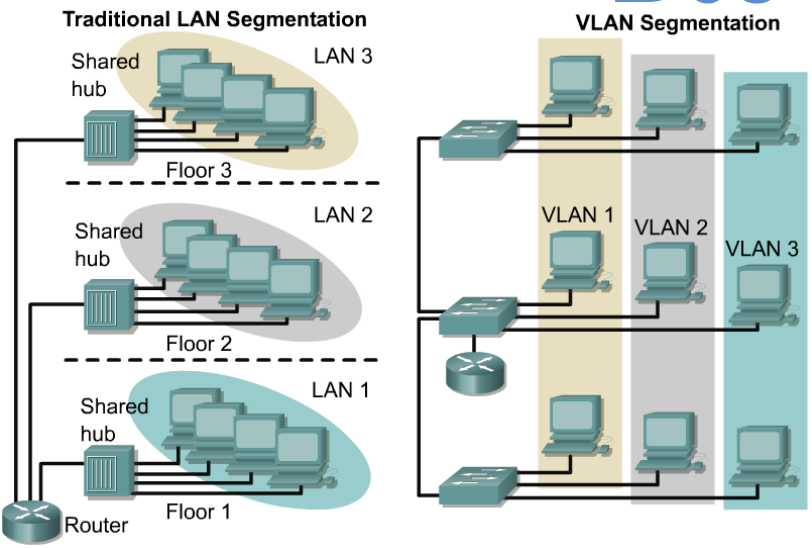
Virtual LANs (VLANs)

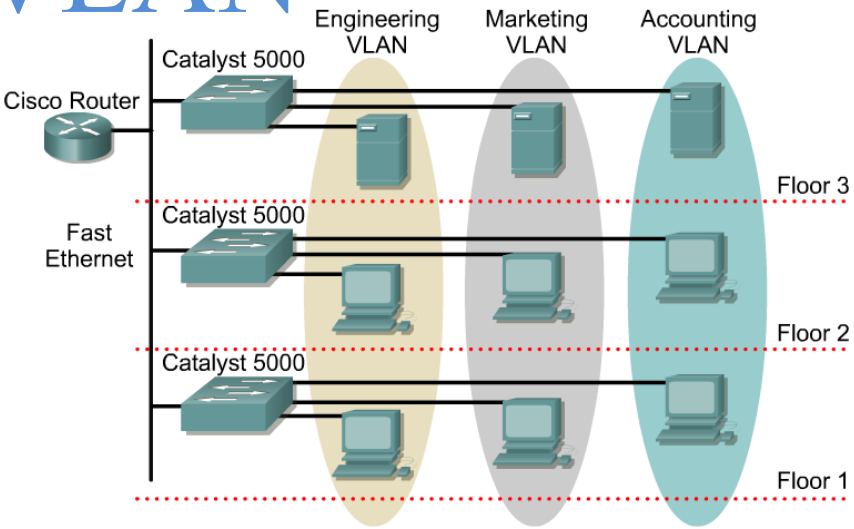
проф. д-р инж. Венета Алексиева

Основни моменти

- Мрежи с/без VLANs
- Предимства на VLANs
- Trunking
- Маршрутизиране между VLANs

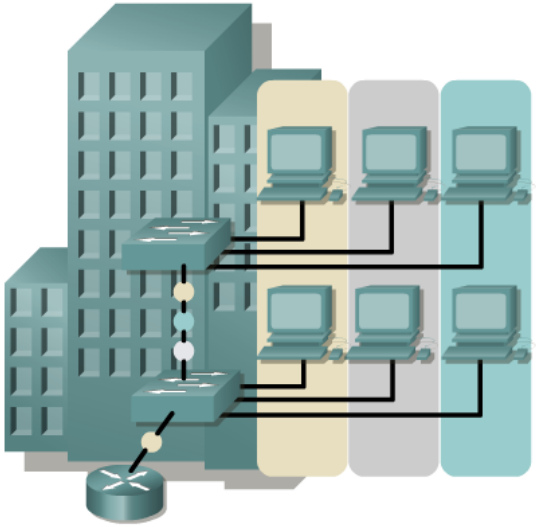
Без и с VLAN





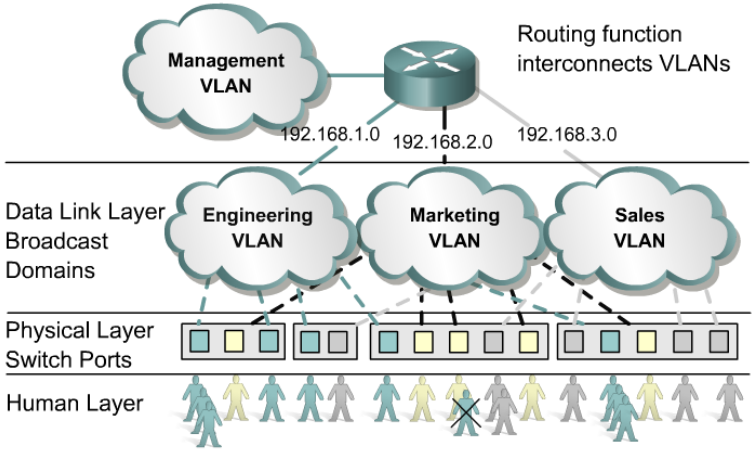
- VLAN сегментира мрежата по функции, групи служители, приложения, без оглед на физическото местоположение.
- Всички работни станции и сървъри от една работна група работят в една VLAN.
- Могат да са базирани на номер на порт, MAC адрес, протокол, приложение.
- Реализират се със софтуер или с ОС на комутаторите.
- Фреймовете получават етикет за принадлежност към съответния VLAN.

Предимства на VLAN(1)



- VLANs осигуряват сегментация.
- VLANs позволяват лесно разрастване на мрежата, несвързано с физическо местоположение.
- Увеличават сигурността.
- Улесняват управлението на мрежата.
- Комутаторите не могат да прехвърлят трафик между VLAN.
- Използват се маршрутизатори, за прехвърляне на трафик между VLANs.
- Маршрутизаторите във VLAN осигуряват филтриране на broadcast, сигурност, управление на трафика.

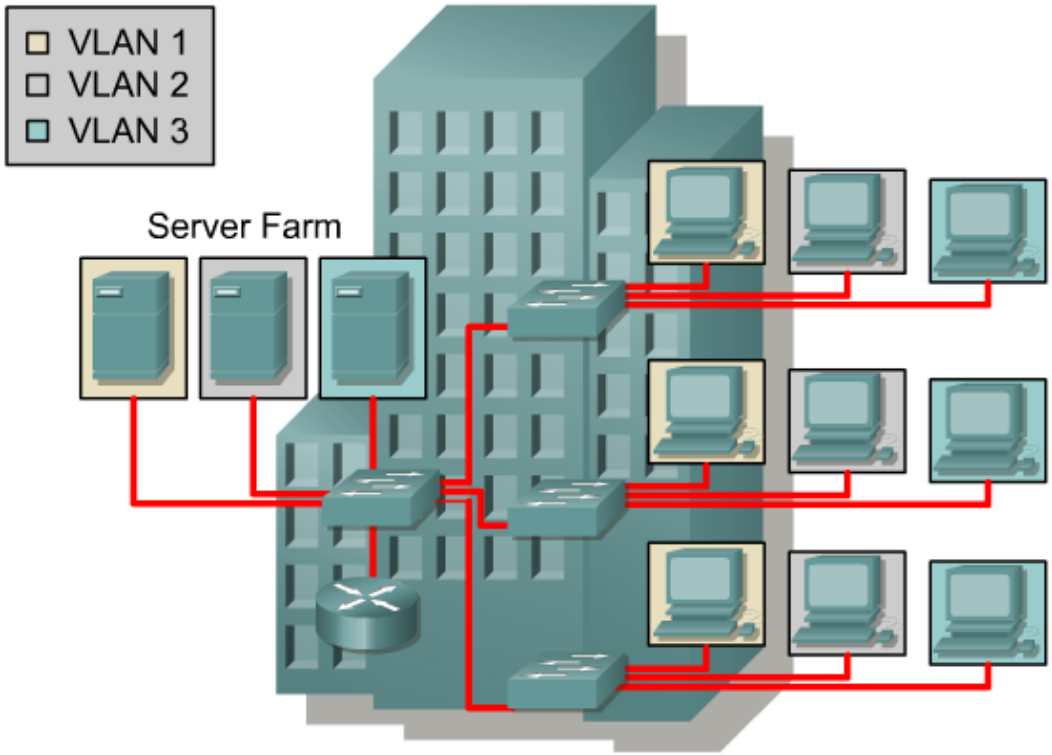
Предимства на VLAN(2)



Ако се включи hub на VLAN порт на комутатора, всички устройства, включени към него, принадлежат към този VLAN.

- VLAN позволяват логическа организация вместо физическа.
- VLAN ограничават broadcast домейните.
- Лесно се местят/добавят работни станции между VLAN.
- Лесно се сменят конфигурациите на LAN.

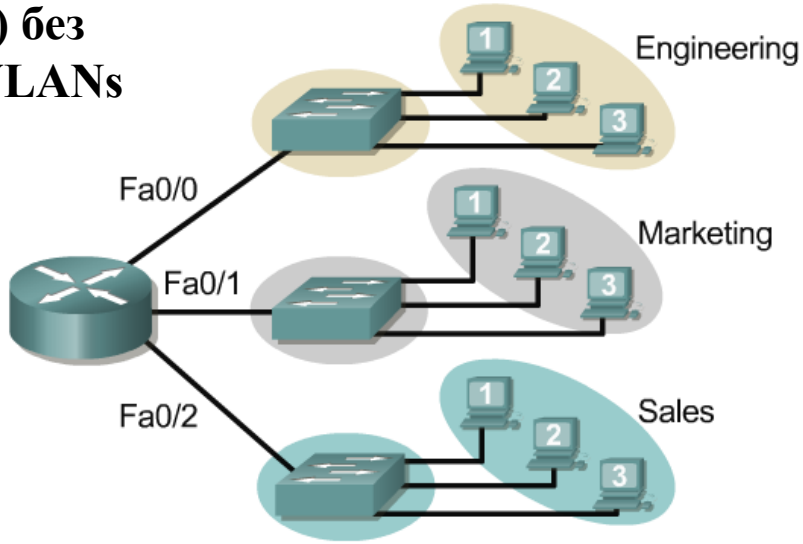
Broadcast домейни с VLAN



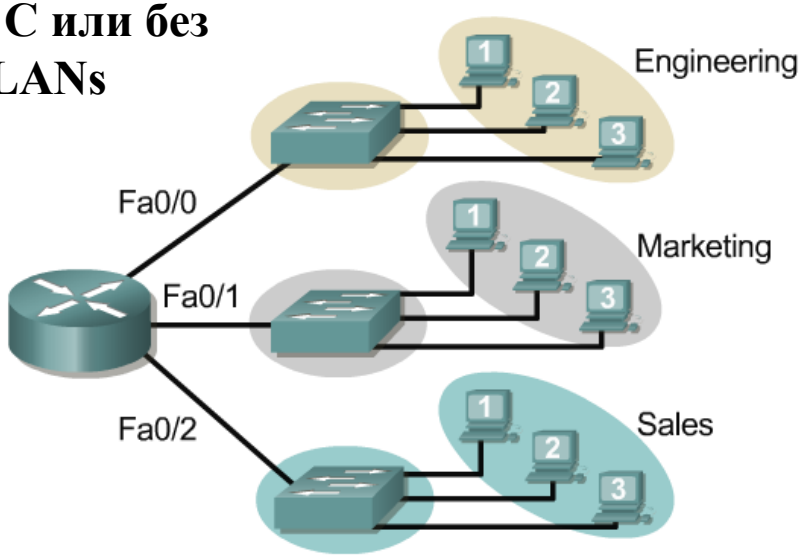
- VLAN е broadcast домейн, обхващащ един или няколко комутатора.

Broadcast домейни с VLAN

1) без VLANs

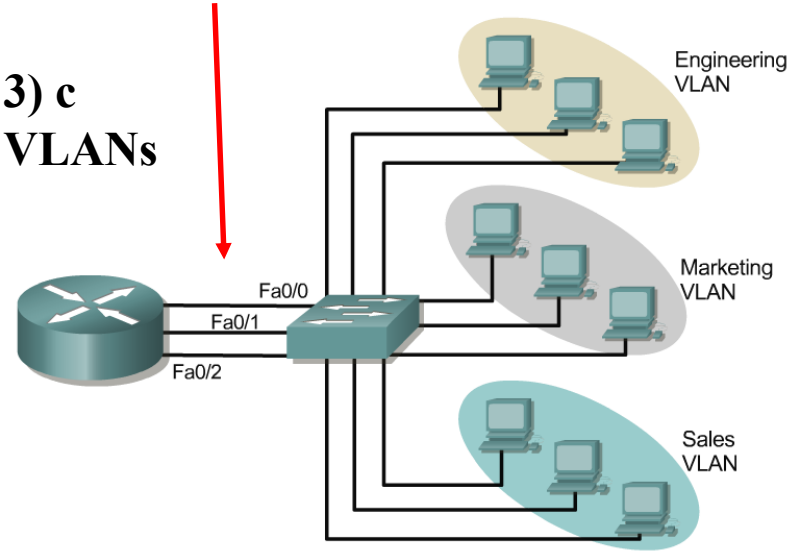


2) С или без VLANs



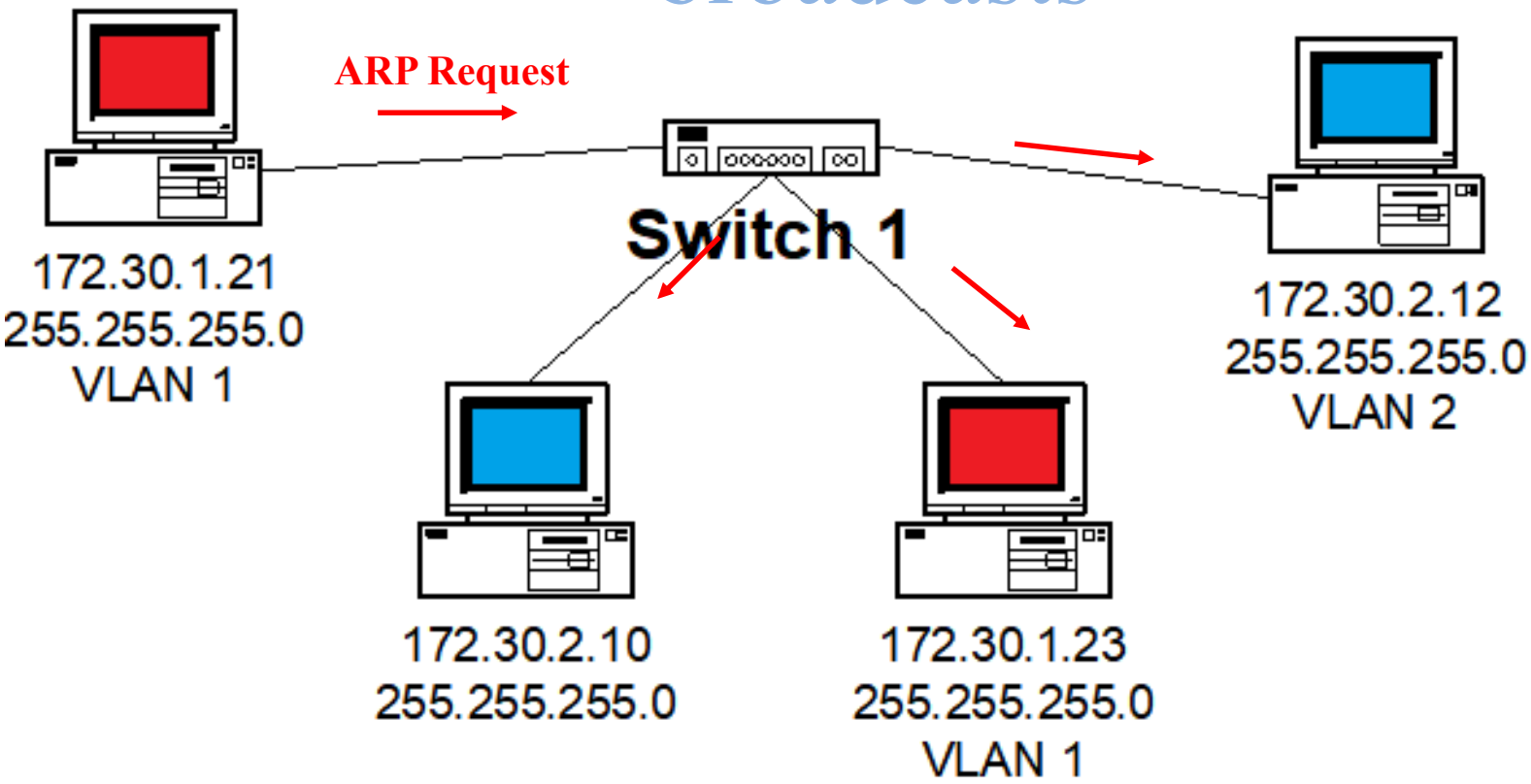
По една връзка за VLAN или с Trunk

3) с VLANs



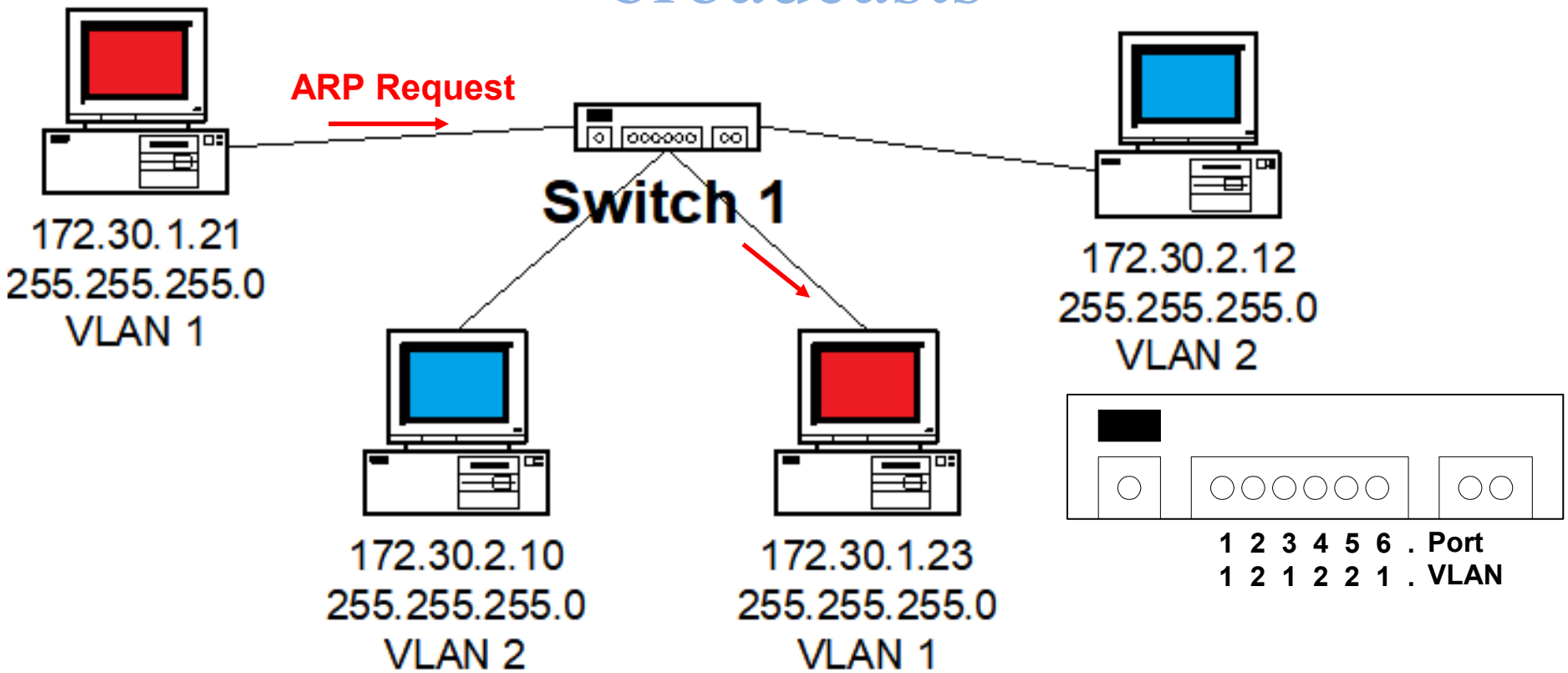
- без VLANs=1 VLAN.
- Колко са broadcast домейните?

Без VLANs – няма контрол на broadcasts



- Всички устройства са в 1 VLAN
- Има 2 подмрежи

С VLANs – има контрол на broadcasts



- Портовете, които поделят един VLAN обменят broadcasts.
- Портовете, които не са в този VLAN не поделят broadcasts.

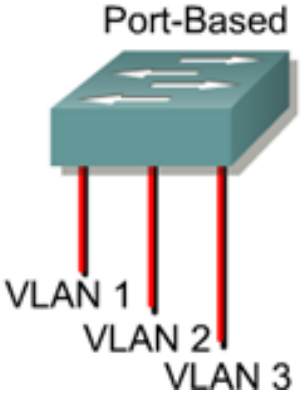
Видове VLAN

- Според начина на конфигуриране:
  - Статични
  - Динамични

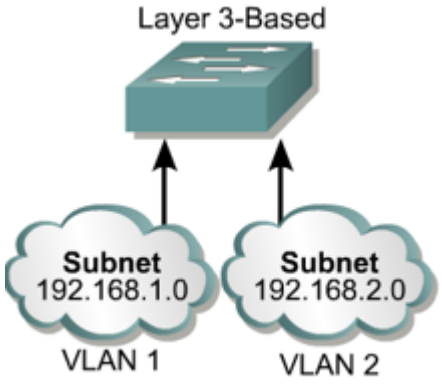
Configuring VLANs	Description
Statically	Network administrators configure port-by-port. Each Port is associated with a specific VLAN. The network administrator is responsible for keying in the mappings between the ports and VLANs.
Dynamically	The ports are able to dynamically work out their VLAN configuration. Uses a software database of MAC address to VLAN mappings (which the network administrator must set up first).

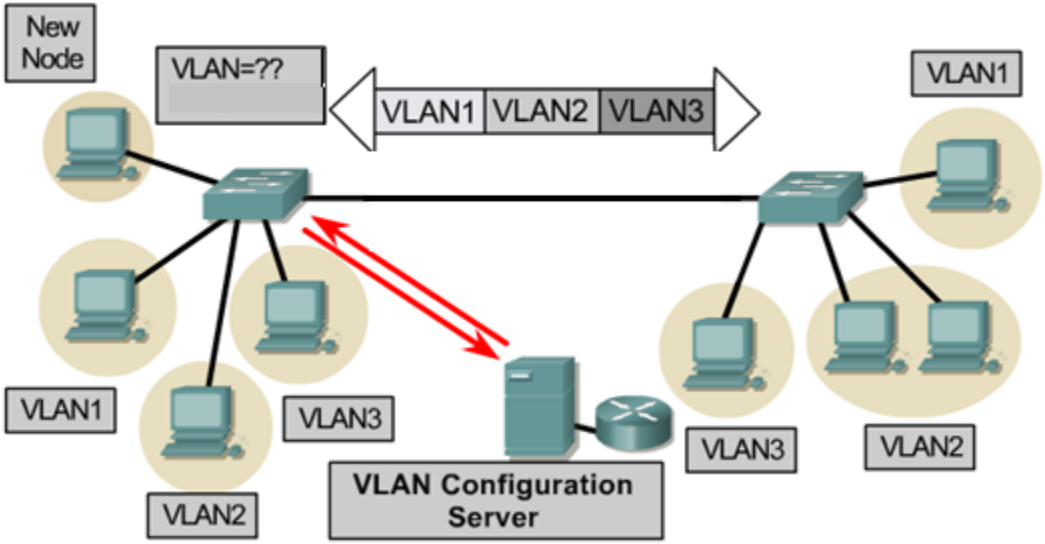
Статични VLAN

- Всеки порт на комутатора е присвоен към някой VLAN.
- Най-често срещан и най-прост метод.
- Портовете се присвояват по един или по групи на един или няколко комутатора.
- Може да се ползва с DHCP.



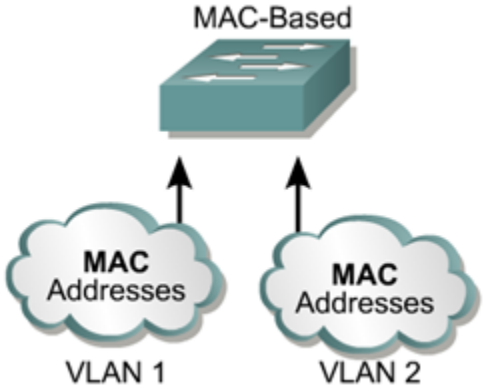
Динамични VLAN-по протокол

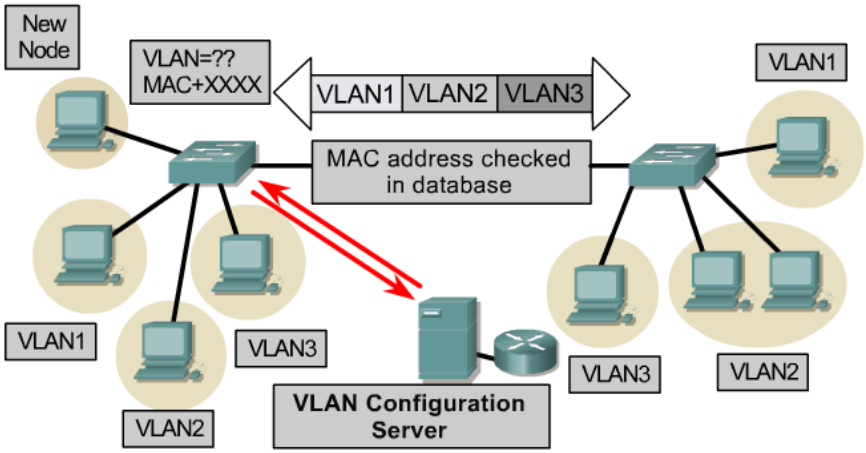




- Рядко се ползва.
- Ползват се IP адреси – една подмрежа – един VLAN.
- Не може да работи с DHCP.

Динамични VLAN - по MAC адрес (1)





- Динамични VLANs се създават със софтуер.
- Принадлежността към VLANs се определя на база MAC адреса на устройството, свързано към порта.
- При включване на устройството към порт на комутатора се проверява в БД към кой VLAN принадлежи.
- По-рядко се ползва.
- Всеки адрес трябва да се въведе в комутатора и да се конфигурира индивидуално.
- По-трудно се администрира, управлява и по-трудно се откриват грешки.

Динамични VLAN - по MAC адрес (2)

Requires Filtering, Impacts Performance

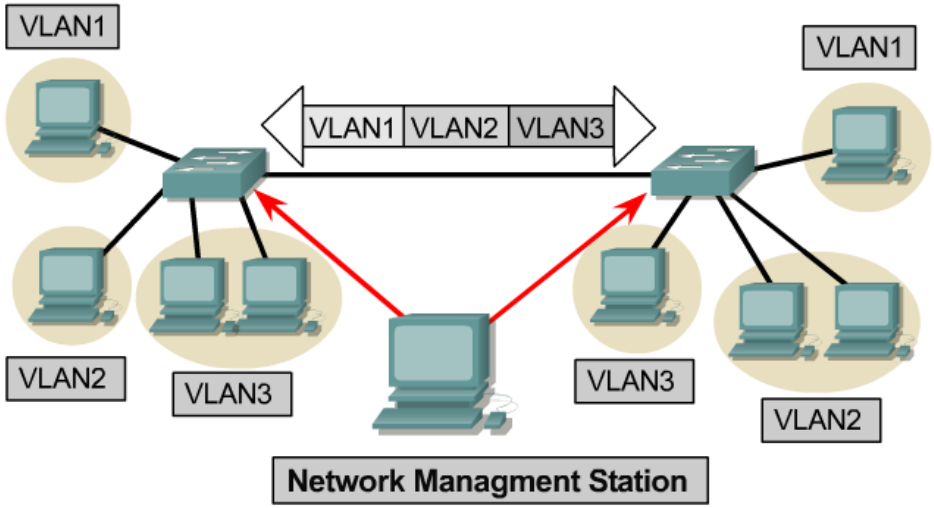
MAC Address Tables
VLAN 1 020701AEF1A OA032192FA2A 026765175GA3A VLAN 2 050503G4GF2A 040404THTB3A 070706GGGF3A

Table Adds
Administrative Overhead

MAC Address Tables
VLAN 1 020701AEF1A OA032192FA2A 026765175GA3A VLAN 2 050503G4GF2A 040404THTB3A 070706GGGF3A

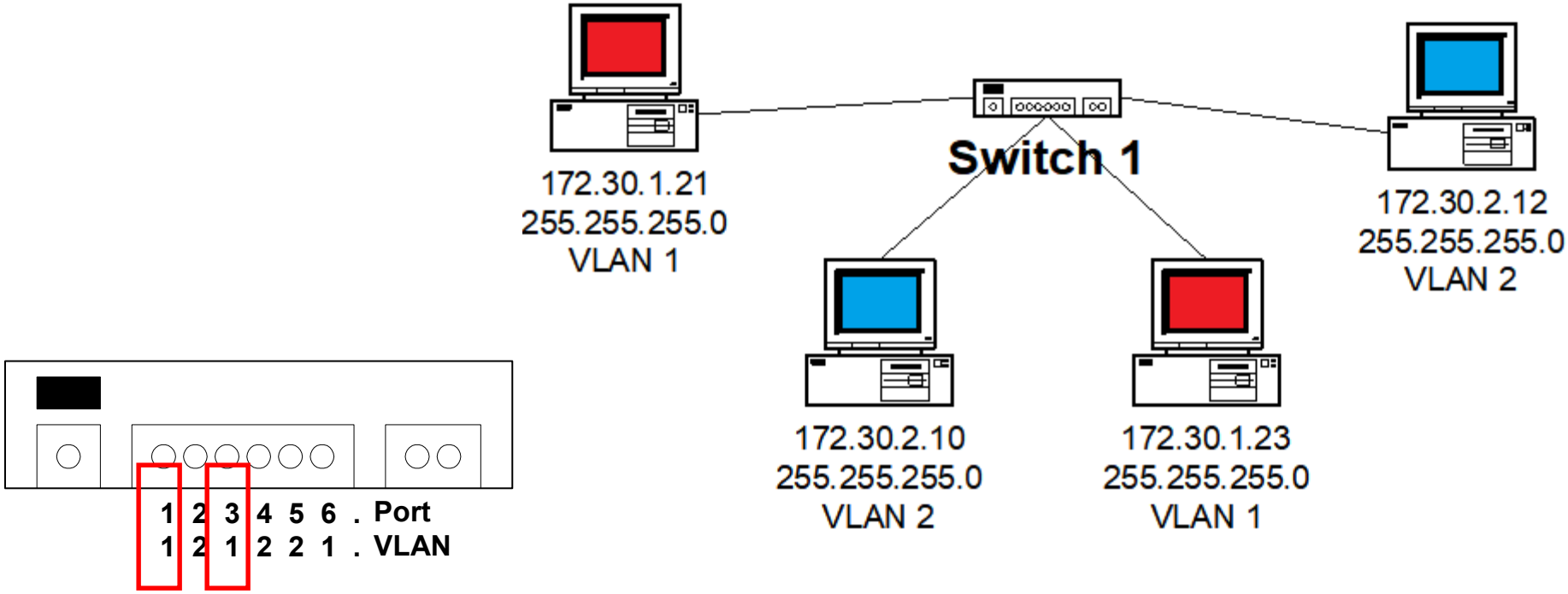
- User assigned based on MAC addresses
- Offers flexibility, yet adds overhead
- Impacts performance, scalability, and administration
- Offers similar process for higher layers

VLAN статично конфигуриране



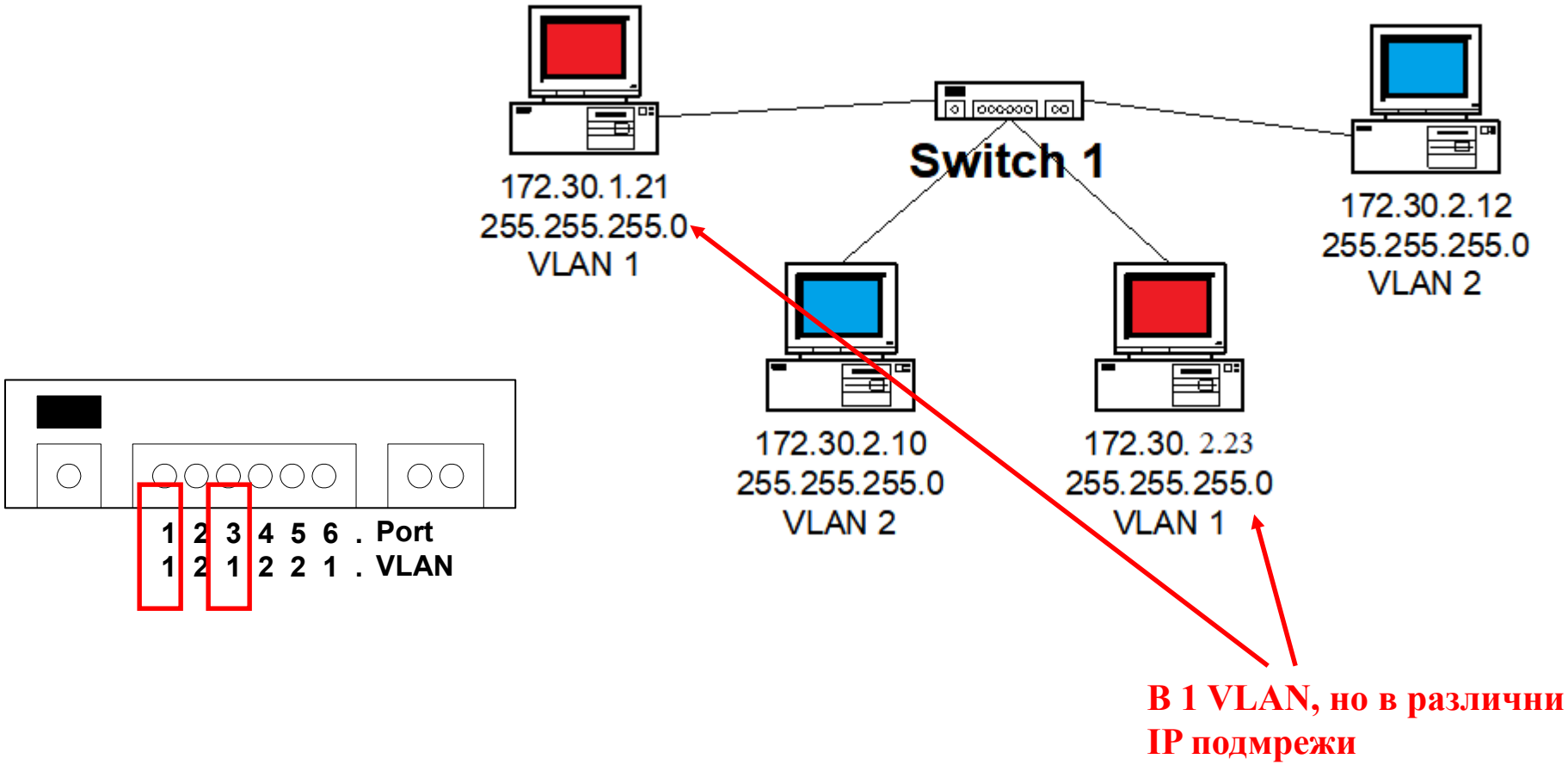
- Static VLANs = port-based = port-centric VLANs.
- Когато устройството се свърже на порта, автоматично се присъединява към групата за VLAN, към която е свързан.
- **default VLAN** за всеки комутатор е **management VLAN**.
- Това е VLAN 1 и не може да бъде изтрит.
- Всеки порт може да бъде присвоен на алтернативен VLAN.

VLAN



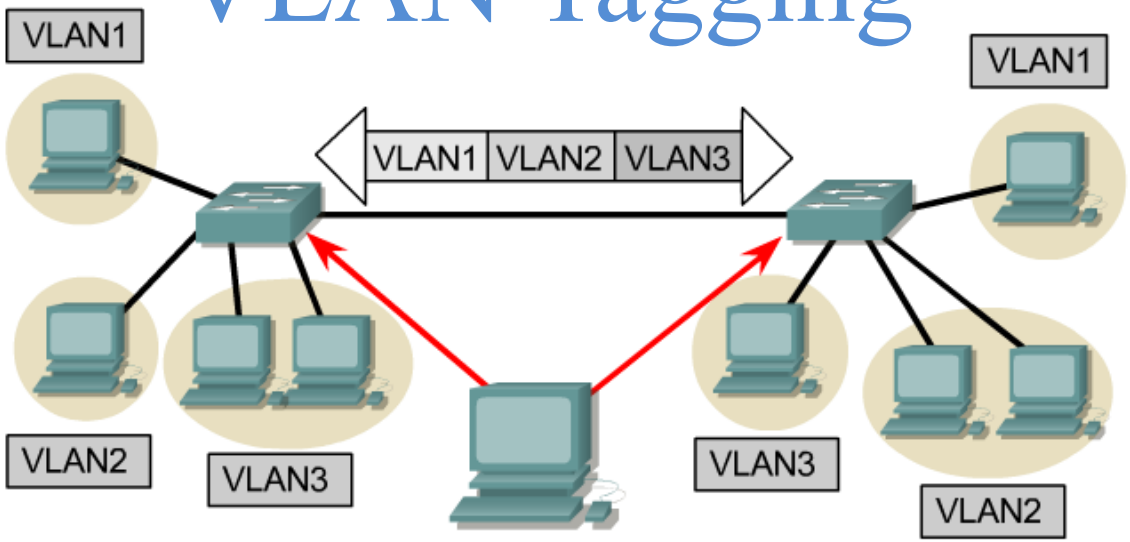
1. VLANs се присвояват на порт на комутатора, а не на хоста.
2. За да бъде хостът част от този VLAN, трябва да получи IP адрес от правилната подмрежа.
3. VLAN = Subnet

VLAN



1. VLANs се присвояват на порт на комутатора, а не на хоста.
2. За да бъде хостът част от този VLAN, трябва да получи IP адрес от правилната подмрежа.
3. VLAN = Subnet

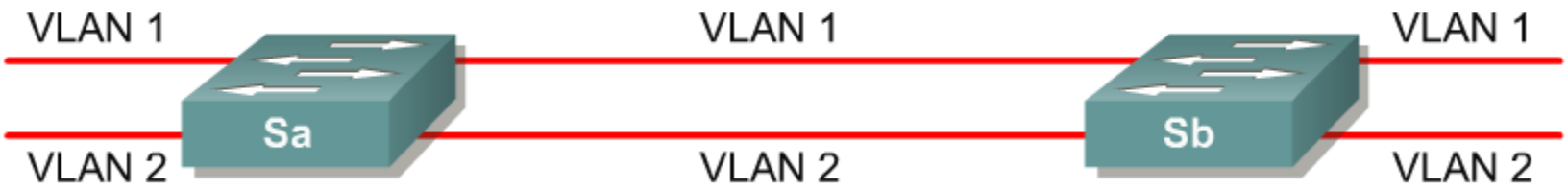
VLAN Tagging



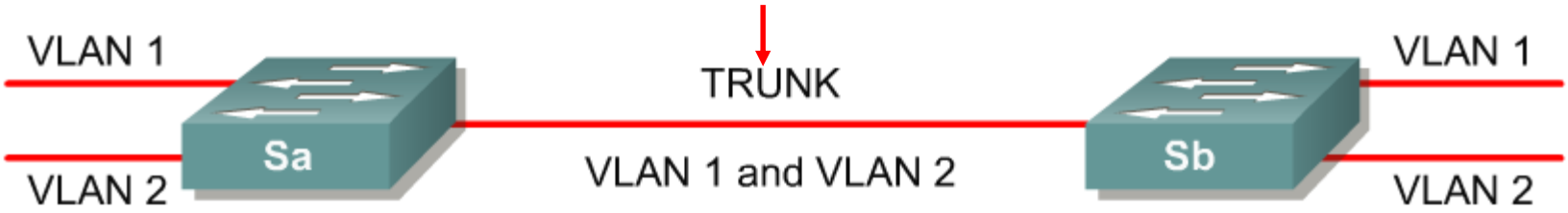
- Служи за пренос на данни по една връзка на повече от един VLAN.
- Добавя се в хедъра на всеки пакет информация за VLAN.
- В последния комутатор VLAN ID се изтрива от хедъра.
- После се предава пакета на портовете, които са към този VLAN.
- Нарича се VLAN trunking.

VLAN Tagging

No VLAN Tagging

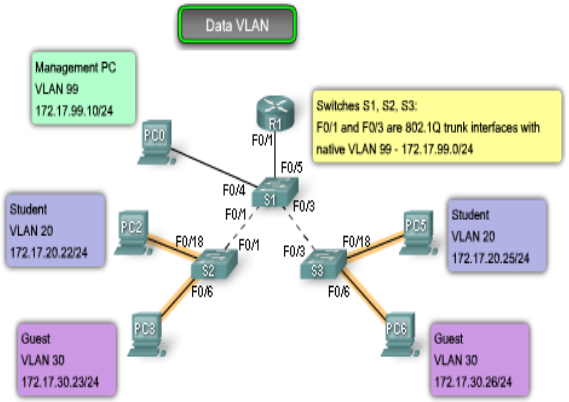


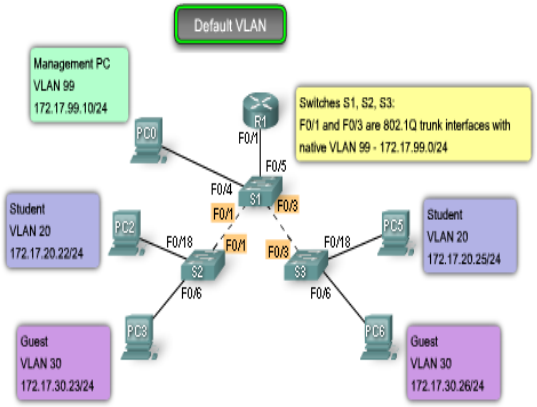
VLAN Tagging



VLAN термини

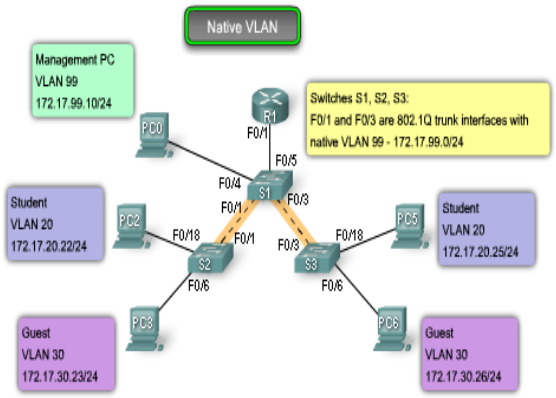
- Data VLAN (user VLAN)
  - За потребителски трафик.
  - Може и глас или управляващ трафик, но се препоръчва те да са отделно.
- Default VLAN
  - След начална инициализация всички портове на комутатора принадлежат към него.
  - по подразбиране е VLAN 1.
  - VLAN 1 не може да се преименува или изтрива.
  - Layer 2 control traffic (CDP ,STP) се пренася от VLAN 1 и това не може да се променя.
  - Но е по-сигурно да се смени default VLAN да не бъде VLAN 1.



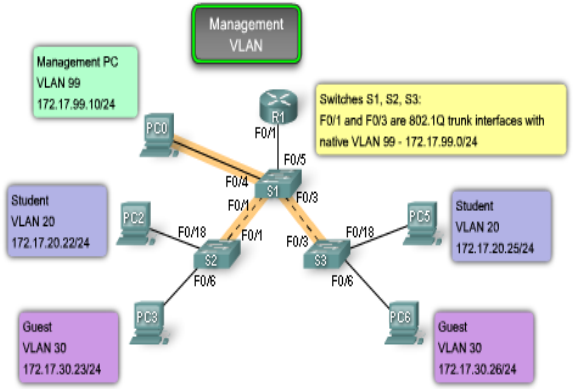


VLAN термини

- Native VLAN
  - –802.1Q trunk port транспортират tagged traffic и untagged traffic (който е по native VLAN).
  - –препоръчва се да се използва друг VLAN вместо VLAN 1 за native VLAN.



- Management VLAN
  - –Който и да е VLAN, в който се конфигурира достъп за управление на комутатора.
  - –Присвоява му се IP адрес и SM.
  - –препоръчва се да се използва друг VLAN вместо VLAN 1 за native VLAN.



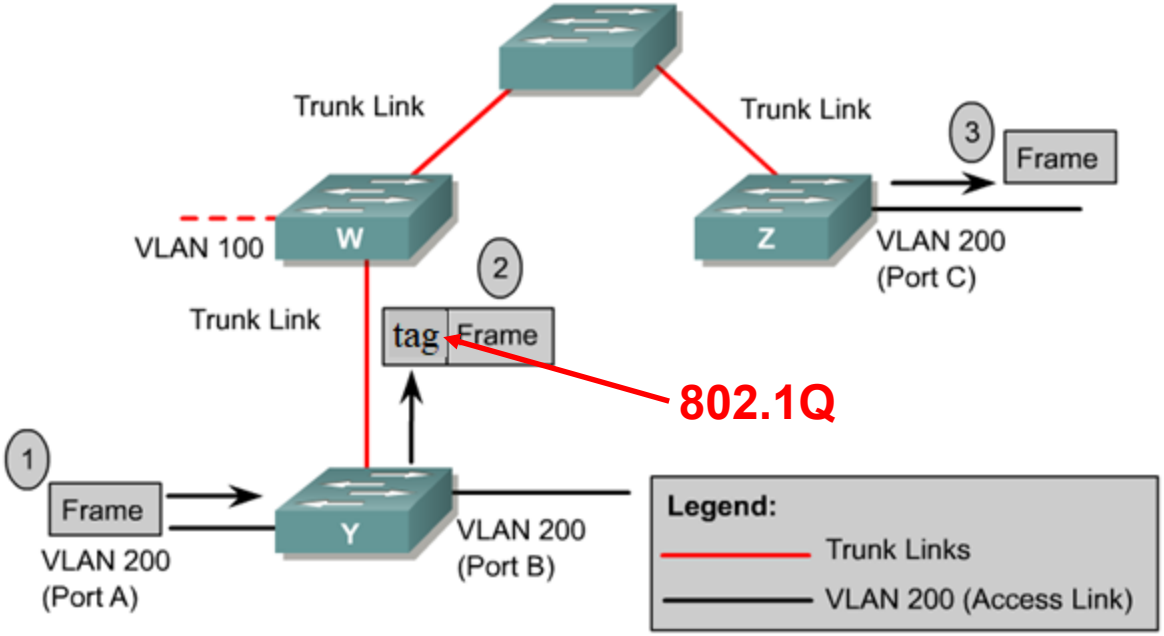
VLAN Tagging 802.1Q

- IEEE 802.1Q - стандартизиран за всички производители.

IEEE 802.1Q

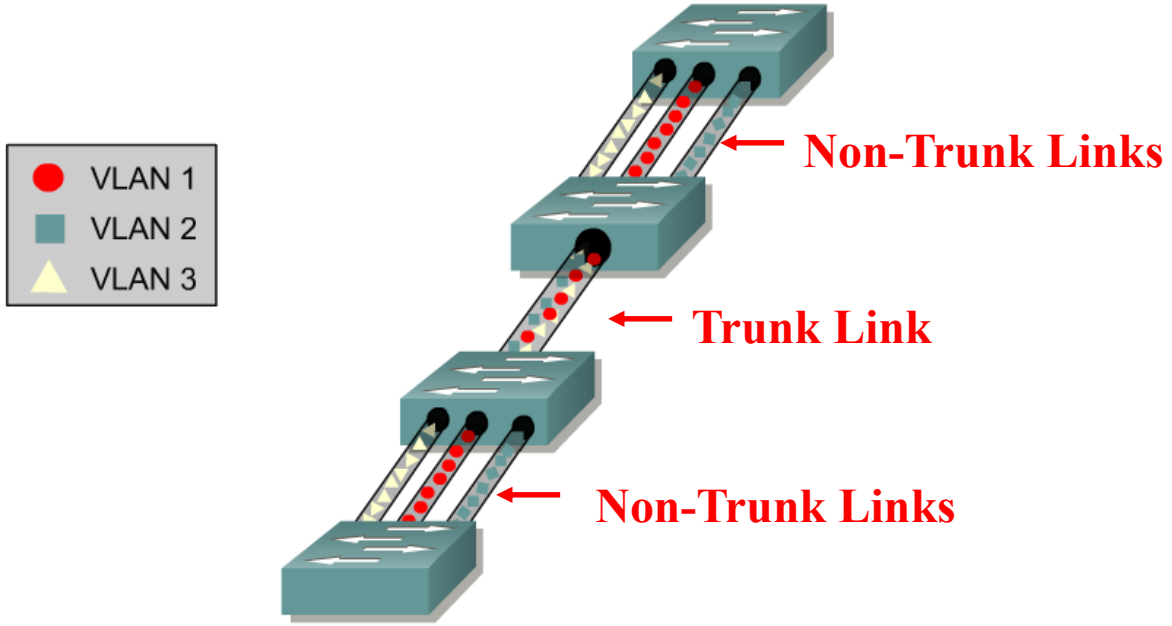
SA and DA MACs	802.1q Tag	Type/Length Field	Data (max 1500 bytes)	*New CRC*

Trunking



- Trunking протоколите са за по ефективно управление на фреймовете от различните VLANs по една физическа връзка.
- Trunking протоколите разпределят фреймовете по асоциираните портове в двата края на trunk връзката.
- Trunk връзките може да пренасят всички VLANs или само специфични VLANs.

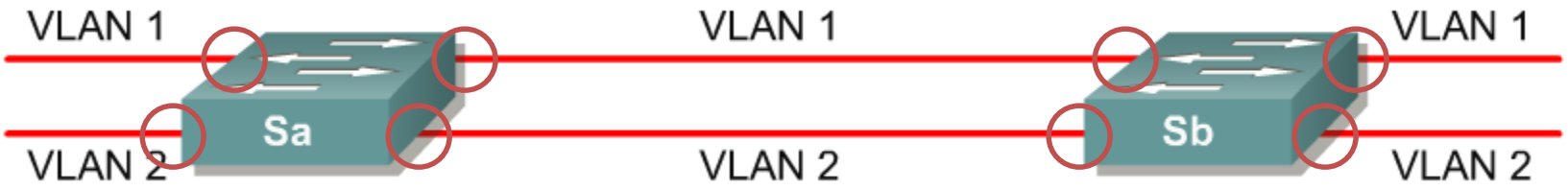
VLANs и trunking



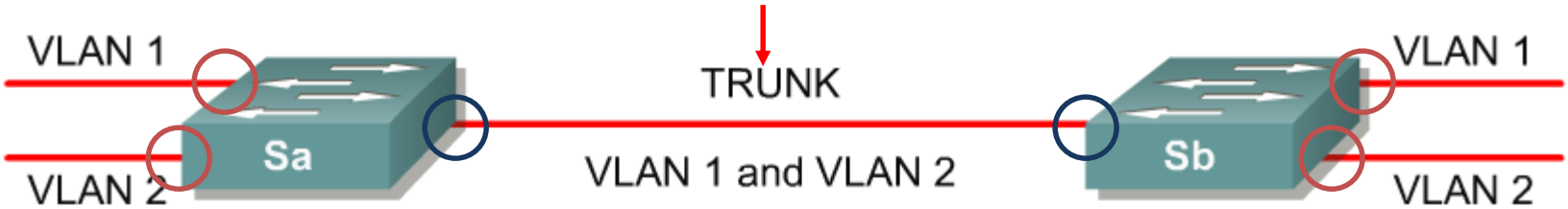
- trunk връзката не принадлежи към конкретен VLAN.
- trunk връзки се конфигурират между комутатори и маршрутизатори или комутатор-комутатор.

С и без Trunking

No VLAN Tagging

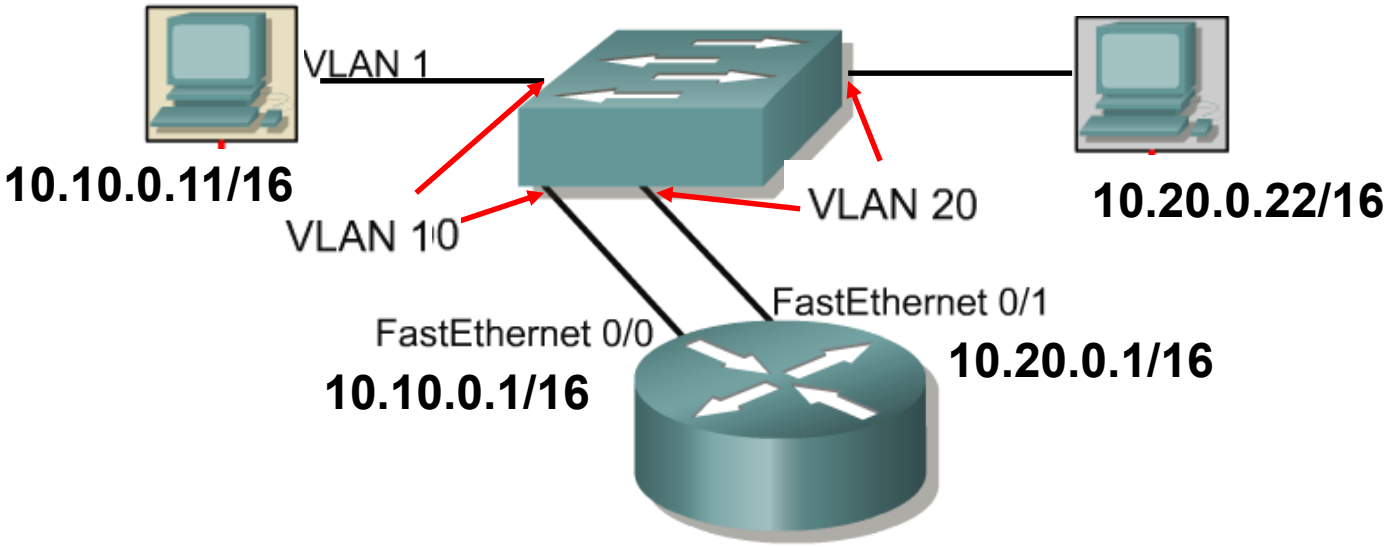


VLAN Tagging

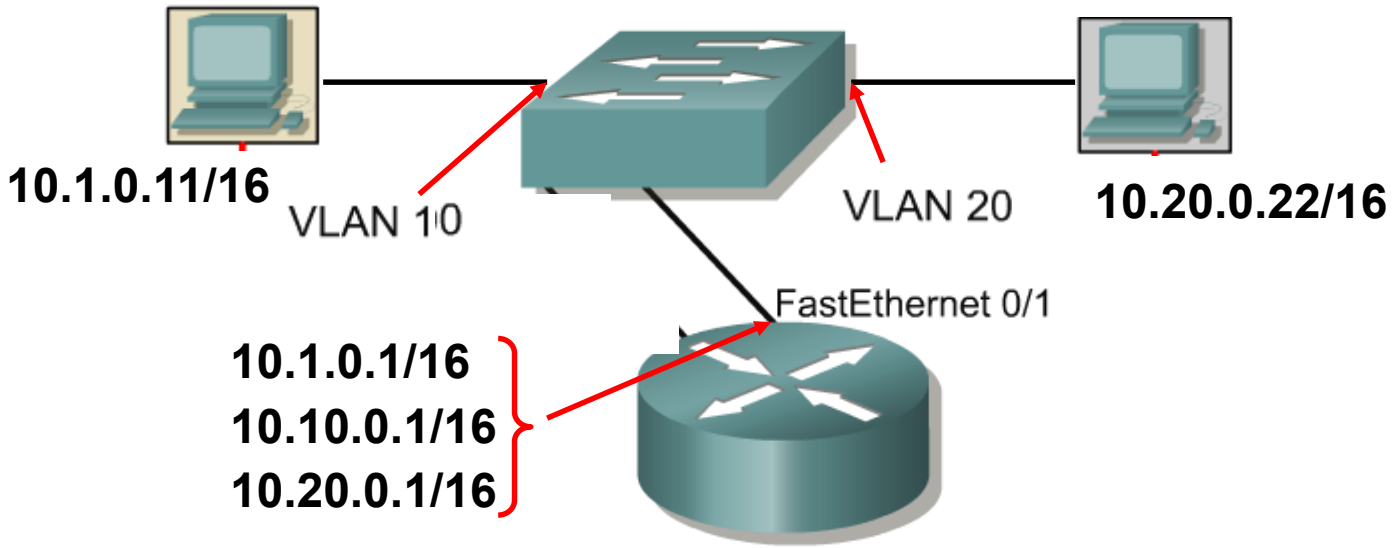


Inter-VLAN Routing

- За да комуникира устройство от 1 VLAN с устройство от друг VLAN, трябва да се ползва маршрутизатор.
- 1 вариант е – към всеки VLAN да има отделна физическа връзка.
- Проблем – повече VLANs- повече връзки.

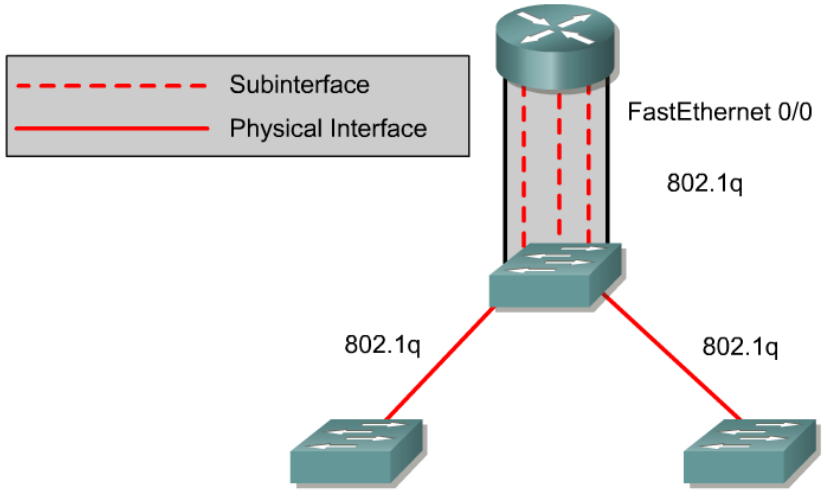


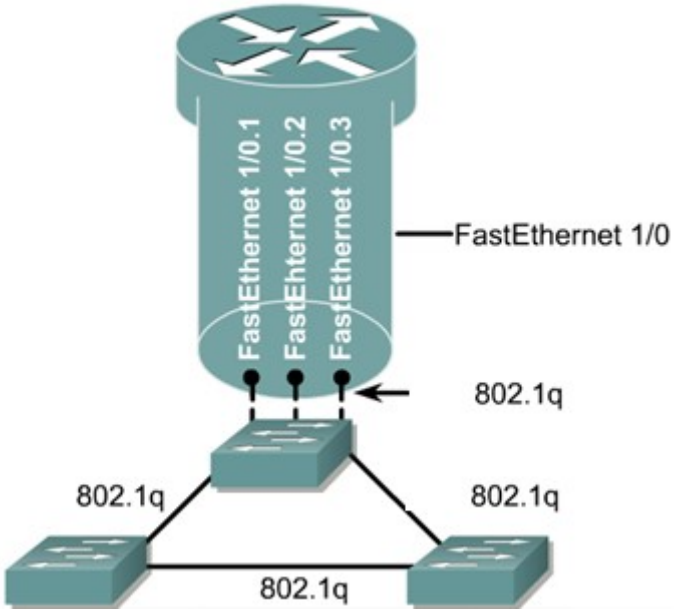
Inter-VLAN Routing – с Trunk



- 2 вариант е да се използва 1 физическа връзка, по която да се пренасят няколко VLANs.
- Реализира се с trunk връзка и подинтерфейси на интерфейса на маршрутизатора.

Физически и логически интерфейси





- Подинтерфейсите на маршрутизатора се ползват за разделяне на физическия интерфейс на няколко логически подинтерфейси.
- Един физически интерфейс може да поддържа до 65,535 логически интерфейси.

Въпроси ?

Благодаря за вниманието !