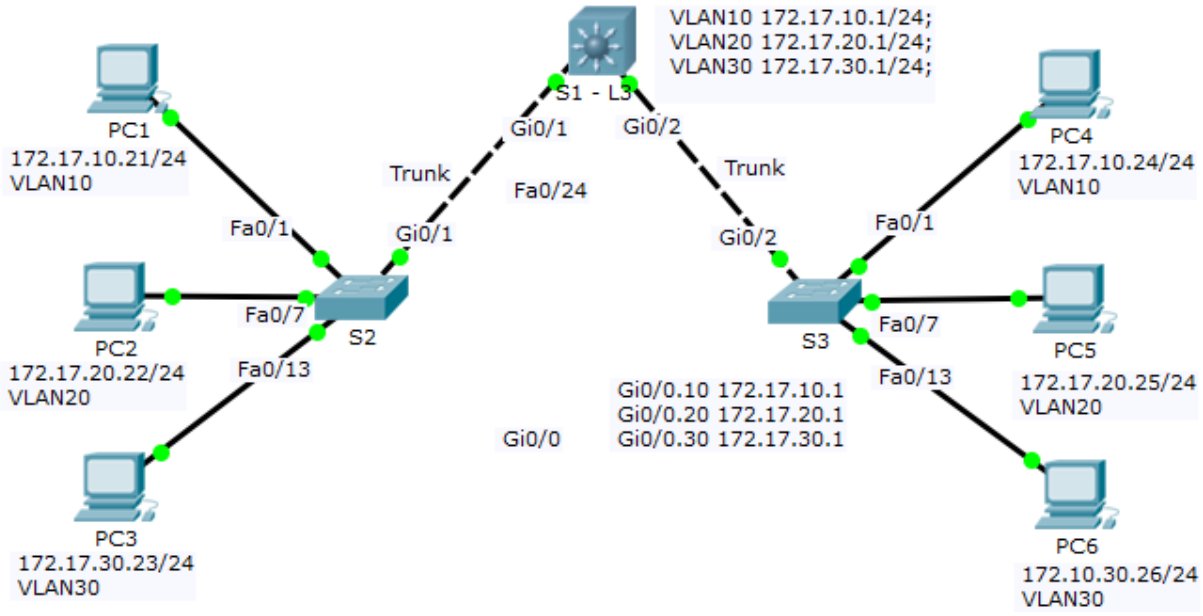
2.3.3 Използване на комутатор от ниво 3 (маршрутизиращ комутатор)

При този начин вместо маршрутизатор се използва комутатор от ниво 3, на който се създават логически виртуални интерфейси и на тях се назначават IP адресите. Предимствата на метода са няколко. Първо, можем да създадем повече логически виртуални интерфейси отколкото физически има комутатора от ниво 3 и

по този начин не сме ограничени от броя на физическите интерфейси, които имаме. Допълнително предимство е, че маршрутизацията вътре в комутатора се извършва с десетки пъти по-висока скорост от тази на физическите интерфейси.

Примерна постановка на метода е показана на фигура 8.4, където комутатор S1 е заменен с маршрутизиращ комутатор и са създадени следните логически интерфейси:

- VLAN10 с IP адрес 172.17.10.1/24;
- VLAN20 с IP адрес 172.17.20.1/24;
- VLAN30 с IP адрес 172.17.30.1/24;



Фиг. 8.3. Маршрутизация с един интерфейс за всички VLAN

3. Задачи за изпълнение

1. Чрез програмата Cisco Packet Tracer заредете файла **VLAN-no-routing.pkt**. Проверете настройките на IP адреси и шлюз (Gateway) на компютрите. Чрез командата Ping проверете достижимостта от PC1 до останалите компютри. Повторете проверката от компютър PC2. Наблюдавайте преминаването на данните в режим на симулация (бутонът долу вдясно на програмата) между PC3 и PC6 и между PC3 и PC4.

2. Заредете файла **VLAN-legacy-routing.pkt**. Разгледайте топологията. Проверете комуникацията между всички компютри. Изчистете ARP таблицата на PC1 с командата arp –d и се уверете, че е изчистена с arp -a. Наблюдавайте в режим на симулация комуникация между PC1 и PC3, между PC1 и PC2 и между PC1 и PC6. До къде достига broadcast пакета, изпратен от PC1?

3. Заредете файла **VLAN-router-on-a-stick.pkt**. Разгледайте топологията. Проверете комуникацията между всички компютри. Изчистете ARP таблицата на PC2 с командата arp –d и се уверете, че е изчистена с arp -a. Наблюдавайте в режим на симулация комуникация между PC2 и PC5, между PC2 и PC1 и между PC2 и PC4. До къде достига broadcast пакета, изпратен от PC2?

4. Заредете файла **VLAN-router-on-a-stick.pkt**. Разгледайте топологията. Проверете комуникацията между всички компютри. Изчистете ARP таблицата на PC2 с командата arp –d и се уверете, че е изчистена с arp -a. Наблюдавайте в режим на симулация комуникация между PC2 и PC5, между PC2 и PC1 и между PC2 и PC4. До къде достига broadcast пакета, изпратен от PC2?

5. Заредете файла **VLAN-L3-Switch.pkt**. Разгледайте топологията. Проверете комуникацията между всички компютри. Изчистете ARP таблицата на PC3 с командата arp –d и се уверете, че е изчистена с arp -a. Наблюдавайте в режим на симулация комуникация между PC3 и PC6, между PC3 и PC2 и между PC3 и PC5. До къде достига broadcast пакета, изпратен от PC3?

4. Контролни въпроси

1. Защо се налага разделяне на мрежа на виртуални локални мрежи (VLAN)?
2. Какви са начините за комуникация между VLAN? Кой е предпочитан и защо?
3. Колко VLAN могат да се назначат на порт за достъп? А на гръбначен порт?
4. Какво ще стане, ако свържем обикновен компютър на гръбначен порт?
5. Трябва ли различните VLAN да са в различни IP мрежи, кога и защо?
6. Може ли да се направи маршрутизация между VLAN, ако две от мрежите имат припокриващи се IP адреси?

5. Допълнителни ресурси

1. IEEE, 802.1Q - Virtual LANs, http://www.ieee802.org/1/pages/802.1Q.html, дата на използване 19.03.2017 г.
2. Firewall.cx, INTERVLAN ROUTING - ROUTING BETWEEN VLAN NETWORKS, http://www.firewall.cx/networking-topics/vlan-networks/222-intervlan-routing.html, дата на използване 19.03.2017 г.
3. Cisco Systems, Configure InterVLAN Routing on Layer 3 Switches, http://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html, дата на използване 19.03.2017 г.