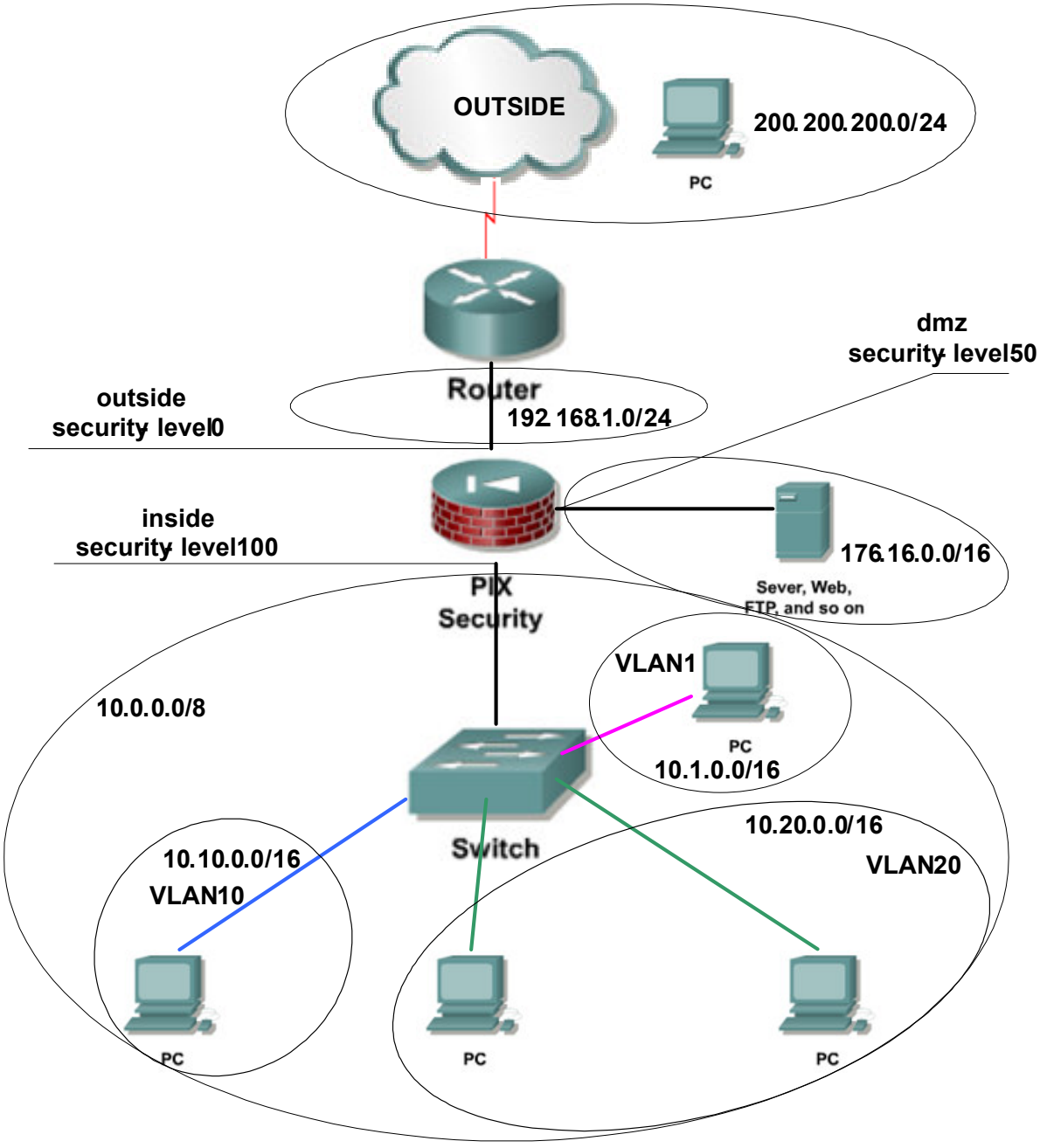
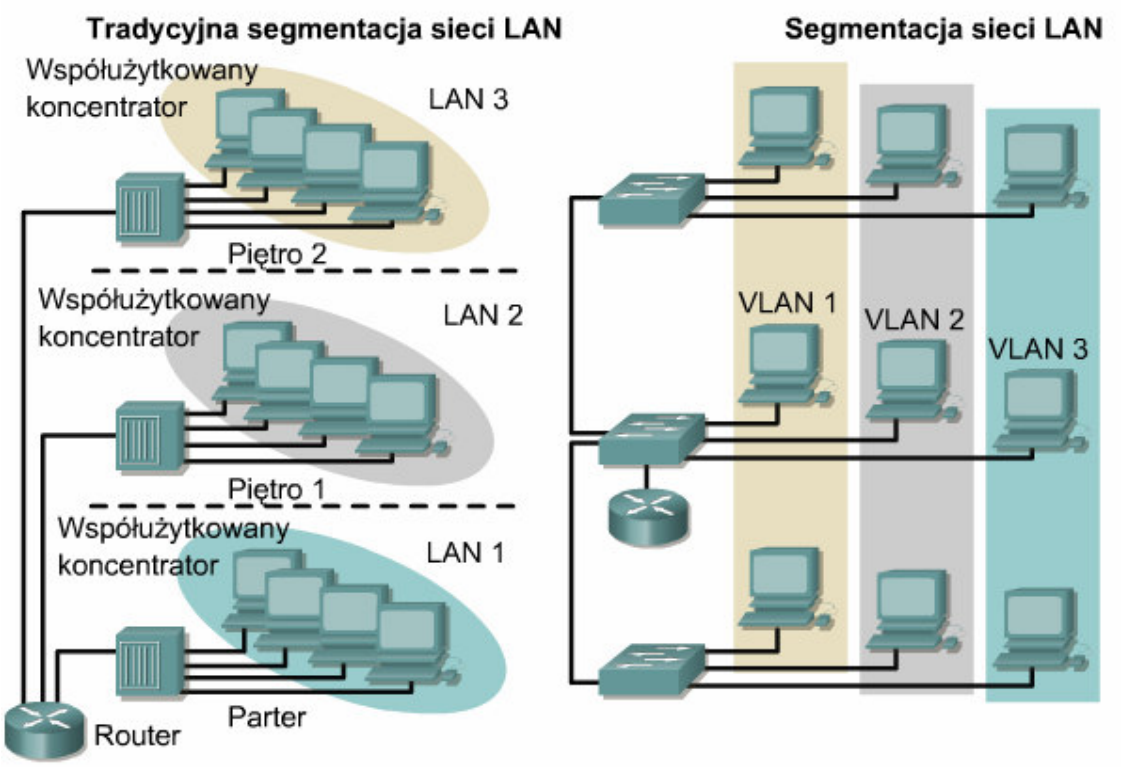
VLAN, trunking, inter-VLAN routing, port-security

Schemat sieci

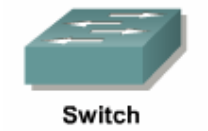


VLAN - Virtual Local Area Network

Segmentacja sieci przy użyciu VLAN



Informacja o sieciach VLAN



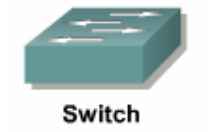
Informacja o wszystkich sieciach VLAN:

Switch# show vlan

Informacja o wybranej sieci VLAN (przykład dla VLAN 10):

Switch# show vlan id 10

Informacja o portach



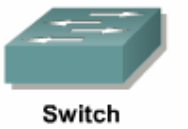
Informacja o portach switcha:

Switch# show interfaces

Informacja o trybie pracy wybranego portu switcha:

Switch# show interfaces fastethernet 0/1 switchport

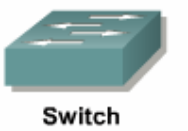
Tworzenie sieci VLAN (przykład dla VLAN 10)



Switch# vlan database

Switch(vlan)# vlan 10 name *<nazwa_sieci_VLAN>*

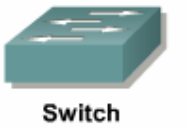
Usuwanie sieci VLAN (przykład dla VLAN 10)



Switch# vlan database

Switch(vlan)# no vlan 10

Przypisanie portu do sieci VLAN (przykład dla VLAN 10 i interfejsu 0/2)

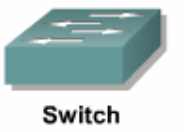


Switch(config)# interface fastethernet 0/2

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

Usunięcie portu z sieci VLAN (przykład dla VLAN 10 i interfejsu 0/2)

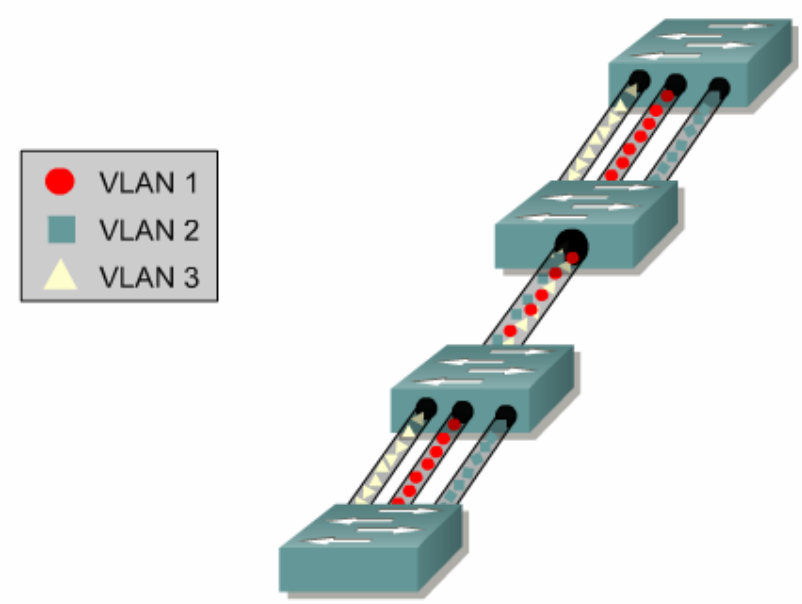


Switch(config)# interface fastethernet 0/2

Switch(config-if)# no switchport access vlan 10

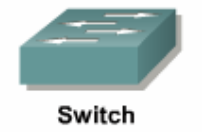
trunking

Idea działania łącza trunkingowego



Tworzenie łącza trunkingowego

(do połączeń switch-switch, switch-router (protokół 802.1Q))



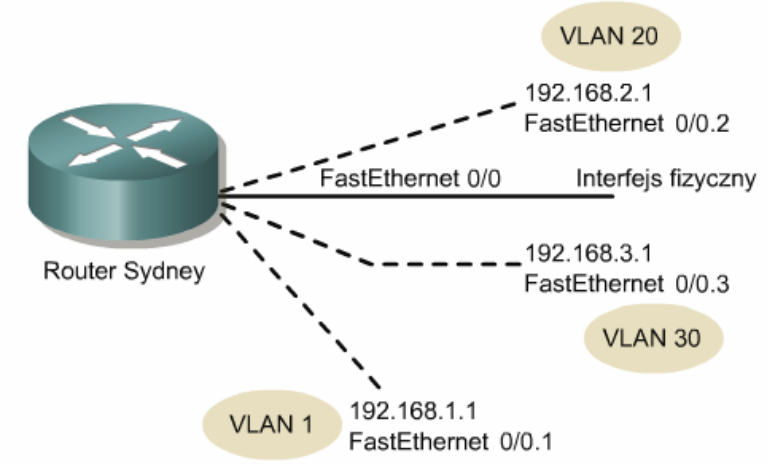
Switch(config)# interface fastethernet 0/1

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk encapsulation dot1q

inter-VLAN routing

Routing pomiędzy sieciami VLAN



Router(config)# interface fastethernet 0/0.1

Router(config-if)# descritption VLAN1

Router(config-if)# encapsulation dot1q 1

Router(config-if)# ip address 10.1.0.1 255.255.0.0

Pix(config)# interface ethernet 0.1

Pix(config-if)# descritption VLAN1

Pix(config-if)# vlan 1

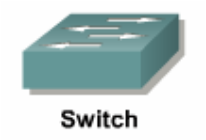
Pix(config-if)# nameif inside-vlan-admin

Pix(config-if)# security-level 100

Pix(config-if)# ip address 10.1.0.1 255.255.0.0

port-security

Bezpieczeństwo portów (ograniczenie liczby hostów na porcie)



Ustawienie bezpiecznego portu na interfejsie FastEthernet 0/4:

Switch(config)# interface fastethernet 0/4

Switch(config-if)# switchport mode access

ograniczenie dostępu hostów do switcha:

Switch(config-if)# switchport port-security

w przypadku naruszenie reguły bezpieczeństwa nastąpi wyłączenie portu:

Switch(config-if)# switchport port-security violation shutdown

ograniczenie do jednego hosta na porcie:

Switch(config-if)# switchport port-security maximum 1

adresu MAC tego hosta switch nauczy się automatycznie (pierwszy podłączony):

Switch(config-if)# switchport port-security mac-address sticky

Testowanie wykonanej konfiguracji: **show port-security, show mac-address-table, show run**

Uwaga: Jeśli nastąpi naruszenie zasad bezpieczeństwa i port zostanie wyłączony, konieczne będzie użycie polecenia **shutdown** a następnie **no shutdown** w celu dokonania reaktywacji tego portu.

Imiona i Nazwiska:

…….

…….

…….

…….

…….

Czynności wstępne:

01. Przywrócić zapisane konfiguracje urządzeń (router i pix) z serwera TFTP.
02. Usunąć zapisaną konfigurację na switch'u.
03. Przeprowadzić testy:
    - Sprawdzić czy można się połączyć ze strefy „inside" do serwera **ftp** w strefie „dmz"……..

      Z jakiego adresu nastąpiło połączenie: ……
    - Sprawdzić czy można się połączyć ze strefy „inside" do serwera **ftp** w strefie „outside"……..

      Z jakiego adresu nastąpiło połączenie: ……
    - Sprawdzić czy można się połączyć ze strefy „dmz" do serwera **ftp** w strefie „outside"……..

      Z jakiego adresu nastąpiło połączenie: ……

Konfiguracja sieci VLAN:

01. Skonfigurować switch zgodnie z tabelą:

Nazwa przełącznika	Hasło dostępu do trybu uprzywilejowanego	Hasło terminala wirtualnego i konsoli	Numery sieci VLAN	Nazwa sieci VLAN	Porty przełącznika należące do określonego VLAN'u	Adres IP
Switch_1	cisco	Test	VLAN 1 VLAN 10 VLAN 20	- Dyrekcja Pracownicy	0/1 – 0/2 0/3 – 0/10 0/11 – 0/24	TAK NIE NIE

02. Podłączyć jeden host do sieci VLAN „Dyrekcja".
03. Podłączyć drugi host do sieci VLAN „Pracownicy". Zainstalować serwer ftp.
04. Podłączyć pix do portu switcha należącego do sieci VLAN „Dyrekcja".
05. Przeprowadzić testy:
    - Czy host z sieci VLAN „Dyrekcja" ping'uje interfejs pix'a? …….
    - Czy host z sieci VLAN „Pracownicy" ping'uje interfejs pix'a? …….

- Czy z hosta z sieci VLAN „Dyrekcja” można się połączyć z serwerem **ftp** w sieci „dmz”? ……..
- Czy z hosta z sieci VLAN „Dyrekcja” można się połączyć z serwerem **ftp** w sieci „outside”? ……..
- Czy z hosta z sieci VLAN „Dyrekcja” można się połączyć z serwerem **ftp** w sieci VLAN „Pracownicy”? ……..
- Czy z hosta z sieci VLAN „Pracownicy” można się połączyć z serwerem **ftp** w sieci „dmz”? ……..
- Czy z hosta z sieci VLAN „Pracownicy” można się połączyć z serwerem **ftp** w sieci „outside”? ……..

Konfiguracja łącza trunkingowego i routingu pomiędzy sieciami VLAN:

01. Na switchu skonfigurować łącze trunkingowe na porcie 0/1.
02. Na pix dodać i skonfigurować trzy podinterfejsy na interfejsie „inside”.

Dla **VLAN1 security-level=100**; **VLAN10 security-level=90**; **VLAN20 security-level=80**.

03. Nadać hostom właściwe adresy IP, w zależności od ich przynależności do VLAN.
04. Przeprowadzić testy:
    - Czy host z sieci VLAN „Dyrekcja” ping’uje interfejs pix’a? ……..
    - Czy host z sieci VLAN „Pracownicy” ping’uje interfejs pix’a? ……..
    - Czy z hosta z sieci VLAN „Dyrekcja” można się połączyć z serwerem **ftp** w sieci „dmz”? ……..
    - Czy z hosta z sieci VLAN „Dyrekcja” można się połączyć z serwerem **ftp** w sieci „outside”? ……..
    - Czy z hosta z sieci VLAN „Dyrekcja” można się połączyć z serwerem **ftp** w sieci VLAN „Pracownicy”? ……..
    - Czy z hosta z sieci VLAN „Pracownicy” można się połączyć z serwerem **ftp** w sieci „dmz”? ……..
    - Czy z hosta z sieci VLAN „Pracownicy” można się połączyć z serwerem **ftp** w sieci „outside”? ……..

Konfiguracja translacji adresów NAT(PAT)

(korekta w związku ze zmianami w strukturze sieci):

01. Skonfigurować system translacji adresów NAT(PAT) tak aby:
    - Z hosta z sieci VLAN „Pracownicy" można się połączyć z dowolnym serwerem w sieci „dmz" ……..
    - Z hosta z sieci VLAN „Dyrekcja" można się połączyć z dowolnym serwerem w sieci „dmz", „outside" oraz VLAN „Pracownicy" ……..

Ograniczenie liczby hostów na porcie switcha

01. Ograniczyć liczbę hostów na portach switcha do 1 (pierwszy podłączony),
w przypadku naruszenia zasad bezpieczeństwa port ma być wyłączony.
02. Przeprowadzić testy:
    - Czy MAC hosta podłączonego do portu jest typu STATIC? …….
    - Czy MAC hosta podłączonego jest w running-config? ……..
    - Czy po podłączeniu do portu innego hosta port został wyłączony? ……

Czynności końcowe:

01. Zapisać konfiguracje urządzeń na serwerze TFTP.
02. Usunąć konfiguracje urządzeń.