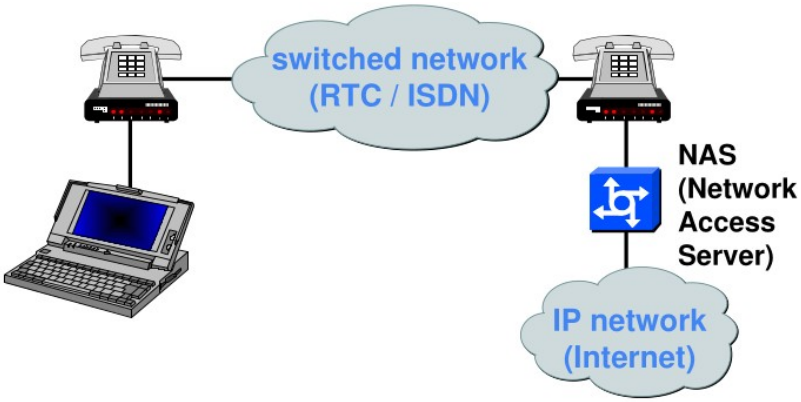
Sicurezza delle reti IP

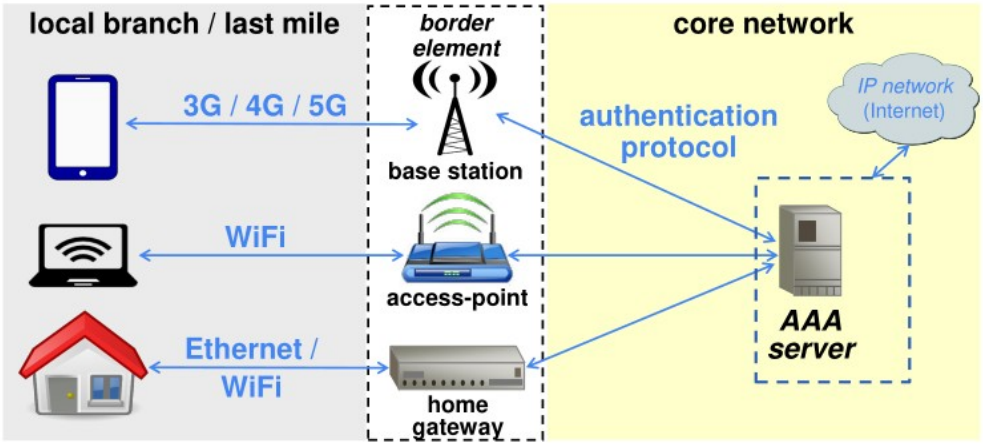
Controllo degli Accessi alle Reti IP



In passato, per controllare l'accesso alle reti IP, specialmente per gli utenti residenziali, venivano utilizzati dispositivi chiamati NAS (Network Access Server). Questi dispositivi avevano il compito di autenticare gli utenti, controllare gli accessi e fornire l'accesso alla rete IP, ad esempio Internet. Questo sistema coinvolgeva l'uso di modem e linee telefoniche. Tuttavia, questo approccio è oggi meno comune nei Paesi occidentali, sebbene alcuni Paesi possano ancora utilizzarlo.

Metodi di Accesso Attuali

Oggi, l'accesso a Internet avviene in vari modi a seconda del dispositivo utilizzato. Ad esempio, gli smartphone utilizzano tecnologie come 3G, 4G o 5G per connettersi alle stazioni base, e si autenticano attraverso un server AAA. Il Wi-Fi può essere utilizzato attraverso gli access point, e i gateway domestici consentono l'accesso a Internet tramite Ethernet o Wi-Fi, richiedendo autenticazione.



- **Access Requester (AR):** È un nodo o dispositivo che cerca di accedere alla rete. Questo può essere qualsiasi dispositivo come computer, server, stampanti, telecamere, telefoni o qualsiasi altro dispositivo con capacità IP. Gli access requester sono talvolta chiamati anche supplicants o clienti.
- **Network Access Server (NAS):** Il NAS funge da punto di controllo dell'accesso per gli utenti che si trovano in posizioni remote. In altre parole, è il dispositivo che si trova alla periferia della rete e gestisce le richieste di accesso provenienti dagli access requester.

    - **Funzioni:**
        - Può includere i propri servizi di autenticazione o fare affidamento su un servizio di autenticazione separato fornito da un server AAA (Authentication, Authorization, and Accounting).
        - Controlla l'accesso alla rete in base alle regole e alle politiche stabilite.
- **AAA Server** (Authentication, Authorization, and Accounting Server): Si tratta di un server che determina quali privilegi di accesso devono essere concessi all'access requester.
    - **Funzioni:**
        - **Autenticazione:** Verifica l'identità dell'access requester attraverso processi come l'utilizzo di credenziali (nome utente e password) o altri metodi di autenticazione.
        - **Autorizzazione:** Decide quali risorse o servizi l'access requester è autorizzato ad utilizzare una volta autenticato. Determina quindi il livello di accesso consentito.
        - **Accounting:** Registra e tiene traccia delle attività dell'utente sulla rete, inclusi dettagli come orari di accesso e risorse utilizzate.
    - **Ricerca di Condizioni/Health dell'AR:** Molto spesso, l'AAA server si basa su sistemi di backend per valutare lo stato o la "condizione" dell'access requester, come ad esempio il suo stato di sicurezza o la presenza di software antivirus aggiornato.

Autenticazione dei Canali PPP

Per trasmettere dati attraverso la rete, è necessario autenticare gli utenti. L'autenticazione inizia quando qualcuno cerca di connettersi, e coinvolge i livelli fisici e logici della trasmissione dati. Il protocollo PPP (Point-to-Point) è spesso utilizzato per incapsulare i pacchetti di rete (livello 3, come IP) e trasportarli su un collegamento PPP fisico o virtuale.

Il PPP può essere implementato su collegamenti fisici, come linee ISDN o reti telefoniche, o su collegamenti virtuali, ad esempio, utilizzando PPPoE (PPP over Ethernet) dal gateway di casa all'ADSL. Inoltre, il PPP è utilizzato per trasportare pacchetti all'interno di connessioni virtualizzate di livello 3 tramite un protocollo chiamato L2TP (Layer 2 Tunnel Protocol), che è incapsulato all'interno di UDP, introducendo così un livello aggiuntivo di sicurezza.

- Il PPP può essere attivato in tre fasi:
    - **LCP** (Link Control Protocol) per stabilire la capacità di trasmettere dati
    - **Autenticazione** (opzionale, con metodi come PAP, CHAP o EAP)
    - **Incapsulamento L3** (ad esempio, IPCP: IP Control Protocol)

Metodi di Autenticazione PPP

Tre metodi principali di autenticazione PPP:

- **PAP (Password Authentication Protocol):** L'utente invia il nome utente e la password in chiaro sul canale PPP. Tuttavia, questo metodo è considerato poco sicuro, poiché se qualcuno intercetta il canale, può acquisire la password.
- **CHAP (Challenge Handshake Authentication Protocol):** Utilizza una challenge response basata sulla password dell'utente. La password non viene inviata direttamente, rendendo difficile la sua intercettazione. Tuttavia, il canale non è completamente protetto.
- **EAP (Extensible Authentication Protocol):** È un protocollo che non specifica un metodo di autenticazione specifico. Il metodo di autenticazione è esterno e può includere challenge response, One-Time Passwords (OTP) o TLS. Attualmente, EAP è il sistema più diffuso per l'autenticazione dell'accesso alla rete, mentre PAP e CHAP sono considerati meno sicuri e meno utilizzati.

In sintesi, l'autenticazione è fondamentale per controllare l'accesso alle reti IP, e i protocolli come PPP forniscono meccanismi per garantire che solo gli utenti autorizzati possano trasmettere dati attraverso la rete.

EAP

Il Protocollo di Autenticazione Estensibile (EAP) è un framework flessibile progettato per il livello 2 (L2) di PPP (Point-to-Point Protocol). La sua funzione principale è fornire un servizio di trasporto generico per lo scambio di informazioni di autenticazione su una rete. Inizialmente, EAP supporta meccanismi di autenticazione predefiniti come MD5-challenge e OTP. Successivamente, sono stati aggiunti altri meccanismi come TLS.

EAP opera su diversi tipi di reti e livelli di collegamento, inclusi collegamenti point-point, LAN e reti wireless. Per garantire la trasmissione sicura di dati di autenticazione, EAP deve creare il suo protocollo di incapsulamento, poiché i pacchetti di livello 3 (L3), come ad esempio quelli basati su IP, non sono ancora disponibili durante l'autenticazione.

Caratteristiche dell'incapsulamento EAP:

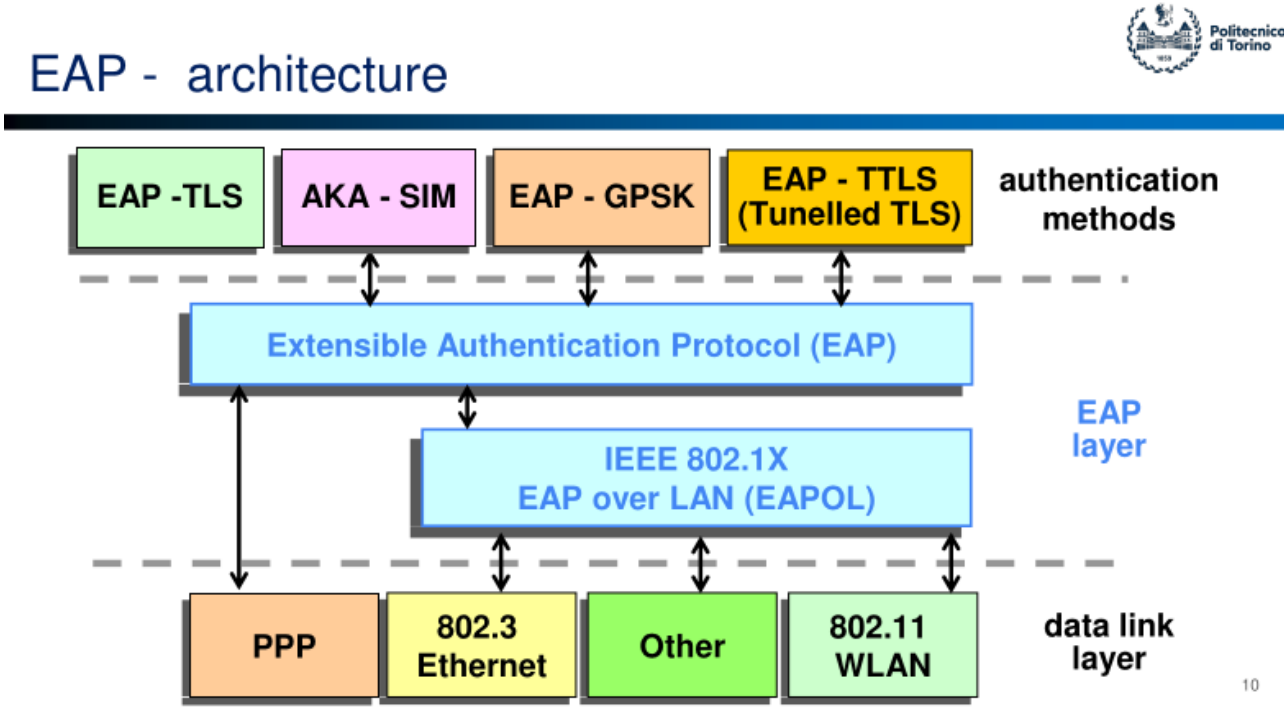
- **Indipendenza da IP:** EAP è progettato per essere indipendente da IP, supportando qualsiasi tipo di livello di collegamento, come PPP, Ethernet (802.3), Token ring (802.5), Wi-Fi (802.11), e altri.
- **ACK/NAK espliciti:** EAP fornisce conferma esplicita o negazione (ACK/NAK) dei pacchetti, ma senza utilizzare il windowing come nel TCP, poiché si presume che i pacchetti non vengano riordinati (anche se questa supposizione potrebbe non essere valida su canali virtuali come UDP e IP grezzo).
- **Ritrasmissione:** La ritrasmissione è prevista, ma con un limite di tentativi, solitamente da 3 a 5, per evitare il fallimento dell'autenticazione in caso di problemi di rete.
- **Nessuna frammentazione:** Non è prevista la frammentazione, ma i metodi EAP devono gestire payload superiori alla MTU minima EAP.

Quando si verifica un problema durante l'autenticazione EAP, potrebbe non indicare un fallimento dell'autenticazione in sé, ma piuttosto un problema di rete. La risoluzione dei problemi potrebbe richiedere l'intervento di un esperto di rete per identificare eventuali cause di fallimento.

In EAP, non si presume che il collegamento sia fisicamente sicuro: ogni metodo di autenticazione deve garantire la sicurezza da solo.

Gli EAP methods includono:

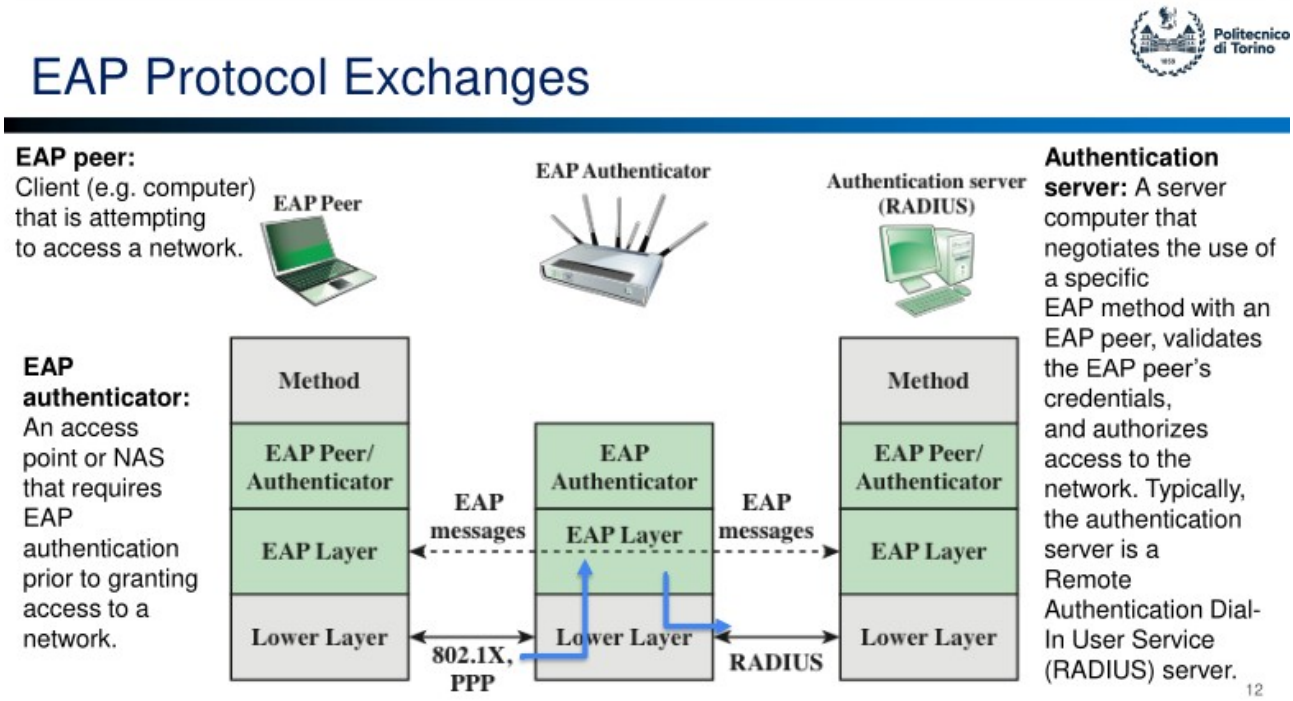
- **EAP-TLS (RFC-5216):** Utilizza il protocollo TLS per la trasmissione sicura dei dati di autenticazione.
- **EAP-TTLS:** Un tunnel TLS che consente l'utilizzo di qualsiasi metodo protetto all'interno di un canale sicuro TLS.
- **EAP-SRP:** Utilizza un sistema di password remota sicura.
- **GSS_API:** Include il protocollo di autenticazione Kerberos.
- **AKA-SIM (RFC-4186, RFC-4187):** Basato sul modulo di identità dell'abbonato, utilizzato nelle reti mobili.



L'architettura generale di EAP coinvolge un peer EAP (cliente), un autenticatore EAP (punto di accesso o NAS) e un server di autenticazione (RADIUS server), che negoziano l'uso di un metodo specifico e autorizzano l'accesso alla rete.

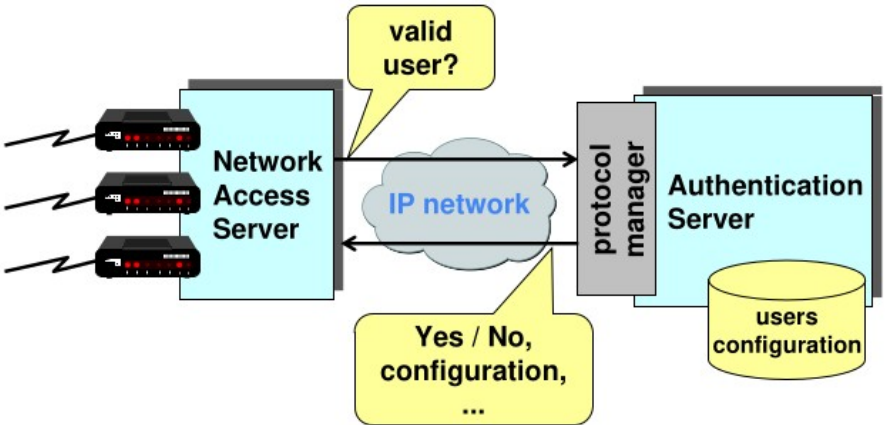
- **EAP Peer:** Un EAP Peer è un client, ad esempio un computer, che sta cercando di accedere a una rete.
  - *Ruolo:* Il suo obiettivo è ottenere l'accesso a una rete e inizia il processo di autenticazione EAP.
- **EAP Authenticator:** Un EAP Authenticator è un punto di accesso o un Network Access Server (NAS) che richiede l'autenticazione EAP prima di concedere l'accesso a una rete.
  - *Ruolo:* Serve da punto di controllo degli accessi e richiede all'EAP Peer di autenticarsi prima di concedere o negare l'accesso alla rete.

- **Authentication Server:** Un Authentication Server è un server che negozia l'uso di uno specifico metodo EAP con un EAP Peer, convalida le credenziali dell'EAP Peer e autorizza l'accesso alla rete.
    - *Ruolo:* Gestisce il processo di autenticazione, confermando l'identità dell'EAP Peer e determinando se concedere o negare l'accesso alla rete. Tipicamente, il server di autenticazione è un server RADIUS (Remote Authentication Dial-In User Service).



Authentication for network access

L'autenticazione per l'accesso alla rete segue un'architettura in cui i collegamenti di comunicazione, come modem, access point o connessioni ADSL/Fibra, terminano in dispositivi ospitati dall'ISP. Questi dispositivi, controllati da un NAS (Network Access Server), ricevono richieste dai client e determinano se l'utente è valido o meno. Il NAS utilizza il protocollo sulla rete IP locale per comunicare con il server di autenticazione centralizzato dell'ISP. Questa struttura è essenziale perché l'ISP ha molteplici punti di presenza con numerosi NAS, tutti condividendo le stesse informazioni sugli utenti.



Il server di autenticazione ha accesso a un database contenente credenziali e configurazioni per ciascun utente in base al contratto stipulato tra l'utente e l'ISP. In risposta alle richieste del NAS, il

server di autenticazione fornisce una risposta (utente valido/invalido) insieme alla configurazione che il NAS deve applicare al traffico dell'utente.

I produttori di NAS enfatizzano che la sicurezza richiede tre funzioni fondamentali, abbreviate come AAA:

- **Authentication:** Verifica dell'identità dell'entità mediante credenziali come password o OTP.
- **Authorization:** Determinazione se un'entità è autorizzata per specifiche attività o per l'accesso a risorse e servizi specifici.
- **Accounting:** Monitoraggio dell'uso delle risorse di rete per scopi di revisione, analisi della capacità o fatturazione dei costi.

Il Server di Autenticazione (SA) svolge queste funzioni interagendo con uno o più NAS attraverso uno o più protocolli.

I protocolli di autenticazione di rete comprendono principalmente tre opzioni:

1. **RADIUS:** Standard de facto e il più ampiamente utilizzato, con la capacità di funzionare come un proxy verso altri sistemi di autenticazione.
2. **DIAMETER:** Un'evoluzione di RADIUS con un focus sul roaming tra diversi ISP e un maggior impegno per la sicurezza.
3. **TACACS+ (TACACS, XTACS):** Originariamente considerato tecnicamente superiore a RADIUS, ha ottenuto una minore accettazione a causa della sua natura proprietaria, implementata solo da Cisco senza specifiche pubbliche.

RADIUS

RADIUS è un protocollo di autenticazione, autorizzazione e accounting utilizzato in molte reti per gestire l'accesso degli utenti. RADIUS opera su un modello client-server, dove un client RADIUS (spesso un dispositivo di rete, come un access point Wi-Fi o un server VPN) comunica con un server RADIUS per gestire le operazioni di autenticazione, autorizzazione e accounting. Il protocollo utilizza una porta UDP (di solito la porta 1812 per l'autenticazione e la porta 1813 per l'accounting).

RADIUS (Remote Authentication Dial-In User Service) è un protocollo sviluppato da Livingston Technologies nel 1991 e successivamente standardizzato dall'IETF. Originariamente concepito per gestire le connessioni Dial-In (quando gli utenti chiamavano un ISP tramite modem), si è evoluto nel tempo supportando authentication, authorization e accountability per controllare l'accesso alla rete.

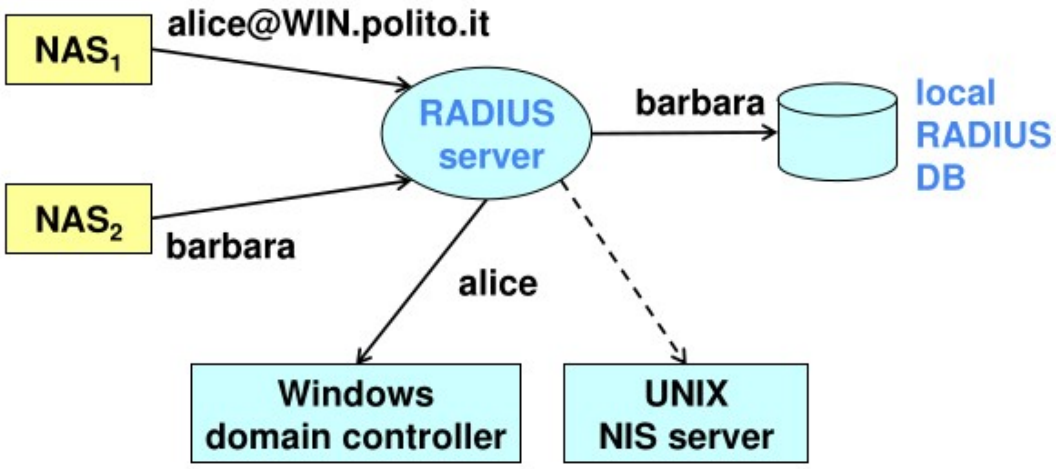
Le sue funzionalità si estendono sia alle porte fisiche, come quelle analogiche, ISDN e IEEE 802, che alle porte virtuali, compresi tunnel e accessi wireless, consentendo così la gestione centralizzata di una rete di punti di accesso. Il protocollo opera secondo uno schema client-server tra il Network Access Server (NAS) e il Server di Autenticazione (SA), utilizzando le porte 1812/UDP per l'autenticazione e 1813/UDP per l’accountability.

Poiché UDP non è affidabile, ogni trasmissione di un pacchetto RADIUS è soggetta a timeout. Se non viene ricevuto alcun ACK dopo il timeout, lo stesso pacchetto viene ritrasmesso e c'è un

numero massimo di appends dopo il quale la comunicazione viene dichiarata impossibile. RADIUS supporta anche la possibilità di configurare server secondari per migliorare le prestazioni e la resistenza del sistema, specie contro attacchi di tipo DoS.

RADIUS proxy

RADIUS può agire come proxy verso altri server di autenticazione. Nella figura, due NAS inviano richieste di accesso a RADIUS, il quale verifica nel suo database locale la validità dell'utente, ad esempio, Barbara.



Se la richiesta proviene da un altro NAS, magari tramite un indirizzo email come alice@WIN.polito.it indica che l'utente Alice non è registrato nel DB RADIUS locale, ma che Alice è un utente definito nel dominio di sicurezza WIN.polito.it a cui il server RADIUS è in qualche modo associato. Ciò significa che RADIUS agirà come proxy per la parte di autenticazione e reindirizzerà la richiesta al controller di dominio Windows. Quindi l'autorizzazione/contabilità potrebbe essere gestita localmente dal server RADIUS. RADIUS può anche essere associato a un altro dominio.

Which security functionalities for Radius?

Per garantire la sicurezza, RADIUS affronta diverse sfide, tra cui:

- ***Sniffing delle richieste NAS:** Rischio di compromissione della riservatezza delle password o violazione della privacy dell'utente.*
- ***Risposta AS falsa:** Possibilità di bloccare utenti validi o consentire l'accesso a utenti non validi. Necessità di autenticazione della risposta.*
- ***Modifica della risposta del SA:** Possibilità di alterare risposte valide in risposte non valide e viceversa. Richiede autenticazione e integrità delle risposte.*
- ***Riproduzione della risposta del SA:** Possibilità di riprodurre risposte non legate a richieste specifiche. Necessità di autenticazione e legame alle richieste del NAS.*
- ***Enumerazione delle password:** Possibilità di ottenere informazioni sulle password. Richiede autenticazione delle richieste del NAS.*

- ***DoS:*** *Attacchi con molte richieste da NAS falsi. La resistenza è proporzionale al numero di server secondari configurati.*

Protezione dei Dati in RADIUS

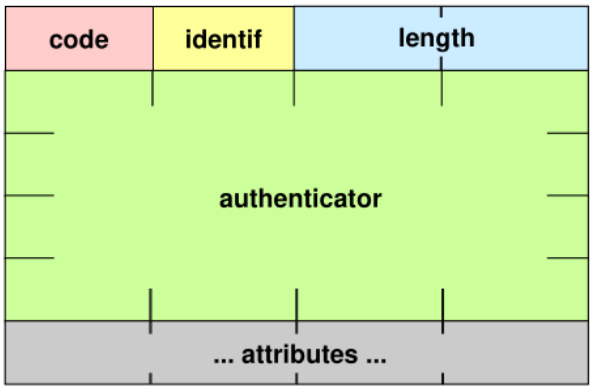
RADIUS implementa misure di protezione dei dati attraverso l'integrità dei pacchetti e l'autenticazione mediante keyed-MD5. Le chiavi condivise, definite come segreti tra il NAS e il server RADIUS, sono essenziali per garantire l'autenticità delle comunicazioni. I client sprovvisti di chiavi vengono ignorati. Nel caso in cui i pacchetti contengano una password, essa viene trasmessa "criptata" utilizzando l'algoritmo MD5, applicato dopo il padding con byte NULL per raggiungere una lunghezza multipla di 128 bit. Non si tratta di una crittografia, ma di un'operazione di digest.

$$\text{password} \oplus \text{md5}(\text{key} + \text{authenticator})$$

Autenticazione Utente in RADIUS

RADIUS supporta diversi metodi di autenticazione, tra cui PAP, CHAP, token-card e qualsiasi altro metodo EAP.

L'aspetto importante è che Radius è un protocollo estensibile, perché ogni pacchetto trasporta alcuni attributi descritti nella forma TLV (tipo di attributo - lunghezza - valore). Ciò consente l'introduzione di nuovi tipi senza interrompere la compatibilità.



Il formato di un pacchetto Radius è il seguente:

- Codice (8 bit);
- Identificatore (8 bit);
- Lunghezza (16 bit);
- Autenticatore (128 bit);
- Elenco TLV di attributi.

Tipi di Pacchetti in RADIUS

I pacchetti in RADIUS assumono vari tipi:

- **ACCESS-REQUEST:** Contiene le credenziali di accesso (es. username e password).
- **ACCESS-REJECT:** L'accesso è negato, ad esempio a causa di credenziali errate.
- **ACCESS-CHALLENGE:** Richiede ulteriori informazioni dall'utente, come un PIN, un codice token o una password secondaria.
- **ACCESS-ACCEPT (con parametri):** L'accesso è consentito, e vengono forniti i parametri di rete.

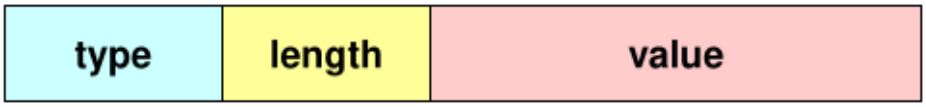
Autenticatore in RADIUS

L'autenticatore in RADIUS ha una duplice funzione:

- Nella richiesta inviata al server RADIUS maschera la password.
- Nella risposta creata dal server RADIUS fornisce autenticazione e protezione da attacchi di replay.

Nell'Access-Request, è denominato Request Authenticator e consiste in 16 byte generati casualmente dal NAS. Nell'Access-Accept/Reject/Challenge (risposte del server), è denominato Response Authenticator e viene calcolato tramite un digest MD5 utilizzando una chiave.

Alcuni Attributi in RADIUS



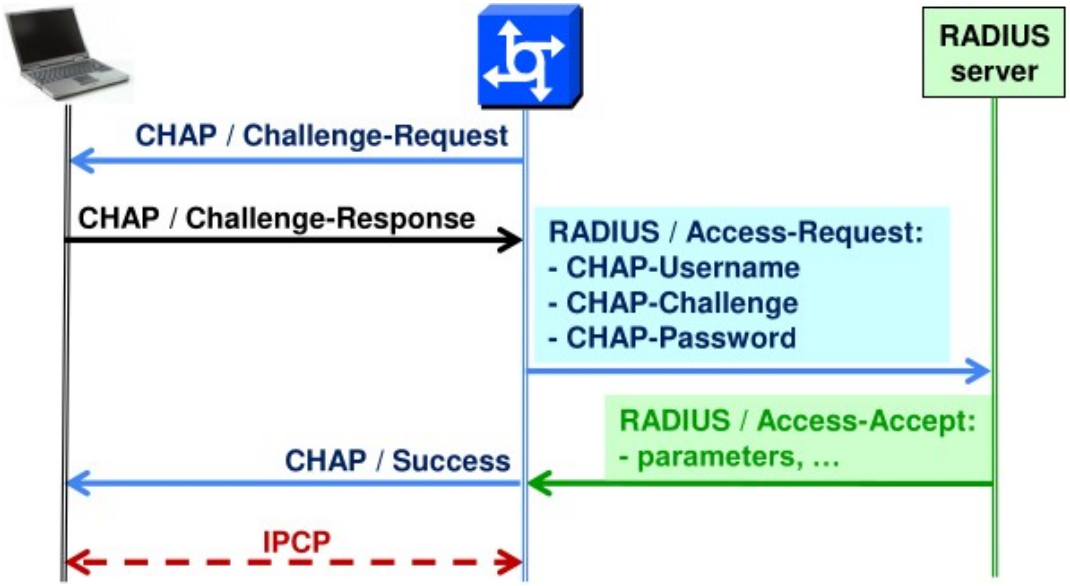
- **Tipo 1 (User-Name):** Il valore può essere una stringa di testo, un identificatore di accesso alla rete (NAI) o un Distinguished Name (DN).
- **Tipo 2 (User-Password):** Il valore è la password trasformata con MD5.
- **Tipo 3 (Chap-Password):** Il valore è la risposta CHAP dell'utente (128 bit).
- **Tipo 60 (CHAP-Challenge):** Il valore è la sfida lanciata dal NAS all'utente.

Network Access Identifier (NAI)

Il NAI distingue se la richiesta proviene da un utente locale o appartenente a un dominio di sicurezza diverso. Si presenta come "username[@realm]" e deve essere supportato fino a 72 byte.

Esempio di Integrazione CHAP e RADIUS

Per illustrare l'integrazione di CHAP e RADIUS, un utente, un NAS e un server RADIUS cooperano.



Nel processo di autenticazione, la Challenge Handshake Authentication Protocol (CHAP) e RADIUS collaborano per verificare l'identità dell'utente. Nella rappresentazione grafica, a sinistra si trova l'utente, al centro il Network Access Server (NAS), e a destra il server RADIUS.

1. **Inizio della Connessione:** Quando un utente si connette al sistema, il NAS invia un pacchetto CHAP contenente una richiesta di sfida all'utente. La sfida (CHAP-Challenge) è un valore generato casualmente dal NAS.
2. **Partecipazione dell'Utente:** L'utente inserisce la propria password e utilizza questa informazione per generare una risposta alla sfida (CHAP-Password). È fondamentale notare che il NAS non ha accesso alla password dell'utente e, di conseguenza, non può verificare direttamente la validità della risposta.
3. **Creazione del Pacchetto RADIUS:** Poiché il NAS non può verificare la risposta CHAP direttamente, crea un pacchetto di Accesso RADIUS che include tutte le informazioni necessarie per la verifica dell'autenticazione. Queste informazioni includono il CHAP-Username fornito dall'utente, la CHAP-Challenge inviata dal NAS e la CHAP-Password, che rappresenta la risposta dell'utente alla sfida.
4. **Verifica da Parte di RADIUS:** Il server RADIUS riceve il pacchetto di Accesso RADIUS e utilizza le informazioni fornite (CHAP-Username, CHAP-Challenge e CHAP-Password) per verificare se la risposta all'autenticazione è corretta o meno. Supponendo che la risposta sia valida, il server RADIUS procede con l'invio di una risposta di Accesso RADIUS positiva (Radius Access Accept).
5. **Traduzione in Pacchetto CHAP di Successo:** Confermata l'autenticità dell'utente, il server RADIUS invia una risposta positiva al NAS con i parametri di rete specifici per quell'utente. Questa risposta RADIUS viene tradotta dal NAS in un pacchetto CHAP di Successo, indicando che l'utente è stato autenticato con successo.
6. **Abilitazione del Livello 3 (IPCP):** Una volta ricevuto il Successo di CHAP, il NAS abilita il livello 3 della connessione, ad esempio, il Protocollo di Controllo dell'Indirizzo Internet (IPCP), permettendo all'utente di accedere alla rete.

IEEE 802.1x

IEEE 802.1X è uno standard di rete che definisce il controllo di accesso alla rete (NAC) e fornisce un meccanismo per l'autenticazione di dispositivi collegati a una rete. Il protocollo è ampiamente utilizzato per garantire l'accesso sicuro alle reti cablate e wireless.

Ecco una panoramica delle caratteristiche principali di IEEE 802.1X:

1. **Controllo di Accesso:** IEEE 802.1X è progettato per controllare l'accesso agli switch Ethernet o ai punti di accesso Wi-Fi in una rete. Prima che un dispositivo sia autorizzato ad accedere alla rete, deve superare una fase di autenticazione.
2. **Autenticazione:** Il protocollo prevede un processo di autenticazione, solitamente basato su protocolli come EAP (Extensible Authentication Protocol). Gli utenti o i dispositivi devono fornire credenziali valide per autenticarsi presso un server di autenticazione.

3. **Port-based Network Access Control (PNAC):** IEEE 802.1X opera a livello di porta, il che significa che il controllo di accesso è applicato alle porte di switch Ethernet o ai punti di accesso Wi-Fi. Le porte possono essere configurate in uno dei tre stati principali: non autenticato, autenticato o inattivo.
4. **Supplicant, Authenticator, Authentication Server:** Nel modello 802.1X, ci sono tre ruoli principali:
    - **Supplicant:** Il dispositivo che richiede l'accesso alla rete.
    - **Authenticator:** Il dispositivo di rete (switch o punto di accesso) che fa da intermediario tra il supplicant e il server di autenticazione.
    - **Authentication Server:** Il server che verifica le credenziali presentate dal supplicant e decide se consentire l'accesso.
5. **EAP over LAN (EAPOL):** IEEE 802.1X utilizza EAPOL per trasmettere i messaggi di autenticazione e controllo tra supplicant e authenticator.

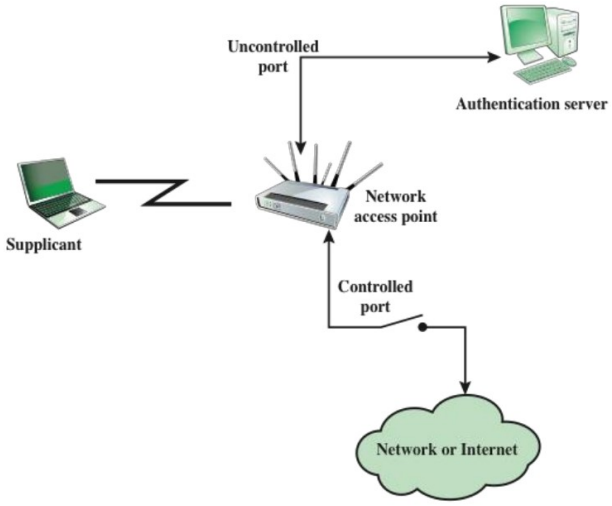
Radius e Diameter sono stati utilizzati per definire IEEE 802.1x, un'architettura più generale nota anche come Port-Based Network Access Control. È un'architettura di autenticazione che funziona su L2. Verifica l'identità e l'autorizzazione degli utenti prima di lasciarli comunicare. Può essere utile in una rete cablata per bloccare un accesso non autorizzato, ma è assolutamente necessario nelle reti wireless. Le prime implementazioni sono state immediatamente realizzate da Windows-XP e dagli access-point wireless Cisco.

IEEE 802.1x è un framework, il che significa che non impone una soluzione di autenticazione specifica, ma ne supporta molte. In particolare, è un framework per eseguire l'autenticazione e la gestione delle chiavi. Il secondo punto è necessario per le reti wireless, perché la parte radio di una comunicazione wireless può essere facilmente sniffata. Con la gestione delle chiavi è possibile definire una chiave simmetrica condivisa che può essere utilizzata per criptare il traffico. Può derivare chiavi di sessione da utilizzare per l'autenticazione, l'integrità e la riservatezza dei pacchetti. Utilizza algoritmi standard per la derivazione delle chiavi (ad esempio, TLS, SRP, ...) e dispone di servizi di sicurezza opzionali (autenticazione o autenticazione e crittografia).

802.1X access control: ports

Il controllo degli accessi 802.1X opera attraverso i concetti di "uncontrolled port" (porta non controllata) e "controlled port" (porta controllata). Questi termini si riferiscono alle porte di un dispositivo di rete, come uno switch, che sono soggette al processo di autenticazione.

Durante la fase di avvio, una porta 802.1X è in uno stato controllato e disabilitato. Solo i messaggi di autenticazione sono permessi sulla porta non controllata, limitando la comunicazione del supplicant. Dopo l'autenticazione riuscita, la porta controllata diventa abilitata, consentendo al supplicant di interagire pienamente con altri dispositivi sulla rete. Questo approccio aiuta a garantire che solo dispositivi autorizzati abbiano accesso completo alla rete e che l'accesso sia negato fino a quando l'autenticazione non è completata con successo.



1. **Uncontrolled Port**:
   - **Stato**: Sempre abilitato (enabled), ma con alcune limitazioni.
   - **Funzione**: Consente solamente lo scambio di messaggi relativi all'autenticazione tra il supplicant (dispositivo utente che cerca l'accesso alla rete) e il server di autenticazione (AS, Authentication Server).
   - **Scopo**: Fornire un canale di comunicazione ristretto che consente al supplicant e al server di autenticazione di negoziare e completare il processo di autenticazione. Questo significa che, prima di completare con successo l'autenticazione, il supplicant può comunicare solo in modo limitato.
2. **Controlled Port**:
   - **Stato**: Inizialmente disabilitato (disabled).
   - **Funzione**: Impedisce lo scambio di frame di dati con il resto della rete.
   - **Scopo**: Garantire che nessuna comunicazione dati avvenga sulla porta fino a quando il supplicant non ha superato con successo il processo di autenticazione. Dopo un'autenticazione riuscita, la porta controllata viene abilitata, consentendo al supplicant di comunicare liberamente con altri sistemi sulla rete.

IEEE 802.1X

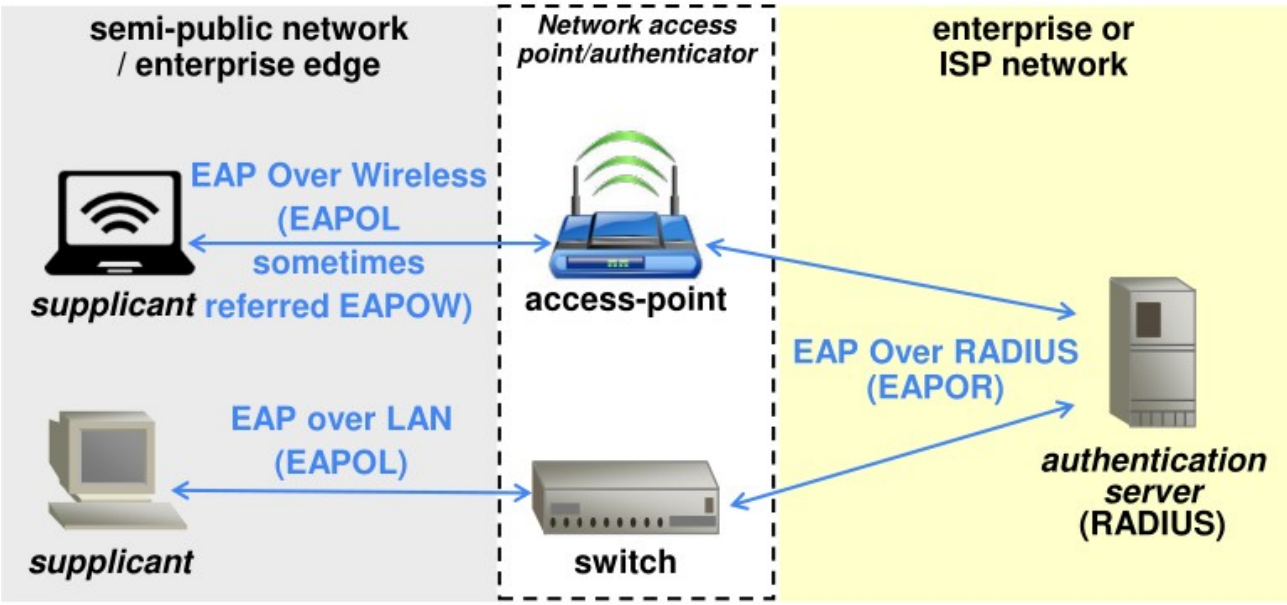
IEEE 802.1X fornisce un framework completo per l'autenticazione e la gestione delle chiavi nelle reti. Questo framework consente ai dispositivi di comunicare attraverso sessioni sicure, utilizzando chiavi di sessione derivate durante il processo di autenticazione.

Il protocollo permette la derivazione di chiavi di sessione, che vengono utilizzate per garantire l'autenticità, l'integrità e la riservatezza dei pacchetti scambiati tra i dispositivi e il server di autenticazione. Questo processo di derivazione delle chiavi coinvolge algoritmi standard ben noti, come TLS e SRP, assicurando un alto livello di sicurezza.

Un aspetto distintivo di IEEE 802.1X è la flessibilità offerta attraverso l'implementazione di servizi di sicurezza opzionali. Gli utenti possono scegliere se utilizzare solo l'autenticazione o aggiungere

anche la crittografia per ulteriori livelli di protezione. Questa caratteristica consente alle reti di adattarsi alle esigenze specifiche di sicurezza, consentendo una personalizzazione del livello di protezione in base alle esigenze dell'ambiente di rete.

802.1X typical use



Nell'illustrazione viene presentata la rappresentazione di una rete semi-pubblica o dell'enterprise edge, che costituisce l'ambiente in cui si trovano i dispositivi desiderosi di accedere alla rete, noti come supplicant. L'elemento che funge da interfaccia tra questa rete periferica e quella centrale è chiamato authenticator o etherNAS. Questo elemento può assumere la forma di un access point, uno switch o un dispositivo simile.

Gli utenti supplicant hanno diverse modalità di connessione a questo authenticator, che rappresenta il punto di accesso alla rete. In particolare, il protocollo 802.1X fa uso dell'Extensible Authentication Protocol (EAP) per gestire il processo di autenticazione. A seconda se tale autenticazione avvenga su una rete wireless o cablata, si denominerà rispettivamente EAP Over Wireless (EAPOW) o EAP Over LAN (EAPOL).

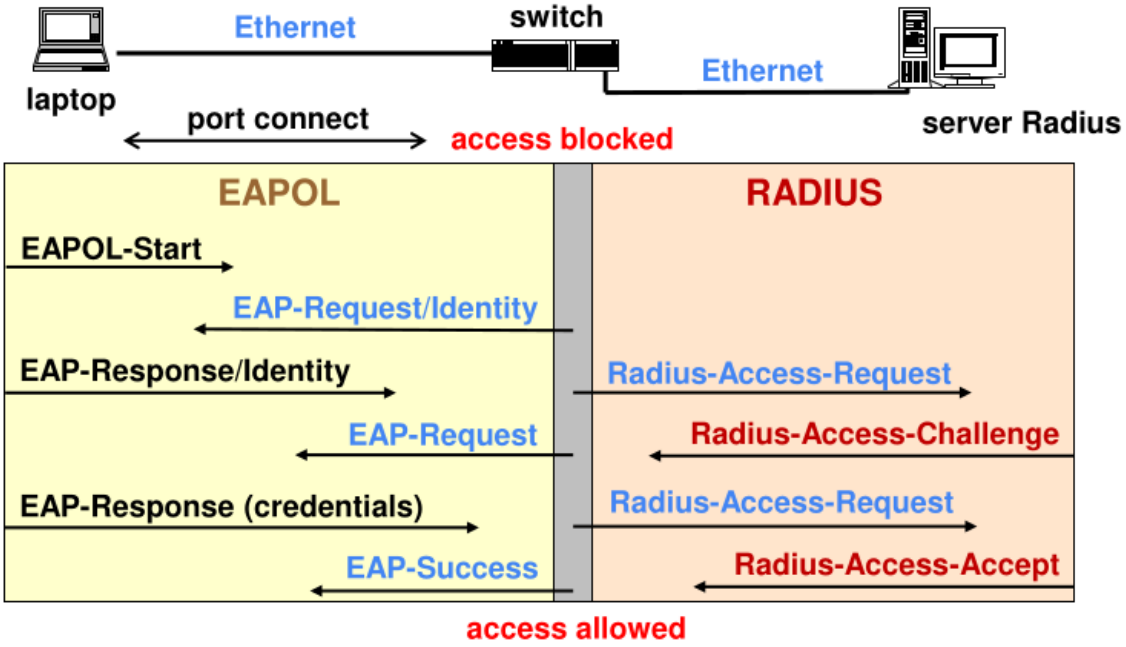
Quando un supplicant invia una richiesta EAP all'authenticator, quest'ultimo verifica la validità di tale richiesta attraverso il processo di decapsulazione e ricapsulazione del pacchetto in un protocollo diverso, tipicamente Radius. Nel retroscena, viene menzionato l'utilizzo di EAP Over Radius (EAPOR) per ulteriori verifiche sulla validità dell'utente.

In breve, l'illustrazione rappresenta la dinamica di connessione tra i dispositivi supplicant e l'authenticator, sottolineando l'uso di EAP per l'autenticazione e introducendo le varianti EAPOW ed EAPOL a seconda del tipo di rete utilizzata. La validità dell'utente viene verificata attraverso il processo di autenticazione che coinvolge anche il protocollo Radius.

802.1x - advantages

Sfrutta il livello applicativo per l'effettiva implementazione dei meccanismi di sicurezza. Esiste un dialogo diretto tra supplicante e AS (server di autenticazione), quindi i dispositivi utente parlano direttamente con il server Radius. La scheda di rete (NIC) e il NAS funzionano come "dispositivo passante", ossia si limitano all'incapsulamento e al decapsulamento. Questo è importante perché non sono necessarie modifiche (a livello di NIC e NAS) per implementare nuovi meccanismi di autenticazione. Questi meccanismi devono essere implementati solo su Radius Server e Supplicant. Questo è importante perché questa architettura di sicurezza non deve cambiare anche se in futuro ci sarà un'evoluzione delle tecniche di autenticazione. Infine, poiché utilizza Radius, questo sistema si integra perfettamente nelle architetture AAA che consentono anche l'accounting.

802.1X – messages (via ethernet)



Nel seguente esempio di autenticazione utilizzando l'architettura 802.1X, un portatile è collegato tramite Ethernet a uno switch. Di default, tutte le porte Ethernet dello switch sono bloccate. Il processo di autenticazione inizia quando il supplicant, ovvero il dispositivo utente, avvia una negoziazione attraverso un messaggio chiamato EAPOL-Start.

In risposta, lo switch invia una richiesta/identità EAP al supplicant, il quale fornisce la propria identità attraverso una risposta/identità EAP. Questa informazione viene poi inoltrata al server Radius tramite una richiesta di accesso Radius dallo switch, configurato come un elemento di passaggio in questo contesto.

Il server Radius risponde con una sfida attraverso il pacchetto Radius-Access-Challenge. Lo switch, fungendo da dispositivo pass-through, traduce i messaggi EAP in protocollo RADIUS e viceversa, mantenendo una connessione end-to-end. Il pacchetto Radius-Access-Challenge viene poi tradotto in un pacchetto EAP-Request dallo switch.

Il supplicant risponde nuovamente con un pacchetto contenente la risposta alla sfida, il quale viene tradotto in un'altra richiesta di accesso Radius dallo switch. Il server Radius, a questo punto, accetta l'utente, e lo scambio di informazioni si conclude con l'invio di un pacchetto EAP-Success al supplicant.

Ora, l'utente autenticato è in grado di comunicare con le reti di livello 3 e superiori, avendo superato con successo il processo di autenticazione secondo l'architettura 802.1X.

eduroam

L'esempio di utilizzo di RADIUS più significativo è la rete Eduroam, una rete globale di controllo degli accessi coinvolgente università e centri di ricerca in tutto il mondo. Eduroam utilizza il protocollo 802.1X e la federazione RADIUS.

Nel contesto di Eduroam, un supplicant rileva un access point in un'università e si connette ad esso, denominato Eduroam. L'access point si riferisce al server di autenticazione (AS) locale, noto come visit AS. Il supplicant utilizza il proprio identificatore (ad esempio, s123456@studenti.polito.it) tramite la sintassi Network Access Identifier (NAI). Il server RADIUS locale sa di dover attraversare la gerarchia Eduroam, nazionale o internazionale, fino a raggiungere il Radius AS in cui il supplicant ha creato le sue credenziali, come il PoliTO Radius Server, chiamato Home AS.

Una volta individuato l'Home AS, si stabilisce una connessione diretta tramite un canale virtuale sicuro End-to-End (ad esempio, EAP-TTLS) tra il supplicant e l'Home AS per eseguire l'autenticazione. Quest'ultimo fornisce la risposta all'access point, consentendo all'utente di navigare sulla rete in modo sicuro. In sintesi, Eduroam sfrutta il protocollo RADIUS e 802.1X per consentire agli utenti di connettersi in modo sicuro e affidabile alle reti di istituzioni accademiche e di ricerca in tutto il mondo.