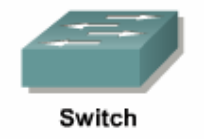
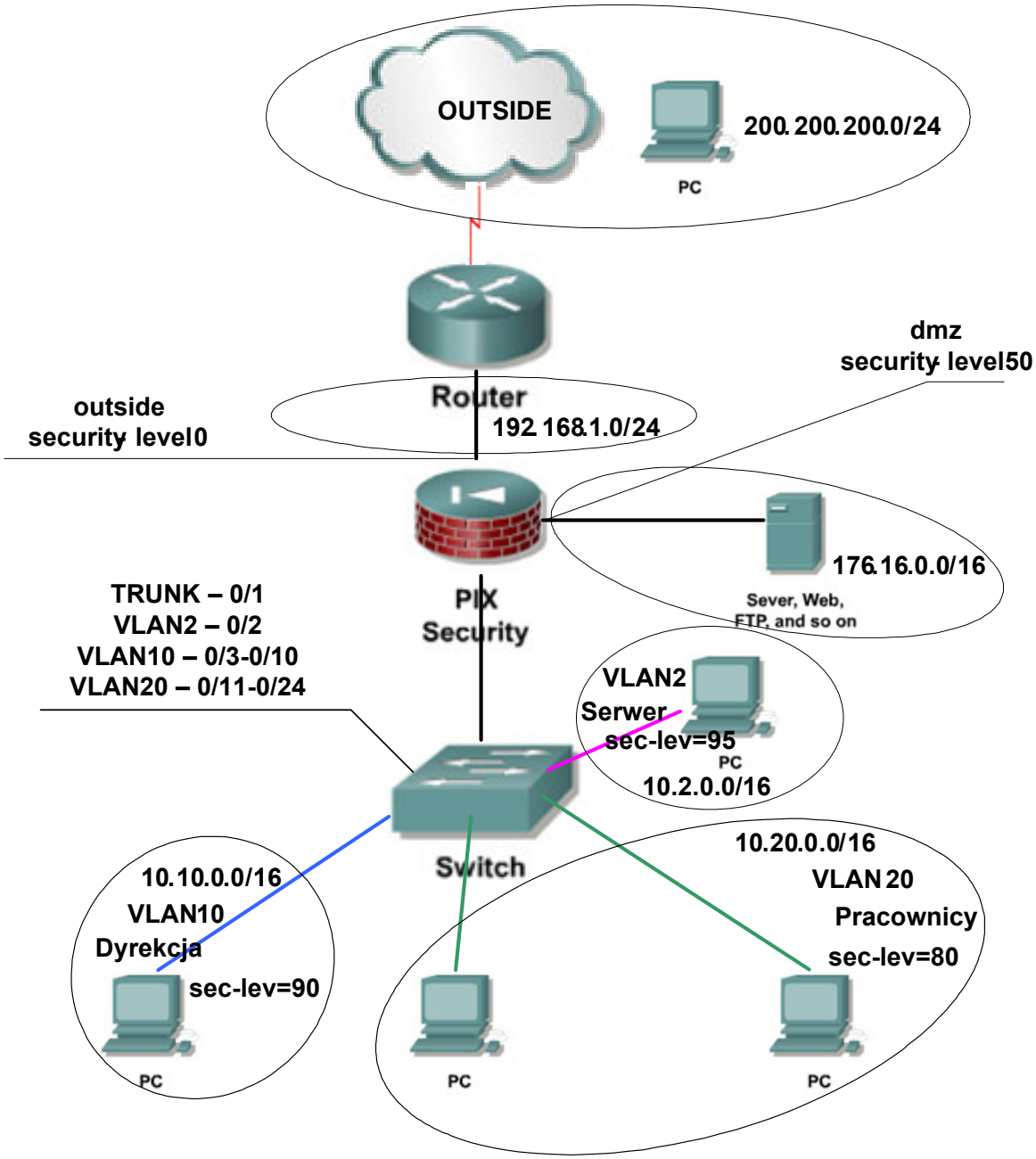
RADIUS - Remote Authentication Dial-In User Service



Schemat sieci



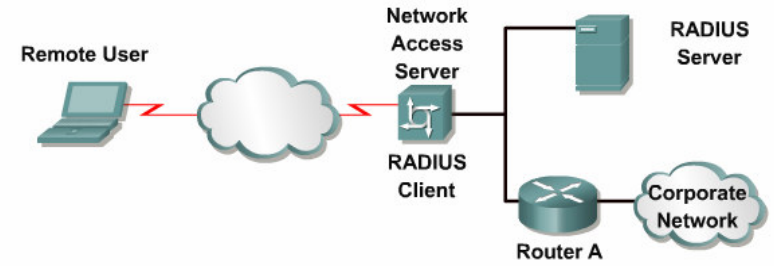
Co to jest RADIUS?

RADIUS (*Remote Authentication Dial-In User Service*) opracowany został przez Livingston Enterprises, Inc (obecnie część Lucent Technologies).

RADIUS jest usługą umożliwiającą uwierzytelnianie, autoryzowanie i rejestrowanie działań użytkownika.

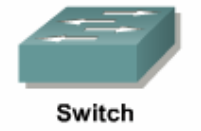
RADIUS składa się z trzech elementów:

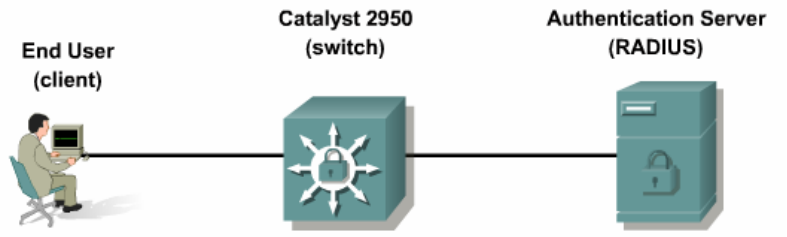
- Protokołu korzystającego z UDP/IP.
- Serwera.
- Klienta.



Konfiguracja 802.1x

IEEE 802.1x protokół gwarantujący bezpieczny dostęp do sieci (a dokładnie do danego portu switcha). Aby uzyskać dostęp do portu switcha należy przeprowadzić proces uwierzytelniania.





Switch(config)# aaa new-model

Do uwierzytelniania wybieramy serwer RADIUS:

Switch(config)# aaa authentication dot1x default group radius

Aktywujemy IEEE 802.1x:

Switch(config)# dot1x system-auth-control

Konfigurujemy wybrany port switcha:

Switch(config-if)# switchport mode access

Switch(config-if)# dot1x port-control auto

Ustalenie adresu serwera RADIUS, portu i hasła do komunikacji z nim:

Switch(config)# radius-server host 10.x.y.z auth-port 1812 acct-port 1813 key klucz

Sprawdzenie działania 802.1x:

Switch# show dot1x all

Switch# show dot1x interface fa0/x

Uwaga: Aby host obsługiwał protokół 802.1x należy w systemie Windows:

- włączyć usługę Konfiguracja Sieci Bezprzewodowej (Wireless Configuration),
- we właściwościach kablowego połączenia sieciowego w zakładce Authentication włączyć protokół 802.1x i wybrać typ EAP *MD5-Challenge*.

Włączenie authentication-proxy

(uwierzytelnianie z wykorzystaniem serwera RADIUS)

Konfiguracja połączenia z serwerem RADIUS:

PIX(config)# aaa-server MOJRADIUS protocol radius

PIX (config-aaa-server-group)# exit

PIX (config)# aaa-server MOJRADIUS (inside-SERWER) host 10.2.0.xx

PIX (config-aaa-server-host)# key klucz

PIX (config-aaa-server-host)# authentication-port 1812

PIX (config-aaa-server-host)# accounting-port 1813

Sprawdzenie konfiguracji:

PIX (config)# show running-config aaa-server

Wymuszenie uwierzytelniania na cały ruch wychodzący z sieci Pracownicy:

PIX(config)# aaa authentication include any inside-PRAC

10.20.0.0 255.255.0.0 0 0 MOJRADIUS

Wyświetlenie statystyk uwierzytelniania:

PIX(config)# show uauth

Usunięcie uwierzytelnionych użytkowników:

PIX(config)# clear uauth

Imiona i Nazwiska:

…….

…….

…….

…….

…….

Czynności wstępne:

01. Przywrócić połączenia urządzeń.
02. Usunąć zapisane konfiguracje na urządzeniach (switch, router, pix).
03. Przywrócić konfiguracje urządzeń (switch, router, pix) z serwera TFTP.
04. Zainstalować serwery **www** i **ftp** na hostach w sieciach „dmz" i „outside" .

Uwaga: strona na serwerze **www** w sieci „outside" i „dmz" powinny się różnić.

05. Przeprowadzić testy:
    - Połączenie z sieci „inside-PRACOWNICY" do serwera **www** w strefie „dmz" ……..
    - Połączenie z sieci „inside-PRACOWNICY" do serwera **ftp** w strefie „dmz" ……..
    - Połączenie z sieci „inside-PRACOWNICY" do serwera **www** w strefie „outside" ……
    - Połączenie z sieci „inside-PRACOWNICY" do serwera **ftp** w strefie „outside" ……
    - Połączenie z sieci „inside-DYREKCJA" do serwera **www** w strefie „dmz" ……..
    - Połączenie z sieci „inside-DYREKCJA" do serwera **ftp** w strefie „dmz" ……..
    - Połączenie z sieci „inside-DYREKCJA" do serwera **www** w strefie „outside" ……..
    - Połączenie z sieci „inside-DYREKCJA" do serwera **ftp** w strefie „outside" ……..
    - Połączenie z sieci „dmz" do serwera **www** w strefie „outside" ……..
    - Połączenie z sieci „dmz" do serwera **ftp** w strefie „outside" ……..
    - Połączenie z sieci „outside" do serwera **www** w strefie „dmz" ……..
    - Połączenie z sieci „outside" do serwera **ftp** w strefie „dmz" ……..

Instalacja i konfiguracja serwera RADIUS:

01. Zainstalować w sieci „inside-SERWER" (VLAN 2) serwer RADIUS (WinRadius).
02. Dodać do bazy WinRadius.mdb użytkownika.
03. Skonfigurować serwer: Adres IP klienta, port nasłuchu, tajny klucz.

Uwaga: Klientami będą PIX i switch.

PIX - Authentication-proxy (uwierzytelnianie z wykorzystaniem serwera RADIUS)

01. Usunąć auth-proxy pobierające dane o użytkownikach z lokalnej bazy danych PIX (LOCAL).
02. Skonfigurować dane o serwerze RADIUS.
03. Dodać auth-proxy pobierające dane o użytkownikach z serwera RADIUS.
04. Przeprowadzić testy:
    - Usunąć wszystkich uwierzytelnionych użytkowników (**clear uauth**).
    - Czy przy połączeniu z sieci „inside-PRACOWNICY" do serwera **www** w sieci „outside" wymagana jest uwierzytelnianie? ……
      Czy uwierzytelnianie powiodło się? ……
    - Czy przy połączeniu z sieci „inside-DYREKCJA" do serwera **www** sieci „outside" wymagana jest uwierzytelnianie? ……

SWITCH - Konfiguracja 802.1x

01. Włączyć obsługę 802.1x w systemie Windows.
02. Włączyć obsługę 802.1x na switch'u.
03. Skonfigurować wybrany port switch'a należący do sieci „inside-PRACOWNICY" tak aby wymagane było uwierzytelnianie 802.1x.
04. Skonfigurować dane o serwerze RADIUS na switch'u.
05. Podłączyć host do portu z włączonym 802.1x (sieć „inside-PRACOWNICY").
06. Przeprowadzić testy:
    - Czy wymagane jest uwierzytelnienie? ……
    - Czy host może ping'ować swoją bramę? ……
    - Czy działa połączenie z hosta do serwera **www** w strefie „outside"? ……

Czynności końcowe:

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