PRACA MAGISTERSKA

ANALIZA MOŻLIWOŚCI ZASTOSOWANIA KONTROLI DOSTĘPU DO SIECI W OPARCIU O STANDARD IEEE 802.1X

Autor: Marek Skrobowski
Praca magisterska wykonana pod opieką:
dr inż. Dariusz Chaładyniak

WARSZAWSKA
WYŻSZA SZKOŁA
INFORMATYKI

Cele pracy magisterskiej

- Przedstawienie mechanizmów funkcjonowania protokołu 802.1X.
- Prezentacja możliwości jakie daje kontrola dostępu do sieci na przykładowym projekcie.

Warszawska Wyższa Szkoła Informatyki

Zakres pracy

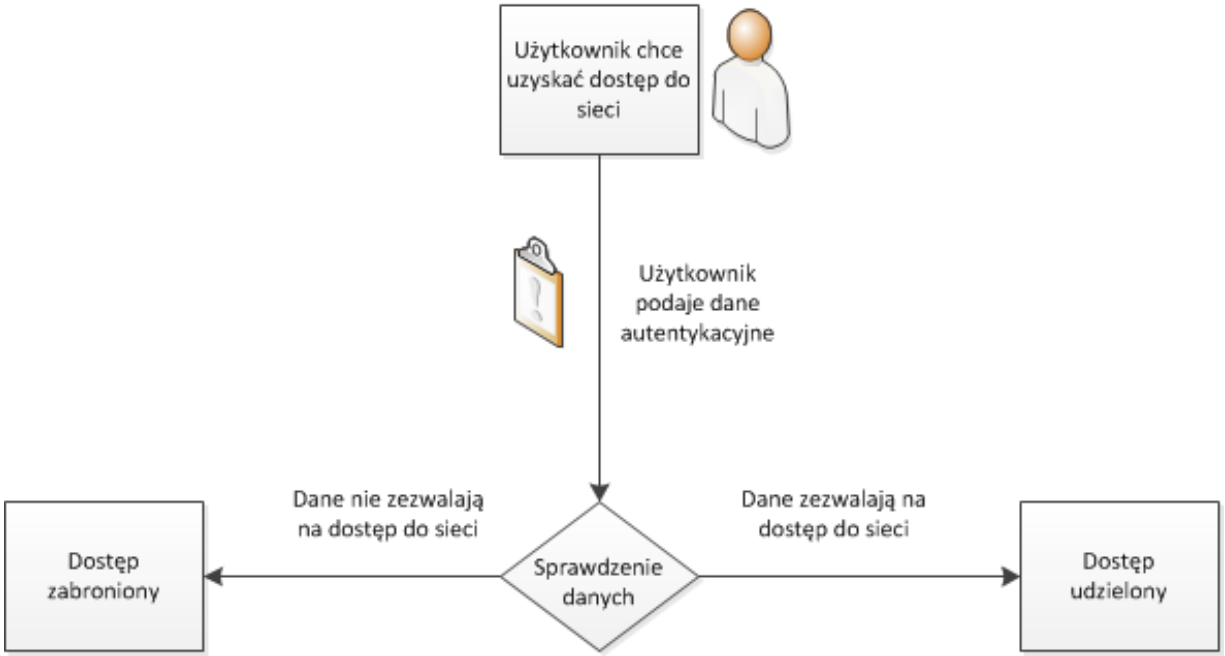
- Przedstawienie elementów funkcjonalnych systemu uwierzytelnienia opartego na portach.
- Charakterystyka 802.1X, wykorzystanych protokołów i standardów niezbędnych do realizacji kompleksowego uwierzytelnienia:
    - IEEE – EAPOL
    - IETF – EAP, EAP-Methods oraz RADIUS.

Dwie części pracy magisterskiej

1. Mechanizmy funkcjonowania protokołu 802.1X.
2. Projekt wdrożenia systemu uwierzytelnienia opartego na portach.

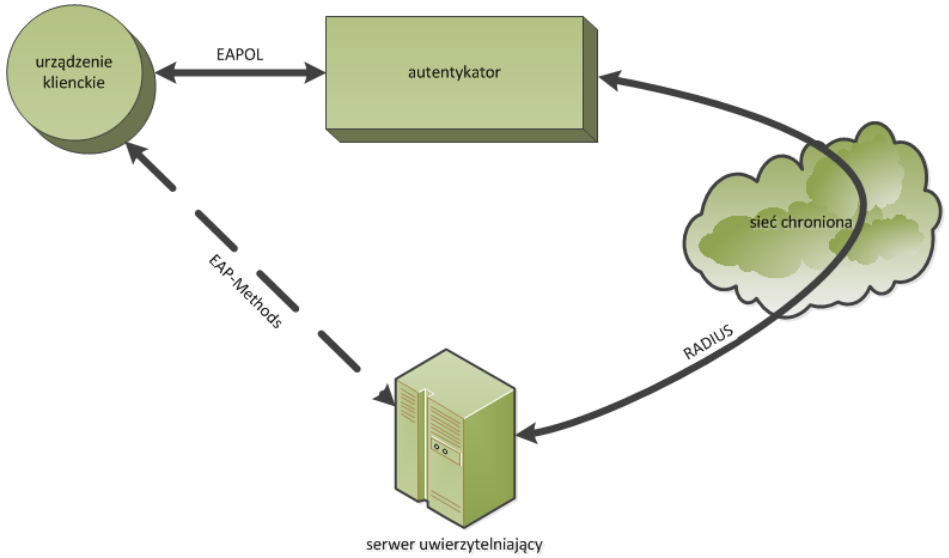
Warszawska Wyższa Szkoła Informatyki

Idea działania standardu 802.1X



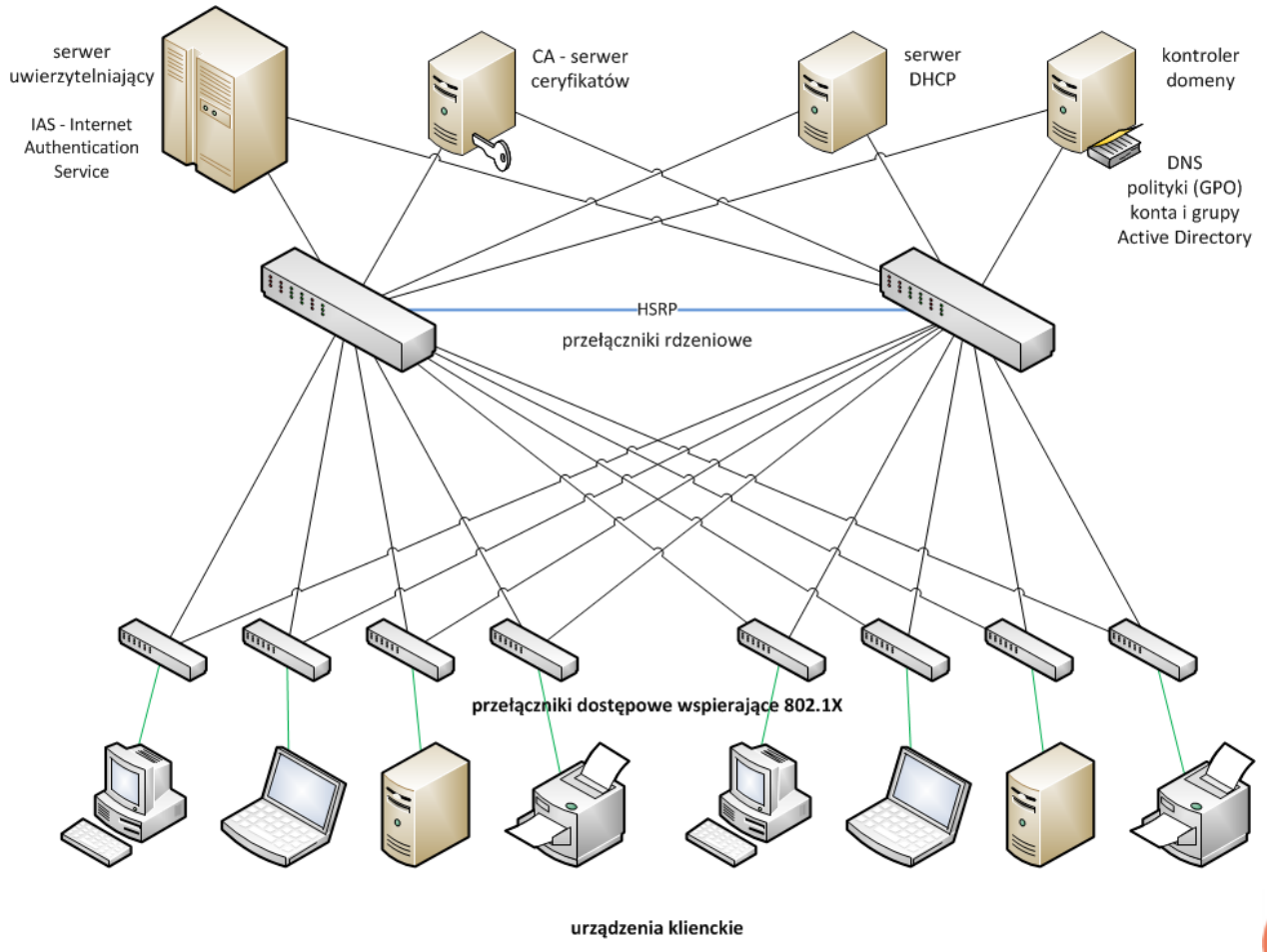
Warszawska Wyższa Szkoła Informatyki

Uwierzytelnianie oparte na portach



- **Uwierzytelnianie** – proces identyfikacji osoby lub rzeczy
- **Port** – “port” urządzenia warstwy drugiej

Schemat infrastruktury



Warszawska Wyższa Szkoła Informatyki

Platforma serwerowa Windows Server 2003

- usługa katalogowa AD
- usługa DNS
- obiekty zasad grupy GPO
- urząd certyfikacji CA
- usługa DHCP
- usługa uwierzytelniania internetowego IAS

Warszawska Wyższa Szkoła Informatyki

INFRASTRUKTURA SIECIOWA

Infrastruktura sieciowa składa się z przełączników zgodnych ze standardem IEEE 802.1X zapewniających autentykowany dostęp do sieci.

WARSZAWSKA
WYŻSZA SZKOŁA
INFORMATYKI

KLIENCI 802.1X

Stacje robocze z systemem Microsoft Windows7 umożliwiające konfigurację protokołu 802.1X.

WARSZAWSKA
WYŻSZA SZKOŁA
INFORMATYKI

Wady i zalety stosowania 802.1X

Warszawska Wyższa Szkoła Informatyki

Wady stosowania 802.1X

- Starsze urządzenia bez wsparcia dla 802.1X.
- Brak wsparcia dla prostych przełączników stosowanych do rozszerzania sieci.
- Problemy występujące przy “wychodzeniu” ze stanu hibernacji w systemach Microsoft Windows.

Zalety stosowania 802.1X

- Eliminacja nieautoryzowanego dostępu do sieci.
- Dynamiczne VLAN'y – zmniejszenie pracy administracyjnej.
- Wsparcie przez większość producentów sprzętu sieciowego oraz producentów oprogramowania systemowego.
- Zastosowanie otwartej architektury bezpieczeństwa.
- Praca niezależna od medium - sieci Ethernet jak i WiFi.
- Scentralizowana identyfikacja użytkowników i jednorodne uwierzytelnianie.

Wnioski i wyzwania na przyszłość

- Standard 802.1X zapewnia uwierzytelnienie na warstwie drugiej, co pozwala na utrzymanie klienta przed połączeniem z siecią do czasu uwierzytelnienia.
- Uwierzytelnienie na warstwie czwartej wymusza zestawienie połączenia do sieci przed rozpoczęciem faktycznego procesu uwierzytelnienia.
- 802.1X nie rozwiązuje wszystkich problemów związanych z bezpiecznym dostępem do sieci.

Warszawska Wyższa Szkoła Informatyki

PODSUMOWANIE

Mam nadzieję, że udało mi się zrealizować cel, którym było przedstawienie standardu IEEE 802.1X zarówno od strony teoretycznej jak i praktycznej. Uważam, że przedstawiona analiza pozwoli na lepsze zrozumienie mechanizmów funkcjonowania systemu uwierzytelnienia opartego na portach co wpłynie na zwiększenie poziomu bezpieczeństwa.

WARSZAWSKA
WYŻSZA SZKOŁA
INFORMATYKI

Dziękuję za uwagę!

Warszawska
Wyższa Szkoła
Informatyki