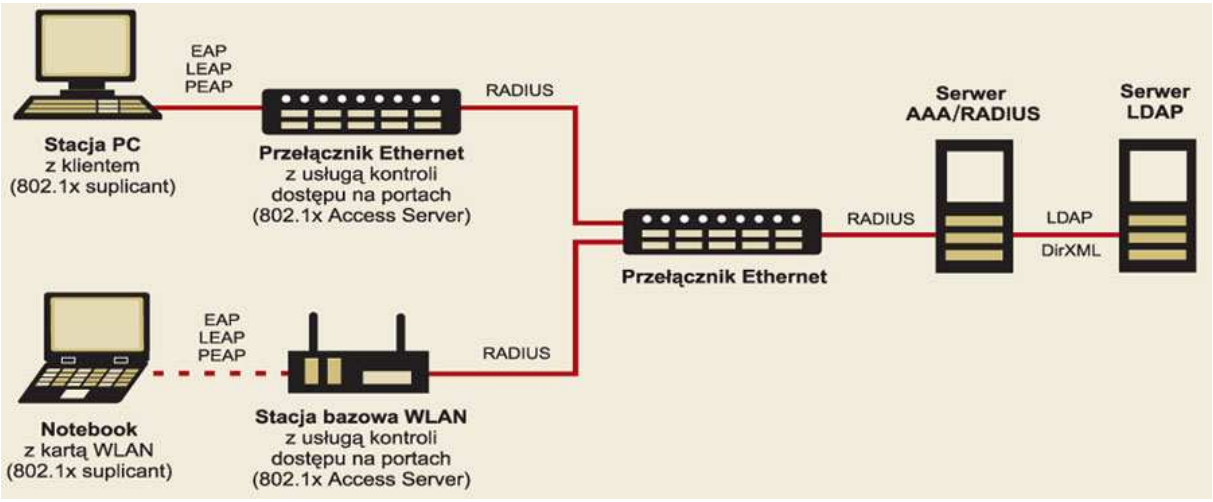
Protokół 802.1x

Protokół 802.1x jest, już od dłuższego czasu, używany jako narzędzie pozwalające na bezpieczne i scentralizowane uwierzytelnianie użytkowników w operatorskich sieciach dostępowych opartych o różnego rodzaju rozwiązania typu Dial-up.
Pozwala on serwerom dostępowym (Network Access Server – NAS) na określenie czy próbujący połączyć się za ich pośrednictwem z siecią użytkownik posiada stosowne uprawnienia oraz na określenie właściwej dla danego użytkownika konfiguracji połączenia (protokół transportowy, jego parametry, adresy IP itp.).

Protokół ten okazał się na tyle niezawodny i elastyczny, że w chwili obecnej może być stosowany w nie tylko w rozwiązaniach typu dial-up, lecz praktycznie we wszystkich najpopularniejszych rodzajach sieci dostępowych:

- łączach pętli abonenckiej opartych na protokole PPP (np. PPP, PPP over Ethernet, PPP over ATM…),
- serwerach VPN,
- sieciach lokalnych typu Ethernet,
- sieciach bezprzewodowych typu WLAN.

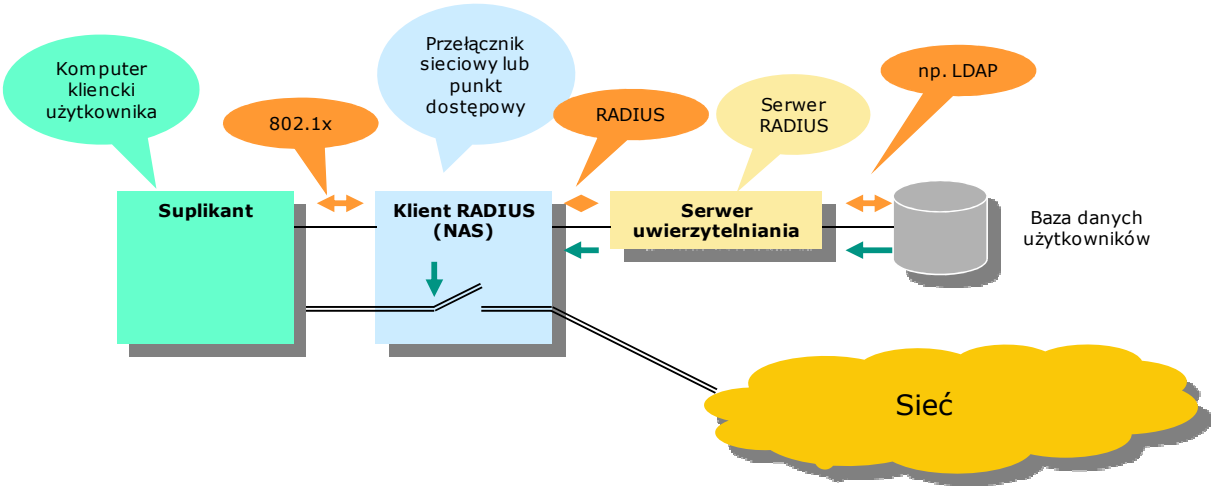
Pozwala on zatem na stworzenie jednolitej struktury mechanizmów uwierzytelniania w złożonej sieci komputerowej, obejmującej zarówno klasyczne sieci LAN, sieci bezprzewodowe WLAN, łącza VPN czy dostępowe łącza abonenckie.



Rys. Przykład wspólnego dla sieci przewodowej i bezprzewodowej systemu uwierzytelniania.

Ogólny sposób pracy 802.1x

Protokół 802.1x używany jest pomiędzy urządzeniem chcącym uzyskać dostęp do sieci (suplikantem), a urządzeniem za którego pośrednictwem powyższy użytkownik/urządzenie będzie do sieci podłączone (klient RADIUS).

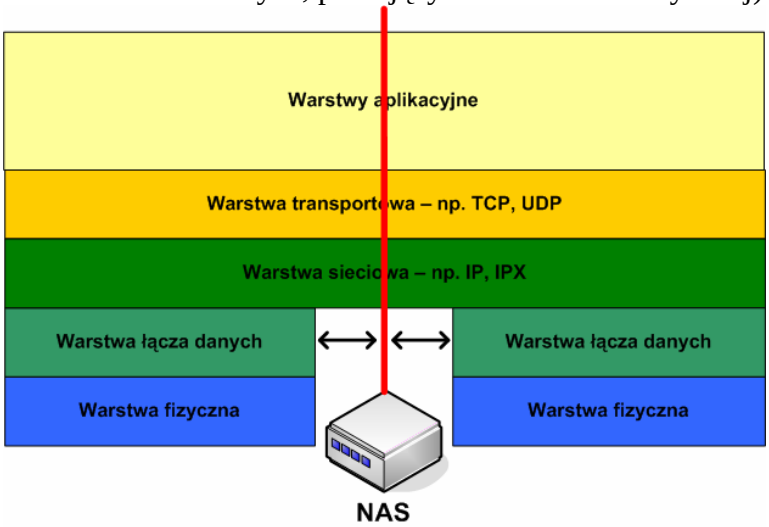


802.1x jest protokołem transportowym, pozwalającym na wymianę informacji uwierzytelniających pomiędzy suplikantem i urządzeniem NAS.
Gdy nowy użytkownik/urządzenie próbuje podłączyć się do sieci, cały ruch od tego urządzenia jest blokowany przez NAS, za wyjątkiem ruchu uwierzytelniającego. Następnie wysyłane jest do podłączającego się żądanie identyfikacji.
Dalsza wymiana informacji zależy od zastosowanych protokołów i metod uwierzytelniania. Urządzenie NAS komunikuje się z serwerem uwierzytelniania (najczęściej jest to serwer RADIUS), który decyduje, czy podłączające się urządzenie można dopuścić do sieci.

Jeśli proces przebiegnie poprawnie NAS odblokowuje ruch od nowego urządzenia do sieci, a także (w przypadku niektórych protokołów uwierzytelniania) może przekazać mu dodatkowe informacje otrzymane od serwera uwierzytelniania, na przykład klucze szyfrujące pozwalające na zabezpieczenie przesyłanego ruchu, czy opcje konfiguracyjne.

Jeśli nowe urządzenie zostanie odrzucone przez serwer, urządzenie pośredniczące NAS wymusza jego całkowite odłączenie od sieci.

Protokół 802.1x pracuje w warstwie 2 modelu ISO-OSI, tak więc bez poprawnego uwierzytelnienia, niemożliwe jest skorzystanie z jakichkolwiek usług sieciowych, czy też (celowe lub przypadkowe) zakłócenie ich pracy. Blokada dostępu w tak niskiej warstwie pozwala na osiągnięcie bardzo wysokiego poziomu bezpieczeństwa: urządzenia typu NAS są w stanie separować wszystkie warstwy od 2 włącznie, a warstwa 1 (fizyczna) jest rozdzielana w przypadku praktycznie każdego z urządzeń sieciowych (za wyjątkiem rzadko już spotykanych koncentratorów sieciowych, pracujących w warstwie fizycznej).



Rys. Separacja dwóch segmentów sieci z użyciem urządzenia NAS.

Protokół 802.1x wymaga co prawda stosowania obsługujących go urządzeń NAS (takich jak przełączniki sieciowe czy punkty dostępowe), a także posiadania na urządzeniach podłączających się do sieci oprogramowania pełniącego funkcję suplikanta, lecz biorąc pod uwagę popularność takich rozwiązań można zakładać gwałtowną popularyzację tego standardu. Obsługuje go w tej chwili znacząca większość sprzedawanych punktów dostępowych WiFi, rosnąca liczba przełączników Ethernet, a system Windows XP SP2 posiada już wbudowaną funkcjonalność suplikanta.

Dzięki możliwości zastosowania nowych protokołów i metod uwierzytelniania, protokół 802.1x jest także atrakcyjny pod względem długookresowej elastyczności. Uniwersalność ta powoduje, iż jest wysoce prawdopodobne, że protokół ten stanie się najpopularniejszym sposobem uwierzytelniania użytkowników w systemach sieciowych.

Kolejną użyteczną cechą protokołu 802.1x jest fakt, iż pracuje on w taki sam sposób niezależnie od konkretnego medium fizycznego, którego używa sieć. Możliwe jest, na przykład, zastosowanie go zarówno w przypadku sieci Ethernet (802.3) jak i WiFi (802.11), a w obu przypadkach będzie on konfigurowany i działał analogicznie.

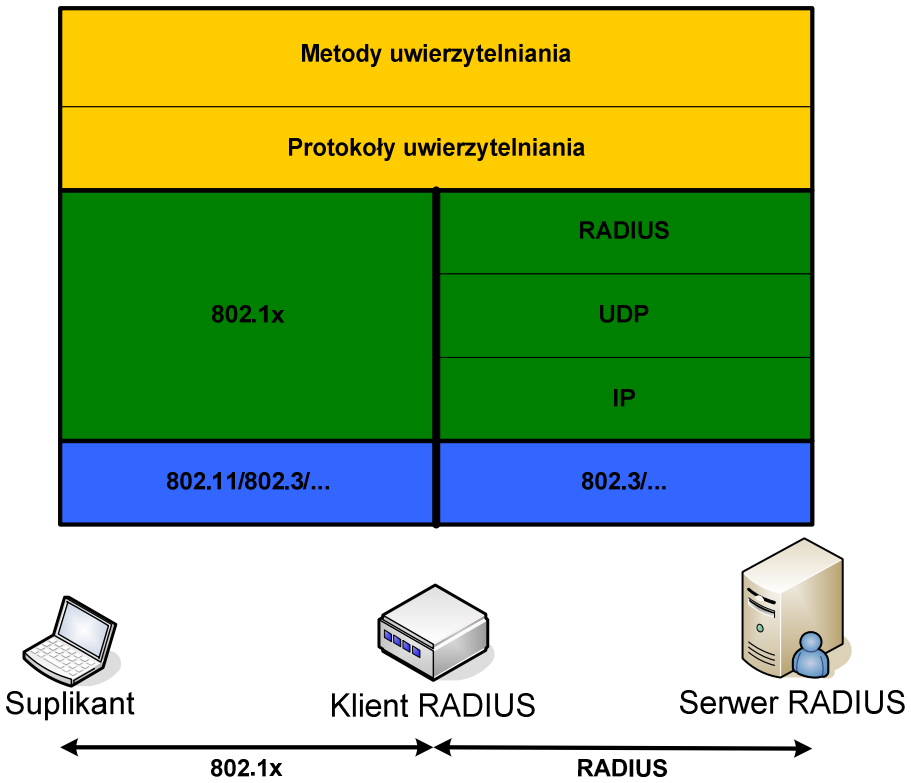
Inną cechą, która decyduje o sukcesie protokołu 802.1x, jest fakt, iż jest to protokół transportowy, pozwalający na użycie wielu protokołów uwierzytelniania, które z kolei mogą wykorzystywać całą gamę metod uwierzytelniania. Protokół 802.1x zapewnia przenoszenie wiadomości generowanych przez te protokoły i metody, dając podstawy do stworzenia bardzo elastycznego i możliwego do praktycznie dowolnej rozbudowy systemu bezpieczeństwa.

Protokół EAP

Jak już wspomniano, protokół 802.1x pozwala na zastosowanie całej gamy protokołów i metod uwierzytelniania. Najpopularniejszym stosowanym protokołem uwierzytelniania jest, w chwili obecnej, Extensible Authentication Protocol (EAP). Stanowi on platformę, która umożliwia obu stronom procesu uwierzytelniania na wymianę wiadomości oraz zawiera mechanizmy pozwalające obu stronom procesu uwierzytelniania na dokonanie wyboru najlepszego, obsługiwanego przez obie strony, sposobu uwierzytelniania.

Protokół EAP przenoszony z użyciem protokołu 802.1x nazywany jest często EAP over LAN (EAPOL), jako że jego komunikaty przenoszone są bezpośrednio przez warstwę 2 sieci – bez użycia dodatkowych protokołów sieciowych (warstwa 3) czy transportowych (warstwa 4), takich jak IP, UDP czy TCP.

Należy pamiętać, że 802.1x, a zatem i EAPOL, stosowany jest pomiędzy suplikantem, a urządzeniem NAS. Komunikacja pomiędzy NAS a serwerem uwierzytelniania odbywa się już z pomocą protokołu RADIUS (a w przypadku stosowania protokołu EAP – EAP over RADIUS), opartego na protokole UDP.

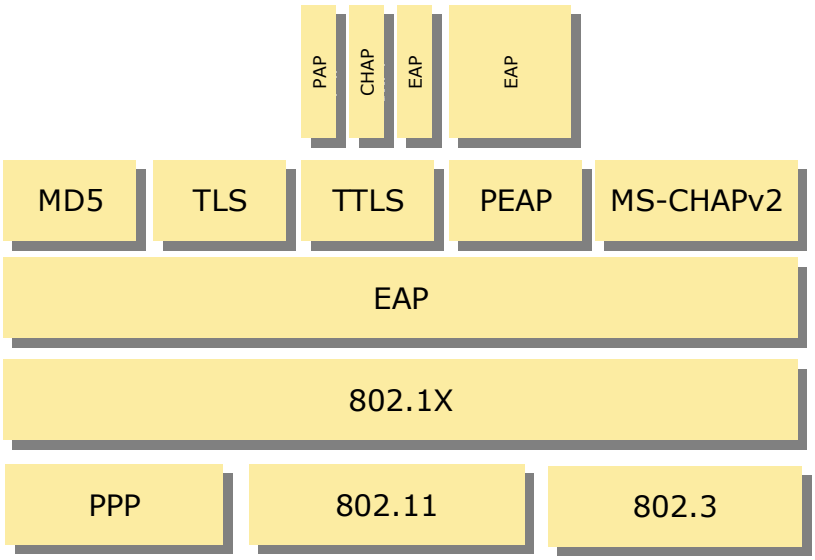


Rys. Model warstwowy protokołów uwierzytelniania na odcinkach suplikant-klient i klient-serwer.

Protokół EAP może występować w kilku odmianach, z których najczęściej spotykane to:

- EAP – podstawowa wersja protokołu. Metody uwierzytelniania takie jak MD5 MS_CHAPv2 itp. wymieniają wiadomości bezpośrednio, korzystając z platformy komunikacyjnej udostępnionej przez protokół EAP.
- Lightweight EAP (LEAP) – opracowana przez Cisco wersja EAP z wzajemnym uwierzytelnianiem przez funkcje skrótów z długimi kluczami;

- EAP-TTLS – na platformie komunikacyjnej udostępnianej przez protokół EAP, zestawiany jest szyfrowany tunel TLS pomiędzy suplikantem i NAS. Metody uwierzytelniania wymieniają dane korzystając z tego tunelu.
- PEAP (Protected EAP) – podobnie jak w TTLS, ale w zestawionym tunelu TLS uruchamiana jest kolejna warstwa protokołu EAP i to z jej pomocą komunikują się metody uwierzytelniania.



Rys. Przykładowe metody uwierzytelnia dostępne z użyciem protokołu EAPOL (EAP over LAN).

Dwa ostatnie warianty protokołu umożliwiają nie tylko uwierzytelnianie podłączającego się suplikanta, lecz również pozwalają mu na sprawdzenie tożsamości serwera uwierzytelniającego, zanim zostaną do niego wysłane poufne informacje.
W ten sposób podłączające się urządzenie ma pewność, że podaje swoje dane właściwemu serwerowi, a nie, na przykład, fałszywemu – podstawionemu przez atakującego system aby poznać hasła użytkowników. Inaczej mówiąc, takie wzajemne uwierzytelnienie, pozwala na obronę przed atakiem typu Man-in-the-Middle.

Z użyciem powyższych protokołów, można wykorzystać szeroką gamę metod uwierzytelniania, czyli mechanizmów które są w stanie potwierdzić tożsamość użytkownika różnymi sposobami.

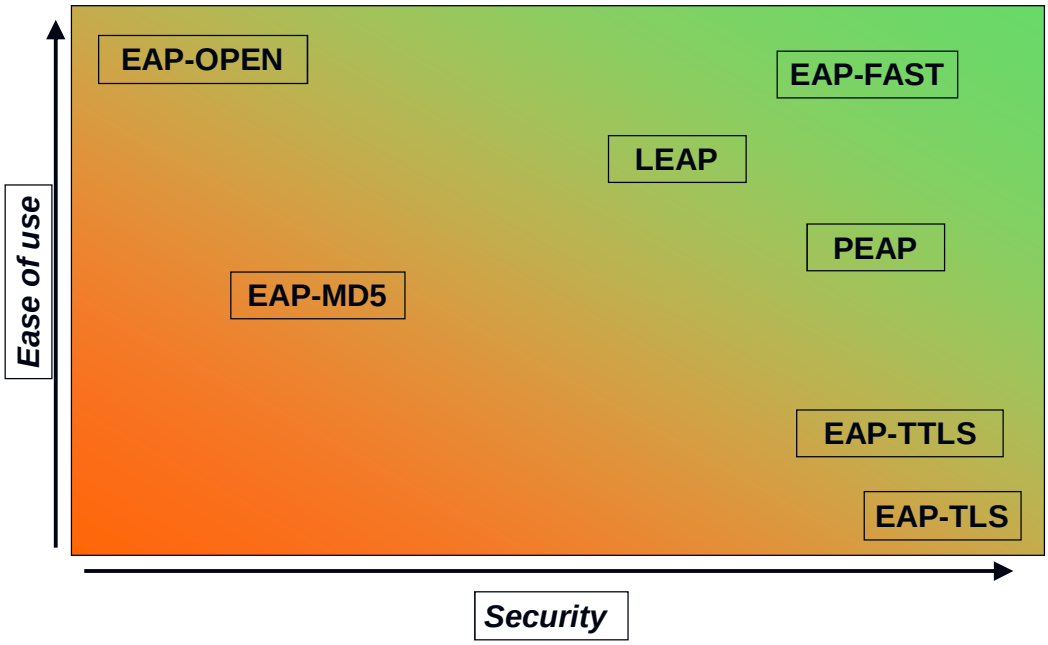
- MD5 - nazwa użytkownika i hasło szyfrowane funkcją skrótu MD5; nadaje się głównie do środowisk przewodowych - w warunkach sieci WLAN jest zbyt podatny na podsłuch i łamanie haseł offline oraz ataki typu man-in-the-middle.
- TLS - metoda oparta na certyfikatach klientów i tunelowaniu TLS/SSL; daje wystarczający poziom bezpieczeństwa w sieciach WLAN i jest powszechnie wspierana przez producentów urządzeń
- MS-CHAPv2 - technologia opracowana przez Microsoft zbliżona w ogólnych zarysach do MD5, lecz stosująca inną funkcję skrótu - MD4.
- PAP – uwierzytelnianie z użyciem stałych haseł przesyłanych otwartym tekstem,
- OTP (One-time Password) – uwierzytelnianie z użyciem haseł jednorazowych,
- GTC (Generic Token Card) – uwierzytelnianie z użyciem kart chipowych,

Należy zwrócić uwagę, że często spotykamy się z zapisem nazywającym połączenie protokołu i metody po prostu protokołem. Na przykład: protokół EAP / metoda MD5 – „uwierzytelnianie realizowane jest z użyciem protokołu EAP-MD5".

Poglądową listę właściwości wybranych metod i protokołów zamieszczono poniżej.

Method	Credential type	Authentication	Pros:	Cons:
EAP/MD5	• Fixed passwords	Challenge handshake authentication (similar to CHAP)	• Fairly easy to implement and deploy • Well supported	• Weak authentication mechanism • Does not provide mutual authentication
EAP/TLS (Transport Layer Security)	• Certificates	Mutual certificate authentication	• Strong authentication mechanism • Provides mutual authentication • Supports dynamic WEP key generation	• Difficult to implement and deploy • Requires public key infrastructure • Certificates required for both server and all client devices
EAP/TTLS (Tunneled TLS)	• Fixed passwords • One-time pass words (tokens) • Certificates	Sever-side authentication itself using a certificate while the client-side authentication occurs inside an encrypted tunnel	• Strong authentication mechanism • Provides mutual authentication • Supports dynamic WEP key generation	• More difficult to deploy than EAP/MD5 • Limited support in both hardware and software
Protected EAP (PEAP)	•Fixed passwords •One-time pass-words (tokens) •Certificates	Similar to TTLS, except the inner authentication is another EAP method	• Strong authentication mechanism • Provides mutual authentication • Supports dynamic WEP key generation	• Emerging standard
EAP/Cisco (LEAP)	• Fixed passwords	Based around the MS-CHAP and MS-CHAPv2 authentication protocols	• Easy to implement and deploy • Provides mutual authentication • Supports dynamic WEP key generation	• Proprietary standard • Weak authentication mechanism if passwords are poorly chosen

Rys. Przegląd protokołów/metod EAP



Rys. Łatwość zastosowania / bezpieczeństwo oferowane przez poszczególne protokoły/metody EAP

Serwer uwierzytelniający

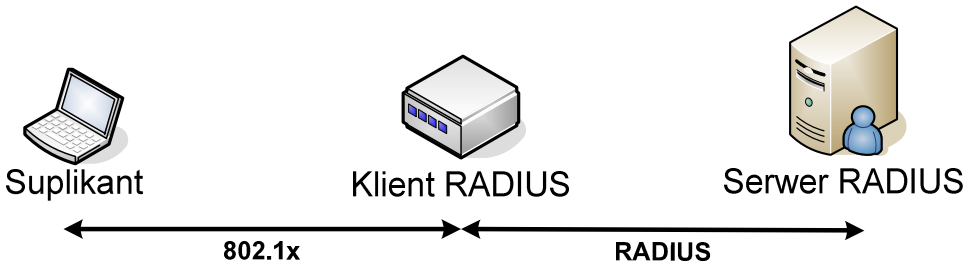
Poza opisanymi już wcześniej elementami systemu kontroli dostępu, tzn. suplikantem oraz NASem, konieczny jest także serwer uwierzytelniający. Jego zadaniem jest komunikacja z NASem, a za jego pośrednictwem także z suplikantem, a następnie:

- potwierdzenie tożsamości tego ostatniego,
- decyzja czy i jaki dostęp mu przyznać,
- określenie opcji konfiguracyjnych, które należy przekazać NASowi i suplikantowi (w rodzaju: typu kompresji, typu szyfrowania, adresów IP, maksymalnej dopuszczalnej wilkości ramki itp.),
- wygenerowanie kluczy szyfrujących,
- przesłanie decyzji o dopuszczeniu lub odrzuceniu podłączającego się urządzenia do NASa i suplikanta,
- przesłanie ustalonych wcześniej lub wygenerowanych opcji konfiguracyjnych i materiału kryptograficznego do NASa i suplikanta.

Najczęściej spotykanym obecnie typem serwera uwierzytelniającego jest serwer RADIUS. W systemie korzystającym z takiego serwera poszczególne jego elementy nazywamy następująco:

- Suplikant – element urządzenia próbującego podłączyć się do sieci, który odpowiedzialny jest za współpracę z mechanizmami bezpieczeństwa systemu w celu jego uwierzytelnienia.
- Klient RADIUS– mechanizmy zawarte w urządzeniu pośredniczącym w podłączaniu się innych do sieci (np. w punkcie dostępowym czy przełączniku Ehternet).
- Serwer RADIUS – serwer uwierzytelniający.

O ile do komunikacji pomiędzy suplikantem i klientem RADIUS wykorzystywany jest protokół 802.1x (a najczęściej jego wersja EAPOL), to do komunikacji pomiędzy klientem i serwerem RADIUS wykorzystywany jest protokół transportowy RADIUS który korzysta z protokołu IP/UDP.



Z jednego serwera uwierzytelniającego może korzystać wielu klientów RADIUS (czyli wiele urządzeń typu NAS), co pozwala na stworzenie scentralizowanego systemu punktu uwierzytelniania.
[rys]

Dodatkową funkcją serwera uwierzytelniającego RADIUS może być zbieranie danych o wykorzystaniu systemu przez użytkowników (np. o czasach połączeń, ilości przesłanych danych itp.). Stąd też tego rodzaju serwery są często nazywane serwerami AAA: Authentication (uwierzytelnianie – potwierdzenie tożsamości), Authorization (autoryzacja – określenie poziomu dostępu do zasobów), Accounting (rozliczanie – zbieranie danych o wykorzystaniu zasobów przez użytkownika).