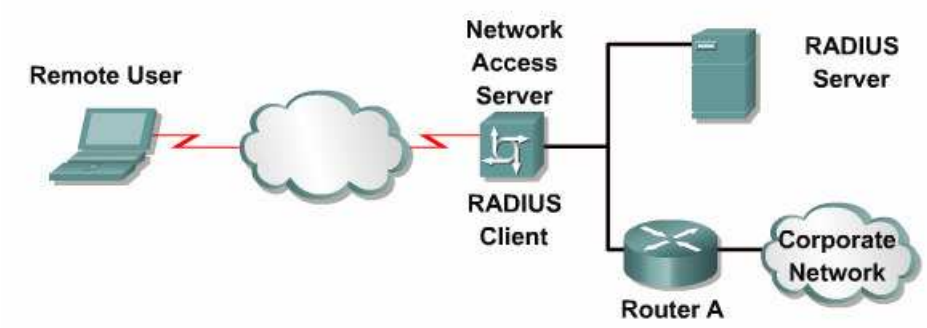
# RADIUS
## Remote Authentication Dial-In User Service

**Informacje ogólne**
**RADIUS** został opracowany przez Livingston Enterprises, Inc. (aktualnie część Lucent Technologies) jako usługa umożliwiająca:
- uwierzytelnianie,
- autoryzowanie,
- rejestrowanie

działań użytkownika (**AAA – 'Authentication, Authorization, Accounting'**). Wykorzystuje **protokół IEEE 802.1x**, zapewniający bezpieczny dostęp do sieci. Na usługę RADIUS składają się trzy podstawowe elementy:
- Protokół korzystający z UDP/IP,
- Serwer obsługujący usługi uwierzytelniania, autoryzacji i rejestrowania,
- Klientów, którzy fizycznie obsługują usługi RADIUS w punktach dostępu do sieci bezpiecznej.

**Architektura i działanie usługi RADIUS**
Przykładowa minimalna implementacja usługi RADIUS wygląda jak na poniższym schemacie[1]:




Klient RADIUS to zwykle urządzenie, przez które przechodzi cały ruch sieciowy:
- Punkt dostępowy sieci bezprzewodowej (Access Point),
- Serwer dostępu wdzwanianego ('dial-in server'),
- Router dostępowy,
- Switch (przełącznik sieciowy).

Klient wysyła do serwera RADIUS wiadomość zawierającą niezbędne parametry uwierzytelniające (w specyficznym formacie), który uwierzytelnia zapytanie klienta oraz przekazuje wiadomość zwrotną. Klient wysyła do serwera także wiadomości konieczne do zliczania ruchu.

Komunikaty RADIUS są przesyłane z użyciem protokołu **UDP ('User Datagram Protocol')** poprzez porty:
- 1812 - do przesyłania wiadomości uwierzytelniających,
- 1813 - do przesyłania wiadomości zliczających ruch.

[1] Rycina zaczerpnięta z Internetu.

W nagłówku pojedynczego pakietu UDP jest przesyłana tylko jedna wiadomość RADIUS. Każdy atrybut nagłówka definiuje fragment informacji, zawartej w żądaniu połączenia:

- nazwę użytkownika,
- hasło użytkownika,
- adres IP serwera dostępowego.

Atrybuty komunikatów RADIUS są opisane przez normy RFC: 2865, 2866, 2867, 2868, 2969, 3162. Warto pamiętać, że bezpieczeństwo wiadomości RADIUS (przesyłanych między klientami i serwerem) jest chronione hasłem dostępu do serwera.

**Protokoły autentykacji i szyfrowania, wspierane przez implementacje RADIUS**

1. **EAP ('Extensible Authentication Protocol')** - pozwala na przekazywanie danych uwierzytelniających między serwerem RADIUS oraz **klientem (NAS)**. Jego obecność sygnalizuje pojawienie się w pakiecie PPP wartości C227hex w trzecim bajcie. Protokół EAP ma kilka wariantów, różniących się poziomem bezpieczeństwa:
    a. **EAP MD5** - opiera się na hasłach szyfrowanych funkcją MD5. Jest podatny na ataki MITM i dlatego nie jest zalecany w dużych środowiskach sieciowych.
    b. **EAP TLS** - opiera się na certyfikatach, zapewnia uwierzytelnianie dwustronne serwera RADIUS oraz NAS. Wymaga implementacji i utrzymywania infrastruktury PKI (ważne certyfikaty dla serwera i klienta). Starszy sprzęt może go zatem nie wspierać.
    c. **EAP TTLS** - podobnie jak **EAP TLS** opiera się na certyfikatach i zapewnia dwustronne uwierzytelnianie RADIUS-a i NAS-a. Znacznie prostszy w implementacji i utrzymaniu, gdyż wymaga wyłącznie certyfikatu po stronie serwera (zatem dobrze współpracuje ze starszym sprzętem). Po stronie klienta stosowane jest hasło szyfrowane protokołem **TLS**. Możliwe jest też wykorzystanie wielu innych typów uwierzytelniania, m.in.: CHAP, MS-CHAPv2.
    d. **LEAP ('Lightweight EAP')** - zmodyfikowana przez CISCO wersja **EAP** zbliżona do **MS-CHAP**. Wykorzystuje algorytmy **MD4** i **DES**, zapewnia dwustronne uwierzytelnienie oparte na hasłach. Z uwagi na liczne podatności na ataki nie rekomendowany do stosowania w złożonych środowiskach sieciowych. Nowszą i bezpieczniejszą wersją **LEAP** jest protokół **EAP-FAST**.
    e. **PEAP ('Protected EAP')** – wykorzystuje certyfikat podczas uwierzytelniania serwera **(EAP-TLS)** oraz hasło przy uwierzytelnianiu klienta. Pierwotnie miał być protokołem wspólnie wykorzystywanym przez wiodących producentów sprzętu i oprogramowania lecz jego twórcy (głównie CISCO i MS) nie zaimplementowały go spójnie: **PEAP** w wersji MS wykorzystuje **MSCHAPv2**.
    f. **MS-CHAPv2** – protokół koncepcyjnie podobny do **EAP-MD5**. Algorytm **MD5** został tutaj zastąpiony słabszym narzędziem - **MD4**.

2. **CHAP ('Challenge Handshake Authentication Protocol')** - oparty na mechanizmach **'Challenge Response'**. W procesie uwierzytelniania użytkowników wykorzystuje algorytm **MD5** do wykonania funkcji skrótu hasła, którą przesyła zamiast hasła. **CHAP**, obok **PAP**, to sposób uwierzytelniania stosowany w połączeniach **PPP** (preferowany). Jest bezpiecznym protokołem uwierzytelniania, gdyż zapewnia ochronę przed atakami wykorzystującymi podsłuch transmisji. Zdefiniowany w RFC 1994.

3. **PAP ('Password Authentication Protocol')** - uwierzytelnia użytkowników przesyłając ich hasła otwartym tekstem i dlatego nie jest uważany za protokół bezpieczny.

Spośród wszystkich w/w protokołów najwyższy poziom bezpieczeństwa gwarantuje **EAP-TLS** z uwagi na obustronną implementację **PKI**. Najbardziej znane i rozpowszechnione implementacje usługi RADIUS, to:

- **MS IAS** w systemach serii Windows 2000 Server (i kolejnych wydaniach), który spośród protokołów uwierzytelnienia wspiera wyłącznie **EAP TLS** i **EAP MD5**,
- **FreeRadius** (na licencji GNU), który pozwala wykorzystać niemal wszystkie dostępne protokoły.

**Właściwości RADIUS-a i zbliżonych implementacji**

Wydaje się, że największe możliwości konfiguracji posiada darmowa implementacja **FreeRadius**, gdyż wspiera ona niemal wszystkie metody uwierzytelnienia. Natomiast komercyjny **MS IAS** może uchodzić za łatwiejszy w konfiguracji i prostszy, oferuje też mniejszą liczbę protokołów, w tym najbezpieczniejszy **EAP/TLS**. Dodatkowo usługa **IAS** dobrze integruje się ze środowiskiem MS.

Alternatywną dla RADIUS-a metodę kontroli dostępu (na poziomie II warstwy modelu ISO/OSI) dla systemów otwartych stanowią rozwiązania wykorzystujące protokół **KERBEROS** w połączeniu z **LDAP**. **KERBEROS**, opracowany przez **MIT** (ang. **'Massachusetts Institute of Technology'**) w połączeniu z usługami katalogowymi umożliwia przeprowadzenie uwierzytelnienia i kontroli uprawnień w sieci lokalnej. Użytkownik po zalogowaniu z użyciem hasła otrzymuje na czas trwania sesji unikalny klucz (ang. **'ticket'**) za pomocą którego może uzyskać dostęp do innych usług w sieci bez konieczności dodatkowego logowania (w wykonaniu użytkownika). Każda sieć powinna posiadać wydzielony serwer **KERBEROS**, zwany **KDC** (ang. **'Key Distibution Center'**). Zadaniem takiego **KDC** jest zarządzanie centralną bazą kluczy:

- wydawanie nowych kluczy,
- odpowiadanie na zapytania dotyczące ich autentyczności.

Protokół **KERBEROS** może także służyć do uwierzytelniania żądań logowania do usługi **AD** (ang. **'Active Directory'**) w systemach z serii MS Windows 2003 Server (i nowszych ich implementacjach).

Protokół **KERBEROS** dobrze sprawdza się w sieciach rozproszonych, w których połączenie jest realizowane w niezabezpieczonym (otwartym) środowisku sieciowym. Tymczasem **RADIUS** jest dedykowanych do sieci wewnętrznych (lokalnych), zawierających lokalną bazę danych o uprawnionych użytkownikach.

**Bezpieczeństwo systemu RADIUS**

Implementacje usługi RADIUS nie są wolne od wad – poszczególne implementacje posiadają wady i błędy logiczne, pozwalające na ataki, w tym m.in.:

- Atak hasło-użytkownik, umożliwiający zmodyfikowanie pakietu **'access request'** na podstawie odpowiedzi otrzymanej po poprzedniej nieudanej próbie, zawierającej wartość **MD5** z sumy współdzielonego klucza (**'shared secret'**) oraz klucza wygenerowanego przez serwer RADIUS (**'request authenticator'**),
- Prosty atak typu **'brute force'**, który może okazać się skuteczny jeżeli w systemie nie zapewniono limitów nieskutecznego logowania (np. 3 próby logowania a następne 5 minut karencji),
- Metody ataków wykorzystujące przewidywalność działania algorytmu **MD5** oraz ochroną hasła względnie prostym szyfrem strumieniowym **RC4**,
- Bardziej złożone ataki z użyciem techniki **MITM (ang. 'Man in the Middle')**, wymagające włączenia do sieci fałszywego serwera RADIUS celem przechwytywania listy pakietów **'request authenticator'**, na podstawie których można:
    - spreparować fałszywe pakiety **'access reject'**,
    - użyć ich do ataku **DoS** na autentyczny serwer RADIUS,

- po jego wyłączeniu lub restarcie dokonać próby wejścia do sieci z użyciem nieuczciwie pozyskanych informacji.

**Interesujące wiadomości uzupełniające i powiązane:**

- http://www.idg.pl/news/92709/Jak.uwierzytelnic.bezprzewodowego.uzytkownika.html
- http://bezpieczenstwo.idg.pl/news/126462/Bezpieczny.Radius.html
- http://serwery.computerworld.pl/artykuly/47973_2/Ochrona.w.tandemie.html
- http://www.komputerwfirmie.pl/itbiznes/1,54788,5988530,Zabezpiecz_siec_firmowa.html
- http://technet.microsoft.com/pl-pl/library/cc783708.aspx
- http://stud.wsi.edu.pl/~dratewka/security/zapory.htm
- http://www.microsoft.com/poland/technet/article/art0100_01.mspx
- http://technet.microsoft.com/pl-pl/library/cc739485.aspx
- http://www.ping.win.pl/z_sieci/radius.htm
- http://web.mit.edu/kerberos/
- http://www.xml-dev.com/blog/index.php?action=viewtopic&id=21
- http://www.gnu.org/software/shishi/