Politechnika Białostocka

Wydział Elektryczny

Katedra Telekomunikacji i Aparatury Elektronicznej

Instrukcja do zajęć laboratoryjnych

Temat ćwiczenia:

Konfiguracja usługi uwierzytelniania na porcie w standardzie 802.1x

Numer ćwiczenia: **4**

Laboratorium z przedmiotu:
Zarządzanie i bezpieczeństwo w sieciach teleinformatycznych

Kod przedmiotu: TS1D6220

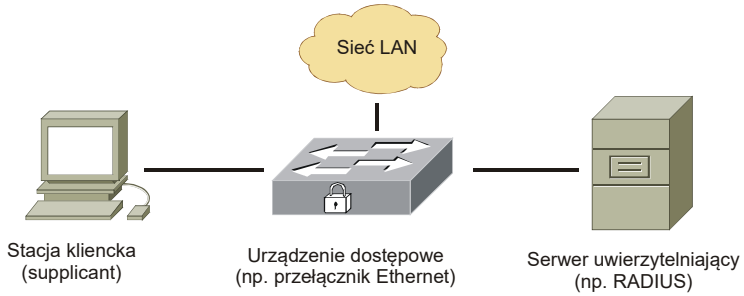
Instrukcję opracował:
dr inż. Andrzej Zankiewicz

Białystok 2020

1. Ogólna charakterystyka ćwiczenia

Kwestie zapewnienia właściwego poziomu bezpieczeństwa systemów teleinformatycznych stanowią obecnie bardzo istotne zagadnienie. Jednym z elementów zabezpieczenia jest uwierzytelnianie użytkowników systemu. Może być ono realizowane na różnych poziomach zaczynając od uwierzytelniania dostępu do portu na poziomie warstwy łącza danych, a kończąc np. na uwierzytelnianiu użytkowników w aplikacjach webowych.

Przedmiotem ćwiczenia jest konfiguracja uwierzytelniania użytkowników sieci LAN na poziomie dostępu do portu przełącznika Ethernet (odpowiada to warstwie łącza danych modelu OSI). Uwierzytelnianie to jest niezależne od stosowanych protokołów w warstwach powyżej warstwy łącza danych. Wykorzystywana w ćwiczeniu technologia kontroli dostępu to standard 802.1x. Na rysunku 1 przedstawiono ogólną strukturę konfigurowanego systemu.



Rys. 1. Ogólna struktura systemu 802.1x

W skład systemu 802.1x wchodzą stacja kliencka zawierająca komponent uwierzytelniania 802.1x (tzw. *supplicant*), brzegowe urządzenie dostępowe do sieci (najczęściej jest to przełącznik Ethernet lub punkt dostępowy Wi-Fi) oraz serwer uwierzytelniający zawierający bazę użytkowników wraz z danymi pozwalającymi na ich uwierzytelniania (np. poprzez sprawdzenie hasła wprowadzonego przez użytkownika). Urządzenie dostępowe po stwierdzeniu próby dostępu przez użytkownika wysyła mu żądanie uwierzytelnienia, na które użytkownik odpowiada wprowadzając swoje dane uwierzytelniające (np. nazwę użytkownika oraz hasło). Dane te są wysyłane przez urządzenie dostępowe do skonfigurowanego w nim serwera uwierzytelniającego, który dokonuje sprawdzenia ich poprawności na podstawie dostępnej mu bazy użytkowników. Wynik uwierzytelnienia serwer odsyła do urządzenia dostępowego, które na jego podstawie udziela lub nie udziela użytkownikowi dostępu do sieci.

Komunikacja uwierzytelniająca pomiędzy stacją kliencką, a urządzeniem dostępowym odbywa się z wykorzystaniem protokołu EAPOP (EAP over LAN). EAP (*Extensible Authentication Protonol* – RFC 3748) stanowi uniwersalny protokół pozwalający na przesył danych uwierzytelniających stosowanych w różnych metodach uwierzytelnienia. Wykaz sposobów uwierzytelnienia obsługiwanych przez EAP dostępny jest pod adresem: http://www.iana.org/assignments/eap-numbers. Obejmują

one m.in. takie metody jak MD5 Challenge, hasła jednorazowe, EAP-TLS, PEAP, EAP-MSCHAP-v2.

Celem ćwiczenia jest praktyczne poznanie możliwości oraz sposobu konfiguracji protokołu 802.1x w lokalnej sieci Ethernet.

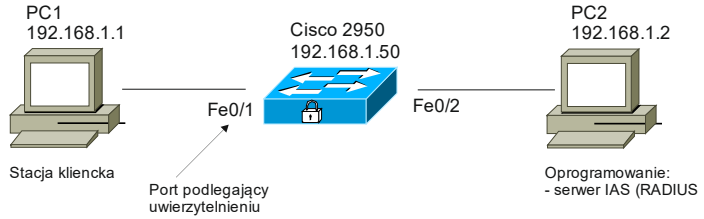
2. Przygotowanie do zajęć

Przed przystąpieniem do wykonywania ćwiczenia należy zapoznać się z następującymi materiałami:

- Całość niniejszej instrukcji.
- Rozdział "*Configuring 802.1X Port-Based Authentication*" z dokumentu „*Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide*" (do pobrania z serwera laboratoryjnego oraz z witryny www.cisco.com.
- Dokumentacja usługi IAS w systemie Windows 2003 Server.

3. Plan wykonywania ćwiczenia laboratoryjnego

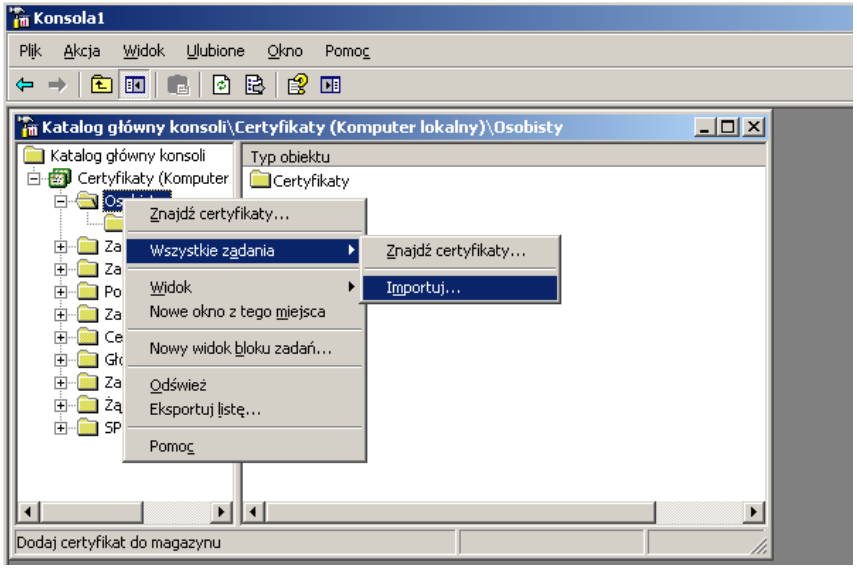
1. Zestawić i skonfigurować układ sieciowy przedstawiony na poniższym rysunku.



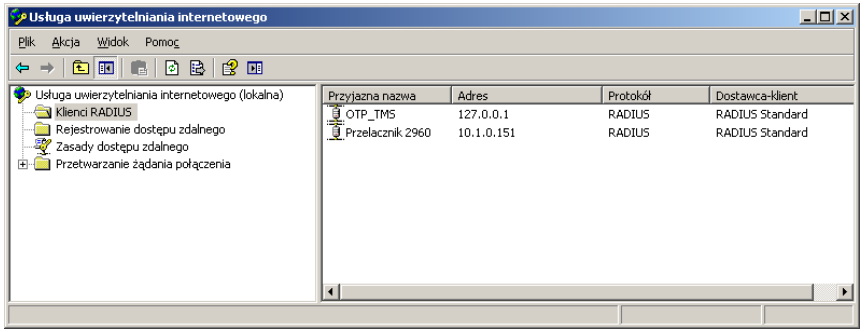
2. Sprawdzić poprawność komunikacji pomiędzy poszczególnymi elementami zestawionego układu (np. poprzez wykonanie testu ping).
3. Skonfigurować w przełączniku Cisco 2950 uwierzytelnianie na porcie Fe0/1. W tym celu należy wykonać następujące operacje:
   a. Włączenie usług AAA:
   `C2950(config)# aaa New-model`
   b. Globalne włączenie uwierzytelniania 802.1x:
   `C2950(config)# dot1x system-auth-control`
   c. Ustawienie uwierzytelniania 802.1x z wykorzystaniem serwera RADIUS:
   `C2950(config)# aaa authentication dot1x default group radius`
   d. Konfiguracja adresu serwera RADIUS oraz klucza komunikacji z tym serwerem:
   `C2950(config)# radius-server host 192.168.1.2 key klucz`
   e. Włączenie uwierzytelniania 802.1x na porcie FastEthernet 0/1:


```
C2950(config-if)# switchport mode access
C2950(config-if)# dot1x port-control auto
```

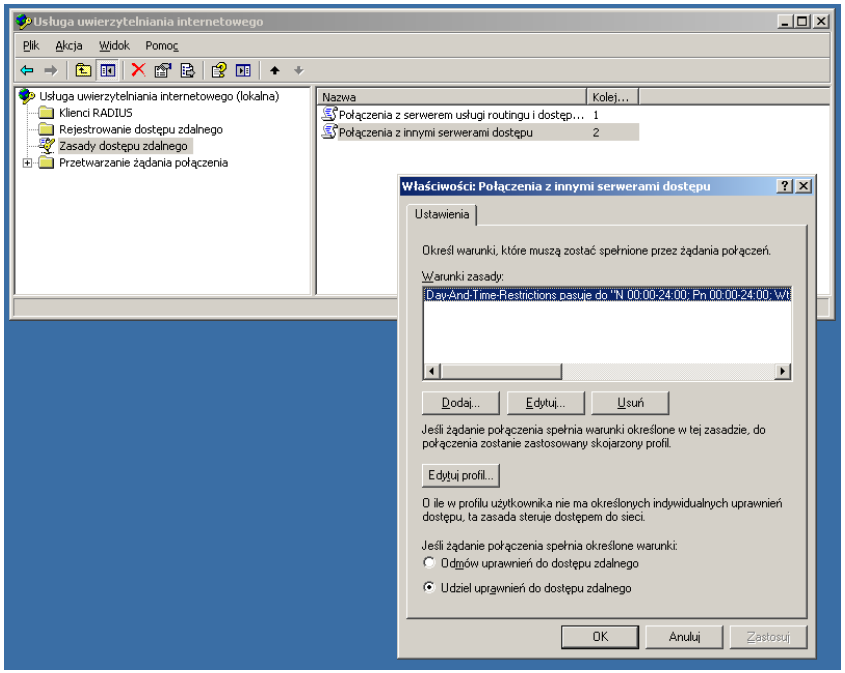
4. Skonfigurować w serwerze RADIUS (usługa IAS) na stacji PC2 współpracę z przełącznikiem Cisco 2950 oraz obsługę uwierzytelniania metodą EAP-MSCHAP v2. W tym celu należy wykonać następujące operacje:
   a. Dodać do magazynu certyfikatów na stacji PC2 (posługując się przystawką *Certyfikaty* **dla konta komputera** w konsoli mmc) certyfikat centrum wystawcy certyfikatów (plik *Cert_CA.cer*, miejsce umieszczenia: Zaufane główne urzędy certyfikacji) oraz certyfikat własny stacji (plik *Cert_RADIUS.pfx,* hasło 1234, miejsce umieszczenia: Osobisty). Certyfikaty te są niezbędne ze względu na to, że zastosowany rodzaj protokołu EAP (PEAP) zabezpiecza kanał komunikacji uwierzytelniającej wykorzystując do tego certyfikat serwera RADIUS.

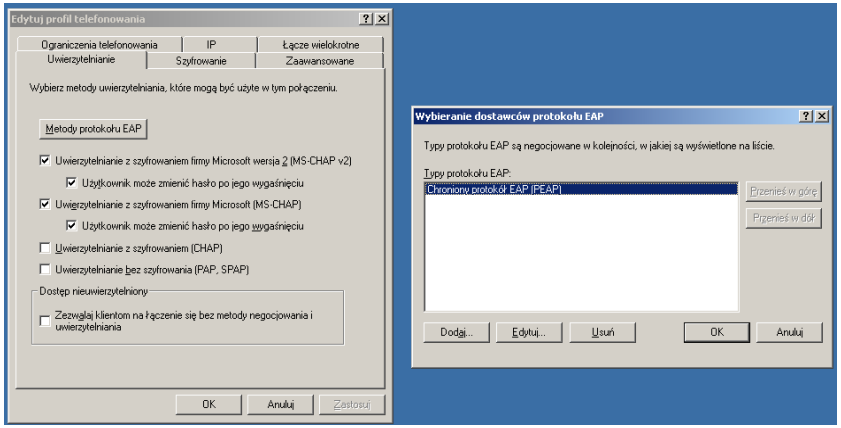


   b. W konsoli zarządzania usługą uwierzytelniania internetowego (IAS) dodać przełącznik Cisco 2950 jako klienta usługi RADIUS. Podany w tym miejscu klucz powinien być identyczny z kluczem skonfigurowanym w przełączniku.



c. W gałęzi „Zasady dostępu zdalnego” dla zasady „Połączenia z innymi serwerami dostępu” ustawić opcję „Udziel uprawnień do dostępu zdalnego” oraz w profilu tej zasady wybrać PEAP jako typ protokołu EAP oraz MS CHAP v2 jako metodę uwierzytelniania.





5. W stacji PC1 włączyć na interfejsie Ethernet uwierzytelnianie 802.1x z protokołem PEAP oraz metodą EAP-MSCHAP v2, **z wyłączonymi** opcjami „*Weryfikuj certyfikat serwera*” oraz „*Użyj mojej nazwy w systemie Windows do zalogowania*”. Po pojawieniu się okienka logowania podać dane uwierzytelniające użytkownika znajdującego się w bazie użytkowników na stacji PC2 (serwerze RADIUS). Supplicant zawarty w systemie Windows 2003 Server domyślnie zapamiętuje dane wprowadzone przy logowaniu 802.1x i automatycznie używa ich przy następnym uwierzytelnieniu. Aby mieć możliwość ponownego wprowadzenia tych danych należy usunąć z rejestru systemu następujący klucz: HKEY_CURRENT_USER\Software\Microsoft\EAPOL\UserEAPInfo
   Aby usprawnić ćwiczenie na pulpicie stacji PC1 przygotowano plik *Kasowanie 802.1x.reg* umożliwiający automatyczne wykonanie tej operacji.
6. Sprawdzić stan uwierzytelnienia na przełączniku:
   `C2950# show dot1x interface FastEthernet 0/1`
7. W logach stacji PC2 (usługa dziennika zdarzeń) odszukać i przeanalizować komunikaty związane z uwierzytelnieniem stacji PC1.
8. Przy użyciu analizatora protokołów (np. *Wireshark*) zarejestrować ramki EAP wysyłane przez stację PC1 do przełącznika oraz komunikację pomiędzy przełącznikiem a serwerem RADIUS.
9. W ustawieniach uwierzytelniania 802.1x na stacji PC1 włączyć opcję „*Weryfikuj certyfikat serwera*” i ponownie wykonać próbę uwierzytelnienia. Ze względu na brak na stacji PC1 certyfikatu centrum CA, które wystawiło certyfikat którym próbował uwierzytelnić się serwer RADIUS certyfikat ten nie mógł być poprawnie zweryfikowany i uwierzytelnienie kończy się niepowodzeniem. W celu usunięcia tego problemu w magazynie certyfikatów aktualnego użytkownika na stacji PC1 należy dodać w grupie „Zaufane główne urzędy certyfikacji” certyfikat właściwego centrum CA (plik *C:\Cert_CA.cer*) i ponownie wykonać próbę uwierzytelnienia.

W sprawozdaniu należy zamieścić wyniki uzyskane przy wykonywaniu poszczególnych części ćwiczenia wraz z danymi zarejestrowanymi analizatorem protokołów oraz odczytanymi z logów serwera RADIUS.

4. Wymagania BHP

Zgodnie z podanymi na pierwszych zajęciach i potwierdzonymi przez studentów zasadami obowiązującymi w pomieszczeniu, w którym odbywają się ćwiczenia. Stosowny regulamin BHP jest też wywieszony w laboratorium.

5. Literatura

1. Józefiok A.: Security CCNA 210-260. Zostań administratorem sieci komputerowych Cisco. Helion, Gliwice 2016.
2. Bragg R.: Bezpieczeństwo w Windows Server 2003. Kompendium. Helion, Gliwice 2006.
3. Ruston N., Peiris C., Hunter L.: Windows Server 2003. Bezpieczeństwo sieci. Helion, Gliwice 2007.
4. Szeliga M.: Bezpieczeństwo w sieciach Windows. Helion, Gliwice 2003.
5. Dokumentacja techniczna *Cisco* dotycząca przełącznika Catalyst 2950 (dostępna w laboratorium oaz w witrynie *www.cisco.com*).