Mengenal Protocol Sistem Keamanan

Deris Stiawan
Fakultas Ilmu Komputer UNSRI

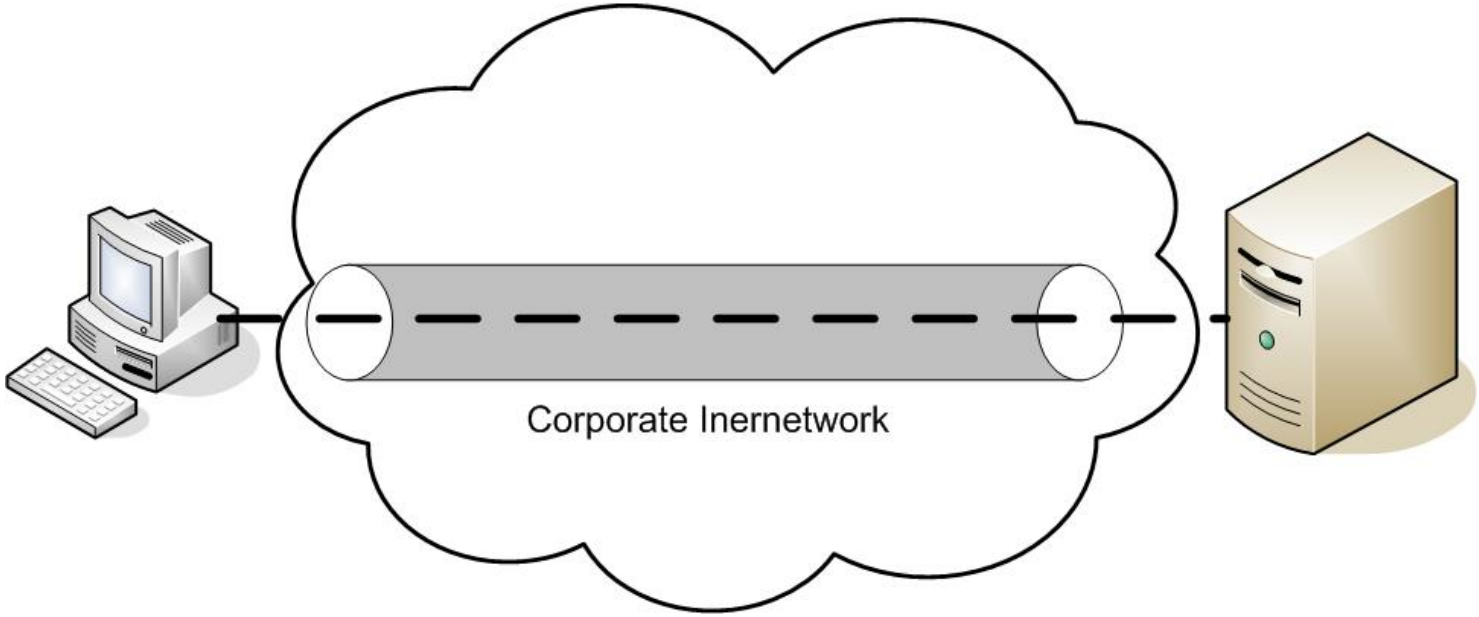
Pendahuluan

- Dibutuhkan suatu metode pengamanan sistem dari sisi hardware dan software
- Metode di software (otentikasi user DB)
- Metode transfer / komunikasi melewati suatu media transmisi jaringan publik / private
- Keseimbangan “dunia undeground” dan “sistem keamanan”
- Metode keamanan selalu diperbaharui dan muncul metode-metode baru

Tunneling Method

- Metode “Tunneling” membuat “Terowongan khusus” untuk membungkus protocol lainnya.
- Biasa digunakan untuk solusi komunikasi data yang lewat di jaringan publik seperti Virtual Private Network (VPN)
- Tunneling melakukan proses encapsulasi, transmisi dan decapsulasi paket yang dikomunikasikan

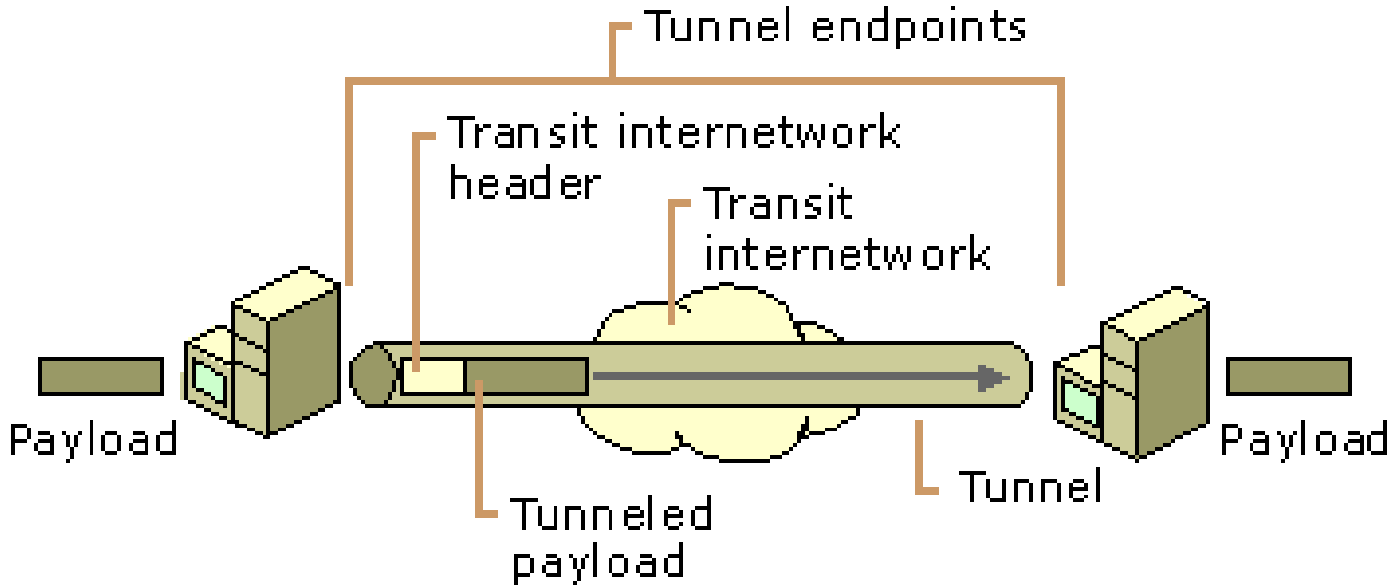
- Contoh protocol Tunneling
  - *PPP (Point to Point Protocol) Based*
    - PPTP (Point to Point Tunneling Protocol)
    - L2TP (Layer 2 Tunneling Protocol



Tunneling

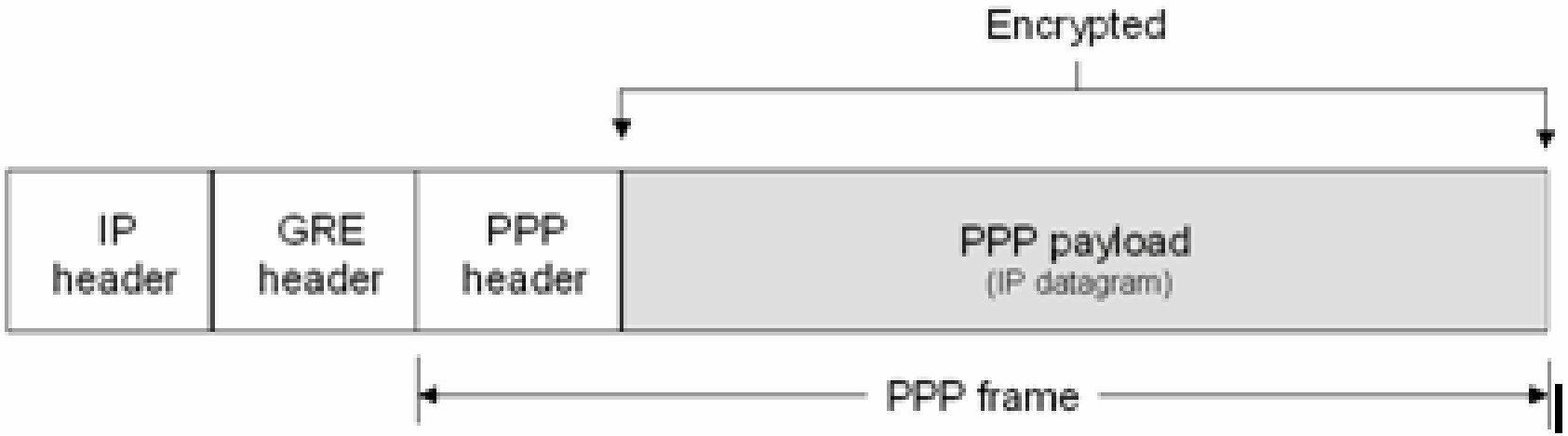
- Untuk dapat terbentuk “Terowongan” antara client dan server harus menggunakan protocol tunneling yang sama
- Biasa di layer 2 dan layer 3. menggunakan frames untuk exchange
- PPTP dan L2TP berada di layer 2 Tunneling. pembungkusan keduanya menggunakan payload pada **Frame** PPP untuk dikirim ke network
- IPSec adalahTunneling di layer 3 network yang menggunakan **packet** dengan memberikan IP Header sebelum dikirim ke network

- Intinya, memungkinkan koneksi established yang dibangun PPP akan tetap aman walaupun di attack karena data di enkripsi oleh L2TP/IPSec.



PPTP **(point to point tunneling protocol)**

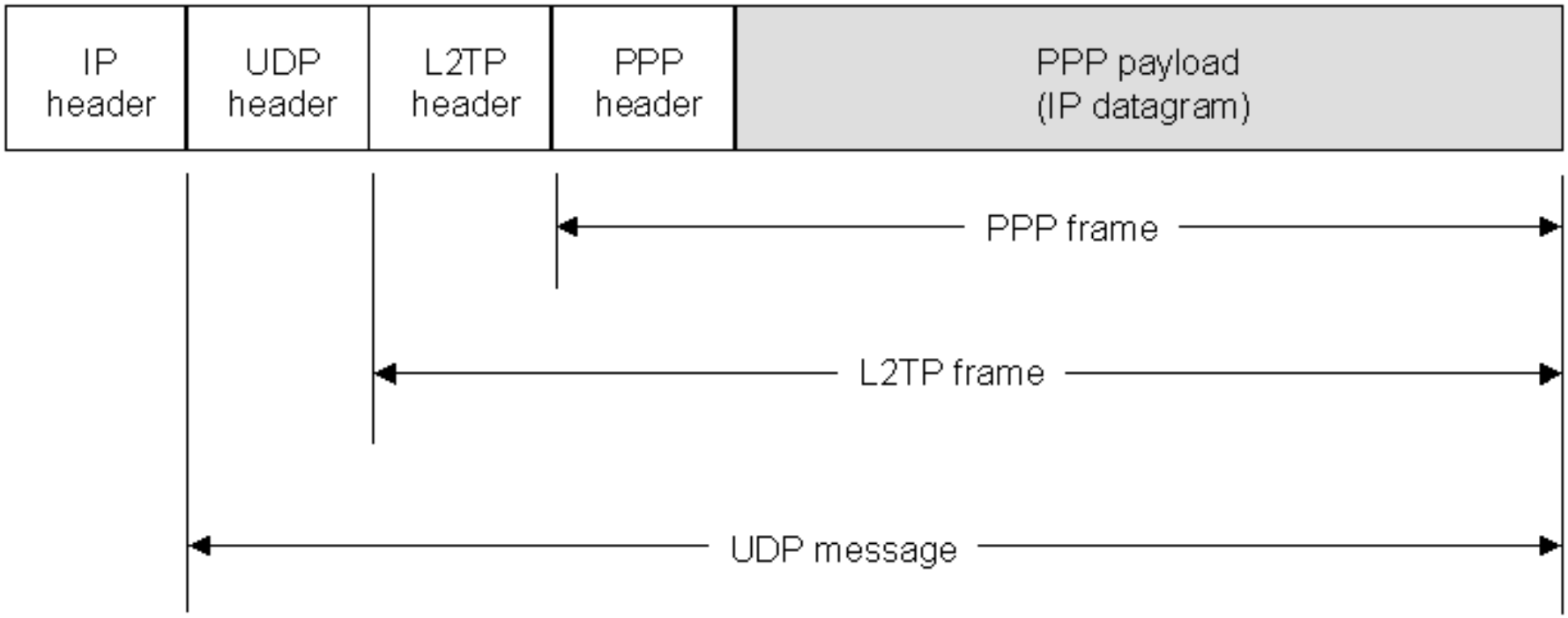
- Memungkinkan membawa traffic IP, IPX, NetBEUI untuk di enkripsi dan dibungkus dengan IP Header untuk dikirimkan ke network
- PPTP membungkus frame PPP
- Menggunakan Koneksi TCP untuk manajemen tunnel dan membungkus frame PPP untuk mentunnel data.
- Payloads dari encapsulasi frame PPP dapat di enkrip dan dekrip

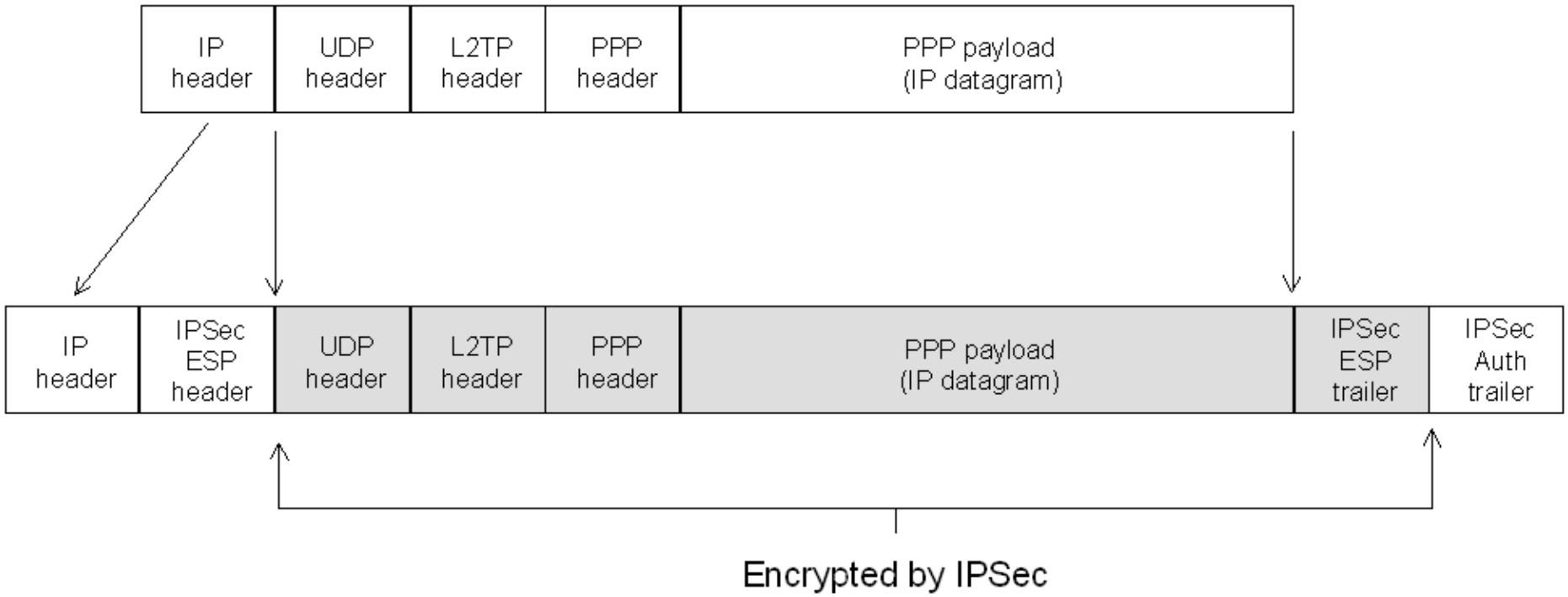

Encrypted
IP header
GRE header
PPP header
PPP payload
(IP datagram)
PPP frame

L2TP **(Layer 2 Tunneling Protocol)**

- Membuat “koneksi session (layer 5)” secara virtual di sebuah komunikasi data
- L2TP adalah kombinasi dari PPTP dan L2F (standar cisco)
- Biasa menggunakan port 1701 dengan protocol UDP untuk mengirimkan L2TP encapsulated PPP frames sebagai data yang di tunnel
- Terdapat penambahan payload dan L2TP Header
- L2TP membungkus frame PPP untuk dikirim lewat Jaringan IP, X.25, Frame Relay atau ATM
- Biasanya dikombinasikan dengan IPSec (metode enkripsinya) yang dikenal L2TP/IPSec (RFC 3193 & 2661)

- Payloads dari encapsulasi frame PPP dapat di enkrip dan dekrip
- Dua titik Tunnel L2TP disebut LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server)
- Pada saat tunnel terbuat, trafic di jaringan baru melakukan koneksi
- LAC / LNS melakukan sessions pada saat koneksi terjadi, traffic antar session ini di batasi oleh L2TP


IP header
UDP header
L2TP header
PPP header
PPP payload (IP datagram)
PPP frame
L2TP frame
UDP message


IP header
UDP header
L2TP header
PPP header
PPP payload (IP datagram)
IP header
IPSec ESP header
UDP header
L2TP header
PPP header
PPP payload (IP datagram)
IPSec ESP trailer
IPSec Auth trailer
Encrypted by IPSec

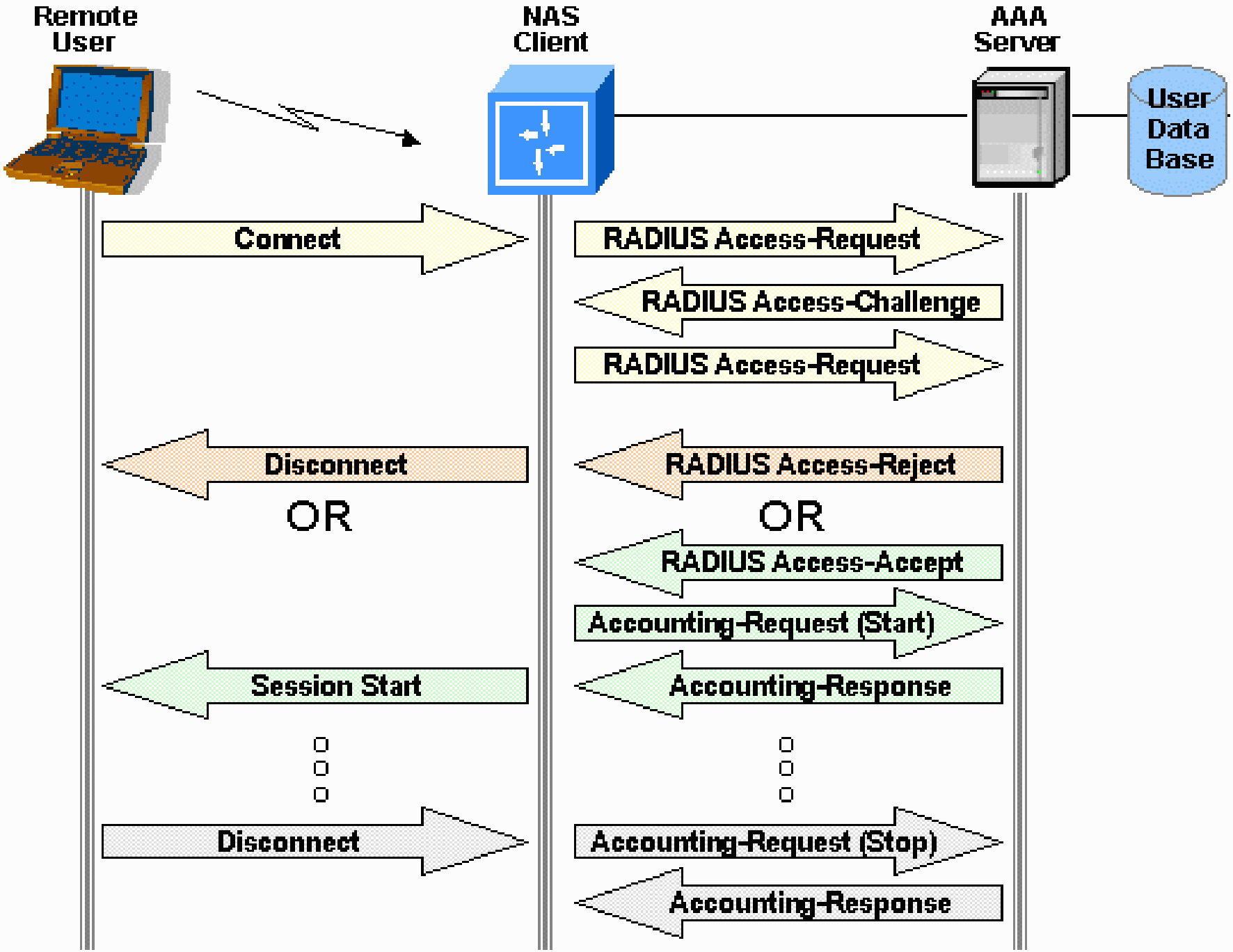
RADIUS

- Remote Access Dial In User Services,
- Sebuah network protocol yang digunakan untuk membuat manajemen akses secara terkontrol pada sebuah jaringan yang besar
- Biasa digunakan oleh perusahaan untuk mengatur akses ke internet atau internal bagi karyawan / pelangganya
- RADIUS menggunakan konsep AAA (Authentication, Authorization, Accounting)

- Protocol RADIUS tidak mengirimkan password cleartext antar NAS dan RADIUS server (bahkan jika menggunaakn PPP)
- Dalam berbagi kunci menggunakan algoritma hashing MD5 dan dibungkus dengan tunnel IPSec
- Ada banyak vendor h/w dan s/w yang menimplementasikan RADIUS sebagai solusi otentikasi user

- Berbasis UDP Protocol
- Bisa ditempatkan dimana saja di internet dan dapat membuat otentikasi (PPP PAP, CHAP, MS-CHAP, EAP) antara NAS dan server
- RADIUS menggunakan RAS Secure ID untuk membuat otentikasi yang kuat dalam pengontrolan akses

- Menggunakan UDP port 1812 (RADIUS authentication) dan port 1813 untuk RADIUS Accounting, namun ada juga vendor yang menggunakan port 1645 / 1646 (cisco) dan 1645 / 1646 (juniper)


Remote User
NAS Client
AAA Server
User Data Base
Connect
RADIUS Access-Request
RADIUS Access-Challenge
RADIUS Access-Request
Disconnect
OR
RADIUS Access-Reject
OR
RADIUS Access-Accept
Accounting-Request (Start)
Session Start
Accounting-Response
Disconnect
Accounting-Request (Stop)
Accounting-Response

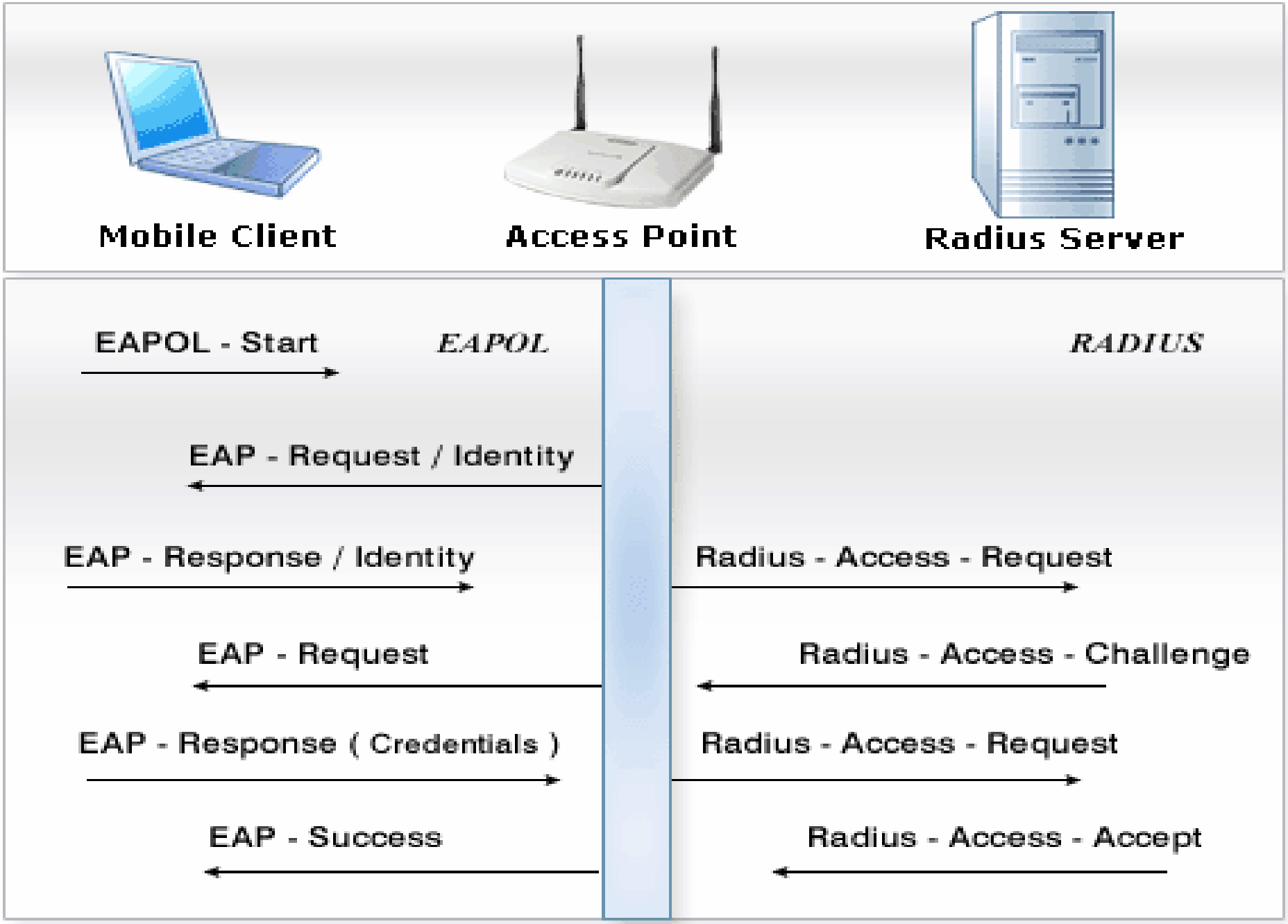
PROTOCOL lainnya

- Extensible Authentication Protocol (EAP)
- IPSec Internet key Exchange (IKE)
- Network Control Protocol (NCP)
- Microsoft Point to point compression (MPPC)
- Microsoft point to point encryption (MPPE)
- Password Authentication Protocol (PAP)
- Challenge-Handshake Authentication Protocol (CHAP)
- Microsoft CHAP (MS CHAP)
- GRE (Generic Routing Encapsulations)

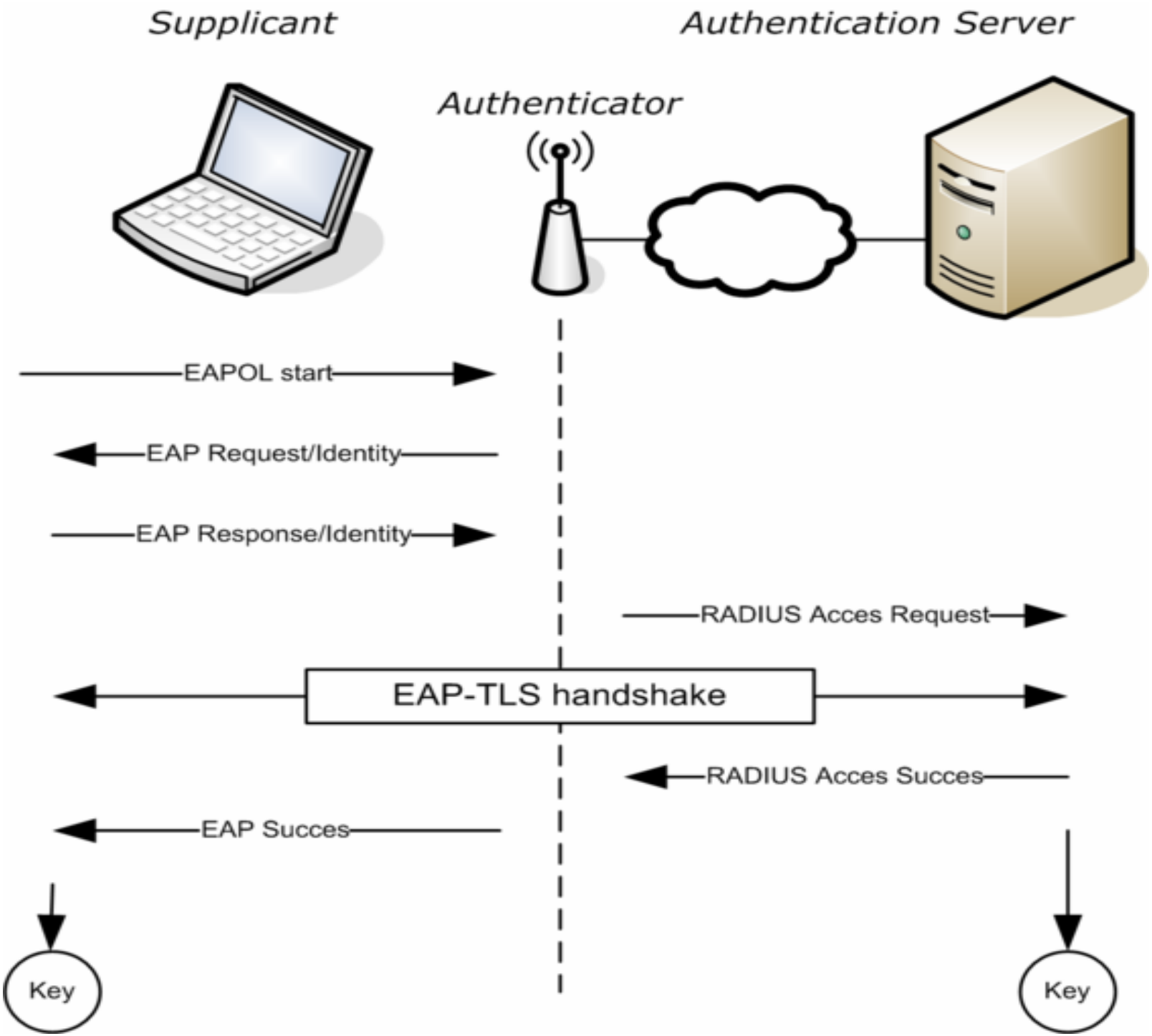
Extensible Authentication Protocol (EAP)

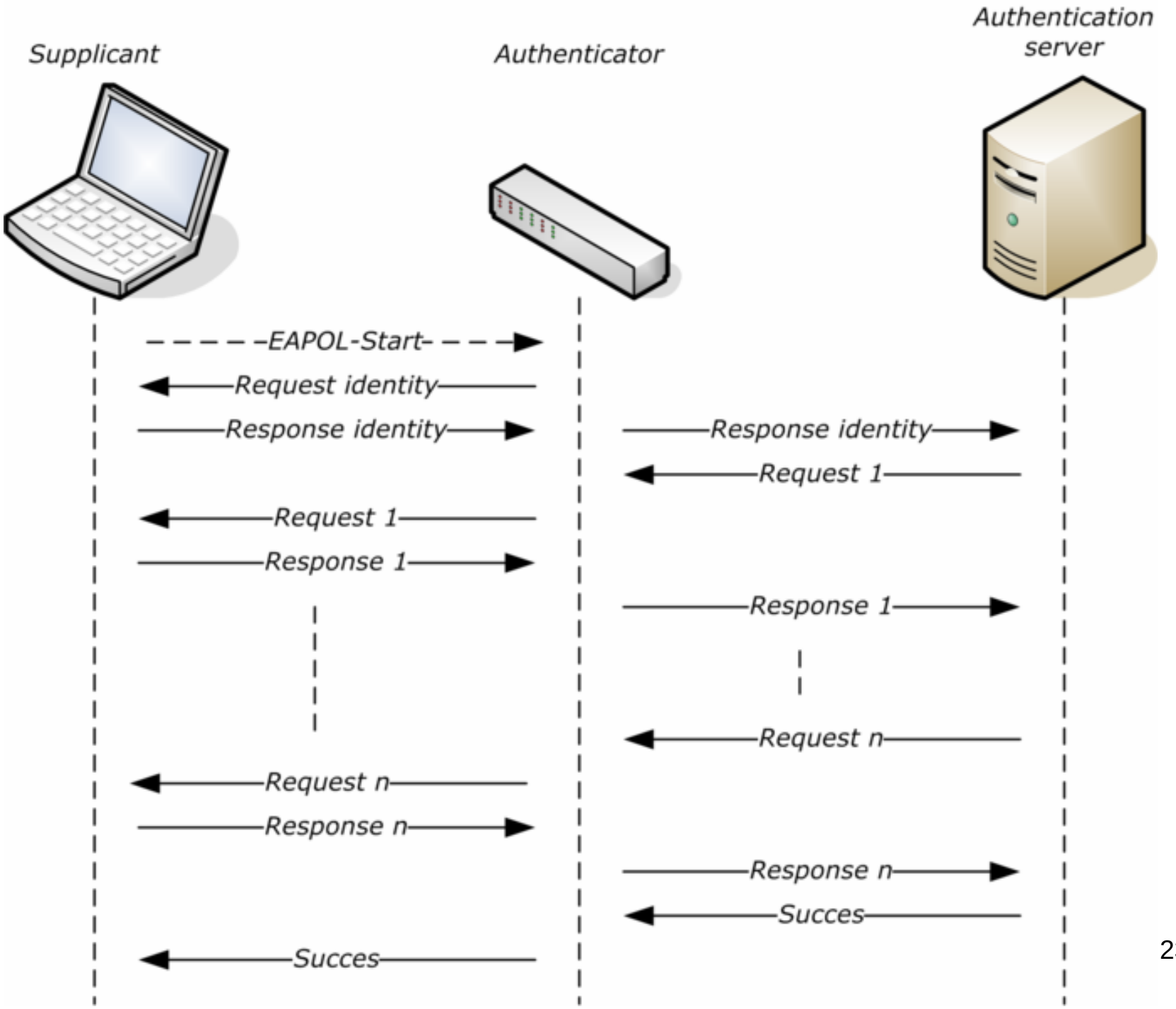
- Mengatasi kelemahan otentikasi pada metode PPP
- Biasa digunakan di jaringan wireless dan koneksi PPP
- Standar IETF untuk PPP dapat melakukan mekanisme otentikasi pada koneksi validasi PPP.
- Didesign untuk mengikuti kondisi dinamik dari otentikasi module plug-in pada kedua ujung koneksi client dan server
- EAP memungkinkan vendor untuk dapat membuat fleksibel yang tinggi pada metode otentikasi yang unik dan variasinya
  - OTP,
  - cryptographic calculators,
  - smart cards
  - Token card passing
- EAP di dokumentasikan RFC 2284 dan didukung penung Windows Server 2003 dan Windows XP.
- RFC 3746

- EAP adalah Frame otentikasi. Membuat beberapa fungsi dan dapat bernegoisasi.
- Ada banyak mekanisme yang digunakan seperti (standar ISTF)
  - EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, and EAP-AKA,
  - Pada wireless include EAP-TLS, EAP-SIM, EAP-AKA, PEAP, LEAP and EAP-TTLS.
  - RFC 4017.
- EAP bukan protocol cable, EAP hanya mendifinisikan bagaimana format pesan tsb.
- Lebih lanjut : http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol



http://manageengine.adventnet.com/


Supplicant
Authentication Server
Authenticator
EAPOL start
EAP Request/Identity
EAP Response/Identity
RADIUS Acces Request
EAP-TLS handshake
RADIUS Acces Succes
EAP Succes
Key
Key


Supplicant
Authenticator
Authentication server
EAPOL-Start
Request identity
Response identity
Response identity
Request 1
Request 1
Response 1
Response 1
Request n
Request n
Response n
Response n
Succes
Succes

IPSec

- IP Security Protocol, sebuah framework open standar yang membuat tentang confidentiality, data integrity, dan data otentikasi antara client dan server yang terhubung.
- Bekerja di layer 3.
- Biasanya menggunakan IKE (internet Key Exchange) untuk menangani masalah protocol yang bernegoisasi dan algoritma yang sesuai dengan policy yang dibuat
- IKE juga membuat metode enkripsi dan kunci otentikasi yang akan digunakan oleh IPSec
- RFC 2401

- IKE, sebuah protocol hybrid yang diimplemetasikan pada Internet framework Association and Key Management Protocol (ISAKMP)
- IKE yang membuat otentikasi di koneksi dengan IPSec, bernegoisasi dengan association keamanan IPSec, dan established kunci IPSec
- RFC 2409
- Komponen kripto yang bisa digunakan didalam IKE
  - DES
  - 3DES
  - CBC (cipher block chaining)
  - Diffe-Hellman
  - MD5
  - SHA
  - RSA Signature

- Implementasi IKE dapat digunakan dengan protocol RADIUS / TACACS+
- ISAKMP, sebuah framework protocol yang mendefinisikan format payloads, mekanisme implementasi kunci pertukaran protocol, dan bernegoisasi pada sistem keamanan

- Kelebihan mengapa IPSec menjadi standar
  - Mengenkripsi trafik (tidak bisa dibaca dan dibajak)
  - Memvalidasi integritas data (agar tidak dapat dimodifikasi di tengah jalan)
  - Mengotentikasi hubungan (memastikan trafik dari koneksi yang terpecaya
  - Anti-replay (melindungi sesion dari serangan replay)

Password Authentication Protocol (PAP)

- Sangat simple, skema otentikasi yang clear text (unencrypted).
- Network Access Server (NAS) request user name & pass, dan PAP mengembalikannya dengan clear text
- Sangat tidak secure karena bisa di attack dan tidak ada proteksi sama sekali

Challenge-Handshake Authentication Protocol (CHAP)

- CHAP mekanisme otentikasi yang di enkripsi untuk melindungi user & pass
- CHAP adalah mekanisme otentikasi menggunakan server PPP untuk memvalidasi user remote pada saat 3-way hanshake
- NAS mengirimkan challenge, yang mana terdiri dari Session ID dan challenge string ke remote client.
- Pada Remote client harus menggunakan **Algoritma MD-5 one-way hashing** untuk mengembalikan user name dan kunci hash dari challenge, session ID dan client password tadi, tetapi user name dikirimkan plain text
- RFC 1994

Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP)

- MS-CHAP adalah mekanis otentikasi yang dienkripsi yang sama dengan CHAP.
- Pada CHAP, NAS mengirimkan challege, dengan session ID dan string challenge kepada remote client
- Remote client harus mengembalikan user name dan enkripsi dari challenge string sebelumnya, session ID dan MD5 password hash.
- MS-CHAP juga membuat tambahan error codes, termasuk sebuah password expired code, dan tambahan pesan enkripsi client-server yang memungkinkan user untuk menukar password pada saat proses otentikasi
- Pada MS-CHAP, client dan NAS bebas untuk mengenerate beberapa inisial kunci enkripsi untuk tukar menukar data enkripsi oleh MMPE (Microsoft Point-to-Point Encryption)